Radiation and Nuclear Safety Authority Regulation on Computational and Experimental Demonstration of the Safety of the Design Solutions of a Nuclear Facility

Content

STUK
SÄTEILYTURVAKESKUS
STRÅLSÄKERHETSCENTRALEN
RADIATION AND NUCLEAR SAFETY AUTHORITY

Osoite | Adress | Jokiniemenkuja 1, 01370 Vantaa | Ånäsgränden 1, 01370 Vanda
Address | Jokiniemenkuja 1, 01370 Vantaa, FINLAND
Puh. | Tfn. | Tel. | (09) 759 881, +358 9 759 881 | www.stuk.fi

In accordance with the Radiation and Nuclear Safety Authority's decision, it is issued, by virtue of Section x of the Nuclear Energy Act (xx/yyyy):

Chapter 1: General regulations

Section 1 Scope of Application

SYT-3144 - This regulation applies to the demonstration of the safety of nuclear power plants and nuclear technical facilities. Chapters 1 and 4; section 6, subsections 1, 2 and 4; section 7, subsections 1, 2 and 3; section 12; section 17, subsection 3; section 18, subsection 1; section 19, subsections 1 and 2; and section 21 of the regulation apply to the disposal facility for nuclear waste before the closure of the disposal facility.

Chapter 1 of the regulation applies to analyses of individual components and structures, and section 18 applies to complex assemblies. In other respects, the analyses of these devices and structures are governed by the Radiation and Nuclear Safety Authority's regulation (Y/x/20xx) concerning the equipment and structures of a nuclear facility.

Section 2 Definitions

For the purposes of this regulation:

1. "early release" shall refer to a release requiring protection of the population in the early phase of an accident at a nuclear facility (five hours from the beginning of the accident);
2. "diversity principle" shall refer to ensuring functionality through systems or components that operate on different principles, each of which individually is capable of performing the function;
3. "controlled state" shall refer to the state of a nuclear power plant in which the reactor is subcritical for a long period, or the reactor power is at a safe and stable level required for the management of an operational occurrence; and where the decay heat removal of the reactor is secured, and there are no significant releases from the nuclear power plant into the environment;
4. "operational occurrence" shall refer to an anticipated operational occurrence as referred to in section X of the Government Decree on Nuclear Facilities;
5. "redundancy principle" shall refer to the implementation of alternative systems, structures and components so that any one of them can perform the required function, regardless of the operational status or faults of the others;

6. “postulated accident” shall refer to a Class 1 postulated accident and a Class 2 postulated accident as referred to in section X of the Government Decree on Nuclear Facilities;
7. “design extension condition” shall refer to the extension of a postulated accident as referred to in section X of the Government Decree on Nuclear Facilities;
8. “large release” shall refer to a release of radioactive substances that necessitates extensive protective actions for the population or extensive and long-term restrictions on the use of land and water areas;
9. “safe state” shall refer to a state of a nuclear facility which can be maintained for an extended period and in which the subcriticality and decay heat removal of the nuclear fuel is secured, and there are no significant releases from the plant into the environment;
10. “safety function” shall refer to a function to ensure the safety of a plant or operation aimed at preventing or mitigating the radiation impacts on employees and the public of normal operation, operational occurrences and accidents;
11. “severe reactor accident” shall refer to an accident in a light-water cooled reactor in which a significant portion of the fuel in the reactor loses its original structure;
12. “controlled state in a severe reactor accident” shall refer to the state of a nuclear power plant following a severe reactor accident, in which the removal of decay heat from the reactor core, its remains or the containment is secured, recriticality is no longer a risk, and there is no significant release of fission products from the reactor core or its remains;
13. “safe state in a severe reactor accident” shall refer to the state of a nuclear power plant following a severe reactor accident, in which the conditions for a controlled state are met and, in addition, the internal pressure within the containment is so low that any leakage is minimal, even if the containment is not leakproof
14. “common cause failure” shall refer to the failure of two or more structures, systems or devices due to the impact of the same single cause;
15. “single failure” shall refer to a failure as a result of which the system, device or structure is unable to perform the function specified for it.

Section 3 Coverage of safety demonstrations

SYT-3111 - The safety of a nuclear facility and the technical solutions of systems, structures and components important for safety shall be justified computationally using deterministic and probabilistic analyses, and, if necessary, experimentally or through a combination of tests and analyses. The safety justifications shall cover the entire life cycle of the nuclear facility in a documented manner.

SYT-3115 - The analyses and tests shall be comprehensive and representative of the subject

of the assessment.

SYT-3110 - The operating experience, disturbances and accidents of the nuclear facility under review and other nuclear facilities, as well as the impact of technological and safety research developments on the comprehensiveness and representativeness of the safety justifications, shall be assessed. Where necessary, the analyses and tests shall be supplemented if the information obtained has an impact on the comprehensiveness and representativeness of the safety justification.

Section 4 Analytical methods and uncertainty assessment

SYT-3127 - The methods used in the analyses shall be verified and validated in a documented manner.

SYT-3126 - Uncertainties related to analyses and tests shall be identified, and their significance for the fulfilment of safety requirements shall be assessed.

SYT-4777 - When assessing the success of safety functions based on analyses or tests, the more important the function, the stricter the requirements that shall be set for the certainty of demonstrating the success of the safety function.

Section 5 Tests conducted to demonstrate safety

SYT-3159 - The tests used to justify the safety of the technical solution of a nuclear facility shall be of a high quality and documented so that their comprehensiveness and representativeness in relation to the design solution under assessment can be evaluated. The comprehensiveness and representativeness of the tests in relation to the design solution shall be assessed.

SYT-3160 - To demonstrate the safety of the technical solution, tests shall be conducted at least in cases where reliable calculation methods, previous test results or applicable operational experience are unavailable, and the solution involves phenomena with significant uncertainties. Particular care shall be taken when tests are used to justify the safety of a technical solution that cannot be tested under real conditions during or after the commissioning of the nuclear facility.

Chapter 2: Deterministic safety analyses

Section 6 Scope of deterministic safety analyses

SYT-3112 - For nuclear facilities, the initiating events to be analysed in more detail and the associated failure assumptions shall be determined on a facility-specific and operation-mode-specific basis so that the facility's behaviour during disturbances and accidents, the resulting radioactive releases, and the radiation doses to the surrounding population can be assessed comprehensively.

SYT-3168 - Deterministic safety analyses shall cover operational occurrences, postulated accidents, design extension conditions, and severe reactor accidents that define or limit the dimensioning of systems and structures implementing safety functions.

SYT-4903 - The analyses of severe reactor accidents shall cover the actions of the nuclear power plant's automation system or operators that are required for the control of a severe reactor accident, as well as the physical and chemical phenomena related to the course of the accident.

SYT-3123 - Operational occurrences and accidents shall be analysed from the initial event that triggers the situation to a safe state.

Section 7 Assumptions used in deterministic safety analyses

SYT-3122 - The initial state of the analyses and the selection of parameter values to be used in the analyses shall be justified. The choice shall be made so that the consequences resulting from the analyses are, with a high degree of certainty, at least as serious as they would be in the actual situation.

SYT-3161 - The impact of the initial state of the analyses and the uncertainty of the parameter values used in the analyses on the results shall be evaluated through sensitivity analyses or statistical uncertainty analysis.

SYT-3120 - In analyses that justify design solutions, it shall be assumed that the nuclear facility operators will act in accordance with the instructions intended for disturbance and accident situations. The time allocated for operators to assess the situation and take action shall be sufficiently long and justified. The accessibility of locally controlled equipment shall be justified.

SYT-3709 - The exclusion of the control element with the greatest reactivity impact from the reactor core shall be assumed in the analysis of operational occurrences and accidents. This assumption does not need to be made separately if the single-failure or common-cause failure assumption made for the case results in a greater impairment of the reactor shutdown function than the exclusion of a single control element.

Section 8 Analysis of operational occurrences

SYT-3238 - In deterministic safety analyses of operational occurrences, either conservative assumptions supplemented by sensitivity analyses if necessary or best-estimate assumptions supplemented by statistical uncertainty analysis shall be used.

SYT-3301 - Minor operational occurrences shall be analysed so that the nuclear facility's systems function as designed, except for the fault or control error considered the initiating event, along with its consequences. The most limiting single failure in terms of the event's consequences shall be assumed for limitation functions. Systems designed to manage a postulated accident shall not be exploited.

SYT-3581 - Extensive operational occurrences shall be analysed so that the nuclear facility's systems function as designed, except for the fault or control error considered as the initiating event, along with its consequences. Systems designed to manage a postulated accident can be exploited, but the acceptance criteria defined for operational occurrences shall be met. The most limiting single failures in terms of the event's consequences shall be assumed for limitation functions and the systems designed for managing a postulated accident.

Section 9 Analyses of postulated accidents

SYT-3165 - In deterministic analyses of postulated accidents in nuclear power plants from the initiating event to a controlled and safe state, only the systems assigned to these functions as systems mitigating the consequences of the event in accordance with the Radiation and Nuclear Safety Authority Regulation on the Technical Safety Requirements of a Nuclear Facility (Y/x/20xx) may be assumed. The operation of other systems shall be assumed if their intended operation may aggravate the consequences of the initiating event.

SYT-5416 - In deterministic analyses of postulated accidents in nuclear technical facilities from the initiating event to a safe state, only the systems assigned to these functions as systems mitigating the consequences of the event in accordance with the Radiation and Nuclear Safety

Authority Regulation on the Technical Safety Requirements of a Nuclear Power Plant (Y/x/20xx) may be assumed. The operation of other systems shall be assumed if their intended operation may aggravate the consequences of the initiating event.

SYT-3239 - In deterministic safety analyses of postulated accidents, either conservative assumptions supplemented by sensitivity analyses if necessary or best-estimate assumptions supplemented by statistical uncertainty analysis shall be used.

Section 10 Analyses of design extension conditions

SYT-3518 - In deterministic analyses of design extension conditions in nuclear power plants from the initiating event to a controlled and safe state, only the systems assigned to these functions as systems mitigating the consequences of the event in accordance with the Radiation and Nuclear Safety Authority Regulation on the Technical Safety Requirements of a Nuclear Power Plant (Y/x/20xx) may be assumed. The operation of other systems shall be assumed if their intended operation may aggravate the consequences of the initiating event.

SYT-5417 - In deterministic analyses of design extension conditions in nuclear technical facilities from the initiating event to a safe state, only the systems assigned to these functions as systems mitigating the consequences of the event in accordance with the Radiation and Nuclear Safety Authority Regulation on the Technical Safety Requirements of a Nuclear Power Plant (Y/x/20xx) may be assumed. The operation of other systems shall be assumed if their intended operation may aggravate the consequences of the initiating event.

SYT-3236 - Deterministic safety analyses of postulated design extension conditions may use best-estimate assumptions for the initial state and the parameter values used in the analyses, supplemented by sensitivity analyses if necessary.

Section 11 Analyses of severe reactor accidents

SYT-3520 - In deterministic analyses of severe reactor accidents from the initiating event to a controlled and safe state, only the systems assigned to these functions as systems mitigating the consequences of the event in accordance with the Radiation and Nuclear Safety Authority Regulation on the Technical Safety Requirements of a Nuclear Power Plant (Y/x/20xx) may be assumed. The operation of other systems shall be assumed if their intended operation may aggravate the consequences of the initiating event.

SYT-3237 - Deterministic safety analyses of severe reactor accidents may use best-estimate assumptions for the initial state and the parameter values used in the analyses, supplemented by sensitivity analyses.

Section 12 Analyses of a disposal facility

SYT-6275 - In deterministic analyses of disposal facilities, only the functions, structures and components assigned to this in accordance with the Radiation and Nuclear Safety Authority regulation (Y/x/20xx) on disposal facilities may be assumed to mitigate the consequences of the event from the initial event to the safe state.

Chapter 3: Probabilistic Risk Analysis (PRA)

Section 13 Scope of probabilistic risk analysis

SYT-3304 - Probabilistic risk analysis shall determine:

1. Chains of events leading to significant damage to nuclear fuel and the frequency of the damage;
2. The quantity, composition and timing of releases of radioactive substances to the environment resulting from significant damage to nuclear fuel, as well as the frequencies of large release and early releases.

SYT-3946 - The scope and level of detail of the probabilistic risk analysis shall be proportionate to the magnitude of the radiation risk posed by the nuclear facility. In addition, the type of nuclear facility and the complexity of its structures, systems, components and functions shall be taken into account.

SYT-3305 - The initiating events shall be analysed for each operation mode, including internal faults, disturbances and human errors, as well as losses of the external power grid and both internal and external events.

Section 14 Methods, assumptions and uncertainty assessment used in probabilistic risk analysis

SYT-3306 - The methods used in probabilistic risk analysis shall be based on best established international practices. The suitability of the methods used, expert assessments and reliability data shall be justified.

SYT-3526 - In probabilistic risk analysis, the behaviour of the nuclear facility during disturbance and accident situations shall be modelled as realistically as is practically possible, avoiding the use of unnecessarily conservative assumptions.

SYT-3307 - Uncertainty and sensitivity analyses shall be presented in probabilistic risk analysis to support conclusions drawn based on the interpretation and analysis of the results.

SYT-3564 - Probabilistic risk analysis shall be kept up to date and further specified as necessary, taking operational experience, plant modifications, new research results and developments in computational methods into account.

Section 15 Success criteria analyses

SYT-5000 - Success criteria analyses used in probabilistic risk analysis shall be conducted using best-estimate assumptions for the initial state and the parameter values applied in the analyses.

Chapter 4: Analyses of releases and radiation doses

Section 16 Coverage of analyses of releases and radiation doses

SYT-3327 - Analyses of releases and radiation doses shall be conducted for normal operation, as well as for disturbance and accident situations that are dimensioning in terms of releases of radioactive substances and radiation doses. The selection of dimensioning cases shall be justified.

SYT-3321 - The analyses shall take the radiation doses caused by external radiation from the nuclear facility, as well as from releases of radioactive substances into the atmosphere and waterbodies, into account.

SYT-3158 - In dispersion and population dose analyses concerning normal operation, the collective dose to the population shall be assessed at a distance of at least 100 km from the facility.

SYT-3324 - The analyses shall examine radiation doses to different population groups through different exposure pathways. In the analyses, a representative individual of the most exposed members of the population shall be identified, and their received radiation dose shall be compared with the population dose constraint. The radiation dose received by the representative person shall be estimated computationally so that no more than 5% of the individuals they represent receive a higher dose.

SYT-3439 - Accident analyses shall also examine the long-term impact of the fallout of radioactive substances.

Section 17 Assumptions concerning the nuclear facility and its environment used in analyses of releases and radiation doses

SYT-6039 - The dispersion and dose analyses of radioactive substances for normal operation shall use release estimates based on the operating experience of the nuclear facilities and the characteristics of the facility in question.

SYT-3318 - At the beginning of the event, the coolant of the nuclear fuel shall be assumed to contain at least the quantities of radioactive substances that are set as maximum quantities in the operational limits and conditions of the nuclear facility.

SYT-3320 - It shall be assumed that systems, structures and components that implement safety functions of the nuclear facility essential to the containment of radioactive substances are available and operating as required in the regulations issued by the Radiation and Nuclear Safety Authority concerning disposal facilities, the technical safety requirements for nuclear power plants and the requirements for the handling and storage of nuclear fuel.

SYT-6040 - The analyses shall take into account the relevant chemical and physical phenomena that affect the release and migration of radioactive substances at the nuclear facility and in its environment.

SYT-3323 - In the analyses of population radiation doses, potential future changes in residential areas, food production and other activities in the vicinity of the facility that may expose the population to radiation shall be taken into account.

Chapter 5: Other analyses and tests

Section 18 Fault tolerance and common-cause failure analyses

SYT-3300 - The fulfilment of failure criteria for systems implementing safety functions, as well as common cause failures, shall be assessed using failure tolerance and common cause failure analyses when designing systems and their modifications. If necessary, the analyses shall be further specified during different phases of the design.

SYT-3527 - A common cause failure analysis shall be prepared for operational occurrences and Class 1 postulated accidents. For the purpose of common cause failure analysis, the implementation of safety functions shall be presented for each initiating event in a manner that demonstrates the use of systems and components applying the principles of diversity and redundancy. Common cause failure analysis shall:

1. Examine one safety function or part thereof at a time, taking the systems implementing the function into account;
2. Examine the common failures of all devices whose common failures or unnecessary actions may affect the implementation of the safety function;
3. Take the initiating event, the consequential effects of the initiating event and, in addition, the common cause failure between devices that are similar or contain significantly similar components into account.

SYT-3515 - The impacts of faults and errors in the controls and functions performed by the automation shall be analysed comprehensively. The scope of examination selected for an individual analysis shall be justified, and the analysis shall consider automation faults that may occur as a lack of activity in a demand situation or as erroneous operation.

Section 19 Analyses and tests of internal and external events

SYT-3313 - The adequacy of design solutions for preparing for internal and external events shall be justified by analyses and, if necessary, by tests so that the achievement of the objectives set out in the regulations of the Radiation and Nuclear Safety Authority on the technical safety requirements for nuclear power plants, on the technical requirements for the handling and storage of nuclear fuel, on the site of a nuclear facility and on disposal facilities is reliably demonstrated.

SYT-3917 - A deterministic fire analysis shall be prepared for the nuclear facility to demonstrate

the structural sustainability of the nuclear facility and the reliable implementation of safety functions. The analysis shall cover all the premises of the nuclear facility that contain permanent or temporary fire loads. The analysis shall also take the possible spread of the fire into account.

Section 20 Analyses related to the operating instructions of the nuclear facility

SYT-3169 - Comprehensive deterministic disturbance and accident analyses shall be carried out to prepare the operating instructions of the nuclear facility and to assess their accuracy.

SYT-3571 - The best-estimate assumptions for the initial state and parameter values used shall be applied in the analyses carried out to prepare the operating instructions of the nuclear facility and to assess their accuracy.

Section 21 Analyses of emergency situations

SYT-5955 - The best-estimate assumptions for the initial state and parameter values used shall be applied in the analyses carried out for the planning of the nuclear facility’s emergency response arrangements.

Section 22 Entry into force and transitional provision

This regulation shall enter into force on X X 202X and shall remain valid until further notice.