

Swedish Radiation Safety Authority Regulatory Code

ISSN 2000-0987



SSMFS 2008:17

The Swedish Radiation Safety Authority's regulations and general advice concerning the design and construction of nuclear power reactors

*Please note that translated versions of the Authority's regulations
lack legal force and are for information purposes only.*

Swedish Radiation Safety Authority Regulatory Code

ISSN 2000-0987

Publisher: Ulf Yngvesson

The Swedish Radiation Safety Authority's Regulations concerning the Design and Construction of Nuclear Power Reactors;¹

SSMFS 2008:17

Published on
30 January 2009

issued on 19 December 2008.

On the basis of Sections 20a and 21 of the Nuclear Activities Ordinance (1984:14), the Swedish Radiation Safety Authority hereby issues² the following regulations.

Application and definitions

Section 1 These regulations apply to measures required to maintain and develop safety in the design and construction of nuclear power reactors with the aim of, as far as reasonably achievable, while taking into account the best available technology, preventing radiological accidents. The regulations comprise provisions on technical and administrative measures.

In terms of application to nuclear power reactors, these regulations supplement the provisions concerning design and construction as well as safety analysis contained in Chapters 2, 3 and 4 of the Swedish Radiation Safety Authority's regulations (SSMFS 2008:1) concerning safety in nuclear facilities.

Section 2 In these regulations, a 'nuclear power reactor' has the same definition as in Section 2 of the Act on Nuclear Activities (1984:3).

'Barrier', 'defence in depth', 'radiological accident' and 'safety function' have the same definitions in these regulations as in the Swedish Radiation Safety Authority's regulations (2008:1) concerning safety in nuclear facilities.

The following terms and definitions are used in these regulations:

<i>diversification:</i>	two or more alternative systems or components that independently of each other perform the same safety task, but in essentially different ways or by having different characteristics
-------------------------	---

¹ These regulations and the general advice were issued previously in the Swedish Nuclear Power Inspectorate's Regulatory Code (SKIFS 2004:2).

² Notification of Section 17 has been made in accordance with Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards (OJ L 24, 21.7.1998, p. 37, Celex 398L0034), amended through Directive 98/48/EC of the European Parliament and of the Council (OJ L 217, 5.8.1998, p. 18, Celex 398L0048).

<i>single failure:</i>	a failure which means that a component cannot fulfil its intended safety task, as well as any consequential failure that arises
<i>common cause failure:</i>	a failure which simultaneously occurs in two or more systems or components due to one specific event or cause
<i>functional separation:</i>	systems or components that do not affect each other's function unintentionally
<i>physical separation:</i>	systems or components that are physically separated through distance or barriers or a combination of these
<i>event class:</i>	<p>classification of events conducted in connection with safety analysis and which reflects an expected probability of an event occurring and affecting reactor performance. The following event classes are used in these regulations:</p> <p><u>Normal operation</u> (H1) Includes disturbances successfully managed by regular operations and control systems without interrupted operation</p> <p><u>Anticipated events</u> (H2) Events that can be expected to occur during the lifetime of a nuclear power reactor</p> <p><u>Unanticipated events</u> (H3) Events that are not expected to occur during the lifetime of a nuclear power reactor, but which can be expected to occur if several reactors are taken into account</p> <p><u>Improbable events</u> (H4) Events that are not expected to occur; this also includes a number of postulated events that are analysed to verify reactor robustness independently of the event frequency. These events are often called 'design basis events'.</p> <p><u>Highly improbable events</u> (H5) Events that are not expected to occur; if the event should nevertheless occur, it can result in major core damage. These events are the basis of the nuclear power reactor's mitigating systems for severe accidents.</p> <p><u>Extremely improbable events</u> (residual risks) Events that are so improbable that they do not need to be taken into account as initiating events in connection with safety analysis</p>

<i>nuclear fuel bundle:</i>	nuclear fuel pins with accessories for load-bearing structures and having housing (boxes) that in boiling water reactors surrounds the fuel pins and load-bearing structure components ³
<i>reactor core:</i>	part of the reactor where nuclear fission is designed to occur and which includes the nuclear fuel bundles, control rods and neutron detectors
<i>redundancy:</i>	two or more alternative – identical or different – systems or components that independently of each other perform the same safety task
<i>safety systems:</i>	systems that have the function of ensuring reactor shutdown and residual heat removal, as well as systems needed to mitigate sequences of events up to and including the event class ‘improbable events’.

Design principles for defence in depth

Section 3 The nuclear power reactor shall be designed so that the safety functions of reactivity control, protection of the primary system integrity, emergency core cooling, residual heat removal and the containment function⁴ can be maintained to the extent needed depending on the operational state during all events up to and including the event class improbable events.

The design shall take into account events in the event class highly improbable events in accordance with Sections 4 to 9 as well as Sections 18 to 20.

Section 4 The following design principles shall be applied in the design of the reactor’s defence in depth to the extent that is reasonably practicable:

- (a) Simplicity and durability in the design of the safety systems
- (b) Redundancy, including diversification as well as physical and functional separation in the design of the safety functions
- (c) Automatic control or passive function in necessary activation and operational change of the safety functions
- (d) Failure in safety classified equipment leading to an acceptable level for safety

³ The term ‘fuel assembly’ is used synonymously with ‘nuclear fuel bundle’ in connection with both boiling water reactors and pressurized water reactors. However, one difference is that pressurized water reactors do not use fuel boxes.

⁴ In the case of boiling water reactors, the containment function refers to its leaktightness function and pressure suppression function; for pressurized water reactors, this refers to the leaktightness function.

(e) Failure in operations classified equipment may not affect the performance of equipment with a safety function

(f) When safety systems are shared between reactors, a failure in one of the reactors shall not affect the possibility to perform shutdown and residual heat removal in the other reactors

Manual measures in connection with necessary activation and operational change of reactor safety functions may only be applied if the personnel is given sufficient time – time for consideration – in order to safely take the measures.

Section 5 The reactor containment shall be designed taking into account phenomena and loads that can occur in connection with events in the event class highly improbable events to the extent needed in order to limit the release of radioactive substances to the environment.

Section 6 Instrumentation shall be available making it possible to monitor the parameters that are essential for dealing with all events up to and including the event class highly improbable events.

Section 7 It shall be possible to cool the reactor core through spraying or sufficient water cover for all types and sizes of coolant loss that can result from breaks in connections to the reactor pressure vessel.

Section 8 It shall be possible in all events up to and including the event class highly improbable events to achieve a stable end state with a water-covered core/core melt and established residual heat removal. It shall be possible to cool a molten core over an extended period of time.

Resilience to failures and other internal and external events

Section 9 The safety functions in accordance with Section 3 shall be able to withstand single failures in all events up to and including the event class improbable events. In connection with events in the event class highly improbable events, the active components that belong to the mitigating systems shall be able to withstand a single failure.

Section 10 Reasonable technical and administrative measures shall be taken in order to counteract common cause failures in connection with design, manufacturing, installation, startup, operation and maintenance of safety systems.

Section 11 In order to counteract simultaneous failure of redundant parts of safety systems, the nuclear power reactor shall be designed so that the redundant parts and their support functions have sufficient physical and functional separation.

The degree of separation shall be determined based on the consequences in the facility of the initiating events, which result in the need to actuate the safety system.

Section 12 The nuclear power reactor shall be able to withstand global and local loads and other effects which can occur in connection with a pipe break.

The consequences of a pipe break as an initiating event shall be analysed and assessed with respect to how such effects have an impact on the barriers and the safety functions credited in connection with the pipe break.

Section 13 Local dynamic effects do not need to be taken into account in the parts of the facility where the pipe systems have been given such a design, operating conditions and environmental conditions that the potential for damage to the piping, as a result of known and identifiable degradation mechanisms, has been reduced as far as possible and where measures have been taken so that damage which in spite of this can arise leads to detectable leakage before pipe break occurs.

Further provisions concerning the design, manufacturing and control of pipe systems are stipulated in the Swedish Radiation Safety Authority's regulations (SSMFS 2008:13) concerning mechanical components in certain nuclear facilities.

Section 14 The nuclear reactor shall be dimensioned to withstand natural phenomena and other events that arise outside or inside the facility and which can lead to a radiological accident. In the case of such natural phenomena and events, dimensioning values shall be established. Natural phenomena and events with such rapid sequences that there is no time to take protective measures when they occur shall also be assigned to an event class. For each type of natural phenomenon that can lead to a radiological accident, an established action plan shall be available for the situations where the dimensioning values run the risk of being exceeded.

Section 15 Equipment with operability requirements may be taken off line for planned maintenance during operation if the nuclear power reactor is designed so that the safety systems concerned can withstand a single failure in connection with the measures and the applied diversification and separation of the safety function concerned can be maintained.

Section 16 Equipment with operability requirements may be taken off line for repair and testing during operation if the nuclear power reactor is designed so that the safety functions in accordance with Section 3 can withstand a single failure in connection with the measures. Such repair and testing may be applied, even if a safety function does not withstand a single failure in connection with the measures, provided that a safety analysis shows that the risk contribution that arises in such a way is very small.

Environmental tolerance and environmental impact⁵

Section 17 The barriers and equipment belonging to the safety systems of the nuclear power reactor shall be designed so that they withstand the environmental conditions that the barriers and equipment can be subjected to in the situations where their function is credited in the safety analysis of the reactor.

Equipment in the nuclear power reactor shall not have such an environmental impact that the performance of the reactor's safety functions is reduced.

Provisions concerning control rooms

Section 18 It shall normally be possible to control and monitor the nuclear power reactor from the main control room during all operational states, and it shall be possible to take measures from the main control room to bring the reactor to a safe state and to keep the reactor in this state during all events up to and including the event class improbable events.

Section 19 Events that can threaten continued activity in the main control room shall be identified and an established action plan shall be available for dealing with such threats while maintaining reactor safety.

Section 20 In the case of events where the main control room is not available, an emergency control post shall be available offering adequate instrumentation and manoeuvring possibilities so that the reactor can be brought to hot shutdown, the residual heat removed and necessary safety parameters can be monitored. The emergency control post shall be physically and functionally separated from the main control room. Monitoring from the emergency control post shall also be possible in the event of a single failure in one of the systems necessary for the safe shutdown and cooling of the reactor.

When bringing the reactor to cold shutdown, other local manoeuvring posts besides the emergency control post may be used. However, it shall be possible to perform the supervision and monitoring of cold shutdown from the emergency control post.

Safety classification

Section 21 Structures, systems, components and devices of the nuclear power reactor shall be divided into safety classes. The detailed quality and functional requirements resulting from this safety classification shall be defined and controlled by specifying sub-classes, including mechanical quality class, electrical function class as well as classification with respect to seismic and environmental tolerance.

⁵ Section 17 with general advice has been notified in accordance with Directive 98/34/EC of the European Parliament and of the Council.

Further provisions concerning quality classification are stipulated in the Swedish Radiation Safety Authority's regulations (SSMFS 2008:13) concerning mechanical components in certain nuclear facilities.

Event classification

Section 22 In order to analyse safety, the initiating events included in the deterministic safety analysis in accordance with Chapter 4, Section 1 of the Swedish Radiation Safety Authority's regulations (SSMFS 2008:1) concerning safety in nuclear facilities shall be divided into a limited number of event classes with specified analysis assumptions and acceptance criteria. These event classes shall cover normal operation, anticipated events, unanticipated events, improbable events and highly improbable events. When analysing events that have not been taken into account in the reactor design, realistic analysis assumptions and acceptance criteria may be applied.

Provisions concerning the reactor core

Section 23 The reactor core and connecting systems shall be designed so that:

- design limits for the core can be met with adequate margins in all events up to and including the event class anticipated events
- power transients are not possible, or can reliably be detected and mitigated without exceeding the design limits of the nuclear fuel bundles

Section 24 The reactor core and connecting cooling systems shall be designed so that the net impact of the core's immediate reactivity feedback counteracts a reactivity increase during power operation.

Section 25 The reactor core and reactivity control systems shall be designed in such a way that the reactivity addition is limited in all events up to and including the event class improbable events, in order to prevent:

- the design limits for the nuclear fuel bundle coolability from being exceeded
- the reactor pressure vessel internals from being damaged so that core coolability is degraded
- the acceptance limits in the design specifications for the pressure-bearing parts of the reactor's primary system from being exceeded

Section 26 There shall be an established limit for the highest power output from the fuel bundles during normal operation.

In connection with the highest power output in accordance with the first paragraph, it shall be possible to cool the core in the event of a loss of coolant accident. The limit for the highest power output shall be determined so that:

- overheating and embrittlement of the fuel cladding and hydrogen production from the bundles are limited in the event of a loss of coolant accident

- the core geometry is not changed in such a way in the event of a loss of coolant accident that cooling is prevented
- the residual heat from the nuclear fuel bundles can be removed

Section 27 For each fuel design and configuration of the core, established operating limits and parameters shall be in place which shall be monitored and followed up during the operation of the core to the extent needed for meeting the provisions of Sections 23 to 26.

The analyses of the design and operating limits for the reactor core shall be described in the safety analysis report of the nuclear power reactor in accordance with Chapter 4, Section 2 of the Swedish Radiation Safety Authority's regulations (SSMFS 2008:1) concerning safety in nuclear facilities.

Exemptions

Section 28 If there are particular grounds, the Swedish Radiation Safety Authority may grant exemptions from these regulations if this can be done without circumventing the aim of the regulations.

These regulations enter into force on 1 February 2009.

Without any impediment from the first paragraph, measures for complying with the provisions in accordance with Sections 3 to 17 and Section 20 shall be taken by the deadlines established by the Swedish Radiation Safety Authority for each nuclear reactor. The same applies to Section 18 with respect to the introduction of additional monitoring equipment, as well as Section 23 with respect to the introduction of equipment for detection and automatic protective measures against power transients.

SWEDISH RADIATION SAFETY AUTHORITY

ANN-LOUISE EKSBERG

Erik Jende

The Swedish Radiation Safety Authority's general advice on the application of the regulations (SSMFS 2008:17) concerning the design and construction of nuclear power reactors;

SSMFS 2008:17

Published on
30 January 2009

issued on 19 December 2008.

The Swedish Radiation Safety Authority hereby issues the following general advice.

Section 3

This requirement means that the reactor pressure vessel internals, which are also important for maintaining the core geometry, are designed to withstand the loads that can arise during events up to and including the event class improbable events.

Section 4

The equipment included in safety systems should be designed and located in such a way that the probability of deficiencies and malfunctions is low and that safety is adequate even if deficiencies and malfunctions should arise in the equipment. In connection with failures such as loss of power or failures due to external environmental impact, the equipment should assume a fail-safe position.

The provision [b] on reasonably practicable separation in the design of the safety functions means for instance that safety functions should be independent at an initial stage in connection with all events up to and including the event class anticipated events; i.e. the execution of the function should not be dependent on the execution of other functions. In this analysis, realistic analysis assumptions and acceptance criteria can be applied. One example of initiating independence in boiling water reactors is that it should be possible for the reactor to be made sub-critical without reliance on pressure relief and it should be possible for pressure relief to occur without reliance on scram.

The provision [b] also means that equipment with the main task of functioning in order to limit radioactive releases in connection with severe accidents shall not be affected by a malfunction in other equipment in the facility.

As a rule, the provision [c] on automatic control or passive function means that necessary activation and change of the safety functions shall be automatic. If this is neither possible nor reasonable, prepared manual measures can be accepted. No initiating events that require activation of the reactor protection system should, however, result in demands on rapid operator action. Information and time for consideration should always be provided to the operator so that he or she can understand the event sequence, the facility status and have time for thought before the design requires manual action to be taken. Measures required within the first thirty minutes after the initiating event in order to bring the reactor to a safe state should be automated for all events up to and including the event class improbable events.

Reasonable time for consideration should also be allowed for operator action in connection with anticipated and postulated events resulting from the initiating events.

The following time for consideration should apply in the event of severe accidents:¹

- Manual measures should not be needed for the first 8 hours.
- The manual measures that may be needed after 8 hours should be well prepared and controlled by procedures.

Other measures, which are not prepared, should not be needed until after 24 hours.

If an automatic safety function should not be activated when needed, it should be possible to manually activate the function in the main control room. If an automatic function were to jeopardize safety, possibilities outside the control room should have been arranged for in order to interrupt or block the automatic function. This kind of extraordinary measure should be thoroughly analysed and controlled by procedures.

Section 5

The design basis for the reactor containment is events up to and including the event class improbable events, as shown in Section 3. To meet the requirement in Section 5, a safety evaluation should be performed of events and phenomena which may be of importance for containment integrity in highly improbable events. Examples of such events and phenomena which can result in the need to take measures include high pressure melt-through of the reactor pressure vessel, steam explosion, re-criticality, hydrogen fire and containment underpressure.

Section 8

The coolability of a molten core should be covered by the safety evaluation mentioned in the general advice for Section 5.

¹ Included in the event class highly improbable events.

Section 9

A single failure should be postulated to occur in any component, at the most unfavourable point in time, in connection with the initiating event or thereafter. A single failure in passive components does not need to be assumed until 12 hours after the initiating event.

Certain components, such as check valves as well as software and circuit card components, have properties which should be subjected to safety assessment before they are considered to be active or passive components in individual cases. A check valve, which must change position in order to fulfil its safety task, should primarily be considered to be an active component in this safety assessment.

The requirement on the capability of consequence-mitigating systems to withstand a single failure can be considered to be fulfilled if the capability to withstand a single failure exists for active components whose function may be needed within 8 hours after the initiating event, and for components which may be difficult to access for corrective measures when their function is demanded.

Section 10

Technical measures are measures for diversification. A suitable and reasonable diversification should be applied to the design of the safety functions in accordance with Section 3, with realistic analysis assumptions and acceptance criteria for events up to and including the event class unanticipated events, pipe breaks excluded. When designing such a diversification, all existing power supply to all plant systems can be credited.

The reactor protection system should, as far as reasonably practicable, be designed so that the need for protection is identified and so that protective measures are initiated through at least two different parameters, for example pressure and neutron flux, in connection with all events up to and including the event class unanticipated events. The various ways of detecting an event should be functionally separated.

Section 12

Examples of global effects in connection with pipe breaks include pressure and temperature loads in the area where the pipe break occurs, as well as in the adjacent areas to which pressure relief occurs, global vibrations due to condensation loads and loads due to flooding and steam release, including other environmental impact.

Examples of local dynamic effects include pipe whips, reaction forces and jets. The capability to withstand such effects, especially in the case where a pipe break can result in the failure of an entire safety function, should be achieved through pipe whip restraints, missile shields or changes in pipe configurations.

When analysing the measures that must be implemented, a pipe break should be assumed to occur where it is significant to safety, as well as:

- where there are basic preconditions for such damage that can lead to a pipe break, and
- in accordance with the criteria in SRP 3.6.1 and 3.6.2.2

Section 14

Examples of natural phenomena that should be taken into account include:

- extreme winds,
- extreme precipitation,
- extreme ice formation,
- extreme temperature,
- extreme sea waves,
- extreme seaweed/algae growth or other biological conditions that can affect the cooling water intake,
- extreme water level, and
- earthquakes.

Examples of other events that should be taken into account include:

- fire,
- explosion,
- flooding,
- aeroplane crash, and
- disturbances to or loss of the offsite grid.

In connection with a fire hazards analysis of the facility, a fire that causes all equipment in a fire cell³ to fail should be assumed to occur. If a fire hazards analysis can show that the probability of failure of an entire fire cell is low, through protective measures having been taken to prevent fire from spreading, the burn-out of the entire cell need not be assumed. Such a fire hazards analysis should encompass all measures necessary until the fire is extinguished. In the first instance, passive protective measures should be applied, such as room dividers, encapsulation or shielding of equipment, minimized fire loads and distance separation between equipment.

If distance separation alone is counted as a protective measure between redundant pieces of equipment, this should apply to sufficiently large areas and provided that the fire hazards analysis confirms that the separation is sufficient to prevent fire from spreading.

² U.S. Nuclear Regulatory Commission Standard Review Plan: (SRP) 3.6.1 – Plant Design for Protection Against Postulated Piping Failures in Fluid Systems Outside Containment, NUREG 0800. SRP 3.6.2 – Determination of Rupture Locations and Dynamic Effects Associated with the Postulated Rupture of Piping, NUREG 0800.

³ Corresponds to ‘fire compartment’ in accordance with IAEA Safety Guide NS-G-1.7: Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants. International Atomic Energy Agency. Vienna, 2004.

Furthermore, fire should be taken into account as follows when analysing initiating events:

- When analysing fire as an initiating event, an additional fire need not be assumed in the facility.
- When analysing initiating events other than fire, which in turn can result in a fire, a fire should be assumed to occur as a possible consequential failure from the initiating event.
- When analysing events other than fire, which in turn cannot result in a fire, a fire should nonetheless be assumed to occur no earlier than 12 hours after the initiating event. This event sequence need not be combined with a single failure. This applies to initiating events up to and including the event class unanticipated events, apart from pipe breaks.

Section 17

This requirement means that structures, systems, components and devices included in safety systems shall be environmentally qualified. Environments that can affect safety systems should be followed up as long as the systems are utilized for their purposes.

In environmental qualification of electrical equipment in safety systems, the principles for ageing management should be applied as specified in IEC 607804, Reg. Guide 1,895 or IEEE 323.6 In connection with this, acceleration factors for thermal ageing exceeding 250 times, ionising radiation lasting less than 10 days or a dose speed greater than 5 Gy/h should be avoided, or the applicability of the results should be specially justified.

In the case of fuel bundles and control rods, the requirement means that these should be able to withstand the irradiation and environmental conditions in general which can occur during all events up to and including the event class anticipated events.

Analyses of how equipment can affect the reactor safety functions from an environmental standpoint should cover all events taken into account in the safety analysis of the reactor.

Section 18

It should also be possible from the main control room to monitor the operability of the safety functions of the facility, i.e. to check that the equipment has assumed the correct position for operation. In the case of

⁴ International Electrical Commission. Qualification of electrical equipment of the safety system for nuclear power plants.

⁵ U.S. Nuclear Regulatory Commission Regulatory Guide. Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants.

⁶ The Institute of Electrical and Electronics Engineers Inc. Standard for qualifying class 1 E equipment for nuclear power generating stations.

events in the event class highly improbable events, it should be possible to perform an overall assessment of the facility's safety status.

The interface between the operator and the technical process of the facility should be designed so that the operator is given adequate, reliable and integrated information which is sufficient to effectively monitor the reactor safety functions, make decisions within the time available, as well as receive feedback on automatic and manual measures. A suitable way of designing the annunciator presentation is pattern recognition.

The adequacy of the main control room and emergency control post should be evaluated and documented within the framework of the periodic safety review of the facility in accordance with Chapter 4, Section 4 of the Swedish Radiation Safety Authority's regulations (SSMFS 2008:1) concerning safety in nuclear facilities, as well as when operating experience shows that an evaluation is warranted. An evaluation should comprise experience from the operation of the facility and similar facilities and simulator training, evaluations of the interfaces in relation to ergonomic requirements, as well as evaluations of how well the control room design supports the work of the operators. Local control rooms in the facility should be evaluated in connection with modifications, as well as when experience shows that an evaluation is warranted.

Ergonomic requirements and other conditions that need to be taken into account in the man-technology-organisation interaction should be specified at an early stage and taken into account in connection with such modifications to the main control room that relate to these conditions. Recurrent verification and validation of the new solutions should be conducted during the design process so that needed corrections can be made successively. Furthermore, verification and validation should be performed of the entire control room function before modifications are introduced which essentially affect ergonomic or other conditions in the interaction between the operators and the technical process of the facility.⁷

Section 19

The threats against continued activity in the control room, to which the regulation refers, include events such as fire, steam release and flooding. A radiological accident in another reactor at the same site should also be taken into account here. Requirements concerning procedures in connection with threats, such as armed intrusion and sabotage, are stipulated in the regulations mentioned on the physical protection of nuclear facilities.

Section 20

When designing the emergency control post, the events and conditions that result in the unavailability of the main control room should be taken

⁷ Examples of methodology for the evaluation of control room modifications are to be found in "U.S. Nuclear Regulatory Commission: Human Factors Engineering Program Review Model", NUREG 0711.

into account. The personnel should be able to reach the emergency control post in a protected way. The interface should be designed to facilitate the transfer to working at the emergency control post.

Examples of local manoeuvring posts other than the emergency control post include relay rooms, switchgear rooms and local control rooms that do not include the emergency control and monitoring function.

Section 21

The classification provides the basis for fulfilment of the provisions of Chapter 3, Section 4 of the Swedish Radiation Safety Authority's regulations (SSMFS 2008:1) concerning safety in nuclear facilities through the design, manufacturing, installation and testing of structures, systems, components and devices with requirements adapted to their safety importance. The division into safety classes should be conducted in accordance with the principles provided in ANSI/ANS-51.1 for pressurized water reactors and ANSI/ANS-52.1 for boiling water reactors.⁸

Section 22

The selection of the initiating events to be included in each event class should be based on an analysed probability with which the event is expected to occur. However, certain initiating events should be included as postulates in order to verify the robustness of the facility independent of the probability of these events occurring. An example of such an event is loss of coolant at a break of the largest pipe or connection to the reactor pressure vessel.

Section 23

In the design of the core, the impact of changes in coolant temperature, coolant flow, reactor power and reactor pressure should be taken into account. In the case of pressurized water reactors, changes in the boron concentration of the coolant should also be taken into account.

In addition to design measures, boiling water reactors should have procedures for measures that need to be taken in the event of core instability. The procedures should state what characterizes instability, how it is detected and how it is mitigated. The personnel concerned should be well acquainted with the procedures and should be trained in handling instability. The stability margins should be calculated for new core loadings.

Section 25

In order to ensure cooling of the nuclear fuel bundle, the design limits stipulate that the nuclear fuel must not be fragmented in connection with a

⁸ ANS-51.1: American National Standard: Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants. American Nuclear Society, 1983. ANS-52.1: American National Standard: Nuclear Safety Criteria for the Design of Stationary Boiling Water Reactor Plants. American Nuclear Society, 1983.

reactivity accident. The reactivity value of the control rods should be limited so that the energy accumulation in the fuel bundles will not become excessive.

Section 26

When analysing the limit for the highest power output, the acceptance limits specified in 10 CFR 50.46⁹ should be used.

Section 27

In addition to limits for the highest power output, limitations should be defined on margins for fuel bundle overheating and limits for conditions that can lead to stress corrosion cracking of fuel bundles. For pressurized water reactors, there should also be limits for asymmetrical power generation in the core.

When analysing the limitations providing a margin for overheating of the nuclear fuel bundles, acceptance criteria in accordance with SRP 4.4¹⁰ should be used.

Further guidance for handling of nuclear fuel bundles at different stages and in various situations during operation and core configuration modifications, as well as analysis, monitoring, follow-up and documentation, is provided in the IAEA safety standard, “Core Management and Fuel Handling for Nuclear Power Plants”.¹¹

This general advice applies as of 1 February 2009.

SWEDISH RADIATION SAFETY AUTHORITY

ANN-LOUISE EKSBERG

Erik Jende

⁹ Section 50.46 – Acceptance Criteria for Emergency Core Cooling Systems for Light-Water Nuclear Power Reactors. U.S. Code of Federal Regulation. Energy Parts 0 to 50.

¹⁰ U.S. Nuclear Regulatory Commission Standard Review Plan (SRP) 4.4 – Thermal and Hydraulic Design, NUREG 0800.

¹¹ Safety Guide NS-G-2.5: Core Management and Fuel Handling for Nuclear Power Plants. International Atomic Energy Agency, 2002.

Strålsäkerhetsmyndigheten
Swedish Radiation Safety Authority

SE-171 16 Stockholm
Solna strandväg 96

Tel: +46 8 799 40 00
Fax: +46 8 799 40 10

E-post: registrator@ssm.se
Webb: stralsakerhetsmyndigheten.se