This publication has been superseded by SSG-39

— the worst permissible configuration of safety systems performing the necessary safety function is assumed, with account taken of maintenance, testing, inspection and repair, and allowable equipment outage times.

Spurious actuation should be considered as a mode of failure when applying the concept. At no time is more than one failure assumed to occur.

Application of the single failure criterion to I&C systems important to safety

4.17. To interpret the single failure criterion as defined in the Requirements for Design, the criterion shall be applied to each safety group incorporated in the plant design. 'Safety group' is defined as that assembly of equipment (frequently referred to as a 'train') which performs all actions required after a PIE in order that the limits specified in the design basis for that event are not exceeded (Ref. [1], para. 5.34).

4.18. For those I&C systems to which the criterion is to be applied, the intended safety functions of the systems should first be identified, as well as the safety group needed to fulfil these functions. This identification should also include all other systems associated with an I&C system whose failure could influence the system's defined safety functions. When the relevant safety group has been identified, the following analysis should be performed:

— PIEs in the design basis which are relevant for the intended safety functions should be identified. The probabilities of occurrence of the PIEs should be determined. If they are credible, the consequential effects of the PIEs should be determined.
— The safety functions, safety systems and supporting features that are required to cope with the PIEs (such as control rod insertion or closing of containment isolation valves) should be determined. These should include alternative 'success paths' through which the safety functions could be fulfilled.
— A single failure should be assumed in the system, and the consequences of the single failure should be determined.
— It should be shown that the safety functions can still be performed.
— In determining the consequences, compliance with the requirements for independence within safety groups (Ref. [1], para. II.11) should be established. The process should include verification that safety groups have no shared equipment or points of vulnerability, as far as practicable.
— If the independent redundancies and trains of the required systems have been identified as being single failure proof, the systems do not need further detailed analysis for potential failures under the single failure criterion.

This publication has been superseded by SSG-39

— If in exceptional cases the single failure criterion is not met, then the design is modified to meet the criterion or, if justifiable, an exemption is established. It should then be ensured that the reliability of the systems is maintained at a very high level by proper in-service inspection, maintenance and operating procedures so as to render their failure in service non-credible.
— If a single failure could preclude adequate reliability of a safety system, it should be ensured that other systems are available to prevent unacceptable consequences.
— In the application of the single failure criterion, the detectability of failures is implicitly assumed. However, there may be failures which are not detected by testing or revealed by alarms or anomalous indications. The systems should be analysed for such undetected failures. The preferred course would be to redesign the system or the test schemes to make the failures easily detectable. If this is not possible, it should be assumed that such undetected failures have occurred and then a single failure should be assumed in addition. It should be ensured that safety functions can be performed under these circumstances.
— Operator actions prescribed for the event sequences of concern should be identified. The consequential effects of incorrect or omitted single random prescribed actions by the operator should be analysed. It should be ensured that under these circumstances the safety functions will be performed.
— In some Member States, the single failure criterion is not applied when one of the redundant trains is out of service owing to testing or maintenance. In such cases, the allowable out of service times that ensure the required reliability should be determined.
— Common cause failures are normally not included in the analysis. Credible common cause failures should be assessed separately, by either deterministic measures or probabilistic safety analysis, or a combination of both. Sufficient independence and diversity should be incorporated to provide reasonable assurance that safety functions can be performed in the event of common cause failures.

4.19. While certain components of I&C systems (cables, printed circuit boards or cabinets) may be considered to be passive, it is seldom necessary or possible to use this provision effectively to relax the single failure analysis.

4.20. Non-compliance with the single failure criterion may be justified for:

— very rare PIEs;
— very improbable consequences of PIEs;
— withdrawal from service of certain components for purposes of maintenance, repair or periodic testing, for limited periods of time;

This publication has been superseded by SSG-39

— features that prevent or mitigate severe accidents; and
— components whose likelihood of failure can be shown to be sufficiently remote as to be discounted.

4.21. Additional guidance on the application of the single failure criterion and strategies for achieving compliance can be found in Ref. [5].

Redundancy

4.22. Redundancy is commonly used in I&C systems important to safety to achieve system reliability goals and/or conformity with the single failure criterion. For redundancy to be fully effective, there should be independence (see paras 4.36–4.48). Taken alone, redundancy increases the reliability of safety actions or safety related actions, but it also increases the probability of spurious operation. Coincidence of redundant signals for equipment or a rejection scheme for spurious signals that is based on intercomparisons of the redundant signals is commonly used to obtain an appropriate balance of reliability and freedom from spurious operation.

Diversity

4.23. Diversity in I&C systems is the principle of monitoring different parameters, using different technologies, different logic or algorithms, or different means of actuation in order to provide several ways of detecting and responding to a significant event. Diversity provides defence against common cause failures, is complementary to the principle of defence in depth and increases the chance that safety tasks will be performed when necessary. Defences at different levels of depth may also be diverse from each other. Types of diversity that may be considered include human diversity, design diversity, software diversity, functional diversity, signal diversity, equipment diversity and system diversity.

4.24. Additional conservatism should be provided where the necessary demonstration of system reliability is not feasible, e.g. where the reliability of a multiple redundant system will be limited by such factors as common cause failures or uncertainties in the design. Specific difficulties may arise in demonstrating the reliability of computer based systems, for example. Diversity is a way to include conservatism in order to compensate for the difficulty of demonstrating the necessary level of reliability.

4.25. The adequacy of the diversity provided with respect to the above criteria should be justified. Both the scope and the type of the diversity should be considered. Achieving the desired level of conservatism may not necessitate extending the scope

This publication has been superseded by SSG-39

of diversity to cover very unlikely PIEs or low consequence PIEs, since the risk of such events may be acceptable despite the possibility of common cause failure.

4.26. Several types of diversity should typically exist. Functional diversity (systems providing different physical functions that have overlapping safety effects) and signal diversity (the use of different monitored parameters to initiate protective action) can also be particularly effective.

4.27. In any application, care should be exercised to ensure that diversity is in fact achieved in the implemented design and preserved throughout the life of the plant. The designer should actively review the design to avoid areas of potential commonality in the application of diversity, such as materials, components, similar manufacturing processes, similar software or subtle similarities in operating principles or common support features.

4.28. The justification for equipment diversity, or for the diversity of related I&C system software such as a real time operating system, should extend to the equipment's components to ensure that actual diversity exists. For example, different manufacturers might use the same processor or license the same operating system, thereby potentially incorporating common failure modes. Claims for diversity based only on a difference in manufacturers' names are insufficient without consideration of this possibility.

4.29. With regard to the diversity of software, experience indicates that independence of failure modes may not be achieved if multiple versions of software are developed to the same software requirements specification. In particular, it is possible that independently developed versions of programs may have common cause failures. Incorporating types of diversity such as functional diversity and signal diversity may be most effective in dealing with this limitation.

4.30. Extended application of concepts such as redundancy, diversity, use of proven equipment, testability, continuous monitoring and maintainability is employed to achieve an additional increment of reliability above the level achieved by meeting the single failure criterion alone.

4.31. In some Member States, reliability requirements have been placed on the protection system in addition to the single failure criterion. This additional reliability is sometimes achieved by using double failure protection in parts of the protection system and/or by using equipment with a wider design margin. In some Member States an overall numerical reliability goal is established, and analytical methods and tests are used to verify that the protection system meets this goal.

This publication has been superseded by SSG-39

Reliability assessment

4.32. For all systems important to safety, the degree of redundancy, diversity, testability and robustness should be justified as being adequate to achieve the required reliability of the safety functions to be performed by the systems. This demonstration may be based on a balance of deterministic criteria and quantitative reliability analysis.

4.33. In the assessment of the reliability of digital I&C systems, the effects of possible hardware and software failures should be considered, as well as the design features provided to prevent or to limit their effects. Hardware failure conditions to be considered should include failures of parts of the computer itself and failures of parts of communication systems. Both permanent failures and transient failures should be considered.

4.34. The contribution of component failure to an I&C system's unavailability should be determined to an appropriate degree of confidence, e.g. by a specified confidence level when a probabilistic approach is used.

Software reliability

4.35. Software faults are systematic faults caused by design errors and therefore do not have the random failure behaviour assumed in the analysis of hardware reliability. Consequently, different methods may be necessary to assess the unreliability introduced by hardware and by software. For example, the reliability of computer based systems may be demonstrated on the basis of a qualitative evaluation, with account taken of the complexity of the design, the quality of the verification, validation and testing of the development process over a wide range of input conditions, and the feedback of operating experience.

INDEPENDENCE

4.36. Independence prevents: (1) propagation of failures from system to system or (2) propagation of failures between redundant parts within systems, and (3) common cause failures due to common internal plant hazards. Independence is also important to ensure that the redundancy and diversity provided to ensure high reliability of systems important to safety are effective.

4.37. Independence should be considered to prevent the propagation of failures:

— between or among system components as a consequence of PIEs;

This publication has been superseded by SSG-39

— between or among systems of the same safety importance; and
— from systems of lower importance to systems of higher importance to safety.

4.38. Safety systems should be independent of safety related and non-safety systems. Systems of lower safety importance may be associated with a safety system, provided that independence is maintained between these systems and that the independence of redundant safety groups is not degraded.

4.39. Redundant safety groups within I&C systems important to safety should be independent of each other.

4.40. Independence should be provided between redundant parts of safety related systems.

4.41. Appropriate independence should be provided between diverse functions. The adequacy of the independence provided should be justified.

4.42. Independence is achieved by means of electrical isolation, physical separation and independence of communications between systems.

4.43. Electrical isolation is required to control or prevent adverse interactions between equipment and components caused by factors such as electromagnetic interference, electrostatic pick-up, short circuits, open circuits, earthing, application of the maximum credible voltage (alternating or direct current) and mechanical interaction. Examples of provisions for electrical isolation are electrical and optical isolating devices, cable shielding, internal mechanical structures or similar devices. When isolation devices are used between systems of different safety importance, they should be associated with the system of higher importance.

4.44. No credible failure on the non-safety side of an isolation device should prevent any portion of a safety system from meeting its minimum performance requirements during and following any PIE which requires that safety function to be performed.

4.45. Physical separation of systems from each other is achieved by distance, barriers, or a combination of the two, and can be used to reduce the likelihood of common cause failures resulting from failures as consequences of PIEs (such as fire, missile, flooding or high energy pipe break). This physical separation additionally reduces the likelihood of inadvertent errors of commission during operation or maintenance occurring in more than one part of these systems.

This publication has been superseded by SSG-39

4.46. The choice of physical separation by distance, barriers or their combination may differ from location to location within the nuclear power plant. It will depend on the need to provide protection against all the PIEs considered in the design basis, including the effects of fire, chemical explosion, aircraft strikes and missiles. References [6–9] provide additional guidance.

4.47. Certain areas in the plant tend to become natural centres of convergence for redundant equipment or wiring. In these areas the extent to which independence might be lost after certain PIEs should be carefully ascertained as a basis for establishing an overall design that meets the reliability requirements and goals. Examples of such centres include containment penetrations, motor control centres, switchgear areas, cable spreading rooms, equipment rooms, the control room and the plant process computer.

4.48. Communications independence is relevant only to designs that incorporate data communications. Communications independence is achieved by selecting system architectures and data communication protocols such that a logical or software malfunction in one system cannot adversely affect the connected systems. Communications independence is achieved by means of adequate arrangements for the buffering of data (including any hardware logic and/or software logic used to support data switching, detection and correction of transmission errors, flow control or transmission control, or protocol handling) such that any malfunctions in sending and receiving modules will not impair the functioning of the processing modules.

FAILURE MODES

4.49. Designing in such a way that failures result in known failure modes is one method of accommodating expected failures of systems or components. Failures should produce not only predictable failure modes but also failure modes that place the system in a safe state. The Requirements for Design require that the principle of fail-safe design be considered and incorporated as appropriate into the design of plant systems and components important to safety (Ref. [1], para. 5.40).

4.50. To facilitate the overall design of safety systems, equipment should as far as practicable exhibit a predictable and revealed mode of failure. The more probable modes of failure in a system important to safety should as far as practicable place the system in a safe state. Consideration should be given to incorporating fail-safe features such as ‘de-energize to trip’ or ‘watchdog timers’ into the design of I&C systems (Ref. [1], para. 5.40). However, where such practice is applied, it does not eliminate the need to meet safety requirements for failures that can occur in the fail-safe design feature itself.

This publication has been superseded by SSG-39

CONTROL OF ACCESS TO EQUIPMENT

4.51. Access to equipment in systems important to safety should be appropriately limited, in view of the need to prevent both unauthorized access and the possibility of error by authorized personnel. Effective methods include appropriate combinations of physical security (locked enclosures, locked rooms, alarms on panel doors) and administrative measures according to the degree of supervision in the area where the equipment is located.

4.52. Two areas of concern in relation to access control are set point adjustments and calibration adjustments, because of their importance in preventing degraded system performance due to potential errors in operation or maintenance.

4.53. For access control to digital computer based systems, means should be employed for restricting electronic access to software and data. These restrictions should be applied to access via network connections and maintenance equipment.

SET POINTS

4.54. The nuclear power plant shall be designed to operate safely within defined ranges of parameters such that the radiological risk to the public and the environment is within the regulatory limits (Ref. [1], para. 5.24). The plant state should change in response to initiating events, but the plant may approach a state that is outside the envelope of safe operation. Certain systems important to safety actuate to effect the necessary actions to return the plant to a safe state. These systems actuate when a monitored variable reaches a predetermined set point.

4.55. For a given monitored variable (e.g. primary circuit pressure, containment pressure) or calculated variable (e.g. reactor power, critical heat flux ratio), a safety limit is established on the basis of safety criteria. This limit should be that value of the variable beyond which unacceptable safety consequences are expected to occur (see Fig. 2).

4.56. The analysis limit[1] is a theoretical value derived from the safety analysis. The safety analysis should demonstrate that, following an initiating event, the safety limit

[1] The analysis limit is a theoretical value derived from the safety analysis such that if, following an initiating event, mitigatory action starts at the analysis limit, the safety limit will not be reached.

This publication has been superseded by SSG-39

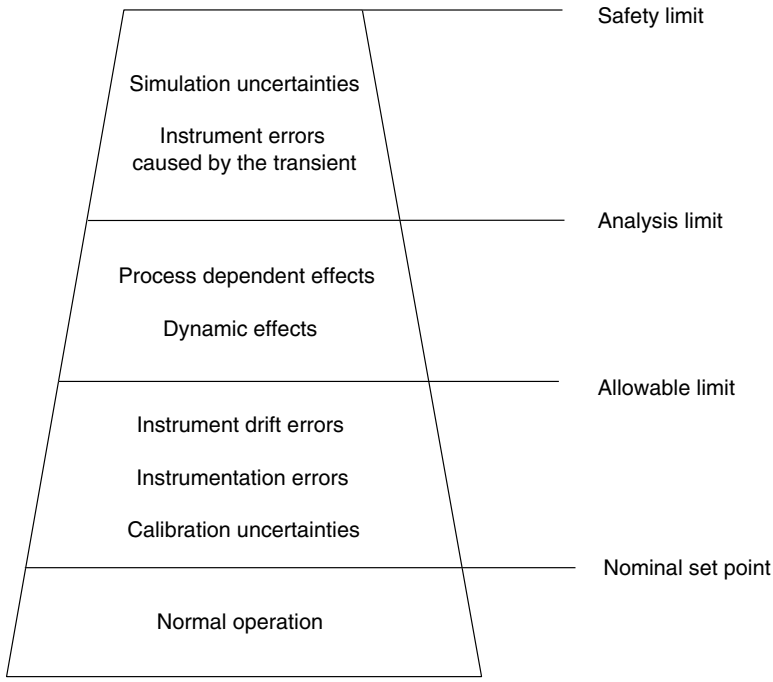

FIG. 2. Example of the relationship between set points and limits.

will not be reached if mitigating action commences at the analysis limit. This analysis assumes availability of the 'as designed' configuration of systems and equipment and appropriately postulated failures. Therefore, the difference between the safety limit and the analytical limit will take into account the uncertainties in simulation and the potential errors in the behaviour of instruments caused by the transient.

4.57. The nominal set point is the value at which the trip function is set. The margin between the nominal set point and the analysis limit should be such that the mitigating action is completed before the analysis limit is reached.

4.58. The 'allowable limit' is used for instruments that require periodic testing and surveillance. The margin between the allowable limit and the nominal set point comprises random uncertainties in instrument calibration, random instrument errors and errors due to instrument drift. If a set point is found to be beyond the allowable limit, immediate corrective action should be taken.

This publication has been superseded by SSG-39

4.59. The bases for nominal set points and allowable limits should be documented and justified.

4.60. In some cases the monitored variable is not identical with the variable used to specify a safety limit. Examples of such cases are:

— The peak cladding temperature for the fuel after a loss of coolant accident which is not monitored. The pressure of the reactor coolant is monitored instead, since decreasing pressure might be an indicator of an accident that would threaten the integrity of the fuel.
— Axial neutron flux, temperatures of hot and cold legs and primary circuit pressure are monitored in a pressurized water reactor, since together they can provide an indication of departure from nucleate boiling, which cannot be measured directly.

HUMAN–MACHINE INTERFACE

4.61. Effective human–machine interfaces for systems important to safety are necessary to provide the operator with accurate, complete and timely information on plant status and to enable proper operation of the systems controlled by the I&C systems. The Requirements for Design require that systematic consideration of human factors and the human–machine interface be included in the design process (Ref. [1], para. 5.50). The human–machine interface for I&C systems important to safety should conform to the guidance given in Section 6 of this Safety Guide.

EQUIPMENT QUALIFICATION

4.62. It should be ensured that the systems important to safety are capable of performing their safety functions when required in normal operations, external events and anticipated operational conditions, and in and after design basis accident conditions. This is fundamental to preventing the release of radioactive materials and to preventing or mitigating radiological consequences for human health and the environment if it occurs.

4.63. Examples of hazardous environmental conditions arising from design basis accident conditions which could cause failure of equipment are the radiological conditions and steam conditions associated with pipe breaks, including breaks of the reactor coolant system. Examples of potentially hazardous process conditions include high velocity two phase flow, high levels of vibration or debris laden process

This publication has been superseded by SSG-39

fluids. In addition to potentially hazardous process events, effects such as overheating, electromagnetic interference, electrostatic discharge and variations in power supply, which also have the potential to cause common cause failures, should be considered.

4.64. The Requirements for Design require a qualification procedure to confirm that the equipment is capable of meeting, throughout its design operational life, the requirements for performing safety functions while being subject to the environmental conditions (vibration, temperature, pressure, jet impingement, electromagnetic interference, radiation, humidity or any likely combination thereof) that may prevail at the time it is needed (Ref. [1], para. 5.45). Qualification is the process of identifying hazards in the environment in which the equipment may be operating and conducting a programme of tests and/or analyses to determine and document whether the equipment can satisfactorily perform its safety function under the specified service conditions. Qualification is one method of minimizing the possibility of environmental events or effects inducing a common cause failure of the equipment.

4.65. Equipment qualification should demonstrate that the equipment is capable of functioning under environmental and operational conditions. The following recommendations, while specific to the design of systems important to safety, should be applied in conjunction with other guidance provided on qualification, e.g. Ref. [10].

Equipment qualification programme

4.66. A qualification programme should be completed to confirm that equipment important to safety will be capable of meeting, until the end of its design life, the design basis performance requirements (such as range, accuracy and response) for the assigned safety task, under the environmental conditions (such as temperature, pressure, radiation, humidity or caustic sprays) likely to prevail at the time the equipment will be needed.

4.67. These environmental conditions should include the expected combinations of conditions for normal operation, during anticipated operational occurrences, and during and after design basis accidents. Consideration of severe accident conditions is not required in the equipment qualification programme. However, equipment credited for response to severe accidents should be shown, with reasonable confidence and to the extent possible, to function under anticipated severe accident conditions (Ref. [1], para. 5.46).

4.68. Where the equipment is subject to external events such as natural phenomena or other external influences, and is required to perform its safety task during or

This publication has been superseded by SSG-39

following such an event, the qualification programme should include the conditions imposed on the equipment by this external event. In addition, any unusual environmental conditions that can reasonably be anticipated and that could arise from specific operating conditions, e.g. conditions that would occur during periodic testing of the leak rate for the containment, should be included in the qualification programme.

4.69. The programme should include a plan to ensure that the equipment is qualified for the intended period of use, and to provide for timely requalification or replacement, if necessary. Consideration should be given to the combined effects of various environmental factors and to the integrated effect of the normal ambient environmental factors over the installed life of the equipment. Further conservatism should be provided, where appropriate, to allow for unanticipated ageing mechanisms. Appropriate provision should be made for monitoring, testing and inspection of the plant equipment in order to identify unanticipated behaviour or degradation (Ref. [1], para. 5.47).

4.70. In the qualification of safety system equipment, preferably an entire piece of equipment should be qualified rather than only those portions directly related to the safety task under consideration.

Methods of qualification

4.71. An appropriate combination of the following methods of qualification should be used in order to meet the aforementioned objectives:

— performance of tests on the type of equipment to be supplied;
— performance of tests on the actual equipment supplied;
— consideration of pertinent past experience in similar applications; and/or
— analysis on the basis of reasonable engineering extrapolation of test data or operating experience under pertinent conditions.

4.72. The chosen method of qualification should provide a degree of confidence commensurate with the equipment's importance to the safety of the system, as described in Section 2. Testing should be conducted for equipment qualification and should be performed whenever practical for safety equipment.

4.73. When protective barriers are provided to isolate equipment from possible environmental effects, the barriers themselves should be subject to a qualification programme to validate their adequacy.

This publication has been superseded by SSG-39

QUALITY

4.74. High quality of design and manufacturing is necessary to ensure that systems important to safety can be demonstrated to meet their safety requirements. Design and manufacturing in accordance with appropriate quality levels are important elements in achieving the requirement established in Ref. [1], para. 5.1.

4.75. Components and modules of systems important to safety should be of a quality that is consistent with the aim of minimizing maintenance needs and failure rates.

4.76. Equipment selected for systems important to safety should be of a proven design whenever possible, should be consistent with the reliability goals, and should facilitate meeting the requirements for calibration, testing, maintenance and repair. In the selection of equipment, consideration should be given to both spurious operation and unsafe failure modes, e.g. failure to trip when required.

DESIGN FOR ELECTROMAGNETIC COMPATIBILITY

4.77. I&C equipment and systems, including associated cables, should be designed and installed so as to withstand the electromagnetic environment in nuclear power plants.

4.78. Appropriate provisions for the grounding, shielding and decoupling of interference should be made in the design. Practices for installation and maintenance should be adequate to ensure that these provisions are appropriately implemented in installation and maintenance. Reference [11] gives additional guidance on grounding. Reference [4] provides examples of typical practices for grounding and shielding.

TESTING AND TESTABILITY

4.79. In-service testing provides assurance that the systems important to safety remain operable and capable of performing their safety tasks. The frequency of tests should be established on the basis of the requirements for availability and reliability of the system. Testability — the ability of a system to be tested — should be built in as part of the design. In designing a testable system, it should be considered whether: (1) the location of the equipment is appropriate, (2) access is suitably controlled, (3) faults in the equipment are readily detectable, and (4) the demonstration of continued functionality is conducted in such a way that the safety of the operating plant is not jeopardized.

This publication has been superseded by SSG-39

4.80. Testability is a necessary part of the design both for the system reliability described in paras 5.32–5.42 of the Requirements for Design and for the in-service testing, inspection and monitoring required in paras 5.43–5.44 of the Requirements for Design. In addition, the protection system should meet the special requirements for reliability and testability described in paras 6.81–6.84 of the Requirements for Design.

Test programme

4.81. The design of I&C systems important to safety should include identification of a testing and calibration programme consistent with their availability requirements.

4.82. This test programme should ensure that the functional capabilities of systems and components important to safety are retained. This should include periodic confirmation that design basis requirements such as those for accuracy, response time and set points are met.

4.83. As far as practicable, tests for I&C systems important to safety should be overall checks (from the sensors to the actuators), capable of being performed in situ and with a minimum of effort. It is acceptable for the test programme to consist of overlapping tests which together test the whole channel. All the output functions important to safety, such as alarms, control actions and operation of actuation devices, should be tested.

Test provisions

4.84. All systems important to safety should include provisions that allow performance of the required testing, including built-in test facilities where appropriate. These should themselves be capable of being checked at regular intervals to ensure continued correct operation. Where equipment to be tested cannot be located in non-hazardous areas, facilities should be provided to allow testing to be conducted remotely from outside the hazardous area.

4.85. Where test facilities are provided, the design should ensure that the system cannot inadvertently be left in a test configuration. Where installed test facilities are provided for periodic testing, the interfaces should be subject to hardware interlocking to ensure that interaction with the test system is not possible without deliberate manual intervention.

4.86. For safety systems, the test method should ideally involve a single on-line test for each function, encompassing all components from the sensors to the actuators.

This publication has been superseded by SSG-39

However, such tests are not always practicable. In such circumstances, the test programme should combine on-line (operational states in which the safety function is or may be required) and off-line (operational states in which the safety function is not required) tests in a series of overlapping test steps, to the extent necessary to achieve the test objectives. Adequacy of the use of overlapping test steps should be demonstrated.

4.87. The design of the safety systems and their test provisions should ensure the safety of the plant during the actual testing, and ideally should minimize spurious initiation of any safety action and any other adverse effect of the tests on the availability of the plant. Conduct of the test programme should not cause deterioration of any plant component beyond that provided for in the design.

Fault detection

4.88. The provisions for periodic testing should provide objective information on system status and should, where appropriate, furnish data on trends to assist in detecting degradation of the system and those conditions that indicate incipient failure within the system. As far as practicable, the design of systems important to safety should employ self-checking features. However, the provision of self-checking features should be balanced by the need for simplicity.

4.89. To the extent practicable, each measured variable sensor should be individually tested, by, for example:

— perturbing the monitored variable;
— introducing and varying, as appropriate, a substitute input to the sensor that is of the same nature as the measured variable; or
— cross-checking between variables that bear a known relationship to each other and for which readouts are available.

4.90. The tests required should detect faults in the safety systems from the sensors to the actuators. The tests should be capable of detecting faults in each redundant part of these systems. Where redundant equipment is provided in a channel, the tests should verify the operability of each redundant part.

Demonstration of system performance

4.91. The selected periodic tests and provisions for calibration should be such that the performance characteristics specified in the design basis for redundant channels in the protection system, the safety actuation systems and the support features for the safety

This publication has been superseded by SSG-39

system can be confirmed. Testing and calibration should generally be performed at different periodic intervals.

4.92. Where combinations of variables are used to generate a particular signal for the protection system, all variables used should be tested and calibrated.

Removal from service

4.93. Where the need for thoroughness of the periodic tests is in conflict with the reliability of the safety group (e.g. where a channel has been removed from service for testing and yet must be properly restored to service for safety), the test method should ensure that both objectives are satisfactorily achieved. For example, when a sensor has been removed from service for a periodic test, visual cross-checking with the redundant sensors (or other equivalent means) should be used to verify its subsequent restoration to service. In addition, the status of items that were disturbed to accommodate the periodic test (e.g. instrument root valve position, maintenance bypasses) should be verified to ensure their return to the original operating state. Adequate attention should be paid in this context to possible human error.

4.94. In the design of safety systems it should be ensured that, when periodic tests are conducted, those parts remaining in service are able to accomplish the required safety task. For a safety system, removal from service of any single component or channel should not result in loss of the required redundancy unless the acceptably reliable operation of the system can be adequately demonstrated (see Ref. [1], para. 6.81). The chosen test method should, to the extent practicable, minimize the time interval during which equipment is removed from service. The preferred method of withdrawal from service is to place the removed channel output into a defined safe state.

4.95. Test procedures for periodic testing of I&C safety systems should neither require nor allow makeshift test set-ups, use of temporary jumpering, removal of fuses or opening of breakers. Temporary connection of test equipment may be used where the safety system equipment to be tested is provided with facilities specifically designed for the connection of this test equipment. These facilities should be considered as part of the safety system and should comply with all the recommendations of this Safety Guide, irrespective of whether the portable test equipment is disconnected or remains connected to these facilities.

Control and conduct of tests

4.96. Arrangements for testing should neither compromise the independence of safety systems nor introduce common cause failures.

This publication has been superseded by SSG-39

MAINTAINABILITY

4.97. A number of factors inherent in I&C systems for nuclear power plants make it necessary to design these systems so as to permit reliable and efficient maintenance. These factors include:

— the long lifetime of a nuclear power plant in relation to the typical lifetimes of various hardware components of I&C systems;
— unavoidable drift, degradation or impairment of instrumentation; and
— wearing out of I&C hardware (i.e., component failure rates which make the replacement of components at least once over the lifetime of the plant unavoidable).

4.98. For systems important to safety, particular attention should be paid to facilitating maintenance activities that preserve the qualification of the system for the environments in which this system must operate. Minimizing the time necessary to make repairs contributes to the overall reliability and availability. Maintainability is an important element in implementing the defence in depth principles set out in paras 2.9–2.11 of Ref. [1].

4.99. I&C systems important to safety should be designed and located so as to facilitate surveillance and maintenance, to permit timely access and, in the case of failure or error, to allow easy diagnosis and repair.

4.100. I&C systems important to safety should be designed with human capabilities for and limitations in performing the required maintenance activities taken into account. Where practicable, I&C systems should be located so as to minimize risks to maintenance personnel and to facilitate maintenance of the equipment. Enough room should be left around the equipment to ensure that the maintenance staff can perform their tasks under normal working conditions. Where practicable, equipment should not be placed in locations for which there is a risk of high radiation levels (see Ref. [12]) or where conditions of extreme temperature or humidity are normal.

4.101. Systems having devices located in inaccessible areas should be carefully reviewed in order to determine whether provision of other strategies for coping with failure would be appropriate. Examples of such strategies include the installation of spare redundant devices, provision of facilities for remote installation, and planning for plant operation at reduced power if the equipment fails and cannot be expeditiously repaired or replaced. During power operation, the locations of certain components may preclude their regular calibration. In this case, special emphasis should be

This publication has been superseded by SSG-39

placed on the long term accuracy and stability of the selected devices, and means should be provided to permit comparison with other devices, for example, to compare neutron power with thermal power.

4.102. In those systems to which the single failure criterion applies, if a channel is bypassed during plant operation for the purposes of maintenance, testing, repair or calibration, the remaining operable channels of the system should continue to meet the single failure criterion unless otherwise justified as discussed in paras 4.15–4.21 of this Safety Guide.

4.103. Means provided for the maintenance of I&C systems important to safety should be so designed that any effects on the safety of the plant are acceptable. Typical examples for such means are the disconnection of one channel in a system with redundant channels, and provisions for alternative manual actions.

DOCUMENTATION

4.104. Confidence in the design of systems important to safety is based to a significant extent on the soundness of the processes applied. Documentation plays an important part in developing confidence in the design and in communicating the basis for confidence to others. The documentation produced in the design and implementation of systems important to safety should be clear and precise.

4.105. A set of documents should be produced and maintained so as to ensure the traceability of the rationale for the design. The appropriate documents should be produced at each step in the development process, and a set of system documents should be provided with the system upon delivery. The details of the extent, type and contents of the documentation are discussed further in Section 7. The following attributes should be achieved for all documents associated with systems important to safety:

— They should be understandable unambiguously by people with a variety of backgrounds and experience who may be involved in the design, construction, commissioning, operation, maintenance and licensing of the facility;
— The language used should be clear, with a well defined terminology; and
— Notation, terminology, texts and diagrams should be used in a uniform way throughout the documentation.

4.106. Documentation should be written for usability, i.e. it should be written in consideration of the needs of its users as follows:

This publication has been superseded by SSG-39

— Requirements, specifications and descriptions of design should allow only one interpretation for each individual requirement, specification or description;
— Tracing from higher level documents to design documents should be possible to check for completeness;
— Tracing back from design documents to higher level documents should be possible to check for unnecessary items;
— The documents should not contain any contradictory or inconsistent statements;
— Each piece of information should have a single, identifiable place in the document and should not be repeated or split up;
— Each requirement or design element should have a unique identifier (which also aids traceability);
— Requirements and design information should be expressed so that it is possible to verify that systems important to safety meet the requirements and are built in accordance with the design;
— The structure and style of documents should be such that any necessary changes can be made easily, completely and consistently; and
— Documents should be understandable to the intended users.

IDENTIFICATION OF ITEMS IMPORTANT TO SAFETY

4.107. Items important to safety should be identified in order to ensure that the requirements on systems important to safety are applied in the design, construction, maintenance and operation of the plant. Identification should be made in order to meet the requirements for safety classification set out in paras 5.1–5.3 of Ref. [1].

4.108. Safety systems and their components should be uniquely identified, e.g. by tagging or colour coding. In addition, within a safety system, redundant channels should be suitably identified to reduce the likelihood of inadvertently performing maintenance, tests, repair or calibration on an incorrect channel. Such identification should not depend on reference to drawings, manuals or other reference material. The identification should be distinguishable from identifying marks used for other purposes. This practice should also be adopted for safety related systems. Components or modules mounted in equipment or assemblies that are clearly identified do not themselves need identification. Configuration management is generally sufficient for maintaining the identification of such components, modules and embedded computer software.

This publication has been superseded by SSG-39

5. SYSTEM SPECIFIC DESIGN GUIDELINES

5.1. The specific guidance given in this Section applies *in addition to* the general guidance given in Section 4.

SAFETY SYSTEMS

5.2. The protection system is that part of a safety system which detects departures from acceptable plant conditions and initiates actions to prevent an unsafe or potentially unsafe condition. Various system configurations are used for this purpose, and the term 'protection system' is not universal in all Member States. The guidance given in the section on protection systems applies to whichever systems perform these functions.

PROTECTION SYSTEMS

5.3. The protection system is provided to maintain safety in situations in which the control systems fail to maintain plant variables within defined limits. Such situations may arise either because a fault has occurred within a control system or because an event has occurred that causes process variables to change too rapidly for the control systems to react adequately, or because of failure of an item important to safety. In such situations, prompt action is necessary to prevent the situation from developing into a potential accident.

5.4. Generally, the action necessitated by a particular situation, namely the safety task for that situation, involves the operation of numerous items of the plant in a co-ordinated manner. The protection system is provided to perform all specified safety tasks, in conjunction with the safety actuation systems and safety system support features.

5.5. The protection system monitors relevant plant variables. These may be process variables such as neutron fluence rates[2] (fluxes) or coolant temperatures and pressures, or they may be variables specific to anticipated operational occurrences or

[2] The fluence rate ($\perp$) is the increment of particle $d\Phi$ in a suitably small interval of time divided by that interval of time: $\perp = d\Phi/dt$.

design basis accident conditions, such as rates of change of process variables, moisture levels, changes of position of equipment or radiation levels. The measured plant variables, either singly or in selected combinations, should permit the detection of all situations in which a safety task is to be performed.

Purpose of the protection system

5.6. The Requirements for Design require (Ref. [1], para. 6.80) that the protection system be designed so as to:

— initiate automatically the operation of appropriate systems, including, as necessary, the reactor shutdown systems, in order to ensure that specified design limits are not exceeded as a result of anticipated operational occurrences;
— detect design basis accidents and initiate the operation of systems necessary to limit the consequences of such accidents within the design basis; and
— be capable of overriding unsafe actions of the control system.

5.7. The protection system is typically required to:

— detect that a plant variable has reached the set point;
— identify a situation necessitating protection;
— initiate, in correct sequence, all safety actions required by the corresponding safety task within the protection system itself, the safety actuation systems and the safety system support features; and
— in some Member States, monitor plant variables and display their values to the operator for use in taking manual protective action.

5.8. The following common safety functions which are identified in the design basis are initiated by the protection system:

— safe shutdown of the reactor;
— maintenance of the reactor coolant pressure boundary within design limits for all operational states;
— removal of residual heat in anticipated operational occurrences and accident conditions;
— emergency core cooling in and following design basis accident conditions;
— isolation of the reactor containment in and following design basis accident conditions;
— reduction of pressure and temperature in the reactor containment after an accident;
— clean-up of the containment atmosphere;

This publication has been superseded by SSG-39

— isolation of effluent radioactive waste; and
— control of airborne radioactive material, including control of its ingress into any operating areas and its escape to the environment.

5.9. Protective actions are initiated when the value of a plant variable reaches a predetermined value, namely, the nominal set point.

Extent of the protection system

5.10. The protection system encompasses all electrical and mechanical devices and all circuitry involved in generating protective action signals from measurements of process variables. Figure 3 shows the interfaces with the following:

— the plant process being protected, through sensors within the protection system;
— the safety actuation systems, through actuation devices within the safety actuation systems;
— any operator information displays that are not included in the protection system but which extract signals from the protection system through isolation devices located within the protection system; and
— control systems, through isolation devices within the protection system.

5.11. For reasons of clarity, Fig. 3 does not attempt to present all possible interface points between the protection system and other systems such as monitoring information systems, safety system support features and control points at field panels.

5.12. The protection system comprises the following items:

— sensors, which may be both:
  • instrument sensing lines from the process, up to and including the input transducer (for example, sensing pressures, flows and positions); and
  • primary sensing devices used for the measurement of plant variables (for example, thermocouples and ion chambers);
— signal conditioning equipment for the primary sensing devices, including trip comparators and analog to digital signal converters;
— the decision making logic used for each measured variable;
— signal conversion equipment providing the outputs, as protective actions, to the actuation devices;
— displays necessary for manual initiation of protective actions;
— isolation devices interfacing with operator information displays and systems of different safety classification;
— panels, racks and enclosures containing protection system equipment;

This publication has been superseded by SSG-39

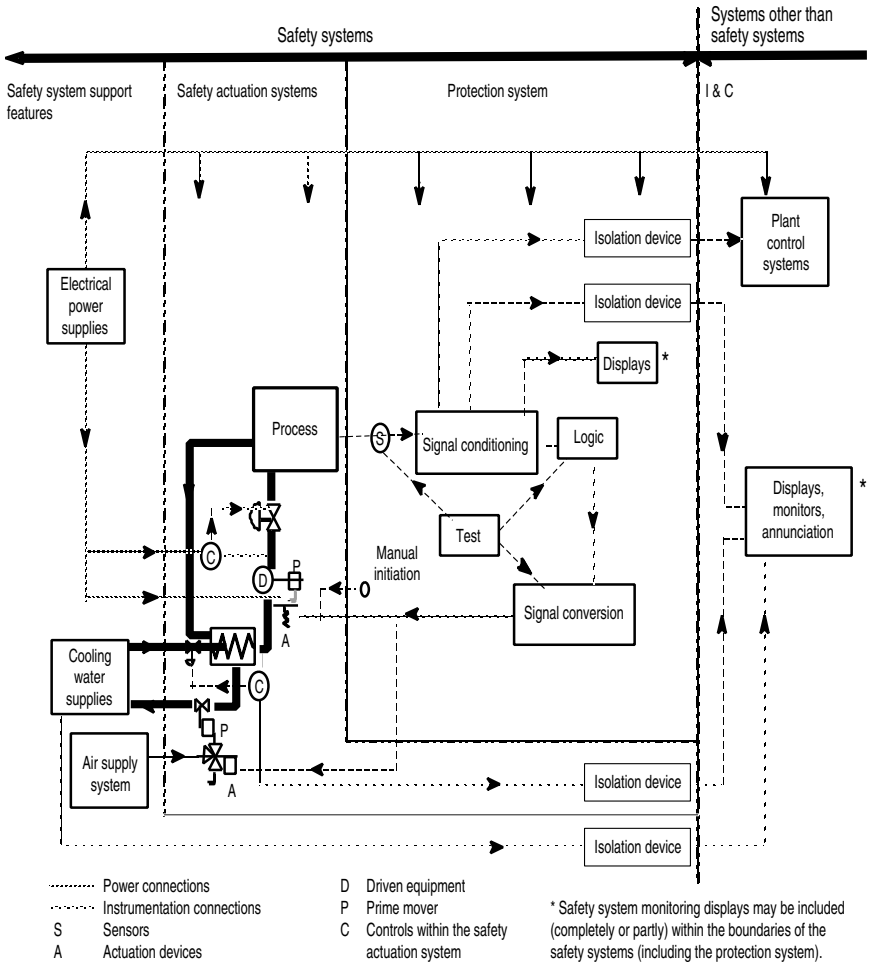

FIG. 3. Typical schematic outline of a protection system and its interconnections with other systems.

— connecting cables and raceways;
— containment penetrations for electrical and instrumentation cables; and
— any other equipment intervening between the process connection and the input terminals of the actuation device.

This publication has been superseded by SSG-39

5.13. The guidance in this Section is also applicable to other safety system equipment that must operate in order to ensure that the functions of the protection system are fulfilled. Such other safety system equipment includes:

— actuation devices receiving output signals from the protection system;
— prime mover equipment operated by the actuation devices; and
— driven equipment operated by the prime mover equipment.

Sensing devices

5.14. The protection system should be used to monitor plant variables and detect deviations from their specified limits so that specified safety functions can be performed. Measurements of plant variables should be consistent with the performance requirements specified in the design basis. To the extent practicable, the plant conditions of concern should be monitored by direct measurement rather than being inferred from other, more indirect, measurements.

5.15. In selecting the range of measurement for each monitored variable, the accuracy, the speed of response and the amount of overrange necessary for the particular function and any necessary post-accident monitoring capability should be taken into account. If more than one sensor is necessary to cover the entire range of the monitored variable adequately, a reasonable amount of overlap from one sensor to another should be provided at each transition point to ensure that saturation or foldover effects do not prevent the required protective function from being performed.

5.16. Set points may be either fixed or variably dependent upon some other plant parameter or condition. When variable set points are employed, the devices used to effect the set point setting are classified as part of the protection system and should meet its requirements. The design of the system should provide the operator with a means for determining the set point values for each protection system channel.

Protection system 'seal-in'

5.17. The action initiated by the protection system should be sealed in[3]. The seal-in should not be voided except by manual operator action after completion of the safety

[3] 'Seal-in' is the property of a component that causes its output signal to take on a new state and remain in that state after the input signal or signals that initiated the new state have returned to their previous values.

This publication has been superseded by SSG-39

action, or by action of the protection system to prevent the limits established in the design basis from being exceeded. Once an action has been sealed in, the intended sequence should continue until the safety task has been accomplished. After seal-in of the action, the protection system should monitor the plant conditions automatically, enabling safety actions as dictated by the conditions of the plant and providing information to support any permissible operator actions. Accomplishment of a safety function should not prevent the protection system from initiating other protective actions that may be required by the subsequent conditions of the plant.

5.18. Components added for seal-in functions should not reduce the reliability of the safety action beyond an acceptable level.

Manual safety action

5.19. Operator action is involved in:

— backup of safety actions;
— direct initiation or termination of certain safety actions; and
— resetting of the protection system after its operation.

5.20. The design of manually operated facilities should be flexible enough to permit safety actions to be initiated in abnormal situations and to permit long term post-accident operation.

5.21. The requirements for most protective actions are such that automatic initiation of the actions will be necessary. In addition, a capability for manual initiation of reactor shutdown and for the initiation of system level action such as containment isolation should be provided. This does not preclude intervention by the operator in a more detailed manner. Where manual actuation is provided for, it should be independent of the equipment of the automatic protection system to the extent practicable.

5.22. In the event of inadvertent manual initiation of a safety action, the protection system should protect the plant by automatic action. Manual initiation or termination of safety actions may be used alone provided that it can be shown that acceptable limits will not be exceeded. Examples of such manual actions are:

— initiation of certain safety tasks after completion of automatic sequences;
— placing of the shut down plant in its most favourable state in the long term after an accident; and
— initiation of certain safety actions that are not required until a considerable time after the PIE.

This publication has been superseded by SSG-39

5.23. In order to substantiate a claim that manual action alone is acceptable, it should be shown that:

— the operator has sufficient and clearly presented safety class information to make reasoned judgements and to initiate the required safety actions;
— the operator is provided with written procedures and training for assistance;
— the operator is provided with sufficient means to accomplish the required actions;
— the operator is allowed sufficient time to evaluate the status of the plant and to complete the required actions; and
— the communication links between operators carrying out the actions are adequate to ensure the correct accomplishment of these actions.

5.24. The time available for planned operator action from the onset of an anticipated operational occurrence or design basis accident conditions varies among Member States, ranging between 10 and 30 min. This period depends upon such factors as the complexity of the decision, the displays available, the need to distinguish between different PIEs and the consequences of a wrong decision.

5.25. Manual safety actions should be facilitated by the design and layout of the control room. All controls, displays and alarms necessary for safe operation, reactor shutdown and removal of residual heat from the reactor as well as for containment system functions should be readily available and should present information to the operator in a clear manner.

5.26. Information about actions important to safety taken by operators outside the main control room should be available immediately in the control room, except in situations where the control room has been damaged or abandoned. In this case, the necessary information should be available in a supplementary control room.

5.27. The Requirements for Design require (Ref. [1], para. 6.84) that the design be such as to minimize the likelihood that operator action could defeat the effectiveness of the protection system in normal operations and anticipated operational occurrences, but not to negate correct operator actions under design basis accident conditions.

Spurious actuation

5.28. Spurious initiation may result from numerous causes, in particular, failures in the equipment, inadequate tripping margins on some parameters in relation to variations occurring in normal operation, or human error during interventions. These may result from the following:

This publication has been superseded by SSG-39

— inadequate consideration of plant responses to operational disturbances and the consequential variations in the parameters being monitored;
— inadequate allowance for inaccuracy of instruments, uncertainties in calibration and drift, or errors in setting trips;
— inadequate treatment for signal noise; or
— a combination of these factors.

5.29. The primary requirement for the protection system should be to carry out its specified protective tasks adequately. Nevertheless, the number of spurious initiations should be minimized to the extent practicable since they can lead to the following:

— unnecessary stress on equipment;
— the need for other safety actions;
— erosion of the operator's confidence in equipment, potentially leading to subsequent disregard of valid signals; and
— loss of capability for production at the plant.

5.30. The protection system should therefore be designed to meet the relevant requirements while the number of spurious initiations is minimized. Spurious output from the protection system should not initiate an event of safety concern. If spurious initiation within the protection system could result in a plant state in which the plant requires protection, then safe conditions should be maintained through actions being initiated and carried out by the unaffected parts of the protection system, the safety actuation systems and the safety system support features.

5.31. Effective measures to reduce the number of spurious initiations include on-line signal filtering, validation of parameters, voting on redundant signals and energizing to actuate.

Interaction between protection system and other systems

5.32. Possible interactions between the protection system and the control systems should be evaluated. The Requirements for Design require that interference between the protection system and the control systems be prevented by avoiding interconnections or by providing suitable functional isolation (Ref. [1], para. 6.86). If signals are used in common by both the protection system and any control system, appropriate separation (such as by adequate decoupling) shall be ensured.

5.33. If the failure of a control system can cause a plant condition that necessitates safety action and can concurrently disable one channel within the safety group that protects against the condition, the safety requirements should continue to be met on

This publication has been superseded by SSG-39

the assumption of a coincident single failure anywhere in that safety group. If operation is permitted with a protection channel bypassed or removed from service for the purposes of testing or maintenance, its bypass or removal should be assumed in the analysis.

5.34. If a PIE can cause a control system action that results in a plant condition requiring safety action, then the same PIE should not prevent proper action of the safety group provided to give protection against that plant condition. Effective measures to prevent interactions of this type include:

— additional equipment in the safety group to deal with the potential interaction;
— provision of barriers and/or alternative plant arrangements to limit the damage resulting from the PIE; or
— a combination of these items so that the safety group and/or plant design is sufficient to maintain the plant conditions within acceptable limits.

5.35. Where an individual actuation device such as a pump motor or valve actuator is controlled by a plant control system and by the protection system, the protection system should be capable of overriding the action called for by the control system. For example, if the control system calls for a pump to run at half speed and the protection system calls for that pump to run at full speed, the protection system demand should have priority and the pump should run at full speed. Similarly, if the control system calls for a valve to close and the protection system calls for that valve to open, the protection system demand should have priority and the valve should open.

Operational bypasses

5.36. The trips that protect the reactor in one mode of normal operation may prevent changes to other operational states. For example, the trips that protect the reactor at low power will prevent the reactor from reaching full power. To permit such changes, the initiation of an unnecessary and unwanted protective action should be inhibited by means of an operational bypass (sometimes referred to as trip conditioning). Such logic conditioning of trip signals should be integrated into the protection system.

5.37. Whenever bypass permissive conditions are not met, the safety systems should automatically prevent the activation of an operational bypass and should accomplish one of the following:

— remove the activated operational bypass,
— put the plant in a condition where the operational bypass is permissible, or
— initiate appropriate protective actions.

This publication has been superseded by SSG-39

5.38. Regardless of the way in which activation is accomplished, the means for activating the operational bypasses is considered part of the protection system and should be in compliance with this Safety Guide.

POWER SUPPLIES

5.39. The power supply (electrical, pneumatic or hydraulic, as necessary) should be compatible with the I&C system. The power supply for I&C systems important to safety should have classification, qualification, isolation, testability, maintainability and indication of removal from service, consistent with the reliability requirements of the I&C systems they serve.

5.40. Power supplies commonly provide a transmission path for electrical interference effects which may originate outside the I&C systems or may stem from other I&C systems that are connected directly or indirectly to the same power supply. The design of the power supplies and the I&C systems should ensure that such interference effects are not large enough to impair the functions of the I&C system. This should be confirmed by testing, analysis or other suitable means of assessing the integrated I&C systems important to safety and their associated power supply system(s) (see also Section 4).

5.41. I&C systems important to safety that are required to be available for use at all times in operational states or design basis accident conditions should be connected to a non-interruptible power supply. The performance requirements of non-interruptible power supplies should satisfy the requirements of the system that they power.

5.42. I&C systems important to safety may be connected by the plant operators or by automatic switching action to a stand-by power supply instead of the normal supply when operating circumstances warrant, provided that the functions of the I&C systems can tolerate the associated interruption in supply. The transfer system should in most cases be considered an extension of the power supply system(s).

DIGITAL COMPUTER SYSTEMS

5.43. Digital computer systems are used in I&C systems important to safety to perform functions of protection, data acquisition, computation, control monitoring and display. If properly designed, they can offer the advantages of improved reliability, accuracy and functionality in comparison with analog systems. The computer system

This publication has been superseded by SSG-39

may take many forms, ranging from a large processor supporting many functions to a highly distributed network of small processors devoted to specific applications.

5.44. Computer systems may be used to advantage in detecting and monitoring faults internal and external to plant systems and equipment important to safety.

5.45. Hardware and software for computer systems should be configured so that the system operates in a predefined safe manner in conditions of credible failures of hardware and software.

5.46. With computers it is possible to have one set of equipment perform several system functions. A disadvantage of this is that if one component goes out of service, several functions may fail simultaneously. Consequently, this factor should be addressed in the design and analysis of the systems.

5.47. When the use of a computer involves two or more functions that fall into different safety classes, the computer system should meet the requirements of the higher safety class.

5.48. Start-up and reset of a digital system (e.g. after a temporary loss of electric power) should initialize the system to a predefined state that ensures continued safe operation.

5.49. The software for the digital system should be well documented and should be developed through a controlled engineering process.

5.50. An IAEA Safety Guide [2] provides additional guidance on the use of digital computer systems.

Maintenance

5.51. Adequate technical expertise in the original technology for the hardware and software should be preserved over the lifetime of the plant. Contrary to what is typical for other plant systems, maintenance of computer systems is not routine. Maintenance staff should have in-depth knowledge of the requirements of the computerized systems and of the development process used for the digital retrofit.

Upgrades to digital systems

5.52. It should be recognized that computerized I&C systems in new power plants will also age, become obsolete and eventually need replacement. Given that suppliers

This publication has been superseded by SSG-39

of digital equipment change their product lines frequently, it becomes difficult to maintain an inventory of spare parts for the lifetime of the plant. The user has to stock a substantial quantity of digital components and, in doing so, should consider the possible deterioration of electronic products that are stored for a long period of time.

Data communication

5.53. Data communication as defined for the purposes of this Safety Guide is the transmission from one location to another of two or more signals or messages over a single data channel by the use of time division, frequency division, techniques of pulse coding or the like. Data communication encompasses a wide range of technical solutions varying from simple hardware only multiplexing to complex self-correcting and multilayer communication protocols controlled by software.

5.54. Data communication channels important to safety should satisfy the recommendations for independence given in Section 4, particularly paras 4.36–4.48.

5.55. The design of the data communication system should provide for detection and, to the extent practicable, for correction of errors and for the status of data in the information transmitted.

5.56. Checking of data communication may be done periodically as an automatic self-check function. The chosen frequency of this self-check should be appropriate for the use of the data and the frequency of demand for the safety functions being performed by the system. Features for the detection and correction of errors can be used to improve the reliability of signal transmission to meet reliability goals.

5.57. The communication technology should be chosen and suitably configured to ensure that it is capable of meeting the requirements for time response under all possible conditions of data loading.

5.58. Where the reliability of the data and the data link are of great importance, suitable communication technology should be selected. The selection and use of more complex technology may offer functional advantages but may also introduce additional failure modes and validation difficulties. Appropriate consideration should be given to the use of redundancy in the data link, to the appropriate level of reliance on the data link in general, and to the ability of the sending and receiving systems to withstand failure by all possible modes. The use of data communications should not defeat the physical or functional channelization of processing or logic elements within the system architecture.

This publication has been superseded by SSG-39

5.59. Data flow from systems of lower safety class to systems of higher safety class should generally be avoided as far as practicable. Where such data flows are essential, measures (such as data validation or data range checks) should be taken to ensure that data from the lower class system cannot jeopardize functions important to safety.

6. HUMAN–MACHINE INTERFACE

6.1. The monitoring and control of systems important to safety involves a combination of automatic measurement and control functions, and monitoring and control by human operators. While automatic control and automatic actuation of safety systems are used extensively in modern nuclear power plants, the plant operators remain in overall command of the plant.

6.2. A basic objective should be to achieve a design which is compatible with the strengths and limitations of the human operators. Attention should be paid in the design of the human–machine interface to the duties and responsibilities of the plant personnel, in order to achieve an effective interface between the operating personnel and the plant. This should include paying attention not only to the operators but also to maintainers, inspectors and administrative and emergency personnel at the plant.

6.3. To assist in the establishment of design principles for information display and controls, the operator has dual roles: that of a systems manager, including accident management, and that of an equipment operator.

6.4. The Requirements for Design require (Ref. [1], para. 5.54) that the operator, in the role of systems manager, have information that permits:

— the ready assessment of the general state of the plant, in whichever condition it may be, in normal operation, in an anticipated operational occurrence or in an accident condition, and confirmation that the designed automatic safety actions are being taken; and
— the determination of appropriate operator initiated safety actions to be taken.

6.5. The Requirements for Design require (Ref. [1], para. 5.55) that the operator, in the role of equipment operator, be provided with sufficient information on parameters associated with individual plant systems and equipment to confirm that the necessary safety actions can be taken effectively.

This publication has been superseded by SSG-39

6.6. In general, because of the large number of plant parameters and equipment that are typically instrumented and managed in a modern nuclear power plant, careful attention should be paid to the design of the human–machine interface to ensure that all the necessary information is available to the operator when and wherever necessary. At the same time, the operator should not be overwhelmed by large amounts of data that could be difficult to assimilate owing to the limitations on human powers of perception, cognition and memory. Similarly, in the design of systems involving operator initiated control actions, careful attention should be paid to both reducing the likelihood of human error and ensuring that the system is robust against errors that may occur.

6.7. The Requirements for Design require (Ref. [1], para. 5.50) that systematic consideration of human factors and the human–machine interface be included in the design process at an early stage of development of the design and continue throughout the entire process, to ensure an appropriate and clear distinction of functions between operating personnel and the automatic systems provided.

6.8. It should be ensured that plant operators and maintainers are provided with the information necessary to understand the status of the plant, so as to enable them to carry out their duties. Implementation of a human factors engineering programme beginning in the earliest stages of design is an effective method for achieving this objective (see paras 7.6–7.10).

6.9. Design, training, operating procedures and team organization relating to I&C systems should be considered in an integrated design cycle (in such a way that, for example, the consequences of the use of a computerized human–machine interface for the behaviour of the operator can be analysed). Detailed discussion of these considerations is beyond the scope of the present Safety Guide. Other safety standards will provide guidance on the overall engineering process for human factors.

6.10. Operator interfaces to the plant are primarily located in the main control room, technical support centre, supplementary control rooms and emergency control centre. These facilities contain safety related displays, safety related controls, accident monitoring systems, alarm annunciators and historical data systems. Guidance on the design of these facilities and systems is provided in this section.

MAIN CONTROL ROOM

6.11. The principal location for safety related control actions is the main control room. The Requirements for Design require (Ref. [1], para. 6.71) that a control room

This publication has been superseded by SSG-39

be provided from which the nuclear power plant can be safely operated in all its operational states and from which measures can be taken to maintain the plant in a safe state or to bring it back into such a state after the onset of anticipated operational occurrences, design basis accidents and severe accidents. In addition, measures can be taken from the control room to mitigate the consequences of severe accidents.

6.12. The Requirements for Design require (Ref. [1], para. 6.73) that the layout of instrumentation and the mode of presenting information provide the operating personnel with an adequate overall picture of the status and performance of the plant. Ergonomic factors are required to be taken into account in the control room design.

6.13. The principal objectives for the functional design of a control room are to provide the operator with accurate, complete and timely information on the status of plant equipment and systems for all operational states and design basis accident conditions, and to optimize the activities of the operator in monitoring and controlling the plant. Requirements for functional isolation and physical separation as well as ergonomic principles should be taken into account in the design of the main control room, which is a centre where the I&C elements of safety systems, safety related systems and systems not important to safety converge.

6.14. In the control room design, human engineering factors such as workload, possibility of human error, operator response time and minimization of the operator's physical and mental efforts should be taken into account, in order to facilitate the execution of the operating procedures specified to ensure safety in all operational states and following design basis accident conditions. The necessary provisions should be made to ensure satisfactory conditions in the working environment, including conditions of lighting, temperature and humidity, and to avoid hazardous conditions such as unacceptable radiation levels, or smoke or toxic substances in the atmosphere. Because safety related displays, annunciators and controls are typically used in all plant operating conditions, the design of the control room should include a balanced consideration of all the conditions assumed. Automatic actions for safety related controls should be employed in many cases in order not to impose an unreasonable burden on the operator in accomplishing safety functions. Human factor considerations have led to the specification of several design goals, the more important of which are as follows:

— The presentation of information by means of displays and instrumentation should be integrated into a harmonized arrangement in order to optimize the operator's understanding of the plant's status and to optimize the activities necessary to control the plant;

This publication has been superseded by SSG-39

— When the process being controlled involves redundant or diverse displays as a means of ascertaining information, the alternative sources of information should, to the extent practicable, be located and configured so that the operator can use both sources with minimum effort in arriving at conclusions, without jeopardizing the required independence of the information sources;
— The control room displays should be arranged so that the operator can readily observe them and ascertain the status of any system;
— Control devices and their functionally associated displays should as far as practicable be located so as to facilitate action by the operator;
— Attention should be paid to the need for the operators to have an effective overview of the plant's status and for the consistency of information presented to different personnel in the control room;
— Some displays may show parameters originating from instrumentation of different qualification levels (i.e. trustworthiness); under these circumstances, the differences in qualification level should be made apparent to the operator on the display.

SUPPLEMENTARY CONTROL ROOMS

6.15. In addition to the main control room, various types of supplementary control rooms and control locations are used. Details of nomenclature and allocation of functions vary among Member States, but other control rooms and control locations include:

— the emergency control room,
— the secondary control area,
— the safe shutdown panel,
— supplementary control rooms, and
— other local control stations.

Further information can be found in Ref. [4]. Guidance on design is provided in the following.

6.16. The Requirements for Design require (Ref. [1], para. 6.75) that sufficient I&C equipment be available, preferably at a single location that is physically and electrically separate from the control room, so that the reactor can be placed and maintained in a shut down state, residual heat can be removed and the essential plant variables can be monitored in the event of a loss of ability to perform these essential safety functions in the control room. This instrumentation is typically situated in a supplementary control room.

This publication has been superseded by SSG-39

6.17. The plant's design basis should define the conditions under which it is no longer possible to perform the control functions from the main control room owing to hostile takeover, fire or other reasons that could necessitate abandonment of the main control room.

6.18. Suitable provision should be made for transferring priority control to a new location and isolating the equipment in the main control room whenever the main control room is abandoned.

6.19. The design basis of a nuclear power plant is usually such that loss of availability of the control room due to a PIE is very infrequent. It is therefore not necessary to postulate that a second PIE will occur when the main control room is unavailable and the necessary safety functions are being performed from a supplementary control room.

6.20. If the design basis requires that damage to equipment in the control room be taken into account, the requirements for independence should be applied to the circuitry feeding these areas so that failures caused by the PIE in one area, e.g. short circuits, open circuits and high potentials, do not prevent performance of the required safety tasks in another area. Depending on the nature of the event and the design of the plant, it may be necessary to install redundant instrument channels, logic channels and other safety equipment for each area. Where common safety actuation equipment is used, the priority of the control point signals should be established in the design basis.

6.21. The design of supplementary control rooms should include suitable provisions for preventing unauthorized access and use.

6.22. Manual control from a supplementary control room should, in general, be accomplished by simple actions such as operating a switch or pressing a button. To the extent possible, displays and controls should be similar to those in the main control room.

6.23. The design of the main control room and the supplementary control rooms should be such that no PIE can simultaneously affect both the main control room and the supplementary control rooms to the extent that required safety functions cannot be performed.

6.24. It should also be ensured that either the main control room or a supplementary control room can be given the necessary priority for initiating a particular safety function.

This publication has been superseded by SSG-39

6.25. Applicable parts of other sections of this Safety Guide should be taken into account in the design of supplementary control rooms, and the differences in purpose and use between the supplementary control rooms and the main control room should be given due consideration.

6.26. Depending upon the nature of the PIE, the provision of instrumentation channels independent of those in the main control room should be considered. Special needs for support features for the safety system should also be considered where necessary.

6.27. Due consideration should also be given to ensuring that an adequately qualified access path is provided in the design to permit operators abandoning the main control room to move safely and conveniently to the supplementary control rooms.

6.28. An adequate indication of potential hazards (such as smoke) and countermeasures (such as breathing masks) should be provided along the qualified access path from the main control room to the supplementary control rooms.

6.29. The supplementary control rooms should be located and configured so that operators can commence their duties at the new location within an acceptable time limit.

6.30. If the safety analysis shows that long term occupation will be necessary, habitability should be ensured, for example, by means of ventilation. Adequate seating, means for writing, access to documents and surface space for laying down documents should also be available.

EMERGENCY RESPONSE FACILITIES

6.31. The main control room is the operators' information and activation centre of the plant for operational states and design basis accident conditions. It may also be used as the primary centre to direct the initial stages of off-site activities in an emergency. However, off-site emergency response operations should not impair the ability of the control room staff to implement procedures for accident management. Consequently, provision should be made to transfer non-operational aspects of emergency response, such as the direction of teams or off-site notification and co-ordination, out of the control room as soon as possible, and to restrict access to the control room in the event of an emergency.

6.32. The Requirements for Design require (Ref. [1], para. 6.87) that an on-site emergency control centre, separated from the plant control room, be provided to serve as a meeting place for the emergency staff who will operate from there in the event of

This publication has been superseded by SSG-39

an emergency. Information about important plant parameters and radiological conditions in the plant and its immediate surroundings should be available there. The room should provide means of communication with the control room, the supplementary control rooms and other important points in the plant, and with the on-site and off-site emergency response organizations. Appropriate measures are required to be taken to protect the occupants for a protracted period of time against hazards resulting from a severe accident.

6.33. In addition to local arrangements for managing an accident, some Member States have found it effective to have an emergency support centre remote from the site to permit the co-ordination of advice from experts. Similarly, suitable information and communication systems should be provided for such a facility.

6.34. Further information on emergency response facilities can be found in Refs [4, 13].

CONTROL FACILITIES

6.35. If equipment important to safety can be controlled both from the control room and from locations outside the control room, the actual source of control should be automatically indicated by visual means (annunciators, testable indicator lights, hand switch positions) in each control location.

6.36. The control room should include all the controls necessary to deal with those accident conditions for which:

— performance of necessary controls outside the control room may be limited by the accident conditions, and
— time constraints on dealing with the accident conditions may prevent the operator from leaving the control room to operate controls in other locations.

6.37. Adequate service functions, such as lighting and facilities for communication and fire fighting, should be provided to enable the plant's operating staff to interpret the monitoring displays and take the proper safety actions after any PIE.

6.38. In the design of control facilities, consideration should be given to non-I&C aspects such as radiological protection [12], habitability [8], protection against lightning, fire protection [6], accessibility and access control, missile protection [7, 8] and seismic resistance [14], on the basis of the PIEs of external and internal origin specified for the plant.

This publication has been superseded by SSG-39

6.39. Oral communications between the main control room, the supplementary control rooms, other suitable plant locations and off-site emergency services are important to safety, particularly under conditions of anticipated operational occurrences or design basis accidents. Such communications should normally be provided with two, preferably diverse communication links and should be electromagnetically compatible with the I&C systems (self-powered telephones, battery operated telephones, hand held portable radios). These communication links should be routed in such a way that fires, failures of electrical systems or other applicable PIEs cannot incapacitate both systems simultaneously.

DISPLAYS

6.40. Displays provide information to the plant operators about the plant's status as well as on the status of systems and equipment which is required in order to monitor, maintain and operate the systems important to safety and to keep the plant within its design basis envelope. Displays are used to accomplish one or more of the following functions:

— to inform the plant operators of the status of systems and the safety status of the plant;
— to inform on-site and off-site safety experts about the safety status of the plant in accident conditions; and
— to provide information on time dependent behaviour of process variables important to safety for immediate or subsequent analyses, and for reporting both within the operating organization and to external authorities.

6.41. Changes in the status of safety systems should be annunciated, and the status should be indicated in the control room.

6.42. In normal operation the operators monitor the plant's status continuously with a subset of displays and annunciators or visual display units that are provided in the main control room. Alarms or other devices indicate deviations from normal operation. When these occur, the operators should be provided with the information necessary in order:

— to identify the actions being taken by automatic systems;
— to analyse the cause of the disturbance;
— to follow the course of the plant's behaviour; and
— to perform any necessary manual counteractions.

This publication has been superseded by SSG-39

6.43. The display facilities should cover appropriate variables, in consistency with the assumptions of the safety analysis and with the information needed by the operator for operational states and design basis accident conditions. The accuracy and range of displays should be consistent with the assumptions of the safety analysis.

6.44. Where redundant displays are used to meet the reliability requirements, they should be functionally isolated and physically separated to ensure that a single failure in this system will not result in a complete loss of information about a monitored variable; for example, by using two keyboards for multiple visual display units.

6.45. Where failure of a single information display channel could result in information being ambiguous (such as a single failure that causes a pair of redundant displays to disagree), this could lead the operator to defeat or fail to accomplish a required safety function. To avoid this, additional means should be provided which allow the operator to resolve such conflicts in information. This may be accomplished, for example, by providing a third channel of information or by displaying another variable which bears a known relationship to the display channels in question and permits identification of the faulty channel. A single display channel with a clearly identifiable failure mode is adequate where the mean time to detect and repair it or to detect and replace it is less than the tolerable out of service time.

6.46. Where knowledge of the trend of a variable is essential to determining the appropriate operator action, a means should be provided to display that trend.

6.47. If part of a system important to safety has been rendered inoperative intentionally by using a feature provided in the design specifically for this purpose, this condition should be automatically displayed in the control room. If part of a system important to safety has been rendered inoperative by other administratively controlled means, this should be clearly indicated in the control room.

MONITORING OF ACCIDENT CONDITIONS

6.48. Reliable, readily accessible and comprehensible displays of information on the status of the plant and the trends in key plant parameters should be provided in order to ensure that the operator can deal effectively with accident conditions and that supporting personnel brought in to assist are adequately informed. Recommendations which pertain to the design of systems and facilities for accident monitoring are provided in the following.

This publication has been superseded by SSG-39

6.49. Information displays for monitoring accident conditions in the plant should be provided in the main control room and, as necessary, in the supplementary control rooms.

6.50. In deciding which information is to be displayed, consideration should be given to the following needs of the operator:

— to recognize a deviation from normal conditions;
— to identify the particular accident and, where possible, its initiating event;
— to verify that the required safety functions are being accomplished;
— to follow the course of the event or accident;
— to determine when conditions are developing that warrant the authorities taking emergency measures outside the boundary of the plant; and
— to resolve conflicts in information which may arise from the redundancy of display channels.

6.51. In order to allow determination of whether the required safety functions are being accomplished, the equipment for monitoring accident conditions should be so designed as to enable the operator to confirm that:

— the reactor is shut down and will remain shut down;
— the residual heat is being removed and will continue to be removed from the core and from other items important to safety to the ultimate heat sink; and
— any designated barrier to prevent radioactive releases to the environment is in place and will remain in place.

6.52. The plant parameters to be monitored for such confirmation should be those appropriate for the design and site of the reactor.

6.53. Equipment for monitoring accident conditions should be capable of operating in the post-accident environment at the time of need and for the necessary period of time. The ranges of measurement of selected key parameters should extend to values that may be reached in events that could challenge barriers to the release of radioactive materials from the fuel, heat transport system or containment, or could result in the release of radioactive materials from one or more of these barriers.

6.54. Displays that are used for post-accident monitoring should be distinct from other displays.

6.55. Where historical information is necessary for accident analysis or emergency measures, a capability for recording and retrieving the relevant data should be provided.

This publication has been superseded by SSG-39

6.56. Facilities should be provided in the plant for communicating adequate data to the emergency facilities specified in Ref. [13] without undue interference with control room activities that occur in an emergency.

SYSTEMS FOR ALARM ANNUNCIATION

6.57. Systems for alarm annunciation, both visual and audible, are used to draw the operators' attention to the need for intervention in the operation of the plant by, for example, manual initiation of safety system functions or the initiation of plant control or maintenance actions to ensure that the plant's status is maintained within its design basis envelope. The following guidelines apply to the use of alarm annunciation in connection with systems important to safety.

6.58. Appropriate visual or audible alarms should be provided at suitable locations in a timely manner, consistent with the underlying requirements for operator actions.

6.59. In the design of the alarm annunciator systems, appropriate attention should be paid to ensuring that the essential information can be effectively distinguished by the operators, particularly in anticipated operational occurrences and accident conditions which may involve large numbers of alarms. Various techniques are available for achieving this goal, including grouping, prioritization and conditioning of alarms, and using audible or visual differentiation to distinguish alarms of different types and priorities.

6.60. Techniques to avoid overloading the operator with alarm information should not be applied in a manner which leads to suppression of the information necessary for identifying the location and potential consequence of the malfunction.

6.61. Means should be provided that permit the operator to acknowledge the alarms, either singly or in groups, in a timely manner.

6.62. Audible alarm signals are commonly used to draw the operator's attention to new alarm conditions. Means for silencing these audible signals should be provided in order to avoid auditory overload and to facilitate the recognition of new alarms which may occur subsequently. If alarms are silenced, visual indications of the alarm conditions should continue until the underlying fault conditions have been cleared, in order that the conditions will not be forgotten. Visual means (change of colour or change from flashing to non-flashing) should be used to distinguish alarm conditions that have been acknowledged from alarm conditions that have not yet been

This publication has been superseded by SSG-39

acknowledged. When the plant status returns to normal, the alarm indication should persist until reset by the operator, in order to preserve the information about the alarm.

RECORDING SYSTEM FOR HISTORICAL DATA

6.63. A capability should be provided for recording, storing and retrieving data from important plant processes which record the performance and history of behaviour of the plant. Such systems for historical data typically support the following:

— backup information for shift operators (giving short and long term trends);
— general operational information for the plant management; and
— short and long term diagnosis and analysis of operation and accidents.

6.64. Traditionally, hard copy systems (paper printouts of data) have been used for these functions. However, the use of computer based systems should be considered because they facilitate more efficient storage, retrieval and processing of the large amounts of data which are typically involved. Generally, with computer based systems, conveniently located printers should be provided so that the users may print out hard copies.

6.65. Terminals for accessing historical information should be situated in and around the main control room, as appropriate. Remote terminals, conveniently situated for the use of engineering support personnel, are useful and should also be considered. In deciding upon the location of terminals and the design of the human–machine interfaces for accessing historical data, attention should be paid to the needs, duties and capabilities of the users.

7. DESIGN PROCESS FOR I&C SYSTEMS IMPORTANT TO SAFETY

7.1. The engineering of a nuclear power plant is a complex activity involving many technical disciplines. Correct information is necessary at appropriate times in a project, for each discipline, to ensure that the design is delivered as required. For systems important to safety, a structured development process embodying conservative design

This publication has been superseded by SSG-39

measures and sound engineering practice should be used, to ensure that the Requirements for Design [1] are correctly applied. Failure to do so because of a poorly organized or badly managed process could jeopardize nuclear safety.

QUALITY ASSURANCE

7.2. To attain the required quality standards, it is important to ensure that the I&C systems important to safety are designed, manufactured, qualified, inspected, installed, operated, tested and maintained in accordance with a quality assurance programme that is prepared by the designer, manufacturer or installer and approved by the appropriate authority. This programme should be in accordance with the relevant Code and Safety Guides (Ref. [3], Safety Guides Q3 and Q10).

7.3. The quality assurance programme should include all the activities necessary (1) to verify the adequacy of the design of the safety systems and (2) to ensure that the safety systems comply with all the applicable standards and requirements.

PROJECT PLANNING

7.4. To ensure the timely and commercially viable delivery of the necessary elements of a design, techniques of project management and project planning should be used. In the project planning activities used to drive a project to completion, the safety requirements of the systems being designed should be considered. Sufficient time should be allocated in the project schedule for presenting the documentation for the design of systems important to safety to the regulatory authority.

CHANGE CONTROL AND CONFIGURATION MANAGEMENT

7.5. Throughout the design process, from conception to operation, in any iteration, control should be exercised over any proposed modification, so that the configuration of the design is being managed. The process for making design changes should be documented and written approval should be sought, in order to ensure that due consideration is given to the proposed change and that its impact can be assessed by persons independent of the designer. In the early stages of the design many iterations may be necessary to determine the design required, and often the approach to managing changes becomes less formal. In these circumstances, periodic design reviews should be undertaken, to ensure that the appropriate personnel outside the design team are made aware of the progress of the design and to obtain confirmation that the

This publication has been superseded by SSG-39

safety requirements continue to be met. However, once a commitment to a specific design is made, there should be a formal process of control for design changes.

INTEGRATION OF HUMAN FACTORS

7.6. Because of the extensive and important roles of operators and other plant personnel in the operation and use of I&C systems important to safety (and of the plant as a whole), human factor processes should be integrated into the overall design process.

7.7. Applicable human factor techniques include functional analysis, task analysis and workload analysis. These are used in the allocation of functions among humans and machines and in the design of the human–machine interface. Guidance on human factor engineering is available, in particular on anthropometrics, human error, design of user interfaces and various other related subjects. To take advantage of this knowledge, systematic attention should be paid to human factors (see also Section 6).

7.8. Applicable design principles or requirements for human factors should be observed to ensure compatibility with the users, comprehensibility and effectiveness of the human–machine interface. The system design process should incorporate user group feedback and appropriate measures for verification and validation of the human–machine interface. The engineering programme for human factors (as stated in Section 6) should be included in the overall project plan. Analyses and findings in relation to human factors should be systematically documented in the course of the engineering design, following applicable engineering guides and references to human factors.

7.9. The evaluation of design choices for the human–machine interface is encouraged, beginning with the first stages of the design, initially using mock-ups and computerized visualization aids. In the late stages of design, a full scope control room simulator should be used to validate the control room design.

7.10. The design should take into account the possibility of human error — both errors of omission and errors of commission — on the part of the system's users. To minimize the likelihood of serious adverse consequences resulting from user errors, the human–machine interface should, to the extent possible, be structured in design such that single errors on the part of the operator are inconsequential and are detectable and correctable. Situations in which human error has both a relatively high likelihood of occurrence and major adverse consequences should be avoided by means of a suitable system structure or design of the user interface, or by automation.

This publication has been superseded by SSG-39

DESCRIPTION OF THE DESIGN PROCESS

7.11. The development of systems important to safety should be a step by step controlled process. In this approach the development process is organized into an ordered set of distinct phases. Each phase uses information developed in earlier phases and provides output information to be used as the input for later phases. Note that the development of systems important to safety is, by its nature, an iterative process. As the design progresses, faults and omissions made in the earlier stages become apparent and necessitate iterations. An essential feature of this approach is that the products of each development phase should be verified against the requirements of the previous phase, to establish that the design is correct. At certain phases of the development, validation is carried out to confirm that the output (the product of that particular phase) complies with all the functional and other requirements, and that there is no unintended behaviour. The activities for verification and validation should be carried out by teams independent of the designers and developers.

7.12. Typical phases of a systematic development process and an outline of the process described in this Safety Guide are shown in Fig. 4. The boxes show the development activities that should be performed, and the arrows show the intended order and the primary information flow. Figure 5 shows the relationship of verification and validation to the requirements and the various phases of design and implementation. The choice of the particular development activities and their order in this figure and in this Safety Guide are not intended to dictate a particular method of development; other variations may be equally capable of meeting the recommendations concerning principles and attributes.

7.13. The overall design of a nuclear power plant begins with the design of the mechanical and process systems and components of the plant. Subsequently, the design of I&C systems should be developed on the basis of results of (deterministic and/or probabilistic) safety analyses of the selected design basis events (see Section 3). The design process should include a systematic process for establishing the list of selected design basis events, since omissions may result in the incorrect specification of requirements for the safety provisions and hence in an unsafe system.

7.14. On the basis of the results of these analyses, the requirements for the safety system are elicited. Specialists in nuclear safety and other engineering disciplines, as appropriate, should contribute to the definition of the requirements for the safety system. Normally, changes to the initial design are necessary and a new design is created, followed again by safety analysis. After a few iterations, a configuration of mechanical, process and I&C systems is reached in which all current nuclear safety requirements are met.

This publication has been superseded by SSG-39

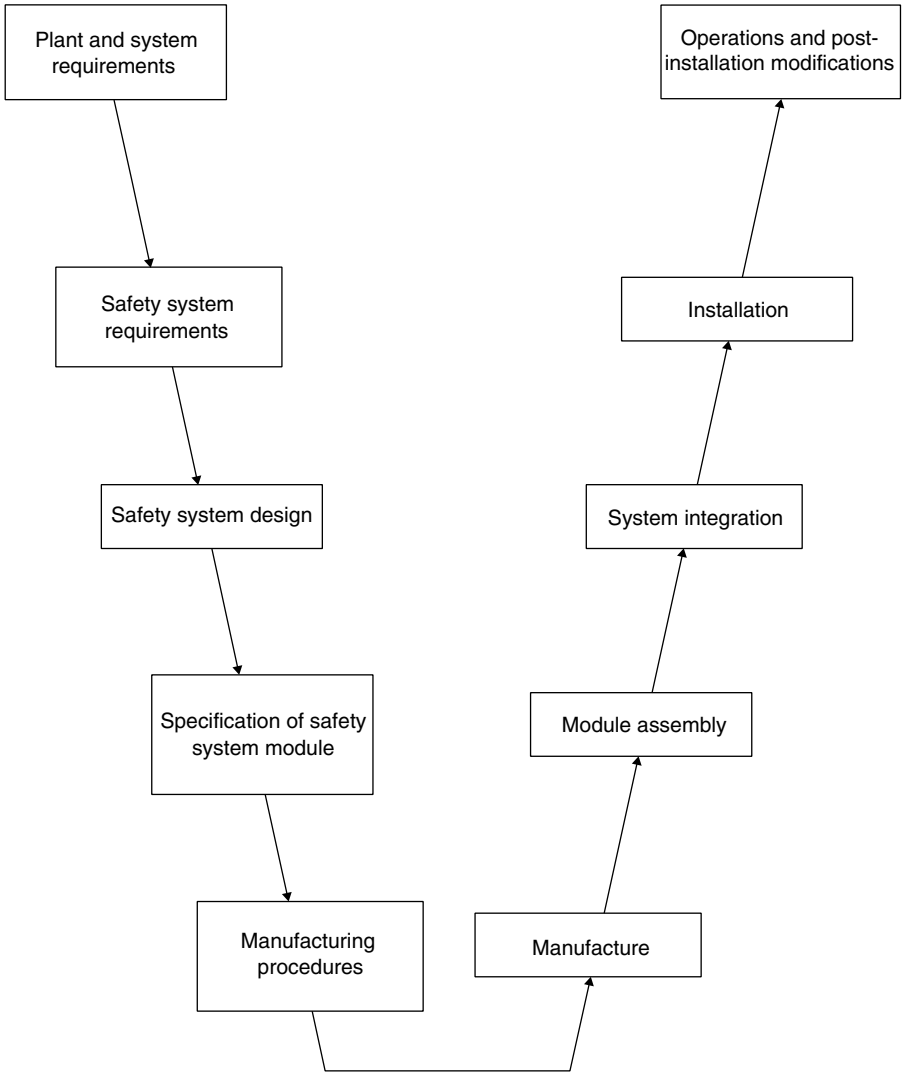

FIG. 4. Development of an I&C system important to safety.

7.15. Once the design has been developed to a stage where it is known how the requirements are to be fulfilled and how the major plant systems and components will be configured, the design documentation is usually issued as specifications for procurement. In negotiating the contracts for plant systems and equipment, the designer

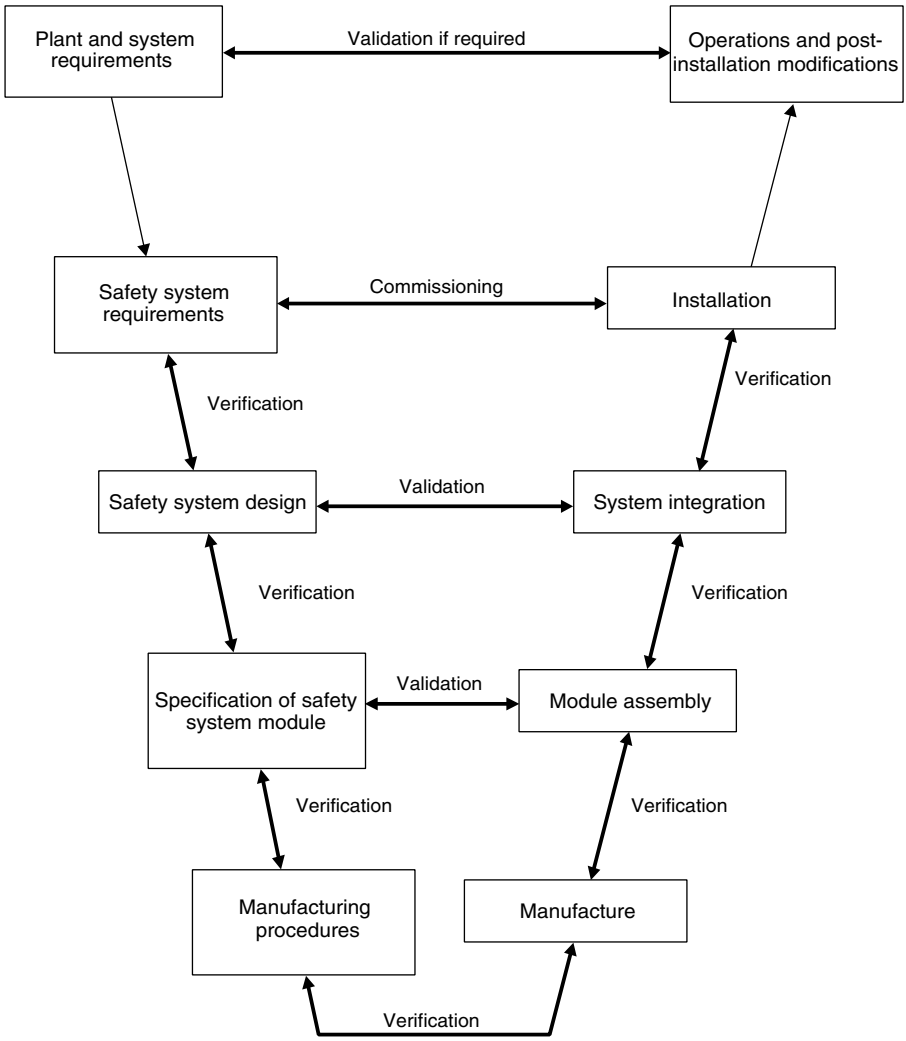

FIG. 5. Verification, validation and commissioning processes.

should establish a means of communication which will ensure that the implementation offered by the suppliers can be shown to meet the requirements of the system. Effective verification and validation activities should be established by the designer and the suppliers.

This publication has been superseded by SSG-39

7.16. Once the requirements for the I&C safety system have been determined, the I&C designer sets out how each requirement will be fulfilled, by preparing the design requirements for the I&C safety system. If a computer based system is proposed, then the designer should prepare the requirements for the computer system and should decide on the systems architecture and the functions to be performed. Similarly, the assignment of human and/or machine functions should also be decided upon. At this stage in the design it will become apparent for which parts of the design readily available techniques can be relied upon and which parts will necessitate specific efforts to develop. Where development is necessary and prototyping is called for, other models of design processes may be more effective, e.g. the spiral model.

7.17. As the I&C design is implemented and modules of the equipment become available, these modules should undergo a series of checks and tests to demonstrate that individual modules or subassemblies perform as required. This is illustrated in Fig. 5. Often at this stage equipment qualification tests begin at the level of the module or subassembly, and generic or type testing may be conducted for equipment that will be used in multiple applications. The individual modules are then integrated into subsystems to perform the functions required by the designer. Further tests, specific to the equipment's configuration, should be carried out to demonstrate that modules function together in their required subsystems. Subsequently the subsystems are combined or integrated to allow a series of 'factory acceptance tests' to be conducted on the system at the supplier's facilities. These tests should demonstrate that the system functionality required by the designer has been correctly implemented.

7.18. Once the designer is satisfied that the system performs the required functions at the supplier's facilities, the equipment is shipped to the site and installed. The shipping or installation itself could affect the performance of the equipment, and comprehensive tests should therefore be performed after installation. These installation tests and 'completion tests', in addition to repeating some of the final factory acceptance tests, should ensure that the whole system is tested as it is intended to operate in practice; for example, multiple redundant systems should be tested working together rather than using simulated signals. For a system requiring a long programme of cabling, it is often not practicable to finish cabling before performance of the completion tests. In these circumstances, to be prudent, the tests should be performed once a representative selection of all the different types of connections to the system have been made. In this way any generic problems with interfaces will be readily identified and can be efficiently resolved. Final tests should be carried out with a fully cabled system. At this point the system can be commissioned and demonstrated to function as required. I&C systems should, to the extent possible, be commissioned and functioning before other commissioning activities are carried out which might place demands on the functioning of the I&C system.

This publication has been superseded by SSG-39

UPGRADES AND BACKFITS

7.19. To ensure that nuclear power plants continue to provide reliable power and meet current safety standards, the I&C systems should be periodically modernized. The nuclear industry has faced problems in finding spare parts for analog I&C systems whose hardware was designed and produced 20–30 years ago. Physical ageing of equipment combined with lack of spare parts has increased failure rates and operation and maintenance costs. Furthermore, a number of vendors have reduced their support for analog systems — and there may be instances in which the original supplier is no longer in business. Owing to the considerable improvements in the reliability of digital electronics in recent years, many nuclear utilities have decided to replace old analog I&C systems with computerized systems.

7.20. Advances in digital technology provide the following additional incentives for upgrades:

— more complex functions can be performed;
— greater precision can be achieved;
— a greater amount and variety of information can be compiled and used;
— the user interface can be made more flexible;
— it is easier for the system to detect and deal with anticipated internal faults;
— functional changes can be made without physical changes or even physical access;
— standard processors of known reliability can be used in many applications.

7.21. When a computerized I&C system is part of a backfit or an upgrade, its function in ensuring the safety of the nuclear power plant should be considered. The safety classification of the I&C system should be established according to the criteria given in Section 2. Requirements for system reliability, qualification and quality assurance and other requirements will be defined in accordance with the safety classification.

7.22. For reasons of practicality, as a first step, a specification of the existing system plus a specification of the new or changed system requirements should be made. The design documentation of the existing analog system may lack completeness and accuracy. Performing some degree of ‘reverse engineering’ to recreate design specifications and requirements from the implementation of the design may be necessary.

7.23. Benefits of changes to the operator interface and/or to the control strategies should be weighed against potential costs. Enhancements to the operator interface may require extensive modification of panels and retraining of operators and

This publication has been superseded by SSG-39

maintenance personnel. Furthermore, control room operators should be consulted before the selection of an operator interface, and they also should provide feedback to the design team at the various phases of the development process.

7.24. Detailed information on I&C upgrades can be found in Refs [15, 16].

ANALYSES REQUIRED FOR SAFETY SYSTEMS

Failure analyses

7.25. Analyses should be performed at appropriate stages in the design process for the safety systems to verify that the combination of the major subsystems (the protection system, the safety actuation systems and the safety system support features) can meet, on a continuing basis, the recommendations of this Safety Guide with regard to single failures (see Section 4) and common cause failures, as well as any other requirements for reliability of the safety systems. This should include failure mode analyses to confirm claims made for fail-safe design. These analyses should be documented.

Assessment of test provisions

7.26. An assessment of the final design should be made to verify the adequacy of the test provisions for the protection system, the safety actuation systems and the safety system support features. The results of this assessment should be documented, and those areas of the design that are sensitive to either equipment failure or human error in any aspect of system testing and equipment testing should be identified in the documentation.

Reliability analysis

7.27. In a Member State in which it has been decided to employ numerical requirements for reliability of the safety systems or parts thereof, an appropriate quantitative reliability analysis should be performed using demonstrably relevant component failure rates and mean repair times, in order to:

— take account of random equipment failures;
— take account of common cause failures, including human errors;
— establish the relative importance to reliability of parts of the safety systems;
— establish the initial test intervals consistent with the applicable component failure rates and the system reliability requirements;

This publication has been superseded by SSG-39

— confirm in the course of plant operation that the rates of failure disclosure are consistent with those assumed and that the reliability goals are being met;
— define the actions to be taken if the actual failure rates exceed, or fall short of, the assumed design failure rates; for example, shortening or lengthening the test interval, or replacement of those components that prevent attainment of the reliability goal.

7.28. The results of this analysis should be documented as well as the results of periodic tests, assessments of in-service reliability and any remedial actions taken.

PROBABILISTIC SAFETY ASSESSMENT

7.29. Insights gained from probabilistic safety assessments (PSAs) should be considered in the design, with the goal of ensuring that no particular feature makes a disproportionately large or uncertain contribution to the overall risk. Detailed information on PSAs can be found in Refs [17–20].

ASSUMPTIONS MADE IN THE ANALYSES

7.30. Assumptions made in any analysis required for design verification should be included in the documentation of that analysis. Each assumption should be stated and justified.

DOCUMENTATION FOR THE I&C SYSTEM

7.31. The purpose of the I&C system documentation is: (1) to provide the means of communicating information between the various phases of and the various parties involved in the design process; (2) to provide a record that shows that the requirements have been correctly interpreted and fulfilled in the installed system; (3) to communicate operationally essential design related information to the plant operators; and (4) to provide a foundation for plant maintenance and for potential future revisions to the design.

7.32. For an I&C system important to safety, a significant number of documents are produced in the numerous activities associated with the design process. To ensure that the significance of these documents is recognized, they should be grouped according to their roles in the design process.

This publication has been superseded by SSG-39

7.33. Primary documents are those documents that are integral to the design process and which constitute the input and output documents for each of the phases. A fault in these documents can lead directly to a fault in the system itself. Primary documentation typically includes documentation of the design basis for the purpose of the plant safety analysis, documentation of the safety systems requirements, logic diagrams and as-built drawings.

7.34. Secondary documents are those documents that are associated with the design process and are used by the designer to prepare the input and output documentation. A fault in these documents will not lead directly to a fault in the system, but they could mask the presence of a fault by incorrect reporting of information. Alternatively, acting on the wrong advice of the document could introduce a fault into the system. Typically, the secondary documents define and record activities associated with the design process, such as the verification and validation activities between phases. The verification and validation records are used to determine the necessity of changing the documentation for its associated phases when faults are found.

7.35. Other documents in the programmes for quality assurance, project planning and equipment qualification support the design process. These supporting documents contribute to the organizational, logistic and strategic decisions to be made concerning the design process, which can have an indirect effect on the design.

7.36. The design of an I&C system important to safety should be fully documented by the time it is completed. Documentation should be comprehensive, complete, traceable and verifiable in order to demonstrate the required functionality and dependability of the system. Adequate documentation will facilitate future modification or modernization of the system.

7.37. At the conclusion of the I&C system design, the final design documentation should include a listing of the relevant documents for design, design verification and design validation, and should contain specific references to those documents.

7.38. Documentation for the I&C system should be kept up to date and any modification of the system should be reflected in the documentation. All documents for the I&C system should be maintained under configuration control.

Codes and standards

7.39. A list of the guides, codes and standards that apply to the design of an I&C system important to safety, as well as the associated indicators of compliance, should be

This publication has been superseded by SSG-39

agreed upon at the outset of the project, and should be documented and communicated to the project authority in the course of the project.

Documentation of the design basis

7.40. The final design basis should be documented. This should include as a minimum the identification and documentation of:

- the plant operational states in which the system is to be operable;
- the PIEs, with an identification of the corresponding safety and protective tasks for the I&C systems, together with the initial PIE conditions and allowable limits of plant conditions for each such event;
- the variables, or combinations of variables, that are to be monitored to control each protective action, either manually or automatically (or both);
- the ranges and rates of change of those variables or combinations of variables which should be accommodated by the I&C systems important to safety;
- the limiting values for activation of safety systems for each of those variables in each applicable plant operating mode;
- constraints on the control system concerning the allowable values for process variables and other important parameters.

7.41. The critical points in time or critical points in plant conditions which govern system actions after the onset of a design basis event should be documented, including:

- the time or plant conditions for which safety functions are required to be initiated;
- the time or plant conditions that require automatic control of safety functions to be started;
- the time or plant conditions that define proper completion of the safety function;
- the time or plant conditions that allow the return of a safety system to its normal stand-by state.

7.42. The methods to be used to determine that the reliability of the safety system's design is appropriate for each safety system function, and any qualitative or quantitative reliability goals that may be imposed on the system design, should be documented.

7.43. Any special bandwidth related constraints (such as required sampling rates and data transmission rates) that have implications for the design of the system should be documented.

This publication has been superseded by SSG-39

7.44. For each protective task identified whose operation may be controlled by manual means from the outset or after initiation, the following should be documented:

— the time and plant conditions for which manual control is allowed;
— the justification for permitting initiation, or control subsequent to initiation, by solely manual means;
— the range of environmental conditions imposed upon the operator in plant operational states and accident conditions throughout which the manual operations are required to be performed;
— the variables, as mentioned earlier, that are required to be displayed so that the operator can take them into account in taking manual action.

7.45. The range of transient and steady state conditions (such as voltage and frequency) of the safety system support features should be identified and documented for those plant operational states and accident conditions in which the systems important to safety are required to function.

7.46. The range of transient and steady state environmental conditions (such as conditions of radiation, temperature, humidity, pressure and vibration) in which the systems important to safety are required to perform should be documented for plant operational states and accident conditions, and for external events.

7.47. Conditions with the potential to functionally degrade the performance of safety systems and for which provisions have been made to retain the capability for performing safety functions (e.g. missile impact, pipe break, fire, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in systems of different safety class) should be documented.

7.48. Those plant conditions in which the bypass of safety tasks is permitted should be identified. The means of enabling such approved bypasses, together with essential indicators, should also be described.

7.49. The processes for engineering design and specification that are to be followed for systems and components should be documented.

Documentation of the I&C system design

7.50. The design of the I&C systems important to safety should be documented. This documentation should include, as a minimum, the following information.

This publication has been superseded by SSG-39

Function

7.51. Each I&C system should be classified, as specified in Section 2.

7.52. The design basis of each system should be documented, including its safety related duties, interfaces with other systems, and the PIEs and plant conditions to which the safety related duties apply.

7.53. The functions provided by each I&C channel should be documented. This includes documents of indicators, alarms and control characteristics, and, where applicable, stability margins.

7.54. For the protective tasks, a precise and clear description of plant conditions and the indicators of these conditions, whose achievement defines completion of the protective task, should be documented.

Performance

7.55. A description of the range, accuracy and response time required for the overall system and for each channel should be provided.

7.56. Documentation should be provided to demonstrate the qualification, functional performance and any other special requirements for the system and its components.

7.57. A listing of the equipment in the I&C system important to safety whose performance may not meet the functional requirements of the system for the full service life of the plant, including the criteria determining the end of equipment life and the expected lifetime, should be part of the documentation.

7.58. For safety systems (i.e. the protection system, the safety actuation system and the safety system support features), information should be provided on the maximum times permitted and the expected times needed to accomplish the required safety functions.

7.59. The safety system analyses identified in paras 7.25–7.28 should be described, with reference made to the related design documentation.

Qualification

7.60. A description should be provided of the environmental conditions in which each component has to operate, including normal conditions, anticipated operational occurrences and design basis accident conditions.

This publication has been superseded by SSG-39

7.61. The power supply or supplies from which each system will operate in normal conditions, anticipated operational occurrences and design basis accident conditions should be identified.

7.62. Verification of the requirements for the qualification of each component or system should be provided.

Test and maintenance

7.63. A schedule for testing, inspection and periodic maintenance, intended to ensure the required availability of equipment, should be specified.

7.64. The requirements pertinent to testing, maintenance and inspection should be specified, together with any potential impairment, risk or degradation that could result from such activity.

Operations

7.65. The principles of system operation in all operational states should be described. The description should specify the related signals and required automatic actions or actions to be performed by the operator.

7.66. Operating instructions and maintenance instructions should be provided.

Procedures and instructions

7.67. Instructions for operation, commissioning and maintenance relevant to the system should be referenced.

Spare components

7.68. Technical purchasing specifications should be available for each component.

7.69. In order to maintain the design basis into the future, the criteria and rationale for the selection of spare components should be documented.

7.70. The documentation requirements for quality assurance set out in IAEA safety standards on quality assurance should be met. (See Ref. [3], Safety Guides Q3 and Q10, for additional guidance.)

This publication has been superseded by SSG-39

Organization of documentation

7.71. Documentation should be organized into a structure such as the following:

— the functions delivered by the system and its functional design;
— the system's design features;
— the system's facilities for testing, diagnostic and maintenance, and their operation;
— documentation of test results;
— equipment qualification;
— the design process and quality requirements followed in the design;
— strategies for maintenance;
— strategies for commissioning;
— methods for verification and validation of the design;
— system operation;
— programmes for maintenance, surveillance and periodic testing;
— provision of spare parts and/or components.

Documentation of the I&C safety system

7.72. When the design of the I&C safety system is completed, the expected functional performance and reliability of the system should be documented. This documentation should include, as a minimum, the following information:

— A summary description of the design basis, the rationale for design changes including input from the review of operating experience (if applicable), the functional design of the system and the philosophy underlying the particular choice of design.
— A comprehensive description of the system, which should include information on all monitored variables (process variables, operator signals) and controlled variables (output to actuators and indicators) for all operational modes of the system. This description should also include the methods of data presentation (e.g. hard wired or computer based methods).
— Details of any dependence on the operating characteristics of any interfaced system, safety actuation systems, other safety related system or safety system support feature, including power supply.
— The variables, or combinations of variables and the combination methods used, that are to be monitored for the purposes of taking protective action. The information to be provided should include the minimum number and locations of the sensors necessary to monitor adequately all variables important to safety, including those that have a spatial dependence (i.e. whose measured values vary

This publication has been superseded by SSG-39

as a function of position in a particular region, as for neutron flux). The calculated ranges and rates of change of the variables or combinations of variables mentioned earlier should be specified.

— The number of I&C channels, their functions and input–output logic, as well as information on indicators, alarms and control characteristics, including margins of safety, production and stability.
— The description of the system should include the locations (e.g. plant grid and elevation, room number or area number) of sensors, racks, cabinets, panels, operator controls and operator displays as well as of facilities for manual adjustment and system testing.
— The PIEs, together with their corresponding tasks for protection and safety.
— The variables, or combinations of variables, that are to be monitored to provide protective actions for each design basis event.
— The limiting safety system settings for each variable listed, in each applicable plant operating mode, including all operational and maintenance bypass conditions and any allowances made for errors in instrument calibration. The margin between the safety system settings and the level considered to mark the onset of unsafe conditions should be identified, together with appropriate information for interpretation.
— The maximum permitted response times of the safety systems necessary to accomplish all the tasks for protection and safety.
— The reliability criterion for each protective task.
— The conditions whose achievement defines completion of the protective task.
— The nominal safety system settings for each variable or combination of variables.
— The range, lifetime and expected accuracy for each item of the safety system equipment.
— The design analyses identified in paras 7.25–7.28.
— The documentation verifying the requirements for qualification and functional performance, and any other special requirements for the safety system equipment.
— A listing of that equipment in the safety system whose performance may not meet the functional requirements of the system for the full service life of the plant. The criteria for determining the end of equipment life and the expected lifetime should be stated.
— A listing of applicable codes and standards for the design of the safety system.
— The plant conditions in which the bypassing of identified safety tasks is permitted (for applicable permissive conditions, see paras 5.36–5.38).

This publication has been superseded by SSG-39

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Software for Computer Based Systems Important to Safety in Nuclear Power Plants, Safety Standards Series No. NS-G-1.1, IAEA, Vienna (2000).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Quality Assurance for Safety in Nuclear Power Plants and Other Nuclear Installations, Code and Safety Guides Q1–Q14, Safety Series No. 50-C/SG-Q, IAEA, Vienna (1996).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook, Technical Reports Series No. 387, IAEA, Vienna (1999).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Single Failure Criterion, Safety Series No. 50-P-1, IAEA, Vienna (1990).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Fire Protection in Nuclear Power Plants, Safety Series No. 50-SG-D2 (Rev. 1), IAEA, Vienna (1992).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection Against Internally Generated Events and their Secondary Effects in Nuclear Power Plant Design, Safety Series No. 50-SG-D4, IAEA, Vienna (1980).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, External Man-induced Events in Relation to Nuclear Power Plant Design, Safety Series No. 50-SG-D5 (Rev. 1), IAEA, Vienna (1996).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Ultimate Heat Sink and Directly Associated Heat Transport Systems for Nuclear Power Plants, Safety Series No. 50-SG-D6, IAEA, Vienna (1981).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Equipment Qualification in Operational Nuclear Power Plants: Upgrading, Preserving and Reviewing, Safety Reports Series No. 3, IAEA, Vienna (1998).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Emergency Power Systems at Nuclear Power Plants, Safety Series No. 50-SG-D7 (Rev. 1), IAEA, Vienna (1991).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Design Aspects of Radiation Protection for Nuclear Power Plants, Safety Series No. 50-SG-D9, IAEA, Vienna (1985).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparedness and Response for a Nuclear or Radiological Emergency, Safety Standards Series No. GS-R-2, IAEA, Vienna (in preparation).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design and Qualification for Nuclear Power Plants, Safety Series No. 50-SG-D15, IAEA, Vienna (1992).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Modernization of Instrumentation and Control in Nuclear Power Plants, IAEA-TECDOC-1016, IAEA, Vienna (1998).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Specifications of Requirements for Upgrades Using Digital Instrumentation and Control Systems, IAEA-TECDOC-1066, IAEA, Vienna (1999).

This publication has been superseded by SSG-39

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Treatment of External Hazards in Probabilistic Safety Assessment for Nuclear Power Plants, Safety Series No. 50-P-7, IAEA, Vienna (1995).

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2): Accident Progression, Containment Analysis and Estimation of Accident Source Terms, Safety Series No. 50-P-8, IAEA, Vienna (1995).

[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants, Safety Series No. 50-P-10, IAEA, Vienna (1995).

[20] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3): Off-Site Consequences and Estimation of Risks to the Public, Safety Series No. 50-P-12, IAEA, Vienna (1996).

This publication has been superseded by SSG-39

GLOSSARY

The following definitions apply for the purposes of the present publication.

accident conditions. Deviations from normal operation more severe than anticipated operational occurrences, including design basis accidents and severe accidents.

actuated equipment. An assembly of prime movers and driven equipment used to accomplish one or more safety tasks.

actuation device. A component that directly controls the motive power for actuated equipment. Examples of actuation devices include circuit breakers and relays that control the distribution and use of electric power and pilot valves controlling hydraulic or pneumatic fluids.

anticipated operational occurrences. An operational process deviating from normal operation which is expected to occur at least once during the operating lifetime of a facility but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions.

availability. The fraction of time during which a system is capable of performing its intended purpose.

bypass. A device to inhibit, deliberately but temporarily, the functioning of a circuit or system by, for example, short circuiting the contacts of a relay.

maintenance bypass. A bypass of safety system equipment during maintenance, testing or repair.

operational bypass. A bypass of certain protective actions when they are not necessary in a particular mode of plant operation.[4]

channel. An arrangement of interconnected components within a system that initiates a single output. A channel loses its identity where single output signals are combined with signals from other channels, e.g., from a monitoring channel, or a safety actuation channel.

[4] An operational bypass may be used when the protective action prevents, or might prevent, reliable operation in the required mode.

This publication has been superseded by SSG-39

coincidence. A feature of protection system design such that two or more overlapping or simultaneous output signals from several channels are necessary in order to produce a protective action signal by the logic.

common cause failure. Failure of two or more structures, systems or components due to a single specific event or cause.

component. A discrete element of a system. Examples are wires, transistors, integrated circuits, motors, relays, solenoids, pipes, fittings, pumps, tanks and valves.

dependability. A general term describing the overall trustworthiness of a system; that is, the extent to which reliance can justifiably be placed on this system. Reliability, availability and safety are attributes of dependability.

design basis accident. Accident conditions against which a nuclear power plant is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits.

diversity. The presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure.

driven equipment. A component such as a pump or valve that is operated by a prime mover.

functional isolation. Prevention of influences from the mode of operation or failure of one circuit or system on another.

item important to safety. An item that is part of a safety group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public.

logic. The generation of a required binary output signal from a number of binary input signals according to predetermined rules, or the equipment used for generating this signal.

multiplexing. Transmission and reception of two or more signals or messages over a single data channel, e.g. by the use of time division, frequency division or pulse code techniques.

This publication has been superseded by SSG-39

normal operation. Operation within specified operational limits and conditions.

nuclear safety. The achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation hazards.

operational states. States defined under normal operation and anticipated operational occurrences.

physical separation. Separation by geometry (distance, orientation, etc.), by appropriate barriers, or by a combination thereof.

postulated initiating event. An event identified during design as capable of leading to anticipated operational occurrences or accident conditions.

prime mover. A component, such as a motor, solenoid operator or pneumatic operator, that converts energy into action when commanded by an actuation device.

protection system. System which monitors the operation of a reactor and which, on sensing an abnormal condition, automatically initiates actions to prevent an unsafe or potentially unsafe condition.

protective action. A protection system action calling for the operation of a particular safety actuation device.

protective task. The generation of at least those protective actions necessary to ensure that the safety task required by a given postulated initiating event is accomplished.

quality assurance. Planned and systematic actions necessary to provide adequate confidence that an item, process or service will satisfy given requirements for quality, for example, those specified in the licence.

quality control. Part of quality assurance intended to verify that structures, systems and components correspond to predetermined requirements.

redundancy. Provision of alternative (identical or diverse) structures, systems or components, so that any one can perform the required function regardless of the state of operation or failure of any other.

This publication has been superseded by SSG-39

reliability. The probability that a system will meet its minimum performance requirements when called upon to do so.

response time. The period of time necessary for a component to achieve a specified output state from the time that it receives a signal requiring it to assume that output state.

safety action. A single action taken by a safety actuation system[5].

safety actuation system. The collection of equipment required to accomplish the necessary safety actions when initiated by the protection system.

safety function. A specific purpose that must be accomplished for safety.

safety group. The assembly of equipment designated to perform all actions required for a particular postulated initiating event to ensure that the limits specified in the design basis for anticipated operational occurrences and design basis accidents are not exceeded.

safety limits. Limits on operational parameters within which an authorized facility has been shown to be safe.

safety related instrumentation and control (I&C) system. An I&C system important to safety which is not part of a safety system.

safety system. A system important to safety, provided to ensure the safe shutdown of the reactor or residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents.

safety system support features. The collection of equipment that provides services such as cooling, lubrication and energy supply required by the protection system and the safety actuation systems[6].

---

[5] For example, insertion of a control rod, closing of containment valves or operation of the safety injection pumps.

[6] After a postulated initiating event, some required safety system support features may be initiated by the protection system and others may be initiated by the safety actuation systems they serve; other required safety system support features may not need to be initiated if they are in operation at the time of the postulated initiating event.

This publication has been superseded by SSG-39

safety task. The sensing of one or more variables indicative of a specific postulated initiating event, the signal processing, the initiation and completion of the safety actions required to prevent the limits specified in the design basis from being exceeded and the initiation and completion of certain services from the safety system support features.

single failure. A failure which results in the loss of capability of a component to perform its intended safety function(s), and any consequential failure(s) which result from it.

system life-cycle. All stages from conception to final disposal through which a system passes.

validation. The process of determining whether a product or service is adequate to perform its intended function satisfactorily. For example, for a system such as an I&C system, the process of confirming that the complete system (hardware and software) complies with all its functional and other requirements and has no unintended behaviour.

verification. The process of determining whether the quality or performance of a product or service is as stated, as intended or as required. For example, for a development process, the process of ensuring that a particular phase in the development process meets the requirements imposed on it by the previous phase.

This publication has been superseded by SSG-39

CONTRIBUTORS TO DRAFTING AND REVIEW

Anani, N.	Atomic Energy Control Board, Canada
Bock, H.W.	Siemens, Germany
Duong, M.	International Atomic Energy Agency
Faya, A.	Atomic Energy Control Board, Canada
Hughes, P.J.	HM Nuclear Installations Inspectorate, United Kingdom
Johnson, G.L.	Lawrence Livermore National Laboratory, United States of America
MacBeth, M.	Atomic Energy of Canada Ltd, Canada
Pachner, J.	International Atomic Energy Agency
Pauksens, J.	Atomic Energy of Canada Ltd, Canada
Rollinger, F.	Institut de Protection et de Sûreté Nucléaire, France

This publication has been superseded by SSG-39

BODIES FOR THE ENDORSEMENT OF SAFETY STANDARDS

Nuclear Safety Standards Committee

Argentina: Sajaroff, P.; *Belgium:* Govaerts, P. (Chair); *Brazil:* Salati de Almeida, I.P.; *Canada:* Malek, I.; *China:* Zhao, Y.; *France:* Saint Raymond, P.; *Germany:* Wendling, R.D.; *India:* Venkat Raj, V.; *Italy:* Del Nero, G.; *Japan:* Hirano, M.; *Republic of Korea:* Lee, J.-I.; *Mexico:* Delgado Guardado, J.L.; *Netherlands:* de Munk, P.; *Pakistan:* Hashimi, J.A.; *Russian Federation:* Baklushin, R.P.; *Spain:* Mellado, I.; *Sweden:* Jende, E.; *Switzerland:* Aberli, W.; *Ukraine:* Mikolaichuk, O.; *United Kingdom:* Hall, A.; *United States of America:* Murphy, J.; *IAEA:* Hughes, P. (Co-ordinator); *European Commission:* Gómez-Gómez, J.A.; *International Organization for Standardization:* d'Ardenne, W.; *OECD Nuclear Energy Agency:* Royen, J.

Commission for Safety Standards

Argentina: D'Amato, E.; *Brazil:* Caubit da Silva, A.; *Canada:* Bishop, A., Duncan, R.M.; *China:* Zhao, C.; *France:* Lacoste, A.-C., Gauvain, J.; *Germany:* Renneberg, W., Wendling, R.D.; *India:* Sukhatme, S.P.; *Japan:* Suda, N.; *Republic of Korea:* Kim, S.-J.; *Russian Federation:* Vishnevskiy, Y.G.; *Spain:* Martin Marquínez, A.; *Sweden:* Holm, L.-E.; *Switzerland:* Jeschki, W.; *Ukraine:* Smyshlayaev, O.Y.; *United Kingdom:* Williams, L.G. (Chair), Pape, R.; *United States of America:* Travers, W.D.; *IAEA:* Karbassioun, A. (Co-ordinator); *International Commission on Radiological Protection:* Clarke, R.H.; *OECD Nuclear Energy Agency:* Shimomura, K.