Australian Government
Australian Radiation Protection and Nuclear Safety Agency

arpansa

Regulatory guide

Construction of an item important for safety

This document provides guidance for licence holders on the identification, classification, design and construction of items important to safety. Construction of such items requires prior approval from the CEO of ARPANSA under section 66 of the Regulations.

REGULATORY SERVICES

REG-RC-SUP-254A v1.2

December 2018

1. Introduction

The holder of a licence, or a person covered by a licence, must have approval from the CEO of ARPANSA under section 66 of the Australian Radiation Protection and Nuclear Safety Regulations 2018 (the Regulations) [1] to construct an item that is important for safety. The item must be identified in the safety analysis report as part of the construction of a controlled facility.

Such an item may be a structure, system, or component (SSC) that contributes to managing safety in a facility. Often the detailed design information about a SSC is not fully available at the time of the application to construct the facility. Section 66 allows construction of the facility to be expedited without compromising safety by providing an application and approval process for items important to safety after the licence has been issued.

This guide describes the process for the safety classification of SSCs for controlled facilities, and the design and construction criteria for such items. Items in safety categories 1-3 are subject to regulatory approval.

2. International best practice

In accordance with Government policy, ARPANSA has adopted the 'trusted international standard' principle, under which additional requirements should not be imposed beyond international best practice, unless it can be demonstrated that there is a good reason to do so. International best practice is explained at http://www.arpansa.gov.au/Regulation/ibp/index.cfm.

This regulatory guide is based on international standards published by the International Atomic Energy Agency (IAEA) specified as references [2], [3], [4], [5], & [7].

3. Purpose and scope

This document sets out the regulatory expectations for identifying and classifying items important to safety and provides guidance for the design and construction of such items in a manner that is commensurate with the safety analysis.

4. Classification of items important for safety

The IAEA provides the following definition of an item important for safety [2].

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. Items important to safety include:

- *Those structures, systems and components whose malfunction or failure could lead to undue radiation exposure of site personnel or members of the public;*
- *Those structures, systems and components that prevent anticipated operational occurrences from leading to accident conditions;*
- *Those features that are provided to mitigate the consequences of malfunction or failure of structures, systems and components.*

The aim of safety classification is to identify and classify the items important for safety that were considered in the preliminary safety analysis report (PSAR). These include SSCs that are required to protect

the health and safety of people and the environment from harmful effects of radiation. The licence holder should consider the classification process described in this document in identifying and classifying the items important for safety in the PSAR.

In classifying the structures, systems, or components, their main safety functions should be taken into account. As part of international best practice, ARPANSA adopts the requirements and recommendations of the International Atomic Energy Agency (IAEA) in its regulatory process. According to the IAEA requirements [3] for classification of structures, systems, or components, the requirements for fundamental safety functions[1] are:

> Requirements 4: Fundamental safety functions
>
> *Fulfilment of the following fundamental safety functions for a nuclear power plant[2] shall be ensured for all plant states: (i) control of reactivity, (ii) removal of heat from the reactor and from the fuel store and (iii) confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases*.

A systematic approach should be considered in identifying items important for safety so that these items fulfil the main safety functions and inherent safety features contributing to fulfilling such functions for all plant states are taken into account.

Further, the IAEA requirements for safety classification state:

> Requirement 22: Safety classification
>
> *All items important to safety shall be identified and shall be classified on the basis of their function and their safety significance*.

Classifying the items important for safety should be primarily based on deterministic methods, which will be complemented by probabilistic methods as appropriate. In classifying the items important for safety the following factors should be taken into account:

- the safety function(s) to be performed by the item
- the consequences of failure to perform a safety function
- the frequency with which the item will be called upon to perform a safety function
- the time following a postulated initiating event at which, or the period for which, the item will be called upon to perform a safety function.

5. Classification process

In classifying the items important for safety the functions of the SSCs considered in the design should be taken into account. Such functions may include primary functions and supporting functions that are expected to be performed to achieve the main safety function. These functions include those identified in the PSAR at various levels of defence in depth, i.e. prevention, detection, control and mitigation safety functions.

[1] IAEA has replaced the term 'fundamental safety function' with 'main safety function'.
[2] ARPANSA uses a graded approach for non-power reactor nuclear installations

The functions of the SSCs should be categorised on the basis of their safety significance taking into account the following factors:

- the consequences of failure to perform the function
- the frequency of occurrence of the postulated initiating event for which the function will be called upon
- the significance of the contribution of the function in achieving either a controlled state or a safe state[3].

For categorisation of functions of the SSCs, the licence holder is expected to use a categorisation system similar to that used by the IAEA [4] as such principles of categorisation of SSCs for nuclear installations are widely accepted. In terms of the safety significance in performing the safety functions of the SSCs the following three levels of severity of consequences are considered:

The severity should be considered 'high' if failure of the function could, at worst:

- lead to a release of radioactive material that exceeds the limits considered in the design basis accidents; or
- cause the values of key physical parameters to exceed acceptance criteria for design basis accidents as they relate to the design limits for the items important for safety and the set of accident conditions derived from postulated initiating events for establishing boundary conditions in the design basis accidents

The severity should be considered 'medium' if failure of the function could, at worst:

- lead to a release of radioactive material that exceeds limits established for anticipated operational occurrences; or
- cause the values of key physical parameters to exceed the design limits for anticipated operational occurrences.

The severity should be considered 'low' if failure of the function could, at worst:

- lead to doses to workers above the authorised limits.

In order to adopt a conservative approach in categorisation of functions, the highest of the three levels should be applied when more than one of the above three definitions is met. In assessing the consequences it should be assumed that function does not respond when challenged.

For anticipated operational occurrences, the assessment of the consequences should assume that all other independent functions are performed correctly.

In terms of safety functions the following safety categories are recommended by the IAEA [4].

Safety Category 1

[3] Controlled state: Plant state, following an anticipated operational occurrence or accident conditions, in which the fundamental safety functions can be ensured and which can be maintained for a time sufficient to implement provisions to reach a safe state
Safe state: Plant state, following an anticipated operational occurrence or accident conditions, [in which the reactor is subcritical (for a nuclear power plant and/or a research reactor)] and the fundamental safety functions can be ensured and maintained stable for a long time.

Any function that is required to reach the controlled state after an anticipated operational occurrence or a design basis accident and whose failure, when challenged, would result in consequences of 'high' severity.

Safety Category 2

- Any function that is required to reach a controlled state after an anticipated operational occurrence or a design basis accident and whose failure, when challenged, would result in consequences of 'medium' severity; or
- Any function that is required to reach and maintain for a long time a safe state and whose failure, when challenged, would result in consequences of 'high' severity; or
- Any function that is designed to provide a backup of a function categorized in safety category 1 and that is required to control design extension conditions without core melt (for a reactor).

Safety Category 3

- Any function that is actuated in the event of an anticipated operational occurrence or design basis accident and whose failure, when challenged, would result in consequences of 'low' severity; or
- Any function that is required to reach and maintain for a long time a safe state and whose failure, when challenged, would result in consequences of 'medium' severity; or
- Any function that is required to mitigate the consequences of design extension conditions, unless already required to be categorized in safety category 2, and whose failure, when challenged, would result in consequences of 'high' severity; or
- Any function that is designed to reduce the actuation frequency of the reactor trip or engineered safety features in the event of a deviation from normal operation, including those designed to maintain the main plant parameters within the normal range of operation of the plant; or
- Any function relating to the monitoring needed to provide plant staff and off-site emergency services with a sufficient set of reliable information in the event of an accident (design basis accident or design extension conditions), including monitoring and communication means as part of the emergency response plan (defence in depth level 5), unless already assigned to a higher category.

If the function of the system is considered to be in more than one category, the highest category should be assigned to this category. This is due to the fact that the function is needed for more than one postulated initiating event. The following table summarises the categorisation in terms of the functions in postulated events [4].

Table 1. Relationships between functions credited in the analysis of postulated initiating events and safety categories

Functions credited in the safety assessment	Severity of the consequences if the function is not performed		
	High	**Medium**	**Low**
Functions to reach a controlled state after anticipated operational occurrences	Safety category 1	Safety Category 2	Safety Category 3
Functions to reach a controlled state after design basis accidents	Safety category 1	Safety category 2	Safety Category 3
Functions to reach and maintain a safe state	Safety category 2	Safety category 3	Safety Category 3
Functions for the mitigation of consequences of design extension conditions[4]	Safety category 2 or 3	Not categorised*	Not categorised*

* Medium or low severity consequences are not expected to occur in the event of non-response of a dedicated function for the mitigation of design extension conditions

NOTE: The categorisation of safety functions should not take account of any redundancy, diversity or independence within the design as these aspects relate to the structures, systems and components that deliver the safety functions.

The categorisation assigned to each safety function should be used to classify the SSCs that deliver the function.

Following the categorisation of the safety functions, the SSCs should be assigned to a safety class in accordance with the functions. The SSCs implemented as design provisions should be identified and classified using the same criteria as those used for the classification of SSCs needed to perform safety functions.

Based on the design of the facility/plant, the design provisions can be directly classified into the following three categories in terms of severity of consequences of their failure:

- *Safety class 1*: Any SSC whose failure would lead to consequences of 'high' severity
- *Safety class 2*: Any SSC whose failure would lead to consequences of 'medium' severity
- *Safety class 3*: Any SSC whose failure would lead to consequences of 'low' severity

Note: Design provisions can be directly classified because the significance of SSC's postulated failure fully defines its safety class without any need for detailed analysis of the category of the associated safety function.

Where a SSC performs several functions of different categories, the highest class should be assigned to that SSC.

If the safety class of the connecting or interacting SSCs is not the same, a device of higher safety class should be used for interface to ensure that there will be no effects from a failure of the SSC of the lower safety class.

[4] Accidents conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. Design extension conditions could include severe accident conditions.

Once the safety class is assigned to each SSC, suitable engineering principles and criteria should be applied for design and construction of the SSC to achieve an appropriate level of quality and reliability.

In applying classification, and design principles and criteria a graded approach should be used as necessary in accordance with the importance of the SSC. The IAEA provides a useful guidance on use of a graded approach in relation to research reactors [5].

6. Design principles and criteria

As part of international best practice the widely accepted fundamental principle is defence in depth. Defence in depth is used to provide a high degree of confidence that accidents in facilities will be prevented, and to ensure that the radiological consequences of any design-basis accidents would be minor and within prescribed limits. Furthermore, defence in depth is used to ensure that the likelihood of any beyond-design-basis accident that could have serious radiological consequences is extremely small.

Defence in depth is implemented in the form of a hierarchy of diverse levels of equipment and procedures. The implementation of defence in depth in the design of a facility provides a graded protection against a wide variety of operational occurrences and accidents, including those that might originate from equipment failures and human error, and events that initiate outside the facility. When properly implemented, the principle should ensure that no single human or equipment failure would lead to injury to the public, and unlikely combinations of failures would lead to little or no injury.

Defence in depth affords substantial protection against common cause failures, including performance failures. Performance failures are the class of common cause failures that occur when a system important to safety functions when required (that is, no components fail), but it functions in a way that does not provide the intended protection.

Further details on defence in depth with emphasis on design aspects are described in ARPANSA's regulatory assessment criteria [6] and in the IAEA INSAG Report [7].

Items important to safety are used at all defence in depth levels. Therefore, these items need to be designed and constructed to a standard and quality that is commensurate with their categorisation by safety significance applying appropriate principles and criteria.

The following principles and criteria are used in assessing the design and construction of an item important for safety. At the time of assessment, ARPANSA considers the relevance of each principle and criterion to allow for different types of controlled facility, controlled apparatus or controlled material. ARPANSA may assess some principles and criteria as being not relevant because they do not apply to the particular controlled facility, controlled apparatus or controlled material being assessed. Any principles and criteria relevant to the particular controlled facility, controlled apparatus or controlled material that involve radiation dose limits are regarded as mandatory.

6.1. Conservative proven design and engineering practice

Conservative design, with safety margins, applies at defence in depth levels 1 through 3. Design of structures systems and components with safety functions at these levels of in depth should adopt a conservative approach, and proven technology should be used so that the safety function is performed at an appropriate level.

1. Conservative, proven design and engineering practice should be used for design of items important for safety at defence in depth levels 1-3. At levels 4 and 5 best estimate methodologies should be used.

2. The design establishes conservative operational limits and conditions that allow for engineered tolerance and margins of error. Those limits thus provide safety margins for each operational state and for accident conditions that are based on the safety analysis. Items important to safety should be designed in a manner that is commensurate with the safety analysis.

3. Conservatism should be used in the specification of materials used for pressure retaining structures and components to afford protection against brittle fracture.

4. Feedback from design and operational experience should be taken into account in the design, including feedback of experience from safety system performance testing, maintenance, and the analysis of incidents and safety performance of similar facilities worldwide.

5. Technologies incorporated in the design should be proven technologies, developed through: innovation, laboratory scale demonstrations, operating prototypes, and use in other facilities.

6. Proven engineering practice and standards should be used in design, manufacture, and construction and commissioning of items important for safety.

6.2. Codes and standards

Appropriate codes and standards should be applied to the design, manufacturing, construction, installation, commissioning, quality assurance, testing and inspection of structures, systems and components that are important to safety.

7. The codes and standards applied should reflect the functional reliability requirements of the structures, systems and components and be commensurate with their safety classification.

8. Nuclear-specific standards and codes should be used as available, leading to a conservative design commensurate with the importance of the safety function(s) being delivered. Each code or standard adopted should be evaluated to determine its applicability, adequacy and sufficiency and should be supplemented or modified as necessary to a level commensurate with the importance of the relevant safety function(s).

9. Appropriate nuclear industry-specific, national or international codes and standards should be adopted for Safety Class 1 and 2 structures, systems or components. For Safety Class 3, if there is no appropriate nuclear industry-specific code or standard, an appropriate non-nuclear-specific code or standard should be applied instead.

10. Where a single item (i.e. a structure, system or component) needs to deliver multiple safety functions, and these can be demonstrated to be delivered by the item independently of one another, then separate codes and standards should be used appropriate to the parts of the item providing each safety function. Where such independence cannot be demonstrated, codes and standards should be appropriate to the class of the item (i.e. in accordance with the highest category of safety function to be delivered). Whenever different codes and standards are used for different aspects of the same item, the compatibility between these codes and standards should be demonstrated.

11. If different design codes and standards are used for different parts or aspects of the same item that is important to safety, the consistency between them should be demonstrated.

12. For items important to safety for which there are no appropriate established standards or codes, an approach derived from existing standards or codes for similar items should be applied, or in the absence of such codes and standards, the results of operational experience, tests and analysis should be applied and justified.

13. The safety item designed according to engineering design codes and standards that are already established in another country or are used internationally, and for which use is justified and also judged as acceptable by ARPANSA.

14. Any fabrication and construction processes should follow the codes and standards that are specific to the country in which the facility will be constructed.

15. Where computer-based systems are used in items important to safety:

    - Appropriate standards and practices should be applied in the development, validation, and testing for verification of performance of the hardware and software at each phase of their development.

- The level of reliability assumed in the design of computer-based systems should be conservative unless it can be shown that there is sufficient test and check data from the operational performance of identical elements used in similar applications.

6.3. Redundancy, independence and diversity

Uncertainties and the susceptibility of structures, systems and components to common cause failures can be reduced by the provision of physical and functional independence and diversity between the levels of defence in depth.

16. Independence and diversity should be provided between levels of defence in depth.

17. Safety systems must have sufficient redundancy so that no single fault can lead to failure of the system, including during testing and maintenance and during shutdowns, when safety systems may be degraded.

18. The design of systems important to safety should be subject to safety analyses to determine the required extent of redundancy.

19. The highest degree of physical and functional independence and diversity should be used in redundant systems where the safety significance is highest.

20. Redundant subsystems in safety systems are to be kept functionally and physically separate, from measurement of the process variable (avoiding common sensors) through to shutdown actuation.

21. Diversity should be used in redundant safety systems, from measurement of the process variable through to shutdown actuation.

22. Items important to safety, including items as different as buildings, pumps, water supply systems, process plant, and software, are designed such that their quality and reliability is commensurate with their categorisation by safety significance.

23. The design of items important to safety should address sensitivities to the assumptions made, the data used, and the methods of calculation. Where the design is sensitive to the modelling assumptions, they are supported as far as practicable by additional analyses using independent methods or by experiments and tests.

24. Items important to safety should be designed and qualified to accommodate the effects of the environmental conditions associated with operational states and design- basis accidents (including loss-of-coolant accidents). In the case of design-basis accidents, the environmental conditions are those that would prevail if the items were required to function. The environmental conditions include vibration, temperature, pressure, jet impingement, electromagnetic interference, radiation, and humidity that may exist at the time of need.

25. Safety systems should be distinguished by clear markings (for example, colour codes or fixed notices) so that they stand out in contrast to systems that are not important to safety.

26. Safety systems additionally must be distinguished from safety-related systems by clear markings to emphasise their different categorisations by safety significance.

6.4. Reliability

There should be due consideration of inherent safety features in design of the structures, systems and components.

27. There should not be unsafe failure modes in the structures, systems and components or they should be failsafe.

6.5. Validation and verification

An appropriate program of design verification and validation should be in place that confirms that the design is adequate and in accordance with the design specifications.

28. The program of design verification should include a review of the design of items important to safety, particularly for new design features where special attention is given to potential new failure modes and performance. The review should establish that all required inspections, examinations and tests of items important to safety can be performed throughout the lifetime of the facility.

29. The program of design verification should address environmental and seismic testing to confirm structure, system and component capability as relevant.

30. Computer modelling programs that are used in the design of items important to safety should be verified and validated, addressing:

    - The use of internationally accepted benchmark calculations.
    - The limitations of the programs and the specific conditions for which they are being applied.
    - Support for their results from experimental measurements and irradiation experience.
    - The formal reporting mechanism that is used if output from the programs that has been used in the design process is found to be invalid.

6.6. Testing, inspection and maintenance

Items important for safety should be designed and constructed in such a way that they can be tested, inspected and maintained before operation and throughout the operational lifetime of the facility to assure that the intended design objectives are achieved and any deficiencies are identified and dealt with appropriately to prevent common cause failures.

31. There should be a plan and program for testing, inspection and maintenance for the items important for safety.

32. Where the testing, inspection or maintenance of a safety system requires a change in the configuration appropriate arrangements should be in place for monitoring of such changes and restoration of those changes and for compensating for the temporary unavailability of the items being tested/inspected/maintained.

6.7. Ageing and degradation

The design of structures, systems and components important for safety should take into account the effective management of ageing so that the safety functions are delivered throughout the period needed. The ageing and degradation management of SSCs should be based on international best practice such as IAEA Safety Standards Ageing Management for Research Reactors, Specific Safety Guide, No. SSG-10, IAEA, Vienna, 2010

33. There should be design conservatism for items important to safety regarding ageing and wear-out mechanisms. Allowance should be made for age-related degradation caused for example by vibration, irradiation and thermal cycling.

34. An appropriate program or arrangement should be in place for ageing management for the SSCs. Such program may include monitoring, inspection, maintenance and testing to monitor ageing and degradation processes.

35. An adequate margin should be considered between the intended operational life and predicted safe working life of the items important for safety.

36. A process should be in place to review the obsolescence of structures, systems and components important to safety.

6.8. Quality Assurance

The QA program addresses the design of all structures, systems and components that are important to safety at all defence in depth levels, including process control systems, safety systems, and modifications. Each level of defence in depth can be effective only if the quality of the design can be relied upon.

37. The QA program should be applied to items important to safety to an extent that is commensurate with their categorisation by safety significance, so that the quality of the design is ensured at all times. For each item, the QA program addresses:

    - Design testing to verify performance under operational state and design-basis accident conditions.
    - The incorporation in the design of feedback from operational experience from similar designs, as relevant.
    - The design basis for:
        - the periodic inspection and testing frequencies and procedures
        - the maintenance program
        - the means of verifying performance
        - periodic safety reviews and their frequency

38. Where an item important to safety is computer-based, the QA program should address:

    - Its safety performance and how that is achieved through the use of properly qualified hardware and software.
    - Verification of its performance.
    - Its independent safety assessment by qualified personnel.

- Documentation that permits a review of the item's whole design process, including its testing for verification of performance and its commissioning.

6.9. Plant layout and access

The design and layout should consider the access requirements to the structures, systems and components that contribute to the significant safety function in operating the facility, and the movement of equipment above the items important for safety.

39. The layout should take into account the factors that can affect ease of access to the item important for safety for operational needs.

40. The layout should consider the aspects of construction, installation, testing, maintenance and inspection.

41. Where possible the layout should minimise the lifting of loads and movement of equipment above the items important for safety.

References

[1] Australian Radiation Protection and Nuclear Safety Regulations 2018

[2] International Atomic Energy Agency, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection, 2007 Edition, IAEA, Vienna, 2007

[3] International Atomic Energy Agency, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1, IAEA, Vienna, 2012

[4] International Atomic Energy Agency, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA Safety Standards Series No. SSG-30, IAEA, Vienna 2014

[5] International Atomic Energy Agency, Use of a Graded Approach in the Application of the Safety Requirements for Research Reactors, Specific Guide No. SSG-22, IAEA, Vienna, 2012

[6] Australian Radiation Protection and Nuclear Safety Agency, Regulatory Assessment Criteria for the Design of New Controlled Facilities and Modifications to Existing Facilities, RB-STD-43-00 (Rev 1), 2001

[7] International Atomic Energy Agency, Defence in Depth in Nuclear Safety, International Safety Advisory Group Report INSAG-10, IAEA, Vienna, 1996