STUK

GUIDE **YVL 5.2** / 24 JUNE 2004

ELECTRICAL POWER SYSTEMS AND COMPONENTS AT NUCLEAR FACILITIES

continues

This Guide is in force as of 1 December 2004 until further notice.
It replaces Guide YVL 5.2, issued on 23 January 1997.

Second, revised edition
Helsinki 2004
ISSN 0783-2400

ISBN 951-712-924-6 (print) Dark Oy / Vantaa 2004
ISBN 951-712-925-4 (pdf)
ISBN 951-712-926-2 (html)

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 Government Resolution (395/1991) on the Safety of Nuclear Power Plants
- Section 13 of the Government Resolution (396/1991) on the Physical Protection of Nuclear Power Plants
- Section 11 of the Government Resolution (397/1991) on the Emergency Preparedness of Nuclear Power Plants
- Section 8 of the Government Resolution (398/1991) on the Safety of a Disposal Facility for Reactor Waste
- Section 30 of the Government 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 Government Resolution (395/1991), which prescribes that *for further safety enhancement, action 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 the YVL guides, STUK shall be presented with some other acceptable procedure or solution by which the safety level set forth in the YVL guides is achieved.

Translation. Original text in Finnish.

1 General

The electrical power systems and components of the nuclear power plant on the one hand generate electrical power and supply it to the external grid and on the other hand supply electrical power to the plant's systems from external and internal power supplies. The reliable operation of these systems is important for ensuring plant safety, accident management and the mitigation of the consequences of accidents.

The Government Resolution (395/1991) presents general safety requirements for nuclear power plants. This resolution contains both general provisions for all safety systems and provisions for the electrical power systems of nuclear power plants. These are stated in more detail in Guide YVL 1.0, which sets forth the safety principles to be applied in nuclear power plant design.

Guide YVL 1.1 describes how STUK controls the design, construction and operation of nuclear power plants. Guide YVL 5.2 gives the detailed design bases and safety requirements pertaining to electrical systems and components at nuclear facilities. Chapter 6 describes STUK's regulatory control of a nuclear facility's electrical systems and components.

Section 5 of the Government Resolution (395/1991) prescribes that 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. Guide YVL 1.4 presents general requirements for quality management systems and Guide YVL 1.9 for quality management during operation.

Guide YVL 2.0 applies generally to the design and regulatory control of nuclear power plant systems – specifically those assigned to a safety class – and specifies in more detail the general design requirements presented in Guide YVL 1.0.

The safety importance of the function a system performs is essential in the focusing of STUK's control activities. The safety classification of systems, structures and components affects their control. Paragraph one of section 21 of the Government Resolution (395/1991) prescribes that the functions important to the safety of the system, structures and components of a nuclear power plant shall be defined and the systems, structures and components safety-classified according to their safety significance. Detailed instructions for safety classification are given in Guide YVL 2.1.

In addition, several other YVL guides apply to electrical power systems and components. Guide YVL 1.8 describes how STUK controls the modification, repair and preventive maintenance of systems, components and structures at nuclear facilities during operation. The guide also presents the obligations imposed upon licensees regarding this work. Guides YVL 2.2 and YVL 2.8 set forth the requirements for safety goals and their demonstration. The requirements for failure criteria are given in Guide YVL 2.7. Diesel generators and their auxiliary systems are dealt with in Guide YVL 5.1; valves and valve actuators in Guide YVL 5.3; instrumentation and control (I&C) systems in Guide YVL 5.5; air conditioning systems and equipment in Guide YVL 5.6; pumps in Guide YVL 5.7; and hoisting and transfer appliances in Guide YVL 5.8. Provision against earthquakes is addressed in Guide YVL 2.6; and fire protection in Guide YVL 4.3. A nuclear power plant's radiation monitoring systems and equipment are dealt with in Guide YVL 7.11; and those radiation protection aspects to be considered in the design and layout of nuclear power plant systems and components in Guide YVL 7.18.

This guide sets forth licensee obligations regarding the design, implementation and operation of electrical power systems and components at nuclear power plants as well as STUK's procedures pertaining to their control and inspection.

In addition to this Guide, the Finnish Electrical Safety Act (410/1996) and Decree apply to nuclear facilities. Electrical safety regulations and other corresponding rules are based on the act and decree. Compliance with the electrical safety legislation is controlled by the competent authorities.

The quality glossary used in this Guide complies with SFS-EN ISO 9000 [9].

2 Design bases of electrical power systems and components

2.1 General

In accordance with the fourth paragraph of section 18 of the Government Resolution (395/1991), a nuclear power plant shall have on-site and off-site electrical power supply systems. The execution of the most important safety functions shall be possible by using either of the two electrical power supply systems

In accordance with Guide YVL 1.0, the plant shall be provided with systems, which enable power supply from the main generator to the plant's safety significant systems in case the connection to the external transmission gird is lost.

The plant's electrical power supply units shall be designed such that the loss of a single electrical power supply unit followed by the loss of the plant's other power supply units, or their loss due to the same cause, is highly unlikely.

The plant's off-site and on-site electrical power supplies shall be designed such that each can alone ensure reactor decay heat removal, primary circuit integrity and reactor sub-criticality.

The electrical power supplies of measuring systems for accident monitoring and management shall be designed in accordance with the accident instrumentation requirements of section 2.5 of Guide YVL 5.5.

For severe accident management and monitoring, the nuclear power plant shall be equipped with monitoring devices, as described in section 3.6 of Guide YVL 1.0, whose electrical power supplies are to be independent of the plant unit's other electrical power supply units.

General design requirements for the electrical power systems of nuclear power plants are set forth in IEEE 308 [1], IEEE 765 [4], KTA 3701 [5] and IAEA DS303 [6], among others, which are referred to in this Guide.

2.2 Off-site grid connections

In accordance with Guide YVL 1.0, for electrical power supply, there shall be two separate, independent grid connections from the external grid to each parallel section of the on-site electricity distribution system. These grid connections shall be so designed that during operational conditions and postulated accidents, the simultaneous loss of both is unlikely. It must be possible to start operation of both grid connections quickly enough after the plant main generator has been separated from the grid.

Plant design shall consider variations of voltage and frequency that occur in the external power transmission grid and affect the electrical systems and components of the nuclear power plant. The external grid connections and their auxiliary systems shall be electrotechnically dimensioned as well as physically and functionally separated from other electrical power systems in such a way that design-basis disturbances in the external power transmission grid do not jeopardise the operation of safety-classified components during plant operational transients and accidents.

The plant unit's off-site grid connections shall be electrotechnically dimensioned such that each connection alone has sufficient capacity to ensure the removal of decay heat, to assure primary circuit integrity and to maintain reactor subcriticality. Several units at the plant may share connections to the off-site power transmission grid. That being the case, each connection alone must have sufficient capacity to simultaneously carry out the aforementioned safety functions at all plant units.

The design of off-site grid connections shall make unlikely the simultaneous failure of both of them from the same cause in consequence of operational transients, postulated accidents, weather phenomena or other external events. Plant design shall also consider all component failures and fires that could be caused by short circuits in the grid connections. In addition, auxiliary systems important for the operability of the connections, e.g. auxiliary voltage supplies and automatic switching devices, shall be designed in a way making the connections as independent as possible.

The plant unit shall be provided with reliable, automatically starting change-over equipment for change-over switching between off-site grid connections. Change-over switching shall be designed to not unnecessarily start the plant's safety systems. Manual change-over must be pos-

sible from the main control room or, in case of the loss of the main control room, from outside the main control room.

2.3 Normal power supply systems

The plant's normal power supply systems supply the necessary electrical power to the plant units' electrical equipment and I&C systems, either from their own electrical power supplies or from the off-site power transmission grid. Normal power supply systems refer here to electrical power systems whose operation is not secured by auxiliary power supply systems.

The design of normal power supply systems shall ensure that the disturbance or failure of a Safety Class 4 or Class EYT (non-nuclear) normal power supply system does not endanger the designed operation of a Safety Class 2 or 3 electrical power or I&C system. The functional separation of Safety Class 4 normal power supply systems shall be designed to render unlikely the deterioration, or failure, of the operating capability of its redundant subsystems due to the same electrical disturbance.

The capability of the plant unit's normal power supply systems shall be electrotechnically dimensioned to supply sufficient electrical power for the fulfilment of essential safety functions.

2.4 Secured alternating current power systems

The operation of Safety Class 2 and 3 alternating current components shall be assured by supplying electric power from onsite emergency power supply systems. Those emergency power supply systems that carry out a safety function only shall be physically separated from plant sections for normal operation. Systems performing the same safety function, and their subsystems - whether they are similar to or different from one another - shall also be separated. The functional separation of safety-classified alternating current power systems shall be designed such that the deterioration, or failure, of their redundant subsystems due to the same electrical disturbance is unlikely.

The systems are to automatically engage to ensure uninterrupted power supply, or power supply if a voltage break of permissible duration has occurred, in case normal power supply is disrupted in a way endangering the operability of components. The on-site emergency power supply systems shall be designed to assure the availability of Safety Class 2 and 3 secured alternating current power systems according to the operating time requirements set to them. It shall be possible to reliably take the emergency power supply systems into service even from the main control room and from local control centres.

The design of the emergency power supply systems shall make them capable of reliably starting, engaging, receiving loads and feeding electrical power even during the most demanding loading situations (e.g. start-up situations) and operating conditions. The quality of the alternating current supply shall be kept such that the operating capability of the supplied components is not compromised. Requirements that apply to the diesel generators of nuclear facilities are discussed in more detail in Guide YVL 5.1.

The emergency power supply systems shall be provided with sufficiently comprehensive, alarming condition monitoring systems to promptly detect and locate failures causing unavailability of the systems.

For the duration of their functional testing, maintenance and repair, it shall be possible to safely disconnect from other electrical power systems those units that belong to the emergency power supply systems. If necessary, it shall be possible to reliably replace the power supply units of battery-backed alternating current systems with stand-by power supply connections facilitating the safe fulfilment of measures relating to the power supply units.

Automatic features (e.g. automatic start-up and switching devices) essential for the operation of redundant subsystems and auxiliary systems (e.g. auxiliary voltage, cooling, fuel, lubrication and compressed air) shall be designed according to the same principles as the subsystems. The auxiliary systems shall be so electrotechnically dimensioned that they are capable, in accordance with the set operating time requirements, of ensuring the operating capability of Safety Class 2 and 3 secured alternating current systems in all plant operational conditions and postulated accidents.

2.5 Total loss of alternating current power

In accordance with Guide YVL 1.0, in nuclear power plant design, the possibility of the on-site and off-site power supply units being simultaneously lost shall be considered. As provision against such a situation, the plant shall have available a power supply unit which is independent of the electrical power supply units designed for operational conditions and postulated accidents. It must be possible to introduce this power supply unit into operation quickly enough and its capability shall be sufficient to remove reactor decay heat, to ensure primary circuit integrity and to maintain reactor sub-criticality.

Plant-unit specific, independent alternating current power supply units shall be dimensioned according to the above capacity requirement. An alternating power supply unit may be shared by several plant units. The capacity of the unit in question shall then be sufficient for the simultaneous removal of reactor decay heat, ensuring of primary circuit integrity and maintenance of reactor sub-criticality for all the nuclear facilities on the site.

The design of an independent alternating current power supply unit shall be such that its failure simultaneously with the external power transmission grid connections, and due to the same cause, in consequence of weather phenomena or other external events is unlikely. In addition, auxiliary systems important for the operability of the supply unit and external grid connections, e.g. auxiliary power supplies and automatic switching systems, shall be designed such that the independent supply unit and external grid connections are as independent of each other as possible.

It shall be possible to quickly and reliably take an independent power supply unit into service, if necessary. The design of the connections shall reliably prevent plant-to-plant spreading of electrical disturbances via them and their unplanned taking into service or engaging; also, their design shall reduce the likeliness of human errors during their planned taking into service and operation.

2.6 Direct current power systems

To assure the operation of Safety Class 2 and 3 direct current equipment, their electrical power supplies shall be ensured by reliable and sufficiently efficient batteries to ensure an uninterrupted supply of direct current power in case of a disturbance in the supply of alternating current power, which endangers their operability.

The batteries and their charging devices shall be dimensioned to reliably assure the operating capability of Safety Class 2 and 3 direct current power systems in accordance with system-specific operating time requirements. Guide YVL 1.0 prescribes that batteries backing up the operation of electrical systems important to safety shall maintain their capability to operate at least for two hours under any circumstances. The design bases of start-up batteries for combustion engines and of other special-purpose batteries shall be given case-by-case.

Charging devices shall be capable of simultaneously feeding direct current to the loads and of charging storage batteries. A charging device shall be dimensioned such that its performance is not endangered even during the most demanding loading situations (e.g. start-up) and operating conditions. It shall be capable of feeding the necessary direct current to the loads even if the storage battery has been disconnected. Even then, the quality of the direct current supplied must not cause malfunctioning of the loads. Charging devices shall be designed to reliably prevent the passing of potential disturbances from alternating current power systems to a direct current power system via them.

Direct current systems performing a safety function only shall be physically separated from plant sections for normal operation. Systems and subsystems for the same safety function, whether they are similar or not, shall be separated from each other. The functional separation of safety-classified alternating current power systems shall make unlikely the operational weakening or malfunctioning of redundant subsystems due to the same electrical disturbance.

Safety Class 2 and 3 direct current power systems shall be designed to be as independent of other systems as possible. Automatic features essential for the operation of redundant subsystems (e.g. protection and possible automatic switching systems), and auxiliary systems (e.g. auxiliary voltage and air conditioning) shall be designed according to the same principles as the

subsystems proper. The auxiliary systems shall be dimensioned such that they are, in accordance with the set operating time requirements, capable of assuring the operating capability of Safety Class 2 and 3 secured alternating current systems in all plant operational conditions and postulated accidents.

The design of direct current power supply systems shall ensure that the disturbance or failure of a Safety Class 4 or Class EYT (non-nuclear) direct current power supply system does not endanger the designed operation of a Safety Class 2 or 3 electrical or I&C system.

Safety-classified direct current power systems shall be equipped with extensive enough alarming condition monitoring devices by which the operability of the systems can be continuously reliably monitored and failures causing their unavailability immediately detected and located.

2.7 Main control room, emergency control posts and local control centres

The main control room of a nuclear power plant shall be equipped with devices providing information about the operational state, and deviations from it, of the plant's electrical systems and the off-site power transmission grids; as well as with systems monitoring the operation of the plant's electrical systems during operational transients and accidents. The need for emergency control operations from outside the main control room for normal and emergency power systems shall be analysed. The design bases for a nuclear facility's main control room and emergency control posts are given in sections 2.3 and 2.4 of Guide YVL 5.5.

Power supplies for the I&C systems of the main control room, the emergency control post and local control centres, which are needed to manage the nuclear power plant unit during operational conditions and accidents, shall be ensured by internal emergency power supply systems. In the main control room, the power supplies of the various subsystems of safety systems shall be reliably functionally separated to make unlikely their simultaneous failure from the same electrical disturbance.

The power supplies for an emergency control post outside the main control room shall be separated from those for the main control room such that the total destruction in a fire of components contained in one fire compartment does not damage both power supplies so much as to prevent the fulfilment of safety functions.

Guide YVL 4.3 prescribes that cables from the safety-related redundant subsystems to the main control room shall be routed through separate fire compartments. In case the cables from different redundant systems must exceptionally be situated in the same fire compartment, they shall be separated inside the compartment by means of distance, fire-resistant materials and fire insulation. The cable space below the main control room is an example of such a compartment.

2.8 Unit-to-unit power supply

The design of the alternating current power supply systems of nuclear power plant units shall enable unit-to-unit supply of electrical power within the site such that, where necessary, one unit can be maintained in a safe state in case of the loss of the off-site grid. The design of the power supply connection shall make unlikely the unit-to-unit propagation of an electrical disturbance via it and also the connection's unplanned taking into service and engaging. The connection shall be available promptly and reliably enough where necessary. The control and switching actions of the connection shall be designed to minimise the probability of human error.

3 General design requirements

3.1 Redundancy, separation and diversity principles

In accordance with the third paragraph of section 18 of the Government Resolution (395/1991), systems which perform the most important safety functions shall be able to carry out their functions even though an individual component in any system would be out of operation simultaneously due to repairs or maintenance (the redundancy principle).

In accordance with Guide YVL 1.0, the onsite electrical power supply system serving the safety functions shall be capable of carrying out its functions during anticipated operational transients and postulated accidents even in the

event of a single failure, although any component would simultaneously be inoperable due to repair or maintenance. According to the redundancy principle, provision for component malfunctions is made by having s everal subsystems perform the same function. These subsystems may be similar to, or different from, one another.

In accordance with section 18 of the Government Resolution (395/1991), safety systems which back up each other as well as parallel parts of safety systems shall be separated from each other so that their failure due to an external common cause failure is unlikely (the separation principle).

Guide YVL 2.0 prescribes that systems that carry out safety functions only shall be structurally separated from plant sections serving the purpose of normal operation. Systems and subsystems carrying out the same safety function, whether or not they be similar or dissimilar, shall be separated from one another as well. In addition, it shall be assured by design that the failure of a Class EYT (non-nuclear) or Safety Class 4 electrical power system does not endanger the designed operation of a Safety Class 2 or 3 electrical power or I&C system.

The functional separation of safety-classified electrical power systems shall be designed to make unlikely the operational deterioration, or failure, of redundant subsystems from the same electrical disturbance. The bases for the functional and structural independence of safety-classified systems are set forth in IEEE 384 [8] among others.

Cross-connections between redundant subsystems shall be avoided, unless improved system reliability can be demonstrated from them. Their design shall reliably prevent unintentional cross-connections and make human errors unlikely during their planned taking into service and operation. The propagation of malfunctions from one subsystem to another via cross-connections shall be reliably prevented.

Section 18 of the Government Resolution (395/1991) prescribes that in ensuring the most important safety functions, systems based on diverse principles of operation shall be used to the extent possible (the diversity principle).

To assure safety functions, the reliability of electrical systems shall be improved and the effects of common cause failures prevented such that, as far as possible, systems, subsystems or components based on diverse principles of operation are employed. Diversity shall be utilised for assurance of safety, particularly when the sufficient reliability of a system or component carrying out a safety function cannot be verified by testing. In applying the diversity principle, it shall always be assured, however, that increased system sophistication does not invalidate the increase in reliability that is attained by the diversity principle. The application of the diversity principle to plant projects and modifications is dealt with in more detail in Guide YVL 2.7.

3.2 Qualification for environmental conditions

The environmental conditions and stresses of a nuclear facility's safety-classified electrical power systems and components as well as cables in all planned operational conditions and during storage and transport shall be defined. The systems, components and cables shall be of such design that, for their entire design service life, their operating capability is maintained within set requirements. The qualification of safety-classified components and cables under design environmental conditions and stresses shall be demonstrated by means of tests and analyses that are in accordance with standards. The environmental conditions shall be defined in the Preliminary and Final Safety Analysis Reports. The tests shall correspond to the combined effects of the most unfavourable operational and environmental conditions possible.

The design of structures and materials of electrical components as well as cables needed in accidents shall be such that, for their entire design service life, their required operating capability in accidents will be in compliance with the requirements.

The type tests of components and cables needed during accidents or after them are to form a uniform series of test frequencies during which the same test specimens are subjected to the design basis operating and environmental stresses in question. Prior to accident condition testing, the test specimens are to be artificially aged to correspond to their design service life.

The artificial ageing of the components or

cables shall be carried out in a way that, with adequate confidence, represents actual ageing. Ageing is usually carried out such that a test specimen is first thermally aged and then subjected to radiation. It then undergoes a mechanical tolerance test and finally the aforementioned tests simulating a postulated accident.

A test simulating a postulated accident shall include exposure to radiation and stresses caused by temperature, pressure and humidity levels equivalent to the accident conditions as well as rapid changes in the conditions representing these situations. The composition of the water used in the test shall be equivalent to that occurring in the accident conditions in question. If a component could become submerged during a postulated accident and must even then maintain its operating capability, its capability to operate in that situation shall be demonstrated as well. The tests shall be designed to verify, with sufficient confidence, the operating capability of a component or a cable in accident conditions for their entire design service life.

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

The qualification of electrical components that must operate during severe accidents shall be appropriately demonstrated. The qualification of electrical components and cables inside the containment, which must operate especially in the high temperatures occurring during severe accidents (possible hydrogen fires included), shall be demonstrated.

3.3 Electromagnetic compatibility (EMC)

The undisturbed operation of electrical systems and components is assured by the electromagnetic compatibility (EMC) of components intended for the same operating environment, i.e. a component's capability to withstand more disturbances than caused by the components around it. The nuclear facility's safety-classified electrical power and I&C components plus their cablings and installations shall be reliably protected against the effects of electrical and magnetic interference fields, mains and radio interference and disturbances caused by telecommunications. Electrical components shall be designed and installed to not themselves cause any harmful electromagnetic interference in their operating environment.

The following types of electromagnetic interference, among others, shall be considered in the design of electrical systems and components:

- (emission of and immunity to) radiated radio frequency disturbances
- (emission via cables of and immunity to) conducted radio frequency disturbances
- electrostatic discharge, ESD.

Other natural or man-made electromagnetic disturbances shall be examined as well.

Earthing systems and lightning protection systems shall be designed, installed and maintained to effectively protect people, buildings, equipment as well as electrical power and I&C systems against overvoltages and overcurrents caused by lightning strikes and other possible electromagnetic interferences due to climatic factors. In the design of the earthing systems, electrical systems shall be considered one entity, since the insufficient earthing of even one part of the system may expose the entire system to disturbances.

The emission characteristics of the radiotelephone systems used at the plant as well as those of repair, maintenance and measuring devices shall be considered during the design phase. The manufacturer's installation instructions shall be closely followed during the installation phase.

To avoid compatibility problems during the upgrading of an operating nuclear facility's electrical systems, specific attention shall be paid to the EMC environment in the location of new systems as well as to the EMC characteristics of new components.

Detailed EMC requirements shall be determined for safety-classified electrical systems and components and their compliance with the requirements demonstrated. General international EMC standards on industrial environments may serve as the basis for the requirements. The requirements shall be supplemented, where necessary, to cover the EMC environments of some components, which may be more demanding. When the EMC requirements are determined, the exposure of components to possible repetitive rapid (e.g. switching off of inductive loads and ringing of relays) and high energy (e.g. various switching transients and lightning) transients in their operating environment shall also be

considered. To establish the EMC environment of electrical systems and components at each nuclear power plant unit, unit-specific analyses shall be performed based on which the adequacy of each electrical component's EMC requirements is evaluated.

The adequacy of the procedures and technical solutions chosen to protect the nuclear facility's safety-classified electrical power systems and components from electromagnetic disturbances shall be justified.

3.4 Protection of electrical power systems and components

The electrical power systems shall be provided with reliable protection devices that in transients and malfunctions remove from service only the failed component or section of the electric power network. In case of short-circuit and overload situations, safety-classified protection devices shall operate selectively in all planned connection circumstances of the electrical power systems. Fault currents shall be cut off rapidly enough to avoid hazards and to minimise disturbances.

All the plant's high-power switchgears shall be provided with reliable arc protection, or other appropriate protection, to minimise switchgear damages caused by potential arc faults and to protect the safety of the plant and its operating and maintenance personnel.

The nuclear facility's earthing and overvoltage protection systems shall be designed to effectively prevent the occurrence of harmful on-site or off-site overvoltages in electrical power and I&C systems.

The protection of redundant subsystems shall be designed according to the same principles as the subsystems themselves. The protection devices of the subsystems shall be independent of one another as regards e.g. auxiliary power supply.

Sufficient alarms are to indicate the operation of the protection devices to promptly detect, locate and repair potential electrical faults. It must be possible to test the operation of the protection devices of safety-classified electrical power systems across the entire protection chain. The devices are to be regularly tested to assure the availability of the protective function.

The safety significance of the blocking of a safety function, brought about by a protection device, shall be evaluated and a device bypass feature designed, where necessary, provided that this does not endanger the availability of any safety-classified electrical power supply.

Individual protection devices possibly installed to safeguard components during testing shall be listed and designed such that their operation does not endanger a system's capability to operate during an actual event.

The general requirements for the protection of safety-classified systems and components at nuclear power plants are set forth in IEEE 741 [3], among others.

In the design of the protection devices of electrical power systems and components of nuclear facilities, also Finnish safety standards that apply to the safety of electrical equipment and electrical installations shall be considered as well as other electrical safety regulations issued by electrical safety authorities (e.g. the set of standards: SFS 6000: Low-voltage electrical installations; SFS 6001: High-voltage electrical installations; and SFS 6002: Safety at electrical work).

3.5 Preventive maintenance and repairs

The plant's design shall make possible the carrying out of operational actions as well as the periodic inspection, maintenance, testing and repair of electrical power systems and components in a way ensuring plant and personnel safety and minimising plant inoperability time caused by the actions.

Periodic inspections and tests shall be extensive enough to facilitate the prompt detection of deterioration in safety-classified electrical power systems and components prior to their failure to fulfil the acceptance limits. In addition, it shall be assured in particular that equipment and components having to do with stand-by power supply, which are not in use during normal plant operation, are always ready for operation. Periodic inspections and tests shall be scheduled such that sufficient stand-by power equipment are always available.

The design of the electrical power supplies of safety-classified electrical components shall facilitate the components' preventive maintenance during the plant unit's annual maintenance outage in the first place.

Guide YVL 2.8 states that the results of PSA

are to be used i.a. in the drawing up of testing programmes and preventive maintenance programmes for safety-significant systems.

3.6 Component identification symbols

In accordance with Guide YVL 1.0, a clear marking system shall be planned to identify components.

To facilitate component identification and to avoid human error, the components and cables of the plant's electrical power systems shall be provided with identification symbols made of durable materials, freely accessible during inspection, maintenance and troubleshooting. In addition, the cables and their routes shall be documented in sufficient detail.

3.7 Information security

In the design, operation and maintenance of electrical power systems, attention shall be paid to security issues. Unauthorised access to rooms containing electrical equipment and their possible software important to the plant's safety and disturbance-free operation shall be prevented by sufficient physical, technical and administrative security measures. The installation of unauthorised parts of software during design, manufacturing, commissioning, periodic testing and maintenance shall be reliably prevented. Authorised accesses to the software of electrical power systems, and any modifications therein during such accesses, shall be traceable.

4 Design and implementation of electrical power systems

4.1 General requirements

In the design of electrical power systems, 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, first paragraph].

Guide YVL 2.0 presents general requirements for systems design and defines in more detail the general design requirements set forth in Guide YVL 1.0. According to Guide YVL 2.8, in the design of system modifications PSA methods shall be employed to assess alternative solutions.

The design and implementation of Safety Class 2 and 3 electrical components and cables relating to essential accident instrumentation (section 6.4) as well as of those electrical components and cables for which specific environmental qualification requirements have been set, which are needed in accidents, shall be based on international electrical equipment standards and, for applicable parts, on nuclear engineering standards and guidelines. In the design of components and cables other than those in the above Safety Classes 3 and 4, applicable international electrical equipment standards shall be used.

The standards used in design and implementation shall be specified and their suitability justified. Potential deviations from the specified standards shall be evaluated and justified for Safety Class 2 and 3 electrical systems, components and cables. The requirements for specification, design, implementation, maintenance and quality management of electrical power systems and components shall be commensurate with their safety class and safety significance. Also the reliability targets of design basis functions shall be accounted for when specifying requirements for the design, implementation and qualification of electrical power systems and components.

4.2 Quality management

4.2.1 General requirements

Section 5 of the Government Resolution (395/1991) prescribes that 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.

Guide YVL 1.1 lists those quality management documents, plus their dates of delivery, which the license-applicant or -holder shall submit to STUK.

Section 21 of the Government Resolution (395/1991) prescribes that the systems, structures and components important to safety shall be designed, manufactured, installed and operated so that their quality level and the inspec-

tions and tests required to verify their quality level are adequate considering any item's safety significance.

In accordance with Guide YVL 1.4, the licensee has overall responsibility for the incorporation of valid regulations and YVL guide requirements in the quality management systems of the various organisations involved. The appropriate application of quality requirements within organisations participating in the design, manufacture, receiving, installation, commissioning and maintenance of electrical systems and components, as well as in their sub-contracting jobs, shall be assured. The licensee is responsible for adherence to established quality requirements and for attainment of an adequate quality level. The licensee shall therefore have available a quality management system that defines systematic procedures for the design, construction and operation of the nuclear facility.

Guide YVL 1.4 presents general requirements for the contents of the quality management systems of organisations applying for a construction and operating licence for a nuclear facility as well as for the quality management system's maintenance and continuous improvement. The requirements for a quality management system for use during the nuclear facility's operation are given in Guide YVL 1.9.

Advanced design, manufacturing and change management methods, taking into account the specific features of the technology applied, shall be utilised in the design, manufacturing, installation, operation and maintenance of electrical power systems and components. Quality management measures ensure consistency of the structure and features of product batches procured to the plant with those of qualified products.

4.2.2 Quality management system

To cover the construction and operational phases of the nuclear power plant, general quality management requirements shall be specified for electrical power systems and components, taking into account the safety importance of items. Quality management during construction shall cover quality management as applied by the various parties engaged in design, manufacturing, receiving, installation and commissioning. Quality management at operating plants shall cover corresponding functions as well as the operation, maintenance and modifications design of existing systems and equipment. All parties contributing to the above functions shall apply quality management in their operations.

The licensee shall specify the procedures for evaluating, selecting and controlling suppliers of electrical power systems and components. Before the supplier is selected, it shall be confirmed that the organisations involved have the prerequisites for high quality work.

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 the electrical components needed in operational and accident situations is maintained at an acceptable level for the entire planned service life of the plant.

4.2.3 Quality plan for the design and implementation of an electrical power system

A quality plan specifying the quality management measures to be used shall be drawn up for the design and implementation of Safety Class 2 and 3 electrical power systems. The plan shall cover the design, implementation and commissioning of a system as a whole as well as the quality objectives set for each phase. It shall be prepared in accordance with the 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 procurement.

The quality plan shall describe the interfaces of organisations participating in design, interface management, responsibilities for project quality functions in the various organisations involved as well as control of subcontractors. The quality plan shall describe the measures to ensure the correctness and completeness of documentation at the end of each project phase. Furthermore, the plan shall specify the change management measures to be used in the design and implemen-

tation of the system as well as the procedures used to change the quality plan.

The quality plan shall specify an appropriate procedure for review of intermediate results. 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 licensee shall consider the making of an independent assessment of how the quality plan for a Safety Class 2 electrical system is complied with. 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.

The suppliers of Safety Class 2 and 3 electrical systems and components shall employ a quality management system that complies with the appropriate standard and has been independently assessed.

4.3 Design process

4.3.1 General requirements

The organisation designing the nuclear power plant's electrical systems shall have sufficient expertise in corresponding tasks and the necessary know-how to comprehensively consider plant behaviour, its layout and characteristics. The distribution of responsibilities within the design organisation shall be unambiguous.

The safety-classified electrical power systems and components 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 different phases of the design process shall be described in the qualification plan (section 4.4).

The technical correctness of the design of a new plant's electrical power systems shall be demonstrated in the safety analysis report. The licensee shall ascertain the acceptability of the design by safety assessments based on own know-how, which is to be sufficiently profound.

The competence of the organisation responsible for designing electrical systems modifications at an operating nuclear power plant shall be demonstrated in the conceptual design plan.

Detailed requirements for a system's design organisation are given in section 2.3 of Guide YVL 2.0.

4.3.2 Requirement specification

The requirement specification of a safety-classified electrical system and component 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 operating lifetime. Safety-related requirements shall be consistent with the assumptions made in the safety analysis of the plant. The man-machine interface of a system, and the interfaces to the other systems of the plant, shall be clearly specified.

The plant-specific requirement specification of a Safety Class 2 and 3 electrical power system and component shall be sufficiently detailed for system validation as well as for the suitability analysis of the system's equipment in accordance with section 4.4.5

A licensee's quality management system shall present the procedure by which the correctness, completeness and consistency of the requirement specification of a Safety Class 2 electrical power system is validated independently of its writers.

4.3.3 Documentation

In the beginning of the design process of an electrical system and component, the documentation requirements and the documentation management procedures, which are applied since the start of the project, shall be specified. In the conceptual design phase, a clear and precise presentation method, understandable to experts in different fields, shall be used for the functional specification of the system.

The documentation describing the system shall be structurally clear and comprehensive.

The information included in it shall be up-to-date and sufficient to support the verification and validation of the system requirements.

The documentation of electrical systems and components shall be updated in connection with modifications. Guides YVL 1.4 and YVL 1.9 present quality management requirements for documentation management.

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 at the beginning of the design process of electrical power systems and components.

4.4 Qualification plan

4.4.1 General requirements

The systems and equipment at a nuclear facility shall be qualified for their intended use. Qualification verifies the conformity of the systems and their components with the requirements. The licensee shall draw up a special qualification plan to demonstrate the suitability of Safety Class 2 or 3 electrical power systems and components for their intended use. The plan shall include material from four areas: design and manufacturing process, tests, analyses, and operating experiences. In the drawing up of the qualification plan, a system's safety significance and the reliability requirements placed on it shall be considered.

The qualification plan shall describe the suitability analyses to be performed (section 4.4.5).

The qualification plan shall describe the procedure for independently assessing the acceptability of the qualification of Safety Class 2 electrical power systems. The assessment may be done by an expert in the licensee's employ, or by an organisation unit, not involved in design. For the qualification assessment of systems with nuclear safety significance, the use of an expert from an independent organisation shall be considered.

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.

General requirements for the qualification of safety-classified electrical power components for nuclear power plants are presented in IEC 60780 [2], among others.

4.4.2 Tests

Tests can be divided into tests performed during the design and manufacturing process and those performed for implemented electrical power systems and components. For the purposes of this guide, components mean both electrotechnical components and their potential field devices.

Tests performed during the design and manufacturing process include unit and system tests, among others. The purpose of these tests is to ensure that the electrical power systems or components fulfill the functional and performance requirements specified for them. These tests are completed by factory tests.

A test plan shall be drawn up for the tests to be performed for an electrical power system and its components. 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 components that could be detrimental for safety. The adequacy of tests performed for a Safety Class 2 system shall be justified and the test coverage analysed against the requirements specified for the system.

The compliance with requirements of an electrical power system or component shall be evaluated after factory tests and prior to transporting the system or component to the plant site. The project time schedule shall allow the making of any necessary design modifications after the factory tests in accordance with procedures commensurate with the safety- importance of the systems and components.

Tests required for the components of a system to be implemented are typically type tests that take into account component-specific environmental and operating condition requirements.

Final testing shall be performed onsite in the final operational environment. The testing shall demonstrate that electrical systems and components fulfill the functional and performance requirements specified for them.

General requirements for the pre-operational and start-up testing of a nuclear power plant and its supervision and control by STUK are described in Guide YVL 2.5.

Specific requirements for computer-based systems and components are given in subsection 4.6.5 of Guide YVL 5.5.

4.4.3 Safety analyses

Demonstration of the fulfilment of functional and performance requirements by analyses is part of the qualification of electrical power systems and components.

Safety Class 2 and 3 electrical power systems shall be subjected to

- a failure mode and effects analysis
- a common cause failure analysis
- an operating experience analysis
- a selectivity analysis to demonstrate the fulfilment of the selectivity requirements for electrical protection
- a safety analysis to demonstrate the fulfilment of safety requirements.

In addition, Safety Class 2 electrical power systems shall be subjected to a quantitative reliability analysis and Safety Class 3 electrical power systems to a quantitative reliability analysis according to their safety significance.

Specific requirements for computer-based systems and components are given in section 4.6 of Guide YVL 5.5.

4.4.4 Operating experience

Operating experiences shall be analysed for Safety Class 2 and 3 electrical systems and their components. The operating experiences shall be collected with a well-specified method. The comprehensiveness of the collection process, the length of the collection period and their significance for the reliability of the data shall be evaluated. The operating experiences shall be representative of the application under consideration. The use of operating experiences from other hardware or possible software versions, setups and operational profiles for the qualification of systems or components shall be justified.

4.4.5 Suitability analysis

General

A suitability analysis shall be performed for all Safety Class 2 and 3 electrical components and cables.

In the analysis, a component's functional and performance capabilities shall be assessed against the requirements specified for it. Its operational performance and environmental tests, electrotechnical dimensioning and protections, EMC characteristics, operational experiences and reliability in relation to safety importance shall be examined in particular. In addition, the supplier's capability to deliver the product in question as per section 4.2 (quality management) shall be described.

The suitability analysis shall be performed in accordance with instructions in the licensee's quality management system. The suitability analysis report shall include the observations made, a justified conclusion about the acceptability of the product and what conditions pertain to the validity of its approval. The licensee shall always justify his conclusions about the acceptability of the suitability analysis.

A suitability analysis performed for an electrical component implemented by programmable technology shall cover the assessment of software and hardware. Further software requirements are given in section 4.6 of Guide YVL 5.5.

Specific requirements

The suitability analysis shall contain a detailed assessment of the quality of design and manufacturing of the below electrical components and cables

- Safety Class 2 electrical components and cables
- electrical components and cables having to do with Safety Class essential accident instrumentation (NRC Regulatory Guide 1.97, cat. 1[7]
- electrical components and cables needed in accidents for which specific environmental qualification requirements have been set.

The fulfillment of the requirements of the standards and applications, which form the design basis of these products, shall be demonstrated by tests, analyses and practical type tests. In addition, an assessment of manufacturing quality shall be interlocked with an assessment of product quality management. Specific attention shall be paid to measures to assure that products in batch production correspond to the analysed product.

Requirements applicable to those making the suitability analysis

The suitability analyses of Safety Class 2 and 3 electrical components and cables may only be carried out by a STUK-approved organisation unit and an expert, who is not the designer, manufacturer or supplier of the electrical components to be analysed, or who is not the authorised representative of any of the aforementioned parties.

The licensee shall apply to STUK in writing for approval of the organisation unit and expert performing suitability analyses for the components and cables in question.

The application shall include at least the below attachments

- a description showing the organisational position and independence of the unit and individuals performing the suitability analysis
- a description of those performing the analysis, giving their education, work experience and competence as well as for what analyses the approval is sought for
- a description of the methods used in and the essential instructions pertaining to the assessments
- further clarifications, if necessary.

The makers of the suitability analysis shall have sufficient professional skill and experience as well as competence proven in practice to assess the fulfilment of technical requirements on electrical components in nuclear power plants, and on quality management systems. This competence shall be actively developed such that international operating experiences and research results can be considered in making suitability analyses.

An approval to perform suitability analyses granted by STUK is valid for five years at a time at most. A renewal of the approval shall be applied for from STUK not later than three months prior to its expiration, if necessary.

4.5 Receiving, installation and commissioning

4.5.1 General

The receiving, installation and commissioning procedures for electrical power systems and components presented in the licensee's quality management system shall describe the tasks, division of duties, and responsiblities of organisations responsible for each function as well as the documentation procedures and the scope of inspections.

4.5.2 Receiving

A receiving inspection shall be performed on safety-classified electrical components and possible related software. The licensee shall ascertain that the components and their software are as designed and that their quality control documents are acceptable. In addition, it shall be ascertained that the components have not become damaged during transport. Inspections and tests relating to the receiving inspection shall be performed acceptably. The receiving inspection shall be appropriately documented.

4.5.3 Installation

The licensee shall perform an installation inspection on installed safety-classified electrical components. The licensee shall thus ascertain the appropriateness of the installations. A schedule for installations and their documentation shall be determined as well as the scope, measures, responsibilities and recording of post-installation checking of installations and couplings, and functional tests.

4.5.4 Commissioning

The licensee shall perform a commissioning inspection on installed and modified safety-classified electrical systems and components. The licensee shall thus verify that installed components and systems comply with accepted plans and that this has been ascertained by sufficient inspections and tests. It shall also be verified that any shortcomings and defects detected in the inspections have been corrected. In addition,

it shall be ascertained that any changes made during commissioning were implemented following the system's established change management procedures.

Implementation of the licensee's quality management requirements shall be verified during commissioning inspections and it shall be ascertained that nothing prevents commissioning. It shall be ensured by the inspections that electrical power systems, components and their installations fulfill the environmental and operating condition requirements set by their place of use. The items must have acceptably passed their installation inspections and receiving tests and no such shortcomings are allowed in commissioning-related inspection protocols as would prevent commissioning. In case any minor non-conformities are observed to a STUK-approved suitability assessment, or to pre-inspection documents, those shall be brought to the attention of STUK's inspectors. Designers are to draw up a non-conformity report of any significant deviations and submit it STUK for approval. It shall also be ascertained that any remarks made during STUK's earlier regulatory activities have been appropriately taken care of.

The licensee shall annually send to STUK for information a report of all commissioning inspections performed and their results.

The commissioning inspections of safety-classified electrical power systems and components may only be performed by a STUK-approved organisation unit and inspector, independent of design. The licensee shall apply to STUK in writing for approval of the unit and inspector in question for the task.

The application shall include at least the below attachments

- a description showing the organisational position and independence of the unit and individuals performing inspections
- a description of those performing the inspections, giving their education, work experience and competence as well as for what inspections the approval is sought for
- a description of the methods used in and the essential instructions pertaining to the inspections
- further clarifications, if necessary.

The inspectors shall have sufficient professional skill and experience as well as appropriately qualified equipment, facilities and methods for performing the inspections.

A STUK-granted authorisation to perform commissioning inspections is valid for five years at most at a time. When needed, an application for its renewal shall be submitted to STUK not later than three months prior to the authorisation's expiration.

4.6 Specific requirements for computer-based systems and components

Specific requirements for computer-based electrical power systems and components are given in section 4.6 of Guide YVL 5.5.

5 Ageing management

In accordance with section 3.15 of Guide YVL 1.0, in nuclear power plant design, the service life and the effect of their 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.

In accordance with section 2.2 of Guide YVL 2.0, 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 nuclear power plant's electrical power systems and components, their installations and cablings and to anticipate the need for replacement. The programme's safety objective is to assure that the performance of the plant's safety functions is maintained at an acceptable level for the plant's entire designed service life. The different ageing mechanisms related to various components, their significance and detection methods shall be considered when planning the programme. The

programme shall cover the methods for collecting and analysing the failure data of the systems and components to detect possible changes in the failure rates and to anticipate the need for replacement. The programme shall cover also possible other analyses and testing to assess the ageing of systems and components. In ageing management, also failure data form other plants and vendors shall be made use of, to the extent possible. The ageing management programme shall include all systems and components important to safety, regardless of their safety class. The choice of systems and components to the programme shall be justified in the programme. Specific attention is to be paid to the condition of components needed in accidents as well as the condition of their cables and installations. The scope and efficiency of the ageing management programme shall be assessed regularly.

The ageing management programme of the electrical power systems and components of the nuclear power plant shall also consider the ageing of the technology of systems and components 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. The annual ageing management report shall be sent to STUK for information.

To monitor their ageing, the various types of cable of safety-classified electrical and I&C components inside the reactor containment shall undergo mechanical and electrical inspection at least every five years. The licensee shall regularly evaluate the adequacy of the cable monitoring programme, taking into consideration e.g. the results of cable inspections, operating experiences and possible significant changes in the environmental conditions of the cables. If need be, the monitoring programme shall be enhanced and extended to cover cable types in use outside the containment. An report of the ageing monitoring inspections shall be drawn up and sent to STUK for information.

STUK controls the implementation and results of the licensee's ageing management programme for electrical power systems and components also in conjunction with the periodic inspection programme.

6 Control by the Finnish Radiation and Nuclear Safety Authority

6.1 General principles

General requirements applicable to the preliminary inspection of systems are set out in Guide YVL 2.0. According to it, systems approval is to be carried out as part of the review of the preliminary and final safety analysis reports. The preliminary safety analysis reports of Safety Class 2 and 3 and, for applicable parts, of Safety Class 4 systems, shall contain analyses required in section 6.2 of the preliminary safety analysis report and, correspondingly, in section 6.3 of the final safety analysis report.

The pre-inspection of an electrical power systems modified or added during plant operation is to be based on a separate conceptual design plan for the modification and pre-inspection documentation. According to the general principle applied in the control of electrical power 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.

STUK's approval shall be obtained for modifications to Safety Class 4 and Class EYT (non-nuclear) systems if the modifications affect the implementation of the design principles set forth in Guide YVL 1.0.

The scope and detail of the pre-inspection documentation of a system modification, which is to be provided in accordance with section 3.4.1 of Guide YVL 2.0, may vary according to the modification's safety significance. A conceptual design plan is not required if the modification is so minimal that it does not essentially alter any of the system's design principles, operating principles or tasks.

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 and 3 electrical components and cables shall be sent to STUK for approval or for information in accordance with section 6.4.

In addition, STUK assesses the quality management systems of vendors and also how the licensee assesses the operation of their own and their suppliers' quality management systems.

6.2 Conceptual design plan

The conceptual design plans and the preliminary safety analysis reports of Safety Class 2 and 3 and, for applicable parts, Safety Class 4 electrical power systems shall contain the below descriptions:

- system design principles and bases
- system functions, operating principles, essential design parameters and 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 section 3.3 of Guide YVL 4.3)
- preliminary safety classification of system functions and equipment
- the operating and environmental conditions and stresses of the system and the consequent design requirements
- requirements and dependencies arising from other systems - e.g. support systems - and the controlling process
- system interfaces, including a possible man machine interface and interfaces with other electrical and 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
- licensee's own safety assessment in accordance with section 2.3 of Guide YVL 2.0.

Class EYT systems shall be described to the extent necessary for assessment of the plant's overall operations.

A system's design bases shall list the guidelines and standards according to which the system is designed.

A qualification plan in accordance with section 4.4, and earlier qualifications to be utilised in the system's qualification process, shall be included in the preliminary qualification plan drawn up in the conceptual design phase. The preliminary qualification plan shall include a schedule on the sending 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 system modifications affect probabilistic safety analyses (PSAs).

6.3 System pre-inspection documents

The pre-inspection documents of Safety Class 2 and 3 electrical power systems and, for applicable parts, those and the final safety analysis report of Safety Class 4 electrical power systems shall include the below descriptions:

- detailed system design bases
- detailed description of system operation and configuration
- system environmental conditions and stresses, and consequent design requirements
- electrotechnical dimensioning of system and its associated components
- technical description of a system's electrical protection and selectivity analysis
- the location, segregation and protection (fire compartments, physical protection) of subsystems important to safety
- impact on the nuclear power plant's other systems and dependencies from other systems (e.g. cooling and auxiliary power supply) as well as prevention of fault propagation
- a probabilistic assessment of the system's impact on plant safety
- quality plan
- qualification plan
- qualification results documentation
- designer's safety assessment of how the system meets its safety requirements
- licensee's own safety assessment in accordance with section 2.3 of Guide YVL 2.0

- system-specific requirements in the Technical Specifications
- potential information security plan
- other necessary descriptions.

Class EYT systems shall be described to the extent necessary for evaluation of the plant's overall operations.

The pre-inspection documents of systems are submitted to STUK for approval in stages such that the qualification results 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 specifications of Safety Class 2 and 3 electrical systems 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 an analysis of the coverage of the self-diagnostics.

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

- principal design diagrams of main and auxiliary electrical power supplies
- principal and functional diagrams representing the control, measurements, regulation, I&C, interlocking, etc of the system
- a summary of the service data of the measurements (symbol, type, measurement range, protection and alarm limits)
- of computer-based systems, also architecture and flow diagrams for software, potential software tools and their functional description.

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 to be sent to STUK for information.

The qualification plan shall include the data presented in section 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.

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 requirements specification are demonstrated as well as the effect on PSA.

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

As regards extensive plans with a significant bearing on nuclear safety, 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 reviews 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 Component suitability analysis

The suitability analyses of Safety Class 2 and 3 electrical components and cables may only be carried out by an organisational unit and expert authorised by STUK at the application of the licensee in accordance with section 4.4.5.

The suitability analyses of the below electrical components are to be submitted to STUK for approval:

- Safety Class 2 electrical components and cables
- electrical components and cables relating to Safety Class 3 essential accident instrumentation (NRC Regulatory Guide 1.97, cat. 1 [1]
- electrical components and cables needed in accidents for whose environmental qualification special requirements have been set.

The suitability analyses of other Safety Class 3 electrical components and cables, and those

needed in accidents, may be sent to STUK for information without the below reference material.

In conjunction with the suitability analysis, the following data shall be submitted on each component:

- plant and application specific requirement specification
- design bases
- functional description and configuration as well as drawings
- vendor data
- quality plan.

The description of a component's design bases shall contain at least the following data:

- safety class
- location and task within the electrical power system
- electrotechnical dimensioning
- electrical protection
- environmental conditions (e.g. temperature, humidity, radiation, pressure and vibrations)
- operating conditions (e.g. power, voltage, current and frequency ranges)
- electromagnetic compatibility in the operating environment
- seismic resistance.

The guidelines and standards to be applied in the design, manufacture, testing and installation of components shall be stated in the design bases of each component. Any deviations from applicable standards and guidelines shall be presented and justified in accordance with section 4.1.

The operation and construction descriptions as well as drawings of components shall be sufficient to facilitate the evaluation of the suitability analysis. Descriptions of potential software tools shall be incorporated in the component descriptions.

Vendor or manufacturer data shall include organisation, competence and assessment of quality system and its outcome.

6.5 Manufacturing and factory tests

STUK controls the manufacturing of electrical power systems and components subject to pre-inspection by inspections at its discretion. During the inspections STUK must be provided with the opportunity to check the manufacturing processess and quality management systems of the manufacturer, the documents on quality control produced during manufacturing and those referred to in the qualification plan, among others.

For the purpose of potential inspections by STUK at the premises of the vendors and suppliers, STUK shall be sent the testing schedules of systems and components (performance and functional tests) for information well in advance. The testing programmes of factory tests, which STUK says it follows, shall be submitted for information.

6.6 Installation

STUK controls the installation of Safety Class 2 and 3 electrical power systems and components at its discretion.

If STUK so requests, the installation schedule of Safety Class 2 and 3 electrical power systems and components subject to pre-inspection shall be sent to STUK for information prior to the commencement of installation. During the inspection the licensee is to present STUK with the plans and instructions for the inspections as well as the result documentation.

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

6.7 Commissioning inspections

STUK controls the pre-operational and start-up testing of the nuclear power plant and the system tests of electrical power systems in accordance with Guide YVL 2.5. STUK witnesses onsite testing and system tests at its own discretion. The test programmes of Safety Class 2 and 3 electrical power systems shall be submitted to STUK for approval and their schedules for information well in advance of the commencement of testing. The result reports of Safety Class 2 and 3 electrical power systems shall be submitted to STUK for approval. During the pre-inspection of Safety Class 4 systems STUK specifies which system's commissioning programmes, test schedules and result documentation shall be submitted to STUK for information.

During the pre-inspection of electrical pow-

er systems STUK specifies the systems whose commissioning inspections it conducts. During STUK's commissioning inspections the licensee shall present STUK with the results of its own commissioning inspections conducted in accordance with section 4.5.4 plus the related result documents. The commissioning inspections of safety-classified electrical power systems and components may only be conducted by an organisation unit and expert authorised by STUK upon application by the licensee.

6.8 Equipment quality management

The licensee shall draw up general plans for quality control in the design, manufacturing, receiving, installation and commissioning phases of Safety Class 2 and 3 components in accordance with section 4.2. The plans shall be submitted to STUK for approval prior to the aforementioned phases.

6.9 Plant operation

During the operation of nuclear facilities STUK controls electrical power systems and components by inspecting the repairs and modifications of systems and components. At the same time STUK assesses the operations of the licensee and the efficiency of their procedures in assuring the reliable operation of the systems and components. 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 to, design and maintenance of electrical systems and equipment
- quality management, equipment procurement, spare parts management and receiving inspections
- the operability and condition of electrical power systems and components is ensured by periodic testing
- assessment of the environmental and operating conditions of components
- assessment of equipment ageing
- maintenance of the accuracy of measuring equipment
- equipment surveillance, failure data, failure data gathering systems and analyses
- appropriate component preventive maintenance, repair and spare parts service.

The periodic testing programmes of safety-classified electrical power systems and components and those subject to the Technical Specifications, the procedures to be followed during testing and condition-monitoring instructions shall be sent to STUK for information. A recording of the test results shall be kept at the plant site.

The acceptability of requirements pertaining to the availability of safety-classified electrical power systems and components, 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 components are properly monitored by measurements at relevant locations and that measures to review maintenance programmes, service life assessments and qualifications are taken, where necessary. STUK checks onsite the measurement results in the extent it deems necessary.

STUK monitors the realisation and results of the licensee's programme to monitor the ageing of electrical power systems and components in connection with the periodic inspection programme, among others. The results of ageing management shall be presented in a report every year, which is to be sent to STUK for information in accordance with chapter 5.

STUK controls the licensee's commissioning inspections. For this purpose, the licensee shall yearly submit to STUK for information by the end of February a description of the commissioning inspections it has conducted plus their results.

6.10 System and component modifications during operation

Guide YVL 1.8 presents requirements pertaining to modifications at nuclear facilities.

Section 3.4 of Guide YVL 2.0 lists the documents, which apply to systems modifications at operating nuclear power plants, that are to be sent to STUK.

STUK conducts the pre-inspection of modifications to safety-classified electrical power systems in the extent specified in section 6.1. STUK reviews the suitability assessments of electrical components and cables in accordance with section 6.4.

In connection with the pre-inspection of electrical power systems, STUK defines what systems' commissioning inspection it conducts. The performance of the inspection by STUK shall be requested for in writing well in advance of the inspection date. The inspection shall be conducted prior to plant start-up from annual maintenance or, during plant operation, prior to system commissioning.

During system commissioning inspections conducted by STUK, the licensee shall present to STUK the results of inspections it has conducted in accordance with section 4.5.4 and also the related result documents.

Safety Class 2 and 3 modifications may only be implemented after STUK has approved a system's pre-inspection documentation and when requirements pertaining to work possibly required in the approval have been fulfilled. STUK's approval shall be obtained for modifications to Safety Class 4 and Class EYT (non-nuclear) systems if they have a bearing on the realisation of the design bases referred to in Guide YVL 1.0. Such modifications may only be implemented after STUK's approval has been obtained.

The test operation programmes of modified system sections and components shall be drawn up such that the impact of the modifications is appropriately tested by means of test programmes corresponding as well as possible to the original test programmes. Prior to a system's commissioning, the licensee shall apply for approval for any changes needed to the Technical Specifications. Prior to a system's commissioning, its operating instructions shall be updated to correspond to the modified system. The maintenance instructions of the system and its components shall be updated without delay during the modification.

After the system's commissioning, all 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.

Integration tests

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

Self-diagnostics

A system or a 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 electrical power systems or components to fulfil the functional and performance requirements imposed on them in all their operating conditions and design basis environmental conditions.

Field device

Field devices are actuators or measuring devices active in a process, which can be used for example for measuring, control, regulation or protection.

Operational conditions

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

Normal operational conditions

Normal operational conditions mean the operation of a nuclear power plant in accordance with the Technical Specifications. They also include system and component 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 component 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 programmable 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, definiable system unit that is often detachable. It can also be an independent piece of equipment containing computer-based technology.

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.

PSA

PSA stands for a Probabilistic Safety Assessment.

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 for 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".

Electromagnetic compatibility (EMC)

EMC is the capability of electrical power systems or equipment to function satisfactorily in their electromagnetic environment without being susceptible to disturbances and such that they does not cause excessive electromagnetic disturbances to any systems or equipment in their environment.

Auxiliary system

An auxiliary system facilitates a system's major function e.g. by feeding electrical power, by cooling, lubricating or regulating.

Systems, structures and components important to safety

Structures, systems and components important to safety are such that

- their malfunction or breakage may significantly increase the radiation exposure of the plant's workers or the environment
- they prevent the occurrence and propagation of transients and accidents
- they mitigate the consequences of accidents.

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 performing 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, components or structures in consequence of the same single failure or cause, either simultaneously or within a short period of time.

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. IEEE 308-2001, IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations.
2. IEC 60780, Nuclear Power Plants – Electrical Equipment of the Safety Systems – Qualification, Second edition 1998-10.
3. IEEE 741-1997, IEEE Standard Criteria for the Protection of Class 1E Power Systems and Equipment in Nuclear Power Generating Stations.
4. IEEE 765-2002, IEEE Standard for Preferred Power Supply (PPS) for Nuclear Power Generating Stations.
5. KTA 3701 (6/99), General Requirements for the Electrical Power Supply in Nuclear Power Plants.
6. IAEA Safety Standard Series DS303, 2/2004, Design of Emergency Power Systems for Nuclear Power Plants.
7. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.97, Instrumentation for Light-Water-Cooled Nuclear Power Plants To Assess Plant and Environs Conditions During and Following an Accident, revision 3, May 1983.
8. IEEE 384-1992, IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits.
9. Standard SFS-EN ISO 9000, Quality management systems. Fundamentals and vocabulary, 12 March 2001.