STUK

GUIDE **YVL 5.5** / 13 SEPTEMBER 2002

INSTRUMENTATION SYSTEMS AND COMPONENTS AT NUCLEAR FACILITIES

continues

This Guide remains in force as of 1 March 2003 until further notice. It replaces Guide YVL 5.5, issued on 7 June 1985.

Third, revised edition
Helsinki 2002
Dark Oy

ISBN 951-712-621-9 (print)
ISBN 951-712-622-0 (pdf)
ISBN 951-712-623-9 (html)
ISSN 0783-2400

STUK • **SÄTEILYTURVAKESKUS**
STRÅLSÄKERHETSCENTRALEN
RADIATION AND NUCLEAR SAFETY AUTHORITY

Osoite/Address • Laippatie 4, 00880 Helsinki
Postiosoite / Postal address • PL / P.O.Box 14, FIN-00881 Helsinki, FINLAND
Puh./Tel. (09) 759 881, +358 9 759 881 • Fax (09) 759 88 500, +358 9 759 88 500 • www.stuk.fi

Authorisation

By virtue of the below acts and regulations, the Radiation and Nuclear Safety Authority (STUK) issues detailed regulations that apply to the safe use of nuclear energy and to physical protection, emergency preparedness and safeguards:

- Section 55, paragraph 2, point 3 of the Nuclear Energy Act (990/1987)
- Section 29 of the Council of State Resolution (395/1991) on the Safety of Nuclear Power Plants
- Section 13 of the Council of State Resolution (396/1991) on the Physical Protection of Nuclear Power Plants
- Section 11 of the Council of State Resolution (397/1991) on the Emergency Preparedness of Nuclear Power Plants
- Section 8 of the Council of State Resolution (398/1991) on the Safety of a Disposal Facility for Reactor Waste
- Section 30 of the Council of State Resolution (478/1999) on the Safety of Disposal of Spent Nuclear Fuel.

Rules for application

The publication of a YVL guide does not, as such, alter any previous decisions made by STUK. After having heard those concerned, STUK makes a separate decision on how a new or revised YVL guide applies to operating nuclear power plants, or to those under construction, and to licensees' operational activities. The guides apply as such to new nuclear facilities.

When considering how new safety requirements presented in YVL guides apply to operating nuclear power plants, or to those under construction, STUK takes into account section 27 of the Council of State Resolution (395/1991), which prescribes that *for further safety enhancement, measures shall be taken which can be regarded as justified considering operating experience and the results of safety research as well as the advancement of science and technology.*

If deviations are made from the requirements of a YVL guide, STUK shall be presented with some other acceptable procedure or solution by which the safety level set forth in the guide is achieved.

Translation. Original text in Finnish.

1 General requirements

The operation of the reactor and the systems at the nuclear power plant is controlled, monitored and protected by the instrumentation and control systems (I & C). The function of the monitoring and information systems is to provide the operators with reliable information on the state of the reactor itself, the systems at the plant or their environment. The instrumentation and control systems are actuated automatically or manually by the operator necessitated as by the plant operation and safety. The protection automation is especially designed to detect departures from acceptable plant conditions and to initiate automatically and maintain the operation of appropriate safety systems as necessary (reactor shutdown, the functioning of the containment building and residual heat removal from the reactor to the ultimate heat sink, etc.).

General safety requirements for nuclear power plants are presented in the Government Resolution (395/1991). In this resolution there are presented general requirements concerning all safety systems and also requirements specific to the instrumentation and control systems of a nuclear power plant. These requirements are presented for detection and control of operational transients and accidents (13 §), ensuring of safety functions (18 §), avoidance of human error (19 §), safety classification (21 §), monitoring and control of a nuclear power plant (22 §). The general requirements are specified in Guide YVL 1.0. Among other things there are requirements concerning protection instrumentation and control, the needed automation degree and possibilities for manual controls.

Requirements for instrumentation and control systems and equipment are presented also in several other YVL guides. Guide YVL 2.0 applies generally to the design and regulatory control of the systems for a nuclear power plant. The requirements related to failure criteria are presented in Guide YVL 2.7. The classification requirements of the instrumentation and control systems are presented in Guide YVL 2.1. In Guides YVL 2.2 and YVL 2.8 are presented requirements for safety goals and their demonstration. Guide YVL 1.8 presents how the Finnish Centre for Radiation and Nuclear Safety regulates modifications, repairs and preventive maintenance of systems, equipment and structures at nuclear facilities during operation. The guide further describes the obligations related to this work imposed on licensees. The general requirements for and regulatory control of nuclear power plant pre-operational and start-up testing are presented in Guide YVL 2.5. Guide YVL 1.1 summarizes STUK's regulatory functions during nuclear power plant design, construction and operation.

According to section 5 of the Government Resolution (395/1991), *advanced quality assurance programmes shall be employed in all activities which affect safety and relate to the design, construction and operation of a nuclear power plant*. General requirements for quality management at a nuclear power plant are presented in Guide YVL 1.4 and the requirements for quality management during operation of nuclear power plants are presented in Guide YVL 1.9. The necessary precondition for assuring the dependability of modern I&C technology is that, in particular the special features of the technology utilized shall be considered in the quality management system.

This guide presents the requirements for licensees concerning the design, implementation and operation of the I&C systems and equipment at a nuclear facility and how STUK controls and inspects these.

2 Design bases of I&C systems and equipment

2.1 Ensuring the safety functions

The protection I&C systems are designed to detect automatically deviations from the normal operation conditions of the nuclear reactor and the systems and to form the signals for initiating and maintaining the required safety functions. The most important safety functions are shut-

down of the reactor, residual heat removal to the ultimate heat sink and functions of the containment. The protection I&C systems encompass all equipment including measurements of the process variables to the actuation devices. The requirements for the protection I&C systems are applied to all I&C systems belonging to systems in Safety Class 2.

According to Guide YVL 1.0, section 3.4, the protection system *shall be so designed that in case of its failure it settles in a state preferable from the plant safety point of view.* So the different failure modes and their causes shall be analysed and the state preferable from the plant safety point of view shall be justified.

According to Guide YVL 1.0, section 3.4, *the protection system which initiates the safety functions shall operate during anticipated operational transients and postulated accidents even in the event of a single failure, although any component affecting a safety function would simultaneously be inoperable due to repair or maintenance. Also the diversity principle shall be complied with in the design of the reactor protection system*.

According to Guide YVL 2.7, chapter 4, *the reactor protection system measures at least two different process parameters which are both physically dependent on a transient or accident and whose trip limits can be so chosen that they are reached early enough. If this is not possible for all protection functions, different measurement principles shall be used in the measuring of the process parameter in question*.

According to Guide YVL 1.0, subsection 3.4, in the first place*, the protection system shall be separated from the control system and other automation systems. Any possible interdependence between the protection, control or other automation systems shall not endanger safety*.

At the main control room the operators shall have reliable information of the status of the protection I&C system.

The functions of the protection I&C systems shall be testable also during the operation of the plant. It shall be ensured by these tests that the design basis functional requirements of the system are met.

The periodic testing of the protection I&C system shall encompass the whole channel including the measurements to the actuation devices themselves. To perform the periodic testing the subsystem shall be set to a state preferable from the plant safety point of view. The possibility for testing shall be incorporated into the system design.

The protection I&C systems shall be designed so that they monitor the validity of the input and output signals and their internal operation and give an alarm signal when needed. The self diagnostics of the protection I&C systems shall be adequate and well tested. The analysis of the coverage of the self diagnostics shall include a separate assessment of hardware and software faults.

According to Guide YVL 2.0 subsystems of the protection system performing the same safety function shall be separated physically. These subsystems shall also be separated functionally. The protection I&C systems shall be functionally separated from other systems and their physical separation from other systems shall be adequate.

Further it is presented in Guide YVL 1.0, subsection 3.4, that *the manual initiation of the protection system shall be implemented using technology as reliable as possible. In addition to the manual initiation of individual devices, it shall also be possible to manually trip protective signals, if necessary*.

The protection I&C systems shall monitor the operating parameters of the plant and display the operators the parameters needed for the manual initiation of the protection signal.

The effects of operator-initiated manual actuations, if needed during different protective tasks,

shall be analysed. Also, where manual actuations are provided, they shall be independent of the equipment of the automatic protection system to the extent practicable. In addition, the manual actuation of the protection signal shall be functionally independent of other systems in the control room.

Probabilistic design goals and numerical goals are presented in Guide YVL 2.8.

2.2 Instrumentation, control and monitoring

Guide YVL 1.0 subsection 3.6 provides that *the plant shall have reliable control systems for keeping the process parameters and systems within the specified operating range. Together with the systems and components they control, these control systems shall ensure that during operational conditions, or in the event of a single failure of the control systems, there will be no need to start safety systems designed for postulated accidents.*

The I&C systems of the plant shall be sufficient for monitoring and control of the reactor and the process systems. The function of these operational control systems is to keep process parameters during operational conditions within the normal operational range of the parameters and to control the condition of the systems and equipment at the plant.

The operational I&C systems shall be designed so that sufficient state and alarm information is available for automatic or operator-assisted actuation of corrective control actions in case the plant parameters depart from the normal operational range.

The alarm limits of the operational I&C systems shall be set such that the mitigation actions like control can be performed and completed so that the limits for the actuation of the safety functions are not reached.

To ensure that a single failure of the operational I&C systems does not change the process parameters so that the limits for the actuation of the reactor safety functions are reached, the operation of the operational I&C systems shall be ensured by milder functions than those of the safety systems.

Guide YVL 1.0, subsection 3.6, provides that *the reactor and other structures, systems and components of the nuclear power plant shall be provided with sufficient instrumentation for monitoring the process parameters and the operation and condition of systems*.

The measurements of the nuclear reactor shall allow precise and reliable enough input data for the calculation of the performance of the reactor and the protection, control and monitoring systems.

At least the following parameters related to the reactor shall be controlled:

- the neutron power and thermal power of the reactor
- the pressure of the reactor
- the water level in the reactor
- the main circulation flow of the reactor
- the temperature at different parts of the primary circuit
- the water level and the pressure of the pressurizer (PWR)
- the flows in and out from the primary circuit
- the water level and pressure of the steam generator (PWR)
- the boron concentration in the primary circuit (PWR)
- the position of the control rods.

In the design of the monitoring of the reactor, the following requirements shall be considered:

- The power distribution in the reactor shall be defined reliably and the thermal margins of the reactor shall be calculated regularly.
- Any incorrect operational conditions of the reactor core shall be able to observe reliably with the aid of reactor instrumentation.
- The reactor shall be monitored by measurements or other means so that any incorrect position of the internals or the fuel can be detected reliably.

- The control of possible loose parts in the process shall be adequate.

According to Guide YVL 1.0 *the measurement systems shall be capable of measuring accurately enough over the entire range within which the measured parameters vary during operational conditions or accidents. As far as possible, the measurements shall be so planned that the operators will easily see if the measurement fails or the measurement range is exceeded*.

Guide YVL 1.0, subsection 3.6, provides *that the control equipment shall be designed to record process parameters indicating plant state and also system control signals so that the plant's operational events can be analysed afterwards*.

2.3 Main control room and man–machine interface

According to paragraph one of section 22 of the Government Resolution (395/1991), *a nuclear power plant's control rooms shall contain equipment which provide information about the plant's operational state and any deviations from normal operation as well as systems which monitor the state of the plant's safety systems during operation and their functioning during operational transients and accidents.*

According to section 19 of the Government Resolution (395/1991), *special attention shall be paid to the avoidance, detection and repair of human errors. The possibility of human errors shall be taken into account both in the design of the nuclear power plant and in the planning of its operation so that the plant withstands well errors and deviations from planned operational actions.*

The functions assigned to the operators and to the automatically actuated tasks shall be designed conducting an analysis of the control functions needed during operational occurrences and accidents so that limitations of human capabilities are considered. During the design of the main control room and its functions the methods provided by control room ergonomics shall be used to minimize human faults in the operation at the control room.

An independent expert assessment of the design of the main control room is included in a good design practice.

The I&C systems at the main control room and the procedures needed to control the nuclear power plant shall be planned as a whole. The functioning of planned systems and procedures shall be verified at the plant simulator. Also changes in the functions of the control room and significant ergonomic changes shall be verified at the plant simulator before making the changes at the control room. The requirements for the plant simulator are presented in Guide YVL 1.6.

According to Guide YVL 1.0 *the control room shall be so designed that the measures necessary to control the plant can be performed there during operational conditions and accidents. The structures and safety systems of the control room shall be so designed that safe working is possible there even during accidents*.

According to Guide 1.0 also *ergonomic principles which apply to control room work and which make possible the reliable performance of control measures shall be considered in the design of the control room, the emergency control post and local control posts. Particular attention shall be paid to the design of control panels, alarm systems and computer-based display systems so that, in the event of a transient or accident, the operators can obtain a good overall picture of the plant state and that data most important for the plant's safety are clearly displayed.*

According to Guide YVL 1.0, *the diversity principle shall be complied with, if possible, in the design of systems which give an overall picture of the plant state and provide data relating to alarms.*

The displays and alarms at the control room shall be designed and implemented so that with the help of these operators get reliable information on any plant occurrences needing operator actions. The alarms shall be prioritized based on the safety significance of the events. The processing and display of alarms of the I&C systems in the control room shall be designed such that

alarms important to safety are noticed as reliably as possible.

The hierarchy of the displays shall be logical and the process information needed shall be easily available. In addition, a logical marking system shall be used when displaying the information of the process systems.

The control room is an essential premise at the nuclear power plant encompassing systems and equipment belonging to different safety classes as well as non-classified systems. In the design of the control room, the physical and functional separation between and/or within redundant safety systems and systems and equipment belonging to different safety classes shall be considered.

The electrical power supply of the I&C systems in the control room shall be ensured according to Guide YVL 5.2.

The requirements of fire protection, protection against flooding, lighting, air conditioning, noise reduction, radiation protection and access control shall be considered in the design of the control room.

2.4 Emergency control posts and local control systems

According to paragraph 3, section 22, of the Government Resolution (395/1991*), there shall be an emergency control post at a nuclear power plant which is independent of the control room and the necessary local control systems by the means of which the nuclear reactor can be shut down and cooled and residual heat from the nuclear reactor and spent fuel stored at the plant can be removed.*

According to Guide 1.*0 the emergency control post shall be so designed that the reactor can be shut down from there and the plant can be brought to a stable shutdown state.* The shutdown of the reactor and the actuation and maintaining of the functions needed for residual heat removal shall be possible from the emergency control post. The emergency control post can be located in one room or in multiple rooms. In addition, adequate facilities for communication shall be ensured.

The plant shall be designed such that it is possible to move safely and fast enough from the main control room to the emergency control post.

According to Guide YVL 1.0 *the control systems of the emergency control post outside the control room shall be separated from the control systems of the control room in such a way that if the equipment in one fire compartment are entirely destroyed by fire this does not harm both control systems so much that safety functions could not be carried out.*

The main control room and the emergency control post shall be independent. This independence shall be carried out using physical segregation and functional independence. The nuclear power plant shall be designed such that the main control room and the emergency control post are located in different fire departments. The functional separation of the main control room and the emergency control post shall be such that they are separated electrically. The design of the nuclear power plant shall be such that the nuclear reactor and the removal of residual heat can be controlled only from the main control room or the emergency control post at a time.

The functions located at the emergency control post and the adequacy of the status information of the plant systems shall be analysed in different situations needing control in case the plant can not be controlled and monitored from the main control room. The applicability of the solutions chosen shall be examined under various circumstances which make the use of the control room impossible.

2.5 Accident instrumentation

2.5.1 General requirements

According to Guide YVL 1.0 *for the purpose of accident monitoring and management, appropri-*

ate measuring and monitoring instrumentation shall be designed for the plant by which the operating personnel obtains sufficient data for event assessment and for the planning and implementation of countermeasures.

The measuring and monitoring systems for accident monitoring and management shall operate also in the case of a single failure.

Information on postulated accidents shall be available for the operators in the main control room. The measurements belonging to the accident instrumentation shall be identifiable at the main control room so that the main control room personnel can easily distinguish them from other measurements.

In the case of an accident the process information shall be recorded so that the data can be analysed afterwards.

The requirements for the environmental qualification of equipment belonging to the accident instrumentation and the severe accident instrumentation are presented in subsection 3.1.

2.5.2 Postulated accidents

At least the following types of measurements shall be included in the instrumentation for the monitoring and management of postulated accidents:

- measurements used in a later phase for manual actuation of safety functions needed which have not been actuated automatically
- measurements to ensure completion of safety functions by the control room personnel
- measurements giving information about the operation of individual safety systems and associated equipment
- measurements to monitor the integrity of multiple, subsequent technical barriers for preventing radioactive releases
- measurements to estimate radioactive releases.

The number of measurements shall be sufficient to facilitate observation of changes in local circumstances, e.g. inside the containment, that have a bearing on accident management.

2.5.3 The accident management support function

According to paragraph 3, section 13, of the Government Resolution (395/1991) *effective technical and administrative measures shall be taken for the mitigation of the consequences of an accident. Counter-measures for bringing an accident under control and for preventing radiation hazards shall be planned in advance (mitigation of consequences).*

The nuclear power plant shall be designed so that, to help the operators in accident management, there shall be a support function in addition to the other alarm information at the main control room. This support function is for monitoring and displaying the status information of the needed safety functions. It shall be implemented using an independent function, a so called accident management support function. The information shall be displayed in such form that the operators can easily define the status of the plant. The information shall be separated from other information at the control room by different means of displaying the information. The accident management support function shall be available during all operational conditions of the plant and during postulated accidents.

The corresponding support function shall be available also for the shutdown state of the plant.

2.5.4 Severe accident

For the management and monitoring of a severe accident the nuclear power plant shall be equipped with the monitoring instrumentation required by Guide YVL 1.0 subsection 3.6.

The design of the monitoring instrumentation for severe accidents shall fulfil the following requirements:

- The measuring methods chosen shall be suitable for monitoring severe accidents.

- The instrumentation shall be independent from all the other instrumentation at the plant.
- The power supply of the instrumentation (electricity, compressed air, etc.) shall be independent from all other power supplies of the plant.

The requirements apply also to control actions possibly needed during a severe reactor accident.

3 General design requirements

3.1 Qualification to environmental conditions

Environmental conditions and stresses of I&C systems and equipment of a nuclear power plant shall be specified for all planned operational conditions and for storage and transportation. The equipment shall be designed such that their functional performance will be maintained in accordance with the specified requirements throughout their planned service lifetime. The safety classified equipment shall be qualified to the planned environmental conditions and stresses through tests prescribed by standards. The tests shall correspond to the most unfavorable, potential local operational conditions.

The structure and materials of automation equipment needed in accidents shall be selected such that the functional performance of the equipment in accidents will be maintained throughout their planned service lifetime, in accordance with the specified requirements.

The influence of environmental conditions and stresses and internal process conditions in postulated accidents shall be accounted for in the design of measurements that use other than electrical signals, such as hydraulic and mechanical signals. An example of such signals occurs in measurements using impulse pipes.

The type tests of equipment needed during or after postulated accident situations shall form a uniform series of tests in which the same test samples are subjected to anticipated environmental stresses of the design basis of the application. Prior to the tests corresponding with the accident conditions, the test samples shall undergo artificial ageing equivalent to the planned service lifetime.

Artificial ageing of the equipment shall be carried out such that it with adequate confidence corresponds to real ageing. The ageing is usually carried out so that the equipment first undergoes thermally induced ageing and then radiation-induced ageing. After this, a mechanical load test is performed for the equipment, and finally the afore-described tests corresponding to the postulated accidents are performed.

A test of the postulated accidents shall include exposures to radiation and stresses caused by temperature, pressure and humidity corresponding to accident conditions, as well as rapid changes in conditions. The composition of water used in the tests, eg. spraying the components, must correspond to that of the water occurring in accident conditions. If the equipment may be submerged in water in a postulated accident and if it needs to function also under such conditions, functional performance shall be demonstrated also for such a situation. The tests shall be designed such that they demonstrate, with a sufficient confidence, the functional performance of the device under accident conditions throughout the planned service lifetime of the equipment.

Seismic tests and analyses shall be performed in accordance with Guide YVL 2.6.

If an automation device is to function in severe reactor accidents it shall be qualified for this purpose by using suitable methods. The maintenance of the functional performance of automation devices located in the reactor containment during hydrogen fires shall be demonstrated if the equipment needs to operate in accident situ-

ations in which the occurrence of hydrogen fires is possible.

3.2 Electromagnetic compatibility

I&C systems and equipment in a nuclear power plant shall be reliably protected against the effects of electrical and magnetic interference fields, mains interference, radio induced interference and disturbances caused by telecommunication.

I&C equipment shall be designed and installed in such a way that they themselves do not cause any harmful electromagnetic interference in their operational environment.

In accordance with section 2.1 of Guide YVL 5.2, *earthing systems and lightning protection systems shall be designed to effectively protect people, buildings, equipment as well as electrical and I&C systems against overvoltages, overcurrents and any other possible electromagnetic interference due to climatic factors.*

Also other sources of disturbances caused by nature and man shall be considered. The methods and technical solutions used for adequate protection of I&C systems at the nuclear power plant against electromagnetic disturbances shall be justified.

3.3 Fire analyses

Guide YVL 4.3 presents requirements for the design and implementation of fire protection at nuclear power plants, as well as the fire protection related documentation to be submitted to STUK. In accordance with section 3.8 of Guide YVL 4.3, *fire hazards analyses shall always be performed for the containment and the control room. By means of the fire hazard analysis of the control room it shall be demonstrated that the control of the necessary safety functions can be accomplished in the event of a fire in the control room or in any other fire compartment.* In this context, also the influence of fires on the cables of I&C systems shall be examined, including the way in which the subsequent disturbances and faults are reflected in the implementation of protection and control functions.

The analyses shall examine such fire situations that may affect the I&C systems and equipment in the form of heat, smoke or other fire induced effects or fire fighting measures and substances.

The potential failure modes of systems, equipment and cables, as caused by elevated temperatures, smoke and fire fighting measures, shall be identified. Their influence on the passing trough and correctness of control signals shall be examined. Failure modes affecting protection functions shall be identified. The risk of a fault or a disturbance spreading through power supplies or the data transmission network, shall be evaluated. The analysis shall examine the availability and correctness of plant status information in the control room and the emergency control post as well as the options for operator action to ensure plant safety functions in different disturbance and fault situations caused by fires.

The analysis shall examine uncertainties associated with the most essential factors.

3.4 Information security

In the design, operation and maintenance of the I&C system attention shall be paid to security issues. Unauthorized access to equipment, software or information systems important to the disturbance free plant operation shall be prevented. Unauthorized access to equipment of systems important to safety shall be prevented by using physical, technical and administrative security measures. The installation of unauthorized parts of software during design, manufacturing, commissioning, periodic testing and maintenance shall be reliably prevented. Authorized accesses to a system, and any modifications made during such accesses, shall be traceable.

3.5 Other requirements

In accordance to section 2.5.3 of Guide YVL 2.0, *subsystems performing the same safety function,*

whether they be similar or diverse to each other, shall be physically separated such that the potential occurrence of a common cause failure due to external influences is very unlikely (separation principle). The I&C systems of the subsystems shall be physically and functionally separated.

In accordance to section 2.7 of Guide YVL 2.0, *when a system connects to another system their interfaces shall be defined and designed such that the connection between the systems does not endanger the operation of systems carrying out a safety function. In addition, the interfaces of a safety system and its support systems shall be designed such, if possible, that the failure of the interfaces does not endanger the system's own, or any other system's, safety function, and so as to prevent failure propagation across interfaces.* It shall be ensured in the design that a function or a fault of an I&C system or equipment belonging to a lower safety class does not cause a failure of a function of an I&C system belonging to a higher safety class.

Data communication inside and between I&C systems shall be designed such that errors in data communication do not cause faulty functions or prevent the functioning of safety functions. The data communication system shall fulfill the response time requirements during normal plant operation, operational disturbances, and accidents. This shall be demonstrated for Safety Class 2 and 3 I&C systems in all their potential load situations.

In accordance with section 3.13 of Guide YVL 1.0, *a clear marking system shall be planned to identify components.* In order to make it easier to identify equipment and to avoid human errors, the equipment and cables of plant I&C systems shall be equipped with labeling of durable material that can be easily read during inspection, maintenance and troubleshooting.

Versions of software and hardware shall be equipped with unambiguous identifications in order to facilitate version management of programmable systems and to avoid human errors. The licensee shall have implemented appropriate configuration and version management procedures that cover different systems, their hardware and software.

In the design of user interfaces for systems and equipment attention shall be paid to human factors.

A particular justification shall be provided for a need to use wireless controls. A device or a system comprising wireless control shall be designed such that the control action is possible only through a connection signal designed for the control and that the system or the device goes quickly enough in a state preferable from the safety point of view in case the control signal breaks off.

Guide YVL 5.2 presents requirements for the power supplies of I&C systems and equipment.

4 Design and implementation of I&C systems

4.1 General requirements

In the design of I&C systems and equipment in nuclear power plants, the principle of prevention shall be employed, according to which *in design, construction and operation proven or otherwise carefully examined high quality technology shall be employed to prevent operational transients and accidents* [Government Resolution (395/1991), section 13 , 1st paragraph].

Guide YVL 2.0 presents general requirements for the organization designing nuclear power plant systems and equipment, for the independent assessment, as well as the deterministic and probabilistic principles to be used in the design.

The general principle is that applicable nuclear guidelines and standards are used in the design and implementation of safety classified I&C systems. Standards and guidelines intended for nuclear engineering applications as well as qual-

ity management measures that comply with them are used in the design and implementation of Safety Class 2 equipment. In the design of Safety Class 3 and 4 equipment applicable standards are used as well as quality management measures that are in compliance with them.

The standards used in design and implementation shall be specified and their applicability justified. Potential deviations from the specified standards shall be evaluated and justified for I&C systems and equipment belonging to Safety Class 2 or 3.

The requirements for specification, design, implementation, maintenance and quality management of I&C systems and equipment shall be commensurate with their safety class and safety significance. Also the reliability requirements of the design basis functions shall be accounted for when specifying requirements for the design, implementation and qualification of I&C systems and equipment.

In accordance with Guide YVL 1.4, the licensee has an overall responsibility that the regulations in force and the requirements in YVL Guides are taken into account in the quality management systems of different organizations. The licensee has the main responsibility to ensure that the specified quality requirements are followed and that a sufficient quality level is achieved. It shall be ensured that the quality requirements are appropriately conveyed to the organizations and their subsuppliers responsible for the design, manufacturing and maintenance of I&C systems and equipment.

4.2 Quality management

4.2.1 General requirements

In accordance with the Government Resolution (395/1991), section 21, 2nd paragraph, *the systems, structures and components important to safety shall be designed, manufactured, installed and operated so that their quality level and the inspections and tests required to verify their quality level are adequate considering any item's safety significance.* Quality management procedures of the licensee shall be used to ensure this. They shall describe the systematic procedures used during design, construction and operational activities of a nuclear power plant, as affecting the quality.

Advanced design, manufacturing and change management methods, taking into account the specific features of the technology being applied, shall be utilized in the design, manufacturing, installation, operation and maintenance of I&C systems and equipment of nuclear power plants. High-standard quality management is essential in the qualification of programmable systems, in particular. Quality management measures ensure that the structure and features of the product batches procured to the plant are in accordance with those of the products that have been qualified.

4.2.2 Quality management system

Concerning the construction and operational phases of a nuclear power plant, general quality management requirements shall be specified for I&C systems and equipment, taking into account the safety importance of the item. Quality management during construction shall cover the quality management of the various parties engaged in design, manufacturing, receiving, installation and commissioning. The quality management of operating plants shall cover corresponding measures as well as the operation, maintenance and modification design of existing systems and equipment. It shall be applied to all the parties involved.

The quality management system used during operation shall include, among other things, procedures for periodic maintenance and tests, evaluation of the test results, repairs and modifications, version management, replacement with spare parts, urgent repairs, and ensuring and maintaining the accuracy of measuring equipment. In addition, the quality management system shall describe the procedures for ensuring that the quality of I&C equipment needed in operational and accident situations is maintained throughout the service lifetime of the plant.

In addition to the general quality management requirements, quality assurance plans shall be prepared. They shall include detailed instructions for the procurement, manufacturing, receiving, installation, commissioning and maintenance phases.

The design, implementation and modification projects of I&C systems shall be facilitated by a separate quality plan, in accordance with subsection 4.2.3.

4.2.3 Quality management of the design and implementation of an I&C system

A quality plan specifying the quality management measures to be used shall be drawn up for the design and implementation of an I&C system. The quality plan shall cover the design, implementation and commissioning of the system as a whole. The quality plan shall be prepared in accordance with an applicable standard. The quality plan shall ensure that potential errors are detected, that adequate measures are taken to correct them, and that the quality management requirements imposed by the licensee are fulfilled in the procurement.

The quality plan shall describe the interfaces of organizations participating in design, interface management, responsibilities for project quality functions in the various organizations involved, as well as the control of subsuppliers. The quality plan shall describe the measures used to ensure the correctness and completion of documentation at the end of each phase of the project. Furthermore, the plan shall specify the version and change management measures to be used in the design and implementation of the system, as well as the procedures used to revise the quality plan.

The quality plan shall specify an appropriate review procedure for intermediate results, where the licensee evaluates the design process of the supplier, in particular. The objective of the reviews is to eliminate design errors as early as possible and to ensure that the design basis, safety, operational and maintenance requirements are taken into account as well as to ensure the correctness of technical implementation and the timely progress of the qualification process. Reviews concerning the design of the system shall cover the system and equipment qualification described in section 4.4.

The quality plan of a Safety Class 2 I&C system shall include an assessment that is independent from design and implementation and assesses compliance with the quality plan and the adequacy of the measures taken to correct any revealed deficiencies. Those making the assessment shall have competence in the quality management of safety applications and in the technology in question. These competences shall have been proven in practice and be relevant to the specific assessment to be performed.

Suppliers of I&C systems and equipment belonging to Safety Class 2 or 3 shall employ a quality management system in compliance with an appropriate standard and that system has been independently assessed.

The licensee shall specify the procedures used to evaluate, select and control the suppliers of I&C systems and equipment. Before design and implementation is started, it shall be confirmed that the organizations involved fulfill the prerequisites for high quality work.

4.3 Design process

4.3.1 General requirements

Simplicity, fault tolerance, and a timely detection of potential failures shall be aimed at in the design of an I&C system for the nuclear power plant. Design and implementation shall utilize fault avoiding and revealing methods.

The I&C systems and equipment of a nuclear power plant shall be designed and documented such that, during the different phases of the design process, it can be ensured that the specified requirements are transferred correctly into the system to be commissioned. The first phase of this so-called life cycle model is the requirement specification. The different phases of the design process shall be described in the qualification plan (section 4.4).

The inputs and the results of each phase shall be documented such that they can be assessed by a person who is independent from the supplier, the licensee, and the design. Each design phase of a Safety Class 2 system shall be verified against the requirements specified by the preceding phase. The design process as a whole shall be transparent and verifiable. A design process consisting of different phases has been described in many guidelines and standards, such as the IAEA guidelines and the IEC standards referenced in this guide.

4.3.2 Requirement specification

The requirement specification of the I&C systems or equipment of a nuclear power plant shall include all significant functional, performance and reliability requirements. In addition, it shall describe other requirements affecting system design such as environmental conditions and stresses as well as requirements concerning interfaces, periodic testing, maintenance, information security and lifetime. Requirements that are important to safety shall be consistent with the assumptions made in the safety analysis of the plant. The man machine interfaces of a system, and the interfaces to the other systems of the plant, shall be clearly specified.

The requirement specification shall be made more precise when the design proceeds to subsequent phases. The final requirement specification of systems, equipment, hardware and software shall be sufficiently detailed and comprehensive, such that implementation can be tested or verified against corresponding requirements. The requirements shall be consistent and unambiguous. The fulfillment of the requirements shall be verifiable. The requirement specification shall be maintained throughout the whole design, manufacturing and operational life cycle of the system.

The plant specific requirement specifications of I&C systems and equipment belonging to Safety Class 2 or 3, shall be sufficiently detailed for the system validation, as well as for the suitability analysis that is performed in accordance with section 4.4.7 for the equipment selected to the system.

The correctness, completeness and consistency of the requirement specification of a Safety Class 2 system shall be independently assessed. The assessment report shall present the observations made, and a justified conclusion.

4.3.3 Documentation

In the beginning of the design process of I&C systems or equipment, the documentation requirements and the documentation management procedures, which are applied since the start of the project, shall be specified. In the principal design phase, a clear and precise presentation method, understandable to experts in different fields, shall be used for functional specification of the system. The use of functional block diagrams or corresponding design presentation methods belongs to a good design practice.

The documentation describing the system shall be structurally clear and comprehensive. The information included in the documentation shall be up-to-date and sufficient to support the verification and validation of the system.

The documentation of I&C systems and equipment shall be updated in connection with modifications. Guide YVL 1.4 presents requirements for the documentation management part of the quality management system of the licensee.

4.3.4 Change management during the design process

An appropriate change management procedure, which is applied throughout the whole design process, shall be specified in the beginning of the design process of I&C systems or equipment.

4.4 Qualification plan

4.4.1 General requirements

The systems and equipment at a nuclear facility shall be qualified to their intended use. The licensee shall draw up a special qualification plan to demonstrate the suitability of Safety Class 2 and 3 I&C systems and equipment for their intended use. The qualification plan shall

include material from four areas: design and manufacturing process, tests, analyses, and operating experiences. If there is little qualification material in one subarea, the lack of it shall be compensated for with additional material from another subarea. The qualification plan shall describe the suitability analyses to be performed. The reports of previous type test approvals of systems or equipment shall be attached to the qualification plan in case they are to be utilized in the demonstration of the qualifications.

Independent expert assessment is used as part of the qualification of a Safety Class 2 system. Plans shall be drawn up for the independent verifications and validations to be performed. The scope, criteria and mechanisms of the independent assessment, the observations of the assessment and a justified conclusion shall be presented in the assessment report.

The licensee shall evaluate and present a justified conclusion on the acceptability of the qualification results.

The qualification plan shall be updated if the requirement specification of the system is changed such that this affects the qualification, or if essential new information has been obtained about the system and this information may be considered to affect the qualification plan.

4.4.2 Design and manufacturing process

The qualification plan shall describe the phases of the system design and manufacturing process, as well as the verification made after each phase and validation.

Those performing the verifications and validation shall be technical experts of the design organization, independent of the design or implementation of the system and piece of equipment. They shall verify that each work phase fulfills the requirements specified by the preceding phase. Verification shall be performed for all design and manufacturing phases of a Safety Class 2 I&C system, and for all essential phases of a Safety Class 3 I&C system, up until the final product. The final product shall be validated against the requirements of the product. The verification and validation plans, and the results, shall be documented such that they can be evaluated by an external party if necessary.

4.4.3 Tests

Tests can be divided into tests performed during the design and manufacturing process and tests performed for the implemented I&C systems and equipment. The equipment consists of field equipment and I&C equipment.

Tests performed during the design and manufacturing process include, among other things, unit tests, integration tests and system tests. The tests performed for software can be divided into static and dynamic tests. The purpose of the tests performed during design and manufacturing is to ensure that the I&C systems or equipment fulfill the functional and performance requirements specified for them. These tests are completed by factory tests. Statistical testing may be used to support reliability considerations, in particular.

A test plan shall be drawn up for the tests to be performed for an I&C system and its equipment. Test experts, who are independent from design and manufacturing, shall perform the tests in accordance with the test plan. The test plan, acceptance criteria and results shall be documented such that they can be independently assessed.

With the testing and analyses it shall also be ensured that there are no unintentional functions in the system or its equipment that could be detrimental for safety.

The adequacy of tests performed for a Safety Class 2 system shall be justified and the test coverage analyzed against the requirements specified for the system.

The compliance with requirements and the fault-freeness of an I&C system or piece of equipment shall be evaluated after the factory tests in order

to ensure that the system or the piece of equipment may be transported to the plant site. The project time schedule shall be designed such that the potential design modifications needed after the factory tests can be made in accordance with procedures commensurate with the safety importance of I&C systems or equipment.

Tests required for the equipment of an implemented system are typically type tests and environmental tests, which are performed taking into account the application (system and plant environment). Acceptance tests and commissioning tests, among other things, are performed for the implemented system at the plant.

The final testing shall demonstrate that the I&C system or equipment fulfill the functional and performance requirements specified for it. The testing can be partially based on simulation. The final testing shall, however, be performed in the final operational environment.

Guide YVL 2.5 presents requirements for the system commissioning tests to be performed at the plant.

Specific requirements for programmable systems and equipment are given in section 4.6.5.

4.4.4 Analyses related to safety

The fulfillment of the functional and performance requirements shall be demonstrated as part of the system and equipment qualification, including the analyses needed for this.

Safety Class 2 systems shall be subjected to a failure mode and effects analysis, a common cause failure analysis, an operating experience analysis, and a quantitative reliability analysis.

Safety Class 3 I&C systems shall be subjected to a failure mode and effects analysis, a common cause failure analysis and an operating experience analyses, and, depending on the safety significance, a quantitative reliability analysis.

Safety Class 2 and 3 systems shall be subjected to a safety assessment, which demonstrates fulfillment of the safety requirements. Plant specific PSA shall be updated to correspond to the modified system.

Specific requirements for programmable systems and equipment are given in section 4.6.

4.4.5 Operating experiences

Former operating experiences shall be analyzed for I&C systems belonging to Safety Class 2 or 3, for Safety Class 2 equipment, and for equipment belonging to essential accident instrumentation in Safety Class 3. The operating experiences shall be collected with a well specified method. The comprehensiveness of the collection process and its significance for the reliability of the data shall be evaluated. The operating experiences shall be representative for the application under consideration. The collection time period shall be long enough. The use of operating experiences from other hardware or software versions, setups and operational profiles, for the qualification of a system or equipment, shall be justified.

4.4.6 Type approval

All equipment in Safety Class 2 and essential accident instrumentation in Safety Class 3 (NRC Regulatory Guide 1.97, cat. 1) shall possess a type acceptance certificate according to an applicable nuclear engineering standard awarded by an accredited body or a body performing inspections with corresponding competence. The certificate shall cover the assessment of the equipment design and the quality management of its manufacturing. The equipment conformity to the requirements shall be demonstrated by tests and analyses and by practical type tests.

The assessment of the quality management shall include the inspection of the equipment manufacturing documents and the evaluation of the manufacturing process. The assessors shall have a competence proven in practice in the evaluation of quality control systems and in the assessment of the conformity with technical requirements of the equipment used in safety applications. Special attention in the evaluation of the quality management shall be paid on measures

used to assure that serial production equipment correspond to inspected equipment.

The certification report shall present the observations made in the inspection, the justification for the acceptability of the product and the terms of the validity of the acceptance.

The certificate of a piece of computer-based equipment shall cover the evaluation of both software and hardware. Additional requirements for the software are presented in subsection 4.6.

4.4.7 Suitability analysis

A suitability analysis shall be performed to all Safety Class 2 and 3 equipment. In the analysis the functional and performance capabilities of the piece of equipment shall be assessed against the requirements specified for it as a part of the I&C system. In particular, one shall examine environmental tests, software evaluation, equipment operating experiences, and the reliability of the functioning of the piece of equipment in relation to its safety importance.

In the suitability analysis it shall be presented how the supplier fulfills the prerequisites for product delivery as per section 4.2.

The suitability analysis shall be performed in accordance with an instruction belonging to the quality management system of the licensee.

4.5 Installation and commissioning

A receiving inspection shall be made to equipment and software belonging to Safety Class 2, 3 or 4. In the receiving inspections, the licensee shall ensure that the I&C equipment correspond to the design plans and that the results of their quality control are acceptable. Furthermore, it shall be ensured that the equipment has not been damaged during transport. Potential tests belonging to the receiving inspection shall be performed with acceptable results. The receiving inspection shall be appropriately documented.

The licensee shall perform an installation inspection on installed equipment belonging to Safety Class 2, 3 or 4. In the inspection, the licensee shall ensure that the receiving inspection has been acceptably performed and that the installation is appropriate. An installation time schedule shall be specified for the installations. Also the procedures used in documenting the installations as well as the scope of installation and connection inspections and of functional tests shall be specified.

The licensee shall perform a commissioning inspection on installed or modified systems belonging to Safety Class 2, 3 or 4. It verifies that the installed system is in accordance with the accepted design documents and that this has been ensured by sufficient inspections and tests. It shall also be verified that any deficiencies and faults identified in the inspections have been corrected. The commissioning inspection shall also ensure that potential changes made in the commissioning phase have been implemented according to procedures specified for change management.

The commissioning inspections shall deal with, and make a collected summary of, the fulfillment of quality management by the licensee and ensure that there are no obstacles for the commissioning. The commissioning inspection shall ensure that the installation place and environment of the equipment and systems are consistent with the requirements specified. The installation inspections and functional tests shall have been acceptably performed and there shall be no such deficiencies in the commissioning result documentation and the protocols related to commissioning as would form obstacles to commissioning. The completion of instructions related to the system shall be ensured. The commissioning inspection shall also ensure that any remarks made by STUK during earlier regulatory measures have been appropriately taken care of.

Procedures used during the receiving, installation and commissioning of I&C systems and equipment shall be presented in the quality management system of the licensee. They shall describe the duties of the organizations responsible for a specific measure, the division of work, the responsibilities, and the procedures used for

documentation and the scope of inspections to be made.

The organization unit responsible of the commissioning inspections shall fulfill applicable requirements concerning inspection bodies presented in Guide YVL 1.3.

4.6 Specific requirements for computer-based systems and equipment

4.6.1 Qualification of the platform and the application

The qualification plan for a computer-based system shall include the qualification of both the platform and the application. Section 4.4.6 presents general requirements for type approvals. These requirements apply also to platform. It shall be considered whether platform and equipment belonging to Safety Class 3, but requiring no type approval according to section 4.4.6, should be subjected to a software evaluation against a suitable standard. This consideration shall be based on the reliability target set for the system or the piece of equipment. The evaluation report shall present the observations made in the inspection, the need for potential corrective measures, and a justified decision on the acceptability of the software for the intended purpose.

The factors used to demonstrate the reliability of a computer-based system are especially a high-standard design process of the platform and the application, the competence of the personnel participating in the design and implementation, as well as the use of standards applicable to software production. Various independent inspections and assessments of compliance with the requirements, as well as applicable tools, are essential parts of a high-standard software design process.

4.6.2 Software tools and design methods

The qualification plan shall identify all software tools, as well as test and design methods, used in the design and implementation of systems and equipment belonging to Safety Class 2 or 3. The tools include for example translators, code generators, analyzers, etc.

The operating experiences of software tools that are used in the design and implementation of Safety Class 2 systems and equipment, shall have been collected and documented in a comprehensive and systematic manner. The design and implementation of Safety Class 3 systems and equipment shall utilize standard software tools, whose version management, maintenance and fault data collection are appropriately documented. Standard software tools shall be used in the design and implementation of Safety Class 4 systems.

Version management, maintenance and modification design of those tools that are used for configuration or object code generation shall be implemented with procedures in accordance with the safety importance of system or equipment.

The influence of a potential tool-induced error on safety shall be accounted for when specifying qualification measures for software tools.

In the potential case of software tool error the procedures used to ensure the reliable functioning of systems installed at the plant shall be documented.

Proven, high-standard tools and test methods shall be used in the design and implementation of software belonging to Safety Class 2 or 3. The tools used for designing and implementing Safety Class 2 software shall be qualified to their intended use.

4.6.3 Pre-existing software and equipment

Pre-existing software is subject to the same requirements as software to be developed. Any potential deficiencies in the documentation and implementation of the design process may be substituted for by analyses and testing. Such compensating measures are evaluated by taking into account requirements corresponding to safety class and safety significance.

Software structure, functions, and functions to be left out shall be analysed for the suitability analysis of pre-existing software.

Documentation of the software and the system shall be comprehensive enough to manage the versions of a piece of equipment or software in accordance with procedures corresponding to the safety importance of the piece of equipment or the software.

4.6.4 Prevention and analysis of common cause failures

Software faults are typically caused by design errors. This means that the same failure mode may surface simultaneously in redundant parts of the system. The risk of a common cause failure related to design errors shall be brought to a low enough level by using the diversity principle and other possible means to ensure a sufficiently high reliability of the system function. The measures taken to avoid a common cause failure shall be documented and justified and presented as part of the analyses required by Guide YVL 2.7.

4.6.5 Testing of a computer-based system or equipment

The test plan and procedures used for a system or a piece of equipment belonging to the safety classes shall be sufficient, taking into account the safety importance and reliability target of system or piece of equipment. Software shall be tested also in the equipment setup to be installed.

The final testing of a system belonging to Safety Class 2 or 3 shall cover all system functions and timings, and, as far as practically possible, self diagnostic functions.

Static and dynamic tests shall be used to test software modules. The test cases shall include, among other things, transient situations used in transient and accident analyses.

The coverage of tests for Safety Class 2 systems and equipment in the various test phases shall be analyzed. The selection and amount of final tests performed for Safety Class 2 systems and equipment shall be justified.

4.6.6 Other requirements for a computer-based system or equipment

The publication “Common position of European nuclear regulators for the licensing of safety critical software for nuclear reactors”, (European Commission’s Advisory Expert Group, Nuclear Regulators Working Group, 2000) presents in detail some differences between the requirements in different safety categories concerning design, implementation and maintenance of software. The requirements of this publication shall be taken into account, when applicable, in the design of I&C systems and equipment.

The design of Safety Class 2 systems and equipment shall aim at simplicity. The structure of a system shall minimize the spreading of the influence of a single software error, and make it possible to verify the requirements specified for the system. The execution cycles of software shall be specified. Those software parts that are unnecessary for functional performance are to be identified and their safety significance shall be analyzed and taken account of in the design of the system.

The failure modes of the software shall be identified and analyzed to a sufficient detail.

Programmable systems and equipment shall be designed with self diagnostic functions that are commensurate with the safety importance of the system.

The coverage of failures by self diagnostic functions and periodic tests shall be analyzed for programmable I&C systems and equipment in Safety Class 2. Also the influence of potential failures in self diagnostic functions on the functioning of the protection I&C, shall be analyzed.

The traceability of requirements in the different design phases of a computer-based system in Safety Class 2 shall be demonstrated as part of the qualification of the system.

5 Ageing management

According to subsection 3.15 of Guide YVL 1.0 *in nuclear power plant design, the service life and the effect of ageing on the safety of all safety significant structures, components and materials shall be assessed using sufficient safety margins. Furthermore, provision shall be made for the surveillance of their ageing and, if necessary, their replacement or repair.*

According to subsection 2.2 of Guide YVL 2.0 *during design, when choosing basic technologies, the life cycles of technologies and components shall be considered and any restrictions resulting thereof anticipated. As great an independence as possible from any single technology shall be aimed at in the design solutions. Also component replacements and potential technological turning points shall be considered in advance so that any modifications required at the plant can be designed controllably and in good time.*

An ageing management programme shall be established to monitor the residual lifetime of the systems and equipment at the plant or the need for replacement. The different ageing mechanisms related to various components and their significance shall be considered when planning the programme. The programme shall cover the methods for collecting and analysing the failure data of the systems and equipment to detect possible changes in the failure rates to anticipate the need for replacement. The programme shall cover also other possible analysis and testing made for the assessment of the ageing of the systems and equipment. Also failure data from other plants and vendors shall be made use of, to the extent possible, in ageing management. The ageing management programme shall include all systems and equipment important to safety, regardless of their safety class. The choice of systems and equipment to the programme shall be justified in the programme. Specific attention is to be paid to the condition of equipment needed in accidents as well as the condition of their cables and installations. The requirements of the ageing management of cables is presented in Guide YVL 5.2. The scope and efficiency of the ageing management programme shall be assessed requlary.

The ageing management programme of the I&C systems and equipment of the nuclear power plant shall also consider the ageing of the technology of systems and equipment and the possible need for remedial actions.

The results of ageing management shall be presented in a yearly report. In addition to the results of the fault history analysis of monitored objects and the results of possible other analyses, any repair measures required as well as development plans with their schedules shall be given.

6 Control by the Finnish Radiation and Nuclear Safety Authority

6.1 General regulatory principles

General requirements applicable to the preliminary inspection of systems are given in Guide YVL 2.0. The guide prescribes that systems approval is to be carried out as part of the review of the preliminary and final safety analysis reports.

During the operation of a nuclear power plant, when a system is modified or added, its preliminary inspection is conducted according to a separate conceptual design documents for the modification and on the basis of pre-inspection documents. According to the general principle applied in the regulation of instrumentation and control systems at nuclear power plants, the conceptual design documents and system-specific pre-inspection documents of Safety Class 2 and 3 systems, as well as those of systems whose inspection is separately required by a STUK decision, shall be sent to STUK for approval. The pre-inspection documents of Safety Class 4 systems shall be sent to STUK for information.

According to subsection 3.4.1 of Guide YVL 2.0 the contents of the documentation submitted

can vary according to the safety significance to safety and the scope of modification.

Any changes required to the final safety analysis report after a modification shall be made without delay. Modifications are dealt with in Guide YVL 1.8.

A suitability analysis of Safety Class 2 I&C equipment and essential Safety Class 3 accident instrumentation equipment shall be sent to STUK for approval. Corresponding analysis of other Safety Class 3 equipment are to be sent to STUK for information.

YVL guides that apply to mechanical components, as well as to their pre-inspections and structural inspections, place requirements on those automation equipment whose mechanical properties have safety-significance, e.g. pressure-bearing equipment.

6.2 Conceptual design plan

The contents of a conceptual design documents for Safety Class 2 and 3 I&C equipment mainly correspond to those of the preliminary safety analysis report. The plan shall contain the descriptions below:

- system design principles and bases
- system functions, operating principles, essential design parameters and the assignment of functions to equipment
- a description of a system's importance in the accomplishment of a safety function proper if the system supports a system performing a safety function
- the separation principles of a system and its components (compartments, shielding) and their preliminary location at the plant, as per subsection 3.3 of Guide YVL 4.3
- preliminary safety classification of system functions and equipment
- the environmental conditions and stresses of the system and the consequent design requirements
- requirements and dependencies arising from other systems including auxiliary systems, support systems and the process controlled by the system
- system interfaces, including man machine interface and interfaces with other I&C systems
- a description of the principles of quality management and of the competence of organisations contributing to system design
- preliminary qualification plan
- designer's preliminary safety assessment
- licencee's own safety assessment in accordance with subsection 2.3 of Guide YVL 2.0.

A system's design bases shall present the guidelines and standards according to which the system is designed. The preliminary safety classification of the system plus its equipment as well as its environmental conditions and consequent design requirements shall also be given.

A plan of qualification according to subsection 4.4, and any previous qualifications to be utilised in the qualification of the system, shall be included in the preliminary qualification plan of the conceptual design plan phase. The preliminary qualification plan shall include a schedule on the provision of the result documentation to STUK.

The preliminary safety assessment shall demonstrate how the system fulfils the safety requirements imposed on it. It shall also give a preliminary assessment of how modifications to the system affect probabilistic safety analyses (PSA).

6.3 System pre-inspection documents

The pre-inspection documents of Safety Class 2 and 3 I&C systems and, for applicable parts, those of Safety Class 4 I&C systems shall primarily contain descriptions equivalent to the contents of the final safety analysis report, and they shall include the descriptions below:

- detailed system design bases
- detailed description of system operation and configuration
- system environmental conditions and stresses, and consequent design requirements
- the location, segregation, protection (fire compartments, physical protection) of subsystems important to safety

- impact on a nuclear power plant's other systems, and dependencies from other systems as well as prevention of fault propagation
- a probabilistic assessment of the system's impact on plant safety
- quality plan
- information security plan
- qualification plan
- qualification result documentation
- designer's safety assessment of how the system meets its safety requirements
- licensee's own safety assessment in accordance with subsection 2.3 of Guide YVL 2.0
- system specific requirements in the Technical Specifications
- other necessary descriptions.

The pre-inspection documents of systems are submitted for approval in stages such that the qualification result documentation and independent assessments are submitted only after design and implementation have reached the relevant phases.

Instructions are provided in Guide YVL 2.0 on what system design bases should be included in the pre-inspection documents. The requirement specification of Safety Class 2 and 3 I&C systems shall be sent to STUK for information. The report of the independent assessment of the correctness, completeness and consistency of the requirements specification of Safety Class 2 I&C shall be sent to STUK for information.

Guide YVL 2.0 contains guidelines on the contents of the description of a system's operation. A system's operational description shall include also the self-diagnostics of programmable systems plus analysis of the coverage of the self-diagnostics.

System construction and operation shall be presented in the form of schematic diagrams, where necessary, showing the below data, among other things:

- principal diagrams and functional diagrams of control functions, automatically actuated tasks, interlocking, etc.
- a summary of the service data of measurements (symbol, measurement range, protection and alarm limits)
- in case of a computer-based system, also the system's and software architecture diagrams and flow diagrams are to be given
- software tools and their functional description
- functional diagrams of electrical protections
- principal design diagrams of auxiliary voltage supplies.

The means of quality management pertaining to system design and implementation shall be presented in a quality plan. The instructions and procedures relating to the quality plan are sent to STUK for information.

The qualification plan shall include data presented in subsection 4.4 of this guide. The qualification result documents shall include the licensee's assessment of the realisation of qualification.

The system's safety significance and the reliability targets of its functions are considered when the quality plan and the qualification plan are reviewed.

An information security plan containing the system's data security related procedures and instructions for operation shall be sent to STUK for information.

A safety assessment shall be conducted for Safety Class 2 and 3 systems by which fulfilment of the provisions of YVL guides and of the requirement specification is demonstrated as well as the effect on PSA.

Along with the system's pre-inspection documents, any impacts to the Technical Specifications at principal level shall be stated.

As regards extensive plans with a significant bearing on nuclear safety, or plans requiring special know-how, the licensee shall consider whether to commission their independent safety

assessment to an assessor entirely independent of the licensee's organisation. The minimum competence required of individuals and organisations conducting design audits and independent safety assessments is that which is required in the design task, and it shall have been proven in practice. After the assessments have been carried out the licensee shall satisfy himself of the acceptability of the design by safety assessments based on sufficiently profound own know-how.

6.4 Equipment suitability analysis

STUK reviews the licensee's suitability assessment as regards the below equipment:

- Safety Class 2 I&C equipment
- Safety Class 3 essential accident instrumentation (NRC Regulatory Guide 1.97, cat. 1 [1]).

A preliminary suitability analysis is submitted to STUK for approval in case a piece of equipment needs to be subjected to type approval as part of its qualification. The preliminary suitability analysis shall state the standards applicable in the type approval process and the competent body. Of that organisation, its accreditation or the data on inspection bodies required in Guide YVL 1.3 shall be given, as applicable.

In conjunction with the suitability analysis, the below data on each piece of equipment shall be submitted for information:

- plant and application specific requirement specification
- design bases
- description of operation, design and construction as well as drawings
- vendor data
- quality plan
- type approval report.

The suitability analysis of Safety Class 3 equipment is submitted for information without the aforementioned documents.

The guidelines and standards to be applied in the design, manufacture, testing and installation of equipment shall be stated in the design bases of each piece of equipment. Possible deviations from applicable standards and guidelines shall be presented and justified in accordance with subsection 4.1.

The operation and construction descriptions as well as drawings of equipment shall be sufficient to facilitate the evaluation of the type approval and the review of the suitability analysis. Software tool descriptions shall be incorporated in equipment descriptions.

Vendor data shall include vendor organisation, competence and how their quality system has been assessed. The assessment results of the quality system shall be presented.

6.5 Regulatory control of manufacturing, factory tests

At its discretion STUK controls by inspections the manufacturing of I&C systems and equipment subject to pre-inspection. During the inspections STUK must be provided with the opportunity to check, among other things, the quality management systems of the manufacturer, the documents on quality control during manufacturing and the documents referred to in the qualification plan.

For the purpose of potential inspections by STUK at the premises of vendors and suppliers, STUK shall be sent for information the testing schedules of systems (performance and functional tests). The testing programmes of those factory tests that STUK informs to monitor shall be submitted for information.

6.6 Regulatory control of installations

At its discretion STUK controls the installation of Safety Class 2 and 3 I&C systems and equipment.

For installation control by STUK the installation schedule of Safety Class 2 and 3 I&C systems and equipment shall be sent for information prior to the commencement of their installation. During the inspection the licensee is to present STUK with the results of its own inspections plus the related documents.

STUK assesses during the inspections that the overall implementation of installations corresponds to the plans in approved pre-inspection documents and that it is up to the required quality level.

6.7 Commissioning inspections

STUK controls the commissioning testing of I&C systems by onsite tests in accordance with Guide YVL 2.5. STUK witnesses onsite testing at its discretion. The commissioning testing programmes of Safety Class 2 and 3 I&C systems shall be sent to STUK for approval and the test schedules for information well in advance of the commencement of start-up testing.

The result documentation of the commissioning tests of the systems belonging to the safety class 2 and 3 shall be submitted to STUK for approval. During the pre-inspection of the safety class 4 systems STUK specifies which commissioning programmes, test schedules and result documentation shall be submitted to STUK for information.

During the pre-inspection of I&C systems STUK specifies the systems whose commissioning inspections it will conduct. During these inspections the licensee shall present STUK with the system modifications implemented and the results of inspections made by the licensee according to subsection 4.5 plus related result documents.

System commissioning inspections by STUK shall be carried out prior to plant start-up from an annual maintenance outage or during operation prior to the commissioning of a system. The licensee shall request for these inspections in writing well in advance of the inspection day.

Commissioning and functional testing required by the operational safety of the measurement and control equipment of a nuclear power plant's pressure equipment other than the reactor pressure vessel are dealt with in Guide YVL 3.7.

6.8 Regulatory control of equipment quality management

The licensee shall draw up general plans for quality control in the design, manufacturing, receiving, installation and commissioning phases of equipment in various safety classes, as required in subsection 4.2. The plans shall be submitted to STUK for approval prior to the aforementioned phases.

6.9 Regulatory control during plant operation

During the operation of nuclear facilities STUK controls I&C systems and equipment by inspecting the repairs and modifications of systems and individual pieces of equipment. At the same time STUK assesses the operations of the licensee and the efficiency of his procedures in assuring the reliable operation of the systems and equipment. Licensee operations are regularly assessed in inspections of the periodic inspection programme.

As part of the periodic inspection programme, STUK ensures that the below functions are appropriately implemented for safety classified objects

- assigning of requirements, design and maintenance of I&C systems and equipment
- quality management, equipment procurement, spare parts management and receiving inspections
- the operation and the condition the operability and condition of I&C systems and equipment is ensured by periodic testing
- assessment of the environmental and operating conditions of equipment
- assessment of the assessment of the equipment ageing
- maintenance of the accuracy of measuring equipment
- equipment surveillance, failure data, failure data gathering systems and analyses
- the preventive maintenance of the equipment, repair and spare part service

- configuration and version management of equipment and systems.

The periodic testing programmes of I&C systems and equipment, the procedures to be followed during them and the guidelines for condition monitoring shall be sent to STUK for information. Test results shall be recorded onsite such that STUK can assess them and compare them with previous test results.

The acceptability of requirements pertaining to the availability of safety-important I&C systems and equipment, as well as the scope of periodic tests, are assessed by STUK during the review of the Technical Specifications of nuclear facilities.

In addition, STUK regularly checks that the environmental and operating conditions of safety-classified equipment are properly monitored by measurements at relevant locations and, where necessary, measures are taken to review maintenance programmes, service life assessments and qualification. STUK checks onsite the measurement results in the extent it deems necessary.

STUK monitors the realisation and results of the licensee's I&C systems and equipment ageing follow-up programme in connection with the periodic inspection programme, among other things.

The results of the ageing management shall be presented in a report every year, which is sent to STUK for information.

6.10 System and equipment modifications during operation

Guides YVL 2.0 and YVL 1.8 present requirements pertaining to modifications at nuclear facilities.

STUK carries out pre-inspections of safety-classified I&C systems and equipment in the extent specified in subsection 6.1.

Work on modifications may only be started when STUK has approved the pre-inspection documents and when requirements for the commencement and supervision of work, which may have been included in STUK's decision on approval, have been fulfilled. The commissioning operation programmes of modified system sections and equipment shall be drawn up such that they, as well as possible, correspond to the original commissioning programmes.

STUK's approval of modifications to Safety Class 4 and non-nuclear (EYT) systems shall be obtained in case they affect the realisation of the design bases presented in Guide YVL 1.0.

Prior to a system's commissioning, the licensee shall obtain approval for any changes that need to be made to the Technical Specifications. Also prior to system commissioning, the emergency, transient and operating instructions shall be updated to correspond to the modified system.

After the system's commissioning, any changes proposed to the Final Safety Analysis Report shall be submitted to STUK for approval without delay.

7 Definitions

Deterministic design principle
System design is based on pre-established design requirements and on a set of postulated initiating events (PIE) whose effect on plant safety is considered in system design.

Dynamic testing
System or component evaluation based on its behaviour during execution of functional tests.

Integration tests
The task of the integration test is to verify interconnections between system units or the compatibility of the system units. The integration tests of a computer-based system assure software/hardware compatibility as well.

Self-diagnostics

A system or piece of equipment's built-in function for monitoring system/equipment error-free operation and failure and which, upon error-detection, carries out pre-determined functions.

Qualification

Qualification demonstrates the ability of I&C systems or equipment to fulfil the functional and performance requirements imposed on them in all their operating conditions and design basis environmental conditions.

Operational conditions

Operational conditions mean a nuclear power plant's normal operational conditions and anticipated operational transients.

Quality plan

The quality plan is a document setting out the specific quality practices, resources and sequence of activities relevant to a particular product or project.

Normal operational conditions

Normal operational conditions denote the operation of a nuclear power plant in accordance with the Technical Specifications. They also include systems and equipment testing, plant unit start-up and shutdown, as well as maintenance and refuelling.

Anticipated operational transients

An anticipated operational transient means such a milder-than-an-accident deviation from normal operational conditions the expectation value of whose occurrence frequency is higher than once in a hundred operating years.

Software tool

A tool used for software development, compiling, generating, testing and analysis.

Computer-based system

A computer-based system is an instrumentation and control system whose functions have, for the most part or entirely, been implemented using a microprocessor, a computer-based piece of equipment or a computer. The system encompasses all system units, such as internal power supply units, sensors and other input units, communication routes, output units and other communication channels to actuators.

A piece of computer-based equipment

A piece of computer-based equipment consists of one or several units in a computer-based system. It is an independent, definable system unit that is often detachable. It can also be an independent piece of equipment containing computer-based technology.

Pre-existing software

Pre-existing software denotes software or program developed prior to a project. It's scope ranges from a simple program to an extensive I&C system.

Postulated accident

A postulated accident means such a nuclear power plant safety system design-basis event as the nuclear power plant is required to manage without any serious damage to the fuel, and discharges of radioactive substances so large that in the plant's vicinity, extensive measures should be taken to limit the radiation exposure of the population.

Accident

An accident means such a deviation from normal operational conditions as is not an anticipated operational transient. There are two classes of accident: postulated accidents and severe accidents.

Accident instrumentation

Accident instrumentation is the measuring and control instrumentation for accident monitoring and management. It provides the operating personnel with sufficient information for situation assessment as well as for the planning and implementation of countermeasures.

I&C system platform

I&C system platform is that section of an instrumentation and control system which is independent of the application and is used as part of an operating system.

Independent inspection or assessment

Independent inspection and assessment comes in three different levels: the performer of an inspection or assessment is an individual, organisation unit or organisation independent of the design and implementation of the object. The level of independence to be used is dictated by the character of the task to be carried out and the assessment result's importance to the assurance of safety. More detailed requirements applicable to the various levels of independencies can be found in standard SFS-EN 45004 "General requirements for the operation of various types of bodies performing inspection".

Application

A computer-based system application is that part of the system which carries out the functions needed for controlling the process.

Static testing

Static testing is a process of assessing a system or component on the basis of its form, structure, content or documentation. Examples of static testing include, among other things, verification of software design, code and compliance with standards (e.g. the Fagan method), analysis of control and data flow diagrams, symbolic program execution and formal code verification.

Unintentional function

An unintentional function is one that is unnecessary for the actual functioning of a system or piece of equipment. Functions not required to accomplish a task, but whose safety significance has been analysed and considered in system design, are not unintentional.

Functional independence

An I&C system's functional independence is implemented by means of electrical and communication independence.

Safety system

A safety system is a system which carries out a certain safety function.

Safety function

Safety functions are safety-significant functions to prevent the occurrence or propagation of transients and accidents or to mitigate the consequences of accidents. A safety function encompasses the equipment carrying out a function, i.e. measuring, logic and actuator.

Severe accident

A severe accident means an event during which a significant part of the fuel in the reactor sustains damage.

Common cause failure

A common cause failure denotes the simultaneous failure of several systems, pieces of equipment or structures in consequence of the same single failure or cause.

Single failure

A single failure means a random failure and its consequent effects which are assumed to occur either during a normal operational condition or in addition to the initial event and its consequent effects. Further guidelines on single failures and how to provide for them can be found in Guide YVL 2.7.

8 References

1. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.97, revision 3, May 1983.

2. “Common position of European nuclear regulators for the licensing of safety critical software for nuclear reactors”, EUR 19265, 2000.

3. IAEA Safety Standards Series, NS-G-1.3, “Instrumentation and control systems important to safety in nuclear power plants”, Safety Guide, March 2002.

4. IAEA Safety Standards Series No. NS-G-1.1, “Software for Computer Based Systems Important to Safety in Nuclear Power Plants”, Safety Guide, September 2000.

5. IEC 61513 “Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems”, First edition 2001-03.

6. IEC 60880 “Software for computers in the safety systems of nuclear power stations”, First edition 1986.

7. IEC 60880-2 “Software for computers important to safety for nuclear power plants – Part 2: Software aspects of defence against common cause failure, use of software tools and of pre-developed software”, First edition 2000-12.

8. IEC 60987 “Programmed digital computers important to safety for nuclear power stations”, First edition 1989-11.

9. IEC 62138 “Nuclear Power Plants Instrumentation and Control-Computers-based systems important for safety-Software aspects for I&C systems of class 2 and 3”, Draft 2001.

10. IEC 60780 “Nuclear Power Plants – Electrical equipment of the safety systems – Qualification”, Second edition 1998-10.