Safety Standards

of the
Nuclear Safety Standards Commission (KTA)

KTA 3501 (2015-11)

Reactor Protection System and Monitoring Equipment of the Safety System

(Reaktorschutzsystem und Überwachungseinrichtungen des Sicherheitssystems)

The previous versions of this safety standard were issued in 1977-03 and 1985-06 .

If there is any doubt regarding the information contained in this translation, the German wording shall apply.

Editor:
KTA-Geschaeftsstelle
c/o Bundesamt fuer kerntechnische Entsorgungssicherheit (BfE)
Willy-Brandt-Str. 5 • 38226 Salzgitter • Germany
Telephone +49 (0) 30 18333-1621 • Telefax +49 (0) 30 18333-1625

KTA SAFETY STANDARD

November 2015	**Reactor Protection System and Monitoring Equipment of the Safety System**	KTA 3501

Previous versions of the present safety standard: 1985-06 (BAnz No. 203 a of October 29, 1985)
1977-03 (BAnz No. 107 of June 11, 1977)

Contents

KTA-Geschaeftsstelle c/o BfE, Willy-Brandt-Str. 5, D-38226 Salzgitter, Germany or kta-gs@bfe.bund.de

Comments by the Editor:

Taking into account the meaning and usage of auxiliary verbs in the German language, in this translation the following agreements are effective:

shall	indicates a mandatory requirement,
shall basically	is used in the case of mandatory requirements to which specific exceptions (and only those!) are permitted. It is a requirement of the KTA that these exceptions - other than those in the case of **shall normally** - are specified in the text of the safety standard,
shall normally	indicates a requirement to which exceptions are allowed. However, exceptions used shall be substantiated during the licensing procedure,
should	indicates a recommendation or an example of good practice,
may	indicates an acceptable or permissible method within the scope of the present safety standard.

Basic Principles

(1) The safety standards of the Nuclear Safety Standards Commission (KTA) have the objective to specify safety-related requirements, compliance of which provides the necessary precautions in accordance with the state of the art in science and technology against damage arising from the construction and operation of the facility (Sec. 7 para. 2 subpara. 3 Atomic Energy Act - AtG) in order to achieve the fundamental safety functions specified in the Atomic Energy Act and the Radiological Protection Ordinance (StrlSchV) and further detailed in the Safety Requirements for Nuclear Power Plants as well as in the Interpretations of the Safety Requirements for Nuclear Power Plants.

(2) The tasks for the instrumentation and controls are derived from requirements of systems technology. In turn, the requirements for systems technology and the respective categorization are derived from the associated safety levels. A correlation of the categories of the I&C functions and the safety levels is presented in SiAnf-Interpretations.

(3) Based on SiAnf and SiAnf-Interpretations, the present safety standard specifies the requirements of the reactor protection system, the protective limitation modules, the process-variables limiting modules and the monitoring equipment of the safety system must fulfill.

(4) The documents for the reactor protection system and the monitoring equipment of the safety system required for the examination in the nuclear licensing and surveillance procedure detailed in ZPI, the “Compilation of the information required for review purposes under licensing and supervisory procedures for nuclear power plants”.

(5) In Section 2.2, the present safety standard categorizes the information and control (I&C) functions of the reactor protection system, of the protective limitation modules, of the process-variable limiting modules and of the monitoring equipment of the safety system are specified.

(6) The present safety standard is supplemented by the safety standards KTA 3503 through KTA 3507.

(7) The requirements specified in Section 8 for the electrical power supply are supplemented by the safety standards KTA 3701 through KTA 3705.

(8) The requirements specified in Section 7 for the ventilation system with regard to the I&C system important to safety are supplemented by the safety standard KTA 3601

(9) The requirements for proving the stability of electrical equipment under design-basis accident conditions are specified in the safety standards KTA 2101.3, KTA 2201.4 and KTA 3706.

(10) Regarding quality assurance, the requirements apply that are specified in safety standard KTA 1401, and regarding ageing management, the requirements apply that are specified in safety standard KTA 1403.

(11) In the present safety standard, it is presumed that conventional requirements and technical standards (e.g., Accident Protection Requirements, DIN standards, VDE regulations) are adhered to under consideration of the safety-related requirements specific to nuclear power plants.

1 Scope

(1) This safety standard applies such equipment of the instrumentation and control system important to safety in stationary nuclear power plants that perform instrumentation and control functions in Category A or Category B as specified in Section 2.2.

(2) This safety standard specifies requirements for the structure, design, equipment quality, installation and testing of equipment that perform instrumentation and control functions in Category A or Category B as specified in Section 2.2. It compiles design criteria, requirements regarding quality and quality assurance and requirements regarding the functionality of the instrumentation and controls important to safety for equipment that perform instrumentation and control functions in Category A or Category B as specified in Section 2.2.

Note:

Requirements with regard to safety-related hazard alarms (Class S alarms) and to mechanical-equipment protective devices whose signals have priority over signals from Cat A equipment are dealt with in separate independent sections.

(3) In addition, the present safety standard also specifies requirements for the logging and servicing equipment used for Cat A and Cat B equipment as well as for Class I alarm equipment.

(4) Not within the scope of the present safety standard are the electrical drives, the power cables, the switchgear feeder branches nor the associated control circuits.

Note:

The requirements for this equipment are specified in safety standards KTA 3504 and KTA 3701 through KTA 3705.

2 Terms and Definitions

2.1 Definitions

The words defined in this section are given here in alphabetical order:

Active safety system equipment	(61)
Actuation signal	(12)
Binary monitor	(72)
Cat A equipment	(1)
Cat B equipment	(16)
Class I alarm	(25)
Class II alarm	(26)
Class S alarm	(24)
Common-mode failure	(11)
Comparator	(69)
Component	(36)
Computer-based module	(30)
Computing circuit	(46)
Control Level	(65)
Critical load test	(31)
Design-basis accident (DBA)	(66)
Device or module	(27)
Dissimilar I&C equipment	(17)
Diverse I&C equipment	(18)
Erroneous actuation	(20)
Failure	(10)
Failure (breakdown)	(70)
Firmware	(21)
Full protective action	(58)
Functional group control	(23)
I&C equipment	(38)
I&C function	(39)
Individual drive control	(19)
Initiation channel	(4)

(1) Cat A equipment

Cat A equipment is the equipment assigned to perform instrumentation and control (I&C) functions in Category A.

(2) Mechanical-equipment protection

The mechanical-equipment protection is a device assigned to a mechanical equipment to help protect this equipment against operating conditions for which this mechanical equipment was not designed or intended.

(3) Initiation level

The initiation level is that part of the Cat A, Cat B or Cat C equipment in which all of the associated initiation-channel groups are combined.

(4) Initiation channel

The initiation channel is a device required for the monitoring and conditioning of process variables and for the creation of an initiation signal. An initiation channel comprises all modules beginning with the sensors and ending at the output of a limit value monitor.

(5) Initiation-channel group

The initiation-channel group is a system of several initiation channels intended for the redundant monitoring of process variables and the creation of redundant initiation signals.

(6) Initiation criterion

The initiation criterion is that condition, under which a protective action is initiated.

(7) Initiation signal (trip signal)

The initiation signal is the output signal of an initiation channel and the input signal to the logic level.

(8) Response delay

The response delay is the entirety of the characteristics of a system that determines the delay time between the onset of the input signal and the output of the output signal.

(9) Non-coincidence monitor

The non-coincidence monitor is a device that monitors binary signals with respect to their unambiguity.

(10) Failure

A failure is the loss of the ability of a device to perform the required function.

Note:

The event “failure” marks the point in time of the transition from a correct to a defective state. A failure may, but does not necessarily occur simultaneously with a failure (breakdown). For instance, a mechanical equipment that has not been demanded action may have failed; its failure (breakdown) will only become evident when it is demanded and cannot perform its function.

(11) Common-mode failure

The common-mode failure is a failure due to the same cause.

Notes:

(1) A common-mode failure of I&C equipment can manifest itself as a simultaneous failure of multiple equipment or as their individual failures in short sequence of each other all due to the same cause.

(2) A common-mode failure can be caused by, e.g., wrong design, faults in a production series, incorrect operating procedure, flooding or fire in the plant.

(12) Actuation signal

An actuation signal is the output signal of the logic level or of the control level that actuates protective actions.

(13) Specified normal operation

A specified normal operation is the operation for which a plant, regarding its technical purpose, is designed and suited; it encompasses the operating conditions and procedures

a) during a functioning condition of the equipment (undisturbed operating condition, normal operation),

b) of abnormal operation (disturbed operation, malfunction) as well as

c) during maintenance procedures (inspection, servicing, repair).

(14) Operational limitation

An operational limitation is a device that limits process variables to specified values with the goal of increasing plant availability.

(15) Operational interlock

An operational interlock is a device for the operational control or operational protection of components or systems.

(16) Cat B equipment

Cat B equipment is the equipment assigned to perform instrumentation and control (I&C) functions in Category B.

(17) Dissimilar I&C equipment

Dissimilar I&C equipment are characterized by being sufficiently dissimilar or unalike to other I&C equipment regarding hardware, software, development tools, development teams, fabrication, testing, and maintenance. Dissimilarity is one aspect of diversity that applies specifically to computer-based or programmable devices.

Notes:

(1) The objective is to design and construct independent systems and partial systems such that their indispensable safety-related functions are sustained even in the case of a postulated systematic failure (breakdown) of one of the independent systems or partial systems. To this end, the dissimilarity of the essential characteristics regarding to control this failure (breakdown) must be demonstrated.

(2) The assessment regarding the sufficiency of dissimilarity may also result in allowing individual aspects to be similar.

(18) Diverse I&C equipment

Diverse I&C equipment are characterized by two or more operational equipment for the achievement of a prescribed function being different in their physical or technical design.

(19) Individual drive control

An individual drive control is the control equipment allocated to an individual drive.

Note:

In this safety standard, the requirements are specified for the individual drive controls of the Cat A and Cat B equipment (including the coupling relays). The requirements for the connected control circuitry are specified in safety standard KTA 3705.

(20) Erroneous actuation

An erroneous actuation is the initiation of an actuation signal that was not warranted by the plant condition.

(21) Firmware

Firmware is the not freely-programmable software installed in a device (embedded software), this software delivering defined device-specific functions. If the firmware is modified the associated device is considered as being a modified device.

(22) Secondary failure (cascading failure)

A secondary failure is a subsequent failure indirectly caused by a design-basis accident or by a postulated initiating event.

(23) Functional group control

A functional group control is an automatic control equipment for functionally related parts of a specific process by which the mutual actuation of the drives with their individual drive controls is necessary for the sequential flow of this process.

Note:

This term was used in version 1985-04 of this safety standard. Due to the newly introduced categorization specified in Section 2.2, this term has become obsolete. Nevertheless, for better understanding, it is kept in this Section 2.1.

(24) Class S alarm

The Class S alarm (safety-hazard alarm) is a signal from a protection-system subunit upon the occurrence of which, it is mandatory for the responsible operating personnel to initiate a protective action within a prescribed period of time.

(25) Class I alarm

The Class I alarm is a signal that alerts the operating personnel of a fault existing in the safety system.

(26) Class II alarm

The Class II alarms encompass all signals that alert the operating personnel of existing faults and that are not Class S and Class I alarms.

(27) Device or module

A device or module is an arrangement of components or parts which performs a specific function.

Note:

Devices consist of hardware and, if applicable, software. An I&C module is an exchangeable device with a standardized interface.

(28) Not-programmable module

A not-programmable module is comprised of individual not-programmable subunits.

(29) Programmable module

A programmable module is comprised of at least one programmable subunit.

Note:

Programmable subunits are, e.g., field-programmable gate arrays (FPGA), programmable logic devices (PLD) and application-specific integrated circuits (ASIC).

(30) Computer-based module

A computer-based module is comprised of at least one processor.

Note:

The module's function is stored in the data memory of the processor.

(31) Critical load test

The critical load test is a test by which the behavior of the module is determined under the most unfavorable combination of operating and ambient conditions for which the module was designed.

(32) Limit value monitor (bistable trip unit)

A limit value monitor is a device which compares the value of a safety variable with a fixed or variable limit value. When the value exceeds or drops below the limit value, the output signal changes abruptly.

(33) Limit value of a limit value monitor

The limit value of a limit value monitor is the value (trip setpoint) preset in the limit value monitor.

(34) Inspection

Inspection comprises measures that are taken to ascertain and assess the actual condition of devices (cf. DIN 31051).

(35) Maintenance

Maintenance comprises all measures for preserving and restoring the required condition as well as all measures for ascertaining and assessing the actual condition. Maintenance is divided into preventive maintenance (with the associated elements of inspections, especially in-service inspections, and servicing) and repair (exchanging or repairing).

(36) Component

A component is a structurally or functionally separate part of a system that is still able to perform independent partial functions.

(37) Instrumentation and controls (I&C)

The entirety of I&C equipment necessary for performing I&C functions.

(38) I&C equipment

I&C equipment are the modules and systems necessary for performing I&C functions and include the sensors and all parts of the individual drive controls dedicated to the actuation of protective actions. I&C equipment comprise both the automatic equipment as well as the equipment required for the process control by an operator.

(39) I&C function

The I&C function is the function of measuring, controlling, monitoring, recording and protecting a process or an equipment.

(40) Logic level

The logic level is that part of the Cat A equipment in which trip signals are interlinked and the evaluation of initiation criteria is performed.

(41) Logic gating (linking)

The logic gating is a procedure by which several binary signals are combined to obtain a single resulting signal.

Note:

A logic gating is, e.g., AND, OR.

(42) Logic rating (coincidence logic)

The logic rating is a procedure by which redundant signals are combined to create a resulting signal that has a greater reliability than that of the individual signal.

Note:

A logic rating is, e.g., a 2-out-of-3 coincidence.

(43) Phase model

A phase model is a model used for defining and structuring the sequentially executed sections of a development process with a description of the relationship between the individual sections (phases) and includes their verification and validation.

(44) Process variable

A process variable is a chemical or physical quantity that can be measured directly within the process.

(45) Reactor protection system

The reactor protection system is that part of the safety system which monitors and processes the values of safety-related process variables essential for the initiation of protective actions to prevent inadmissible loads and essential for the detection of design-basis accidents, and which actuates protective actions such that the condition of the nuclear power plant is kept within safe limits. As part of the safety system, the reactor protection system comprises all devices related to data acquisition and signal processing, to the logic level and to those parts of the individual drive controls dedicated to the actuation of protective actions. The I&C functions of the reactor protection system are typically categorized as Category A.

Note:

The number and type of the process variables to be measured and evaluated by the reactor protection system and the resulting safety variables, the specifications of their limit values as well as the specification of number and type of the protective actions are all results of the design-basis accident analysis.

(46) Computing circuit

The computing circuit is a module which calculates a not directly measurable safety variable from the values of one or more process variables.

Note:

A computing circuit is, e.g., the circuit for determining the reactor period from the neutron flux or for determining the departure-from-nucleate-boiling from the values of pressure and temperature.

(47) Redundancy

The redundancy is the existence of more operational technical devices than are necessary for fulfilling the anticipated functions.

Note:

In this safety standard, the requirement for redundancy is considered as being fulfilled if similar technical devices are employed.

(48) Redundancy group

The redundancy group is the aggregation of modules correlated to one redundancy while maintaining a sufficient independence of the mutually redundant modules.

(49) Non-interaction

The non-interaction of a device is its characteristic that the input signal to the device is not inadmissibly influenced by faults at its output.

Notes:

(1) Faults can be, e.g., short circuit, overvoltage, short-to-ground, open circuit.

(2) 'Not inadmissibly influenced' implies that despite a possibly present interaction the required task can still be performed.

(50) Protective action

A protective action is the actuation or operation of active safety system equipment that are necessary for the control of design-basis accidents.

(51) Safety-oriented protective action

The safety-oriented protective action is a protective action which, in the event of its actuation, will not prevent any other protective action and will always lead to a process-technologically safe condition.

Note:

In this sense, the reactor scram is a safety-oriented protective action.

(52) Not clearly safety-oriented protective action

The not clearly safety-oriented protective action is a protective action which, in the event of its actuation, either can prevent other protective actions or, depending on the condition of the power plant, will not always lead to a process-technologically safe state.

(53) Protective limitation

The protective limitation is a module which actuates such protective actions that cause the value of the monitored safety variable to be returned to a value at which it is permissible to continue specified normal operation.

Note:

This term was used in version 1985-04 of this safety standard. Due to the newly introduced categorization specified in Section 2.2, this term has become obsolete. Nevertheless, for better understanding, the term is kept in this Section 2.1.

(54) Partial protective action

The partial protective action is the actuation or the operation of one or of several mutually redundant components of an active subunit of the safety system, these components being necessary to influence the course of design basis accidents and to reduce damaging effects.

(55) Protective subsystem

The protective subsystem is that part of the Cat A equipment which is needed for actuating a partial protective action.

Note:

A protective subsystem is, e.g., that part of the Cat A equipment that is necessary for starting up one of several mutually redundant pumps.

(56) Protection bypass

The protection bypass is a measure by which a function of the Cat A equipment is modified depending on the operational condition.

N o t e :

Protection bypasses are put into effect at the logic level or at the control level. One example of a protection bypass is the start-up prohibition (a reactor trip in case of impermissible neutron flux measurement signals during reactor start-up).

(57) Protection-system subunit

The protection-system subunit is a specific part of the Cat A equipment which, because of its operating principle, forms a unit.

N o t e :

Examples of protection-system subunits are, e.g., initiation level, logic level, control level.

(58) Full protective action

The full protective action is the actuation or operation of an active safety system equipment which, by itself, accomplishes the required safety function.

N o t e :

A full protective action is, e.g., the reactor scram.

(59) Self-monitoring

Self-monitoring is the characteristic of components or systems to automatically rend their failures to be detectable.

(60) Safety margin

The safety margin is the difference between the actuation value preset in the limit value monitor and the hazard limit value established in the design-basis accident analysis.

(61) Active safety system equipment

The active safety system equipment is a technical device of the safety system which performs protective actions.

N o t e :

An active safety system equipment is, e.g., equipment for shutting down the reactor, for the residual heat removal, for the isolation of the containment vessel penetrations.

Safety system equipment that perform a protective action without a final control element or mechanical device (e.g., core coolant confinement, containment vessel, shielding) are called passive safety system equipment.

(62) Safety system

The safety system is the entirety of all equipment of the nuclear power plant that has the purpose of protecting the power plant from inadmissible load conditions and, in the case of design basis accidents, of keeping their effects on the operating personnel, the power plant, and the environment within specified limits.

(63) Subunit of the safety system

A subunit of the safety system is that part of the safety system equipment which is necessary for accomplishing a partial protective action.

(64) Safety variable

The safety variable is derived from one or more process variables and its value characterizes the safety of the power plant and is necessary for the actuation of protective actions.

(65) Control Level

The control level is a protection system subunit in which actuation signals of the logic level are adapted to the circuit-technological requirements of the active safety system equipment.

(66) Design-basis accident (DBA)

A design-basis accident is an event or chain of events that is not expected to occur during the operating life of the power plant, for which the power plant nevertheless must be designed such that the design principles, verification objectives and verification criteria for Safety Level 3 are observed, and upon whose occurrence the operation of the plant or the activity cannot be continued for safety-related reasons.

(67) Validation

Validation is the affirmation by tests and certifications that the design specifications are met as required.

(68) Verification

Verification is the affirmation by tests and certifications that the results of an activity have achieved the goals and requirements that were specified for this activity.

N o t e :

Within the framework of a phase model, the individual phases are finalized by the verification.

(69) Comparator

A comparator is a device which compares with each other the values of two safety variables or of two process variables and which issues a binary signal in case of a specified deviation.

(70) Failure (breakdown)

A failure (breakdown) is the non-functioning or malfunctioning of active systems when their function is required.

N o t e :

Non- or malfunctions can be caused by failures of components or devices but can also be caused by latent faults that may become effective only under particular boundary conditions.

(71) Priority control module

A priority control module is a control equipment which causes a specific control signal to be treated with priority over one or more other control signals.

(72) Binary monitor

A binary monitor is a binary measuring equipment which converts a process variable directly (i.e. without intermediate processing by a limit value monitor) into a binary output signal.

N o t e :

One example of a binary monitor is, e.g., a pressure monitor.

(73) Works inspector

A works inspector is an expert authorized by the manufacturer and who is independent of the fabrication in the manufacturing plant.

(74) Random failure

A random failure is a failure which occurs statistically independent of the failures of other similar devices.

(75) Process-variable limiting module

A process-variable limiting module is a device that limits the values of process variables such that the initial conditions of anticipated design-basis accidents are sustained.

N o t e s :

(1) An example is, e.g., the limitation of the reactor power to that level that was anticipated as an initial condition in the analysis of the loss-of-coolant accident.

(2) This term was used in version 1985-04 of this safety standard. Due to the newly introduced categorization specified in Section 2.2, this term has become obsolete. Nevertheless, for better understanding, it is kept in this Section 2.1.

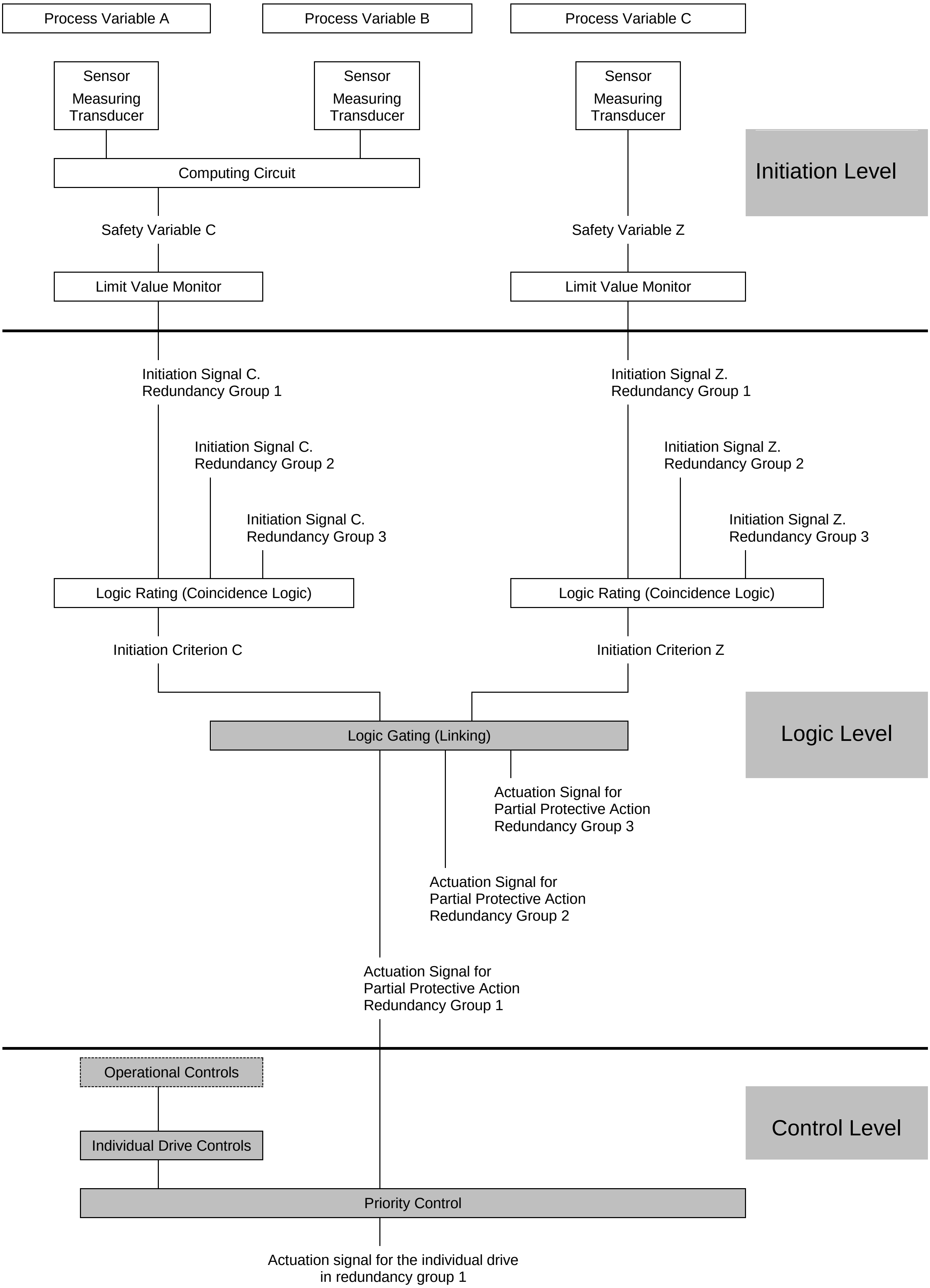

Figure 2-1: Exemplary correlation of the defined terms to the functional design of Cat A equipment

2.2 Categorizing the Functions of the I&C System Important to Safety

(1) Regarding their safety-related importance, the instrumentation and control functions including those of the accident measuring system shall be categorized according to their graduated requirements as follows:

a) Category A

I&C functions in Category A comprise all functions required to control design-basis accidents.

b) Category B

I&C functions in Category B comprise all functions required to control abnormal operating conditions (cf. Appendix 1 of SiAnf) such that the occurrence of design-basis accidents is prevented.

c) Category C

I&C functions in Category C comprise all other functions important to safety.

(2) I&C functions that do not perform functions important to safety are not categorized.

3 Task Determination

3.1 Basic Requirements

(1) An analysis of the chains of events specified in Section 3.2 for the power plant shall be performed to determine the tasks which the Cat A and Cat B equipment must fulfill. The assumptions made in this analysis shall be well substantiated. This analysis shall result in a complete compilation, categorization and description of the process-technological tasks that the I&C functions of the Cat A and Cat B equipment must fulfill including the necessary manual measures. This analysis shall also consider the effects of the erroneous actuations specified in Section 4.1.3.4.

Note:

The probability of certain chains of events can be reduced by technical means outside of the Cat A equipment to such an extent that these events do not need to be considered in the design of the Cat A equipment and of the active safety system equipment.

(2) The I&C functions (based on, e.g., process variables, safety variables, algorithms, limit values, characteristic curves, temporal behavior) shall be determined by analyses that consider the operation-related plant transients, the dynamic event procedures, the measurement errors and the response delays of the Cat A and Cat B equipment and associated systems.

(3) The process-technological design of the reactor plant shall be such that, normally, not clearly safety-oriented protective actions by Cat A equipment are prevented. Any necessary, not clearly safety-oriented protective actions shall be well substantiated.

(4) The safety margins associated with the I&C functions in Category A shall be specified.

3.2 Chains of Events and Their Effects

(1) The chains of events in accordance with Appendix 2, Tables 5.1 and 5.2 of SiAnf shall be considered for the power, low-power and shutdown operation of nuclear power plants.

(2) In addition to the chains of events in accordance with SiAnf, any faults that reduce or cancel the functional capability of active safety equipment shall also be considered.

3.3 Initial Plant Condition

The initial plant condition assumed in the analysis of the chains of events shall basically be normal operation. However, regarding the effects of an event, the most probable operating condition of the plant shall be chosen for each chain of events. Additional analyses shall be performed regarding unfavorable initial conditions. In these cases, and assuming quasi-steady-state operating conditions from the point of view of the instrumentation and controls, any tolerance-related deviations of the measurement values of the process variables from their required values as well as deviations of the process variables due to a single random failure within the entire measuring or control system shall be considered.

3.4 Detection of Design-Basis Accidents

(1) In the course of the analyses of chains of events, representative safety variables shall be identified that are suited for the detection of design-basis accidents.

(2) At least two physically different initiation criteria shall basically be assigned to each design-basis accident to be controlled by the Cat A equipment. For each initiation criterion, a separate analysis of the chains of events specified in Section 3.1 shall be carried out.

Note:

This serves to cover the uncertainties in the analysis of the accident chain of events and to control common-cause failures of the data acquisition.

(3) If the requirement under para. (2) is technically not feasible or cannot be fulfilled, data acquisition shall be expanded to involve different measurement procedures, different measurement devices in the corresponding initiation channel groups, as well as the self-detection of failures, shorter test cycles or equivalent measures.

(4) The sequential execution of the protective actions shall be analyzed for the first and second initiation criterion regarding response delay and accuracy of the initiation channels; the effect on the progression of the design basis accidents shall be described.

(5) If mutual process variables are used for Cat A equipment and for equipment of lower importance to safety, analyses of faults in the data acquisition shall be carried out taking paras. (1) and (2) into account.

Note:

In these analyses, it is considered that a common-mode failure will result in a simultaneous failure (breakdown) with similar effects of all those devices in the signal channels that are similar and of the same brand.

(6) These analyses may be waived, if diverse measuring devices are employed for the general controls on one hand and for the Cat A equipment on the other and, therefore, a common-mode failure need not be assumed for these measuring devices.

4 Design Principles

4.1 Design Requirements for Cat A Equipment

4.1.1 Basic requirements

(1) It shall be demonstrated that the Cat A equipment in its interaction with the active and passive safety system equipment is designed, manufactured and operated such that intolerable effects from design basis accidents and internal and external hazards are prevented.

(2) In this context, the postulated initiating events described under Section 4.1.2.1 and 4.1.2.2 shall be assumed to occur either as random failure or common-mode failure simultaneously with the design-basis accident. If a postulated initiating event from the ones described under Section 4.1.2.1 and 4.1.2.2 itself causes a design-basis accident (dependent DBA), then no additional design-basis accident needs to be assumed. However, in this case, one additional postulated initiating event shall be assumed either as a random failure or common-mode failure.

(3) The failures resulting from these postulated initiating events shall be combined as specified in Section 4.1.3 unless they can be excluded from occurring by technical means.

Notes:

(1) This demonstration may be presented collectively for the entirety of all components of the safety system.

(2) Regarding common-mode failures and potentially overreaching events (e.g., fire, flooding), if suitable measures ensure a sufficient limitation of the range of impact (cf. Section 5.1.5), the assumed common-mode failure is presumed to affect only this limited impact range.

(3) Requirements regarding fire protection are dealt with in safety standard KTA 2101.1.

4.1.2 Postulated initiating events

4.1.2.1 Postulated initiating events within the Cat A equipment

Postulated initiating events within the Cat A equipment shall be taken into consideration; these events are, e.g.,

a) failures caused by short circuits, open circuits, malfunctioning of the sequential execution of the program or of the data transfer, shorts to ground, changes in voltage and frequency, line-conducted and field-bound electromagnetic interferences, mechanical failures (breakdown) or fires,

b) multiple failures specified under item a) occurring simultaneously or in rapid succession of each other that have a common cause within the system itself (e.g., fabrication defects, design defects, drift), and

c) errors during operation, testing, servicing, and repair of the Cat A equipment caused by the personnel.

4.1.2.2 Postulated initiating events inside the nuclear power plant

Within the framework of the „single-failure concept", postulated initiating events inside the nuclear power plant shall be considered.

Note:

Cf. Appendix 4, SiAnf ("Principles for applying the single failure criterion and the maintenance"). Examples for postulated initiating events inside the nuclear power plant are line-conducted and field-bound electromagnetic influences, fire, flooding, pipe whip, debris from a failing component, mechanical jet effects of media like steam, water, gas, and oil.

4.1.2.3 Design against postulated initiating events outside the nuclear power plant

It shall be demonstrated that sufficient protective measures in accordance with Sec. 2.4, SiAnf ("Protection concept against internal and external hazards as well as against very rare human induced external hazards") are taken against external hazards like fire, grid disturbances, flooding, lightning, storms and induced vibrations such that these events will not inadmissibly influence the functioning of the Cat A equipment.

4.1.3 Failure combinations

4.1.3.1 Basic assumptions

(1) The following failures shall be considered:

a) Random failure Z,

b) Common-mode failure S,

c) Secondary failure F,

d) Maintenance (inspection, servicing, repair) I.

(2) It shall be demonstrated that the entirety of Cat A equipment in cooperation with the active and passive safety system equipment, in addition to the design-basis accident, is able to control

a) one random failure Z,

b) plus one common-mode failure (if it cannot be precluded as specified under para. (6)) S,

c) plus secondary failures F.

Note:

A random failure or a common-mode failure may be caused by the postulated initiating events specified in Sections 4.1.2.1 and 4.1.2.2.

(3) During specified normal operation of the nuclear power plant the failure combination shown in **Figure 4-1** regarding occurring design-basis accidents shall be mitigated and controlled whereby, in a maintenance case (I) it is not required to assume that the common-mode failure (S) and random failure (Z) occur simultaneously within a time span of 100 h. The maintenance case begins with the point in time of detecting the failure.

(4) If, within their individual redundancy, the I&C equipment of redundant process-technological components are supplied by different equipment systems, then it is not required to assume that the random failure (Z) and the common mode failure (S) will occur simultaneously, provided, the following prerequisites are fulfilled:

a) a high degree of self-monitoring with respect to failures,

b) observance of short repair times.

Note:

Para. (4) applies, e.g., to the 4 *x* 50 % design of process-technological redundancies which pairwise contain different equipment systems. In case of a common-mode failure, the remaining redundancies will fulfill the process-technological task.

(5) The random failure and the maintenance case need to be assumed as occurring only once within the entirety of the safety system components required for the mitigation and control of a design-basis accident.

(6) When designing Cat A equipment, the potential for, and effects from common-mode failures (breakdown) of the I&C equipment on accident sequences shall be analyzed taking the process-technological specifications into account. Precautionary measures shall be taken to prevent common-mode failures (breakdown) and, thus, minimize their probability of occurrence to such a level that, regarding the demonstration of the mitigation and control of design-basis accidents, common-mode failures (breakdown) do not anymore need to be assumed.

(7) If, according to the state of the art in science and technology, the requirements specified under para. (6) cannot be demonstrated for the I&C equipment, precautionary measures shall be taken to such an extent that any common-mode failure (breakdown) of hardware and software of the Cat A equipment is mitigated and controlled by diverse or dissimilar I&C equipment meeting similar quality requirements. The range of diversity and the structure shall be chosen such that a common-mode failure (breakdown) with its associated

effects will not inadmissibly influence the mitigation and control of the design-basis accident by the remaining diverse equipment.

N o t e :

In hardwired systems, the probability of occurrence of common-mode failures can be sufficiently reduced (e.g., by choice of suitable equipment systems, test cycles, critical load tests) that common-mode failures do not need to be considered anymore in the failure combination specified under para. (2).

(8) Fault-preventing and fault-controlling measures shall be provided for computer-based and programmable Cat A equipment. This comprises, foremost, suitable system characteristics and a suitable system design.

N o t e s :

(1) Fault-preventing measures for computer-based Cat A equipment are, e.g.:

a) No synchronization of absolute time is contained (this also has failure-controlling effects).
b) The computer-related processing of user functions and of data transfers occur in fixed time cycles (this also has failure-controlling effects).
c) The data transfer via data bus is carried out such that all data are cyclically transferred independently of whether they have changed or not (data polling; this also has failure-controlling effects).
d) None of the computers and data busses in the actuation path have a direct data bus connection to the outside. (They have only indirect data bus connections to the outside via an interface computer which is a Cat A equipment too.)
e) All computers in the actuation path are connected to a single computer (interface computer) in the same I&C redundancy that enables the data connection to the outside. The term “outside” refers to the maintenance computer, the process computer system of the power plant and, possibly, further function-related computers.
f) In operating mode, programming of computers in the actuation path is not possible. Leaving the operating mode is alerted.
g) The range of functions of Cat A equipment is limited to the extent necessary for the respective tasks.

(2) Fault-controlling measures for computer-based Cat A equipment are, e.g.:

a) Assigning the I&C functions to separate partial systems that are independent of each other.
b) Employing diverse and dissimilar I&C equipment for the mitigation and control of common-mode failures.
c) Employing independent and diverse I&C functions especially for the mitigation and control of failures related to process-technological tasks.

4.1.3.2 Full Protective Action

The actuation of the full protective action shall be ensured in all cases of the basic assumptions specified in Section 4.1.3.1.

N o t e :

Examples that fulfill these requirements are shown in **Figures 4-2** through **4-7**. **Figure 4-2** shows the unperturbed operation and **Figures 4-3** through **4-7** various failure combinations. Only those failures are considered that impair safety.

In this context, full protective actions refer only to those that are clearly safety oriented, e.g. reactor scram.

4.1.3.3 Partial protective actions

4.1.3.3.1 Clearly safety-oriented partial protective actions

Considering the basic assumptions specified in Section 4.1.3.1, the actuation of clearly safety-oriented partial protective actions shall be ensured such that the partial protective actions that remain enabled under the assumed failure combinations will be able to fulfill the required safety-related functions.

N o t e :

Figures 4-8 and **4-9** show examples that fulfill these requirements. Only those failures are considered that impair safety.

4.1.3.3.2 Not clearly safety-oriented partial protective actions

N o t e :

The partial protective actions considered in this context are those which, in the case of their erroneous actuation, could prevent other protective actions.

(1) Considering the basic assumptions specified in Section 4.1.3.1, the actuation of not clearly safety-oriented partial protective actions shall be ensured such that the partial protective actions that remain enabled under the assumed combinations of failures will be able to fulfill the required safety-related tasks.

(2) In the case of an erroneous actuation of not clearly safety-oriented partial protective actions caused by a random failure, it shall be ensured that, even with an ongoing maintenance case within the safety system, the remaining protective actions will be able to fulfill the required safety-related functions of the safety system.

(3) With regard to erroneous actuations of not clearly safety-oriented partial protective actions caused by random failures, the requirements of Section 4.1.3.1 para. (6) shall be applied.

N o t e :

In designing this part of the Cat A equipment, special attention shall also be paid to failures resulting in an actuation, because any erroneous actuations can inadmissibly reduce the effectiveness of the safety system.

4.1.3.4 Erroneous actuations of protective actions

Considering the basic assumptions specified in Section 4.1.3.1, any erroneous actuations of protective actions shall be prevented if they can lead to failures that go beyond the effects of the design basis accidents to be considered. Even with an ongoing maintenance case in the safety system, a random failure including secondary failures occurring in the Cat A equipment shall not lead to design-basis accidents with sequential damages.

4.1.4 Initiation of protective actions

4.1.4.1 Specification of the safety variables

A safety variable shall normally be created from only one process variable (cf. Section 5.1.7.1.1).

4.1.4.2 Degree of automatization

(1) The Cat A equipment shall normally actuate protective actions automatically. Manual measures (e.g., actuation, interruption or resetting of protective actions) may shall normally be planned to be executed only for well-substantiated exceptional cases. The safety system shall be designed such that no manually actuated protective actions for the mitigation and control of design-basis accidents will be required in the first 30 minutes.

N o t e :

Well-substantiated exceptions are permissible in the case of actuating protective actions that are provided for the mitigation and control of very seldom events (e.g., external hazards during the refueling process).

(2) A possibility of manually actuating a reactor scram shall be provided for. This shall be manually actuated independently of the computer-based equipment.

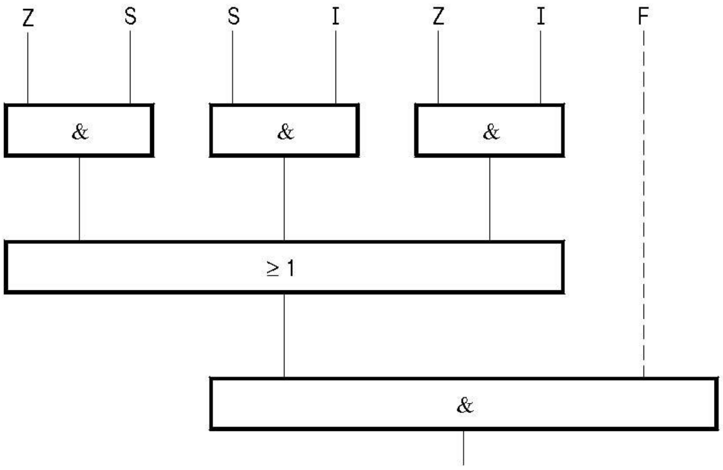

Figure 4-1: Failure combinations to be applied

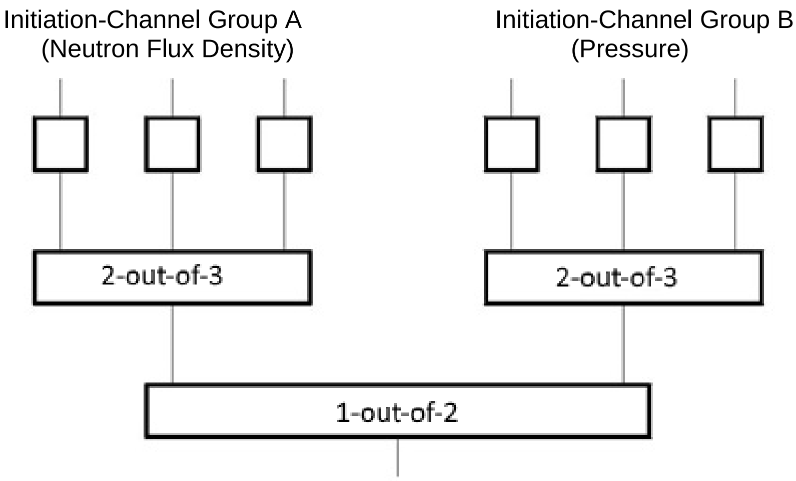

Figure 4-2: A possible schematic for the actuation of the reactor scram; it is caused by reactivity disturbances where two actuation criteria derived from different process variables (e.g., neutron flux density and pressure) are available and any secondary failures in data acquisition can be precluded.

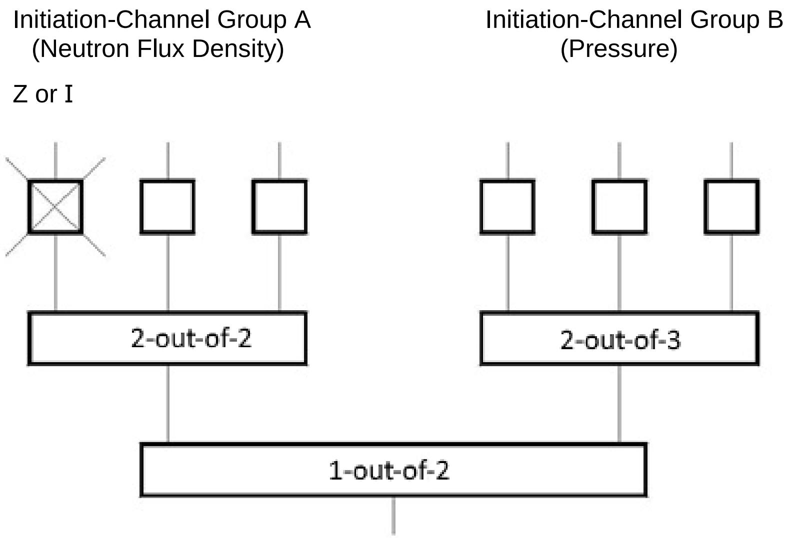

Figure 4-3: Schematic where one initiation channel of Initiation-Channel Group A is inoperable because of maintenance or due to the failure of one initiation channel caused by a single random failure. The design-basis accident is covered at least by Initiation-Channel Group A (2-out-of-2) and Initiation-Channel Group B (2-out-of-3).

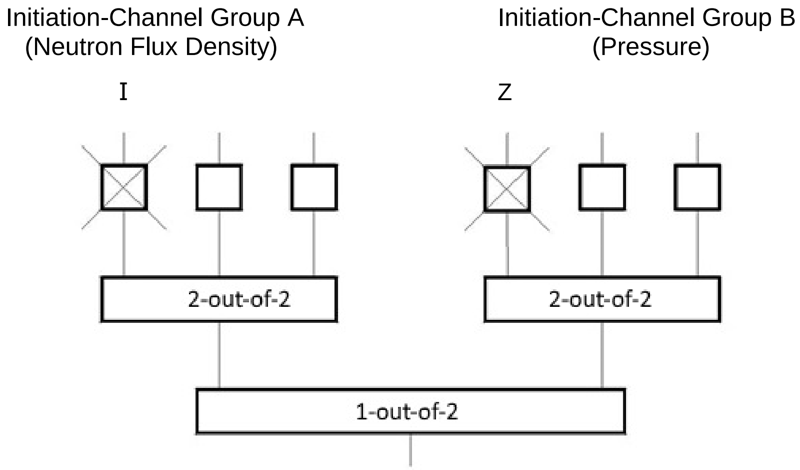

Figure 4-4: Schematic where one initiation channel in Initiation-Channel Group A is inoperable due to repair and a random failure occurs in Initiation-Channel Group B. The design-basis accident is covered by Initiation-Channel Group A (2-out-of-2) and by Initiation-Channel Group B (2-out-of-2).

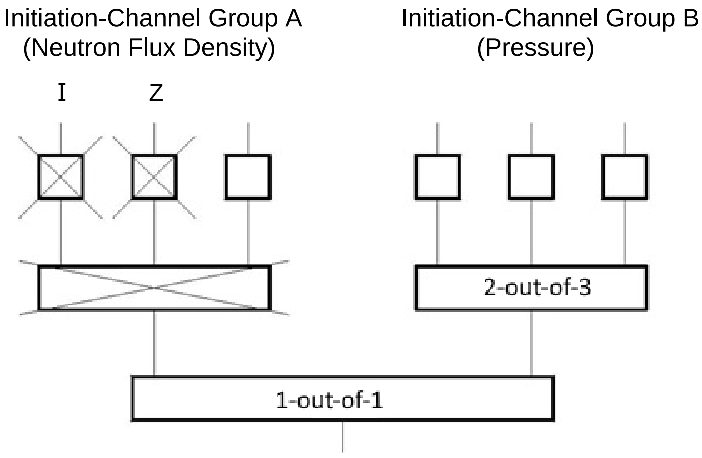

Figure 4-5: Schematic where, during the repair of one initiation channel in Initiation-Channel Group A, a random failure occurs in another initiation channel of the same initiation-channel group. The design-basis accident is covered by Initiation-Channel Group B (2-out-of-3).

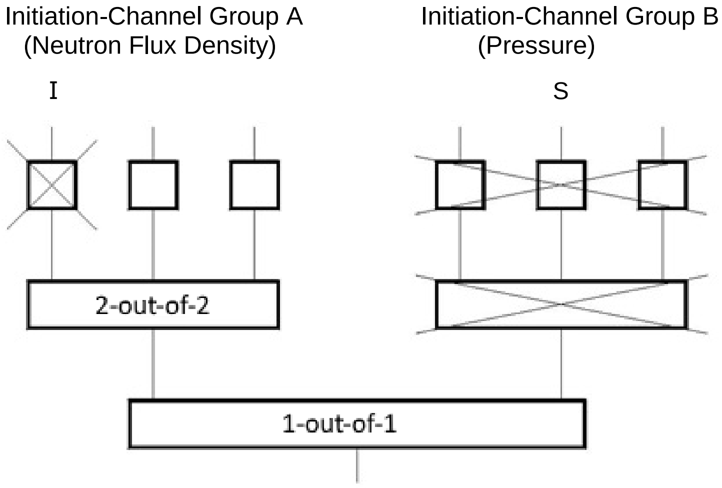

Figure 4-6: Schematic where a common-mode failure occurs in Initiation-Channel Group B during the repair of an initiation channel in Initiation-Channel Group A. The design-basis accident is covered by Initiation-Channel Group A (2-out-of-2).

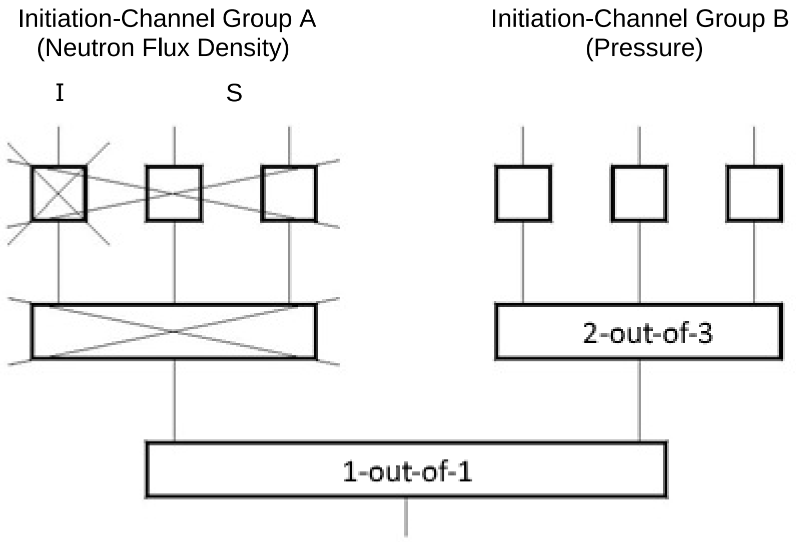

Figure 4-7: Schematic where, during repair of one initiation channel in Initiation-Channel Group A, a common-mode failure occurs in the same initiation-channel group. The design-basis accident is covered by Initiation-Channel Group B (2-out-of-3).

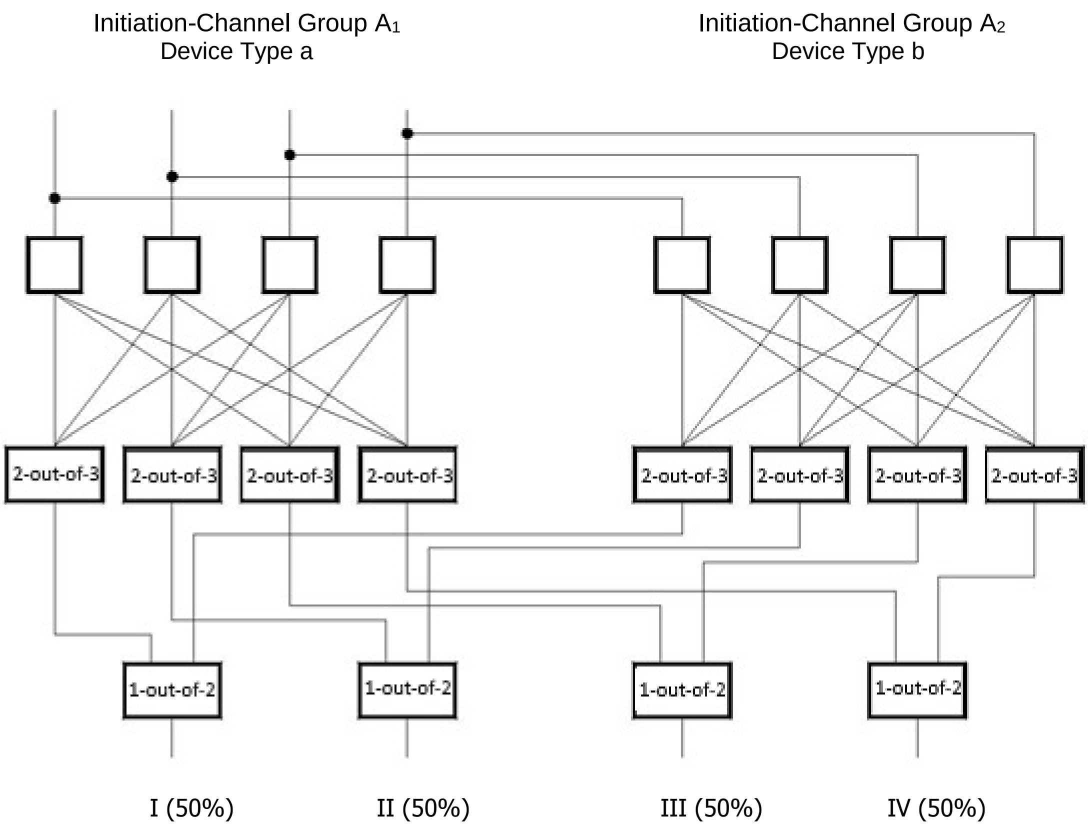

Figure 4.8: Schematic showing the basic layout for the actuation of the fourfold mutually redundant 50 % subunits of the safety system in case of a design-basis accident where only a single safety variable is available and where secondary failures in data acquisition (e.g., a break in the differential pressure line) must be assumed as physically possible and as not being actuation oriented. The devices for data acquisition up to and including the measuring transducers in the two initiation-channel groups are of diverse types (Device Type a, Device Type b)

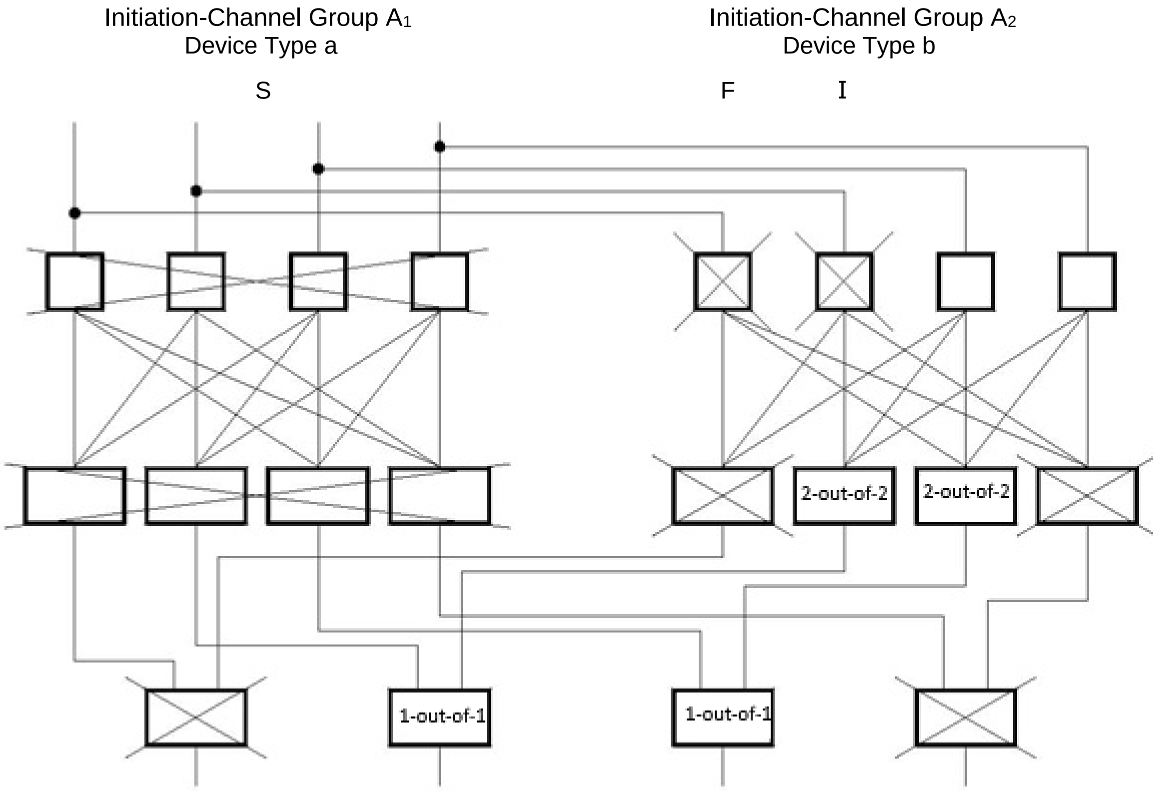

Figure 4-9: Schematic showing how the situation shown in **Figure 4-8** may develop in case of the most unfavorable failure combination: During repair of one initiation channel in Initiation-Channel Group A_1, a common-mode failure occurs in the Device Type a. Additionally, one actuation channel in Initiation-Channel Group A_2 becomes inoperative due to a secondary failure. The design-basis accident is sufficiently covered by actuating two of the 50 % subunits of the safety system.

4.1.4.3 Data logging

The initiation signals of the Cat A equipment and additional alarms from the active safety equipment shall be documented clearly and in the correct sequential order. This documentation shall normally be in the form of an automatically created sequential alarm log. The alarm log may also contain other signals not associated with a design-basis accident, provided, clarity is not impaired.

4.1.5 Redundancy and independence

(1) The Cat A equipment shall be redundantly designed to be able to mitigate and control postulated initiating events within the Cat A equipment.

(2) Redundancy groups shall be sufficiently independent of each other such that, in case of failures within redundancy groups caused by a postulated initiating event as specified in Sections 4.1.2.1 and 4.1.2.2, the remaining equipment will suffice for the mitigation and control of the design basis accident.

(3) At the interconnecting points between multiple redundancy groups of Cat A equipment existing at, e.g., comparator, evaluator and data averaging modules, the different redundancy groups shall be decoupled to ensure their independency. The decoupling devices shall delimit the redundancy groups from each other in a non-interactive way.

(4) Only system-specifically suited servicing or programming devices may be employed. They shall be assigned to the equipment in Category A. No data-technological connections are permissible between the servicing or programming devices and other computer-based systems.

(5) To protect against postulated initiating events within the Cat A equipment and inside the nuclear power plant, mutually redundant components shall normally be positioned spatially separated from each other. A spatial separation is not required if these events will not prevent the actuation of protective actions and will only lead to the actuation of safety-oriented protective actions.

4.1.6 Separation of Cat A equipment from other systems

(1) In well-substantiated cases, components of the Cat A equipment may be also employed for tasks that are of lower importance to safety.

N o t e :

However, under the aspect of simplicity, it is expedient to keep Cat A equipment free of other functions as far as possible.

(2) The Cat A equipment shall be sufficiently independent of any equipment of lower importance to safety such that, during specified normal operation and in case of postulated initiating events within this equipment of lower importance to safety, the functions of the Cat A equipment remain preserved.

(3) Connections from Cat A equipment to I&C equipment of lower importance to safety shall be minimized to the technically and operationally required extent. In case signals of the Cat A equipment are used for signal processing outside of the Cat A equipment (e.g. signals for plotters or display devices), these signals shall be decoupled non-interactively.

(4) When using mutual measurement devices for controls and Cat A equipment, it shall be demonstrated that the failure of these measurement devices will either not lead to design-basis accidents or that this failure is already specified in Section 3.4 paras. (1) and (2), and Sections 4.1.4.1 and 4.1.4.2.

(5) The controls of active safety equipment by Cat A equipment shall be designed such that the signal for the actuation of protective actions has priority over control signals of a lower importance to safety, provided, this is not overridden by the requirements under Section 6.

(6) The Cat A equipment shall be designed against, and decoupled from any system-unrelated overvoltage to be considered. The plant-specific voltage levels and voltage tolerances shall be taken into consideration.

4.1.7 Maintenance

(1) In case, during maintenance activities on the Cat A equipment, the remaining effective parts of the safety system – assuming an additional random failure including secondary failures – cannot anymore perform its safety-related task, the nuclear power plant shall immediately be transferred to a safe state.

(2) Transferring to a safe state may be accomplished, e.g., by an immediate repair or by the shutdown of the nuclear power plant. An immediate repair shall be given priority, provided, the repair is completed in a shorter time than required for a shutdown of the nuclear power plant.

(3) Requirements regarding the exchange of hardware and software components shall be specified during the development of the overall system and individual system parts. These shall include preparing instructions with respect to execution, testing, and documentation.

(4) If maintenance measures need to be performed during operation of the nuclear power plant and these measures require manual actions on Cat A equipment, it shall normally be possible to perform them without manipulation of the wiring on preinstalled and tested action points by following preplanned instructions.

(5) After completion of the maintenance measures, the operational capability and as-specified function of the Cat A equipment shall be demonstrated by corresponding functional tests.

(6) A complete documentation of the devices and circuitry shall be available for performing the maintenance.

(7) The maintenance tasks shall be performed by the personnel authorized to perform these tasks.

(8) Repair measures shall basically employ only type-identical replacement parts. If novel or modified components are employed, the tests specified in Sections 10.1.1.2 and 10.1.1.3 shall be performed.

(9) Any failures detected during maintenance activities, their causes and type of repair shall be documented. The operating experience gained from maintenance of Cat A equipment shall be collected, documented and systematically evaluated.

4.1.8 Coordination between Cat A equipment and the active safety system equipment

(1) Cat A equipment shall be designed such that it is not the determining factor for the unavailability of the safety system.

(2) Cat A equipment shall be constructed such that the specified redundancy of the active safety system equipment is sustained. A mutual data acquisition for the controls of redundant active safety system equipment is permissible, provided, the requirements specified in Section 4.1.3 are met.

4.1.9 Monitoring for operational capability and for testability

4.1.9.1 Monitoring for operational capability

(1) An informational display shall be provided presenting an overview of the conditions of the components of Cat A equipment and of active safety system equipment including their power and auxiliary media supply.

(2) Cat A equipment shall normally be designed to be self-monitoring. For those functions and characteristics not covered by self-monitoring, equipment shall be provided that enables their regular and overlapping testing. These tests shall normally be easily performed using auxiliary test equipment at interfaces provided for this purpose. Test procedures and manual actions shall be specified such that necessary safety functions are not prevented nor that the reliability of their initiation is significantly reduced.

> N o t e :
> Means for self-monitoring are, e.g., the signal comparison between redundant channels, non-coincidence monitoring, dynamically working systems, cyclical data-storage tests, data transfer monitoring.

(3) It shall be possible to sufficiently locate detected failures in Cat A equipment to enable their repair.

> N o t e :
> Locating means are, e.g., optical displays in the control room, on cabinet rows, on cabinets and plug-in units as well as system failure alarms (cf. Section 10).

4.1.9.2 Testability of Cat A equipment

(1) Cat A equipment shall be designed such that the required tests to demonstrate the as-designed functioning can be performed during specified normal operation without an inadmissible reduction of the safety of the power plant. The independency of the redundancy groups shall remain sustained during these tests. A simultaneous testing of redundant partial systems shall be prevented if this would impair the functional capability of the Cat A equipment. In this context, technical measures shall be given preference over administrative measures.

(2) Cat A equipment shall be designed such that the deviations from as-designed tolerance values of the individual devices and modules as well as the correct functioning of protection system subunits and of the entire Cat A equipment can be checked within the framework of pre-operational tests and tests performed during shutdown periods of the power plant.

> N o t e :
> The evaluation of the test results may take into consideration the process-technology related permissible tolerance.

(3) During power operation of the nuclear power plant, it shall normally be possible, using preplanned testing actions and devices and without manipulation of the wiring, to perform tests that ascertain the proper functioning of protection system subunits. By these tests of the protection system subunits, it shall be possible to demonstrate correct functioning of the entire Cat A equipment. Partial tests may be feasible in an overlapping way. The extent of the tests shall be specified taking the effectiveness of self-monitoring into account (cf. Sec. 3.1 para. (2) of safety standard KTA 3506).

> N o t e :
> Equipment suitable for fulfilling these requirements are, e.g., test sockets, test switches, displays that allow the superposing of simulation signals and the signaling of a successful completion of the test.

(4) The Cat A equipment shall normally be designed and operated such that functional tests can be performed from test locations preassigned for this purpose (e.g., from testing panels or service stations).

Note:

Measuring transducers and sensors are usually subjected to a decentralized testing.

(5) It shall normally be possible at a central location to detect that tests on Cat A equipment are performed.

(6) If the test for functional capability of Cat A equipment is performed by automatic test equipment (hardwired or freely programmable test equipment) the following requirements shall be met:

a) The quality and suitability of the test equipment shall be demonstrated.

b) The test equipment shall be specified in a configuration and identification documentation (cf. Section 11).

c) The test equipment shall normally (self-)check the correct coupling connection to the equipment to be tested.

d) After connection to the equipment to be tested and the start of the test procedure, the test equipment shall normally perform the test automatically.

e) The quality of automatic tests shall correspond at least to the quality of comparable manual tests.

4.1.10 Manual actions

Note:

The term ‘manual actions’ does not extend to modification of the planned hard- and software.

(1) If manual actions for the adjustment of Cat A equipment are necessary to be performed during operation of the nuclear power plant, it shall be possible to perform them without manipulation of the wiring and on preinstalled and tested action points by following preplanned instructions.

Note:

Examples for permissible adjustments are:

a) during isolation of a process-technological train: the conversion of the associated actuation channel into the actuated condition,

b) the activation of parameters for stretchout-operation, and

c) the substitute value programming.

(2) Preventive measures shall be taken to avoid faults from errors and negligence during the performance of necessary manual actions related to the operation and maintenance of Cat A equipment; these measures shall be in the form of

a) preferably, circuitry-related measures during the design of the system,

b) alarm equipment of the safety system,

c) administrative instructions regarding operation and maintenance,

and measures shall be considered for limiting the effects of failures.

Note:

In this context, suitable measures are, e.g.,

a) redundant structure of the Cat A equipment,

b) decoupling of the Cat A equipment from equipment of a lower importance to safety,

c) priority of the Cat A equipment signals over test signals,

d) interlocks preventing a simultaneous testing of redundant equipment,

e) employment of self-monitoring systems,

f) incorporation of test equipment,

g) appropriate system design to minimize the number of on-site tests that cannot be performed by the test equipment,

h) unambiguous identification marking of the systems and components,

i) status signals from active components of the safety system,

j) monitoring analog sensor channels by comparators,

k) alarm equipment regarding failure detection and failure localization,

l) plug-in monitoring of electrical modules,

m) securing the operating settings of components by seals or other mechanical devices,

n) unambiguous instructions for the operation of Cat A equipment,

o) execution of maintenance tasks on Cat A equipment only by qualified personnel following written instructions,

p) checking the maintenance task whether they are properly executed and documented, and

q) clearly structured, ergonomic arrangement of the components of the safety system.

(3) It shall be made difficult for unauthorized personnel to perform manual actions on Cat A equipment

a) preferably by technical measures, and

b) administrative measures.

Note:

In this context, suitable measures are, e.g.,

a) spatial separation of redundant components,

b) monitored access barriers for buildings, rooms and cabinets, and

c) administrative guidelines governing access authorization and access monitoring regarding Cat A equipment.

(4) The measures hindering unauthorized personnel from performing manual actions shall be designed such that required operation and maintenance tasks by authorized personnel is not unacceptably impeded.

(5) Regarding I&C functions required in the respective plant conditions, it shall be ensured by technical and administrative procedures that manual actions can only be performed sequentially in the individual redundancies. The manual actions shall be signaled – preferably by technical measures – to the control room and shall be documented.

Note:

Measuring transducers that are exclusively modified on-site are usually secured by seals.

4.2 Design Requirements for Cat B Equipment

4.2.1 Basic requirements

(1) It shall be demonstrated that the Cat B equipment will, in case of demand, fulfill the safety-related tasks specified in Section 2.2 item b) even during the postulated initiating events specified in Section 4.2.2.

(2) The failures resulting from these postulated initiating events shall be combined as specified in Section 4.2.3 unless they can be prevented from occurring by technical means.

4.2.2 Postulated initiating events

The following postulated initiating events shall be considered:

a) plant-internal events (including those within the Cat B equipment): e.g., failures due to short circuits, flooding, open circuits, malfunctioning of the sequential execution of the program or of the data transfer, shorts to ground, changes in voltage and frequency, line-conducted and field-bound electromagnetic interferences, mechanical failures (breakdown) or fires,

b) errors during operation, testing, servicing, and repair of the Cat B equipment caused by the personnel, and

c) plant-external events: e.g., fire, grid disturbances, flooding, lightning, storms, and earthquakes. Precautionary measures shall be demonstrated for these events, such that these events will not inadmissibly influence the safety of the power plant.

4.2.3 Failure combinations and basic assumptions for Cat B equipment

(1) It shall be demonstrated that Cat B equipment together with the entirety of its final control equipment will, in a demand case, control

a) one random failure Z,

b) plus secondary failures F.

Note:

A random failure may also be caused by one of the postulated initiating events specified in Section 4.2.2.

(2) During a maintenance case (inspection, serving, repair), a simultaneous demand case shall be assumed.

(3) The following applies to the local protection of the reactor core: If an I&C function in Category B is overlapped by an I&C function in Category A that mitigates and controls the design-basis accident at a higher, still permissible damage limit, then it is not necessary to detect a similar process variable at the same location for the I&C functions in Category B. For the I&C functions in Category B, no redundant measurement of the same process variable at the same location is required, if the I&C function in Category B is overlapped by an I&C function in Category A, that controls the design-basis accident at a higher, still permissible damage limit.

4.2.4 Erroneous actuations of Cat B equipment

Erroneous actuations of Cat B equipment shall not induce a design-basis accident.

4.2.5 Initiation of Cat B equipment

4.2.5.1 Degree of automatization

The Cat B equipment shall normally be actuated automatically.

4.2.5.2 Data logging

The response of the Cat B equipment shall be documented in the correct sequential order. This documentation shall normally be in the form of an automatically created sequential alarm log.

4.2.6 Redundancy and independence

(1) The Cat B equipment shall be redundantly designed to be able to mitigate and control postulated initiating events within the Cat B equipment.

(2) Redundant partial systems shall be sufficiently independent of each other such that, in case of failure of partial systems caused by a postulated initiating event as specified in Sections 4.2.2, the remaining partial systems will suffice for the mitigation and control of the design basis accident.

(3) Only system-specifically suited servicing or programming devices shall be employed. They shall be assigned to the equipment in Category B. No data-technological connections are permissible between the servicing or programming devices and other computer-based systems.

4.2.7 Separation of Cat B equipment from other systems

(1) Components of the Cat B equipment may be also employed for tasks that are of lower importance to safety.

(2) The Cat B equipment shall be sufficiently independent of any equipment of lower importance to safety such that, during specified normal operation and in case of postulated initiating events within this equipment of lower importance to safety, the functions of the Cat B equipment remain preserved.

(3) Connections from Cat B equipment to I&C equipment of lower importance to safety shall be minimized to the technically and operationally required extent. In case signals of the Cat B equipment are used for equipment of lower importance to safety, these signals shall be decoupled non-interactively.

(4) The controls of Cat B equipment shall be designed such that these control signals have priority over control signals of a lower importance to safety.

(5) The Cat B equipment shall be designed against, and decoupled from any system-unrelated overvoltage to be considered. The plant-specific voltage levels and voltage tolerances shall be taken into consideration.

4.2.8 Maintenance

(1) In case, during maintenance activities on the Cat B equipment, the still effective part – assuming an additional random failure including secondary failures – cannot anymore perform its safety-related task, appropriate plant- and function-specific measures shall be specified for the continuing of plant operation.

Note:

The requirements regarding the exchange of hardware and software are specified during the development of the overall system and the individual systems. These include case-specific instructions that are prepared with respect to execution, testing, and documentation.

(2) During maintenance activities within the Cat B equipment, it may become necessary to make certain adjustments, e.g. adjustment of stretch-out-operation parameters. If manual adjustments are involved, they shall be performed on preinstalled action points.

(3) After completion of the maintenance measures, the operational capability and as-specified function of the Cat B equipment shall be demonstrated by corresponding functional tests.

(4) A complete documentation of the devices and circuitry shall be available for performing the maintenance.

(5) The maintenance tasks shall be performed by the personnel authorized to perform these tasks.

(6) Repair measures shall basically employ only type-identical replacement parts. If novel or modified components are employed, the tests specified in Sections 10.1.1.2 and 10.1.1.3 shall be performed.

(7) Any failures detected during maintenance activities, their causes and type of repair shall be documented. The operating experience gained from maintenance of Cat B equipment shall be collected, documented and systematically evaluated.

4.2.9 Coordination between Cat B equipment and the associated process-technological equipment

(1) Cat B equipment shall be designed such that it is not the determining factor for the unavailability of the associated process-technological equipment.

(2) Cat B equipment shall be constructed such that the specified redundancy of the correlated process-technological equipment is sustained.

4.2.10 Monitoring for operational capability and for testability

4.2.10.1 Monitoring for operational capability

(1) An informational display shall be provided presenting an overview of the operational capability of the Cat B equipment including their power supply.

(2) Cat B equipment shall normally be designed to be self-monitoring.

Note:

Means for self-monitoring are, e.g., the signal comparison between redundant channels, non-coincidence monitoring, dynamically working systems, cyclical data-storage tests, data transfer monitoring.

(3) Those parts of Cat B equipment that are not self-monitoring shall be equipped with devices that allow testing in their switch-off pause; if required for reasons of reliability, this check shall also be possible during normal operation.

(4) It shall be possible to sufficiently locate detected failures in Cat B equipment to enable their repair.

Note:

Locating means are, e.g., optical displays in the control room, on cabinet rows, on cabinets and plug-in units as well as system failure alarms.

4.2.10.2 Testability of Cat B equipment

(1) Cat B equipment shall be designed such that tests can be performed during specified normal operation without an inadmissible reduction of the safety of the power plant. A simultaneous testing of redundant partial systems shall be prevented if the operating condition of the power plant necessitates the functional capability of the Cat B equipment. In this context, technical measures shall be given preference over administrative measures.

(2) Cat B equipment shall be designed such that the deviations from as-designed tolerance values of the individual devices and modules as well as the correct functioning of protection system subunits and of the entire Cat B equipment can be checked within the framework of tests performed during shutdown periods of the power plant.

Note:

The evaluation of the test results may take into consideration the process-technology related permissible tolerance.

(3) During power operation of the nuclear power plant, it shall normally be possible, using preplanned test actions and devices and without manipulation of the wiring, to perform tests that ascertain the proper functioning of system subunits. By these tests of the system subunits, it shall be possible to demonstrate correct functioning of the entire Cat B equipment. Partial tests may be feasible in an overlapping way. The extent of the tests shall be specified taking the effectiveness of self-monitoring into account.

Note:

Equipment suitable for fulfilling these requirements are, e.g., test sockets, test switches, displays that allow the superposing of simulation signals and the signaling of a successful completion of the test.

(4) The Cat B equipment shall normally be designed and operated such that functional tests can be performed from test locations preassigned for this purpose (e.g., from testing panels or service stations).

(5) It shall normally be possible at a central location to detect that tests on Cat B equipment are performed.

(6) If the test for functional capability of Cat B equipment is performed by automatic test equipment (hardwired or freely programmable test equipment) the following requirements shall be met:

a) The quality and suitability of the test equipment shall be demonstrated.

b) The test equipment shall be specified in a configuration and identification documentation (cf. Section 11).

c) The test equipment shall normally (self-)check the correct coupling connection to the equipment to be tested.

d) After connection to the equipment to be tested and the start of the test procedure, the test equipment shall normally perform the test automatically.

e) The quality of automatic tests shall correspond at least to the quality of comparable manual tests.

4.2.11 Manual Actions

Note:

The term ‘manual actions’ does not extend to modifications of the planned hard- and software.

(1) If manual actions for the adjustment of Cat B equipment are necessary to be performed during operation of the nuclear power plant, it shall be possible to perform them without manipulation of the wiring and on preinstalled and tested action points.

(2) Preventive measures shall be taken to avoid faults from errors and negligence during the performance of necessary manual actions related to the operation and maintenance of Cat B equipment; these measures shall be in the form of

a) preferably, circuitry-related measures during the design of the system,

b) alarm equipment of the safety system,

c) administrative instructions regarding operation and maintenance.

Note:

In this context, suitable measures are, e.g.,

a) redundant structure of the Cat B equipment,
b) decoupling of the Cat B equipment from equipment of a lower importance to safety,
c) interlocks preventing a simultaneous testing of redundant equipment,
d) employment of self-monitoring systems,
e) incorporation of test equipment,
f) appropriate system design to minimize the number of on-site tests that cannot be performed by the test equipment,
g) unambiguous identification marking of the systems and components,
h) status signals from active components,
i) monitoring analog sensor channels by comparators,
j) alarm equipment regarding failure detection and failure localization,
k) plug-in monitoring of electrical modules,
l) securing the operating settings of components by seals or other mechanical devices,
m) unambiguous instructions for the operation of Cat B equipment,
n) execution of maintenance tasks on Cat B equipment only by qualified personnel following written instructions,
o) checking the maintenance task whether they are properly executed and documented, and
p) clearly structured, the ergonomic arrangement of the components.

(3) It shall be made difficult for unauthorized personnel to perform manual actions on Cat B equipment

a) preferably by technical measures,

b) administrative measures.

Note:

In this context, suitable measures are, e.g.,

a) spatial separation of redundant components,
b) monitored access barriers for buildings, rooms and cabinets, and
c) administrative guidelines governing access authorization and access monitoring regarding Cat B equipment.

(4) The measures hindering unauthorized personnel from performing manual actions shall be designed such that required operation and maintenance tasks by the authorized personnel is not unacceptably impeded.

(5) Regarding I&C functions required in the respective plant conditions, it shall be ensured by technical and administrative procedures that, during power operation of the power plant, manual actions can only be performed sequentially in the individual redundancies. The manual actions shall be signaled – preferably by technical measures – to the control room and shall be documented.

Note:

Measuring transducers that are exclusively modified on-site are usually secured by seals.

4.3 Modifications of the I&C System Important to Safety

In case of modifications of the I&C system important to safety, the extent and the effects of these modifications shall be analyzed and the modifications shall be performed in conformance with the provisions of the present safety standard. The modified equipment shall fulfill the requirements of the present safety standard. In case of modifications, the tests specified in Section 10 and in safety standard KTA 3506 shall be performed.

4.4 IT Security

Note:

Requirements for the protection of IT systems against disruptive actions or other third-party interventions are specified in the SEWD-Guideline IT.

5 Design and Construction

5.1 Design and Construction of Cat A Equipment

The safety-related characteristics of Cat A equipment are determined by

a) the device quality (hardware and, if applicable, firmware/software) – cf. Section 5.1.1,

b) the quality of the system software and the application software – cf. Section 5.1.2, and

c) the functional and physical system structure – cf. Section 5.1.3.

5.1.1 Device quality

5.1.1.1 Demonstration of suitability for devices with a certification of proven performance

(1) Only devices with a certification of proven performance shall normally be employed.

(2) The certification of proven performance shall be carried out as a statistical analysis of the service records based on the operational characteristics specified in the data sheet and on the operating conditions.

Note:

Further details are specified in safety standard KTA 3507.

(3) Regarding certification of proven performance, the supplementary type tests specified in Section 10.1.1.1 shall be carried out if the operating conditions exceed the operational characteristics specified in the data sheet or if they were not covered by the certification of proven performance.

(4) The suitability of programmable and computer-based devices cannot be demonstrated alone based on a certification of proven performance. To demonstrate their suitability, additional demonstrations regarding software quality are necessary.

Note:

Further details are specified in safety standards KTA 3503 and KTA 3505.

5.1.1.2 Demonstration of suitability for newly developed or modified devices

(1) The fabrication and design quality of the I&C modules, devices and system parts shall be demonstrated.

(2) The quality required for fabrication and design shall at least reach Level B in accordance with DIN EN 61192-1.

Notes:

(1) Instead of Level B in accordance with DIN EN 61192-1, the Class 2 in accordance with IPC A 610 may also be applied.

(2) A review of the application-specific requirements may show that Level C in accordance with DIN EN 61192-1 is necessary.

(3) In case of modified devices, this requirement concerns only the affected range of the modification.

(3) Newly developed or modified devices shall be subjected to the type tests specified in Section 10.1.1.2.

5.1.1.3 Requirements for the design of newly developed or modified devices

(1) The circuit concept shall be simple, clear and purpose oriented.

(2) Proven and reliable components and circuits shall normally be employed; operating experience shall be taken into account.

(3) The device shall be designed such that a test of its function can be carried out without modification of the wiring.

(4) The device shall be designed for the ambient influences specified in Section 5.1.4.

(5) Regarding their static and dynamic characteristics, the devices shall satisfy the requirements of the I&C function in Cat A.

Note:

This is in respect of, e.g., stability, accuracy, signal-to-noise ratio, drift, hysteresis, response time and reproducibility.

5.1.1.4 Reliability and quality testing

(1) Data regarding the reliability of the device types shall be presented based on, e.g., statistical methods, failure effect analyses, critical load tests, or on the evaluation of operating experience.

(2) The device quality required of fabrication series shall be verified within the framework of the factory tests on a representative random sample that is subjected to the operating and limit loads.

(3) The quality assurance system applied to ensure the device quality shall be demonstrated.

Notes:

(1) Requirements for the quality assurance system are specified in KTA 1401.

(2) Additional quality requirements regarding the firmware in devices are specified in Section 5.1.2.

5.1.2 Software quality

5.1.2.1 Basic requirements

(1) The software shall be developed from a phase model in verifiable steps. This shall include developing the application software based on the process-technological task involved.

(2) The functions of the application software and of the system software shall be implemented in independent software units. The software architecture shall be such that the application software is separated from the system software.

N o t e s :

(1) In the following, the term software is understood to include application software as well as system software and firmware.

(2) System software includes, e.g., the operating system and, in multi-computer systems, the software for the communication between the computers.

(3) The software shall be designed such that there will be no inadmissible interactions from I&C equipment of a lower safety category to I&C equipment of a higher safety category.

(4) It shall be ensured that the task-specific sequential execution of the programs is independent of the type and extent of temporal variation of the input signals.

(5) Software shall be developed and qualified such that a consistent verification of the correct working of the software is ensured.

(6) Software shall normally be simple in its structure.

(7) The software's functional range shall normally be limited to the extent necessary for the respective function.

(8) The programs shall be designed to be robust and self-monitoring.

N o t e s :

(1) Robustness implies an insensitivity to conditions that are not in conformance with the as-specified conditions.

(2) Software robustness implies that undefined conditions are prevented. At any point in time, every input value shall result in a well-defined output value.

5.1.2.2 Quality assurance

5.1.2.2.1 Structural quality assurance

(1) The software shall be designed and implemented in the individual steps of the phase model by utilizing formalized and computer-aided construction methods and test methods.

(2) The software shall be constructed from clearly delimited modules, each module having only a small range of functions. These software modules shall be programmed to be as simple as possible and to be limited to the indispensable commands and interfaces; the individual modules shall be assembled to form a clearly structured program.

5.1.2.2.2 Analytical quality assurance

(1) The results of the individual phases of software development shall be entirely verified with respect to the specifications using systematic analyses and tests derived from these analyses. In this context, tests shall be performed at defined milestones using computer-aided tools.

(2) After the software is installed in the target hardware, the as-specified behavior of the hard- and software systems shall be validated. If the validation is performed in multiple steps, these individual validation steps shall, together, cover the entire systems.

5.1.2.2.3 Organization and administration

(1) The organization and administration of the software development and quality assurance shall be structured such as to ensure that the software is created and applied following complete development, test, modification and quality assurance plans. The independence between development and quality assurance shall be sustained throughout. A complete and current user documentation, as well as a complete and current documentation of development and quality assurance, shall be present.

(2) The consistency of the software configuration shall be ensured (configuration management).

5.1.2.3 Application of pre-developed software

(1) The application of pre-developed software that was not designed as specified in Sections 5.1.2.1 and 5.1.2.2 shall normally be limited to indispensable components in which any software modifications shall normally be avoided. These components shall be subjected to tests that, regarding extent and depth, shall be equivalent to the verifications specified in Sections 5.1.2.2.1 and 5.1.2.2.2.

(2) The evaluation of equivalency shall normally be based on:

a) references regarding the manufacturer of the software,

b) development, quality assurance and user documentation of the software,

c) results of independent appraisals (certifications) of the software.

d) operating experience with the software taking the user profile into account, and

e) additional software tests.

5.1.3 System characteristics and structure

(1) To ensure the independence of the individual redundant and diverse partial systems, error propagation barriers shall be created in the form of functional, device-oriented and data technological barriers.

N o t e :

Aspects regarding the creation of error propagation barriers are dealt with in DIN EN 62340.

(2) The I&C functions shall be appropriately distributed over independent I&C equipment such that a failure in one I&C equipment will not affect those I&C functions that, from a process-technological standpoint, must be effective independent of the failed function.

(3) Appropriate preventive measures shall be taken in the system design to reduce the probability of occurrence of common-mode failures.

N o t e :

This can be achieved by, e.g., the following measures:

a) no direct communication between processing modules whose independency must be ensured.

b) point-to-point connections for the communication between redundant processing modules, and

c) different relative ages of the system in the redundant equipment (e.g., system startup at different points in time).

(4) To be able to mitigate and control those common-mode failures that cannot be excluded in accordance with Section 4.1.3.1 para. (6), diverse system structures shall be created.

(5) Within the framework of a Failure Mode and Effect Analysis at the system level (System FEMA), any deployed computer-based or programmable devices shall be analyzed, and the effects that active or passive failures of their components might have on the power plant shall be described. Failures that could lead to not clearly safety-oriented protective actions and to critical power plant conditions shall be determined, and appropriate measures shall be provided for the mitigation and control of these failures. The behavior of the output signals when failures occur shall be specified.

N o t e :

Active failures lead to faulty actuation signals. Passive failures block actuation signals in a demand case.

(6) The I&C system shall normally exhibit a deterministic system behavior.

N o t e :

Deterministic system behavior ensures that the resulting behavior of the implemented system is solely determined in a predictable way by the planned design alone. The essential characteristics of a computer-based device family required to ensure the deterministic behavior of implemented systems are, e.g.:

a) strictly cyclic processing of all system functions,
b) static memory allocation for programs and data,
c) no interrupts that are dependent on a technological process,
d) invariance of the processing cycle with respect to arbitrary trajectories of the input data from the technological process,
e) communication loads that are independent of the process-technological transients.
f) reaction times that are independent of the process-technological signal trajectories, and
g) possibilities for the calculation and measurement of the system loading.

(7) Any manual actions in the I&C equipment shall be possible to be detected and shall normally be signaled to the control room. The necessary access protection measures shall be identified within the framework of an analysis. Effective interlocks shall be installed to limit manual actions to the necessary extent. If the manual action occurs from central equipment (e.g., service stations) effective interlocks shall be installed to prevent a manual action from being simultaneously performed on multiple redundancies.

5.1.4 Ambient influences

5.1.4.1 Load conditions during specified normal operation

(1) All components of the Cat A equipment, e.g., sensors, measuring transducers, wiring or penetrations, shall withstand the ambient and operational conditions to be assumed at the place of installation or positioning. It shall, especially, be demonstrated that their functioning is not inadmissibly influenced by:

a) mechanical loading (e.g. vibrations),
b) influences from the measuring medium,
c) temperature, pressure, moisture and radiation,
d) chemical effects, and
e) electromagnetic influences regarding interference immunity and emitted interference for line-conducted and field-bound interferences.

Note:

For instance, in the case of resistance thermometers, the self-heating from the measuring current and the heating from radiation absorption shall not lead to inadmissible measurement errors. In the case of thermocouples, the following effects, e.g., shall not lead to impermissible measurement errors:

a) structural change of the cladding tube caused by neutron irradiation,
b) alteration of the ceramic insulation material caused by neutron and gamma irradiation,
c) structural alteration of the thermo-couple arms caused by thermal neutrons, and
d) heating of the thermo-element from gamma irradiation and heat radiation.

(2) Initiation channels shall be constructed such that galvanically, inductively or capacitively induced interference voltages will neither prevent the actuation of protective actions nor cause erroneous actuations.

Notes:

(1) Examples of appropriate measures against galvanically coupled interference voltages are, e.g., single-point grounding (sensors insulated from the housing, or measuring transducers with galvanic isolation), separate power supply.

(2) Examples of measures against inductively coupled interference voltages are, e.g., twisting the wires, magnetic shielding by running the sensor cables in steel conduits, electric shielding by running the sensor cables in electro-conductive tubes, sufficient distance of the sensor cables from other influencing cables (power cables).

(3) Examples of suitable measures against capacitively coupled interference voltages are, e.g., electric shielding, running of sensor cables in electro-conductive tubes, using coaxial or triaxial cables in case of small measuring currents.

5.1.4.2 Load conditions during leakage rate tests of the containment vessel

The devices, cables and cable connections installed inside the containment vessel shall normally be capable of withstanding the load conditions arising from leakage rate tests. If in exceptional cases this is not the case, they shall be removed prior to the leakage rate tests, or they shall be protected against the load conditions from leakage rate tests. After the leakage rate tests, the tests in accordance with KTA 3506 shall be performed.

5.1.4.3 Load conditions during design-basis accidents

(1) Components of the Cat A equipment which must survive design-basis accidents – because they are still required after the start of the design-basis accident, e.g., for residual heat removal – shall be designed and constructed such that the components (sensors, components of the signal path and supply lines including cable conduits and cable penetrations) will withstand the respective conditions during the design-basis accidents and their effects, and that the quantities to be measured are monitored continuously throughout the entire as-designed range.

Note:

For example, the temperatures and pressures, the steam or water caused by the design-basis accident at electric penetrations, devices and distribution boxes, as well as the resulting thermal stresses at material interfaces, may not inadmissibly impair the functional capabilities.

(2) Parts of the Cat A equipment which are required only for actuating the necessary protective actions at the onset of a design-basis accident and may then become inoperative shall be proven to be designed such that the components will withstand the respective accident conditions (e.g., radiation, temperature, pressure and moisture) until the required protective action has been actuated, and such that their failure will not inadmissibly influence the components of the Cat A equipment required for the mitigation and control of the design-basis accident.

5.1.5 Spatial arrangement and separation of redundant systems

5.1.5.1 Overall system

(1) Mutually redundant devices of the Cat A equipment shall basically be arranged and separated sufficiently from each other such that a single postulated initiating event as specified in Sections 4.1.2.1 and 4.1.2.2 cannot lead to the failure of an inadmissible number of redundant equipment.

(2) If a spatial separation is not possible, adequate mechanical protection shall be provided, e.g., installation behind protective walls or in bunkers. A mechanical protection or the installation in separate cabinets is not required if a damage would not prevent actuation of protective actions and would only lead to the erroneous actuation of safety-oriented protective actions.

5.1.5.2 Cables

(1) Cables of mutually redundant devices of the Cat A equipment shall be spatially separated as specified in Section 5.1.5.1 or shall be routed such that they are physically protected from each other.

(2) Signals from mutually redundant devices of Cat A equipment shall not be fed through one and the same cable, local cable distributor or cable penetration.

(3) An unprotected routing of cables of the Cat A equipment is only permissible if, during specified normal operation, an unintentional mechanical damage is impossible. In all other cases, cables must be physically protected, e.g., by protective conduits or steel sheet covers.

(4) Cables of the Cat A equipment shall be routed spatially separated from components that may be hazardous to them, e.g., pipes, or they shall be physically protected.

(5) Signal transmission cables and power supply cables of the mutually redundant sensor and control equipment of the Cat A equipment shall normally not be routed to the signal processing modules through central main distribution racks.

5.1.5.3 Differential pressure lines

(1) The requirements of Section 5.1.5.1 shall be applied to differential pressure lines.

(2) Separate pressure tapping points shall normally be provided for redundant measurement arrangements at a single measuring location, e.g., at a common throttle device. Common pressure tapping points are permissible, provided, the requirements of Section 4.1.3 are met.

(3) An unintentional closing of shutoff valves in differential pressure lines shall be prevented, e.g., by the removal of hand wheels. Automatic shutoff devices shall normally not be installed.

(4) Depending on the measurement arrangement, technical devices for the flushing, filling, emptying and venting of differential pressure lines shall be taken into consideration.

5.1.6 Mechanical construction

5.1.6.1 Connectors and connections

(1) Screw and plug-in connections shall be secured such that no self-unplugging is possible or that the disconnected condition is automatically indicated by an alarm.

(2) A sufficient space shall be provided between the connections of different equipment belonging to the same redundancy group such that the inadvertent bypass of an actuation or an erroneous actuation is prevented; otherwise, equivalent measures shall be taken.

5.1.6.2 Identification markings

(1) Cat A equipment shall be legibly and unambiguously marked.

(2) Cables of the Cat A equipment shall be legibly and unambiguously marked at both ends.

(3) In case of modular systems, the locations and modules assigned to these locations shall be legibly and unambiguously marked.

5.1.6.3 Adjusters and setting mechanisms

(1) Pre-set adjusters shall be provided for those devices that require readjustment during operation, or for those operating-condition dependent function parameters that must be adjusted or must be set during running operation.

(2) All adjustment devices on Cat A equipment shall be positioned or secured such that they are protected against an unintentional adjustment or a self-adjustment by the equipment itself.

(3) It is inadmissible to provide any access to Cat A equipment from outside of its technical surroundings (e.g., from the administrative building, from outside of the power plant) by which software functions or data could be influenced.

(4) In the case of computer-aided adjustments that are performed from a corresponding control unit, the following requirement shall, additionally, be met:

a) The user guidance shall be simple and unambiguous.

b) All actual adjustment settings shall easily be retrievable from the target system and be clearly logged.

(5) It shall be ensured, preferably by technical means, that during operation of the Cat A equipment adjustments in multiple redundancies can only be made sequentially, one after another. If technical means are realized, the redundancy which is to be released for adjustment shall be unambiguously indicated and shall be displayed and documented in the control room.

Note:

One possible technical security measure is the use of key- switches.

5.1.6.4 Accessibility

(1) The Cat A equipment shall normally be positioned such that it is easily accessible for maintenance tasks.

(2) To facilitate and speed up maintenance tasks and to reduce the radiation exposure of maintenance personnel, systems shall normally be employed that have easily exchangeable devices and modules.

Note:

For example, the electrical connections for on-site devices may be constructed as plug-in connections.

5.1.7 Construction of protection system subunits

5.1.7.1 Initiation channels

In the initiation channels, devices shall normally be used that permit a continuous measurement signal acquisition and processing.

5.1.7.1.1 Analog initiation channels

The safety variable shall normally be a continuous function of the process variable. If a direct measurement of the safety variable is not possible (e.g., DNB-ratio) or if the use of a direct measuring procedure is technically not reasonable, computing circuits may be used, e.g., flow measurements using an orifice plate together with a measurement transducer that outputs the square root of the signal.

Note:

Analog initiation channels process the sensor signals over a continuous range of values. The sensor signal acquisition and processing may be performed with analog or digital equipment.

5.1.7.1.2 Limit value monitors and comparators

(1) Normally self-monitoring limit value monitors shall be used. In the case of electronic limit value monitors, the limit value itself (reference voltage) shall normally be monitored.

Note:

A self-monitoring of the comparators is not required.

(2) Limit value monitors and comparators shall normally have an adjustable switching-hysteresis and shall not be latching.

(3) The limit value shall be adjustable directly at the unit with an accuracy (resolution) corresponding to the requirements. It shall normally be possible to check the limit value during operation without having to change its setting.

(4) Under consideration of the accuracy and hysteresis of the limit value monitor, the measuring range of the initiation channel shall be specified such that a sufficient distance is maintained from the end-points of the measuring range.

(5) The response of limit value monitors and comparators shall be indicated on the respective device and in the control room.

(6) In the case of computer-based devices, the comparison of mutually redundant sensor signals may be performed within the computer.

5.1.7.1.3 Binary monitors

Binary monitors shall normally only be used where an analog measurement cannot be realized in a quality necessary for Cat A equipment. The contacts shall be monitored by appropriate control circuits (non-coincidence monitoring, wire breakage monitoring).

5.1.7.1.4 Limit switches

(1) Limit switches for the generation of initiation signals shall normally only be employed if an analog measurement cannot be realized in a quality necessary for Cat A equipment.

(2) If limit switches are employed that are not equipped with positively driven contacts for creating initiation signals, then – provided, no second initiation criterion is available – the requirements of Section 4.1.4.2 (2) shall be met. The contacts shall be monitored by appropriate control circuits (non-coincidence monitoring).

(3) The actuating devices of redundant limit switches (e.g., spindles, pushrods, cams, switching bars) shall normally be constructed individually for each redundant limit switch.

5.1.7.2 Logic Level

(1) Each one of the mutually parallel signal paths at the logic level responsible for a reactor scram shall be allocated to a different redundancy group. Their outputs shall normally be combined at least twofold in a logic gating. Each one of these logic gating output signals shall lead to an actuation.

(2) An individual signal path shall be provided for the actuation of each one of the multiple parallel partial protective actions. Each one of these parallel signal paths shall be allocated to a different redundancy group.

(3) If the analysis of the chains of events specified in Section 3.1 results in making provisions for the manual actuation of protective actions regarding the mitigation and control of design-basis accidents, these manual intervention possibilities shall normally not be realized at the control level but rather at the logic level of the Cat A equipment.

5.1.7.2.1 Interlocks

(1) In case only one initiation criterion is available for the detection of a design basis accident, the protection bypass of this initiation criterion shall be designed as specified in Section 4.1.4.2 para. (2).

(2) In the case of a redundant construction of the initiation channels, the devices for the switchover or transfer of measurement ranges shall also be redundantly constructed.

(3) The switchover and transfer of measuring ranges as well as the protection bypasses shall be cancelled automatically if the enabling conditions are not given anymore.

5.1.7.3 Control level

5.1.7.3.1 Individual drive controls

The individual drive controls of a process-technological system shall be constructed such that the redundancies are non-intermeshing.

Note:
It is assumed that the process-technological systems are redundantly constructed. A typical system is, e.g., the fourfold redundant high-pressure injection system.

5.1.7.3.2 Priority controls

(1) The priority of the signals from the Cat A equipment over control signals of a lower importance to safety shall be ensured. The control signals of a lower importance to safety shall be decoupled from the signals of the Cat A equipment. They shall normally be coupled only at the control level of Cat A equipment, this control level being downstream from the logic level.

(2) The priority control module shall be constructed to be in accordance with the process-technological redundancies. After priority formation, any interconnection of signals between process-technological redundancies is impermissible.

(3) The interconnection of signals of different importance to safety shall normally occur at the control level in accordance with their priorities.

(4) Coupling elements, e.g., coupling relays, shall function reliably within the permissible limits of the input and output voltages.

(5) When control signals are transformed to different voltages and frequencies by employing coupling elements, e.g., coupling relays, the inputs and outputs of the coupling elements shall be reliably decoupled from each other.

(6) The coupling elements, e.g., coupling relays, shall be designed and arranged such that switching operations in the switch gear will not cause any inadmissible mechanical, thermal or electrical loadings.

5.1.8 Interconnection

The interconnection of Cat A equipment shall be structured such that an unambiguous functional procedure is ensured. Component characteristics (e.g., response time, tolerances, drift behavior and behavior during design-basis accidents) shall not inadmissibly influence the chronological sequence of control signals.

5.2 Design and Construction of Cat B Equipment

The safety-related characteristics of Cat B equipment are determined by

a) the device quality (hardware and, if applicable, firmware/software) – cf. Section 5.2.1,

b) the quality of the system and application software – cf. Section 5.2.2, and

c) the functional and physical system structure – cf. Section 5.2.3.

5.2.1 Device quality

5.2.1.1 Demonstration of suitability for devices with a certification of proven performance

(1) Only devices with a certification of proven performance should normally be employed.

(2) The certification of proven performance shall be carried out as the statistical analysis of service records be based on the operational characteristics specified in the data sheet, and on the operating conditions.

(3) Regarding certification of proven performance, the supplementary tests specified in Section 10.1.1.1 shall be carried out if the operating conditions exceed the operational

characteristics specified in the data sheet or if they were not covered by the certification of proven performance.

(4) The suitability of programmable and computer-based devices cannot be demonstrated alone based on a certification of proven performance. To demonstrate their suitability, additional demonstrations regarding software quality are necessary.

N o t e :

Further details are specified in safety standards KTA 3503 and KTA 3505.

5.2.1.2 Demonstration of suitability for newly developed or modified devices

(1) The fabrication and design quality of the I&C modules, devices and system parts shall be demonstrated.

(2) The quality required for fabrication and design shall at least reach Level B in accordance with DIN EN 61192-1.

N o t e s :

a) Instead of Level B in accordance with DIN EN 61192-1, the Class 2 in accordance with IPC A 610 may also be applied.

b) A review of the application-specific requirements may show that Level C in accordance with DIN EN 61192-1 is necessary.

c) In case of modified devices, this requirement concerns only the affected range of the modification.

(3) Newly developed or modified devices shall be subjected to the tests specified in Section 10.1.1.2.

5.2.1.3 Requirements for the design of newly developed or modified devices

(1) Proven and reliable components and circuits should normally be employed; any operating experience shall be taken into account.

(2) The device shall be designed such that a test of its function can be carried out without modification of the wiring.

(3) The equipment shall be designed for the ambient influences specified in Section 5.2.4.

(4) Regarding their static and dynamic characteristics, the devices shall satisfy the requirements of the I&C function in Cat B.

N o t e :

This is in respect of, e.g., stability, accuracy, signal-to-noise ratio, drift, hysteresis, response time, reproducibility.

5.2.1.4 Reliability and quality testing

(1) Data regarding the reliability of the device types shall be presented based on, e.g., statistical methods failure effect analyses, critical load tests, or on the evaluation of operating experience.

(2) The device quality required of fabrication series shall be verified within the framework of the factory tests on a representative random sample that is subjected to operating loads and limit loads.

(3) The quality assurance system applied to ensure the device quality shall be demonstrated.

N o t e s :

(1) Requirements for the quality assurance system are specified in KTA 1401.

(2) Additional requirements regarding firmware in the devices are specified in Section 5.2.2.

5.2.2 Software quality

5.2.2.1 Basic requirements

(1) In the development and qualification of software for the I&C equipment in Category B, descriptions and computer-based test procedures shall be employed that will support demonstrating the correct operation of the software.

(2) The programs shall be designed to be robust and self-monitoring.

N o t e :

(1) Robustness implies the insensitivity to conditions that are not in conformance with specifications.

(2) Software robustness implies that undefined conditions are prevented. At any point in time, every input value shall result in a well-defined output value.

5.2.2.2 Quality assurance

5.2.2.2.1 Structural quality assurance

(1) The software shall be developed according to a phase model and by utilizing computer-aided tools as far as possible.

(2) The software shall, regarding their function, be constructed from clearly delimited modules. These software modules shall normally be programmed such that they are limited to indispensable commands and interfaces; the modules shall be integrated into a clearly structured program.

5.2.2.2.2 Analytical quality assurance

(1) The results of the individual phases of software development shall be subjected to a documented testing. All safety-related parts of the program shall be tested by a combination of test procedures where the functional tests shall normally completely overlap each other.

(2) The as-specified behavior of the hardware and software system shall be validated.

5.2.2.2.3 Organization and administration

(1) The organization and administration of the software development and quality assurance shall be structured such as to ensure that the software is created and applied following complete development, test, modification and quality assurance plans. The independence between development and quality assurance shall be sustained throughout. A complete and current user documentation, as well as a complete and current documentation of development and quality assurance, shall be present.

(2) The consistency of the software configuration shall be ensured (configuration management).

5.2.2.3 Application of pre-developed software

(1) The application of pre-developed software that was not designed as specified in Sections 5.2.2.1 and 5.2.2.2 shall normally be limited to indispensable components and shall normally avoid any software modifications. These components shall be subjected to tests that, regarding extent and depth, shall be equivalent to the proofs specified in Sections 5.2.2.2.1 and 5.2.2.2.2.

(2) The evaluation of equivalency shall normally be based on:

a) references regarding the manufacturer of the software,

b) development, quality assurance and user documentation of the software,

c) results of independent appraisals (certifications) of the software.

d) operating experience with the software taking the user profile into account, and

e) additional software tests.

5.2.3 System characteristics and structure

(1) To ensure the independence of the individual redundant partial systems, error propagation barriers shall be created in the form of functional, device-oriented and data technological barriers.

Note:

Aspects regarding the creation of error propagation barriers are dealt with in DIN EN 62340.

(2) Using a systematic method for identifying failure modes and analyzing the effects of these failures, any deployed computer-based or programmable devices shall be analyzed, and the effects that active or passive failures might have on the power plant shall be described. The behavior of the output signals when failures occur shall be specified.

Note:

Active failures lead to faulty actuation signals. Passive failures block actuation signals in a demand case.

(3) The I&C system shall normally exhibit a deterministic system behavior.

Note:

Deterministic system behavior ensures that the resulting behavior of the implemented system is solely determined in a predictable way by the planned design. The essential characteristics of a computer-based device family required to ensure the deterministic behavior of implemented systems are, e.g.:

a) strictly cyclic processing of all system functions,

b) static memory allocation for programs and data,

c) no interrupts that are dependent on a technological process,

d) invariance of the processing cycle with respect to arbitrary trajectories of the input data from the technological process,

e) communication loads that are independent of the process-technological transients.

f) reaction times that are independent of the process-technological signal trajectories, and

g) possibilities for the calculation and measurement of the system loading.

(4) Any manual actions in the I&C equipment shall be possible to be detected and shall normally be signaled to the control room. The necessary access protection measures shall be identified within the framework of an analysis. Effective interlocks shall be installed to limit manual actions to the necessary extent. If the manual action occurs from central equipment (e.g., service stations) effective interlocks shall be installed to prevent a manual action from being simultaneously performed on multiple redundancies.

5.2.4 Ambient influences

5.2.4.1 Load conditions during specified normal operation

(1) All components of the Cat B equipment, e.g., sensors, measuring transducers, wiring or penetrations, shall withstand the ambient and operational conditions to be assumed at the place of installation or positioning. It shall, especially, be demonstrated that their functioning is not inadmissibly influenced by:

a) mechanical loading (e.g. vibrations),

b) influences from the measuring medium,

c) temperature, pressure, moisture and radiation,

d) chemical effects, and

e) electromagnetic influences regarding interference immunity and emitted interference for line-conducted and field-bound interferences.

Note:

For instance, in the case of resistance thermometers, the self-heating from the measuring current and the heating from radiation absorption shall not lead to inadmissible measurement errors.
In the case of thermocouples, the following effects, e.g., shall not lead to inadmissible measurement errors:

a) structural change of the cladding tube caused by neutron irradiation,

b) alteration of the ceramic insulation material caused by neutron and gamma irradiation,

c) structural alteration of the thermo-couple arms caused by thermal neutrons, and

d) heating of the thermo-element from gamma irradiation and heat radiation.

(2) Initiation channels shall be constructed such that galvanically, inductively or capacitively induced interference voltages will neither prevent the actuation of protective actions nor cause erroneous actuations.

Notes:

(1) Examples of appropriate measures against galvanically coupled interference voltages are, e.g., single-point grounding (sensors insulated from the housing, or measuring transducers with galvanic isolation), separate power supply.

(2) Examples of measures against inductively coupled interference voltages are, e.g., twisting the wires, magnetic shielding by running the sensor cables in steel conduits, electric shielding by running the sensor cables in electro-conductive tubes, sufficient distance of the sensor cables from other influencing cables (power cables).

(3) Examples of suitable measures against capacitively coupled interference voltages are, e.g., electric shielding, running of sensor cables in electro-conductive tubes, using coaxial or triaxial cables in case of small measuring currents.

5.2.4.2 Load conditions during design-basis accidents

Components of the Cat B equipment which must survive design-basis accidents – because they are still required after the start of the design-basis accident – shall be designed and constructed such that the components (sensors, components of the signal path and supply lines including cable conduits and cable penetrations) will withstand the respective conditions during the design-basis accidents and their effects

Note:

For example, the temperatures and pressures, steam or water caused by the design-basis accident at electric penetrations, devices and distribution boxes, as well as the resulting thermal stresses at material interfaces, may not inadmissibly influence the functional capabilities.

5.2.5 Mechanical construction

5.2.5.1 Connectors and connections

Screw and plug-in connections shall be secured such that no self-unplugging is possible or that the disconnected condition is automatically indicated by an alarm.

5.2.5.2 Identification markings

(1) Cat B equipment shall be legibly and unambiguously marked.

(2) Cables of the Cat B equipment shall be legibly and unambiguously marked at both ends.

(3) In case of modular systems, the locations and modules assigned to these locations shall be legibly and unambiguously marked.

5.2.5.3 Adjusters and setting mechanisms

(1) Pre-set adjusters shall be provided for those devices that require readjustment during operation, or for those operating-condition dependent function parameters that must be adjusted or must be set during running operation.

(2) All adjustment devices on Cat B equipment shall be positioned or secured such that they are protected against an unintentional adjustment or a self-adjustment by the equipment itself.

(3) It is impermissible to provide any access to Cat B equipment from outside of its technical surroundings (e.g., from the administrative building, from outside of the power plant) by which software functions or data can be influenced.

(4) In the case of computer-aided adjustments that are performed from a corresponding control unit, the following requirement shall, additionally, be met:

a) The user guidance shall be unambiguous.

b) All adjustment settings shall be retrievable from the target system and be clearly logged.

(5) It shall be ensured, preferably by technical means, that during operation of the Cat B equipment adjustments in multiple redundancies can only be made sequentially, one after another. If technical means are realized, that redundancy which is to be released for adjustment shall be unambiguously indicated and shall be displayed and documented in the control room.

Note:

One possible technical protection measure is the use of a key-switches.

5.2.5.4 Accessibility

(1) The Cat B equipment shall normally be positioned such that it is easily accessible for maintenance tasks.

(2) To facilitate and speed up maintenance tasks and to reduce the radiation exposure of maintenance personnel, systems shall normally be employed that have easily exchangeable devices and modules.

Note:

For example, the electrical connections for on-site devices may be constructed as plug-in connections.

5.2.6 Construction of subsystems

5.2.6.1 Data acquisition and processing

(1) The input data for functions in Category B shall, preferably, stem from analog measurements. The employment of binary signal generators is permissible, provided, they are monitored by appropriate control circuits (non-coincidence monitoring, wire breakage monitoring).

(2) The validity of the measurement values shall normally be monitored by validation functions.

(3) The response of limit value monitors and comparators shall be indicated on the respective device and in the control room.

(4) Limit switches shall basically be equipped with positively driven contacts. If these cannot be realized, the contacts shall be monitored by appropriate control circuits (non-coincidence monitoring).

5.2.6.2 Signal processing

(1) Cat B equipment shall be independent and decoupled non-interactively from I&C equipment of lower importance to safety. Mutually redundant functions in Cat B shall be realized in independent equipment.

(2) The validity of the signal processing results shall normally be monitored by validation functions.

5.2.6.3 Priority controls

(1) The priority of the signals from the Cat B equipment over control signals of a lower importance to safety shall be ensured. The control signals of a lower importance to safety shall be decoupled from the signals of the Cat B equipment.

(2) The coupling elements shall meet the requirements specified in Section 5.1.7.3.2.

5.2.7 Interconnection

The interconnection of Cat B equipment shall be structured such that an unambiguous functional procedure is ensured. Component characteristics (e.g., response time, tolerances and drift behavior) shall not inadmissibly influence the chronological sequence of control signals.

6 Mechanical-Equipment Protection

(1) In a demand case for Cat A equipment, the protective equipment of the mechanical and auxiliary equipment necessary for protective actions shall normally be suppressed from becoming effective. This suppression is not permissible if this could lead to secondary failures that would impair the reactor plant safety more than would the failure of the respective mechanical equipment. The suppression of the mechanical-equipment protection shall be carried out by the Cat A equipment.

(2) If it is necessary for a protective equipment to override I&C functions in Category A (high-priority mechanical-equipment protection), the respective protective equipment shall basically meet the requirements specified for functions in Category A.

(3) Protective equipment may be exempted from having to meet the requirements specified for I&C functions in Category A, provided, it is demonstrated that failures of the protective equipment are unlikely enough that it is not anymore necessary to assume the occurrence of an erroneous actuation caused by such failure.

(4) A random failure in a device of the high-priority mechanical-equipment protection shall not cause the actuation of a protective action with sequential damages as specified in Section 4.1.3.4, or shall not prevent the actuation of a full protective action. The devices of the mechanical-equipment protection shall normally shut down the mechanical equipment by a 2-out-of-2 or 2-out-of-3 evaluation logic when limit values are exceeded.

(5) Devices of the mechanical-equipment protection whose signals have priority over signals of the Cat A equipment shall be correlated to the mechanical equipment to be protected.

(6) Devices for manually bypassing the mechanical-equipment protection shall be designed such as to hinder any unauthorized manual intervention.

7 Ventilation Systems for Cooling the Compartments of Cat A Equipment

(1) The spatial accommodation of the Cat A equipment shall basically be such that the permissible room temperature is not exceeded for the Cat A equipment even upon failure of the entire ventilation. Otherwise, ventilation systems shall be provided that shall be designed as specified under paras. (2) and (3) of this section.

N o t e :
To maintain the permissible room temperature, e.g., equipment not relevant to safety may be shut down.

(2) The ventilation systems for the Cat A equipment shall be constructed redundantly including their respective cooling circuits. The cooling of Cat A equipment shall remain in functioning order even in the event of a random failure in the Cat A equipment or of a postulated initiating event in accordance with Section 4.1.2.2 such that the functional capability of the Cat A equipment is ensured.

N o t e :
Failure of a ventilation system is considered to be a postulated initiating event as specified in Section 4.1.2.2.

(3) Cat A equipment that requires cooling shall be provided with ventilation systems that are connected to the emergency power supply.

(4) Deviating from the requirements under paras. (2) and (3), those Cat A equipment that are positioned in plant component or measuring-transducer rooms may, due to the comparatively negligible heat production, be cooled by the general ventilation systems of the restricted-access area, provided, the requirement under para. (1) are met.

8 Electrical Power Supply

(1) Both the Cat A equipment and the Cat B equipment that are necessary in an emergency power situation shall be supplied from an uninterruptible emergency power supply with batteries as energy storage operating in parallel with rectifier units. The corresponding emergency power supply system shall meet the requirements in accordance with safety standard KTA 3701. The power supply equipment inside Cat A equipment shall fulfill the requirements specified in Sections 5.1.1 and 10.1.

(2) The power supply of Cat A equipment shall be redundantly constructed such that the entire Cat A equipment is sufficiently supplied even upon occurrence of a postulated initiating event specified in Sections 4.1.2.1 and 4.1.2.2 in conjunction with the basic assumptions under Section 4.1.3.1.

(3) The power supply equipment shall be designed to supply sufficient power such that, even in case of the failure of a subsystem of the power supply, the necessary power requirements of the entire Cat A equipment are covered.

(4) The design of the power generating and distribution facilities, of the distribution grids and the I&C equipment shall be coordinated with each other such that the basic load values and the static and dynamic limit values of the permissible supply voltages do not exceed the corresponding values specified for the I&C equipment.

(5) The batteries shall meet the requirements in accordance with safety standard KTA 3703.

9 Alarm Equipment

9.1 General Requirements

(1) The following classes shall be distinguished in the design of alarm equipment:

a) Class S alarms (safety hazard alarms),

b) Class I alarms, and

c) Class II alarms.

(2) The components employed shall be suitable for the individual task. The assessment of the component suitability shall be based on their task-specific relevance to safety and on the assumed operating conditions.

9.2 Class S Alarm Equipment

9.2.1 Application

The manual initiation of protective actions is permissible, provided, the requirements specified in Section 4.1.4.3 are met and a sufficiently large time-span exists between detection of the design-basis accident and initiation of the protective action. These countermeasures that are required to be initiated following Class S alarms (safety hazard alarms) shall be unambiguously correlated to the Class S alarms, and the protective measures including associated time-spans for initiating the measures and for the expected feedback signals and displays shall be available to the operating personnel in a binding, written form.

9.2.2 Design

(1) In accordance with their individual safety relevance, the quality of the devices shall meet the requirements specified in Sections 5.1.1 or 5.2.1.

(2) Class S alarms shall signal the hazard condition by optical and acoustical means.

(3) Class S alarm equipment and the optical and acoustical alarm facilities shall be designed such that, in the event of a design-basis accident, an accident alarm is issued even in case of a random failure in the Class S alarm facility.

(4) Class S alarm equipment shall be constructed to be redundant and independent of each other and shall be able to be tested during specified normal operation. The corresponding signals may be decoupled from that part of the Cat A equipment that is used for the automatic actuation of protective actions. These signals shall be decoupled non-interactively.

(5) Class S alarms shall be displayed distinctly different from the Class I and Class II alarms.

(6) Class S alarms shall be stored.

(7) Within the framework of the respective control room concept, the optical Class S alarms shall be spatially grouped together.

(8) The optical Class S alarms shall be designed such that the state of the alarm (e.g., registered, acknowledged, cancelled) is continuously indicated.

(9) The optical Class S alarms shall be supplied from an uninterruptible emergency power supply with batteries as energy storage operating in parallel with rectifier units.

(10) It shall be ensured by appropriate lettering, illumination and unambiguous wording that Class S alarms are clearly recognizable as such.

(11) The optical Class S alarm equipment shall normally be designed to have a sufficient operating life, and such that they can be tested at any time with the aid of built-in auxiliary test equipment.

9.2.3 Software for Class S alarm equipment

In accordance with their individual safety relevance, the software shall meet the requirements specified in Sections 5.1.2 or 5.2.2.

9.3 Class I Alarm Equipment

9.3.1 Application

The Cat A equipment and the active safety system equipment shall be equipped with Class I alarms for alerting the operating personnel to remove the respective fault.

N o t e :
In case of the Cat A equipment, this includes, e.g., the collective alarm „Limit value monitor triggered “, in case of the emergency feed-water supply the alarm „Demineralized water supply tank level too low ”, and in case of actuator drives the collective alarm “Operating-readiness setting faulted “.

9.3.2 Design

(1) Class I alarms shall signal the hazard condition by optical and acoustical means.

(2) Class I alarms shall normally be displayed differently from Class II alarms, such that they can be distinguished from each other.

(3) The individual alarms of functionally related components may be combined into collective alarms, provided, the origin of the individual alarms can be localized. In this case, the individual alarms need not be correlated to Class I.

(4) Within the framework of the respective control room concept, the optical Class I alarms which functionally belong together shall normally be spatially grouped and displayed together.

(5) The optical Class I alarms shall be designed such that the state of the alarm (e.g., registered, acknowledged, cancelled) is continuously indicated.

(6) The Class I alarm equipment including the individual alarms combined into a collective alarm shall be supplied from an uninterruptible emergency power supply with batteries as energy storage operating in parallel with rectifier units.

(7) It shall be ensured by appropriate lettering, illumination and unambiguous wording that Class I alarms are clearly recognizable as such.

(8) The optical Class I alarm equipment shall normally be designed to have a sufficient operating life, and that they can be tested at any times with the aid of built-in auxiliary test equipment.

9.3.3 Software for Class I alarm equipment

The software for Class I alarm equipment shall be developed using established software-technological methods.

N o t e :
One established method is, e.g., specified in DIN EN 62138 and there, possibly, the method for Category C.

10 Tests and Inspections

10.1 Tests and Inspections of Cat A and Cat B Equipment and of Class S Alarm Equipment

10.1.1 Suitability Testing of the Device Types

10.1.1.1 Supplementary Type Tests of Devices with a Certification of Proven Performance

(1) In the case of devices with a certification of proven performance, supplementary type tests shall be carried out to demonstrate certain characteristics not certified as specified in Sections 5.1.1.1 para. (2) or 5.2.1.1 para. (2).

(2) The documents for the theoretical part of the type tests shall normally be prepared by the manufacturer. These documents shall normally be presented for review to the nuclear licensing authority or an appointed authorized expert (under Sec. 20 AtG). The test program for the practical part of the type tests shall normally be prepared by the manufacturer in coordination with the nuclear licensing authority or an appointed authorized expert (under Sec. 20 AtG). The practical tests should be carried out by a works inspector. It is permissible to have these tests performed by a suitable testing organization.

10.1.1.2 Type testing of newly developed or modified devices

(1) It shall be demonstrated by a type test that newly developed or modified devices are in compliance with the characteristics specified in the data sheet.

(2) The documents for the theoretical part of the type tests shall normally be prepared by the manufacturer. These documents shall normally be presented for review by the nuclear licensing authority or an appointed authorized expert (under Sec. 20 AtG). The test program for the practical part of the type tests shall normally be prepared by the manufacturer in coordination with the nuclear licensing authority or an appointed authorized expert (under Sec. 20 AtG). The practical tests should be carried out by the works inspector. It is permissible to have these tests performed by a suitable testing organization.

(3) Modules for Cat A and Cat B equipment shall be subjected to type tests in accordance with safety standard KTA 3503. The sensors and measuring transducers for Cat A and Cat B equipment shall be subjected to type tests in accordance with safety standard KTA 3505.

10.1.1.3 Demonstration of suitability

The plant-specific suitability of equipment with a certification of proven performance specified in Section 5.1.1.1 para. (2) or of the type tested devices specified in Sections 10.1.1.1 or 10.1.1.2 shall be demonstrated by comparing the characteristics of the equipment or devices with the requirements specified in Sections 4 and 5 and, in the case of Class S alarm equipment in Section 9.2.

N o t e :
The demonstration of suitability can lead to the result that further practical or theoretical tests are required in addition to the type testing specified in Sections 10.1.1.1 or 10.1.1.2.

10.1.2 Factory Tests

The correct fabrication of the I&C modules, devices and system parts shall be demonstrated by factory tests.

N o t e :
Requirements regarding factory tests are dealt with in safety standard KTA 3507.

10.1.3 System Tests

The system tests shall be performed in accordance with safety standard KTA 3506.

10.2 Tests and Inspections of Class I Alarm Equipment

(1) Class I alarm equipment shall be subjected to factory tests.

N o t e :
Requirements regarding factory tests are dealt with in safety standard KTA 3507.

(2) Class I alarm equipment shall be subjected to system testing in accordance with safety standard KTA 3506.

11 Configuration and Identification Documentation

(1) A configuration and identification documentation shall be prepared for an I&C system; this documentation shall identifiably specify the associated hardware and software modules including their settings as well as the system structure.

(2) The requirements for the configuration and identification documentation specified in safety standard KTA 3506 shall be met.

Appendix A

Regulations Referred to in the Present Safety Standard

(Regulations referred to in the present safety standard are valid only in the versions cited below. Regulations which are referred to within these regulations are valid only in the version that was valid when the latter regulations were established or issued.)

AtG		Act on the peaceful utilization of atomic energy and the protection against its hazards (Atomic Energy Act – AtG) of December 23, 1959, revised version of July 15, 1985 (BGBl. I, p. 1565), most recently changed by Article 307 of the Act of August 31, 2015 (BGBl. I 2015, No. 35, p. 1474)
StrlSchV		Ordinance on the protection from damage by ionizing radiation (Radiological Protection Ordinance – StrlSchV) of July 20, 2001 (BGBl. I, p. 1714; 2002 I, p. 1459), most recently changed by Article 5 of the Act of December 11, 2014 (BGBl. I, p. 2010)
SiAnf	(2015-03)	Safety Requirements for Nuclear Power Plants (SiAnf) of 22 November 2012 (BAnz AT 24.01.2013 B3), revised version of 3 March 2015 (BAnz AT 30.03.2015 B2).
SiAnf-Interpretations	(2015-03)	Interpretations of the "Safety Requirements for Nuclear Power Plants of 22 November 2012" (BAnz AT 24.01.2013 B3), revised version of 3 March 2015 (BAnz AT 30.03.2015 B2)
SEWD-Guideline IT	(2013-07)	Guideline for the protection of IT systems in nuclear facilities and in safety category I and II facilities against disruptive actions and other third-party interventions (SEWD-Guideline IT) of July 8, 2013, (GMBl. No. 36/2013)
ZPI	(1982-10)	Compilation of the Information Required for Review Purposes under Licensing and Supervisory Procedures for Nuclear Power Plants (ZPI) of October 20, 1982 (BAnz No. 6a/1983 of January 11, 1983)
KTA 1401	(2013-11)	General requirements regarding quality assurance
KTA 1403	(2010-11)	Ageing management in nuclear power plants
KTA 2101.3	(2015-11)	Fire protection in nuclear power plants; Part 3: Fire protection of mechanical and electrical plant components
KTA 2201.4	(2012-11)	Design of nuclear power plants against seismic events; Part 4: Components
KTA 3503	(2015-11)	Type testing of electrical modules for the I&C system important to safety
KTA 3504	(2015-11)	Electrical drive mechanisms of the safety system in nuclear power plants
KTA 3505	(2015-11)	Type testing of measuring sensors and transducers of the I&C system important to safety
KTA 3506	(2012-11)	System Testing of the I&C Equipment Important to Safety of Nuclear Power Plants
KTA 3507	(2014-11)	Factory tests, post-repair tests and the certification of proven performance of modules and devices of the I&C system important to safety
KTA 3601	(2005-11)	Ventilation systems in nuclear power plants
KTA 3701	(2014-11)	General requirements for the electrical power supply in nuclear power plants
KTA 3702	(2014-11)	Emergency power generating facilities with diesel-generator units in nuclear power plants
KTA 3703	(2012-11)	Emergency power facilities with batteries and AC/DC converters in nuclear power plants
KTA 3704	(2013-11)	Emergency power facilities with static and rotating AC/DC converters in nuclear power plants
KTA 3705	(2013-11)	Switchgear facilities, transformers and distribution networks for the electrical power supply of the safety system in nuclear power plants
KTA 3706	(2000-06)	Ensuring the loss-of-coolant-accident resistance of electrotechnical components and of components in the instrumentation and controls of operating nuclear power plants

DIN 31051	(2012-09)	Fundamentals of maintenance
DIN EN 61192-1	(2002-11)	Workmanship requirements for soldered electronic assemblies - Part 1: General (IEC 61192-1:2003); German version EN 61192-1:2003
DIN EN 62340 (VDE 0491-10)	(2010-12)	Nuclear power plants - I&C systems important to safety - Requirements for coping with Common Cause Failure (CCF) (IEC 62340:2007); German version EN 62340:2010
DIN EN 62138 (VDE 0491-3-3)	(2010-03)	Nuclear power plants - I&C important for safety - Software aspects for computer-based systems performing category B or C functions (IEC 62138:2004); German version EN 62138:2009