Model Reference Control and Protection Theory and Implementation for Nuclear Power Plants using Real-time Simulations

AC Cilliersa, ASJ Helbergb

a Post-graduate School for Nuclear Sciences & Engineering, North West University, Potchefstroom, South Africa
bFaculty of Engineering, North West University, Potchefstroom, South Africa

Abstract. This paper shows that when combining the real time data from nuclear power plant measurement equipment with a real time simulator of the plant it is possible to perform tighter control and unwanted operation can be recognised earlier. As soon as the unwanted operation is identified as a fault, the cause, severity and location in the plant can be deduced. The traditional protection and control of nuclear plants by measuring variables inside the plant and initialising processes based on predefined rules set up from the design knowledge base - is effective but not without shortcomings. As plants become more complex the predefined protection and control rules become more complex and large safety margins has to be designed into these rules. Information from measurement equipment provides a picture of the plant at any time, but without predefined operational limits, it can not provide any indication of the expected behaviour of the plant. The advancements in processor speeds and the development of sophisticated numerical algorithms allows the simulation of plant processes in real time. The simulator, however, can only predict expected plant behaviour because it is blind to faults that occur in the plant. Combining the information from the measurement equipment with the ability of the simulator to predict what should be happening inside the plant in real time provides a very effective method to address the shortcomings of the existing protection and control philosophies. We use these principles to introduce an Automated Protection Layer (APL) into the existing Control & Protection System of the Nuclear Power Plant.

1. THE MODEL CONTROL & PROTECTION THEORY

The model control & protection theory consists of two parts:

A dynamic operating window around the operating point that moves along with the operating point, this allows tighter control as well as early recognition of unexpected behaviour.
Fault isolation & identification, once unexpected behaviour has been recognised the fault data is isolated from expected transient information and analysed to classify the fault into a category, location, size and cause.

- The Dynamic operating Window

In theory the measured operating point of the nuclear plant should always be predicted exactly by the plant simulator and any variation from the predicted dynamic operating point constitutes faulty behaviour. Taking into account equipment and calculation inaccuracies, the predicted operating point is enlarged to a predicted dynamic operating window around the measured operating point[1].
The following parameters are monitored for direct reactor trips:

- Nuclear flux,
- Coolant temperature ("Tavg" and "ΔT")
- Coolant pressure (pressuriser pressure)
- Pressuriser water level,
- Coolant flow rate and reactor coolant pump breaker position,
- Coolant pump speed,
- Steam generator steam and feedwater flow rates,
- Steam generator water level,

- Operating status of the turbo-alternator set,
- Safety injection, containment spray or Phase B containment isolation.

To allow for start-up, shutdown, and transient conditions different trip set-points apply under different conditions.

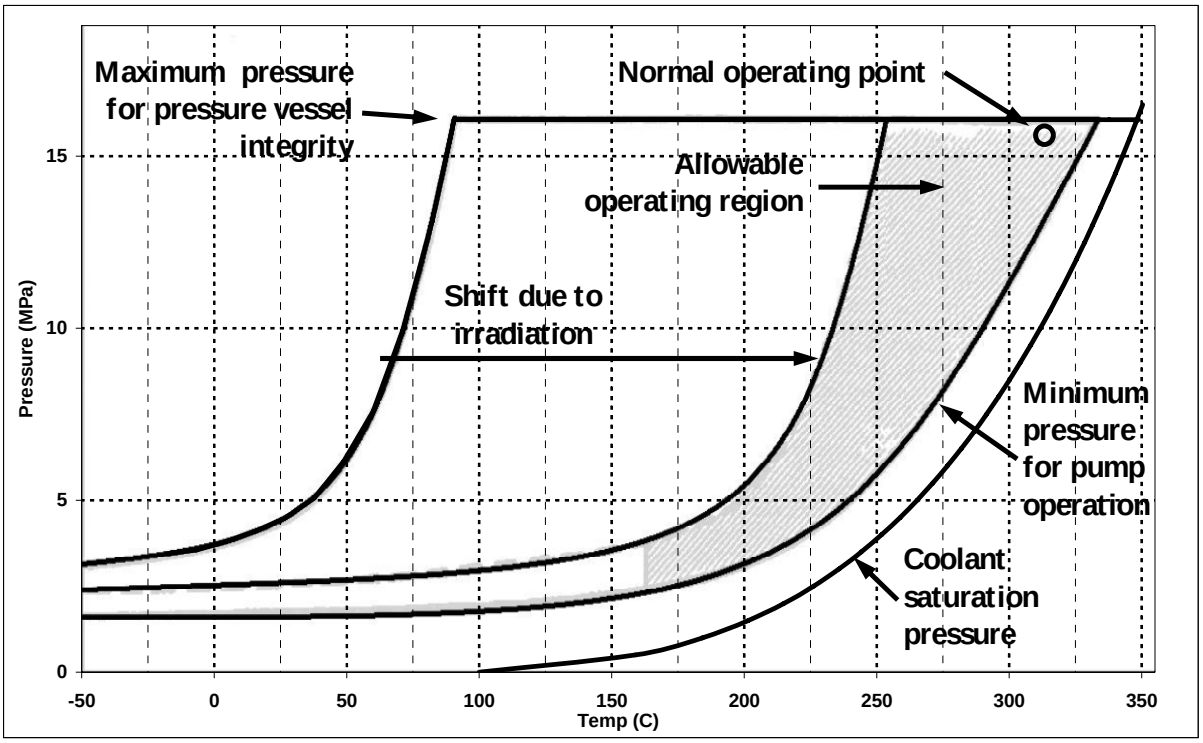

Fig. 1. PWR Pressure Temperature (P-T) Curve

In Figure 1, an example of an operating window with respect to pressure and temperature is shown. These are two very important parameters, since while maintaining the reactor coolant system pressure and temperature within the thermal and structural design specifications, the plant will remain in a safe condition even though a fault might have occurred. This is somewhat counter productive, since the control system is designed specifically to keep the plant within the designed operating window. As such, the effect of faults that would result in the operating point moving outside of the operating window is often hidden and only identified once a secondary effect of the fault is picked up. This is shown in Figure 2, where an expected transient without a fault (Load Change) is compared with the same transient with the added effect of a 50mm2 break in the primary coolant. The effect of the fault is very small and remains within the safe operating window of the plant. The fault is only realised by the system 1 hour after the break occurred. In this case it is picked up by a rise in the reactor building pressure above the predefined setpoint.

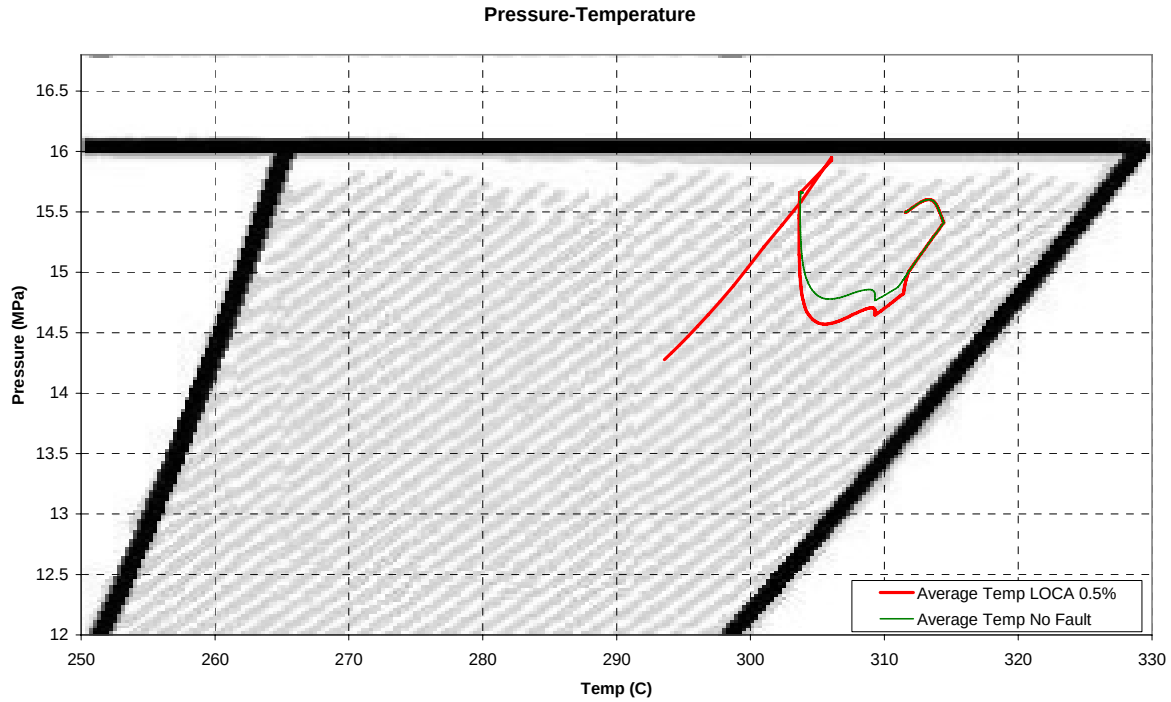

Fig. 2. Load Change (100%-60%) P-T Path

Having a simulator running in real time continually comparing simulated measurements with plant measurements, creates a small dynamic operating window around the operating point. The maximum size of the dynamic operating window in this case is only determined by the maximum error of the measurement equipment and the accuracy of the simulator. Faulty behaviour can be identified as soon as the plant behaviour differs from the predicted behaviour from the simulator. The compared behaviour inlcudes plant measurents as well as plant control data.
If the fault countering effect of the control system can be isolated in the measured data, the difference between the simulated measurements and plant measurements would become more visible with the effect of the fault clearly represented in the data. This way the fault can be identified much earlier than was previously possible.

- FaUlt isolation and identification

As described, to identify any unexpected behaviour we need to be able to devide data received from the plant into expected transient information and unexpected transient information. This is complicated by the fact that the instrumentation inside the plant such as pressuriser heater, pressuriser spray and control rods together with the control system works to maintain the normal operating pressure and temperatures of the reactor coolant system. This is required because ultimitely the safety of the plant relies upon maintaining the reactor coolant system's mechanical integrity and preventing coolant Departure From Nucleate Boiling (DNBR). Unfortunately this also tends to disguise small faults in the plant for a long time such as leaking valves or cracks in one of the steam generator tubes. The plant could essentially operate for very long periods of time with the control system maintaining operating pressure and temperatures despite a leaking reactor coolant system. In Figure 3 a possible solution to this problem is depicted. There are two possible implementations of this solution.

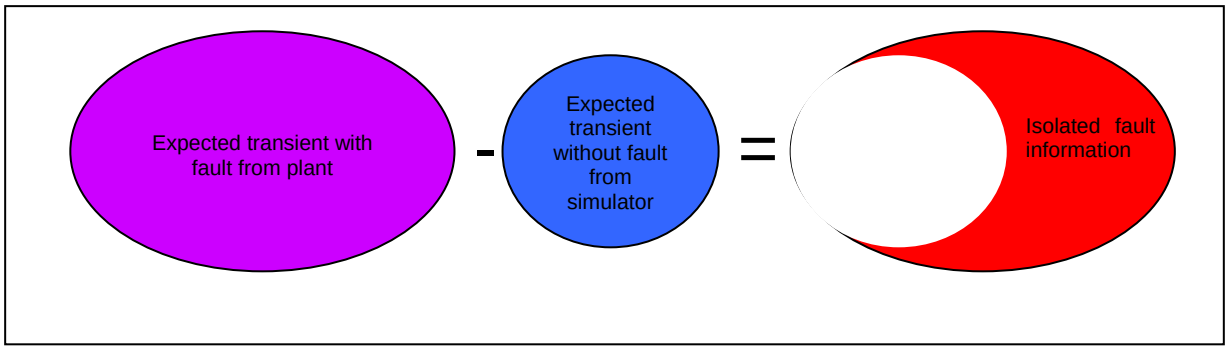

Fig. 3. Concept of isolating fault data from transient data

The one possible implementation is to isolate the fault data is by recording real measured data from the plant, and comparing it with expected real time data from the plant simulator. The difference between the two data sets constitute unexpected plant operation information. This is possible because the real-time simulator only provides information on the expected transient and no information on the fault. The implementation of this solution is difficult since the calculations are not always simple linear subtraction.

The second and more practical method is by comparing the expected operation of the control instrumentation under expected conditions with the actual control instrumentation operation. By then removing the stabilising effect of the control instrumentation from the measured data, results in transient data showing all faulty behaviour without this behaviour being countered by the control system. It should be mentioned that up to this point the the actual plant is operating exactly as it normally would, all fault isolation calculations is made simply from data being fed to the system from the plant. The new transient information can easily be analysed to calculate the type of fault as well as the magnitude.

The effectiveness of our proposed APN system can be shown using the example of a break smaller than the classified small break Loss Of coolant Accident (LOCA). A small break LOCA is defined as a break with an equivalent diameter between 9.5mm and 25mm. A break smaller than 9.5mm translates into a opening smaller than 70,9mm2. When the equivalent diameter of a break is less than 9.5mm, the leakage can be compensated by make-up flow from the Reactor Chemical and Volume Control/Reactor Boron and Water Make-Up system (REA) systems, thereby maintaining the pressuriser level. In this case the fuel cladding is not damaged and only radioactive products normally contained in the primary system are released into the containment. This also means that the plant protection systems remain unaware of the fault for an extended period of time.

In Figure 4, the measured pressure from the plant is depicted together with the calculated pressure if no control systems were to mitigate the pressure drop. The fault occurs after 400 seconds and the fault would normally be detected after 64 minutes of its occurence. The reactor trip is initiated by a Reactor Building High Pressure detection and the mitigating sequence following such a detection. No indication is given as to what the cause of the Reactor Building High Pressure is. This is displayed in Table 1.

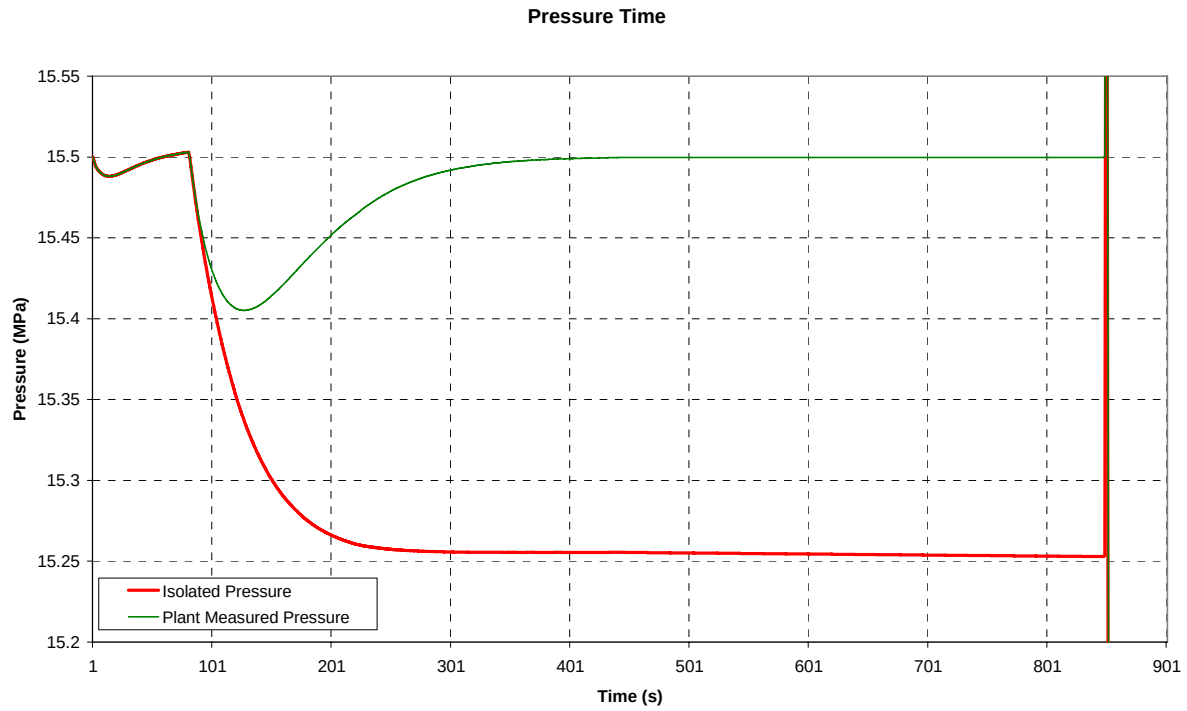

Fig. 4. Steady State operation with a 50mm2 break in the RCS.

In this case is clear that the proportional heater is used to keep the primary pressure at 15.5MPa. This is achieved and importantly – also required – since it prevents the coolant from entering DNBR. However, were the heater only to act upon expected transients, which in this case does not occur, a clear pressure drop would be seen that would act as an indicator of the fault type and magnitude. The faulty behaviour could be recognised the moment the positive effect of the heater can be measured.

Table 1. Sequence of events after a 7.97mm break in the primary coolant circuit.

000000.0 sec	PZR Proportional Heater Capacity Change: 0%
000293.0 sec	PZR Proportional Heater Capacity Change: 0%
000401.0 sec	Malfunction # 2 Fraction = 00.5 %
000405.5 sec	PZR Proportional Heater Capacity Change: 0%
004238.5 sec	HPSI start high RB Press 0.13 MPa
004238.5 sec	HPI Pump #1 Position Change: 100%
004238.5 sec	HPI Pump #2 Position Change: 100%
004238.5 sec	Letdown Valve #1 Position Change: 0%
004238.5 sec	HPI Pump #3 Position Change: 0%
004238.5 sec	Ctmt Vent Valve #1 Position Change: 0%
004238.5 sec	RBS Pump #1 Position Change: 100%
004238.5 sec	Ctmt Spray Starts 1.3 kg/cm2
004239.0 sec	Letdown Valve #1 Position Change: 100%
004239.5 sec	Reactor Scram

In the case of the Figure 4 example, the rate of change of the measured pressure becomes positive after 640 seconds, 240 seconds after the fault occurred. After this time the positive effect of the heater outweighs the negative effect of the fault. Since the unexpected heater effect can be removed from the measured data it is clear that the plant is losing pressure due to an unexpected cause. This would alert the operator of the fault within 4 minutes, 60 minutes earlier than would be the case in existing systems.

Combining the isolated fault information from various measurements inside the plant and correlating this information with various pre-simulated faults identifies the fault with an increasing level of certainty as the fault effects unfold over time and this information becomes available to the real time system. The following sequence is followed:
The system identifies that the plant measurements do not correspond to expected measurements
The system identifies the control system is operating different from expected.
The effect of the unexpected control system operation is isolated, to show the "true" faulty behaviour.
The fault is categorised by matching the behaviour with known behaviour of certain fault categories.
The fault is identified by following behaviour trend of a number of measured variables.
The position of the fault is identified by triangulating the measurement equipment that indicated the fault first.
The magnitude of the fault is calculated from rate of change in the time domain.

In Figure 5 and Table 2, the same fault as previously is depicted. This time the fault occurs during a load reduction transient. During such a transient it would be much more difficult to recognise faulty measurements since it looks very similar to the expected transient.

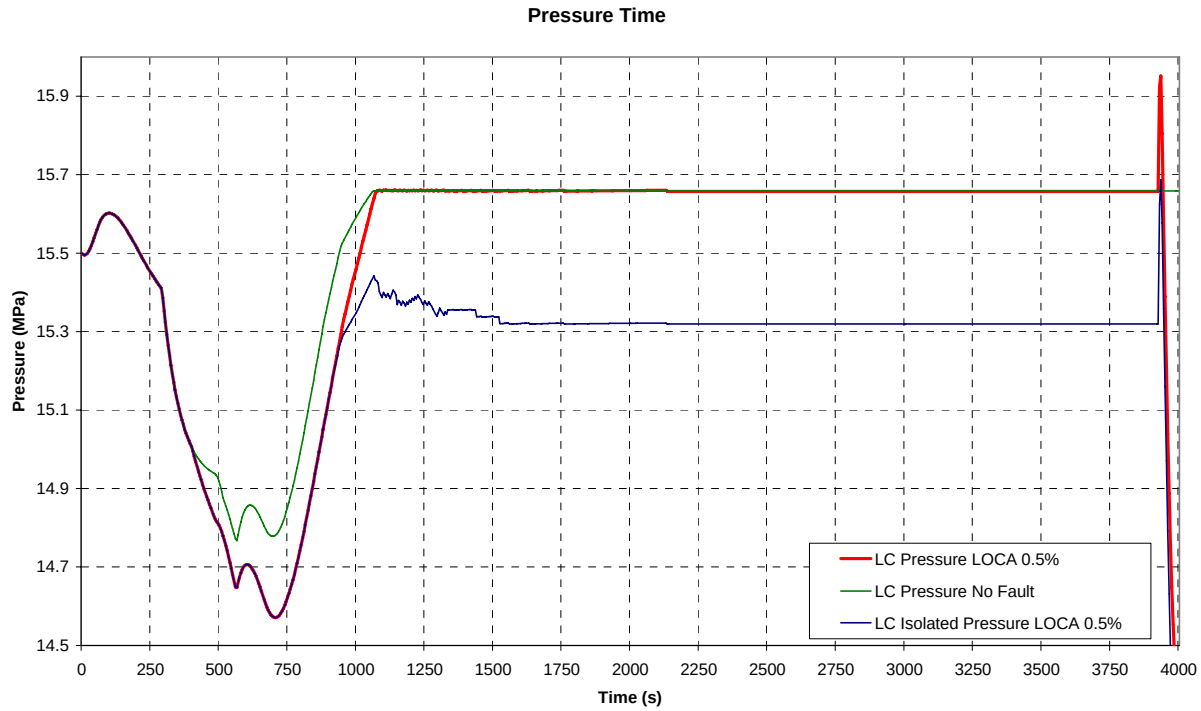

Fig. 5. Transient operation with a 50mm2 break in the RCS

Again, the proportional heater is used to keep the primary pressure at 15.5MPa. This is achieved and required since it prevents the coolant from entering DNBR. However, were the heater only to act upon the expected transient – load change, a clear pressure drop would be seen that would act as an indicator of the fault type and magnitude. The faulty behaviour could be recognised the moment the positive effect of the heater can be measured.

Table 2. Sequence of events after a 7.97mm primary coolant circuit break, during load change.

000000.0 sec	PZR Proportional Heater Capacity Change: 0%
000293.0 sec	PZR Proportional Heater Capacity Change: 0%
000401.0 sec	Malfunction # 2 Fraction = 00.5 %
000405.5 sec	PZR Proportional Heater Capacity Change: 0%
003924.0 sec	Ctmt Spray Starts 1.3 kg/cm2
003924.5 sec	Letdown Valve #1 Position Change: 100%

003925.0 sec	Reactor Scram
003924.0 sec	Ctmt Spray Starts 1.3 kg/cm2
003924.5 sec	Letdown Valve #1 Position Change: 100%
003925.0 sec	Reactor Scram

In the case of the Figure 5 example, the added effect of the heater on the fault is not recognised at first because the heater is operating at full capacity to stabilise the effect of the expected transient. This is an extreme example where the load change occurs at the maximum rate the plant is designed for. The heater however, is expected to proportionally decrease capacity as the transient is stabilised, during this time the unexpected effect of the heater can be detected and removed from the expected effects.
The rate of change of the measured pressure does become positive after 1100 seconds, 700 seconds after the fault occurred. After this time the positive effect of the heater outweighs the negative effect of the fault and the pressuriser spray. Since the unexpected heater and spray effect can be removed from the measured data once the heater is not expected to be running at full capacity it is clear that the plant is losing pressure due to an unexpected cause. This would alert the operator of the fault within 11 minutes 40 seconds, 47 minutes earlier than would be the case in existing systems.

- Automated protection layer (APL) Implementation

One of the most important aspects to keep in mind during the development of any technology to be used in a nuclear power plant is to do all development in line with the nuclear regulator requirements. This importance increases if the technology would have an impact on the protection systems of the plant. History has proven that an evolutionary approach to introducing new technologies in the nuclear industry is more effective and easier to licence. With this in mind a few important statements should be made regarding the design philosophy that will be followed during the development of the Model Reference Control & Protection Theory and subsequent implementation of the APL.

In order to keep the safety systems of a nuclear plant as robust as possible it is required that they are designed as simple as possible. This system consist of a limited number of critical measurement instruments coupled with specific operating limits, where once outside these operating limits the plant is considered unsafe[2]. This system is generally kept independent from the plant control system. An illustration of such a system is depicted in Figure 6. The control system on the other hand usually operates in distributed fashion, looking after specific modules of the plant to be controlled. Keeping these systems separate is a very important and non-negotiable aspect of the safety philosophy[3]. However, the distributed control systems encapsulate a lot of important information about the health of the plant and should therefore be utilized to provide fault precursors long before the plant protection system identifies unsafe plant conditions.

In Figure 6 the integration of the Automated Protection Layer (APL) can be seen. The integration is done in such a way that it can, in no way compromise the protection system, but can provide early warning signals on plant operation moving outside the expected parameters. It should be proven that this system will in all cases provide at least the same fault information, earlier or at least at the same time as the conventional protection system.

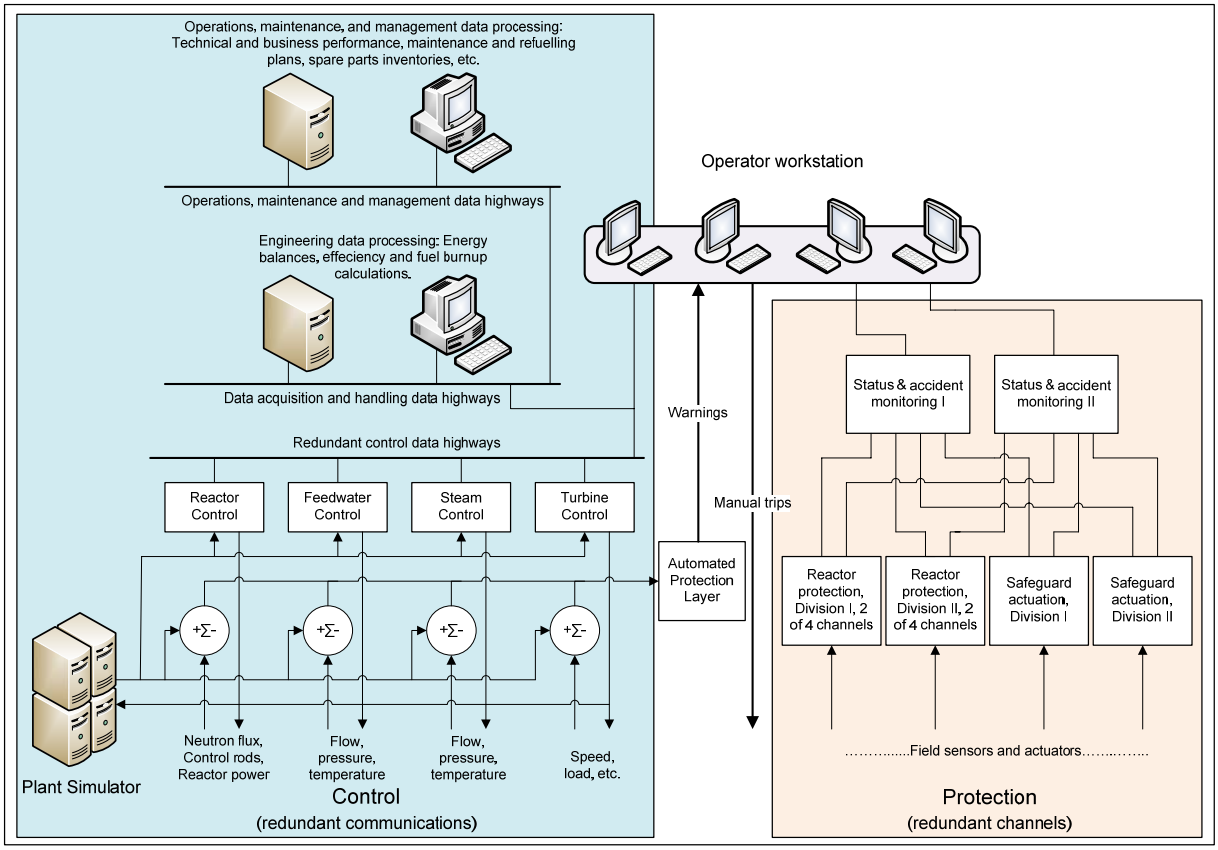

Fig. 6. Implementation of the Automated Protection Layer

It is clear that, although the APL will be able to use information originating from all control equipment to flag possible fault conditions in the plant, it would in no way be possible for the APL to impact negatively on the primary protections system of the plant as licensed by the nuclear regulating authorities. In this case the APL can be implemented to piggy-back on existing nuclear plant control system as an early warning system.

The APL Human Machine Interface (HMI) should be implemented in such a manner as being unobtrusive to controllers but still highlighting unexpected behaviour and – during system stabalising procedures – direct the controllers to possible fault causes to prevent mistakingly identifying a wrong fault cause and following the wrong procedure.

REFERENCES

[1] WESTINGHOUSE, PWR Course Manual, Vol 6B.

[2] JEFFERY LEWINS, 1978, Nuclear Reactor Kinetics & Control, Pergamon Press, London. England.

[3] COMMITTEE ON APPLICATION OF DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS TO NUCLEAR POWER PLANT OPERATIONS AND SAFETY, 1997, Digital Instrumentation and Control Systems in Nuclear Power Plants, National Academy Press, Washington, D.C. USA.

[4] FINC, P, ET AL, 2006, WORKSHOP ON SIMULATION AND MODELLING FOR ADVANCED NUCLEAR ENERGY SYSTEMS, Office of Nuclear Energy, Office of Advanced Scientific Computing Research, U.S. Department of Energy, Washington. D.C. USA.