

# 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-Geschaefsstelle

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

|                                                                                              |    |
|----------------------------------------------------------------------------------------------|----|
| Basic Principles.....                                                                        | 5  |
| 1 Scope .....                                                                                | 5  |
| 2 Definitions .....                                                                          | 5  |
| 2.1 Words .....                                                                              | 5  |
| 2.2 Categorizing the Functions of the I&C system Important to Safety .....                   | 11 |
| 3 Task Determination.....                                                                    | 11 |
| 3.1 Basic Requirements.....                                                                  | 11 |
| 3.2 Chains of Events and Their Effects .....                                                 | 11 |
| 3.3 Initial Plant Condition .....                                                            | 11 |
| 3.4 Detection of Design-Basis Accidents .....                                                | 11 |
| 4 Design Principles.....                                                                     | 11 |
| 4.1 Design Requirements for Cat A Equipment.....                                             | 11 |
| 4.2 Design Requirements for Cat B Equipment.....                                             | 19 |
| 4.3 Modifications of the I&C System Important to Safety.....                                 | 22 |
| 4.4 IT Security .....                                                                        | 22 |
| 5 Design and Construction .....                                                              | 22 |
| 5.1 Design and Construction of Cat A Equipment .....                                         | 22 |
| 5.2 Design and Construction of Cat B Equipment .....                                         | 26 |
| 6 Mechanical-Equipment (Aggregate) Protection .....                                          | 29 |
| 7 Ventilation Systems for Cooling the Compartments of Cat A Equipment .....                  | 29 |
| 8 Electrical Power .....                                                                     | 30 |
| 9 Alarm Equipment .....                                                                      | 30 |
| 9.1 General Requirements.....                                                                | 30 |
| 9.2 Class S Alarm Equipment.....                                                             | 30 |
| 9.3 Class I Alarm Equipment .....                                                            | 30 |
| 10 Tests and Inspections.....                                                                | 31 |
| 10.1 Tests and Inspections of Cat A and Cat B Equipment and of Class S Alarm Equipment ..... | 31 |
| 10.2 Tests and Inspections of Class I Alarm Equipment .....                                  | 31 |
| 11 Configuration and Identification Documentation .....                                      | 32 |
| Appendix A Regulations Referred to in the Present Safety Standard .....                      | 33 |

PLEASE NOTE: Only the original German version of this safety standard represents the joint resolution of the 35-member Nuclear Safety Standards Commission (Kerntechnischer Ausschuss, KTA). The German version was made public in the Federal Gazette (Bundesanzeiger) of January 08, 2016. Copies of the German version may be mail-ordered through the Wolters Kluwer Deutschland GmbH ([info@wolterskluwer.de](mailto:info@wolterskluwer.de)). Downloads of the English translations are available at the KTA website (<http://www.kta-gs.de>).

All questions regarding this English translation should please be directed to:

**KTA-Geschaefsstelle c/o BfE, Willy-Brandt-Str. 5, D-38226 Salzgitter, Germany or [kta-gs@bfe.bund.de](mailto: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:

|                        |                                                                                                                                                                                                                                                                              |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>shall</b>           | indicates a mandatory requirement,                                                                                                                                                                                                                                           |
| <b>shall basically</b> | 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 <b>shall normally</b> - are specified in the text of the safety standard, |
| <b>shall normally</b>  | indicates a requirement to which exceptions are allowed. However, exceptions used shall be substantiated during the licensing procedure,                                                                                                                                     |
| <b>should</b>          | indicates a recommendation or an example of good practice,                                                                                                                                                                                                                   |
| <b>may</b>             | 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)  |

|                                                                                                                                                                                                                  |      |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Initiation criterion                                                                                                                                                                                             | (6)  | (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.                                                                                                                                                                                                                                           |
| Initiation level                                                                                                                                                                                                 | (3)  | (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.                                                                                                              |
| Initiation signal (trip signal)                                                                                                                                                                                  | (7)  | (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.                                                                                                                                                                                                      |
| Initiation-channel group                                                                                                                                                                                         | (5)  | (6) Initiation criterion            | The initiation criterion is that condition, under which a protective action is initiated.                                                                                                                                                                                                                                                                                                 |
| Inspection                                                                                                                                                                                                       | (34) | (7) Initiation signal (trip signal) | The initiation signal is the output signal of an initiation channel and the input signal to the logic level.                                                                                                                                                                                                                                                                              |
| Instrumentation and controls (I&C)                                                                                                                                                                               | (37) | (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.                                                                                                                                                                                                           |
| Limit value monitor (bistable trip unit)                                                                                                                                                                         | (32) | (9) Non-coincidence monitor         | The non-coincidence monitor is a device that monitors binary signals with respect to their unambiguity.                                                                                                                                                                                                                                                                                   |
| Limit value of a limit value monitor)                                                                                                                                                                            | (33) | (10) Failure                        | A failure is the loss of the ability of a device to perform the required function.                                                                                                                                                                                                                                                                                                        |
| Logic gating (linking)                                                                                                                                                                                           | (41) | 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. |
| Logic level                                                                                                                                                                                                      | (40) | (11) Common-mode failure            | The common-mode failure is a failure due to the same cause.                                                                                                                                                                                                                                                                                                                               |
| Logic rating (coincidence logic)                                                                                                                                                                                 | (42) | 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.                                                                                                                                                                                 |
| Maintenance                                                                                                                                                                                                      | (35) |                                     | (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.                                                                                                                                                                                                                              |
| Mechanical-equipment protection                                                                                                                                                                                  | (2)  | (12) Actuation signal               | An actuation signal is the output signal of the logic level or of the control level that actuates protective actions.                                                                                                                                                                                                                                                                     |
| Non-coincidence monitor                                                                                                                                                                                          | (9)  | (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                                                                                                                                                                                                          |
| Non-interaction                                                                                                                                                                                                  | (49) |                                     | a) during a functioning condition of the equipment (undisturbed operating condition, normal operation),                                                                                                                                                                                                                                                                                   |
| Not clearly safety-oriented protective action                                                                                                                                                                    | (52) |                                     | b) of abnormal operation (disturbed operation, malfunction) as well as                                                                                                                                                                                                                                                                                                                    |
| Not-programmable module                                                                                                                                                                                          | (28) |                                     | c) during maintenance procedures (inspection, servicing, repair).                                                                                                                                                                                                                                                                                                                         |
| Operational interlock                                                                                                                                                                                            | (15) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Operational limitation                                                                                                                                                                                           | (14) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Partial protective action                                                                                                                                                                                        | (54) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Phase model                                                                                                                                                                                                      | (43) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Priority control module                                                                                                                                                                                          | (71) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Process variable                                                                                                                                                                                                 | (44) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Process-variable limitation module                                                                                                                                                                               | (75) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Programmable module                                                                                                                                                                                              | (29) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Protection bypass                                                                                                                                                                                                | (56) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Protection-system subunit                                                                                                                                                                                        | (57) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Protective action                                                                                                                                                                                                | (50) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Protective limitation                                                                                                                                                                                            | (53) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Protective subsystem                                                                                                                                                                                             | (55) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Random failure                                                                                                                                                                                                   | (74) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Reactor protection system                                                                                                                                                                                        | (45) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Redundancy group                                                                                                                                                                                                 | (48) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Redundancy                                                                                                                                                                                                       | (47) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Response delay                                                                                                                                                                                                   | (8)  |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Safety margin                                                                                                                                                                                                    | (60) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Safety system                                                                                                                                                                                                    | (62) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Safety variable                                                                                                                                                                                                  | (64) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Safety-oriented protective action                                                                                                                                                                                | (51) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Secondary failure (cascading failure)                                                                                                                                                                            | (22) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Self-monitoring                                                                                                                                                                                                  | (59) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Specified normal operation                                                                                                                                                                                       | (13) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Subunit of the safety system                                                                                                                                                                                     | (63) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Validation                                                                                                                                                                                                       | (67) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Verification                                                                                                                                                                                                     | (68) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| Works inspector                                                                                                                                                                                                  | (73) |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |
| (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. |      |                                     |                                                                                                                                                                                                                                                                                                                                                                                           |

**(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 unlike 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.

**Note :**

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.

**Note :**

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.

**Note :**

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

**(59) Self-monitoring**

Self-monitoring is the characteristic of components or systems to automatically render 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.

**Note :**

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.

**Note :**

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.

**Note :**

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.

**Note :**

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.

**Notes :**

(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.

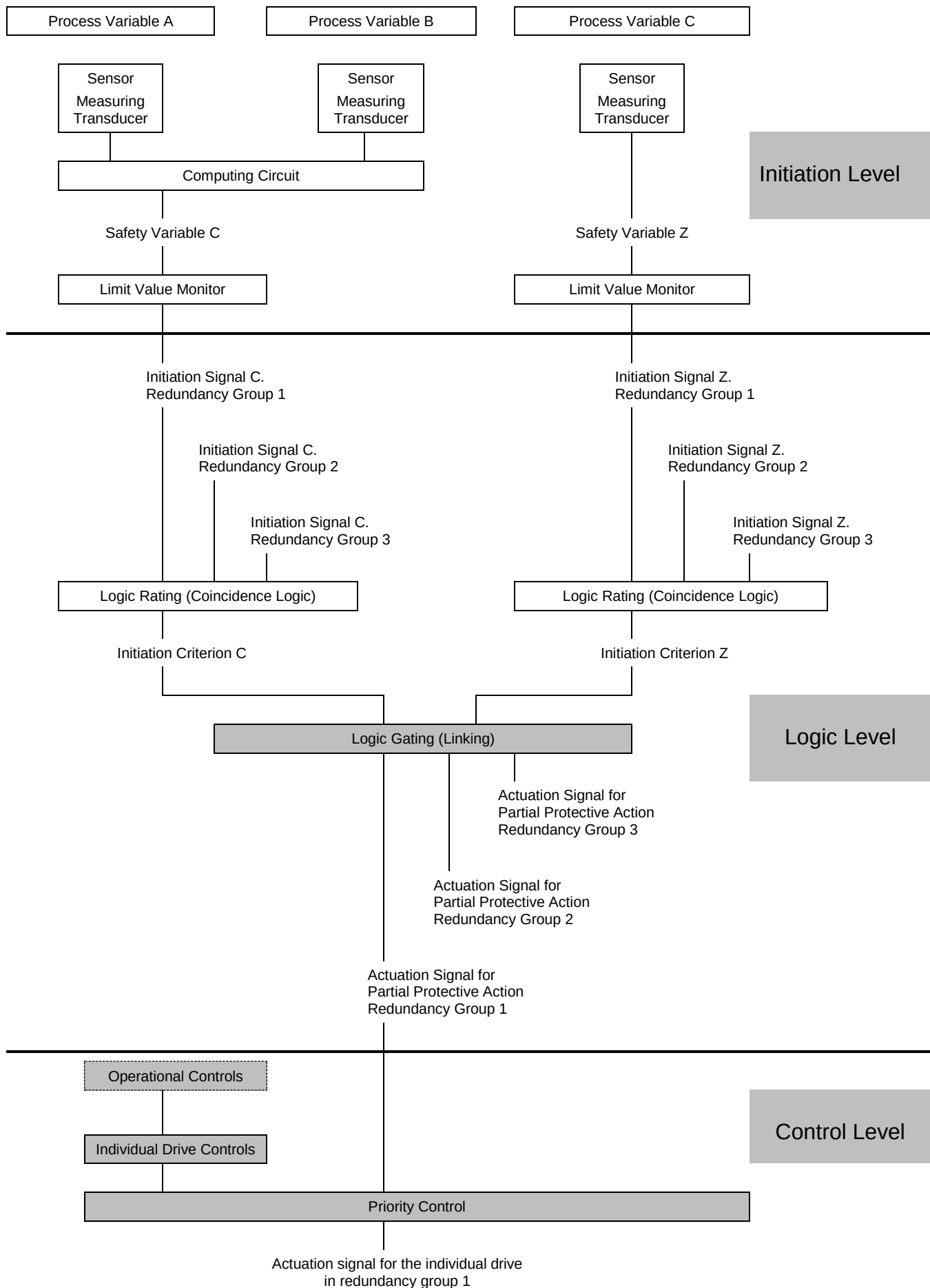


**Figure 2-1:** Exemplary correlation of the defined terms to the functional design of Cat A equipment

## 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.