Digital Instrumentation and Control Systems for Research Reactors

Second Part

EDITORIAL NOTE

CONTENTS

INTRODUCTION TO THE SUPPLEMENTARY FILES

These supplementary files are the second part of the publication and contain examples of different new and upgraded digital I&D projects conducted at different research reactors. These contributions provide a variety of project descriptions and concentrate on different aspects of the projects. The International Atomic Energy Agency (IAEA) is not responsible for the content of the Member State's reports, and all questions should be directed to the individual authors or organizations. The papers were presented in three technical meetings held at IAEA Headquarters in Vienna on May 2012, July 2017 and July 2019.

MODERNIZATION OF INSTRUMENTATION AND CONTROL SYSTEMS IN NUCLEAR RESEARCH REACTORS

A. AVILA – D. DELBIANCO – A. VIDAL
Instrumentation & Control Department, INVAP S.E.
Av. Luis Piedrabuena 4950, San Carlos de Bariloche, Río Negro, Argentina

IAEA Technical Meeting (EVT1803985) on Digital Instrumentation and Control Systems for Upgrades and New Research Reactors, Vienna, Austria; 1–5 July 2019

ABSTRACT

The Instrumentation and Control (I&C) systems have an important role in the safe operation of Research Reactors (RR). The modernization of the I&C systems could be driven by an undesired reason such as equipment ageing or the obsolescence of the systems. However, the modernization could be driven by an Improvement of the plant such as the improvement of Human Machine Interface (HMI) and automation or the re-utilization of the RR to radio-isotopes production.

The replacement of the I&C systems allows the implementation of state of the art technology complying with current standards thus improving safety, availability, operation and maintenance of the reactor and associated facilities.

This paper presents ways to replace the I&C systems partially or totally adapting them to an existing reactor.

The replacement of the Reactor Protection System (RPS) is presented in a flexible and compact design being able to adapt to the existing logic. The RPS technology options are analysed: based on hardwired technology, based on fully digital technology and based on hardwired & digital technology.

The replacement of the Reactor Control and Monitoring System (RCMS), based on a SCADA platform allows the operators to interact with the plant in a simple and versatile way. The RCMS technology options are Programmable Logic Controller (PLC) or Distributed Control System (DCS).

The replacement of the reactor control console presents improvements in HMI and human factors. The new design preserves the visual appearance and the operability of the original console implementing modern features.

1. INTRODUCTION

The term "I&C modernization" is used to explain the planned changes in I&C systems and components. These changes are the replacement (partially or totally) of the existing I&C systems, the addition of new I&C systems (e.g. post-accident systems) or the addition of new instrumentation loops to the existing systems.

The benefits of a modernization in I&C systems are unquestioned. New technologies provide the opportunity to improve the plant performance and reliability.

However, it must be considered the economic investment and the time that takes the modernization. As a major change in the reactor, the licensing authorization process shall be considered.

Additionally, it shall be considered that during the installation of the new systems, unforeseen events may arise producing deviations in the project such as underestimate the feasibility of the installation or damage caused by the manipulation of existing components. In both cases this could generate extra costs and/or delays. From the project management point of view, there is more uncertainty in the modernization of an existing reactor than in the installation of I&C in a new reactor.

2. REASONS FOR MODERNIZATION

The decision to carry out a process of modernization of the I&C are generally framed in one of the reasons:

Update to new requirements or safety regulations

As the requirements may have been changed from the requirements that were valid when the plant was built, it may be necessary to establish new licensing requirements.

The general requirements, usually issued by the licensing body or authority of the country, are established to improve the safety of the plant and to be able to modify the plant so that it can meet current safety standards.

One of the differences between the RR prior to the decade of 1990s is the marked division between the safety systems and the safety related systems, mainly the separation between the RPS and the RCMS.

Improvement of HMI and automation

When the installation of new digital I&C equipment is planned, a change of the balance between automation and human actions should be considered. Due to technical and operational factors, it may be desirable to increase the level of automation to improve safety and plant availability and also for maintenance. This can be done in an easier and more cost-effective manner than before due to the capabilities of modern supervision technology.

The advance in control and information technology makes possible to present information to operators in the control room in better and more friendly ways. This feature has a direct improving efficiency in the operator's actions and responses during the operation of the plant.

Re-utilization of the Research Reactor

The re-utilization of the reactor changing its purpose, for example from a research and training reactor to a production of radio-isotopes reactor is a major change that requires the study and modification of most of the process systems. This change may require the increase of reactor power. In any case the re-utilization of the reactor is a separated case study not included in this publication. The I&C systems shall be modified as part of this process.

Addition of new instrumentation loops

New regulations and requirements may require to add more measurements either for safety systems or for the safety related systems increasing this way the safety margins and providing more supervision and automation. In this case, a complete instrumentation loop is installed, considering new detectors, transmitters, wiring, logic intervention and modification of the HMI on the console.

Upgrade the post-accident instrumentation

Nowadays, it can be assured that all reactors have reliable safety systems that will shut down the reactor in a reliable manner. Nevertheless, the focus of new requirements may demand to update the Post Accident System (PAM).

As specified in reference [3], the PAM should be an independent system from the RPS and the RCMS.

“3.6. The instrumentation and control system architecture should:

(a) Implement a defence in depth concept. For instrumentation and control, defence in depth includes implementing successive instrumentation and control functions designed to limit the consequences of a postulated initiating event despite the failure of the instrumentation and control functions designed to respond first.

(b) Not compromise the strategy to meet the defence in depth concept of the facility design.”

The addition of a completely new PAM could be a significant economic investment. Therefore, the addition of instrumentation declared for post-accident could be an option for smaller RR. This instrumentation should be as independent as possible from the other systems.

Equipment ageing

The degradation of the performance or dependability of I&C equipment with time is understood by ageing. This degradation is due to physical mechanisms inherent to materials component and linked to the I&C equipment design, assembly and functional characteristics. It is influenced by the stresses from the equipment environment and from the equipment operation.

Some examples of stress factors, ageing mechanisms, and ageing effects are given as follows:

High temperature environments, high humidity environments, contact with water or chemicals, vibration and mechanical shock, exposure to radiation, wear-out of semiconductor components, operation of electronic components above specified maximum supply voltage, repeated maintenance operations entailing the withdrawal/reinsertion of electronic cards.

It is important to address the I&C ageing issues in terms of plant life management and license renewal not only for normal operation but also, and more importantly, for the response of the safety systems during and after the Design Basis Events (DBE).

At the end of the I&C equipment lifetime the failure rate of the component and hence the I&C equipment or system becomes greater ("bathtub" reliability curve). The reliability is no longer statistically predictable and hence the equipment becomes undependable.

Equipment is qualified to operate for a limited period of time. After this period expired, the manufacturer does not assure that the equipment is able to operate under the design basis conditions. Therefore, the degraded parts of the equipment or the complete equipment must be replaced.

Equipment obsolescence

Obsolescence of the systems components most of the times makes very difficult and expensive to get spare parts. The growing obsolescence problem with I&C systems is a significant contributing factor that increase the probability of running out of spare parts, increasing costs for plant operation and maintenance and decreasing the plant availability.

Rapid pace in the evolution of electronic technology is a significant factor in I&C equipment obsolescence. The inability to obtain spare parts and supplier support is a major problem.

3. I&C GENERAL CONTEXT

The general context diagram of I&C systems is presented in the Figure 1. The reactor plant variables are measured by Nucleonic Instrumentation System (NIS), Process instrumentation and Radiation Monitoring System (RMS). The signals are connected to the RPS, the safety system that performs the protective actions; and the RCMS, the safety-related system that implements the reactor control and provides the main interface of visualization of the reactor variables to the operators.

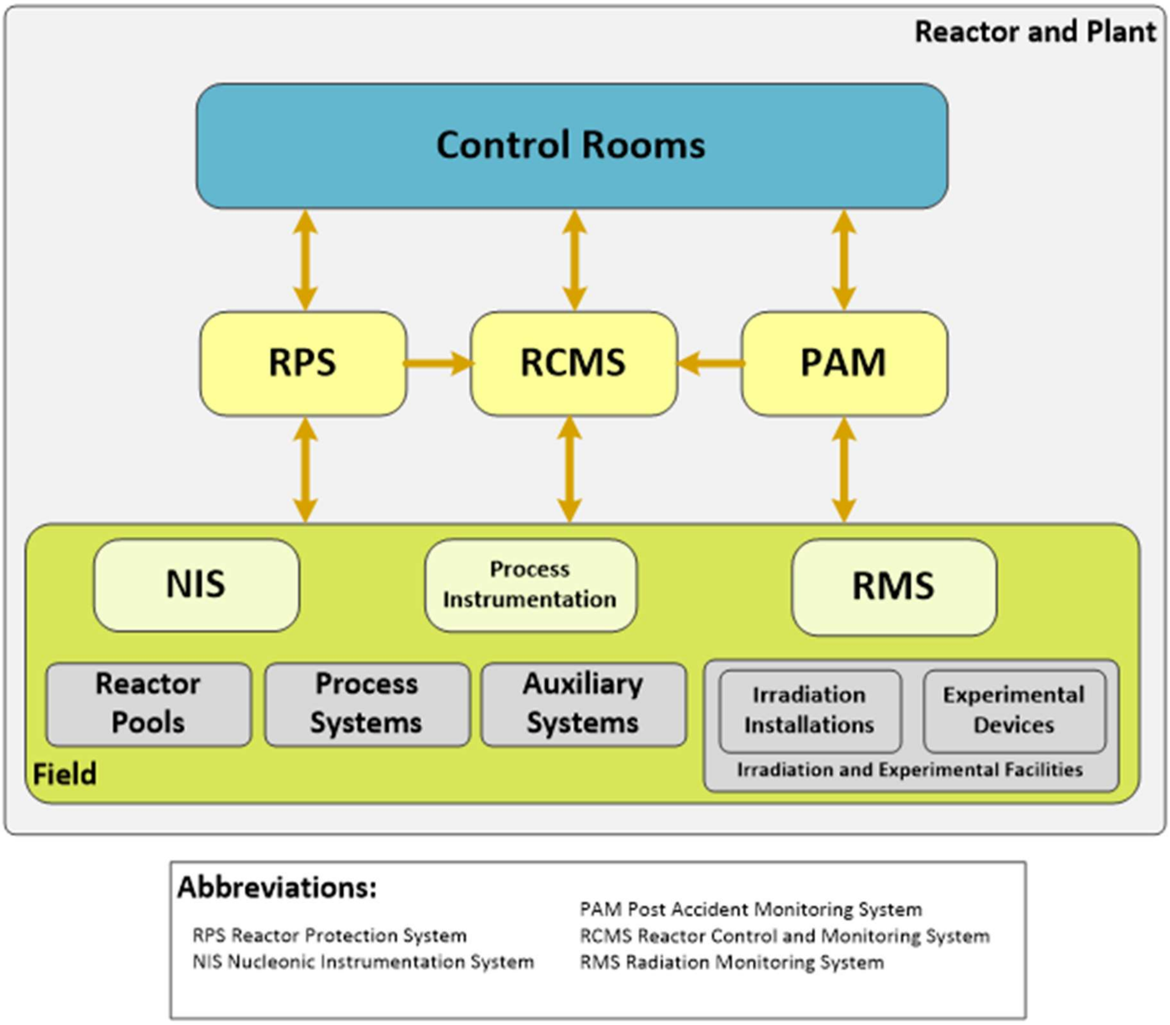


Fig. 1: I&C Generic Context Diagram

Note: The I&C context diagram shows arrows as information flow. The unidirectional arrows mean that the electrical signals shall be galvanically isolated.

The architecture used in the I&C systems in RR follows the architecture used in the Nuclear Power Plants (NPP). I&C systems are classified in accordance to their importance to safety. The safety classification for I&C systems used for a NPP is applicable for a RR. Additionally, the design features applied to NPP are applied to RR. These are: redundancy, fail safe, single failure criterion, separation between systems, separation between redundancies, equipment reliability, prevention of Common Cause Failures (CCF) and simplicity.

Nevertheless, the qualification process for equipment to be installed in a RR is different from those installed to be installed in NPPs. Equipment in a RR in most cases is exposed to mild environments while equipment in NPPs in most cases is exposed to harsh environments inside the reactor containment. For mild conditions the use of industrial equipment is allowed if the corresponding nuclear qualification process is performed.

4. EVALUATION

The process of modernizing the I&C systems begins with a review of the safety including the Postulated Initiating Events (PIE) and DBE associated with the definition of the coverage matrix.

Changes in the I&C systems should be reflected in the Safety Analysis Report, specifically in the I&C chapter (usually chapter 8).

The safety analysis conforms the basis information for the I&C modernization analysis.

Safety classification

The safety analysis shall review the classification of the original I&C systems and the categorization of their safety functions. The International Atomic Energy Agency (IAEA) classifies in Systems important to safety and Systems not important to safety. Then, Systems important to safety are classified in Safety Systems and Safety related systems.

Then, it shall be verified the separation and independence between them. It is a mandatory requirement that the Safety Systems shall be separated and independent from other reactor systems. In particular, the RPS shall be separated and independent from the other I&C systems. The channels of the Safety Systems shall be also separated and independent.

It is important to verify that all components of the instrumentation loops, such as sensors/transmitters, wiring, logic panels and console, which are part of the Safety Systems comply with the separation and independence criteria.

Some existing plants may not comply with the current separation and independence criteria for safety variables. Therefore, the modernization of I&C systems is the opportunity to provide a new design that complies with the current requirements and regulations.

Defence in Depth classification

In order to achieve the fundamental nuclear safety objective of protecting the people and the environment from harmful effects of ionising radiation throughout the entire lifetime of the reactor, I&C systems are conceived at and allocated to different levels of Defence-in-Depth (DiD) so as to comply with the objective of each level without requiring the actuation of I&C systems of the following level.

a) DiD Level 1: Reactor normal operation. Prevention of abnormal operation and failures. This level is supported by the RCMS. The automatic control loops and the manual operation allow the reactor operation at this level. The operation is facilitated with the appropriate HMI designed to provide the reactor information in a clear way to operators displaying variables, alarms and the status of the process.

b) DiD Level 2: Control of abnormal operation and failures. This level is supported by the RCMS. The RCMS provides the Limitation Functions which take place at this level: The RCMS receives the safety variables sent by the RPS and triggers the Limitation Functions when these safety variables reach a set point configured in RCMS. This way the Limitation Function is triggered before the safety variables reach the Safety System Settings configured in RPS.

c) DiD Levels 3: Control of accident to limit radiological releases and prevent escalation to core melts conditions. This level is supported by the RPS.

d) DiD Level 4: Control of accident to limit radiological releases. This level is supported by the PAM.

e) DiD Level 5: Mitigation of radiological consequences of significant releases of radioactive material.

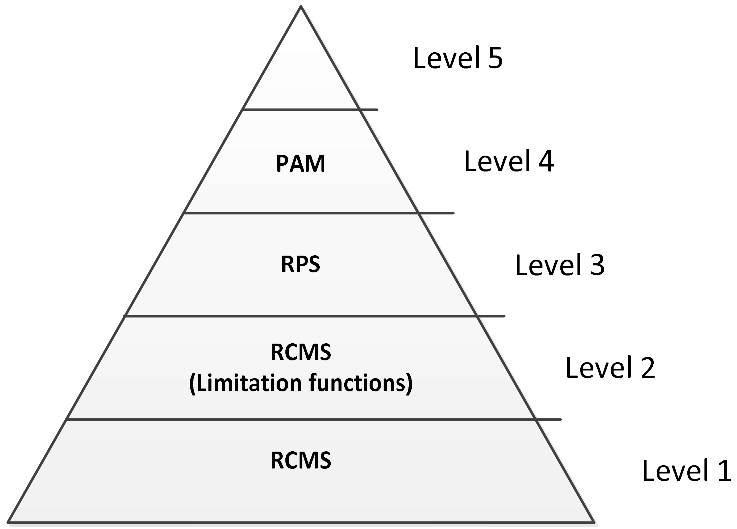


Fig. 2: Defence in Depth – Generic I&C systems

Nuclear qualification

Following the nuclear qualification process in NPP the tendency at nuclear research reactors is to qualify the equipment belonging to Safety Systems as nuclear class equipment. Standard "IEC/IEEE 60780-323 Nuclear Facilities-Electrical equipment important to safety-Qualification" can be applied in order to determine the qualification process considering only those relevant parts of this standard that are applicable to the RR.

After the modernization, either the new systems/components or the original components that remain installed shall comply with this standard.

The IEC/IEEE 60780-323 is the international Standard that describes the basic requirements for qualifying electrical equipment important to safety and interfaces (electrical and mechanical) in nuclear facilities. The principles, methods and procedures described are intended to be used for qualifying equipment, maintaining and extending qualification, and updating qualification, as required, if the equipment is modified.

The primary objective of equipment qualification is to demonstrate with reasonable assurance that the equipment important to safety can perform its safety function(s) without experiencing CCF resulting from environmental conditions occurring before, during, and after a DBE.

The DBEs considered for a NPP are not comparable with the DBEs for a RR. The qualification of equipment according to IEC/IEEE 60780-323 considers the specific DBEs conditions.

Therefore, the qualification of the instrumentation and wiring inside the containment envelope in a NPP will be more demanding. The accident conditions for a NPP are orders of magnitude higher than the accident conditions of a RR in terms of pressure, temperature and radiation. The nuclear containment of an NPP must withstand pressures of around 4 bar(g) and temperatures above 150 °C in accidental conditions; while for an Open Pool RR under accidental conditions, the pressure is essentially atmospheric (1 bar) and the temperature is below 100 °C.

Codes and standards

The new design shall be based in a set of codes and standards. IAEA standards and guidelines are the basis for the design. Furthermore, a set of codes and standards shall be selected based in local and international regulations such as the IEEE and IEC.

The similarities in the architecture between NPP and RR for I&C systems justifies that most of the codes and standards that are issued for NPP are applicable to RR.

The standards published by the IAEA provide the global fundamental principles, requirements and recommendations to ensure nuclear safety. The IAEA publications concentrate information from the experience and global participation.

There are differences between the set of IEC standards and the set of IEEE standards that can be saved. For example: the IEC standards allow the categorization of I&C systems by its function. In this way, each system has a safety class and one or more function categories; while the IEEE standards classifies the systems based only on the safety class.

Most areas of design are covered by international standards. In most cases, a design developed for one standard could be demonstrated to be valid using other standard. Many analyses are available that provide comparisons between standards. These analyses are called "harmonization". For example, Harmonization of IEEE 1012 and IEC 60880 standards regarding verification and validation of nuclear power plant safety systems software.

International standardization organizations cooperate to develop the best possible International Standards to achieve this. The IEC and the IEEE have harmonized in a single double logo International Standard qualification practices formerly given in two distinct publications. For example, the International Standard, IEC/IEEE 60780-323:2016.

Figure 3 shows the equivalence of safety classification between different standards.

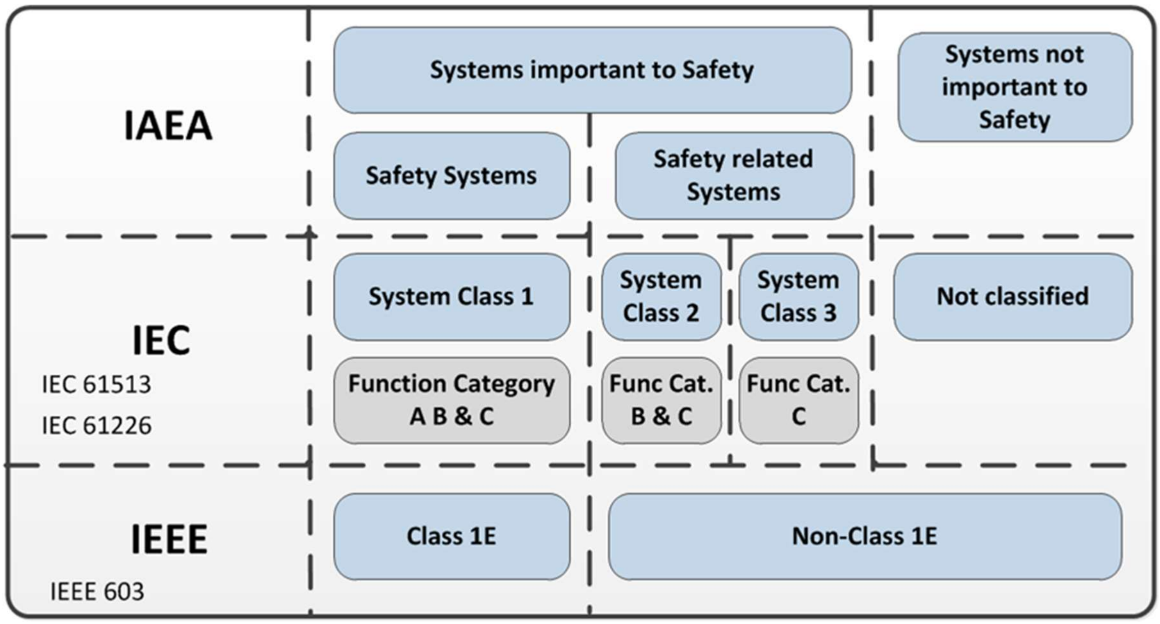


Fig.3: I&C Correlation between safety classes

Graded approach

Once the code and standard have been selected, a graded approach analysis is performed. The graded approach means that the code and standard are applied considering the characteristics of a facility. Ref [3] is an IAEA guide that presents the use of graded approach.

According to [3] all codes and standards (including software) that are important to safety are required first to be identified and then to be classified according to their function and significance for safety. The classification of systems and components in a research reactor facility should be based on the safety function(s) performed by the system or component and on the consequences of the systems and components failure to perform its function.

The following graded approach factors are usually considered:

a) In case the standard is issued for a NPP, there are requirements applicable to a NPP that are not applicable to a RR. In this case, a graded approach is performed. According to [3] grading implies the proportional application of certain requirements, depending on the potential risk to the environment.

b) The design of systems and components is based on the safety classification of systems and Components defined by the project. The safety classification defined by the codes and standards may be different from the safety classification defined by the project. Therefore, an equivalence of safety classification shall be stated.

5. HUMAN FACTORS EVALUATION

Once the decision to upgrade the I&C systems has been made, a careful analysis of the human factors shall be done in order to elaborate requirements for the new I&C systems.

The human factors analysis of the particular reactor shall include an HMI proposal that considers the same way in which the reactor is operated. On the new console consider: console dimensions, signal and alarm tags, HMI language, alarms blinking, alarms sound, colour encoding, analog recorders replaced by electronic recorders or SCADA. Mimics replaced by screens.

On instrumentation panels, consider the new space to be occupied. The default condition is to replace equipment that occupies the same space, but almost never this condition is complied.

6. PLANT WALKDOWN

The plant walkdown is important to determine the condition of the plant. The following items shall be considered:

a) The condition of the I&C systems and the condition of the plant installations:
   i. The feasibility of removing panels or equipment that will be replaced.
   ii. The feasibility of removing cables.
   iii. The aging conditions of the wiring, panels and equipment that remain and will serve as interface.
   iv. The operation of the remaining systems that will be the interface.
   v. The route of entry and egress of heavy and bulky panels and equipment.

b) The plant layout in order to verify the feasibility of routing by separated trays or conduits. The physical separation between systems is one of the biggest challenges in a modernization project. Separation of wiring shall be maintained for systems of different safety classification (for example: RPS separated from RCMS and between the RPS channels). The survey of trays observing the space available for cables and if the separation between systems and channels is according to the standard. Usually it is preferred to use conduits instead of trays because it is allowed to have less separation.

c) It is important to identify the equipment belonging to a safety function that in their design does not comply with the single failure tolerant design. For example: the instrumentation of the position of the flap valves could require that the position switches are redundant.

7. I&C SYSTEMS

Nucleonic Instrumentation System

The following neutron flux measurement channels (a, b, c, d) and gamma measurement channel (e) can be used to replace the existing instrumentation:

a) Start-up Channel: 5 measurement decades. Used at start-up range. (generally connected to RPS).

b) Compensated Ionisation Chamber Channel: 7 measurement decades. Used at power range (generally connected to RPS).

c) Campbell processing Fission Chamber Channel: 10 measurement decades. Used at start-up and power range (generally connected to RPS).

d) Self-Powered Neutron Detectors: used at power range (generally connected to RCMS).

e) Nitrogen 16 gamma Channel: used at power range for global core power measurement. (generally connected to RCMS).

Reactor Protection System

Architecture of the Reactor Protection System

For small RR that have to be modernised with cost-effective systems, it is usually recommended to install a hardwired system based on discrete electronics and relays.

For large reactors that require increasing the number of safety variables, it is recommended to install a digital system already qualified for nuclear safety applications.

The RPS architecture should be flexible allowed to be adapted to the existing reactor safety instrumentation and safety logic. An architecture based on two or three independent measurement channels shall be implemented. Two channels comply with safety requirements. Three channels comply with safety and availability requirements. Four channels are usually used in NPP that require more availability.

The following figure shows the architecture implemented with three measurement channels using a two out of three (2oo3) voting logic for each safety variable.

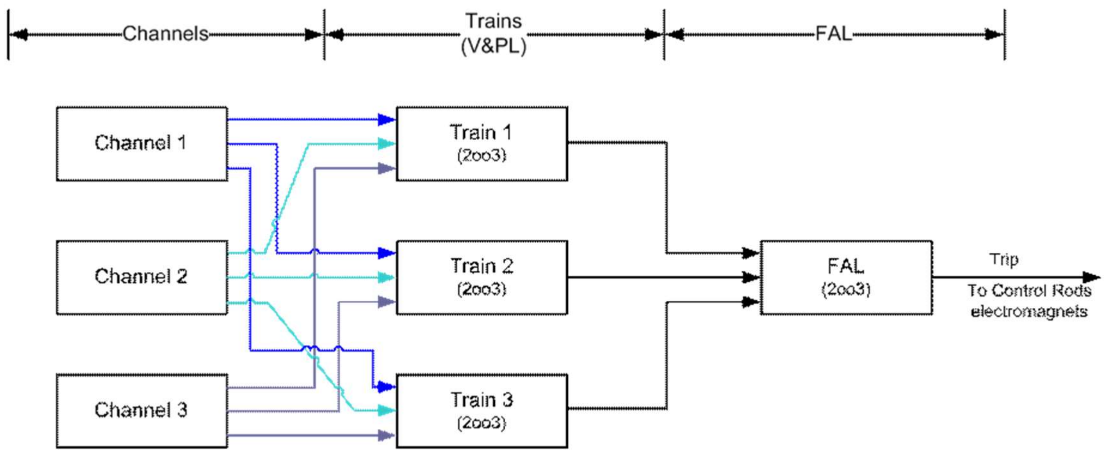


Fig.4: Three channels RPS Architecture

Each measurement channel is acquired by each of the three Trains. Each Train performs a 2oo3 logic for each measurement channel. Then, the output of the three Trains is voted in a 2oo3 in the Final Actuation Logic (FAL).

This architecture is flexible and has more availability than other triple redundant architectures.

In our experience, the flexibility of this RPS architecture allows finding the appropriate configuration for the reactor requirements. For example: The already modernized reactors show a cost-effective solution combining a dual redundant Train architecture with triple redundant channels for nucleonic variables and dual redundant channels for the other safety variables.

This system is required to be modular and scalable to provide flexibility to be configured and to facilitate maintenance tasks. Scalable equipment can be used in a wide range of nuclear facilities, ranging from critical facilities, research reactors and / or production of radioisotopes to large nuclear power plants.

Technology of the Reactor Protection System

Historically the technology used in Safety Systems, such as the RPS, was based in hardwired systems implementing analog electronic and relays logic. It has been demonstrated that this technology works reliably and the nuclear agencies of the local countries will accept it to continue.

On the other hand, today everything tends to be digital. Digital technology can be used in safety systems as long as safety design features are considered in the product and the design process.

Some reactors have two RPS, a First RPS that triggers the insertion of all the Control Rods and a diverse Second RPS that shutdowns the reactor in a diverse form. In these cases, the combination of a digital system for First RPS and a hardwired system for the Second RPS is widely accepted and desired, in order to mitigate the consequences of the CCF.

Hardwired Technology

Hardwired RPS is present on most existing reactors. This technology refers to relays logic, discrete electronic logic and analog electronic.

Figure 5: Electromechanical Relay

Advantages

a) Well proven technology.

b) probabilistic and deterministic reliability calculations by traditional methods.

c) cheaper for systems that have few input signals.

Disadvantages

a) more instrumentation cabinets and more space in the instrumentation rooms.

b) Large amount of cables and connections for the hardwired logic.

c) Large amount of cables and connections for the communication to RCMS.

Fully digital technology

This technology refers to microprocessor (or microcontroller) based system or an FPGA based system. A fully digital system normally uses a safety controller.

This safety controller shall comply with safety properties such as:

a) fault tolerant feature: the equipment identifies and compensates for failed control system elements and allows repair while continuing an assigned task
b) self-testing feature
c) sequential execution of the program with no interruptions (in case of microprocessor based systems)
d) compiling software demonstrated to be reliable (for microprocessors). Synthesizing hardware demonstrated to be reliable (for FPGA).
e) intensive Verification and Validation (V&V) of the software (for microprocessors) or hardware (for FPGA).
f) Intensive V&V of the system

Advantages:

a) The equipment occupies less space
b) Less amount of cables
c) Digital communication to RCMS
d) Cost-effective for large number of input signals
e) Flexible to program
f) Scalable Logic

Disadvantages

a) More expensive
b) intensive V&V of the software and the compiler for microprocessors. intensive V&V of the hardware and the synthesizer for FPGA.
c) Intensive V&V of the system
d) Cyber-security analysis
e) Unnecessary complexity: Millions of transistors integrated in a microprocessor or FPGA for a simple logic.

Example: Tricon Fault Tolerant Controller

The Tricon is a commercial state-of-the art controller manufactured by Invensys that provides fault tolerance by means of Triple-Modular Redundant (TMR) processors. TMR integrates three isolated, parallel control processing and extensive diagnostics in one control system. The system uses two-out-of three voting to provide high-integrity, error-free, uninterrupted process operation with no single point of failure. The TMR is implemented in each Train and shall not be confused with the triple architecture of the RPS.

The RPS uses three identical channels. Each channel independently executes the control program in parallel with the other two channels. Specialized hardware/software voting mechanisms qualify and verify all digital inputs and outputs from the field, while analog inputs are subject to a mid-value selection process.

Fig. 6: Fault Tolerant Controller

The FPGA is a digital technology. Although FPGA do not run a software, they have to be programed through a Hardware Description Language (HDL). A HDL have similarities to a software programming language. It is a textual description consisting of expressions, statements and control structures. However, the FPGA differ because the processing is not sequential as expected in software. The HDL have to be synthesized (the function of the compiler in software is called synthesizer in HDL).

For both technologies (microprocessors and FPGA), it has to be demonstrated that both, compilers and synthesizers, transform the source code into the final function always in a reliable way.

Hardwired and digital Technology

The combination of digital technology with hardwired technology allows obtaining a hybrid system that allows executing a function using both technologies simultaneously in a redundant and diverse way.

The use of hardwired/digital, modular protection systems, where the safety functions are carried out by electronics called hardwired and the supervision function by the micro-controlled layer allows on one hand the self-diagnostic functions and on the other hand the communication through isolated unidirectional buses to RCMS system, with the advantage of reducing wiring.

Advantages:

a) less amount of cables

b) Probabilistic and deterministic reliability calculations by traditional methods

c) Digital communication to RCMS

d) Intrinsically redundant and diverse

e) modular and scalable system

Disadvantages:

a) less cost-effective for large amount of input signals

Example: Invap - Priuss

The PRIUSS system is modular, scalable and configurable. The architecture is based on modules with specific functions, arranged to satisfy with the requirements of functionality and interface, covering any combination of logic. The modular feature allows configuring any required architecture, meeting with the independence criteria and electrical isolation between redundancies and with other system.

The system is based on two layers: hardwired and digital, thus the design takes advantage of both technologies.

The hardwired technology guarantees probabilistic and deterministic reliability calculations by traditional methods based on part Count (Reliability Predictions) and Mean Time Between Failures (MTBF) MIL-HDBK-217F Reliability Prediction of Electronic Equipment.

The digital layer is based on microcontrollers with embedded software. The advantages of the digital technology allow not only self-diagnostic functions and communications, but also the Sequence of Events (SOE) sent after a trip of the channel, which is a fundamental tool for the analysis of reactor events.

As a Safety System, the components are environmentally and seismically qualified.

The proposed system is based in an intrinsically diverse platform that is the most distinctive aspect of this system. This double layer configuration provides intrinsic diversity to the modules which helps to prevent a CCF.

The output of the logic modules are relays with potential free contacts.

Figure 7 shows a channel composed of modules that fulfil functions in successive stages of processing of a protection signal. Analog processing modules, comparison modules, logic modules and galvanic isolation modules are presented.

Figure 8 shows a generic module implementing both layers.

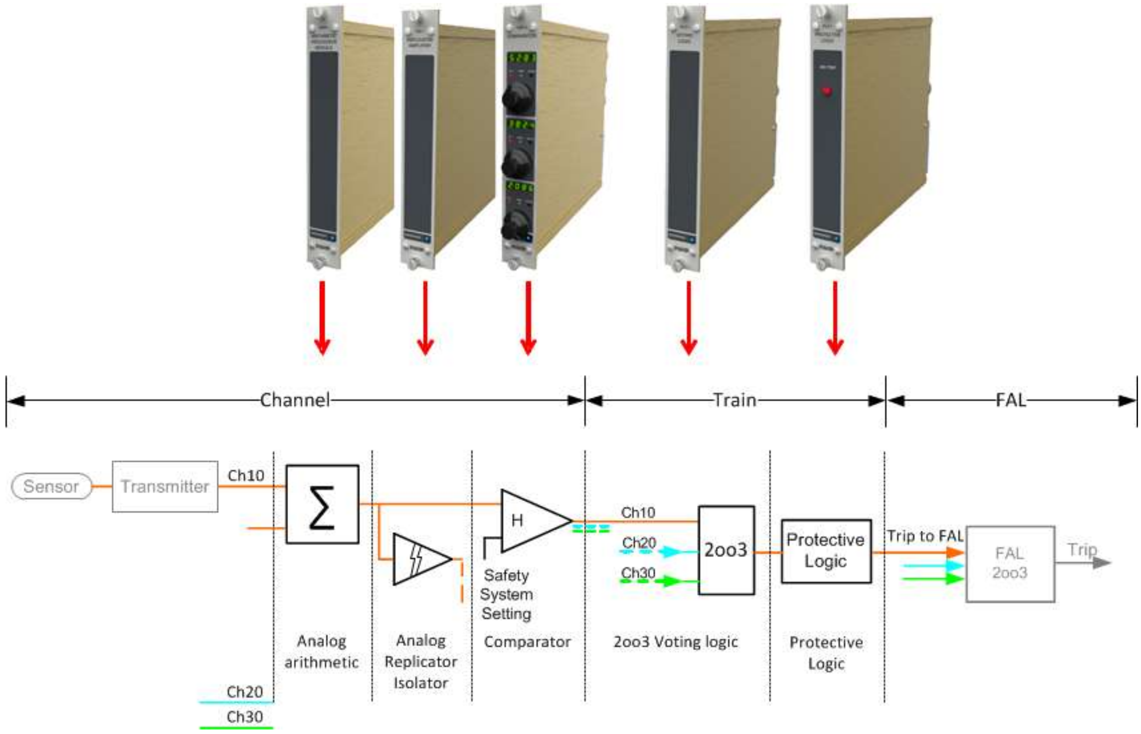


Fig. 7: Channel implemented with Hardwired & digital RPS modules

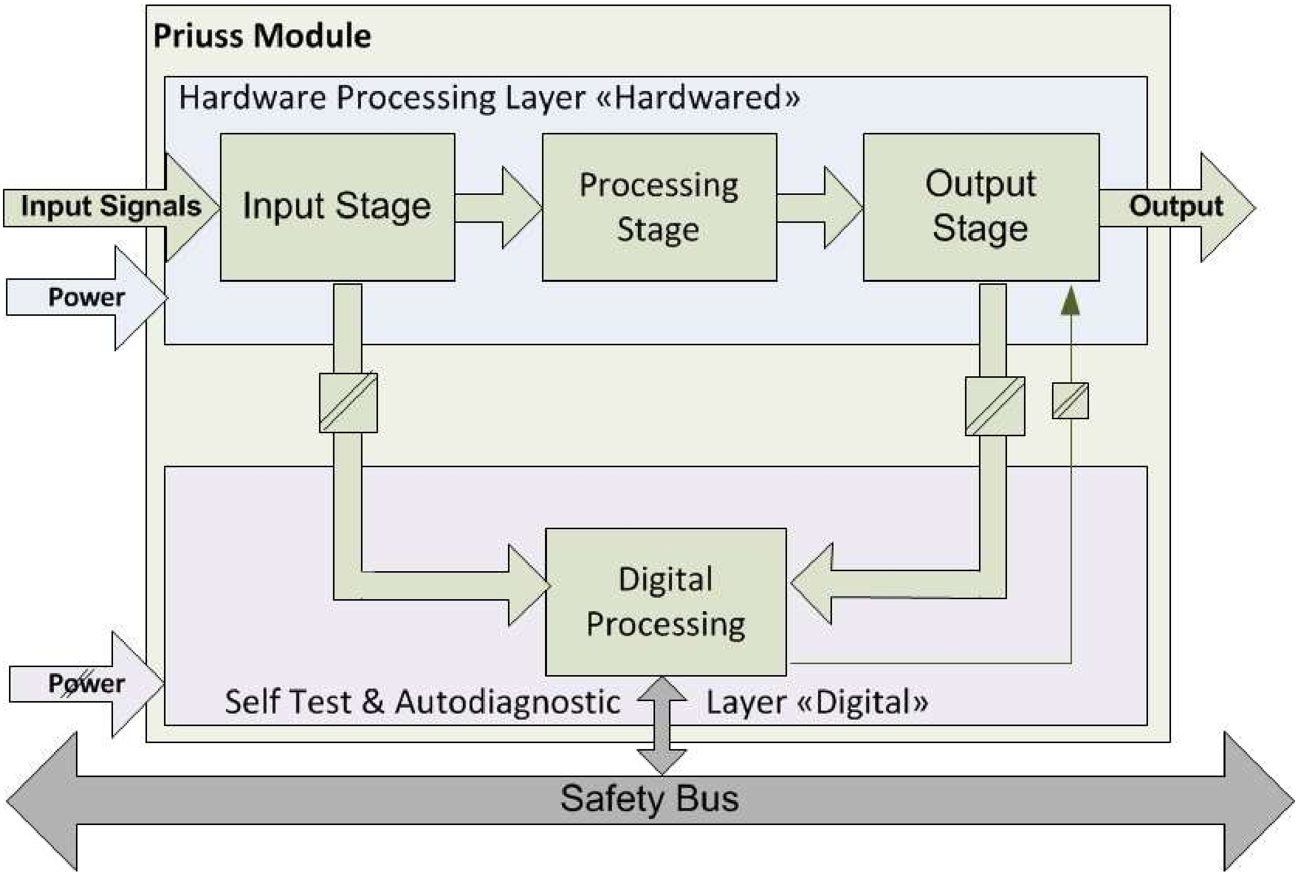


Fig 8: Priuss Module Block Diagram

The digital processing layer is implemented with a safety qualified microcontroller.

The PRIUSS system meets the following design criteria:

a) Proven technology

b) Simplicity

c) Single failure criterion

d) Fail safe

e) Intrinsic diversity

f) Designed to implement redundant Channels and Trains

g) Designed to implement physical separation, independence and isolation between Channels and Trains.

h) Self-test feature

i) Designed to run tests manually

j) Tolerance to failure on demand

Reactor Control and Monitoring System

The main functions of the RCMS are:

a) Reactor supervision

b) Process control

c) Reactivity control by the Control Rod Drive system

d) Limitation functions

e) Reactor States transition logic

f) Data acquisition & recording

g) Alarms annunciation

Architecture of the Reactor Control and Monitoring System

The modernization of the RCMS is potentially the most visible change in the I&C systems.

This modernization allows increasing the automatic and manual actions to provide new operational features to the reactor and the overall plant.

Modern systems present all information efficiently to operators in a user-friendly manner. New alarms and limitation functions can be added to maintain the reactor parameters within operational limits without reaching safety limits.

The architecture of a modern RCMS is usually divided in three levels:

a) Supervision

b) Control

c) Field

The communication between the three levels is provided by the field network and the control network, in that way there are savings in costs and space compared to the standard point to point philosophy where signals are wired individually.

Designed and Tested for Nuclear Reactors:

1. Three Basic Levels: Supervision, Control, Field
2. Based on Commercial Of The Shelf (COTS) systems.
3. High Availability figure: 99.9%
4. Redundancy (hot-standby)
5. Cybersecurity plan from the development
6. V&V Plan from development
7. Designed to maintainability of the system itself and the entire plant.
8. Minimization of number of components
9. Modularity of software and hardware
10. Extension and expansion capability
11. Integration capacity: Intelligent Instrumentation, Irradiation Monitoring Equipment, Electrical System.

Distributed Control System

A DCS is a computerised control system implemented in a plant. It is usually implemented in plants with large numbers of control loops. The autonomous controllers are distributed throughout the plant, but there is a central supervisory control. This is in contrast to systems that use centralized controllers; either discrete controllers located at a central control room or within a central computer. The DCS concept increases reliability and reduces installation costs by localising control functions near the process plant, with remote monitoring and supervision.

Fig 9 shows the architecture of a RCMS based on a DCS used in the OPAL (Australia) reactor.

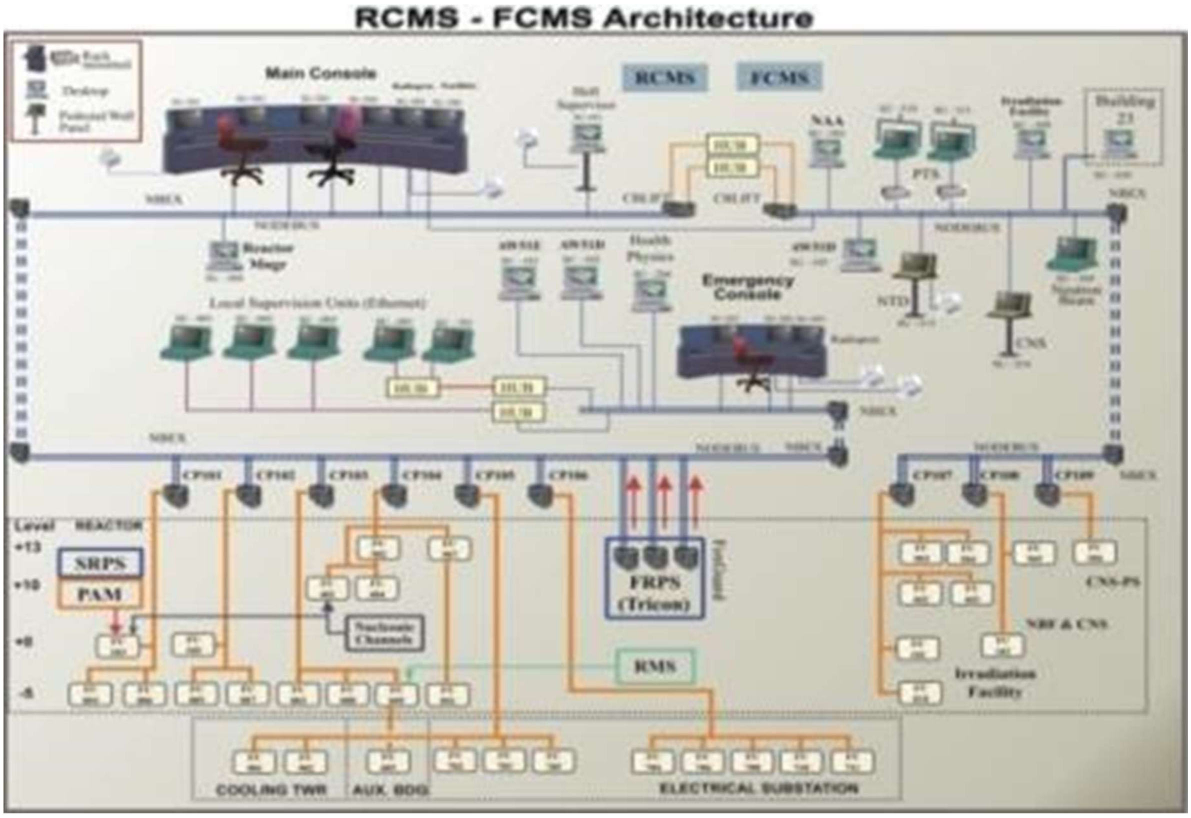


Fig. 9: RCMS - DCS based architecture

Programmable Logic Controller

PLC-based RCMS systems allow the automation of functions that make it easier for operators to perform daily operation functions. Through the use of distributed periphery in the reactor plant, field signals are acquired and then sent to the central PLCs through the use of field buses, this way decreasing the amount of wiring in the plant.

All data acquired by the RCMS are presented in the consoles in a friendly and orderly way to the operators. The old operation mimics are replaced with the SCADA, which can be represented in monitors, both in the console and in the previous location of the mimics. The paper recorders may also be replaced by standalone data loggers.

All the information acquired by the RCMS is stored in historical databases with which it can be obtained the historical operation data that are used to organise the preventive maintenance strategies.

Figure 10 shows the architecture of a RCMS based on PLCs.

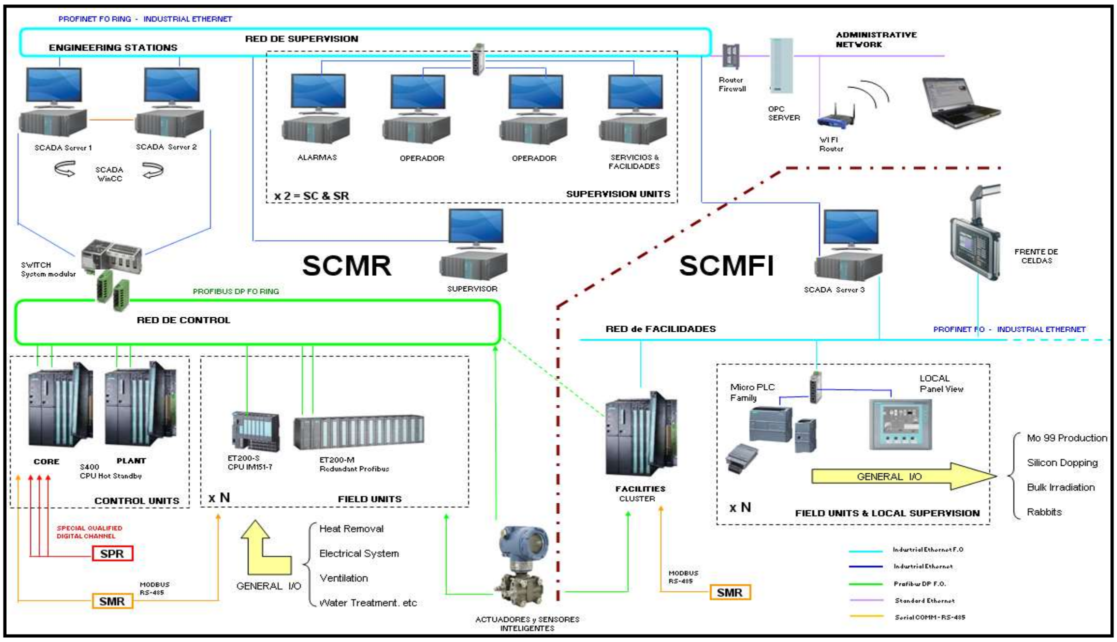


Fig. 10: RCMS - PLC based architecture

Automatic Power Regulation System

The Automatic Power Regulation System (ARPCS) is implemented completely as a software module in the RCMS. This system is responsible for the regulation of the reactor power to the power set point determined by the operator. This function compensates normal reactivity changes due to effects associated with temperature, xenon, target insertion/removal and fuel burn-up. This function performs power changes to new levels upon modification of the power set point.

Human Machine Interface

The extensive data acquired by the RCMS, the information processing and display capabilities of modern technology provide the ability to improve considerably the HMI in RCMS. This includes the effective use of Video Display Units (VDU) and large overview screens in the Control Room. The presentation of complex conditions by means of specialized graphs and diagrams and the rapid access to the information supports the safer and more efficient operation of the plant. These improved HMI capabilities reduce the potential for human errors.

The Supervision workstations run the SCADA application that allow operators to supervise and command the reactor using mimics that show the reactor process schematically. Figure 11 shows an example of a process page.

The main variables of the reactor such as neutron flux, reactor power, position of control rods, are shown on dedicated screens.

Plant variables are stored in historic data recordings which allow trending visualization. Historic data also allow operation and maintenance staff to keep historic values that can be used in for future analysis.

It is highly recommendable that the reactor staff is involved in the modernization project in an early stage particularly to verify that the new HMI satisfies their needs and is consistent with existing procedures.

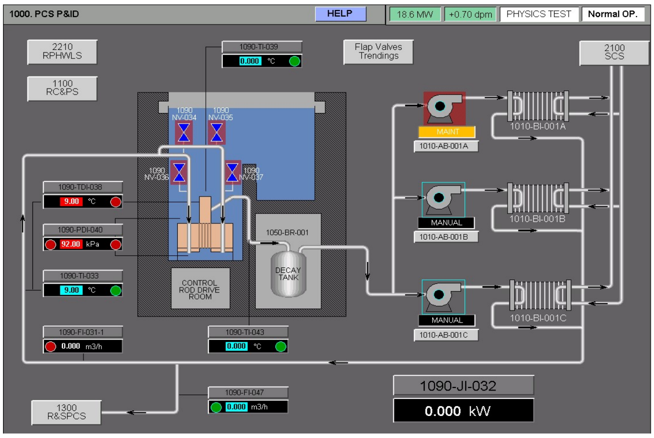


Fig. 11: Example of a process page

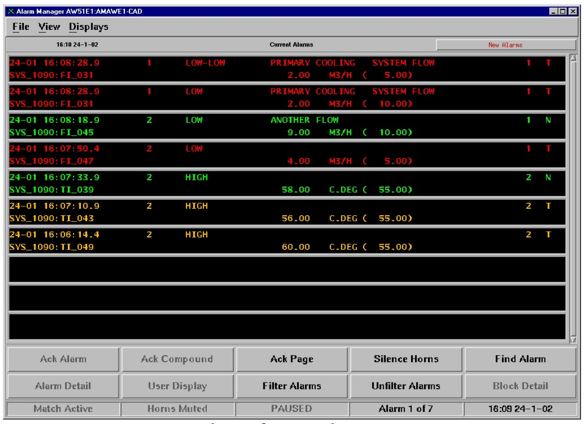


Fig. 12: Example of an alarm page

The HMI defines colour codes in order to easily visualise the status of a reactor process variables and alarms: Figure 12 shows the alarm page where reactor alarms are shown ordered by date and time.

Interface from RPS to RCMS

As presented in Figure 1 there is a one-way communication from RPS to RCMS. If the RPS is triple redundant, there will be three independent communications, one from each redundancy. The communications have galvanic isolation in order to guaranty RPS independence from RCMS.

The use of a digital buses instead of hardwired signals reduce the implementation costs.

The data transferred from RPS usually are:

1. RPS input signals
2. RPS Trip signals
3. RPS Safety System Settings
4. RPS status

Console

A key aspect to take into account in the modernizations is the human factors. The operational experience and staff training shall be taken into account. All implemented changes should facilitate the operation maintaining the procedures and operation behaviours in the reactor in order to avoid human errors.

It is convenient that the console maintain similarity with the original design so as not to disturb the way of operating the reactor, but on the other hand, the distribution of components in the console shall take into account the physical divisions between systems and redundancies.

A part of the console is dedicated to the RCMS for reactor operation based on SCADA systems. It should be noted that although most of the operation is done through the SCADA system using buttons and virtual indicators drawn on the screens, for the operation of the control rods it is preferred to keep physical buttons and physical indicators.

The other part of the console is dedicated to the RPS, in which the safety variables are displayed using individual indicators with analog representation that emulate the operation of the old needle indicators; indicators with digital representation and lighting indications indicating status signals and trip signals. This set of indicators allows the operator to evaluate the reactor safety variables and, if necessary, bring the reactor to a safe condition having a reliable visualization of the values or states of the safety variables.

Fig. 13: Example of a console with three supervision stations – RPS (left) RCMS (center and right)

Control Rooms

If the desired control room layout requires major modifications, it is recommended to plan a global replacement of the panels during a suitable outage in order to install newer technology that will allow further incremental implementations. For that condition, the easier solution is to plan the entire migration process by taking into account the availability needed of essential functions during the outage.

Regardless of the scope of the modernization project, it is necessary to evaluate the potential problems of operating old and new systems in parallel. Sometimes major parts of the old control room equipment are left unchanged and the new systems are implemented in the middle of old equipment.

In such cases, special care to harmonise the old and the new systems should be exercised. Control room changes should always be considered carefully to make sure that new problems are not introduced when the operators have to transfer from a familiar to an unfamiliar system, which in addition may contribute to potential human errors.

An example of this case is the modernization of the 14Mw TRIGA Research Reactor at Pitesti, Romania. Here, the console of the steady state reactor was replaced by a new console which design is very similar to the original console.

8. EXAMPLES OF MODERNIZED AND NEW REACTORS

8.1. ICN Triga Reactor (Romania)

14MW TRIGA Research Reactor at Pitesti, Romania. Replacement of the RPS and RCMS.

Fig. 14: Factory Acceptance Test *Fig. 15: Systems installed at Pitesti,*

8.2. TRRL (Libya)

10MW reactor in Tajoura, Libya. Note: At Factory Acceptance Test stage only (2011). Not installed.

Fig. 16: Factory Acceptance Test at Bariloche, Argentina

8.3. Central Nuclear Embalse (Argentina)

Central Nuclear Embalse (CNE): NPP – Candu6 type

Addition of new instrumentation loops and replacement of existing instrumentation and cables in Shutdown System 1 (SDS1), Shutdown System 2 (SDS2) and Emergency Core Cooling (ECC).

Fig.1: CNE console PL4 (SDS1) – before modernization (2015)

Fig.2: CNE console PL4 (SDS1) – after modernization (2018)

8.4. LPRR Reactor (Saudi Arabia)

Research reactor for Saudi Arabia, currently at Factory Acceptance Test stage (2018).

Fig 19: Factory Acceptance Test at Bariloche, Argentina (2018)

8.5. RMB Reactor (Brazil)

30 MW Research Reactor for Brazil, currently at engineering stage.

Fig. 20: RMB - Main Control Room

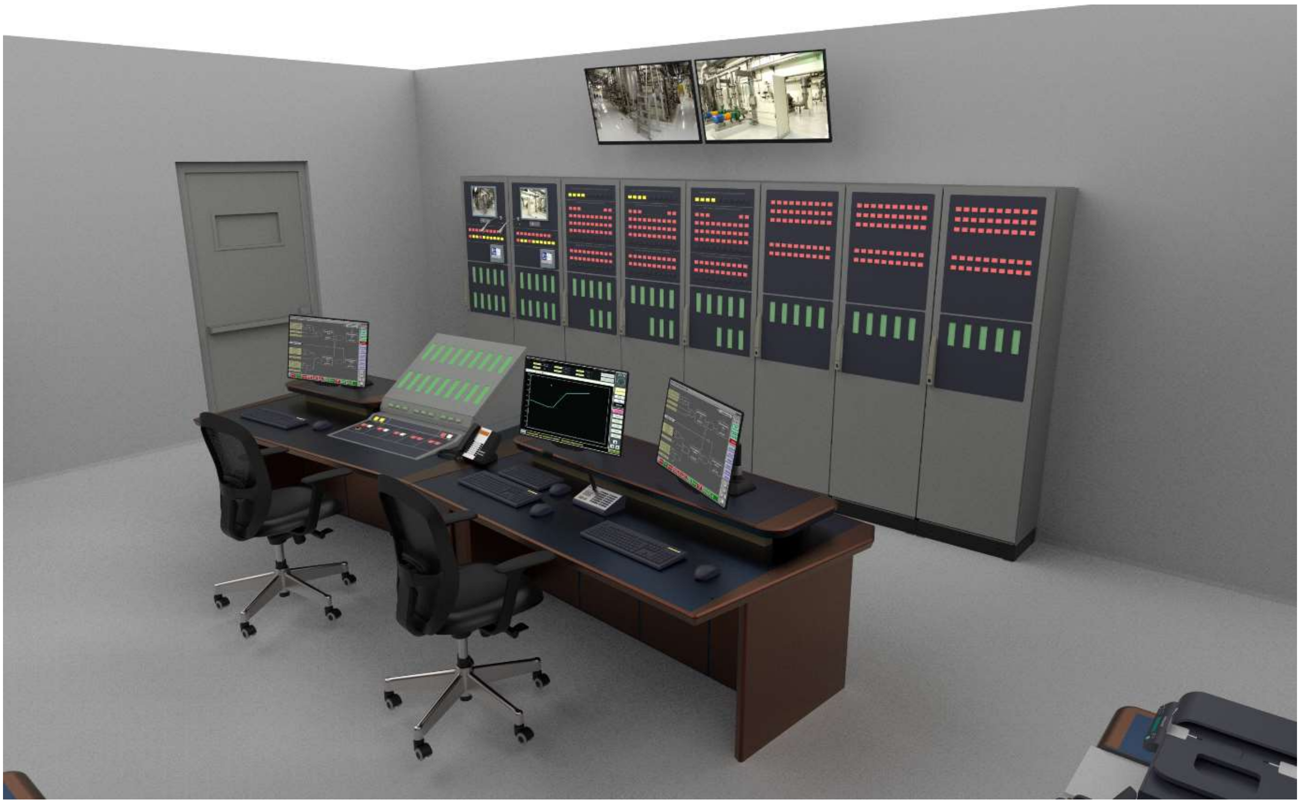


Fig. 21: RMB - Emergency Control Room

8.6. Future designs

Future designs for modernization of small RR may require a console with the RPS supervision station (left) and two or three supervision stations (center and right) for RCMS.

The RPS supervision station will continue to be metallic due to the seismic requirements. While the RCMS supervision stations could be constructed in wood. Although the consoles of RCMS shown previously are metallic, the use of wood provides easier ways to modernizes the console in a future. This criterion is part of the obsolescence plan for the console.

Fig. 22: Proposal for New Control Rooms

Fig. 23: Proposal for new consoles

9. CONCLUSIONS

The nuclear reactors look forward for extended future operation and licensing renewal and they will inevitably continue the replacement of their ageing and obsolete equipment or they will need to adapt the I&C to current safety standards and to an efficient plant operation.

On the other hand, the technology development of the I&C has been growing fast over the last decades.

For that reason, the use of modern technology in the research reactors offers the opportunity to enhance safety, to increase productivity, to reduce maintenance costs and to support plant staff in the performance of their jobs. Modem technology can be used to improve availability, improve reliability and increase productivity of the plant.

The modernization is the opportunity to review the safety analysis, analysing functions of control, protection, the safety classification and defence in depth of each system. A set of codes and standards shall be defined and a graded approach may be applied if necessary.

The separation of systems and redundancies in the plant layout is usually the most challenged task.

The human factors shall be considered from the beginning of the project in order to maintain or improve the operation. Proper use of this technology can not only reduce the potential for human errors, but can also support improved human performance.

A careful planning of the I&C life cycle should consider the modernization of the I&C equipment or systems taking advantages of modern architectures and technologies in the area of instrumentation, RPS, RCMS and PAM to provide a safe, reliable and cost-effective operation of the reactor keeping as low as possible the impact in the plant layout and enhancing the reactor operation while maintaining the human factors in the console.

10. REFERENCES

[1] IAEA SSR-3 Safety of Research Reactors

[2] IAEA SSG-37 Instrumentation and Control Systems and Software Important to Safety for Research Reactors

[3] IAEA SSG-22 Use of a Graded Approach in the Application of the Safety Requirements for Research Reactors

[4] IAEA SSG-24 Safety in the Utilization and Modification of Research Reactors

[5] IAEA NNS No. 33-T Computer Security of Instrumentation and Control Systems at Nuclear Facilities

[6] IAEA NNS No. 17 Computer Security at Nuclear Facilities

[7] IAEA-TECDOC-1147 Management of ageing of I&C equipment in nuclear power plants

[8] IAEA-TECDOC-1402 Management of life cycle and ageing at nuclear power plants: Improved I&C maintenance

[9] IAEA-TECDOC-1016 Modernization of instrumentation and control in nuclear power plants

[10] IAEA-TECDOC-1389 Managing modernization of nuclear power plant instrumentation and control systems

[11] IAEA TECDOC 973 Research Reactor Instrumentation and Control Technology

[12] IEC/IEEE 60780-323 Nuclear facilities-Electrical equipment important to safety-Qualification

[13] ISO/IEC/IEEE 29148:2018 Systems and software engineering - Life cycle processes - Requirements engineering

[14] NEN-ISO/IEC/IEEE 12207:2017 Systems and software engineering - Software life cycle processes

[15] IEEE Std 379 Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems.

[16] IEEE Std 384 Standard Criteria for Independence of Class 1E Equipment and Circuits.

[17] IEEE Std 7-4.3.2, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generation Stations, IEEE, 2010

UPGRADING OF THE REAL TIME MONITORING SYSTEM (RTMS) FOR ES-SALAM RESEARCH REACTOR.

A. MESSAI[1], H. BABAAMEUR[1] AND H. BOUHZILA[1], I. ABDELLANI[1]
[1]Centre de Recherche Nucléaire de Birine (CRNB\COMENA), Algeria

E-mail contact of main author: messai_adnane@yahoo.fr

Abstract. To assure a continued safe and reliable operation of a nuclear facility, it is essential that accurate online information on the current state of the entire system be available to the operators. This function is mainly performed by the I&C system of the installation which is similar to the functions of the brain and neural network in a human body. The issue of obsolescence and aging of the electronic components that make up this system mean that the required functions are often not guaranteed. In order to avoid such a situation for our reactor, we decided to renovate some critical parts of the reactor's I&C system. Among the sub-systems that was affected by this operation we notice the Real Time and Monitoring System “RTMS”. This one was originally built around the famous 16-bit PDP/1173 microcomputer and began to show signs of aging and frequent breakdowns. The new adopted system uses a hardware platform provided by National Instruments (NI). The big amount of measured parameters (419 parameters) led us to use two independent data acquisition sites. The first one is used to acquire thermo-hydraulic and radioprotection parameters such as flow, pressure, radiation measurements …etc, through an external chassis and a PC plug-in card with a PCI-bus expansion slots. While the second one was reserved to the core assembly temperature measuring RTD sensors. These last parameters are acquired via field-point units connected to a local network bus. The whole acquired data is then stored directly into a high performance computer, where it can then be analyzed, displayed, plotted and so on. The developed software part transforms the PC and the data acquisition hardware into a complete data acquisition, analysis, and presentation system. To carry out this task, we have used two development environment software products (***LabVIEW, LabWindows™/CVI***) to create a complete instrumentation, acquisition, and control applications. The whole system is now operational and is used to monitor all measured parameters around Es-Salam research reactor.

Key Words: Research Reactor I&C System, Digital Data Acquisition System, real Time Monitoring System, Upgrading.

1. INTRODUCTION

Effective and resilient control of nuclear research reactor is essential for their continued safe operation. The control and monitoring tasks task are primarily based upon the Instrumentation and Control (I&C) systems which are installed throughout the nuclear facility are vital parts of normal, abnormal and emergency operations. They monitor all aspects of the plant combining the information provided by multitude sensors and pre-defined supervising rules **[1]**. Therefore, it appears that it is crucial for the sensing elements to precisely convey the physical parameters: as neutron flux, temperature, pressure, level, and flow rate of plant processes to assure the continued safe and reliable operation of a given facility. Trying to ensure this feature and to enhance the global performances of the I&C systems related to our reactor, we have installed the system described below.
The Algerian research reactor “Es-salam” was equipped with a Real Time Monitoring System (RTMS) based on the famous PDP/1173 minicomputer. Unfortunately, in such system higher level programming facilities, needed for development and research tasks, are usually not

available. Besides to this, the system components (mother boards, processors, interfacing cards) became increasingly obsolete and often tend to fall down. To resolve this problem, we decided to replace the old RTMS by a new system which was successfully integrated into the I&C system of the reactor during the few last years. This new system is based on the-state-of-the-art National Instruments (NI) chassis and modules and uses powerful recent computers able to support a big amount of compilers and needed applications.

2. DESCRIPTION OF THE NEW INSTALLED SYSTEM

To monitor, record and analyse measured data around the reactor, we have installed a new real time data acquisition and monitoring system with its two essential aspects: hardware and software parts **[2]**.

2.1. Hardware Part

Within the new system, the majority of the measurement hardware was provided by National Instruments corporation. The main data acquisition unit consists of an industrial PC with a standard data acquisition (*NI-M-SERIES-DAQ*) board. The inputs of the DAQ card are extended using the of 32-channel multiplexers (*NI-SCXI 1100*). The system is able to make measurements with arbitrary selection of the input signals with programmed or manual start.

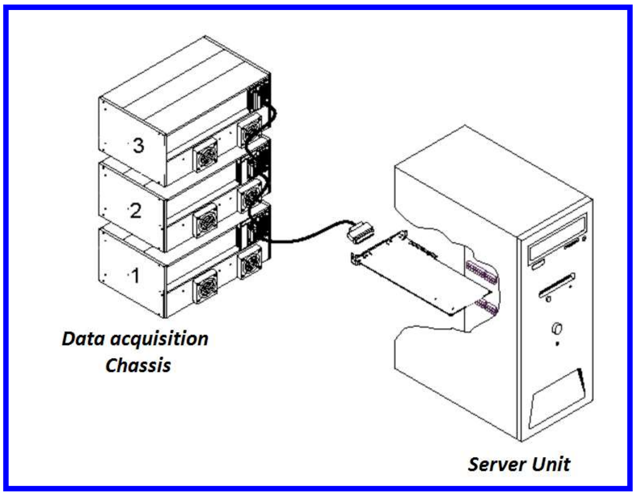


FIG. 1. Data acquisition chassis

Data acquisition task is performed by a server unit in an autonomous manner, but measurement sessions can be remotely controlled from the client computer. Digitized data are stored locally on the server machines, but selected binary files can be transferred to the client computer via the network. Detailed data evaluation can be performed on the client node. All communication tasks are carried out by using the standard TCP/IP interface.

The important number of being measured parameters led us to use two independent data acquisition sites. The first one is used to acquire thermo-hydraulic and radio-protection parameters such as flow, pressure, radiation measurements, … etc. As we can see in the figure below, the acquired data is stored directly into the computer, where it can then be analyzed, through an external chassis and a PC plug-in card with a PCI-bus expansion slots.

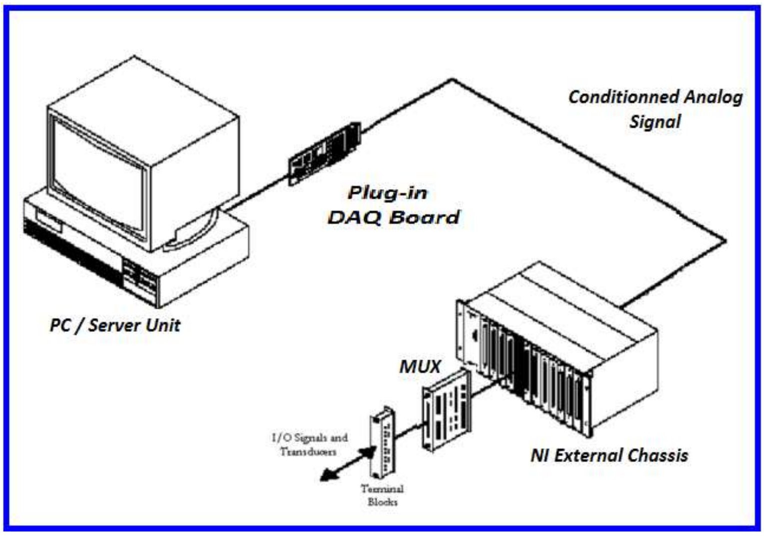


FIG. 2. First technical local for different parameters data acquisition.

We note here that, before being injected into the *NI* modules, the measurement signals issued from the reactor must first be conditioned inside the spec-200 Foxboro cabinets. The conditioning task include the following processing functions:

- Amplification,
- Attenuation,
- Isolation,
- Simultaneous sampling,
- Sensor excitation.

The second site is used to measure the different fuel assemblies temperatures inside the reactor core. The used *NI* field-point modules (*FP-122*) interface directly the temperature sensors (*03 wires Platinum RTDs*), digitize the measuring obtained signal and then send the exploitable information to the plant computer via the Ethernet network over the TCP/IP protocol [4].

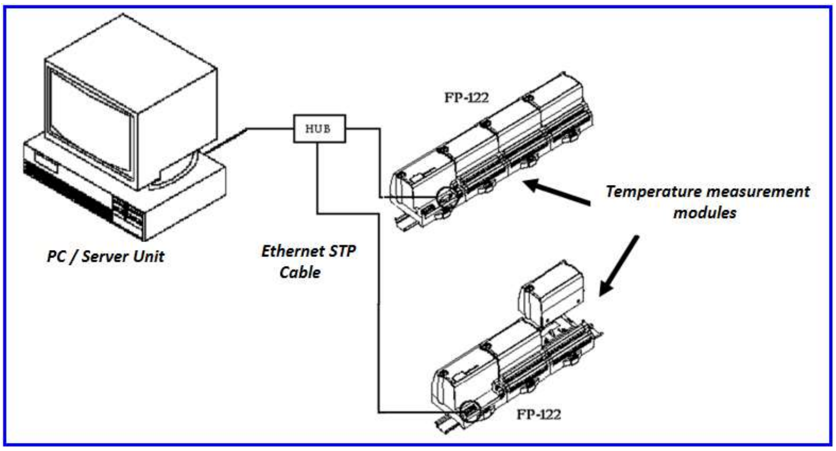


FIG. 3. Second technical local for core temperature measurement.

2.2. Software Part

Without the software part, which will be used to control or drive the hardware, the data acquisition system described above will not work properly. The association of the software and hardware parts will transform the plant PC or the server unit and the *NI* data acquisition hardware into a complete data acquisition, analysis, and presentation system. To concretize this task, we have used two development environment software products *(LabVIEW, LabWindows™/CVI)* to create a complete instrumentation, acquisition, and control applications [5].

The data acquisition software handles signal selection, sets the data acquisition software handles signal selection, sets measurement parameters (e.g., individual gains), carries out and monitors the measurement session itself and contains some simple, measurement parameters (e.g., individual gains).

A sample of the developed graphical user interfaces through this step, depicting some parameter windows, are given in the figures below.

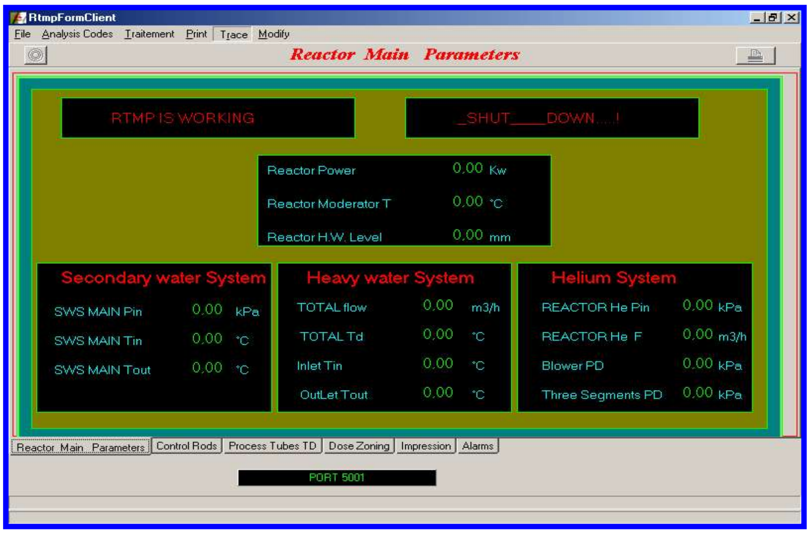


FIG. 4. Graphical user interface illustrating the reactor main parameters.

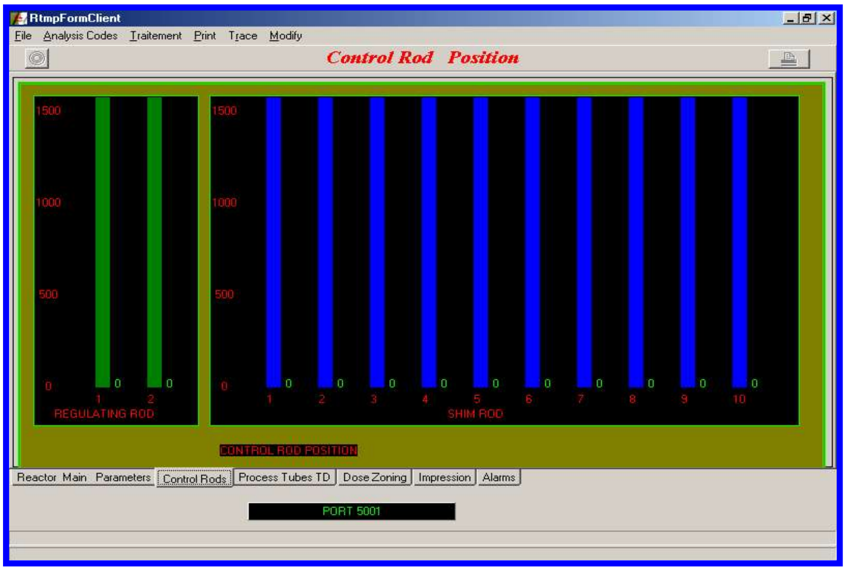


FIG. 5. Graphical user interface illustrating the regulating and control-rod position parameters.

3. CONCLUSION

The new developed system enabled us to collect all real word measured signals around the Es-Salam reactor into a powerful plant computer. We note also that additional enhancements were incorporated to this system. As an example, we note the adjunction of the higher level programming facilities, which allows us to implement the On Line Monitoring (OLM) techniques to improve the calibration and maintenance practices around the reactor.

REFERENCES

[1] ALBERT D. HELFRICK and WILLIAM D. COOPER, Modern electronic instrumentation and measurement techniques, Englewood Cliffs, N.J.: Prentice Hall, (1990).

[2] MIKE TOOLEY, PC-Based Instrumentation and control,third edition, Elsevier (2005).

[3] National instruments, M series user manual, 371022K-01, July (2008).

[4] National instruments FieldPoint Operating FP-RTD-122 and cFP-RTD-122, Eight-Channel Three-Wire RTD and Resistance Input Modules, 373348B-01, April (2003).

[5] LabWindowsTM/CVITM Core 1 Course Manual, Part Number 325668A-01, Course Software Version 2010 January (2011).

DIGITAL I&C SYSTEMS AND RELATED LICENSING ISSUES FOR THE OPAL REACTOR

A. E. VELASCO
OPAL Reactor, Engineering and Maintenance Section,
Australian Nuclear Science and Technology Organisation (ANSTO),
Australia

Abstract

This paper will present the "OPAL Reactor Digital Instrumentation System" focusing primarily on the digital First Reactor Protection System but also outlining the analogue Second Reactor Protection System and the Post Accident Monitoring System. This paper will describe the functions, architecture and the logic implementation of these systems. The paper will also outline the applied Standards and design documents, Human Factors, as well as the regulatory and design considerations that were applied during the design and implementation phases. A brief overview will also be given on the related Safety Category 2 Systems; the Reactor Control and Monitoring System and the Facilities Control and Monitoring System and their relationship and interfaces with the Reactor Protection Systems. Finally, the Verification and Validation processes employed in the Project will be described.

1. OPAL REACTOR GENERAL INFORMATION

OPAL	Stands for Open Pool Australian Light water reactor
Designed by:	INVAP Argentina
Type:	Open Pool, 20 MW_t
Plate type fuel:	U_3Si_2-Al dispersion
LEU	19.75%
Number/s:	Plates: 21, FA: 16
Core dimensions, cm (LxWxH):	104.5 x 80.5 x 80.5
Control plates:	5 hafnium (Hf)
Fluids:	H_2O moderated, D_2O reflector Upwards forced cooling of reactor core

OPAL Functions:

1. Production of Radioisotopes;
2. Neutron Beams for Experimentation;
3. Silicon Irradiation;
4. Sample Irradiations.

2. OPAL REACTOR PROTECTION SYSTEMS

The design principles adopted to achieve and maintain safety requirements:

— Redundancy and single fault;

— Diversity. The FRPS and the SRPS designs are based in different technologies;

— The RPS equipment (output boards and power supplies) on the Main Console and on the Emergency Console is physically separated;

— Independence.

— Separation - the three RPS trains are in separate instrumentation rooms. RPS cabling is routed in separate cable trays or conduits for each redundant train, including routing to sensors, actuators, racks and panels;

— The FRPS has fail-safe, fault tolerant and hot swappable design;

— Once a protective action is initiated, no manual operator intervention can prevent the trip completing its action;

— Once the system is in the tripped state it requires deliberate operator action to be reset;

— The RPS and PAM cabinets are powered by three independent Uninterruptible Power Supplies (UPS). The system additionally requires Normal Power System or Standby Power System (Diesel Generators) for its operation;

— The safety parameters and safety settings of the FRPS are transmitted to the RCMS, through a read only, electrically isolated interface;

— This allows presentation of safety information using the VDU (Video Display Units) and recording of the data using the storage system of the RCMS;

— Operators are able to manually initiate the protective actions from the MCC and ECC;

— RPS instrumentation is “floating” monitored with “Ground Fault Detectors” in the FRPS.

2.1 First reactor protection system, digital

(a) Triplicated TRICON PLC Systems. Voted in 2oo3 in the First Final Actuation Logic;

(b) Certified Class IEEE-1E (nuclear);

(c) Floating instrumentation with Ground Fault Detectors.

First Reactor Protection System Function:

— Fast Insertion of Control Rods;

— Reactor Containment Isolation;

— Containment Energy Removal;

— Reactor Protection Interlocks.

2.2. Second reactor protection system

(a) Triplicated Analogue system, based on Foxboro Spec 200. Voted in 2oo3 in the Second Final Actuation Logic;

(b) Certified Class IEEE-1E (nuclear);

(c) Floating instrumentation.

Note: Spec 200 is operating in over 100 Nuclear Power Plants with over 1 000 000 modules-hours in operation.

Second Reactor Protection System Function:

(a) Partial draining of the Reflector Vessel.

2.3 Post-accident monitoring system

(a) Dual redundant Analogue system, based on Foxboro Spec 200;

(b) Certified Class IEEE-1E (nuclear);

(c) Floating instrumentation.

Post-Accident Monitoring System Function:

(a) Displays to operators Monitored Plant Variables;

(b) Triggers Evacuation Alarm;

(c) Surveillance TV cameras;

(d) Paging and communication System.

3. FRPS ARCHITECTURE

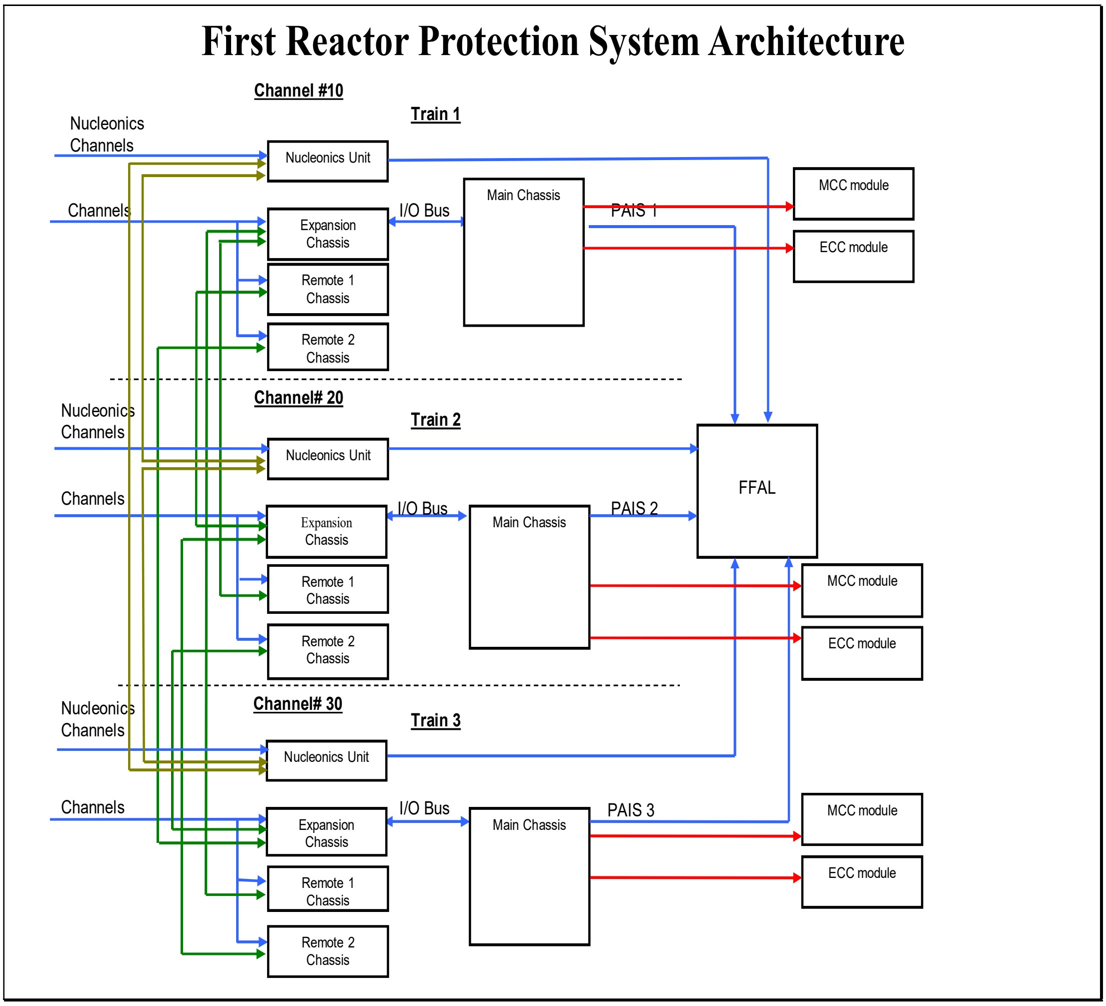


FIG. 1. FRPS - system architecture.

3.1. Architecture description

The FRPS incorporates all three channels of each of the field inputs into each of the three TRICON (trains). Each train includes four TRICON chassis as follows:

(a) Main Chassis;

(b) Expansion Chassis;

(c) Remote chassis 1;

(d) Remote chassis 2.

Each TRICON independently performs all the bistable comparisons for all of the field inputs and performs the 2oo3 logic on the bistable outputs within the same operating cycle. This in effect removes the downstream Main Processor from the operating cycle.

Each input channel (process variable) is connected to three input modules, one for each train. Each of the three trains has three TRICON Main Processors Modules located in a main chassis. The interconnections between the input channels in the Expansion Chassis and the three Main Processors are via copper cable. The interconnections between the input channels in Remote Chassis and the three Main Processors are via isolated fibre-optic cable; this provides Class 1E isolation between the inputs related to different channels of the related main Chassis.

In this scheme each field input is converted independently in all three trains, thus increasing the number of field inputs by a factor of three. It should be noted that within each train, all the bistable and trip logics are completely repeated (three times) in each TRICON Main Processor.

Each train produces a Protection Action Initiating Signal, and they are voted in a 2oo3 Configuration in FALs (using relays).

Each train is powered from an independent battery backed UPS.

3.2. Trip 1 – reactor shutdown

The drawing (OVERVIEW-REACTOR SHUTDOWN) in Fig. 2 shows a simplified overview of the Trip 1 system. In the input boards analogue or digital, each input channel is triplicated into three internal channels, then going through a validation process (median select for analogue input and two-out-of-three for digital). The validated input signal is converted by software to engineering units and then compared to the set point to generate a trip signal. The trip signals are voted in the 2003 voting logic and finally the Protective Logic driving the triplicated output boards for tripping the First Shutdown System when required.

3.3. Containment Isolation (CI)

Containment Isolation (CI) represents the second of the FRPS protective actions of the reactor. The validation process is performed as before. When any of the Stack Activity or Stack Rate signals exceed their Safety Setting Values OR there is a “Group 1 Request” the Group 1 Valves will close.

3.4. Containment Energy Removal System (CERS)

Containment Energy Removal System (CERS) represents the third of the FRPS protective actions of the reactor.

The purpose of the CERS is to enable the operation of the RPS logic to control the commutation of the chillers and associated equipment after a pre-set time delay. Automatic commutation is triggered by related field inputs exceeding setpoints. The FRPS logic provides for both automatic and manual control of the CERS.

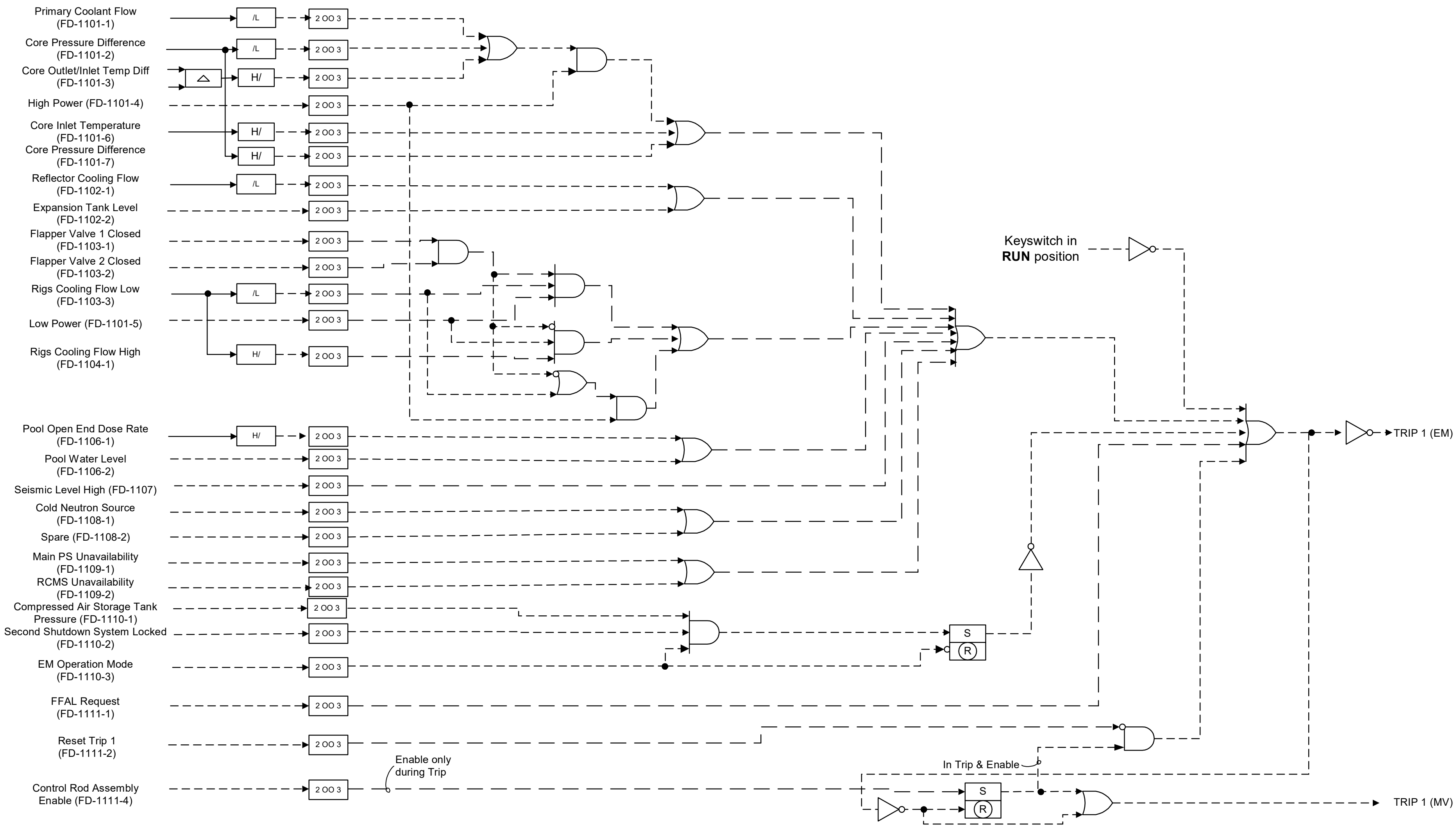


FIG. 2. Overview – Trip 1 reactor shutdown.

4. SECOND REACTOR PROTECTION SYSTEM

4.1. SRPS system function

The Second Reactor Protection System is a hardwired (non-sampling) control system, which monitors the 5 Control Rod Down statuses to insure proper completion of the reactor shutdown when the Trip1 command is initiated by the FRPS. The SRPS also monitors Process Variables and operator selected modes to provide a tripping capability independent of the FRPS. Logic evaluates the system inputs and generates a trip (Trip 2) when necessary and transmits it to the Second Final Actuation Logic (SFAL) system.

The system contains 3 main processing functions Input conversion, Processing and Logical operation, and output conversion and isolation. The input conversion portion of the system converts the field signal levels of 4-20 mA, to 0-10 Vdc analogue values and dry contact closure logic states to 0.5-15 Vdc, respectively. The processing and logic portion of the system performs operations to evaluate process conditions based on FRPS Trip status, and operator selected operating modes. The output and isolation portion provides conversion of the internal analogue and logical signals to 4-20 mA and Contact closure outputs. This portion of the system is responsible for providing isolation between the trains and between 1E and Non-1E systems.

5. POST-ACCIDENT MONITORING SYSTEM

5.1. PAM system function

The Post-Accident Monitoring System (PAMS) provides primary information required to allow operators to take specific actions that are essential for the safety systems to meet their safety function beyond the Design Basis Accident (DBA). Moreover, it supplies information to indicate whether plant safety functions are being met, while also being a very important tool to implement manual recovery actions.

(a) The measurement channels of the Post-Accident Monitoring System are capable of reporting the state of the engineered safety features and that the reactor is in safe shutdown mode.

(b) The Post-Accident Monitoring System comprises all electrical devices and circuits that generate the signals that will be displayed at the Main Control Room and Emergency Control Centre.

(c) Plant variable monitoring is implemented with hardwired technology, Foxboro Spec 200.

(d) Surveillance TV cameras. Certified Class IEEE-1E (nuclear).

(e) Paging and communication System. Certified Class IEEE-1E (nuclear).

6. REACTOR CONTROL & MONITORING SYSTEM

(a) Foxboro I/A Series, Distributed Control System.

(b) Interface between First Reactor Protection Systems and Reactor Control & Monitoring System function through isolated and read only dual redundant digital communication channels. Foxboro Proprietary Communication links to the three Triconex safety trains.

(c) Interface between Second Reactor Protection System and Post Accident Monitoring System and the Reactor Control & Monitoring System Function through IEEE-1E certified analogue and digital isolators.

(d) Foxboro I/A Series DCS with two separate functions, RCMS and FCMS.

(e) Modbus communication with:

— Cold neutron source, Eurotherm controller;

— Radiation monitoring, INVAP microcontrollers;

— Building HVAC system;

— Fire protection system;

— Diesel generators.

6.1. Facilities control and monitoring system

(a) Beam ports.

(b) Cold neutron source:

— Control and monitoring;

— Protection system.

(c) Irradiation facilities:

Long residence time (pneumatic) facilities;

— Bulk irradiation facilities;

— Silicon facilities;

— Irradiation scheduling program.

7. HUMAN MACHINE INTERFACE

(a) Operator consoles:

— Visual display units driven by the RCMS;

— Alarm manager;

— Radiation monitoring, electrical, irradiation facilities;

— Protection systems parameters;

— Control rods.

(b) PAM panel:

— PA system, evacuation alarm, data recording;

— Video display;

— All parameters displayed;

(c) Wall panels:

— Hardwired control and indication panels;

— Status display for reactor protection systems. One panel per train;

— Post accident monitoring system display.

8. OPAL I&C LICENSING ISSUES RELATED TO I&C SYSTEMS

Regulator required to approve every Safety, and Safety related systems package prior to a step in the process e.g. design to manufacture, to installation.

Regulator inexperience with digital systems. Consultants used.

The supplier of the digital reactor protection system was not known at the time of contract award. The regulator was concerned about the use of uncertified products. Even when TRICON was chosen it was not Class 1E certified. Approximately 6 months later certification was achieved and this was a big plus in the licensing process.

Verification & Validation, and Human Factors issues were the two main areas of concern for the regulator.

Regulator had concerns about the inadvertent movement of two control rods and/or the speed of withdrawal of a control rod. These concerns resulted in a new Safety Cat 1 system being used to monitor and inhibit excessive control rod withdrawal speed and simultaneous rod withdrawal (control rod movement protection interlock CRMPI).

Regulator was also concerned with isolation devices used between safety trains and between safety and non-safety systems.

Regulator was also concerned with using the same brand of relays for Final Actuation Logic in FRPS and SRPS. The SFAL design was changed.

Regulator was also concerned with channel separation in RPS consoles. The consoles were redesigned after FAT-BRC and tested exhaustively.

Regulator was also concerned with channel separation in FRPS Nucleonics Isolation modules. During installation qualified opto-couplers were added for sending voting signals between channels.

Concerns about the scan rate of the PLC led to use of hardwired Protection System for nucleonics.

The FRPS application software used Foxboro standard corporate products, using corporate software designed in accordance with procedures and processes developed to satisfy the requirements of ASME NQA-1. In this application there was no need to generate any source or object code specifically for OPAL.

9. VERIFICATION AND VALIDATION

The V&V process was done according to the Verification and Validation plan during all the phases of the process to assure the systems met the functional, performance and reliability requirements. The key document used throughout the V&V process were the Functional Drawings (FD), see Figures 1, 2 and 3. The plan was according to Safety category 1 (IAEA safety System, NRC Safety Related). The Verification of all equipment was done at unit and system level and validation at the system level only. The application used Foxboro standard corporate software designed in accordance with procedures and processes developed to satisfy the requirements of ISO 9001 and ASME NQA-1 as appropriate. The application software did not generate any source code or object code built specifically for OPAL. In this case the term software includes firmware, microcode and documentation. Because of the nature of the scope of the application the plan for the V&V processes were focused on documentation effort. The FRPS was designed to use safety software assembled by a linkage processor (Tristation 1131) for implementation and Configuration.

TABLE 1. VERIFICATION AND VALIDATION PROCESSES

V&V Methods and tools:	Manuals (criticality level: 1/low) Plans (criticality level: 2/moderate) Reports (criticality level: 3/major) Procedures and drawings (criticality level: 4/high)
Life cycle processes	**Task**
1-Management.	System Project management plan System Verification and Validation Plan QA Plan System Configuration and Control Plan. IEEE qual. Plan. Risk management Plan. Maintenance requirements and Surveillance test Plan.
2-Preliminary design	System architecture sketch. Traceability Analysis.
3-Detail design	Functional Drawings. Functional Block Diagrams. FRPS software V&V review for Functional Blocks. Rack Load Drawings. Termination Drawings. Connection Drawings. Power Drawings. Steel Drawings. System Description. Factory Acceptance Test Procedure. Failure Modes and Effect Analysis. Hardware Requirements Specifications. Reliability Analysis. Mean Time Between Failures/ Mean Time to Repair
4-Implementation.	No V&V activities.
5-Integration and test	Functional Drawings. System Testing (Checkout)
Demonstration	**Factory Acceptance Test**
Shipment.	All System Drawings: FD; RL; CD; TD; PWR; SF. Certificates of Conformance (Individual module)
Surveillance and maintenance	Operations, Surveillance, and Maintenance Manuals.

Programming for FRPS/RCMS was done by Foxboro. INVAP Nuclear Division reviewed it and used INVAP's Space Division to do an independent V&V.

ANSTO did not have the personnel to do V&V to the level INVAP was working, so instead reviewed the V&V procedures and participated extensively in Factory, and Integrated, Acceptance Test programs.

10. V&V TESTING REQUIREMENTS

(a) Foxboro Factory Acceptance Tests (Foxboro Mass. June 2003).

(b) INVAP Integrated Systems Test (S.C. Bariloche Arg. June 2004). Using Automatic Test Unit for FRPS, SRPS and PAM.

(c) Pre-commissioning Tests.

(d) Commissioning Tests.

11. HUMAN FACTORS LICENSING GENERAL ISSUES

(a) Regulator required ANSTO to provide external expert to review HFE program.

(b) AXIOM Technology trained ANSTO personnel using Nureg 0700 principles.

(c) I&C in charge of HFE program at OPAL.

(d) Program for HFE reviews during installation inspections initiated.

12. MAIN I&C HFE ISSUES

(a) Main Control Room and Emergency Control Centre consoles and panels.

(b) RCMS screens. ANSTO provided INVAP with a Graphical Interface design manual and this was used in the screen setup (eg for the use of colours).

(c) Ergonomics of field instruments for operators and maintenance.

13. SUMMARY

I&C Design complies with Australian and International regulations, codes, and IEEE standards.

All Safety Category 1 and 2 I&C components preapproved by the regulator prior to manufacture, purchase, installation and testing.

Protection Systems supplied from Qualified Nuclear Suppliers with excellent Operational History.

DCS system supplied from the same company as the Protection systems, eliminating problems in communications between systems.

Human Factors and Ergonomic principles adopted for all areas of Human Machine Interface

Planning started for Digital system replacement using 10 year rule.

14. STANDARDS AND RELEVANT DOCUMENTS FOR RPS CATEGORY 1 SOFTWARE AND QUALIFICATION

[1] IEEE Std 1012 – 1998, IEEE Standard for Software Verification and Validation.
[2] IEEE Std 1058 - 1998, IEEE Standard for Software Project Management Plan.
[3] IEEE Std 1042, IEEE Guide for Software Configuration Management.
[4] IEEE Std 730 – 1998, IEEE Standard for Software Quality Assurance Plans.
[5] IEEE-ANSI 7.4.3.2 – 1993, Standard Application Criteria for Programmable Digital Computers In Safety Systems of Nuclear Power Generating Stations.
[6] IEC 880, Software for Computers in Safety Systems in Nuclear Power Stations.
[7] SPEC 200 Qualification Documentation Book 170.
[8] Triconex Qualification Documentation.
[9] INVAP Engineering Documents.

MODERNIZATION OF BAEC TRIGA RESEARCH REACTOR BY INSTALLING DIGITAL CONTROL CONSOLE SYSTEMS AND ASSOCIATED FACILITIES

M. A. SALAM*, A. HAQUE, M. A. MALEK SONER, M. MEZBAH UDDIN, M. B. SHOHAG, R. HASSAN, M. MOTIAR RAHMAN, M. A. SARDER

Center for research Reactor, Bangladesh Atomic Energy Commission
E-mail of main author: masalam61@gmail.com, crr.baec@gmail.com

Abstract: Digital instrumentation & control (I&C) systems of BAEC TRIGA Research Reactor (BTRR) was installed in June 2012, replacing the old analog control systems. BTRR was achieved its first criticality in September 1986. The thermal power of the research reactor is 3 MW. The reactor has been used for manpower training, research, radioisotope production, and various R&D activities. Analog based control console as well as the associated instrumentation and control (I&C) system of the reactor got backdated day by day because of the advent of PC based digital control system. Most of the spare parts of the analog console and the I&C system are out of production and as such are not available in the market. Considering these facts, installation of a digital control console and I&C system based on the state-of-the-art digital technology became necessary. The I&C system includes dedicated hardwired displays and controls such that safe operations can be continued even when the computers are not available. The system consists of three separate computer systems: the Data Acquisition and Control Unit (DAC), the Control System Console (CSC), and the User Interface Terminal (UIT). The CSC and DAC systems run under Linux operating system and the UIT runs on Windows. The Reactor Protection System (RPS) is contained within the CSC and DAC. The digital I&C system of the reactor includes wide range of instrumentations for monitoring reactor parameters during all operational states and for recording values of the process variables important to safe reactor operations. Besides this, the Neutron Radiography (NR) facility has been modernized by the addition of a digital neutron radiography set-up at the tangential beam port. The Neutron Scattering (NS) facility also has been upgraded by the installation of a high performance neutron powder diffractometer at the radial beam port-2 of the reactor. A project funded by Bangladesh government has been submitted for strengthening the safety of the research reactor. Under this project modernization, refurbishment, extension and upgradation of different systems of reactor will be done including procurement of spare parts for digital instrumentation and control system. Bangladesh Government has taken decision to install a new high power multipurpose research reactor in near future. The paper focuses on the features of the digital I&C system, different systems renovation and modernization activities of the BTRR.

Key words: Research reactor, Digital control console, Reactor safety, System upgradation

1. INTRODUCTION

Since its commissioning in 1986, the 3 MW TRIGA Mark-II research reactor has been operated for manpower training, radioisotope production (Iodine-131, Sc-46, Tc-99m), and various R&D activities in the field of neutron activation analysis (NAA), neutron radiography (NR), and neutron scattering. The reactor can be operated in pulsing mode with a maximum reactivity insertion of up to \$2.00 (1.4% $\Delta k/k$). With the present core configuration, the peak power during pulsing is 852 MW with a half maximum pulse width of about 18.6 ms. The reactor can be operated up to a power level of 500kW under natural convection cooling mode. Operation above 500kW needs forced convection cooling.

The reactor was in operation with an analog I&C system for about 25 years. The system included several sub-systems each of which consisted of various types of analog electrical and electronic circuits and a wide range of electromechanical and pneumatic devices and components. With the passage of time it became very difficult to get spare parts for old the analog system. So, it was decided to replace the analog control system by a digital one. As such, a project was implemented in 2012 under the framework of Annual Development Program (ADP) of the government for procurement and installation of a digital control system involving the original reactor supplier, the General Atomics of the USA.

2. DIGITAL INSTRUMENTATION AND CONTROL SYSTEM

The digital reactor I&C system has been designed and manufactured to comply with the guidance given in American Nuclear Society (ANS) ANSI Guide ANSI/ANS 15.15-1978, 'Criteria for the Reactor Safety Systems of Research Reactors' and the IAEA Safety Series 35-S1, particularly with respect to physical separation and electrical isolation of the reactor protection system (RPS). The reactor I&C system include instrumentation for monitoring reactor parameters during all operational states and for recording all variables important to reactor operation. It also manages all control rod movements taking into account the choice of operating mode and interlocks. The I&C system is a computer-based system, but includes dedicated hardwired displays and controls so that safe operation can continue if the computer become unavailable. Fig. 1 shows a photograph of installation of Digital Control Console system at the control room of the BAEC TRIGA reactor facility. The major components of the I&C system are described below.

Control System Console (CSC): The CSC is a desk-type control console. The reactor operator controls the operation of the reactor from the CSC using several control switches such as mode switches, keyboard in the CSC, etc. Information is fed back to the operator through high-resolution color monitor and various indicators and annunciators. The rod positions are adjusted by UP/DOWN push buttons on the CSC Rod Control Panel. During reactor operations, the CSC receives data from the DAC, processes these data, and presents the data in meaningful engineering units and graphic displays on several peripheral systems. The CSC also provides data storage and logging capabilities on the computer hard drive.

Data Acquisition and Control Unit (DAC): The DAC is a computer-based system that provides interface functions between the CSC and the reactor. It acquires data in the form of electronic signals from instrumentation in the reactor and auxiliary systems, processes it, and transmits it to the CSC for display.

Fuel Temperature Monitoring Channels (NFT-1000): There are two fuel temperature-monitoring channels, each of which monitors the fuel temperature measured by a thermocouple inserted in to the instrumented fuel rod. There are three thermocouples located in each of the instrumented fuel rods, which are installed in the inner part of the reactor core. Each fuel temperature channel is an independent fuel temperature monitoring system housed within a compact enclosure. Each channel contains a millivolt-to-current signal conditioner, power supplies, trip circuits, isolation devices, and computer interface circuitry. The trip circuit is hardwired into the scram circuit. The isolated analog outputs are monitored by the DAC and are hardwired to analog temperature indicators on the CSC and to the multi-point recorder.

Wide-Range Log Power Channel (NLW-1000): This component is a wide-range, fission-chamber-based, logarithmic power-monitoring channel housed within a compact enclosure. It combines count rate and current measuring techniques to cover ten decades of neutron flux ranging from less than 0.3 to 10^{10} nv (n/cm^{2}sec), and provides adjustable bistable trips for local and remote alarms and signals for isolated

FIG. 1: Digital Instrumentation and Control System of the BTRR.

digital and analog outputs. The channel includes power, period, and high voltage meters. The isolated analog outputs are monitored by the DAC and are also hardwired to analog power indicators on the CSC and to the multi-point recorder.

Multi-Range Linear Power Channel (NMP-1000): This component is a linear, current-to-voltage signal conditioner with manual or automatic range switching. The input range is 10^{-11} to 10^{-3} amps from a compensated ion chamber. The unit has adjustable bistable trip circuits for local and remote alarms, and isolated analog and digital outputs. The ranges can be controlled remotely from the CSC or locally at the channel itself. The unit is enclosed in a compact enclosure. The isolated analog outputs of the NMP-1000 are monitored by the DAC and are also hardware to the analog power indicator on the CSC and also to the multi-point recorder.

Safety Power Channel: Safety power channel is an independent linear power monitoring system housed within a compact enclosure located in the DAC cabinet. Each channel contains a neutron detector, current-to-voltage signal conditioner, power supplies for the channel electronics and the neutron detector, trip circuits, isolation devices, and computer interface circuitry. The power trip circuit is hardwired into the scram system. The isolated analog outputs are monitored by the DAC and are hardwired to analog power indicators on the CSC and to the multi-point recorder. The safety power channel can be modified to include reactor pulse monitoring through the use of neutron flux (nv) and fluence (nvt). BAEC TRIGA reactor has two safety power channels NP-1000 and NPP-1000. The safety power channel, NPP-1000 is associated with pulsing mode of operation of the reactor.

Control Rod Drives: The digital control system permits the control rods to be move either as a bank or individually. The control rod drives are mounted on the reactor bridge. The control rod drive mechanism is an electric stepping-motor-actuated linear drive equipped with a magnetic coupler and a rod position potentiometer. A stepping motor drives a pinion gear and a 10-turn potentiometer via a chain and pulley gear mechanism. The potentiometer is used to provide rod position information. The pinion gear engages a rack attached to the magnet drawtube. The control rod drives are connected to the control rods through a connecting rod assembly. An electromagnet, attached to the lower end of the magnet draw tube, engages an iron armature that is screwed and pinned into the upper end of the connecting rod. The lower end of the connecting rod is attached to the control rod assembly. The magnet, the armature, and the upper portion of the connecting rod are housed in a tubular barrel that extends below the reactor bridge. A piston is located part way down the connecting rod. The lower portion of the barrel has a water snubber to provide a damping action when the electromagnet is de-energized and the control rod is released.

Reactor Protection System (RPS): The RPS initiates a reactor scram in response to a trip in the scram circuit, a manual scram signal, or an external scram signal by interrupting the current to the electromagnets that link the control rods to the control rod drives. After a delay of only about 25 ms (for the magnetic field to decay), the magnets release the control rods, which fall into the core by gravity, taking about one second to fully insert. All scram conditions are automatically indicated on the display monitor. The manual scram may be used for a normal fast shutdown of the reactor. The reactor can also be scrammed by turning the magnet power key switch to the off position. The RPS is automatic and completely independent of other systems, including the power regulating system. The scram circuits and components are completely hardwired and do not in any way depend on the CSC computer, the DAC, or any software to perform a scram. Furthermore, the reactor I&C system and RPS are designed such that there are no means available to the reactor operator to bypass the trips and operate the reactor at conditions that are beyond the limits defined by the trip set points. The safety channels comprising the RPS are both physically separated and electrically isolated from the reactor I&C system and all other peripheral I&C systems. The highest voltage anywhere in the reactor I&C system is 750Vdc. The design satisfies the electrical isolation requirements of IEEE 603. The CSC and DAC computers are continuously monitored for proper operation via watchdog circuits which are capable of shutting down the reactor in the event of computer malfunction

Peripheral I&C System: The peripheral I&C system being used in the BAEC TRIGA reactor includes the thermal power calculator (TPC), ECCS (Emergency Core Cooling System) status monitoring system, area radiation monitoring system, etc. Presently all those systems use analog electronic. However, it is expected that the above systems would also be upgraded in near future using digital technology based systems.

DIGITAL CONSOLE SOFTWARE SYSTEM

The basic control system consists of three separate computer systems: the Data Acquisition and Control Unit (DAC), the Control System Console (CSC), and the User Interface Terminal (UIT). Fig. 2 shows the Digital Console software architecture. The CSC and DAS systems run under Linux operating system and the UIT runs on Windows operating system. The UIT is simply a display terminal and is not used at all in the control of the reactor. The computerized control components of the TRIGA system communicate with one another using the TCP/IP protocol across an Ethernet network. The TRIGA Digital Console Software is responsible for the following functions:

- reading the inputs and status of the reactor,
- as needed, interpreting and computing results based on those inputs,

- displaying the results on the UIT display, and
- scramming the reactor and handling other system trips.

The software scrams the reactor only when there is a connection failure among the CSC or DAC, DAC or UIT, CSC or UIT. But other safety related scram is not dependent on software and other scrams are hardware dependent.

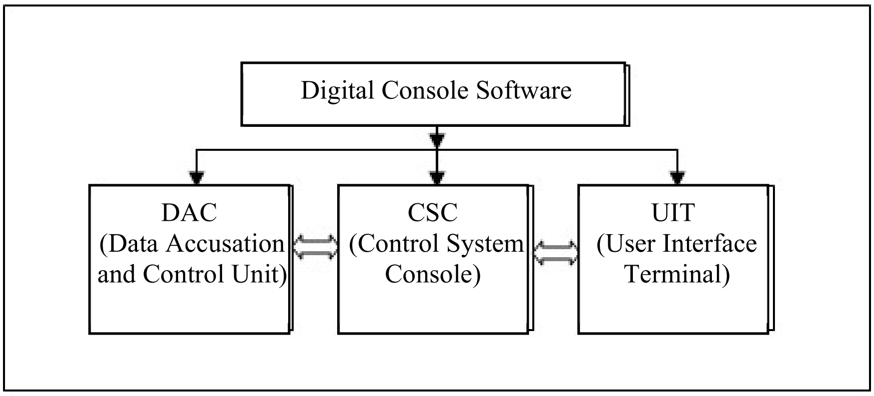


FIG. 2: Digital Console System Software

The CSC is the master component in the system. The DAC and UIT receive commands and are controlled by the CSC. During system startup, the three systems go through independent initialization phases. After initialization, the DAC and UIT await for commands from the CSC. The CSC, after initialization, waits for the DAC and UIT to come on line (initialization is a asynchronous operation for the three systems) and once they are all on line, the CSC sends them an "all ready" message and the main processing begins.

The DAC system is, essentially, an Ethernet-based digital and analog I/O subsystem. It reads data from analog and digital inputs and sends this data over the Ethernet to the CSC and it receives data from the CSC via the Ethernet and writes that data to the analog and digital outputs. The DAC also has a background task that checks system integrity and verifies that it is receiving commands from the CSC on a periodic basis. Should the background task determine that communication has been interrupted; it will SCRAM the reactor (if operating), reinitialize itself, and wait for the post-initialization communication sequence from the CSC.

The UIT, which is a graphical display process, is responsible for maintaining the graphic displays and (optionally) processing mouse events. This process responds to command requests sent from the CSC and sends commands to the CSC (independent of requests from the CSC). The UIT is a Win32 system that is responsible for the user interface for the TRIGA applications.

The digital I&C system of the BAEC TRIGA reactor can be used to operate the reactor in five different modes namely, manual, automatic, pulse, square wave and prestart. The manual and automatic modes apply to the steady-state reactor condition. These modes may be used for reactor operation from source level to 100% power level. The pulse mode allows the operator to produce very high, short duration power pulses [with a peak power of 852 MW (max) and half maximum pulse width of about 8.6ms]. The square wave mode allows the power level to be raised quickly (within a few second) to a desired level. After the power has risen to a certain limit, then the system switches to automatic mode. Once in automatic mode, the system maintains a constant power level. The prestart mode is used to run diagnostic tests on the various system devices. Prestart tests are limited to those devices which can cause the reactor to scram.

4. MODERNIZATION OF BEAM PORT FACILITIES

The TRIGA Mark II has four beam ports namely tangential, piercing, radial-1 and radial-2. Two modern experimental facilities have been installed in the tangential beam port and radial-2 beam port under different annual development projects (ADP) of Bangladesh. Tangential beam port is used for digital neutron radiography facility and radial beam port -2 is used for the high performance neutron diffractometer – SAND (Savar Neutron Diffractometer).

4.1 Installation of Digital Neutron Radiography Facility

Neutron Radiography Facility was used for nondestructive testing (NDT) of materials with an objective to utilize the reactor more potentially. The film neutron imaging method is being used from the beginning of the facility. Recently, digital neutron radiography set-up has been added to the facility along with a change in biological shielding arrangement. Introduction of digital neutron set-up has significantly reduced the experimental time and digitized images of the objects are obtained very fast and processed by software to improve the quality. The digital neutron radiography set-up has been procured under the ADP project of Bangladesh government. However, film technique is still used in parallel for some specific purposes. Fig. 3 shows the schematic diagram of the digital neutron radiography set-up.

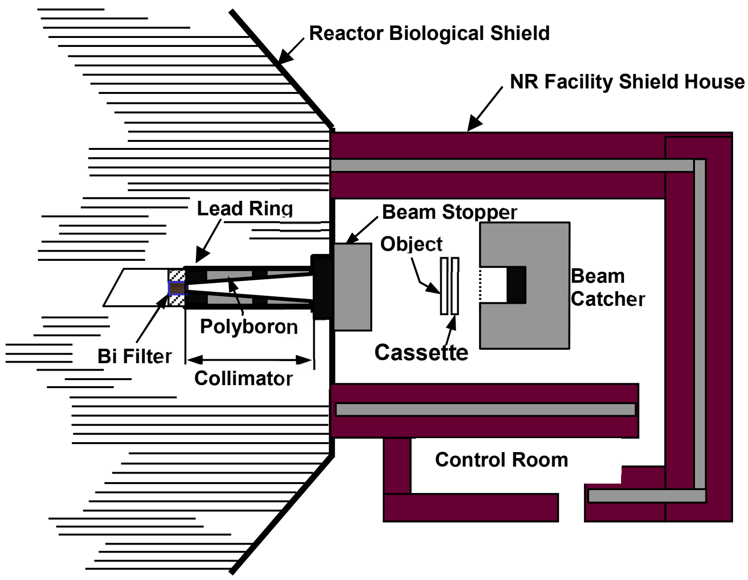


FIG. 3: Schematic Diagram of the Digital Neutron Radiography Facility.

4.2 Installation of High Performance Neutron Diffractometer

The program of Reactor and Neutron Physics Division (RNPD) is entrusted with the responsibility to utilize the TRIGA Mark II research reactor which is the only one of its kind in Bangladesh. The high performance neutron diffractometer – SAND (Savar Neutron Diffractometer) has been installed on Radial Beamport-2.

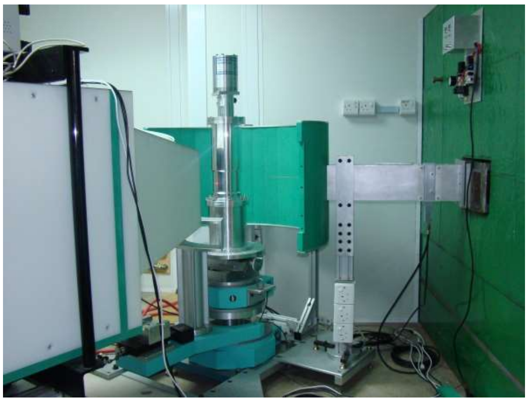


FIG. 4A: Savar Neutron Powder Diffractometer

FIG.4B: System Control Electronics and Detector

Fig. 4 shows the Savar Neutron Diffractometer (SAND). Neutron Scattering (NS) experiments involve directing a beam of neutrons at a specimen and then detecting the energy of neutrons at which they are scattered at different angles after interacting with the atoms in the specimen. The NS experiment is mainly concentrated on elastic scattering or diffraction phenomena. Internal details of condensed matter such as its crystalline state, location of atoms in the crystal lattice, phase transitions and other structural information can be determined by this technique.

5. FUTURE PLAN FOR UPGRADATION, MODERNIZATION AND RENOVATION OF DIFFERENT SYSTEMS OF BTRR

A project title: "Balancing, Modernization, Refurbishment and Extension (BMRE) of Safety Systems of the 3 MW TRIGA Mark-II Research Reactor Facility at AERE, Savar, Dhaka" funded by Bangladesh Government has been submitted to the government for strengthening the safety of the research reactor. The main objectives of the project are-(i) To increase operating life of the reactor (about 20 years) by implementing ageing management of different system/components of the reactor including electrical sub-station; (ii) To continue nuclear research, isotope production, manpower development and training & education for the students of different universities, assuring safe operation of the reactor; (iii) Procurement of spare parts for Digital Control Console and other associated systems of the reactor and (iv) Construction of spent fuel storage facility for TRIGA spent fuel elements. The main renovation and replacement works of different systems of the reactor to be carried-out under this project are - Reactor Hall Ventilation System, Emergency Core Cooling System, Fire Detection & Alarm System, Electrical Substation, Physical Protection System & Security Lighting and Radiation Monitoring System Major modernization works under this project are- Digital Area Radiation Monitoring System; Digital Reactivity Meter and High Radiation Tolerant Under Water Video Inspection System for Reactor Pool Liner Inspection.

6. CONCLUSIONS

The I&C system plays the key role to ensure safe operation of nuclear reactors. With the advent of digital technology, reactor I&C systems are also becoming more and more digital. Unavailability of analog spare parts is also a factor for digitalization. The dedicated hardwired displays and controls as well as the watchdog circuits of the PC based digital I&C system of the BAEC reactor provide a strong safety regime for the operation of the reactor under all operational modes. After modernization of the beam port facilities, neutron based R&D activities have been increased significantly. Different systems renovation, modernization and upgradation of BTRR will be done under the research reactor BMRE project. The digital I&C system will also be helpful for the BAEC professionals to develop better understanding about the I&C systems of the future high power research reactor as well as power reactors in Bangladesh.

7. BIBLIOGRAPHY

[1] Safety Analysis Report of the BAEC 3 MW TRIGA MARK-II Research Reactor, BAEC, Dhaka (2006).

[2] General Atomics (San Diego, CA), "Operation and Maintenance Manual TRIGA Reactor Control System for BAEC", Document No. T8S100A100-001 Revision A December 10 2012 Document Level 1.

[3] M. A. Salam, A. Sarder, A. Kalam, A. Haque. M.A.M.Soner. M.M. Uddin, M. Shabuddin, M. M. Rahman, A. Rahman, B. Shohag, M. Rahman, M. G. S. Islam I. Kamal, M.M. Haque, and M. A. Zulquarnain "Refurbishment, Modernization and Ageing Management Program of the 3MW TRIGA Mark-II Research Reactor of Bangladesh." Conference of International Group of Research Reactor (IGORR) 2013 & IAEA Technical Meeting, October 13-18, 2013, Daejeon, Republic of Korea. Proceeding of IGORR 2013, Abstract page 95, Full paper: CD Rom, Index Number: 02-1038.

[4] M. M. Haque, M. A. M. Sonar, P. K. Saha, M. A. Salam, M. A. Zulquarnain, "Operation an Maintenance Status of the 3 MW TRIGA Mark-II Research Reactor of Bangladesh"-International seminar on nuclear safety, operation and maintenance of nuclear facility course, RADA, Japan, Sep. 26-Oct. 07, 2005.

[5] General Atomics (San Diego, CA), "Reactor Instrumentation & Control system console upgrade, BAEC TRIGA Reactor Facility at Savar, Bangladesh".

[6] General Atomics (San Diego, CA), "TRIGA Digital Console Software Specifications".

[7] IAEA Safety Series No. 35-S, Code on the Safety of Nuclear Research Reactors: Design, International Atomic Energy Agency (IAEA), Vienna, 1992.

[8] Hashemian H.M, "Nuclear Power Plant Instrumentation and Control", Analysis and Measurement Services Corp, United States (www.intechopen.com).

I&C SYSTEMS OF THE NEW BRAZILIAN MULTIPURPOSE REACTOR – RMB

B. SERRÃO[1]
[1]Amazul S.A., São Paulo, Brazil
bruno.serrao@amazul.gov.br

Abstract. The Brazilian Multipurpose Reactor (RMB) has been developed to be the new Brazilian research reactor and will be used for radioisotope production and material tests. The RMB structures, systems and components are similar to OPAL Australian reactor, which has already completed 10 years of successful operation. This study aims to present and discuss the I&C systems that are being used in the preliminary engineering design stage of the RMB reactor, as a new facility sharing contribution. All components of I&C Systems classified as safety related will be safety qualified and for other systems classified as non-safety related components will be “off shelf” type. The Reactor Protection System (RPS), Post-Accident Monitoring System (PAMS) and Radiation Monitoring System (RMS) are those systems safety related. The Control and Monitoring System (CMS) is non-safety related. The RMB reactor I&C Systems will be digital technologies applied for protection, controlling and monitoring the process variables by digital and analog human-machine interfaces (HMI). These architecture and engineering concepts reduce the potential for human errors and relieve the stress for personnel operating, ensuring high safety to the facility, making it an “walk away” reactor.

Key Words: RMB, I&C Digital Systems, Research Reactor, Open-pool Type Reactor.

1. INTRODUCTION

The RMB design has been developed in Brazil to meet two main objectives: radioisotope production, for medical and industrial applications, and material tests, with a wide range of neutron flux. Medical radioisotopes decay with time, some of them with a really short mean-life, what justifies a national production of these products.

The reactor will be of open-pool type and will be able to operate in four states: Power State, with reactor power up to 30 MW; Test State, with reactor power up to 400 kW; Shutdown, with reactor in a safe shutdown mode; and Refueling State, where core configurations can be carried out.

In order to protect and control the reactor, which can have maximum neutron flux values around 4 x 10^{14} n/cm².s, digital technologies to I&C systems have been developed to assure high reliability for RMB reactor.

This paper aims to present and discuss the I&C systems that were used in the preliminary engineering design stage of the RMB reactor, as a new facility sharing contribution, and discuss possible improvements in next design stages. Some difficulties of implementation are also discussed through document.

2. INSTRUMENTATION AND CONTROL (I&C) SYSTEMS

The RMB mixes analog, digital and hybrid I&C systems. Table I shows an overview about types of RMB I&C systems.

TABLE I. OVERVIEW OF I&C SYSTEMS TYPES

Instrumentation and Control System	Type
Neutronic Instrumentation System (NIS)	Digital
First Reactor Protection System (FRPS)	Digital
Second Reactor Protection System (SRPS)	Analog
Control and Monitoring System (CMS)	Digital
Post-Accident Monitoring System (PAMS)	Analog
Radiation Monitoring System (RMS)	Digital
Human-Machine Interface (HMI)	Hybrid

All I&C Systems are required in order to ensure safety for RMB reactor, mostly because the concept that this is a "walk away" reactor, a reactor with a set of intrinsic safety functions and actions which guarantees a reactor safe condition even without personnel operating interventions. Only digital parts of I&C systems will be fully described during next sections. Analog parts will only be presented.

2.1. Neutronic Instrumentation System (NIS)

NIS ensures the neutron flux measurement covering the reactor's operating range from start-up level to 125% of full power level. Each channel – start up channel, wide range log channel, power channel, wide auto-range linear channel, nitrogen 16 linear channel and Self Powered Neutron Detector (SPND) linear channel – performs measurements on his own range, and sends signals to different systems – RPS, PAMS and CMS.

NIS safety related channels, which means providing real time data to FRPS, SRPS and PAMS, work sending data through direct hardwired signals. NIS non-safety related channels, which means sending information to RCMS and FCMS, work sending information through electrical isolation devices to keep electrical and physical separation with other lower safety class systems. Those, FRPS, SRPS, RCMS and FCMS, are subsystems of RPS and CMS, which will be described on the next subsections.

Table II presents an overview of the NIS channels.

TABLE II. NIS OVERVIEW

Quantity	**Neutronic Instrumentation Channel**	**Signals Destination System**				
		FRPS	SRPS	PAMS	RCMS	FCMS
3	Start Up	X			X	
3	Wide Range Log	X		X	X	
3	Power		X		X	
1	Wide Auto-Range Linear				X	
1	Nitrogen 16				X	
19	Self-Powered Neutron Detector					X

Each channel possesses one unit that allocates the electronic processing modules, except for SPND channels that are grouped in three units.

2.2. Reactor Protection System (RPS)

The Reactor Protection System (RPS) has the function of trigger reactor trip automatically when a safety variable reaches a Safety System Setting and request for reconfiguration of confinement ventilation. For each safety variable on which a safety limit is required, a set point is defined. These are called Safety System Settings and provide the minimum acceptable safety margin to initiate trip protective action. It can also be started manually by operating personnel. Once a trip action was started, no manual intervention is permitted and it proceeds to completion. Once trip action had been finished, return to operation requires deliberated operator action in order to ensure safety variables to meet their design criteria.

Furthermore, RPS was also designed to contemplate some important criteria as: fail safe, redundancy, single failure, independence, functional isolation and diverse systems. It has two independent and technological diverse systems: First Reactor Protection System (FRPS) and Second Reactor Protection System (SRPS). The FRPS has two protective actions: reactor shutdown, through control rods drop (Trip 1) triggered by the First Final Actuation Logic (FFAL), and confinement isolation. The SRPS has two protective actions: reactor shutdown, through drainage of reflector tank (Trip 2) triggered by the Second Final Actuation Logic (SFAL), and Trip 1 through FFAL.

FRPS comprises Cabinets 1, 2 and 3, and FFAL. Each one of these components is placed in a different room to attend criteria mentioned above. SRPS comprises Cabinets 1, 2 and 3, whose are placed in the same room of analogue FRPS Cabinets, and SFAL which is placed in a different room.

Table III summarizes the type of all RPS components.

TABLE III. SUMMARY OF RPS COMPONENTS TYPE

Component	Type	Description
FRPS Cabinet 1	Digital	Processing Module
FRPS Cabinet 2	Digital	Processing Module
FRPS Cabinet 3	Digital	Processing Module
FFAL Cabinet	Analog	Relay
SRPS Cabinet 1	Analog	Discrete Processing Module / Field Logic Module
SRPS Cabinet 2	Analog	Discrete Processing Module / Field Logic Module
SRPS Cabinet 3	Analog	Discrete Processing Module / Field Logic Module
SFAL Cabinet	Analog	Relay

2.3. Control and Monitoring Systems (CMS)

The Control and Monitoring Systems (CMS) are distributed, computer-based, high-availability systems which acquire all plant and reactor information, presents it to operator at the main and emergency control rooms and local supervision centers, and enables reactor control, process command and overall data-management.

The CMS comprise two groups, one dedicated to the reactor operation, called Reactor Control and Monitoring System (RCMS), and the other that serves primarily to the operation of the facilities, Facilities Control and Monitoring System (FCMS).

The RCMS communicates with many plant systems: RPS, PAMS, RMS, NIS, FCMS, Fire Protection System, External CMS (Secondary Cooling System), Fire Detection, Demineralized Water Supply, Compressed Air, Ventilation Chilled Water, Electrical System, Main Control Room Ventilation and Emergency Control Room Ventilation.

In the same way, RCMS provides basic operation reactor's logics that comprises those relative limitation criteria – bank insertion, power reduction, etc. - and those supervising transitions between reactor states – Shutdown, Power, Test and Refueling.

RCMS units comprise Supervision Units (SU), Control Units (CU) and Field Units (FU). SU are office computers, industrial computers, engineering workstation, data server and historical server. CU are controllers or industrial programmable logic controllers (PLC). Finally, FU are distributed peripheral for systems interfaces.

2.4. Post-Accident Monitoring System (PAMS)

The PAMS is a hardwired redundant system (redundancies 40 and 50) RCMS and RPS independent. It has four main functions, which are displayed in Main Control Room (MCR), Emergency Control Room (ECR) and Crisis Management Center:

- Provide reliable information to the operators about safety variables, to determine if the reactor shutdown systems have been correctly executed.

- Provide information so that operators can evaluate the execution of non-automatic actions after an accident.

- Provide indication about the state of the barriers against release of radioactive products.

- Provide information to determine if there is radioactive material release.

PAMS acquire analog and digital signals from field, RMS and RPS, inside its units. Then, units isolate and replies analog and digital signals, and distribute them to Control Rooms, Crisis Management Center and to RCMS.

2.5. Radiation Monitoring System (RMS)

The Radiation Monitoring System (RMS) carries out all radiation monitoring and supervision functions, in a continuous mode, in processes involving liquids, gases, area and personnel supervision within the reactor. All information coming from RMS is sent to RCMS in a variety of ways: directly, through RPS and through PAMS.

Discrete analog-digital (hybrid) technology instrumentation is used for RMS highest safety class signals. RMS exchanges data with RCMS using 4-20 mA for analog signals and potential-free contact for digital signals, or digital communication channels (RS-485/MODBUS).

RMS comprises: Area Radiation Monitors, Personal Contamination Monitors, Portable Monitors, Liquid Effluent Monitor, Gaseous Effluent Monitors, Tritium Monitors, Failed Fuel Element Monitors, Active Streams Monitors, Secondary Cooling System Activity Monitor and Personal Dosimeters.

There are two different Area Radiation Monitors: Analog hardwired Area Radiation Monitor (ARM) that sends information for RPS and Digital microprocessor based Area Radiation Monitor (ARMi) that is operated by software

Basically, almost all output signals of RMS are both digital and analog, except for signals to RPS and PAMS, which are only analog.

Alarms from all contamination monitors will be shown in the reactor control room, emergency control room and at specific point if it is required.

2.6. Control Rooms

The Control Rooms allow operators to control and monitor the facility in normal and abnormal conditions, including reactor operation in every status and operation of reactor facilities. It means habitability and comfort for operator personnel in these rooms. In addition, provide necessary information to operate the reactor safely and efficiently in accordance with Human Machine Interface (HMI) criteria.

2.7. Main Control Room (MCR)

The MCR will centralize the HMI provided by RPS, PAMS, RCMS, FCMS, Communication System and CCTV.

Main components of the MCR are: the main console, RPS wall panel, PAMS wall panel and supervisor console.

The main console is composed by nine Supervision Units (SU). The SU distribution is:

a) Supervision Unit 1 CNSCMS – Cold neutron Source (CNS).

b) Supervision Unit 2 FCMS – Beams.

c) Supervision Unit 3 FCMS – Irradiation.

d) Supervision Unit 4 Operation.

e) Supervision Unit 5 Control Rods.

f) Supervision Unit 6 Operation / CCTV.

g) Supervision Unit 7 Alarms.

h) Supervision Unit 8 RPS.

i) Supervision Unit 9 RMS.

The RPS wall panel consists of lighted indicators to provide the status of reactor trip variables to the operator. The RPS redundancies 10, 20 and 30 are displayed separately in the wall panel (independence requirement). The information provided in the wall panel in conjunction with RPS SU are sufficient to monitor nuclear and safety parameters of the plant.

The PAMS wall panel consists of lighted analog and digital panel indicators to provide the status of reactor PAMS variables. The PAMS redundancies 40 and 50 are displayed separately in the wall panel (independence requirement). The information provided in the wall panel is sufficient to monitor nuclear and safety parameters of the plant.

The supervisor console has enough information to monitor the reactor status during normal and abnormal operation. It is not possible to operate or control any reactor system from this console, once it is a monitoring console only. The supervisor console is composed of

a) Supervision Unit 10 Supervisor.

b) Supervision Unit 11 Supervisor.

Fig. 3 and ***Fig. 4*** shows the layout of MCR.

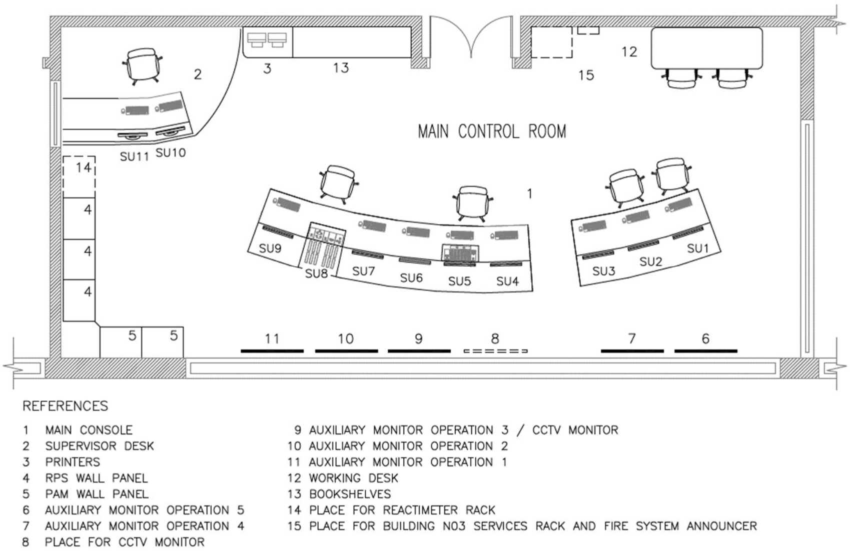


Fig. 3 – Layout of Main Control Room – Upper View.

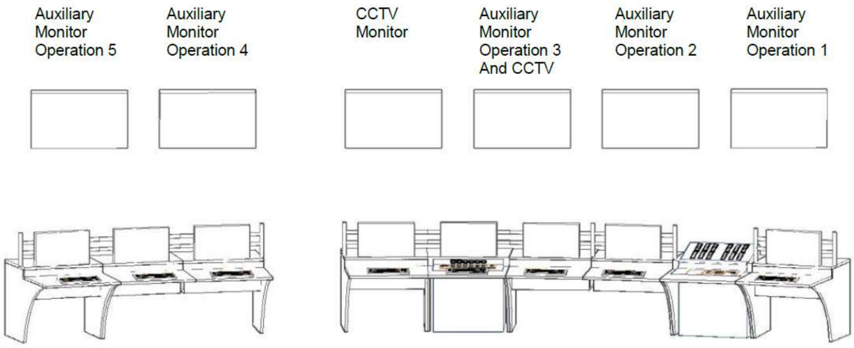


Fig. 4 – Layout of Main Console and Monitors – Door's View.

2.8. Emergency Control Room (ECR)

The ECR will be used just in case of inhabitability of the MCR. In this room, only monitoring and shutdown actions are permitted, which means that the reactor cannot operate in any state different from Shutdown State.

Main components of the ECR are: the emergency console, RPS wall panel and PAMS wall panel. All plants parameters will be showed on those panels.

The emergency console is composed by four Supervision Units (SU). The SU distribution is:

a) Supervision Unit 1 Alarms.

b) Supervision Unit 2 RPS.

c) Supervision Unit 3 Operation.

d) Supervision Unit 4 Facilities / CCTV.

The RPS wall panel consists of lighted indicators to provide the status of reactor trip variables to the operator. The RPS redundancies 10, 20 and 30 are displayed separately in the wall panel (independence requirement). The information provided in the wall panel in conjunction with RPS SU are sufficient to monitor nuclear and safety parameters of the plant.

The PAMS wall panel consists of lighted analog and digital panel indicators to provide the status of reactor PAMS variables. The PAMS redundancies 40 and 50 are displayed separately in the wall panel (independence requirement). The information provided in the wall panel is sufficient to monitor nuclear and safety parameters of the plant.

Fig. ***5*** shows the layout of ECR.

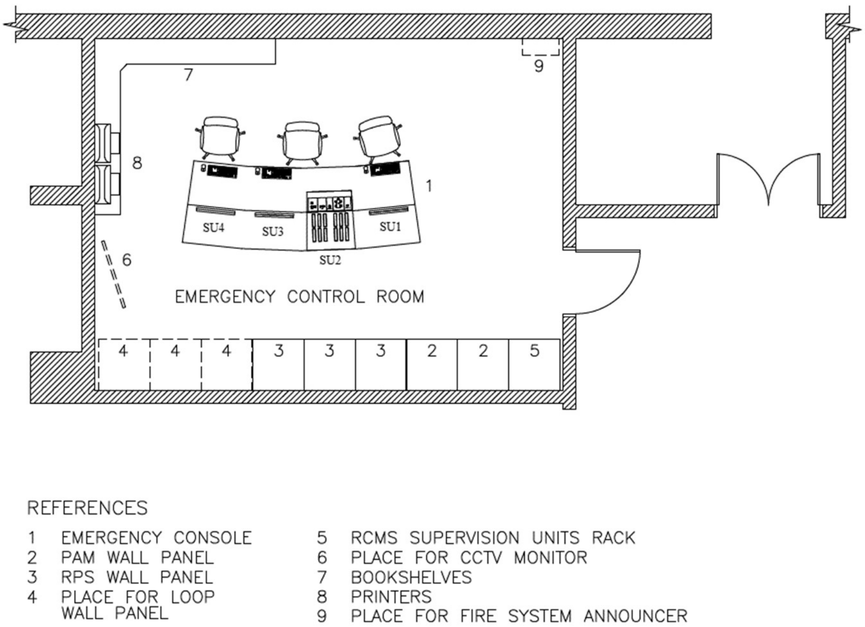


Fig. 5 – Layout of Emergency Control Room – Upper View.

3. DISCUSSIONS

Summarizing, NIS, FRPS, CMS and RMS are those digital I&C systems of RMB. The Human-Machine Interface (HMI) presents many digital components showing a tendency to change, at least in this field of application. A plan for Verification and Validations (V&V) for I&C systems of RMB was developed using standards documents [1][2]

The main difficult to implement digital I&C in RMB design is the obsolete thought about I&C systems. In spite of digital systems be proven technology, it is hard to convince most people that these are as much reliable as analog ones, simpler and that they can reduce operator personnel failures, occasioned by complex architectures.

4. CONCLUSIONS

As conclusion, in RMB preliminary engineering design stage, hybrid I&C systems were clearly adopted. The preliminary engineering design stage was completed 3 years ago and was based on OPAL Australian reactor [3]which had his operation started in 2007. After 10 years of operation, OPAL design has shown great practice, what not exclude the possibility to improvements, mainly in I&C area.

The implementation of full digital I&C systems should be considered and assessed in RMB detailed engineering design stage. It goes to meet International Atomic Energy Agency (IAEA) considerations [4] and the fast progress in electronics and information technology areas. If this assessment would not be performed, all equipment will become obsolete, less reliable or will not be capable to undergo maintenance.

5. REFERENCES

[[1] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, IEEE Std 7-4.3.2-1993 , New York, (1993).

[[2] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, Standard for Software Verification and Validation, IEEE Std 1012-2004, New York, (2004).

[[3] INTERNATIONAL ATOMIC ENERGY AGENCY, The Opal Reactor's I&C Systems, Technical Meeting on Instrumentation and Control in Advanced Small and Medium-sized Reactors (SMRs), Vienna, (2013).

[[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Instrumentation and Control Systems (I&C) in Nuclear Power Plants: A Time of Transition, 52nd IAEA General Conference, Vienna, (2008).

UPGRADE OF I&C AT VR-1 TRAINING REACTOR

M. KROPIK, J. RATAJ, L. SKLENKA
VR-1 Training Reactor, Department of Nuclear Reactors,
Faculty of Nuclear Sciences and Physical Engineering,
Czech Technical University,
Prague, Czech Republic

Abstract

This contribution describes the upgrade of the instrumentation and control (I&C) system of the VR-1 training reactor at Czech Technical University in Prague. The reactor was put into operation in the 1990s. The original digital I&C seemed to be obsolete and its upgrade was carried out. The new reactor I&C consists of a protection system, a control system and a human-machine interface. The protection system contains the operational power measuring (OPM) and the independent power protection (IPP) systems. The OPM is a full power range system. The IPP system works in the two highest power range decades. The computers of both systems calculate the reactor power and power rate, compare them with the safety limits, and if they are exceeded, the safety action is initiated. The OPM and IPP systems are diverse – they differ in types and location of chambers, in hardware, in software algorithms, development tools and teams for the software manufacturing. The control system is based on a high quality industrial PC mounted in a 19" crate. The human-machine interface (HMI) was designed with respect to functional, ergonomic and aesthetic requirements. Czech and English interface versions are available. The history server completes the HMI and provides storage of all reactor operational data for evaluation of experiments and evidence of safe reactor operation. The I&C upgrade was carried out in gradual stages, started in 2001 and successfully finished in 2010. Quality assurance, Configuration management, verification and validation accompanied the software development. Finally, thorough non-active and active tests were carried out after every phase of the upgrade. The new I&C improves the nuclear safety and operability of the reactor, and enables a prolongation of its functionality and maintainability for at least the next 10 years.

1. INTRODUCTION

This contribution describes the structure, installation and testing of a new I&C at the VR-1 nuclear training reactor at the Department of Nuclear Reactors, at the Faculty of Nuclear Sciences and Physical Engineering of the Czech Technical University in Prague. The VR-1 reactor (see Fig.1) is a pool-type light-water reactor based on enriched uranium (under 20%). Its thermal power is rated up to 5 kW. The reactor is utilized primarily for training university students and future nuclear power plant staff. The training at the VR-1 reactor is oriented to the reactor and neutron physics, dosimetry, nuclear safety, and control of nuclear installations.

The VR-1 training reactor has been operated since 1990. The original reactor control and safety system (I&C) was developed in the mid- 1980s. The system was digital. Even though the original control and safety system fully covered the demands that were put on it, its technical design was obsolete, and there were problems with maintenance. Therefore, it was decided to upgrade the present control and safety system with the aim to apply the latest available techniques and technology observing the relevant guidelines, standards and recommendations.

The principal upgrade of the reactor I&C started in 2001. Because of the frequent utilization of the VR-1 training reactor during the academic terms, it was decided to carry out the upgrade gradually – in stages during holidays so as not to affect the training at the reactor. The first stage was the human-machine interface (HMI) and the control room upgrade (2001), next the control rod drives and the safety circuits upgrade (2002). The upgrades continued with the control system upgrade (2003) and the independent power protection system upgrade (2005). The further stage was the operational power measuring system upgrade and the installation of the complete I&C into a new I&C room (2007) with up-to date cabinets and a much better access to the systems for the inspections and maintenance than in the previous I&C location. Next, new supplementary technology systems for the water level and conductivity measurements were installed (2008). Finally, the new HMI software, equipment, history server and PC for evaluation of experiments were installed (2009) and the English interface of the HMI was improved (2010).

The general contractor of the I&C upgrade was Škoda Nuclear Machinery Pilsen, the subcontracts were Tedia Pilsen for the independent power protection system and dataPartner České Budějovice for the operational power measuring system, the control system and the HMI. Our Department of Nuclear Reactors prepared the requirements for all upgraded systems, cooperated in hardware and software development, provided experience with the neutron flux measurement, carried out the verification & validation and co-operated in the systems licensing process.

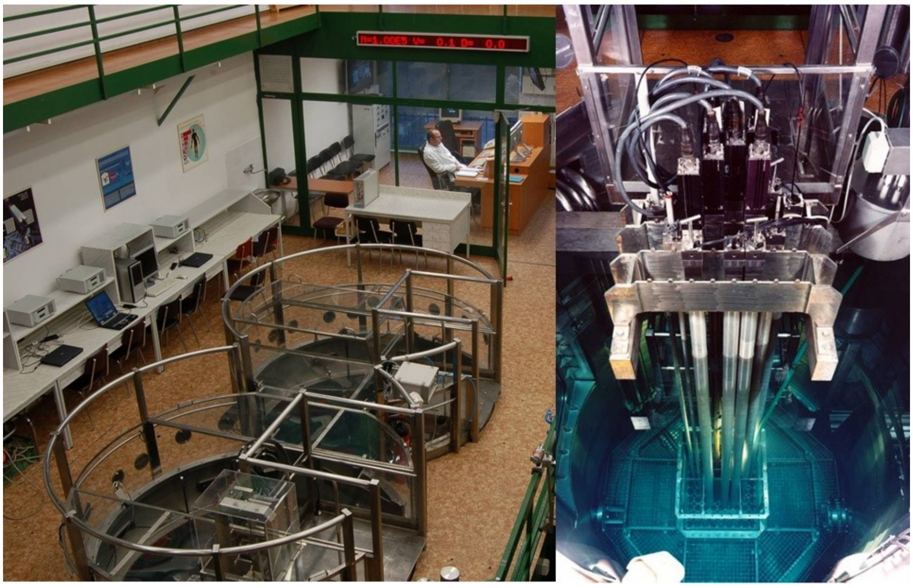


FIG. 1. VR-1 reactor hall and VR-1 core.

2. REACTOR I&C

This section explains the complete reactor I&C structure. A block diagram of the reactor I&C is shown in Fig. 2. The system structure has to meet the requirements of the Czech State Office for Nuclear Safety Ref. [1].

2.1. Description of system structure

The safety (protection) part of the I&C is described in this section. This part is the most important one for nuclear safety. Four operational power measuring channels (OPM) receive signals from wide range fission chambers (OPMCH), evaluate them, calculate the reactor power and the power rate, and send the values to the control system and to adjacent individual displays on the operator's desk of the human machine-interface (HMI) in the control room. Four channels equipped with boron chambers (IPPCH) work as an independent power protection system (IPP). They also evaluate the power and the power rate, send data to the control system and to their displays, and initiate a safety action (reactor scram) if safety limits are exceeded.

The control system receives data from the OPM and IPP channels, checks received values with each other and against the safety limits. The control system calculates the average values of the reactor power and the power rate; next, it evaluates the deviation between the real power and the demanded power value set by the operator. The control system sends data to the HMI and receives commands from it. If the commands are permitted, it carries them out. The control system also serves as an automatic power regulator system and controls the movement of absorbing rods to achieve the required reactor power. The absorbing rods movement is actuated by absorbing rod drivers. There are up to 7 absorbing rods in the VR-1 reactor. Three absorbing rods are safety rods. These rods are in upper positions during standard reactor operation and if any problem occurs, they fall down (together with all other absorbing rods) into the core and safely shutdown the reactor. The experimental rods compensate for influence of experimental facilities on reactivity of the reactor core; these rods are in fixed positions during standard reactor operation. It is possible to use none, one or two experimental rods. The two control rods control the chain fission reaction in the reactor core. These control rods can be used for manual or automatic control of the reactor power.

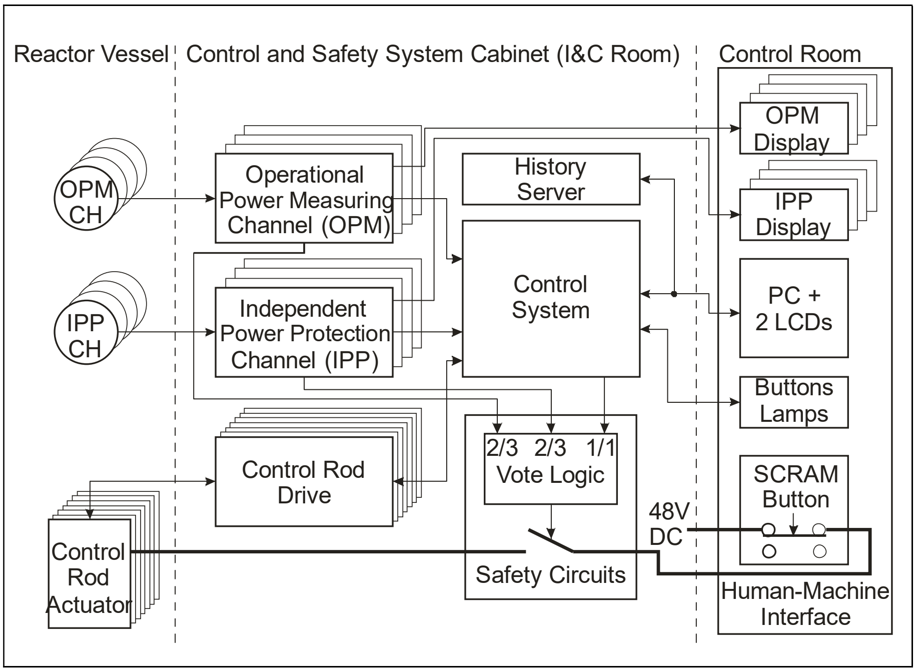


FIG. 2. Block diagram of I&C.

The HMI enables control of the reactor operation by an operator. It consists of a computer with liquid crystal displays (LCDs) and indicators showing the operational status of the reactor, as well as a keyboard, buttons and light indicators to control the reactor. The HMI interface receives commands from the operator, evaluates them and sends them to the control system. It also receives messages from the control system, displays them and stores data about the reactor operation in a history server.

2.2. Safety features of I&C

Defense in depth, redundancy and diversity are applied in the reactor I&C to enhance its safety and reliability. Under standard conditions, the control system operates the reactor (the first level of the defense in depth), monitors the safe operation of the reactor, and if necessary, stops the chain reaction in the reactor (reactor scram). If any problem appears within the control system, the protection system (the second level of the defense in depth) consisting of the OPM and IPP channels, independently checks the reactor status; if the safety limits are exceeded, it stops the chain reaction by the reactor scram. To fulfill the single failure criterion, the protection system uses redundancy. To avoid a common mode failure, the protection system applies diversity. (See details in Chapter 3).

The control system evaluates the reactor power, the power rate, the deviation in data of single OPM channels, and system and technology status. If any failure appears (e.g. in the reactor technology, in the rod drives or an improper reactor status), it sends the safety signal to initiate the reactor scram. The OPM and IPP channels independently compare the reactor power and the power rate with the safety limits; if these limits are exceeded, or any internal error appears, they send safety signals. The safety signals status is represented by safety relays statuses of the OPM, IPP channels and the control computer. If the safety relay is off, it means the safety signal activation. The outputs of the relays are connected to a vote logic described in the next paragraph.

The vote logic receives the safety signals. The relays-based vote logic evaluates the safety relays statues from the OPM channels in the logic 2 out of 3, from the IPP channels independently 2 out of 3, and the safety signal from the control system is evaluated in the logic 1 out of 1. If the conditions for the safety action request are met in at least one group (OPM or IPP or control systems), the power supply (48V DC) to the absorbing rods is broken by the safety circuits, the rods fall down and stop the chain reaction (reactor shutdown - scram). The reactor shutdown can be also initiated manually by pressing one of the scram buttons. One scram button is located on the operator's desk of the HMI, additional buttons are situated close to the reactor vessel, the radial channel output, in the I&C room or at the entrance door of the reactor hall. Because of the low power of the VR-1 training reactor, there is no need to remove residual heat from the core after the reactor shutdown.

3. REACTOR PROTECTION SYSTEM

The reactor protection system consists of two parts – the operational power measuring (OPM) Ref. [4] and the independent power protection (IPP) Ref. [3] systems. The OPM and IPP systems receive signals from neutron chambers, evaluate them, calculate the reactor power and the power rate, and initiate a safety action (reactor scram) if safety limits are exceeded.

To fulfill the single failure criterion, the protection system utilizes redundancy. There are four OPM and four IPP channels, three of them are active, the fourth OPM and IPP channels operate in the stand-by mode. The channels are fully independent so that consequences of a single failure in any channel cannot penetrate to the other ones. Safety signals from both OPM and IPP channels are evaluated in the logic 2 out of 3.

To protect against the common mode failure, the protection system applies diversity. There are diverse OPM and IPP channels. They vary in sensors (fission and boron chambers), hardware (an industrial PC and a tailor made microcomputer-based system), and software (Microsoft Visual C++, Phar Lap operating system, dataPartner company team and Keil µVision 2 ANSI C with NRC restrictions, no operating system, Department software team).

3.1. Operational power measuring system

The Operational Power Measuring (OPM) system is a part of the reactor safety (protection) system (see the Chapter 2). The OPM channels receive signals from the wide range fission chambers RJ1300, evaluate it according to the reactor power in pulse or current range, calculate the reactor power and the power rate, and send the values to the reactor control system and to the adjacent individual display on the operator's desk of the HMI in the reactor control room. The channels also compare values of the power and the power rate with the safety limits, and if the limits are exceeded, the request for a safety action is sent to the vote logic. Next, the OPM channels send the calculated reactor power and power rate together with the system status, etc. to the control system.

The following Chapters describe the IPP channel hardware and software.

3.1.1. OPM channel hardware

The operational power protection channel consists of an analog and a digital section. The analog section processes the RJ1300 fission chamber signal and transforms it so that it is suitable for the digital section. The analog section (see Fig. 3) processes the neutron chamber signal either in pulse, Campbell or DC current ranges and provides signals proportional to the neutron flux density (reactor power).

The digital section (see Fig. 3) of the OPM channel is based on a high quality industrial PC with an appropriate additional hardware – an input unit for reading data from analog section; a supervisory unit for the supervision of the OPM hardware and software; communication unit for communication with the control system, the control desk individual display and service computer; local display for the OPM status presentation and a safety relay to control the safety circuits.

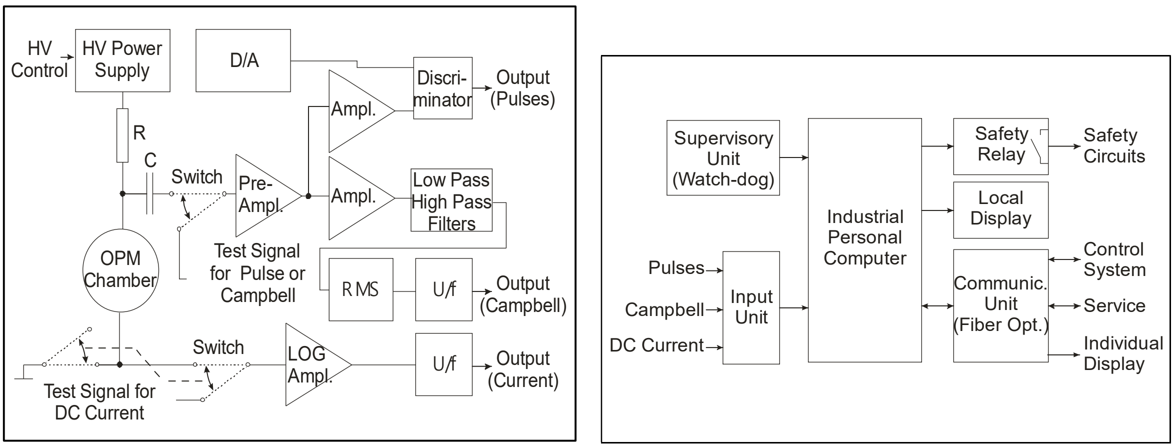


FIG. 3. Block diagram of OPM analog and digital section.

3.1.2. OPM channel software

The OPM channel software has to fulfil quality requirements for the safety (protection) systems of nuclear facilities; quality assurance, Configuration management, verification and validation activities must fulfil respected standards and guides, e.g. IEC 880, 1986 and IEC 60880-2, 2000. The computer operating system is the reputable system Phar Lap, the software is coded in the C Language. Corresponding software life cycle documentation was delivered together with the software. The OPM system development was finalized by detailed validation of the OPM system (see the Chapter 8.1).

3.2. Independent power protection system

The Independent Power Protection (IPP) system of the VR-1 training reactor at Czech Technical University in Prague is also a part of the reactor safety (protection) system (see the Chapter 2). The IPP channels receive a signal from the boron chambers SNM-12, evaluate it in pulse range, calculate the reactor power and the power rate, and send the values to the reactor control system and to the adjacent individual display on the operator's desk of the HMI in the reactor control room. The channels also compare values of the power and the power rate with the safety limits, and if the limits are exceeded, the request for a safety action is sent to the vote logic. Next, the IPP channels send the calculated reactor power and power rate together with the system status, etc. to the control system.

The following Chapters describe the IPP channel hardware and software.

3.2.1. IPP channel hardware

The IPP channel hardware consists of an analog and a digital section. The analog section processes the signal from the boron neutron chamber, amplifies it, and provides proper discrimination of neutrons. The digital section counts pulses from the neutron chamber, evaluates the reactor power and the power rate. Next, it compares gained data with the safety limits and sends the safety signal (controls the safety relay). It also communicates with the reactor Control system via fiber optics lines, controls the individual display on the operator's desk and provides testing of the channel.

The structure of the analog section of the IPP channel is shown in Fig. 4. The channel sensor is the neutron boron chamber SNM-12 from Russia. The power supply for the chamber provides a high voltage power supply. The high voltage power supply is controlled by the digital part to provide chamber characteristics measurements. The signal from the chamber is amplified by an amplifier and evaluated by a discriminator. The discriminator level is set by the D/A from the digital part Auxiliary Unit (see later). The variable setting of the discrimination level can be used for chamber characteristic measurement and low discrimination tests during the reactor start-up. The signal from the chamber can be replaced by a test signal to provide tests of the channel. The test signal of proper frequency is connected to the amplifier and a corresponding response of the channel is checked.

The pulses from the discriminator are connected to the counter of the IPP channel digital part that counts the number of pulses in 0.1 second. The digital part computer units then read the frequency of neutron pulses (during standard operation proportional to the reactor power).

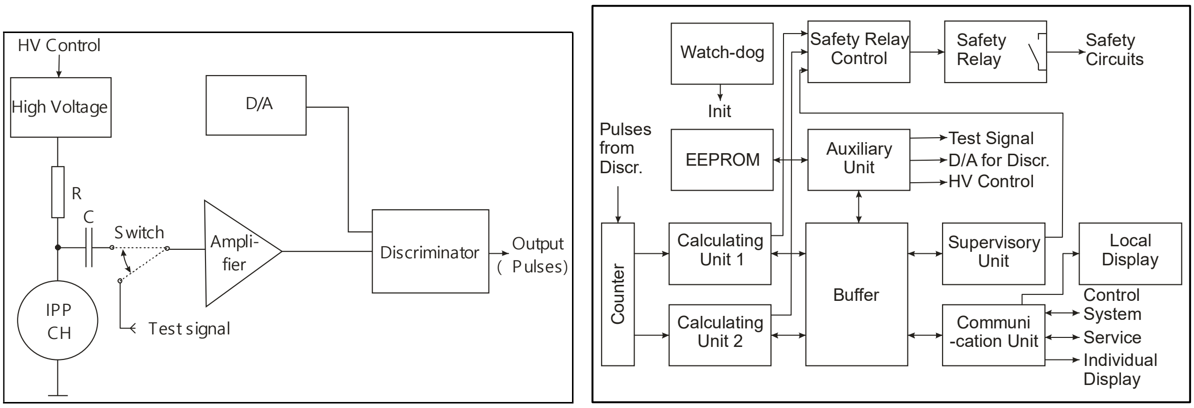


FIG. 4. Block diagram of analog and digial section of the IPP channel.

A block scheme of the digital section of the IPP channel is also shown in Fig. 4. The digital section consists of 5 microcomputer units. The reason for the utilization of more microcomputers was to divide single functions to separate microcomputers to guarantee easier structure of the system hardware and, in particular, of system software. The communication among individual microcomputers is provided via buffer in an FPGA (Field-Programmable Gate Array).

The 16 bit Counter counts the number of neutron pulses from the analog part. The interval of the counter is 0.1 second. The Calculating Units 1 and 2 read data (count of neutron pulses) from the Counter, calculate the reactor power and the power rate. Furthermore, they check safety limits and send a safety signal to the Safety Relay Control if the safety limits are exceeded. There are two units in the channel. They work in parallel and are synchronized, and The Supervisory Unit examines if both units give the same results. This feature provides protection against unit memory or microcomputer failure. The Supervisory Unit reads data from Calculating Unit 1 and 2, checks that data appear on time, compares them, and if a difference appears, it sends the safety signal to the Safety Relay Control that switches the Safety Relay off. The Safety Relay Control is implemented in a CPLD that receives signals from the Calculating Units 1, 2 and the Supervisory Unit.

The Communication Unit is responsible for communication among the IPP channel, the Control system, the Local Display, and individual display. The Auxiliary Unit initiates the FPGA after the channel is switched on, reads calibration data from the EEPROM, sets D/A converter for the discrimination level, provides the analog part test signals, and controls the high voltage power supply. The Watch-dog periodically receives signals from the system, and if one of the signals does not appear on time, it resets (initiates) the whole channel. The Local Display is situated on the front panel of the IPP channel and represents data and operational status of the channel.

3.2.1.1. Safety measures

Certain safety measures were implemented into the IPP channel to improve the reliability and safety of the channel. If any problem appears, the Safety Relay has to be switched off. There are two Calculating Units in the channel checked by the Supervisory Unit, and if any problems in one of these units appear or if safety limits are exceeded in any of the Calculating Unit, it forces the Safety Relay to switch off. The Calculating and Supervisory Units, Safety Relay Control, and Watch-dog use different clock sources to avoid clock common mode failure.

Data sent or received via the Buffer through the Communication Unit are supplemented by the CRC; the CRC is checked after the data reception. The Watch-dog initiates (resets) the IPP channel if the corresponding signals are not received on time. After the reset, the Safety Relay is switched off.

3.2.2. IPP channel software

The IPP channels are components of the reactor protection system (see the Chapter 2). There are stringent requirements for their quality, reliability and availability. To achieve these goals, the appropriate standards were applied, e.g. IEC 880, 1986. The functional division of the IPP channel into the single microcomputers facilitated the software development because the software was then considerably less complex. Also, it was not necessary to utilize interrupts in the software of the Calculating Units, which is the most critical for safety. Detailed description of the IPP software was provided because this software was developed by our Department of Nuclear Reactors.

3.2.2.1. Software life cycle

The IPP channel software life cycle was in accordance with the IEC 880 standard, 1986. Firstly, the principal documents for the software development were established – the Quality Assurance, Verification & Validation, and Configuration Management Plans. These documents define basic procedures and techniques during the development and testing of the software. The software life cycle started with the setting of requirements, and continued with the software design, and coding and integration of hardware/software. The whole life cycle was accompanied by verification & validation. During the whole life cycle, the relevant documents were prepared.

3.2.2.2. Software requirements

The Software Requirements were prepared as a standard text. Detailed requirements for all microcomputer units, regimes of the channel operation and transitions among them, single data messages, and their format are set there. Focus was also put on requirements for the reactor power and velocity of power changes calculations (basic parameters for reactor safety evaluation). The principle requirements for safety functions of the IPP channel were prepared with care. The warning and safety limits for the reactor power and velocity of power changes were set. The unacceptable channel states were defined. The reactor's physics and operation experts were involved in the preparation of the Software Requirements.

3.2.2.3. Software design

The software was designed according to the Software Requirements. The software structure for the single units and communication standards among them were established. The software was designed in the top-down manner. The basic algorithms and data structures were proposed, and the algorithms (e.g. for the reactor power and velocity of power changes) were thoroughly tested.

3.2.2.4. Software coding

The software coding life cycle phase continued after the software design. During this phase, the designed software was coded into the programming language. The principal programming language was the ANSI C language with restrictions according to standard with respect to NUREG document Review Guidelines on Software Languages for Use in Nuclear Power Plant

Safety Systems, 1996. The software was coded in the bottom-top manner. For the software coding and production, the reputable µVision 2 development system for 8051 compatible microcomputers of the Keil Software Company was utilized.

3.2.2.5. Integration HW/SW

During the hardware/software integration phase, the developed software was programmed into the microcomputer units, and the integrated system was thoroughly tested. The tests revealed several minor problems, which were gradually removed. All channel safety, operational and test functions, regimes of operation, and setting and calibration were checked. After integration HW/SW, detailed validation of the IPP system followed (see the Chapter 8.1).

3.3. Safety circuits

The safety circuits provide the vote logic of the safety signals from the OPM, IPP channels and the Control system. The safety circuits utilize high quality relays with forced contacts to guarantee high reliability of operation. The safety circuits are installed in a 19’’ crate for easy installation in new cabinets of the I&C (see the Chapter 7).

4. REACTOR CONTROL SYSTEM

4.1. Control system structure

The control system (Ref. [2]) utilizes an industrial PC and Simatic S7-200 PLCs for distributed functions. The operating system of the PC is Microsoft Windows XP with the real time support RTX of the VentureCom Company. The block diagram of the new control system and its incorporation into the reactor I&C is shown in Fig. 5.

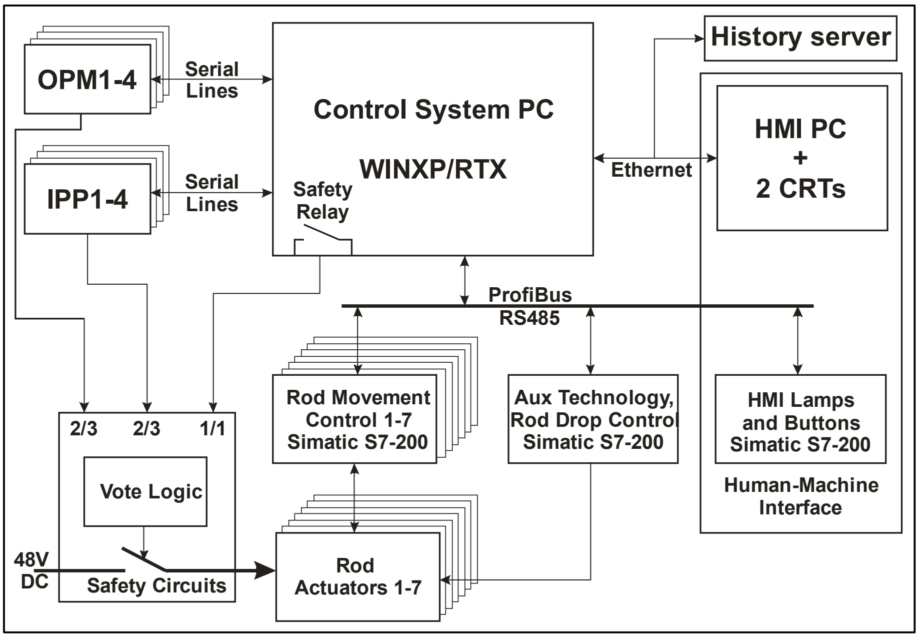


FIG. 5. Block diagram of control system.

The upgraded control system is based on a high quality industrial PC mounted in a 19" crate. The control computer receives data from the OPM channels in the full power range and the IPP channels in the two highest power decades range via serial lines. The control computer checks received data from the OPM and IPP channels mutually and against the safety limits. If either the safety limits or allowed deviations between individual channels are exceeded or if there are any problems in the system, the safety action is initiated by the control computer.

Next, the control system controls the reactor operation and provides the I&C diagnostics. It also serves as an automatic power control system; it controls the movement of the reactor control rods to obtain the required reactor power.

The control computer drives the absorbent rod movement via the rod actuators based on the Simatic S7-200 PLCs and connected with the control computer via a ProfiBus (RS485) interface. The ProfiBus, together with the adjacent Simatic PLC, is also utilized for auxiliary technology and individual rod drop control, then one also for lamps control and buttons scan on the operator's desk of the human-machine interface.

The control computer sends data via the Ethernet network to the human-machine interface computer and receives commands from there. If the commands are permitted, it carries them out. Data from the control system are also sent to the history server (see Chapter 5.1.3).

4.2. Control system software

The control system software represents a complex product. The software, together with the whole control system, is categorized according to the importance to nuclear safety as safety related. The quality assurance process, covering the whole software life cycle and including software requirements, design, coding, HW/SW integration and installation, was carried out. The documents 'Quality assurance plan', 'Verification and validation plan' and 'Configuration management plan' were prepared. Software development was accompanied with thorough testing, and the integrated system was carefully validated by simulated input signals and then in normal reactor operation.

The software requirements were prepared as a text document. The extent of the software requirements is of 170 pages. The requirements define the reactor operational modes and submodes. The requirements for cooperation with other reactor I&C (OPM, IPP channels, human-machine interface) were also formulated.

The control system software was prepared according to the requirements in the Microsoft Visual C++ development tool with RTX support. The software for single Simatic PLCs was established by proper Siemens development tools. The control system software consists of safety, control and diagnostics functions.

Firstly, the safety functions are described. The control system is equipped with a safety relay. If the safety action (reactor scram) is required, then the safety relay is switched off. The safety relay output is connected to the vote logic of safety circuits, and this signal is evaluated in the logic 1 out of 1. This means that if the control system safety relay is switched off, then the reactor is scrammed. The control system receives data from the OPM and IPP channels, compares power and velocity values with safety limits, it also compares data from individual channels and if the safety limits are exceeded, then it initiates the safety action. It calculates the average values of power and velocity and evaluates the deviation between the real power and the demanded power value set by the operator. If the deviation limit is exceeded, the safety action is also initiated. The control system also checks the technology (e.g. control rod drives, PLCs, communication), and if any problem occurs, it initiates the reactor scram.

Next, the control functions drive reactor modes, submodes and transition among them. The control system also receives commands and button signals from the human-machine interface, and if the action is in current operational mode and submode permitted, then appropriate response is executed. The software also calculates average values of the reactor power and velocity of power changes and sends them to the human-machine interface. The control system also provides the function of the automatic power regulator. The regulator compares the demanded (given) power with the real reactor power and according to the deviation, it controls the rod movement.

Finally, the control system also provides diagnostic functions. It can check proper operation of the OPM and IPP channels and correct communication with other parts of the reactor I&C. The absorbent rod test was added to the original control system. This test can check the movement speed and the drop time of any rod, which is important for rod verification and maintenance.

4.3. Absorbing rod drives

The control rod drives and motors were innovated significantly. The old rod motors were replaced by new ones that provide appropriate qualities and dimensions. Necessary mechanical changes on the control rod mechanism, induced by the utilization of the new motor, were made. High quality connectors were utilized for the connection of cables to the motors. The PLCs (Programmable Logic Controllers) Simatic S7-200 equipped with proper power electronic boards serve as motor drives. The PLCs communicate with the control system via a ProfiBus (RS485) line.

5. HUMAN-MACHINE INTERFACE

The human-machine interface (HMI) is situated in the control room of the reactor. Prior to the upgrade, all reactor I&C was installed in the control room. But after the complete I&C upgrade, the I&C was built in a new I&C room. So, the control room is now more usable for reactor operation and training of students.

FIG.6. HMI operator's desk.

The principle component of the HMI is the operator's desk (see Fig. 6) which provides all facilities to control the nuclear reactor. The operator's desk was completely changed during the HMI upgrade in the year 2001. In 2009, new software for HMI, new buttons, LCD displays, indicators with LED, computer and printer were installed. Next, the English interface in the HMI was significantly improved in the year 2010.

5.1. HMI structure

The HMI provides the control or the reactor operation. The HMI communicates with the reactor Control system, receives data regarding the reactor status and sends commands to control the reactor operation. A block diagram of the HMI is shown in Fig. 7. The individual components of the HMI are described in this Chapter.

The principal part of the HMI is a personal computer. The IBM compatible PC with enough computational performance equipped with AMD 3.11 GHz microprocessor, 4GB RAM and 500MB HDD was used. The HMI PC communicates with the reactor Control system and the History server (see the Chapter 5.1.3) via an Ethernet 100Mb/s computer network. The computer uses 2 LCD monitors, the first one for the alphanumerical and the second one for graphical data representation. Figure 8 shows the screenshot of the graphical monitor during batch command execution with regular movement of R1 absorbing rod (violet) and presentation of reactor power (red) and power rate (blue).

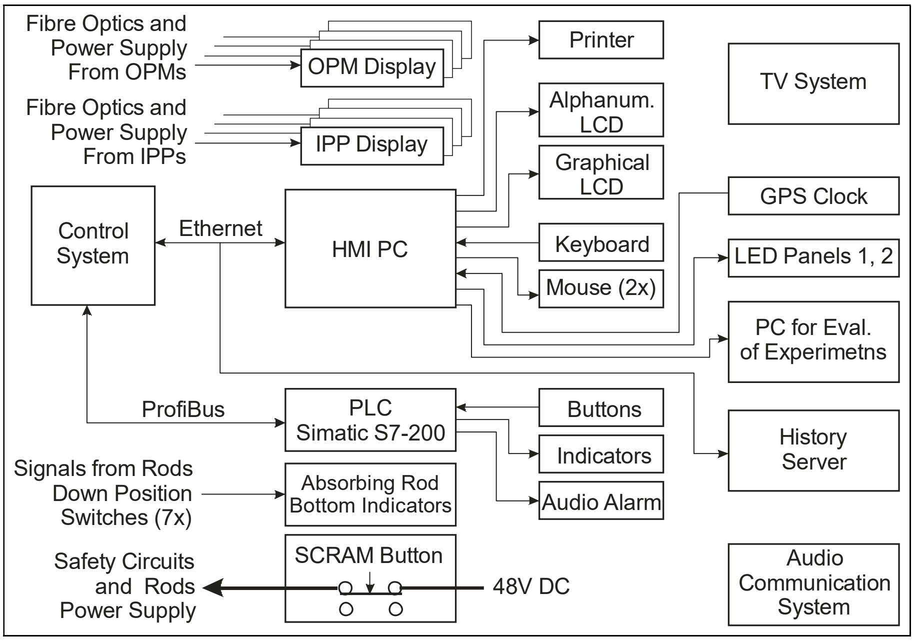


FIG.7. Block diagram of HMI.

The HMI PCI is equipped with a keyboard and two computer mice (one for the reactor operator and one for a teacher during reactor trainings). The second mouse is typically used to point out details on the HMI PC monitors during training. The Microsoft Windows XP operating system is used in the HMI PC. The HMI application program in C# was developed by dataPartner company.

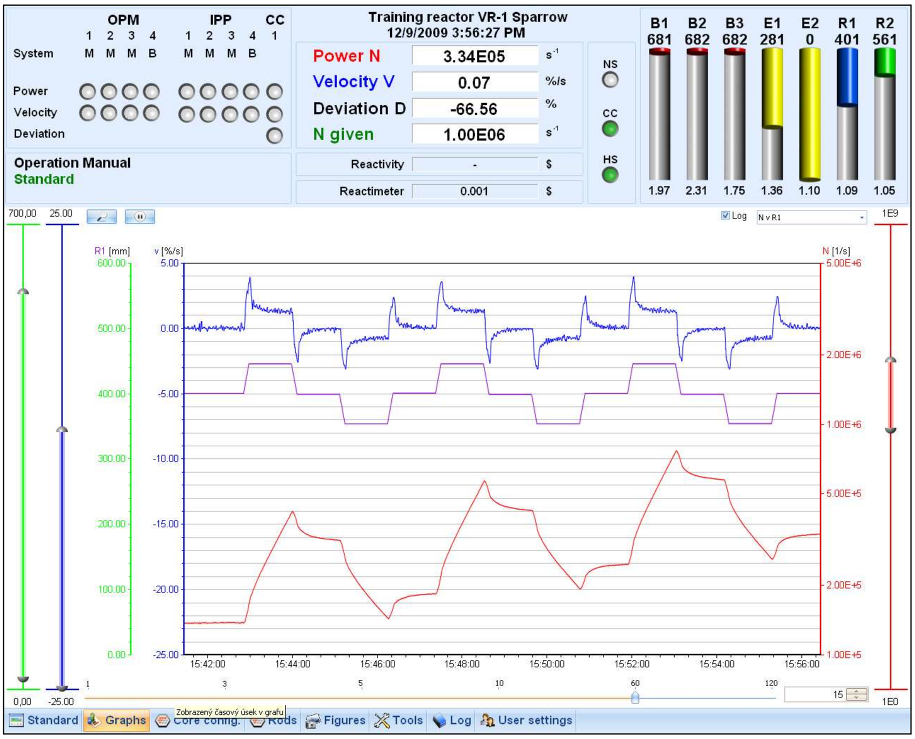


FIG.8. HMI graphical monitor screenshot with batch command presentation.

The HMI PC is connected to a printer. The printer is important for documentation of the reactor operation history. Commands and important data with date and time stamps are printed to document safe reactor operation. According to the Czech authority (Czech State Office for Nuclear Safety), it is necessary to print on zig-zag fold ("endless") paper and then store it for at least 5 years. The high quality and reliability dot matrix printer Epson LQ590 was selected, because there was no laser printer available for zig-zag fold paper.

The HMI PC is also connected to a GPS clock unit. The GPS clock is used to provide exact time for the reactor I&C. The HMI sends the exact time from the GPS unit to the Control system and the History server. The exact clock is important for data storage and synchronization of data during reactor experiments.

The PLC Simatic S7-200 is used to provide buttons and indicators functions in the HMI. The PLC is directly connected to the reactor Control system via the Siemens Profibus communication network. The PLC scans the status of operator's desk buttons and sends it to the Control system. Generally, the reactor can be controlled by pressing buttons or sending commands from the HMI PC keyboard. Some actions can be initiated in both ways, some only by the buttons and some only from the keyboard. The PLC also controls indicators on the operator's desk. These indicators represent, e.g., the selected mode of operation (either manual or automatic) and the rod power supply on. Finally, the PLC controls the audio alarm unit. The PLC receives commands from the Control system via the ProfiBus network, and if necessary, it activates the audio alarms.

5.1.1. SCRAM buttons

The SCRAM button on the operator's desk initiates manual shutdown of the reactor. It cuts off the power supply to absorbing rods, and the power break causes the fall of absorbing rods into the reactor core and stopping the fission chain reaction. Besides the SCRAM button on the operator's desk there are additional SCRAM buttons located close to the reactor pool, the radial irradiation channel output, in the I&C room and at the reactor laboratory entrance door. The SCRAM button on the operator's desk is shown in Fig. 6 with the name STOP.

5.1.2. *Absorbing rod bottom position indicators*

Regarding the nuclear safety, the absorbing rods bottom position indicators are a very important part of the HMI. These indicators work independently on the computerized reactor I&C and provide information about the bottom position of the absorbing rods. If all absorbing rods are in the bottom position, the reactor is safely stopped (shutdown status). The system consists of bottom position limit switches in every absorbing rod, back up power supply 48V DC, wires and LED indicators.

5.1.3. *History server*

The History server stores data from the operational history of the VR-1 training reactor. The History server is connected via the Ethernet network to the Control system and the HMI PC and stores all operational data every 0.1 second. The History server also provides these data to the HMI PC upon request. These data can be also transferred from the HMI PC to the PC for evaluation of experiments (see the Chapter 5.1.4). The History server is an IBM PC compatible industrial computer with Intel Quad Core microprocessor, 4GB RAM and two 500 GB HDDs (RAID1). The operating system is Microsoft Windows Server 2008 64 bit operating system. The application was developed in Microsoft SQL Server 2008 64 bit by dataPartner.

5.1.4. *PC for evaluation of experiments*

A PC for evaluation of experiments is connected to the HMI PC. Because of HMI PC safety, the communication between the HMI PC and the PC for evaluation of experiments is based on a one way fibre optics line with output from the HMI PC. This measure provides protection of the HMI PC against external harmful influences, e.g. viruses or spy ware, because the PC for evaluation of experiments is connected to the standard computer network within the university. The high speed serial card MOXA with fibre optics interface and baud rate up to 921 kb/s was used for communication. Reactor operational data can be sent to this PC either from the immediate reactor operation, or the History server (through the HMI PC) can provide any data from the operational history of the reactor.

The software Experimental Studio from the dataPartner company has been installed on this PC. This software very significantly supports the evaluation of reactor experiments. It is possible to prepare tasks in the Experimental studio as a combination of standard programming languages (C#, Visual Basic Jscript, IronPython, etc.) and graphical oriented tools.

6. SUPPLEMENTARY TECHNOLOGY SYSTEMS

The new supplementary technology systems provide measurement of the water level in the reactor tanks and the water conductivity. The water level measurement is based on the hydrostatic principle; the difference between the air and water column pressure is evaluated and the result is represented on a display. The system Waterpilot FMX167 was used. The water conductivity measurement is very important for evaluation of the water quality. If the water conductivity exceeds the safety limit, it is necessary to purify water. The system Condumax W CLS19 was used. The data from the technology together with a water pumping system are represented on a new 42'' display controlled by an industrial computer.

7. I&C INSTALLATION

The previous I&C was originally installed in the reactor control room. The space in the control room was very limited, and only a few students could have been present in the control room during the training. Also, the accessibility to the I&C for inspections and maintenance was constricted.

A new room for the reactor I&C was found near the reactor hall. There is enough space for the complete I&C with sufficient room for inspections and maintenance. The I&C components were built into 19'' racks of the Rittal company. These racks can be opened on their front and rear side, and access to the I&C electronics is very comfortable. Figure 9 shows the reactor I&C racks in the new control room.

FIG. 9. Photograph of I&C room.

8. I&C TESTING

The new reactor I&C was thoroughly tested. The tests consisted of three basic parts – the OPM and IPP channels validation, the non-active tests and active tests.

8.1. OPM and IPP validation

A detailed validation of the protection system (OPM and IPP channels) was done. The validation was carried out by simulating the input signals from the computer controlled generators (simulation of pulses and eventually current from neutron chambers) and checking the response of the channels.

The arbitrary signal generator HPE1441A in a VXI rack provided a simulated neutron pulse signal for both OPM and IPP channels, and the universal source HP3245A generated a DC current signal for the evaluation of the DC current range of the OPM channels (see Fig. 10). The PC controlled the VXI devices via a FireWire line and the HPIB devices using a HPIB card. The pulse signal was modified by a simple electronic circuit to get small pulses comparable with the neutron chamber signal. The output data from the OPM and IPP channels were received by the other PC. The second PC was used to achieve enough performance for the signal simulation PC. The signal of the safety relay (for the safety function initialization) was scanned by the multimeter HP34401A. The second PC read the safety relay status from the multimeter via the HPIB.

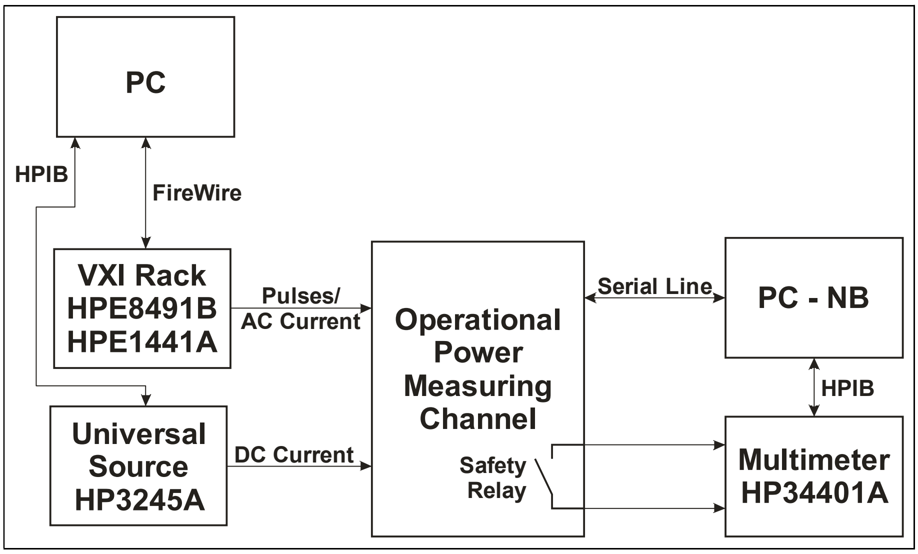


FIG. 10. Block diagram of OPM validation test.

The software was designed with the HP (Agilent) VEE graphical development tool. The software consists of three programs CD_OPM/CD_IPP (create data), SF_OPM/SF_IPP (send file) and RD_OPM/RD_IPP (read data). The program CD_OPM/CD_IPP generates the reactor power course for the validation tests according to the requirements. It is possible to set the constant reactor power, increase the power with the constant power rate, change the power linearly or exponentially between two given values, change the power rate, generate the harmonic power changes, change the power or power rate in steps, etc. The program SF_OPM/SF_IPP sends data prepared by the program CD_OPM/CD_IPP to the generators and provides the simulation of the neutron chamber signals. The program RD_OPM/RD_IPP receives data from the OPM or IPP channel, reads the status of the safety relay, can also send data to change the OPM or IPP channel setting (like the control system in the real reactor I&C) and stores all data of the validation tests into a file.

Three basic tests of the OPM and IPP channel were carried out:

(a) Communication with the control computer – sending messages and receiving commands to/from the control computer;

(b) Measurement of the reactor power and power rate – accuracy and time response tests;

(c) Generation of warning and safety signals – tests of proper generation of warning and safety signals in the case of the reactor power and power rate under standard or stricter levels, correct control of the safety relay in accordance with the safety signals and the IPP channel operational mode.

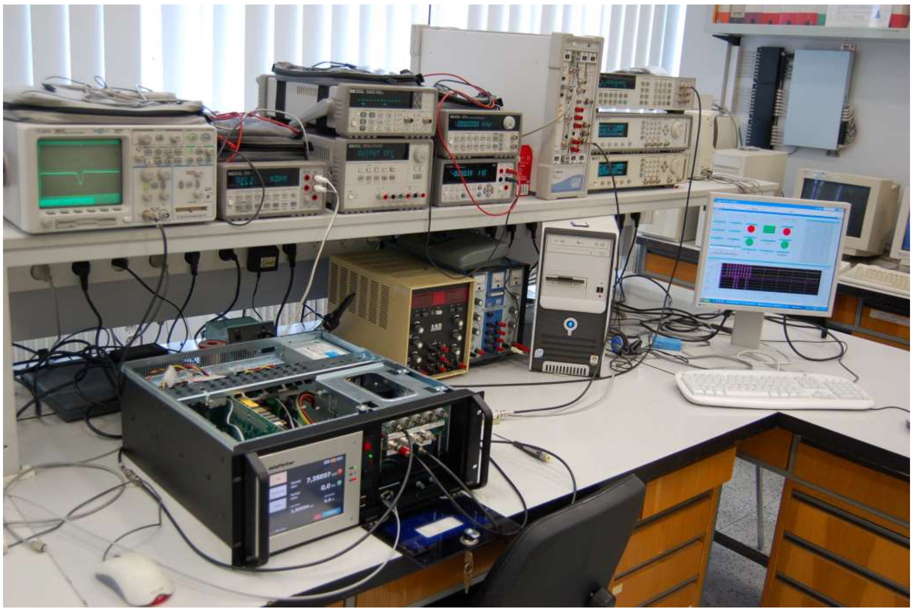


FIG. 11. Photograph of OPM validation test.

All validation tests were documented by the screenshots of the RD_OPM/RD_IPP program and its stored data files that describe the tests carried out. An extensive document on the results of the OPM and IPP channel validation tests was prepared.

8.2. Non-active tests

The objective of the non-active tests was to check the new I&C after its installation with simulated input signal and the sub-critical reactor active core (2 fuel elements removed) before the real operation with the standard reactor active core. During the non-active tests the following topics were checked:

(a) Rods control;

(b) Human-machine interface;

(c) Complete I&C tests with the simulated reactor operation.

The non-active tests were done twice, once after the control system upgrade in 2003 and the second time after full I&C upgrade and reinstallation in 2007. The HMI test was also repeated after the HMI software innovation in 2009.

8.2.1. Rods control test

During the rods control test, the behaviour of the rods and the cooperation with the control system were checked. The rods are controlled by Simatic S7-200 PLCs that communicate with the control system via a ProfiBus. Special software for the control system was developed to manipulate the absorbing rods without a start-up of the reactor (movement of only one rod in a moment is allowed because of safety reasons). The movement of the rods to the given position and the velocity of their movement were checked.

8.2.2. *HMI test*

The HMI PC communicates with the control system via an Ethernet line, the indicators and buttons of the HMI are controlled and read by a Simatic S7-200 PLC that is connected to the control system via a ProfiBus line. During the tests, proper communication between the HMI and the control system was checked. Commands that don't need cooperation with the OPM and IPP channels were first carried out and verified.

Also the communication among the OPM, IPP channels, their individual displays in the HMI and the control system were examined. Some minor problems in the message exchange between the OPM channels and the control system were revealed and corrected. Finally, commands from the HMI that require the OPM and IPP channels response were checked, e.g., channel modes, safety and warning limit changes.

8.2.3. *Complete I&C tests with simulated reactor operation*

During these tests, the operation of the reactor was simulated by the pulse and current signals from generators that were controlled by a PC to generate a proper reactor power course (see Fig. 12). The block diagram of the tests arrangement is shown in Fig. 13. The software for generation of the simulated reactor power was again prepared in the HP (Agilent) VEE development tool.

FIG. 12. Photograph of non-active tests arrangement.

During the non-active tests, the automatic I&C check, the reactor start-up and operation were examined. Special attention was paid to the safety (protection) functions of the I&C. Also different settings of the safety limits and other parameters were tested. The tests were documented by screenshots of the HMI monitors. The detailed report on the non-active tests was written – Ref. [7]

8.3. Active tests

At the beginning of the active I&C tests, the signals from the neutron chambers were connected to the I&C instead of the simulated signals that had been used during the non-active tests. The first tests were done with the 2 fuel elements taken out. The behavior of the I&C was carefully checked during this Configuration. Next, the 2 missing fuel elements were added to the active core, and the standard Configuration of the active core was restored. So, it was possible to start-up the reactor, to achieve the standard reactor operation and the critical status.

The safety functions, standard and non-standard operation, mode changes and parameter setting were carefully examined. Again, the screenshots of the HMI screens with comments were used to document the tests. Thorough document Ref. [8] describes the accomplished active tests of the reactor I&C.

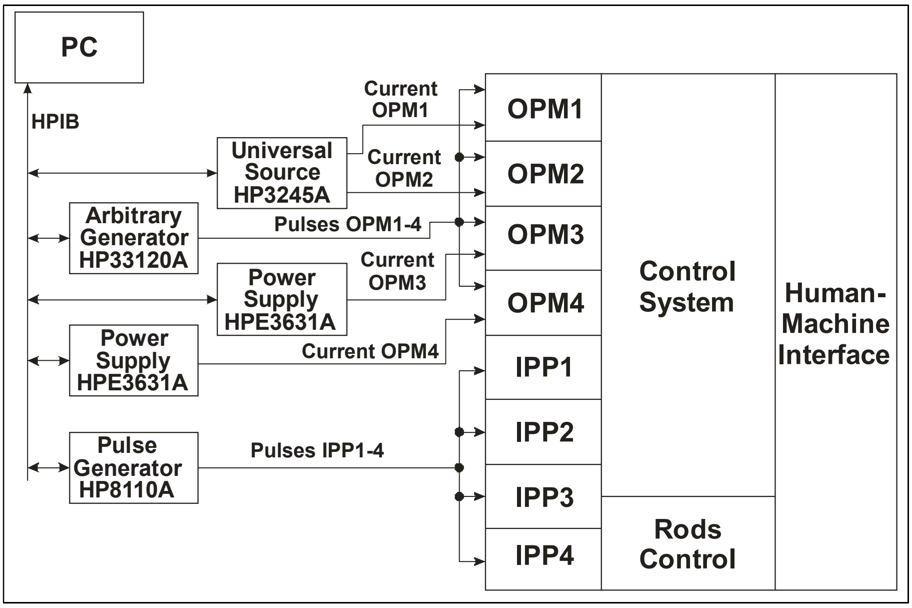


FIG.13. Block diagram of non-active tests arrangement.

9. LESSONS LEARNED

During the I&C development, installation and testing, much experience has been gained. First, we have found that correct requirements are very important for the successful manufacturing and operation of the I&C. It is necessary to analyze carefully the safety and operation of the system and put attention on special and rare operational modes. We have also observed that even thorough tests, verification and validation cannot reveal all potential failures of the I&C (especially of the software). The evaluation of the operational experience in the software and the whole system is very important for the revelation and the amendment of problems.

Finally, we met problems with electromagnetic interferences. The switching drives of step motors of absorbing rods with their long cables were the source of these interferences. The interferences negatively influenced the neutron flux (reactor power) measurement. Ferrite toroids on the step motor cables, proper shielding and grounding suppressed the influence of interferences.

10. CONCLUSION

The paper describes structure, installation and testing of the new reactor I&C at the VR-1 reactor. It describes the I&C status after all upgrade stages that started in 2001 and finished in 2010. The I&C was installed in the new I&C room with much better accessibility and maintainability than the I&C system in its old location. After the installation, the I&C was carefully tested. Validation tests of the new independent power protection and operational power measuring channels were accomplished. Next, the non-active tests with the simulated signals were carried out. Finally, active tests finished the process of the I&C upgrade. Successful I&C tests were a basis for the licensing of the reactor operation for the next period by the Czech State Office for Nuclear Safety.

The new I&C provides, compared to the previous one, better testability and maintainability, and uses up-to-date technology in both hardware and software. The neutron chamber signal processing provides more accurate reactor power measurement. Also, the quality requirements in both hardware and software were fulfilled during the I&C upgrade, according to respected international guidelines and standards. The complete upgrade brings the reactor I&C to top-level conditions and enables a prolongation of their functionality and maintainability for at least next 10 years.

Reliable and safe operation of the VR-1 training reactor is a highly important objective because the reactor is intensively used for training of students and future NPP staff in the framework of the Czech CENEN program in nuclear education. Every year around 200 university students from Czech Technical University in Prague, Charles University in Prague, Technical University in Brno and other locations get acquainted with the reactor. We must not forget to mention the cooperation with other European universities, for instance Fachhochschule in Aachen, Technical University in Budapest, Technical University in Vienna, Slovak Technical University in Bratislava, Royal Naval School of Marine Engineering (UK) and Royal University in Stockholm. The reactor is also involved in a number of international programs such as the IAEA technical cooperation program and training courses, and the European program ENEN for the nuclear education, e.g., Eugene Wigner Training Courses - Ref. [9], [10].

REFERENCES

[1] State Office for Nuclear Safety Requirements for Nuclear Safety, Radiation Protection, Physical Protection and Emergency Preparedness of Research Nuclear Equipment, Czech State Office for Nuclear Safety, Prague (2004).

[2] KROPIK, M., MATEJKA, K., CHAB, V. Upgrade of Training Reactor VR-1 Control System, Enlarged Halden Program Group Meeting, Sandefjord, Norway (2004).

[3] KROPIK, M., MATEJKA, K., JURICKOVA, M., New Independent Power Protection System for VR-1 Nuclear Training Reactor, Enlarged Halden Program Group Meeting, Lillehammer, Norway (2005).

[4] KROPIK, M., MATEJKA, K., KROPIK, M., New Operational Power Measuring System for VR-1 Nuclear Training Reactor, Enlarged Halden Program Group Meeting, Storefjell, Norway (2007).

[5] KROPIK, M., JURICKOVA, M., SKLENKA, L., New Digital I&C for VR-1 Training Reactor, Sixth American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC&HMIT 2009, Knoxville, Tennessee, USA (2009).

[6] KROPIK, M., RATAJ, J., JURICKOVA, M., New Human-Machine Interface at VR-1 Training Reactor, 18th International Conference on Nuclear Engineering, Xian, China (2010).

[7] KROPIK, M., JURICKOVA, M., Non-active tests of innovated I&C of VR-1 Training Reactor, FNSPE CTU in Prague, Czech Republic (2007) (in Czech).

[8] KROPIK, M., SKLENKA, L., JURICKOVA, M., Active tests of innovated I&C of VR-1 Training Reactor, FNSPE CTU in Prague, Czech Republic (2007) (in Czech).

[9] SKLENKA, L., KROPIK, MATEJKA, K., Improvements of the Training Reactor VR-1 - Only Way how to be Attractive for Students and Scientists, IAEA Conference on Research Reactors: Safe Management and Effective Utilization, Sydney, Australia (2007).

[10] RATAJ, J., Extensive utilisation of VR-1 Reactor for education and training, 14th RRFM 2010 conference, Marrakech, Morocco (2010).

EXPERIENCE WITH UPGRADES TO DIGITAL I&C SYSTEM OF FOUR REACTORS: TRIGA MARK II (AUSTRIA), VR-1, LR-0, AND LVR-15 (CZECH REPUBLIC)

M. KOCHOVÁ[1], P. STRNAD
[1]dataPartner s.r.o. (dP), České Budějovice, Czech Republic
E-mail contact of main author: kochova@datapartner.cz

Abstract. Research reactor operators (RRO‘s) face challenges during planning I&C digital upgrades which are needed due to various reasons. These issues range from regulatory authority approval, validation of new safety classified HW/SW to financial aspects. RRO’s realize that a systematic approach is essential in all stages of a new I&C system implementation along with selection of a qualified I&C supplier. Since 2005, European RRO’s of four reactors have selected a Czech company, dataPartner s.r.o. for I&C upgrades. Each upgrade was successfully completed on time and within budget. The success was based on joint graded approach of RRO’s, regulators, and the supplier in all phases of projects following applicable IAEA standards. This paper summarizes experience from I&C upgrades on the following reactors in Czech Republic: **VR-1** at Prague University, **LR-0** and **LVR-15,** both at Research Facility Rez. IAEA Safety Standard No. SSG-24 was applied for new systems. Also, IEC Standards (61513, 61226, 60780, 60880, … etc.) were followed in HW/SW development, IV&V and classification of safety function category A and B. Advanced planning, project management and close cooperation of state authority/reactor operator/supplier resulted in relatively short outage lasting 2,5 months. Operating License was issued in 2014. As of June, 2017, the LVR-15 I&C system has been in faultless performance for over 37 000 operating hours. The last I&C upgrade for Technical University of Vienna for **TRIGA® 250 kW** Reactor was completed in 2016. The dP I&C Systems proved excellent compatibility with various types of neutron chambers and reactors including rod controls. The I&C included newly developed wide range system for measurement of high power pulses of 250 MW. Reactor controls are based on programmable logic controllers. Experience from four reactor I&C upgrades prove that a project duration and cost depend on systematic planning and automated work progress monitoring throughout the project entire life cycle.

Key Words: I&C Upgrade, Neutron Flux Instrumentation, HW/SW Qualification, Safety Category Function A and B

1. INTRODUCTION

Three research nuclear reactors (types LR-0, VR-1, LVR-15) with digital I&C systems are currently operating in the Czech Republic. The dataPartner, a Czech company implemented the new safety digital I&C systems on these reactors over the years 2005-2015. For the latest installation on the LVR-15 reactor, the neutron instrumentation system was redesigned, so that it could be qualified along with the other components to fulfill the nuclear safety functions of categories A and B (according to IEC 61226) applying graded approach. Following experience gained on three Czech reactors, a complete I&C system refurbishment on the TRIGA Mark II 250 kW reactor in Vienna was undertaken and completed/licensed in 2016. Applicable industry practices and principles for such projects as well as the operators' experience of the previously implemented projects are adequately described in the IAEA/IEEE standards, manuals and technical TECDOC documents.
This document therefore provides some additional supplier’s experiences from these projects with focus on useful information for Research Reactor (RR) Operators who may consider future reactor I&C upgrades. It highlights some key project processes that can

help improve collaboration of operator/regulator/supplier. Using the information shown here (among others), the paper describes road to achieve compliance with safety and quality assurance policies that lead to the approval and a license issue from the regulator for an upgraded digital I&C system.
During preliminary meetings with operators, dataPartner encountered variation in applicable site specific requirements which was based on:

- the reactor type (safety category) and power level
- the specific reactor systems being upgraded (safety classification)
- the reactor projected life and operator financial capability

The estimated reactor I&C upgrade scope was one of cornerstone decisions for operators to upgrade I&C system.
In general, RR operators may consider the following I&C upgrades based on the existing I&C vintage:
complete I&C replacement with a new system of „4th generation“ digital I&C (description of 4 I&C generations in part 6.3 of IAEA Tech Report 482 for TRIGA is also useable for other RR‘s).
upgrade to a hybrid I&C from 2nd (just analog) to 3rd generation I&C (partially digital). Typically, safety systems remain analog and other systems are upgraded to digital to various extent. Can be done „4th generation ready“ for future full digital upgrade integration.
upgrade of the existing obsolete hybrid 3rd generation I&C to a more advanced 3rd generation. It can also be done „4th generation ready“ for future full digital upgrade integration.
obsolete analog I&C replacement with a modern analog (to maintain superior time responses of analog safety systems) with some digital I&C features
All four the above mentioned operators selected 4th generation I&C upgrade i.e. a complete reactor I&C replacement based on the following:

➢ *Operators and dP defined Site Specific Requirements*

- Deriving specific from general requirements by reviewing reactor systems and applying graded approach principles with justifications for new I&C on four different RR‘s
- Using also support from experts from UJV Rez and cooperating company TechCom International, Inc. from USA
- Subsequently, functional and system/equipment safety classification were established for each project

➢ *Operators clarified Site Requirements with Regulator*

- Supplier participated in clarifying pre-licensing meetings
- Operators applied for approval to proceed and after licensing process completion got Operating Licenses

However, it is recommended to RR operators, who have not upgraded yet, to examine the following options prior to considering I&C upgrade:
Operators undergoing/planning license renewal may incorporate the site specific I&C requirements for a future upgrade into the renewal license application*. These preapproved requirements may significantly simplify and shorten the future Regulatory reviews thus reducing licensing process time and future cost. DataPartner can assist in development of facility specific criteria for future I&C upgrades.

Operators may gradually install smaller scope I&C upgrades w/o a need of license update. The modern digital or analog I&C systems may be installed without affecting safety systems working in parallel with the existing I&C (sharing sensors including neutron flux channels if the existing equipment accommodates sharing). The smaller upgrades can be integrated into a larger I&C upgrade in the future.
*Alternatively, I&C site specific requirements can be documented in facility Strategic Utilization Plan to estimate future upgrade scope/cost

2. KEY ISSUES FOR EFFICIENT I&C UPGRADE

RR operator shall evaluate if he has sufficient expertise to manage the project or if the project shall be managed by an external Project Manager.
The following are identified key issues for a successful I&C upgrades based on dataPartner experience:

2.1. Quality Tender Documents

The Operator and the Regulator pre-application meetings determine the Basic Requirements for I&C upgrade. The resulting Tender Documents shall define and specify:

- Subject and scope of project
- Technical and functional requirements with necessary details
- I&C Upgrade Interface points and links to the existing systems
- Classification of Safety Functions
- Safety Requirements for the I&C System (based on Reactor and HW specifics)
- Defense in Depth, Redundancy, Independence, Diversity, Common cause failure, reliability, testability, responses to errors...
- Graded Approach and System/Qualification Requirements
- QA Documentation, Qualification, Technical and Users Documents, Inputs for Regulatory Documents
- Requirements for quality certificates, qualifications, methodology
- A realistic timetable with a time allowance for the Regulatory approval

Quality Tender Documents should provide basis for Quality Technical/Price Offer resulting in selection of a qualified and competent supplier thus assuring the successful completion of the project.

Supplier Participation in Meetings with Regulator

Country Specifics for Licensing and Approval of I&C Upgrades

For example, Czech Regulator, SUJB does not certify a specific vendor of I&C systems, but issues permission to operate only one specific site

Open Communication – Operator/Regulator/Suppliers

Suppliers participate in pre-application meetings with Regulator including input to submittals to Regulator. Emphasis on Safety SW development (unique process required by Czech legislative) – requirements to perform detailed audits at all SW development steps. Option for Regulator to witness audits. Full „100%“ SW testing.

Collaboration of the Supplier in preparation of documents for licensing

Supplier prepared: General Analyses on selected topics – System Architecture, Equipment Qualification, Reliability Assessment, Power Supply and Interfaces, and Final Reports
Operator prepared additional documents: e.g. Safety and security requirements, Nuclear Safety concepts, external connections and interfaces, Existing safety documentation updates, Audit Results…

2.2. Quality Assurance & Automatic Project Management

Governing document is Quality Assurance (QA) Plan generated by Operator and approved by Regulator (in Czech republic). The QA plan includes V&V, Audits and other QA items for the projects. It is the source for all Supplier QA documents including Supplier Project QA Program, Protocols, etc. The following Figure shows dataPartner Requirement Management System (RMS = automated tool) for maintaining QA at all project production steps

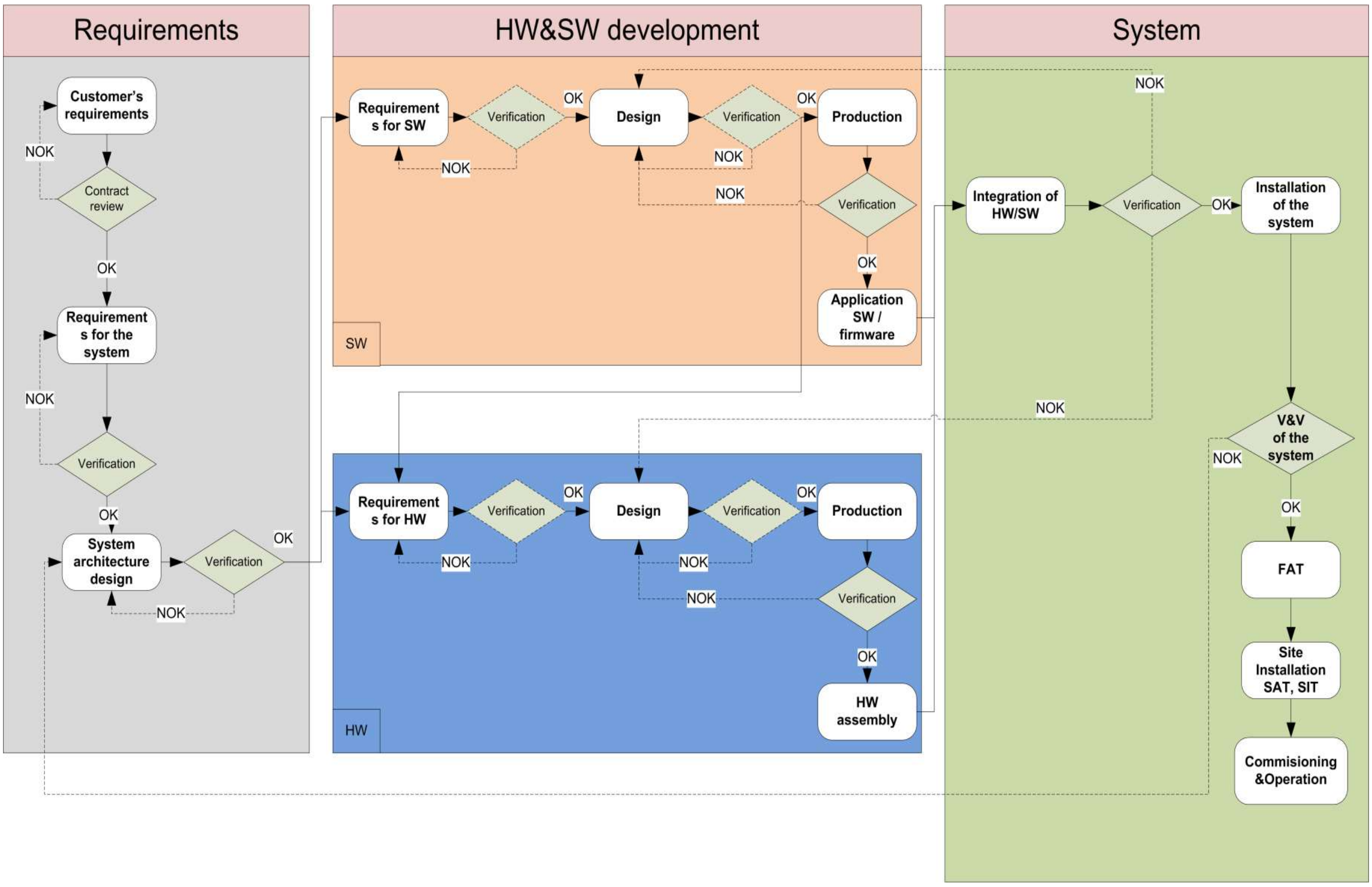


Fig. 1: Process Flow Chart and V&V

RMS is open access database system used by DataPartner to manage and trace projects from product requirements to the product turn over

- Introduced in the I&C Upgrade for Reactor LVR-15 in 2013
- Allows traceable verification of QA of all implementation steps
- Provides online QA basis for confidence of Customers, auditors, and regulators

- Monitors each requirement vs. project implementation process during entire project life cycle from design, implementation to testing, inspection hold points and operation. Shows requirement hierarchy (governing or secondary requirement) including requirement primary source.
- Defines work stages and milestones to meet specific requirements (e.g. for SW requirement it could be the following phases: „SW design“, „SW Coding“, and „SW Verification“)

RMS provided excellent results by tracing work from source requirements to implemented HW/SW functions during numerous independent and regulatory audits.
Typically, this relatively costly automated tool is utilized on quite larger projects, but dP could justify it anticipating repetitive application.

2.3. Qualification of Safety Function SW

Key issue was SW qualification for category A and B safety functions. Safety SW development processes were performed per IEC 60880, IEC 62138:

SW QA and Safety Classification, SW Configuration Management, The process of providing security SW, SW Requirement Specification, Process of selecting already developed SW, SW Development, SW Code Generation, Process SW integration: SW + HW, SW Implementation, SW Verification, SW Installation, SW Validation

Example: NI Module SW Development

Processor Hercules, Texas Instruments (TI) which was developed for safety and security applications, application-oriented programing C language, no operating system

SW Development Tools for TI processors (Code Composer Studio v5, TI ARM C/C++ Compiler v5.1.4, HALCoGen 03.08.01, HET IDE 3.3)

SW Development – Basic Principles

Documentation of the developed software is attached to source files with developed source code, documenting compliance by physical confirmation - protocols.

Documented functions - each function is stored in a separate source file

SW Qualification

Texas Instruments SW Development Tool Qualification

By comparing with the provisions of IEC 60880 - in SW documentation (RMS)

Independent Audits - Reports forwarded to the Regulator

SW Operation and Maintenance

Methodology example for Implementation programming language and encoding

No operating system is used on the modules (see PSW-SP-35 *) and all application software is written in hardware-specific C language (PSW-SP-38)*. The version of ANSI C89 (or ISO C90) is used, with the possibility of extending the C99 supported by the compiler used. Coding in C complies with MISRA rules: 2004. All the required rules are complied with in their own source code. Any suppression of the rule was limited to the minimum required area, and any suppression of the rule in its own code was justified (PSW-SP-33)*.

When the source code was translated, compiler optimization (PSW-SP-32)* was turned off

Protocols for all steps - design, coding, release testing, etc.

Entries to each function

Categories (A, B, C), reference to the standard, description of I/O, return values, description of function, version, list of directly called functions with marking, change table, test rule, ... – testing

**Requirement unique ID from RMS*

3. METHODOLOGY FOR DESIGN OF I&C SAFETY SYSTEMS

DataPartner has developed an internal methodology that monitors and controls individual process steps with an iterative approach. With consistent adherence to this procedure no process step has to go more than one step back if an error is detected.

3.1. Independent Audits and V&V

A prerequisite for successful licensing - ensuring an independent assessment

Independent Validation of NI Modules was performed by the Department of Nuclear Reactors of the Faculty of Electrical Engineering of the Czech University in Prague by simulation of NI Channel Input Signals and System Response Testing - Automatic Tests.

Then, Reactor Tests on VR-1, LVR-15 followed (done by Operator)

Experts hired by Operator performed independent audits of safety SW of Category A, SW planning documentation, compliance with IEC 60880 and Czech legislative requirements.

4. DATAPARTNER STRENGTHS IN I&C UPGRADES

Four successfully completed RR I&C upgrade projects involving R&D, component and system production, installation and start up

Competitive pricing

State of the art NIS developed and designed by dP

Scientific and technical support of Research Facility Rez (over 200 nuclear experts) and also by the Nuclear Engineering of Prague University experts

Close cooperation with Skoda Nuclear SJS for rod drives and TechCom International, Inc. a California I&C corporation for installations in US territory or research reactors in other areas applying the US licensing requirements per NUREG 1347. For example, US NRC position is that digital system upgrades require new system evaluations, a requirement driven primarily by the use of software SW V&V process is not a substitute for diversity 10 CFR 50.59 process alone is not sufficient if SW components are added

5. I&C REFURBISHMENT OF FOUR NUCLEAR RESEARCH REACTORS

5.1. Training Reactor VR-1 - Zero Power

The first dP experience was gained during replacement of the Control System of VR-1 at the Czech Technical University in Prague in 2003. DP worked there under the General Contractor, SKODA Nuclear Machinery, SJS a.s. which is a major Czech supplier of various nuclear equipment. In 2007, the upgrade of I&C continued and a new Neutron Instrumentation (NIS) System was installed. See table below in this section for more details on NIS channels and chamber types.

TABLE 1: NIS CHANNELS IN REACTORS VR-1 AND LR-0

NIS Channels and Detectors	Reactor VR-1, Prague University	Reactor LR-0, Rez Facility
Wide Range Operational Power Channels (OPM) ranges from startup to max power	4 Channels*	4 Channels**
OPM Channel Detector Type	Pulse Chamber RJ 1300	
Emergency Independent Power Protection Channels (IPP)	4 Channels*	3 Channels**
IPP Channel Detector Type	Low Sensitivity Current Chamber SNM12	

*One of OPM + one IPP channel serve as ***online*** back up during normal operating conditions
One of OPM + one IPP channel serve as ***offline* back up (spare parts)

Upgraded reactor control system also provides automatic power control integrated into control computer.

New HMI System on operator desk and at the panel in front of the operator consists of PC for visualization of reactor control process with 2 LCDs. Moderator circuits visualization is on independent HMI PC. Control SW for demineralized water treatment station (for moderator preparation) was supplied and "Experimental Studio" SW for setting and monitoring reactor experiments and also as the teaching tool for the students.

5.2. Research Reactor LR-0 - Zero Power

Refurbishment of I&C system for research nuclear reactor LR-0 at Nuclear Research Institute Rez, Czech Republic was finished in the year 2008. A new Neutron Instrumentation System (NIS) was installed. See table above in Section 3.1 for more details on NIS channels and chamber types. The following systems were replaced: SCRAM Logic, Control System, HMI, Emergency Buttons, Reactor Moderator Level Measurement, Neutron Source Position and Control, Status of Main Air Pump for valves, and interconnection of main moderator circuit. Refurbished **Reactor Control System** consists of the following subsystems: Control Computer, Rod Control, Automatic Power Control, Distributed Inputs and Outputs subsystem, and Operational Data Recording.

5.3. Research Reactor LVR-15, 10 MW

Operator: Research Facility Rez s.r.o.
Reactor I&C Upgrade Implementation: 2013 - 2015
General Contractor: ZAT a.s., Subcontractor: dataPartner

- Reactor Protection System and HMI
- Neutron Instrumentation (NI)
  - 3 NI Reactor Power Channels PMV
  - 3 NI Reactor Power Independent Channels NVO
  - 3 NI Reactor Start UP Channels SMV
- Automated Safety Logic Loops (HR)
  - Relay System for Reactor Emergency Shut Down
- Retrofit of Operator Console for Manual controls

5.3.1. LVR-15: State Regulator and Reactor Operator Requirements

Safety Function classification per IEC 61226 - Category A, B, and C
Reactor I&C Functions shall remain unchanged with minimal supplements
Operating Conditions for Programmable Safety System
  Monitored QA of SW Development Life Cycle meeting IEC 60880 (IEC 62138) requirements, SW Qualification per applicable standards, Complete SW testing, Complete documentation of Functional and System Design, Independent Audits
Safety Related Equipment Qualification:
  Equipment life 15 years – proof by accelerated temperature ageing
  Verification electromagnetic compatibility (EMC) by testing
  Verification of seismic resistance per NPP Standards by testing
  Functional Testing prior nad after environmental effects
  Safety System probability of failure is 10^{-4} per year
Independent Equipment Category A and B Validation – Neutron Instrumentation
Reactor LVR-15 of Safety Category II, has some construction limitations
  therefore, some aspects of I&C upgrade used graded approach with respect to NPP Standards
The following Standards were applied: IEC 61513, EN 61226, IEC 60880, IEC 60987, IEC 60780, IEC 980, IEEE-830.

5.3.2. LVR-15: Newly Designed Neutron Flux Channels

Basic Functions and Features
  Neutron flux measurements including relative speed change during normal and abnormal reactor conditions
  Shutdown signal generation following reactor operation outside specified boundaries and failures
  Wide range ranges (range up to 10 decades), speed and accuracy measurements
  NI Equipment supports start up, operation control, and shutdown. Reactor power can be controlled in both, manual and automated mode.
  Uninterrupted reactor status monitoring with signalization, auto diagnostics, and on-line/off-line testing
  Simple nad fast basic parameter setting (neutron chamber power supply, AZ compensation, calculation coefficients, dead time compensation for SMV)
  Compatibility features + flexibility (measured range changes, measured signal processing, NI system adaptation to neutron detectors)
  Qualification: specified equipment life is 15 years, EMC, seismic resistance, SW Qualification per IEC 60880 respectively 62138 with graded approach

5.3.3. LVR-15: Qualification of I&C Equipment for Safety Functions Category A and B

Qualification per Czech Standard CSN IEC 60780 JE – Electrical Equipment for Safety Systems – Qualification Verification
List of Qualification Tests
  Functional tests (before, at simulation, after - dataPartner)
  EMC Tests (ABEGU)
  Accelerated thermal aging (UJV Rez)
  Seismic Resistance Tests (Rizzo Associates Czech, Inc.)
Normal Operating Conditions (Mild Environment)

Average operating temperature: 30 °C
Maximum range of temperature changes: 15-35 ° C
Maximum pressure: 100 kPa, maximum humidity: 50%
Minimum equipment lifetime: 15 years
The environment of NI equipment placement is considered without elevated radiation (background level)

5.4. TRIGA MARK II 250 kW Reactor I&C system refurbishment

Operator: Technische Universität ATOMINSTITUT Wien, Austria
I&C Upgrade Completed: July 2016
General Contractor: Skoda Nuclear, SJS a.s.

- 1 fission wide-range chamber, 2 compensated and 1x non-compensated ionization chambers
- Control Rod Drives

Subcontractor dataPartner

- Neutron Instrumentation (NI)
  - 1 NI Reactor Power Channel OPM
  - 2 NI Independent Reactor Power Channels IPM
  - 1 NI Reactor Power Pulse Channel PPM
- LOGIC SCRAM Automatic
  - Relay system for rapid emergency shutdown of the reactor
- Control System, DAS, HMI, Experimental Studio
  - Manual/automatic reactor power control, operator stations, records and data processing...

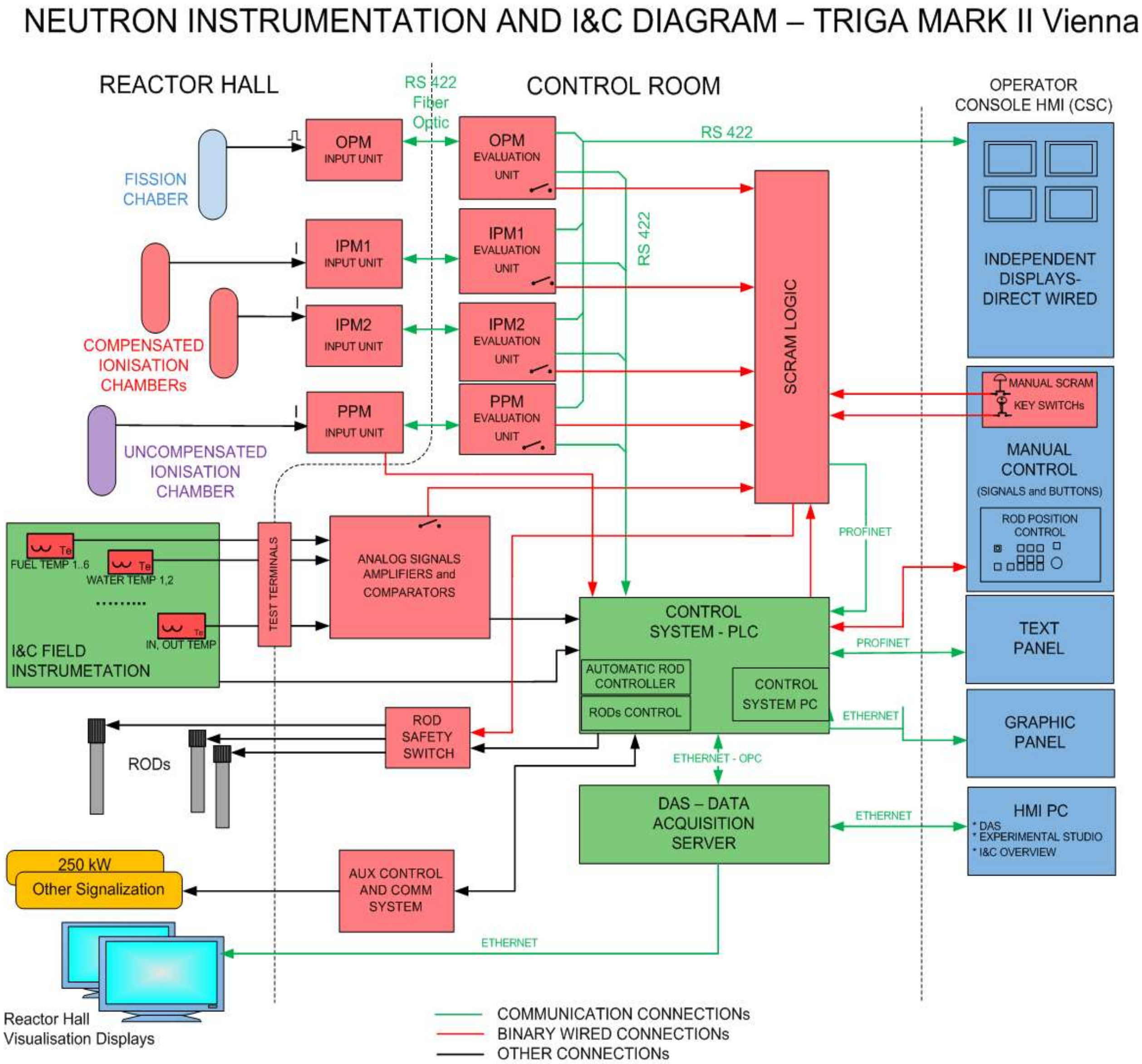


Figure 2: TRIGA Mark II

MEASUREMENTS ENHANCEMENT OF THE INSTRUMENTATION AND CONTROL FOR RESEARCH REACTORS

S. HAGGAG
Atomic Energy authority, Nuclear Research Center,
Egyptian Second Research Reactor (ETRR-II)
E-mail: sd_haggag@yahoo.com

Abstract. The Research Reactor (RR) is a pool-type reactor with an open water surface and variable core arrangement, the core cooling by light water, moderated by water and with beryllium reflectors. It has plate-type fuel elements with aluminum clad. the core thermal power 22 MW. The Reactor Protection System (RPS) commands two diverse and independent reactor shutdown systems that extinguish the nuclear reaction. The Thermal power is measured by summation of the heat exchanger power of core cooling system with pool cooling system or the power of the secondary side (cooling tower power consumption). The transmitters of the temperature were recalibrating. Accurate measurements are fundamental to operation and power control of any Research Reactor. This paper is to propose and discuss methods for verifying accurate measurements in a typical open pool RR. The recalibration technique is proposed for verifying the calibration of temperature instrumentation. Most critical process temperatures in Nuclear Research Reactor are measured using resistance temperature detectors RTDs. In addition to excellent reliability and accident survivability, nuclear safety related RTDs are expected to have good calibration and fast dynamic response time, as these characteristics are important to plant safety and economy. The power measuring system base on ^{16}N (Nitrogen-16) measurement can ensure accurate relationship between indicated power and actual core power. The reactor thermal power calibration is very important for precise neutron flux and fuel element burn up calculations.

Keywords: Nuclear Research Reactor, Temperature Transmitter and RTD

1. INTRODUCTION

In the RR we measure the power with three methods. The first is related to the neutronic flux we can execute the power by a constant factor depend on the core configuration, which is considered as a safety parameter. Second method is depending on the ionization of oxygen into nitrogen 16 with flow of the core cooling system and the third one is by the temperature difference on the heat exchanger in the primary cooling circuit with flow. A rise in the core cooling system flow to nominal operating conditions is deemed necessary in view of the observation made in the annex from the technical committee with respect to the fact that the said flow 10% lower than that registered by RPS and the values Registered after start-up and in further operations. The 10% mismatch is a consequence of the difference between the Flow meter and the transmitter scales. As a result of this change, there will be a rise in the pressure drop through the core. This rise makes it necessary to revise not only the mechanical design conditions but also SCRAM Safety System Setting due to both high and low pressure drop through the core, and to also carry out a new thermal balance at full power [1].

2. RESISTANCE TEMPERATURE DETECTORS (RTD)

Temperature transmitter is one of the most important transmitters in the reactor. It is used for resistance temperature detector (RTD) signal conditioning. It has built-in current excitation, instrumentation amplifier, linearization and current output circuitry which amplifies the RTD signal and gives linearization to it. Most critical process temperatures in Research Reactors

are measured using resistance temperature detectors (RTDs). In addition to excellent reliability and accident survivability, nuclear safety-related RTDs are expected to have good calibration and fast dynamic response time, as these characteristics are important to plant safety and economy. In Research Reactors where RTDs are installed in thermowells in the primary coolant pipes, response-time requirements have a range of 4 – 8 sec [2].
The calibrations are performed manually and involve two steps; each of which requires essentially the same work. The two steps are:

2.1. Determine if Calibration is Needed.

The step is performed by providing the instrument with a series of known inputs covering the operating range of the instrument. The output of the instrument is recorded for each input and compared with the acceptance criteria for the instrument.

If the instrument does not meet its acceptance criteria, it is calibrated by providing the same series of input signals as in Step 1 while adjusting the output to meet the acceptance criteria.The first step can be automated and performed while the plant is operating. This approach is therefore referred to as on-line calibration monitoring, on-line calibration testing, or on-line drift monitoring. It involves tracking the output of instrument channels over the fuel cycle to indention drift, bias errors, noise and other anomalies. The advantage of this approach is that it identifies calibration problems as they occur, accounts for installation and process condition effects on calibration, and prevents unnecessary calibration of instruments that have maintained their calibrations. Furthermore, it can include most components of an instrument channel in the calibration test as opposed to the conventional procedures which require some components to be calibrated individually. The method may be used for pressure, level, flow, temperature, neutron flux, and other process instrumentation channels including both safety related and non-safety related channels in the primary and secondary systems of research Reactors [3].

3. RR MEASUREMENTS AND INSTRUMENTATION

the measurements and instrumentation for a typical open pool RR plant As shown in Fig 1. The nuclear and process measurements of interest are indicated in the schematic view of the plant. In some RR the cooling systems consists of two core cooling loops and pool cooling system with interconnection system [1] [5].

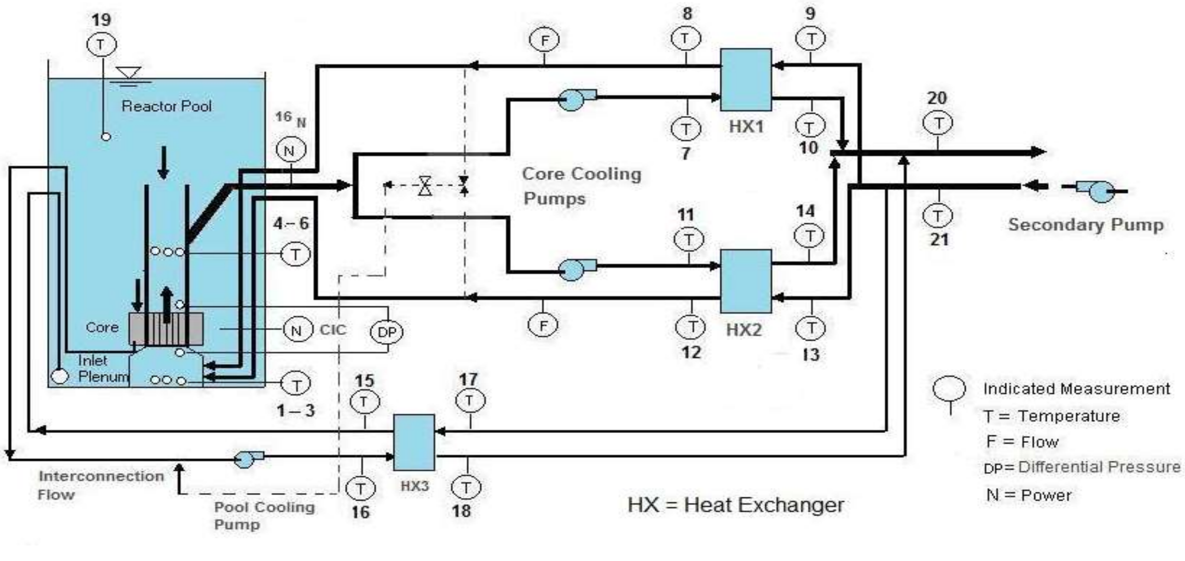


Fig. 1. Schematic view of typical open pool type RR plant

Temperatures (T) are measured with RTDs (Resistance Temperature Detectors), which use platinum elements, have very high sensitivity, linearity and precision. RTDs can be used safely up to temperatures of 500°C, and in general have larger time constant than thermocouples. The temperature is indicated through a measurement of the resistance R(T) of the element [6]:

$R(T) = Ro\,(1+ \alpha\, T)$ (1)

Detectors used are platinum 100 RTD type (Ro = 100 ohm and α = 0.00385), specified in accordance to DIN 43760 Class A with maximum allowable deviation of +/- 0.13 ohm. Each core inlet (outlet) coolant temperature measurement assembly includes two platinum 100 detectors. The first detector is used for inlet (outlet) coolant temperature measurement. The second detector is used for core coolant Differential Temperature (DT). Each coolant temperature measurement includes platinum 100 detectors are connected to RTD and to current converters to provide a 4 - 20 mA output current. The current is wired to monitoring and control system and protection system [1].

Despite the several techniques of flow measuring, the most common type of flow meters use differential pressure transmitters to measure the difference in pressure caused by orifice plates or venture tubes placed in the piping system. Accuracies of the order of 3% are easily achievable, and the instruments are simple and extremely reliable, therefore suitable for safety systems [1]. The subsystem is calibrated to evaluate the Flow (F) as a function of the Differential Pressure (DP). Maximum flow and operation temperature should be specified.

$F = \text{constant} \sqrt{DP}$ (2)

It is also important to notice that the differential pressure can be measured in other locations like in the reactor core itself. The reactor core is a restriction to the flow, and it causes a differential pressure. The coolant flow is measured directly on the reactor core and this signal known as core DP, is usually used in the reactor protection system. Most of them are used to assure that there is coolant flowing in the system. Differential pressure through the core is measured by means of differential pressure transmitters. Transmitters used are of the capacitive sensor type and develops a 4 - 20 mA current output. Maximum inaccuracy must be equal or lower than 0.2 % of full span [1].

Compensated Ionization Chambers (CICs) are used to measure the core neutron flux. The main reason to monitor neutron flux in a RR is that it is proportional to the power density, and this is the variable which operators are concerned about. Detectors are located in fixed positions about or around the reactor core, and the quantity measured is often the leakage flux, i e, the flux exterior to the core to place it as far as possible from the core. This will reduce radiation hazard to the detector and also limit the effect of gamma induced current [1]. The measured neutron flux is calibrated using thermal power measurements during power rise procedures ensuring linearity and accurate relationship between indicated and actual core power. The core power is calculated using core Differential Temperature (DT_{core}) and power transferred to the pool (P_{Pool}) and expressed as [4]:

$P_{Core} = 1.16\,(\text{Core Flow} \times DT_{core} + P_{Pool}) \pm 0.08$ (3)

Where P_{Pool} = Pool Flow × pool heat exchanger primary side inlet and outlet temperature difference. This method has the advantage of its faster estimation of the core power and therefore number of calibration points can be obtained. However, possible temperature non-uniformity between RTDs that are used in measuring the outlet core temperature is the main disadvantage of this method.

The second method of thermal balance needs not less than 6 hours. The core power is calculated using the measured flow (F) and heat exchanger primary side inlet and outlet temperatures (Ti HX and To HX respectively). The subscripts 1, 2, and 3 denote, respectively, core cooling loop 1, core cooling loop 2, and pool cooling system.

P_{core} = rho_1 Cp_1 F_1 (To HX_1 – Ti HX_1) + rho_2 Cp_2 F_2 (To HX_2 – Ti HX_2) + rho_3 Cp_3 Pool Flow (To HX_3 – Ti HX_3) (4)

Where the water density (rho) and specific capacity (cp) is calculated at the average temperature using the equations [8]:

$$rho = 2.080 \times 10^{-5}\ T^3 - 6.668 \times 10^{-3}\ T^2 + 0.04675T + 999.9 \quad (5)$$

$$Cp = 5.2013 \times 10^{-7}\ T^4 - 2.1528 \times 10^{-4}\ T^3 + 4.1758 \times 10^{-2}\ T^2 - 2.6171T + 4227.1 \quad (6)$$

^{16}N activity is produced by the activation of ^{16}O (oxygen-16) within the reactor core, through the nuclear reaction: 'n (neutron) + $^{16}O \longrightarrow {}^{16}N + {}^{1}p$ (proton). The ^{16}N level is therefore proportional to the reactor integral flux, or the integral power. Hence a detector that is located near a core coolant discharge line can be used to monitor the activity ^{16}N level and hence the core power. This approach provides a method for corroborating the obtained power from neutron detectors and thermal balances. However, it should be recognized that the power signal from a ^{16}N detector will be delayed relative to the true core power by the time required for the coolant to flow from the core to the detector location.

Power = conversion parameter × ^{16}N current (PA) (7)

^{16}N activity is measured by an ionization chamber. This conversion parameter of the power measuring system is estimated first using thermal power measurements.

4. CALIBRATE AN RTD TRANSMITTER

The RTD Transmitter is usually factory calibrated to the temperature range shown on the device name plate. When the performances deteriorate and the transmitter needs recalibration, the transmitter is normally calibrated by using a resistance decade box.

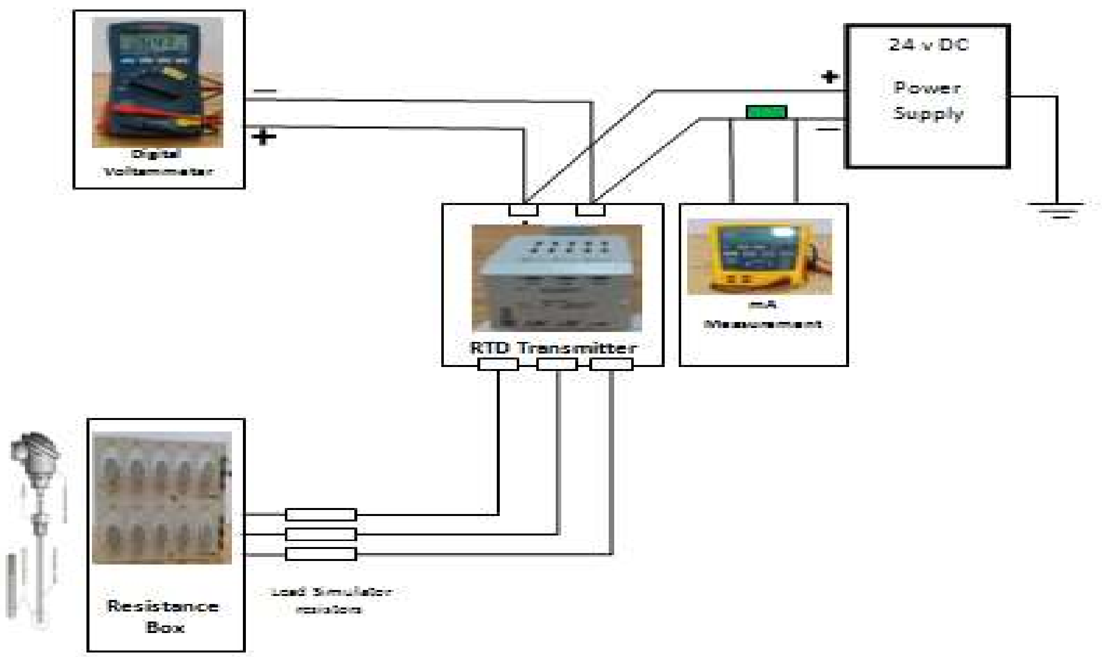


Fig.2. Calibrate the RTD transmitter.

To calibrate the RTD transmitter, the following equipment will be required:

1. DC Voltage Power Supply (any voltage from10 - 36 VDC)
2. Digital Malltimeter for measuring mille Ampere
3. Sensor Input Calibrator. Precision Decade Box (0 - 200 Ohms).

4. Process calibrator

Connect the equipments as shown in Fig.2 and setup the calibration steps:

1. Locate the RTD transmitter terminal by removing the housing cover
2. If an RTD is already connected, remove all the RTD lead connections
3. Determine the RTD resistance at the desired base (0 C) and full scale temperatures
4. Turn the power supply on
5. Set resistance decade box to the resistance that corresponds to the desired base temperature. Adjust the zero pot (potentiometer) of transmitter until the output is 4mA
6. Set resistance decade box to the resistance that corresponds to the desired full scale temperature. Adjust the span pot (potentiometer) of transmitter until the output is 20 mA
7. Repeat the above steps until both 4 and 20 mA readings are obtained without readjusting span and zero potentiometers.

we have 2 heat exchanger for the core cooling circuit and one for pool cooling circuit, mean 3 instrumentation sets for measuring the power, so we make a calibration for the 3 sets of instrumentation, inlet temperature, outlet temperature and flow meter. We made a calibration for 3 sets of primary circuit. And do the same for the secondary circuit, and the calibration data after and before are attached. Typical Resistance and Sensitivity values for PT-100 as shown in Fig.3 and acceptable deviations in Ohm and Temperature values for a Pt100 as shown in Fig.4.

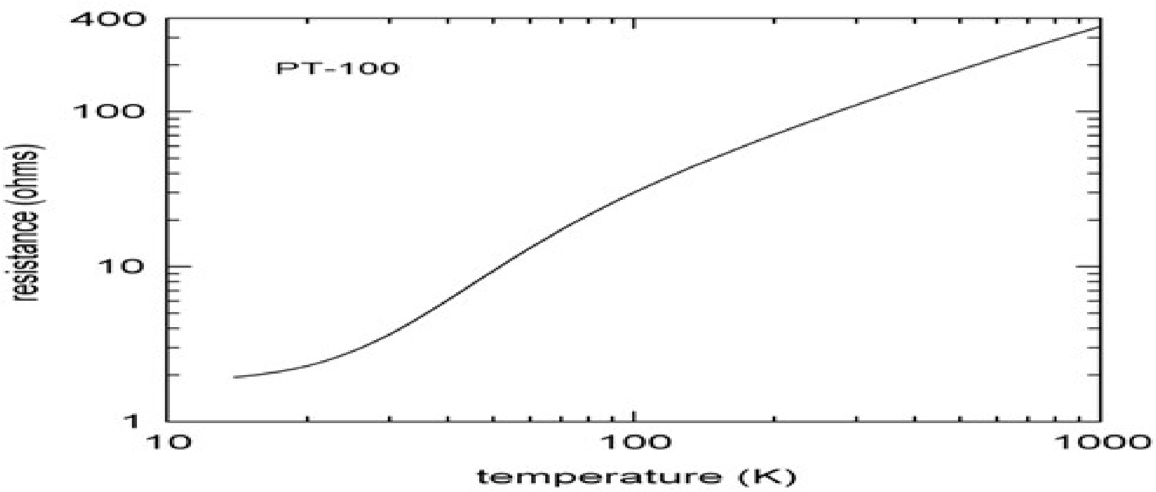


Fig.3. Typical Resistance and Sensitivity values for PT-100s.

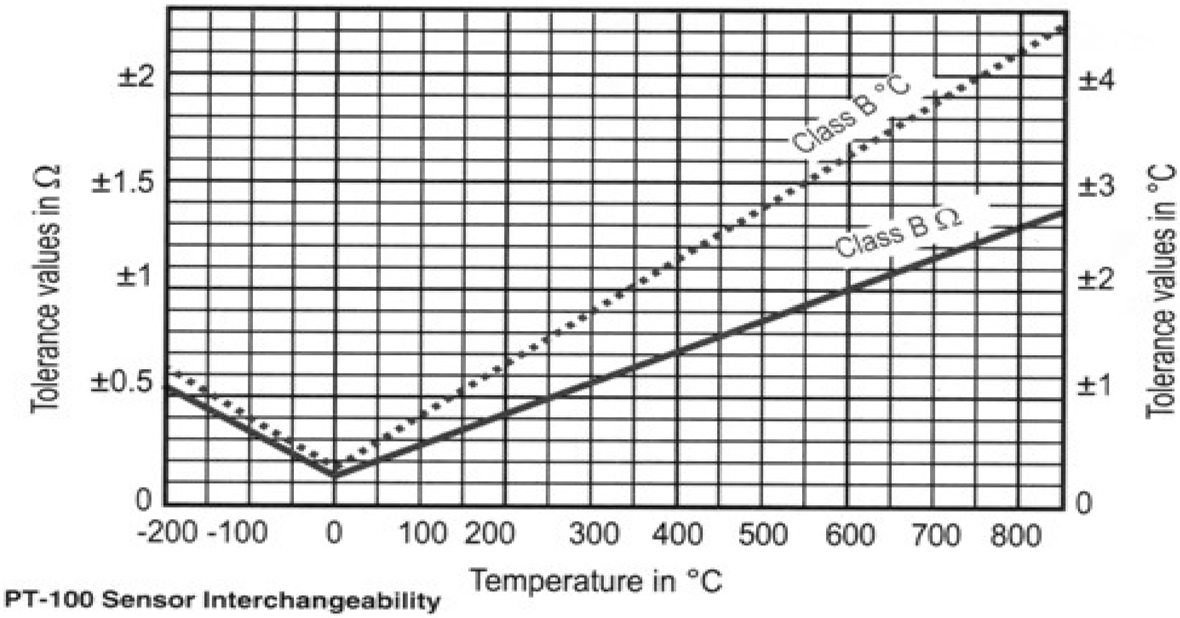


Fig.4. Acceptable deviations in Ohm and Temperature values for a Pt100

5. RESULTS OF TEMPERATURE TRANSMITTER CALIBRATION

Results of Calibration of the temperature of outlet and inlet heat exchanger in the primary cooling circuit and all sensors RTD temperature and transmitter affecting the calculation of thermal power. Table 1 shows calibration result in the range (10-70 C^0) .Table 2 shows calibration result RTD in the range (0-100 C^0). Table 3 shows calibration result RTD in the range (0-50 C^0). Table 4 shows calibration result on RTD of core coolant Differential Temperature (DT) in the range (0-20 C^0). The linear and vertical curve shown in Fig.5. shows the temperature values before and after calibration. The Fig. 6. shows example of error results of temperature values before and after calibration and shows the electronic channel error. Fig.7. shows the thermal power (MW) after calibration of outlet RTD temperature transmitter.

TABLE 1: CALIBRATION RESULTS OF THE RTD TEMPERATURE TRANSMITTER (0-70 C)

D - CALIBRATION RESULTS										
Input	Output of Transimetter			Output on	ransm. Output Err		ansm. Output Er		Output	Electronics
[Enginnering units]		[mA]		monetoring	[mA]		[% of span]		Total Error	channel
				screens			(a)		© = (a) + (B)	Error (b)
[C°]	ref.	As found	After Calib.	[Co]	As found	After Calib.	As found	After Calib.	%of Span	(b) =© -(a)
10	4	3.95	3.97	9.79	-0.05	-0.03	-0.3125	-0.18773	-0.35	-0.162265332
16	5.6	5.53	5.57	15.92	-0.07	-0.03	-0.4375	-0.18773	-0.13333333	0.054401335
22	7.2	7.11	7.16	21.98	-0.09	-0.04	-0.5625	-0.25031	-0.03333333	0.216979558
28	8.8	8.7	8.79	27.82	-0.1	-0.01	-0.625	-0.06258	-0.3	-0.237421777
34	10.4	10.3	10.38	33.85	-0.1	-0.02	-0.625	-0.12516	-0.25	-0.124843554
40	12	11.89	11.96	39.71	-0.11	-0.04	-0.6875	-0.25031	-0.48333333	-0.233020442
46	13.6	13.49	13.59	45.89	-0.11	-0.01	-0.6875	-0.06258	-0.18333333	-0.120755111
52	15.2	15.11	15.16	51.96	-0.09	-0.04	-0.5625	-0.25031	-0.06666667	0.183646224
58	16.8	16.71	16.79	57.97	-0.09	-0.01	-0.5625	-0.06258	-0.05	0.012578223
64	18.4	18.32	18.38	63.92	-0.08	-0.02	-0.5	-0.12516	-0.13333333	-0.008176888
70	20	19.93	19.97	69.85	-0.07	-0.03	-0.4375	-0.18773	-0.25	-0.062265332

TABLE 2: CALIBRATION RESULTS OF THE RTD TEMPERATURE TRANSMITTER IN THE RANGE (0-100 C^0)

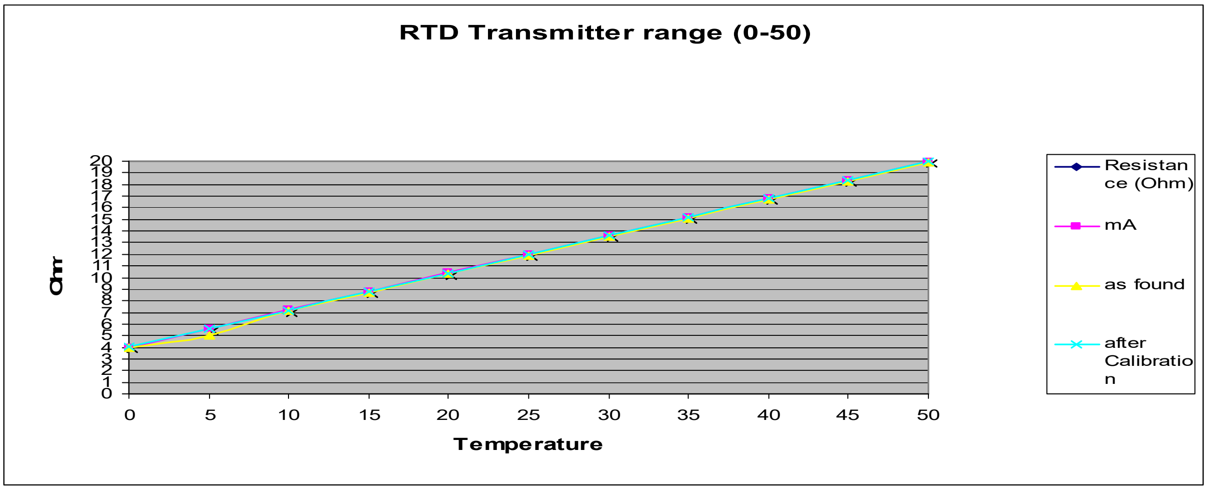
D - CALIBRATION RESULTS										
Input	Output of Transimetter			Output on	ransm. Output Err		ransm. Output Err		Output	Electronics
[Enginnering units]		[mA]		monetoring	[mA]		[% of span]		Total Erro	channel
				screens			(a)		© = (a) + (B	Error (b)
[C°]	ref.	As found	After Calib.	[Co]	As found	After Calib.	As found	After Calib.	%of Span	(b) =© -(a)
0	4	4.018	4.02	0	0.018	0.02	0.1125	0.12444002	0	-0.12444002
10	5.6	5.64	5.61	10.01	0.04	0.01	0.25	0.06222001	0.01	-0.05222001
20	7.2	7.26	7.22	20.19	0.06	0.02	0.375	0.12444002	0.19	0.06555998
30	8.8	8.87	8.82	30.3	0.07	0.02	0.4375	0.12444002	0.3	0.17555998
40	10.4	10.43	10.41	40.3	0.03	0.01	0.1875	0.06222001	0.3	0.23777999
50	12	12.07	12.01	50.4	0.07	0.01	0.4375	0.06222001	0.4	0.33777999
60	13.6	13.65	13.61	60.5	0.05	0.01	0.3125	0.06222001	0.5	0.43777999
70	15.2	15.29	15.2	70.5	0.09	0	0.5625	0	0.5	0.5
80	16.8	16.88	16.81	80.4	0.08	0.01	0.5	0.06222001	0.4	0.33777999
90	18.4	18.49	18.42	90.5	0.09	0.02	0.5625	0.12444002	0.5	0.37555998
100	20	20.09	20.02	100.4	0.09	0.02	0.5625	0.12444002	0.4	0.27555998

TABLE 3: CALIBRATION RESULTS OF THE RTD TEMPERATURE TRANSMITTER IN THE RANGE (0-50 C^0)

D - CALIBRATION RESULTS															
Input [Enginnering units]	Output of Transimette [mA]			Simulated Input in eng. Units reflecting mA input. IN [Co]		put on monetoring scre IN [Co]		ansm. Output Err [mA]		ansm. Output Er [% of span] (a)		Electronics error [mA]		Total error [% of span]	
IN [C°]	ref.	As found	After Calib	As found	After Calib.	As found	After Calib.	As found	After Calib.	As found	After Calib.	As found	After Calib.	As found	After Calib.
0	4	3.95	4.01	-0.15625	0.03125	-0.2	0.15	-0.05	0.01	-0.3125	0.0625	-0.0875	0.2375	-0.4	0.3
5	5.6	4.98	5.59	3.0625	4.96875	3.05	5.05	-0.62	-0.01	-3.875	-0.0625	-0.025	0.1625	-3.9	0.1
10	7.2	7.12	7.19	9.75	9.96875	9.89	10.28	-0.08	-0.01	-0.5	-0.0625	0.28	0.6225	-0.22	0.56
15	8.8	8.7	8.77	14.6875	14.90625	15.4	15.11	-0.1	-0.03	-0.625	-0.1875	1.425	0.4075	0.8	0.22
20	10.4	10.29	10.38	19.65625	19.9375	20.09	20.26	-0.11	-0.02	-0.6875	-0.125	0.8675	0.645	0.18	0.52
25	12	11.88	11.97	24.625	24.90625	25	24.76	-0.12	-0.03	-0.75	-0.1875	0.75	-0.2925	-2.2E-15	-0.48
30	13.6	13.49	13.58	29.65625	29.9375	30	30.27	-0.11	-0.02	-0.6875	-0.125	0.6875	0.665	3.55E-15	0.54
35	15.2	15.08	15.18	34.625	34.9375	35.16	35.21	-0.12	-0.02	-0.75	-0.125	1.07	0.545	0.32	0.42
40	16.8	16.69	16.8	39.65625	40	39.87	39.92	-0.11	0	-0.6875	0	0.4275	-0.16	-0.26	-0.16
45	18.4	18.28	18.4	44.625	45	45.09	44.95	-0.12	0	-0.75	0	0.93	-0.1	0.18	-0.1
50	20	19.88	20	49.625	50	49.98	49.98	-0.12	0	-0.75	0	0.71	-0.04	-0.04	-0.04

TABLE 4 : CALIBRATION RESULTS OF THE RTD TEMPERATURE TRANSMITTER IN THE RANGE (0-20 C^0)

D - CALIBRATION RESULTS											
Input [Enginnering units]		Output of Transimeter [mA]			Output on monetoring screens	Transm. Output Error [mA]		Transm. Output Error [% of span] (a)		Output Total Error © = (a) + (B)	Electronics channel Error (b)
[C°]	Ohm	ref.	As found	After Calib	[Co]	As found	After Calib.	As found	After Calib.	%of Span	(b) =© -(a)
0	100	4	4.008	4.05	-0.1	0.008	0.05	0.05	0.3109066	-0.5	-0.8109066
2	100.77	5.6	5.65	5.62	2	0.05	0.02	0.3125	0.1243626	0	-0.1243626
4	101.54	7.2	7.25	7.22	3.9	0.05	0.02	0.3125	0.1243626	-0.5	-0.6243626
6	102.31	8.8	8.84	8.84	5.9	0.04	0.04	0.25	0.2487253	-0.5	-0.7487253
8	103.08	10.4	10.43	10.42	8.1	0.03	0.02	0.1875	0.1243626	0.5	0.37563736
10	103.85	12	12.02	12.02	10	0.02	0.02	0.125	0.1243626	0	-0.1243626
12	104.62	13.6	13.65	13.62	12.1	0.05	0.02	0.3125	0.1243626	0.5	0.37563736
14	105.39	15.2	15.26	15.22	13.9	0.06	0.02	0.375	0.1243626	-0.5	-0.6243626
16	106.16	16.8	16.86	16.83	16.1	0.06	0.03	0.375	0.186544	0.5	0.31345604
18	106.93	18.4	18.47	18.44	18.1	0.07	0.04	0.4375	0.2487253	0.5	0.25127472
20	107.76	20	20.09	20.05	20	0.09	0.05	0.5625	0.3109066	0	-0.3109066



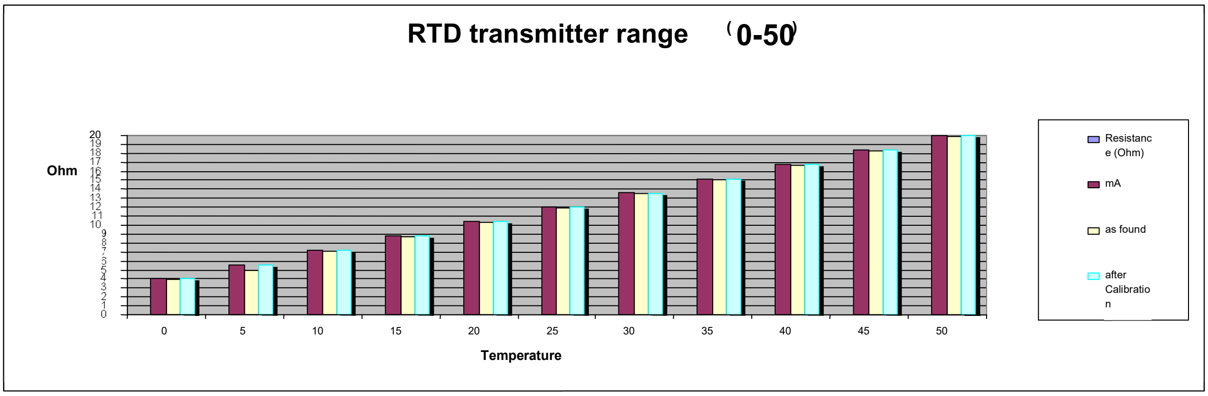
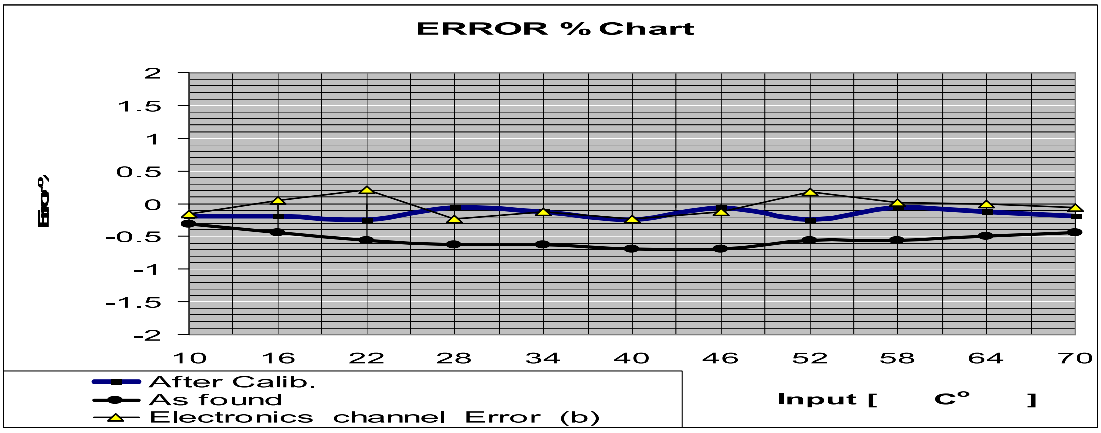


Fig.5.The Temperature values and mili Ampere before and after calibration



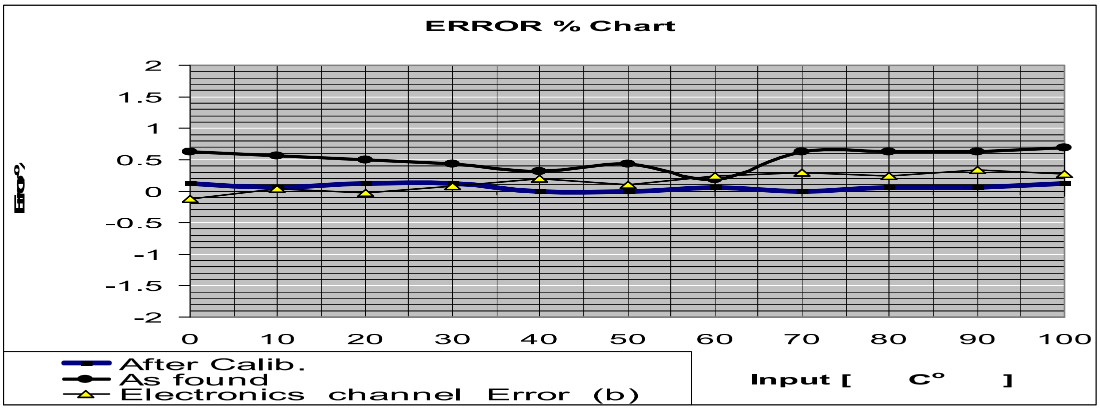


FIG 6: Example of Error Results after Calibration of the temperature of outlet and inlet heat exchanger in the primary cooling circuit

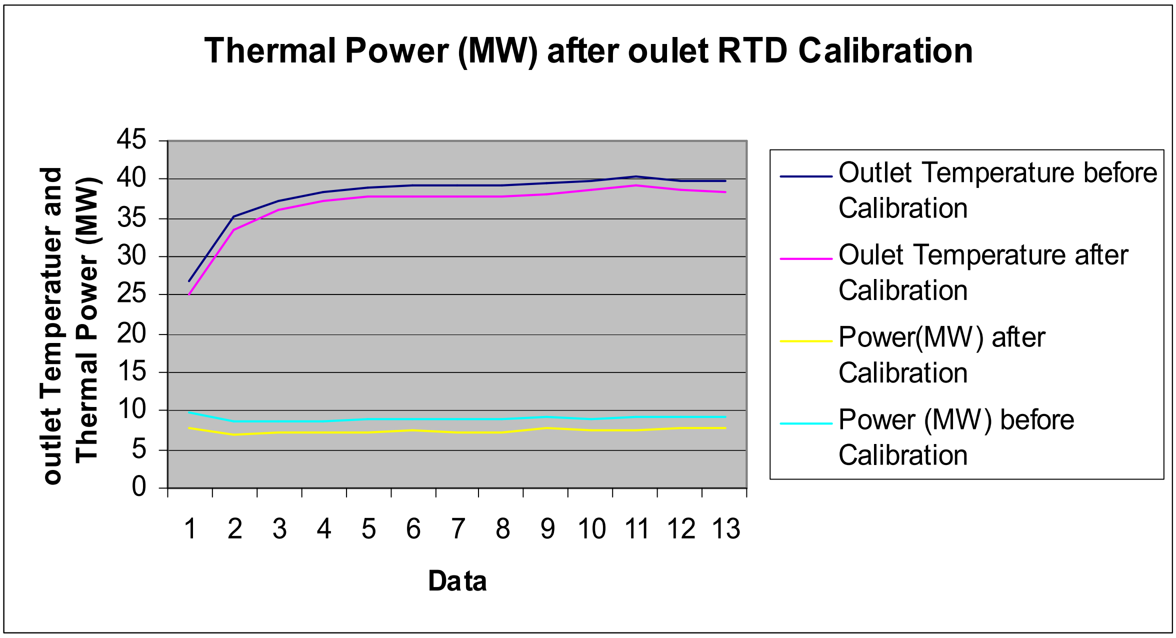


Fig.7. The Thermal Power (MW) after calibration of outlet RTD temperature transmitter

6. CONCLUSIONS

Most critical process temperatures in Research Reactors are measured using resistance temperature detectors (RTDs). In addition to excellent reliability and accident survivability, nuclear safety-related RTDs are expected to have good calibration and fast dynamic response time, as these characteristics are important to plant safety and economy. The calibration was success to improve the temperature measured after calibration the thermal Power is equal to the N16 power measurement. Methods for verifying accurate measurements of research reactor temperature, core flow and power have been reviewed. The methods of calibration verification comply satisfactory with the operational requirements and thus it is proposed for use in similar RR plants. the instrumentation for temperature and flow signal measurement was incorporate in the data acquisition system. The evolution of this parameter is displayed, in real time, and recorded on the digital monitoring system computer developed for the reactor . The reactor thermal power calibration is very important for precise neutron flux knowledge for many irradiation experiments and fuel element burn up calculations.

References

[1] M. A. Gaheen,"Methods for verifying Accurate Measurements in Research Reactors "RRFM European Research Reactor Conference,18-22 March,2012 ,pp 41-47.
[2] Amir Z. Mesquita, H. C. Rezende, R. M. Souza, "Power Calibration of the TRIGA Mark I Nuclear Research Reactor", Vol. XXIX, No.3,July – September 2007, pp 240-245.
[3] Amir Z. Mesquita, H. C. Rezende, R. M. Souza, "Thermal Power Calibrations of the IPR-R1 TRIGA Nuclear Reactor"20th International Congress of Mechanical Engineering Copyright © 2009 by ABCM November 15-20, 2009, Gramado, RS, Brazi.
[4] International Atomic Energy Agency, "Research Reactor Instrumentation and control technology," IAEA –TECDOC-973, Vienna, October 1997.
[5] J. E. Moorman, P. A. Beeley, J.P. Highton, "A Review of Four Methods for the Independent Monitoring of Core Power in the Jason Argonaut Reactor," IAEA-SM-

360/50P, Research Reactor Utilization, Safety and Management, Symposium held in Lisbon, Portugal, 6–10 September 1999.
[6] H. M. Hashemian, “Maintenance of Process Instrumentation in Nuclear Power Plants,” Springer-Verlag Berlin Heidelberg 2006.
[7] G. Gennuso, A. Doval, “steps for power rise,” Procedures No. 767-5420-3ppcg-011-10, 23 Nov 1997.
[8] Gee Y. Han, “Mathematical Dynamic Modeling and Thermal-Hydraulic Analysis of HANARO,” International Communication of Heat and Mass Transfer, Vol. 28, pp. 651-660, 2001.

FEASIBILITY STUDY FOR THE EGYPTIAN FIRST RESEARCH REACTOR POWER UPGRADING FROM 2 MW TO 10 MW

M.S. EL-KOLIEL
Atomic Energy Authority, Nuclear Research Center, Reactors Dept.
Cairo, Egypt

Abstract

After 50 years of the Egyptian First Research Reactor (ET-RR-1) operation, a modernization program for the reactor systems is required in order to achieve two main objectives: safe operation of the reactor in accordance with the provisions of the updated safety standards and reactor utilization in a competitive environment to satisfy the current and future demands and requirements of nuclear research. In view of changing experimental needs and isotope production at high neutron fluxes as well as future safe reactor operation, it should be decided to upgrade the reactor power. Partial decommissioning of ET-RR-1 will be required before incorporating improvements in the systems and installation of equipments for the upgrading and refurbishment activities. Power upgrade, will demand detailed reactor design calculations pertaining to core neutronics, thermal hydraulics, shielding, accident analysis, and radiological consequence analysis. The current condition of the reactor allows for its safe operation for at least 20 – 25 more years if all reactor systems are refurbished, modified or changed. Thus, extending reactor operations till 2035 should be considered the strategic goal. The main goal of the present study is to introduce an outline plan for the power upgrading of ET-RR-1 from 2 MW to 10 MW, in order to improve the current applications and to develop new ones. To achieve this objective, a new reactor core with other fuel elements and a beryllium reflector will be developed. The concept of power upgrading should take into account all feasible and available possibilities, such as fuel questions, core Configuration with increased irradiation facilities, technical capabilities including utilization issues, as well as future operation and maintenance questions. The problem of finding an ultimate solution of the spent fuel problem (which already exists in the spent fuel storage tanks) should be considered. Finally, on the basis of the considerations listed above, the reconstruction and upgrade project should be drafted including an outline of the project schedule and the required resources, including financial and human demands. At an early planning stage, the future of the facility has to be shown to the national political authority by providing a detailed business plan, where the costly upgrading project should be compared against the cost of decommissioning the facility. However, in both cases, very well-planned and skilful management of these activities are required.

1. INTRODUCTION

ET-RR-1 is a tank-type research reactor, moderated, cooled and reflected by distilled light water, and went critical in 1961. The reactor is of former Soviet Union origin (WWR-S design standard), has nominal thermal power of 2 MW, with a corresponding maximum thermal neutron flux of about 2×10^{13} n/cm^2 sec. For almost 50 years, the reactor has been in operation with some interruptions due to various incidents, mostly in the reactor cooling and electrical systems. The total full power operating time is equal to ~ 17,500 hours. The reactor operates by the well known Aluminum claded, 10% enriched EK-10 type fuel pins in 4×4 fuel assemblies. The reactor was shutdown in April 2010 and the core was entirely unloaded into the old spent fuel storage tank. The vertical and horizontal views of ET-RR-1 are shown in Fig. 1 and Fig. 2, respectively.

The main purpose of the power upgrade of ET-RR-1 is to increase the radioisotope production capabilities of direct impact to social developments, as well as to increase the activities in nuclear physics research, such as neutron activation analysis, neutron radiography, radiochemistry, shielding investigations, and neutron scattering. More importantly however, is its mission to establish and maintain an active nuclear research culture in the country. In the present case of ET-RR-1, the samples are irradiated at the reactor shield and required long irradiation times because of the low neutron flux at that location. The core will be redesigned and a central irradiation facility can be created in the centre of the core, where the maximum thermal neutron flux will be on the order of ~ 1.5×10^{14} $n \cdot cm^{-2} \cdot s^{-1}$.

Safety studies related to the project should be performed in order to obtain a license for the entire facility, not only because of the modifications but also to generate updated regulatory documents, including the safety analysis report, the code of practice, the operation manual, the maintenance manual, etc. As a consequence of an increased neutron flux at 10 MW (~ 1.5×10^{14} $n \cdot cm^{-2} \cdot s^{-1}$) and an extended operation period (5 full power days/week), other applications and services such as silicon doping with phosphorus by neutron irradiation, neutron radiography, and neutron activation analysis will have better performance. It should be emphasized that training for the reactor operations and maintenance personnel, academic research and postgraduate teaching are very important programs in the effective utilization of the reactor. Therefore, in this context, development of a strategic plan for the effective utilization of the research reactor is an essential step. During the upgrade, the following systems will be subject to either change, refurbishment, addition or modification: reactor core configuration, number and type of control rods, chimney and emergency core cooling system (ECCS), beryllium reflector, cooling system (primary and secondary; including new heat exchangers and cooling tower), emergency ventilation system, electrical system, the instrumentation and control (I&C) system, the reactor shielding, etc.

The refurbishment of the I&C system is a major task that needs careful planning taking many aspects into account. It is very important to prove that the biological shield of the reactor has sufficient strength to withstand the increased power. The cooling system capacity will increase to meet the requirements of the planned power upgrade to 10 MW.

One of the new engineered safety features of the upgraded reactor system is an emergency core cooling system (ECCS). This system prevents consequences associated with a possible exposure of the reactor core during a loss of cooling accident (LOCA). During a LOCA, the system will spray water on the top of the reactor core in order to remove the decay heat. Another new engineered safety feature provided for the reactor is an emergency ventilation system. This is to prevent release of gaseous fission products into the environment during abnormal reactor operations or a fuel cladding failure. The system consists of a ventilation path that has an active carbon (charcoal) filter. In normal mode, this ventilation path is bypassed, while during the emergency mode, the air flow in the ventilation system is directed to the emergency ventilation system manually.

Additional vertical irradiation tubes in the core for radioisotope production and neutron activation analysis could be significantly increased. There is also a plan to develop the unused experimental facilities such as the thermal column and radial beam ports to strengthen the R&D activities associated with the reactor. At present, the old and new spent storage pools for the reactor has storage space for 60 and 176 spent fuel elements, respectively. The available pool storage space will not be sufficient for about 25 years of reactor operation at 10 MW for operation cycle of 5 days/week. A new project for spent fuel management/storage should be initiated to investigate the possibility of an alternate dry storage space.

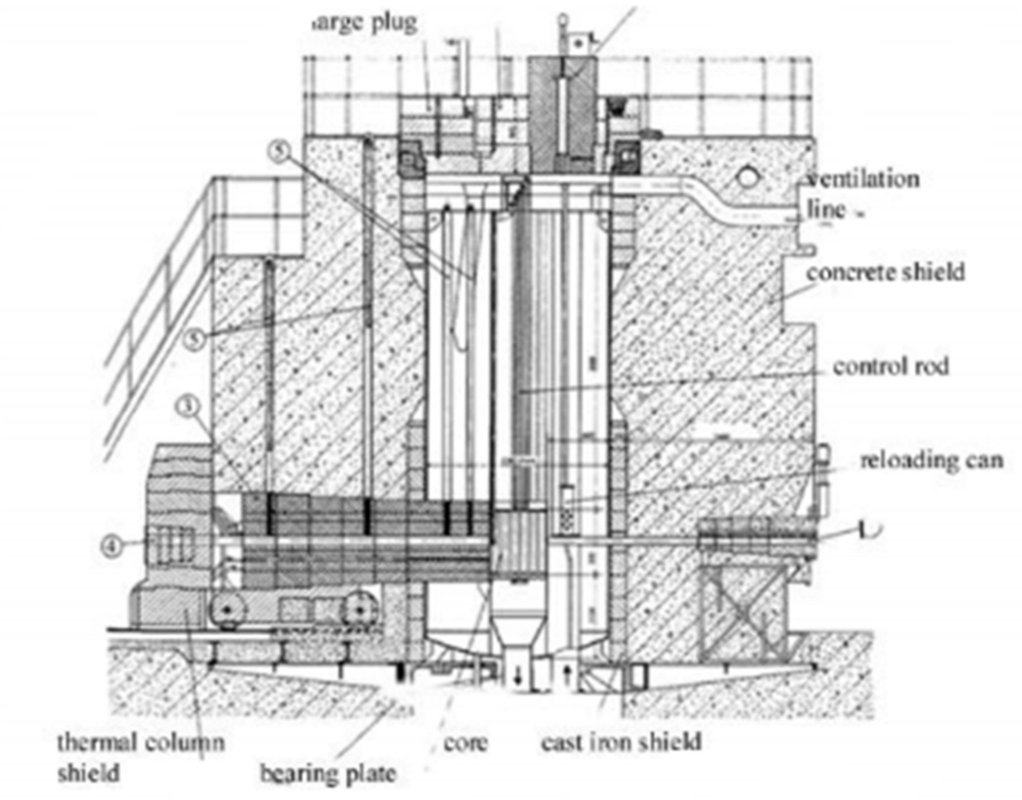


FIG. 1. ET-RR-1 Vertical section.

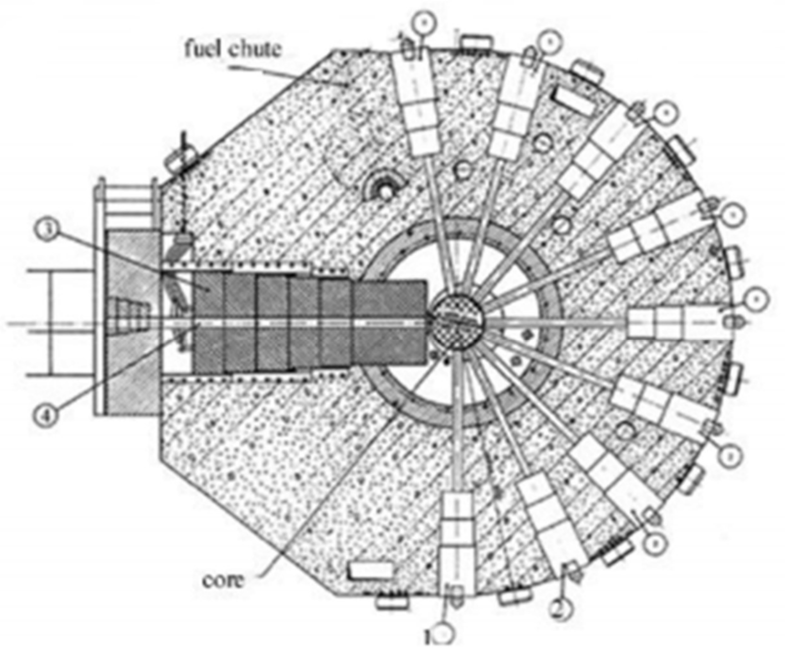


FIG. 2. ET-RR-1 Horizontal section.

2. REACTOR FACILITIES

The ET-RR-1 reactor is better suited than ET-RR-2 for beam research. Also, ET-RR-1 is equipped by vertical channels and hot cells for isotope production which are of growing importance and have a clear long term potential. There are 9 beam horizontal channels and thermal column. In the reflector area, there are nine vertical channels; 8 wet channels and one dry channel. They are used for isotope production and neutron activation analysis. Figure 3 shows the distribution of the vertical channels around the core. In addition, the reactor is equipped with a pneumatic rabbit system for short and intermediate half-life isotopes for activation analysis measurements. Also, the reactor was used for neutron scattering, radiochemistry, shielding investigations and neutron radiography, as well as manpower training. Regarding the human factor, the ageing of personnel was a real problem a few years ago, but a systematic program created had led to the employment of 19 young colleagues in the last few years. This program is expected to continue. Anyway, ET- RR-1 employs about 130 people including support staff in addition to about 60 users in the department of reactor physics as well as about 35 in radioisotopes production department. The reactor is administrated by the Nuclear Research Center (NRC). Table 1 provides the pertinent data for ET- RR-1.

3. CURRENT STATUS OF ET-RR-1

During the early eighties, signs of ageing started surfacing and were reflected in the availability factor of the reactor, due to the increase in the frequency of equipment outages and the considerable effort and time requirement for bringing the equipment back into service after repairs. Therefore, at that point, various modernization and refurbishing works were introduced for improved availability, safety and life extension of the reactor. Table 2 presents the systems that have been updated through the modernization project during the period 1982 to 2011. The ET-RR-1 reactor is currently operated with an analogue instrumentation and control system. Even if the original I&C system completely met the demands that were put on it, the reliability of the I&C system was degraded because of ageing of equipment and electronic components, which are the main reasons for its renovation and modernization. It will be good to replace the old analogue control console of ET-RR-1 with a digital control console, applying the latest available recommendations and standards. Therefore, the I&C system should be almost completely redesigned. Also, the PLC-based protection system should be, hopefully, only reprogrammed.

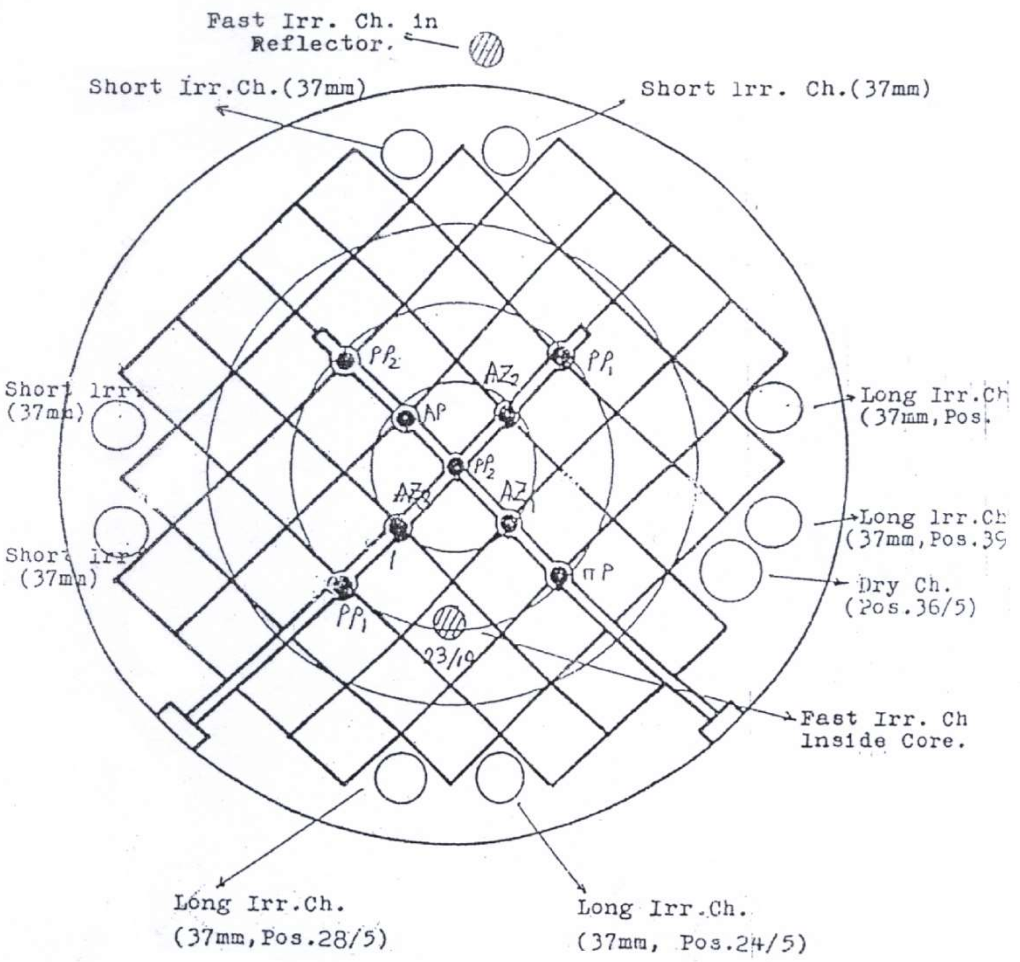


FIG. 3. The distribution of vertical channels around the core.

TABLE 1. THE MAIN ET-RR-1 REACTOR CHARACTERISTICS

Reactor power	2MW
Physical start up:	25 March 1959
First criticality	1961
Fuel assembly:	EK-10 (WWR-S type), 10% enrichment
Number of fuel assemblies (WWR-S type)	51 (max), 38 (min)
Core volume	62 L
Operating loading of U^{235}	4.5 Kg
Control	3 safety rods (B4C); 4 manual rods (B4C); 1 automatic (B4C); 1 fine rod (SS)
Maximal density of heat flow	490 kW/m^2
Water flow rate through primary circuit	850 - 900 m^3/h
Water flow rate through secondary circuit	350 m^3/h
Secondary circuit pressure	6×10^5 Pa
Primary coolant pressure	$2.3 – 2.5 \times 10^5$ Pa
Water flow rate in the core	2.6 m^3/s
Water pressure at the core input	1.35×10^5 Pa
Pressure difference in the core	1.5×10^5 Pa
water temperature at the core outlet	36 ºC
Coolant temperature difference	2 ºC
Maximal temperature of the fuel assemblies	92 ºC
Maximum rate of heat transfer through the surface of fuel elements	3.8×10^5 K. Joul/m^2.h
Maximal density of the thermal neutron flux	– in core; 2×10^{13} n/cm^2 s – near reflector (isotope channels); 1×10^{11} n/cm^2s
Maximum flux at the outer end of the horizontal experimental channels	7×10^9 n/cm^2 s

4. REACTOR INSPECTIONS

Three routine inspections have been performed on ET-RR-1 in 1996, 1998—2000 and 2011. The inspection results have shown that no significant defect indications were detected from the visual and dimensional inspections and there has been no change in the overall reactor vessels integrity (core barrel, central tank and shield tank). The last inspection discovered slight corrosion on the reactor vessels (the most significant pits app. < 0.3 mm depth).

The radiation damage of the vessels did not reach a level which would prevent its further use. Also, it seems to be very probable that radiation damage of concrete and its ageing problems are not really serious. In fact, there are ageing problems and the expected degradation appeared on the I&C, mechanical and electrical systems. The degradation is in accordance with the service life of the reactor. From the last inspection results and the activation analysis of the secondary water, it was found traces of slight concentration of Cesium. Therefore, the existing heat exchangers should be replaced. Although the heat exchangers are made of stainless steel, they remain in permanent contact with the water of the secondary cooling circuit of higher chloride content, which leads to progressive corrosion for the heat exchanger tubes. Anyway, the heat exchangers do not have enough capacity for the expected upgraded power. The upgrading of the reactor can be started in parallel with the replacements, indicated to be necessary on the basis of the inspection results.

TABLE 2. THE UPDATED REACTOR SYSTEMS THROUGH THE MODERNIZATION PROJECT

Installation of a new automated fire alarm system	2011
Installation of new Radiation Protection System (RPS)	2008
AC electrical power supply replacement	2007
Radioactive liquid waste disposal and treatment system	2005
Rehabilitation of Secondary Cooling System	2004
Installation of New Spent Fuel Storage Facility	1998-2000
Installation of Data Acquisition System (DACUS),	1998-2000

Horizontal channels control system refurbishment	1998-2000
Modernization of the fuel handling & transportation mechanism	1998-2000
Replacement of instrumentation and control system (I&C)	1990
Rehabilitation of signaling system	1990
Refurbishment of Computerized Safety Logic System (CSLS)	1990
Replacement of measuring system of operating parameters (flow, temperature, pressure, water level …)	1988-1990
Replacement of Nuclear Instrumentation and Control System	1982-1984

5. RECONSTRUCTION AND UPGRADE SCOPE

The extent of reactor use is basically determined by its power level, which in turn determines the neutron flux. Reactor utilization also depends on the operations schedule. Low power levels and short operational cycles (only few hours of operation each day) are particularly inconvenient, both for high quality research and for the production of useful radioisotopes. On the other hand, high power levels, in conjunction with a prolonged operational cycle (several weeks of continuous operation), result in high fuel consumption and require an expensive maintenance program. Thus, the flux level should be chosen to accommodate a wide range of experiments and reactor uses. In view of changing experimental needs and isotope production at high neutron flux, power upgrading is a reasonable target. The fuel type itself has a large influence on the flux level at a given rated power, but the application of a beryllium reflector and other solutions may largely contribute to the flux level increase. The ET-RR-1 reactor was fueled from the beginning by Russian EK-10 fuel elements (see Fig. 4). Though fuel performance was really excellent, these types of fuel elements are not in production anymore and the reactor should be fueled by another fuel type during the future, continued operation. Therefore, all the components related to reactor core and the active part of the reactor protection system (absorber rods) will be modified. Core loading with MTR plate type fuel (UAl_3 cermets with 19.75 % U^{235} in Al matrix) seem to be the most suitable option. The primary goal of the proposed plan is the coordination of activities between operations, researchers, and users from different organizations.

Discussions began about whether to extend the life of the reactor or begin preparations for final shutdown and decommissioning as an alternative solution. Because the access to the new reactor is difficult, the decommissioning option was really not considered. On the basis of the inspections results, it is concluded that the reactor power can be increased if the proper changes in the mechanical, electrical and I&C systems are carried out. It was the consensus that further reactor operations are needed and the Egyptian Atomic Energy Authority (EAEA) made the decision to prepare a feasibility study on the continued operation of the reactor beyond 2012, and to go ahead with an upgrade and reconstruction of the ET-RR-1 reactor, to take advantage of the reactor's special features, and because many experiments could benefit from higher flux. Also, similar reactors were already operating at 10 MW in other countries. So, a power increase of ET-RR-1 to about 10 MW is physically possible. The fuel stock is nearly exhausted and future reactor operation requires a decision anyhow. The upgrading decision should take into account all feasible and available possibilities, such as fuel questions, core configuration with increased irradiation facilities, technical capabilities including utilization issues, as well as future operation and maintenance questions. Also, the decision should include a real cost–benefit analysis and define the design basis and design requirements including safety issues. Finally, on the basis of the considerations listed below, the reconstruction and upgrade project should drafted including an outline of the project schedule and the required resources, including financial and human demands. The strategic arguments for the necessity for further reactor operations and upgrades are grouped as follows:

(a) The main reason is that the supply of the present fuel elements (EK-10) is not assured for the run and the reactor should be fueled by another fuel type during continued operation.

(b) Ageing is the main driving force for the upgrading project, many components have become obsolete, and increasing difficulty is foreseen in obtaining spare parts to maintain the systems in satisfactory conditions.

(c) The technological progress in I&C systems during the past decades that have led to higher reliability of I&C systems, improvement of man-machine interface, and extensive and fast data collection and processing.

(d) To enhance the safety level and features of the ET-RR-1 reactor by refurbishment, modification, replacement and addition of components and systems to improve efficiency, safety and reliability.

(e) To improve current applications and to develop new ones, where many experiments could benefit from higher flux. There are new industrial and commercial applications that can be developed, such as silicon doping, development of nuclear instrumentation, tests and certification for industry by neutron and gamma radiography.

(f) Research activities in the field of condensed matter, materials science, activation analysis, radiochemistry, nuclear gamma spectroscopy, reactor safety, health physics, etc. would be highly desirable to continue and/or extend or, in some cases, start.

(g) To provide in-core irradiation facilities capable of producing higher quantities of high specific activity radioisotopes for medical and industrial applications, to alleviate all of the national demand for these isotopes and to minimize importation costs. In addition, the radioisotopes used for medical diagnostic purposes are always of short half-lives to avoid unnecessary irradiation of patients. The import of short half-life isotopes is complicated, sometimes impossible. In this field, the ET-RR-1 reactor can serve as a backup to the ET-RR-2 reactor.

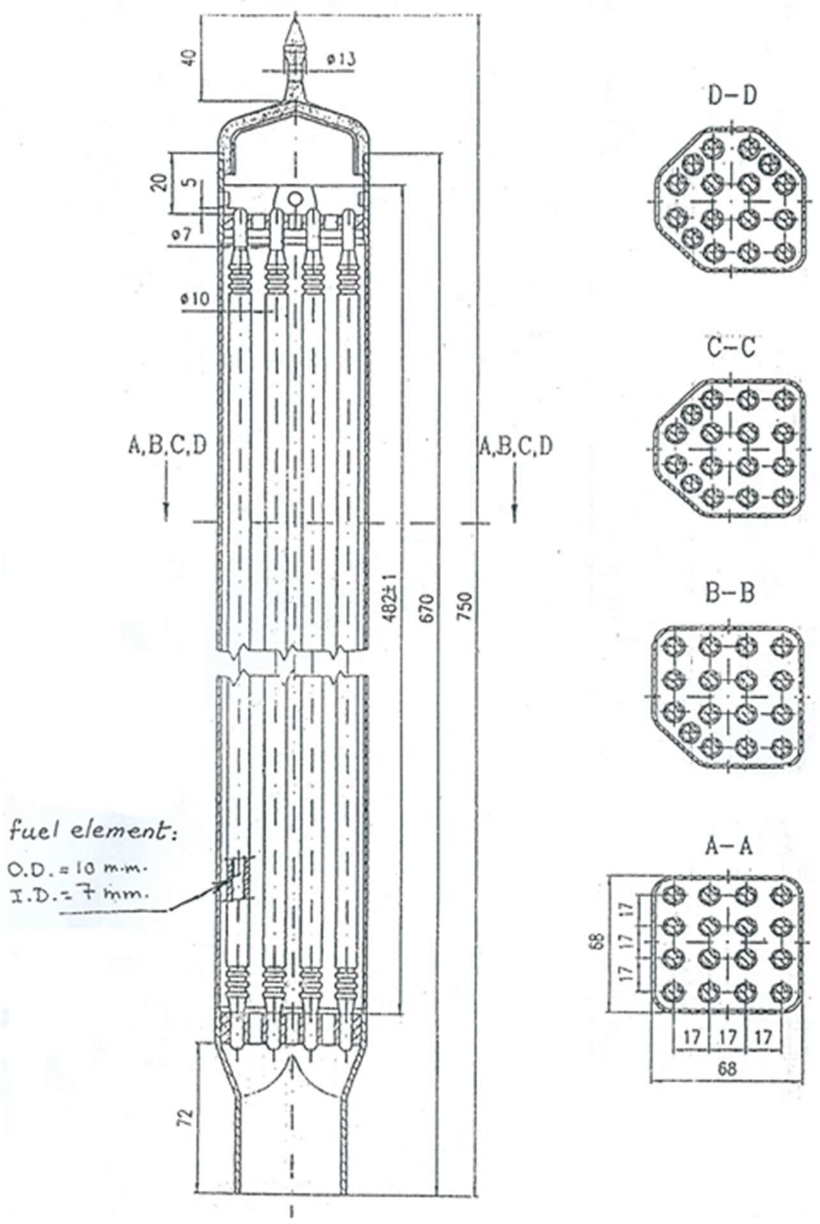


FIG. 4. EK-10 fuel assembly drawing.

(h) Serve as an efficient tool in training nuclear engineers/operators to obtain licensing for the country deciding to build Nuclear Power Plants (NPPs), and to supply the Nuclear Power Plant Authority (NPPA) with necessary personnel with nuclear qualifications.

(i) Contribution to postgraduate (nuclear engineering/physics) education and hosting international training courses (e.g. at the request and with the participation of the IAEA). Also, serve as a regional center for AFRA, Mediterranean Network and the Arab Atomic Energy Organization. We emphasize that the training possibilities have to be explored more extensively than were done before.

6. PLAN FOR UPGRADE OF ET-RR-1 REACTOR

In addition to the above circumstances, and by comparing the refurbishment costs to the construction and commissioning of a new facility that has precisely the same capabilities or to the facility decommissioning, we can conclude that the continued operation of the reactor, if it is safe and technically feasible, seems to be an attractive option. The study compares the following three options:

(a) Component replacement/ Reconstruction of the reactor with upgraded power/flux level and continued operation by 2035;

(b) Component replacement/ Reconstruction of the reactor at the present power/flux level and continued operation by 2035;

(c) Permanent shutdown and subsequent decommission of the reactor.

Obviously, the costs of permanent shutdown and the removal of system and components to be decommissioned arise in any option. Reconstruction of the reactor for continued operation has a considerable cost. The lists of systems and components to be replaced differ from each other only *slightly* if the reactor power is left unchanged or upgraded. So, the third option seems to be out of the question. The second option does not seem very attractive as well. The main reason is that the supply of the present fuel elements (EK-10) is not assured for the long run. Other reasons, e.g. that the need of the applications for high neutron flux cannot be satisfied by the present construction, might play a significant role as well. The first option, i.e. to upgrade the reactor and to reach a power of 10 MW, seems to be attractive compared against the cost of facility decommissioning or operation at the nominal power.

Let us confront the costs of the program of part replacement/refurbishment with and without power increase. The most expensive part of the program is the instrumentation replacement, independent of the magnitude of power. Costs of coolant capacity addition and solving the dosimetry problem increase with power but their contribution to the total costs are small. A small increase in costs produces a great increase in benefits. On the basis of the above consideration, the study recommends a way of executing all the tasks that are needed to reach the aimed situation, i.e. the operation of reconstruction + power/flux upgrade + continued operation. The power upgrade and the necessary modifications of the ET-RR-1 reactor can be performed in several (eventually overlapping) steps, but the entire project should have a master plan. This statement follows from the fact that certain elements of the modifications can be designed in a straightforward way only for the entire reactor. The following elements belong to this category:

(a) Electric system;

(b) I&C.

These systems should be designed and manufactured for the entire reactor in a uniform manner. Their connections to the existing, modified and new systems should be carefully designed in advance, before the separate modifications and new systems are designed. At the same time certain modifications can be designed and modified separately. The following modifications belong to this category:

(a) Core, reflector, control rods, vertical irradiation channel replacement;

(b) Cessel, internals of the reactor block, horizontal channels and thermal column;

(c) Primary circuit pumps, heat exchangers, bypass filter, isolation valves;

(d) Secondary circuit, cooling tower;

(e) Dosimetry;

(f) Ventilation, air conditioning and exhaust system;

(g) Building crane, auxiliary systems, water purification system, physical protection system;

(h) Fire-detection and fire-Fighting equipment with installation of smoke detectors, sprinklers and new fire hydrants.

Protection system signals should be reconsidered. The functionality of the protection system will be probably only slightly modified, but redundancy and diversity requirements will lead to the completely new design; while together with protection system signals, other signals should be also be considered which are displayed in the control room and archived in the plant computer. The DACQUS data acquisition system probably can be used further on, after certain modifications. The PLC logics should be definitely reprogrammed; even if the system itself will be probably used also in the future. The functionality of the protection system is a basic safety issue and the design should be prepared. Also, some minor modifications mentioned in connection with the inspections, safety or power upgrade should be carried out. Laboratories can be also established or modified almost independently of each other, but their connections to the reactor should be considered. It is important to pay attention to the connections of pumps and heat exchangers to the electric and I&C systems. Installation of an additional (makeup) water purification unit in order to increase the output of the initially available system should be considered.

If one wants to continue the operation of a research reactor designed in the fifties, the fulfillment of up-to-date safety principles should be considered and taken into account in designing the reconstruction of the reactor. The redundancy, diversity and fail-safe design should be analyzed for each safety system. The eventual shortcomings shall lead to design changes. The original design does not contain any particular protection against severe accidents, i.e. core melting, since it was not required before the eighties. The upgrading project should take the following design items into consideration:

(a) Main reactor components:

- Core (fuel type, core size, attainable burnup, refueling strategy, introduction of a core drop pressure meter, a neutron flux mapping facility using self-powered neutron detectors);
- Startup neutron channels, safety neutron channels, log. Current channels, control channels;
- Control rod system (control rod type(s), main reactivity values, and control rod position, control rod drives);
- Reflector layout;
- Vertical irradiation channels;

— Connections to mechanical systems (support plates, control rod drives);

— Connection to the I&C system.

(b) Primary circuit, reactor block:

— Flow rate, main thermo-hydraulic parameters;

— Vessel modifications;

— Modifications of the thermal column and the horizontal channels;

— Modifications of the ventilation system;

— Spray system;

— Leak-tight covering of the shaft;

— Leak-tight man-hole in the wall between the shaft and he pump room;

— Automatic closing device on the air ventilation pipe in the shaft walls;

— Valves on all tubes crossing the shaft walls;

— Activation of the re-circulation tank of 6 m3 at the bottom of the shaft;

— Recirculation pumps in the shaft.

(c) Pumps and heat exchangers:

— Pump and the heat exchanger capacity, main parameters;

— Connections to electric and I&C systems;

— Pump replacement design;

— Heat exchanger replacement design;

— Replacement of the bypass filter system;

— Modifications of the primary circuit pipelines in the pump room;

— Leak-tight painting of the pump-room wall surfaces;

— Remote closing possibility of the pump-room sunk;

— Recirculation pumps in the pump room.

(d) Secondary circuit and cooling tower:

— Capacity, main parameters;

— Connections to electric and I&C systems;

— Design of the new secondary system;

— Design of new cooling tower;

— Installation of a chemical injection system.

(e) Ventilation system:

— Main parameters of modifications;

— Modifications of ventilation system.

(f) Civil engineering:

— Main parameters of replacements, modifications and new installations;

— Modifications in the building, physical protection;

— Crane, other equipment in the reactor hall;

— Auxiliary systems;

— Water purifications.

(g) Electric system:

— Up-to-date design requirements (fire resistance, shock-proof protection);

— Concept of electric supply safety levels;

— Capacity requirements;

— Upgrading of the electrical distribution system;

— Modernization of emergency AC and DC power supply system.

(h) I&C system:

— Protection system signals;

— Other signals, displaying in the control room, archivation;

— Safety system actuation signals;

— Modifications of the PLC logics;

— Substitution of reactor control console.

(i) Human factors:

— Operational procedures to be prepared or modified;

— Documents to be prepared;

— Education and training.

(j) Laboratories:

— Activation analysis and the rabbit systems;

— Silicon doping possibilities, irradiation channels;

— Isotope production channels;

— Beam ports, laboratories;

— Hot cells (manipulators and their accessories) rehabilitation;

(k) Spent fuel storage pools - the spent fuel storage facilities have to accommodate for the storage of the new fuel elements.

7. TECHNICAL AND SAFETY FEATURES OF THE RECONSTRUCTED REACTOR

Additional measurements should be made as a consequence to cope with the development of safety principles, these measures can be recommended as follows:

(a) *Reactor core.* In the core modification plan, the top and bottom grid plates will be replaced in order to accommodate the new MTR plate type core configuration. At that point, it will be needed to fabricate and install a new core structure with a beryllium reflector. The core with LEU fuel elements will be designed in order to increase the power, but to further increase the flux, the power produced by a single element will be increased as well. This will require more intensive cooling of the assemblies and will be ensured by the adequate design of the primary and secondary cooling systems (pipes, pumps, heat exchangers, etc.). The primary and secondary cooling systems are shown in Fig. 5 and Fig. 6, respectively.

(b) The increased number of irradiation places, where the neutron flux is relatively high, resulted in a rather complicated core. To ensure a suitably long refueling cycle, the number of control rods has to be increased as well to guarantee a safe shutdown and to increase the ability to control the core excess reactivity. Figure 7 shows the control rods distribution in the reactor core.

(c) The main circulating pumps should be replaced anyhow. It seems that three main circulating pumps should be enough, two of them are in operation at nominal power and the third one is the reserve. Also, the valves built in the primary loop should be replaced. Water conductivity and ph meters can be added in the primary loop circuit.

(d) The previous open secondary circuit should be replaced by a new, closed system. A new plate-type heat exchanger can be installed to replace the old shell and tube-type heat exchanger. The new heat exchanger required several changes in the piping layouts of both the primary and the secondary cooling loops. A microprocessor-based chemical controller can be installed for the secondary cooling loop to maintain the secondary water chemistry parameters (conductivity, total alkalinity, chlorides, total hardness, silica, phosphonate) within permissible limits.

(e) One of new engineered safety features of the upgraded reactor system is an emergency core cooling system (ECCS). This system plays a key role in protecting the reactor fuel in the event of a loss of coolant accident (LOCA). So, it is recommended (due to safety considerations) to install two emergency circulating pumps with limited capacity, which can be operated from the emergency electric supply (diesel generators). In order to cover the short period between the loss of power and the actuation of the emergency circulating pumps, a so-called gravity tank should be installed, and connected to the reactor tank. Supplying the emergency circulating pumps from the battery station can solve the problem of the time gap between the blackout and diesel generators start-up. The five existing pump positions can be used with slight modifications of the primary circuit pipelines in the vicinity of the pumps.

(f) Installation of a continuous vibration monitoring system for rotating machinery; the rotating machinery is primarily the water circulating pumps. As part of the reactor upgrade plan, a continuous vibration monitoring system should be installed. This will provide accelerometer data to a central processing unit that will monitor the changes in the vibration levels of the pump-motor system. Defects such as imbalance, misalignment, looseness, and bearing faults can be detected before a catastrophic failure occurs.

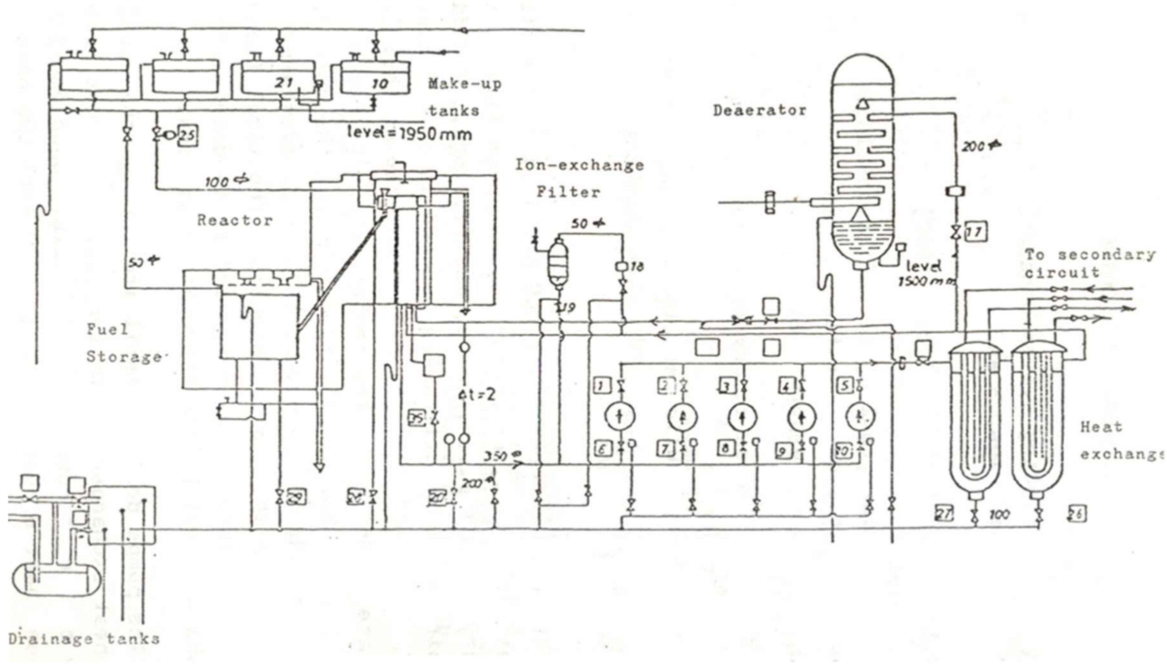


FIG. 5. The primary cooling circuit of ET-RR-1.

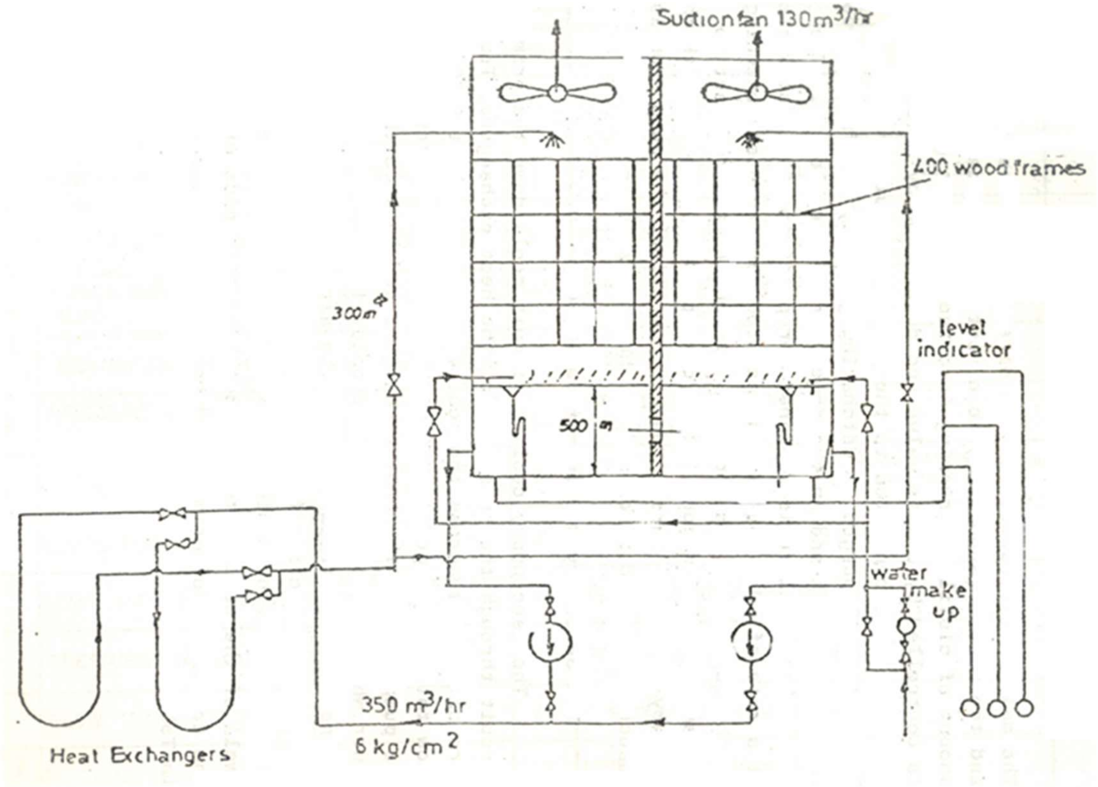


FIG. 6. The secondary cooling circuit of ET-RR-1.

(g) The electric supply system should be partially replaced; this follows from the obvious results of inspection due to ageing, and as well from the significant changes of design requirements (consequent application of the single failure principle, fire resistance standards, and shock-proof protection standards). The supply needs should be carefully designed and DC and AC capacities should be determined on a solid basis. Electric system capacity needs will increase with power upgrading.

(h) The reactor is supplied by electricity from two independent lines. Two diesel generators should be installed (one of them is in standby mode) and the capacity of batteries should be increased and inverters ensure the AC supply in case of emergency should be added. The new electric system should be designed in one stage for the entire reactor.

(i) Radiological safety: Shielding, liquid wastes, gaseous release evaluation for the new operating conditions, implementation of a continuous gaseous release monitoring system, modification of the pneumatic irradiation facility, relocation of area monitors, etc.

(j) Modification of the biological shield arrangements around the reactor and measurements should be made as a consequence of reactor development.

(k) Revision and fitting of the instrumentation and control system for the new operating conditions. The safety logic should be up-to-date and highly reliable. The fail-safe principle should be realized in the actuation of the safety rods.

(l) The emergency ventilation system should be modified because of two reasons. Firstly, the inspection pointed out some shortcomings, secondly safety considerations also involve the ventilation system. This is to prevent release of gaseous fission products into the environment during abnormal reactor operations or a fuel cladding failure. Filters should be added to mitigate the consequences of accidents that may lead to radioactive releases.

(m) Sealing of the reactor hall should be improved to minimize the leakages from the reactor building penetrations. Necessary building repairs should be carried out to keep the leak rate within limits. For this purpose, all airlock door seals should be replaced and air supply and exhaust damper seals should be improved.

(n) Installation of a new failed fuel detection system based on gamma radiation monitoring is necessary.

(o) Modernization of physical protection system is essential.

(p) Special attention should be devoted to water chemistry. Filters system should be designed in connection with the reconstruction of the reactor to ensure that water quality remains good enough to minimize corrosion problems.

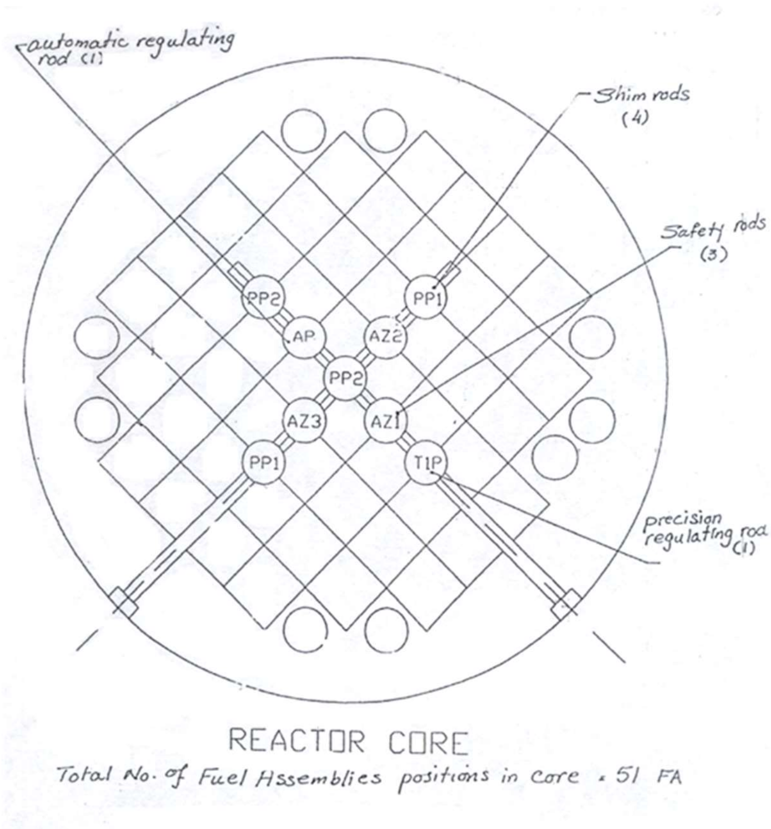


FIG. 7. The core configuration including the distribution of control rods.

8. LICENSING-RELATED ANALYSES AND OBLIGATORY DOCUMENTATIONS

The project should be well-documented and the certificates and records for demonstrating compliance with the requirements should be settled and retained. Prior to the upgrading execution, SAR for licensing the shutdown and reconstruction should be elaborated according to the status of the reconstruction project. The status of the following documents and other items is considered:

(a) Safety analysis report;

(b) Technical specifications;

(c) Operational & maintenance procedures;

(d) Documentation of operational events and maintenance findings;

(e) Investigation of causes of operational events;

(f) Retraining, guidance and education of personnel in operation and maintenance: New systems may introduce the need for new training and skills in both the operations and the maintenance staff;

(g) Safety culture.

The licensing procedure was strongly based on the guidelines and recommendations published in IAEA Safety Series No. 35, for example:

(a) Code on the Safety of Nuclear Research Reactors: Design (Safety Series No. 35-S1);

(b) Code on the Safety of Nuclear Research Reactors: Operation (Safety Series No. 35-S2);

(c) Safety Assessment of Research Reactors and Preparation of the Safety Analysis Report Safety Guide (Safety Series No. 35-G1);

(d) Safety in the Utilization and Modification of Research Reactors Safety Guide (Safety Series No. 35-G2).

9. REACTOR UTILIZATION

Better utilization of ET-RR-1 can be achieved by collaboration with countries that have no research reactors and with other research reactor institutes. The modes of collaboration are to maximize the use of ET-RR-1 for regional benefit and improve the reactor products and services and exchange experience. In the framework of the reactor utilization program, the hot cells rehabilitation should be done. ET-RR-1 is used for various purposes, this includes irradiation and neutron research, the latter being the main utilization (to serve as a neutron source). Irradiations are performed in nine vertical channels (and should be increased). The reactor is equipped with a pneumatic rabbit system that serves for neutron activation analysis. In contrast, experiments are carried out at the horizontal neutron beam ports. A highly radioactive sample handling facility should be installed. The utilization of ET-RR-1 reactor for basic and applied research can be considered by the following means:

(a) Elastic and inelastic neutron scattering.

This is the most important field of neutron research. The devices already installed (two-axis neutron spectrometer, etc.) can be more extensively utilized when the reactor is upgraded. The only missing tool is a device for small angle neutron scattering. It is highly recommended to install a small angle scattering spectrometer device, as it is very flexible, consequently it can be used for other purposes (studies of polymer and copolymer structures, magnetic fluids, frozen solutions of ferrous salts, liquid structures, membranes, inorganic gels, amorphous systems etc.). besides the research needs, the small angle neutron scattering has a lot of applications such as, detection of distribution and shape of bubbles in different technological material, investigation of helium and other absorbed gases in mechanically exposed material, etc.

Society requires more and more complex and sophisticated materials that are lighter, stronger and smaller and that can help provide solutions to major sociological and technological problems of the 21st century, including energy, healthcare and the environment. This demand for increasingly complex materials with specialized properties and functions depends on a variety of techniques to unravel and optimize their properties. Neutron scattering has and will continue to play a vital role in the portfolio of analysis techniques delivering inputs into areas as varied as: energy, nanotechnology, materials processing, drug design, biotechnology, 'green' technology and information technology. A key driver for future development is the need to observe processes and reactions in real time and link these observations with increasingly sophisticated computer simulations'. The upgrading of the ET-RR-1 reactor to be in the medium range of thermal neutron flux ($> 10^{14} n/cm^2.s$) with enhanced experimental instrumentation and support facilities will allow the entrance to a new range of structural and dynamical studies of matter, especially related to engineering and biological systems. This will be achieved through the following:

(a) Upgrading and improving the existing facilities:

   i. Computerized tomography by neutrons and gamma rays;

   ii. The Cairo Fourier Diffractometer Facility (CFDF);

   iii. Neutron – Gamma Transmission Technique.

(b) Introduce irradiation facilities.

(c) Installation of three modern neutron scattering techniques as:

   i. High-resolution powder diffractometer;

A high-resolution powder diffractometer that can accurately resolve complex atomic and magnetic structures of powders and is used, amongst other things, for research into batteries and creating better building products.

   ii. Small-angle neutron scattering instrument;

The small-angle neutron scattering instrument is a powerful technique for investigating the structure of materials on the nanoscale. Also used for studying materials such as polymers, superconductors, porous materials, geological samples, alloys, ceramics and biological molecules such as proteins and membranes.

   iii. Triple-axis spectrometer;

The thermal triple-axis spectrometer used to measure neutron inelastic scattering, which is a key technique for the measurement of excitations in materials. These measurements provide information on the forces between atoms, or interactions between magnetic moments.

(d) Reactor as a complex irradiation source;

Neutrons, together with alpha, beta and gamma rays can be used for materials testing, for hot atom chemistry, to study irradiation damages and to perform biological irradiations, dosimetric, nuclear safety etc. investigations as well. This field provides with a great variety of investigations, using neutrons, that is not yet explored at ET-RR-1. The greatest emphasis here could be on biological investigations, as biology is considered to be the science of the future. According to modern trends the influence of low doses on life can be investigated on the level of the cell. The fields mentioned above are important; they have been more or less carried out at ET-RR-1. After finishing the reactor power upgrading, activities can be extended into all the fields.

(e) Radioisotope production;

The production of radioactive isotopes can be considered, as one of the main applications of the reactor. The radiopharmacological industry needs, even today, a lot of radioisotopes, but the isotope production can rather extensively grow in the future, as the merits of industry are not fully explored yet. The main product today is ^{131}I. The current neutron flux of the reactor does not allow producing more than 500 mCi in one batch. After upgrading the reactor this activity can be easily increased, as the produced activity is proportional to the neutron flux. The iodine production units are suitable for the production of higher activation, so this extension does not involve any additional investment needs.

Besides ^{131}I, other iodine isotopes, mainly ^{125}I and isotopes of phosphor and sulphur, are produced as well. The production of these isotopes can be increased in the upgraded reactor. Also, the reactor can produce special radioisotopes such as ^{41}Ar and ^{82}Br for industrial processes inspections, ^{192}Ir and ^{198}Au radiation sources for use in brachioscopy therapy, ^{153}Sm for pain palliation in bone metastases, calibrated gamma sources of ^{133}Ba, ^{137}Cs, ^{57}Co, ^{60}Co, ^{241}Am, and ^{152}Eu used in clinics and hospitals practicing nuclear medicine and research laboratories. The production of ^{99}Tc can be developed.

(f) Neutron radiography;

Neutron radiography devices were already installed at ET-RR-1, but it was not practiced well. The buildup of a radiography channel can be highly recommended, as this general tool can meet a lot of industrial needs. Collimate neutron beam is used to investigate objects in closed volumes. In dynamic radiography moving objects or processes can be recorded. Static radiography provides better resolution. A few examples on the use of radiography: turbine blades, pipelines, compressors of refrigerators, heat exchangers, valves. One beam for neutron radiography will be useful, but the use of a second beam (to divide dynamic and static investigations) can be considered as well.

(g) Activation analyses;

Activation by reactor neutrons is a very sensitive analytical method. About 70 various chemical elements can be detected in an extremely wide range of content, i.e. from 10^{-8} – 10^{-10} g/g concentrations. Applications of neutron activation analysis might be important in the pharmaceutical industry, in geology, biology, in archaeology and in police investigations (traces) as well. The special situation of Egypt emphasizes the application in archaeology. The construction of a neutron activation analysis basis, including a radiochemical laboratory was recommended.

— Neutron diffraction related to analyze molecular and crystalline structures;

— Radio-chemistry and radiation chemistry including various activation analyses;

— Silicon doping by neutron irradiation.

ET-RR-1 should be designed to cater to growing world demand for silicon irradiation, and this helps offset the operational costs of the reactor. Silicon irradiation, or Neutron Transmutation Doping (NTD), changes the properties of silicon, making it highly conductive of electricity. Large, single crystals of silicon shaped into ingots are irradiated inside the reactor reflector vessel. Here the neutrons change one atom of silicon in every billion, to phosphorus. The irradiated silicon is sliced into chips and used for a wide variety of advanced computer applications. NTD increases the efficiency of the silicon in conducting electricity, an essential characteristic for the electronics industry. Irradiated silicon is essential for certain components, such as high power discrete devices, transistors and memory chips used in sophisticated computers, video cameras, and air conditioning units.

(h) Education and training;

ET-RR-1 can fulfill the following aims in the field of education:

— Providing university and postgraduate programs with an experimental facility and education opportunities;

— Training for specialists in nuclear industry, shielding radiography, etc.;

— Participation in research projects and international training courses (e.g. involving IAEA). Also, an agreement can be made between IAEA and EAEA, under which the occupation of the reactor and its facilities can be shared by experimenters who are from Arab countries, Africa and the Mediterranean network.

The main engineering tasks that will be performed during the upgrading project:

It will be very important to do all the theoretical calculations which prove the design of the reactor systems has sufficient strength to withstand the increased power, namely:

— Neutronics: fuel element definition, critical core configuration, fuel assembly technical specifications, peak factor, reactivity feedback coefficients, kinetics parameters, startup and transition core Configurations, etc.;

— Fuel management: maintain the maximum length of operating cycle and keeping fuel consumption to minimum, alternative fuel cycles and different discharge fuel burnup will be studied. Operating cycle length of 5 days followed by 2 days regular reactor shutdown is an attractive option. This shutdown period is used for installation and reloading of the irradiation channels, maintenance and for refueling. The operation cycle gives theoretical attainable operating coefficient of ~ 70%;

— Thermal-hydraulics: maximum flow rate admissible in the primary circuit, flow rate determination in the different core channels (hydraulic experiment), convection coefficients determination (thermal experiment), hot channel characterization, technical specifications for the heat exchanger, pumps and cooling towers, etc.;

— Shielding: modification of the biological shield arrangements around the reactor; it was very important that the calculations should prove that the biological shield of the reactor has sufficient strength to withstand the increased power;

— Nuclear safety: selection of initiating events, evaluation of individual event sequences, probabilistic safety assessment (PSA) Levels 1, 2 and 3, comparison between PSA results and the Egyptian Regulatory Authority acceptance criteria, etc.;

— Mechanics: primary and secondary circuits layout, core pressure drop monitoring system, etc.;

— Electricity: revision and fitting of the electrical system for the new operating conditions, etc.;

— Licensing: safety studies related to the project should be performed in order to obtain a license for the entire facility, and to generate updated regulatory documents; including the safety analysis report, the code of practice, the operation manual, the maintenance manual, etc.;

10. CONCLUSIONS

A general consensus was reached that for practical technical purposes there is a need for an extension of the reactor operation. From the point of view of users the main demand is a higher flux, mainly for R&D and radioisotopes production. Researchers require about ten times higher neutron flux than that of ET-RR-1. As a result of the assessment of the inspection results, it is concluded that an extensive refurbishment of the reactor facility, including auxiliary technical systems and the reactor building as well as I&C equipment, is needed. Actually, during the upgrade, almost all reactor systems were refurbished, modified or changed. With these modifications which will be introduced in the reactor, a new safety analysis report should be prepared and submitted to the regulatory body for the 10 MW license applications. By comparing the refurbishment costs to the commissioning and construction of a new facility has precisely the same capabilities or to the facility decommissioning, we can conclude that the continued operation of the reactor, if it is safe and technically feasible, seems to be an attractive option.

Power upgrading is not possible using the present type of fuel elements, and they are also not available anymore. A new fuel type should be selected to be used after the reconstruction and upgrading. The proposed core configuration is focused on installing in-core irradiation facilities as well as for maximizing the performance of the external beam tubes facilities.

In the future, continuous efforts should be made to maintain the reactor utilization index as high as possible. The production of radioisotopes for medical and industrial application is essential, as it provides immediate and visible social benefits, but reactor utilization in academic and applied research, manpower training and education are equally important and cannot be ignored. We emphasize that the training possibilities have to be explored more extensively than were done before.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Research Reactor Modernization and Refurbishment, IAEA-TECDOC-1625, IAEA, Vienna (2009).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Research Reactor Renewal and Upgrading Programme, IAEA-TECDOC-214, IAEA, Vienna (1978).

[3] Proceeding of International Meeting on Reduced Enrichment for research and test reactors, Cape Town, Republic of South Africa, Oct. 29- Nov. 2, 2006.

ET-RR-1 Safety Analysis Report, Atomic Energy Authority, Egypt (2002).

MODERNIZATION OF DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS OF GHANA RESEARCH REACTOR-1

B. EMI-REYNOLDS, E. O. AMPONSAH-ABU, A.G. AMPONG, H. OBENG, P. D. GASU, J. K. GBADAGO
Ghana Research Reactor-1 Centre, Nuclear Reactors Research Institute,
National Nuclear Research Institute, Ghana Atomic Energy Commission,
Ghana

Abstract

Ghana Research Reactor-1 (GHARR-1) is a 30 kW tank-in-pool type reactor, which is cooled and moderated by light water and reflected by metallic beryllium blocks. It uses 90.2% enriched uranium aluminium alloy as fuel. Control of the reactor is by means of a centrally located cadmium rod cladded with stainless steel. The control of the nuclear reactor is carried out using two systems, the Control Console and the Microcomputer Closed-loop Control System (MCCS). These systems enable the control and monitoring of important parameters such as temperature and water levels to ensure the safe operation of the reactor. A new MCCS has been installed and been in operation since March 2008, through IAEA Project GHA-4-012-001N. Some modifications in the new MCCS system include the change to Microsoft Windows XP/2000 Operating System environment from DOS environment, improvement on the reliability of the electronic circuitry and the addition of other relevant monitoring parameters like reactor and pool water conductivity. The fission chamber now has an in-built power supply unit. The control rod drive mechanism and the control rod have been recently replaced. Other modifications include the creation of a large sample irradiation site and addition of beryllium shim plates. These modifications made it necessary for a recalibration of the control systems.

1. INTRODUCTION

GHARR-1 is cooled by natural convection and can be operated at a maximum thermal neutron flux of 1×10^{12} n/cm^2.s. The reactor complex contains 5 major components i.e. the reactor assembly, control console, auxiliary systems, irradiation system and the pool.

The reactor assembly consists of the reactor core, beryllium (Be) reflector, small fission chamber for detecting neutron fluxe, 1 central cadmium (Cd) control rod and its drive mechanism, and thermocouples for measuring inlet and outlet temperatures of the coolant. The main specifications of GHARR-1 are as follows:

TABLE 1: MAIN SPECIFICATIONS OF GHARR-1

Type	Tank-in-pool
Nominal core power	30 kW (th)
Coolant/Moderator	Deionized light water
Loading of U-235 in core	998.12g
Reflector	Metallic Be alloy
Excess reactivity – cold, clean	4 mk
Daily operation fluence in inner irradiation sites	$< 9 \times 10^{15}$ n/cm^2
Fuel life in core	$> 9 \times 10^{19}$ n/cm^2 .s
Neutron flux at inner irradiation sites	3×10^{12} n/cm^2, stability ± 1%, horizontal, vertical variation < 3%
Number of irradiation sites	5 inner sites at 1×10^{12} n/cm^2.s (max), 5 outer sites at 5×10^{11} n/cm^2.s (max)
Control rod	1, stainless steel clad, Cd absorber
Reactor operation	Manual and automatic
Temperature in irradiation sites	Inner sites < 50 °C; outer sites < 45 °C – at pool temperature of 20°C
Core reactivity temperature coefficient	-0.1 mk/°C for core temp. of 15-40°C
Average radiation dose in reactor hall	< 0.001 mSv/h

The reactor is designed to have self-limiting power excursion characteristics with a control rod at the centre of the reactor core. The single cadmium rod is used for regulating the power level, compensating for fuel consumption, as well as reactor startup and shutdown. The control console consists of the reactor control system, the radiation monitoring system readouts, monitoring panel of auxiliary systems and the power supply system of the console.

A Microcomputer Closed-Loop Control System (MCCS) has been developed for the reactor with a compatible computer. The system, in addition to controlling the reactor, also acts as a data acquisition and reactivity monitoring system. There are monitoring systems for water temperature and dose-rate levels, radiation detection and measurements of dose-rates at the top of the reactor vessel, the working area of the reactor hall and the reactor water deionizer column. There are other auxiliary systems for the utilization of the reactor such as the pneumatic transfer systems. A multi-channel analyzer computer system is available for neutron activation analysis.

The Microcomputer closed-loop control system is constituted of a computer connected through a control interface board and a switch board to the Control Console. An analog-digital (AD)-

digital-analog (DA) converting board is inserted in the computer as a channel for the computer to communicate with the outside. The reactor is controlled by the control signal sent by the computer through the DA converter of this board.

FIG. 1. The control console.

The neutron flux of the reactor is detected by a miniature fission ionization chamber which is powered by a 135 v battery in the interface cabinet. The ionization current of neutrons is sent to an automatic micro-current amplifier. The ionization current is converted by the amplifier in voltages V_1 and V_2 suitable for the interface board. The position indicating signal of the control rod in the reactor core is given by a multi-turn potentiometer geared with the control rod drive motor. This signal is sent to the AD interface board through the interface cabinet. The following temperature signals of the reactor inlet, outlet and the pool water temperatures are measured by NiCr-NiAl thermocouples, whose cold ends are compensated by the copper constant bridge. These signals, having been amplified 1000 times in the interface cabinet, are sent to the AD interface board. All the parameters of the reactor are therefore channelled through the interface cabinet to the computer interface board.

FIG. 2. The MCCS unit.

2. CABLE CONNECTIONS

The micro-computer closed-loop system is powered through an earth leakage circuit breaker, a stabilizer and an Uninterrupted Power Supply (UPS) unit. There is a switch board in the control console which serves as a junction box to receive the temperature, conductivity, gamma dose on top of the reactor and the signal from the control drive mechanism for the movement of the control rod. There are two switch knobs used to either select the Control Console or the MCCS for the control of the reactor designated by white and black respectively. A 19 –core cable is used to convey all the signals in the reactor to the various control equipment used at the facility.

3. PARAMETER SENSORS

The MCCS has temperature signal amplifiers for reactor water inlet and outlet and pool water for detecting temperature signals. The sensors, which are NiCr-NiAl armoured thermocouples are installed at the inlet and outlet of the reactor core coolant and the reactor pool coolant. These thermocouples have an accuracy of ± 1.5%.

The Fission Chamber provides input signals to the control system and is used for the determination of thermal neutron fluxes in the inner irradiation sites at varying positions in the reactor.

The conductivities of the reactor and pool water are measured by a purification measuring system. This system provides information to the water purification control and to the input of the computerized desk and the output scope of the computerized control system.

4. CONTROL SOFTWARE (TYPE II)

A computer software application was developed by the manufacturer to ensure the precision in control, response time, stability and safety of the control system.

The software collects and displays in real time various operating parameters of the reactor including neutron flux, control rod position, temperatures of the reactor inlet, outlet and pool water, electrical conductivity of the reactor water and pool water.

It also compares collected data with the set value to determine whether or not regulation is needed as well as how much adjustment needs to be made to stabilize the system. The control software detects any non-conformity of the control rod's movement and the control signals being transmitted. A failure warning is sounded when this is detected.

The Type II software also compares various operation parameters with their limit values and when these limits are exceeded, corresponding warning signals are given. The software records the parameter changes during the operation of the reactor. These parameters include the temperatures of both inlet and outlet temperatures of reactor water, that of the pool water, the control rod position, reactor and pool water conductivities and the neutron flux. The data recorded is stored on the computer for retrieval later and can be printed out.

5. MCCS INSTALLATION PROBLEMS

Despite a general improvement in the overall reliability of the control systems, a few problems still persist. The sensor for the gamma detection at the top of the reactor could not be interfaced with the new MCCS. The IC that provides the interface for gamma monitoring appears electrically overloaded, it easily gets overheated and burns out often. The gamma signal to the MCCS is therefore disabled to prevent the continual replacement of the IC. The Type II application, although having a display for reactivity on the user interface is unable to interpret the measurements of the reactor's reactivity at any given time. To compensate for these deficiencies, the gamma ray dosimeter (which is fixed into the control console) is used for manually recording the gamma dosage at the top of the reactor during operation.

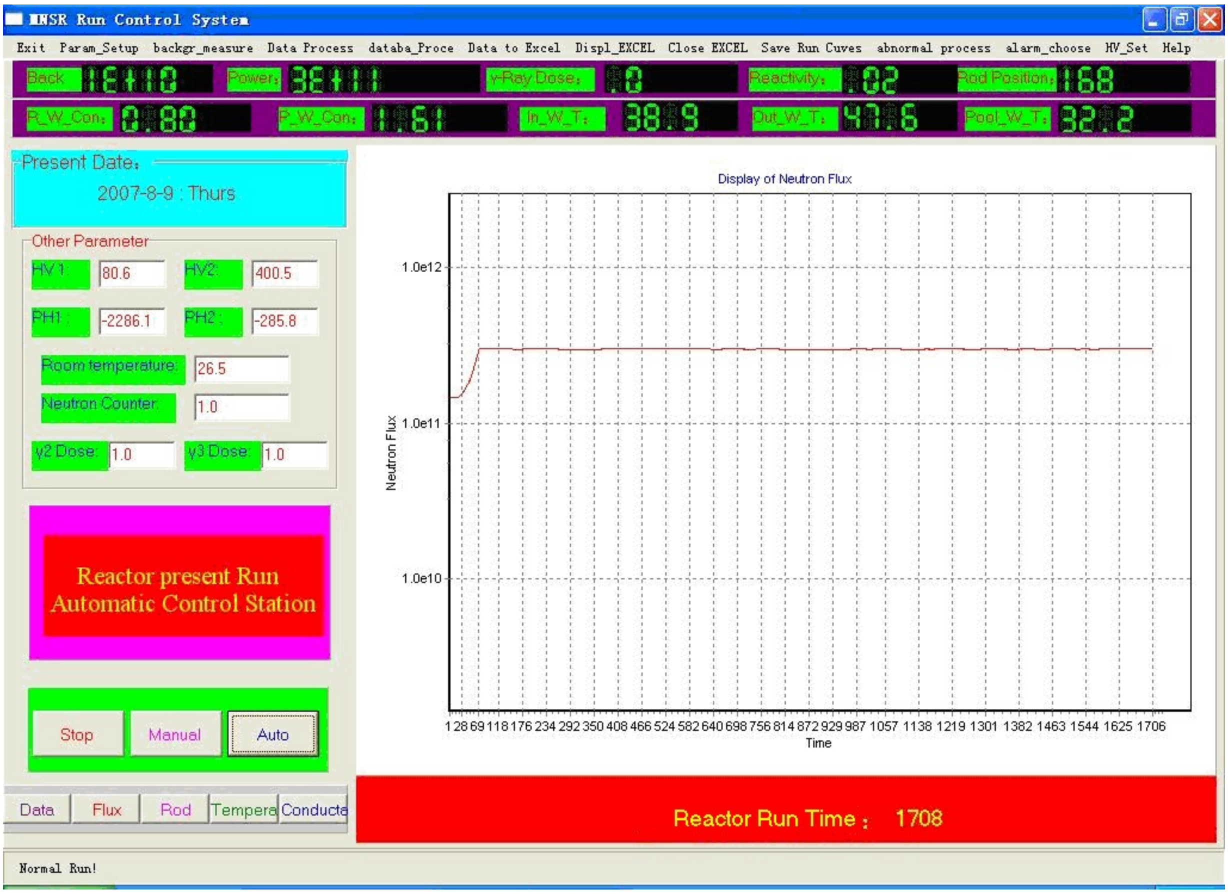


FIG. 3. Screenshot of Type II software application.

For excess core reactivity measurements, a DOS application has been written by personnel at the center which is used to calculate the excess core reactivity. This measurement is taken on the first day of operation in the week when the reactor is operated at a neutron flux of $1 \times 10^9 n\ cm^{-2}s^{-1}$.

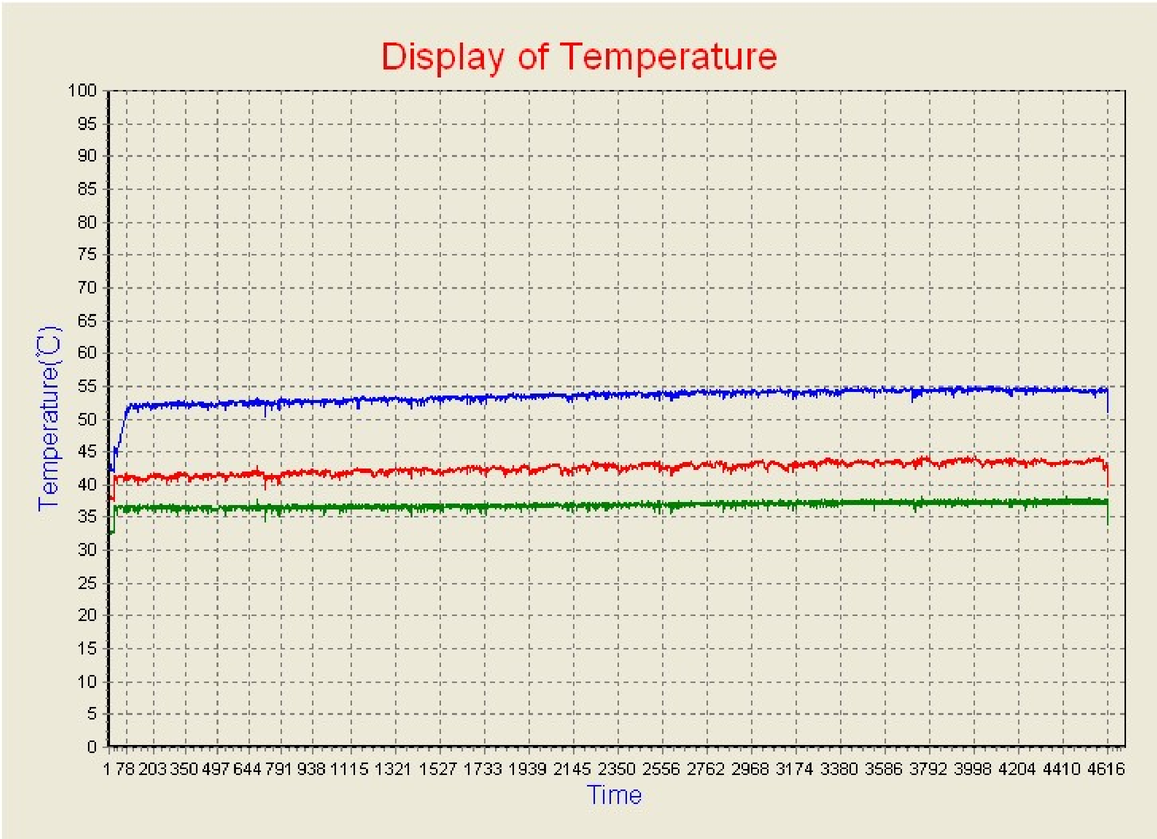


FIG. 4. Temperature trend display on Type II software application.

6. PERFORMANCE OF THE MCCS

6.1. Control rod position displacement

The microcomputer closed-loop control system is the main system used in operating the reactor. During the year 2011, the parameters of both the control console and the microcomputer were compared to identify any variance. Among these parameters, the control rod position was identified as giving the greatest variance with about 10 mm difference realised between the two systems. Thus for any recorded rod position on the MCCS, that on the Control console registered 10 mm more. Also, the control rod position dial on the control console exceeded the upper limit of 230 mm during start-up of the reactor when neutron flux is building up.

It was realised that wear and tear over a prolonged period of usage was responsible for the lack of synchronisation between the Control Console and the newly installed MCCS.

6.2. Electronic failures

Occasionally, some integrated circuit components (ICs) in the MCCS had to be replaced due to their malfunctioning. In one instance, during reactor operation, the computer screen displayed a black screen. The system was scrammed and operation was switched over to the control console. Since the problem has not recurred since, it is difficult to determine the cause of it and provide a solution as well as a means of preventing it from happening again.

In another instance, reactor water conductivity displayed false readings especially at reactor operation start-up. It was discovered that there was a dry capacitor terminal on the interface board. The capacitor was removed and re-soldered to fix the problem.

The minimum neutron flux value recorded by the MCCS at shutdown was always within the 10^8 n/cm^{2}s range whiles that of the control console was within the range of 10^7 n/cm^{2}s. At higher neutron fluxes, the measured fluxes are approximately the same.

The computerized control system is designed to achieve a stable flux with accuracy of ±1.0%. All the peripheral circuits including the micro-current amplifier are fixed in the cabinet of the MNSR control interface.

With the computerized control system, an operator password is required to operate the reactor. Maintenance frequency is prescribed by facility management, and as and when it becomes necessary to carry it out. This is done in accordance with provisions of the facilities Safety Analysis Report (SAR).

In accordance with the Operating Limit and Conditions (OLCs) of the facility's SAR, operability of all operating systems is required and ensured at all times. This is required for safe operation of the facility and associated instrumentation. This is achieved by compliance with prescribed operation and maintenance (O&M) procedures and protocols provided in the SAR and also in accordance with the national regulatory body's requirements and international standards.

7. CONCLUSION

The upgrade to the new system has improved the overall reliability of the control system and its operation has been satisfactory but for the unavailability of certain vital measurements like excess core reactivity, gamma dosage etc. Alternative means of taking these measurements have been identified but it is hoped that a means of fixing these anomalies will be realized soon.

BIBLIOGRAPHY

[1] LI,Y., YU, Y., ZHANG, Y., Report of Installation, Testing and Commissioning of New Computerized Control System for GHARR-1 Facility-IAEA Project GHA4012, National Nuclear Research Institute, Ghana Atomic Energy Commission (2008).

[2] AKAHO, E.H.K., et al., Ghana Research Reactor-1 Safety Analysis Report, National Nuclear Research Institute, Ghana Atomic Energy Commission (2008).

[3] ANIM-SAMPONG, S., Operational Safety, Regulatory Requirements, Advances and Expected Outcomes in the GHARR-1 Computerised Control System Upgrade Project, National Nuclear Research Institute, Ghana Atomic Energy Commission (2007).

DESCRIPTION OF THE NEW DESIGN FOR THE RENOVATION OF THE PCS-RELATED I&C SYSTEM

M. EVANGELOS
National Center of Scientific Research 'Demokritos'
Athens, Greece

Abstract

A renovation project of the Primary Cooling System (PCS) and related sub-systems of the Greek Research Reactor (GRR-1) is underway. The project includes the renovation of the PCS-related I&C sub-system which will be upgraded to include redundant analog safety-related controls, digital monitoring equipment and digital non-safety-related controls. The new PCS-related I&C sub-system will be interfaced with the existing analog-based Main Control System. In consistency with the international codes and standards, several hardware options were examined including SCADA-PLC, DCS, Digital Controllers. Reliability, maintainability, flexibility, upgradeability and cost were considered, along with design and construction obstacles. The design process is in the final stages. The present state of a new PCS-related I&C sub-system design of the GRR-1 and its interface with the existing Reactor Protection System is presented.

1. INTRODUCTION

1.1. Reactor overview

The Greek Research Reactor (GRR-1) is a pool-type, light water moderated and cooled, heterogeneous reactor designed by AMF. GRR-1 went critical for first time on June 1961. Since April 1964, the reactor operated at thermal power of 1 MW. In 1971 the reactor was upgraded to 5 MW. Upgrade works included replacement of the cooling system with a new one, consisting of primary and secondary circuits equipped with heat exchangers and cooling towers, replacement of the tile liner of the pool with a stainless steel one, installation of new power supply systems and change of the fuel elements from Low Enriched Uranium (LEU) to High Enriched Uranium (HEU). In 1990 a further upgrade of the reactor was performed by the introduction of beryllium reflector blocks at the two sides of the core. In the time period from 1999 to 2004, gradual replacement of spent HEU fuel elements by fresh LEU elements took place and the reactor operated with a mixed core consisting of both HEU and LEU fuel elements. The reactor was shut-down for refurbishment and modernization in 2004. A major refurbishment of the reactor building was completed in 2008. In 2009 a program aiming to replacement of the Primary Cooling System (PCS) and improving the reactor design and control system was initiated.

1.2. I&C system refurbishments

The analog safety/control system architecture of the reactor has not changed during reactor's 50 years of operation although several I&C system refurbishments took place:

1970s:

— The manual pool isolation valves were replaced by pneumatic isolation valves that provided the fail-safe feature to the pool isolation system.

1980s:

— The Ionization chamber amplifiers, the Fission Products Radiation Detector and all Control Room recorders were replaced.

1990s:

— Primary Cooling System Flow elements and indicators were replaced;

— Secondary Cooling Systems Flow elements were replaced;

— Inside Control cabinets, all relays were replaced;

— The Radiation Area monitor was replaced;

— The Control rods adjusting controller was replaced.

2. REACTOR MODERNIZATION PROJECT

2.1. Project overview

In 2004 a modernization project was initiated aiming to extend reactor's lifetime for at least another 15 years and ensure its safe and reliable operation. The project included:

— Confinement structure renovation including static reinforcement and ceiling reinforcement with carbon fibers. Sub-project was completed in 2008;

— Electrical infrastructure replacement including switchboards replacement and emergency power generation systems upgrade;

— Primary Cooling System replacement including flapper, grid plate, relevant instrumentation, emergency cooling system and water purification system;

— I&C upgrade including control room and instrumentation modernization.

2.2. Contractual arrangements

In 2009 through an international call for bids for the above mentioned project, a contract was awarded for the:

— Provision of scientific – engineering advice on the replacement of the Research Nuclear Reactor's primary cooling system of NCSR 'Demokritos'.

According to the contract, the underbidding company would design and supervise the installation of the new GRR-1 Core Primary Cooling System and the related control room instrumentation. The reactor's manager had full responsibility of the project implementation and was also responsible to hire external constructors to apply the design and deliver complete and operating PCS and PCS-related I&C systems.

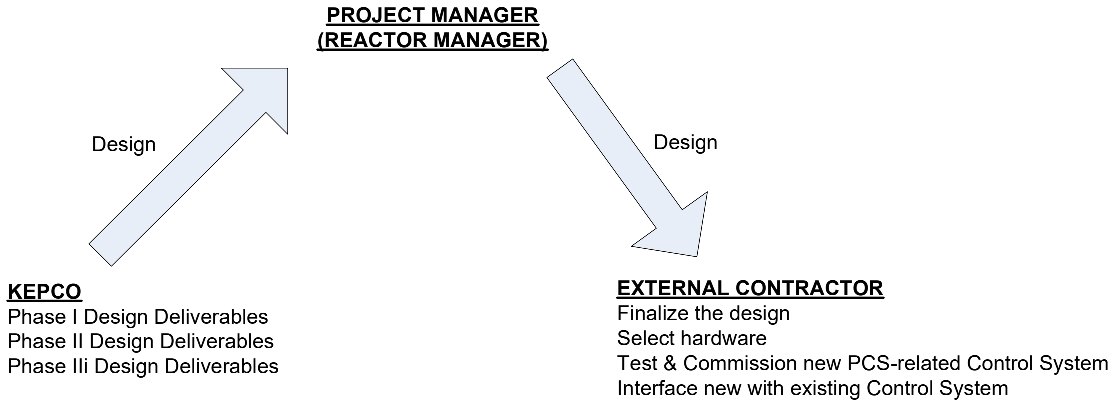


FIG. 1. Contract structure.

Contractor's obligations regarding the I&C system replacement were:

- The categorization and classification of processes;
- The description of all PCS related controls and interlocks;
- Detailed specifications of PCS related control system and field instruments;
- Applicable codes and standards definition;
- Control room layout drawings;
- General description of human-Machine interfacing devices;
- Interfacing the new PCS-related control system with the existing Main Control System;
- Control logic and C&I diagrams that would describe in detail all the processes and actions taken by the control/safety systems.

Construction company's obligations were:

- The provision of the detailed design of the new PCS-related control system;
- The selection of the appropriate hardware for control, operating interface and data acquisition for Reactor Protection System and non-safety related control;
- The development of the necessary software for the microprocessor based controls and interfacing devices and systems for the non-safety-related part of the new PCS-related control;
- The interconnection of the new PCS-related I&C Subsystem with the existing Main Control System;
- The implementation of the final design ("turn-key" project).

3. I&C MODERNIZATION

3.1. Basic concept

A new Primary Cooling System (PCS) design includes the I&C system. Instrumentation associated with control functions related to the new PCS is distinguished into two parts: a) Safety Related Control functions and corresponding system; and b) Non-safety-related control functions and corresponding system. The former monitors and handles all the safety related parameters in the new PCS, processes them and transmits them to the main Reactor Protection System. The latter comprises the non-safety-related processes monitoring, the data acquisition and storage and the graphical Human-Machine-Interface.

The new **Reactor Protection System (RPS)** would process all important to safety process parameters of the PCS and was designed to be fully analog.

Non-safety-related control system would undertake the non-safety-related processes, the data acquisition and storage and the graphical Human-Machine-Interface. The non safety-related-control system was designed to be digital.

3.2. Regulatory framework

The GRR-1 Reactor is operating under the supervision of the Greek Atomic Energy Committee (GAEC) that regulates and supervises all Greek nuclear facilities. GAEC's regulatory oversight regarding the research reactor is consistent with the applicable IEAE and European codes and standards.

3.3. Design requirements and considerations

The design requirements and considerations for the new I&C system were based on the applicable international codes and standards, international common practice in reactors design and particularities and demands of the specific project.

The graded approach of international codes and standards of research reactors I&C systems was applied. IAEA safety standards, IEC and IEEE codes, technical guidelines and standards were followed to demonstrate safety and performance of all systems and components

Reliability of all important to safety parameters was met. PCS-related I&C Design fulfilled the Single Failure Criterion by following the redundancy requirement for all Important-to-Safety components (1oo2).

Safety improvements were considered. Fail-safe systems and components were implemented to control all safety-related parameters of the process and provide in-depth defense.

Human-machine interface was designed to preserve the safe and reliable operation of the facility. Existing control room layout and panel arrangement remained. Facility supervision equipment, such as electronic recorders and process mimic displays were added. Special attention was given to the operators, technicians and supervisors training on the new systems.

PCS-related I&C Systems and components were classified and categorized. Safety functions were examined independently. Important-to-Safety Input Signals had to go through as few as possible electronic processes in order to generate the appropriate Output Signals, none of which were software based, to avoid common cause software failure.

Modular components that could be replaced with the system on-line would were selected.

Commercial-off-the-shelf items were preferred to lower the implementation and operational costs and increase market availability. Maintainability and spare parts availability were also considered, hence the equipment of well-established firms was selected.

Flexibility & ease to upgrade of the new I&C system was considered, in case additional features would be required in the future.

The availability of contractors/constructors/suppliers was examined.

3.4. Reactor Protection System

The Reactor Protection System (RPS) of GRR-1 protects the reactor from unsafe conditions by allowing the rapid insertion of the control roads into the reactor core and stopping the fission process. The RPS consists of a) the appropriate instrumentation monitoring a number of important reactor operation parameters, b) the reactor protection logic system, and c) the control-rods system.

The instrumentation subsystem measures various important parameters, processes them and generates appropriate signals that are fed to the Reactor Protection Logic system, the non-safety related control system, and the recording and HMI display system.

The Reactor Protection Logic System receives the input signals from the RPS instrumentation channels processes them and provides a SCRAM signal that releases the control rods into the reactor core.

The control rod system comprises the five control rods, the control rod drive mechanisms, the magnets holding the control rods connected into the drive mechanisms and the power supply to the magnets.

A SCRAM signal generated by the Reactor Protection Logic system cuts off power to the magnets holding the control rods and causes the rapid insertion of the rods into the reactor core. There are two kinds of SCRAM signals: Fast SCRAM and “slow” SCRAM. The fast SCRAM causes an interruption of the current of the magnets in 5mescs leading to the release of the rods. The “slow” SCRAM causes a cut of the power supply to the magnets in 20msecs leading to the release of the rods.

3.5. Fast SCRAM

Fast SCRAMS are generated by two independent signals:

(a) Reactor Power Period < 3 sec;

(b) Power > 6.5MW (>130% of nominal power).

Reactor period is measured by the Log-N and period amplifier and associated electronics and from the neutron flux in the core.

Reactor power is measured by two independent “safety channels” each consisting of an Uncompensated Ionization Chamber and associated electronics. The measurement is based on the neutron flux in the reactor core. The high reactor power SCRAM signal is therefore, based in a 1-out-of2 logic.

All the fast SCRAM instrumentation concerns parameters (neutron flux and rate of increase) that are not part of the new PCS system and hence are not affected by the new PCS related I&C system.

3.6. Slow SCRAM

Slow Scrams are generated by the following signals:

(a) Flappers position;

(b) Pool water level;

(c) Core outlet temperature;

(d) PCS flow;

(e) Core inlet temperature;

(f) PCS process radiation level;

(g) Bridge unlocked;

(h) Guide tube lifted;

(i) Entrance to primary pumps room;

(j) Manual SCRAM.

Signals a) to f) are related to the new PCS design and were therefore, redesigned. Signal a) existed in the present GRR-1 design but the new PCS will comprise two flappers so the new system will have two independent flapper signals. Signals b) to e) existed in the original GRR-1 design but they were single channel signals. In the new design each of them will be replaced by two redundant channels. Signal f) is a new SCRAM signal added in the new design. This too will consist of two redundant channels.

The new I&C design’s safety-related operation could be illustrated by examining one important-to safety parameter: In the case of the pool water level, two signals are transmitted by two independent ultrasonic water level transmitters. Both signals are received by one controller installed inside the control room. One-out-of-two (1oo2) logic creates an output signal which is fed to the existing Reactor Protection System. In case one of the two signals goes beyond a set-point, an ALARM/SCRAM is generated by the existing RPS.

Signals g) to j) are not related to the PCS and therefore they will not be redesigned or changed.

3.7. Reactor protection system logic

The Reactor Protection System Logic will remain as in the existing design, being fully analog. As described in the previous two subsections the new PCS I&C system simply replaces some of the existing safety channels with new ones consisting of two redundant channels and a logic one-out-of-two switch. The output of this switch will feed directly the existing location in the analog reactor protection logic. One additional signal (out of the 1-out-of-2 switch) of the RPS Process Radiation Level is readily addable to the existing RPS logic which has the capability of receiving additional inputs.

4. FINAL REMARKS

The safety related I&C design changes introduced by the new PCS design does not alter the basic logic concept of the RPS which remains fully analog. It simply adds a degree of redundancy to the PCS relate signals which now are generated by two redundant channels, whilst in the existing design are single channels.

A full replacement of the RPS is envisaged for the future. Depending on the regulatory requirements digital control logic will be examined at that time.

4.1. Non-safety-related control system options – comparison

For the non-safety-related parameters of the new I&C sub-system, a few alternative design concepts were available:

(a) **Analog-based Controls** with Individual Controllers (non-software based) and printed circuit boards for non-safety-related signals processing. The use of analog based controls would require custom design and construction of analog circuits for the new signals processing, I/Os combined with individual controllers and individual indicating and recording hardware that would operate as the Human-Machine Interface (HMI).

(b) **Distributed Control Systems (DCS).** Installation of custom designed and constructed digital control systems by well established international firms, utilizing custom-made electronic systems, controllers, Programmable Logical Controllers (PLCs) and I/O cards, flat panel displays, all combined into one rigid "black box" undertaking all non-safety-related control processes, HMI and data acquisition operations.

(c) **SCADA Systems combined with PLCs.** Such control system would require the use of commercial off-the-shelf electronics, PLCs and computer based data acquiring and graphical representation software. All controls and automations would be undertaken by the PLCs. Data acquisition and graphical representations would be undertaken by PC based software.

Based on the specific requirements and considerations of the project an extensive market research was performed in order to determine the most suitable of the options for the new I&C system design. The results of the research are summarized in Table 1.

TABLE 1: NON-SAFETY RELATED CONTROL SYSTEM OPTIONS COMPARISON.

	Reliability	**Demand for Maintenance**	**Flexibility Upgradeability**	**V&V Effort**	**Contractors Availability**	**Cost**
Analog-Based Control	High	Difficulty into finding spare parts	Low	Low	Low	High*
Analog Cards & Individual Controllers (non-software based)	High	Low	Low	Medium	Medium	Low
DCS	High	Reliance on external contractor	Low	Low (Contractor does the V&V for its equipment)	Medium	High*
SCADA	High	Low	High	High	High	Low

* Because the total amount of input signals (23) is relatively low, the cost per signal could be very high.

5. PRESENT STAGE – CHOSEN DESIGN

The selected design separates the non-important from the important to safety I/O signals.

Because the total Important-to-Safety input signals are relatively few, the use of individual controllers was not prohibitive. For the Reactor Protection System the use of analog controls was decided from the beginning of the project. The Important-to-Safety parameters (new redundant input signals) are transmitted directly to assigned Controllers that take the appropriate actions and their output signals are driven into the existing Main Control System. This way the safety controls remain fully analog and the existing analog system architecture unchanged.

Non-Important-to-Safety parameters are transmitted to the PLC which generates the appropriate output signals and these are fed into the existing Main Control System. PLCs also receive the Important-to-Safety parameters only to transmit them to the SCADA Workstation. The Workstation connected to the PLC runs graphical representation diagrams and displays them to a flat panel display, operating as the Human-Machine Interface. The workstation also does the data acquisition and storage of all process parameters.

Figure 2 shows roughly the interconnections of the new I&C sub-system.

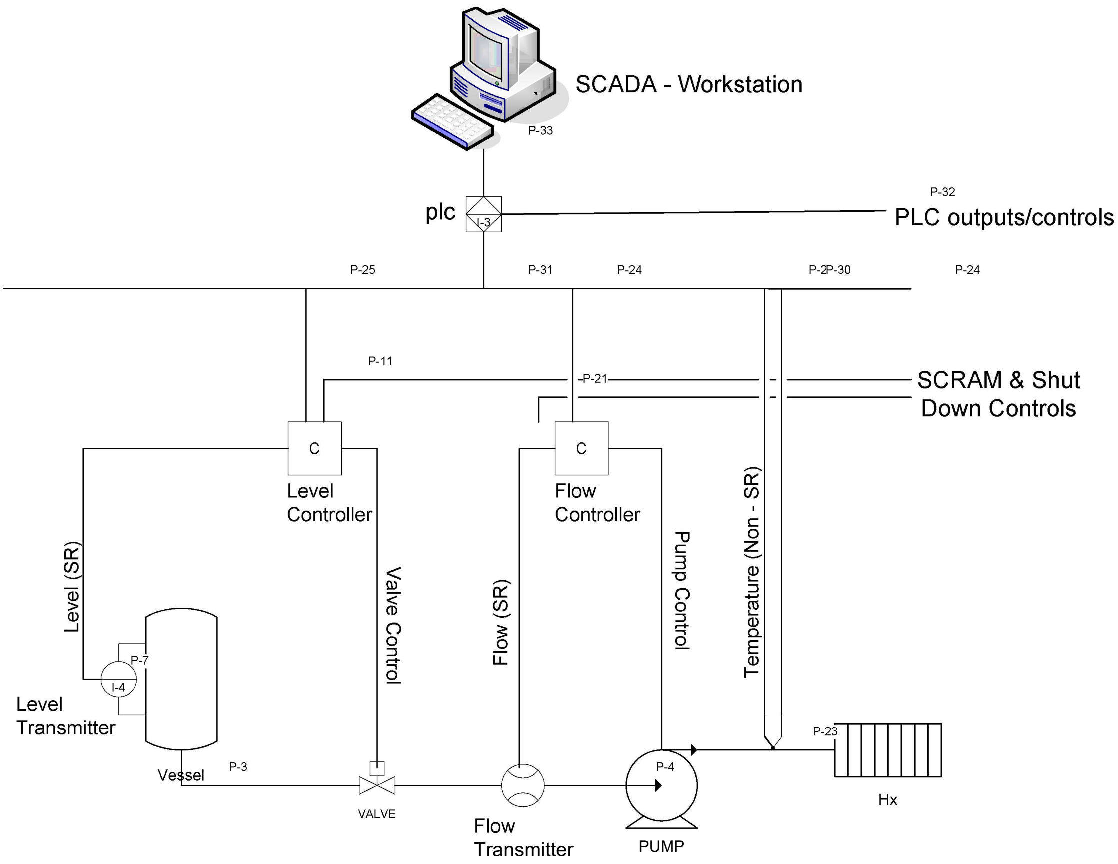


FIG. 2. Representation of new I&C system architecture.

EVOLUTION OF REAL TIME COMPUTER BASED INSTRUMENTATION AND CONTROL SYSTEM FOR FAST BREEDER TEST REACTOR (FBTR)

K.VINOLIA, S.SRIDHAR, B.ANANDAPADMANABAN
Fast Breader Test Reactor, Indira Gandhi Centre for Atomic Research,
Kalpakkam, Tamil Nadu, India

Abstract

In the evolution of computers their first generation was characterized by the use of vacuum tubes. These computers were expensive and bulky. They did not support multitasking. In the 1960s, transistor based computers replaced vacuum tubes. Transistors made computers smaller cheaper and energy efficient. But transistors were responsible for the emission of large amounts of heat from the computer. Due to this computers were subject to damage. The use of transistors marked the second generation of computers. The use of Integrated circuits ushered in the third generation of computers. Transistors were miniaturized and placed on silicon chips, called semiconductors, which drastically increased the speed and efficiency of computers. This increased the speed and efficiency of computers. Thousands of integrated circuits placed onto a silicon chip made up a microprocessor. Introduction of microprocessors was the hallmark of fourth generation computers. The evolution of computers continues. This paper deals with the evolution of computer based system used in supervising and controlling the Fast Breeder Test Reactor (FBTR), Kalpakkam for the past three decades. The Fast Breeder Test Reactor is a 40MWt, loop type, sodium cooled fast reactor built at Indira Gandhi Centre for Atomic Research (IGCAR), Kalpakkam, India. FBTR uses mixed carbide/oxide of Plutonium & Uranium as fuel and liquid sodium as coolant. The Central Data Processing System (CDPS) of FBTR consists of real time, fault tolerant computer based systems to carry out safety critical supervision such as supervision of fuel sub-assembly temperatures for any flow blockage, clad hot spot and undesirable power excursion and to take safety action in the event of detection of any one of them. The system does safety related functions such as Group supervision, Discordance supervision of triplicated neutronic parameters Event sequence recorders etc. This paper explains the pros and cons of various computer based systems starting from the third generation computer systems installed and commissioned at FBTR since criticality. The issues related to retrofitting are also dealt with in this paper.

1. INTRODUCTION

Fast breeder reactors constitute the second stage of India's three-stage nuclear energy program, for effective utilization of the country's limited reserves of natural uranium and exploitation of its large reserves of thorium. FBTR is a 40 MWt, loop type, sodium cooled fast reactor. Heat generated in the reactor is removed by two primary sodium loops, and transferred to the corresponding secondary sodium loops. Each secondary sodium loop is provided with two once-through steam generator modules. Superheated steam at 480°C & 120 kg/cm^2 from the four steam generator modules is fed to a common steam water circuit comprising a turbine-generator and a 100% dump condenser (Fig.1). The core consists of 745 closely packed, hexagonal shaped subassemblies. The subassemblies are vertical and freestanding, supported at the bottom by the Grid plate and held on to the latter by collapsible hold-down springs. During the reactor operation, the heat generated in the core is removed by the liquid sodium coolant. Fuel subassemblies are at the centre, surrounded by nickel reflectors, thoria blankets and steel reflectors. The sodium enters the fuel subassembly from the bottom and leaves at the top, removing the heat produced during fission. If coolant flow is blocked, the clad temperature increases beyond design limits and may lead to clad rupture and further to fuel melt down. Hence, continuous monitoring of the core cooling and initiation of safety actions in case of any abnormal temperature rise in the core are essential. **Fault tolerant Real time computer systems** are used in **FBTR** for carrying out safety critical supervision such as supervision of fuel sub-assembly temperatures for any flow blockage, clad hot spot and undesirable power excursion and to take safety action in the event of detection of any one of them. Safety related supervision functions carried out by these real time computer systems in FBTR are start-up check for reactor, discordance supervision of triplicated neutronic parameters, general supervision of process parameters against alarm limits, event sequence recorder, auto flooding initiation condition supervision, siphon break line supervision and start-up check for fuel handling.

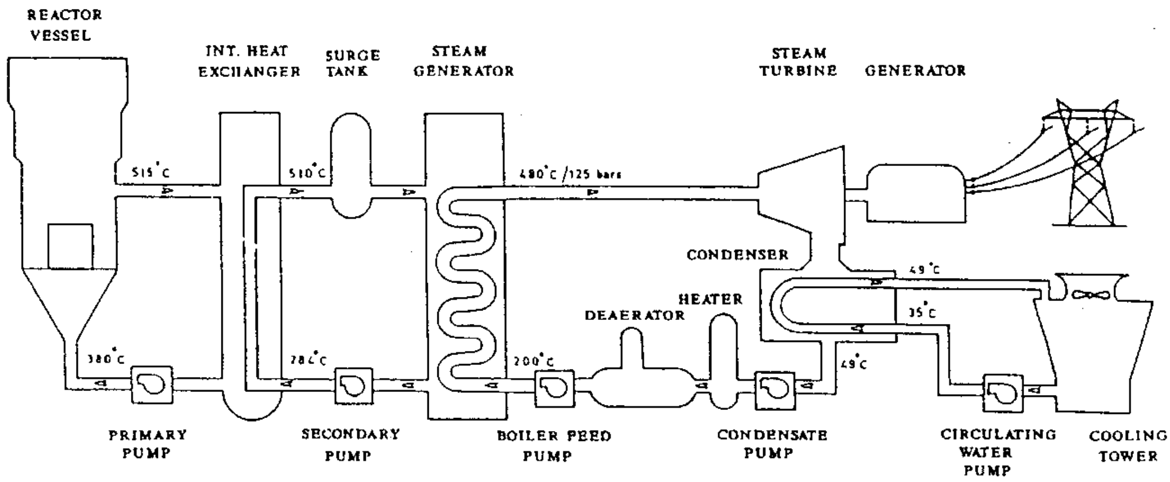


FIG.1. Simplified schematic of FBTR.

These systems supervise and control over 640 analog and 320 digital signals from the plant. This paper elucidates how the central data processing system (CDPS) evolved from the third generation computer based system to the present state of the art embedded real time computer based system.

2. THIRD GENERATION COMPUTERS

The CDPS (in the Eighties) originally consisted of two TDC 316 computers connected in fault tolerant configuration as shown in Fig.2. Each computer has two buses, namely Input/output bus (I bus) and Memory bus (M Bus). To the I bus, input and output peripherals like analog input sub system, digital input / output sub systems, real time clock, card reader are connected. In the M Bus 24K core memory is connected. Direct memory access peripherals like magnetic tape units, disc, and line printer are connected to both M Bus and I Bus. In both systems the real time clock is programmed to give repeated interrupts at 31.25 m sec interval. The online diagnostics program will be operational every 31.25 m sec. The program checks the healthiness of different units of the computer system. If found ok, it will send a watchdog pulse to the Switch Over Logic Circuit (SOLC) through digital output system. Normally, when both computers are operational, computer-I will be executing the full plant software. The digital outputs of the computer-I will be connected to the plant by SOLC through Oring logic. The common bus will be linked to the I bus of computer-I. In computer- II only online diagnostics will be under execution. This program periodically sends watch dog pulses to SOLC indicating that the system is alive. If the Computer –I becomes faulty, SOLC will interrupt the Computer – II. On receiving the interrupt, computer-II will start executing the full plant software. The common bus will be connected to computer-II at this time. In the common bus, peripherals like cathode ray display unit, matrix printer, and analogue output sub system are all connected. When computer-I becomes operational, switch over back to computer-I will take place. During switch over, the interruption in plant supervision is minimized by information spared through common core memory.

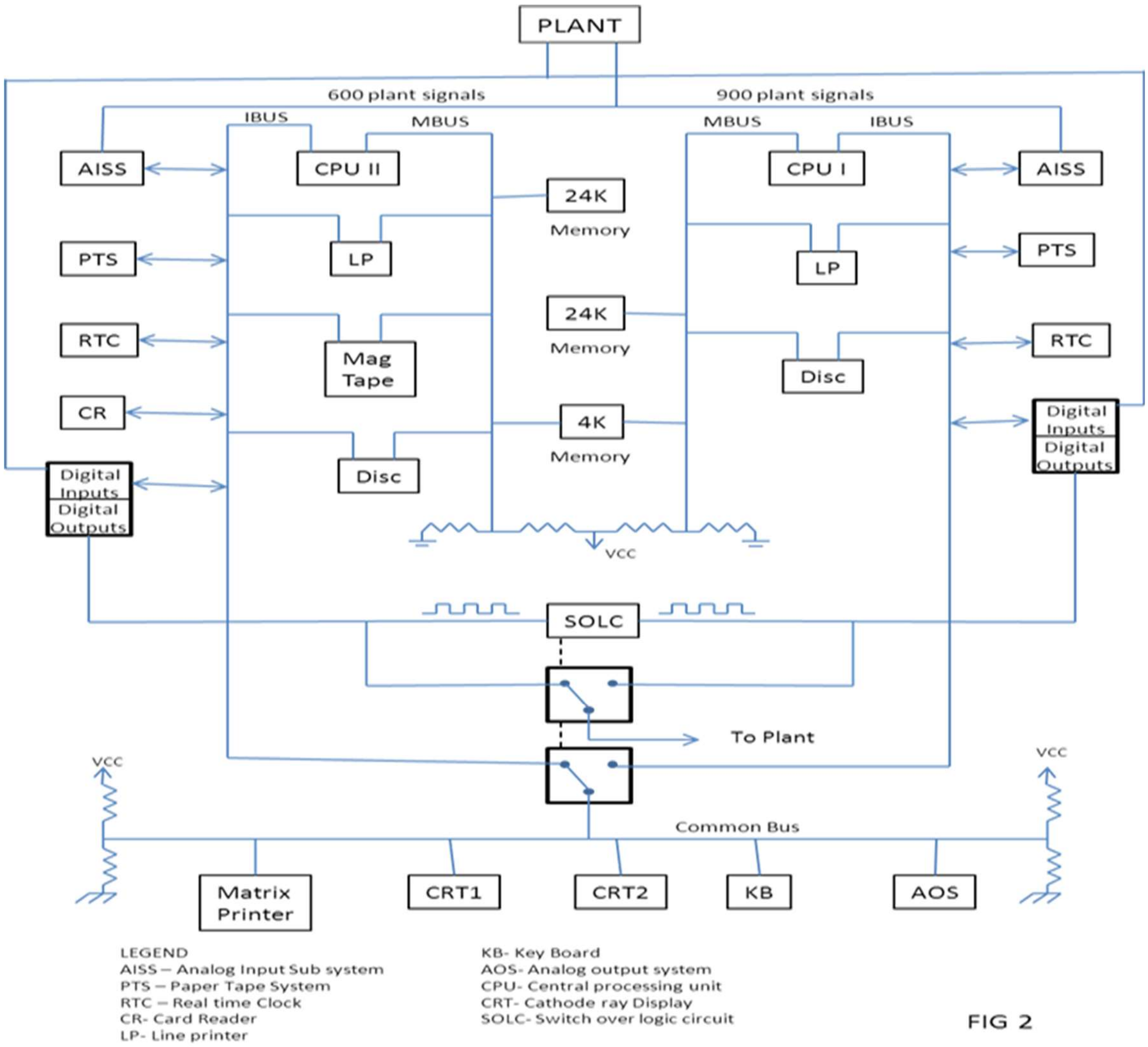


FIG. 2. Central data processing system.

Nearly 900 analog signals representing temperature, flow, pressure, level of sodium and neutronic signals are wired to computer-I. Nearly 600 important analog signals are duplicated to computer-II. The analog signals are classified as fast scanned signals which are scanned every one second, medium scanned signals that are scanned every 20 seconds and slow scanned signals that are scanned every 5 minutes interval. In Computer-II there are no slow scanned signals. 500 digital signals representing neutronic trips for alarm, LOR and scram conditions etc. are wired to both computer systems. The analog signals are compared by CDPS against upper and lower threshold. If the signals exceed the threshold, then alarms are energized through digital outputs. The digital outputs of each computer are wired to 'ORING' logic. The ORed output is fed to the plant.

2.1. Limitations of TDC 316 systems

2.1.1. Size

The design of CDPS was carried out in 1971. Hence the system was built around SSI chips. With the result, the size of the computer is very large. The CPU itself was made of 20 PCBs.

The memory is made of core memory. For just 28K, it occupies four module holders, with each module holder housing about 20 double size cards. Because memory capacity is limited, entire CDPS software could not be housed in core memory. Part of the software, like general supervision, trip supervision, discordance supervision etc., are housed in disc units.

2.1.2. Terminal

Alpha numeric terminal used in CDPS works on parallel interface mode and does not have graphic facility.

2.1.3. Paper tape system

For initial loading of program, only paper tape reader was available. They are very slow compared to floppy drives.

2.1.4. Floating point processor

Hardware floating point processor was not available and so, the floating point operation was carried out by software. This takes a long time for completing a calculation.

2.1.5. Memory

Since memory capacity is limited to 28K, part of the CDPS software is housed in disc. The disc resident programs have to be brought to core memory periodically, executed and written back into disc.

2.1.6. Languages

The plant software including monitor program was developed in assembly language. Debugging the software is quite difficult.

3. RETROFITTING OF TDC316 SYSTEMS

3.1. PDP 11/84 system

Frequent failure of TDC 316 systems was faced due to ageing and maintenance became difficult due to component obsolescence. In the year 1988, the sub system –I was replaced with 4th generation, mini computer system, namely PDP 11/84. The system with J11 microprocessor @ 18MHz, had hardware floating point processor, 1MB ECC memory, 450 MB Hard disk, Magnetic tape, Floppy disc along with Analog I/O and Digital I/O subsystems. Here the analog signals were classified as fast with 1 second scanning interval and medium with 20 seconds scanning interval. The system used disc based RSX -11M real time multitasking, multi user operating system with compilers for FORTRAN –IV. The application software were developed in FORTRAN –IV and all the application software were memory resident and were running in parallel under the control of operating system. The human machine interface (HMI) commands were retained as in TDC 316 systems for ease of use. Due to the increased memory size, additional facilities were added to CDPS as given below:

(a) Reactivity calculation;

(b) Hydrogen leak detection;

(c) Control rod level discordance check;

(d) History dump during LOR or Scram;

(e) Operator console for functions like call a measure, trend, compute ‘ai’ constants for core thermocouple etc.;

(f) Graphical user interface for plant mimics, Graphical trend, History, dump on demand, classified logs etc.;

(g) Auto flooding condition check;

(h) Siphon break line check;

(i) Rate of raise of power check;

(j) Log power supervision;

(k) History storage for messages.

3.1.1. Limitations of PDP 11 /84 system

PDP 11/84 system has overcome the limitations of earlier third generation TDC 316 computers. Also the application development was made easy due to the availability of high level language compiler. Configuration of software data was made easy as these data were stored in editable data files. A software simulator was developed to test the software and for software debugging. However the system had the following limitations:

(a) The task length is limited to 32KW including the common memory. Hence the thresholds had to be hard coded in applications where the task length is more. In such applications online modification of thresholds is not possible. The application has to be recompiled on modification of thresholds. The smaller applications where the thresholds are stored in data file have to be rerun once the data file is edited to change the threshold;

(b) All the application programs were running in parallel and the control of CPU was given based on the priority assigned to each of the software. Scanning software scans all the analog input signals and stores them in the common area. Supervision programs, takes these partially scanned values for limit checking;

(c) Segregation of safety critical, safety related and non-safety functions, is not there and so a single CPU has to process all the applications;

(d) The operating system is disc based. Hard disk being a mechanical device, is prone to failure. Once hard disk fails, the application software cannot run;

(e) Event sequence recorder was a part of PDP 11 system and so the software was running at 1 sec. interval only whereas the response time of Reactor Shutdown system is 40 milli second;

(f) Printers were connected to the computer directly through Current loop to RS232 converters for printing messages and log.

3.2. UNIPOWER-30 system

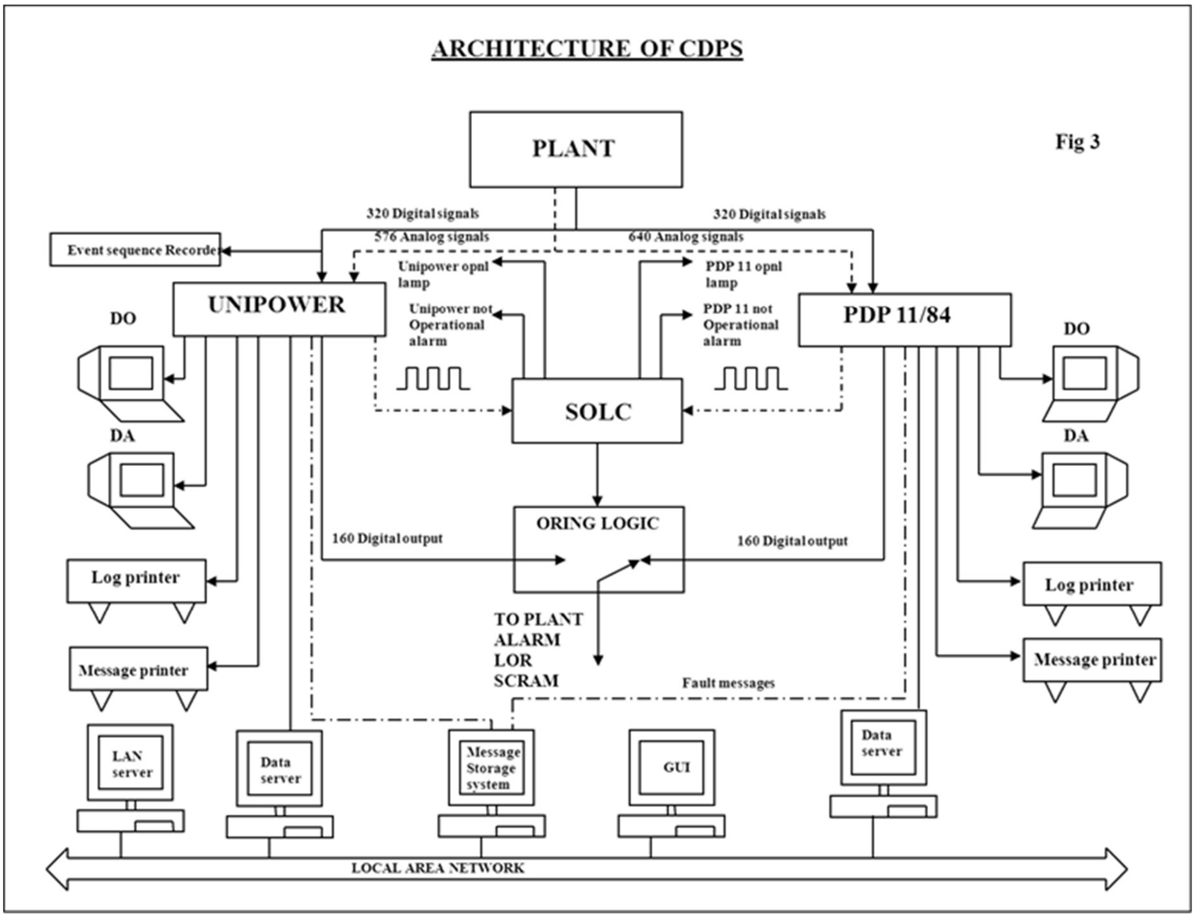


FIG. 3. UNIPOWER-30 system.

In the year 1994, the second TDC 316 system was replaced with VME Bus based Motorola 68030 processor @25MHz, 4MB ECC memory, 540MB SCSI hard disk, Magnetic tape with Analog I/O and Digital I/O systems as shown in Fig.3. The system used Disc based Versa DOS real time, multi tasking, multi user operating system. The application programs as in PDP 11 were developed in ANSI C language. As in PDP 11 system software simulator program was developed in C to test the application programs. Also utility software was developed here to modify the software parameters online. Unlike PDP 11, the parameters in common memory can be modified online without the need to restart the software. A monitor program will give control to all the application programs sequentially depending on the interval in which application has to run. For instance, core monitoring program runs every second, fine impulse test program runs every 3 seconds interval, general supervision program runs every 20 second interval, and so on.

3.2.1. Limitations of Unipower-30 system

Unipower -30 system had no limitation on the length of the task. Hence the thresholds can be modified online by an Edition program. The neutronic trip signals were removed from the Unipower-30 system and were connected to a dedicated Industrial PC based system called Event Sequence Recorder with a scanning interval of 20 millisecond. Also here the non safety related applications like reactivity calculation and history dumping of data during LOR /Scram were removed from the Unipower-30 system to remove the CPU load. These applications were running on a dedicated data server system connected to the Unipower-30 system. A common PC based message server system was developed to receive the messages from PDP 11 and UNIPOWER-30 systems directly through COM ports for information storage and retrieval as shown in Fig. 3. IEEE guidelines were followed in development of the software. Independent V&V was carried out and the comments of the V&V team were incorporated. However this system had the following limitations:

(a) The operating system is disc based. Hard disk being a mechanical device, is prone to failure. Once hard disk fails, the application software could not run;

(b) Printers were connected to the computer directly through RS232 line drivers for printing messages and log.

4. REAL TIME EMBEDDED SYSTEMS

The PDP 11 and Unipower-30 systems were connected in fault tolerant configuration such that PDP 11 system was online and Unipower-30 system was active standby. These systems were working satisfactorily. Due to ageing the hard discs were failing frequently and hence it was difficult to maintain due to non availability of spares. It was decided to replace these systems one by one. Unipower-30 system was replaced in 2006 and PDP 11 was replaced in 2009 by identical Motorola 68020 @25MHz based real time embedded systems as shown in Fig 4. The VME bus based CPU card has M 68882 FPP, 1 MB EPROM, 2 MB SRAM with EDAC facility, 128 KB EEPROM, programmable watchdog timer, 2 Nos. Hardwired TCP/IP ports and 4 Nos. RS 232C ports.

During replacement, the safety critical functions were segregated from safety related and non-safety functions. Thus there were three ED-20 based embedded systems namely, SCS, SRS and NSS as shown in Fig 4. Unlike earlier systems, now both systems are made identical with respect to number of analog signals, digital input and output signals, functions, hardware etc., a waterfall model was used and IEEE guidelines were followed for software development. Independent V&V was carried out in each phase of software development. The functional test was carried out by the operation personnel as per test plan. Also the event sequence recorder is identical. The software is developed using C programming language using a tasking compiler and is downloaded to EPROM in the CPU. The configurable data are stored in EEPROM. While the embedded system supervises and takes safety action, the non safety related functions like printing and displaying the messages, or providing data to the graphical user interface are done by a dedicated industrial PC based systems. A dumb terminal is connected to the embedded systems for modifying the thresholds online under administrative control. The PC based GUI provides information for the operator and is password protected. The design of the system is such that no external system failure would affect the embedded system and any internal failure of the embedded system would initiate a switch over to the standby system or order shut down to the plant as the case may be. Since there are no hard disks attached to the embedded system, and there is no operating system the reliability of the system is high when compared to the earlier systems. Since the system uses in-house developed hardware and software, problems like obsolescence and functional modification of software due to requirement change would not arise. The diagnostic routine in the embedded system is such that the routine will print the exact card number when it fails on the console and so maintenance is easy and down time is reduced. Modular design both in hardware and software helps in ease of maintenance.

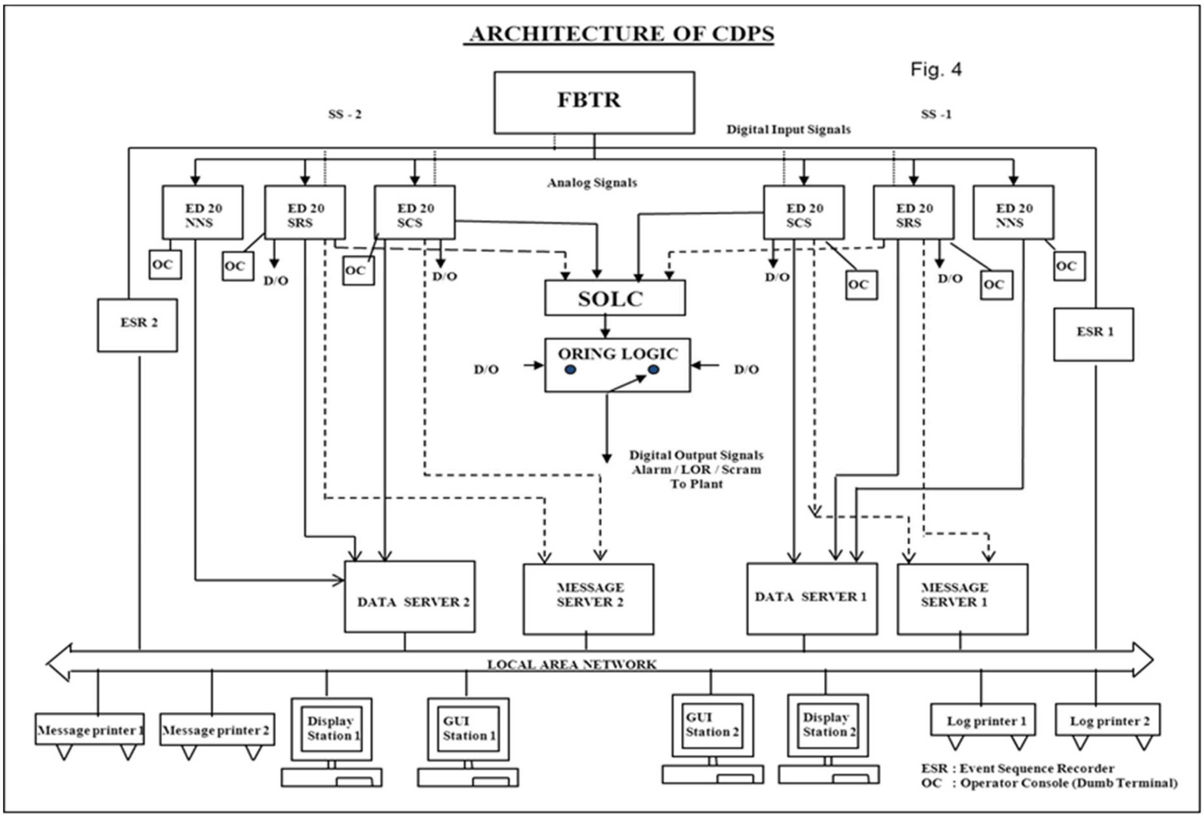


FIG. 4. Motorola based real time embedded system.

5. ISSUES OF RETROFITTING

The advantage of retrofitting of real time computer systems is that the processing requirement is well known. The hardware and software limitations that were prevailing in the earlier system were considered while designing the new system. Also, additional plant requirements which could not be realized using the earlier system were also considered during the design. GUI was modernized to issue commands through a mouse unlike the text based commands used in third generation computers. However there were issues that had to be addressed while back fitting the computer based systems. They are given below:

(a) The scheme for back fitting is such that the existing instrument cables, control cables both at the input stage and output stage of real time systems are not disturbed;

(b) The design of analog data acquisition and digital data acquisition should be such that existing conventional instrumentation channels should not be affected. Ground isolation should be provided for analog and digital signals;

(c) If proven hardware is not selected, feasibility analysis is required;

(d) To the extent possible existing HMI format is retained, such that the plant operator is comfortable in the operation of new system;

(e) To improve the quality, verification and validation is very much important at every stage of development cycle;

(f) Testing of software as per the test plan should be carried out;

(g) The schedule of back fitting is drawn such that the operation of the plant is least disturbed;

(h) Well trained personnel has to carry out the back fitting project;

(i) Budget has to be planned.

6. CONCLUSION

In FBTR, in addition to carrying out supervision and control functions efficiently, real time computer systems send data to dedicated Industrial PC based servers for Data processing, data storage and presentation of data. The Graphical User Interface (GUI) developed is user friendly. However obsolescence, changes in system requirement and updated regulatory guidelines, etc. necessitates replacement of these real time systems. The experience gained in revolutionizing the computer based systems with the passage of time is enormous. It gives us an impetus to apply more and more computer based systems to functions important to plant safety.

ACKNOWLEDGEMENT

The authors thank Mr. S.C. Chetal, Director, IGCAR and Mr G. Srinivasan, Director, ROMG for their continuous support and encouragement in our endeavours.

UP-GRADATION OF SAFETY CLASS IA AND IB I&C SYSTEM IN RESEARCH REACTOR USING QUALIFIED PROGRAMMABLE LOGIC CONTROLLER

Mohit Kalra.[1]; Prema Kumar Kavalan.[1]; Sanjay Jain.[1]; S.T. Sonnis.[1]; D.A. Roy.[1]; U.W.Vaidya.[1]; Debashis Das.[1]

[1]Electronics and Instrumentation Group, Bhabha Atomic Research Centre, Mumbai, India

Abstract

The Control & Instrumentation (C&I) Systems of Dhruva Research Reactor were designed in late seventies. The maintenance and upkeep of the systems was the major challenge on account of several factors like non-availability of spares due to obsolescence, dominating end-of-life symptoms of mechanical components, non-availability of module/subsystem level self-supervision features etc. This necessitated evolving a generic platform based on digital technology in around 2009, which qualifies for implementation/up gradation of critical safety and safety related C&I systems. The considerations of platform development were mainly based on long-term sustainability with highest availability factors besides being reliable and verifiable for safety system deployment. The systems considered for up gradation were Reactor Trip Logic System (RTLS) &Start-up Logic System (SULS) both of safety class IA and Alarm Annunciation System of Safety class IB.

The specific key factors in design upgrade of above systems include fail-safeness, high availability, robust and exhaustive diagnostics, low MTTR and hot plug-in electronic modules. The Upgraded systems now facilitate time stamped recording of alarms/events and cyclic recording of process parameters at high periodicity rates for analysis to aid efficient operation &maintenance of the reactor. The systems are reconfigurable and programmable for quick adaption of changing requirements arising due to operational needs in research reactors as long-term sustenance. The upgraded digital I&C systems has significantly contributed to improved plant availability associated with reduced burden on operator and maintenance staff. While harnessing the benefits offered by digital design, adequate measures have been incorporated to ensure that the system design is robust to protect itself and thereby the plant against cyber vulnerabilities.

These systems were built using the homegrown generic platform named as Trombay Programmable Logic Controller (TPLC-32). The system architecture is commensurate with the safety class and incorporates specific design features in the individual systems towards reducing spurious trips for improved availability and diagnostics and data logging features. The paper discusses the features noted above and being first of its kind deployed to perform safety class IA function of the reactor, the regulatory qualification aspects for the PLC platform and application software of individual systems are dealt with in the paper.

Key Words: PLC, class-IA and IB, TPLC-32

1. INTRODUCTION

RTLS system of Dhruva Research Reactor is intended to prevent reactor conditions from deviating beyond safe limits and, if safe limits are exceeded, to mitigate the consequences. The RTLS system is a safety class IA system. The earlier RTLS was a hardwired 2/3 voting logic system, to take care of single channel failure. To process the trip parameters and generate the trip signal, 192 hardware modules were required for RTLS system. The system was working for last 20 years and in recent years spurious trips were being generated due to failure of components. Due to limited diagnostic coverage, tracing the type and nature of failures was difficult. Most of the components had become obsolete and maintaining the system became very difficult. Hence it was proposed to upgrade this system to a triplicated computer based system.

The earlier start-up logic system (SULS) was a single-channel system, which provided all the required permissive for a reactor start-up. The transition from the 'reactor tripped' state to any desired power level is accomplished through a set of manual operations, which are to be performed through the control console in a certain sequence. The SULS is a safety class IA system. Being a single channel system, there have been many incidences of spurious reactor trips. Further, since the system hardware made use of relay drives & solid-state CMOS logics many of which are obsolete, it was proposed to upgrade it to a triplicated computer based system.

The earlier Alarm Annunciation (AAS) System was a three channel microcomputer system based on 8-bit microprocessor with each channel in a dual configuration. The system faced problems in operation and maintenance due to obsolescence of components, degradation of connectors and lack of documentation. To overcome these problems, it was proposed to upgrade the system to a dual channel computer system which could tolerate single failure and with self-diagnostic and testability features and improved event-sequencing and data logging capability.

It was proposed to upgrade the above systems based on qualified configurable platform Trombay Programmable Logic Controller-32 (TPLC-32) indigenously developed in Reactor Control Division (RCnD), BARC.

2. TPLC-32 PLATFORM

TPLC-32 is a PLC platform developed in RCnD, BARC to configure and build computer based safety and safety related C&I systems for Nuclear Reactor. TPLC-32 architecture is shown in Fig. 1. TPLC-32 architecture mainly consists of PC based Engineering console & TPLC-32 hardware. PC based Engineering console provides graphical user interface to build the application logic through a software package called Application Development Environment (ADE). It facilitates defining I/O configuration details of the I&C system & provides a Function Block Diagram (FBD) Editor for graphical programming using Function Block Diagram language complying with IEC-61131.

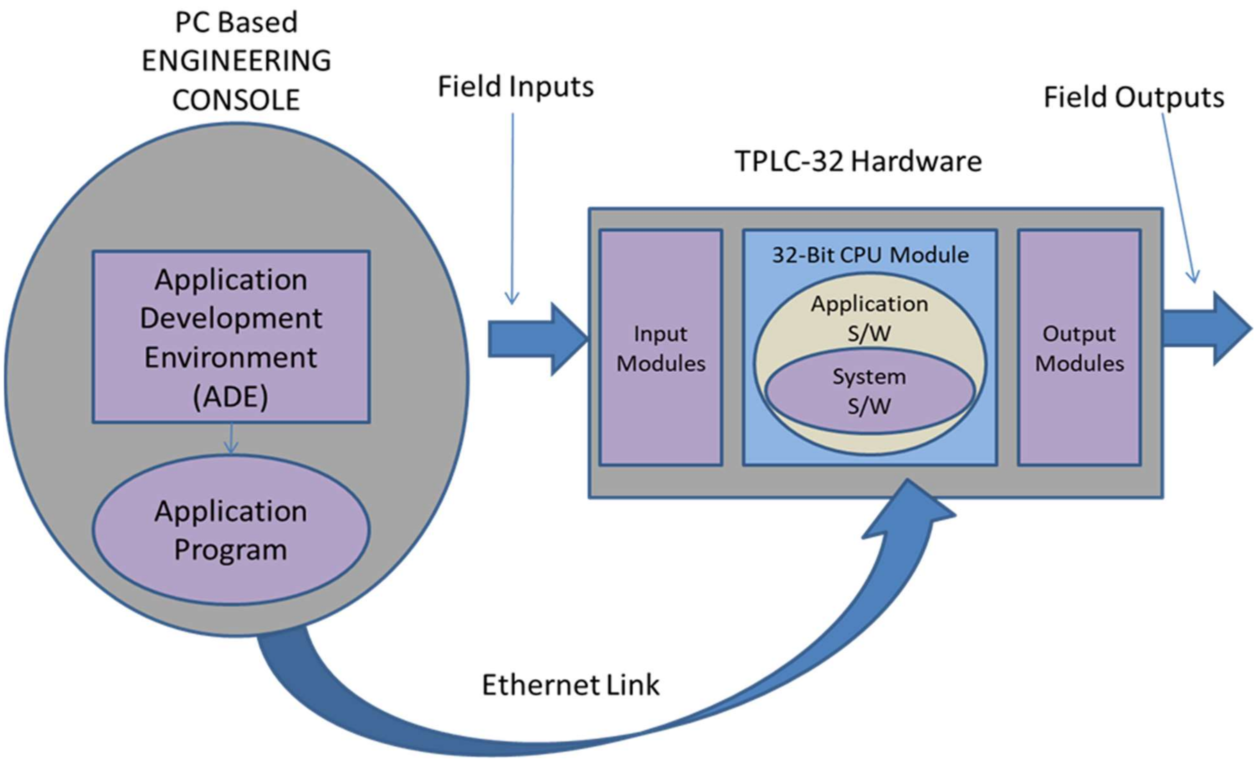


Fig. 1 TPLC-32 Architecture

TPLC-32 hardware is an embedded computer system, which consists of intelligent input/output boards for field Interface and 32-bit processor based CPU board. It also consists of intelligent Ethernet communication boards for operator console interface.

PC based Engineering console generates application binary file (application software), which includes I/O configuration & application logics. This binary file is downloaded to the TPLC-32 hardware from PC based Engineering console using Ethernet communication as shown in fig.1. This application software is stored in flash memory in CPU board along with pre installed system software. The application logics are executed by system software under in-house developed Real Time Kernel named Embedded System Operating System (ESOS).

2.1. features OF TPLC-32

The salient features of TPLC-32 are simple & modular design, systematic development process, qualified hardware & software, fail-safe design etc. Some are described in detail below.

2.1.1 Systematic Development Process

The complete design and development is carried out following a Systematically Controlled development process based on Regulatory Guidelines given in AERB/NPP-PHWR/SG/D-25& IEC 60880. Various Design Documents have been produced as part of the design process.

2.1.2 Qualified Hardware & Software

Verification and Validation has been carried out for both hardware and software by an independent team of engineers based on Verification and Validation Plan as per regulatory review process given in AERB/NPP-PHWR/SG/D-25. Failure rates estimation of intelligent Input/Output boards was carried out.

2.1.3 Simple & Modular Design

PC based Engineering Console provides Simple, User friendly, tree control based Graphical User interface for programming the System configuration details of I&C system. The graphical application programming environment is based on Function Block Diagram. Function block diagram editor with associated help and error detection features simplifies application software development.

The Software design is highly modular based on TOP-DOWN design approach with high cohesion and low coupling among the modules. The system software uses in-house developed small footprint pre-emptive multitasking kernel having predefined static task priority structure. No memory allocation has been used during run time. Usage of interrupts is restricted, only for essential activities. The design facilitates hardware redundancy at System level and embedding fault tolerant features during system configuration and Application development. If facilitates easy maintenance with built-in automated on line fault detection and annunciation.

2.1.4 Real Time & Deterministic Performance

TPLC-32 system Software sequentially executes all processing, control and safety functions at specified fixed cycle time under all load conditions without any jitter. It also ensures deterministic execution of all diagnostics function of the system. This is achieved using in house developed RTOS ESOS. ESOS also provides memory protection functions.

2.1.5 Robust Diagnostics

Various diagnostics are carried out on all I/O hardware modules periodicity. On failure detection, time stamped Diagnostics message is generated detailing about the failure in the board/system. Integrity of System software, application software & alterable parameters are also checked periodically. Health of hardware watchdog is also checked as part of diagnostics.

2.1.6 Software Self Supervision

It has built-in software self-supervision functionality to check timely execution of important tasks at programmed periodicity. In case of any delay in execution of important tasks beyond programmed periodicity, system generates failsafe output. The software program flow in all tasks is monitored to check that all the functions of tasks are executed every cycle in required sequence. If any discrepancy is detected the system generates failsafe outputs.

2.1.7 Fail safe Design

On detection of input board failure, for all further processing, it uses predefined failsafe values for input signals assigned to the failed board. On Output board failure, it generates the predefined fail safe output values to field. In case of any error in software integrity or self supervision, the system declares failure and generates failsafe outputs. Watchdog detects Gross software failure and generates predefined failsafe outputs.

2.1.8 Cyber Safety and Access Control

The TPLC-32 platform software has been fully reviewed through independent V&V process. It does not contain any malicious code.

The System and Application software is stored in Flash memory on processor board and are periodically checked for integrity as part of diagnostics. To change system or application software, physical access to the system cabinets is required which is located in a physically secure environment in the plant. Further the robust and proprietary protocol is used to download application and system software from Engineering Console using two-man-rule access authentication.

In-house developed Real Time Kernel is used in the system which eliminates any backdoors or traps. Engineering console facilitates role based privilege authentication for application software development. The design of communication interface has strong inbuilt features to protect against DOS and other network attacks.

3. SYSTEMS DEPLOYED

Three systems namely RTLS, SULS & AAS have been deployed based on TPLC-32 platform. The details of the systems and their architecture are described below.

3.1 RTLS System

The existing RTLS system was upgraded to a design based on qualified programmable TPLC-32 platform. The RTLS is a triplicated computer based system with each system capable of processing 160 Analog Inputs, 128 Digital inputs, 96 Digital Inputs and 48 Relay outputs.

The key features of RTLS include scan time of 20 mSec & input validation for three scan cycles, Grouped Local Coincidence feature for generation of trip, incorporation of Alarm Annunciation Function (AAS) for the Trip parameters, Pre-trip functionality for analog parameters, generation of trips on Irrational Low and Irrational High condition, Alterable Parameter Change Units (APCU) for changing design parameters of the system and PC based Operator Consoles (OCs).

RTLS consists of three computer based systems known as RTLS Channel-A, RTLS Channel-B and RTLS Channel-C. It also has two redundant PC based Operator Consoles (OCs). The Architecture of RTLS is show in figure-2.

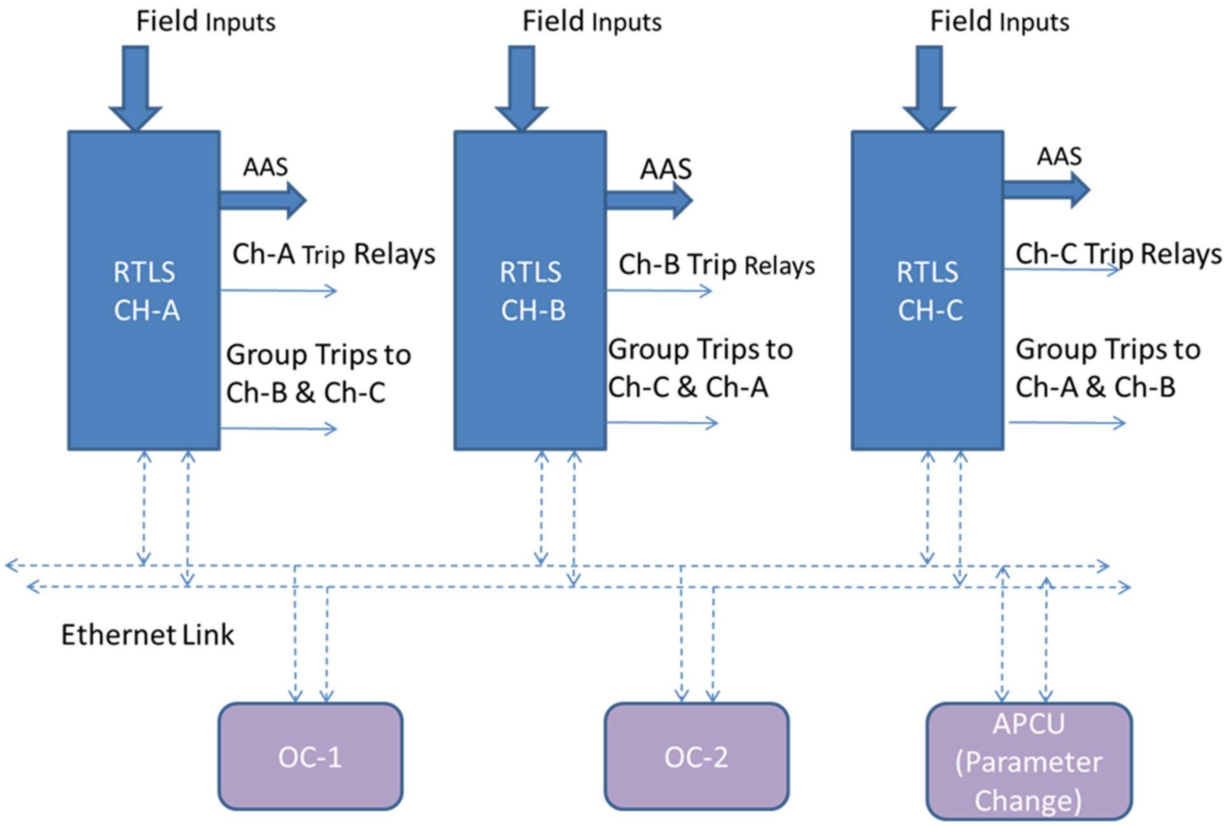


Fig. 2 Architecture of RTLS

The three channels of RTLS communicate with the two OCs over dual redundant isolated Ethernet links. Each channel of RTLS scans all the trip inputs corresponding to that channel periodically and in the event of any valid change of status in any of the inputs; it drives the corresponding outputs based on application logic. It also sends time stamped information to OCs for the purpose of recording and event sequencing. In the event of failure of any channel of RTLS, it's outputs go to fail-safe state. The sample of application logic for group trip generation is shown in figure 3.

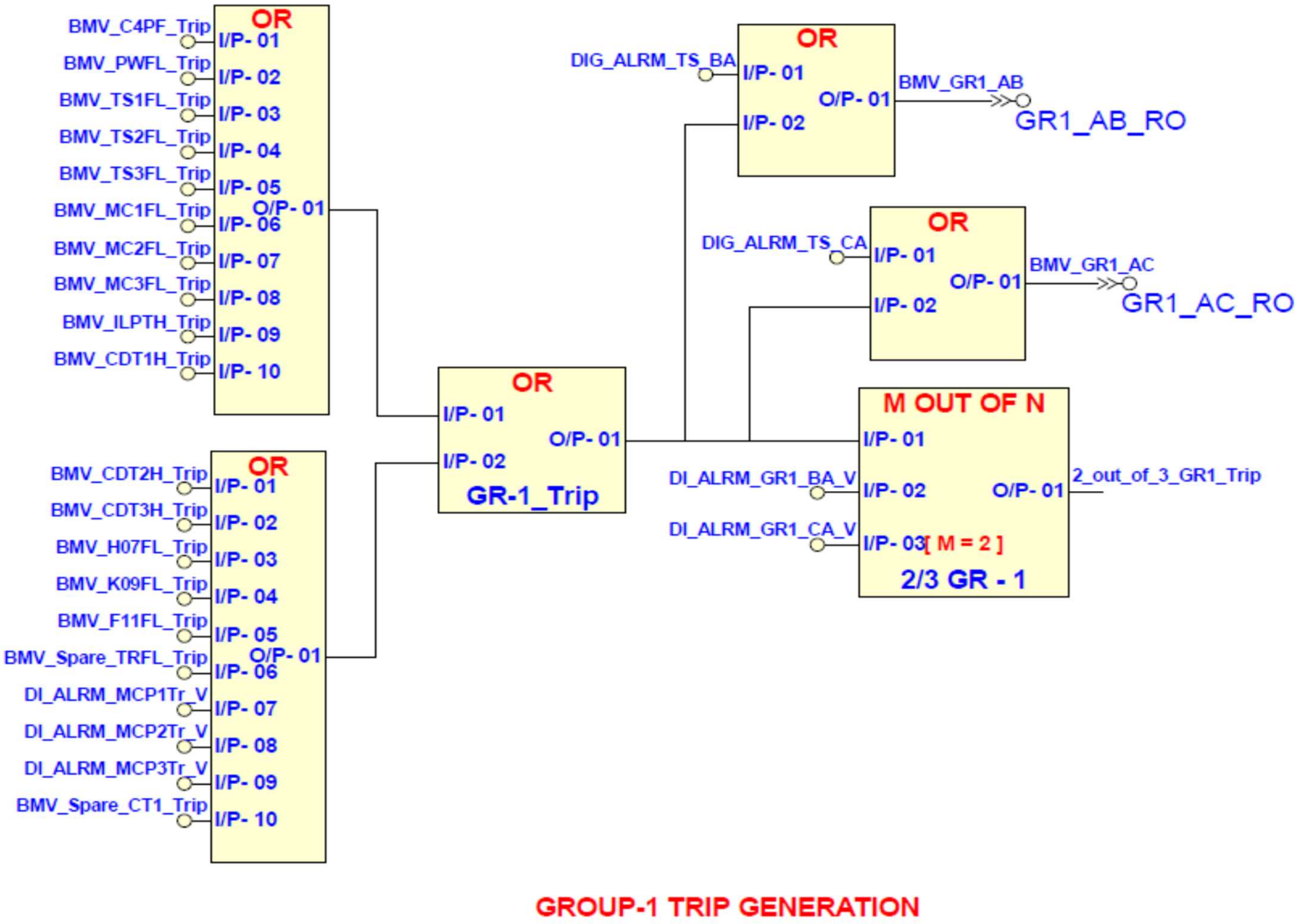


Fig. 3 Application Logic using FBD

One of the issues considered during system architectural design was to use the existing field cables and to accommodate the system hardware in the existing panels of Dhruva. The size of modules and bins of earlier system was similar to TPLC-32 platform boards and bin size, hence it could be easily accommodated in existing panels of Dhruva and the existing field cables needed no change.

3.2 AAS

The existing AAS system was upgraded to a design based on TPLC-32 platform. The AAS is a Dual computer based system with each system capable of processing 544 Digital inputs and 480 Digital Inputs.AAS is used for processing the field alarm inputs and to alert the control room operator by driving alarm window lamps, hooter and buzzer. AAS consists of two independent systems, namely, AAS-1 & AAS-2. The field inputs to both AAS-1 & AAS-2 are connected in parallel and the outputs of AAS-1 & AAS-2 are connected in parallel to drive the alarm window lamps and other outputs. The system have two independent Operator Consoles (OC) named as “AAS-OC-1” and “AAS-OC-2”. The AAS-1 & AAS-2 communicates with the OCs through dual Ethernet links. The Architecture of AAS is shown in figure 4.

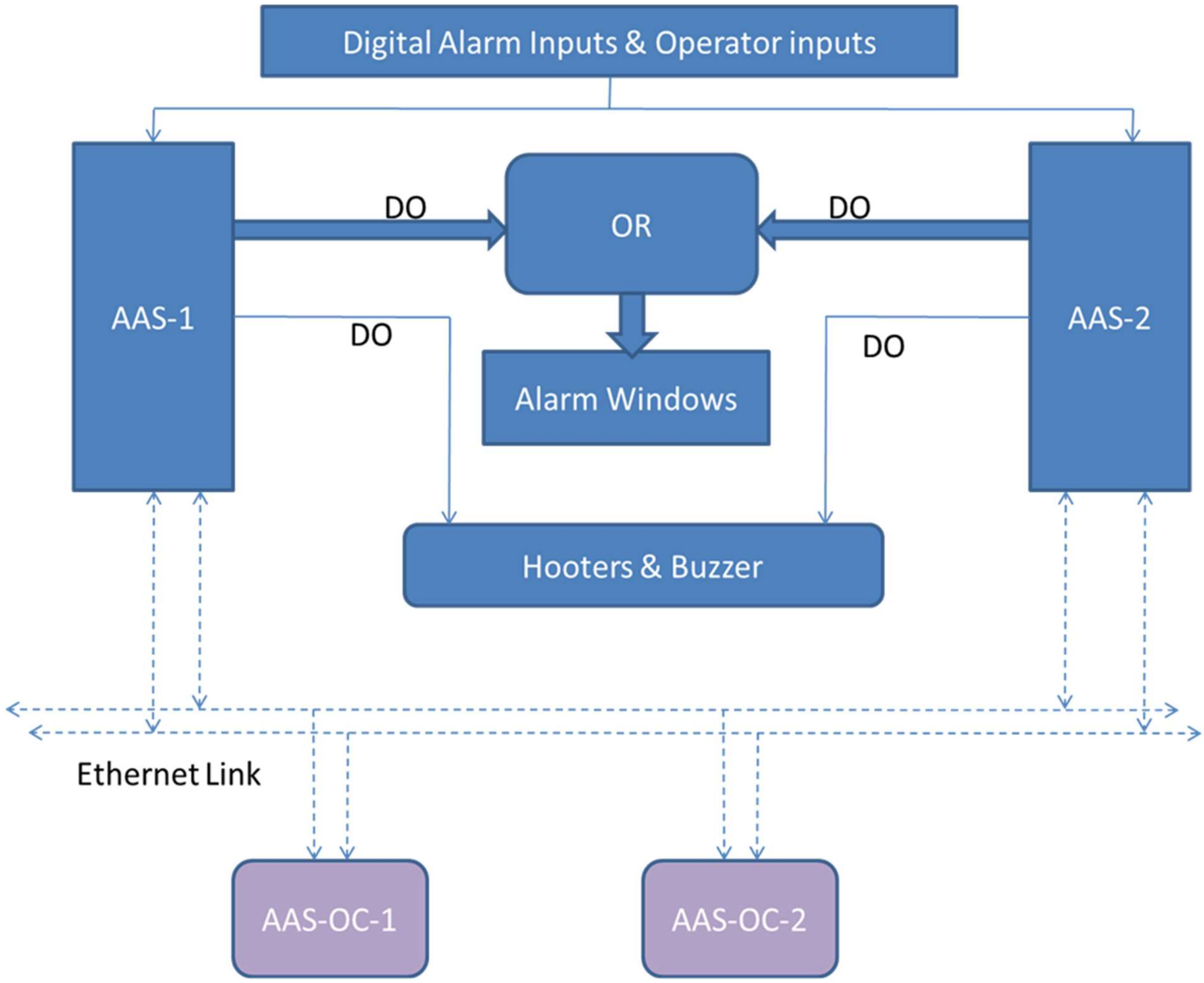


Fig. 4 Architecture of AAS

The key features of AAS includes Scan time of 10 msec, driving the lamps of Alarm Windows when the change in input status persists for 6 validation cycles and fault tolerant, with faults in one system not affecting functioning of other system.

3.3 SULS

The SULS for Dhruva is a triplicated computer based system capable of acquiring the 106 number of digital inputs, processing them as per pre-defined logics pertaining to the pre-start-up requirements and generating the 30 trip outputs. SULS is used for providing startup permissive for the reactor. The transition from the 'reactor tripped' state to Reactor Start Up is accomplished through a set of manual operations which are to be performed from the control console in a certain sequence. These operations will not be effective unless certain conditions are fulfilled. SULS implements these interlock conditions and generate Absolute Trip (AT) for the reactor.

SULS has a triplicated configuration consisting of 3 computer-based systems viz. SULS Channel-A, SULS Channel-B and SULS Channel-C. The architecture of SULS is shown in figure 5.

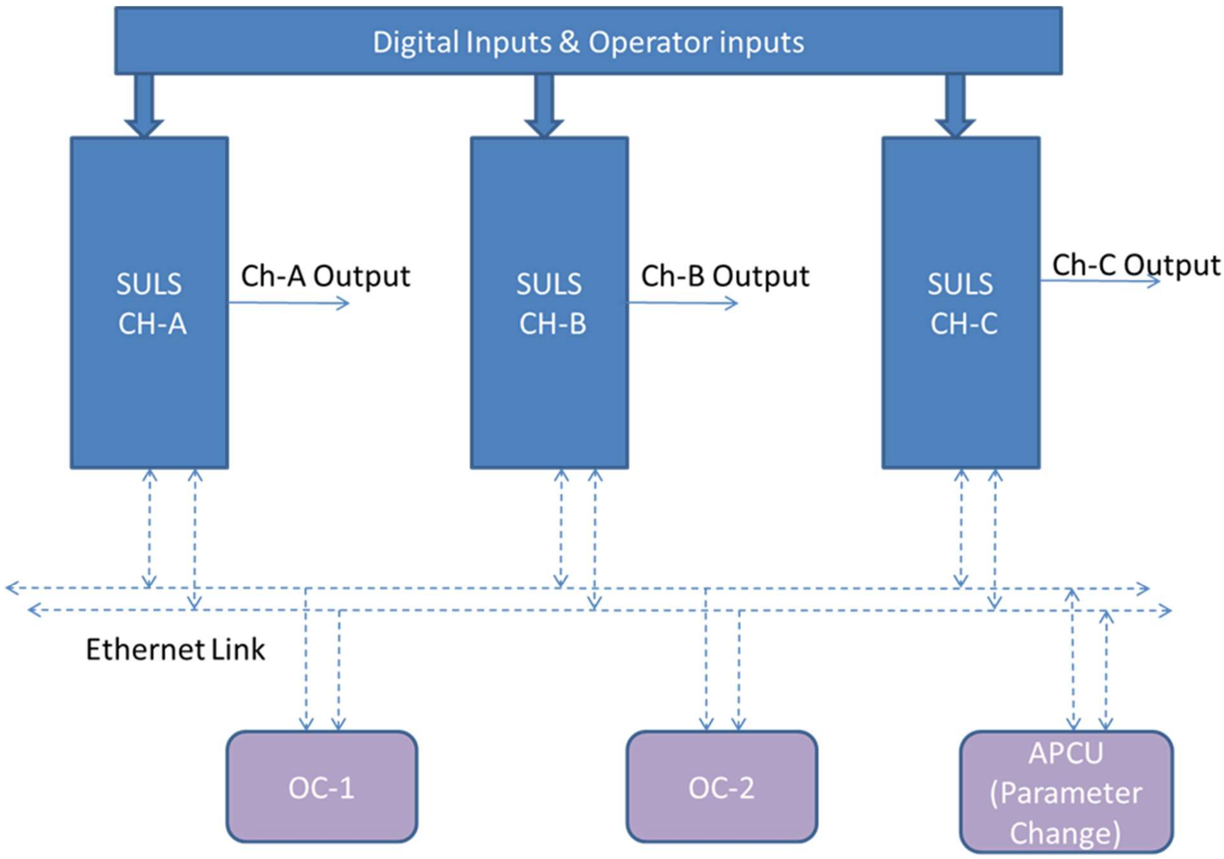


Fig. 5 Architecture of SULS

The field inputs to all three channels are connected in parallel and raise/lower outputs of the three channels are connected in a 2/3 ladder for raising /lowering each SOR. The trip signals of each channel are connected to corresponding channel of RTLS. The SULS system has two independent Operator Consoles (OC) named as “SULS-OC-1” and “SULS-OC-2”. The 3 channels of SULS communicate with the OCs through dual Ethernet links.

The key features of SULS includes Scan time of 10 msec, generating the required output when the change in input status persists for 6 validation cycles and fault tolerant, with faults in one system not affecting functioning of other system.

4. REGULATORY REVIEW OF RTLS, AAS & SULS

TPLC-32 platform was qualified for use in safety class IA & IB systems of NPP as per the standard regulatory review process guidelines of AERB/NPP-PHWR/SG/D-25.Independent verifications and validations (IV&V) of Hardware & software were carried out by independent engineers for the TPLC-32 platform. The IV&V activity was carried out concurrently with the software development as per the Software Verification and Validation Plan (SVVP). Since the TPLC-32 platform was qualified separately, only the application software of RTLS, AAS & SULS needed to be qualified for system qualification.

Safety case document was prepared for each system and submitted for the regulatory review. The Safety Case document mainly focused on the compliance to regulatory guides & the safety issues and safety features pertaining to development of these systems. Failure mode & effect analysis was carried out for all the systems &and it was confirmed that the failure in the systems has no effect on the plant safety. Various documents like System Requirements Specifications (SyRS), System Architecture Design (SAD, Software Requirements Specifications (SRS), System validation Plan (SVP), System Validation Report (SVR) etc. were generated and reviewed during this process.

5. CONCLUSION

In this paper, three systems namely RTLS, SULS & AAS of Dhruva research reactor which were upgraded to TPLC-32 platform based systems have been discussed. The earlier systems were very difficult to maintain due to obsolescence issues & spurious trips were being generated due to failure of components. The new systems were implemented based on qualified TPLC-32 platform, which uses state of the art technology in both hardware & software and provides better testability and maintainability features. We also discussed the salient features of the TPLC-32 platform like systematic development process, robust diagnostics, self supervision etc.

We also discussed the regulatory review process of the above systems, since TPLC-32 platform was already put through rigorous Verification and Validation procedure & cleared for use in safety class IA & IB system. For the systems, only application software was reviewed for regulatory clearance. This methodology reduced the qualification efforts required for each system. In addition, any modification can be achieved with very minimum efforts. The use of same platform for three systems will also help plant to maintain the systems very effectively with added benefit due to reduced inventory.

Reactor Trip Logic System Installed & Commissioned in 2015. System is working satisfactorily with only 2 I/O modules reported faulty till today.

Start up Logic System Installed & Commissioned in 2015. System is working satisfactorily with only once one channel SULS Ch-B reported trip due to power supply module malfunction till today.

Alarm Annunciation System Installed & Commissioned in 2013. System is working satisfactorily with only 1 communication modules reported faulty till today

BIBLIOGRAPHY

1. AERB Safety Guide No. AERB/NPP-PHWR/SG/D-25 (2010) Computer based systems of pressurized heavy water reactors. Atomic Energy Regulatory Board, Mumbai, India
2. Software Aspects of Computer based systems performing category-A functions, IEC60880, second edition, 2006-05
3. Indigenously developed Programmable Logic Controller for Safety Class IA and IB systems, SACI-2014, 24-26 November 2014
4. Graphical Programming Environment of indigenous Safety PLC, SACI-2014, 24-26 November 2014
5. IEC 61131-3 (Ed. 3.0) (2013–02) Programmable Controllers—Part 3 Programming Languages.

PROGRESSION OF UPGRADES IN I&C OF INDIAN RESEARCH REACTORS

C. Sengupta[1], P. Punekar[1], K. V. Gadgil[1], N. Ramkumar[1], S. Panyam[1], S. Bhattacharaya[1]
[1]Research Reactor Maintenance Division, Bhabha Atomic Research Centre, Mumbai (India)
E-mail: csen@barc.gov.in

Abstract. The Instrumentation & Control (I&C) Systems of Nuclear Research Reactors has evolved over the years. Right from Pneumatic instruments to Modern Digital I&C, it has passed through different phases. Though during design and construction of Reactor the I&C systems relevant safety standards of that time was adopted but current safety standards are to be fulfilled by the operating reactors. Due to obsolescence of C&I systems, C&I upgrade needs to be initiated. Upgraded C&I systems also provide better self-diagnostics, operator interface, enhanced safety & reliability. Research Reactor Dhruva, which was designed in late seventies & is operating safely since commissioning. The I&C systems were facing not only obsolescence but also having limited testability & diagnostic features. Regulatory requirements of current safety standards were also difficult to fulfil. The major Safety Class IA & IB Instrumentation and Control systems of Dhruva are upgraded to modern Digital I&C systems. The upgrades were taken in a phased manner to minimize the downtime of the reactor. The Pneumatic instruments were replaced by Digital Electronic Instruments. The Differential Pressure gauges of Channel Flow Monitoring System were replaced by Indigenously developed Digital instruments, fulfilling the regulatory requirements of current standard. The major I&C systems such as Reactor Trip Logic System, Start-up Logic System and Alarm Annunciation System etc. are replaced by an in-house developed Programmable Logic Controller (PLC). The systems were designed & developed using qualified configurable platform. Additional diagnostic features, better operator interface and security features were incorporated in the system. Verification & Validation (V&V) of the individual systems were carried out as per requirements of present standards. The Radiation Monitoring System, Fire Alarm System, Reactor Regulating System were also upgraded with Digital I&C with better operator interface, additional information & features and redundancy. This paper covers upgrade of different I&C Systems of Dhruva Reactor.

KEY WORDS: DIGITAL I&C, PLC, I&C UPGRADE

1. INTRODUCTION

Dhruva (100MWt) is a high power operating research reactor at BARC, Trombay, commissioned in 1985. The reactor is natural uranium fueled, with heavy water used as moderator and as primary coolant. Dhruva is used extensively for applied research, isotope production and manpower training.

The design of the instrumentation of Dhruva were incorporated, based on the operating experience of the Cirus reactor and the technology available during early eighties. The instrumentation and control system of Dhruva generally consists of pneumatic instruments with pneumatic indicators, recorder and pressure switches. Apart from this, Reactor Regulation, Radiation Monitoring, Fuel Channel flow, temperature and activity monitoring instruments were of analog type. Reactor protection system logic was a hybrid of solid state and relay logics. The Alarm Annunciation System was based on Dual microcomputers and had fast response and the capability to store the alarms. In the field of process instrumentation, a mix of both pneumatic and electronic instrumentation was employed.

However, with a few years of reactor operation, a need for upgradation of some of the instrumentation was felt in the data acquisition and processing systems, due to either obsolescence or for augmenting the facilities provided by the existing systems. Later upkeep of the pneumatic instruments was becoming extremely difficult due to component obsolescence and availability of spares. To begin with main control room analog and pneumatic recorders were replaced by digital recorders. This was followed by in-house development and implementation of dedicated PC based plant radiation data acquisition system, DAS for Reactor Regulating system, computer based fuel channel low flow trip logic processing system. In the recent past, the Main Control Room instruments were replaced by state of the art digital recorders and large screen display units which are operator friendly. Currently major upgrade of safety and safety related systems i.e. Reactor Trip Logic system, Main Control Room Alarm Annunciation system, Start-up Logic System has been completed.

Hardware and software of these systems, developed on PLC platform, have undergone rigorous testing, quality assurance program, system integration tests.

All the pneumatic transmitters and associated pneumatic instruments were upgraded with Digital Electronic transmitters, Indicating Alarm Meters (IAM), Alarm Trip Units (ATU) and Digital Chartless Recorders.

2. UPGRADE OF FUEL CHANNEL FLOW MONITORING DIFFERENTIAL PRESSURE GAUGES WITH ELECTRONIC DIFFERENTIAL PRESSURE SWITCHES(EDPIS)

As a part of C&I upgrades of Dhruva, all the Coolant Channel Flow Monitoring Differential Pressure (DP) gauges were replaced with Electronic Differential Pressure Indicating Switches (EDPIS) (*see FIG.1.*) due to the difficulties experienced in maintaining the old differential pressure gauges [1]. Apart from local flow indication existing gauges were generating low flow trip contact and high flow alarm contact. The main problems of existing DP gauges were obsolescence, unavailability of spares, aging and non-compatibility with computer based system.

2.1. Design criteria & site constrains

EDPIS was designed as per requirements of AERB/NPP/PHWR/SG-D10 & SG/D25, for class-IA components [2]. The EDPIS comprises of an electronic flow transmitter (giving 4 to 20 mA output signal) along with a micro-controller based indicating switch for low flow & high flow contacts. A digital flow indicator along with a semi-circular bar-graph display (similar to the dial of the existing gauge) is provided on the facia of the EDPIS. In order to minimize man-rem consumption during installation & commissioning and reduction of reactor shutdown period it was decided to install the EDPIS units in the existing DP gauge locations without changing impulse tubing, electrical connector & cabling on field side. Same form factor was maintained while designing the EDPIS units.
Electronic differential pressure transmitters are required to provide 4-20 mA signals as input to new PLC based Reactor Trip Logic System (RTLS). Processing of this signal & generation of low and high flow set-points as well as display information will be done by RTLS. Till RTLS is installed this instrument will generate contacts for Coolant Low Flow Trip and high flow alarm and EDPIS will act as differential pressure switch with local indication (*see FIG.2.*).

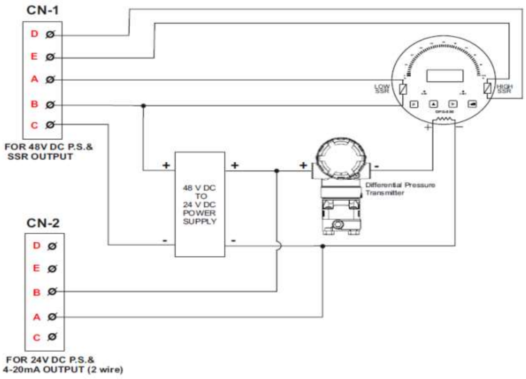


FIG.1. New EDPIS *FIG.2. Two connectors of EDPIS*

The EDPIS switches provides alarm contacts as well as current output & thus it can be used with existing Coolant Flow Monitoring System (CFMS) accepting contact input as well as new RTLS, which accepts current input.

2.2. Design Review, Qualification and Testing

A detailed design review of the micro-controller based hardware along with Verification & Validation (V&V) of the software has been carried out. EDPIS was also subjected to following type tests:

Failure Mode Effect Analysis (FMEA): As a part of hardware design review process, detailed FMEA was carried out for ensuring that failure of the hardware brings the instrument to failsafe state. The FMEA was carried out up to component level.

Software Verification & Validation (V &V): As the instrument uses microprocessor for performing important safety function, V&V of the software was carried out as per AERB safety guide D-25.

Climatic Test: The instruments are mounted in reactor hall which normally has a controlled environment at 25 °C with a relative humidity of around 50 %. But during ventilation shutdown condition, especially in summer the temperature can reach to 35 °C as well. It is estimated that maximum relative humidity can reach up to 90 % in the unlikely event of major heavy water/ process leakage. In view of these climatic conditions the instrument was subjected to Dry Heat (55 °C, 40% RH) & Damp Heat (40 °C, 95% RH) tests at as per IS-9000 Part V & IS-9000 Part III. The instrument was qualified in this test.

Radiated EMI Susceptibility test: There are no major EMI sources of inside reactor building, where the instruments are mounted. In view of this the test was carried out at as per IEC 61000-4-3, for frequency range of 80 to 2500 MHz and intensity of 1V/m. The instrument was qualified for radiated EMI susceptibility test.

Conducted EMI Susceptibility test: There are no major sources of high frequency EMI inside reactor hall. In view of this the test was carried out at as per IEC 61000-4-6, for frequency range of 150 kHz to 80 MHz and amplitude of 1Vpp. The instrument was qualified for conducted EMI susceptibility test.

Seismic testing: This test was carried out as per IEEE-344. Ground Response Spectrum (GRS) for the Trombay site was used as reference. Required Response Spectrum was obtained (RRS) from the GRS by considering the highest elevation & mounting arrangement for the instrument. A Test Response Spectrums (TRS) was prepared such that it envelopes the RRS for OBE & SSE conditions. The test instrument was subjected to 5 cycles of OBE level & 1 cycle of SSE level TRS. Duration of each cycle was 30 seconds & frequency range was 0.5 to 50 Hz. The instrument was kept energised during the tests & the outputs were being monitored. The integrity of the instrument was checked after each cycle and found to be qualifying.

Ingress protection (IP) Test: During installation & removal of the instrument there is a possibility of water jetting on the instrument. In view if this enclosure was designed for ingress protection class of IP-65. The type test was carried out as per IS: 13947 (Part-1)-1993 and the instrument was qualified for the IP test

Qualification Tests: Total 450 EDPIS units (396 for installation and remaining spares) were manufactured based on the satisfactory design review and type testing. Following acceptance tests were carried out on all the 450 units after manufacture:

- Burn test was carried out for 168 hours
- Over all dimensions and process connections checks
- Helium leak test at 1 kg/cm2 pressure
- Reverse Polarity Test
- Insulation resistance test at 100 VDC IR should be > 100 Mega Ohms
- Five point calibration check and set-point checking
- All the EDPIS units passed through the above mentioned tests.

Installation & commissioning of the EDPIS was carried out in a phased manner through an approved procedure (*see FIG.3.*).

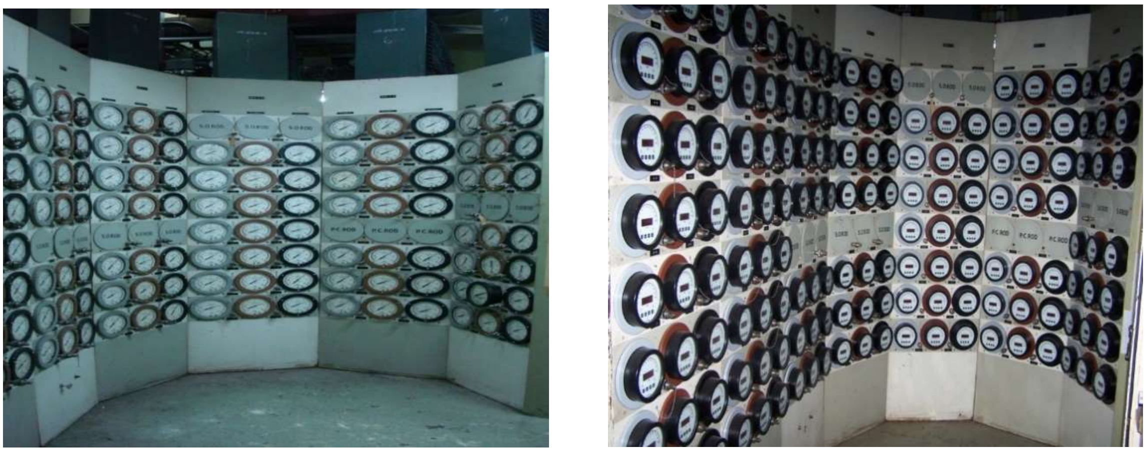


FIG.3. Old DP gauges were Upgraded with EDPIS units

3. UPGRADATION OF I&C SYSTEM USING PLC BASED SYSTEM

Safety Class IA & IB are upgraded with in house developed PLC based system.

3.1. Design Bases for PLC Based Systems

The design of the computer based PLC, is based on the new hardware, the design of which has evolved, based on the recommendations of a DAE committee for standardization of computer based hardware. The efforts at standardization addressed issues pertaining to long term availability in the face of obsolescence and technology denials, while ensuring safety. For the computer based systems incorporated in Dhruva, the hardware makes use of a “Power-PC” based SBC (single-board computer) along with Ethernet cards, on a VME bus architecture. A protocol converter, converts the signals from the VME bus to the I/O bus, for mounting the remaining cards, viz. analogue input cards, digital input cards, etc.

The system development primarily comprises of building a configurable PLC platform, which would remain common to all the systems. Appropriate application soft-wares, would then developed for each of the other systems, viz. RTLS, SULS, AAS.

3.2. Salient features of PLC Based system:

Design based on Systematic Development Process: The complete design and development is carried out following a Systematically Controlled well documented development process [3] based on AERB SG D25 and IEC60880-2.

Deterministic Performance: Control and Safety functions are executed in fixed time cycles in all load conditions.

Cycle time Estimate: Application Development can estimate the cycle time for an application project.

Robust Diagnostics: Diagnostics is carried out on input/output modules. Check on integrity of system software, application software and alterable parameters were also done. Health of hardware watchdog timer is checked. Health status is displayed.

Fail Safe Design: On detection of failure in input module, output module or system failure the Output is driven to failsafe state.

Cyber Safety & Access control: Software fully reviewed by V&V, no malicious code. Application software is stored in flash memory on processer board which in a secured area with access control. Access to online alterable parameter change needs pass word and hardware pass key. PLC is having only one way communication through Ethernet with Operator Console.

Simple design, Modular & Scalable: Simple user friendly Graphical User Interface. 19” rack mountable unit. Any combination of I/O module can be chosen and can be configured.

Built-in Diagnostics: All the in-house designed hardware modules have built-in fault detection features, viz. the digital input cards have Finite Impulse Test (FIT), analog input cards have test signals, digital output cards have read-back facility, etc. by which complete on-line diagnosis of the cards are possible.

3.3. Reactor Trip Logic System (RTLS):

This system caters to all the trips pertaining to Absolute Trip/ Conditional Trip (AT/CT) and the trips of the existing Coolant Channel Flow Trip (CLFT). One of the salient features of the RTLS [4], is conversion of the existing global coincidence logic scheme to a grouped local coincidence logic scheme. By this logic, the related protection system parameters, are grouped together. The coincidence logic philosophy provides global coincidence logic (between triplicate channels, A, B, & C) only within a particular group and local-coincidence logic among the different groups. Simultaneous annunciation of trip parameters in more than one channel (A, B, or C), for parameters located in separate groups, would not result in a reactor trip. (*see FIG.4., FIG.5. & FIG.6.*).

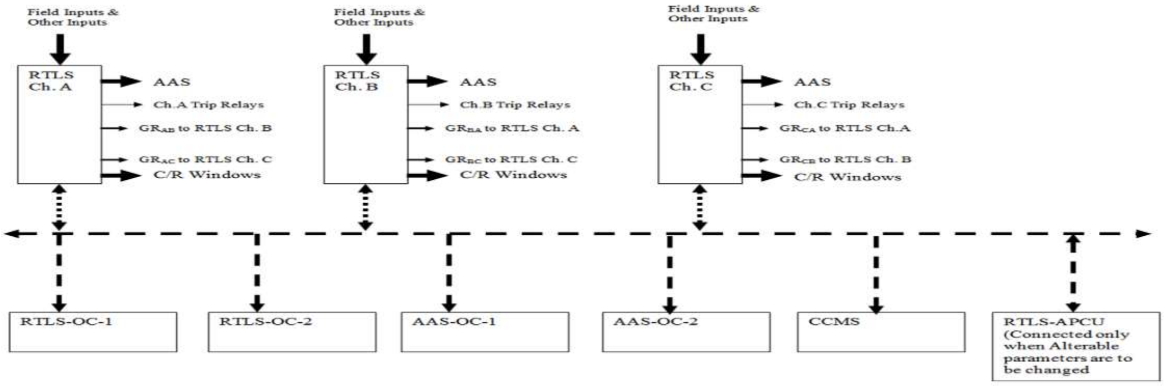


FIG.4. Schematic of RTLS using PLC

FIG.5. RTLS installation at Dhruva *FIG.6. Operator console for RTLS*

Further, unlike in the earlier system, where annunciation of trip and alarms are actuated from a common AAS, in new system all the alarms pertaining to the reactor trips are incorporated within the RTLS. This will avoid discrepancy in annunciation & actuation of trips. The main AAS only takes care of the plant alarms.

Other salient features of new RTLS are:

- Triple Redundancy
- Scanning of every input at every 20 ms with 3 validation cycles
- Process parameters directly as Analog Inputs to the RTLS
- Annunciation of trips in Main Control Room by RTLS itself
- Time stamping by PLC based system which helps in thorough analysis of events
- Extensive Self-Diagnostic capability
- Capability to synchronize the time with Central Clock
- Generation of un-validated event and displaying the same on Operator Consoles(OC)
- Redundant OCs over redundant Networks
- I/O Discordance generation by OCs
- Modular Hardware with hot pluggable I/O Modules

- High system reliability and availability

3.4. Upgradation of DHRUVA Alarm Annunciation System

The Alarm Annunciation System (AAS) in Dhruva consists of three independent channels, each channel being capable of receiving and displaying alarm status trip & alarm parameters. Each of the triplicated systems comprises of two 8085 microprocessor based microcomputer systems, one On-line and other as hot standby. A watchdog unit monitors the functioning of both the microcomputers and effects the changeover to the standby microcomputer, whenever the active system develops a fault. The conventional annunciator display windows are located in control room panels and have standard features like fast or slow flashing of lamps on parameter going to alarm or normal status, steady lamp after acknowledgment of the alarm status and a dual frequency common audio buzzer. For logging purposes, a single 8085 based system receives the data from the three channels of the AAS and displays parameter title, window location, time, changed status (alarm or normal) on a printer as well as on an intelligent colour CRT in control room.

3.5. Upgrade of Startup Logic System:

Single channel Start-Up Logic System (SULS) of Dhruva was upgraded with TPLC-32 based triplicated channel Start-Up Logic System. The system is developed on dual redundant LAN. A large number of contact multiplying relays and interconnecting wiring was removed which would result in better availability, reliability and maintainability. A number of hardwired interlocks were embedded in new SULS resulting in reduced complexity in wiring and ease in trouble-shooting. A large number of timer cards and time indicators were removed as these functionalities have been incorporated in SULS. Embedded Unit and SULS OC respectively. A large number of additional inputs, which were used in interlocks and alarm generation,

were brought to SULS directly for alarm & interlock generation as well as their continuous monitoring (*see FIG.7.*).

Advantages of TPLC-32 based SULS:

- Increased reliability, availability and maintainability due to triplicated channels.
- Enhanced reliability, availability and maintainability due to removal of contact multiplying relays and interconnecting wiring.
- Comprehensive diagnosis of hardware and software
- Easy trouble shooting due to embedding of interlocks into SULS which earlier were relay based.
- Information rich Operator Consoles for precise and crisp analysis of events.

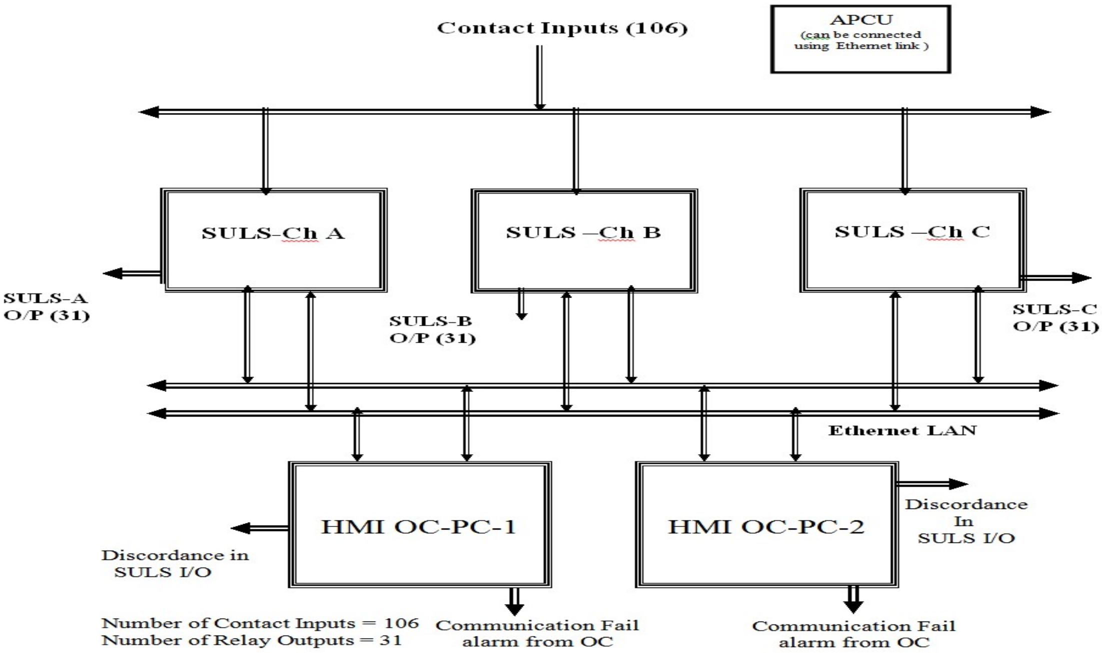


FIG.7. Block Diagram of SULS

3.6. Upgrade of Control room Alarm Annunciation System (AAS):

The AAS of Dhruva is a Safety Class IB system that is used for processing alarm inputs and alerting the Main Control Room operator by driving LED based windows and audio annunciation in the Main Control Room. The AAS is also used for sequencing and logging of alarms on Operator Console. (*see FIG.8.*).

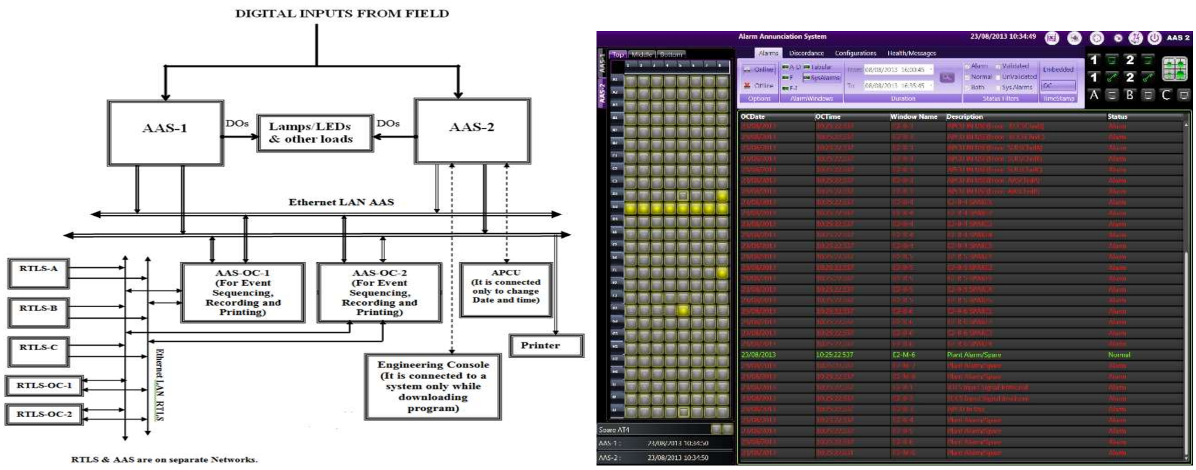


FIG.8. Block Diagram and OC of AAS

TPLC-32 based AAS consists of two computer based systems namely AAS-1 and AAS-2. It also has two redundant PC based Operator Consoles (OC). The two systems communicate with the OCs on dual redundant isolated Ethernet links. The inputs and outputs are connected in parallel to both the systems.

Salient Features of AAS:

- Dual Redundancy
- Scanning of every input at every 10 ms with 6 validation cycles
- Generation of un-validated event and displaying the same on Operator Consoles(OC)
- Time stamping by TPLC based system which helps in thorough analysis of events
- Ring back sequence with Lock-In for alarm annunciation
- Extensive Self-Diagnostic capability
- Dynamic Alarm generation capability
- Capability to synchronize the time with Central Clock
- Redundant OCs over redundant Networks
- I/O Discordance generation by OCs
- Modular Hardware with hot pluggable I/O Modules
- 99.92% Availability and 20000 hours of MTBF

3.7. Radiation Data Acquisition System

The Dhruva RADAS is a fully redundant system capable of monitoring 128 analog signals with a scan time of 1 second and on-line history of one-month. Dhruva-RADAS has two redundant Industrial PC based RADAS Units namely RADAS1 and RADAS2. Each unit performs the function of data acquisition and also acts as an operator console (HMI). Each RADAS unit consists of an industrial PC, four 32 channel (single ended) analog input data acquisition PC ADD-ON cards, one 64 channel digital I/O card and two 100Mbps Ethernet cards (see ***FIG.9.)***.

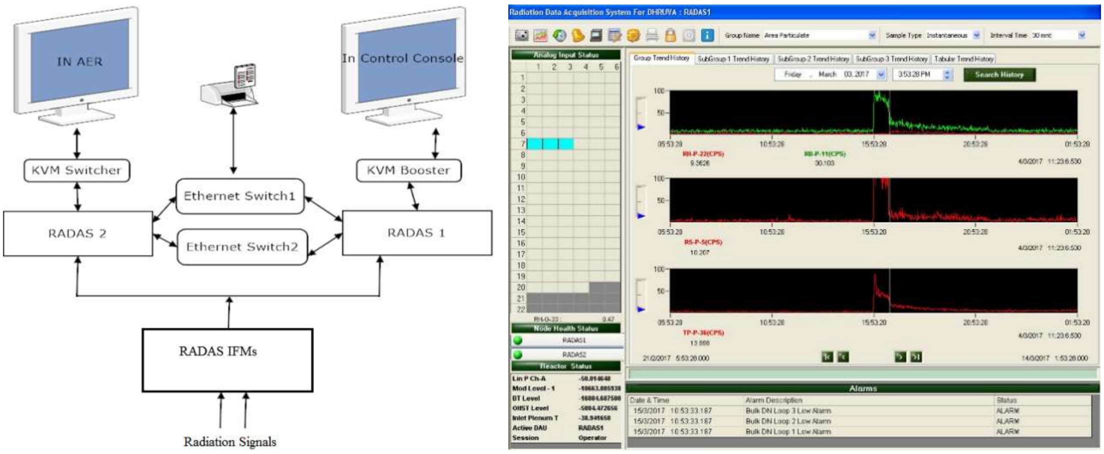


FIG.9. Block Diagram and OC of RADAS

Each RADAS unit scans all the RADAS signals (FFD REs, BCG, Bulk DN, Area Radiation Monitors etc.) once in a second. The display interval of the signals is programmable viz. 1, 10, 30, 60 seconds. If the display interval selection is more than the scan time (1 sec), the average/maximum/minimum/instantaneous of the scans can be selected and displayed on the screen. Both RADAS units exchange the scanned data among themselves for rationalization and if the scanned data differ by more than a certain value, a message indicating the disagreement is generated on OC. On power up, RADAS1 becomes active and RADAS2 remains in standby mode. Normally both the RADAS units scan the analog input signals. When active unit fails, standby unit becomes active. The active RADAS unit saves the scanned data in its database and also sends the scanned data to the standby unit. Standby unit saves the data received from the active unit. Both the units display the data (of the active unit) in a graphical & tabular format.

3.8. Reactor Regulating System - Data Acquisition System

In Dhruva, many parameters related to Reactor Regulating System (RRS) and Nuclear Channels were displayed in the control room on Chart Recorders. The maintenance of these recorders had become difficult for quite some time due to non-availability of spare parts. Also there was a need to record many additional parameters related to RRS, which were not covered by then recording system. In view of this, it was planned to replace these recorders by Digital Recording System. Reactor Regulating System and other Reactor Nuclear Parameters are upgraded by a PC Based system called as the RRS Data Acquisition System (RRS-DAS).

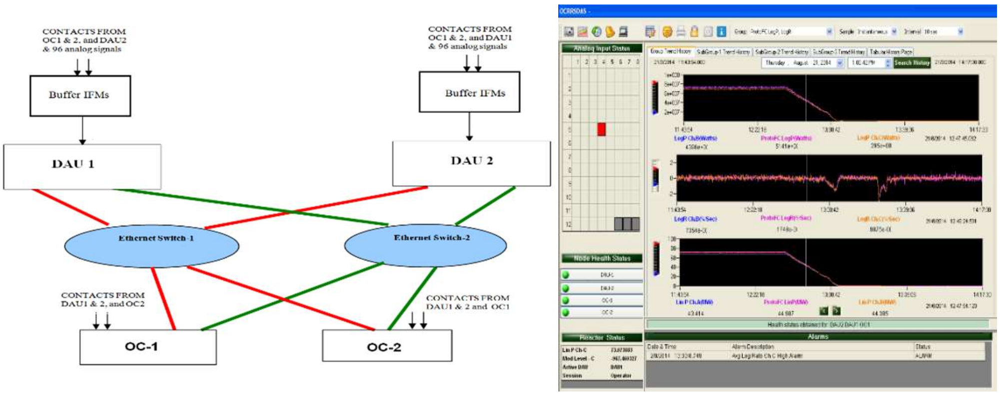


FIG.10. Block Diagram & Screen-shot of RRS-DAS

The RRS-DAS has two PC based Data Acquisition Units (DAU) (one active unit and the other standby unit) and two PC based Operator Consoles (OC) (*seeFIG.10.)*. Each DAU consists of an industrial PC, three 32 channel (single ended) data acquisition PC ADD-ON cards, one 64 channel digital I/O card, two 100Mbps Ethernet cards and one relay card. Each DAU scans the RRSDAS signals once in 100 milliseconds and the active DAU sends the raw data to the OCs through redundant Ethernet links. Each OC consists of an industrial PC, one 64 channel digital I/O card, three 100Mbps Ethernet cards and one relay card. The OCs receive the data from the active DAU, organizes into a record structure and stores the data in the hard disk and displays the data in a graphical & tabular format. On failure of the active DAU, the OCs receive the data from the standby DAU automatically. The DAUs & OCs alternate their roles from active to standby and vice versa periodically. The Trip/Alarm level for selected group of parameters was provided, in the graphical as well as tabular modes of operation, wherever applicable. The configuration files for engineering units conversion resides on DAUs as well as RRSDAS OCs. RRSDAS OCs stores the data in SQL server database for future retrieval.

3.9. Upgrade of Fire Alarm Data Acquisition System (FADAS)

The earlier Fire Alarm System in Dhruva consists of 187 Ionisation type detectors, 27 Photo Electric Type detectors, 21 heat detectors, 11 Flame detectors and 27 manual Call Points distributed over 12 Local Indication Panels (LIP). The detectors are grouped into 26 groups depending on their location and the group indication from each LIP is available in the Main Control Panel (MCP) and in the fire alarm system matrix indication in Control Room. The 26 groups are distributed over different LIPs. The main disadvantage of the system was that whenever a fire alarm registers in the control room due to actual fire sensed by any detector or fault in the detector/card (which is not a short or open fault), subsequent alarms generated by others detectors would not generate any alarm in the Control Room. Most of the hardware components used in the design of the system had become obsolete.

Hence a new system called the Dhruva Fire Alarm Data Acquisition System (Dhruva-FADAS) was developed retaining the existing fire alarm detectors. The new Fire Alarm Data Acquisition System (FADAS) has two redundant PC and 4 Local Indication Panels (LIPs) namely LIP-A, LIP-B, LIP-C and LIP-D. Each LIP consist of a no. of 8 channel analog input modules (ADAM-4017), one 16 channel Digital I/O Module (ADAM-4055) and one relay Interface module, two Moxa Device Server Modules mounted inside the respective LIPs, three LED Indications and one Reset Button (*see **FIG.11***.).

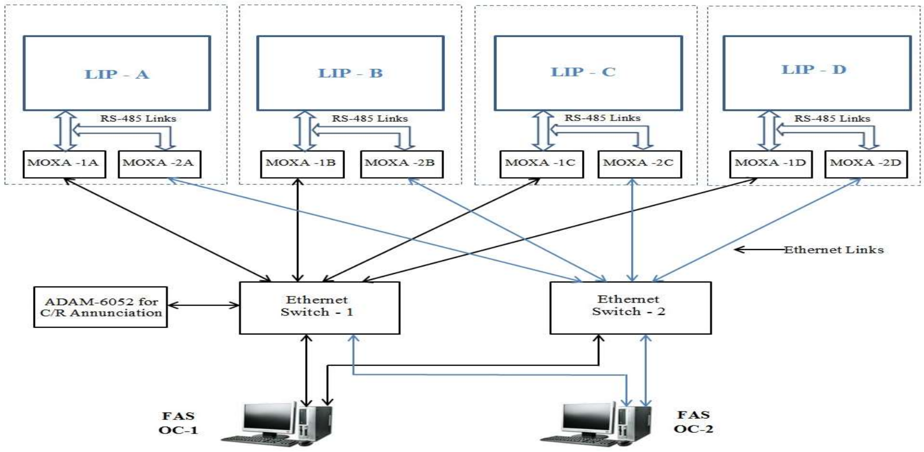


FIG.11. Block Diagram of FADAS

FADAS OCs have one Ethernet based Digital I/O module with relay board for alarm generation. Normally FADAS-OC1 remains active and FADAS-OC2 remains standby. The active FADAS OC scans the status of each ADAM module through Ethernet links, stores the data, compares the data with set point and generates an alarm when it crosses the set point. There are three set points namely Very High, Low and Very Low. When the active OC fails, then the standby OC becomes Active. There are three dynamic alarms generated from this system namely Fire Alarm in Group1, Fire Alarm in Group2 and FADAS off-normal.

4. CONCLUSION:

Significant upgradations have been implemented in the C & I Systems in Dhruva reactors, by either modifying the old systems or incorporating new systems, based on computer based systems and digital recorders. Availability of system increased and the associated maintenance is reduced to a large extent. The HMI and Operator interface has also improved to a great extent with more information, trending analysis available with operator.
Based on this C & I Upgradation in Dhruva, the future research reactor C & I design will see more of such type of systems.

Acknowledgments: We acknowledge the efforts and dedication of developers, designers, reviewers of BARC during various stages of the system development and commissioning.

References

[1] Upgrade of Dhruva Fuel Channel Flow Instrumentation: SACI-2014, BARC: Kaustubh Gadgil, P.K.Awale, C.Sengupta, P.Sumanth, Kallol Roy

[2] AERB Safety Guide AERB/NPP-PHWR/SG/D-25 Computer Based Systems of Pressurised Heavy Water Reactors.

[3] Report No. : BARC/2012/I/015: Trombay Programmable Logic Controller TPLC - 32 platform Salient Features and Specifications: U.W. Vaidya, G. Ganesh, B.B. Biswas, R.K. Patil- Electronics & Instrumentation Group.
[4] Trombay Programmable Logic Controller-32 (TPLC-32) Based Reactor Trip Logic System (RTLS) for Absolute Trips (ATs) and Conditional Trips (CTs) of Dhruva Research Reactor: DAE VIE 2016, IGCAR : N.Ramkumar et. al

MODERNIZATION AND REFURBISHMENT OF INSTRUMENTAION AND CONTROL SYSTEM OF TEHRAN RESEARCH REACTOR (TRR)

A.Ezati – A.H. Tajbakhsh
Reactor and Nuclear Safety Research School
Nuclear Science and Technology Research Institute,
Atomic Energy Organization of IRAN
aezati@aeoi.org.ir

Abstract: The Tehran Research Reactor was commissioned in 1965 at a power level of 5 MW. The reactor was originally designed for HEU fuel with 93% enrichment in the form of UAL_X-Al. The reactor control system remained unchanged since1979. However, several factors, including obsolescence of equipment and the non-availability of spare parts, forced a refurbishment program. For this purpose, development of a new and modern instrumentation to replace old transistor-based instrumentation and control system was started.
The desirable features of the existing instrumentation were retained, while others were modified, improved, and to ensure safe and reliable operation of the reactor. The control system was commissioned in November 2014 to make preparations for the transition from the old console to a new one. All archived parameters were compared with the existing system. Initial tests and measurements indicated that various systems of the reactor control system were conducted according to the designed specifications and most of the experimental results were in line with the theoretical design. The major part of TRR control system was refurbished. Specifications of the remaining parts (neutron detectors) were obtained which makes the renovation path smoother.

1. INTRODUCTION

The Tehran University Atomic Centre was founded in 1956. Two years later the nuclear research Centre established in an area almost 36 hectar in the university campus in Amir Abad district. The construction of a pool-type research reactor and corresponding laboratories completed in 1967 by AMF-Atomics. The first criticality of the TRR was achieved in Nov. 1967. The initial fuel of the TRR was 93% enriched uranium (HEU). In 1993 the core conversion project was carried out with corporation of INVAP from Argentina. The fuel converted into 19.99% enriched uranium (LEU).

The original I&C system was based on the old thermionic tube instruments. Although In 1978 under the agreement between Atomic Energy Organization of IRAN and General Atomic from USA, a project for changing the TRR to TRIGA reactor started, they just changed the I&C system to transistor Type and other issues were suspended. During the operation several monitoring were added to control system.

2. OBJECTIVES AND SCOPE OF MODERNIZATION OF THE I&C SYSTEM

Due to the aging, several factors forced the facility to take up a renewal program for I&C. These factors included:

a. The non-availability of spare parts, obsolescence of equipment, Problem for maintenance and repair,
b. Non compatible with new technology ,
c. Not cover new requirement and
d. New experiment.
e. Reactor had to be shutdown whenever any of the neutron power monitoring channels became unavailable.

f. Because of the amplification of noise, too many spurious scrams (shutdown) were experienced during the start up.
g. Process instrumentation was generally found to be inadequate as well as area radiation monitors.

It was proposed that the instrumentation and controls (I&C) system be modernized according to the current technology and to meet the current stringent safety and operation needs. The instrumentation needs were reassessed taking into account feedback from long time operation history, monitoring more parameters, and increasing the accuracy of display parameters to be measured and the new experiment. All components of I&C system including sensors and transmitters, cables, junction boxes, control console and cabinets, actuator and rod driver were subjected to refurbishment program.

3. REFURBISHMENT AND MODERNIZATION OF INSTRUMENTATION AND CONTROL SYSTEM PROJECT

In early 2010, the reactor instrumentation development program began to take up renovation of the I&C system of the TRR. The old system had obsolete and was posing operation problems as well as problems in repair and maintenance. The desirable features of the existing instrumentation were retained, while others improved to ensure safe and reliable operation of the reactor. The entire design was based on the principles of fail-safe, redundancy and diversity [1].

The Program was divided in 6 phases:

1. Initiation phase
2. Definition phase
3. Design phase
4. Development phase
5. Implementation phase
6. Follow-up phase

A state-of-the-art instrumentation and control system using DCS technology provides replacement of older, existing instrumentation and control systems that contain obsolete components. Increased flexibility, higher availability, and lower maintenance costs are only a few of the good reasons to convert to this system. Our features include:

1. Elimination of most manual data logging.
2. Provides automatic and manual reactor operation mode.
3. Provides complete real-time operator display.
4. Replays full history of historical operating data on monitors or printers.
5. Eliminates parts replacement problems.
6. Meet all applicable national standards and specifications

The complete system consists of three major subsystems-the process sensors and Detectors System, the Data Acquisition and Signal conditioning System, and the Control Console and signal processing system. The Signal Processing and Control Console System each have independent computers (EWS and OWS) for monitoring and control purposes. The Data Acquisition and Signal Processing System include the hot redundant equipment. The combination of FPGA and SSR technology are used for voting (safety scram and shutdown circuits).

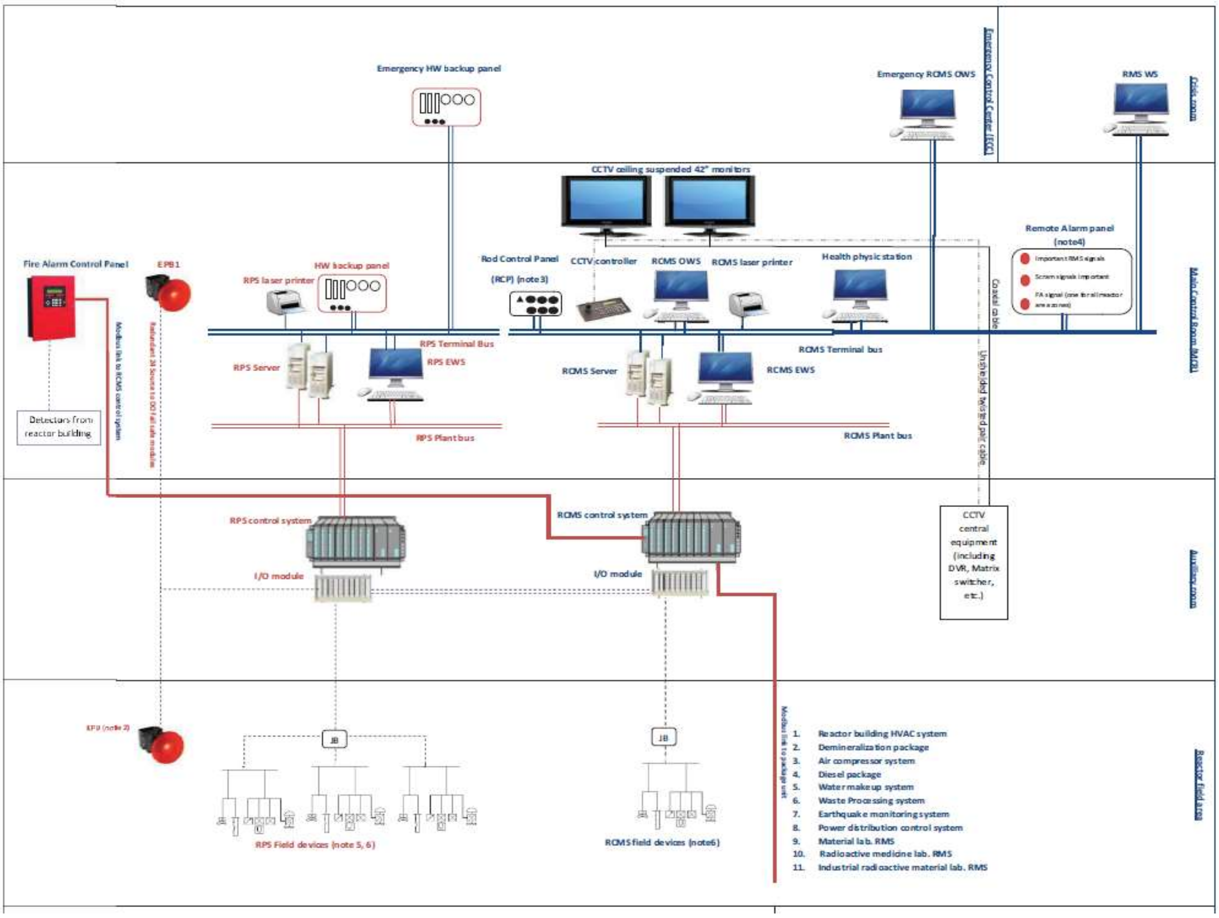


Fig. 1: Simplified Control System Block Diagram

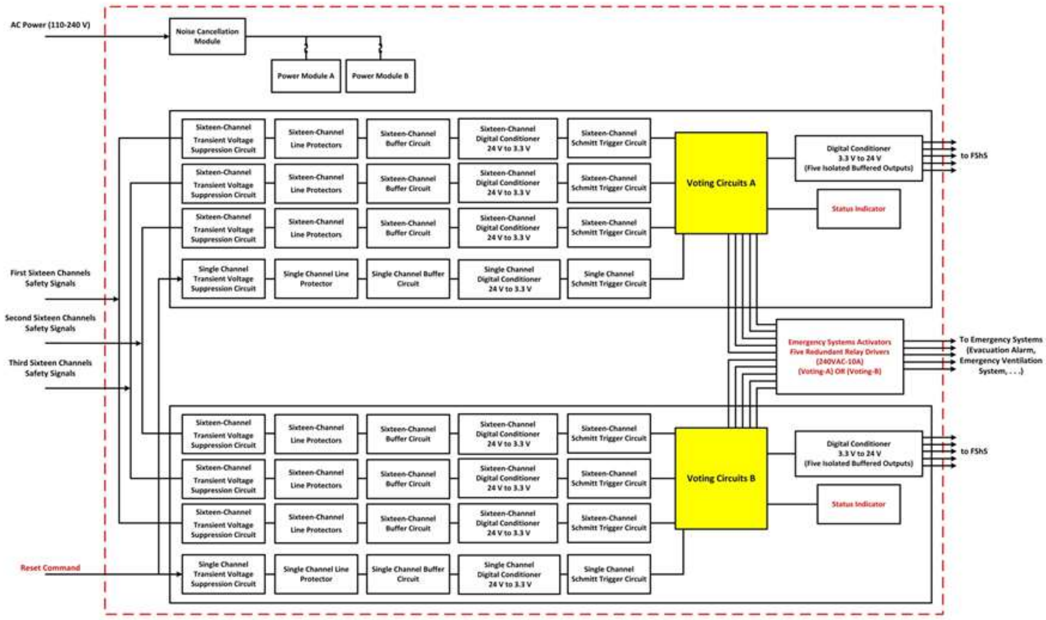


Fig. 2: Reactor Protection System block diagram

Fig. 3 Control rod console

Information on all aspects of reactor operation is displayed on the Control Console System. The three color graphic monitors can display real-time operation data in concise, accurate, and easily understood formats. Bar graph indicators and visual and audible annunciators are also provided. The information displayed on the three monitors can be recorded on the hard copy by using the graphic printers in the Control Console System. The DAC collects data during reactor operations and stores it in a historical database. The Reactor operations can then be replayed in real-time or slow motion. This record is a powerful tool that can be used for operations review and maintenance troubleshooting.

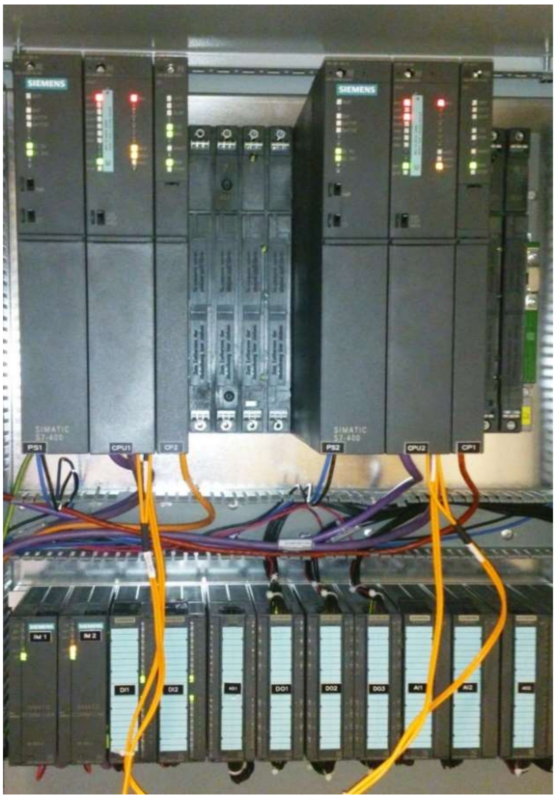


Fig. 4 Data Acquisition and Signal Processing System

Reactor control rod position commands are transmitted via a high-speed Ethernet link from the Control Console System to the Data Acquisition and Signal Processing System and in turn to the rod drive mechanisms. This reduces the complexity, vulnerability, and cost of data transfer. The Data Acquisition and Signal Processing System computer controls rod positions using integral software during automatic mode operation.

The WRLC provide power indication. The WRLC can measure reactor power from source to full power range and provide wide range log power and period. The MRPA provides multi-range linear power in to 8 decade. The analogue safety channels (SCs) monitors' percent power. These channels determine power or source mode of reactor operation and also send a signal for interlocks.

3.1. Safety Features

The three independent, redundant percent power safety channels are provided to ensure safe operation of the reactor. These channels are designed to meet all applicable specifications and also have automatic pre-startup on-line self-diagnostic/testing and calibration verification with data display and documentation printout. They also have isolated outputs for display and safety scram circuit inputs. Redundancy and diverse designs ensure against reactor instrumentation and control system common mode failure. Safety/scram circuits are also hardwired to voting inputs.

3.2. Data Display and Storage

Three color monitors provide real-time information, one shows reactor operations graphics and the other displays important operating parameters. Hard copies of the displays can be made using the graphics printer. All reactor data can be display in left monitor according to location on 8 HMI pages that make easy understanding of reactor status for operator and avoid operator data overloading.

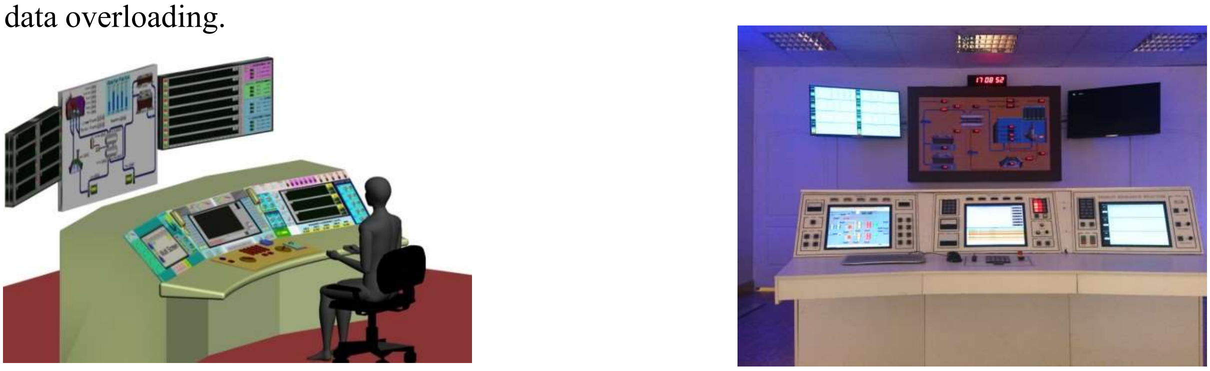


Fig. 5 Control console

3.3 Control rod driver

The following figures represent a system block diagram. A central core is a FPGA base digital controller. This system implemented on the hardware base electronic boards, and then it has high reliability. Thank to mechanism characteristics, Operators can control RODs with high accuracy. Furthermore using the FPGA causes good access and control on I/Os. Reg. ROD control is located in one unit and four other RODs are located in two units.

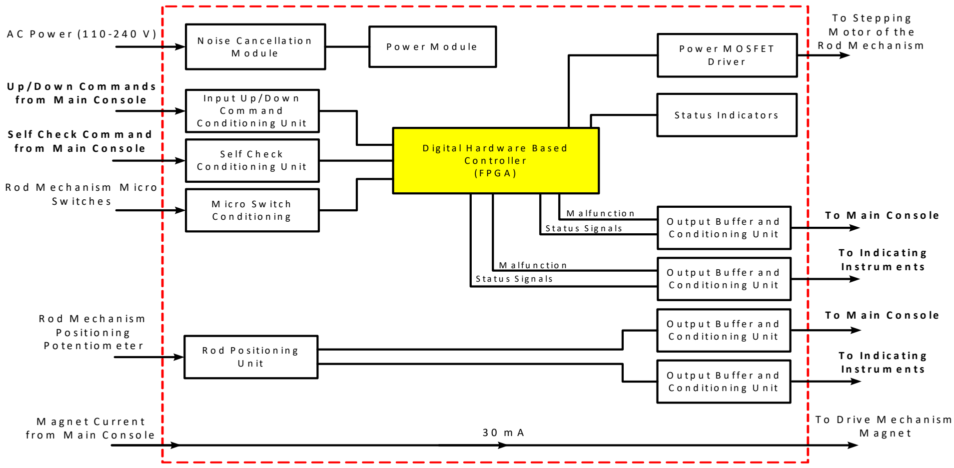


Fig. 6 System block diagram

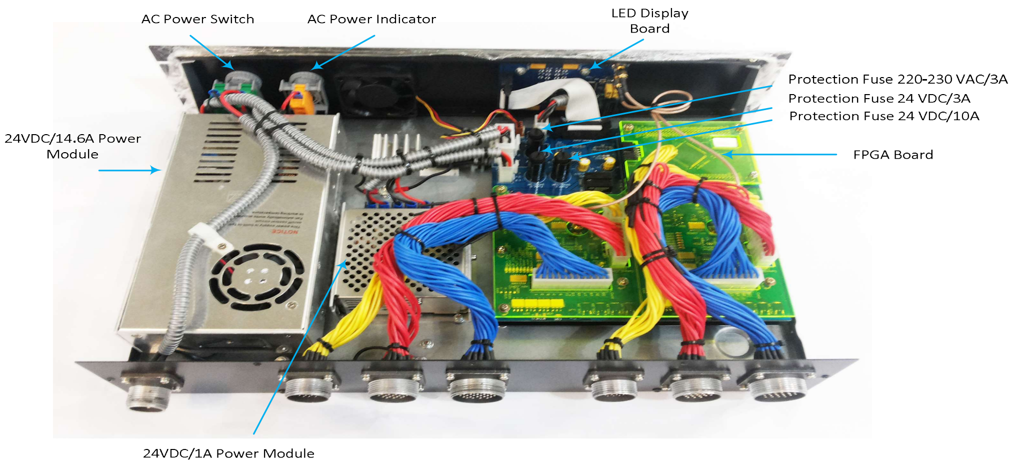


Fig. 7 FPGA base digital controller

4. COMMISSIONING OF NEW I&C

Non-nuclear part of the control system was decommissioned in November 2014 to make preparations for the transition from old console to new one. All archived parameter were compared with existing system. Initial tests and measurements indicated that various systems of the reactor control system performed according to the design specifications and most of the experimental results were in agreement with the theoretical design. After that the buffered signals from old neurotic instrument consist of two UICs and one CIC and a fission chamber feed to new control system.

5. LESSONS LEARNED

The difficulties during and after project led to very important lessons:

a) If economically possible the best choice is refurbishing all at once instead of separately and gradually replacement of system during long time.
b) Before taking up any activities, the prerequisites must be very carefully considered. Discussion among the experienced personnel and careful planning is essential before starting off the project.
c) Every work that carried out on I&C system should be recorded for future improvements of system. Especially the tacit knowledge of long timer expert should be converted to report.
d) Neutron detector was the stumbling block to finish the project.
e) Because of unique nature and low frequency project for national contractor it is better to done with the collaboration of international fame company.
f) Record keeping of reactor parameter in various environmental condition and seasons smooth the way of verifying activity for new system.
g) Operating personnel could participate in project to be able solve problems during reactor operation, especially in shift working.
h) All activities carried out should be properly documented for future use.

6. CONCLUSION

The renovation work comprised a review of I&C system needs in light of the latest design practices in the field. As a result, a revised I&C configuration and logic was worked out. The I&C system was completely designed with industrial PLC. The standard criteria for single failures — fail-safe design, redundancy, diversity, and channel independence were incorporated to the extent that they were feasible.

The new instrumentation was designed so that all probable accidents and initiating parameters were reliably covered. A number of channels were duplicated and a few new channels were added such as N16, Cherenkov power indicator channels. All of the process instrumentation such as secondary flow measuring channels, vibration sensor for main rotating component, etc. was increased to improve redundancy and diversity. The scope of radiation measurement and monitoring was extended. A new CCTV system was installed for the surveillance of the building and reactor operations. Communication within the building and outside was improved.

The new I&C system divided in tow category, Nuclear and non-nuclear. Non-nuclear and nuclear parts except neutron detectors were installed in 2014 and have performed very well. The procured instruments and developed modules and channels were first assembled and tested in the laboratory with signal sources. The instrument channels were then tested under actual operating conditions and their performance compared with the old channels. Comparison of archived data with old control system show that system worked correctly and precisely. Safety systems set point limits and interlocks were kept according to the old instrumentation and the OLCs for domestic fuel. However, scram for the core temperature difference was also provided.

The major part of TRR control system refurbished. Specifications of the remaining parts (neutron detectors) were obtained which makes the renovation path smoother.

REFERENCES

[1] S.M Mirvakili and et al, technical report for design and construction of new control room for Tehran Research Reactor 2014, NSTRI, AEOI.

HOME-MADE REFURBISHMENT OF THE INSTRUMENTATION AND CONTROL SYSTEM OF THE TRIGA REACTOR OF THE UNIVERSITY OF PAVIA

A. BORIO DI TIGLIOLE*, M. CAGNAZZO*, G. MAGROTTI*, S. MANERA*, A. SALVINI*, G. MUSITELLI**, R. NARDÒ**
TRIGA Reactor of University of Pavia
27100 Pavia, Italy
*Laboratorio Energia Nucleare Applicata (L.E.N.A.)
**Theoretical and Nuclear Physics Department

1. INTRODUCTION

The Instrumentation and Control (I&C) System of the TRIGA reactor of the University of Pavia was dated (see Fig.1) and, in order to grant safe and continuous reactor operation for the future, it became necessary to substitute or to upgrade the system. Since the substitution of the I&C system with a newly made one was very difficult due to long authorization procedures, a homemade refurbishment was planned. Using commercial components of high quality, an almost complete substitution, channel-by-channel, of the I&C system was realized without changing the operating and safety logics (see Fig. 2). The refurbished I&C system shows very good operational behavior and reliability and will assure a continuous operation of the reactor for the future.

FIG. 1. The old I&C system.

FIG. 2. The refurbished I&C system.

2. REACTOR LINEAR POWER CHANNEL AND CHART RECORDER

The Linear Power channel provides the measure of the reactor power from source level (about 10 mW) to nominal power (250 kW). It is made of a compensated ion chamber, a current amplifier, a power range selector and a chart recorder (see Fig. 3).

The output current coming from the chamber (ranging from few pA at source power up to 1 mA at nominal power) is amplified by a low noise linear current amplifier and then processed by a multi-scale selector which provides the input to the digital chart recorder. The input range of the digital recorder is 0 ÷ 10 mV DC and the conversion current-to-voltage is made by the range selector through a high precision resistor bridge.

The new recorder installed is a *Honeywell DPR 250* (see Fig.5) which is able to monitor up to 64 analogue inputs or any combination of analogue inputs, digital inputs and outputs up to a total of 80. It also provides 48 static and electro-mechanic output relays.

The reactor power level is read every 100 milliseconds and it is continuously shown on a digital display and printed on a 10 scale range chart. The zero and span check are tested manually by the operator using the range selector. The recorder set up parameter values are periodically printed on chart. Data are also stored in a removable compact memory card mounted on the recorder.

In order to maintain the same SCRAM logic, an output relay operates whenever the input signal reaches the value of 100% of each scale range (i.e. the voltage of 10 mV). The output relay opens the SCRAM loop, automatically causing the drop of the control rods inside the reactor core.

The recorder input signal is also replicated, through a dedicated analogue output board, in order to provide 4 ÷ 20 mA reference signal for the automatic reactor power control (i.e. the regulating rod automatic drive system).

The recorder also displays and prints on a chart the reactor power level output of the Logarithmic channel.

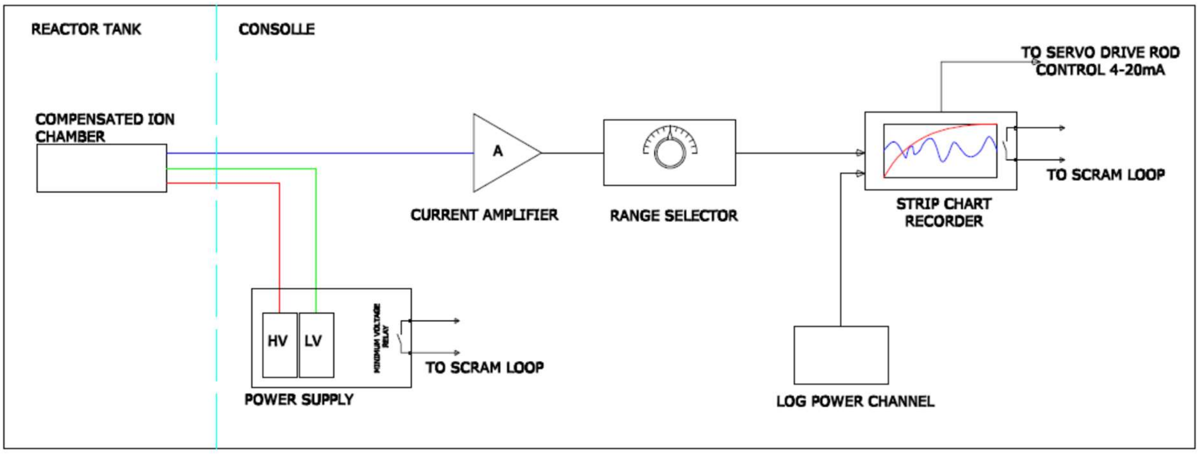


FIG. 3. Linear power channel lay-out.

FIG. 4. Old linear power chart recorder.

FIG.5. New linear power chart recorder.

3. REACTOR PERCENT POWER SAFETY CHANNEL

The Percent Power Channel measures the reactor power in percent units of the nominal power value of 250 kW (0% ÷ 100%) and it is used also for safety purpose (see Fig.6). The channel is connected with a non-compensated ion chamber which gives an output current ranging from pA up to µA. The channel amplifier is a *FEMTO HCA-2M-1M-C* ultra low noise linear amplifier which provides a 10^6 A/V gain. The amplifier is placed close to the signal source to avoid signal degradation due to cable capacity and noise pickup. This amplifier is especially designed for sensitive current measurements in the pico to femto ampere range. An additional amplifier stage with a variable voltage gain of x1 and x10 was added to offer greater flexibility for different applications and signal amplitudes. Signal changes can be monitored with a rise time down to 200 ms.

The amplifier output is processed and displayed by a high performance process meter *Endress+Hauser RIA-452*, with a relay connected to the SCRAM loop (see Fig.8). The relay is activated when the 110% of the reactor nominal power of 250 kW is measured. An external circuit is implemented in order to periodically test the functionality of the SCRAM relay.

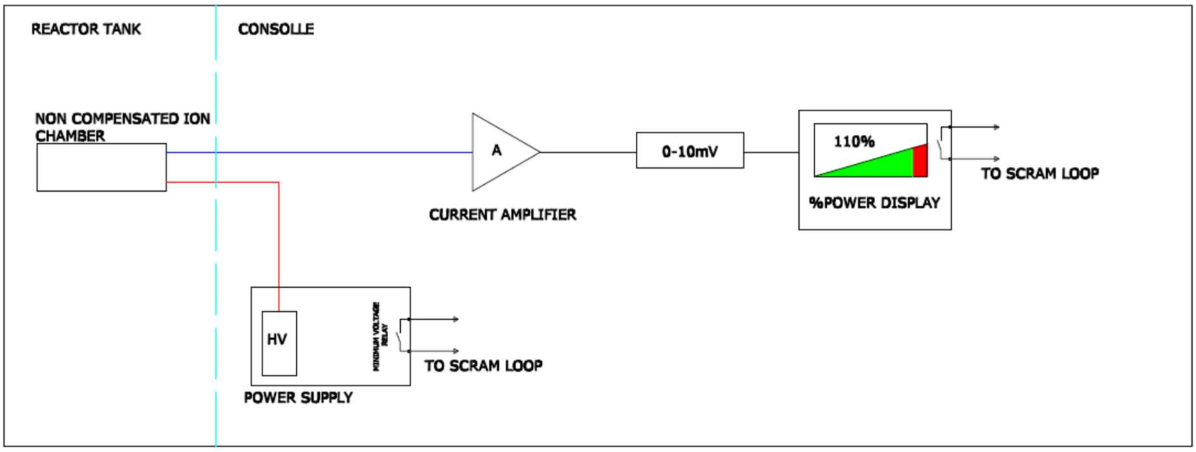


FIG. 6. Percent power channel lay-out.

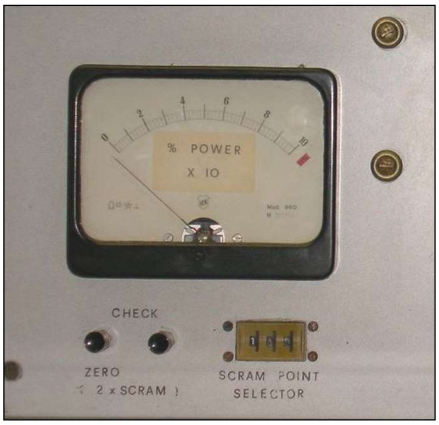


FIG. 7. Old percent power channel and SCRAM test circuit.

FIG. 8. New percent power channel and SCRAM test circuit.

4. HIGH VOLTAGE AND LOW VOLTAGE POWER SUPPLY.

The high voltage power supply *Bertan 602C10P* provides high DC voltage (700 ÷ 1000 Volt DC) to the ion chambers of the reactor power measuring channels (see Fig.10). There are three high voltage supply channels (one for the compensated ion chamber of the Linear Power channel, one for the non-compensated ion chamber of the percent power channel and a spare power supply as a backup). The power supply of the fission chamber of the logarithmic power channel is provided directly by the original GA-NLW unit. There is also a low voltage power supply *Lamba Cotand HBS24-1,2LF* (0 ÷ 50 Volt DC) used for the compensation of the chamber of the linear power channel. All the power supplies provide are specifically developed for nuclear instruments purposes.

The output voltage of each power supply is controlled locally by an internal multi-turn potentiometer. Remote analogue voltage or resistance programming capability is included and allows the operator to modify precisely the output according with the ion chamber specification in order to obtain the best performance. Analogue monitor outputs are also included for remote monitoring of both voltage and current outputs.

All the supply units are connected, via a voltage relay, to the SCRAM loop. The relays operate on the event of an output voltage failure. An external circuit is implemented in order to periodically test the functionality of the SCRAM relays.

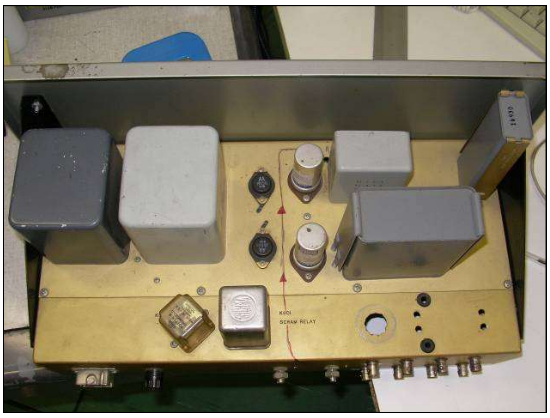


FIG. 9. Old power supply chassis.

FIG.10. New power supply chassis.

5. AUTOMATIC REACTOR POWER CONTROL

The Automatic Reactor Power Control provides the automatic regulation of the position of the regulating control rod, in order to maintain the power level at the desired value set manually by the operator (see Fig.11). The controller is a microprocessor PID *GEFRAN 1800* (see Fig.13). The instrument provides a complete operator interface, with keys, LED displays, and output relays. The main input for the process variable is universal and provides the possibility to connect many types of input sensor. In our case the main input is the reactor power level provided by the chart recorder of the linear power channel described in §.2. A second auxiliary isolated analogue input is available, which can also be configured for a linear input, potentiometer or current transformer. In our case the second input is used as a remote set point.

The controller actuates two output relays operating the regulating rod motor drive: one in insertion and one in extraction. A selector allows shifting to manual operation, excluding the power control unit.

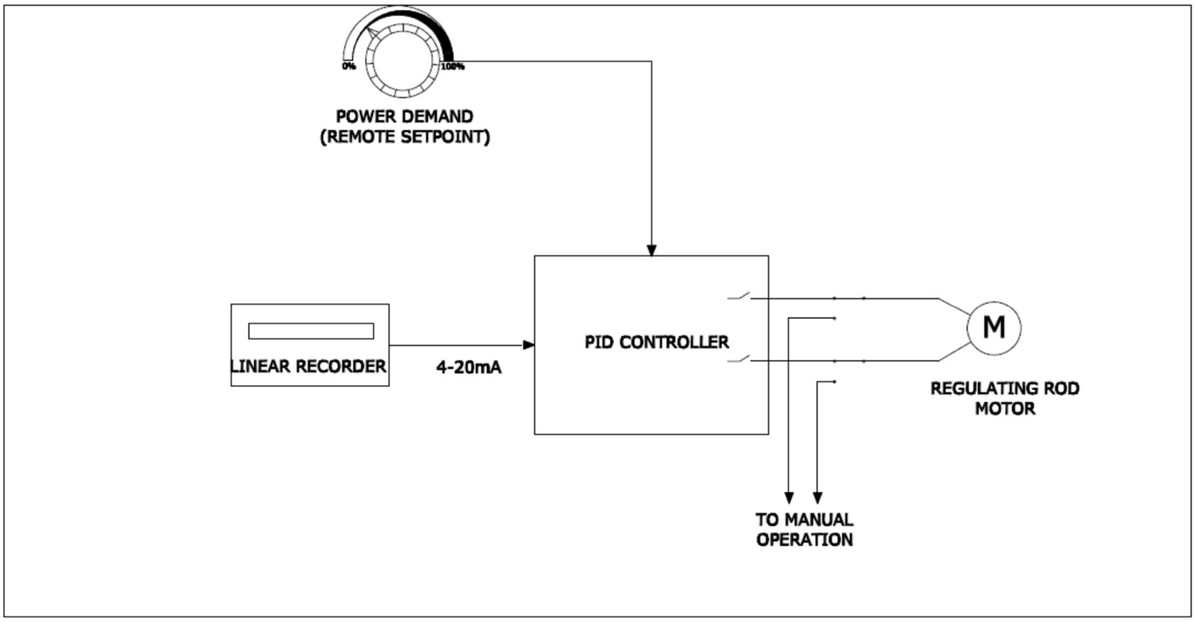


FIG.11. Automatic reactor power control lay-out.

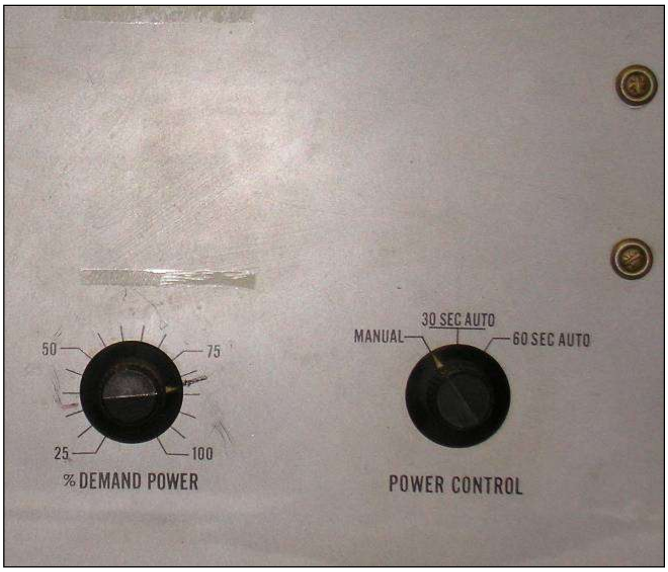


FIG. 12. Old automatic reactor power control.

FIG. 13. New automatic reactor power control.

6. FUEL ELEMENTS AND COOLING-WATER TEMPERATURES MEASURING CHANNELS.

The purpose of these channels is to measure and display fuel elements and cooling-water temperatures during the reactor operation. Fuel temperature signals come from 6 different type K thermocouples placed in the instrumented elements positioned in the B ring of the reactor core. Reactor cooling-water temperature is measured by a PT100 thermo-resistance placed in the reactor primary cooling system just before the primary/secondary circuit heat exchanger.

The single-channel process display unit *Endress+Hauser RIA-452* monitors and displays analog measured values (see Fig.15). The measured value is displayed using the seven-digit 14-segment LC display with a resolution of 0.1°C. The instrument displays numbers and units, the 0% ÷ 100% bar graph, the limit value flags and digital inputs status. Up to 8 freely programmable relays monitor the measured value for limit value overshoot and undershoot. Other operating modes for the relays include sensor or device malfunction. The scalable analogue output offers many different ways of forwarding the input signal: zoom function, linearisation, offset, inversion and signal conversion (input/output conversion).

The analogue measured value acquisition takes place via an analog/digital converter. The digital status inputs are scanned cyclically.

Only the fuel temperature measurement has an output relay configured in order to open the SCRAM loop whenever the temperature reaches the maximum level set at 400°C. An external circuit is implemented in order to periodically test the functionality of the SCRAM relay.

The cooling-water temperature meter activates an output relay connected to an acoustic alarm whenever the water temperature exceeds the value of 50°C.

FIG. 14. Old fuel elements temperature channel.

FIG. 15. New fuel elements and cooling-water temperature channels.

7. WATER CONDUCTIVITY MEASURING CHANNEL.

The water conductivity channel monitors the water conductivity across the ion exchange resins of the primary cooling circuit. The channel is made of two different low conductivity cells mounted across the resins and two instruments for processing and display data *Endress+Hauser Liquisys M CLM223/253* (see Fig.17). The transmitter can be equipped with additional software and hardware modules for special applications. The instrument also provides a water temperature compensation for higher accuracy measurement. These instruments are not connected with the SCRAM loop.

FIG. 16. Old water conductivity monitor.

FIG. 17. New water conductivity monitor.

INSTRUMENTATION AND CONTROL SYSTEMS OF RSE NNC RK REACTOR FACILITIES

A. KOROVIKOV, V. YERMAKOV, B. SERIKBAYEV
National Nuclear Center of the Republic of Kazakhstan, Department of Automation of Control and Management Systems, Republic of Kazakhstan

Abstract

Currently in Kazakhstan there is one energy and four research reactors. Research reactor WWR-K is located in Alatau village, not far from Almaty city at the Institute of Nuclear Physic. Other three Kazakhstani research reactors IGR, IVG.1M and RA are placed at the former Semipalatinsk Nuclear Test Site (SNTS) near Kurchatov town at National Nuclear Center of RK. IVG.1M reactor power start-up was conducted in 1975. RA research reactor was created on the basis of bench prototype construction NRE and put into operation in 1987. The reactor has been used for different testing on NRE creation program up to 1997 and in 1998 in accordance with government agreement the fuel was extracted out of reactor and transferred to Russian Federation. The CRR IGR was created in 1961. In 2008, we started the work on complex upgrading of I&C system of IVG.1M reactor. It was developed technical project that includes Process Equipment Automatic Control System Monitoring Subsystem, Control and Protection System Parameters Monitoring Subsystem, Technological Parameters Monitoring Subsystem, Coolant activity Monitoring Subsystem, Radiation Monitoring Subsystem. Designed system consists of three levels (controllers, engineering workstations, stations of the operators). Currently upgrading was partially performed, equipment were gained and installed. Modernization is carried out of the funds of the Republic of Kazakhstan and the technical cooperation program with IAEA.

1. ANALYSIS OF EXISTING INSTRUMENTATION AND CONTROL SYSTEMS

The hardware complexes, which were worn out physically and morally and systematically organized using equally obsolete software, are used as technical means of computer systems for instrumentation and control systems (I&C system) of reactor plants. For example, I&C system of the IVG.1M reactor is constructed using terminals based on 16-bit machines: an interactive computer complex, an aggregate system of computer facilities (ASVT-M), a computer communication terminal with an object (SM- 1634) - a family of Soviet personal computers in the mid-80s - early 90s of the XX century (Figure 1). As an operating system, an aggregate software system is used. This equipment is a set of constructive with a height of 2 m and occupying an area of about 450 m^2. The amount of RAM of each computer is only 128 KB; information is recorded on tape drives. The main method of data display to operator screens is a monochrome alphanumeric method without graphical mode. With the passage of time, the issue of further exploitation of this equipment is became critical, as the number of spare parts for restoring the operability of the main equipment as well as the amount of maintenance personnel are reduced that can eliminate the problems that have arisen. I&C system of the IGR reactor is also based on outdated equipment (Figure 2).

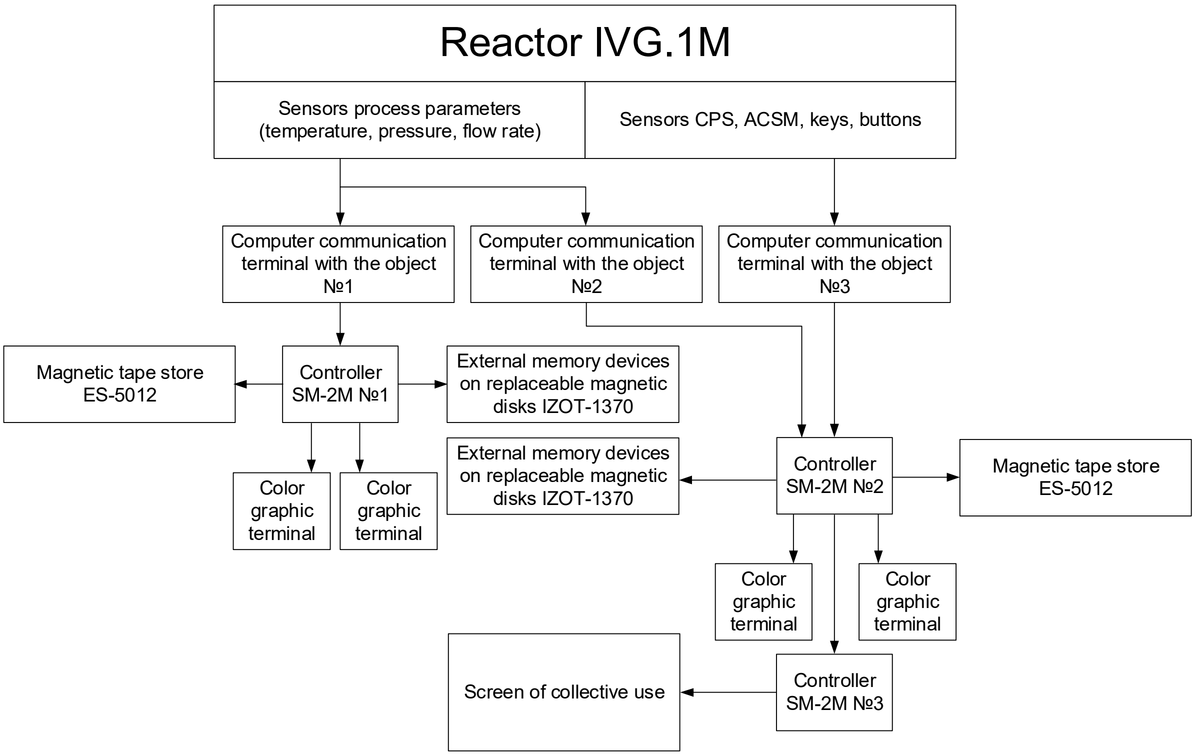


Fig. 1. Existing I&C system of IVG.1M

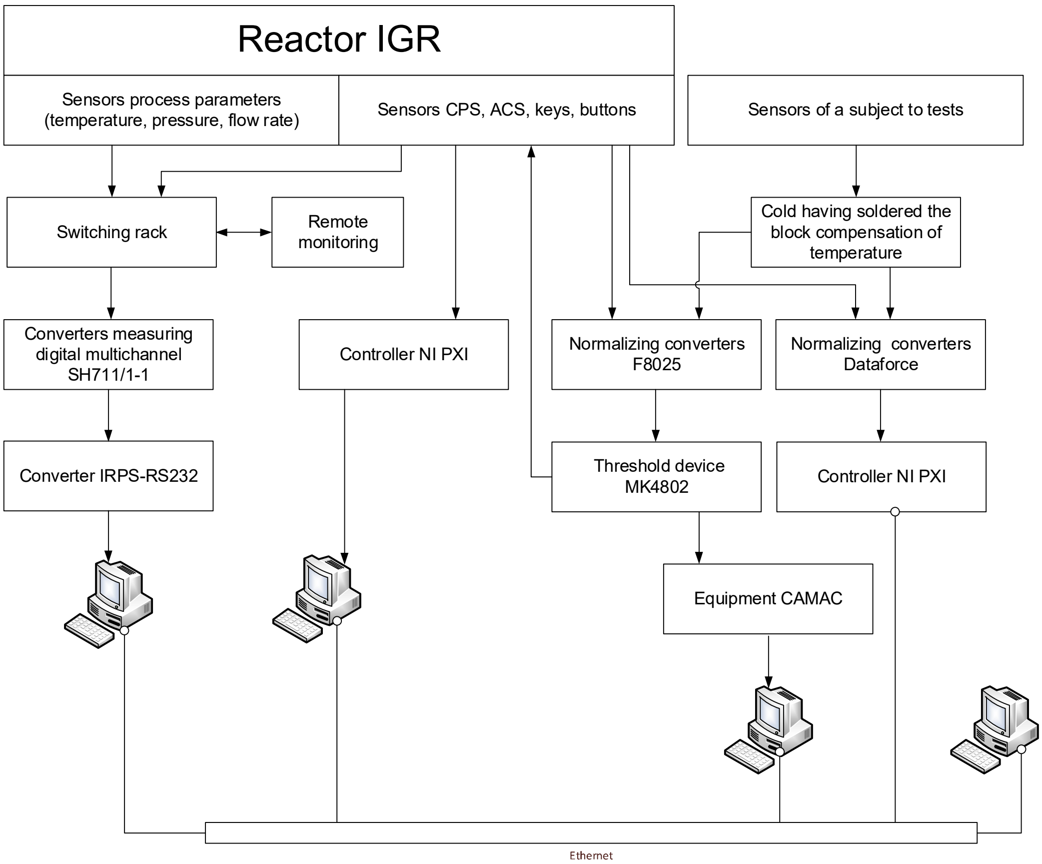


Fig. 2. Existing I&C system of IGR

An analysis of the existing I&C systems of reactor installations has shown that the following major shortcomings are inherent in equipment:

- lack of unification of technical means. Each of the subsystem is implemented on elemental-constructive basis, which leads to hardware redundancy, increasing the number of maintenance personnel, increasing the service time and, as a result, reducing the reliability of the system;
- IIS software and hardware do not allow the interrogation of primary transmitters (PPs) more often than once per second;
- low ergonomic indicators and methods of data displaying lead to the complexity of perception and, as a consequence, the low speed of staff response to the relevant events;
- inflexible subsystem configuration for digital registration, there is no possibility of expansion or modification;
- there are no software tools for analysis and processing of experimental information;
- there are no means of visualizing and displaying of monitored parameters for the operator in a convenient and informative way;
- basic computer systems are morally and technically obsolete (the life of the system components is 15 years and more, which exceeds the assigned resource of work two or more times), require considerable efforts to keep them in working state providing frequent failures and, in fact, have exhausted their resource.

2. MODERNIZATION PROJECT

In 2008, we started the work on complex upgrading of I&C system of IVG.1M reactor. It was developed technical project that includes Process Equipment Automatic Control System Monitoring Subsystem (ACSM), Control and Protection System Parameters Monitoring Subsystem (CPS), Technological Parameters Monitoring Subsystem (TPMS), Coolant activity Monitoring Subsystem (CAMS), Radiation Monitoring Subsystem (RMS).

Design concept of I&C system for IVG.1M reactor is implemented on the basis of the radial topology computer network and includes automated operator workstations, seven information collection and processing controllers, two database servers (DB) and a collective display screen.

I&C system of IVG.1M reactor is a wide area system, unified by interfaces and protocols with three levels of hierarchy (Figure 3):

- lower level (level I) - realizes functions of real-time measurement by specified parameters, collection, registration, primary processing of measurement information about controlled technological parameters, generation and issuance of warning signals and emergency protection;
- middle level (level II) - receives data from the subsystem controllers of the lower level and registers the current values of the measured parameters, processes and displays the current state of the subsystems of the lower level, transfers commands for switching the modes of the lower level controllers;
- the upper level (level III) - performs the functions of managing the operating modes of I&C system in general; provides centralized storage of measurement information; coordinates the work of I&C system levels among themselves; provides informational support of operator workplaces in the console, displays specified groups of current values of measuring and service information in the form of tables, graphs, histograms, mnemonic diagrams and other visual fragments on the collective display screen.

Rockwell Automation equipment was chosen as the equipment of the lower level of the system, as it is listed in the register of the state system for ensuring the uniformity of measurements of the Republic of Kazakhstan and has high operational and technical characteristics, including such factors as availability, average time between failures, time Restore, assigned work resource.

Rockwell Automation software package: RSView32 Works, RSView32 Runtime, RSLogix 5000, RSLinx, and a Microsoft SQL Server 2008 database were selected to develop the information measuring system of the IVG.1M reactor.

In the I&C system, a "display" method of monitoring and control, a "display" setting of the operating modes of the equipment and regulators, a collective screen, microprocessor means of the lower level and a high level of automation will be used.

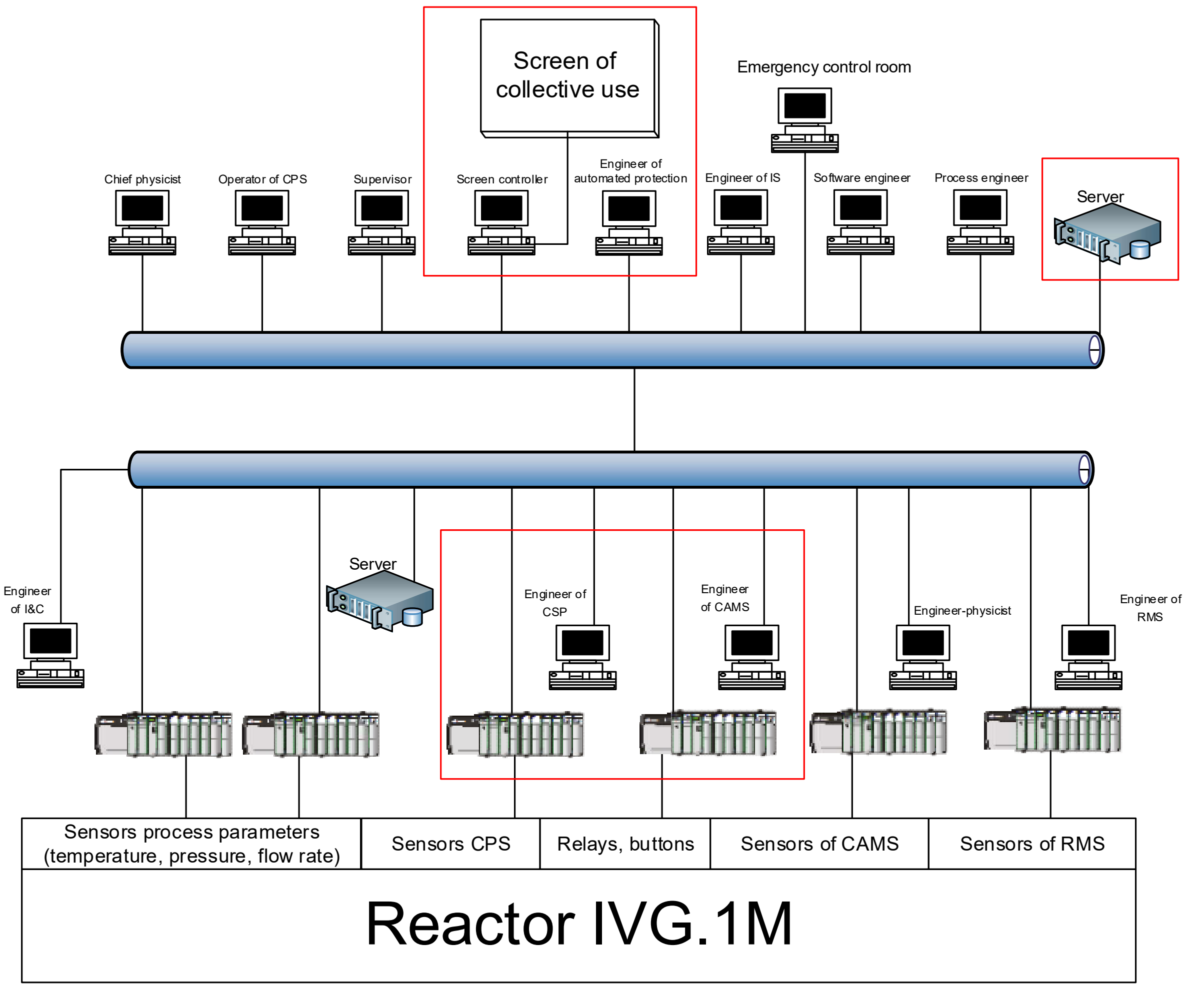


Fig. 3. Structure of new I&C system of IVG.1M

Technical means of I&C IVG.1M will provide:

- collection and recording of measurement information with a channel survey period of 0,1; 1; 10 s;
- the output of discrete signals (for ACSM);
- autonomous registration of the current values of the measured parameters for all analog and discrete channels with the registration period on the controllers 0,1; 1; 60 s. The total time of registration is at least 10 hours;
- duplication of the survey channels and registration of the instrumentation system;
- two data logging servers;
- mismatch in time counts between two registration servers is not more than 100 ms;
- functional independence of all operator's workplaces and local remotes from each other;
- the readiness time of the I&C when switched on not more than 30 minutes;

- data display to the collective screen;
- printing of reports;
- archiving of measurement information.

3. THE FIRST STAGE OF MODERNIZATION

In the period from 2012 to 2014, the first stage of modernization was carried out, in the framework of which modernization of ACSM and CPS was carried out, operational documentation was developed. The modernization was carried out at the expense of the budget of the Republic of Kazakhstan.

Figures 4-9 show the results of the modernization. A comparison of the effectiveness, developed and existing IMS, showed that the IMS significantly exceeds the existing system for all performance indicators:

- Speed. Due to the use of modern equipment and software, produced by Allen Bradly, the frequency of polling of all infrared systems of 50 Hz and the speed of data recording to the server - 10 Hz. This indicator is more than 10 times higher than the indicators. Existing IMS research reactor facilities of the Republic of Kazakhstan;
- Scalability. The proposed multi-level system structure allows increasing the number of controllers, modules in controllers, local consoles, operator stations. New controllers can be located practically in any room of the reactor installation, for inclusion in the system; you only need to bring the Ethernet interface to this room. With the modern development of network technologies, this is not difficult (copper or optical cable, Wi-Fi, etc.);
- Reliability. The developed model of the system is highly reliable, due to the use of the main equipment, which has high MTBF. The calculation shows that the probability that the systems of automatic control systems and control systems will be in working order more than 99.99%;
- Automatic diagnostics and metrological certification. In the IIS model, the equipment and primary converters included in the register of the state system for ensuring the uniformity of measurements of the Republic of Kazakhstan are used. The developed software allows carrying out static and dynamic diagnostics of equipment, including software and hardware Watchdog system controllers.
- User’s handy. The proposed methods of information display (SCADA system, operator stations, local consoles, collective display screen on the basis of LCD TV), due to more flexible structure and centralization of the information source for local operator panels and collective display screen, provides an institutional tool for organizing experimental information in various Modes of operation of the reactor installation and allows you to build and modernize the system while maintaining the basic principles of efficiency and.

Fig. 4. Controller of ACSM

Fig. 5. ACMS operator's workstation

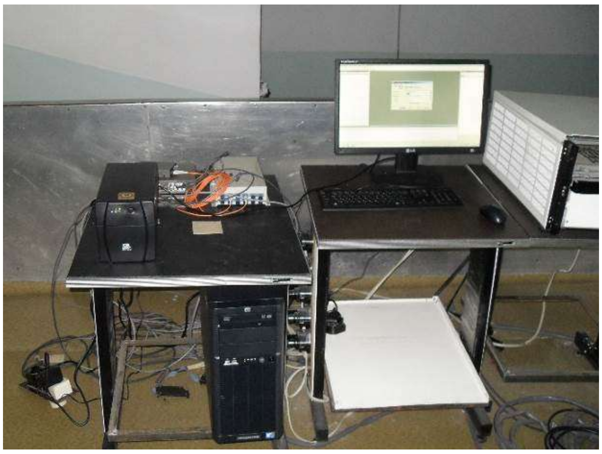


Fig. 6. I&C server of IVG.1M reactor

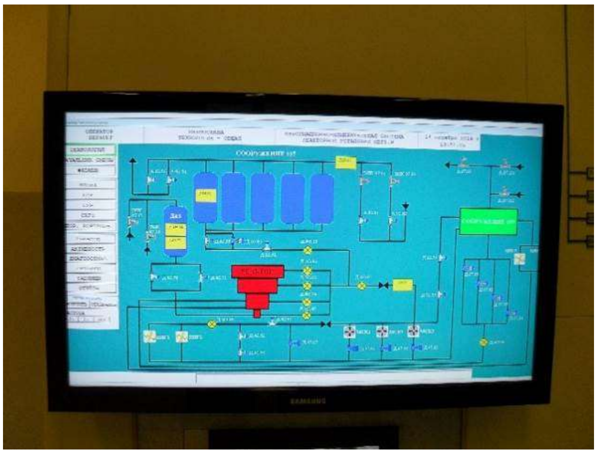
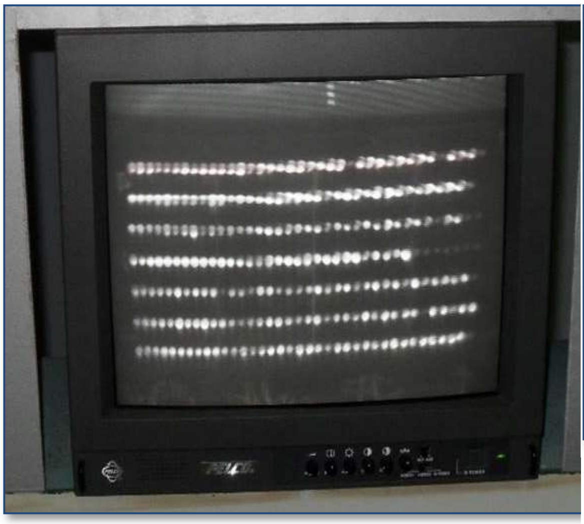


Fig. 7. Remote viewing display

Fig. 8. Controller of CPS

Fig. 9. Automated working station of CPS

Ergonomic characteristics of the new I&C system significantly exceed the existing I&C system (Figures 10-13).



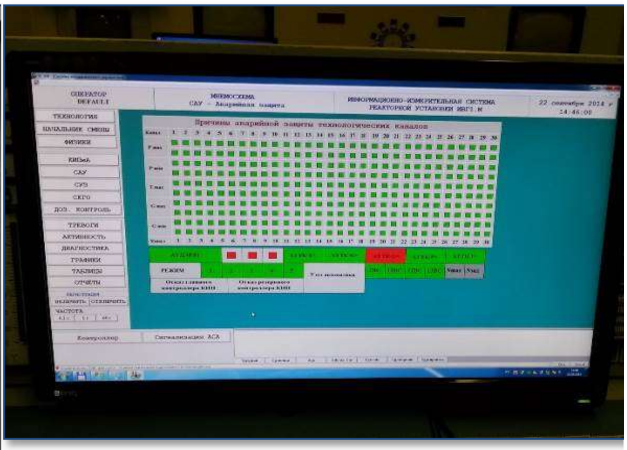


Fig. 11. Presentation of data in new ACSM

Fig. 10. Presentation of data in the ACSM

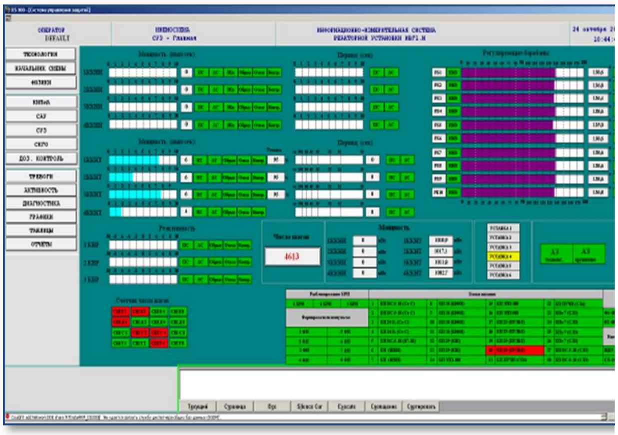


Fig. 13. Presentation of data in new CPS

Fig. 12. CPS operator workplace

4. THE SECOND STAGE OF MODERNIZATION

Since 2016, the National Nuclear Centre has been implementing the KAZ1004 project on the technical cooperation program with the IAEA "Development of the Information and Measuring System of the Reactor Unit". The project budget is 212800 euros. The project will modernize TPMS, CAMS, RMS, an evaluation of the modernization project and the progress of work carried out by IAEA experts, and personnel training.

In 2016, the first part of the equipment was delivered (controllers, analogy-digital converters, power supplies, terminal blocks, network cards, etc.) for modernization TPMS.

This equipment is mounted (Figures 14-15) and the adjustment work is carried out.

Fig. 14. The first controller of TPMS

Fig. 15. The third controller of TPMS

From 8 to 10 November, the National Nuclear Centre of the Republic of Kazakhstan was visited by IAEA experts who analysed safety aspects of the modernization project (Figure 15).

According to the recommendations of the experts, changes were made to the project of modernization of TPMS, which include:

- redundant channels, provide functional independence that includes physical separation, and electrical isolation. This could be achieved by placing redundant channels in separate cabinets, powered by different sources and locating cabinets in different rooms;

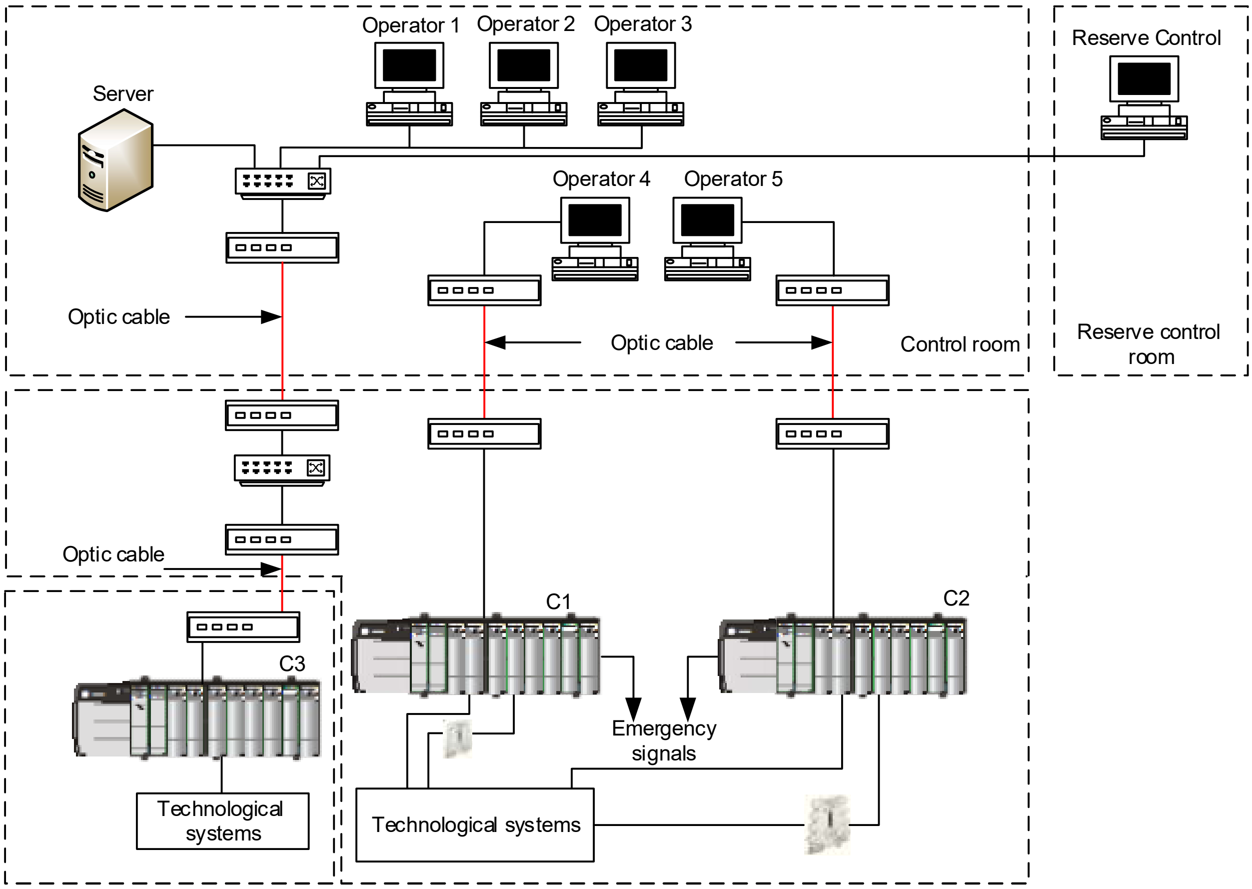


Fig. 16. Structure of TPMS (taking into account the expert's recommendations)

5. CONCLUSION

Modernization of the information system is a priority. Because modernization will increase reactor safety, improve metrological and ergonomic characteristics. Allows the training of young professionals in information systems. The ongoing modernization meets all IAEA safety standards. In the plans for 2018-2025 to modernize the control and protection system of the IVG.1M and IGR reactors.

NEWLY DIGITALIZED I&C SYSTEM DESIGN FOR NEW RESEARCH REACTOR

S.H. BAE, K.Y. PARK, Y.K. KIM
Korea Atomic Energy Research Institute,
105 Dukjin-dong, Yusong-gu, Daejon 305-353
Republic of Korea

Abstract

The newly digitalized I&C system is continuously required to be applied to the new research reactor to cut wn the maintenance cost and extend the operation interval. The existing analogue type of safety system is being fully changed into digital components such as PLC and data communication device including peripheral components is expected to be remarkable improvement. This digitalized system is perfectly complied with the safety requirement of the digital computer I&C system and thus the interface related with modified system should be changed. Furthermore the diversity required to deal with common mode failure by software fault should be applied to this system. The newly digitalized I&C system has still a couple of problems like COTS dedication, V&V problems and diversity issues, etc. but it is expected that these problem will be solved by more coordination with system design development.

1. INTRODUCTION

This paper introduces the newly digitalized I&C system that will be applied to the New Research Reactor (NRR). The existing analogue type of safety system such as RPS, including PAMS is fully changed into digital equipment such as PLC. Also there will be remarkable improvement of data communication methodology. This digitalized system sufficiently complies with the safety requirement of the digital computer I&C system. Furthermore the diversity that is required to deal with common mode failure by software fault is introduced, how it is to be applied to this system. The DPS is also added to compensate for the coverage of RPS in case RPS doesn't perform the safety function properly. When it comes to seismic monitoring, the function of that is enhanced through the ASTS which transfers the trip signal directly. The newly digitalized I&C system has a couple of issues like COTS dedication, V&V problems and diversity. Appropriate action for these problems will be taken after sufficient consideration.

2. SYSTEM DESCRIPTION OF NRR I&C SYSTEM

2.1. System classification of NRR I&C system

2.1.1. Hierarchy of NRR I&C system

Most of the I&C systems of NRR are implemented by digital computer technology. All I&C systems and equipment are designed, constructed and maintained in such a way that their specification, verification and validation, quality and reliability are commensurate with their classification. I&C systems are identified based on the safety and system functions for protecting, controlling and monitoring the facility. The RPS and PAMS are categorized into the safety class, while the other systems are non-safety class as presented in Figure 1. Most of the I&C systems of NRR are implemented by digital computer technology. All I&C systems and equipment are designed to ensure that verification and validation, quality and reliability are commensurate with their classification. The I&C systems of the NRR are composed of Reactor Protection System (RPS), Post-Accident Monitoring System (PAMS), Reactor Regulating System (RRS), Diverse Protection System (DPS), Information Processing System (IPS), Process I&C System (PICS), Automatic Seismic Trip System (ASTS), Radiation Monitoring System (RMS), Main Control Room (MCR) and Supplementary Control Room (SCR).

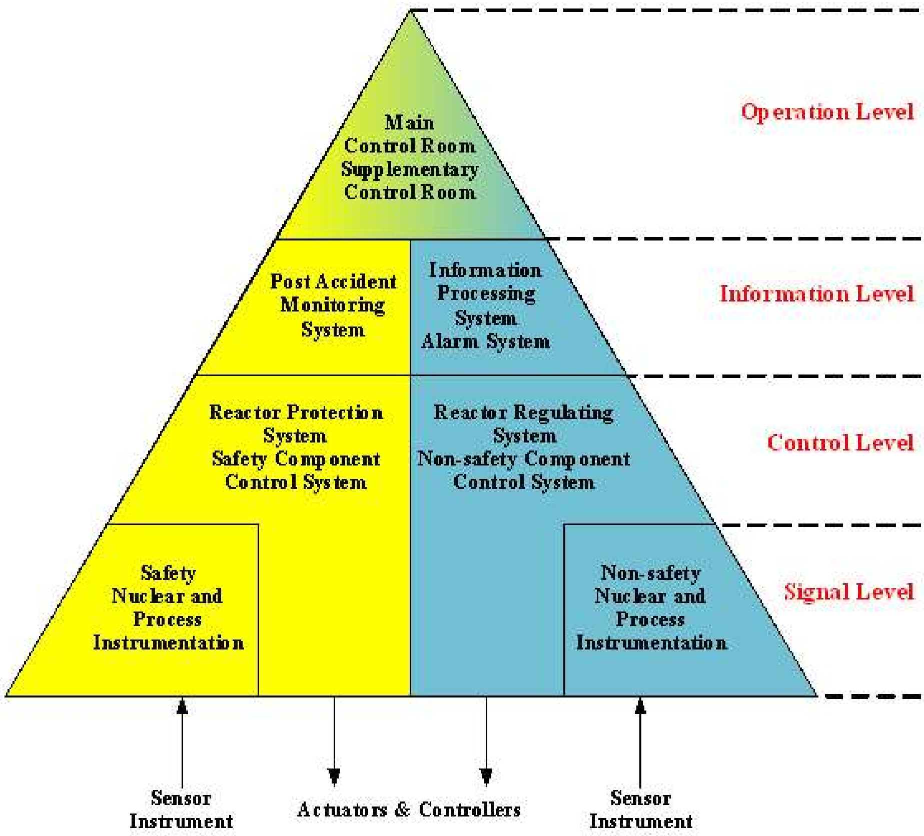


FIG. 1. Hierarchy of I&C system in NRR.

2.1.2. Classification of NRR I&C system

The classification of safety class, seismic and quality condition in the NRR I&C system is as shown in Figure 2. The RPS which give direct protective action and PAMS, which is the system for monitoring after accident, are categorized as safety system of which other requirements are subject to safety class, including seismic and quality condition. The other system in the I&C system are given as non-safety system, that means no related safety function, but DPS and RRS are categorized as quality class T because this system has a very critical function for stable operation and backup measurement in case of the RPS failure. The ASTS is reasonably classified as Seismic Category 1, because the system should maintain continuous and complete performance under seismic conditions.

TABLE 1. SUMMARIZED I&C SYSTEM CLASSIFICATION

System	Safety Class	Electrical Class	Seismic Category	Quality Class
RPS	SC-3	1E	I	Q
PAMS	SC-3	1E	I	Q
RRS	Non-Safety	Non-1E	Non-Seismic	T
IPS	Non-Safety	Non-1E	Non-Seismic	S
PICS	Non-Safety	Non-1E	Non-Seismic	S
RMS	Non-Safety	Non-1E	Non-Seismic	S
ASTS	Non-Safety	Non-1E	I	T
DPS	Non-Safety	Non-1E	Non-Seismic	T

2.2. System design bases and description of NRR I&C system

2.2.1. Safety function and design basis for NRR I&C system

Safety functions of the NRR I&C system is composed of i) a reactor shutdown, ii) a decay heat removal, and iii) confinement of radioactive materials, which shall be satisfied by implementing appropriate inherent and passive safety features, safety systems and engineered safety features. Provided that potential human errors and unexpected mechanical failures occurr, it is important to ensure that the reactor design and operation incorporates multiple levels of protection against accident.

This I&C system has many digitalized components in the safety related system and this may result in the unintended consequence of common mode software errors concerning I&C systems. Thus diversity is considered necessary to offer the final defense against Common Mode Failures (CMFs) like Table 2. All critical safety functions, such as reactivity control, inventory control and heat removal, can be controlled by both the control systems and the protection system as shown in Figure 3. These systems are functionally diverse, as are the fluid /mechanical systems they control. In addition, to correspond with the hardware diversity of these systems, software diversity is subject to protection I&C systems to eliminate the potential for CMFs. This diversity exists in all software-based aspects of these systems, including processors, I/O modules, communication networks and MMI devices.

TABLE 2. DIVERSE DESIGN APPROACH FOR RELIABLE SAFETY FUNCTION

Function	System Design I	System Design II
Mechanical Reactor Trip	First Shutdown System by CRDM	Second Shutdown System by SSDM
Reactor Trip	Reactor Protection System	Diverse Reactor Trip by DPS
Reactivity Controls	Reactor Regulating System for Normal CAR Control	Reactor Protection System for Shutdown by Insertion of CARs/SSRs
Alarm and Indication	Flat Panel Display at Operator Workstation in MCR	Large Display Panel in MCR
Safety Parameter Monitoring	Safety Display at Reactor Protection System	Flat Panel Display & Large Display Panel
Accident Monitoring	Display at Post-Accident Monitoring System	Display of Accident Monitoring Function at MCR
Manual Reactor Trip Environment	Manual Trip Buttons at MCR	Manual Trip Buttons at SCR

2.2.2. System description for each subsystem

2.2.2.1. Overall configuration of I&C system

The RPS is a digitalized safety system that causes a reactor trip, to protect the core by generating trip signals to insert four Control Absorber Rods (CARs) and two hydraulic actuated Second Shutdown Rods (SSRs) into the core whenever the trip parameters exceed the trip setpoint. In addition, the RPS provides engineered safety features actuation to mitigate the consequences of accidents and to prevent the release of radioactive material to the environment. Three independent measurement channels with electrical isolation and physical separation are provided for each parameter used for the direct protective action of the RPS. The PAMS provides the necessary information for operators to monitor and take action during and after a design basis event. The PAMS is a dual redundant system consisting of two independent channels. The RRS is a computer-based system which regulates the reactor power level using four Control Absorber Rods (CARs). The RRS performs the reactor control function including reactor startup, changing power levels, and maintaining the power at required level. The RRS is separated functionally, physically and electrically from the RPS. The DPS performs a diverse reactor trip function to mitigate the effects of a postulated common cause failure of the RPS. The DPS initiates a reactor trip when the dedicated parameter exceeds the predetermined value in case that the RPS safety function has failed. The DPS design uses a two-out-of-two coincidence circuit to actuate the four CARs and two SSRs. The ASTS has two different functions. One is to shut the reactor down automatically if an earthquake greater than the Operating Basis Earthquake (OBE) occurs at site. The other is to monitor the seismic motion of the site on a continuous basis. The ASTS includes all the necessary acquired earthquake data of the NRR site. Overall configuration of I&C system is given below in Figure 2.

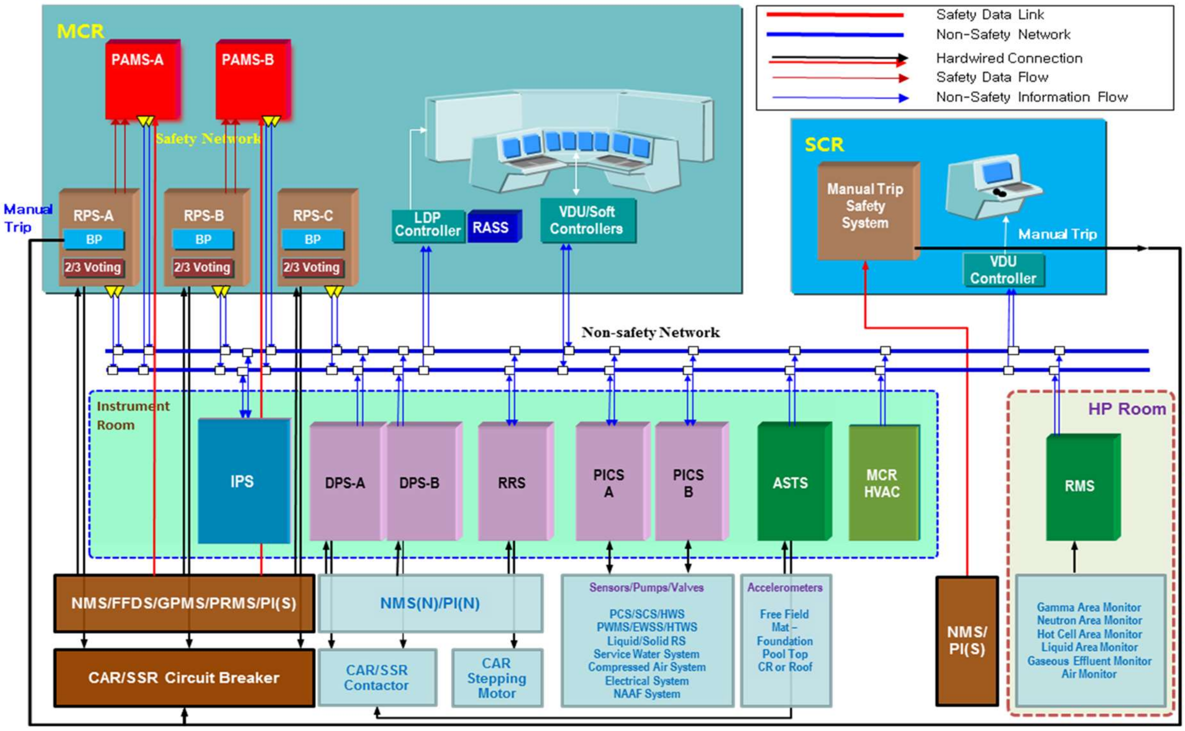


FIG. 2. Configuration of NRR I&C system.

2.2.2.2. System and components description for NRR I&C system

The RPS consists of three redundant channels as shown in Figure 3. Each channel consists of sensors, bi-stable processor (BP), coincidence circuit (CC), initiation circuit (IC), actuation circuit (AC), interface and test processor (ITP), maintenance and test processor (MTP), and other equipment necessary to monitor selected reactor conditions, and to provide reliable and rapid reactor protective action if monitored conditions approaches specified safety system settings. The BP generates trip signals based on the measurement channel value exceeding a setpoint. The BP provides trip signals to CC located in the three redundant channels to de-energize its associated coincidence trip relays when any trip parameter reaches its setpoint. Each BP sends status data to the ITP and the MTP via the PLC data communication module. The MTP is a main human-machine interface for the RPS. Each MTP in three redundant RPS cabinets provides the displays and controls needed to support the operation of RPS. The MTP provides data communication gateways to send RPS status to the IPS and RRS. System surveillance testing or maintenance can also be monitored using its display panel. The ITP monitors the status of each RPS channel and provides the channel status information to the MTP. It provides the interface between ITPs in other redundant RPS channels and interfaces to external systems for status indication. The ITP provides the interface to PAMS for sending values of the process input variables.

The PAMS consists of two different displaying architectures. One is the two safety cabinets for the safety related PAMS variables and the other is the non-safety displaying monitor for non-safety PAMS variables which are displayed at the OWS. The safety related PAMS variables are continuously displayed on the Flat Panel Displays (FPDs) that are mounted on the PAMS cabinets. Each cabinet includes a cabinet assembly, a sensor input module, a communication link module, a PAMS processor, and a display-purpose PC including a 19 inch qualified flat panel. The data displayed is also stored in the memory with high capacity via a storage device. The signal storage device need not follow the requirements for the PAMS system. The safety signals from the display-purpose PC should be sent to the IPS through signal isolators. The non-safety PAMS variables are displayed at the OWS display unit. The safety-related PAMS variables are redundantly displayed at the OWS for diversity.

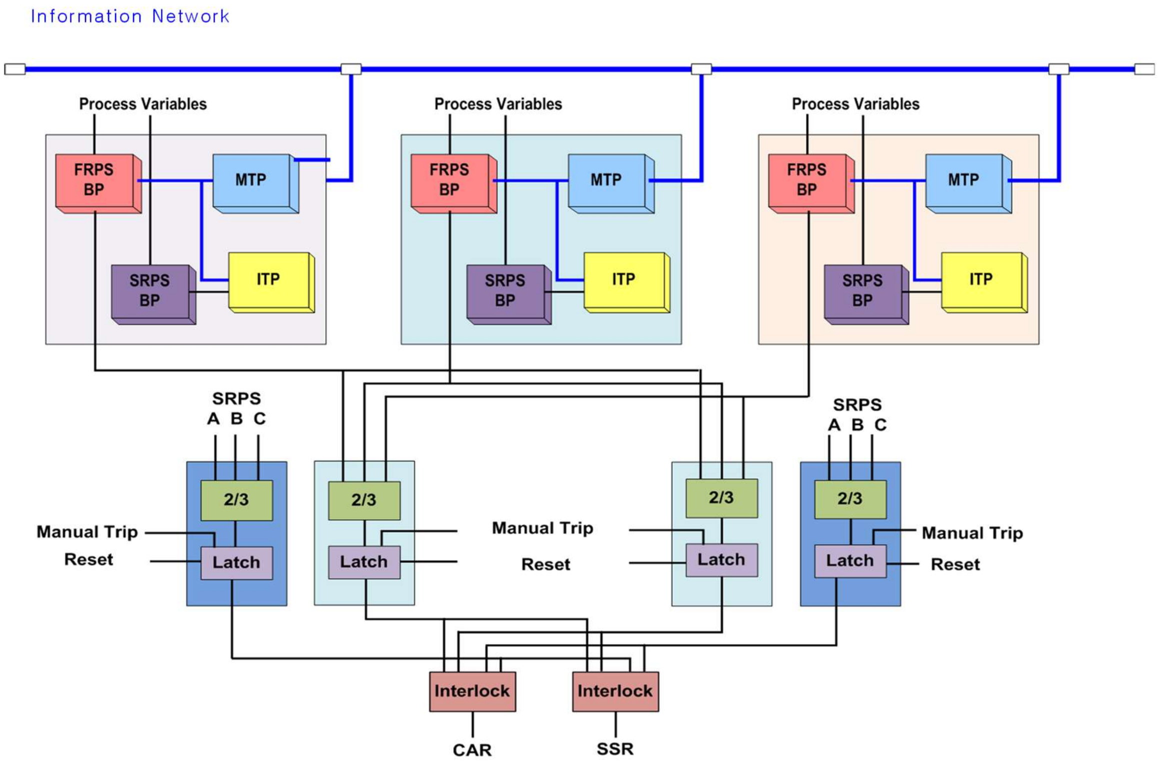


FIG. 3. Schematic diagram of RPS.

The IPS includes a Real-Time Database Management System (RTDBMS) that manages the primary source of operational parameters and perform many functions as represented in Figure 4. This database logically groups all operational and descriptive fields for one addressable point into one record. It is reliable, responsive and has an integrated set of tools. The database provides configuration capability for parameters such as rationality limits, alarm limits, process group, alarm ignoring/conditioning, etc. The diagnostic function checks the component integrity of IPS, such as CPU, memory and others at on-power condition. Also, the IPS monitors working status of the IPS components continuously. Furthermore, it monitors communication status with other I&C systems. The failover function copes with any malfunction or performance deterioration detected by the diagnostic function. This switching over technique is an important function to continuously maintain the functional integrity of the system.

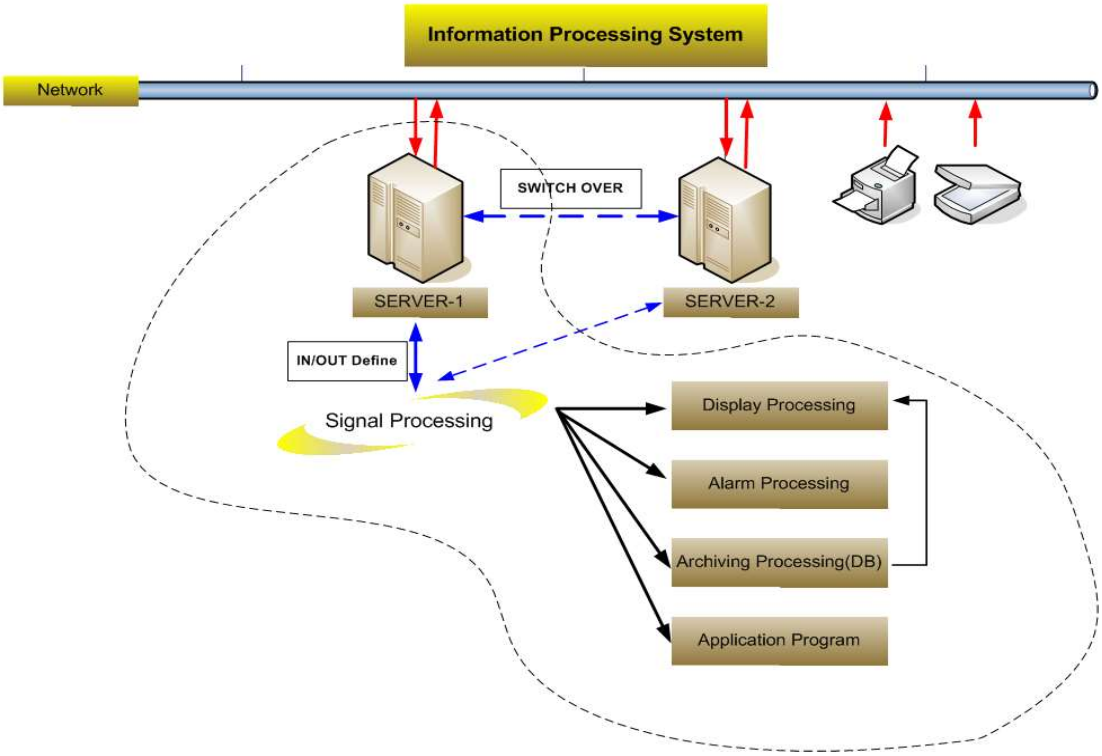


FIG. 4. Functional block diagram of IPS.

The MCR is continuously manned, by at least two persons (a reactor operator and a supervisor), and is a protected enclosure in which actions are normally taken to operate the reactor under normal and abnormal conditions. For all supposed abnormal and emergency situations, the MCR hasthe capability to overcome those situations and is able to shut down the system. The equipment of the MCR consists of an LDP (Large Display Panel), OWSs (Operator Workstations), and other facilities as shown in Figure 5. The SCR is designed with a design capability for prompt shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during shutdown and with the potential capability for subsequent shutdown of the reactor through the use of suitable procedures, in situations where reactor operation in the MCR is impossible.

FIG 5. Overview of the MCR.

2.4. Software development life cycle applied to NRR

The activities cover the entire life cycle of a software project, from the planning & concept phase to the test phase of the software system. The activity groups are further grouped into five sections according to IEEE Std 1074-2006. The activity groups of project management include activities that initiate, monitor, and control a software project throughout its life cycle. The activity groups of pre-development include the activities that explore and allocate system requirements before software development can begin. The activity groups of the development include the activities performed during the development and enhancement of a software project. The activity groups of post-development include the activities that install, operate, support, maintain, and retire a software product. The activity groups of support include the activities that are needed to successfully complete project activities. The activities for the SDLC of the NRR I&C system are shown in Figure 6.

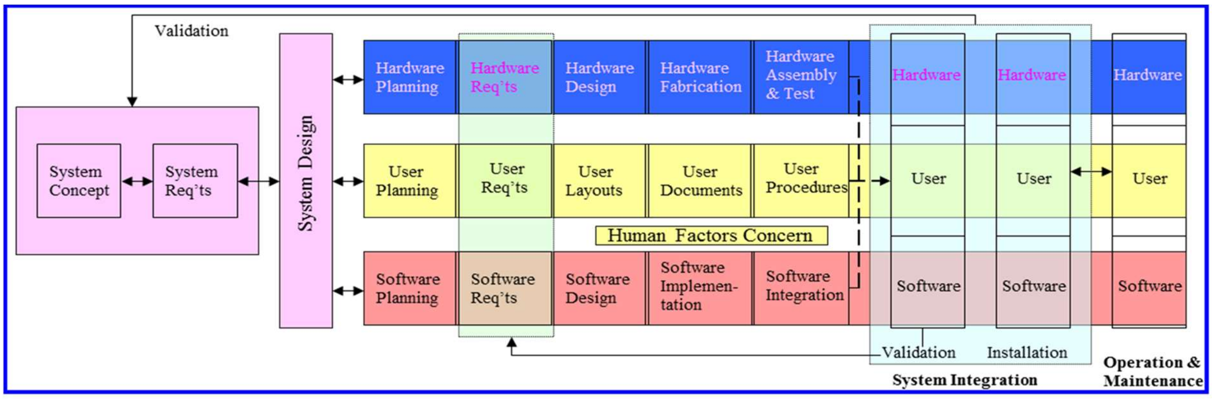


FIG. 6. Software development life cycle.

2.5. Equipment Qualification Requirement for NRR I&C system

The safety I&C equipment, called class 1E meets or exceeds the specification requirements. The equipment qualification ensures that the class 1E equipment performs its safety functions without failure mechanisms that could lead to common cause failures under postulated service conditions. This is the primary role of the equipment qualification. The panels for the RPS and the PAMS shall be subject to type testing including seismic and environmental qualification testing, in accordance with the requirements of RG 1.89, 1.110, IEEE Std. 323-2003 and IEEE-344. The required qualification testing shall proceed with the test plan and procedures under quality program and be integrally documented as a test report. The field safety I&C equipment, including nucleonic instruments, will be acquired as a qualified item by the manufacturer's generic test program. The manufacturer shall submit all detailed quality verification documents to verify the successful equipment performances under the postulated seismic and environmental conditions. The performance of safety-grade hardware and software used in computer-based safety systems will be demonstrated based on IEEE 7-4.3.2 and practices for development, verification and validation.

3. CONCLUSION

As above, the NRR I&C system is applied to an optimized approach for the digitalized I&C system. This implies that in a fully changed safety system such as RPS, PAMS is implemented by a kind of PLC and consequently requires complete compliance with IEEE Std 7.4.3-2-2010 and SRP 7.0(BTP 7-14) of NUREG-0800. The enhancement of the diversity is expected to make it easy to cope with common mode failure by software fault through the DPS. The engineered safety features are also designed to meet the requirement of defense-in-depth, with an interface that is fully qualified by appropriate methodology. The newly digitalized I&C system has still a couple of difficulties, like COTS dedication, V&V problems and so on. Appropriate action for these problems will be taken by after tough discussions between the system engineer and system designer if necessary, and the regulatory body will be included.

EXPERIENCE IN REFURBISHING HANARO REACTOR CONTROL COMPUTER

Hyung Kyoo Kim*, Min Woo Lee, Young San Choi, Yun Taek Yim, Seung Kyoo Doo and Hoan Sung Jung
Korea Atomic Energy Research Institute
111 Daedeok-daero 989beon-gil, Daejeon, Korea
kimhk@kaeri.re.kr

ABSTRACT

HANARO (High-flux Advanced Neutron Application Reactor), which is an open-tank-in-pool type research reactor with 30MW thermal power, achieved its first criticality in 1995. Recently, there has been a fast development in the field of electronics. Many manufacturers of I&C equipment or components have disappeared or merged with others. The HANARO reactor control computer, which was a programmable controller system named as Multi Loop Controller (MLC) manufactured by MOORE (Canada), had been utilized for 20 years since its initial criticality. However, its supplier no longer produced the required components and disappeared from the scene, and thus support for this system could no longer be guaranteed. Its refurbishment was completed successfully in 2015. The goal of the refurbishment program was a functional replacement of the reactor control system in consideration of suitable interfaces, compliance with no special outage for installation and commissioning, and no change of the well-proved operation philosophy. New control computer named HCCS is a DCS (Discrete Control System) using PLC manufactured by RTP. The control algorithm has been migrated into a new control computer system. Software V&V has been committed on the basis of IEEE Std. 1012, which was issued in 2004; and the Software Development Life Cycle (SLDC) framework consists of seven phases such as: planning, requirements, design, implementation, test, installation and checkout, and operation and maintenance. This paper describes the refurbishment program of the HANARO control system and the V&V activities performed during implementation of the replacement of the HANARO control computer.

Key Words: programmable controller, research reactor, software, verification, validation, HANARO, SLDC

1. INTRODUCTION

HANARO (High-flux Advanced Neutron Application Reactor) is a 30MWth multi-purpose research reactor. The HANARO has been utilized in various fields such as nuclear in-pile tests, radioisotope production, neutron beam research, neutron transmutation doping, and neutron activation analysis since the first criticality was achieved in February 1995. The original HANARO control computer system consist of two major parts, programmable controller called MLC (Multi-Loop Controller) and MMI (Man-Machine Interface) called BCS (Basic CRT System). The HANARO control computer system is being utilized not only for regulating reactor power but also for a reactor power display, indications, data collection, process system alarms, and trend records, etc. The MLC was used for processing the control algorithms of not only reactor regulating system but also various process systems in order to regulate reactor power. The BCS was used for displaying, storing, and recording various plant signals and enabled operators to measure the necessary actions. Recently there is a fast development in the field of electronics. The many manufacturers of I&C equipment or components are disappeared or merged with the others. This is a major reason to decide modernization and upgrade of I&C system at a given facility because of obsolescence of the present I&C system, the unavailability of spare parts and an increased failure rate of the I&C system leading to frequent reactor shut downs. The supplier of control computer produced the components no longer and also disappeared, and thus the ageing, obsolescence, and a short supply of spare parts have caused great problems. We made a plan to refurbish the control computer because the system supplier no longer provides technical support and thus no spares are available. The upgrade of BCS to OWS was completed in 2009. The first consideration for a replacement of the MLC dated back to 2007. The refurbishment program objective was a functional replacement of the reactor control system in consideration of suitable interfaces, compliance with no special outage during installation and commissioning, and no change of the well-proven operation philosophy. The refurbishing

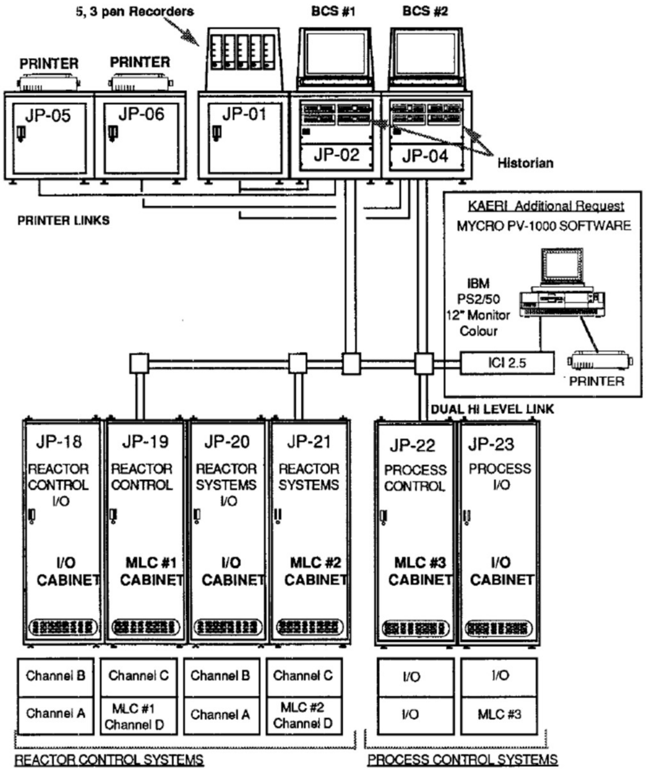


Figure 6. BCS and MLC of HANARO

plan of the control computer was established in 2009 and its replacement was successfully completed in 2015. Figure 1 shows the old HANARO control computer (MLC) and BCS [1].

In the development of a computer based system, it is important to be able to determine and assess if the system meets the requirements and specifications, and if its outputs are correct. Faults can lead to system failures causing public hazards, financial loss or property damage and as well as a deterioration in the reliability of the system. Early detection results in a better solution rather than quick fixes. The purpose of V&V is to help the development organization build quality into the system during the life cycle. The V&V processes provide an objective assessment of the products and processes throughout the life cycle [2]. The V&V is carried out in parallel with the software/system development process to find and correct errors in the development life cycle as early as possible. A Software Verification and Validation Plan (SVVP) is required for software applicable on a computer-based control system and shall specify the activities to be performed during the software management and development process in accordance with IEEE 1012. The V&V activities include analysis, evaluation, review, inspection, assessment, and testing conducted by a competent person or group. IEEE 1012 describes the SDLC phase activities for software V&V including Independent Verification and Validation (IV&V) for nuclear power plants in a truly general and conceptual manner, which requires the upward and/or downward tailoring on its interpretation for practical V&V. It contains crucial and encompassing check points and guidelines to analyze the design integrity, without addressing the formalized and specific criteria for IV&V activities confirming the technical integrity.

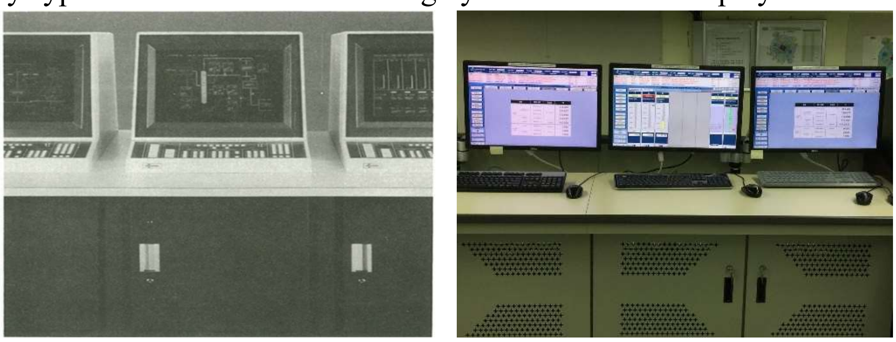
The new HANARO Control Computer System (HCCS) is a Discrete Control System (DCS) using PLC manufactured by RTP. The software V&V was conducted in order to assess whether the new control system is consistent with the specifications and requirements.

2. UPGRADE OF HANARO CONTROL COMPUTER

2.1. Upgraded BCS to OWS

The computer system plays a role of an integrated information storage system of a plant, and is in charge of the generation of a control rod driving signal, collection of an input/output signal, display, trend record, alarm function, and so on in accordance with software realized through a power control algorithm. The MLC is connected to instrumentation such as detectors and sensors, and monitors and controls the states of all the systems to operate the reactor safely. The operators can access all signals through man-machine interface which is main console of computer system at the supervision level. The BCS is a main interface in which operators control the various information of the plant by collecting and storing data from the MLC and displaying the data on the CRT. Also if an abnormal condition occurs at a certain system, the BCS alarms and notifies to the operators through a printer message.

The BCS has been upgraded in two phases. The BCS had provided operator monitoring and control of the process. It contained a 19" CRT screen as a display unit and a multiprocessing system computer with an 8" floppy disk as system drive for the system configuration. The BCS was out-of-date and obsolete, and it was thus difficult to obtain spare parts and repairs. In 2002, the first upgrade of BCS to OWS, which was to replace the BCS with PC-based workstation provided by Siemense which was called OWS, was carried out but one of the original systems had been left for a use in an emergency. In 2009, a second upgrade was carried out. It was an integration of newly installed utilization facilities, fuel test loop (FTL) and cold neutron source (CNS) into HANARO. That upgrade was done on both the hardware and software. The software used for the monitoring and control was developed and the graphic display type was added to the existing system. The new display was designed to



(a) BCS **(b) OWS**

Figure 2. Old and New MMI of HANARO

meet the requirements of the human engineering guidelines. Figure 2 shows old and new MMI of HANARO.

2.2. Multi-Loop Controller

The MLC is a distributed control system (DCS) that provides process digital control for implementation of simple and complex regulatory control strategies. It has the ability to process a local analogue and discrete I/O, to perform as a distribute element, and to function as a stand-alone controller. The MLC has a watchdog timer and high-level link (HLL) interface except for I/O cards with a 19" card rack and power supply system. The watchdog timer consists of two cards and dual output assemblies, functions to detect a failure such as a power failure, scan failure, failure to transfer control, and major on-line error. The HLL is a data highway interconnecting operator consoles such as OWS and an independence computer interface (ICI) and satellite stations. The HLL has two independent links: link A and link B. If one link fails, the HLL will continue to operate on the remaining link. The ICI provides a means of connecting a computer used for maintenance or engineering to the control system. The ICI is used to simplify task of interfacing both software and hardware.

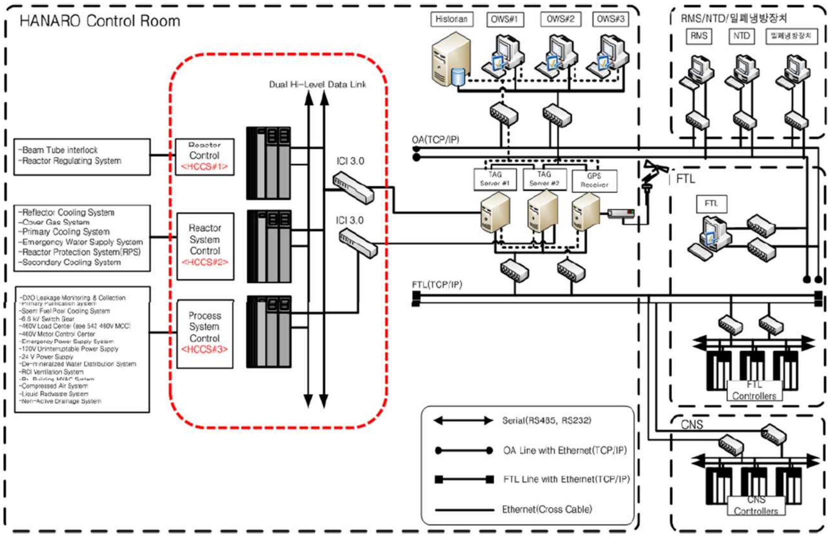


Figure 3. Architecture of HANARO control computer

Figure 3 shows the architecture of the computer system of HANARO.

The MLC monitors and controls the states of all the systems so as to operate the reactor safely. Input/output units, power supplies and other important hardware are two-fold for an improvement of the system reliability and availability factor. The MLC is composed of a main controller and a backup controller. If the main controller fails, the backup controller takes over all the functions immediately, and therefore the reactor can be operated continuously. The characteristics of the MLC can be summarized briefly as follows.

1) Input/output signal processing capability

- Analog input: 128 units
- Analog output: 64 units
- Digital input/output: over 400 units

2) Control function of 64 loops

3) Handling 128 software blocks within 0.1 sec or 0.2 sec

4) Utilization of a simple programming using a block configuration

5) Utilization of a Multi-Processing using 4 microcomputers

6) Two-folded structure of all hardware

As shown in figure 1, three MLCs were used in HANARO control system. Each MLC consist of two fully redundant programmable controllers. Both programmable controllers run simultaneously, but only one (primary or secondary) was in control and output to the field. Each programmable controller had its own I/O cards. Both programmable controller cards were redundant and wired to the same I/O terminals [1].

2.3. New Control Computer System (HCCS)

The new HANARO control computer system (HCCS), in common with the MLC, is composed of three control computers, Reactor Control System, Reactor Systems and Process Control System. Each system is configured in two cabinets, as shown in figure 4.

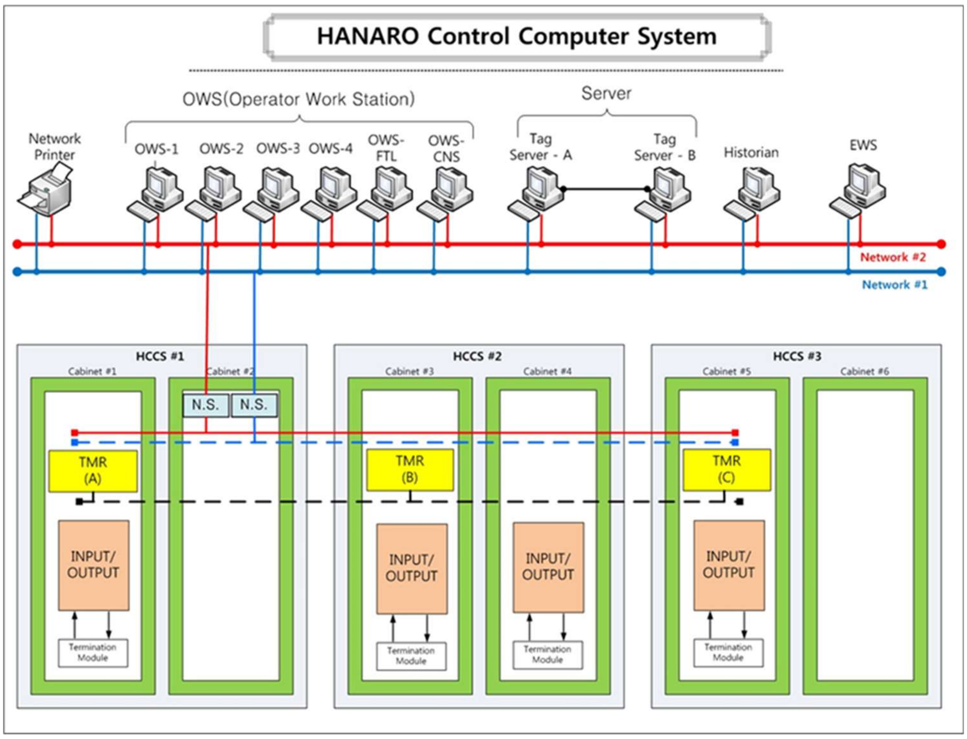


Figure 4. Configuration of HCCS

HCCS consists of triple modular redundant (TMR) processors, and dual redundant I/O modules and a power supplies. The TMR processors and dual I/O module will provide high reliability in the following methods: 1) Redundant I/O modules run simultaneously and each I/O module communicates with all processors for signal validation; 2) One I/O module communicates with all processors upon failure of a single I/O module.

The characteristics of TMR processors are:

1) Three processors run simultaneously with signal validation;

2) The signal validation produces one representative value from three redundant processors;

3) The signal validation produces one representative value from two redundant processors upon failure of a single processor;

4) The signal validation produces one representative value from two cycle values of the other processor upon failure of the dual processors.

Each processor and I/O module is hot swappable and is provided to protect the cards from damage, and to prevent the degradation of control and data signals on the bus, when plugged into a HCCS chassis during service. The engineering workstation (EWS) is equipped with the maintenance system for modifying the logic and configuration of I/O signals in the HCCS. During this configuration, the other console can handle the displays. The configuration is to be developed in off-line mode and using special keyboards if required. The method of configuration is to use a high level language that does not require programming expertise. Functions to perform the configuration on an external computer and to download or upload the control logic to or from the HCCS are provided.

3. SOFTWARE VERIFICATION AND VALIDATION OF HCCS

3.1. Overview of Software Verification and Validation

V&V is one of the software engineering disciplines for improving the quality of the system during the development process or during the life of a computer-based system. IEEE 610 defines verification and validation as follows [3]:

- Verification: The process of evaluating a system or component to determine w hether the products of a given development phase satisfy the conditions impos ed at the start of that phase.
- Validation: The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies the specified requirements.

The verification process provides objective evidence for whether the products perform the following:

- Conform to the requirements (e.g., for correctness, completeness, consistency, and accuracy) for all activities during each life cycle process
- Satisfy the standards, practices, and conventions during the life cycle processe s
- Successfully complete each life cycle activity and satisfy all the criteria for ini tiating the succeeding life cycle activities (i.e., builds the product correctly)

In addition, the validation process provides evidence for whether the products perform the following:

- Satisfy the system requirements allocated to the products at the end of each lif e cycle activity
- Solve the right problem (e.g., correctly model physical laws, implement busin ess rules, and use the proper system assumptions)
- Satisfy the intended use and user needs in the operational environment (i.e., bu ilds the correct product)

While verification and validation have separate meanings, the verification and validation processes are interrelated and complementary, and use the results from each other to establish better completion criteria and analysis, evaluation, review, inspection, assessment, and test V&V tasks for each life cycle activity. Therefore, V&V as an integrated activity provides several benefits [4]:

- Early detection of high-risk error giving the design group to drive a comprehe nsive solution rather than quick fixes;
- Evaluation of the products solving the "right problem" against software requir ements;
- Objective evidence of software and system in compliance with quality standar ds;
- Provision of information on the quality and progress of the software and syste m development;
- Support for process improvements with an objective feedback on the quality o f the development process and products.

The HCCS software including firmware was developed to ensure its reliability and completeness by the systematic methodologies using a software verification and validation (V&V) program during the software development and implementation processes.

3.2. HCCS V&V Philosophy

This section gives an overview of the V&V activities for replacement of HCCS (hereinafter referred to as the HCCS project). Software V&V activities for HCCS was conducted in order to assess whether the new control system met its specifications and requirements. To determine the minimum V&V tasks for HCCS project, software integrity level (SIL) was classified based on IEEE 1012.

SIL is a range of values representing the software complexity, criticality, risk, safety level, security level, desired performance, and reliability, and defines the importance of software to the users [1]. The control and regulating system of the HANARO research reactor is important in terms of availability, but is a non-safety system. HCCS software was therefore assigned to integrity level 2. Table 1 shows the classification of software integrity level.

TABLE 1. SOFTWARE INTEGRITY LEVEL CLASSIFICATION

Software Integrity Level				
Software Program Manual	Safety Critical (SC)	Important to Safety (ITS)	Important to Availability (ITA)	General
Software Integrity Level (IEEE 1012)	SIL-4	SIL-3	SIL-2	SIL-1

The general philosophy for V&V activities are as follows:

- To ascertain that the control algorithm being used at the old control computer will ported to the HCCS without any changes.
- To simulate the operational conditions using a dynamic test bed for conductin g the tests in a practical manner.

- To verify that the new control computer system will not impact other operatio nal systems.
- To conduct V&V by a competent group independent from the design group, as shown in Figure 5.

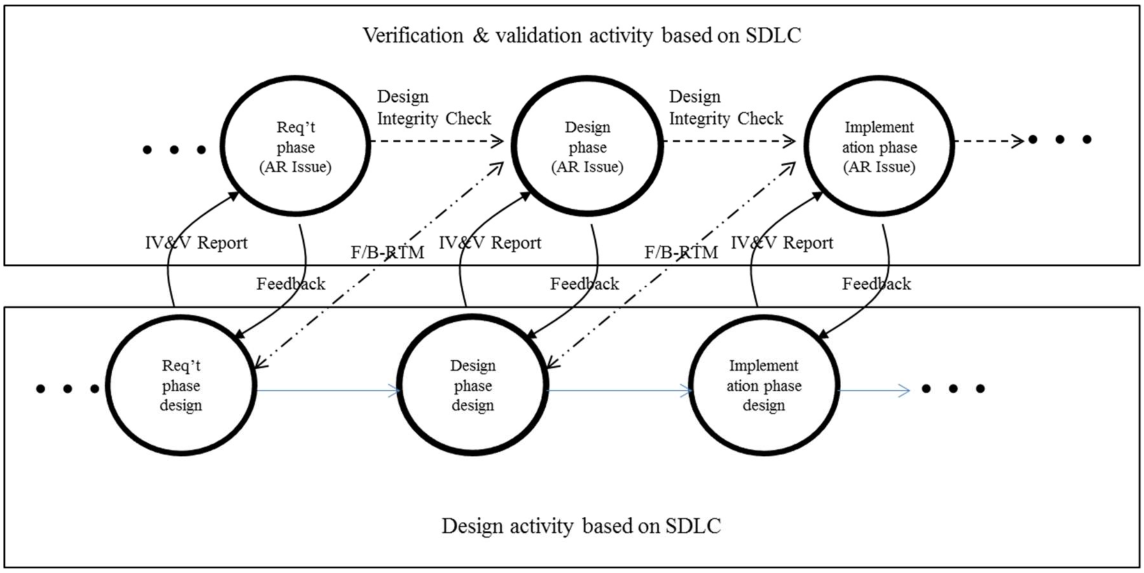


Figure 5. Interface between Design and V&V based on SDLC

3.3. HCCS V&V Activities

The software development life cycle (SLDC) for developing HCCS was composed of seven phases: planning, requirement, design, implementation, testing, installation and checkout, and operation and maintenance [5]. A traceability matrix of the critical requirements was established by analyzing the identified relationships for correctness, consistency, completeness, and accuracy throughout each phase of SDLC.

In the planning phase, planning documents for the project, including a software development plan, quality assurance program, V&V plan, and software configuration plan including cyber security plan and procedure, were established. V&V was performed for the requirements of the installation and checkout among the seven phases of SDLC. Anomalies were also cleared through each iteration of the V&V phase, changes to the program, and testing. The system and software, which were inputs to V&V, were to be modified for anomaly corrections, quality improvement, or requirement changes in the course of the V&V. When a system or software was modified, additional V&V activities were repeated according to the iteration policy. An evaluation of the cyber security and a risk analysis were conducted while performing V&V tasks by an independent competent group. Table 2 shows the V&V tasks, and the required inputs and outputs, in each phase.

TABLE 2. HCCS V&V TASK

Phase	V&V Tasks	Required inputs	Required outputs
Planning	Stakeholders meeting, Milestone and strategy establishment	Legacy design inputs, project circumstances, existing plan and procedure for software development	Quality assurance plan, Software development plan, V&V plan and procedure, configuration management plan and procedure, cyber security plan
Design	Design evaluation Traceability analysis on software design	SDD	Design V&V report RTM Anomaly report Check list
Implementation	Source code evaluation Traceability analysis on source code	Source code Control logic diagram	implementation V&V report RTM Anomaly report Check list
Testing	Test procedure and report evaluation Traceability analysis on testing	Source code Test plan and procedure Test reports	testing V&V report RTM Anomaly report Check list
Installation and Checkout	Cyber security analysis Risk analysis Installation checkout	Installation package Security and risk analysis report	V&V report including security and risk analysis Anomaly report

4. CONCLUSIONS

The MLC of HANARO has been used for 17 years, since HANARO achieved first criticality. The lifetime of the electronics is shortening with a growth in informatics technology. The supplier of the MLC disappeared, and thus the technical support for this system is no longer guaranteed and no spare parts are available. The refurbishment program of the HANARO control computer was launched in 2010 and was completed in 2015. Through a functional analysis of the previously programmed system, a software quality plan including all required software documentations for approval from the regulatory agency was achieved. In particular, the algorithm used in the RRS (Reactor Regulating System) was simulated using the DTB (dynamic-test-bed) before the new control computer system was installed. Independent verification and validation of software were conducted throughout SLDC based on IEEE 1021. The V&V activities were iterated until all crucial anomalies were resolved. The V&V activity on HCCS was completed successfully and its function was confirmed through functional tests using a dynamic test bed during the V&V activities. All tests at each phase showed satisfactory results, and the new system was successfully installed. However, an on-site functional test and its verification and validation were postponed owing to seismic retrofitting of the reactor containment building.

REFERENCES

1. “Refurbishment Program of HANARO Control Computer System”, H.K. Kim, ICAPP 12, Chicago, USA (2012)
2. “IEEE Standard for Software Verification and Validation”, IEEE Std. 1012 (2004)
3. “IEEE Standard Glossary of Software Engineering Terminology”, IEEE Std. 610.12 (1990)
4. Dolores R. Wallace and Roger U. Fujii, “Software Verification and Validation: An Overview”, *IEEE Software*, **May 1989**, pp.10-17 (1989).
5. “Software V&V Plan & Procedure for HCCS”, KHCCS-VV101 (Rev.3) (2014)
6. “Risk Analysis Report on HANARO Control Computer System”, HCRA-PD-RAR-2013080R0 (2013)

SAFETY EVALUATION ACCORDING TO CONTROLLER CONFIGURATION USING SAFETY INTEGRITY LEVEL

M.G. CHUN
School of Electronics Engineering, Chungbuk National University, Korea
E-mail : mgchun@cbnu.ac.kr

Abstract

A SIL(Safety Integrity Level) assignment method is used for preventing failure action. The goal of safety system for processing automation is to reduce the human fatal risk. Even if we have developed the processing automation according to developing technology, we are also realized on increasing the human fatal risk cause of unexpected accidents. This study is directed the solution of decision for safety level for safety system and the best architecture for safety system in process automation.

1. INTRODUCTION

Beginning with the 18th century James Watt steam engine, the history of control has been developed brilliantly. In modern times, the important classifications of control systems are divided into PLC (Programmable Logic Controller) and DCS (Distributed Control System), but as the technology develops, such distinction between these systems is becoming blurred. These control systems are becoming more complex and diverse as each part is modularized. Also, because the requirements of the basic components are designed not to be a single configuration but to a redundant or triplet configuration depending on the field and the process applied to the process, rather than merely dividing the functions of the control system, it is a requirement for automation systems in modern industrial processes that continuous operation is required without affecting the operation of the process even if a failure occurs [1][2]. In the reflection on these requirements, it is true that the profitability aspect of industrial process is a tremendous increase but, in terms of humanism, interest in safety is also growing also and, Having the optimal requirements of these two aspects is getting a big issue in modern industrial processes. However, due to the lack of various interests and information sharing in the control system configuration for safety, there are few cases applied to the industrial process.
The distribution of casualty cases investigated by the Safety and Health Executive (HSE), a representative safety agency in the UK, show that occupational accidents after the commissioning of factories accounted for more than 60% of all accidents. In fact, to solve these problems, the USA released the "the Standard of Safety Instrumented System" with the ISA (Instrument Society of America) and IEC (International electrotechnical Commission) in 1996. Prior to performing the Safety Instrumented System, the safety integrity level (SIL) of the system must be set in advance. In order to solve the problems that can occur with the qualitative decision method proposed by ISA / IEC, a method of determining the safety integrity level of the control system using the tool, which is a quantitative risk assessment method, has been proposed [3-5].

In this study, we propose the optimal operation method of the controller by calculating the safety level according to the inspection period and configuration of the control system based on the SIL of the International Electrotechnical Commission (IEC) which is the safety standard of the modern industrial process.

2. THE SAFETY INTEGRITY LEVEL AND CONFIGURATION OF CONTROLLER

2.1 Safety Integrity Level (SIL)

The SIL is a rating of the probability of satisfactorily performing within a certain period of time for a unit process. In general, the SIL is classified as 1 to 4 according to the value of PFD (Probability of Failure on Demand per year) as the table 1, it means that the higher the number of ratings, the higher the probability of being performed normally [6][7].

In order to calculate the PFD value, various setting values is used such as Proof Test Interval (PTI), Mean Time To Repair (MTTR), Diagnostic Coverage (DC), and so on.

TABLE 1: SIL ACCORDING TO PFD

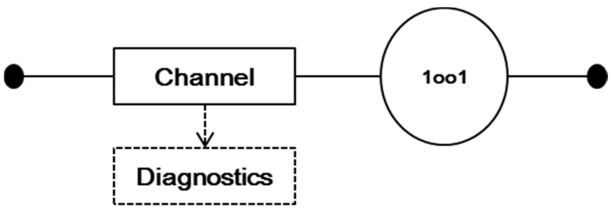
SIL	PFD
SIL 4	$10^{-5} \leqq$ PFD $\langle 10^{-4}$
SIL 3	$10^{-4} \leqq$ PFD $\langle 10^{-3}$
SIL 2	$10^{-3} \leqq$ PFD $\langle 10^{-2}$
SIL 1	$10^{-2} \leqq$ PFD $\langle 10^{-1}$

2.2 The Configuration of Controller [8][9]

(1) The 1oo1 configuration

As shown in Figure 1, the 1oo1 configuration consists of a single channel for each channel. Here, all dangerous faults lead to failure of the safety function on demand. This configuration does not provide fault tolerance and failure mode protection.

Fig. 1 1oo1 Diagram



(2) 1oo1D configuration

As shown in Figure 2, the 1oo1D configuration consists of a single channel for each channel. During normal operation, the channel needs to require a safety function before the safety function occurs. If a diagnostic test detects a defect in the channel or a mismatch that cannot be assigned to the channel is detected, the output becomes safe state. This configuration represents the enhancements used for safety applications. Diagnosis can convert detected dangerous failure into safe failure. In general, an additional failure rate has to be included in the quantitative analysis, taking into account additional diagnostic channels.

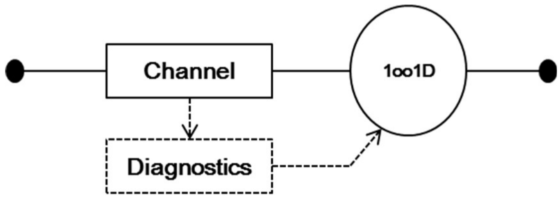


Fig. 2 1oo1D Diagram

(3) 1oo2 configuration

As shown in figure 3, the 1oo2 configuration is composed of two channels arranged in parallel so that each channel can process the safety function. Therefore, there may be danger, that is, there can be a fault in both channels before the safety function fails. Diagnostic tests represent faults that have occurred and do not change output state or output boating.

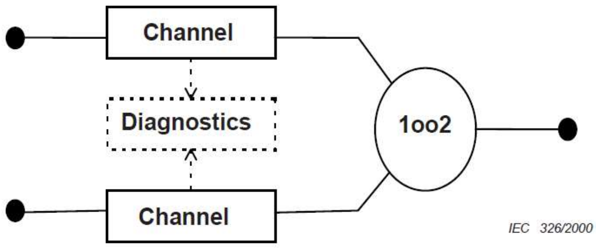


Fig. 3 1oo2 Diagram

(4) 2oo2 configuration

As shown in figure 4, the 2oo 2 configuration is composed of two channels in which respective channels are connected in parallel. Therefore, before safety functions occur, both channels need to require safety functions. Diagnostic tests represent faults that have occurred and do not change output state or output boating.

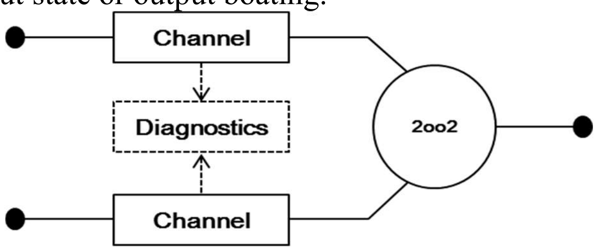


Fig. 4 2oo2 Diagram

(5) 2oo3 configuration

As shown in Figure 5, the 2oo3 configuration is composed of three channels connected in parallel to a number of boat devices with respect to an output signal. Thus, the output state is not changed when merely one channel does not match the other two channels. Diagnostic tests represent faults that have occurred and do not change output state or output boating.

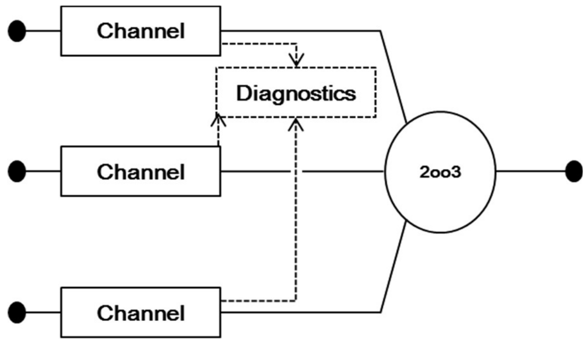


Fig. 5 2oo3 Diagram

(6) 1oo3 configuration

As shown in Figure 6, the 1003 configuration is constituted by three channels in which each channel is made in parallel, and the output state follows 1 o 3 boating. Diagnostic tests represent faults that have occurred and do not change output state or output boating. The configuration diagram is the same as 2oo3, but the output guarantees the output even though only one of the three inputs is normal

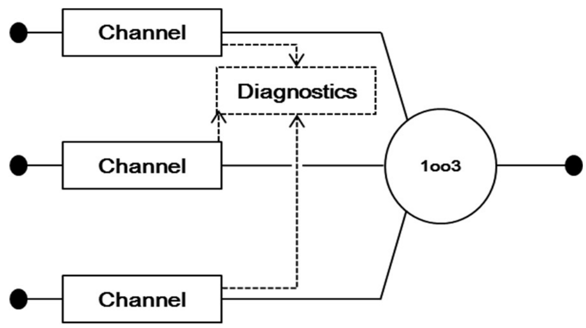


Fig. 6 1oo3 Diagram

(7) 3oo3 configuration

As shown in Figure 7, the 3oo3 configuration consists of three channels with each channel in parallel, and the output state follows 3oo3 boating. Diagnostic tests represent faults that have occurred and do not change output state or output boating. The diagram is the same as 2oo3, the output guarantees the output only if all three inputs are normal.

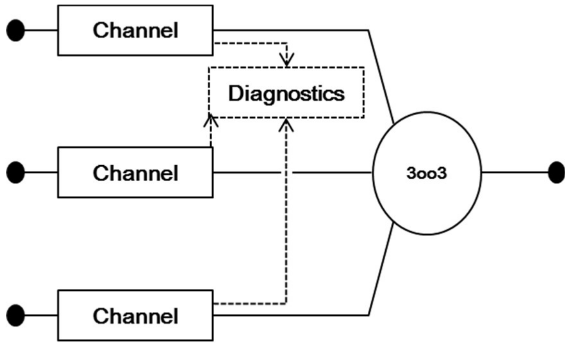


Fig. 7 3oo3 Diagram

3. THE EVALUATION OF STABILITY OF CONTROLLER USING SIL TECHNIQUE

3.1 Stability evaluation method of controller

In this paper, the system was constructed as shown in Figure 8 in order to evaluate the inspection cycle of the controller and the stability due to the components. In Figure 8, the sensor means a flowmeter and output part represents a valve for control the flow rate. The controller considered RTP (Real Time Products), which is widely used in nuclear and petrochemical processes due to its high safety rating. The RTP controller shown in Figure 9 is a module in which power supply, input / output card, and central processing unit are all modular, so that each module can be configured as single, double, triple or quadrature.

In this study, we try to evaluate the SIL rating of the whole system according to the inspection period and the components of the controller. For decision of SIL rating, the mean time to repair (MTTR) of the input element, the flow sensor and the output element were set to 24 hours, the diagnosis range (DC) was 90 [%], and the inspection period (PTI) was 1 year, and the stability of the controller was evaluated by using the exSILentia program provided by Exida [10].

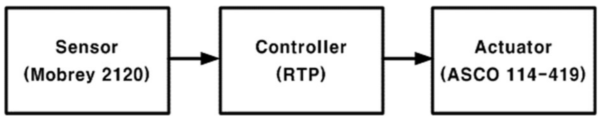


Fig. 8 System configuration

Fig. 9 RTP Controller

3.2 Stability evaluation according to the proof test interval of the controller

In order to evaluate the stability according to the proof test interval of the controller, the controller configuration was set to 2oo3, the Mean Time To Repair (MTTR) was 24 hours, and the diagnosis range (DC) was 90 [%], and then the stability of controller according to the proof test interval was evaluated. The proof test interval divided into 1 month, 3 months, 6 months, 9 months, 1 year, 2 years, 3 years, 4 years, 5 years, 6 years, 7 years, 8 years, 9 years, and when without proof test, and the stability evaluation of controller was performed.

Figures 10 and 11 showed PFD according to time when without proof test, and PFD according to time when the proof test interval was 1 year. As shown in Fig. 10, the SIL of the controller is judged to level 2 when there is no proof test. On the other hand, if the proof test interval is one year, the SIL of the controller is shown as level 3, and if operated with an appropriate proof test interval, it can be seen that the SIL can be operated properly within the desired SIL rating.

Figure 12 compared the PFD, which is the annual failure probability of the controller and the system (SIF), according to the proof test interval of the controller. In Figure 12, the first bar (blue) represents the PFD_{avg} of the system (SIF), the second bar (red) represents the PFD_{avg} of the controller (SIF). As shown in Figure 12, the shorter the proof test interval, the lower the PFD_{avg}. Also, at the point when the proof test interval is 1 year, the PFD_{avg} of the system becomes smaller than 10^{-3}, and the SIL level is upgraded from SIL 2 to SIL 3.

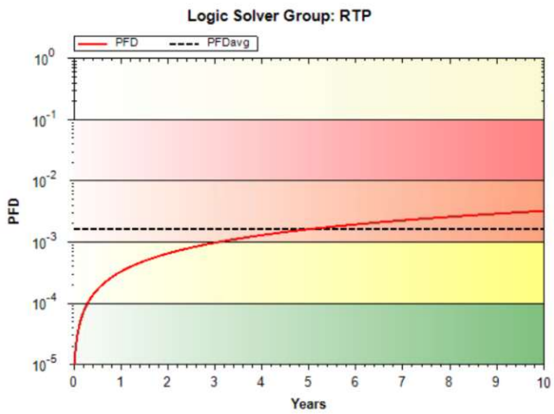


Fig. 10 PFD without proof test according to time

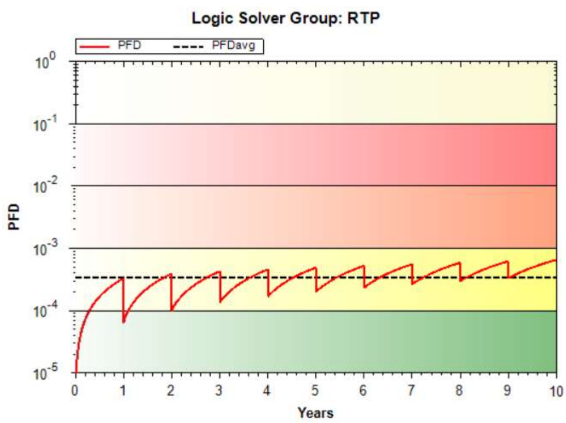


Fig. 11 PFD with proof test(1 year) according to time

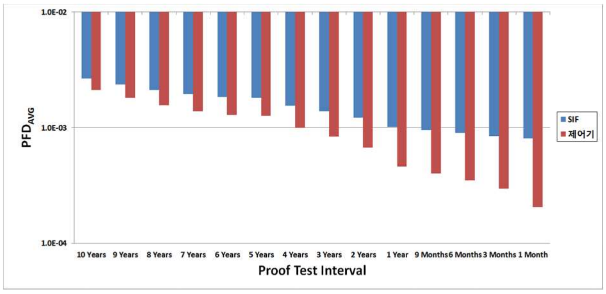


Fig. 12 PFD for controller and system according to proof test interval

3.3 Stability evaluation according to controller configuration

The proof test interval of the controller was fixed at 1 year, and the PFD, which is the annual failure probability of the controller and the system according to the configuration of the controller, was analyzed. In Figure 13, the First bar(blue) represents the PFD_{avg} of system(SIF), and the second bar(red) represents the PFD_{avg} of the controller. As shown in Figure 13, the PFD of the controller changes as the configuration of the controller changes, and the PFD of the overall system changes accordingly. In particular, if the controller structure is changed from 3oo3 to 2oo2, the PFD of the system becomes smaller than 10^{-3}, and the SIL level increases from SIL 2 to SIL 3

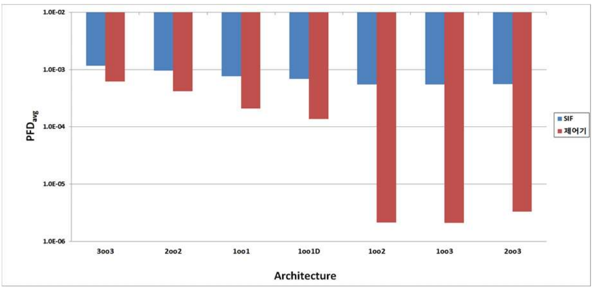


Fig. 13 PFD according to controller configuration

Here, it is necessary to discuss correlations with availability that is important to process efficiency rather than simply discussing only the PFD values that determine safety ratings. Availability means that the system performs the function normally without failures, and expressed as formula (1). In formula 1, MTTF(Mean Time To Failure) means the average time from the present failure point to the next failure point, MTTR(Mean Time To Repair) means average recovery time.

$$\text{Availability} = \frac{\text{MTTF}}{\text{MTTF+MTT}} \qquad (1)$$

Figure 14 compares the availability of the overall system according to the controller configuration with the PFD. In the Figure 14, the first bar(blue) represents the availability of the system, and the second bar(red) represents PFD of the system. As shown in Figure 14, when the controller configuration is 2oo3, it is confirmed that both the availability and the PFD values are satisfactory.

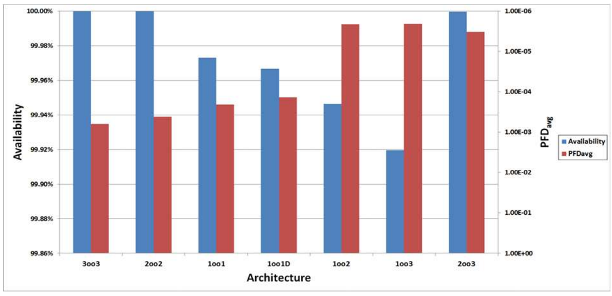


Fig. 14 Availability and PFD according to controller configuration

5. CONCLUSION

In this paper, PFD, which is the annual failure probability according to the inspection period and controller configuration, was evaluated using a model consisting of sensor (flow meter) - controller (RTP) - output (valve) widely used in nuclear and petrochemical fields, and using the evaluated PFD the Safety Integrity Level(SIL) was decided. As a result of the evaluation according to the inspection cycle, it was confirmed that the SIL grade was upgraded from 2 to 3 when the inspection cycle was within 1 year. In addition, as a result of the safety evaluation according to the controller configuration, the 2oo3 controller configuration showed that the PFD value that affects the safety level has good results in terms of the critical point of SIL 3 and the availability in which the system can function normally without obstacle, it was found that this is an optimal solution when designing. it is considered that this experiment can be applied to establish a safe and highly usable control system in all industrial fields.

References

[1] Sung-Kyun Ryou, Jae-Young Park, Hak-Sun Yun, “An Allocation of Safety Integrity Level to Inductive Loop type Train Control System,” JKIECS, Vol. 8, No. 12, pp. 1905-1910, 2013.

[2] Deung-Ryeol Yoo, Key-Seo Lee, “A Study on Architecture Design of Power Supply for SIL4 Safety Related System,” JKIECS, vol. 10, no. 9, 1001-1008, 2015.

[3] J. Beugin, D. Renaux, L. Cauffriez, “A SIL quantification approach based on an operating situation model for safety evaluation in complex guided transportation systems,” Reliability Engineering and System Safety, Vol. 92, pp. 1686–1700, 2007.

[4] Hamid Jahaniana, QamarMahboobb, “SIL determination as a utility-based decision process,” Process Safety and Environmental Protection, Vol. 102, pp. 757–767, 2016.

[5] Feng Wang, Ou Yang, Ruibo Zhang, Lei Shi, “Method for assigning safety integrity level (SIL) during design of safety instrumented systems (SIS) from database,” Journal of Loss Prevention in the Process Industries, Vol. 44, pp.212-222, 2016.

[6] IEC61511-1, 2003. Functional Safety-Safety Instrumented Systems for the Process Industry Sector–Part 1: Framework, Definitions, System, Hardware and Software Requirements. International Electrotechnical Commission.

[7] IEC61508-4. 2010. Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-Related Systems. Part 4: Definitions and Abbreviations. International Electrotechnical Commission.

[8] IEC61508-6, 2000. Functional Safety of Electrical/Electronic /Programmable Electronic Safety-

Related Systems. Part 6. Guidelines on the Application of IEC61508-2 and IEC61508-3. International Electro -technical Commission.
[9] IEC61508-6 2010. Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-Related Systems. Part 6. Guidelines on the Application of IEC61508-2 and IEC61508-3. International Electrotechnical Commission.
[10] http://www.exida.com/exSILentia

DESIGN AND IMPLEMENTATION OF DIGITAL INSTRUMENTATION AND CONTROL SYSTEM FOR PUSPATI TRIGA MARK II REACTOR, MALAYSIA

Maslina Mohd Ibrahim, Ridzuan Abdul Mutalib, Mohd Sabri Minhat, Mohd Khairulezwan Manan, Mohd Fairus Abdul Farid, Alfred Sanggau Ligam, Nurfarhana Ayuni Joha
Malaysian Nuclear Agency, 43000 Kajang, Selangor, Malaysia
E-mail: maslina_i@nm.gov.my

Abstract. The Reactor PUSPATI TRIGA Mark II (RTP) console and control system was designed, constructed, installed and commissioned by General Atomic Company (GA). The RTP has been operated by using this system since 1982 before it being decommissioning and upgrades to a new system in 2014. The upgrading to digital instrumentation and control system was completed in 2014 by a collaboration between Nuclear Malaysia and Korea Atomic Energy Research Institute (KAERI) under the project titled; Reactor Digital Instrumentation and Control System (ReDICS) for PUSPATI TRIGA Reactor (RTP). The project was first instigate due to the increased in system instability, errors on system indicators, nonfunctional functions and other concern factors that indicate the aging and degradation of the old system. The scope of modernization for the instrumentation and control (I&C) system are comprises of two independent system which are; Reactor Control and Monitoring System (CMS) and Reactor Protection System (RPS). The CMS provide operator information about the plant operation, to run under open loop control, under close loop control and to process command from the operator. While the RPS is totally hardwired design type for automatic shut-down the reactor operation whenever operating parameters exceeding the safety limit setting. The general design bases for the safety-related are following the International Atomic Energy Agency safety guide documents; IAEA Safety Standard on "Safety of Research Reactor " NS-R-4. The process of the implementation is divided into three stages which are; pre-implementation phase, implementation phase and post implementation phase. This paper will describe the design and implementation of the modernization that consist of these three stages.

Keywords: instrumentation and control system, Reactor Control and Monitoring System, Reactor Protection System

1. INTRODUCTION

The Reactor PUSPATI TRIGA Mark II (RTP) is located at Malaysian Nuclear Agency and is the only nuclear research reactor in Malaysia. The reactor starts its operation in 1982 and reached its first criticality on 28 June 1982. The instrumentation and control of the RTP was the state-of-the-art of the system which were an analog base engineering with some digital components. The system was used to control and monitor the 1 MW thermal reactor power with maximum neutron flux of 1x 10^{13} $ncm^{-2}s^{1}$, reactor safety and plant operation. The new Instrumentation and Control (I&C) system called 'Reactor Digital Instrumentation and Control System' (ReDICS) was replaced the old system by using digital approach while maintaining the system functionality as well as system safety. The decision of the modernization of the old console was basis on the studied that was done since 2003.

The process of modernization can be categorized by three phases which are pre-implemention, implementation and post-implementation. The pre-implementation was included the series of discussion with the regulator on project management, standards, safety criteria, quality assurance and safety analysis. The draft documents on quality assurance and preliminary safety analysis report for the intended system design was prepared in this stage.

The stages of the internal process on the project proposal starts by the full engineering studies by reactor instrumentation maintenance group, engineering audit by internal committee, IAEA expert report, Nuclear Infrastructure Safety committee and SHE committee, formation of Technical & Project management group and management finance division. The Implementation phase consists of activities such as fabrication, installation and commissioning.

The implementation of the project is manage by the Technical & Project Management Group. The design of the new instrumentation is the combination of an analog, digital and computer-based system. It is a modular type comprises of several cabinets such as Reactor Protection System 1 and 2, Control and Operation Console, Data and Acquisition interface and communication cabinet. The Operation and Control console where the reactor operator to operate and control the reactor by controlling the movement of control rods. The control rods movement are using control rod buttons via microprocessor-based control rod controller. Operation and control data are monitored using liquid crystal display. The Wide-range channel receiving the analog signals from the fission chamber and process by digital signal processor. The flux controller is using an industrial computer and software for flexibility and functioning in reactor operation and control, data and records, fuel burn-up calculation and archive. Meanwhile, the Reactor Protection System (RPS) is totally hardwired design type for automatic shut-down the reactor operation whenever operating parameters exceeding the safety limit setting. During this stage, the staff of Nuclear Malaysia were also attached to KAERI to be involved directly during the design and development of the project under the programmed called Transfer Technology Programmed (TTP). The final, post implementation stage was the process of training/retraining the reactor operators for familiarity and to obtain the required license for operating. The proper and complete document are also established for the operation and maintenance staff.

2. BASIS FOR MODERNIZATION

The studied was done due to the increase of system instability, errors on system indicators, non-functioning functions, intermittent signals in the system, increased of reactor down time and increased in maintenance time. The effort to fix the majority of the fault area hinder by major difficulty due the aging of the system components and modules, obsolescence of spare parts, no technical support from the manufacturer and the pensioning of experience staffs. Hence, the operation shown the obvious decrease to less than 50% of operating time and the increase of the downtime of the reactor.

To confirm the needs for modernization, the engineering assessment on the reactor I&C were made in the year 2003 and 2007. In the year 2003 an internal audit committee was set up. The committee members were personnel of a nuclear engineer from Engineering Department, physicist from Industry Department and electronic engineer from the Instrumentation and Automation Department. The assessment by the internal audit team concluded that changing the reactor I&C to a new system shall be seriously considered in order to fulfill the safety aspect and following the technology trend of today. In the year 2007, the International Atomic Energy Agency (IAEA) expert was invited to do the assessment and they had recommended that the present human machine interface of reactor console was currently very poor. A replacement towards a digital Control and Monitoring system is recommended. Table I below shows the summary of the assessment report that was made by the audit team and IAEA expert for old I&C system before the replacement of ReDICS.

TABLE I. SUMMARY OF ENGINEERING ASSESSMENT OF I&C SYSTEM

No.	System Failure / Problems	Reactor Audit Team (2003)	IAEA Expert (2007)
1	Square –wave Mode (operating mode)	Not functioning	Could not do testing
2	Automatic Mode (operating mode)	Not functioning	Could not do testing
3	Pulsing Mode (operating mode)	Not functioning	Could not do testing
4	Left Compartment of I&C Console	Hotter need extra ventilation	Extra fan installed in the left compartment
5	Wide range Log power channel	Wide range channel problem	Startup shows unstable reading
6	Control Button / Switch; Transient, safety, shim2	Need to change	Very poor and avoid jamming
7	Log wide range power channel	Need to change	Obsolescence problems on channels

3. SCOPE OF THE MODERNIZATION

The scope of modernization was carefully studied to make sure that the succeeding of the project. The modernization objective was not only to replace the old I&C system in order to prolong the used of the reactor but it also has to meet the functionality and performance of the old I&C system. At the same time the new system should not compromise all the safety aspect and meet all the regulatory aspect. As a result, the ReDICS was designed to comprise the following sub-systems:

3.1 Data Acquisition and Control system (DACS)

The DACS used the redundant computer system with I/O boards and network cards. The DACS receive data from field instruments via input board, processes appropriately, send the display parameters to the operator workstation (OWS), and transfers the control signals to the control rod drive mechanism via output board. The data were stored in the storage device in the computer and they could be retrieved for future use. The field instruments such as radiation monitoring system and seismic monitoring system were added on to those specified on the old I&C system.

3.2 Operator Workstation (OWS)

The OWS comprises of an operator console, which houses the hardware of DACS and RPS, the display devices for the monitoring of the reactor status, and any control devices used for the manipulation of the reactor. The values and status of the reactor parameters were displayed in an appropriate format for ease of recognition of the reactor status. Operator may intervene on the control loop if necessary. Otherwise reactor can be operated without any interruption of operator. The Human Machine Interface (HMI) was designed with applications of the ergonomics and human factors principles. There are 3 operation modes such as MANUAL, AUTOMATIC, and SQUARE-WAVE.

3.3 Reactor Protection system (RPS)

The RPS shut down the reactor if a trip parameter exceeds its set points. It consists of the sensors, measuring systems, logics, and actuators. The design RPS is "fail safe" concept following the IAEA Safety Series documents. Any abnormalities or failures occurs during the reactor operation, the RPS shall shut down the reactor immediately without any interference or intervene by the reactor operator. The basic safety system design was following the requirements of the present system technical specifications, some new operator's needs, quality assurance and advices from the internal safety committees for main facility and the regulator. The basic design being used by the supplier as the reference to produce the Basic Design document which was one of the important document for construction approval. Trip parameters and set-point for ReDICS is shown as Table II below:

TABLE II. TRIP PARAMETERS AND SET POINT OF RPS

	Trip parameters	**Normal Value**	**Trip Set Point**
1	Fuel Temperature Hi	250oC	500oC
2	Over Power	1000Kw	110%
3	Short Period	<3 sec	3 sec
4	Low Pool Water Level	Top reactor tank	Below 30cm
5	Malfunction on WR-NMS	750 Volts for fission chamber	25% of nominal operating voltage

The 4 control rods were dropped into the core if the RPS system generates the reactor trip signal by disengaging the electromagnet of the SHIM, SAFETY, REGULATING rods and by discharging the compressed air through solenoid valve of the TRANSIENT rod. The control rods were also drop with a manual trip button at the console and remote.

3.4 Wide Range-Neutron Measuring system (WR-NMS)

The WR-NMS receives pulse signal from the fission chamber located outside the reactor core. The signals were amplified by the pre-amplifier and processed further by the appropriate detection system. The neutron flux level (either linear or log scale) and the reactor period signals are transferred to the DACS or RPS accordingly.

3.5 Control Rod Drive (CRD)

Four (4) control rods are used in RTP namely SAFETY, SHIM, TRANSIENT, and REGULATING. All rods were positioned at the specified position by activation of the manual control mode. Only the regulating rod can be controlled by setting the specified power level at the automatic operation mode. The rod movement signal generated in DACS transfers to the control rod driver through the I/O board. The control rod drive mechanism located on the reactor bridge contains the electromechanical devices to control the rods together with rod position indicators.

4. APPLICATIONS AND LICENSING

4.1. Project Management

In order to successfully implemented the modernization of the I&C system, one of the most important factor is the creation of project management. The project management was the main structure that control all the operation of the project especially on the applications and licensing. The project management team is divided into four project groups to allow better management control. The project management committee which consists of technical and management team, including the regulatory body are needed to manage and balance the needs and expectations in such to ensure the success of this project. The project technical, safety, quality control and licensing group are led by a project manager that has been appointed by the project advisor. The project manager was the interface between the supplier and the Radiation Protection Officer (RPO). All communications between the regulators is done by the RPO of Nuclear Malaysia.

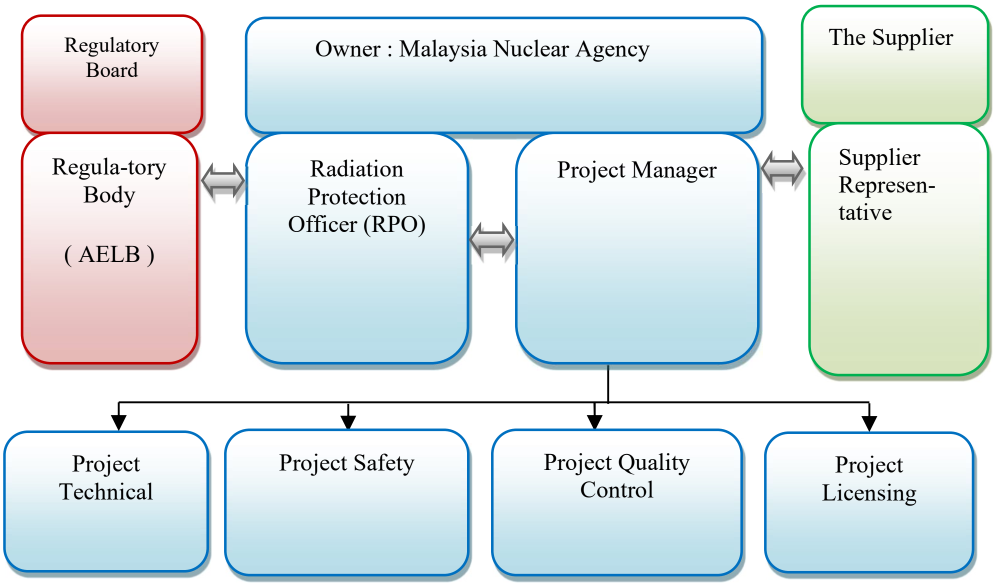


FIG.1.The Project Management Structure

4.2 Safety Requirement

The general design base for the safety-related are following the International Atomic Energy Agency safety guide documents; they are the IAEA Safety Standard on "Safety of Research Reactor " NS-R-4 especially on para 6.6 – 6.11; Defense in Depth, para 6.35 – 6.43 ; Design for reliability, para 6.90 - 6.94 ; Reactor shutdown system and para 6.95 - 6.105 ; Reactor protection system. The IAEA Safety Series No.35-S1 especially on para 646 – 651; Requirements for instrumentation and control system and The IAEA Safety Series No.35-G5; Safety Assessment of Research Reactors and Preparation of the Safety Analysis Report on para A.8; I&C System in reactor protection system, reactor power regulating system, alarm system interlocks, other instrumentation systems for safety and control room. The safety of the I&C systems is designed to ensure the required performance and reliability of safety function even at postulated abnormal conditions.

4.3 Process Design Review and Approval

All reports on the I&C system were compile into a special report. The report was presented to the Safety Committee of Main Facilities and budget request to the Ministry of

Finance. A Project Committee was set up for project management, technical, licensing and quality assurance. The regulator and Nuclear Malaysia had done a lot of discussion to finally agree to the proposal of a new basic I&C system design. During the time of discussion taking place, Nuclear Malaysia also has started the preparation on the technical specification on the new I&C system.

The development of the project is following the local regulator requirement, the Standards for Modification of Research Rectors (LEM TEK 53) under Category A of the Malaysia Atomic Energy Licensing Board. The stages for approval consist of three (3) main stages, they are pre-implementation phase, implementation phase and post implementation phase. For the pre-implementation, two discussion being done with the regulator on project management, standards, safety criteria, quality assurance and safety analysis. Nuclear Malaysia needed to prepare the draft documents on quality assurance and preliminary safety analysis report for the intended system design.

In the Implementation phase, three stages of activities were implemented which are fabrication, installation and commissioning. In this phase, the appointed supplier (KAERI) is the main and important agency with the support of Nuclear Malaysia to fulfill the requirement of the regulator. The following chapters in an application document were produced and the review of chapters 2, 8 and 16 of the present SAR document of the RTP for the construction approval by the regulator. For obtaining the commissioning approval of the I&C system Nuclear Malaysia demonstrated that the modified SSCs were installed according to the design intents to the regulator. The commissioning program has been produced for checking and verifying the safety of the modified I&C system. Application for the commissioning approval to the regulator was supported by the revised safety report for the modification. Finally the approval for the routine operation of the reactor, Nuclear Malaysia had submitted the revised safety report and the commissioning result including the assessment that the design intents of the modification of the I&C system that has been archived. FIG.2. below shows the flow of the design review and approval.

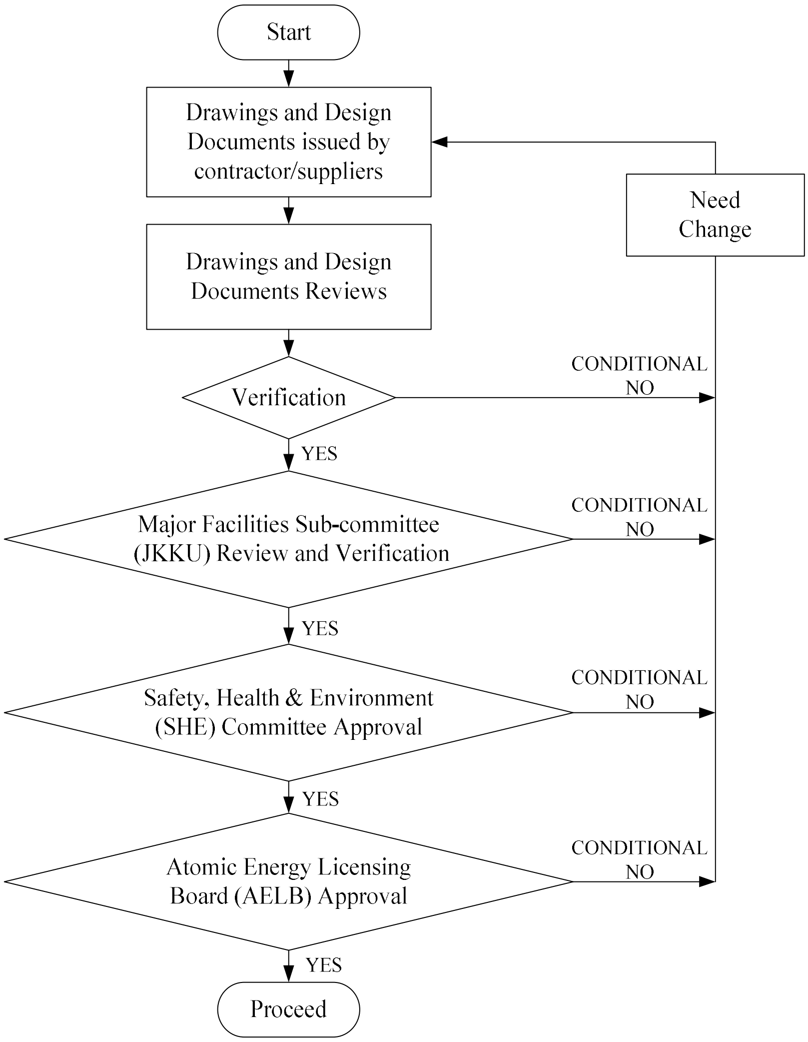


FIG.2.Process Design Review and Approval

4.4 Training/retraining and qualification

The operating license was given after the completion of commissioning stage. For obtaining the approval for routine operation of a modified reactor, Nuclear Malaysia submitted to the AELB the documents; Updated Safety Analysis Report, new operating limits and conditions, and commissioning results; including an assessment that the design intents of the modification project have been achieved.

5. DESIGN, FABRICATION, INSTALLATION AND COMMISSIONING

5.1. Design and fabrication

Basically the instrumentation and control system comprises of two independent system, the reactor protection system and reactor control and monitoring system. The system is to provide operator information about the plant operation, to run under open loop control, under close loop control and to process command from the operator. Those I&C system's function enable the operator to performed operating the plant safely and efficiently in all its operation state, to take measures to maintain the plant in its safe state or to bring it back to it safe state after an onset of either accident condition or design basis event and to supervise specific tasks. The components of the instrumentation and control system are man-machine interface, control console and supervision desk, open-loop and close loop control system, instrumentation racks, condition units and sensor and also actuator.

The reactor can be operated in two operation modes namely NORMAL and SQUARE-WAVE. An operation mode is selectable by setting operation mode switch on reactor operating console. In NORMAL operation mode, all control rods can be controlled upward or downward. The SQUARE-WAVE operation mode allows the power level to be raised quickly to a desired power level by manually firing transient rod. All functions essential to operation of the reactor are controlled by the operator from a desk-type console that contains the electronics of the instrumentation and control system. The Safety Criteria for the design of the I&C system are;

The Single Failure Criteria

> The RPS performs all safety functions required for a design basis event in the presence of any single detectable failure within the RPS concurrent with all identifiable but non-detectable failures, all failures caused by the single failure and all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions.

The Completion of Protective Action

> The RPS is designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features will continue until completion.

Independence

> Among the channels, physical separation, electrical isolation and communication, independence is to be maintained. Any credible failure on the other side channels should not prevent protective action.

Reliability

> The reliability of the RPS is designed to achieve high reliability.

Common Cause Failure Criteria

> Plant parameters are maintained within acceptable limits established for each design basis event in the presence of a single common cause failure.

Capability for Testing and Calibration

> The RPS provides means for checking, with a high degree of confidence, the operational availability of each response and command features input sensor required for a reactor trip during reactor operation.

All the components design for the new console was fabricated at KAERI and their supplier. The Factory Acceptance Test (FAT) and Inspection and Test Plan (ITP) was performed before being shipped to Malaysia.

5.2. Installation of ReDICS

The control console which houses the DACS, OWS, and RPS were installed in the control room. The field instruments and actuators were installed at the appropriate local site of RTP. The control cables between field devices and control room were interconnected and the appropriate electrical power were supplied through the power cables. All the installation was done together between KAERI and Nuclear Malaysia.

5.3. Commissioning of ReDICS

After installation of ReDICS, series of tests such as CAT(Construction Acceptance Test), SPT(System Performance Test), IST(Integrated System Test), and RPT (Reactor Performance Test) at fuel loading/ initial criticality/ low power/ power ascension stages was performed.

6. TECHNOLOGY TRANSFER PROGRAM

The technology transfer and training program was one of the important program for human resource development. The program was included in the system specification on which the supplier shall provide to the Nuclear Malaysia.

The human resource development program objective were;

i) To develop capacity and capability by sharing of knowledge between Supplier and Nuclear Malaysia on development and design of the console.
ii) To get involved in the process of testing and quality assurance activities
iii) To get involved in the process of the installation, commissioning and application process of licensing.
iv) To train in the maintenance and operation of the system.

The engineering coverage include the design concept, basic design, preparation of SAR, quality assurance & quality assurance program, detail design, fabrication, manufacturing and industrial testing of the system. The program was implemented at the supplier premise and factory. It was planned for the whole development and manufacturing of product.

7. CONCLUSIONS

The upgrades to Digital Instrumentation and Control Systems for RTP is one of the important step taken by Nuclear Malaysia in order to prolong the life of the reactor that facing challenges in several I&C areas due to ageing and obsolescence of components. The modernization also ensuring the safety of the RTP. There are a lot of factors that contribute to the successful of the project, but the proper plan and management were the key factor for the success since the project needs to covers a wide range of the system engineering including local human capacities, needs of future system maintenance and manufacturer support. Besides, project management, regulator and supplier have to be working very closely with each other. Other than that, an early involvement of regulator is very important for smooth implementation of project.

A NEW CONTROL SYSTEM BASED ON DIGITAL TECHNOLOGY FOR THE ININ TRIGA REACTOR IN MEXICO

L. CELIS DEL ANGEL, T. RIVERO, E. SAINZ, J.L. GONZÁLEZ, J. PALACIOS, J. BENITEZ.
Instituto Nacional De Investigaciones Nucleares
Carretera Mexico-Toluca s/n, La Marquesa,
Estado de Mexico, C.P. 52750,
Mexico

Abstract

The Mexican National Institute of Nuclear Research (ININ) has a 1MW TRIGA Mark III Reactor. The TRIGA MARK III is a pool type reactor with movable core and has been designed for research in the nuclear field, as well as both radioisotopes production and staff training. Its first criticality was reached on November 8th, 1968. In 1998 ININ started a project to replace the original General Atomics reactor's control console with a new one based on digital and optical electronics. In 2002, the new control console was installed. In February of 2012 Mexican TRIGA core was converted from HEU mixed core to use only LEU (30/20) fuel, as a part of this process, and considering the obsolescence of equipment and non-availability of spare parts, the instrumentation and control system is going to be modernized, by changing the actual control system to a new one using digital technology. In this work the design of the proposed new control system is shown. This control system will be based on hot stand-by redundant PLCs and will be integrated with the reactor protection system and a new HMI fully developed by ININ. This paper describes the 2002 installed control console as well as the 2012 proposed design for the upcoming I&C system and control console.

1. INTRODUCTION

The Mexican National Institute of Nuclear Research (ININ) has a 1MW TRIGA Mark III type reactor, designed and built by Gulf General Atomic. This facility is a pool type reactor with a movable core, and has been designed for research in the nuclear field, as well as both radioisotopes production and staff training. Its first criticality was reached on November 8th, 1968.

The reactor´s original control console and its associated instrumentation were based on 1960s technology. The console functioned well. However it was imperative to proceed with a renewal of these systems, mainly for the following reasons: (a) many of the electronic components were obsolete, (b) the aging of these components started causing system instability, and (c) it was necessary to overcome the limitations on the reactor operation imposed by the reduced flexibility provided by the old instrumentation when compared to the digital equipment standards

For that reason, a project to design and construct a new reactor control console to replace the original General Atomics (GA), was launched in 1993, and completed in its first stage in 1997. In 1998 ININ started a more ambitious project modernizing the 1997 design and developing a new protection system based on digital electronics and a new I&C system. In 2002, the new control console was installed.

The reactor operated until 1988 with standard 20% enriched uranium TRIGA fuel, in a uranium-zirconium hydride matrix an 8.5 wt% of uranium. Since 1989 the reactor has been operated with a mixed core compound of standard TRIGA fuel (LEU 8.5%) and FLIP fuel (HEU – 70% enriched uranium).

In February of 2012 reactor´s core was converted to use only LEU (30/20) fuel. As a part of this process and considering the obsolescence of equipment and non-availability of spare parts, the instrumentation and control system is going to be modernized by changing the actual control system to a new one using digital technology. This control system will be based on hot stand-by redundant PLCs and will be integrated with the reactor protection system and a new HMI fully developed by ININ.

Original General Atomics 2002 ININ

FIG. 1. ININ´s TRIGA control console.

2. THE ACTUAL CONTROL CONSOLE INSTALLED IN 2002

The original GA reactor´s control console operated for 34 years. In 1993 ININ started a project to replace it. The Department of Automation and Instrumentation of ININ designed and built, under a quality assurance program, a digital control console (CCD). This console bases its operation on the virtual instrument concept, where the indicators and controls are shown on a computer screen, to observe its changes and modifications that are based on the process control of the reactor itself. Surveillance monitoring is done by a computer and a network of instruments based on microcontrollers, which increases the security, flexibility and reliability of the operation. The control program was developed using oriented objects programming techniques and embedded OLE servers, allowing continuous evaluation and optimization of the process. Its installation was finished in 2002 [1].

All signals of the reactor core and the operating conditions are concentrated in the CCD. The role of instrumentation and control systems is to continuously monitor the operating parameters, such as the operating power, fuel temperature, flow and coolant temperature in the primary system, radiation levels in various areas of the facility and other parameters. The new console has the flexibility to control different reactor operation modes:

(a) Manual: control is made by the operator;

(b) Automatic: the reactor´s power is set up to 1 MW, and the control console moves two control rods to reach the previously set power;

(c) Step: the reactor´s power is set up to 1 MW and the control console extracts the transient rod, so the power is incremented very quickly but stabilized to a maxim of 1 MW; and

(d) Pulse: prompt extraction of the transient rod, so the power could reach approximately 2000 MW, for about 10 milliseconds, and the due to the intrinsic safety characteristics the reactors power down to less than 1 MW.

Also, it is possible to trace the power profile and it could perform automated diagnostic tests, such as the power calibration or the periodic review of control rod´s reactivity.

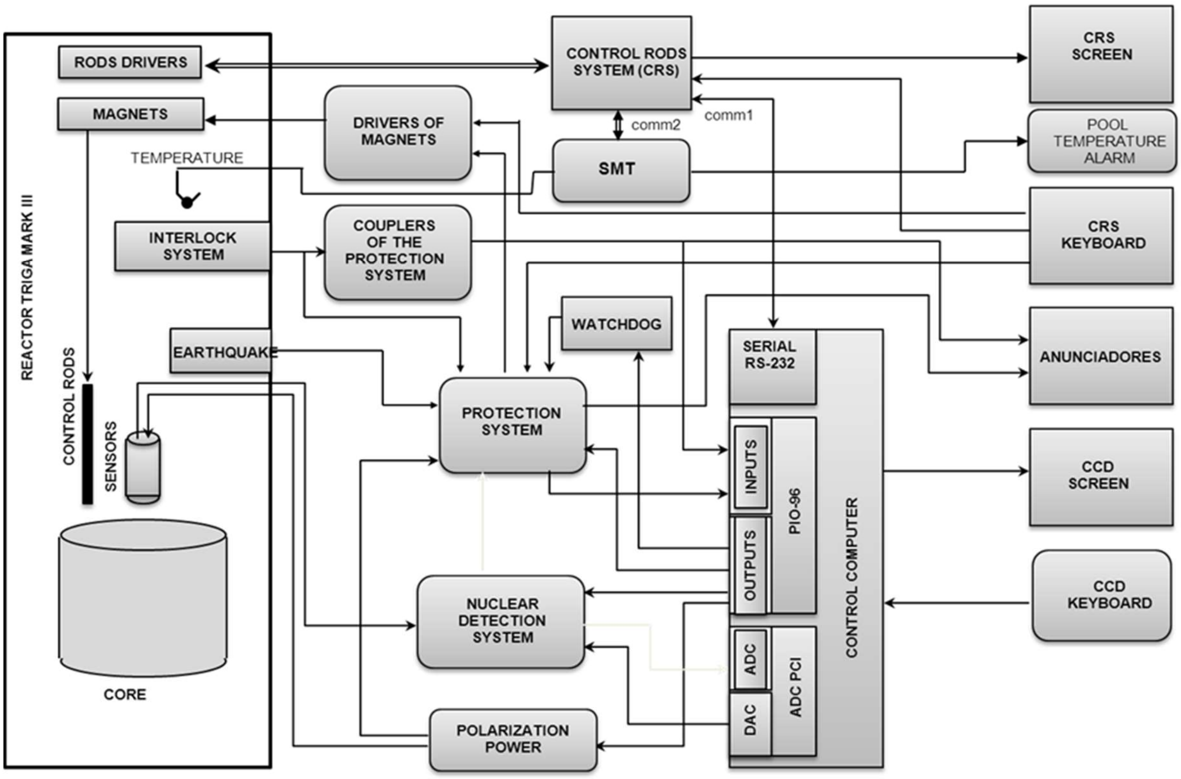


FIG. 2. Diagram of the control system designed and built by ININ in 2002.

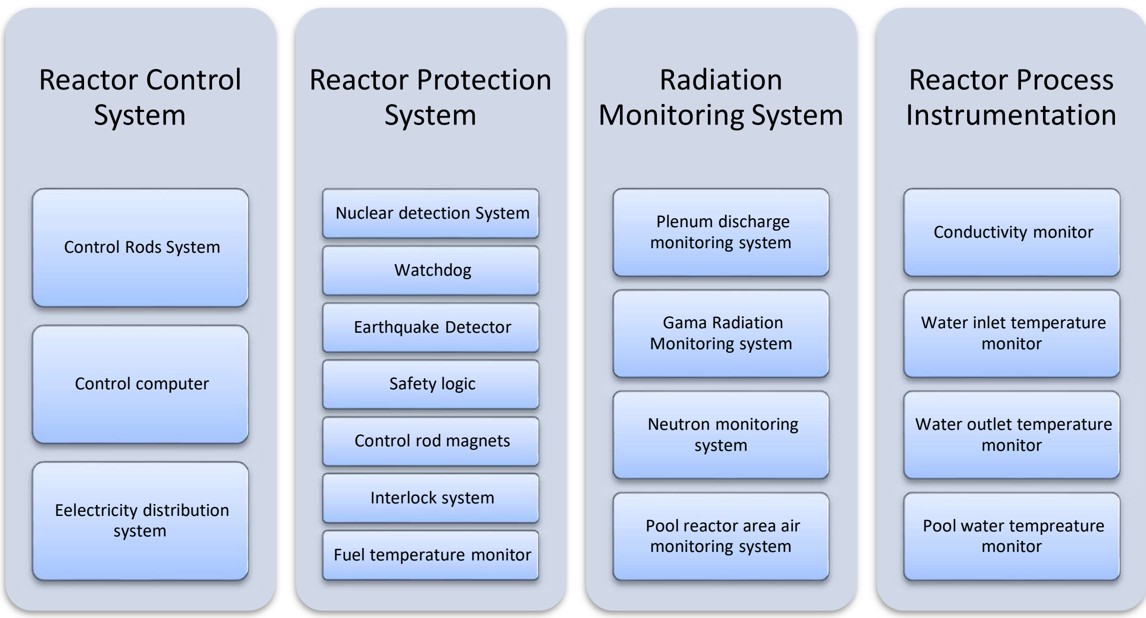


FIG. 3. ININ TRIGA reactor I&C.

2.1. Reactor protection system

The new reactor's protection system was designed as an integral component of the control console and was based on modern digital and optical electronics, integrating solid-state components [2]. In compliance with the norms applicable to the safety aspects of this kind of nuclear facility, the protection system was designed to maintain its computer-free operational characteristics, while the rest of the new console system was allowed to incorporate digital computers and processors to control the normal operation of the reactor. The protection system, compared to the original one, enhances the scram functions and improves the safety and operability features of the system's circuits.

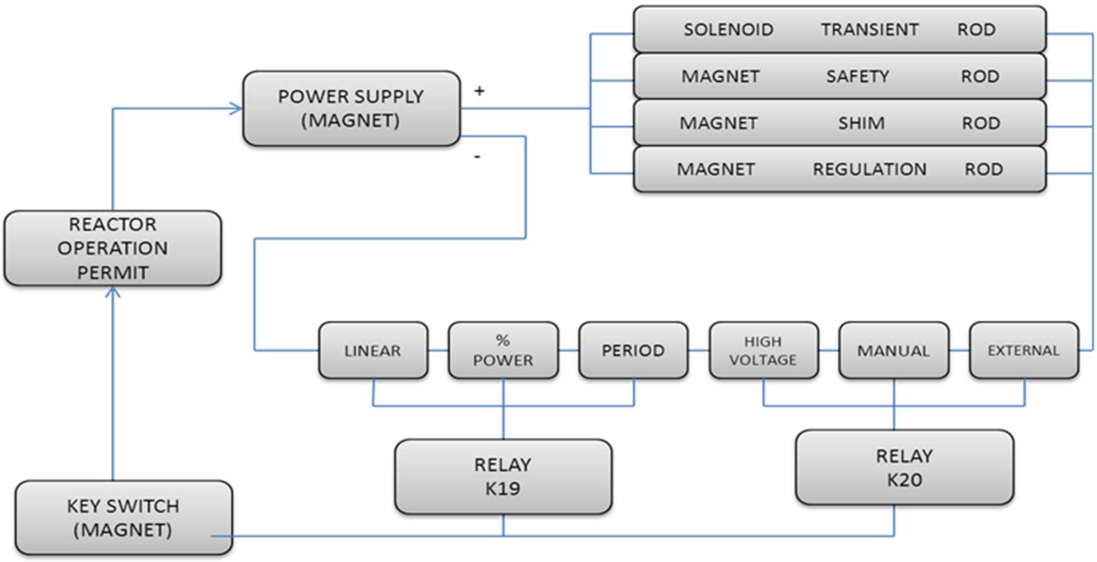


FIG. 4. ININ reactor protection system.

2.2. Software-based Neutron Flux Measurement Channel (NFMC)

Once the reactor's control console was updated in 2001, from analogue discrete electronic technology to a digital computer-based platform, the next step was to consider the use of computer-based virtual instrumentation and software-based signal processing on the nuclear channels.

Thus a new channel was developed [3]. This channel uses the second order moment of a fission chamber signal to determine the reactor power. This channel would then be in position to replace the current starting count channel for powers from source level to 100 W and the two power channels (the linear and the logarithmic channels) for powers from 1 W up to 1 MW. The starting count channel uses a fission chamber operating in count mode. Each power channel uses a compensated ionization chamber filled with boron trifluoride as the active element for neutron detection, delivering at the output a current of about 1 × 10–9 A for 1 W up to 1 × 10–3 A for 1 MW. It is proposed that the new channel (NFMC) will cover the entire power interval using a single detector instead of three, thus saving space and reducing the channel complexity. The NFMC operation mode will be based on the measurement of the neutron signal fluctuation (Campbell method). The channel's computer will perform the signal conditioning and processing, the graphical and numerical visualization of power and period, and the generation of the safety and interlock signals (source level presence and 1 kW level) required to connect the channel to the rest of the control console instrumentation. The flexibility provided by the channel's computer will allow the operation in other modes, for instance, different order moments, by modifying the software-based signal processing algorithms.

NFMC measures the reactor power through six decades using the correlated signal of a wide range fission chamber. The correlation between the Root Mean Square (RMS) value of the detector current fluctuations and the reactor power is known as the Campbell technique, thus leading to the name Campbell channel. In this new version of the channel, the signal from the amplifier is captured by a fast data acquisition card that sends the data to a computer. Signal processing and visualization algorithms are implemented by software, thus reducing considerably the number of discrete analogue and/or digital electronic components. This system offers a greater versatility to carry out modifications or replacements of signal processing algorithms and power monitoring sequences. The experimental tests carried out to measure the reactor's power show a very good agreement with the actual power, measured with current measuring channels through six decades of power, obtaining a correlation factor of 99.61%.

A schematic diagram of the hardware components of the NFMC is shown in Figure 5. A brief description of the operation of each of the main components is presented next.

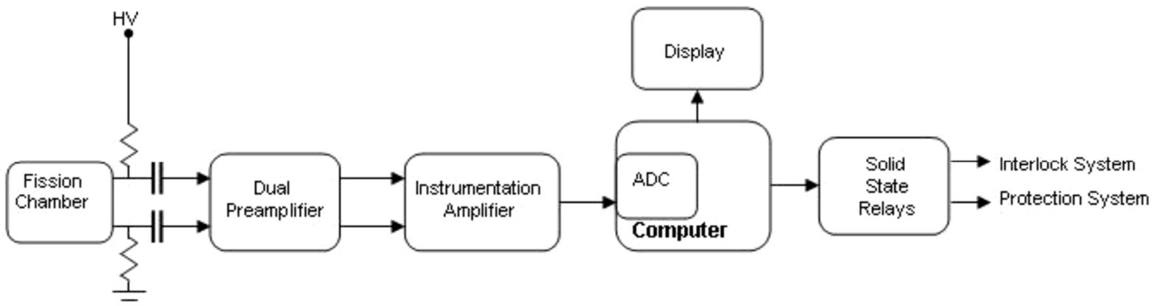


FIG. 5. NFMC components.

The use of software-based mathematical functions allows a simpler design of systems that involve data acquisition, signal filtering and processing, data scaling, virtual instruments, and graphical and numerical data visualization. Software-based systems possess greater flexibility for updates, modifications or improvements without the need to modify or to alter the system's physical components.

The software gives functionality and versatility to the NFMC. Within an infinite cycle, the program carries out the tasks of data acquisition, signal processing and data display, either graphically or numerically. The program was developed in Microsoft Visual Basic 6 with insertable objects and functions provided by the National Instruments Measurement Studio [4].

Further work related to the NFMC is the inclusion of an algorithm to determine the value of either the reactor's instantaneous period value or the inserted reactivity, which would be applied to the same input signal. Due to its relatively low cost and the simplicity of implementation/ modifications and/or additions, this measuring channel could be proposed to other research centers that operate TRIGA reactors for updating their nuclear channels.

2.3. TRIGA simulator interface for training and validation of power control algorithms

The development of a user interface whose main purpose is the testing of new power control algorithms in a TRIGA Mark III was done [5]. The interface is fully compatible with the current computing environment of the reactor's operating digital console. The interface, developed in Visual Basic, has been conceived as an aid tool in the testing and validation of new and existing algorithms for the ascent, regulation and decrease of the reactor power. The interface calls a DLL file that contains the control program, makes available to the user the plant and controller parameters, and displays some of the key variables of the closed loop system. The system also displays the condition of the reactor with respect to the nuclear safety constraints imposed by the Mexican Nuclear Regulatory Commission (CNSNS). One of the algorithms under test is based on a control scheme that uses variable state feedback gain and prediction of the state gain that guarantee the compliance of the safety constraints.

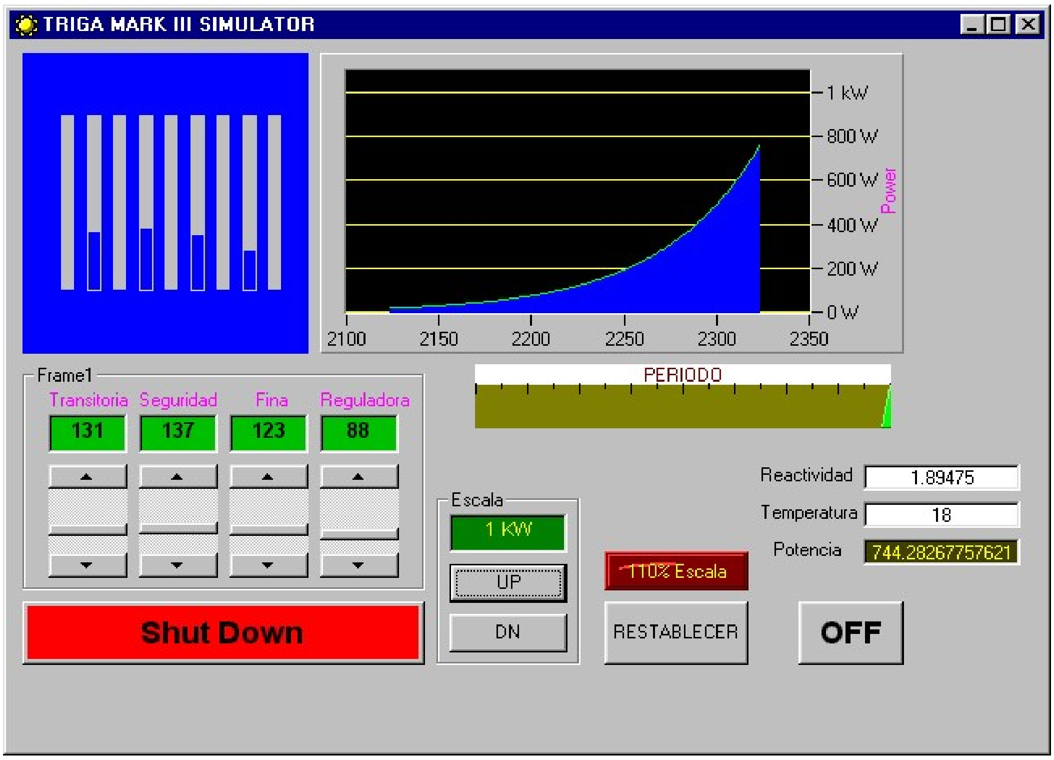


FIG. 6. ININ TRIGA simulator for training and algorithm analysis.

2.4. PROPOSED 2012 I&C SYSTEM DESIGN

In February of 2012, the reactor´s core was converted to use only LEU (30/20) fuel as a part of this process and considering the obsolescence of equipment and non-availability of spare parts, the instrumentation and control system is going to be modernized, by changing the actual control system to a new one using digital technology. In this work the design of the proposed new control system is shown. This control system will be based on hot stand-by redundant PLCs and will be integrated with the reactor protection system and a new HMI fully developed by ININ.

The I&C system will include the following systems:

(a) Control system;

(b) Instrumentation system; and

(c) HMI.

2.5. Control system

The proposed Reactivity Control System is based on hot stand-by redundant PLCs. It will take the signals from the neutronic channels, operation modes, encoders, fuel temperature sensors, water temperature, control rod positions, etc. It will execute the algorithms for automatic control of the reactor´s power and will send the control signal to the actuators. All this information will be presented to the operator at the control console through TCP/IP Ethernet on the HMI. Thus the operator could see on the console screens all previous information and take the corresponding actions.

This control system will take into account the different reactor operation modes, automatic and manual and all the required interlocks. This configuration, using a principal PLC and a second PLC named "Standby PLC" that has a mirror configuration as the principal one, will allow us an instantaneous and automatic transfer from the primary control to the standby one. This redundancy is a key design feature and is according to IAEA NS-R-4 [6]. To avoid common cause failures, the system will be independent in such a way that all signals will be opto-coupled.

This proposed Hot Standby control system will give us, among others, the following advantages:

(a) High system availability, that allows maintenance during operation;

(b) Development environment compatible to IEC 61131- 3, 5 language standard: LD, ST, FBD, SFC, IL;

(c) High multilevel CPU task performance;

(d) Ethernet TCP/IP Transparent Ready services: E/S scanning, global data, Web server, e-mail messages, data base direct access, open to TCP, Network Time Protocol, etc.; and

(e) Communication ports: USB, CANopen, ETHERNET TCP/IP web, etc.

2.6. Instrumentation system

The instrumentation system will be based on a PLC with USB and ETHERNET communication ports and indication LED's for process status, it will include the following systems:

1. Radiation Monitoring System:

   — Plenum discharge monitoring system;

   — Gama radiation monitoring system;

— Neutron monitoring system; and

— Pool reactor area air monitoring system.

2. Reactor Process Instrumentation:

— Conductivity Monitor;

— Water inlet temperature monitor; and

— Water outlet temperature monitor.

To avoid common cause failures, the system will be independent, in such a way that all signals will be opto-coupled.

2.7. HMI system

The main reason for obsolescence in the control system based in computers with ISA, EISA or PCI bus type interface is the lack of availability of compatible spare parts with these technologies. The same case is also for the associated software because it should be compatible and configured with these technologies, and should be continuously updated, but even with long waiting times and high costs, itsometimes cannot be updated.

Considering this, we designed a distributed system in order to eliminate dependency on I/O cards or modules. The HMI system will use TCP/IP communication between all the components and will be based on commercial PC servers. These PCs will display all the information on LCD screens. The software will be developed on a JAVA platform making it independent of the operating system. System visualization screens are designed in compliance with NUREG-0700 [7] ergonomic rules, so that operators can assimilate all the information and take correct safety related decisions. All the software will be developed following the ININ´s quality assurance program [8] that is based on IEEE and IAEA standards.

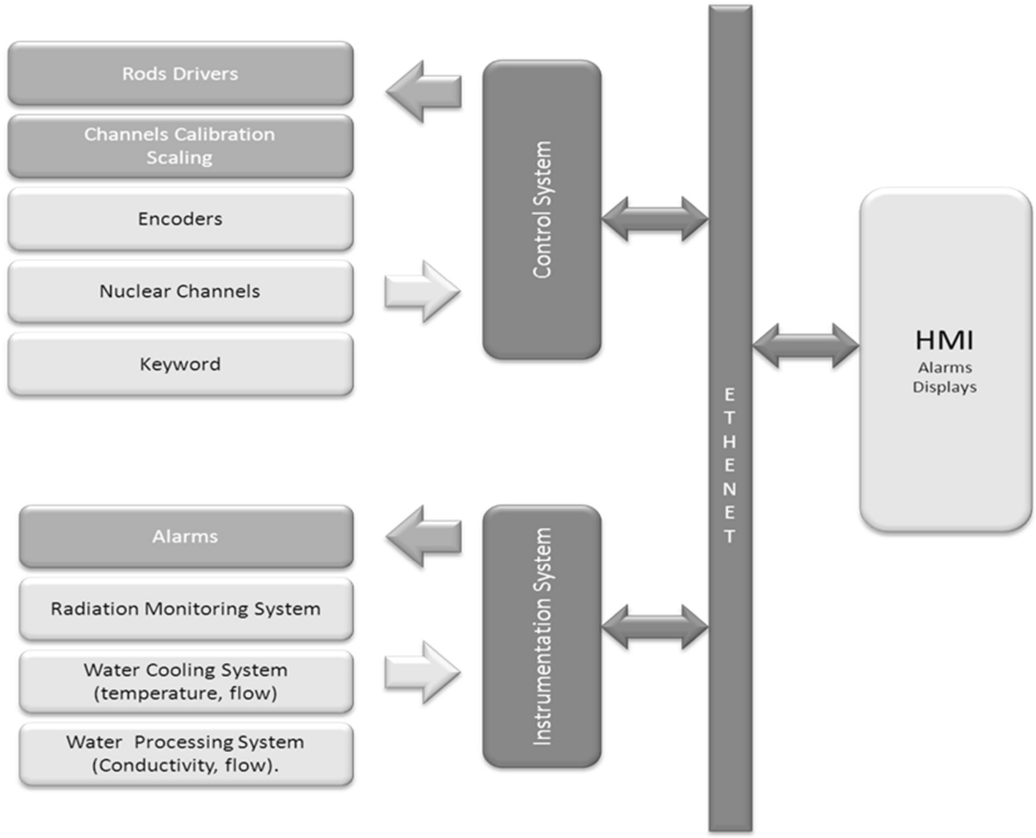


FIG. 7. Schematic diagram for the ININ TRIGA proposed I&C Systems.

3. REGULATORY CONSIDERATIONS

In the I&C proposed design the following guides/standards were considered:

(a) 10CFR50 Appendix A Criterion 13 of the NRC;

(b) NRC Regulatory Guide 1. (97) Rev. 3;

(c) IEEE Standard 384-1977 Criteria for Independence of Class 1E Equipment and Circuits;

(d) NS-R-4 Requirements on the Safety of Research Reactors;

(e) Utilization and Modification of RRs SS-35-G2;

(f) Safety Guide No. NS-G-1.1 - Software for Computer Based Systems Important to Safety in Nuclear Power Plants; and

(g) Safety Guide No. NS-G-1.3 - Instrumentation and Control Systems Important to Safety in Nuclear Power Plants.

The first two establish that under an accident condition, it will be necessary to consider which system must continue operating. For the TRIGA reactor, this condition consists of damage to the nuclear fuel by a container rupture. The third establishes the isolation criteria to avoid a propagation fault between the diverse systems of the reactor control console. This criterion is accomplished by using the isolation and decoupling components of signals.

4. DISCUSSION

The original GA reactor´s control console operated with no major problems for 34 years. Due to aging and obsolescence of electronic components, this original console was replaced in 2002 by a new digital console fully developed by ININ and has been operating with no problems. This control console is being continuously updated, but considering the obsolescence of equipment and non-availability of spare parts, mainly in the I/O modules and the associated software, ININ decided to modernize the instrumentation and control system, by changing the actual control system to a new one using digital technology. This control system will be based on hot stand-by redundant PLCs and will be integrated into the reactor protection system and to a new HMI fully developed by ININ.

Some of the expected advantages of this new I&C digital design are the following:

(a) Logical separation of functions by applying concepts of distributed control and modular instrumentation;

(b) The reactor protection system is kept with direct cabling to avoid performing functions of security through software;

(c) Use of TCP/IP standard to achieve inter-connectivity systems and reducing the signal and into the reactor and console wiring;

(d) Commercial screens spacious and high resolution in the HMI for panoramic sample of the parameters of operation and control of the reactor;

(e) Programming HMI using codes of open source and multiplatform. This will help to reduce costs; and

(f) The reactor protection system design remains unchanged.

REFERENCES

[1] Instituto Nacional de Investigaciones Nucleares. Informe de Seguridad del Reactor TRIGA MARK III del ININ (2003).

[2] RIVERO-GUTIÉRREZ, T., et al., Protection System of the New Control Console of a TRIGA Mark III Nuclear Research Reactor. Nuclear Technology. Vol. 126. No. 3. pp. 340-347 (1999).

[3] RIVERO-GUTIÉRREZ, T. et al., Software-based Neutron Flux Measurement Channel (NFMC) Int. J. Nuclear Energy Science and Technology, Vol. 5, No. 2, (2010).

[4] National Instruments (2008a) 'Measurement studio', www.ni.com.

[5] RIVERO-GUTIÉRREZ, T., et al., User interface for intelligent control schemes in a TRIGA Mark III reactor. International Journal of Nuclear Knowledge Management, Vol. 2, No.3 pp.268 – 284 (2007_

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Research Reactors Safety Requirements, IAEA Safety Standards Series No. NS-R-4. IAEA, Vienna (2005).

[7] NUREG 0700 Human System Interface Design Review Guidelines (2002).

[8] GAYTÁN-GALLARDO, E., RIVERO-GUTIÉRREZ, T., 'Software Quality Assurance plan (Plan de Garantía de Calidad del Software)' [in Spanish], PL.GC-2, Rev. 1, Instituto Nacional de Investigaciones Nucleares, February (2007).

SURVEILLANCE AND POWER CONTROL SOFTWARE FOR PAKISTAN RESEARCH REACTOR 1

S. H. QAISER, J. QADIR, M. IQBAL
Pakistan Research Reactor 1, Nuclear Engineering Division,
PINSTECH, Islamabad,
Pakistan

Abstract

Software for automatic power control and condition monitoring for Pakistan Research Reactor 1 (PARR-1) has been designed and implemented at PARR-1. The software has been designed in labVIEW® 7 under windows operating system. The developed software records various system parameters and keeps a log of them. It also provides user interface to set a demand power of the reactor and automatic control of the reactor power according to the given set point. The power control is provided by controlling one of the control rod movements of the reactor while the power is measured from the linear channel. It also displays control rod positions, startup and shut down times of the reactor, reactivity of the reactor, error messages; saves data in the sequential file; and graphically displays various signals and control rod movement. The software acquires thirteen signals for manipulation with separate logic for each.

1. INTRODUCTION

The Pakistan Research Reactor (PARR-1) is a 10 MW pool type research reactor. It was provided by American Machine Foundry (AMF) and was first made critical on 21st December 1965. Originally designed for 5MW, the reactor was redesigned to operate with Low Enriched Uranium (LEU) fuel at a power level of 10MW. In this reactor 19.99% enriched uranium fuel plates are used and control rods are made of an alloy of cadmium (5%), silver (80%) and indium (15%). The MTR fuel element is basically a stack of straight fuel plates supported by side plates at both ends throughout its height. PARR-1 core is assembled on a grid plate, having 54 holes arranged in 9x6 array, with a lattice pitch of 81.0x77.1 mm. It is a combination of fuel elements, control rods, graphite reflector elements, water boxes for irradiation of samples and fission chambers with guide tubes. One side of the parallel-piped core is reflected by graphite, i.e. thermal column, while the opposite side is reflected by a blend of graphite reflector elements and light water. The bottom side is reflected by a combination of aluminum and water. The rest of the three sides, i.e. top and two lateral sides, are reflected by light water only. At PARR-1, five (Ag-In-Cd alloy) control rods are employed for: (a) startup (b) shutdown, and (c) reactor operating power level control. In addition to this PARR-1, the core is designed to have negative coefficients of reactivity, a reflection of the fail-safe principle. These control rods can be relocated in any future core configuration as per design requirements [1-3].

PARR-1 has two cooling modes: (a) cooling by natural convection when reactor power < 100 kW, and (b) cooling by gravity-driven downward flowing coolant when reactor power ≥ 100 kW. The heat produced in the PARR-1 core is carried away by the primary coolant system (PCS). The PCS consists of core, plenum, outlet piping & valves, hold-up tank, centrifugal pumps, heat exchangers and inlet or return piping & valves. This PCS of PARR-1 transfers its excessive heat to the secondary cooling system, which dissipates this energy to atmosphere via cooling tower. Both primary and secondary cooling systems have auxiliary systems for the makeup of the coolant, both quantitatively and qualitatively. For quantitative losses water make-up systems are incorporated while water quality is maintained through a water purification system. There are five control rods. The reactor becomes critical when these rods are withdrawn about 56% from their fully inserted position. After the reactor becomes critical, a single rod is used to regulate the reactor power [1].

The instrumentation system of this reactor consists of power measuring channels, radiation measuring channels and process channels. Power measuring channels are generally classified according to the power range. They are start up channels (0-200 W), intermediate channels (100 W to 20 MW) and power channels (10 kW to 20 MW). These channels successively overlap one another to provide continuous measurement of the neutron flux level at all power levels [4]. The channels are provided with alarm set points and channel fault monitoring modules to warn the reactor operator in case of high reactor power level or any abnormality in the operation of the channel. Channels available at PARR-1 in this category are startup channels, linear channels, logarithmic channels, safety channels, and N-16 channels.

The radiation monitoring channels monitor the release of radioactive materials within the containment. There are twelve radiation monitoring channels installed around PARR-1, ten of which are FHT 155-A type having Geiger-Muller tube detector and the remaining two are locally fabricated. The process channels include flow, pressure, temperature and water level measurement channels [1].

The paper presents software developed in labVIEW for auto power control and reactor surveillance. For controlling output power, a controller built in software manipulates the control rod position with the help of a data acquisition card depending upon the error (the difference of the reference power and measured power) to obtain the desired effect on the output power. Different reactor parameters are also logged and displayed in a graphical GUI. The paper is organized as follows. After introduction the motivation/problem formulation is given in Section 2, Section 3 discusses control system with hardware and software details. Results and conclusions are discussed in Section 4 which also concludes the paper.

2. MOTIVATION/PROBLEM FORMULATION

The conventional power controller in PARR-1 is a PID controller, which has gotten quite old and has started to show some problems. There was a need for a system which can control the power in case of its failure or may run in parallel as a diverse controller. For safe reactor operation the updated status of different reactor parameters provides useful information to operators, which helps in avoiding any catastrophic condition. Hence different reactors parameters were also logged and displayed graphically for helping operators in safe reactor operation. This system also provides a supervisor or operator the facility to check any system variable behavior for the past many hours. Keeping with these requirements, a software system has been developed and implemented at PARR-1, which runs in parallel with the PID controller. The operator can switch to any mode as desired. The developed system proved very useful and some time back, when the PID controller was out of order, the whole operation was switched to this software based controller. The developed system behaved very well and the new PID controller has been installed, it continues to provide a good alternate and experimental facility for operators.

3. CONTROL SYSTEM DESCRIPTION

The control system is developed in labVIEW with 6024 data acquisition card. The linear channel output is used to maintain the power at a desired level. As the control rod speed is much slower, a high speed controller is not required and a simple controller which compares the current power level with desired power and depending upon the error can manipulate the control rod position. So for designing the power controller the control input is taken as the control rod position, which inserts positive or negative reactivity. The output is neutron flux or reactor power and the control objective is to maintain power at desired level within 1% accuracy. The reactor control regulating rod is moved down when the power crosses the set point set by the operator. If the power remains below the set point, the rod up signal is communicated. This process continues for maintaining the desired power level. To regulate the reactor power precisely, control band is limited to 1% otherwise it shows server error, these steps are described in the flow chart in Fig 1.

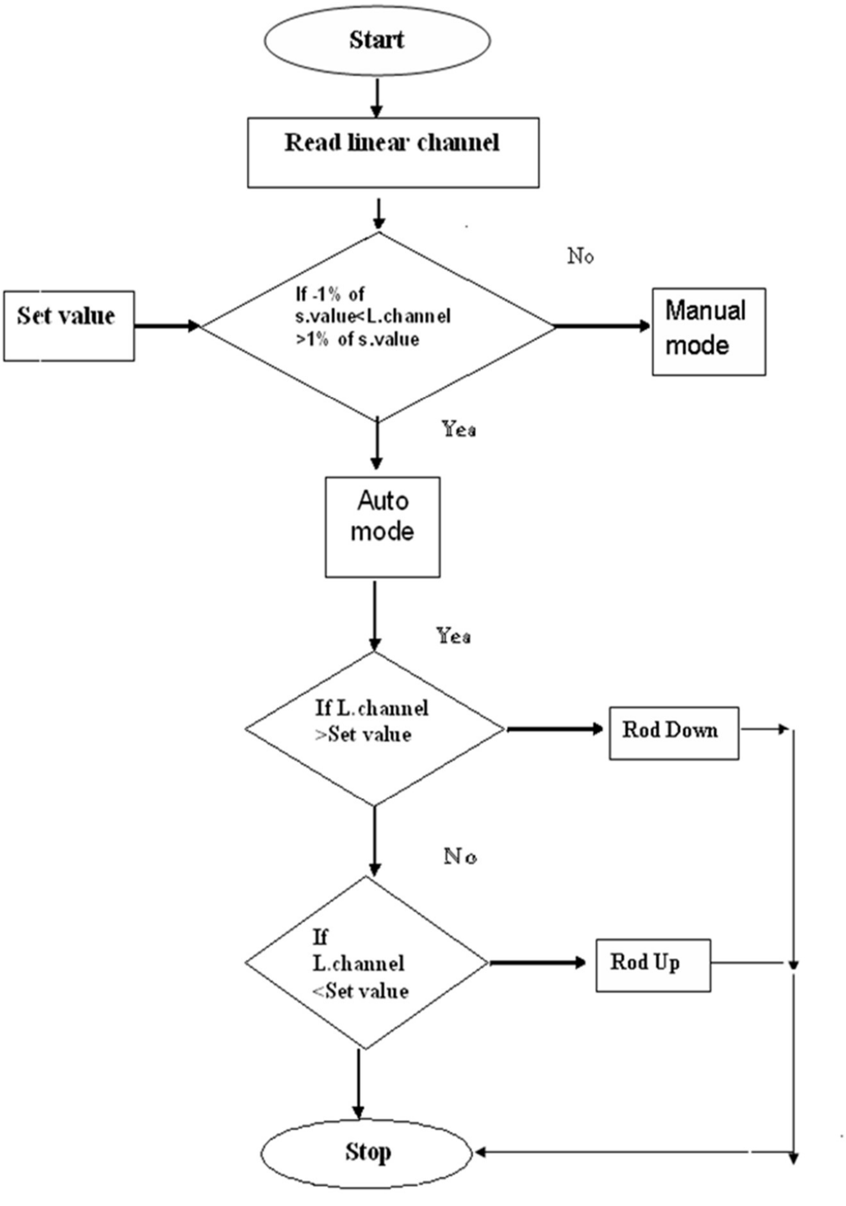


FIG. 1. Flow chart of control software.

3.1. Hardware description

The hardware system comprises of a control computer with labVIEW control software NI 6024E data acquisition card and interface circuitry [5]. This card have 16 channels (eight differentials) of analog inputs, two channels of analog outputs, a 100-pin connector, and 32 lines of digital I/O. This device has three input modes-non-referenced single-ended (NRSE), referenced single-ended (RSE), and differential (DIFF) input. The single-ended input configuration provides up to 16 channels. The DIFF input configuration up to eight channels, configuration used in this software is referenced single-ended (RSE).

The devices have a bipolar input range that changes with the programmed gain. Each channel can be programmed with a unique gain of 0.5, 1.0, 10, or 100 to maximize the 12-bit analog-to-digital converter (ADC) resolution. With the proper gain setting, these devices supply two channels of analog output voltage at the I/O connector. The bipolar range is fixed at ± 10 V [3].

3.2. Software description

The software has been developed in labView which acquires thirteen signals for reactor parameters manipulation with separate logic for each parameter. The experimental setup block diagram for data acquisition and control is shown in Fig 2, which includes linear channel, log channel, N-16 channel, inlet, outlet, and secondary temperatures, pool level deviations, flow and radiation signals. Linear signal is utilized for generating the auto-controller movement voltage at certain lower and upper limits. The controller employs the shim rod as the fine control element. While the reactor is in auto mode, there are no considerable fluctuations observed in other parameters.

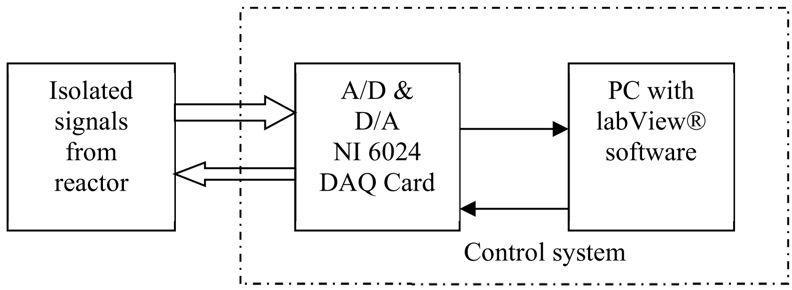


FIG. 2. Experimental data acquisition and control setup.

Reactor power and reactivity are manipulated through log signal, calculation of reactor power is done through a transfer function which is generated with the collection of real time data, and another important aspect of this software is a reactivity meter. The advantages of using a reactivity meter in a reactor are manifold. In the operation of nuclear reactors continuous reactivity surveillance is necessary to safely and efficiently reach the operating power level. At higher power levels, careful monitoring of reactivity is needed to determine temperature, poison and power coefficient of reactivity. The reactivity meter is also very useful in determining the reactivity worth of new fuel elements or the irradiated samples added to the core [6].

The software receives an input error signal, which is a function of the demand power level and actual reactor power. It determines the rate and amount of the power correction required by the proportional, integral and differential formalism and produces an output to operate the fine control element, In this way the reactor power is maintained at its desired value or demand set point. The current setting of the maximum allowable input error in the auto-control mode is 1% of the demand set point. Beyond the 1% power variation the controller action is automatically disabled and the reactor is returned to manual mode [7-9].

4. RESULTS/CONCLUSIONS

A system for automatic power control and condition monitoring for Pakistan Research Reactor 1 (PARR-1) has been designed and implemented at PARR-1. The developed system also records various system parameters and keeps a log of them. Demand power is provided by the user with the help of a user interface to automatically maintain the power at a desired set point. The system after implementation of the control software is behaving satisfactorily and the power variations have minimized, as compared to the older PID (Proportional with Integral and Derivative) based controller. Figure 3 shows the power output of the PID based controller and illustrates the output of the new system. These figures are taken from the chart recorder of actual reactor operations. Here power is shown on x-axis and time is on y-axis. From these two figures it is observed that new controller performs in a good way, as compared to old one..

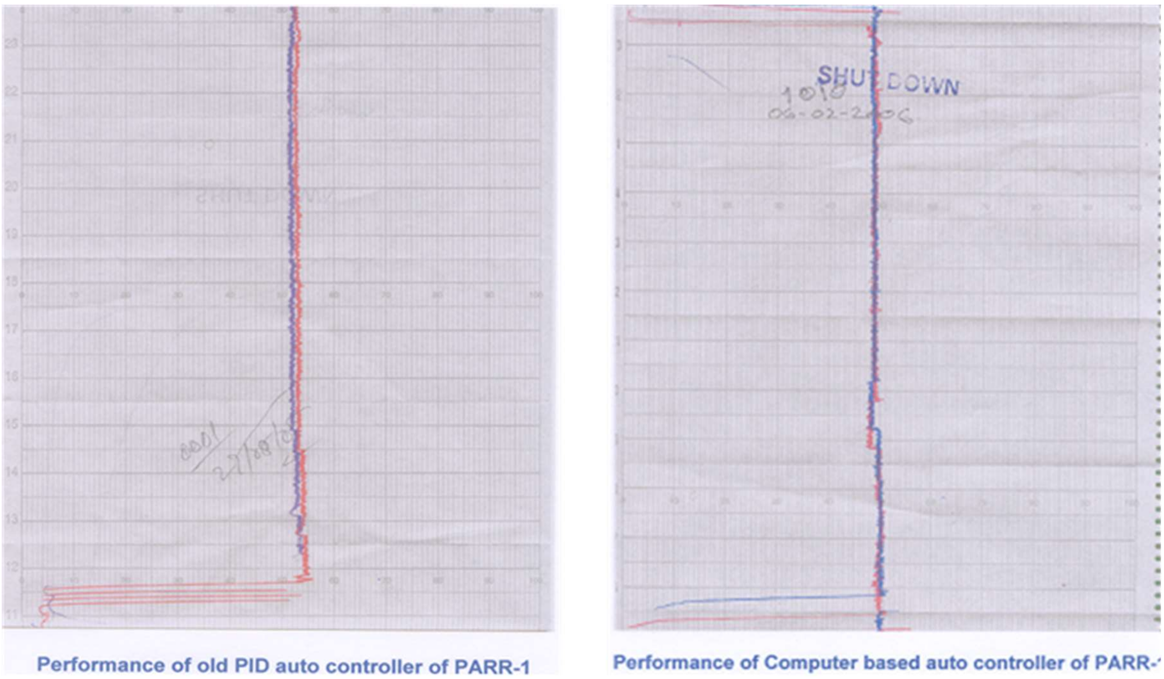


FIG. 3. Comparison of classical and new controller performance.

The new surveillance system GUI is shown in Fig. 4

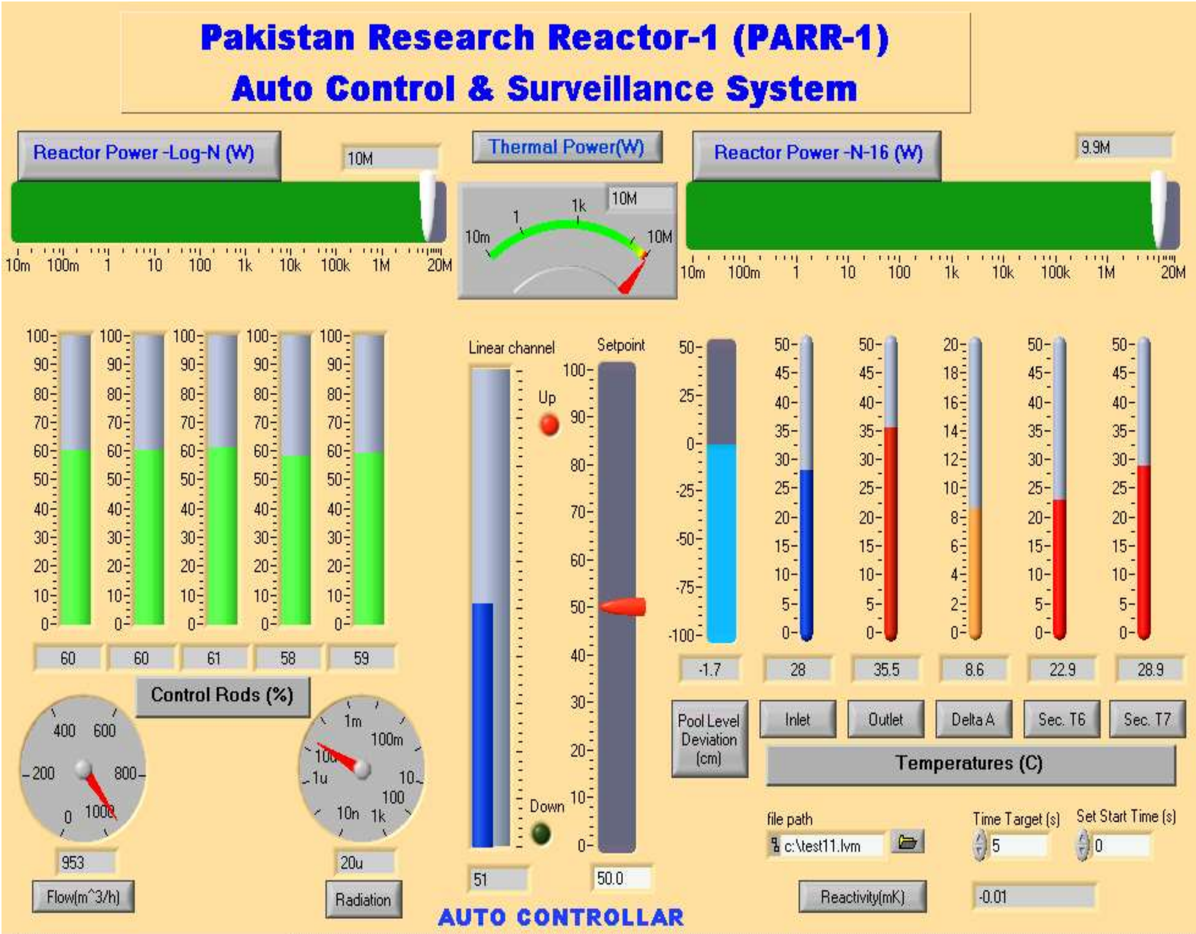


FIG. 4. Surveillance and control system GUI.

ACKNOWLEDGMENT

The authors wish to thanks Mr. Maqbool Alam and other reactor operators of the Nuclear Engineering Division, PINSTECH for providing technical support.

REFERENCES

[1] FSAR, Final Safety Analysis Report, Pakistan Research Reactor-1 (2001).
[2] ANSARI, S.A., et al., "Critical and power Experiments on the Low-Enriched Uranium Core of the Upgraded Pakistan Research Reactor-1," Nuclear Technology **108** (1994) 13-25.
[3] AYAZUDDIN, S.K., ANSARI, S.A., "Reactor Transfer Function Measurement at PARR By Neutron Noise Analysis," Nuclear Engineering Division, PINSTECH-105 (1984).
[4] M. Tahir. K., Imran Z., Hameed Q., Iftikhar G., and Ashraf A., “A New Wide Range Reactor Power Measuring Channel”, IEEE Transactions on Nuclear Science **150** 6 (December 2003).
[5] National Instruments 6024E Data Acquisition Card Users Manual (2000).
[6] IQBAL, M., MIRZA, N.M., MIRZA, S.M., AYAZUDDIN, S.K., “Study of the Void Coefficients of Reactivity in a Typical Pool Type Research Reactor”, Ann. Nucl. Energy **24** 3 (1997).

[7] QAISER, S.H., BHATTI, A.I., IQBAL, M., QADIR, J., “System Identification and Robust Controller Design for Pool Type Research Reactor”13th IEEE/IFAC International Conference on Methods and Models in Automation and Robotics (MMAR 2007), 27-30 August Szczecin Poland (2007).
[8] QAISER, S.H., BHATTI, A.I., IQBAL, M., KHALEEQ, M.T., “Robust Control System Design for Pool Type Research Reactor using H_∞ Loop Shaping Technique”, First International Conference on Physics and Technology of Reactors and Applications, Morocco, March 14-16 2007, GMTR (2007).
[9] QAISER, S.H., et al., "Model Validation and Higher Order Sliding Mode Controller Design for a Research Reactor," Annals of nuclear energy **36** (2009) 37-45.

CONCEPTUAL DESIGN FOR THE UPGRADING AND DIGITITATION OF THE INSTRUMENTATION AND CONTROL OF THE RP0 AND RP10 NUCLEAR REACTORS OF PERU

Emilio Veramendi L., Marco Corimanya M.
Instrumentation and Control Nuclear Reactor RP-10
Peruvian Institute of Nuclear Energy, Av. Canadá 1470, Lima 41, Perú

Abstract

The RP-10 Nuclear Reactor is a multi-purpose research reactor (production of radioisotopes and applications in the industry) that develops a thermal power of 10 Megawatts, the present article presents an overview of the nuclear and conventional instrumentation existing in the reactor RP10 research, in addition explains the operation, operation and technology that is being used and which is wanted to improve and update maintaining the security, availability and reliability of their systems, in addition to three projects already made annexed to the instrumentation they scan The signals from the reactor serving as a log, transmission, digitization and graphical visual aid for the safe operation of the reactor, such projects are the basis for improvement and continuous updating, since the reactor is about to reach its useful life implementation is necessary And information on new technologies for its improvement and updating.

1. INTRODUCTION

The Peruvian Institute of Energy has a Research Reactor RP10 of 10 Mega Watts of power, for the production of Radioisotopes and applications in the industry, has associated Nuclear Instrumentation in the stage of start with nuclear detectors of type fission chambers for The power stage with nuclear sensors of the Compensated Ionization Chamber type, the instrumentation processes the signals from the detectors by providing the protection system with linear, logarithmic, neutron flux-derived (period) neutron flow information, as well as the levels of Tripping associated with the protection system, the conventional instrumentation Teleperm C siemens which gives input temperature information, output, core temperature difference, primary, secondary, cooling, core pressure difference. Information on conventional parameters of heat exchangers primary cooling circuit, secondary and cooling towers. As well as the safety trip levels to the protection system. The RP10 Nuclear Reactor Protection System receives electronically processed information from the sensor to the actuators. It consists of Safety Logic, Sequence Logic / Motion / Inhibit Control Bars, Start Logic, Run Logic, Power Reduction Logic , Automatic Logic Logic, Auto Pilot Logic, Scram Logic has performance levels of the safety parameters of Alarms, Power Reduction, Automatic Input, Scram (Drop of all Control Bars, automatic shutdown of the Nuclear Reactor).

2. INSTRUMENTATION AND CONTROL

The instrumentation attached to the operation of the reactor is of two kinds:

* Conventional instrumentation
* Nuclear instrumentation

2.1. **Conventional Instrumentation**

It has conventional electronics based on SIEMENS brand measuring equipment, TELEPERM C models, which are responsible for the measurement and census of the conventional parameters (Temperature, Temperature Difference, Pressure Difference, Flow, Conductivity, PH).

This system was designed in such a way as to be redundant, reliable and safe for the safe operation of the reactor, but at the present time this line of TELEPERM C equipment is discontinued and does not have spare parts in the market for its maintenance.

It has three racks in charge of the measurement of conventional parameters each rack is in charge of the measurement of core temperature, core temperature differential and pressure differential in the core, plus other auxiliary parameters.

The safety and availability is controlled by the Redundyn module that averages the three signals of the three rack of a parameter (Temperature Delta) and uses the resulting one for the thermal power control of the reactor.

When a malfunction of one of the modules occurs, the Redundyn module will disable the function of that rack and only the two two-rack signals will be averaged, in the same way when the second rack fails, the redudyn will work with only one rack.

Fig 1: Analog Indicators T(°C), dT(°C), dP(mbar) and flow(m3/h)

<u>Redundancy in Measurement Chains</u>

In order to increase the reliability of the system against the risky faults of its components the chains have been redounded:

1. Core temperature difference.
2. Core outlet temperature.
3. Pressure difference in the core.
4. Low refrigerant level (SCRAM) in the reactor tank.

The first three monitor the proper cooling of the core and the last one protects the personnel against a possible level of dangerous radiation in the mouth of the tank before a request for refrigerant.

2.2. **Nuclear Instrumentation**

The nuclear electronics is made up of three rack-based electronic CMOS, each rack with a start and run channel

The starter channels are responsible for carrying the signal from the CF neutron detector to the starter amplifier for processing and comparison.

The signal to handle a nuclear pulse detected by a purely analog electronics that to the step of the Booster amplifier generates a Gaussian wave and later pulses tables for its count.

The run channels are responsible for bringing information from the compensated ionization chamber type neutron detectors to the running amplifier. This equipment translates the current signal (pA), amplifies it and generates the digital signal for processing and comparison.

All signals from both nuclear and conventional electronics are interconnected to the logic of safety, interlocking and SCRAM logic, these logic work with 2 of 3 logic, giving reliability, safety and availability to the safe operation of the reactor.

* Starter Chains, Fission Chambers.
* Chains of march, Chambers of Ionización Compensada.
* Area Monitors, Geiguer Muller detector.

Fig 2: Starter Chains

Design Bases

* Separation of protection and safety systems from other control systems
* Redundancy of measurement sets in protection systems
* Testing of protection systems (from sensor to control systems)
* Diversity of electronic systems associated with the protection system
* Availability and Reliability Analysis
* Diversity among the parameters involved in the measurement sets of the protection system
* Dangerous fault
* Common mode failure

Safety related instrumentation and control systems

* Starter Chain
* Chain of March
* Tank Mouth Exposure Monitors
* Primary Flow
* Core Pressure Differential
* Core Temperature Differential
* Core Output Temperature
* Main tank coolant level
* Seismic warning
* Clapet State
* Start Logic
* Logic of March

3. IMPROVEMENTS AND ADAPTATIONS TO SOME SYSTEMS APPENDED TO THE REACTOR RP10 INSTRUMENTATION

3.1. **Digital Data Acquisition System of the Area Monitors for the Control of Radiological Emergencies of the Nuclear Reactor RP10**

Implementation and development of a data acquisition system for the data transmission system of the radiological emergency system.

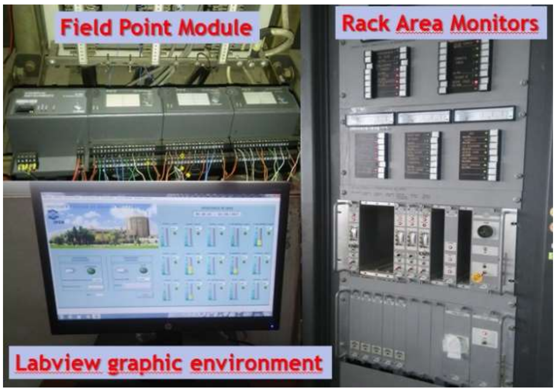


Fig 3: Digital data acquisition system of the area monitors

In charge of the acquisition of signals from the area monitors (28 Monitors in the vicinity of the nuclear reactor RP10), which are acquired with Field Point equipment and processed in a PC, under a graphical environment developed in with Labview software of National Instruments , Which provides real-time information on the dose rate, has a record and alarms for each eventuality, in addition the information is sent to another building (Radiological emergency room), two-way Ethernet, and RF transmission.

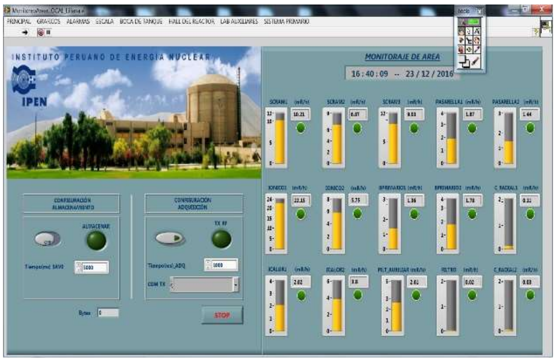


Fig 4: Graphical environment in Labview

3.2. Automatic emergency switching of the ventilation system of the RP-10 nuclear reactor

Implementation and development of a visualization and control system of noble gas monitor for the emergency of the ventilation system.

This is formed by a monitoring equipment of noble gas emission (MAP1000), which sends a signal via RS485, such signal is conditioned and retransmitted from basement to control room for reception by a digital equipment based on Microcontroller (PIC16F877), which visualizes the reported doses and also compares the signal and actuates the emergency system for the ventilation of the reactor in case of an incident of contamination of noble gases in the enclosure.

Fig 7: Noble Gases MAP1000 Module

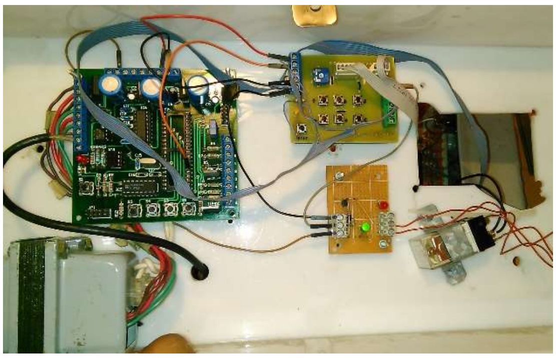


Fig 8: Electronic Based Microcontroller

3.3. **Data Acquisition System (SAD)**

Implementation of a data acquisition system with MIO and DIO cards of the National Instruments brand, with corresponding associated electronics

The system allows the visualization and monitoring of data and parameters of the conventional and nuclear instrumentation of the reactor RP10, under a graphical environment realized in software LabWindows/CVI which allows the visualization of parameters in real time in the PC dedicated to this function.

Fig 9: Data Acquisition System (SAD)

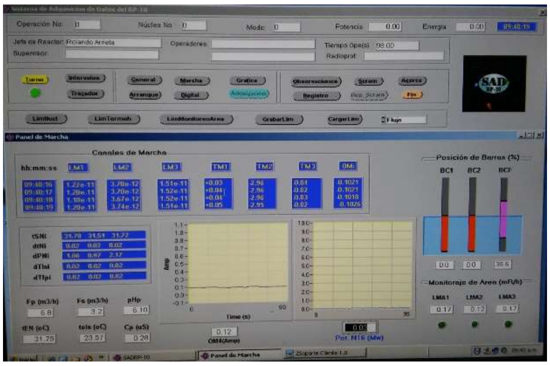


Fig 10: Graphical environment in LabWindows/CVI

4. PLANS FOR IMPROVING AND UPDATING SYSTEMS OF REACTOR INSTRUMENTATION RP10

3.1. **Update of Data Acquisition System**

COMPAQ equipment using National Instruments DAQ for the acquisition and processing, we can access real-time parameters to perform different programs with specific applications such as:

* Bar Calibration by dubbing time method
* Real-time thermal power measurement
* Reactor Simulator
* Real-time data transmission via Ethernet to monitoring point
* Other applications for our users

4. CONCLUSIONS

* The technology used in conventional instrumentation is reliable and robust but needs to be replaced and improved by a similar one with better technology and additional electronic enhancements.
* Nuclear electronics has a high degree of protection and security, due to its age, it is necessary to make improvements with compatible devices of the same standard.
* The acquisition and digitization of data is of great assistance for the monitoring, recording, transmission of data for different uses and does not affect the safe operation of the reactor.

BIBLIOGRAPHY

- IAS CAP08: Instrumentation and Control
- Safety Report RP10, Peruvian Institute of Nuclear Energy.
- http://www.ipen.gob.pe/
- Technical Scientific Report 2013, Pag. 147-150, Peruvian Institute of Nuclear Energy.
- http://dspace.ipen.gob.pe/handle/ipen/318

MODERNIZATION OF THE TEMPERATURE MEASUREMENT SYSTEM AND SCRAM LOGIC IN THE MARIA REACTOR

T. Witkowski,
National Center for Nuclear Research ,Poland
MARIA Reactor Operations Division (EJ2)
Tomasz.Witkowski@ncbj.gov.pl

Abstract. The purpose of this paper is to provide basic information of the temperature and flow measurement system in the primary fuel element cooling system in the Reactor Maria. Although Maria reactor's core has a characteristic channels type construction however to this day outlet temperature from individual fuel channel is not included to SCARM logic. The International Atomic Energy Agency's POL1014 mission gives a great opportunity to significantly increase the safety of our reactor by the upgrading the outlet temperature measurement system. Upgrading scheduled for 3rd quarter 2017 include replacement olds RTD in to a new four 2mm RTD in each channel. The system will operate in 2oo3 logic. The presentation is focuses on the technical aspects of the project with usage: process transmitters, control units and Programmable Logic Controllers. PLC will take a full control for data acquisition, data recording, fuel channel power calculation and burnup

1. INTRODUCTION

The purpose of the upgrade is to increase the safety of the reactor as well as to increase the accuracy of the measurement and reduction of delays between the actual measured channel temperature and the recorded temperature.

In addition, this system, with a small time constant, could partially duplicate the function of flow measurement in fuel channels based on 1oo1 logic.

The aim was to develop a system that would have a simple and fault-tolerant structure, modular design and ready for future upgrades. Additionally system must be compatible with the currently used recording and visualization system (SAREMA) and synoptic panel controller (SAIA)

2. MARIA RESEARCH REACTOR DESCRIPTION

The Maria reactor is Poland's second research nuclear reactor and the only one still in use. Maria is a multifunctional research tool, with a notable application in production of radioisotopes, research with utilization of neutron beams, neutron therapy, and neutron activation analysis. It operates about 4000 hours annually, usually in blocks of 100 hours.

Maria is a pool type reactor with a power of 20 to 30 MW (thermal). Primary cooling system is divided into two independent circuits:

- fuel elements cooling system
- core cooling system (beryllium as a moderator +graphite as a reflector)

Currently the core consists of about 25 fuel elements with a power rating of 1.44MW or 1.64MW. The core configuration changes according to production needs.

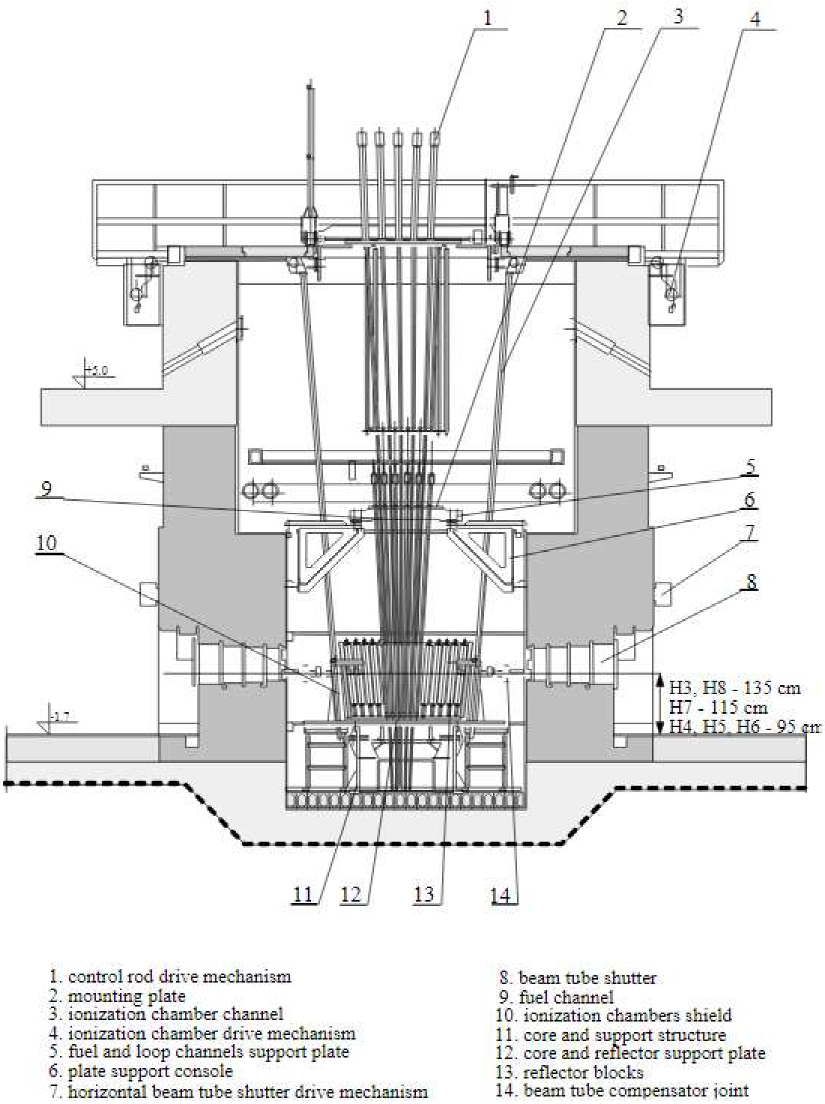


Fig. 1. Vertical cross-section of MARIA Reactor

The reactor is equipped with 13 absorption rods inserted into the core by gravity.

- 6 safety rods
- 6 compensation rods
- 1 for automatic compensation

SCRAM is performed by opening the supply circuits of the electromagnets holding the rods.

3. PROJECT JUSTIFICATION

Due to its channel type structure the reactor has the ability to accurately monitor operating parameters of each fuel Chanel such as: flow rate, outlet water temperature, channel power, burnout, fuel-cladding integrality.

Reactor Maria has been modernized many times to successively increase its safety (such as the modernization of the cooling system of fuel channels in 2013). However there are some technological systems whose modernization is extremely difficult. One of the few is measurement of cooling efficiency in an individual fuel channel.

The differential pressure (0-63kPa)from orifice plate is directed to the Rosemount 3051 pressure transducer where it converts to a 4-20mA signal (proportional to the square root ΔP). Nominal flow rate in the individual fuel channel is 25m3 to 30m3 (depending of the power).

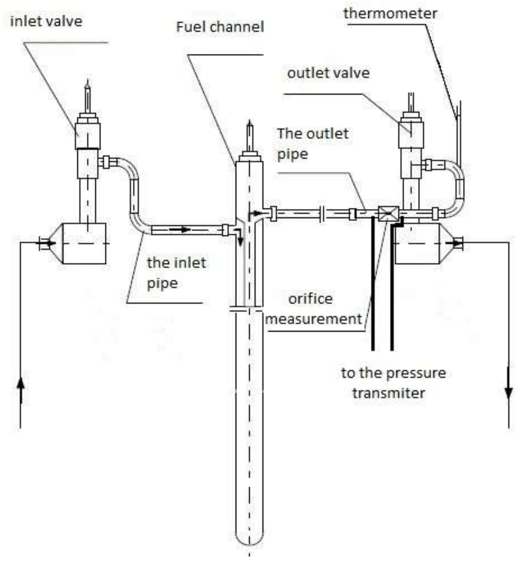


Fig. 2. Fuel channel instrumentation

Redundancy of the above mentioned system is extremely difficult due to problems with installation of additional orifice plates .

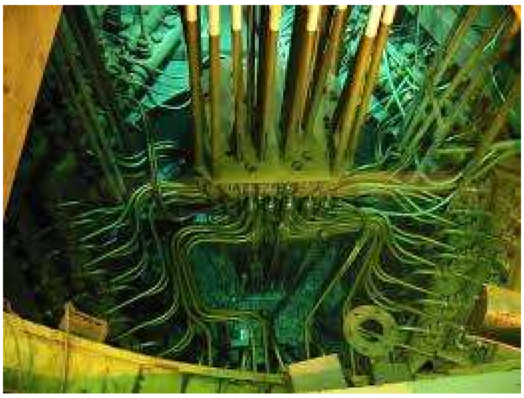


Fig. 3. MARIA RR pool

As a result of the 2014 IAEA-POL1014 mission, one of the suggestions of the inspectors was to include the outlet temperature from the fuel channels in to the SCRAM logic of the MARIA reactor. We have also decided to replace the RTD thermometers in the global measurement of the inlet temperature for the 1T1 fuel channels. Three 2-channel thermometers will be installed. They will be used to determine the reference point for calculating the fuel element power.

3.1. RTD's instalation

For increased reliability we decided to use 4 independent RTD thermometers (PT-100). The project involves the installation of 120 RTD resistance thermometers (PT-100) in 30 fuel channels. The length of each of them varies from 5.6m to 7.2m.

The choice was justified by the simple measurement of resistance, ease of calibration and testing, no need to refine the reference point (as for TC).

2mm diameter thermometers have a time constant of about 2s (similar to TC) and our old thermometers have a time constant of over > 23s

Four 2mm diameter RTD will be placed as one set in an aluminum 9mm diameter holder and then installed in an existing guide tube. They will operate 4.5 m under water. Three of the RTDs will be connected to the measurement system + 1 not connected as a reserve.

The RTD used allows temperatures ranging from 0-150 degrees Celsius

3.2. Instrumentation

TMT 112 will be used as resistance transducers (resistance to 4-20mA).

The device has SFF factor above 75%, PFDavg under 4.85E-4 and MTBF 237years. Implemented in the transmitter functions accordance with NAMUR-42 can determine a safe state of the device even if faults has been detected.

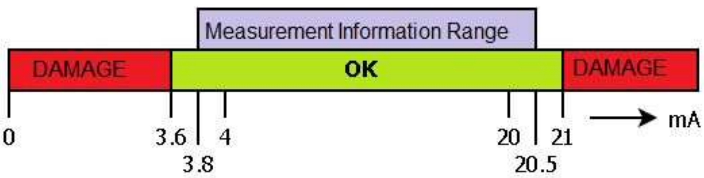


Fig. 4. Current values according to Namur-42

Another transmitter with control unit is RMA42 with 2 analog inputs / 2 analog outputs and 2 output relays (CO type) + Digital status output (open collector). Data exchange between TMT 112 and RMA42 is via an analogue 4-20mA signal. The project is intended to use the OC output to control auxiliary relays.

TMT 112 transmitter and RMA42 Control unit programming is performed using HART protocol through FieldCare software. Application of hart protocol significantly enhance the effectiveness of scaling and failure detection.

Finally, an alarm or fault signal control the safety coupling relays connected in series to the solenoids-power circuit. Operating in 1oo2 mode

Safety coupling relays are ready for SIL 3 high-demand applications.

Basic safety coupling relays parameters according to IEC 61508

- SFF: >99%
- PFH: 2.02 x10^{-11}
- MTBF: 342 years.

For the user-friendly visualization of the thermo-hydraulic parameters in the fuel primary cooling system, SAREMA's visualization and archiving system was put into service in 2007. This is a system consisting of a modular SAIA PLC with 10 input modules with 8 channels each.

Fig. 5. Sarema's main screen

The measurement resolution is 12 bits for 4-20mA inputs. This system does not directly fulfill the safety function, it is used for the acquisition of analogue data from fuel channels such as outlet temperature ,flow rate , fuel power, fuel burnout in each fuel channel and Tc99m activity calculation. Due to the increase in the number of recorded signals, SAREMA system need to be upgraded by installation of 8 additional analog input modules.

After modernization, the system will monitor over 140 signals from the primary cooling system.

In 1997 warning system of SAIA was installed, tested and implemented into operation

The SAREMA controller is connected to the SAIA PCD4 synoptic control panel via the S-bus protocol. The function of SAIA is to provide information to the operator about an alarm or warning signal with LED indicators and sound signals. Communication between SAIA via SAREMA is not necessary for proper operation of the reactor because SAIA reads data directly from the SCRAM relay outputs.

4. CONCLUSION

Significant increase reliability will be achieved by multiplication of the temperature sensors and controlled devices. Four thermometer will be instaled in each fuel channel. System logic will operate 2 of 3 for SCRAM, and 1 of 3 for warning. No need to replace SAREMA and SAIA system because a spare parts are still available.

INR PITESTI EXPERIENCE IN DESIGN, MANUFACTURING AND INSTALLATION OF DIGITAL CONTROL SYSTEMS FOR TRIGA 14 MW REACTOR MODERNIZATION

G. RADU, D. CIOBANU, M. MOCANASU, L. GRUIA, A. PULPA
INR TRIGA Reactor, Institute for Nuclear Research,
Pitesti, Romania.

Abstract

The modernization of TRIGA 14 MW reactor from Institute for Nuclear Researches Pitesti includes the primary and secondary circuits control systems up-grade and the modernization of the dosimetric system and of the control systems for many irradiation reactor facilities. This paper shortly presents all technical areas relevant to the process of I&C systems modernization and the use of digital I&C in the TRIGA modernization projects. The digital control system for an irradiation facilities will be presented, focusing on the following aspects of this new project: scope of project, specific project objectives, I&C functions improved in the modernization project, software conception and testing, project organization, design phase, installation, testing and acceptance, standards used in all phases and training for the operation and maintenance of new system. Some aspects relevant to digital I&C use in all INR TRIGA 14 MW research reactor modernization projects are presented too.

1. INR PITESTI PRESENTATION

Founded in 1971, The Institute for Nuclear Research has the main mission of supporting research and activities related to nuclear energy for peaceful purposes. During the past 41 years, the Institute has developed methods, computer codes and infrastructure with the objective of obtaining experimental equipment, specifically nuclear technologies and services. Involved in nuclear energy development, the Institute is technical support for safe and efficient operation of the Cernavoda nuclear plants with respect to international agreements.

- The main activities of the Institute are:
- Reactor physics and nuclear safety;
- Testing the irradiation;
- Post-irradiation examination materials and nuclear fuel;
- Radioisotopes and radiation technology;
- Nuclear materials and corrosion;
- Performance evaluation of nuclear fuel;
- Testing outside the reactor;
- Characterization and nuclear waste;
- Electronics, instrumentation and control;
- Qualification tests and tests for equipment, components and nuclear equipment;

— Radiation protection, environmental protection and civil defense;

— Nuclear equipment design.

Infrastructure:

— Research reactors (Material Testing): TRIGA SSR reactor station (14 MW) and pulsed reactor TRIGA ACPR;

— Post-Irradiation Examination Laboratory;

— Irradiation plant range of high activity;

— Laboratory facilities to obtain advanced nuclear fuel elements experimental;

— Equipment for testing and investigating nuclear fuel, materials and equipment used in nuclear and non-nuclear;

— Stands for testing the CANDU machine loading-unloading nuclear fuel;

— Loops for thermo-hydraulic tests at high pressure and temperature;

— Conditioning and treatment of radioactive waste.

2. TRIGA 14 MW REACTOR MODERNIZATION

2.1. TRIGA reactor description

The nuclear reactors TRIGA SSR-14 MW and TRIGA ACPR started to operate in 1979. They are both of American design, with high inherent nuclear safety, intended for research in both steady state and pulse modes.

ICN converted the TRIGA-SSR reactor from its operation on highly enriched uranium fuel (HEU) to low enriched uranium fuel (LEU). This activity began in 1992, comprised several stages and ended in 2006. During this period, the TRIGA-SSR reactor always displayed high performance.

The active zone of TRIGA – SSR-14 MW Reactor includes 29 LEU fuel elements, 8 control roads and vertical channels for neutron irradiation (neutron flux values between 2.7×10^{13} and 3.2×10^{14}).

The TRIGA-ACPR reactor have an annular pulsing zone working in the maximum 20000 MW pulse and a central channel allowing the nuclear fuel or structure materials irradiation in pulsing regimes.

Experimental installations:

(a) Standard irradiation devices:

- LOOP A-100KW: max. Temperature: 310°C; max. Pressure: 120 bars;
- CAPSULE C1, C2: max. Temperature: 300°C; max. Pressure: 120 bars;
- C5 CAPSULE: max. Temperature: 290°C; max. Pressure: 6 bars;

— C6 CAPSULE: max. Temperature: 50°C; max. Pressure: 4 bars;

— C7 CAPSULE: max. Temperature: 310°C; max. Pressure: 110 bars;

— C9 CAPSULE: max. Temperature: 300°C; max. Pressure: 120 bars.

(b) High resolution neutrons diffraction facility, DIR 1:

— Neutron radiography facility;

— PGNA spectrometry facility;

— Thermal column;

— High Activity Irradiation Gamma Facility (SIGMA).

2.2. TRIGA Reactor Modernization Activities

For the TRIGA reactor, modernization work was selected to be an approach of the "All at once" type, the method which improves the compatibility amongst implicated systems. This work included the replacement of following parts:

(a) Reactor control and safety systems including a new reactor console;

(b) Primary reactor cooling circuit control system;

(c) Radiation monitoring system;

(d) Ventilation and air conditioning equipments;

(e) And the refurbishment activities for the following parts:

(f) Secondary reactor cooling circuit (replacement of the cooling turns and of the circuit control system);

(g) Ventilation and air conditioning equipments (new air conditioning apparatus and new ventilation control system);

(h) Loop A irradiation device (replacement of the field instruments and a new control system);

(i) Capsule C2 irradiation device (replacement of the field instruments and a new control system);

(j) Capsule C9 irradiation device (new control system).

To cover all this, large areas of activities were to be simultaneous and started many projects with ICN Pitesti coordination, including collaboration with INVAP Argentina (in technical assistance IAEA project ROM 4/024) for the new reactor console.

Once the intended scope of the modernization was defined, it was needed to assess that the existing design basis documentation fulfills the necessary requirements of the modernization demands.

3. DIGITAL I&C MODERNIZATION PROJECTS

3.1. I&C modernization activities description

(a) Reactor main console

The old General Atomics production console, based on the 1970's conception, was be replaced with a new INVAP production console.

The components of the console are:

— One logarithmic large scale channel with fission chamber type detector for 10 decades neutronic power and for reactor power evolution period; the period channel have a 3 second safety period limit;

— One liniar large scale channel using the same detector like the logarithmic channel for 10 decades neutronic power;

— Three channels with separate fission chamber type detector each used for safety system;

— Three fuel temperature channels with separate thermocouple each used for safety system;

— Pool water temperature monitoring system coupled to three thermoresistors;

— Reactor control circuits for the 8 roads used in reactor power control or reactor scram;

— Reactor safety system (Scram for over power or detector high voltage fail in 2/3 logic, fuel temperature too high in 2/3 logic, period above 3 seconds, external or manual command).

(b) Primary and secondary cooling circuits control system

The old relay logic control system was replaced with a new one, based on PLC's with process dedicated real-time software, DI/DO and AI/AO bridge structure and PC for data acquisition in SCADA system.

The system performs the acquisition, storage and displaying with alarms status for process parameters like temperature, pressure or flow values and the status of circuit components (valves, level indicators, etc.)

(c) Radiation monitoring system

A new radiation monitoring system was designed and commissioned for the INC Pitesti TRIGA reactor. The concept of this system includes more radiation monitoring units (area monitors, gaseous effluents monitors, water effluents monitors) coupled to a central alarm station. All effluents monitors are based on Canberra developed on-line spectroscopy using NaI detectors and dedicated software.

(d) Irradiation devices control systems

The control systems for the irradiation devices Loop A and Capsule C2 was designed, manufactured and commissioned in INC Pitesti, replacing the old control systems together with the irradiation devices. The process diagram and safety actions diagram for each device was

was used for the same structure of the field instruments (transducters and actuators). The hardware structure of the control systems is practically the same excepting I/O modules configuration and the specific character was be done by the application software modules. The technical characteristics of the Capsule C2 device control system will be done later in this presentation.

3.2. Digital I&C Projects Execution

The modernization project execution includes the following phases:

(a) Feasibility phase - to select and define the scope of the project;

(b) Requirements specification phase based on the overall requirements specification;

(c) The preliminary design – during this activity the system architecture is selected , system requirements are allocated to hardware components, software components and to personnel and a system requirements analysis are performed;

(d) The overall system architecture design phase to identify items of hardware, software and manual operations and its requirement specifications;

(e) Implementation phase – manufacturing or procuring hardware components and the development of new software components;

(f) Integration and testing phase , normally in simulated environment;

(g) Installation and commissioning, training and operation;

(h) Licensing activity.

A safety demonstration for the I&C modernization projects encompasses the entire project life cycle, involving preparation of documentation and the collection and integration of evidence from verification, validation and audit activities for all phases of the system life cycle.

Each project was classified using CNCAN (Romanian Regulatory Body) norms which have like classification factors nuclear safety class, design complexity, implementation complexity and economic effects.

Digital I&C modernization projects that use non-nuclear qualified COTS equipment needs development of a qualification process to ensure a desired level of quality. For customized digital equipment and software developed for nuclear applications, the required assurance was developed by controlling and monitoring the hardware and software design, the implementation process, the integration process and testing, as well through formal V&V programs. The following documents must be followed in this situation:

(a) Design Service Dossier containing Technical Specification, Design Plan, design verification and design modification documentation;

(b) Quality Plan cf. SR ISO 10005/2007 (romanian version of ISO 10005/2005) covering implementation, integration and testing.

For each activity, it is mandatory to respect a QA procedure documented by the Quality Assurance Management Department.

The software V&V is included in Quality Plan and the software verification team is mandated to not include personnel from the software development team. The process consists of adequacy of the software performance to requirements verification, decomposition into software functional modules control, the configuration control and the integrated system verification (functional tests report).

4. DIGITAL CONTROL SYSTEM FOR CAPSULE C2

4.1. Hardware configuration

The Capsule C2 control system is based on the industrial Siemens – SIMATIC components connected through a PROFIBUS communication line. This distributed control structure includes:

— Central station (PC Siemens Simatic Panel type) with the role of operator console, data acquisition, data procesing and preparing of data reports;

— Two PLC's (Siemens Simatic S7 -300) for process parameters aquisition and commands, identical as hardware structure and software components. These PLC's is connected to Central Station by Profibus and operate independently like redondant control structure;

— One PLC (Siemens Simatic S7 -200) connected to Capsule C2 Console by RS485 line and used for power heating modules control and LOCA experiment monitoring;

— Process data acquisition circuits (amplifiers, splitters, local power sources, computer acquisition circuits and ADAM devices) and command execution circuits (relay logic circuits, lamps, connectors, etc).

The process parameters are transmitted to the TRIGA Reactor central server by an Ethernet line after acquisition and processing.

The Capsule C2 control system is mounted in two standard 19 inch racks, one for field instruments connexion, process data acquisition circuits, S7-300 type PLC's and commands execution circuits for field actuators and the second for S7-200 type PLC and power electronics.

The components are from normal industrial production, ISO 9002 certified.

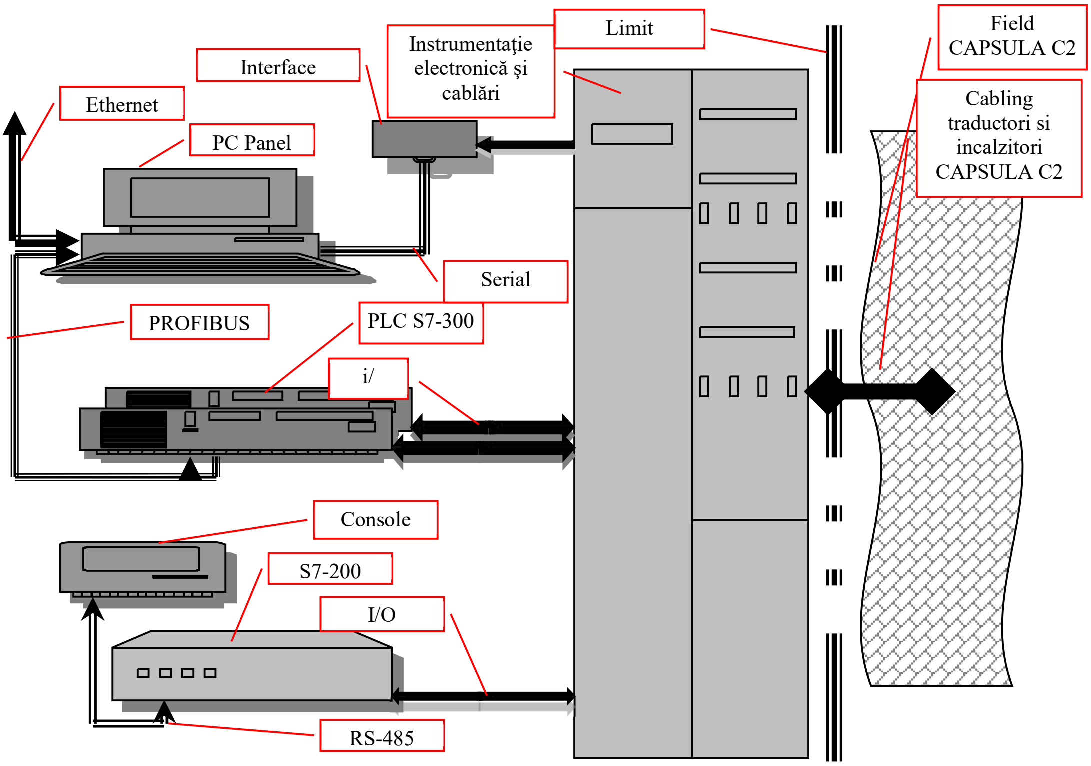


FIG. 1. Hardware configuration.

4.2. Software configuration

All control-command functions like the system functions are implemented by a specific programme for each programmable component. For the relation between process events and legal time, like for the marking of data acquisition reports, the Central Station internal clock and date is used.

The main software modules are:

— Operator console software – generate pages used like virtual console (virtual control commands and lamps, parameters values and alarms) on Central Station;

— Local control and safety software on redondant PLC's;

— Local control-command software on PLC S7-200.

S7-300 type PLC's uses SO Windows platform with STEP 7 programm and the S7-200 type PLC uses MicroWin and TP Design programms. The operator interface is generated on an SO Windows platform using WinCC and Visual C++ programms. All user licences for these programmes are transmitted to the end-user.

The process control software is delivered in an executable implemented format, as aresource programmes too.

4.3. Control system tests

(a) Components verification;

(b) Operator console preliminary verification – computer operating system;

(c) Field signals conditioning test using an field signals simulator included in control system structure;

(d) Virtual panel testing;

(e) Control and safety functions testing using the field signals simulator;

(f) Data acquisition and storage time verification.

5. CONCLUSIONS

The design, implementation, testing, installation, commissioning and licensing activities relative to digital I&C systems developed by ICN Pitesti Romania are aimed to provide higher performance and an economic and rapid process for the TRIGA reactor modernization.

All digital applications included in the TRIGA reactor modernization activities have regulatory body supervision in all execution phases of the modernization projects and is licensed in normal operation.

The Institute for Nuclear Research is considered the most important R&D unit in our country, assuring the technical support for Cernavoda NPP's and other nuclear facilities. The Instrumentation and Control Department will continue the digital I&C projects based on the combination of subsystems created by integrating different sensors and equipments with proprietary software.

For future applications, these systems and equipment will be designed in a flexible manner, being able to present any type of data, with the opportunity to assess the availability and adequacy of local response plans, area mapping, and local coordination.

TRR-1/M1 INSTRUMENTATION AND CONTROL UPGRADE PROJECT: EXPERIENCES ON DESIGNING THE NEW I&C SYSTEM

S. Wetchagarun[1], C. Tippayakul[1], A. Petchrak[1], K. Sukrod[1], and P. Knoonkamjorn[1]

[1]Thailand Institute of Nuclear Technology (Public Organization), Bangkok, THAILAND

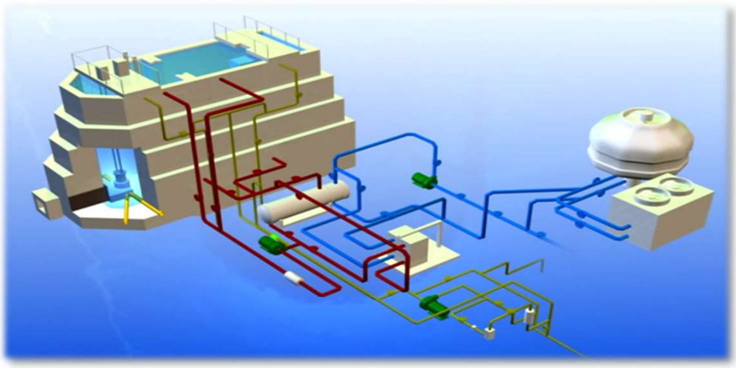
E-mail contact of main author: saensuk@tint.or.th

Abstract. Thai Research Reactor 1 Modification 1 or TRR-1/M1 has been served the country as the only research reactor in Thailand since 1977 after the core was converted from the Thai Research Reactor 1, TRR-1. During the core conversion process, some of the reactor structures and components such as the reactor pool, the cooling system and the ventilation system had been retained as the original structures. Some parts of the reactor, including the instrumentation and control (I&C) system, were modified to suite the new reactor core. For decades, TRR-1/M1 structures and components have been carefully maintained in order to ensure the safe operation throughout its lifetime. As the reactor aged, however, TRR-1/M1 were facing challenges especially its I&C system as it faced component ageing and obsolescence. Some of the I&C components of TRR-1/M1 encountered lack of spare part problems as they were discontinued from their manufacturer process. This situation has impact on safe and reliable operation of the reactor. TRR-1/M1 Instrumentation and Control Upgrade Project was initiated in 2009 in order to extend the operating lifetime and increase capability of the reactor. The reactor new I&C system had been designed, installed, tested and commissioned primarily by TRR-1/M1 staffs with technical advices and supports from Korea Atomic Energy Research Institute (KAERI) experts. The new reactor regulating system was digitalized while the reactor protection system was maintained the original concept as a hard-wired system. The objective of this paper is to share experiences obtained throughout the I&C upgrade project regarding to the designing of the new TRR-1/M1 I&C system.

Key Words: Instrumentation and Control upgrade, Digital I&C, I&C of research reactor, TRR-1/M1

1. INTRODUCTION TO TRR-1/M1

For more than 40 years, Thai Research Reactor 1 Modification 1, TRR-1/M1 has been served as the only research reactor in Thailand. It is located at the north edge of Bangkok, the capital city of Thailand. TRR-1/M1 has wide ranges of utilization from medical, agricultural, industrial, education, training to research and development. The reactor core is TRIGA Mark III, open pool type using light water as coolant and moderator. The reactor was currently licensed for 1.3 MW with the operation time of 52 hours per month. **Error! Reference source not found.** illustrates the configuration of TRR-1/M1 facility.



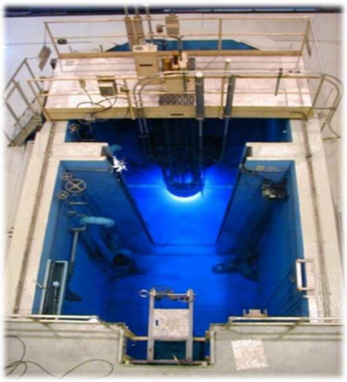


Fig. 7 TRR-1/M1 facility

2. BACKGROUND OF TRR-1/M1 INSTRUMENTATION AND CONTROL UPGRADE PROJECT

As TRR-1/M1 has been in operation for decades, the old instrumentation and control (I&C) system, which was the analog type, was out-of-date and many components were obsolete. It was quite difficult to find spare parts to replace the failed components and to maintain the system [1]. In order to extend the reactor operating lifetime, ensure safe and reliable operation and increase capability of the reactor, a project to replace the old I&C system with a newer one was proposed. It was expected that the new system would extend the operating life of TRR-1/M1 for at least another 10 years [1].

The TRR-1/M1 I&C Upgrade Project was under a Memorandum of Understanding (MoU) for technical cooperation on nuclear technology between Thailand Institute of Technology (Public Organization), TINT and Korean Atomic Energy Research Institute (KAERI). The project was officially initiated in November 2009. Under this Project, TINT staffs were the main designers of the system while KAERI experts acted as technical consultant providing a training course, technical consultations, document reviews and technical review visits. The project lasts for more than 7 years as the hot commissioning of the new I&C system was completed in March 2017.

Under the I&C Upgrade Project, the following systems had been designed and replaced or refurbished.

- Reactor Protection System (RPS)
- Reactor Regulating System (RRS)
- Motor for control rod drive mechanism (CDM)
- Neutron detection system
- Reactor control room

This paper provides some experiences on designing process of the new TRR-1/M1 I&C system TINT staffs earned during the I&C Upgrade Project.

3. EXPERIENCE AND LESSONS LEARNED FROM DESIGN THE NEW I&C SYSTEM

This section described the design process and major lessons learned during the design phase of the TRR-1/M1 I&C Upgrade Project gathering from TINT technical team performing the design tasks.

3.1. Design of the new system

Design of the new systems under TRR-1/M1 I&C Upgrade project performed primarily by TRR-1/M1 technical staffs. The design process could be divided into 4 steps: 1) initial training, 2) system basic design, 3) concept validation, and 4) system detail design. The details of each steps are as follows.

3.1.1. Initial training

A one-week training workshop for upgrade the reactor I&C system was provided to TINT staffs by KAERI experts at the very beginning phase of the project. The workshop covered important issues needed to be considered for the modification of the reactor I&C system. The topics included, for example, reactor safety and design, cable and standard, RRS/RPS design and upgrade, reactor control dynamics, commissioning, and licensing documents. It is very important for a technology transfer project that the technical team learned and understood the main processes needed to perform from the beginning phase, so the plan can be set accordingly. From the TRR-1/M1 I&C Upgrade Project, it is found that the learning curve of the research reactor's I&C system technology was quite steep.

3.1.2. System basic design

The first system designing step was to perform system basic design. In this stage, the design change requirement for each system including RPS, RRS, motor for CDM, NDA were addressed. The design change requirement provided the scopes for subsequent design works. It described performance requirement, interfacing requirement, functional requirement, design requirement, reliability requirement, testing and maintenance requirements etc. The more concrete of the design change requirement, the easier for the subsequent design works. To specify the design change requirement for each system, the project technical team explored the I&C design of other research reactors as well as the original design of TRR-1/M1. The investigated systems were analyzed and carefully selected based on the safety, performance, reliability, price, and licensing aspect. The chosen design was then documented into the design change requirement for each modified system. For the new I&C system, the safety, safety-related, and non-safety systems were clearly separated. The design change requirement issued for each TRR-1/M1 I&C upgrade system are as follows.

a) Reactor Protection System (RPS)

The new RPS was decided to be analog type like the original TRR-1/M1 safety system. The decision was based on the fact that digitalized the reactor safety system would be difficult for the licensing process because the experience in using digital safety system was still not widely accepted in the country at the time. Therefore, in the design change requirement, all components for the RPS was defined to be analog system. The RPS for TRR-1/M1 included neutron detection systems, annunciators, fuel temperature assemblies, and trip circuit assemblies. Trip logic was the important part of the RPS and was designed based on the original TRR-1/M1 trip system with one additional trip—reactor period in order to increase safe operation of the reactor. The trip circuit assemblies used relay to perform function of the reactor trip circuit. **Error! Reference source not found.** showed the RPS logic diagram.

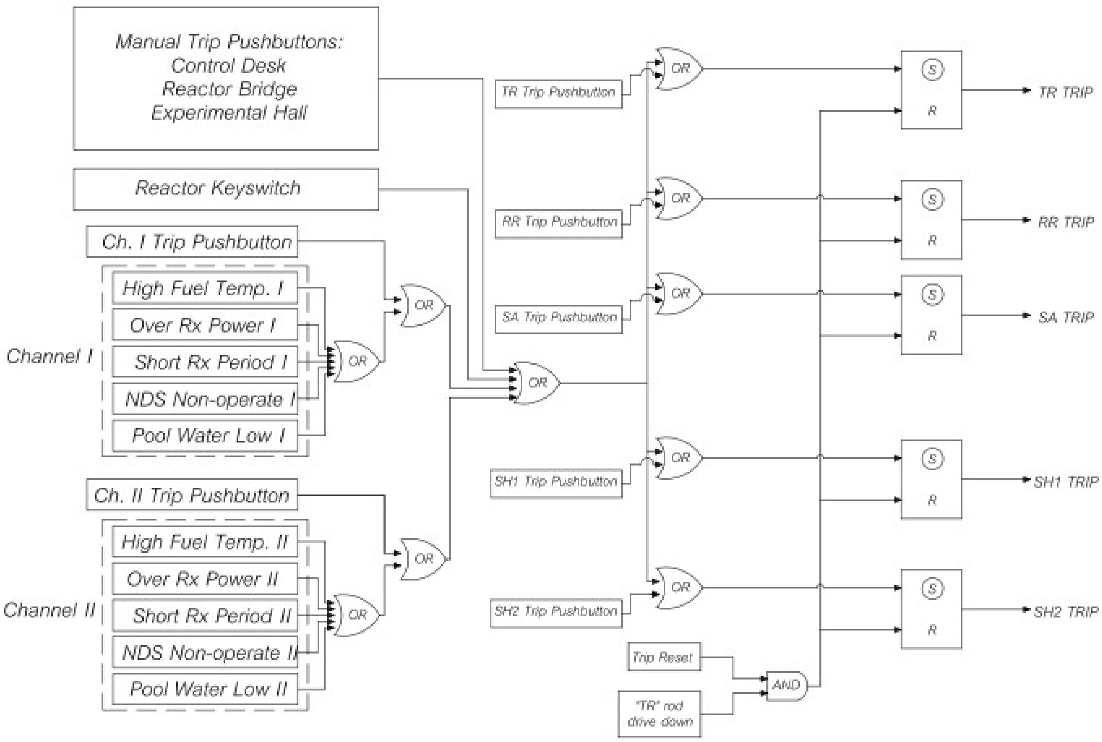


Fig. 8 RPS logic diagram [2]

b) Reactor Regulating System (RRS)

The RRS was selected to be digitalized to take advantage of its easy operation, good performance for monitoring, controlling, and data logging, and availability of the components in the market. An industrial microcontroller was used as the central processing for the RRS.

The RRS, which has the function to regulate the reactor power and to monitor reactor and process parameters, is designed to be a programmable controller-based system. The RRS applies the redundancy principle, i.e., there are two programmable controllers and two operator workstations to increase reliability. The general connection diagram of RRS is shown in **Error! Reference source not found.**.

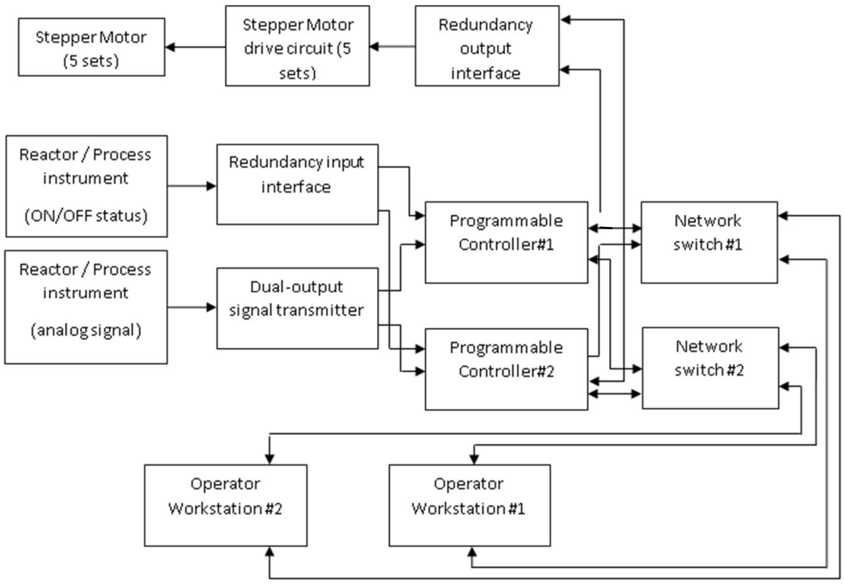


Fig. 9 Overview diagram of RRS [4]

The motor for control rod drive mechanism was also replaced. The stepper motors were chosen to replace the original servo motors. This selection increases the capability on controlling and monitoring the movement of the control rods.

3.1.3. Concept validation

After the basic design of the I&C system was set up, some major concepts were validated before proceeding to the system detail design in order to increase the confidence of the design concepts.

a) Hardware

To validate the design concept and test the hardware compatibility interface between systems, conceptual hardware had been procured or built to test the function and compatibility. For example, a pilot-scale relay circuit was built in order to validate some key functions of the reactor trip circuit such as trip function and resetting. A stepper motor was also procured to test its control function and interface compatibility with the existing control rod drive mechanism.

b) Software

In the TRR-1/M1 I&C Upgrade Project, LabView technology was selected to be a software platform for the new RRS due to its long time well performance in an industrial setting, high availability for industrial I&C, widely used with active users worldwide and relatively simpler to learn and program. With all the reasons considered, it is expected that LabView platform would not be obsolete in a relatively short time.

The LabView platform was procured to test the conceptual design software of the RRS during this stage. Different parts of the RRS program were tested by using small programs including testing of signal input from field instrumentations and stepper motor controller.

c) Control algorithm

Another important part in the I&C upgrade system which was tested during the design validation stage was the control algorithm. The function of the reactor control algorithm was to regulate the reactor power by using mathematic formula to perform feedback loop control.

In order to test the control algorithm, a TRR-1/M1 kinetic model along with the reactivity feedback from Xenon poisoning, fuel temperature, coolant temperature, and control rod position was developed on SIMULINK platform. The reactor kinetic model was validated with another model developed by m-script files in order to increase the confidence of the model correctness. After the model validation, it was used to evaluate the reactor control algorithm performance by coupling both programs, kinetic model and control algorithm, in SIMULINK. The coefficients in the control algorithm were adjusted until the simulation result met the desired criteria [1]. The validated control algorithm was then ready for reactor power control. Step-by-step testing with small programs was found efficient in identifying the part that needed correction or improvement.

3.1.4. System detail design

After the basic design and concept validation were completed, the detail design for each component were performed. The detail design stage covered both before and after the procurement of the components. This stage included preparing technical specification documents for procurement, system manual, safety analysis for modification permit, system layout and drawing, installation plan and procedure, and etc. Quality assurance requirements were specified for suppliers/manufacturers of procured components. This is found to be useful in keeping quality of all components to the required standard, especially for those in the safety system.

There were several challenges encountered during this detail design stage. For example, interface compatibility between new I&C system and other existing systems, lack of as-built wiring diagram/information of cables needed to be connected with the new I&C system, limited of a formal quality assurance program in some domestic supplier/manufacturer organizations as specified in the product quality requirement.

Aside from the I&C system design, the reactor control room and operator console desk refurbishment were also included as parts of the I&C Upgrade Project. The design of the control room layout and the operator console configuration considered both operating experience and ergonomic consideration. Combining these two aspects was found to be beneficial in case of TRR-1/M1 operation because the reactor operators experienced comfortable operating environment, which was similar to the old I&C system, but not scarified their health with the non-ergonomic postures.

Error! Reference source not found. to **Error! Reference source not found.** showed the final systems for RPS, RRS, and control room layout.

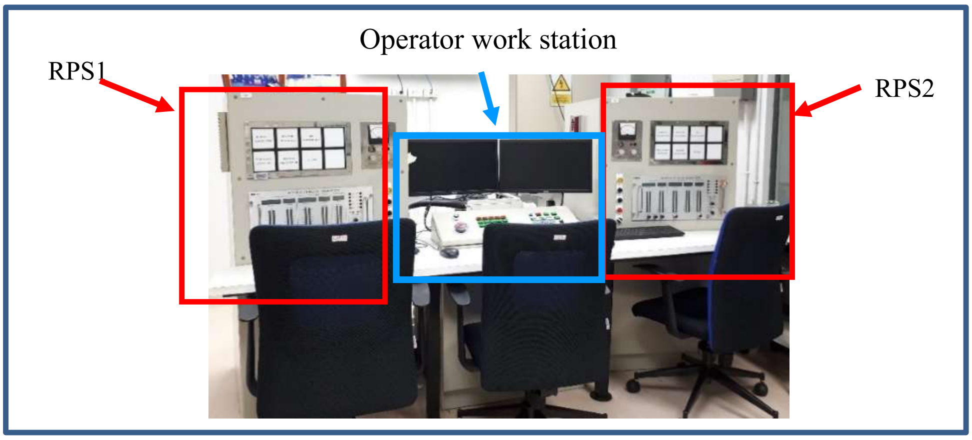


Fig. 10: Operator console desk

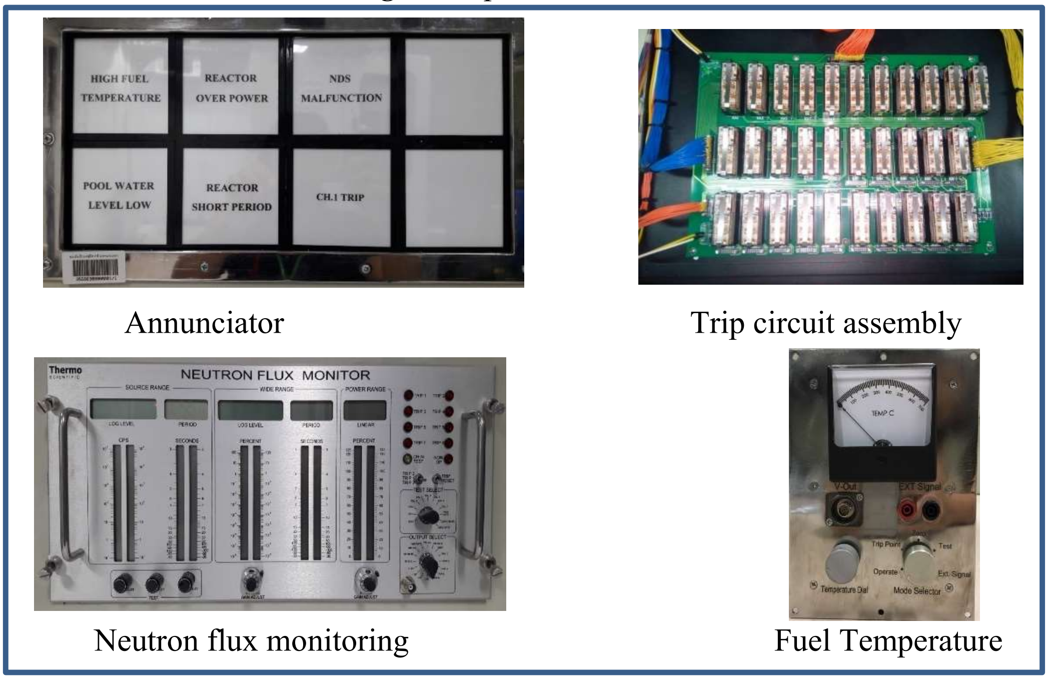


Fig.5: RPS components [3],

Fig. 6: Some RRS components [5]

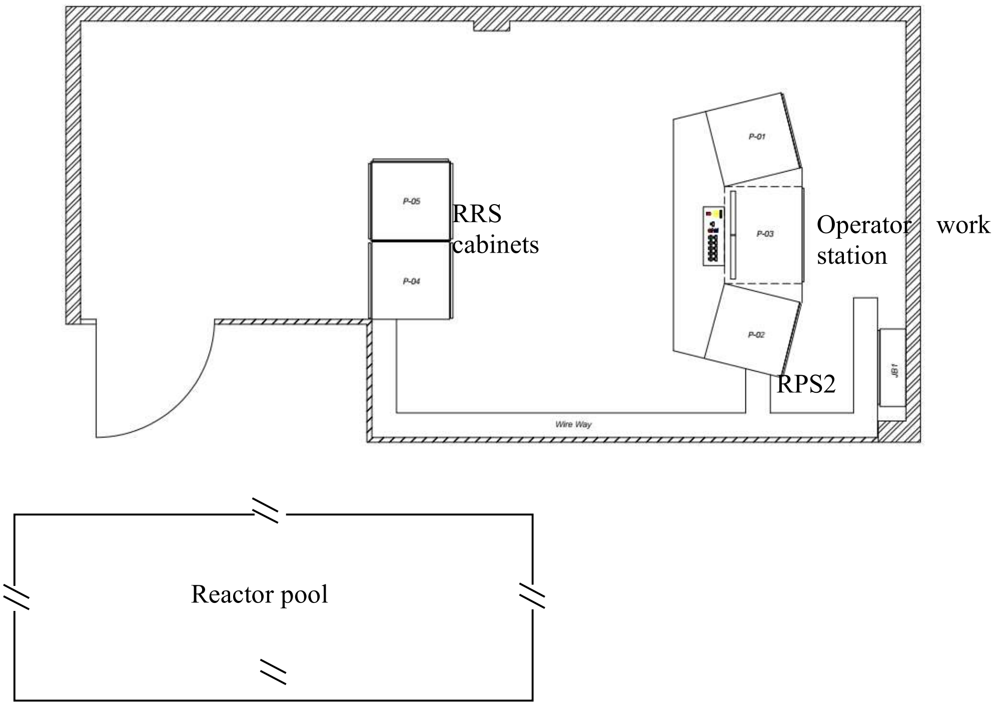


Fig.11: New control room layout [5]

3.2. Lessons learned

There were a number of lessons learned throughout the design process of the new TRR-1/M1 I&C system. Some highlights are:

- Cooperation with experienced organization was crucial for the success of the technology transfer project, especially for an inexperienced institute. Technical advices and knowledge transfer from KAERI experts were very beneficial in many aspects for example reduce trials and errors time, assist with organizing well-planed design process, and help initiate design ideas.
- The learning curve for the project related to technology transfer was steep for inexperience organization. It is very important to allocate enough time at the beginning of the project for the staffs to learn new concepts and technology.
- The quality assurance (QA) program for the technology-oriented project was very important in the project management. The QA program should be established and implemented from the beginning of the project. During the design phase, it is found that implementation of the established QA program through procedure for document control, reviewing of the design, verifying of the design, component and system testing and validation was very beneficial. Tracking of the design documents were easy and well organized.
- Validation of the conceptual design parts by parts helped avoid project failure at the end due to incompatible or inappropriate design of components or systems.

4. CONCLUSION

TINT initiated the TRR-1/M1 Instrumentation and Control Upgrade Project in 2009 in order to extend the reactor's safe and reliable operating lifetime as well as to increase the reactor capability through its modernized I&C system. The project last for more than 7 years as this project was the first major reactor modification performed primarily by TINT staffs. Good cooperation with experienced experts from KAERI was one of the major key success factors of this project. Well planned and step-by-step design and validation process help avoid failure of the project when integrate all parts, components and systems together. Lessons learned from this project may be useful for other operating organizations planning to upgrade or modernize the I&C system of their nuclear facility in the future.

REFERENCES

[1] TIPPAYAKUL, C., Project Summary Report: TRR-1/M1 Instrumentation and Control Upgrade Project, ICU-SPD-MEM-064, Thailand Institute of Nuclear Technology (Public Organization), Bangkok (2017).

[2] WETCHAGARUN, S., Design Manual for Reactor Protection System: TRR-1/M1 Instrumentation and Control Upgrade Project, ICU-RPS-DSM-001, Thailand Institute of Nuclear Technology (Public Organization), Bangkok (2015).

[3] Operation Manual Trip Circuit Assembly (TCA), Siam Integration Systems, Bangkok (2016)

[4] WETCHAGARUN, S., Design Manual for Reactor Regulating System: TRR-1/M1 Instrumentation and Control Upgrade Project, ICU-RRS-DSM-001, Thailand Institute of Nuclear Technology (Public Organization), Bangkok (2015).

[5] TIPPAYAKUL, C. and WETCHAGARUN, S., Instrumentation and Control system Operation Manual: TRR-1/M1 Instrumentation and Control Upgrade Project, ICU-GEN-ICM-018, Thailand Institute of Nuclear Technology (Public Organization), Bangkok (2017).

DIGITAL I&C SYSTEMS FOR NEW FACILITIES AND MODERNIZATION OF EXISTING RESEARCH REACTORS

F. WIJTSMA
PALLAS
Petten, The Netherlands

A new high flux research reactor, PALLAS, is being realized in Petten, the Netherlands to replace the well-known High Flux Reactor (HFR) who has come to its end-of-life phase characterized by the need for increased maintenance and refurbishment.

The safety demonstration will be fully based on the IAEA safety requirements for RR and, due to its power level, requirements for NPP will be applied using the graded approach. PALLAS will be, like the HFR, one of the major suppliers of radioisotopes and transmutation silicon and will be also tailored for the irradiation of materials (fuel and structural materials) for nuclear industry and science. Its main features are:

— Tank-in-pool reactor type;

— Flexible power level from 30 to 55 MW;

— Isotope production and nuclear research capacity in the reflector zone and in-core;

— A Supplementary Control Room (SCR) fully independent of the Main Control Room (MCR).

Additional safety requirements expected from Dutch licensing authorities, including but not limited to:

— Withstand high internal pressure (“Borax accidents”);

— Aircraft crash (both military and commercial type);

— Long “grace period” in case of accidents (including BDBA);

— Core Damage Frequency < 10^{-6};

— Requirements of the post-Fukushima evaluations.

The general requirements for the protection system and control and monitoring systems are based on the international guidelines and best practices for RRs, and are a combination of digital and analogue systems which are fully diverse, independent and physically separated. The requirements comprise:

— All instrumentation and equipment monitored and controlled from MCR and SCR.

— The SCR to monitor and control the 3 basic safety functions but not to operate PALLAS.

PALLAS to be equipped with:

— First Reactor Protection System (digital) and connected First Shutdown System;

— Second Reactor Protection System (analogue) and Second Shutdown System;

— Post-Accident Monitoring System.

All systems and components to be designed and installed based on:

— Reliable with (extreme) low failure rates under design and DBA conditions;

— Common cause and common mode proof;

— Diverse, redundant and independent;

— Physically separated in lay-out and cabling routes.

The main objective of the RPS is to bring the reactor into a safe state, after the occurrence of a postulated initiating event which can be either an internal event, external event or a combined event (‘multiple events’) in case there is a relation between the occurrence of single events (post-Fukushima evaluation). The PALLAS reactor protection system shall be:

— Designed to be automatic and independent of all other systems;

— Physically separated from the reactor control and monitoring system;

— Automatically initiate a scram on the basis of the safety system settings or as required by OLCs;

— Automatically initiate shutdown upon loss of off-site power;

— Incorporate a seismic detection system to trigger a reactor scram.

Where the RPS main objective is to ensure a safe and reliable shutdown of the reactor and to mitigate any further negative effects, the Reactor Control and Monitoring System (RCMS) is designed to continuously monitor the status and trends of the parameters of all systems and control these within the required limits. The design criterion for the RCMS is:

— To control and monitor the status of all SSCs unless only local control is appropriate from a safety/operational point of view.

The RCMS shall be equipped with:

— Instrumentation for monitoring the process systems in normal operation and for recording all variables important to safety;

— Necessary controls, both manual and automatic, to maintain parameters within specified operating ranges;

— Wide range of indicators and recording instrumentation to monitor important reactor parameters during and following anticipated operational occurrences and DBAs;

— Instrumentation and controls for safely shutting down the reactor and maintaining it in a safe state in the MCR and SCR;

— Sufficient capacity for the SSCs of all support systems and for output signals to the Emergency Control System (ECC) and newly developed applications/modifications;

— Audio and visual alarm systems for the early indication of changes in the operating conditions of the reactor that could affect its safety;

— Equipment that shall be as much as possible of the “off-the-shelf” type;

— Irradiation facilities shall be equipped with the necessary instrumentation for control and monitoring of their operational behaviour and process parameters and for recording all parameters important to safety.

Finally a Post-Accident Management System (PAMS) will enable monitoring all safety relevant parameters after the postulated occurrence of an accident; its main features are:

— The indicators and recording instrumentation connected to the PAMS will monitor important reactor parameters during and following (DBAs) and (DBDAs);

— PAMS shall be integrated in the MCR and SCR;

— PAMS shall have sufficient I/O devices to connect monitoring equipment to the ECC;

— Area radiation monitoring equipment shall be installed to enable the operator to have an overview of radiation levels throughout the installation.

With the design requirements for the RPS, RCMS and PAMS summarized above, PALLAS will meet the most stringent requirements on safety and reliability and will result in a powerful nuclear tool for the production of radioisotopes and fulfilling the demands of nuclear R&D for science, technology and industry.

EXPERIENCE ON MODERNIZATION OF REACTOR CONTROL AND PROTECTION SYSTEMS OF RESEARCH REACTORS

A. Zaikin, A. Lokantsev, M. Romanichev
JSC “SNIIP-SYSTEMATOM”
Moscow, Russia

Abstract

JSC “SNIIP-SYSTEMATOM” performs full scope of works from the development of the technical specification and manufacturing to the commissioning and maintenance of equipment for control and protection systems of nuclear power plant’s reactors as well as research reactors (RR). Since 2000 through 2016 seven RRs of various types in Russia and abroad were upgraded with new equipment supplied and commissioned by SYSTEMATOM. There were also RR IVV-9 (Dalat, Vietnam in 2007) and WWR-SM (Tashkent, Uzbekistan in 2013) among them modernized within the framework of technical cooperation projects of IAEA.

Each research reactor is special, (even reactors are of the same type, e.g. WWR) in terms of technical characteristics, number of monitored parameters, algorithms of reactor protection and control. Therefore instrumentation and control system for each research reactor demands a customized design. New equipment, consisting mainly of digital devices, comes to replace the obsolete equipment that has run out its resource. Modern digital technologies (programmable logic and microcontrollers) make it possible to apply the same hardware solution to several projects with specific requirements by redesigning of firmware and software. High logic volume of field programmable gate arrays and high performance of microcontrollers allow to implement the basic functions and to add new features to the system: expand or add new self-diagnostics function, significantly improve the human-machine interface, archive all signals, lock root cause of emergency shutdown and reduce the influence of "human factor".

Since 2000 when SYSTEMATOM developed the first generation of equipment for the research reactor, electronic components have changed significantly; changes mainly relay to digital microcircuits, controllers, computers and displays. Many of the components and devices used in the development of equipment in 2000 are obsolete now. Only design concept and basic system operation principles of equipment for control and protection system of RR remain unchanged. We develop reliable and resilient I&C systems, because system architecture is based on the company's experience in safety system’s design and practical operation data, up-to-date requirements for safety systems, reliability and fault-tolerance. Fourth generation Complexes of equipment for reactor control and protection system made of modern components are supplied at present time to RRs. The following paper details the architecture of complex of equipment for protection and control system of RRs, designed by SYSTEMATOM, new features implemented, installation and commissioning process on WWR type RRs.

1. INTRODUCTION

Nowadays I&C systems of most research reactors in the world need modernization due to physical degradation of equipment. An integral part of the reactor safety system is the electronic equipment of reactor control and protection system (CPS). CPS equipment, often developed and installed in the 1960s … 1980s, run out its resource, has an increased failure rate and in some cases does not fully comply with modern requirements for nuclear safety. To maintain acceptable performance of the equipment by repairing or partial replacing the failing units becomes practically impossible due to the obsolescence of spare parts and components. Therefore, to ensure the stable reactor operation in the long term a complete modernization of CPS equipment is the most appropriate solution.

SYSTEMATOM performs full scope of works from the development of the technical specification and manufacturing to the commissioning and maintenance of equipment for control and protection systems for WWER and BN types of reactor of nuclear power plant's as well as research reactors. Since 2000, new equipment for control and protection systems has been manufactured and delivered to 12 research reactors of various types in Russia and abroad (Table 1). By the middle of 2017, new I&C systems manufactured by SYSTEMATOM have been put into operation and currently used on seven RRs and one critical assembly. There were also RR IVV-9 (Dalat, Vietnam in 2007) and WWR-SM (Tashkent, Uzbekistan in 2013) among them modernized within the framework of technical cooperation projects of IAEA. Four new complexes of equipment for reactor control and protection systems are delivered to end-users (RRs in Russia: BOR-60, WWR-M, IVV-2M, RBT-10/2), ready for installation and commission.

TABLE 1: I&C SYSTEMS MODERNIZED BY SYSTEMATOM ON RRS

RESEARCH REACTOR	Reactor I&C systems modernized (I&C systems supplied by SYSTEMATOM)												
	Nucleonic (safety)	Nucleonic (Emergency Control	Process	Process Instrumentation (non-safety)	Seismic Protection	Control Rod' s position monitoring	Reactor Protection	Reactor Control Logic	Automatic Power	Reactivity Meter	Main Console	CPS Data Recorder	Data Base Server and Terminal(s)
MIR.M1, Russia	✓	✓				✓	✓	✓	✓	✓	✓	✓	
IVV-9, Vietnam	✓		✓			✓	✓	✓	✓	✓	✓	✓	
PIK, Russia	✓	✓	✓			✓	✓	✓	✓	✓		✓	
IBR-2, Russia	✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓
WWR-SM, Uzbekistan	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Critical Assembly, Kazakhstan						✓	✓		✓	✓		✓	
WWR-c, Russia	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓	
WWR-K, Kazakhstan	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓		✓

Reactor I&C systems modernization scope depends on objectives (replacement of obsolete equipment, improvement of characteristics, expansion of capabilities) and available funding. The list of upgraded systems at various research reactors is shown in Table 1. Even small refurbishment, for example, replacing rod's position monitoring devices or replacing the automatic power regulator, leads to updating the display system on the operator console and the data recorder system. With large-scale modernization of I&C systems, various systems are combined into I&C complexes and designed simultaneously, that makes possible integration of various systems at the production stage, the implementation of a common human-machine interface (HMI) and data archiving system for all systems. Integration testing of a whole complex of equipment at the manufacturing plant significantly reduces the time of I&C system installation and commissioning at a site.

2. BASIC TECHNICAL DESIGN PRINCIPLES AND SYSTEM FEATURES

Reactor control and protection systems as systems important to safety must meet a number of specific requirements aimed at achieving high reliability and fault-tolerance in capability of a system to perform safety function [1, 2]. The reactor protection system should have redundancy, predictable failure state and fail-safe design, meets criterion of independence (functional independence, electrical isolation, physical separation, etc.). Taking into account all mentioned above requirements SYSTEMATOM has designed and developed the reactor protection and control system (signals initiation electronic part of the system) with both protection and control functions, it also provides monitoring function. The basic unit of the system is Integrated Reactor Protection Channel (IRPC) which has all instrumentation to process the full set of process parameters and signals needed to perform reactor protection and control functions. Protection and control system structure is described in the section below, more detailed description of IRPC is given in the section 2.2.

2.1 Reactor protection and control system structure

Typical reactor protection and control system structure with three independent IRPCs and "2 out of 3" vote logic (2oo3) is shown on Fig. 1. For simplicity of the drawing only nucleonic part of reactor protection system is shown, approach for other instrumentation of safety parameters (temperature, coolant flow, coolant pressure, seismic, etc.) is the same as for nucleonic. Each module of the IRPC performs its function independently from the same modules of other IRPCs. Reactor protection and control system architecture and device configuration of each IRPC in a system depends on reactor specific process instrumentation configuration.

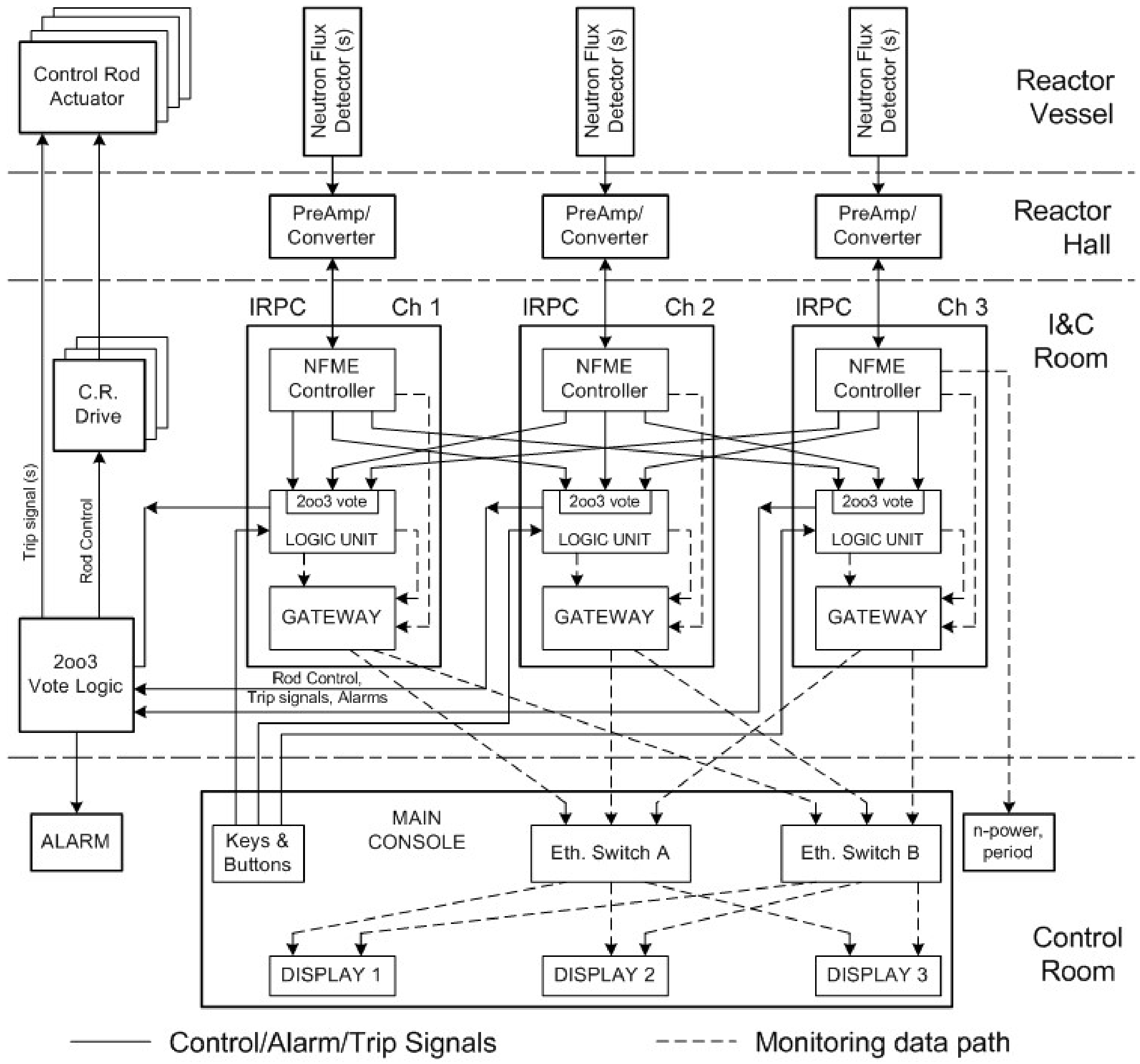


FIG. 1 Simplified Protection and Control System structure (with nucleonic channels only) (Note: IRPC – Integrated Reactor Protection Channel, NFME – Neutron Flux Measurement Equipment)

Old movable detectors of start-up/intermediate power range were replaced with unmovable multi-range detectors. These detectors combine up to three neutron sensors with high/medium/low sensitivity, and could withstand high neutron and gamma flux rates. Each sensor of the detector has an output (pulse or current) which is connected to the corresponding signal conditioner: amplifier for pulse channels and current-to-pulse converter for current channel. Nucleonic signal conditioners may be separate devices that are arranged in reactor hall close to detectors as well as an integral part of IRPC. Then all signals in the pulse form are processed by a digital controller (NFME Controller) which automatically selects active range, calculates reactor neutron power and period, and compares them with safety system settings to produce channel's warning and emergency signals.

NFME Controller has individual serial data interfaces with each of three logic units (one in the same IRPC and to other IRPCs) and with the gateway of the same IRPC, each serial data line has electrical isolation. Warning and emergency signals as well as ready/fault (and other signals needed for reactor protection and control) of the nucleonic channel are sent to logic units. The same information together with all other channel data (reactor power, period, setpoints, active range, etc.) sent to the IRPC gateway to transfer to main console displays and database server and for local monitoring.

The logic unit of each IRPC receives data from NFME Controller of the same IRPC and from two other channels, compares it and, if it's found an emergency condition at least in two channels, produces common trip signal. Trip signals from three IRPCs are compared again with each other on external 2oo3 voting unit and finally activate safety action. All three IRPC logic units process the full set of binary signals needed for reactor protection and control: warning and emergency signals from every source (nucleonic, process parameters important for safety, SCRAM buttons, etc.), keys and buttons of reactor control system, control rod's limit switches and others. Each logic unit forms signals to drive reactor control rods, to switch on/off automatic regulator and other control signals taking into account all interlocks and reactor operation modes specific to given research reactor. Same logic units drive signaling indicators which duplicate displays in control room with most important safety system status information, and also drive sound alarms. All output signals (except channel operation status for signaling) from IRPC logic units go to external 2oo3 voting unit, resulting signals connected to corresponding drives.

Described system structure allows processing various numbers of independent redundant measurement channels of selected parameter. Voting logic of the reactor protection system could be easily adjusted for desired process instrumentation configuration (1oo1, 2oo3, 2oo4) individually for every process variable.

The gateway in IRPC is a part of monitoring system. It receives data from all IRPC modules via serial data interfaces with full information about measured parameters, system settings, actual states of every input signal, internal system variables values. Gateways of each IRPC are connected to the main monitoring system (main console) via redundant Ethernet interfaces. Ethernet switches distribute the information between three displays on main console, system archive server and other terminals. Gateway also provides monitoring service of the channel data in which it is installed; data could be seen on the local display. Complete information on all control channels and the status of the control and protection system is displayed on each of the three displays of the control console (Fig. 2). All information is presented on several slides; slides are switched on each display independently and can be adjusted depending on the current reactor operation mode or the preference of the operator.

Fig. 2 New main console in the control room of reactor WWR-SM

Industrial fan-free computers are used in monitoring system (gateways, display drives) with additional interface cards and usually preinstalled operation system from a PC vendor. There is relatively high probability of a common-cause failure of the computer based system. To prevent the total loss of information for operator about reactor condition in case of malfunction of main console displays it is recommended to use simple digital displays connected directly to safety instrumentation to indicate the most important reactor operation parameters. As example, each NFME Controller is connected directly to the corresponding stand-alone digital display (Fig. 1, display shown only for Ch 3) placed in control room to show reactor n-power and period measured by this nucleonic channel.

2.2 Integrated Reactor Protection Channel

All devices of Integrated Reactor Protection Channel are combined in one cabinet and wired inside the cabinet. IRPC structure is shown on Fig. 3.

IRPC consists of the following functional units:

- one nucleonic channel that operates in a wide range of neutron flux to monitor reactor in all operation modes from shutdown state and up to 120%FP;
- automatic power regulator unit (without motor drive);
- reactivity meter which internally connected with nucleonic channel of the same IRPC;
- up to 16 analog inputs with signal conditioners for technological parameters important for reactor safety;
- logic unit that has up to 200 binary inputs, up to 100 binary outputs, up to 32 serial data interfaces for data communication with other system devices (inside and out of the IRPC);
- power supply unit with number of AC/DC converters to power all channel's function blocks and also auxiliary devices connected to the IRPC;
- gateway that receives data from all function blocks of the IRPC and transmits this data to the main monitoring system on main console;
- display which is driven by gateway and allows monitoring all parameters of the IRPC and self-diagnostic information.

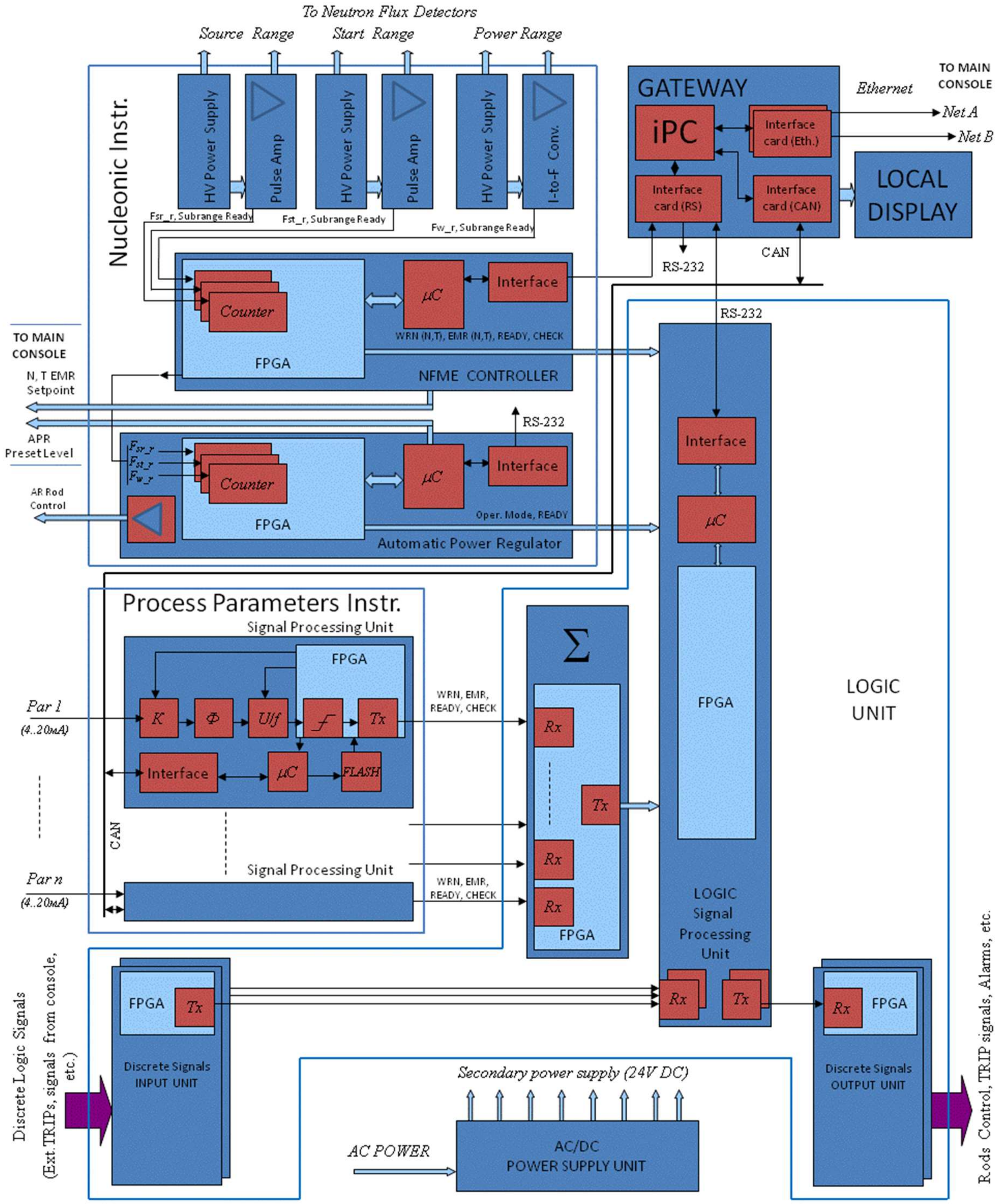


FIG. 3 Integrated Reactor Protection Channel structure
(with nucleonic signal conditioners as a part of the IRPC)

Nucleonic instrumentation unit of IRPC consists of the neutron flux detectors preamplifiers/converters, HV power supply modules, digital Neutron Flux Measurement Equipment Controller (NFME Controller), reactivity meter and automatic power regulator. Signals from every neutron detector are converted to the pulse signal form and go to NFME Controller inputs. NFME controller performs the conversion of the input signals to digital form, automatically selects the active range of operation, calculates the current reactor power and period, compares them with safety system setpoints and produces corresponding warning and emergency signals. NFME controller also retransmits (repeats) signals from neutron detectors in the pulse form to the output for transmission to the automatic power regulator and the reactivity meter. All digital inputs and outputs of NFME controller are galvanically isolated.

Field Programmable Grid Array (FPGA) and microcontroller are used in NFME controller to process signals. Digital circuits for converting pulse signals to digital code are implemented in FPGA, the rest of functions are performed by the microcontroller. The program for the microcontroller is written without using third-party libraries or functions, it neither uses operating system. The program source code is completely transparent for verification. Validation of the controller and FPGA is performed in several stages, starting with the program testing on the microcontroller emulator in the NFME controller and ending with NFME controller testing in IRPC.

Electronic components similar to those used in NFME controller are also used in other electronic modules of IRPC. In the logic unit all signal processing for both protection and control functions is performed on the FPGAs only, without microcontrollers. All modules in FPGA are implemented based on "hard logic" principle and do not contain processors. In some circuits microcontrollers act as a "bridge" with a monitoring system and provide diagnostics of the FPGA at the same time. Protection circuits are mainly implemented on programmable logic circuits, rather than on microcontrollers. All elements of the circuit connected directly to the protection system elements also belong to the protection system.

Functional units of IRPC are connected by serial interfaces with the logic unit and the gateway. Individual galvanically isolated interfaces are used to transfer data to displays and to transmit data inside protection and control schemes. All connections are organized in a point-to-point manner. Data transfer between IRPC devices is performed cyclically without requests from the data receiver. If communication fails with any unit, which is a source of data on parameters important for safety, the missing real data is assigned on receiver side with values that are seem to be the most safe state of the protection system - the absence of data for any parameter important for reactor safety is equivalent to the presence of an alarm level for this parameter.

While modernizing control and protection systems, new equipment, as a rule, should function exactly according to the same algorithms (especially protection system) as the equipment being replaced. Programmable logic, microcontrollers and computers make it possible to apply the same hardware solution to several projects with different specific requirements by redesigning only the firmware and software. However, changing the programs or configurations of FPGAs in safety systems leads to the need to re-conduct verification and validation procedures.

2.3 Advance reactor control features

High logic volume of field programmable gate arrays and high performance of microcontrollers and computers allow to implement the basic system functions and to add new features to the system: to expand or add new self-diagnostic function, significantly improve the human-machine interface and reduce the influence of "human factor", to lock a root cause of emergency reactor shutdown, to archive all signals. Below are listed several additional control functions implemented in reactor protection and control systems produced by SYSTEMATOM for research reactors of the WWR type.

The automatic reactor power regulator can operate on signals from any of the neutron flux monitoring channels available in the protection and control system; there is no need for a separate monitoring channel. There is a choice: to work on one selected channel or on the average from several selected channels. With a significant change in the distribution of the neutron flux during irradiation of materials, as well as loading/unloading of irradiated materials while the reactor is at full power, the possibility to select nucleonic channels as a signal source for the autoregulator gives an additional advantage for achieving reactor stable operation.

The autoregulator can not only stabilize the reactor power at a given level, but also automatically change the reactor from one power level to another, both in the direction of increasing power and its reduction. The change in power can be carried out both with the maintenance of a certain preset period, and with maintaining a constant (fixed) rate of change in the neutron (thermal) power. Autoregulator may support both operation modes and switch between them automatically depending on reactor power level. The regime with the maintenance of a constant rate of power change allows reducing the thermal load on reactor elements.

Automatic Rod (AR) position autocompensation feature is intended for reactivity compensation and moving AR back to the most effective position (usually corresponds to the midpoint of the AR movement range) by automatic movement of Compensation Rod (CR, one selected or consecutively selected rods). When the automatic power regulator is operating, the position of AR is monitored and, if it goes beyond the effective operating range (for example, from 20 to 80% of the full range of movement), the logic unit generates a signal for the corresponding movement of the selected CR. The movement of CR is carried out with small steps of reactivity, so as not to cause a significant decrease in the period. The autoregulator monitors the change in reactivity (by the power change) and gradually returns the AR to the middle position, compensating changes in reactivity caused by the movement of the CR. After the AR has reached a middle position, the process is completed.

Reactor shutdown is not less important than start-up of the reactor. The simplest and fastest way to shut it down is to press the SCRAM button. Each reactor trip and rods movement with emergency speeds is a burden on the rods itself. When the reactor shutdown is planned, there is no need for an immediate termination of the chain reaction, as it occurs when an emergency protection is activated. The manual shutdown process of the reactor can also be automated. By the command of the operator from the control console, the control system automatically moves all control rods according to the given algorithm with working speeds and brings them to the position corresponding to the reactor shutdown.

3. I&C SYSTEM COMMISSIONING

The equipment that has passed all Factory Acceptance Tests is delivered to the facility. In case of complexes of equipment are delivered, all equipment is finally tested being connected to each other by the regular connection scheme (as it will be connected at the facility). Installation and connection of the equipment at the facility are conducted in accordance with the recommendations and direct participation of SYSTEMATOM specialists. The quality of installation, compliance with all requirements for placement and connection of the devices of the complex largely determine the reliability of the entire system and the achievement of a high level of immunity to electromagnetic interference.

Site Acceptance Test is performed in two stages after all the devices have been installed. First, stand-alone tests of the control and protection system are performed without connection to sensors, drives/actuators and other related systems; at this stage, the correctness and completeness of the connection of all devices of the complex is confirmed. At the second stage, integration test is conducted with full connection to all related sensors, devices and systems. System instrumentation and interaction of all system units are checked during integration test.

Protection and control system with new equipment are tested sequentially as all reactor systems are ready to various reactor power levels. As a rule, tests of the new reactor control and protection system are completed after the reactor operation at 100% FP.

In parallel with stand-alone and integration tests, reactor operating and maintenance personnel are trained to work with new equipment. Involving reactor staff in installation, commissioning and testing processes from the very beginning of work allows service personnel and operators to better understand the purpose and functions of individual components of new system, memorize the names and locations of equipment, find the necessary information in the documentation, get used to the new interface of the system.

New technologies (components, tools, knowledge) are transferred to end-user together with new I&C systems, as well as new devices for periodic servicing and testing. New knowledge and technology can be used in the further operation of the facility.

3.1 Lessons learned

The most important lessons learned from several I&C modernization projects on RR are (vendor view):

- The technical specification for the new control and protection system should take into account all possible modes of reactor operation, including procedures that are performed once during reactor loading with fuel or that are necessary periodically to determine the parameters of the reactor itself, so that the new system is provided with appropriate modes of operation, necessary check points and additional inputs / outputs for extra signals.
- Modification of digital systems (mainly software) seems for customer to be a simple matter at first glance. It should be remembered that all changes, especially in safety systems, must be carefully documented, repeated tests of the modified device should be carried out in all modes of its operation. In this sense, the lack of source text of the programs for the end user seems to be an advantage.
- It is necessary to evaluate in advance the real operating conditions of I&C system: the characteristics of the premises in which the equipment will be installed (the availability of air conditioning / heating, the necessary space for access to equipment), the quality of the main power supply, etc. New I&C must be supplemented with system support features, like UPS, if necessary. Evaluation of the facility should be carried out for the readiness for receiving and placing new I&C system before it is shipped by the supplier to the site.
- I&C system modernization does not eliminate the lack of spare parts problem, but only pushes it off for a while. Such elements as displays have a relatively small resource and can be used for about 5 years with continuous operation. Device models (their sizes and interfaces) are completely changed during this time and it is difficult to find a suitable equivalent. Close interaction with the manufacturer of I&C system helps to solve refurbishment issues.

4. CONCLUSION

New I&C systems manufactured by SYSTEMATOM, including reactor control and protection systems that were installed on research reactors in place of obsolete equipment, have a positive operation experience. The renewal of safety systems allows to ensure stable and safe operation of the reactor, to focus on the scientific and practical work that requires reactor operation.

SYSTEMATOM has developed reliable and resilient reactor control and protection systems, because system architecture is based on the company's experience in safety system’s design and practical operation data, up-to-date requirements for safety systems, reliability and fault-tolerance. Modern digital technologies make it possible to apply the same hardware solution to several projects with their specific requirements by redesigning only firmware and software. This allows to reduce significantly the time for I&C system development and manufacture and, in turn, reduce the overall implementation time of reactor I&C systems modernization project.

BIBLIOGRAPHY

1. Safety of Research Reactors, IAEA Safety Standards Series No. SSR-3, IAEA, Vienna, 2016.

2. Instrumentation and Control Systems and Software Important to Safety for Research Reactors, Specific Safety Guide No. SSG-37, IAEA, Vienna, 2015.

DESIGN ASPECTS AND SAFETY ASSESSMENT OF I&C SYSTEMS OF NUCLEAR SUBCRITICAL FACILITY

Oleksandr Klevtsov, Serhii Trubchaninov

State Scientific and Technical Center for Nuclear and Radiation Safety (SSTC NRS)

Ukraine

The paper is devoted to consideration of overall I&C of nuclear subcritical facility, which was constructed in Ukraine. Short overview of nuclear subcritical facility is made. Structure, design aspects and main functions of I&C systems of nuclear subcritical facility are considered. Regulations and standards that were used during the licensing process for I&C systems are presented. The main results of safety assessment of I&C systems of nuclear subcritical facility are given in the paper.

1. CONSTRUCTION OF THE NUCLEAR SUBCRITICAL FACILITY

National Science Center Kharkiv Institute of Physics and Technology (NSC KIPT) (Ukraine) with the financial and technical support of Argonne National Laboratory (USA) started the construction of new research facility which is called Nuclear subcritical facility «Neutron source based on subcritical assembly driven by the accelerator of electrons» (NSF «Neutron Source») in 2011. NSF «Neutron Source» is intended for research of subcritical systems, gaining the neutrons and using them for application and fundamental research. Also NSF «Neutron Source» will be used for producing of the medical isotope Technetium-99.

The NSF «Neutron Source» was design by Kharkiv designing-development institute «TEPLOELEKTROPROEKT-SOYUZ» (Ukraine) [1].

The construction of NSF «Neutron Source» was finished in the beginning of 2019. The physical start of NSF «Neutron Source» is planned after the finishing of licensing procedures in the second half of 2019.

NSF «Neutron Source» is the new type of nuclear facility. The special feature of NSF «Neutron Source» is the use of accelerator of electrons for generating the neutrons because of photonuclear reactions in tungsten or uranium target (plate) caused by inhibition of electrons in the target (as a result of the scanning target by the beam of electrons). These initial neutrons stimulates the fission of Uranium-235 in the nuclear material of subcritical assembly. NSF «Neutron Source» is classified as Accelerator Driven Systems (ADS) according to the IAEA classification.

The geometry and mass of fissile material are chosen so that effective rate of neutron multiplication is always less than 1. This is a fundamental difference from the research and power reactors that operates in the mode of self-sustaining chain reaction.

The main parts of NSF «Neutron Source» are as follows:

- subcritical assembly with the biological protection;
- neutron-generating target for producing of initial neutrons;
- linear accelerator of electrons (LAE) with the vacuum transportation channel;

– experimental neutron channels;
– spent fuel storage pool;
– cooling circuits and technological systems;
– electrical equipment including diesel-generator;
– overall I&C and control room.

The general scheme of NSF «Neutron Source» is presented in Figure 1.

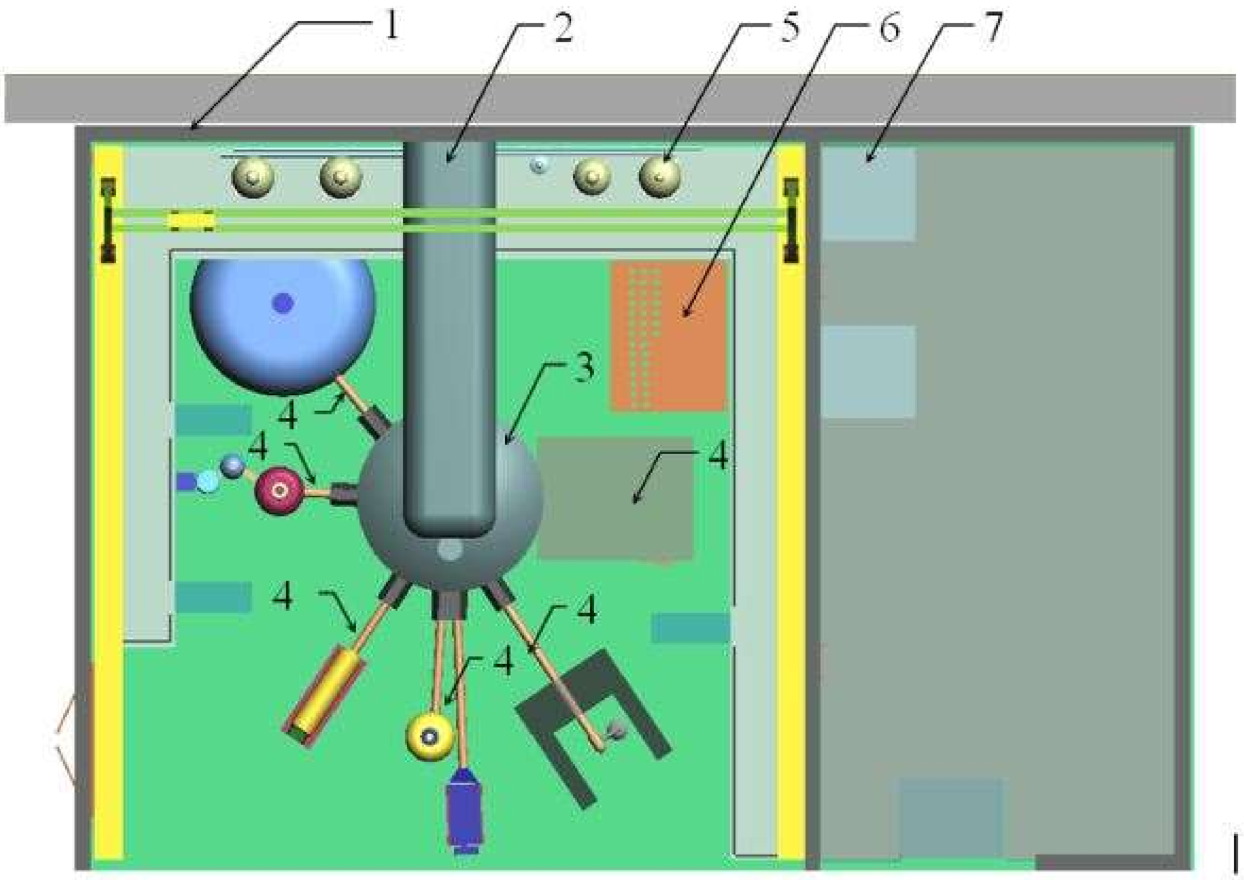


Fig.1: General scheme of NSF «Neutron Source» (1 – building, 2 – linear accelerator of electrons with the vacuum transportation channel, 3 – subcritical assembly, 4 - experimental neutron channels, 5 – cooling system, 6 – spent fuel storage pool, 7 - glove-box area)

NSF «Neutron Source» has separate cooling circuits for core, neutron-generating target and LAE.

The use of LAE instead of control rods for power control is the peculiarity of NSF «Neutron Source». LAE has been delivered by Institute of High Energy Physics (IHEP), Chinese Academy of Sciences.

2. I&C SYSTEMS OF THE NUCLEAR SUBCRITICAL FACILITY

The overall I&C of NSF «Neutron Source» is called «Automated monitoring and control system» (AMCS). AMCS was designed and produced according to the main requirement specification [2] (and a few separate requirement specifications for some individual systems). It is a spread human-machine automated system that uses for monitoring and control of all technological processes and for safe operation of NSF «Neutron Source» in all operation modes. AMCS was designed and produced by the group of manufacturers from Ukraine, China and Russia.

AMCS includes 14 individual digital I&C systems:

- protection and interlock system (PIS), produced by «Khartron-Arkos», Ukraine;
- control system of 1-st cooling circuits equipment (CS CCE-I), produced by «Khartron-Arkos», Ukraine;
- control system of 2-nd cooling circuits equipment (CS CCE-II), produced by «Khartron-Arkos», Ukraine;
- monitoring system of cooling pond technological parameters (MSCPTP), produced by «Khartron-Arkos», Ukraine;
- information and calculating system (ICS), produced by «Khartron-Arkos», Ukraine;
- technological alarm and visualization system (TAVS), produced by «Khartron-Arkos», Ukraine;
- control panel (CP), produced by «Khartron-Arkos», Ukraine;
- neutron flux monitoring system (NFMS), produced by «Khartron», Ukraine;
- control system of electrical mechanisms of biological protection (CSEMBP), produced by KEP, Ukraine;
- control system of linear accelerator of electrons (CS LAE), produced by IHEP, China;
- automated radiation monitoring system (ARMS), produced by «Sosny», Russia;
- automated monitoring and control system of building engineering systems (AMCS ES), produced by «Sosny», Russia;
- system of accident alarm about self-sustained chain reaction in cooling pond (SAA SCR), produced by «Sosny», Russia;
- refueling machine control system (RMCS), produced by «Diakont», Russia.

The main task of AMCS is the ensuring of normal operation of NSF «Neutron Source» equipment, safety parameters monitoring for detection of deviations from normal operation and realization of automatic protections and interlocks for prevention of the development of deviations from normal operation into accidents.

Hierarchically the AMCS is a spread multilevel system and it includes:

- low level – sensors for measuring of technological parameters and actuators for the control of technological equipment;
- middle level – hardware and software for receiving and handling of measuring signals and forming and output of commands to actuators for protection, interlocks and control;
- high level – control room.

Control room ensures the choice of operation modes, monitoring of technological parameters and state of facility, automated control for technological equipment, alarm, presentation and saving the information about technological processes, state of technological systems and actions of operators and shutdown of NSF «Neutron Source». Control room includes:

- control panel for shift supervisor;
- two control panels (main end reserve) for NSF «Neutron Source» operators;
- control panel with four main and four auxiliary monitors for CS LAE operators;
- control panel for RMCS operator;
- control panel of AMCS ES;
- information monitor of NFMS;
- information monitor of ARMS;
- TAVS (five information monitors for the presentation of alarm signals, safety parameters, events journal, diagrams of main technological parameters and state of technological systems).

The structure of AMCS is shown in Figure 2.

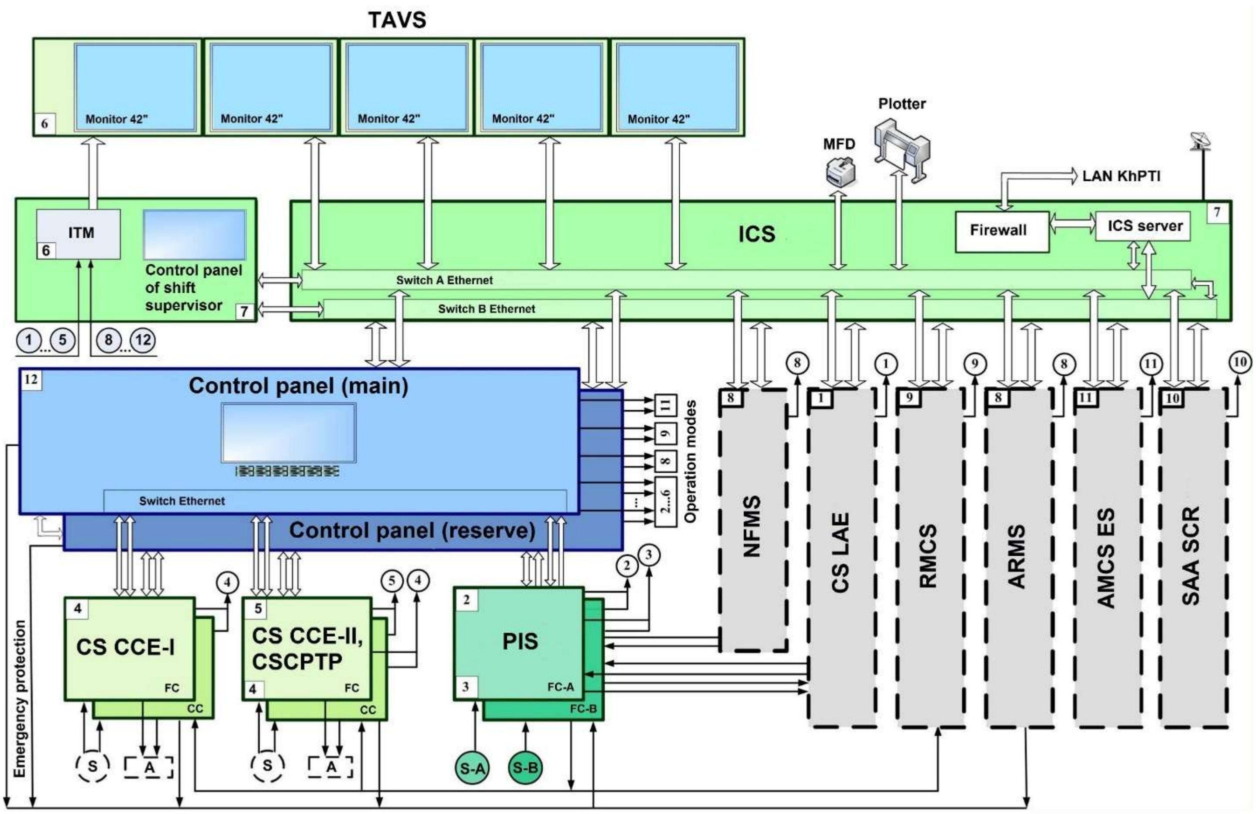


Fig. 2: Structure of AMCS of NSF «Neutron Source»

All I&C systems of NSF «Neutron Source» are classified according to Ukrainian regulation NP 306.2.183-2012 [3].

PIS, CS LAE, NFMS and RMCS has safety class 2 as safety systems or systems, which failures can lead to design basis accidents.

The other systems has safety class 3 as normal operation systems important for safety (not included to safety class 2) or radiation protection systems.

Let us consider two most important safety systems (PIS and CS LAE) in more details.

PIS realizes all main protections and interlocks for NSF «Neutron Source». Particularly, it performs the following functions:

– monitoring of the technological parameters of cooling circuits through the own measuring channels;
– determining of unacceptable deviations of technological parameters and forming the protection, interlock and alarm signals;
– receiving the protection and interlock signals from other I&C systems and from seismic sensors;
– forming and output of permitting signal for switching on the LAE under the condition of normal operation of all technological and I&C systems of NSF «Neutron Source» (LAE can be switched on only if it receives the permitting signals from two channels of PIS at the same time and LAE switches off if permitting signal absent in one or two channels of PIS in case of any deviations from normal operation);
– blocking of simultaneous operation of different systems (e.g. LAE and RMCS, LAE and CSEMBP, etc.);
– output of current information and alarm signals to TAVS and control panels for alerting the staff;
– diagnosis of state of its own hardware and software.

In fact, PIS is the analogue of reactor trip system of power reactors but it withdraw the permitting signal for immediate switching off the LAE instead of output the command for inserting control rods into the core.

Another difference between PIS and reactor trip system of power reactors is the use only two channels. Reactor trip system of power reactors has three channels, which use the logic «2-of-3» for forming the output signals. It is necessary to avoid the false positive that can lead to essential financial loss. For research reactors it is not so important. Thus, it is enough to use only two channels that allows to shutdown of the NSF «Neutron Source» in case of absence of permitting signal even in one channel of PIS.

CS LAE is the most complicated I&C system of ACMS (see Figure 3).

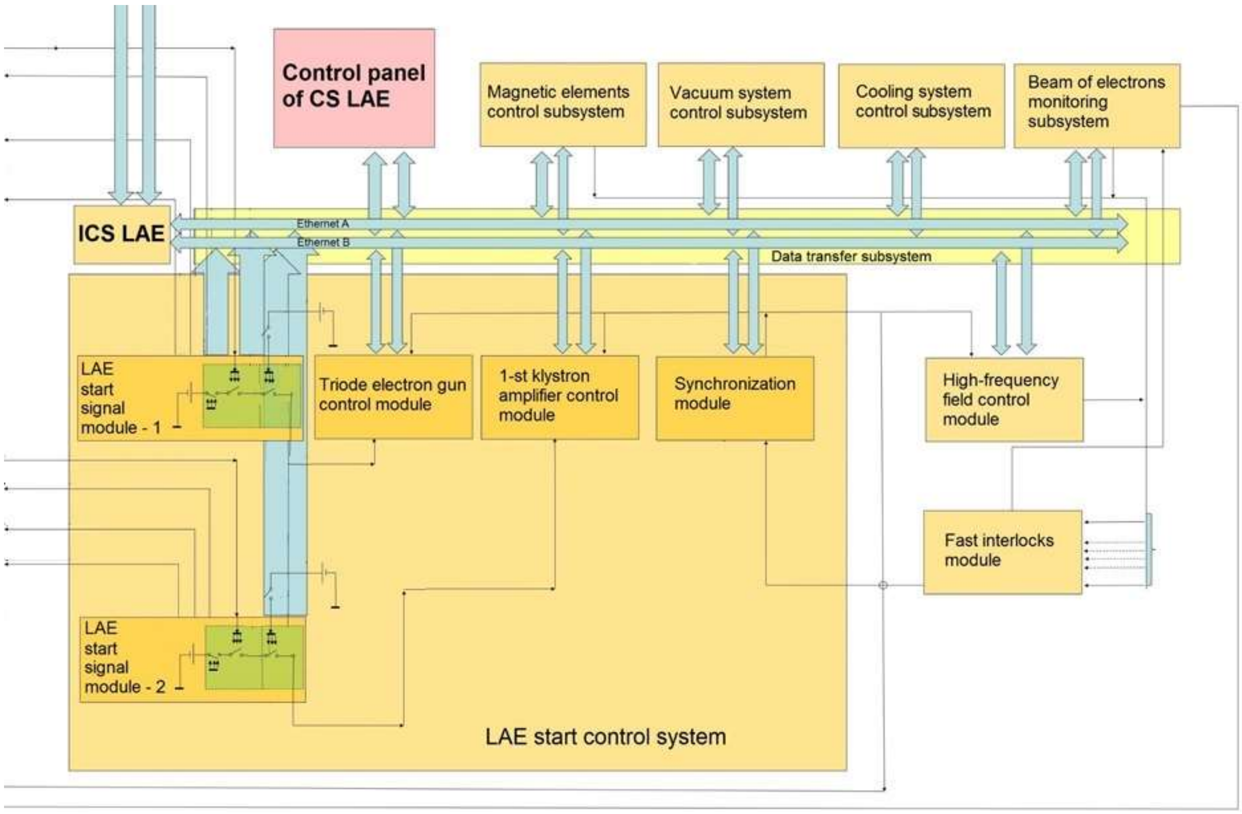


Fig. 3: Structure of CS LAE of NSF «Neutron Source»

The most important part of CS LAE is the LAE start control system that performs the function of switching off the LAE (i.e. shutdown of the NSF «Neutron Source»). LAE start control system is built as a reserved and diverse system. The LAE switching off is realized in one of two possible ways. The system locks the triode electron gun in case of absence of permitting signal in the first channel of PIS. And the system turns off the first klystron amplifier in case of absence of permitting signal in the second channel of PIS. Also the system turns off the synchronization module in case of any internal interlocks in CS LAE. Each of these three actions leads to impossibility of forming of electron beam on the output of LAE. Thus, NSF «Neutron Source» immediately returns to subcritical mode in the conditions of absence of external source of electrons for generating of initial neutrons.

The internal interlocks prevent possible failures of LAE. The most dangerous of such failures are as follows:

- the wrong direction of beam of electrons (when the beam is not directed to target and can damage biological protection or technological equipment in the core);
- the failure of scanner of beam of electrons (when beam directed to one point on the target that can lead to overheating and destroying the target).

3. REGULATORY FRAMEWORK

Construction of NSF «Neutron Source» as well as development and implementation of ACMS are licensed by the State Nuclear Regulatory Inspectorate of Ukraine (SNRIU) according to Law of Ukraine № 1370-XIV «About authorization activity in nuclear energy use» [4].

SSTC NRS (technical support organization of SNRIU) has participated in the licensing of NSF «Neutron Source» and particularly has performed the safety assessment of all 14 I&C systems included in AMCS during last 8 years.

There was no special regulations in Ukraine with the requirements to nuclear subcritical facilities in 2011.

For solving this problem, SNRIU and SSTC NRS developed the new regulation NP 306.2.183-2012 [3] in 2012. It contains the general requirements to nuclear subcritical facilities, but also it includes several groups of the requirements to I&C systems:

- safety control systems (including reactor trip system);
- normal operation systems;
- automated radiation monitoring system;
- control room.

Requirements to safety control systems also contains the group of requirements to reactor trip system (PIS fulfils these functions in ACMS).

According to NP 306.2.183-2012 [3] NSF «Neutron Source» should be equipped by the following normal operation systems:

- neutron flux monitoring system (ACMS contains NFMS with the extended functions of reactivity monitoring);
- control system of accelerator of charged particles (CS LAE perform these functions in ACMS);
- control system of cooling circuit equipment (ACMS contains CS CCE-I and CS CCE-II);
- information and calculating system (ACMS contains ICS);
- control system for transport-technological operations (RMCS perform these functions in ACMS).

Also ACMS includes ARMS and control room according to requirements of NP 306.2.183-2012 [3].

It should be noted that NP 306.2.183-2012 [3] contains only the general requirements to safety assurance of NSF I&C. There are no other regulations or standards with the detailed technical requirements to NSF I&C in Ukraine. Therefore, for development, testing, implementation and safety assessment of ACMS were used guides, rules and standards, which contain the requirements to nuclear power plants (NPP) I&C. The regulation NP 306.5.02/3.035-2000 [5] was used at first stage (until 2015). This regulation contained detailed technical requirements to I&C, particularly, requirements to:

- functions;
- redundancy, independence, diversity, single failure principle and protection against common-cause failures;
- accuracy, response rate;
- prevention of personnel errors, protection from unauthorized access, human-machine interface;
- reliability;

- technical diagnosis;
- resistance against environmental influences, mechanical and seismic influences, changes of power supply parameters, electromagnetic interferences;
- fire protection;
- software;
- quality assurance;
- testing.

New regulation NP 306.2.202-2015 [6] and standard SOU NAEK 100:2016 [7] came into force in 2015 and 2016 instead of NP 306.5.02/3.035-2000 [5]. They were used for further activity concerning development, testing, implementation and safety assessment of ACMS after 2015. These documents updated and tightened most of the requirements of NP 306.5.02/3.035-2000 [5], especially requirements to resistance against seismic influences and electromagnetic interferences, to software, to reliability and to testing. Some new requirements were added to NP 306.2.202-2015 [6] and SOU NAEK 100:2016 [7] such us requirements to emission of electromagnetic interferences, to protection from intrusion into software, to dataware, to development of hardware, software and I&C systems, to equipment qualification, to maintenance, repair and modernization, to configuration management, etc.

The requirements of above mentioned regulations [5], [6] and standard [7] concern the NPP I&C but they were adopted to peculiarities of NSF «Neutron Source» (e.g. redundancy by using of two channels in safety systems of NSF «Neutron Source» instead of three channels in safety systems of NPP that is sufficient for such facility).

GND 306.7.02/2.041-2000 [8] was used for safety assessment of ACMS. It contains the requirements to documents substantiated safety of I&C systems (requirement specification, design documentation, verification plan and report, programs of factory acceptance tests and site acceptance tests, safety analysis report (SAR), reliability analysis report, quality assurance program, etc.).

SAFETY ASSESSMENT OF I&C SYSTEMS OF THE NUCLEAR SUBCRITICAL FACILITY

Licensing process covered all life-cycle stages of each individual I&C system from the design to site acceptance tests. It was complex project because the object of expert review was not individual I&C system, but overall I&C from 14 different systems produced by six different manufacturers.

SSTC NRS fulfilled the safety assessment of large amount of documents, which substantiate safety of each I&C.

First group included the documents, which substantiate safety of NSF «Neutron Source» as whole but also contain the chapters concerning I&C systems. For example, one of such documents was preliminary SAR [9]. It contained general information about structure, functions of ACMS and its components, which should be reviewed. More detailed information about I&C systems was given in separate SAR for different I&C systems.

Second group included the documents, which directly substantiate safety of I&C systems. These documents cover the following stages of I&C life cycle:

- development of requirement to I&C system (requirement specification);

- technical project (design documentation, quality assurance program);
- development of software (software verification plan and report);
- manufacturing of I&C components and factory acceptance tests (FAT) (program of FAT);
- mounting of I&C (preliminary SAR, reliability analysis report);
- site acceptance tests (SAT) (program and methods of SAT);
- commissioning (final SAR).

The volume of expert review of documents substantiated safety of individual I&C systems which are the parts of AMCS of NSF «Neutron Source» is presented in Table 1.

TABLE 1. EXPERT REVIEW OF DOCUMENTS SUBSTANTIATED SAFETY OF I&C SYSTEMS OF NSF «NEUTRON SOURCE»

I&C system	**Documents**							
	Requirements specification	**Design documentatio**	**Program of FAT**	**Software verification plan and**	**Preliminary SAR**	**Reliability assessment report**	**Program of SAT**	**Final SAR**
PIS	+	+	+	+	+	+	+	–
CS CCE-I	+	+	+	+	+	+	+	–
CS CCE-II	+	+	+	+	+	+	+	–
MSCPTP	+	+	+	+	+	+	+	–
ICS	+	+	+	+	+	+	+	–
TAVS	+	+	+	+	+	+	+	–
Control panel	+	+	+	+	+	+	+	–
ARMS	+	+	+	+	+	+	+	–
AMCS ES	+	+	+	+	+	+	+	–
SAA SCR	+	+	+	*	+	+	+	–
NFMS	+	+	+	+	+	+	+	–
RMCS	+	+	+	+	+	+	+	–
CS LAE	+	+	+	+	+	+	+	–
CSEMBP	+	+	+	+	+	+	+	–
* – Verification is not needed because of absence of software important for safety								

Table 1 shows that safety assessment was fulfilled for all life-cycle stages of all I&C systems of NSF «Neutron Source» except the stage of commissioning. The final SAR should be reviewed after the experimental operation of AMCS.

The experimental operation is the very important stage for approbation of I&C systems operation in the real conditions with the nuclear fuel in the core. All stages of previous testing were fulfilled without the fuel. For example, experimental operation is necessary for calibration of nuclear flux monitoring system because the facility is absolutely new and there no information about the real neutron flux for different power levels of accelerator. Thus, such calibration can be done only during the experimental operation with the different amount of fuel assemblies and different power levels of accelerator.

It should be noted that special attention was paid to expert review of CS LAE (it took more than 6 years) as a very important safety systems which should switch off the LAE in case of any deviations from normal operation. The importance of CS LAE is confirmed by the accident at research facility in Japan in 2013 [10]. The reason of accident was the failure of accelerator which generated the proton beam during a very short period of time (5 ms instead of design value 2 s). This leads to overheating and damage of target. Accelerator was switched off by the protection system but it was switched on again because of operators' mistake.

4. CONCLUSIONS

NSF «Neutron Source» is a new nuclear research facility constructed in Ukraine.

Overall I&C of NSF «Neutron Source» contains 14 different I&C systems, including safety systems, normal operation systems, automated system of radiation monitoring and control room which ensure the monitoring and control of all technological processes at facility.

Licensing process for I&C systems of NSF «Neutron Source» based on Ukrainian regulatory framework that includes the general requirements to nuclear subcritical facility and detailed technical requirements to NPP I&C adopted to the peculiarities of NSF «Neutron Source».

Safety assessment covered all life-cycle stages of I&C systems of NSF «Neutron Source» except the review of final safety analysis report, which will be reviewed after the experimental operation of AMCS.

References

1. Nuclear subcritical facility «Neutron source based on subcritical assembly driven by the accelerator of electrons». Design documentation – Kharkiv: «Kharkiv designing-development institute «TEPLOELEKTROPROEKT-SOYUZ», 2012. – 2122 p.
2. Nuclear subcritical facility «Neutron source based on subcritical assembly driven by the accelerator of electrons». Automated monitoring and control system. Requirements specification. – Kharkiv: National Science Center Kharkiv Institute of Physics and Technology, 2012. – 117 p.
3. NP 306.2.183-2012 General safety provisions of nuclear subcritical facilities. Kyiv: State nuclear regulatory administration of Ukraine, 2012. – 67 p.
4. Law of Ukraine № 1370-XIV «About authorization activity in nuclear energy use» – Kyiv: Journal of Parliament of Ukraine, 2000. – №9. – P. 68.

5. NP 306.5.02/3.035-2000 Requirements to nuclear and radiation safety of instrumentation and control systems important for safety of nuclear power plants. – Kyiv: State nuclear regulatory administration of Ukraine, 2000. – 86 p.
6. NP 306.2.202-2015 Requirements to nuclear and radiation safety of instrumentation and control systems important for safety of nuclear power plants. – Kyiv: Official journal of Ukraine. – 2015. – P. 99-151.
7. SOU NAEK 100:2016 Instrumentation and control systems important for safety of nuclear power plants. General technical requirements. – Kyiv: National Nuclear Energy Generating Company "Energoatom", 2016. – 153 p.
8. GND 306.7.02/2.041-2000. Assessment methods of compliance of instrumentation and control systems important for NPP safety with requirements to nuclear and radiation safety – Kyiv: Ministry of ecology and natural resources of Ukraine, 2000. – 48 p.
9. Nuclear subcritical facility «Neutron source based on subcritical assembly driven by the accelerator of electrons». Preliminary safety analysis report. – Kharkiv: National Science Center Kharkiv Institute of Physics and Technology, 2012. – 752 p.
10. Accelerator Facility Accident Report. Incorporated Administrative Agency — Japan Atomic Energy Agency Inter University Research Institute — High Energy Accelerator Research Organization, 31 May 2013.

IMPLEMENTATION OF DIGITAL UPGRADES TO THE UNIVERSITY OF FLORIDA TRAINING REACTOR (UFTR) PROTECTION AND CONTROL SYSTEMS

G. BICKFORD, J. LEWIS, K. A. JORDAN
Department of Materials Science and Engineering
University of Florida, Gainesville, FL 32611
United States of America

Abstract

The University of Florida Training Reactor (UFTR), commissioned in 1959 is upgrading its current analog control and protection systems, last refurbished in 1970, to encompass digital protection and control systems. This will be a first of its kind fully digital safety-and-control system that will become an operational testing and training platform for these technologies, helping shepherd the use of these systems for future commercial nuclear power plants. This paper gives some history of this project and the current status of these efforts.

Key Words: Training Reactors, Digital Control, UFTR

1. INTRODUCTION

The University of Florida Training Reactor (UFTR) is an ARGONAUT (Argonne Nuclear Assembly for University Training) type reactor that first went critical in Dec. 1959, two years after the class prototype was built at Argonne National Laboratories. It was licensed for an initial power of a 10 KW under license number R-56, which was modified in 1964 to allow a maximum power of 100 kW. The UFTR originally operated with Low Enriched Uranium (LEU) and converted to Highly Enriched Uranium (HEU) in 1970 [1]. It was re-converted from HEU back to LEU in 2006 [2].

The basic design of the UFTR is shown in Fig. 1. It has a "two-slab geometry" consisting of 24 assemblies in 6 water-filled aluminum boxes, which are surrounded by a graphite moderator. There are 4 electrically driven control blades – three safety blades and one regulating blade – which are used for reactivity control. The fuel meat is U_3Si_2-Al enriched to 19.75% (nominal) with 6061-Al Cladding. The reactor is water cooled with an unpressurized primary loop. The UFTR has several beam ports and experimental access points, shown in Figure 2. As with most reactors, the UFTR has negative temperature and void coefficients. The excess reactivity is limited to 1.4% $\Delta k/k$.

2. INSTRUMENTATION AND CONTROL SYSTEM

The current Instrumentation and Control (I&C) System is entirely analog. In July of 2008 UF, AREVA, and Siemens agreed to a project to upgrade the reactor to full digital control. This upgrade is intended to include both the Reactor Protection System (RPS) and the Reactor Control System (RCS). The agreement made provisions for a division of responsibilities that roughly went as follows: the university staff with the aid of AREVA would design a fully digital Reactor Protection System consisting of a Teleperm XS (TXS) Safety control system. AREVA would then perform the construction of and training of University personnel on the TXS system. Siemens would design, supply and train the University personnel on a T3000 Control platform for plant management.

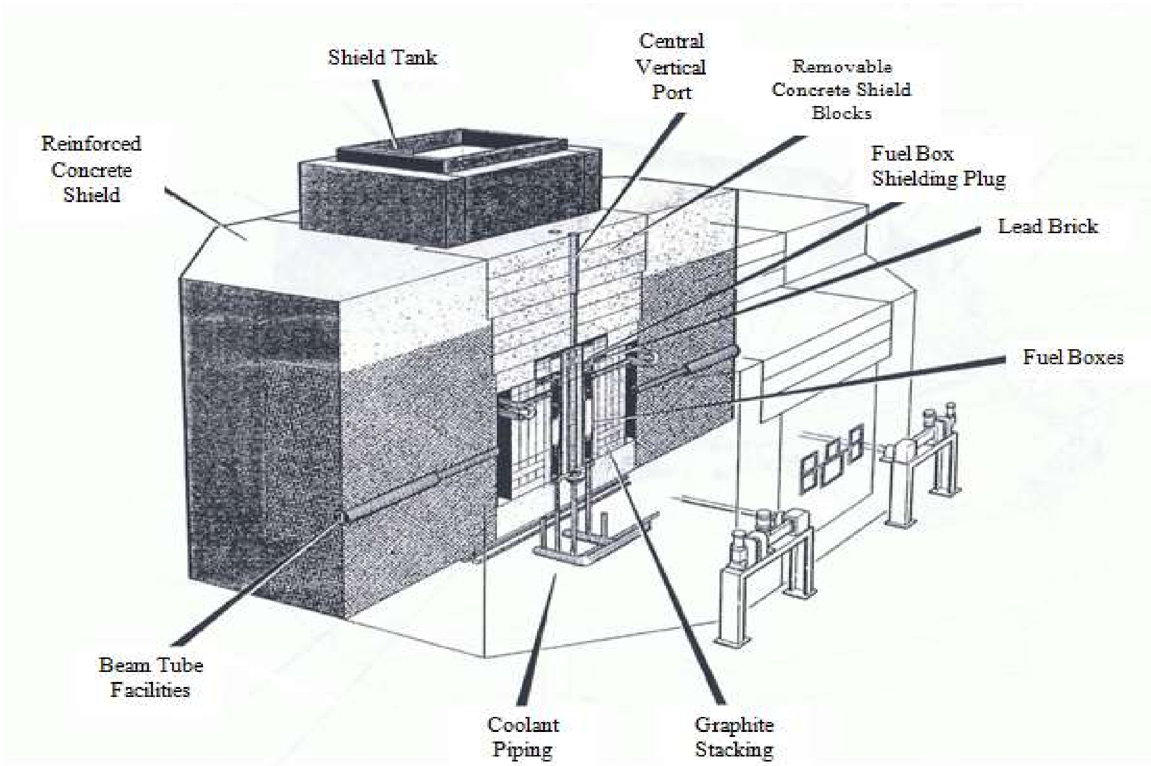


FIG. 1. An east-west cutaway of the basic design of the UFTR.

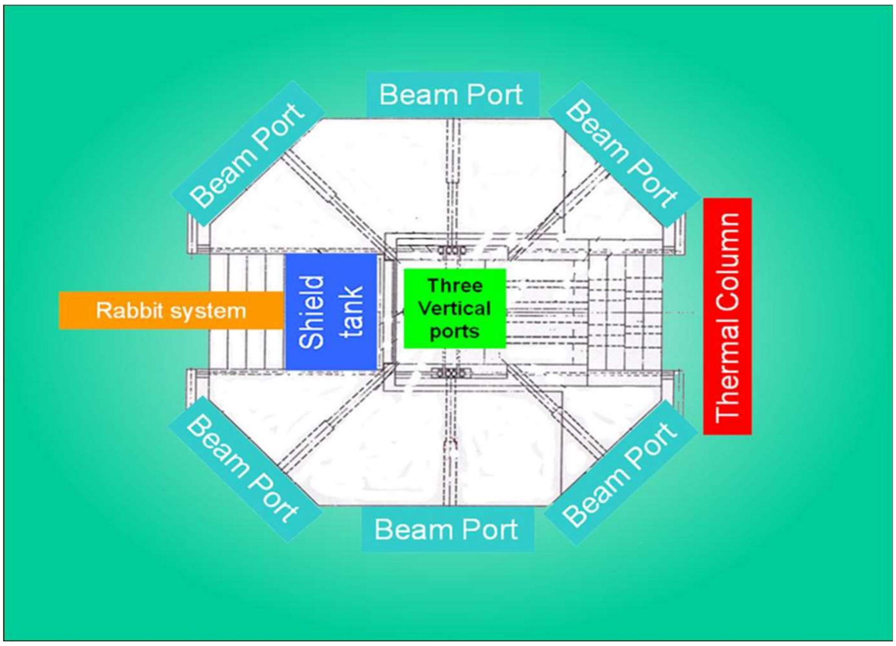


FIG. 2. A cutaway view shows the experimental ports.

3. MOTIVATION FOR THE CONVERSION

The UFTR control system is over 40 years old. It is increasingly difficult to find replacement parts that meet the technical specifications.

After conversion, the UFTR will be the first fully digitally controlled reactor in the United States. The University will be on the ground floor of training a new work force in new and relevant technology, helping shepherd the trend in electrical design toward digital as new plants adopt digital controls. Partnerships with local community colleges to provide extension courses are possible, and education for students in the nuclear engineering program will be enhanced.

In addition to the training opportunities available, the benefits of a digital protection and control system include reduced cost of maintenance and reduced maintenance time. Reduced cost of maintenance is reflected in a time and part replacement savings. Troubleshooting becomes more of a card replacement exercise. Parts are less expensive and operational down time is shortened. The circuit cards in the digital system have a self-check feature that gives an indication of problems with the card and give feedback to the processor for historical records and display to the operator. Maintenance time is reduced because many of the checks that are currently done manually can be done electronically and remotely. The current UFTR Standard Operating Procedures require Daily, Weekly, Quarterly and Annual checks that if done in their current state with the analog metering and control, will require anywhere from 20 minutes to an hour to accomplish. With a digital control system, any portion of the checks that currently require physically reading a meter in the reactor cell will be able to be moved to a digital readout and a digitized check that can be programmed. If desired, a wide variety of the SOP checklists can be done in real time during operation.

Modification of system control points through software controls is possible rather than through redesign and replacement of analog components. This makes Verification and Validation (V&V) a much simpler process not only for initial installation, but also for any future design changes. This benefits installation on a research reactor, as it allows for easier design modifications on a non-power system that is designed for experimentation.

4. DESCRIPTION OF THE REACTOR PROTECTION SYSTEM

The RPS trips the reactor under given conditions. The RPS monitors reactor parameters and initiates a trip when an unsafe condition is met. Trips can be initiated either manually or automatically.

The UFTR has 2 types of Reactor Trips: Blade Drop and Full. A Blade Drop trip electrically disengages the clutch, and the blades drop due to gravity. This is initiated in response to a process input. Since the control blade clutches are electrically driven, they disengage and drop on a loss of power. A Full trip is a Nuclear Instrumentation (NI) induced trip, which involves the gravity drop of the 4 control blades and the dumping of the primary coolant water into a storage tank. Table 1 provides a description of the parameters monitored and the range of values that would initiate a trip.

The digital upgrade has a redundant design that will allow multiple pathways to initiating a reactor trip. The Nuclear Instrumentation (NI) and environmental sensors give simultaneous inputs to both the RPS and the Control system. The digital system does the Analog to Digital (A/D) conversion of the input signals from the sensors and processes those inputs. When trip conditions are met, the system sends a signal to the Reactor Trip System (RTS) and initiates an appropriate trip of the system. The control monitors the input signals, displays both raw and derived operating conditions to the operator and allows the operator to control the plant and if necessary activate the Manual Reactor Scram (MRS). A block diagram of the flow of information is given in Fig 3.

TABLE 1. A LIST OF MONITORED OPERATING PARAMETERS AND THEIR ASSOCIATED TRIPS

Automatic	
Period ≤ 3 sec	Full
Power ≥ 119% of full power	Full
Loss of NI high voltage ≥ 10% Loss of electrical power to control console	Full Full
Primary cooling system: — Loss of primary pump power — Low water level in core (≤ 42.5") — No outlet flow — Low inlet water flow (≤ 41 gpm)	Blade-drop
Secondary cooling system (≥ 1 kW): — Loss of flow (well water ≤ 60 gpm) — Loss of secondary well pump power	Blade-drop
High primary coolant inlet temperature (≥ 99°F)	Blade-drop
High primary coolant outlet temperature (≥ 155°F)	Blade-drop
Shield tank low water level (6" below established normal level)	Blade-drop
Ventilation system: — Loss of power to stack dilution fan — Loss of power to core vent fan	Blade-drop
Manual	
Manual scram bar	Blade-drop
Console key-switch OFF	Full

The safety system is a three-part system for reactor protection consisting of:

— Standardized hardware: allows ease of manufacture and ordering of parts;

— Qualified system software: qualified to safety standards for power reactors;

— Specification and coding environment: allows initial writing and future modification of system software to standards and with consistency that are suitable for individualized systems.

The safety system also interfaces with any additional external systems, such as the control and Reactor Trip System in the UFTR's case.

At startup of the control system, the Service Unit (SU) error checks the code. The SU is a computer that uploads software to the control system and keeps track of the software used.

Cyber security is a concern that the UFTR handles by the use of an "air gap" method as its primary tool. All system computers are isolated from the Internet and all installation programs are distributed under a process control that will minimize the number of personnel having access to them.

The flow of information from the safety system to the control system is unidirectional through a Gateway. This is a computer that directs the flow of information via a high speed messaging system to the appropriate displays, processors and historical recorders of the control system. The one-way nature of the information flow to the Gateway ensures that any operational inputs made on control will not affect the RPS. The protection system collects the incoming digital signals and runs them through an analog to digital converter and then processes the digital signal in the Acquisition and Processing (AQP) portion of the safety system. If trip conditions are met, it sends a signal to the Reactor Trip System (RTS) and shuts down the reactor. The Monitoring and Service Interface (MSI) then sends the digital signals to the control system which then processes and displays the operating conditions for the operator. (The control unit also gets signals from other sensors that are not safety related and would not provide input to scram the system. Annunciator lights on, doors open and closed, etc.) The logical flow of information is shown in Figure 4.

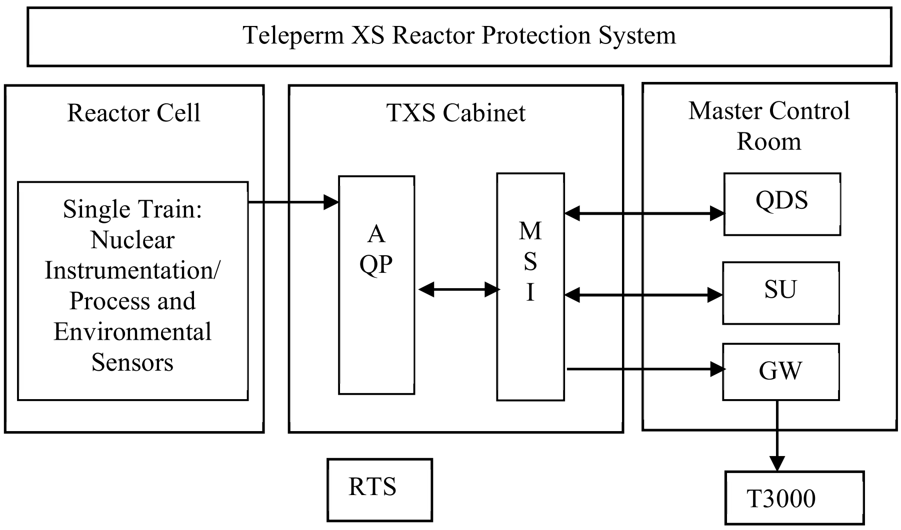


FIG. 4. The logic flow of information between the sensors, TXS and T3000 system.

The UFTR has a single train of inputs to the RPS. This has been determined to be an acceptable level of safety due to the aforementioned inherent design safety features [5]. There is one train of signal inputs that goes to the TXS. It goes to the Acquisition and Processing (AQP) side of the TXS and then proceeds to the Monitoring and Service Interface, (MSI). From there it goes to the Qualified Display System, the Service Unit and the Gateway to the T3000. The signals sent to the TXS system fall into 7 main groups as listed in Table 2:

TABLE 2. DEVICES SENDING SIGNALS WITHIN THE SINGLE TRAIN

Monitored Parameter	Monitoring Device	Monitored Region
Whole power range	Fission chamber (FC), Ion Chamber (IC)	Core
Whole power range, Reactor period	Boron Tri-fluoride detector (BF3), IC	Core
Temperature	Resistive Temperature Detector (RTD)	Core, primary & secondary loops
Flow rate	Flow Rate Monitor (FRM)	Primary & secondary loops
Water level	Water Level Monitor (WLM)	Core, Storage tank, shield tank
Area radiation level	Area Radiation Monitor (ARM)	East, North, South & West
Monitored Parameter	Monitoring Device	Monitored Region
Fan air flow	Fan Monitor (FM)	Core ventilation, stack dilution

5. PROJECT DEVELOPMENT

Any proposed project that affects a nuclear power plant (power or non-power) must be compared to the Safety Analysis Report (SAR) to determine if it will affect the safe operation of the plant. This analysis must then take into consideration the Technical Specifications (Tech Specs) that are a part of the SAR. Then an analysis of the Design Basis for the project must be considered and a determination made regarding how the Functional Requirements Specifications (FRS) need to be written. The FRS drives the specifics of the project's hardware and software design. The final specifications are the documents that the manufacturer will use to actually make the system. The conceptual design for this process is shown in Figure 5.

Each of the horizontal levels in the Figure roughly corresponds to a particular Phase in the planning of the project. The UFTR Digital Controls project is currently in the second level of this diagram: The System Specifications level. As is shown in Fig. 5, the entire process is somewhat iterative; as the design stages progress changes must be made to previous levels of design to accommodate any unforeseen requirements that are encountered.

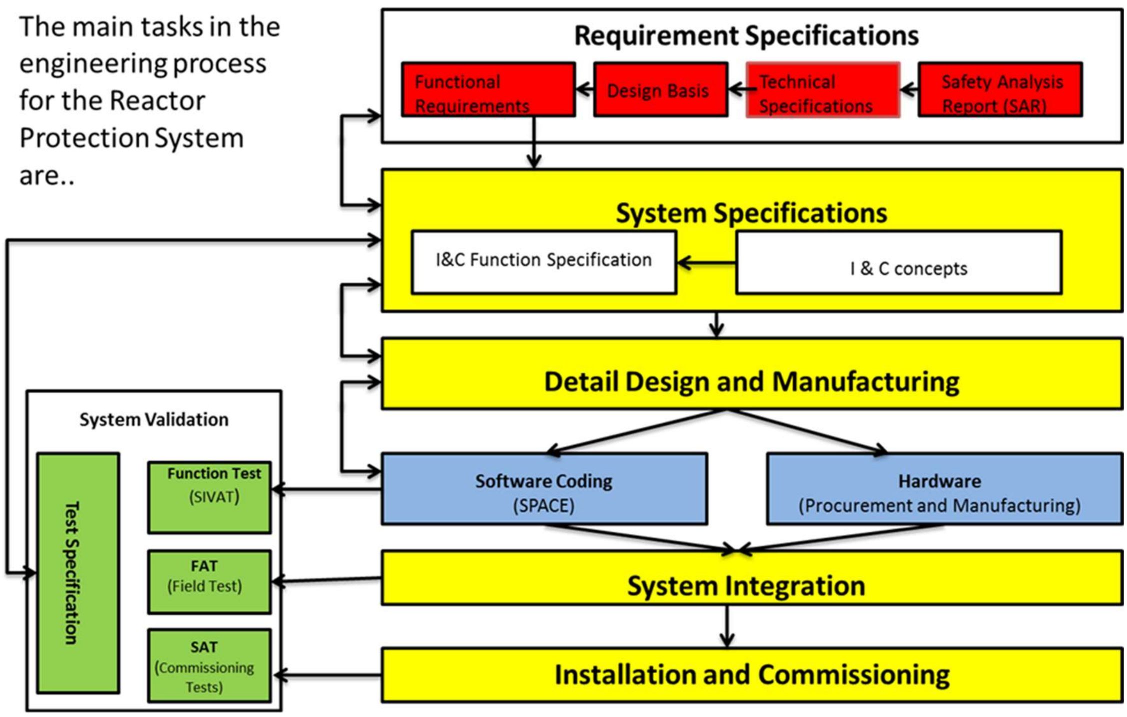


FIG. 5. The conceptual design of organization of digital controls engineering project.

The project process for the control system is simpler. It does not require licensing by the NRC except where it interacts with the RPS. Since the UFTR is a research reactor, the staff may need to monitor aspects of projects, unusual parameters and have the ability to monitor different aspects of the plant that a conventional plant operating system will not need to consider.

6. 10 CFR 50.59 CHANGE VS. LICENSE AMENDMENT REQUEST (LAR)

There are two different options for making a change to the plant of this type. Converting the I/C system from an analog to a digitally controlled system does not materially affect the functions as described in the FSAR. This allows the choice of pursuing a change to the plant using the Chapter 10 of the Code of Federal Regulations Chapter 50.59, (10CFR 50.59) criteria. Paragraph (c) (2) of this section of the CFR lists the 8 criteria for deciding if a license amendment is required.

A preliminary analysis for the UFTR indicated that the criteria from this section do not apply. However, the University has decided to proceed with a License Amendment Request (LAR) and submitted the first batch of documents to the NRC in Feb 2010 while publicly reserving the right to proceed with the upgrade using the 50.59 processes [5].

7. PLANNING AND PROGRESS

The beginning point for any project/conversion that affects a Nuclear Power Plant is the Final Safety Analysis Report (FSAR). This report details all the functions and procedures necessary to ensure the safe functioning of a Nuclear Reactor. The University is currently undergoing a license renewal and is operating under the license issued in 1982 and was up for renewal in 2002. A Safety Analysis Report (SAR) was submitted in 2002 for license renewal and is still in review with the NRC [1].

The project has been divided into several phases; either 4 or 7 depending upon what aspect of the project is being discussed. The licensing portion has a 4-phase breakdown while the design, manufacture and installation portions of the system are broken down into 7 phases.

TABLE 3. LICENSING AND PROJECT PHASES FOR DIGITAL UPGRADE

Licensing (LAR-NRC)	**Project (UF/Vendor)**
Phase 0. Pre Application	1. Project Startup/Conceptual Engineering
Phase 1. Initial Application	2. Basic Hardware/Software Design 3. Detailed Hardware/Software Design
Phase 2. Continued Review and Audit	4. Manufacturing 5. Testing
Phase 3. Implementation and Inspection	6. Installation & Commissioning 7. Final Documentation

8. LICENSING PHASES

The licensing phases are:

(a) Pre Application: A presentation on Conceptual Design that covered the initial design work and concepts. The following documents were presented to the NRC: Software Verification and Validation Plan (SVVP), Diversity and Defense-in-Depth (D3) Analysis, and the Functional Requirement Specifications (FRS).

(b) Initial Application: This Phase contains information in greater detail and includes information that is sufficient to address a) Defense-in-depth & Diversity, b) Hardware Design & Single Failure, c) System Modifications & Configuration Control, d) Data Communication, e) Software Design & Development, f) V&V Plan, Cyber Security, and g) the technical specifications.

(c) Continued Review and Audit: This Phase should contain sufficient information to address any remaining subject areas, including additional V&V Plan information not available during Phase 1, equipment qualification, testing and calibration.

(d) Implementation and Inspection: This Phase is related to installing the system, effecting associated procedural and technical specification changes, and completing startup testing. The startup testing is conducted in accordance with the plan submitted during Phase 2 as addressed in Section "Test and Calibration." Test reports and user documentation are also generated in this phase.

9. PROJECT PHASES

The project is divided into seven project phases, as described UFTR Quality Assurance Project Plan. These are summarized as follows:

(a) Project Startup/Conceptual Engineering: Develop General overview of the system components and their interrelationships, the Input Output (I/O) list and the associated technical specifications and the Functional Requirements Specifications (FRS).

(b) Basic Hardware/Software Design: Breakdown FRS into hardware and software requirements, design of the system components, racks for cards and CPUs, design of the network architecture and supplying equipment data sheets for field equipment not supplied by the vendor.

(c) Detailed Hardware/Software Design: Design documentation phase, design the testing and FAT plan; develop Final system descriptions; perform calculations as required and review project documentations as necessary.

(d) Manufacturing: Manufacturing of the parts and materials. Purchasing of necessary spare parts by UF.

(e) Testing: Perform Factory Acceptance Testing (FAT). Perform Integration testing.

(f) Installation and Commissioning: Establish As-Built Documentation, Establish Overall/ System operating manual/Maintenance Manuals Develop Basic Operational Courses.

(g) Final Documentation: Develop final As-Built documentation: User manuals, SOPs etc.

10. CONCLUSIONS

The analog to digital conversion of a Reactor Protection System and Reactor Control System from is a complex and detail oriented project, even for as safe and reliable a system as the University of Florida's Training Reactor. However, the benefits to the University and to the nuclear community at large in operationally implementing a completely digitally controlled reactor provide benefits in many aspects of plant systems operation, maintenance and engineering. Benefits include the ability to capture and analyze a wide variety of operating parameters for use in trend analysis and system maintenance. We will also be able to customize the operational controls and displays for different operating modes and train a new work force in digital control as the industry trends toward digital systems.

ACKNOWLEDGMENTS

The authors would like to thank all colleagues, staff and students who contributed to this project to date. Their input, hard work and dedication has made the daunting task of this conversion achievable. In addition we would like to acknowledge the patience and support of AREVA NP Inc. and Siemens International during this development and specification process.

REFERENCES

[1] Diaz and Vernetson, Final Safety Analysis Report (FSAR), 1981 updated to Rev. 11, University of Florida (1998).
[2] A. Haghighat, Submittal Report to Cover Analyses of UFTR Conversion from HEU to LEU Fuel, Second Version (August 2009).
[3] A. Haghighat, Annual Report for University of Florida Training Reactor
[4] License R-56, Nuclear Regulatory Commission, Docket 50-83 (5 March 2010).
[5] A. Haghighat, Presentation on UFTR Licensing Amendment Application Phase 0 (16 Oct 2009).
[6] A. Haghighat, UF Pre-Submittal Review of Digital I&C Amendment Application (19 Jan 2010).

OPTIMIZING RESEARCH REACTOR LICENSING BASIS TO ALLOW FOR EFFECTIVE 10 CFR 50.59 SCREENING ON EXTENSIVE REACTOR CHANGES

J. LEWIS, G. BICKFORD, K. A. JORDAN
Department of Materials Science and Engineering
University of Florida, Gainesville, FL 32611
United States of America

Abstract

Due to the reduced requirements for the review of research reactor licensing documents, evaluating a change using the 10 CFR 50.59 requirements can be difficult. Specifically for a large modification effective evaluation may be impossible unless the licensing basis is well organized and efficiently written. This paper will discuss the issues the UFTR has faced when evaluating a digital controls system change to the reactor using the 10 CFR 50.59 guidance and proposes a plan for reconstituting the disjointed licensing basis to ensure future modifications can be more easily evaluated. *Key Words*: UFTR, Research Reactor, Digital Controls.

1. INTRODUCTION

Performing a change to a reactor under the 10 CFR 50.59 guidelines can be a difficult process. There are several key documents that must be examined prior to being able to answer the nine questions in the 10 CFR 50.59 effectively which generally include but are not limited to the safety analysis report (SAR), technical specifications (TS), and emergency plan (EP). For power reactors the SAR is a “living” document which is reviewed annually by the Nuclear Regulatory Commission (NRC) and will accurately reflect safety analysis for the current status of the power reactor. Research reactors do not have the same requirement.

“Even though regulations do not require the licensee for a non-power reactor to periodically update the SAR (as is required in 10 CFR 50.71 (e) for power reactors), the NRC staff encourages non-power reactor licensees to maintain current SARs on file at NRC after initial licensing or license renewal by submitting replacement pages along with applications for license amendment and along with the annual report that summarizes changes made without prior NRC approval under 10 CFR 50.59.”

The SAR for a research reactor is reviewed when the reactor license is up for renewal. Research reactors can make changes to their reactor, document the change, and the only reporting requirement is to inform the NRC of the change in the annual report. There is no requirement for the NRC to review the change or review the SAR to ensure it has been updated to reflect the change. This can lead to a SAR that does not accurately reflect what is actually at the reactor unless all of the modification paperwork is appropriately incorporated in a timely manner. Another problem this causes is that the up to date licensing basis for the plant is not in just 3 documents, SAR, TS, EP, but in many documents. Modification paperwork, conversion SARs, unapproved SARs and old SAR’s are just a few documents that can contain the true status of the reactor system. This is not usually much of a problem for relatively minor changes. Many changes are not even significant enough to warrant a 10 CFR 50.59 review but on the occasions that a modification is a significant enough to warrant such a review, the process can be difficult and complex for even a relatively minor plant change.

2. UFTR LICENSING BASIS

The licensing basis for the UFTR is not contained in just the three documents mentioned earlier. Over the 53 years the reactor has been licensed the three main documents have expanded over several versions and have been built up with unnecessary requirements. The following sections will give a brief history of how the licensing basis from the UFTR has become far from optimized.

2.1. History of the UFTR SAR

The University of Florida Training Reactor (UFTR) is a training reactor and so it is not required to have its SAR updated and reviewed annually. Its license review history is as follows. In 1959 the UFTR was licensed to operate up to 10 kW. This was a provisional license to ensure the plant worked and was safe for operation. In 1962 the license was upgraded to allow operations up to 100 kW. This was a 40 year license with a review required at 20 years. In 1982, 20 years later, the license was reviewed and this required a complete update, resulting in a 1982 SAR, technical specifications and emergency plan. This was the last time those documents have been reviewed and officially approved by the NRC. In 2002 the 20 year license expired and the UFTR staff submitted a new SAR, TS, and EP for license renewal. This new SAR incorporated all of the changes and modifications to the reactor prior to its submittal. At this point the safety analysis for the UFTR is in two documents, the approved 1982 SAR and the docketed 2002 SAR.

The NRC gives themselves 10 years to review the licensing bases for renewal. Just before 2002 there were significant national events which lead to many security changes being implemented by the NRC. This most appropriately took precedent over the renewal of the license for the UFTR and so the docketed 2002 SAR has not been approved by the NRC as of 2012.

In 2005 the UFTR applied to convert its fuel from high enriched uranium (HEU) to low enriched uranium (LEU). The request required a separate safety analysis report, modification to the Reactor License, and changes to the TS. The new safety analysis report, the HEU-LEU conversion SAR (CSAR), was completed by following the guidelines for a fuel conversion safety analysis in chapter 16 of the NUREG 1537. The guidance required several comparisons between the safety analysis of the HEU core and the proposed analysis of the new LEU core. The fact that the last approved SAR was the 1982, however; the most up to date analysis was in the docketed 2002 SAR lead to the CSAR using parts of the HEU analysis from both of these documents.

The NRC reviewed the CSAR and changes to the TS and approved the conversion in 2006. This allowed the UFTR to convert and use LEU, however; the 2002 SAR on the docket did not contain this information, and now the actual status of the UFTR is in 3 documents, the 1982 SAR, 2002 SAR, and 2006 CSAR. At this point the licensing basis for the UFTR is spit into 3 different SAR's and several modification packages.

2.2. UFTR technical specifications

TS are required by 10 CFR 50.36 and any change to a technical specification is required to be reviewed and approved by the NRC according to 10 CFR 50.59. This requirement ensures that the TS are up to date and accurately reflect the current status of the reactor. Briefly, the TS are required to define safety limits to prevent against the uncontrolled release of radioactivity, limiting safety system settings (LSSS) to prevent a safety limit from being violated, and limiting conditions for operation (LCO) to ensure the reactor is operated with the functional capability to enforce the LSSS. The other required sections will not be discussed. These three sections define the requirements for safe operation of the reactor.

The two safety limits for the UFTR listed below are to prevent damage to the fuel cladding because damaging the cladding is the only way to get an uncontrolled release of radioactivity.

(a) The fuel and cladding temperatures shall not exceed 986 F;

(b) The specific resistivity of the primary coolant water shall not be less than 0.4 megohm-cm for periods of reactor operations over 4 hours.

The first SL is to prevent melting of the fuel cladding and the second is to prevent corrosion of the fuel cladding. The fuel cladding is the physical barrier preventing the release of radioactivity and so its integrity must be maintained.

According to 10 CFR 50.36, LSSS are settings for automatic protective devices related to variables having significant safety functions. Additionally, when an LSSS is placed on a variable that has a safety limit associated with it, the setting should be chosen so that the automatic action will correct the abnormal situation before the safety limit is exceeded. Examining the two safely limits one would expect few LSSS, however; the UFTR TS has twelve LSSS. Upon further examination of the TS it is apparent that they are not the minimum operational safety requirements based on safety analysis and the established safety limits but are minimum operational capabilities of the as built protection systems. The TS has specific LSSS for each of the trips that the reactor protection system is capable of initiating regardless if the trip has a significant safety function or not. Due to this fact the TS include too much system specific requirements that are not necessarily required for safe operation of the reactor.

The LCO continue this trend and require a large number of components to be functional in order to operate the reactor. All of the equipment required for the 12 LSSS protective actions is required by the LCO to operate the reactor. Additionally, the LCO are specific to the actual equipment installed which limits the ability to change equipment but maintain the same protective action abilities.

Overall the UFTR TS contain extraneous specifications for requirements that are not significant safety functions. Many of these specifications, which do not have a basis in from the SAR, are contained in the TS because “they were there before.”

2.3. Modifications

Changes and modifications to the reactor are common for a research facility. Between the 1982 SAR and the 2002 SAR there were 23 documented modifications ranging from replacing a pen recorder to installation of the pneumatic delivery rabbit system. The 2002 SAR documented and incorporated all of these changes, however; changes made since 2002 are not. During the past 10 years several needed modifications have been made to the UFTR and appropriately document but they have not been included in the docketed 2002 SAR, the most notable example being the HEU-LEU conversion. During the process of converting the fuel, several other changes were made to the reactor because of the unique access to the support structures without loaded fuel. Many of these changes are not in any specific SAR and end up being additional documents that require reviewing prior to making new changes to the reactor.

3. PLANNED DIGITAL CONTROL UPGRADE

After the successful completion of the fuel conversion the UFTR staff decided to embark on an upgrade to completely replace the aging analog reactor control and reactor safety systems with a completely digital system. The staff found external technical support, funding, and expertise to help with the project. The project was started and much progress was made in designing the new digital control system; however, the licensing issues for the upgrade where not fully realized. The project stalled out a year later once a review of the licensing basis for the reactor was completed. The digital controls upgrade pointed out a few significant issues with the ability to make any change to the reactor. The managers of the project realized that in order to maintain the relationships with the external support, an accurate timeline of events would be needed for the completion of the digital upgrade. By reviewing the licensing requirements for such an upgrade there were two distinct options.

3.1. License amendment request

The first option is to request a license amendment request (LAR) from the NRC. Completing the project down this path, the NRC reviews any needed changes to our licensing basis prior to implementation of the changes and their approval are required. With regard to license changes, this is the easier route to take because the licensing basis can be changed as needed during the LAR and upgrade process. The major downside to this route is the inability to schedule. There are no guaranteed dates for the NRC review and approval process which leads to an upgrade that could potentially spends years in the approval process with no ability to perform the upgrade. In fact, there is no guarantee the NRC will even approve the upgrade! This option is risky for the external support due to the uncertain time tables and possibility of denying the upgrade all together.

3.2. Change under 10 CFR 50.59

The second option, to perform the upgrade per the 10 CFR 50.59 guidelines would, if all of the guidelines were met, allow the upgrade to be implemented without NRC approval. This would allow for a more concrete time table and would not rely on a potentially lengthy and unpredictable NRC approval process. The catch is that the upgrade has specific requirements it must meet in order to be implemented under the 10 CFR 50.59 guidelines. Most of the requirements require comparing the proposed upgrade to the current SAR and TS. There have been several guides written specific to upgrading a reactor with a digital system under the 10 CFR 50.59 guidelines, and one of these guides has been approved by the NRC.

3.3. Issues preventing an effective choice

The 10 CFR 50.59 guidelines determine whether or not an LAR is required for a given change to the reactor. Meeting all of the guidelines in the regulation would allow a modification to the reactor to be implemented without an LAR. To effectively make this determination the proposed modification and its effects on the reactor must be compared to the current licensing basis and, via the eight 10 CFR 50.59 guidelines, shown not to substantially affect the safety of the reactor. To do this there must be a clear and understandable licensing basis and a detailed description of the proposed modification and how it will affect the reactor.

With regards to this determination there are two significant problems. First, the UFTR is in a particularly interesting situation because the approved SAR from 1982 and the docketed 2002 SAR contain safety analysis for the HEU core, however; the approved CSAR has the safety analysis for the LEU core. This complicates the ability to understand the licensing basis because of the differences in analysis in each of the SAR's. If this problem were solved all of the analysis was in a single, approved SAR that accurately reflects the current status of the UFTR, it would then be possible to compare it against a proposed modification.

Second, the functional requirement specifications (FRS) of the digital controls modification or any modification must be known. All aspects of how the upgrade will change the current reactor must be known in order to make an effective comparison to the SAR using the 10 CFR 50.59 guidance. The FRS created for the digital control upgrade was long, contained too much information and was not tailored for easy comparison to the SAR.

3.4. Example system change

What follows is an example of a simple change to the reactor system that was evaluated using the UFTR standard operating procedure for evaluating modifications to the reactor. Modifications generally fall into three categories. The simplest can be completed without a full 10 CFR 50.59 review. These modifications do not affect the reactor in any significant way. The second category is modifications that must be evaluated using the 10 CFR 50.59 guidelines. These are modifications that affect the safety system of the reactor. The last are changes that are specifically controlled by other guidance such as any change affecting the emergency plan or technical specifications.

The proposed change is to replace an old CRT computer monitor for the temperature monitoring/data acquisition system with a new, smaller LCD monitor. This is a fairly straightforward change that passes the common sense test of not having a large effect on the reactor system. First, the applicability of a 10 CFR 50.59 screening in determined. The three questions that are addressed are:

— Does the proposed activity involve a change to the technical specifications or operating license?

— Does the proposed activity involve a change to the security plan or emergency plan?

— Is the proposed activity controlled by other more specific requirements and criteria established by regulation?

If all of these are answered no, which is correct in this case, then a 10 CFR 50.59 screening is required for the modification. For the screening, 4 more questions concerning the modifications effect on the SAR are answered. For the sake of brevity in this example, the change of monitor did not affect the SAR in a significant way so a 10 CFR 50.59 evaluation was *not* required and the change could be implemented without any further investigation.

The difficulty in this simple example of changing a monitor is in the documents that were required to be reviewed to accurately justify the answers to the six applicability and screening questions. The 1982 SAR, 2002 SAR, CSAR, TS, several modification packages and the emergency plan were all were reviewed. In total about 17 different sections in these various documents contained relevant information about the temperature monitoring system and were used to justify *not* performing a 10 CFR 50.59 evaluation. Going through this process with a modification that would require a 10 CFR 50.59 evaluation and answering the additional 8 questions would require an even more in depth analysis of the licensing documents. Completing this evaluation with an invasive modification such as the digital control system upgrade would be nearly impossible.

3.5. Feasibility

The rest of this paper will discuss the changes to the licensing basis that would be needed in order to effectively evaluate the upgrade. There are several documents that give guidance on how to perform this specific evaluation and effectively design the digital control upgrade and so these topics will not be covered in this paper. NEI 96-07, Guidelines for 10 CFR 50.59 Implementation [1] contains specific guidance for implementation of a 10 CFR 50.59 screening process. NEI 01-01, Guideline on Licensing Digital Upgrades [2] gives specific guidance for designing and implementing a digital control upgrade and serves as a supplement to [1]. The NRC has endorsed the NEI 01-01 report. These documents prove the feasibility of evaluating a digital control upgrade using the 10 CFR 50.59 guidelines.

The UFTR staff more fully understands the licensing issues with a digital control upgrade, and on a more basic level understands that it needs to combine and update its several licensing documents to have just one correct, well written, and eventually approved SAR and technical specifications. In order for the UFTR to be able to screen the project for a 10 CFR 50.59 evaluation, the functional requirement specifications for the upgrade will have to be finalized and compared to an updated and consolidated SAR. Understanding this problem presents the opportunity to fix the issues with the SAR and design the digital upgrade so that its effects on the SAR can be more easily evaluated.

4. OPTIMIZATION OF THE SAR AND TECHNICAL SPECIFICATIONS

There are several steps the UFTR staff is planning to take in order to be able to effectively evaluate whether future modifications can be implemented using 10 CFR 50.59 guidelines. The licensing basis will have to be reconstituted and optimized. By understanding the guidelines in the 10 CFR 50.59, the SAR can be written to allow for easy comparison to proposed modifications. The main focus will be on determining the minimum requirements for reactor safety and removing extraneous requirements and specifications. This will not only allow a reasonable evaluation of the 10 CFR 50.59 process for a digital upgrade, but streamline the process for any future reactor upgrade. The digital control upgrade has been used as an example in this paper because it is the primary modification of concern for the UFTR.

4.1. Safety Analysis Report (SAR)

To be able to consider reactor modifications efficiently, the SAR should reflect the current state of the facility at all times. There should be one SAR with the current status of the reactor and the most recent safety analysis and although it is not required to be submitted to the NRC for review, the revisions from the NRC approved SAR should be well documented and easy to follow. From the NUREG 1537 the second purpose of the SAR is “It gives information for understanding the design bases for the 10 CFR 50.59 change process” [4]. The UFTR has been working on consolidating the design bases into a single document and this process will be completed soon.

The next step is to complete new safety analysis to highlight the inherent safe design features of the UFTR design in order to reduce the number of automatic trips. The UFTR has limited available excess reactivity and negative void and moderator temperature coefficients of reactivity. In fact, the UFTR has the ability to dump the primary coolant from the core which inserts several times more negative reactivity than the maximum available positive reactivity. General analysis detailed in NUREG/CR-2079, Analysis of Credible Accidents for Argonaut Reactors*,* shows that a power excursion from the rapid insertion of a maximum available excess of reactivity would not be sufficient to cause fuel melting [6]. This analysis can be conducted on the UFTR core to get specific maximum temperatures and show that no credible power excursion could cause fuel damage.

Finally, it should be shown that it is not possible to startup the reactor without moderator in the core and, in the unlikely situation that the core is full of moderator but the water is not flowing (stagnate water), that boiling the moderator will shutdown the reactor due to negative void and moderator coefficients of reactivity and not lead to high fuel temperatures. It will need to be shown that the primary coolant is not needed for reactor safety. Completing this and the previously mentioned analysis will justify removing several of the LSSS that are in place to prevent fuel and fuel cladding temperature from reaching the SL.

4.2. Technical specifications

Any change to the TS requires a LAR and approval from the NRC. To reduce the number of LARs, the TS should be minimized to only the required specification needed for reactor safety and safe reactor operation. They should also not be based on the installed equipment, but on the requirements for safe operation. Following guidance in ANSI/ANS-15.1-2007, The Development of Technical Specifications for Research Reactors [5], each specification shall include related information in the following format:

(a) applicability: This is a statement that indicates which components are involved and when they are involved;

(b) objective: This is a statement that indicates the purpose of the specification(s);

(c) specification(s): This statement provides specific data, conditions, or limitations that bound a system or operation. This statement is the most important statement in the technical specifications agreement;

(d) basis: The basis is a statement that provides the background or reason for the choice of specification(s), or references a particular portion of the Safety Analysis Report that does.

The current safety limits in the TS are for protecting the fuel cladding from damage. The fuel cladding in the UFTR is the principle fission product barrier. The two SL, shown in Section 2.2, are a temperature limit and minimum resistivity limit. These are two good SL and should not be changed. Next, the 12 LSSS should be considered. According to [5] "**The LSSSs are chosen so that automatic protective action will terminate the abnormal situation before a safety limit is reached**". Several of the LSSS do not have a clear basis as to the reason for being a LSSS. The proposed new analysis in the SAR will be used to justify when a LSSS is or is not required.

What follows is a summarized list of the 12 LSSS from the TS and brief recommendations on how to remove or modify each of them to minimize the number of specifications in the TS. This is just the initial analysis of the TS and once it has been determined that a current LSSS is not needed, the rest of the TS should be evaluated to take into account that fact.

(a) Power level ay any flow rate shall not exceed 119 kW;

(b) The reactor period shall not be faster than 3 sec;

(c) Te primary coolant flow rate shall be greater than 41 gpm;

(d) The average primary coolant inlet temperature shall not exceed 99 F and outlet temperature shall not exceed 155 F;

(e) Primary coolant pump shall be energized;

(f) Primary coolant flow rate shall be monitored at the return line;

(g) The primary coolant core level shall be at least 2in. above the fuel.

These LSSS were originally selected to prevent the onset of nucleate boiling from occurring in the reactor during steady state or transient operations. It was shown in the CSAR that adhering to these limits prevents the possibility of flow instabilities. All of these LSSS can be removed by showing that the reactor will not reach the SL of 986 F under any power, flow, or coolant temperature combination. Referring to the recommended additional SAR analysis, a step insertion of the maximum excess reactivity will give the highest power and fastest period, and primary coolant is not required for preventing a SL violation. Power level would still be limited by the reactor operating license.

(a) Secondary coolant flow shall be provided at power levels equal or larger than 1kW;

(b) High voltage to safety channels 1 and 2 neutron chambers shall be 90% or greater.

The secondary coolant cools the primary coolant and if it is shown that the SL will not be reached for any credible range of primary coolant temperature, then this LSSS is not required. Next, the high voltage required to be at least 90% of the normal value so that the power indications from these two neutron chambers are accurate and will trip the reactor at the given power limit. If there is no power limit required to prevent exceeding a SL then this LSSS is not required.

(a) Reactor shall be shutdown when the main ac power is not operating;

(b) The reactor vent system shall be operating during reactor operations;

(c) The water level in the shield tank shall not be reduced 6 in. below the established normal level.

These last three LSSS should be limiting conditions for reactor operation, not limiting safety settings. The vent system and water level are requirements for radiological safety and do not prevent exceeding a SL. By showing in the SAR that the safety limit of 986 F cannot be violated under any credible conditions, the need for extensive LSSS is removed.

5. CONCLUSION

The need for a consolidated and optimized licensing basis is crucial for effective analysis of reactor modifications via the 10 CFR 50.59 process. Reducing the number of systems that are considered safety systems optimizes the licensing basis and eases the process of determining if a modification has an effect on reactor safety. The UFTR design basis needs new analysis to make use of the fact that the UFTR has many passive properties which make it an inherently safe reactor in order to optimize its licensing basis. The current basis reflects the installed operational capability of the UFTR as opposed to the minimum operational safety requirements. This has caused the design basis to become complicated and an impediment to needed changes to the reactor. Determining the actual requirements for safety of the reactor in the SAR and using that analysis to eliminate extraneous LSSS from the TS will streamline the evaluation and implementation of future modifications.

ACKNOWLEDGMENTS

The authors would like to thank the UFTR staff: Brian Shea, Daniel Cronin, and Matt Berglund for their hard work and help with this paper.

REFERENCES

[1] NEI 96-07, Revision 1, "Guidelines for 10 CFR 50.59 Implementation" (November 2000).
[2] EPRI TR-102348, Revision 1, "Guideline on Licensing digital Upgrades" (March 2002).
[3] Code of Federal Regulations Title 10, Part 50.59, "Changes, Tests and Experiments."
[4] NUREG-1537 Part 1, "Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors." (February 1996).
[5] ANSI/ANS-15.1-2007, "The Development of Technical Specifications for Research Reactors" April 2007, American Nuclear Society (2007).
[6] HAWLEY, S.C., KATHREN, R.L., ROBKIN, M.A., "Analysis of Credible Accidents for Argonaut Reactors", NUREG/CR-2079 PNL-3691, US Nuclear Regulatory Commission (1981).

IMPLEMENTING SUCCESSFUL SOFTWARE FOR DIGITAL INSTRUMENTATION AND CONTROLS AT THE HIGH FLUX ISOTOPE REACTOR

K.L. SHAW, H.H. OBERHOLTZER, M.A. LINN
High Flux Isotope Reactor, Oak Ridge National Laboratory
Oak Ridge, Tennessee
United States of America

Abstract

The High Flux Isotope Reactor (HFIR) is an 85 megawatt research reactor operated at the Oak Ridge National Laboratory for the US Department of Energy. Beginning operation in 1965 for isotope production, its primary role now is to support thermal and cryogenic neutron scattering in addition to isotopes production, material irradiation, and neutron activation analysis. Under the HFIR original design, its safety and operation incorporated the most advanced analog instrumentation available with a large percentage designed and built at ORNL for HFIR specific use. While this high degree of instrumentation specialization was a benefit at initial operation, it is now more of an impediment as analog parts and human expertise in the nuances of the original HFIR analog design are no longer available. As a result, the HFIR has begun a transition from analog to digital instrumentation for several systems. In our preparation for designing digital systems for the HFIR, our investigations into software engineering found that although the efforts to standardize terminology, develop software life cycles, and define guidelines and professional standards were extensive, designers and regulators continued to struggle with developing "error-free" software with most problems residing not in the hardware but the software. Statistics aggregated on the topic of software errors show that defects from a variety of sources are to be expected throughout the software development process. The HFIR software engineering group has developed a software development process that incorporates all expected software quality assurance documentation and includes a rigorous matrix of training and project management guidance; requirements definition and code development tools; and structured reviews and testing. Since 2007, the meticulous application of our process has resulted in only nine software defects of low severity significance and zero defects of high severity significance in 135,000 hours of operation of four systems with complete analog-to-digital replacement.

1. INTRODUCTION

As the uses of nuclear technology expand into the 21st century, the facilities to enable that expansion remain rather static. Regulatory, safety, and most often, significant costs prevent a matching expansion of new nuclear facilities. While notable exceptions to these hindrances have or are being built, there is tremendous pressure to extend the useful life of the existing reactor and non-reactor nuclear facilities beyond their original design lifespan. As most of these facilities were built in period of time from 1950 to 1970, the problems associated with their age are several. This paper relates to the issue of aging instrumentation and controls.

The High Flux Isotope Reactor (HFIR) is an 85 megawatt research reactor operated at the Oak Ridge National Laboratory for the US Department of Energy. The HFIR began operation in 1965 for the purpose of isotope production. However, its primary role today is to support thermal and cryogenic neutron scattering in addition to isotopes production, material irradiation, and neutron activation analysis. Under the HFIR original design, its safety and operation incorporated the most advanced analog instrumentation available at that time with a large percentage of it designed and built at ORNL for HFIR's specific use. While this high degree of specialization of analog instrumentation was considered a benefit at initial operation, it has now become more of an impediment. In many instances, analog replacement parts no longer have the performance characteristics of the original components due to different manufacturing processes or due to different or, ironically, improved materials. Thus the simple replacement of a failed transistor in a complex circuit becomes somewhat of a “trial-and-error” exercise that may require modifications or adjustments to other components to achieve the original design output. And in this age of standardization, locating highly specialized components becomes increasingly more difficult. And during our efforts to maintain the aging analog systems at the HFIR, we found an unexpected vulnerability in analog system maintenance—the human expertise in the nuances of the original HFIR analog design is no longer available. While there is extensive documentation on “how” a particular circuit was designed, the “why” of the design has, in many cases, been lost, making repair or redesign efforts, such as “reverse engineering,” of the highly specialized HFIR systems difficult to complete with a high confidence in the product. As a result, the HFIR has been transitioning from analog to digital instrumentation for several systems. In our preparation for designing digital systems for the HFIR, our investigations into software engineering found that although the efforts to standardize terminology, develop software life cycles, and define guidelines and professional standards were extensive, designers and regulators continued to struggle with developing “error-free” software—most recorded problems of digital systems resided not in the hardware but the software. Statistics aggregated on the topic of software errors show that defects from a variety of sources are to be expected throughout the software development process. Armed with this evidence of practicality, the HFIR has developed a software development process that incorporates all expected software quality assurance documentation and a culture that recognizes the effects (positive and negative) of the human element in the production of a quality software product. A brief description of that process is provided.

2. HFIR SOFTWARE PROCESS DESCRIPTION

2.1. Software engineering group

The HFIR has adopted the definition of software engineering as the application of a systematic, disciplined, and quantifiable approach to software development, operation, and maintenance that communicates both an engineering process and a culture in order to achieve a quality product. Note the HFIR definition includes the presence of a “culture.” The research by HFIR engineers of software development studies found the human plays a rather complex role in preparation of quality digital software, much more so than with analog instrumentation design. In recognition of this role, a software engineering group has been created within the engineering organization that is dedicated to the design, development, and implementation of digital instrument design and its supporting software. High quality software at a minimal effort will result only when the software is recognized as the primary product, not the hardware used for its implementation. The HFIR software development process is defined by director level administrative procedures which are strictly enforced. Regulatory requirements are scrupulously reviewed and included as necessary to ensure such impacts are correctly considered at the beginning of the project. Each process is begun with the objective to tailor the product to fit the customer’s needs, keeping it tightly focused, and not adding “flexibility” (that is, complexity) simply because of the ease to do so. Larger projects are assigned a project manager, whose role is to keep the project members focused on their assigned tasks, manage progress, prevent “scope creep,” and ensure independence of reviews. The individuals of the software engineering group have been selected not only based not on their technical ability, but on their willingness to work as an integrated team. For each project, training is provided on any specific software and hardware to be used as well as any project-related standards to ensure consistency with the development within the project members. Each project member attends regularly scheduled meetings used to communicate status, decisions, and any corrections to project course or details.

2.2. Model selection

Successful software engineering programs use a process model as the foundation as the model frames the activities across the entire process. The HFIR process model is a combination of a sequential process model and a prototype process model.

This combined model can be iterated if the project is suited for development in stages. In the sequential model, the flow of work occurs in a reasonable linear fashion, from initial communication of the project through deployment and maintenance. This presents the most straightforward, resources-efficient, and simple process to manage. However, as it is increasingly difficult for a system hardware design to follow a sequential flow as the size of the project increase, it is similarly difficult for all software requirements to be explicitly defined at the beginning of the project, creating a high potential for errors due to changes during a sequence-oriented process. In addition, a working version of the hardware is not available until late in the project and therefore major deviations from the customer expectations can be disastrous from a project management standpoint.

To alleviate these issues, HFIR has incorporated a prototyping model as a first step in its sequential model. Implemented within the context of the sequential process model, a quick initial design leads to a prototype which is used as the basis for the formal design. As part of the prototype model, general requirements and functionality are discussed with the customer and prospective hardware is purchased for evaluation of its suitability. General tasks such as hardware communication, establishing user preferences, and preparation of a workable human-machine interface are conducted. Any appropriate training is identified and provided to the project team. Software preparation is limited primarily to an initial draft of functional requirements and demonstrating "proof-of-principal." This iterative part of the model process allows both feedback and time for project refinements until the customer and the software engineer agree the prototype is an accurate reflection of the desired final product. The prototype model assists the software engineer in better understanding the needed software system while the customer's requirements are not yet clearly defined. At the same time, the user gets a hands-on impression for the actual system being developed. A pitfall to be avoided is the temptation to take the prototype straight to implementation by assuming remaining changes require only "small fixes," This only short-circuits the quality processes needed to ensure a low defect product. Also to be avoided is the acceptance of compromises made during the prototype design to demonstrate workability. While acceptable from a prototype standpoint, such workarounds will lead to defects and unintended consequences if allowed to remain in the design and are not exposed to the full software quality processes.

2.3. Gathering of requirements

System requirements provide the foundation for the overall software design. Studies show that for complex software systems, defects were not due to the complexity of the software so much as due to discrepancies between the documented requirements, the requirements for actual system function, and misunderstandings about software interfaces with other parts of the system. Consequently, for the HFIR software process close attention is paid to further refinement of the draft functional requirements prepared during the prototype model. This preparation of a functional description is typically a multi-discipline task and provides details regarding user inputs and operational requirements, needed outputs, software interfaces, and processing logic and order in a readable manner that facilitates a common understanding of the system. When ready for approval, the functional description is subjected to a quality sub-process called a structured walkthrough. A structured walkthrough is where a detailed review and document approval is performed in an open discussion environment between the HFIR project manager, software engineers, customers, and quality assurance engineers. This team-oriented walk-through process can be used at any time during the software development process and its frequent use significantly reduces errors due to communication and interface lapses.

It should be noted there are two areas of requirements that are prepared prior to initiation of any software project and, once prepared, should remain relatively constant throughout any future projects. A software methodology standard has been prepared and approved by the project team, it establishes guidelines and requirements for the actual software code design and development. A human-machine interface (HMI) standard is also prepared and approved by the project team and it establishes guidelines and requirements for HMI (e.g., symbols, colors, layouts, etc.). Both these standards should remain relatively stable throughout plant lifetime to ensure consistency of software design, usability, safety, and accuracy and to ensure completed projects always present a consistent interface to plant personnel.

2.4. Software design

Once the functional description is approved, a software requirements specification is written that translates the functional requirements into a format that provides the software engineer with the input, output, interface, and process requirements necessary to begin preparing detailed code. Finally, a software requirements list is prepared from the software requirements specification to identify and catalog the individual software requirements as defined in the specification. Each requirement is assigned a unique identifier to enable its tracking to ensure its incorporation during the implementation step, for audit in subsequent quality assurance steps, and for developing simulation testing.

After these documents are approved, changes are strongly discouraged and are only approved if technically necessary. If a change is approved, the affected documents are revised and the entire software requirements development process is initiated from the beginning—"patches" to the software requirements are not allowed.

2.5. Implementation

2.5.1. Preparation of software code

With an approved functional description, software requirements specification, and software requirements list, the software engineer can begin preparing code in accordance with the approved software methodology and HMI standards. One or more structured walkthroughs of all prepared code are performed as needed to ensure high quality. Code documentation that adequately describes software flow, relationships of data, and interfaces with external components is necessary to ensure the ability of an accurate understanding of the system ten years later.

2.5.2. Backup and recovery

A written plan is developed and strictly followed beginning at initial code preparation for software backups and for recovery of the software in the event of corruption or loss.

2.5.3. *Evaluation of risks*

Software risks are evaluated in a proactive and continuous manner to assess what failures could occur, if the consequences of the failure are important, and to implement actions to address any risks. Both safety and security software risks are assessed. Potential hazards of reasonably postulated software faults should be assessed and evaluated for elimination or mitigation during the design process, not after field implementation. The HFIR software engineers have found the simplest and most effective means to address security risks is to "air-gap" the server upon which the process software resides, where the server is stand-alone and is physically isolated from the network or allows only outbound data traffic.

2.5.4. *Configuration control*

Once a baseline software Configuration is defined, a unique numbering system is implemented to track each subsequent revision. The HFIR process provides for tracking of both "major" and "minor" revisions. Software changes are documented, evaluated, and approved prior to release for implementation, including testing and verification activities if required. Although previously mentioned, it is worth noting again that two practices common to software development should be avoided—the apparent ease of coding "patches" and the temptation to implement desirable "enhancements." Both present risks to a quality end-product and both violate the HFIR philosophy to address only the system requirements and to keep the coding as simple as possible. Once the software has been implemented in the field, any changes to either the developed software or the underlying operating system are strictly controlled and are handled in the same manner as any other HFIR modification.

2.5.5. *Performing reviews and audits*

Before software is ready for installation at the HFIR, multiple reviews and audits have been performed by the software team and external organizations, or both together. But each review is focused with its purpose and scope defined beforehand; this is especially important for reviews by external reviewers.

2.5.6. *Identification and removal of defects*

The preparation of software is no different from any design or production process where defects should be expected, identified, and corrected as soon as possible. The key to an effective defect removal process for software is the mindset that the identification of defects is a positive and successful outcome. Simple checking for expected outputs given the anticipated inputs is not sufficient to identify hidden errors. The review of requirements documentation and testing are used with the intent of finding a defect. Reviews and audits augment this "fault-finding" mindset. Approved changes are subject to the entire process, recognizing the change has the potential to create as well as solve problems.

2.5.7. *Software quality*

The requirements of the software provide the foundation against which the quality of the software is assessed. Software is no different than valves, machinery, or any other physical devise—quality must be designed into the software; it cannot be imposed after the fact. Both explicit (perform a specific function or calculation) and implicit (ease of maintenance) effects of the software should be addressed. It is recommended that some form of a software quality assurance plan (SQAP) always be prepared. Subjects that have been considered for inclusion in the HFIR SQAP are processes, methods, standards, procedures, project and risk management, Configuration control, procurement management, requirements identification and implementation, software safety, verification and validation, problem reporting and correction, and training. However, the details of the plan can be much smaller based on a graded approach depending on the complexity and importance of the software.

2.5.8. Verification and validation

Reviews continue as part of the verification of the software. Validation through testing begins. Plans for component tests and integrated system testing are written and reviewed. The value of an independent simulation computer cannot be overestimated. As a minimum, it is used prior to installation of the software in the field. The software requirements list identifies all individual software requirements that need to be included in the simulation test. A detailed and extensive test plan thoroughly tests different combinations of equipment, faulty field inputs and induced failures, and the actual actions performed by the system (i.e., when two desired but separate outputs are combined within the overall system, an undesired result can be created). Testing should begin at the component level and progress step-wise to the entire system. At field implementation, component tests are performed to demonstrate correct inputs and outputs.

2.5.9. Installation and maintenance

Upon satisfactory completion of component, integrated, and comprehensive simulation tests, final reviews and audits, and final approvals, the software and associated hardware are ready for installation. At the HFIR, this type of installation is treated no different from any other plant modification. This includes appropriate modification package preparation, approvals, and post-installation testing defined and implemented according to our Configuration control processes. This is in accordance with our Configuration control for all HFIR changes. However, it is recommended that a deliberate process for installation of the digital equipment be used to ensure correct installation and expected results. Once installed, performance is monitored and defects are documented and classified for both type and severity appropriate for the application. As an example, the class and severity classifications used for HFIR defect tracking are shown in Table 1.

TABLE 1. HFIR SOFTWARE DEFECT CLASSIFICATION

Severity	Type
— Defect has no effect on system operation (misspelled word) (Cosmetic - 1) — Defect is inconvenience to operators (display of known incorrect value) (Minor - 2) — Defect results in operator actions to work around the problem (system failure resulting in operator actions) (Moderate - 3) — Defect has operational impact outside the software system (reactor trip) (Major - 4) — Defect causes equipment damage or personnel injury (Catastrophic – 5)	— Logic problem — Computational problem — Interface problem — Database problem — Display problem — Documentation problem — Quality problem — Performance problem — Unintended problem from fix — Other

Under each classification type, subclasses are defined in order to permit detailed tracking and trending of specific defects. This "granularity" of defect classifications allows areas of program weakness to be more specifically and quickly identified. In this way, the software undergoes continuous "life-cycle" maintenance that provides improvement feedback to both the specific software application and the overall HFIR software development program.

3. RESULTS

Since 2007, the HFIR has completed and installed a comprehensive distributive control system for complete operation of the liquid hydrogen HFIR Cold Neutron Source, including multiple touch-screens for control at redundant operator stations, all controlled with a staff of three operators. Software monitors over 1300 I/O points from 27 sub-systems on a real time basis. The system monitors the cold source status, provides information to the operating staff, accepts operator commands, activates alarms, and controls equipment automatically or based on operator inputs. The HFIR Data System gathers information from approximately 60 data inputs for display in the control room, the emergency operations center, the laboratory shift supervisors office, and the ORNL emergency operations center. Certain parameters that are not directly measurable (core regional flows, thermal power, and megawatt days of operation) are calculated by the HFIR Data System from monitored parameters. Because of the HFIR reactor core design, there is a need for a fast scram response when safety limits are reached. The Time-of-Flight measurement system measures the time for safety rod travel from the time of a test initiation signal to the time the safety rods are fully inserted (less than 400 ms). Previously monitored by an 80486 computer with MS-DOS, this system has been replaced with PLC components and HMI interface (system accuracy of ± 0.15 ms) to provide sub-millisecond timestamps of the rod insertion sequence. Meticulous application of the software development process discussed previously has resulted in only nine software defects of low severity significance (1, 2 or 3) and zero defects of high severity significance (4 or 5) in 135,000 hours of operation, or less than 2 per operating year, for these digital systems.

Whereas, the previous examples describe the application of software-based digital system to new applications or to replace antiquated digital equipment, the most recent digital software development project for the Wide Range Counting Channels (WRCC) represents a true conversion of analog to digital. While the reactor safety system maintains override authority when safety limits are reached, the WRCC provides for normal control of reactor power during startup and indications of reactor power during low power operation. Three independent WRCC channels are housed in separate cabinets in the main control room. Over the last 10 years, there has been a steady increase in the frequency of problems with the WRCC and the resources required in performing troubleshooting and repair. Significant and extended outages of the WRCC have the potential for affecting plant operation. While the WRCC analog channels have not yet been replaced, all three digital channels have been built and undergone bench-testing. Replacement is scheduled to be accomplished in a staged manner over the next two years. The significant difference of the WRCC operator interface shown in Figure 1 is a direct reflection of the magnitude of change to occur where the analog hardware for a single channel will be reduced from a cabinet of 120 cm high and 60 cm wide to a volume the size of a two shoeboxes and mean time between hardware failures extended to millions of hours.

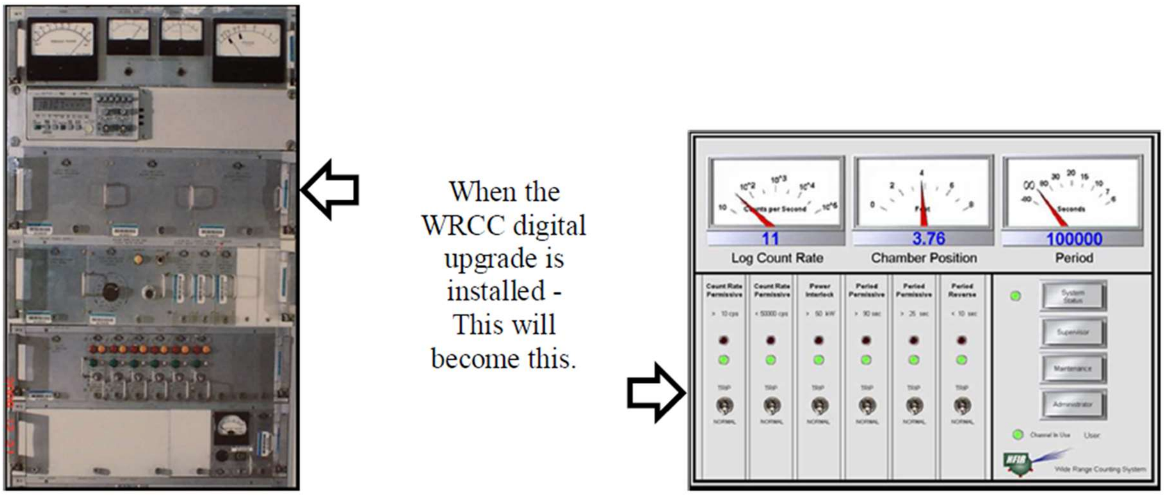


FIG. 1. Analog and digital interfaces for the HFIR WRCC.

4. CONCLUSIONS

The development of the HFIR software development program was not a simple process and required persistence by the software engineers to implement. The recognition of the need for a distinct and dedicated software engineering staff was an essential first step. While other organizations may not find such a staff dedication to be cost effective, the principle behind this decision can be implemented within any size organization—that the development of a digital system intended as a replacement for an existing analog system requires the same level of design attention as the original system that it replaces. But the HFIR experience has shown that digital installations even at a nuclear facility need not be resource intensive. Indeed, at the HFIR, the digital installations completed to date have been performed by a staff of two dedicated software engineers with only part-time support of other design, procurement, safety, and quality assurance engineering. The presence of a structured process that is always followed is critical to a consistent and quality product. The temptation of quick fixes, patches, and easy scope additions should be resisted. Team-work of designers, reviewers, and management is essential to a streamlined product within a reasonable period of time and budget. With these tools and the mindset that defects are expected and simply waiting to be discovered, there is no reason to anticipate any outcome but a successful one.

DIGITAL INSTRUMENTATION AND CONTROLS AT THE HIGH FLUX ISOTOPE REACTOR

K. L. SHAW, H. H. OBERHOLTZER, M. A. LINN
High Flux Isotope Reactor, Oak Ridge National Laboratory
Oak Ridge, Tennessee
United States of America

Abstract

The High Flux Isotope Reactor (HFIR) is an 85 megawatt research reactor operated at the Oak Ridge National Laboratory for the US Department of Energy. Beginning operation in 1965 for isotope production, its primary role now is to support thermal and cryogenic neutron scattering in addition to isotopes production, material irradiation, and neutron activation analysis. In the HFIR original design, the reactor's safety and operation were managed by the most advanced analog instrumentation available with a large percentage designed and built at ORNL for HFIR specific use. While this high degree of instrumentation specialization was a benefit at initial operation, it is now more of an obstacle as analog parts and human expertise in the nuances of the original HFIR analog design are no longer available. As a result, the HFIR has begun implementing digital instrumentation for new and existing systems. Beginning with the gradual replacement of analog process monitoring equipment with digital, a data collection and archival system for reactor process information has been implemented with many process parameters monitored in real time and archived for trending and evaluation. Strict adherence to network separation allows reactor conditions to be monitored at remote locations with high confidence in data quality. Designed and constructed in the early 2000s, the cryogenic facility for advanced cold neutron research utilizes a "touch-screen" distributed control system for cold source monitoring and operation as an application of digital instrumentation for new facilities. Digital replacements of the plant computer and safety rod time of flight computers are currently in operation. The three analog channels of the reactor wide range counting system used during reactor startup are waiting digital replacement, with future plans for digital replacement of the analog reactor control and reactor safety systems.

1. INTRODUCTION

The High Flux Isotope Reactor (HFIR) is an 85 megawatt research reactor operated at the Oak Ridge National Laboratory for the US Department of Energy. The HFIR began operation in 1965 for the primary purpose of isotope production. Today, while isotope production remains an important mission for the HFIR, its primary role is to support thermal and cryogenic neutron scattering in addition to material irradiation and neutron activation analysis. The original HFIR design incorporated into its safety and operation the most advanced analog instrumentation available. Because research reactor facilities with power levels as high as the HFIR were not routinely being built, a large percentage of its instrumentation and controls (I&C) was designed and built at ORNL for HFIR's specific use. While this high degree of specialization of analog instrumentation was considered a benefit at initial operation, HFIR design, maintenance, and operations personnel has found it now to be more of an obstacle to reliable, long-term operation. Difficult to repair and maintain, these systems are now experiencing many of the expected issues associated with the aging of instrumentation and controls. This paper provides several examples of implementing digital I&C at the HFIR and provides some information on the issues that were encountered and solved in their deployment.

2. DIGITAL INSTRUMENTATION AND CONTROLS INSTALLATIONS AND UPGRADES

The initial large-scale commitment to the application of digital I&C at the HFIR was in the replacement of the process instrumentation in the plant. As the frequency of problems with gauges, transmitters, and pressure and temperature sensors began increasing due to aging, the decision was made to replace the existing analog I&C with equivalent digital instruments as a long-term and persistent commitment. This method of incremental replacement served to minimize expenditure of resources and impacts on plant operation along with simplification of installed equipment, improved human-machine interactions, and increased reliability. Both non-safety-related and safety-related instrumentation have been replaced. Safety-related instrumentation was purchased as nuclear-safety qualified when possible. If nuclear-safety qualified instruments were not available or were cost prohibitive, standard instrumentation was purchased and formally dedicated for safety-related applications. Certain parameters that are not directly measurable (core regional flows, thermal power, and megawatt days of operation) are calculated by programmable logic controls (PLC) from data collected by the HFIR Data System, a process data collection system made possible by the ongoing replacement of analog process equipment with digital. The HFIR Data System is currently monitoring approximately 60 reactor and process parameters with data recorded every 15 seconds and archived for evaluation and trending if needed. The HFIR Data System provides live, highly reliable data inputs for display in the HFIR control room, the HFIR emergency operations center, the laboratory shift supervisor's office, and the ORNL emergency operations center. While only for data collection and display and not control, its high quality allows the data to be used for reference by the operators and by others at remote locations, including for emergency conditions when the main control room has been evacuated.

Because of the HFIR reactor core design, there is a need for a fast scram response when safety limits are reached. The Time-of-Flight measurement system measures the time for safety rod travel from the time of a test initiation signal to the time the safety rods are fully inserted (less than 400 ms). Previously monitored by an 80486 computer using MS-DOS, this system has been replaced with PLC components and HMI interface (system accuracy of ± 0.15 ms) to provide sub-millisecond timestamps of the rod insertion sequence to ensure safety rod travel times remain within specification and allow detection of increasing times.

Commissioned in 2007, the HFIR cold source permits neutron-scattering research when it is important to match the wavelength and energy of the neutron to the length and energy of the materials under investigation. Operating at 14 bar (absolute) and 14-24 K, the cold source system provides forced circulation of approximately 1 liter/second of supercritical liquid hydrogen through a vessel approximate 4 inches from the reactor core, increasing the wavelength of the available thermal neutron flux to a range of 4 to 12 Å and producing slower, long-wavelength neutrons better suited for studies of soft matter and low-energy excitations. A distributed control system (DCS) for the cold source employs supervisory control and data acquisition computers to gather data from approximately 1300 input/output points in 27 sub-systems and to provide control instructions to PLCs which interface with cold source instrumentation and equipment. Process data is backed up on a regular frequency. The PLCs are conFigured as pairs where control will automatically switch or "failover" to the redundant unit should the primary fail. The Human Machine Interfaces (HMI) for the cold source have varying levels of capability for monitoring and control and provide information as well as system control capability to the cold source operators. Touch screen monitors allow input commands for processing and transmittal to the appropriate component.

The Wide Range Counting Channel (WRCC) is a three-channel system that provides control and permissives for the reactor during startup and power indications during periods of low power operation. The fission chamber for each channel is located in a thimble and is positioned by its own positioning servo system through access at the bottom of the reactor vessel using complex feedback loops of tachometers, potentiometers, vernistat positioners and analog function generators. Raw pulse information from each chamber is transmitted by a "balanced" pre-amplifier/transformer circuit to reduce noise, provided to an amplifier, and then screened by a pulse height discriminator, with the fission pulses counted with a conventional scaler. The selected pulses are then converted into two signals, one linearly proportional to count rate and one logarithmically proportional. The linear signal is input to the fission chamber positioning servo system where the difference between the measured and reference signals (error) instructs the positioning servo to insert the chamber to a location of greater exposure or to withdraw it to a more shielded position as required to minimize the error. Thus, the servo system attempts to position the fission chamber so that it will count at a (nominal) constant rate of 10,000 counts per second. The position of the fission chamber position for each channel is then used to correct the log count-rate signal for flux attenuation at the chambers due to their location so that the corrected log count rate signal is proportional to the logarithm of the actual neutron flux of the reactor. Through networks of resistors, capacitors, and operational amplifiers, both the corrected and the uncorrected log count-rate signals for each channel are used to operate various permissive relays for the control system, drive recorders, and to calculate reactor power and period. Because the WRCC has important functions for reactor startup, problems with its operation can have detrimental effects on reactor operating schedules. Over the last 10 years, such effects began to present themselves with an ever-increasing frequency. Excessive signal noise, failures that required extended periods of troubleshooting to locate, and increasing difficulty in finding replacement parts all signaled an increasing risk of a wide-spread failure that would result in an extended unplanned reactor outage. After consideration of options (including its replacement with an identical analog system), the decision was made to replace the entire WRCC system with PLCs conFigured to perform the equivalent functions of the analog system. The digital PLC design maintains the WRCC Configuration of three independent channels. The pulse-transformer circuit of the analog channels for pulse signal noise control has been removed as digital outputs and fiber optic cable eliminate signal noise issues. The complex servo feedback system, with its maintenance-intensive potentiometer containing slip rings and brushes, has been replaced by a brushless resolver to track and output fission chamber position. Resolvers are rotary transformers where the magnitude of the energy through the resolver windings varies in a predictable and repeatable manner as the shaft rotates, thus eliminating brushes and slip rings and their associated high maintenance requirements. And, most importantly, the functions and interfaces of the digital WRCC remain identical to those of the analog equipment to be replaced—digital relay output interfaces provide signals to the reactor control relays and trips that are identical to those of the analog system. In short, the WRCC digital system will be a "black box" replacement for the existing analog system but with significant reductions in space requirements, improved HMI interface for the operators, fault monitoring and self-checking capability not available with the analog system, and module mean time between failures on the order of millions of hours. At this time, all three digital WRCC channels have been fabricated, bench-operated for a period of "burn-in," and are awaiting installation. As a conservative path forward, one complete digital channel will be installed early next year (the other two analog channels will remain in service) and operated for several reactor startups in order to gain additional experience and system confidence. When satisfied with performance of the digital channel in service, the remaining two analog channels will be replaced.

3. MANAGING DIGITAL I&C INSTALLATIONS AND UPGRADES

The primary contributor to the HFIR decision to begin replacing the original analog equipment was the continuing increase in the consumption of resources required to keep the analog equipment operating correctly. A second contributor was the pressure of budgets which remained level or even decreased from year to year. These two overarching contributors cascaded to other problems such as decreased reliability, increased signal noise and disruption, and risks to tight reactor operating schedules due to system failures. However, solutions to both contributors are being realized as the HFIR continues to expand the use of digital I&C throughout the plant.

In the case of new systems such as the DCS for the HFIR Cold Source, the choice of digital was not a difficult one. The complexity of the cold source systems and their need to operate at extreme physical conditions and delicate thermal-hydraulic balance meant that an analog system was not economically feasible compared to a digital system. But even if financially comparable, an analog system for the cold source would have presented a significant, and probably insurmountable, burden on the staff to operate the system in a reliable manner. It is simpler to design control and feedback capability for a digital system than for an equivalent analog system.

In many instances, replacement parts for analog components of the age of HFIR have become difficult to find. Cannibalizing existing spares for parts has been a rather routine practice over the years but eventually that inventory disappears and new replacement parts must be found. During these searches, the HFIR staff often found that new replacement parts do not have the same performance characteristics as the original components, particularly in the case of electronic components. Performances differences can result from variances in the manufacturing processes over the years or due to the use of different or, ironically, improved quality raw materials. Thus the simple replacement of a failed transistor in a complex circuit becomes somewhat of a “trial-and-error” exercise that may require modifications or adjustments to other circuit components to achieve the original design output. Another issue is the emphasis on “component standardization” that is now found in today’s manufacturing processes. While standardization permits consistency and quality of the products, success in locating highly specialized analog components becomes increasingly more difficult.

The HFIR staff also uncovered a much unexpected vulnerability while trying to maintain analog systems designed over 50 years ago—the human expertise in the nuances of the original HFIR analog design is no longer available. While there is extensive documentation on “how” a particular circuit was designed, the “why” of the design has been lost, making repair or redesign efforts, such as “reverse engineering,” of the highly specialized HFIR systems difficult to complete with a high confidence in the new product. In further “pulling this thread,” we have found that the industry seems to be undergoing a fundamental transition from analog to digital technology. Expertise in the design of new applications for analog instrumentation is becoming more difficult to find, it would seem that analog instrumentation design may become a “specialized skill” in the future.

The benefits to operations and maintenance staffs in the transition to digital go beyond just replacement of hardware. For example, over the last 10 years, approximately 50 analog gauges, dials, chart recorders have been replaced with digital equivalents which have resulted in a significant improvement in the human-machine interface for the reactor operators. It is just easier to read numbers on a digital output than interpret the value from a needle width half the size of the dial increment. Trends on digital charts can be “zoomed” for close inspection in contrast to the fixed resolution of pen and ink chart recorders.

Reliability improvements were also created due to complete elimination of system dependencies. The original HFIR I&C had several analog systems with some dependency upon pneumatics for operation as a method of diversity. While fully adequate from a control application, this dependency on compressed air required increasing resources to maintain while the equipment continued to decrease in reliability with age. The negative effects of this dependency was recognized early in the HFIR transition to digital and all compressed air dependencies for I&C have now been removed through the use of digital instrumentation.

If a reduction in space or area footprint for hardware is of importance, it has been our experience that 2-meter tall cabinets, completely full of instrumentation, wiring, terminal blocks, and pneumatics have been reduced to an equivalent functioning digital system on the order of one-tenth cubic meter. The positive impacts on maintenance resources of this reduction in system complexity and size are obvious. Costs of design and maintenance are also reduced through the use of standard, "off-the-shelf" digital components to the extent possible. Specialized components are only used when necessary to provide a unique capability or function. To date, HFIR staff has been able to identify standard equipment for all design needs. For example, in the Time-of-Flight measurement system, a "sequence of events" digital module is used to time stamp the safety rod drop sequences; the previously mentioned resolver is a rather standard device for tracking equipment movement and rotation. Digital design philosophies of self-checking with automatic failover from faulted instrumentation are used to increase system reliability. This philosophy was extensively employed in the DCS for the HFIR cold system to avoid problems due to power supply and PLC failures. Ease of maintenance is improved by modular designs ("plug and play") and the addition of extensive diagnostic capabilities for "in-situ" troubleshooting of the system by the maintenance staff, a capability not available for the analog designs.

In our preparation for designing digital systems for the HFIR, our investigations into software engineering found that although the efforts to standardize terminology, develop software life cycles, and define guidelines and professional standards were extensive, designers and regulators continued to struggle with developing "error-free" software with most digital instrumentation problems residing not in the hardware but the software. Statistics aggregated on the topic of software errors show that defects from a variety of sources are to be expected throughout the software development process. Armed with this evidence of practicality, the HFIR has implemented a software development process that incorporates all expected software quality assurance documentation and a culture that recognizes the effects (positive and negative) of the human element in the production of a quality software product. Once a digital system or application has been installed in the plant, training is conducted for appropriate personnel. As part of the design process, simulators that are prepared for testing of software and equipment interfaces serve double duty as training aids to familiarize staff with the new system. However, formal training of digital replacement systems is minimized by having a design process that actively seeks input and feedback from operations and other affected staff on the developing design.

To ensure usefulness and quality in the field of the finished digital application, all new and replacement digital designs are subject to the HFIR formal plant modification process. Changes to both instrumentation and software are subject to the same rigor of change management as given to any modification to the plant. In this way, any modification, change, or revision to plant hardware or software is in compliance with Department of Energy orders, standards, and guidance. While this rigor is for compliance with HFIR formal Configuration control requirements, it is recommended that an appropriate but deliberate process for installation of the digital equipment be used to ensure correct installation and expected results. Once installed, performance is monitored and defects are documented and classified for both type and severity appropriate for the application. This enables feedback on weaknesses in both the individual system designs and the overall software design process.

4. RESULTS

Replacement of analog systems with digital technology has increased reliability at the HFIR and has reduced maintenance costs and manpower. By upgrading to digital instruments, most calibration intervals have been increased from every two years to every four or five years. This is due to the stability and accuracy of the digital components which have no mechanical or electronic drift. The impacts of this movement to digital have been fully consistent with expectations. Since installation of the first digital instrument approximately 15 years and out of almost a hundred analog instruments exchanged for digital, less than a half dozen of the new digital instruments have been replaced due to failures.

5. CONCLUSIONS

While the original, custom-developed analog systems have served the HFIR well for over 40 years, the technology now presents many challenges to maintenance and reliability. Also, the industry seems to be undergoing a fundamental transition from analog to digital technology, for some of the same reasons including difficulty in finding replacement parts for analog components, complexity in design of control and feedback capability using analog components, and loss of analog design expertise. Of a practical nature, digital systems have smaller footprints and the availability of standard commercially available PLC's having a very wide array of capability provide for reduction of the costs associated with procurement. Our most valuable lesson from our experience has been the understanding of the critical importance that software has in implementing a digital system, especially when the digital system is designed as a partial replacement to interface with existing equipment.

The complexity of HFIR systems and their need to operate at precise and repeatable conditions led the HFIR to digital designs that were economically feasible when compared to analog replacement designs. Some examples of implementing digital instrumentation and controls at the HFIR, and information on the issues that were encountered and solved in their deployment, have been presented. As evidence of the substantial positive operational and maintenance impacts of digital technology at HFIR, the decision has been made to dedicate two engineers within the HFIR I&C group to the full-time task of software engineering with part-time support on a project-based need. This is a HFIR decision and not an indication of the difficulty with digital designs. We firmly believe that replacement of aging analog I&C with digital systems of equivalent function and improved reliability and maintenance is very cost effective and not a burdensome proposition. However, such undertakings will be successful only if the digital system design and implementation are given the engineering attention and rigor due any system or equipment to be used in the operation of a reactor or other nuclear-related facility.