Nuclear Regulation
NEA/CNRA/R(2017)3
February 2019
www.oecd-nea.org

Survey on the Regulatory Practice to Assess Passive Safety Systems used in New Nuclear Power Plant Designs

First Stage Report

OECD
BETTER POLICIES FOR BETTER LIVES

NEA
NUCLEAR ENERGY AGENCY

Nuclear Energy Agency

NEA/CNRA/R(2017)3

Unclassified

English text only

11 February 2019

NUCLEAR ENERGY AGENCY
COMMITTEE ON NUCLEAR REGULATORY ACTIVITIES

Survey on the Regulatory Practice to Assess Passive Safety Systems used in New Nuclear Power Plant Designs

First Stage Report

JT03442910

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 36 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Commission takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1 February 1958. Current NEA membership consists of 33 countries: Argentina, Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, Norway, Poland, Portugal, Romania, Russia, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Commission also takes part in the work of the Agency.

The mission of the NEA is:

– to assist its member countries in maintaining and further developing, through international co-operation, the scientific, technological and legal bases required for a safe, environmentally sound and economical use of nuclear energy for peaceful purposes;

– to provide authoritative assessments and to forge common understandings on key issues as input to government decisions on nuclear energy policy and to broader OECD analyses in areas such as energy and the sustainable development of low-carbon economies.

Specific areas of competence of the NEA include the safety and regulation of nuclear activities, radioactive waste management and decommissioning, radiological protection, nuclear science, economic and technical analyses of the nuclear fuel cycle, nuclear law and liability, and public information. The NEA Data Bank provides nuclear data and computer program services for participating countries.

COMMITTEE ON NUCLEAR REGULATORY ACTIVITIES (CNRA)

The Committee on Nuclear Regulatory Activities (CNRA) is responsible for the Nuclear Energy Agency (NEA) programmes and activities concerning the regulation, licensing and inspection of nuclear installations with regard to both technical and human aspects of nuclear safety. The Committee constitutes a forum for the effective exchange of safety-relevant information and experience among regulatory organisations. To the extent appropriate, the Committee reviews developments which could affect regulatory requirements with the objective of providing members with an understanding of the motivation for new regulatory requirements under consideration and an opportunity to offer suggestions that might improve them and assist in the development of a common understanding among member countries. In particular it reviews regulatory aspects of current safety management strategies and safety management practices and operating experiences at nuclear facilities including, as appropriate, consideration of the interface between safety and security with a view to disseminating lessons learnt. It promotes co-operation among member countries to use the feedback from experience to develop measures to ensure high standards of safety, to further enhance efficiency and effectiveness in the regulatory process and to maintain adequate infrastructure and competence in the nuclear safety field.

The Committee promotes transparency of nuclear safety work and open public communication and oversees work to promote the development of effective and efficient regulation.

The Committee focuses on safety issues and corresponding regulatory aspects for existing and new power reactors and other nuclear installations, and the regulatory implications of new designs and new technologies of power reactors and other types of nuclear installations consistent with the interests of the members. Furthermore it examines any other matters referred to it by the Steering Committee for Nuclear Energy. The work of the Committee is collaborative with and supportive of, as appropriate, that of other international organisations for co-operation among regulators and consider, upon request, issues raised by these organisations.

Foreword

The use of passive safety systems, nowadays, is one of the trends in many new reactor designs.

Due to the fact that passive systems rely on natural forces, the number of active components and (or) support systems can be reduced. Therefore, sources for failures may be reduced. However, these systems generate new questions, for instance regarding testability, determination of reliability, specification of required boundary conditions, applicability of thermo-hydraulic codes, and applicability of the single failure concept. In addition, passive safety system may change some understanding of the defence-in-depth concept.

Therefore, it is relevant that regulators share their knowledge and discuss how a review and assessment of passive systems can be performed thoroughly. This is especially important due to the fact that existing regulations oftentimes were developed for nuclear power plant (NPP) with mainly active safety systems.

The purposes of the current survey are:

- firstly, to improve the regulatory review and assessment of passive safety systems that are used in new NPP designs by identifying good practices and knowledge gaps, and by sharing experience and guidance;
- and, secondly to compare national approaches to defining and regulating the use of these passive safety systems.

Acknowledgements

This report, prepared by Dr Mikhail Lankin (VO Safety, Russian Federation), is based on discussions and input provided by members of the CNRA Working Group on the Regulation of New Reactors in responding to a survey. Mr Janne Nevalainen (STUK, Finland) and Mr Young Joon Choi (NEA Secretariat) chaired the meetings and supervised the work carried out by the group.

The following individuals contributed to the preparation of the survey report:

- Chantal Morin, Canada
- Bjorn Becker, Germany
- David Walden, the United Kingdom
- John Monninger, the United States

Table of contents

List of abbreviations and acronyms

AC	Alternating current
AGR	Advanced gas cooled reactor
CNRA	Committee on Nuclear Regulatory Activities
DC	Direct current
ECCS	Emergency core cooling system
IAEA	International Atomic Energy Agency
LOCA	Loss-of-coolant accident
NPP	Nuclear power plant
NRC	United States Nuclear Regulatory Commission
NSC	Nuclear safety codes
OLC	Operating Limits and Conditions
ONR	United Kingdom Office of Nuclear Regulation
PWR	Pressurised water reactor
RB	Regulatory body
SAP	Safety assessment principles
SAR	Safety analysis report
STUK	Finnish Radiation and Nuclear Safety Authority
WGRNR	Working Group on the Regulation of New Reactors

EXECUTIVE SUMMARY

At the 15th Meeting of the Committee on Nuclear Regulatory Activities (CNRA) Working Group on the Regulation of New Reactors (WGRNR), the Working Group agreed to initiate a survey on Regulatory Practice to Assess Passive Systems Used in New Nuclear Power Plant Designs. It was decided to split the survey into two stages.

The current report is devoted to the first stage of the survey and focuses on passive safety systems which are primarily intended to cope with anticipated operational occurrences and design-basis accidents. Passive systems used for mitigating severe accidents are not within the scope of this report. It is also agreed that the scope of a potential second stage of the survey will be considered by WGRNR later.

Survey questions were grouped into five chapters namely:

- requirements for passive safety systems;
- testing and analyses of passive safety systems;
- regulatory review of passive safety systems;
- commissioning and periodic verification testing;
- experience with passive safety systems.

Based on a comparison of the information provided in response to the survey, the following observations were made as a result of the study:

- Some countries have a formal definition for passive systems in their regulatory framework, while other countries do not have a formal definition. Definitions of passive safety systems (for those countries which have such formal definition), to some extent, vary country to country (e.g. some countries assume existence of movable parts as an attribute of active systems only, while other countries consider that movable parts can belong to either active or passive systems). Nevertheless, the general understanding of what is a passive system is similar among countries which provided responses to the survey.
- The regulatory frameworks of a number of countries favour the use of passive systems over active ones and these countries have explicit requirements for passive systems. Other countries encourage the usage of passive systems.
- There are no differences in the regulatory treatment of systems irrespective as to whether they are acknowledged as passive or active in responding countries in the following areas:

  – providing system descriptions in the safety analysis report;
  – protection from tampering;
  – establishing operational limits and conditions;
  – safety classification;
  – protection against external events;
  – functional failures identification and consideration;

  - substantiation of system parameters;
  - instrumentation and controls;
  - demonstration of the maximum number of passive safety system actuations (including false actuations), and consideration of the equipment design life and environment that it is operating in;
  - false actuation considerations and system starting considerations;
  - testing during commissioning;
  - testing during operation.

- The application of single failure criteria in some countries is the same for both active and passive systems; while in a number of countries, the approaches on application of single failure criteria are different for passive and active systems.
- Despite the fact that there are no differences in the regulatory frameworks for safety principles to be demonstrated for active and passive systems, it is worth noting that the demonstration of passive systems' performance is more focused on experimental justification.
- If there is a possibility of negative effects due to concurrent operation of several passive safety systems (or trains), the effects should be analysed and if necessary verified by experiments.
- Most countries do not have specific requirements for passive systems reliability analyses. One country issued regulatory guidance which provides specific methods for conducting reliability analysis for passive safety systems. Also, another country highlighted the necessity to pay special attention to uncertainties that accompany reliability analyses for passive systems.

The complete survey responses are in Appendix I of the Report.

INTRODUCTION

Usually, a passive system is understood as a system that either is composed entirely of passive components and structures or that uses active components in a very limited way to initiate subsequent passive operation. Passive operation typically implies the reliance on natural forces (e.g. convection) and (or) stored energy (e.g. gravity flow).

The task encompasses passive safety systems that are used in new nuclear power plant (NPP) designs, but not passive components of active systems.

Both systems intended to operate in design-basis accidents and non-severe accident design extension conditions are subjects of the survey. Systems designed to operate mainly during severe accidents are out of the scope of the first stage of the survey. The Working Group on the Regulation of New Reactors (WGRNR) will consider whether to undertake a Second Stage of the Survey which would focus on severe accidents.

Only fluid safety systems are subjects of the survey. A “fluid safety system” is a system that uses movement of liquid or gas as an essential part of its operation and that is not primarily intended to initiate or facilitate any chemical reactions. So, such systems as hydrogen recombiners or scram control rods are out of the scope of this stage of the survey.

The following countries participated in the survey and provided responses to the questionnaire: Finland, Germany, Hungary, Korea, Poland, Russia, the Slovak Republic, the United Kingdom and the United States.

SURVEY RESULTS

The survey consists of five thematic areas where the peculiarities of passive safety systems (in comparison with active systems) could potentially be identified, namely:

- requirements for passive safety systems;
- testing and analyses of passive safety systems;
- regulatory review of passive safety systems;
- commissioning and periodic verification testing;
- experience with passive safety systems.

Requirements for passive safety systems

In the chapter "(Regulatory) requirements for passive safety systems" countries were asked how a passive safety system is defined in their own national regulatory framework, as well as whether this regulatory framework differentiates between active and passive safety systems.

The International Atomic Energy Agency (IAEA) Safety Glossary (IAEA, 2007) has no definition for a passive system. Only the term "passive component" is defined: "A passive component is defined as a component whose functioning does not depend on an external input such as actuation, mechanical movement or supply of power" (IAEA, 2007). Practically all respondents have a "passive component" (or "passive element" or "passive equipment") term defined slightly differently in their regulatory framework compared to the IAEA definition.

Several countries indicate that in their regulatory framework, passive systems are defined as systems consisting of passive components (or elements). However, some countries do not have an exact definition for a passive system. In some cases "passive safety" or "passive safety features" concepts are used to establish further regulatory requirements or recommendations for nuclear power plant (NPP) safety.

The next question was on preferring the use of passive safety systems over active safety systems in a national regulatory framework as well as on the reasoning for giving such preference.

Several countries that answered the survey indicated that their regulatory frameworks express explicit favour for using passive systems over active ones. Some countries report that despite the absence of explicit requirement, they encourage licensee to give preferences to passive systems over active ones. Some countries expressed "preference for inherent safety" requirement which is stricter than just "favour to passive safety systems" requirement. Some countries responded that they do not distinguish between passive and active systems.

Overall, a variety of approaches exist in the preference between active and passive systems.

Countries were also asked to summarise any additional requirements for passive systems in a number of areas (description in safety analysis report [SAR], protection from tampering, establishment of operational limits and conditions, implementation of single failure criterion, safety classification, and protection from external hazards).

All countries responded that they use similar approaches for describing active and passive safety systems in the SAR. Also no differences were reported for tampering, for submittal of operational limits and conditions, for safety classification, and for protection from external events.

A more complex situation exists with the application of the single failure principle. Requirement 25 of IAEA Safety Standard SSR-2/1 (IAEA, 2016) specifies that the single failure criterion shall be applied to each safety group incorporated in the plant design. "The design shall take due account of the failure of a passive component, unless it has been justified in the single failure analysis with a high level of confidence that a failure of that component is very unlikely and that its function would remain unaffected by the postulated initiating event" (IAEA, 2016).

Some countries report that they do not distinguish between passive and active systems when applying the single failure criterion. At the same time, a number of countries indicate that they use, in one form or another, an approach similar to the IAEA Standard (IAEA, 2016).

Testing and analyses of passive safety systems

Survey respondents were asked what safety principles must be demonstrated through testing and analyses. Respondents were also asked about their expectations for the validation of computer codes and the conduct of testing used to demonstrate safety performance.

There are no significant differences in the approaches applicable for active and passive systems. Nevertheless, some countries indicate that passive safety systems as a rule require more emphasis on experimental substantiation than on analytical approaches.

The next point of interest was the concurrent operation of several different passive safety systems (trains), in particular the expectations for the testing and analyses required to be demonstrated by the licensee. The same question was formulated for concurrent operation of passive and active safety systems. Responding countries did not report any difference between the passive or active nature of a system. The possible negative effects from concurrent operation of safety systems (either passive or active) shall be analysed and if necessary tested.

Regulatory review of passive safety systems

The next set of questions was grouped under "Regulatory review of passive safety systems".

The first question was how are functional failures identified and considered in the safety demonstration (specifically containment isolation challenged by a leaking passive system penetrating the containment wall and non-condensable gases collecting in heat exchangers).

No differences in approaches for active and passive systems were reported.

Then the respondents provided information on their expectations for the applicant or licensee to provide substantiation of passive safety system parameters (e.g. pressure, temperature, flow rates, inventory, procedures, concentration of neutron absorbers, pressure resistance of lines, valve characteristics).

No differences in expectations for active and passive systems were reported.

The third question was related to expectations for the applicant or licensee to provide the results of quantitative and qualitative analysis of passive safety systems reliability. Additionally; any special considerations for the reliability analysis because of passivity should be described by respondents.

A number of respondents indicated that there are no significant differences between passive and active systems here. At the same time, two countries reported that specific attention is necessary to reliability analysis of passive safety systems. One country indicated that the reason for this particular attention was the fact that passive safety systems rely on natural forces, such as gravity, to perform their safety functions. Such driving forces are small compared to those of pumped systems, and the uncertainty in their values, as predicted by a best-estimate thermal-hydraulic analysis, can be of comparable magnitude to the predicted values themselves. Another country indicated that its regulatory body issued regulatory guideline on system reliability analysis, where special chapter, devoted to passive system reliability analyses, considers all corresponding specific aspects.

The next question was on regulatory expectations for the review of instrumentation and controls supporting passive systems. No differences in expectations for instrumentation and controls supporting active and passive systems were reported.

The next two questions in this chapter were related to expectations for the applicant (licensee) to demonstrate the maximum number of passive safety system actuations (including false actuations) and to evaluate the impact of false actuation (starting) of passive safety systems. Countries were also asked to share any special considerations in the starting procedure of passive safety systems.

The countries did not report any differences in expectations for active and passive systems.

The final question was related to expectations for the applicant or licensee to submit information on the response of liquids and gases in the passive flooding systems tanks, such as droplet carryover and possibility for blowdown.

The countries reported that there are no differences on this subject. At the same time, some countries indicated that in the case when phenomena mentioned in the question could negatively impact the performance of passive safety systems, they must be addressed in the design and demonstrated to not impact safety performance. That approach seems reasonable.

Commissioning and periodic verification testing

The fourth set of questions was devoted to commissioning and periodic verification testing. Questions were asked in the following areas:

a) expectations for testing passive safety systems during commissioning;
b) expectations for the interval and scope of periodic checks and testing of passive safety systems during nuclear power plant operations.

No differences between active and passive systems were reported by respondents.

Experience with passive safety systems

In the final survey chapter, the respondents were asked to share their experience with passive safety systems.

A number of passive safety systems were listed by countries that participated in the survey: passive core flooding systems, passive residual heat removal systems, passive containment cooling systems, passive auxiliary feedwater sytems, passive autocatalytic recombiners, etc. Given this experience, it is evident that the regulatory framework and bodies of various countries have dealt with passive safety systems and are in a good position to address them in new reactor applications.

CONCLUSIONS

Based on a comparison of the information provided in response to the first stage of the survey, the following observations were made as a result of the study:

- Some countries have a formal definition for passive systems in their regulatory framework while other countries do not have a formal definition. Definitions of passive safety systems (for those countries which have such formal definition) vary to some extent from country to country (e.g. some countries assume existence of movable parts as an attribute of active systems only, while other countries consider that movable parts can belong to either active or passive systems). Nevertheless, the general understanding of what is a passive system is similar among countries which provided responses to the survey.
- The regulatory framework of a number of countries favours the use of passive systems over active ones and these countries have explicit requirements for passive systems. Other countries encourage the use of passive systems.
- There are no differences in the regulatory treatment of passive or active systems in a number of aspects. Such aspects are:
  - providing system descriptions in the safety analysis report;
  - protection from tampering;
  - establishing operational limits and conditions;
  - safety classification;
  - protection against external events;
  - functional failures identification and consideration;
  - substantiation of system parameters;
  - instrumentation and controls;
  - demonstration of the maximum number of passive safety system actuations (including false actuations), and consideration the equipment design life and environment that it is operating in;
  - false actuation considerations and system starting considerations;
  - testing during commissioning;
  - testing during operation.
- The application of single failure criteria in some countries is the same for both active and passive systems; while in a number of countries, the approaches on application of single failure criteria are different for passive and active systems (e.g. passive components in a whole or partially can be considered as not covered by single failure criteria).
- Despite the fact that there are no differences in the regulatory framework for safety principles to be demonstrated for active and passive systems, it is worth noting that the demonstration of passive systems performance is more focused on experimental justification.

- If there is a possibility of negative effects due to the concurrent operation of several passive safety systems (or trains), the effects should be analysed and if necessary verified by experiments.
- Most countries do not have specific requirements for passive systems reliability analyses. One country issued regulatory guidelines which provide specific methods for conducting reliability analyses for passive safety systems. Also, another country highlighted the necessity to pay special attention to uncertainties that accompany reliability analyses for passive systems.

REFERENCES

IAEA (2016), Safety Standards. Safety of Nuclear Power Plants: Design, Specific Safety Requirements, SSR-2/1 (Rev.1), Vienna.

IAEA (2013), Passive Safety Systems in Advanced Water Cooled Reactors (AWCRs). Case Studies, A Report of the International Project on Innovative Nuclear Reactors and Fuel Cycles (INPRO) IAEA-TECDOC-1705, IAEA, Vienna.

IAEA (2009), Passive Safety Systems and Natural Circulation in Water Cooled Nuclear Power Plants, IAEA-TECDOC-1624, IAEA, Vienna.

IAEA (2007), Safety Glossary – Terminology Used in Nuclear Safety and Radiation Protection, Vienna.

IAEA (1996), Technical feasibility and reliability of passive safety systems for nuclear power plants, IAEA-TECDOC-920. Proceedings of an Advisory Group meeting held in Julien, Germany, 21-24 November 1994, IAEA, Vienna.

NEA (2002), Passive System Reliability – A challenge to Reliability Engineering and Licensing of Advanced Nuclear Power Plants, Proceedings of an International Workshop hosted by the Commissariat à l'Energie Atomique (CEA), NEA/CSNI/R(2002)10, Paris.

NRC (1994), Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems in Passive Plant Designs, Policy Issue, SECY-94-084, dated 28 March 1994, Washington, DC, http://pbadupws.nrc.gov/docs/ML0037/ML003708068.pdf.

APPENDIX I. COUNTRY RESPONSES TO SURVEY

Chapter I. Requirements for passive safety systems

Question 1. How is a passive safety system defined in your regulatory framework? Does your regulatory framework make any difference between active and passive system?

Finland

There is no definition of a passive system in the Finnish regulation except what is referred in Question 2 (systems and components which do not require a power supply). There are minor differences in the regulatory framework. These are described in the following questions.

Germany

In the German regulatory framework, passive and active safety systems are defined as follows:

Active equipment of the safety system:

"The active equipment of the safety system is technical equipment of the safety system that carries out a safety function. Active safety systems are for example systems to shut down the reactor, to remove residual decay heat, to carry out containment isolation."

Passive equipment of the safety system:

"Passive equipment of the safety system is equipment, that carries out a safety function without actuators or without auxiliary equipment, e.g. the primary circuit, the containment and shielding are called passive equipment of the safety system."

Furthermore, the German regulations define passive components as follows:

"A system part is passive if there will be no change in its positioning in case of challenge (e.g. pipes, vessels, heat exchangers). Self-acting system parts (functioning without external power or remote control) shall be considered as passive if the position of the system part under consideration (e.g. safety valve or check valve) is not changed in the course of fulfilling its intended function."

Hungary

In the regulations – Nuclear Safety Codes (NSC), which are the Annexes of Govt. Decree 118/2011 (VII.11.) – there are two definitions – in the Nuclear Safety Code (NSC), Volume 10, Nuclear Safety Code Definitions – related to the passive systems: the passive safety system and the passive system component.

"Passive system component: Those system components that provide their functions without moving parts, or the change of their shape or characteristics."

"Passive safety system: A safety system that contains passive system components and such elements that do not require external power source or control to operate, their functions are executed by simple physical processes."

For active systems the definition is the following:

"Active system component: A system component performing a safety function by means of its moving components or by changing its shape or characteristics."

Korea

The current rules and regulations have no definition of passive safety system. In our regulatory framework, the two systems are not separately handled.

Poland

There is a definition of a passive component in the Polish regulatory framework.

"Passive component – a component whose functioning does not depend on external input such as: actuation, mechanical movement or supply of power." (Article 1, paragraph 4 – Regulation of the Council of Ministers of 31 August 2012 on nuclear safety and radiation protection requirements which must be fulfilled by a nuclear facility design).

Active component depends on external input.

Russia

Russian national federal norms "General provisions for ensuring safety of nuclear power plants" NP-001-05 defines passive system (element) as system (element) whose functioning is associated only with an event causing its operation and does not depend on operation of other active system (element), e.g. control system, energy source, etc. On the other hand active system (element) is a system (an element), functioning of which depends on the normal operation of another system (element), e.g. control system, power supply systems, etc.

Slovak Republic

The Slovak Republic regulatory framework does not strictly divide safety systems on active and passive. In the regulation No. 430/2011 there is a requirement that the nuclear facility has to remain in a safe state through the passive safety features or through the activity of safety systems that are in constant working order and are activated in reaction to the postulated trigger event. Achievement of the requirement must be documented in the project through the results of the deterministic or probabilistic safety analyses. As resulted from previous mentioned our framework does not favour any kind of safety system.

United Kingdom

ONRs safety assessment principles (SAPs) define passive safety as a means of providing and maintaining a safety function without the need for an external input such as actuation, mechanical movement, supply of power or operator action. It is noted that a passive safety system is not necessarily inherently safe.

Inherently safe is defined as preventing a specific harm occurring by using an approach, design or arrangement that ensures that harm cannot happen. Inherently safety is a higher standard that passive safety in that the former requires a demonstration that it is physically impossible for the harm to arise.

Application of inherent safety should minimise the need for, and reliance on, safety systems and the challenges placed on them. Nevertheless, where safety measures are required the SAPs state that safety should be secured by characteristics as near as possible to the top of the list below:

- passive safety measures that do not rely on control systems, active safety systems or human intervention;
- automatically initiated active engineered safety measures;
- active engineered safety measures that need to be manually brought into service in response to a fault or accident;
- administrative safety measures;
- mitigation safety measures (e.g. filtration or scrubbing).

The SAPs do not give justification for the hierarchy but it is obviously perceived that the lack of moving parts or the need for support services should generally ensure that a passive safety system is more reliably than an active safety system.

United States

The US NRC does not have an official definition for passive safety systems. Rather, the NRC views the characteristics of passive safety systems to be those systems that use only natural forces (e.g. gravity, natural circulation, natural convection, differential pressure), and require no continuously operating, electrically alternating current (AC) powered, mechanical components (such as pumps). These systems may require limited direct current (DC) power to initiate, but are not reliant on continued sources of power. Passive safety systems do not require support functions (e.g. service air, service water) or operator actions to function. In general, the US NRC regulatory framework is the same for both active and passive safety systems; however, there are some minor differences. In SECY-94-084, "Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems in Passive Plant Designs," dated 28 March, 1994 (http://pbadupws.nrc.gov/docs/ML0037/ML003708068.pdf), the NRC discusses various technical, regulatory, and policy considerations associated with the use of passive safety systems in nuclear power plants. In addition, the responses to the questions below highlight a few of the differences in the regulatory framework for active and passive safety systems.

Question 2. Does your regulatory framework favor the use of passive safety systems over active safety systems? If so, what is the reason for favoring passive safety systems?

Finland

STUK Regulation on the Safety of a Nuclear Power Plant (STUK, Y/1/2016) gives a preference for passive safety systems by requiring (Section 11 Safety functions and provisions for ensuring them):

"2. If inherent safety features cannot be utilised in ensuring a safety function, priority shall be given to systems and components which do not require a power supply or which, in consequence of a loss of power supply, will settle in a state preferable from the safety point of view."

The regulation states an order of preference: 1) inherent safety features; 2) systems and components which do not require a power supply; 3) active systems. The rationale is to decrease dependence from power sources.

Germany

Yes, the § 3.1 (2) and § 3.1 (3) of the "Safety Requirements for Nuclear Power Plants" state:

Safety-enhancing design, manufacturing and operating principles shall be applied to the measures and equipment on levels of defence 1 to 4a as well as the measures and equipment needed for internal and external hazards as well as for the measures and equipment needed for internal and external hazards as well as for human-induced external hazards with regard to all operational modes (see also Subsection 2.1 (13)). In particular, the following shall be implemented:

a) well-founded safety factors in the design of components depending on their safety significance; here, established rules and standards may be applied with regard to the case of application;
b) preference to inherently safe-acting mechanisms in the design;
c) use of qualified materials and manufacturing and testing methods and of equipment that has been proven by operating experience or which has been sufficiently tested;

[…]

3.1 (3) To ensure sufficient reliability of the equipment of level of defence 3 (safety equipment), the following design principles shall be applied in addition to Subsection 3.1 (2):

a) redundancy;
b) diversity;
c) segregation of redundant subsystems, unless this is conflicting with safety benefits;
d) physical separation of redundant subsystems;
e) safety-oriented system behaviour upon subsystem or plant component malfunctions;
f) preference of passive over active safety equipment;
g) the auxiliary and supply systems of the safety equipment shall be designed with such reliability that they ensure the required high availability of the equipment to be supplied;
h) automation (in the accident analysis, equipment that has to be actuated manually shall in principle not be credited until 30 minutes have passed).

However, this has to be understood in the context of the definition of passive systems mentioned above.

Hungary

The regulations favour the use of passive safety systems over active ones:

"During design, simplicity and clarity shall be aimed at. The use of passive protective systems is preferable to active solutions." (NSC 3a.2.2.9100.) [V. Principles of design for safety].

"During the design of systems, structures and components, passive, inherently safe solutions shall be applied to the extent reasonably achievable, which ensure that the failure

of the systems, structures and components, even without external interventions, leads to a safe condition." (NSC 3a.3.1.0400.) [3a.3.1. Design of safety class systems].

"Passive safety solutions shall be applied to the extent reasonably achievable when on-site storage is designed." (NSC 3a.6.1.0300.) [3a.6. Management and Storage of Nuclear Fuel and Radioactive Waste].

These requirements are from the NSC Volume 3a. Design requirements for new nuclear power plants, and for operating power plants these requirements are the same (NSC Volume 3. Design requirements for operating nuclear power plants).

The following requirement is only for new NPPs:

"In the case of systems containing irradiated fuel assemblies, such as the shutdown nuclear reactor or spent fuel pool, capabilities shall be provided for passive heat removal." (NSC 3a.4.3.1000.) [3a.4.3. Heat removal].

The reason for favouring can be found in the N3a.12 Regulatory guide for general design principles for new NPPs: the passive systems are more simple, so it is easier to prepare, interpret and review safety analyses, and it's beneficial in terms of building, operating and maintaining. Passive systems do not require external power source and control, and the fulfilment of function is ensured by physical processes, therefore less exposed to human errors.

Korea

No.

Poland

Polish regulations give the highest priority to inherent safety features. If inherent features cannot ensure safety, priority is given to passive systems, which do not require a power supply.

In order to ensure the fulfilment of the safety function for nuclear facility design solutions, the use shall be made, where possible, of inherent safety features of systems, structures and components of the nuclear facility, which are important for ensuring nuclear safety and radiation protection. Whenever it is not possible to ensure the fulfilment of safety functions by using inherent safety features, in the first instance application shall be made of nuclear facility systems, structures and components not requiring off-site electricity supply or which, in the event of loss of electrical power, will adopt the preferred state from the viewpoint of nuclear safety. (Article 34, paragraph 3 – Regulation of the Council of Ministers of 31 August 2012 on nuclear safety and radiation protection requirements which must be fulfilled by a nuclear facility design)

Independence from electricity power supply increases the safety of the nuclear facility.

Russia

Para 3.1.10 of federal norms "General provisions for ensuring safety of nuclear power plants" NP-001-05 states that "When designing the systems (elements) of NPP and Reactor Installation, it is necessary to give preference to the systems (elements) with design based on the passive principle of action and inherent safety features (self-control, heat retention, natural circulation and other natural processes) as well as on the fail-safe principle".

Slovak Republic

The requirements on the safety systems are not divided into requirements for active and passive systems.

United Kingdom

ONRs safety assessment principles (SAPs) define passive safety as a means of providing and maintaining a safety function without the need for an external input such as actuation, mechanical movement, supply of power or operator action. It is noted that a passive safety system is not necessarily inherently safe.

Inherently safe is defined as preventing a specific harm occurring by using an approach, design or arrangement that ensures that harm cannot happen. Inherently safety is a higher standard that passive safety in that the former requires a demonstration that it is physically impossible for the harm to arise.

Application of inherent safety should minimise the need for, and reliance on, safety systems and the challenges placed on them. Nevertheless, where safety measures are required the SAPs state that safety should be secured by characteristics as near as possible to the top of the list below:

- passive safety measures that do not rely on control systems, active safety systems or human intervention;
- automatically initiated active engineered safety measures;
- active engineered safety measures that need to be manually brought into service in response to a fault or accident;
- administrative safety measures;
- mitigation safety measures (e.g. filtration or scrubbing).

The SAPs do not give justification for the hierarchy but it is obviously perceived that the lack of moving parts or the need for support services should generally ensure that a passive safety system is more reliably than an active safety system.

United States

While not required, the use of passive safety systems for advanced reactors is encouraged by the US NRC. In general, the NRC's views on passive safety systems are discussed in its Policy Statement on the Regulation of Advanced Reactors (www.nrc.gov/reading-rm/doc-collections/commission/ policy/73fr60612.pdf). In the Policy Statement, the NRC stated its expectations that advanced reactors will provide enhanced margins of safety and/or use simplified, inherent, passive, or other innovative means to accomplish their safety functions. The NRC indicated that advanced reactor designers are expected to consider highly reliable and less complex shutdown and decay heat removal systems. As a result, the use of inherent or passive means to accomplish this objective (negative temperature coefficient, natural circulation, etc.) is encouraged. In addition, the NRC noted the need to consider simplified safety systems to reduce required operator actions and to facilitate operator comprehension, reliable system function, and more straightforward engineering analysis.

Over the past 40 years, various studies on the safety of nuclear power plants have been conducted. Many of these studies used probabilistic risk assessments and evaluated operational experience to identify safety and risk insights associated with nuclear power

plant operations. These studies highlighted the impact on safety and contribution to risk from areas such as: the availability and reliability of active safety systems; the reliance of active safety systems on support systems such as emergency ac-power, service water, and service air; and the critical role of operators in correctly diagnosing and responding to accidents. Passive systems have the potential to eliminate these dependencies.

Question 3. What are your requirements for passive safety systems? Summarise any additional requirements for passive safety systems in the following areas.

A. Providing a description in the Safety Analysis Report

Finland

There are no additional requirements for passive safety systems concerning the safety analysis reports. The passive safety systems should be described at the same level of detail as the other safety systems.

Germany

The same requirements as for active safety systems apply for passive systems.

Hungary

There are no specific requirements for passive systems in this topic.

Korea

As mentioned, we don't have any specific requirements. Instead, the applicable requirements and standards including US ANSI/ANS, SECY Papers, Regulatory Guides have been used for review of passive auxiliary feedwater system (PAFS) of APR+ design.

We are currently developing regulatory requirements for passive systems through R&D projects and referring to regulatory requirements of other countries; for example, regulatory treatment of non-safety active system, application of single failure criteria to the check valve, flow instability, testability of passive system, etc.

Poland

There are no additional requirements for the description of passive systems in the SAR. The passive safety systems will be described in a similar way as the other safety systems.

Russia

There are no additional requirements for passive safety systems concerning the SARs. The passive safety systems should be described at the same level of details as the other safety systems.

Slovak Republic

The requirements on the safety systems are not divided into requirements for active and passive systems.

United Kingdom

The safety assessment principles (SAPs) do give not give specific requirements for passive systems. However, the SAPs do give considerable engineering guidance on the generic requirements for safety systems. Specifically: ONRs expectation would be that the engineering design substantiation would be provided in the safety case for the facility.

United States

For both active and passive safety systems, the SAR must describe the facility, present the design bases and the limits on its operation, and present a safety analysis of the structures, systems, and components and of the facility as a whole. In addition, the SAR must contain a description and analysis of the structures, systems, and components of the facility, with emphasis upon performance requirements, the bases, with technical justification therefore, upon which these requirements have been established, and the evaluations required to show that safety functions will be accomplished. For passive plants, there are additional requirements for the SAR in 10 CFR 52.47(c)(2) which specifies that the application shall address how the requirements in 50.43(e) have been met (e.g. demonstration of safety performance, acceptable interdependent effects, sufficient data to assess analytical tools).

B. The protection from unauthorised tampering

Finland

There are no additional requirements concerning protection from unauthorised tampering.

Germany

The issue of unauthorised tampering is considered as a security issue rather than a safety issue, therefore regulations are undisclosed.

Hungary

There are no specific requirements for passive systems in this topic.

Korea

See answer to 3A.

Poland

There are no additional requirements for protection from unauthorised tampering. Passive safety systems are subject to physical protection on the same basis as other safety systems.

Russia

There are no additional requirements concerning protection from unauthorised tampering.

Slovak Republic

The requirements on the safety systems are not divided into requirements for active and passive systems.

United Kingdom

The safety assessment principles (SAPs) do give not give specific requirements for passive systems. However, the SAPs do give considerable engineering guidance on the generic requirements for safety systems. Specifically: SAP ELO.2 covers control of unauthorised access to structures, systems and components.

United States

There is no difference in the requirements (10 CFR Part 73) associated with protection from tampering for active safety systems and passive safety systems.

C. The submittal of operational limits and conditions (e.g. Technical Specifications)

Finland

There are no additional requirements for passive safety systems. Operational limits and conditions will be required.

Germany

The same requirements as for active safety systems apply for passive systems. OLCs have to be submitted in the safety case.

Hungary

There are no specific requirements for passive systems in this topic.

Korea

See answer to 3A.

Poland

There are no additional requirements for passive safety systems. Operational limits and conditions will be required.

Russia

There are no additional requirements for passive safety systems. Operational limits and conditions will be required.

Slovak Republic

The requirements on the safety systems are not divided into requirements for active and passive systems.

United Kingdom

The safety assessment principles (SAPs) do give not give specific requirements for passive systems. However, the SAPs do give considerable engineering guidance on the generic requirements for safety systems. Specifically: SAP FA.9 states that DBA should provide an input into the safety classification and the engineering requirements for systems, structures and components performing a safety function and the limits and conditions of safe operation.

United States

There is no difference in the requirements (10 CFR 50.36) associated with submitting proposed operational limits and conditions (e.g. Technical Specifications) for active safety systems and passive safety systems.

D. The use of single failure criteria

Finland

There is some difference between failure criteria of active and passive systems. STUK Regulatory Guide for safety design of a nuclear power plant (YVL B.1) requires that:

"448. In the event of anticipated operational occurrences or postulated accidents, it shall be possible to accomplish decay heat removal from the reactor and containment by one or several systems that jointly meet the (N+2) failure criterion and the 72-hour self-sufficiency criterion in such a way that the limits set forth for fuel integrity, radiological consequences and overpressure protection in the respective design-basis category DBC2, DBC3 or DBC4 are not exceeded. If the decay heat removal systems or their auxiliary systems have passive components that have a very low probability of failure in connection with the anticipated operational occurrence or postulated accident, the (N+1) failure criterion may be applied to those components instead of the (N+2) failure criterion."

Germany

Appendix 4 ("Principles for applying the single failure criterion and the maintenance") of the "Safety Requirements for Nuclear Power Plants" gives further details on the regulations for applying the single failure concept. Para 2.5 addresses passive components:

2.5 (1) In the single failure concept, a failure of passive equipment needs not be postulated if it is demonstrated that this equipment is designed in accordance with the following requirements:

- Consideration of maximum load/stress in all relevant conditions during operation and of all predictable changes in material property conditions with sufficient factors.
- Use of suitable materials for the intended functions and conditions.
- The equipment is manufactured, assembled, tested and operated based on a comprehensive quality assurance system to ensure the required reliability.
- The measures and safety factors to be applied shall be defined also according to the safety significance of the safety equipment.

2.5 (2) The safety demonstration required in Subsection 2.5 (1) can be considered as verified if the requirements regarding design, construction, material selection, manufacturing and testability of the equipment are fulfilled according to regulations taking the safety significance of the equipment into account.

However, this is to be understood in the context of the definition of passive systems/components in the German regulatory framework. Therefore a passive "fluid safety system" (as defined in the scope of the survey) might be considered as a normal safety system with implications on requirements for redundancy (n+2) etc.

Hungary

In the analyses of events resulting in DBA2-4 operating conditions, the single failure of systems providing safety functions, which mostly determines the consequences of the given event and results in the most severe consequences, or a human error shall be assumed. However, there is no need to assume the failure of a passive system component if it can be demonstrated that there is very low probability for the failure of the given system component or that it is not affected by the occurrence of the assumed initiating event. (NSC 3a.2.3.1200).

During design, the requirement of single failure tolerance shall be applied. The possibility of the inadvertent operation of system components shall be handled as a possible mode of failure. The failure of a passive system component shall be taken into account, unless it can be demonstrated that the failure of the passive system component is highly unlikely or does not influence the given function. (NSC 3a.3.1.1100).

Under DBA2-4 operating conditions, the removal of the residual heat from the reactor, the spent fuel pool and the containment shall be ensured by means of one or more redundant heat removal systems in such a way that jointly they are capable of performing heat removal even if one of the systems or a redundant branch of a system is lost due to a failure and, simultaneously, another system or redundant branch is inoperable due to maintenance or testing. If the heat removal system or its service system contains passive system components, for which an extremely low probability of failure can be demonstrated for the given operating condition, it is sufficient to design the passive system components to be single failure tolerant. (NSC 3a.4.3.0500).

Korea

See answer to 3A.

Poland

A single failure criterion applies to each safety group included in the nuclear facility design.

“The required reliability of a given safety group for each postulated initiating event, on the assumption that a single failure will take place, shall be ensured by the appropriate selection of technical solutions covering the application of proven components, redundancy, diversity, physical and functional separation and the isolation of components.” (Article 37, paragraph 2 – Regulation of the Council of Ministers of 31 August 2012 on nuclear safety and radiation protection requirements which must be fulfilled by a nuclear facility design).

There are no additional requirements for passive safety systems.

Russia

There is some difference between failure criteria of active and passive systems. Para 1.2.12 of the federal norms “General provisions for ensuring safety of nuclear power plants”. NP-001-05 states that: “The established limits for design-basis accidents shall not be exceeded at any initiating event considered by the NPP design with a coincidental independent failure of one of the following safety system elements according to the single failure principle: an active element or a passive element with mechanical movable parts, or a passive element without movable parts whose probability of safety function performance failure is equal to 10^{-3} or higher or one human error in dependent of the initiating event.”

In addition to one failure independent of the initiating event in one of the above elements, it is necessary to consider all failures that are consequence of a given single failure, failures that are consequence of the initiating event, as well as failures of elements affecting the accident evolution which could not be revealed in the course of NPP operation.

Failures of elements (systems which they make part of) may not be considered if high level of their reliability is demonstrated or when the element (system) is in outage for a determined period of time for maintenance and repair.

The reliability level is considered to be high if indicators of reliability of elements (systems) are not lower than appropriate indicators of the most reliable passive elements of safety systems without movable parts.

The permissible time of outage an element for maintenance and repair is defined on the basis of the reliability analysis of the system, to which this element belongs, or based on the probabilistic safety analysis, and it is established in the NPP design.

Slovak Republic

The requirements on the safety systems are not divided into requirements for active and passive systems. Generally, the safety systems have to fulfil following requirements, which are elaborated in more details in the regulation of UJD SR No. 430/2011 Coll.:

- single failure criteria;
- common cause failure criteria;
- fire protection;
- protection against external events;
- conservative approach.

United Kingdom

The safety assessment principles (SAPs) do give not give specific requirements for passive systems. However, the SAPs do give considerable engineering guidance on the generic requirements for safety systems. Specifically: SAP EDR.4 requires that no single random failure assumed to occur anywhere within the systems provided to secure a safety function, should prevent the performance of that safety function. ONR would expect unrevealed single passive failures to be considered so far as is reasonably practicable.

United States

There is no difference in the requirements (10 CFR 50, Appendix A) associated with consideration of the single failure criteria for active safety systems and passive safety systems.

E. The safety classification requirements

Finland

There are no differences. According to the STUK Regulatory Guide on Safety Classification (YVL B.2) system safety classification is determined by the safety function, i.e. “312. Systems accomplishing safety functions shall be assigned to (the Finnish) Safety Class 2 if they are designed to provide against postulated accidents to bring the facility to a controlled state and to maintain this state for as long as the prerequisites for transfer to a safe state can be ensured.”

Safety class 3 includes all the other safety systems.

Germany

The safety classification in German regulation is according to the safety significance and therefore independent of passive or active characteristics.

Hungary

"Methods substantiated by safety analyses and using operating experiences shall be applied for categorisation of passive systems into safety classes." (NSC 3a.2.2.1900.)

Korea

See answer to 3A.

Poland

Safety systems (passive and active) shall be allocated to the appropriate safety class, depending on the importance of the safety functions which they fulfil.

"The nuclear facility design shall identify the systems, structures and components of the nuclear facility which are important for ensuring nuclear safety and radiation protection; these shall be allocated to the appropriate safety class, depending on the importance of the safety functions which they fulfil." (Article 11, paragraph 2 – Regulation of the Council of Ministers of 31 August 2012 on nuclear safety and radiation protection requirements which must be fulfilled by a nuclear facility design).

Russia

There are no differences.

Slovak Republic

The requirements on the safety systems are not divided into requirements for active and passive systems.

United Kingdom

The safety assessment principles (SAPs) do give not give specific requirements for passive systems. However, the SAPs do give considerable engineering guidance on the generic requirements for safety systems. Specifically: SAP ECS.1 states that safety functions should be identified and categorised based on their safety significance and ECS.2 states that the structures, systems and components that deliver these safety functions should be classified on the basis of those functions and their significance to safety.

United States

There is no difference in the safety classification requirements (10 CFR 50.55(a)) for active safety systems and passive safety systems.

F. The protection from external events (e.g. seismic events, aircraft impacts, extreme atmospheric conditions, fires in the vicinity)

Finland

There are no additional or different rules for passive safety systems concerning protection from external events.

Germany

The protection concept applies in general. ("Safety Requirements for Nuclear Power Plants" §2.4).

Hungary

There are no specific requirements for passive systems in this topic.

Korea

See answer to 3A.

Poland

There are no additional requirements. Passive safety systems are designed considering external events. The protection from external events shall be met for example by appropriate redundancy and diversity of systems and components of equipment, their physical separation and design so as to attain a safe state after failure. (Article 110, paragraph 2 – Regulation of the Council of Ministers of 31 August 2012 on nuclear safety and radiation protection requirements which must be fulfilled by a nuclear facility design).

Russia

There are no additional or different rules for passive safety systems concerning protection from external events.

Slovak Republic

The requirements on the safety systems are not divided into requirements for active and passive systems. Generally the safety systems have to fulfil following requirements, which are elaborated in more details in the regulation of UJD SR No. 430/2011 Coll.:

- single failure criteria;
- common cause failure criteria;
- fire protection;
- protection against external events;
- conservative approach.

United Kingdom

The safety assessment principles (SAPs) do give not give specific requirements for passive systems. However, the SAPs do give considerable engineering guidance on the generic requirements for safety systems. Specifically: SAP EHA.1 requires the identification of all external and internal hazards that could affect safety and EHA.6 requires these to be analysed taking into account hazard combinations, simultaneous effects, common cause failure, defence in depth, and consequential effects.

United States

There is no difference in the requirements for protection from external events (i.e. 10 CFR 50, Appendix A, General Design Criterion 2; 10 CFR Part 100, Subpart B; 10 CFR 50.150) for active safety systems and passive safety systems.

Chapter II. Testing and analyses of passive safety systems

Question 1. What safety principles must be demonstrated through testing and analyses?

Finland

STUK Regulation on the Safety of a Nuclear Power Plant (STUK Y/1/2016) requires that the safety of a nuclear power plant shall be assessed when applying for a construction licence and operating licence, in connection with plant modifications, and at Periodic Safety Reviews. It also requires that the nuclear power plant safety and the technical solutions of its safety systems shall be assessed and substantiated analytically and, if necessary, experimentally.

Passive safety systems are typically systems, from which experimental demonstration will be required.

Germany

Same requirements as for active systems apply.

Hungary

There are no special requirements in the case of passive systems in this topic.

Korea

The important safety features must be tested and analysed to the extent as possible. In particular, the performance of the passive systems depends largely on the geometrical configuration, T-H condition, etc. and must be tested and analysed for various conditions that can occur during transients and accidents.

Poland

All technical solutions used in a nuclear facility must undergo tests and analyses.

“In the design and construction process of a nuclear facility, no solutions or technologies shall be used which have not been demonstrated to be appropriate in practice in other nuclear facilities, or by means of tests, studies and analyses.” (Article 36b – Act of Parliament of 29 November 2000 Atomic Law).

It is necessary to evaluate the effectiveness of safety systems. The Atomic Law in Poland requires analyses in order to obtain the appropriate licences.

Russia

There are no differences for active and passive safety systems in regulatory framework for demands to safety principles to be demonstrated.

Para 3.1.8 of federal norms “General provisions for ensuring safety of nuclear power plants” NP-001-05 states that “Safety important systems and elements shall be capable of performing their functions within the NPP design scope and with due consideration of the natural effects (earthquakes, tornadoes, flood sand other natural phenomena within the NPP site), external human-induced events typical for the NPP site and (or) under possible

hydraulic, mechanical, thermal, chemical and other impacts occurred as a result of accidents at which work of the considered systems and elements is required."

Appendix 4 of federal norms "Requirements to Content of Safety Analysis Report for NPP of VVER-type" NP-006-16 states that SAR should describe the computer programs used in the design to analyse the strength, the operability of the system and its elements, the input data for calculations, assumptions and limitations of the numerical schemes, the results of calculations and conclusions. SAR should provide information about the certification of the computer programs and their verification.

If to justify the efficiency of the system experiments were conducted, SAR should describe the experimental conditions, an analysis of the compliance of these conditions the actual conditions of the system, describe the experimental base, metrological support of experiments, give the main results of the experiments.

Passive safety systems are typically systems, for which experimental demonstration will be required.

Slovak Republic

There are no specific requirements regarding testing and analyses of passive safety system. The aim of all tests and analyses is to demonstrate that the systems are able to fulfil their task in compliance with design during all states inclusive design-basis accident, single failure and design extension conditions.

United Kingdom

SAP AV.1 requires the assurance of validity of data and theoretical models.

SAP AV.2 requires that analytical models should be validated by comparison with actual experience, appropriate experiments or tests. Models should be validated for each application made in the safety analysis. The validation should be of the model as a whole or, where this is not practicable, on a module basis, against experiments that replicate as closely as possible the expected plant condition. Care should be exercised in the interpretation of experiments to take account of uncertainties in replicating the range of anticipated plant conditions. The limits of applicability of analytical models should be identified. Where validation against experiments or tests is not possible, a comparison with other, different, calculational methods may be acceptable.

SAP AV.3 requires data used in the analysis of aspects of plant performance with safety significance should be shown to be valid for the circumstances by reference to established physical data, experiment or other appropriate means. Where uncertainty in the data exists, an appropriate safety margin should be provided. The limits of applicability of the available data should be identified and extrapolation beyond these limits should not be used unless justified.

SAP AV.6 requires studies to be carried out to determine the sensitivity of the analysis (and the conclusions drawn from it) to the assumptions made, the data used and the methods of calculation. Where predictions of the analysis are sensitive to the modelling assumptions, they should be supported by additional analysis using independent methods and, where relevant, computer codes.

United States

Generally, the same safety principles must be demonstrated for both active safety systems and passive safety systems. Examples of these safety principles include the performance of the system achieve its safety function (e.g. decay heat removal, core cooling), the absence of adverse systems interactions, and an understanding of the systems performance across all anticipated operational and accident conditions.

Question 2. What are your expectations for the validation of computer codes and the conduct of testing used to demonstrate safety performance?

Finland

STUK Regulation on the Safety of a Nuclear Power Plant (STUK Y/1/2016) requires that the analytical methods employed to demonstrate compliance with the safety requirements shall be reliable, verified and qualified for the purpose.

The STUK Regulatory Guide on deterministic safety analyses (YVL B.3) further requires that:

"407. If reliable calculation methods are not available, the acceptability of the technical solution in question shall be justified by means of experiments."

Germany

Generally "Safety Requirements for Nuclear Power Plants" §5 (4) state that:

"5 (4) In the computational analysis of event sequences or states,

a) calculation methods shall be used which are validated for the respective scope of application; and
b) any uncertainties associated with the calculation shall be quantified or covered by suitable methods."

This applies also for passive systems.

Hungary

There are no special requirements in the case of passive systems in this topic.

Korea

In general, validation is required to demonstrate that computer codes used in the safety analyses give a reasonable prediction of thermal-hydraulic characteristics. The separate effect and integral effect tests are conducted for code validation.

From our review experience of the passive auxiliary feedwater system (PAFS) for APR+ design, the code validation must be made against a wider spectrum of conditions that can occur in various accident scenarios.

Poland

Computer codes have to be validated and verified. The work of passive systems has to be properly reflected in the modelling included in the computer codes and the results should be validated with reference to best knowledge and experimental work. International experiments can be used to justify the proper work of the computer codes. In case of

doubts, it is possible to ask the licensee for additional demonstration of the work of system or component. Independent verification is essential and stressed as a general rule.

"The performance of safety analyses shall be included in the quality assurance programme. In particular the source of origin of all data shall be indicated and documented and the entire analysis process shall be documented and archived in a manner permitting it to be subject to independent verification." (Article 12 – Regulation of the Council of Ministers of 31 August 2012 on the scope and method for the performance of safety analyses prior to the submission of an application requesting the issue of a license for the construction of a nuclear facility and the scope of the preliminary safety report for a nuclear facility).

Russia

There are no differences for active and passive safety systems in regulatory framework for demands to safety principles to be demonstrated.

Para 3.1.8 of federal norms: "General provisions for ensuring safety of nuclear power plants" NP-001-05 states that:

Safety important systems and elements shall be capable of performing their functions within the NPP design scope and with due consideration of the natural effects (earthquakes, tornadoes, flood sand other natural phenomena within the NPP site), external human-induced events typical for the NPP site and (or) under possible hydraulic, mechanical, thermal, chemical and other impacts occurred as a result of accidents at which work of the considered systems and elements is required.

Appendix 4 of federal norms "Requirements to Content of Safety Analysis Report for NPP of VVER-type" NP-006-16 states that:

SAR should describes the computer programs used in the design to analyse the strength, the operability of the system and its elements, the input data for calculations, assumptions and limitations of the numerical schemes, the results of calculations and conclusions. SAR should provide information about the certification of the computer programs and their verification.

If to justify the efficiency of the system experiments were conducted, SAR should describe the experimental conditions, an analysis of the compliance of these conditions the actual conditions of the system, describe the experimental base, metrological support of experiments, give the main results of the experiments.

Passive safety systems are typically systems, for which experimental demonstration will be required.

Slovak Republic

Based on legislative requirements the way of ensuring verification and validation of the computer codes for safety analyses has to be content of the QA programme for nuclear facility. Validation should test the accuracy of modelling single mechanisms and processes, the way of the mechanisms and processes connection and should find if the whole important facts have been taken into account. The validation should set and evaluate the accuracy of assessed software.

United Kingdom

SAP AV.1 requires the assurance of validity of data and theoretical models.

SAP AV.2 requires that analytical models should be validated by comparison with actual experience, appropriate experiments or tests. Models should be validated for each application made in the safety analysis. The validation should be of the model as a whole or, where this is not practicable, on a module basis, against experiments that replicate as closely as possible the expected plant condition. Care should be exercised in the interpretation of experiments to take account of uncertainties in replicating the range of anticipated plant conditions. The limits of applicability of analytical models should be identified. Where validation against experiments or tests is not possible, a comparison with other, different, calculation methods may be acceptable.

SAP AV.3 requires data used in the analysis of aspects of plant performance with safety significance should be shown to be valid for the circumstances by reference to established physical data, experiment or other appropriate means. Where uncertainty in the data exists, an appropriate safety margin should be provided. The limits of applicability of the available data should be identified and extrapolation beyond these limits should not be used unless justified.

SAP AV.6 requires studies to be carried out to determine the sensitivity of the analysis (and the conclusions drawn from it) to the assumptions made, the data used and the methods of calculation. Where predictions of the analysis are sensitive to the modelling assumptions, they should be supported by additional analysis using independent methods and, where relevant, computer codes.

United States

Passive safety systems may introduce new technical issues that must be addressed to ensure adequate protection of the public health and safety. Reactor designers are responsible for documentation and research necessary to support a specific application. Research activities would include testing of new safety features that differ from existing designs for operating reactors, or that use simplified, inherent, passive means to accomplish their safety function. The testing shall ensure that these new features will perform as predicted, will provide for the collection of sufficient data to validate computer codes, and will show that the effects of system interactions are acceptable.

Question 3. For the concurrent operation of several different passive safety systems (trains), what are your expectations for the testing and analyses required to be demonstrated by Licensee?

Finland

If there is a possibility of negative effects (the trains disturbing each other) due to concurrent operation of several passive safety system trains, the effects should be analysed and if necessary tested.

Germany

No specific requirements available, same requirements as for active systems apply.

Hungary

There are no special requirements in this topic.

Korea

We do not have experience of the testing and analyses for concurrent operation of several different passive safety systems. We are to develop the requirements for future use of several different passive systems in a reactor.

Poland

A combination of work of several different passive safety systems might lead not only to positive effects. If there is a possibility of negative effects due to concurrent operation of several passive safety systems, the effects should be analised and discussed. If necessary, such a situation should be tested and the results should be accepted. International experiments can be used in the demonstration.

Russia

If there is a possibility of negative effects (systems or trains disturbing each other) due to concurrent operation of several passive safety systems (or trains), the effects should be analysed and if necessary verified by experiments.

One of practical example is concurrent operation of SG passive heat removal system and passive core flooding system in case of LOCA accompanied with active ECCS in AES-2006 design (Moscow variant). Such concurrent operation can be negatively affected by non-condensable gases entered to heat exchanger surfaces from containment through leakage. Experimental justification based on specially constructed experimental stand was submitted by licensee to Regulatory Body, the justification shows necessary efficiency of the mentioned above systems with taking into consideration the non-condensable gas entering phenomenon.

Slovak Republic

The RB expectations regarding tests and analyses are the same in all safety systems. It does not matter if it regards active or passive safety systems. The expectation is, that licensee demonstrates that the systems are able to fulfil their task in compliance with design during all states inclusive design-basis accident, single failure and design extension conditions.

United Kingdom

Where there is scope for interaction between various passive systems ONR would expect integral testing to be performed to confirm that such interactions are well understood and acceptable in terms of the safety case, consistent with the requirements of AV.2 discussed above.

United States

Reactor designers are expected to address concurrent operation of different safety systems and demonstrate that any interdependent effects are acceptable.

Question 4. For the concurrent operation of passive and active safety systems, what are your expectations for testing and analyses to be demonstrated by Licensee?

Finland

If there is a possibility of negative effects due to concurrent operation of passive and active systems, the effects should be analysed and if necessary tested.

Germany

No specific requirements available, same requirements as for active systems apply.

Hungary

There are no special requirements in this topic.

Korea

We do not have experience of the testing and analyses for concurrent operation of passive and active safety systems.

Poland

The work of passive safety systems in combination with active safety systems might lead not only to positive effects. If there is a possibility of negative effects due to concurrent operation of passive and active systems, the effects should be analysed and discussed. If necessary, such a situation should be tested and the results accepted. International experiments can be used in the demonstration.

Russia

If there is a possibility of negative effects due to concurrent operation of passive and active systems, the effects should be analysed and if necessary tested.

If safety function can be fulfilled by either active or passive safety system the SAR should contains substantiation for both cases: a) when only active systems are in operation and b) when only passive systems are in operation.

Slovak Republic

The RB expectations regarding tests and analyses are the same in all safety systems. It does not matter if it regards active or passive safety systems. The expectation is, that licensee demonstrates that the systems are able to fulfil their task in compliance with design during all states inclusive design-basis accident, single failure and design extension conditions.

United Kingdom

Essentially, the answer is the same as the previous one and for the same reasons.

United States

Generally, new reactor designs have not proposed a mixture of active safety systems and passive safety systems to mitigate design-basis events; however, some designs do include active systems (e.g. for reactor coolant makeup and decay heat removal) for defence-in-depth purposes. In the event they are proposed, reactor designers are expected to address concurrent operation of different safety systems and demonstrate that any interdependent effects are acceptable.

Chapter III. Regulatory review of passive safety systems

Question 1. How are functional failures identified and considered in the safety demonstration? Summarise any considerations given to the following potential functional failures.

A. Containment isolation challenged by a leaking passive system penetrating the containment wall

Finland

STUK Regulatory Guide on containment (YVL B.6) requires that every line penetrating the containment pressure boundary and communicating with the reactor coolant or containment atmosphere shall be equipped with at least two independent isolation valves in series. This is required of active and passive systems.

Germany

There are no special requirements for passive systems. Containment by-pass needs to be eliminated.

Hungary

There are no special requirements in the case of passive systems in this topic.

Korea

We do not have experience of reviewing such failure of passive system as cited.

In reviewing PAFS of APR+ design, potential functional failures discussed were flow instability and water hammer, unexpected heat loss, fouling, and check valve failure, etc. The check valve is not installed in the configuration repositioned for safety function of the PAFS. The functional failures of the passive systems are to be studied in the R&D project.

Poland

The Polish regulatory framework requires that lines penetrating the containment shall be equipped with at least two independent isolation valves in series.

The pipeline shall be equipped with at least two valves cutting off the reactor containment or back-flow valves, lined up, located as close as possible to the reactor containment, capable of reliable and independent actuation. The design of reactor containment area cut-off (isolation) shall take into account the single failure criterion. Exception from the requirements shall be permitted only in reference to the specific types of components, such as impulse tubes in measurement systems, or when the failure to apply these exceptions would lead to deterioration of safety system reliability, which comprises the pipeline passing through the reactor containment. (Article 70, paragraph 2-3 – Regulation of the Council of Ministers of 31 August 2012 on nuclear safety and radiation protection requirements which must be fulfilled by a nuclear facility design).

Russia

Federal norms NP-001-15 and NP-010-16 requires that every line penetrating the containment pressure boundary and communicating with the reactor coolant or containment atmosphere shall be equipped with at least two independent isolation valves in series. This is required for both active and passive systems.

Slovak Republic

Consideration of the functional failures in the safety demonstration is covered by application of the conservative approach in the safety analyses. The regulatory body does not identify potential failures. It is up to applicant for licence. There no strict criteria for identification of failures set up in our legislation.

United Kingdom

Generally, our expectations are the same as for active safety systems. The SAPs set out a large number of safety principles which an engineered safety system would be expected to meet. These include but are not limited to:

- SAP ECS.2 on the classification of safety systems;
- SAPs ECS.3 to ECS.5 on the use of appropriate codes and standards, experience, tests and analysis;
- SAP EQU.1 on equipment qualification;
- SAPs EDR.1 to EDR.4 on design for reliability including failure to safety, redundancy, diversity and segregation, common mode failure, single failure criterion;
- SAPs ERL.1 to ERL.4 on reliability claims including margins of conservatism. Specifically, with regard to failure modes, SAP ERL.2 calls for reliability analysis to be performed for both random and systematic failures. Where reliability data is inadequate, appropriate measures should be taken to ensure that the onset of failures will be detected and that the consequences of failure minimised;
- SAP ECM.1 on commission testing;
- SAPs EMT.1 to EMT.6 cover maintenance, inspection and testing including frequency, type testing, functional testing and continuing reliability following events (which would include spurious actuation);
- SAPs EAD.1 to EAD.5 on ageing and degradation;
- SAPs EHA.1 to EHA.19 on internal and external hazards;
- SAPs ESS.1 to ESS.27 on safety system control and instrumentation.

ONR would expect the design of the containment isolation system to be tolerant to a single random failure and, in the case of frequent SBLOCA, to be tolerant to the common mode failure of the containment isolation valves.

United States

Reactor designers are expected to conduct a systematic evaluation to identify and evaluate potential functional failures. In addition to functional failures considered for active safety systems, designers must complete a full evaluation to determine whether any new or unique functional failures have been introduced through the use of passive safety systems. Containment isolation provisions for passive safety systems are the same as those for active safety systems. Both active and passive safety systems may penetrate the containment boundary.

B. Non-condensable gases collecting in heat exchangers

Finland

The parameters should be provided to the extent needed to understand and demonstrate the operation of the safety system.

Germany

There are no special requirements for passive systems.

Hungary

There are no special requirements in the case of passive systems in this topic.

Korea

We do not have experience of reviewing such failure of passive system as cited.

In reviewing PAFS of APR+ design, potential functional failures discussed were flow instability and water hammer, unexpected heat loss, fouling, and check valve failure, etc. The check valve is not installed in the configuration repositioned for safety function of the PAFS. The functional failures of the passive systems are to be studied in the R&D project.

Poland

The applicant or licensee should analyse the effects of non-condensable gases collecting in heat exchangers. In case when the amount of gases might lead to a threat to safety, he should propose a solution to this problem.

Russia

The licensee should provide analyses of the effects of non-condensable gases and a strategy to prevent collection of them in heat exchangers (steam generators). This is part of the safety demonstration of the system. See also answer to Question 3 of Chapter II.

Slovak Republic

Consideration of the functional failures in the safety demonstration is covered by application of the conservative approach in the safety analyses. The regulatory body does not identify potential failures. It is up to applicant for license. There no strict criteria for identification of failures set up in our legislation.

United Kingdom

Where there is the possibility of the presence of non-condensable gases in the primary circuit with the potential to reduce the effectiveness of natural circulation as a heat removal mechanism ONR would expect the safety case to demonstrate with high confidence through testing and analysis that the system is either tolerant of such effects or the presence of such gases has been prevented by design.

United States

Reactor designers are expected to conduct a systematic evaluation to identify and evaluate potential functional failures. In addition to functional failures considered for active safety systems, designers must complete a full evaluation to determine whether any new or unique functional failures have been introduced through the use of passive safety systems. To the extent that non-condensable gases could collect in heat exchangers and negatively impact the performance of passive safety systems, they must be addressed in the design and demonstrated to not impact safety performance.

Question 2. What are your expectations for the applicant or licensee to provide substantiation of passive safety system parameters (e.g. pressure, temperature, flow rates, inventory, procedures, concentration of neutron absorbers, pressure resistance of lines, valve characteristics)?

Finland

The parameters should be provided to the extent needed to understand and demonstrate the operation of the safety system.

Germany

Same requirements as for active systems apply.

Hungary

There are no special requirements in the case of passive systems in this topic.

Korea

All the parameter affecting the intended safety function should be provided.

As an example, a lot of parameters have been provided regarding the ECCS sump clogging.

Poland

The applicant or licensee should provide substantiation of passive safety system parameters. He should prove that safety systems fulfil safety requirements, lead to benefits and cannot influence an increase in the risk of an incident.

Russia

The parameters should be provided to the extent needed to understand and demonstrate the operation of the safety system.

Slovak Republic

Expectation of RB are, that applicant shows, that the safety system`s parameters are set up appropriately to ensure, that the safety system will be able fulfil their task in compliance with design during all states inclusive design-basis accident, single failure and design extension conditions.

United Kingdom

Generally, our expectations are the same as for active safety systems. See the response to Q1 above.

United States

Reactor designers must identify and provide a technical basis for safety system parameters that are used to verify system operation. The technical basis could come from existing experience with similar systems, or from experimental testing and analysis.

Question 3. What are your expectations for the applicant or licensee to provide the results of quantitative and qualitative analysis of passive safety systems reliability? Are there any special considerations for the reliability analysis because of passivity?

Finland

There are no system specific requirements for safety system reliability in the Finnish regulation. All systems important to safety shall be qualified. STUK Regulatory Guide for safety design of a nuclear power plant (YVL B.1) requires that:

"362. The systems, structures and components important to safety shall be qualified for their intended use. The qualification process shall demonstrate that the systems, structures and systems are suitable for intended use and satisfy the relevant safety requirements. Aside from the assurance of the correctness of the design bases and the sufficiency of the quality management of design and implementation, the qualification process shall also include environmental qualification."

Germany

Same requirements as for active systems apply.

Hungary

There are no special requirements in the case of passive systems in this topic.

Korea

Quantitative analysis of the reliability will be preferred when developing the requirements.

Poland

There are no special specific requirements for passive safety systems reliability. It depends on what safety class system is classified.

"Systems and components of construction and equipment of the nuclear facility belonging to a higher safety class shall have to meet higher quality and reliability requirements than the systems and components of construction and equipment which belong to a lower safety class." (Article 11, paragraph 7 – Regulation of the Council of Ministers of 31 August 2012 on nuclear safety and radiation protection requirements which must be fulfilled by a nuclear facility design).

Russia

Para 3.1.17 of federal norms "General provisions for ensuring safety of nuclear power plants" NP-001-05 states that:

In NPP Safety justification Report the reliability analyses of fulfilment of functions by the safety important systems and reliability indicators of the safety important elements shall be presented. The reliability analysis shall be conducted with due consideration of the common cause failures and human errors.

The reliability indicators of the safety important systems and elements shall be supported during the operation life by proper maintenance, repair, and control of the metal (including welded joints) state performed with due consideration for the requirements of the federal norms and rules in the field of the use of atomic energy with the frequency proved in the NPP design.

In connection to this requirement Rostekhnadzor issued Regulatory guide "Recommendations on order of execution reliability analysis of systems and components of nuclear power plants important to safety and their functions" RB-100-15. The guide

describes general order of fulfilment qualitative and quantitative reliability analysis of safety important systems. Besides this general order the guide consider several specific cases of reliability analysis – computerised systems analyses, complicated technological complexes – such as refuelling machines – analyses, peculiarities of passive systems analysis.

Reliability analysis order presented in the last chapter is recommended to systems which reliability model which takes into account the performance of passive elements, experiencing the effects of operational loads such as own weight, the pressure of the working medium (fluid pressure, fuel or oil), nourishing or cooling water in the pipe or heat exchange unit, the gas pressure in the pressure vessel, hydrostatical pressure in the storage container or in tank) temperature at the load, etc., as well as experiencing the effects of an emergency and a special loads (e.g. emergency pressure, temperature, shock, including water hammer, fire load, accidental pressure protective shell) and loads due to external influences (e.g. inertial loads, shock loads).

To assess the reliability of passive components limit the following computational methods are recommended by the guideline:

- method of safety factors (the model of "load-strength");
- methods of two moments (method of reliability of the first order "FORM" and method reliability of the second order "SORM");
- statistical modelling techniques (e.g. Monte-Carlo method, Monte-Carlo sampling importance simulations with a regionalised sample, for example, the method of Latin hypercube).

Slovak Republic

The expectation of RB is, that the results of quantitative and qualitative analyses shows, that the safety system will be able fulfil their task in compliance with design during all states inclusive design-basis accident, single failure and design extension conditions.

United Kingdom

ONR expects there to be a limit place on the reliability of a safety system. For passive structures such as the pressure vessel of a PWR high integrity arguments may be acceptable. However, even for very simple safety systems SAPs EDR.3 places a quantitative limit of 10-5 per demand. For moderately complex systems worst figures than this should be assumed. In practice, for frequent initiating faults (>10-3 per year) we would therefore expect a deterministic demonstration (i.e. qualitative analysis?) of functional diversity in which the common mode failure of a system has to be assumed.

United States

Reactor designers must conduct a design specific probabilistic risk assessment of the entire reactor design, which would include modelling of passive safety systems. The results of the probabilistic risk assessment must be submitted with the application. For reactor designs using passive safety systems and active defence-in-depth systems, reactor designers are expected to perform sensitivity studies without crediting the non-safety related defence-in-depth systems. These studies provide additional insights about the risk importance of the defence-in-depth systems that are taken into account in selecting non safety-related systems for additional regulatory treatment.

Reactor designers are also expected to address thermal-hydraulic uncertainties in passive plant designs that arise from the passive nature of the safety-related systems used for accident mitigation. Passive safety systems rely on natural forces, such as gravity, to perform their safety functions. Such driving forces are small compared to those of pumped systems, and the uncertainty in their values, as predicted by a best-estimate thermal-hydraulic analysis, can be of comparable magnitude to the predicted values themselves. Therefore, some accident sequences with a frequency high enough to impact results, but not predicted to lead to core damage by a best-estimate thermal-hydraulic analysis, may actually lead to core damage when probabilistic risk assessment models consider thermal-hydraulic uncertainties. One approach to addressing this issue is to perform sensitivity studies to see the effect of assuming bounding values for thermal-hydraulic parameters on success criteria and performing studies of the sensitivity of changes in success criteria on the core damage frequency.

Question 4. What are your expectations for the review of instrumentation and control systems for passive safety systems? What information is required to be submitted?

Finland

There are no specific requirements for passive safety systems. STUK Regulatory Guide for safety design of a nuclear power plant (YVL B.1) requires that:

"5214. Nuclear power plants shall be provided with accident instrumentation necessary for bringing the plant to, and keeping it in, a controlled state and capable of indicating the completion of safety functions in accident conditions. Such accident instrumentation shall include all the devices in the data transmission connection all the way from the sensor to the display unit."

The information required and review of I&C for the passive and active systems would be similar.

Germany

Same requirements as for active systems apply.

Hungary

There are no special requirements in the case of passive systems in this topic.

Korea

It should be discussed. However, general requirements on I&C systems should be consistently applied to the passive system including redundancy and diversity.

Poland

There are no specific requirements for passive safety systems.

"There shall be a suitable review and assessment system in place enabling the permanent monitoring of nuclear safety issues and the performance of periodic nuclear safety assessments." (Article 8, paragraph 6 – Regulation of the Council of Ministers of 11 February 2013 on requirements for the commissioning and operation of nuclear facilities).

Russia

There are no specific requirements for passive safety systems. The information required and review of I&C for the passive and active systems would be similar.

Slovak Republic

The information required to be submitted are set up in the act No. 431/2004 Coll. and in the regulation of UJD SR No. 431/2011 Coll. Based on these information must be cleared that I&C systems are able to fulfil their tasks. Our expectation is that I&C systems are in compliance with legislative requirements and with project.

United Kingdom

Generally, our expectations are the same as for active safety systems. See the response to Q1 above. The I&C design should be justified in the safety case.

United States

There is no difference in the expectations for review of instrumentation and control systems between active safety systems and passive safety systems. A description of the instrumentation and control systems shall be submitted with the application. Instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges.

Question 5. What are your expectations for the applicant or licensee to demonstrate the maximum number of passive safety system actuations (including false actuations), and consider the equipment design life and environment that it is operating in?

Finland

There are no specific requirements to evaluate the maximum number of actuations. STUK Regulation on the Safety of a Nuclear Power Plant (STUK Y/1/2016) requires that systems important to safety shall operate as designed through the plant operating life. STUK Regulatory Guide for Safety Design of a Nuclear Power Plant (YVL B.1) requires that:

"406. Systems performing safety functions shall be so designed as to ensure that their operability can be tested or otherwise verified during the operation of the plant under operational states and operating conditions as close as possible to the actual operational states and operating conditions for which they were designed. Components important to the operability of a safety function shall be accessible for inspection."

Germany

Same requirements as for active systems apply.

Hungary

There are no special requirements in the case of passive systems in this topic.

Korea

In general licensee should demonstrate the maximum number of passive system and consider the environmental condition. It should be described in the requirement.

Poland

There are no specific requirements to evaluate the maximum number of actuations.

When designing systems and components of construction and equipment of the nuclear facility important for ensuring nuclear safety and radiation protection, provision shall be made for the appropriate safety reserves which take into account the consumption mechanisms of these systems and components and their potential technical degradation connected with ageing, so as to ensure the capacity of nuclear facility systems and components of construction and equipment to perform safety functions throughout the period of use determined in the facility design. (Article 42, paragraph 1 – Regulation of the Council of Ministers of 31 August 2012 on nuclear safety and radiation protection requirements which must be fulfilled by a nuclear facility design).

Russia

There are no specific requirements to evaluate the maximum number of actuations.

Slovak Republic

RB's expectations are, that the safety systems are designed to fulfil their task during all life time of NPP. Assessment of this ability is also a part of PSR.

United Kingdom

Generally our expectations are the same as for active safety systems. See the response to Q1 above.

United States

There are no specific requirements for the maximum number of passive safety system actuations. The equipment design life and the qualification of equipment to operate under normal, abnormal, and accident conditions must be evaluated and submitted with the application.

Question 6. What are your expectations for the applicant or license to evaluate the impact of false actuation (starting) of passive safety systems? Are there any special considerations in the starting procedure of passive safety systems?

Finland

STUK Regulatory Guide for deterministic safety analysis (YVL B.3) requires that the inadvertent actuation of every system accomplishing a safety function – active or passive – should be evaluated as an initiating event.

Germany

Same requirements as for active systems apply.

Hungary

There are no special requirements in the case of passive systems in this topic.

Korea

We have an experience with the PAFS and we have reviewed the false actuation of at that review. The impact of false actuation should be considered in the design requirement.

Poland

There are no special considerations in the starting procedure of passive safety systems. The applicant or licensee should provide analyses of all the possible failures that can occur in a nuclear facility.

Russia

Russian Regulatory Guides for deterministic and probabilistic safety analyses requires that the inadvertent actuation of every system accomplishing a safety function – active or passive – should be evaluated as an initiating event.

Slovak Republic

RB's expectations are, that applicants prove that false actuation of safety system has no negative impact on safety and that he has the system for prevention of false actuation.

United Kingdom

Generally, our expectations are the same as for active safety systems. See the response to Q1 above. ONR would expect the system to be qualified for fault conditions including spurious actuation.

United States

False or inadvertent actuation of passive safety systems must be addressed in the application consistent with other anticipated operational occurrences. Passive safety systems are designed to actuate automatically in response to abnormal conditions at the plant. In addition, provisions exist for operators to manually initiate passive safety systems.

Question 7. What are your expectations for the applicant or licensee to submit information on the response of liquids and gases in the passive flooding systems tanks, such as droplet carryover and possibility for blowdown?

Finland

The information should be provided, if it is needed to demonstrate that the system will operate as designed.

Germany

Same requirements as for active systems apply.

Hungary

There are no special requirements in the case of passive systems in this topic.

Korea

We have never considered the case.

Poland

The applicant or licensee should provide the information. If it is needed to demonstrate that the system will operate as designed.

Russia

The information has to be provided, if it is needed to demonstrate that the system operates as designed.

Slovak Republic

Our expectation is that applicant proves the function of the system in compliance with the design, which of course has to be in compliance with the legislative requirements.

United Kingdom

We would expect all potential failure modes of a system to be identified including any that are due to thermal-hydraulic phenomenon. We would then expect the safety case to demonstrate with high confidence through testing and analysis that the system is either tolerant of such effects or they are prevented from arising by virtue of the design.

United States

To the extent that non-condensable gases could collect in heat exchangers and negatively impact the performance of passive safety systems, they must be addressed in the design and demonstrated to not impact safety performance.

Chapter IV. Commissioning and periodic verification testing

Question 1. What are your expectations for testing passive safety systems during commissioning?

Finland

Passive safety systems, as any safety systems, should be tested during commissioning to the extent feasible. Active components of the passive systems should be tested.

There may be examples of passive systems (core flooding tanks?) which may not allow full testing. It is expected that the passive safety systems under review in Finland (see V.1) can be tested when the plant will reach commissioning phase.

Germany

Not applicable for Germany since no new NPP will be commissioned.

Hungary

There are no special requirements in the case of passive systems in this topic.

Korea

Passive systems should be tested as close to the design condition during commissioning. Technical difficulties in performing the test as close to the design condition should be identified and alternative mean should be introduced if acceptable.

Poland

There are safety systems that cannot be tested during commissioning. The Polish regulatory framework requires that safety systems should be tested before commissioning phase. It is not specified in the regulation, how to test passive safety systems.

Russia

Passive safety systems, like any other safety systems, has to be tested during commissioning to the extent feasible. Active components of the passive systems shall be tested.

Slovak Republic

RB's expectation is demonstration the ability of the systems to fulfil their task in compliance with design during all states inclusive design-basis accident, single failure and design extension conditions.

United Kingdom

Generally, our expectations are the same as for active safety systems. SAP ECM.1 requires that commissioning tests should:

- demonstrate that, as built, the design intent claimed in the safety case has been achieved;
- collect baseline data for the equipment and systems for future reference;

- validate the operating instructions for which the commissioning tests provide representative activities;
- familiarise the operators with the operation of the plant;
- identify errors remaining following the design, manufacture and construction stages or confirm the absence of such errors;
- provide assurance of safety, including human error.

United States

Passive safety systems are tested during commissioning. The purpose of the testing is to demonstrate that the constructed design meets the specified design acceptance criteria. Commissioning testing is not intended to provide proof of principle for safety systems. Rather, these safety systems must be demonstrated through testing and analysis done in support of submitting a licence application.

Question 2. What are your expectations for the interval and scope of periodic checks and testing of passive safety systems during nuclear power plant operations?

Finland

Passive safety systems, as any safety systems, should be tested in operating plants to the extent feasible. Testing under power operation, as for active systems, may not be possible. Active components of the passive systems should be tested.

Germany

Test interval and scope of the testing are part of the Testing Manual (see KTA 1202) as part of the OLCs. During the licensing process, the licensee proposes the scope and frequency for the testing, which is then approved by the regulator and is thus part of the license. However, scope and frequency depend on the component/system. For selected SSCs non-binding regulations such as KTA Standards exist.

For example, the Testing Manual could specify that an accumulator would need to be tested every forth revision (one accumulator per revision, 4 accumulators) witnessed by an authorised expert.

Hungary

There are no special requirements in the case of passive systems in this topic.

Korea

It should be based on the safety importance and the reliability of the passive system considered.

Poland

There are no special specific requirements for passive safety systems. Safety systems should be designed to allow testing.

“Safety systems, including in particular the protection system, shall be designed in a manner permitting the periodic testing of their functionality during reactor operations, taking into account the independent testing of channels with the purpose of detecting failures and possible loss of redundancy.” (Article 88, paragraph 2 – Regulation of the

Council of Ministers of 31 August 2012 on nuclear safety and radiation protection requirements which must be fulfilled by a nuclear facility design).

Russia

Passive safety systems, as any safety systems, should be tested in operating plants to the extent feasible. Testing under power operation, as for active systems, may not be possible. Active components of the passive systems should be tested.

Slovak Republic

Expectation is that the testing of systems are in compliance with the requirements from L&C.

United Kingdom

Generally, our expectations are the same as for active safety systems. SAP EMT.1 requires periodic in-service testing, inspection and other maintenance procedures.

United States

Periodic checks and testing of passive safety systems in done similar to that for active safety systems. Some of the testing is specified in technical specifications and other testing requirements are specified in the SAR or through conformance to industry standards. It is anticipated that the majority of testing for passive safety systems will occur during plant outages.

Chapter V. Experience with passive safety systems

Question 1. What are your experiences with passive safety systems? For the systems below, describe (1) the purpose of the system and the safety functions to be performed, (2) the events the system is designed to mitigate, (3) the parameters (e.g. reactor vessel level) that initiate the system, and (4) any special features that control the operation of the system.

A. Passive reactor core flooding system

Finland

None.

Germany

In PWRs accumulators are used as safety injection system in addition to active safety systems. These are used in particular for LOCA and are actuated by low pressure in the primary system. Two valves can be used to disconnect the accumulators from the primary circuit.

Hungary

Hydroaccumulators: the main purpose of hydroaccumulators is to ensure sub-criticallity, heat removal from reactor core, restore coolant inventory in the case of a LOCA event initiated by small pressure.

Korea

None.

Poland

There is the system of emergency flooding of the core in the reactor MARIA. Two valves are an essential part of the system. Valves will open to the inertia of the large pressure drop in the cooling circuit fuel channels. As a result, fuel will always be under water, despite the leaks in the cooling circuit fuel channels.

Russia

AES-2006 design (Moscow variant) uses passive reactor core flooding system with 2nd stage hydro accumulators, VVER-TOI design includes passive reactor core flooding system with 2nd stage and 3rd stage hydro accumulators.

Slovak Republic

Slovak Republic has experience with passive reactor core flooding system – hydroaccumulators.

Core flooding performed safety function: reactivity regulation, heat removal.

LOCA with black out.

Primary circuit pressure < 6 MPa (EBO) or 3.5 MPa (EMO).

No.

United Kingdom

Accumulators (1) are used on PWRs throughout the world for reactor core flooding following large break LOCA faults (2). Although there is a moving check valve that will be reconfigured initially due to (3) the differential pressure across the valve caused by the depressurisation transient their function is mostly passive. The flow from the accumulator is governed by its initial pressure, the flow resistance of the injection line and the initial volume of the cover gas (4). ONR is not aware of any failures during testing of the accumulators during outages at the Sizewell B power station.

United States

The NRC has experience with evaluating passive core cooling systems for various reactor designs including the Westinghouse AP600 pressurised water reactor, Westinghouse AP1000 pressurised water reactor, General Electric simplified boing water reactor, and General Electric Hitachi economic simplified boiling water reactor. The purpose of the passive core cooling systems is to ensure that the specified acceptable fuel design limits are not exceeded. The passive core flooding system is intended to mitigate events such as decrease in reactor coolant system inventory and shutdown events. Examples of these events include steam generator tube rupture, loss-of-coolant accident, and loss of residual heat removal during shutdown operations. The parameters that actuate the passive core cooling system are typically pressuriser low pressure, pressuriser low level, steam line low pressure, containment high pressure, cold leg low temperature, and manual actuation.

B. Passive heat removal systems

Finland

The AES-2006 VVER is under construction licence review in Finland. It has two passive safety systems:

- passive containment heat removal system mainly for severe accidents; and
- passive heat removal system connected to the secondary side of the steam generators for design extension conditions.

The passive containment heat removal system is operating in all operating conditions from normal operation to severe accidents. There is an active containment heat removal system for design-basis accidents (containment spray) but this is not credited in severe accidents. The passive containment heat removal system is the only system assumed available in severe accident analyses.

The passive steam generator heat removal system is needed in some design extension condition, loss of ultimate heat sink for example. Operation of the system will need manual operator actions. Details for these are not yet available at STUK.

Germany

In BWRs the wet well is used as heat sink in the early phase of an accident sequence. At a later stage an active system has to take over. The systems are regularly tested by actuating the pilot valves of the safety valves.

Hungary

None.

Korea

None.

Poland

Natural convection cooling in the fuel channel allows for effective removal of heat generated in the fuel after shutdown of the reactor MARIA**.**

Russia

The AES-2006 design (Saint Petersburg variant) has two passive safety systems:

- Water-cooled passive containment heat removal system; and
- Water-cooled passive heat removal system connected to the secondary side of the steam generators.

The AES-2006 design (Moscow variant) and VVER-TOI design have one passive safety system:

- Air-cooled passive heat removal system connected to the secondary side of the steam generators.
- The passive containment heat removal system is operating in all operating conditions from normal operation to severe accidents.
- The passive steam generator heat removal system is needed in some BDBAs, loss of ultimate heat sink for example.

Slovak Republic

None.

United Kingdom

Natural circulation (1) is used as a means of removing decay heat (2) from the primary circuit of both advanced cooled reactors (AGRs) (failure of forced circulation) and the PWR (loss of grid) in the United Kingdom (as well as on the former Magnox reactors). The flow starts naturally (3/4) once forced circulation is stopped. There is no experience of this natural phenomenon failing during either tests or fault conditions.

United States

The NRC has experience with evaluating passive residual heat removal systems for various reactor designs including the Westinghouse AP600 pressurised water reactor, Westinghouse AP1000 pressurised water reactor, General Electric simplified boing water reactor, and General Electric Hitachi economic simplified boiling water reactor. The purpose of the passive heat removal systems is to remove decay heat from the reactor core. The passive heat removal system is intended to mitigate events such as increase in heat removal by the secondary system and decrease in heat removal by the secondary system. Examples of these events include inadvertent opening of steam generator power-operated relieve or safety valve, steam system piping failure, loss of main feedwater flow, and feedwater system piping failure. The parameters that actuate the passive heat removal system are typically steam generator low level, core makeup tank actuation, automatic depressurisation actuation, pressuriser water level, and manual actuation.

C. Other passive safety systems

Finland

PWR accumulators can be considered as passive components within the active ECCS systems. All PWR operators have experiences of these.

Germany

None.

Hungary

Passive autocatalytic recombiner: the main purpose is to remove hydrogen from the containment and prevent containment damage after core damage.

Bubble condenser: the main purpose is to reduce pressure in the containment and prevent containment damage.

Korea

We have an experience with PAFS for APR+ design. The purpose of the PAFS is to provide a feedwater for all the accidents which needed auxiliary feedwater. Thus, main steam line break, feedwater line break, and events related to heat removal through the secondary side are included. Steam generator water level (AFW actuation signal) initiates the PAFS. One of the most important controls was the PAFS actuation after confirming Main Steam Isolation Valve Closure.

Poland

None.

Russia

None.

Slovak Republic

Slovak Republic has experience with passive safety system for confinement pressure decreasing – bubbler tower:

protect the confinement, safety function: safety barrier protection;

LOCA with Black Out;

confinement overpressure > 5 kPa;

no.

United Kingdom

The control rods (1) on the AGRs and the PWR fall into the core under the influence of gravity (2/4) to automatically trip the reactors following loss of grid (3). Again there is no experience of this natural phenomenon failing during either tests or fault conditions.

United States

The NRC has experience with evaluating other passive safety systems such as passive containment cooling systems for various reactor designs including the Westinghouse AP600 pressurised water reactor, Westinghouse AP1000 pressurised water reactor, General Electric simplified boiling water reactor, and General Electric Hitachi economic simplified boiling water reactor. The purpose of the passive containment cooling system is to limit the containment pressure and temperature rise following design-basis accidents. The passive containment cooling system also functions to transfer decay heat to the environment. The passive containment cooling system is designed to mitigate events resulting from ruptures to piping in the primary or secondary system. The system is actuated based upon containment pressure levels.