Note:
This is a translation of the RSK statement entitled "Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken" In case of discrepancies between the English translation and the German original, the original shall prevail.

RSK/ESK Secretariat

"Computer-based instrumentation and control (I&C) systems important to safety for use in the highest safety category in German nuclear power plants"

Presentation of the consultation results from the RSK working group on USE OF COMPUTER-BASED INSTRUMENTATION AND CONTROL SYSTEMS *(EINSATZ RECHNERBASIERTE LEITTECHNIK - ERL)*

20 September 2011

TABLE OF CONTENTS

1 Cause of the discussion

At its 200th meeting on 4 June 2009, the RSK Committee on Electrical Installations adopted its position paper entitled "Computer-based instrumentation and control systems important to safety for use in the highest safety category in German nuclear power plants" [1.1]. This position paper addresses five specific aspects:

- measures to prevent and control common-cause failures (CCF);
- qualification and complexity; distinction between type testing and performance testing;
- maintenance measures and modifications to computer-based instrumentation and control systems;
- security;
- reliability and use of probabilistic methods.

A consensus position was reached on the last four aspects, which was supported by all members of the Committee on Electrical Installations. No consensus position could be reached on the measures for preventing and controlling CCF.

Against this background, the RSK Ad Hoc Working Group on 'Use of Computer-Based Instrumentation and Control Systems' (AG ERL) was established and, at the 426th meeting of the RSK on 20 May 2010, was tasked with drafting a proposal for RSK deliberations on overarching requirements for computer-based instrumentation and control systems important to safety.

The working group is therefore required to compile and justify proposals for overarching requirements for computer-based instrumentation and control systems important to safety intended for use in reactor protection systems. In particular, attention must be paid to requirements designed to ensure the prevention/control of systematic failures (common cause failures – CCF)[1] of computer-based instrumentation and control functions within the framework of the defence-in-depth concept. This compilation is intended to provide a transparent basis for the subsequent RSK deliberations.

As part of the working group's deliberations, an assessment is to be carried out of the current state of international discussions, taking into account the requirements underpinning both planned and completed realisations of computer-based instrumentation and control systems important to safety. In doing so, the working group is to consult relevant international standards and draft standards as well as other relevant sources.

[1] In the following, the term CCF is used exclusively.

In addition to issues relating to instrumentation and control systems, the working group shall also include process engineering issues in its deliberations. The findings of the RSK's ERL working group are set out below. The recommendations contained in the position paper [1.1] regarding the points of

- qualification and complexity; distinction between type testing and qualification testing

- maintenance measures and modifications to computer-based instrumentation and control systems

have been incorporated into the ERL working group's recommendations. The aspect of "security" considered in [1.1] was not discussed by the ERL working group.

2 Terms and abbreviations

2.1 Definitions of terms

- **Failure**: The loss of the ability of a component to perform its required function when specified conditions are met.

  Note: Refers only to hardware, i.e. to objects that change their physical state and may therefore fail. The 'failure' event marks the point in time at which the system transitions from a correct state to a fault state (the terms in [2.1] to [2.3] are used in this sense).

- **Closed-loop simulation**: Simulation of the instrumentation and control system in a closed-loop control circuit in which the output and input values of the instrumentation and control system are coupled to a process model.

- **Common Cause Failure (CCF)**: The failure of two or more structures, systems/subsystems or components (SSC) as a result of a single specific event or cause.
  (source: [2.4])

- **Diversity**: The existence of two or more different methods or means of achieving a specific objective. Diversity is used in particular as a safeguard against CCF. It can be achieved by employing physically distinct systems or through functional diversity, whereby similar systems achieve a specific objective using different methods.
  (source: [2.5])

- **Dissimilarity:** A specific form of diversity for computer-based systems with the diversity characteristics specified in VDI/VDE 3528 [2.6]:
  "A dissimilar technique employs devices that are demonstrably sufficiently dissimilar or distinct in terms of hardware, software, development tools, development teams, manufacturing, testing and maintenance.

  Note 1: The aim is to design independent systems or subsystems in such a way that their indispensable safety-related functions are maintained even in the event of the postulated systematic malfunction of one of the independent systems or subsystems. To this end, the degree of dissimilarity in the characteristics relevant to fault control must be demonstrated."

Note 2: Computer-based systems may also be designed to be diverse in individual aspects without being dissimilar; in this case, the term ‘diversity characteristics’ is used generally in the following.

- **Emulation:** Simulation of the behaviour of a system or device.

- **Fault**: Deficiency in a hardware, software or system component.
  (source: [2.4])

- **Functional diversity:** Application of diversity at the functional level (e.g. deriving a shutdown criterion from pressure as well as temperature limits).
  (source: [2.4])

- **Active malfunction:** A malfunction of an instrumentation and control system in such a way that actuation signals are generated which are not specified in the functional specifications.

- **Passive malfunction:** A malfunction of an instrumentation and control system in such a way that the actuation signals specified in the functional specifications are not generated.

- **Category of an instrumentation and control function**: one of three possible safety classifications (A, B, C) for instrumentation and control functions, determined by the safety relevance of the functions to be performed. If the function is not significant for safety, no safety classification (categorisation) is assigned.
  (source: [2.4])
  Note: DIN EN 61226 [2.7] sets out guidelines for the categorisation of instrumentation and control functions.

- **Class of an instrumentation and control system:** one of three possible classifications (1, 2, 3) of safety-relevant instrumentation and control systems, in accordance with the requirement to implement control functions of varying safety relevance. If an instrumentation and control system does not implement any safety-relevant functions, no safety classification is assigned.
  (source: [2.4])

- **Complexity:** The degree of difficulty in understanding and verifying a system or component due to its design, implementation or behaviour.
  (source: [2.4])

- **Life cycle:** Activities required in connection with the implementation of safety-related systems and equipment within the instrumentation and control system architecture, starting with the derivation of instrumentation and control system requirements from the plant’s safety design basis and continuing until the point at which none of the instrumentation and control systems are available for use.
  (source: [2.4])

- **Computer-based system:** An instrumentation and control system whose functions depend largely or entirely on microprocessors, programmable electronic devices or computers, or are carried out by them.
  (source: [2.4])

- **Independent instrumentation and control systems:** Independent systems have the following characteristics:
  a) The capability of each of the two systems to perform its intended function is not affected by the operation or malfunction of the other system.
  b) The systems' capability to perform their functions is not affected by effects arising from the postulated initiating event for which these functions are required.
  c) Sufficient robustness against common external influences (e.g. earthquakes and electromagnetic interference) is ensured by the design of the systems. (Quelle: [2.5])

  Note 1: Modes of design intended to achieve independence include electrical and physical separation, independent communication, and absence of feedback effects from the processes being controlled.

  Note 2: Whilst independence defined in this way is a necessary condition to ensure that systems will not malfunction simultaneously, it is not regarded in this form, in the context of the text in hand, as being sufficient to control CCF.

- **Malfunction** A deviation of the actual behaviour from the intended behaviour. (source: [2.8])

- **Controlled malfunction**: The malfunction of an instrumentation and control system in a predefined manner (direction) such that a defined state is established at the outputs**.**

2.2 Abbreviations used

AI&CS	Additional instrumentation and control systems
CC	Common cause
CCA	Common cause analysis
CCF	Common cause failure
CCI	Common cause initiator
COTS	Commercial-of-the-shelf
EMC	Electromagnetic compatibility
EN	European norm
FMEA	Failure mode and effects analysis
FTA	Fault tree analysis
HALT	Highly accelerated lifetime testing
HW	Hardware
IEC	International Electrotechnical Commission
ISI	In-service inspection
ISO	International Organization for Standardization
RP	Reactor protection
RPS	Reactor protection system
SW	Software
V&V	Verification and validation

3 Course of discussions

The working group held a total of nine meetings. At its first meeting on 21 May 2010, the working group commenced its work in accordance with the RSK's assignment and drew up a schedule for further discussions. A more detailed account of the proceedings, including a list of the supporting documents, can be found in Appendix 1.

4 Safety-relevant aspects of the use of computer-based instrumentation and control systems important to safety

The use of computer-based instrumentation and control systems now reflects the state of the art in measuring, control and automation technology at both national and international levels. This technology has also found its way into nuclear instrumentation and control systems; at national level, this is particularly evident in the operational aspects of instrumentation and control and in limitation systems, whilst at international level it is also evident in the field of reactor protection.

In this respect, the question arises – particularly in the context of retrofitting or modernisation projects – as to whether computer-based instrumentation and control technology can be used in reactor protection systems. In this context, it should also be noted that the use of software-based equipment technology is becoming

increasingly important in the field of peripheral devices for reactor protection systems as analogue-based equipment technology is often no longer available. Depending on the application, this involves the use of technology that is sometimes complex as the devices in question are generally intended for a wide range of commercial applications.

Computer-based safety instrumentation and control technology has both advantages and disadvantages compared to hard-wired analogue or digital technology. The advantages include:

- improved maintainability;
- inherent capability for self-monitoring and fault detection;
- semi-automated project planning (error-free generation of detailed specifications and code from project briefs);
- reduction of the error rate during implementation through tool-assisted plausibility checks;
- automated documentation of functionality and of change management;
- automated functional testing;
- no drift in the set limits;
- in the event of faults, diagnostic tools allow a more comprehensive and rapid fault analysis than the analogue technology currently in use;
- it is easily possible to implement emulations of instrumentation and control system functions on simulators and to keep the simulators up to date with any functional changes; the simulator thus provides comprehensive support for analysing failure scenarios and allows realistic training of operating personnel even before changes are implemented.

Depending on the specific task at hand, not all of the above aspects will apply.

General disadvantages of computer-based instrumentation and control systems are:

- high functional density on individual assemblies, meaning that a single assembly failure can affect many functions;
- short innovation cycles force change;
- use of more complex components not developed in accordance with nuclear regulations (COTS), e.g. processors, firmware;

- there are new ways for third parties to carry out malicious acts (IT security);

- for licensees and authorised experts, updates provided by the manufacturer are difficult to comprehend (restriction of the four-eyes principle); this also applies to manufacturers with regard to their supplies from subcontractors;

- significant effort required to gain an understanding of the system;

- limited / more difficult assessment of reliability;

- hardware and software are designed with versatility in mind and are therefore more extensive and complex than necessary;

- full verifiability is not possible due to the high complexity of the application-independent system hardware and software.

There remains potential for CCF, particularly in the area of system software, which requires additional measures in the case of homogeneous systems.

5 Requirements of national and international regulations and the need for adaptation

5.1 Requirements under current German regulations

With regard to the prevention and control of CCF in the reactor protection system, the following codes and guides of the German nuclear regulatory framework should be considered:

- BMI Nuclear Power Plant Safety Criteria of October 1977 (SiKri)

- RSK Guidelines for Pressurized Water Reactors, 1996 edition

- KTA 3501 Reactor Protection System and Monitoring Equipment of the Safety System, 06/1985 edition

- KTA 3503 “Type Testing of Electrical Modules for the Instrumentation and Control System Important to Safety“, 11.2005

- KTA 3506 “System Testing of the Instrumentation and Control Equipment Important to Safety of Nuclear Power Plants “, 11.1984

The requirements set out in the international DIN IEC and DIN EN standards, which are also applicable at national level, are outlined in Chapter 5.2.

Criterion 6.1 of the **BMI Nuclear Power Plant Safety Criteria** of October 1977 sets out requirements for the reactor protection system. According to this, a nuclear power plant must be equipped with a reliable reactor protection system that triggers protective actions when specified response thresholds are reached. It must be designed in such a way that it can fulfil its safety function even during maintenance operations in the event of a single fault occurring in the system. Commands issued manually must neither impair nor prevent necessary protective actions. Footnote 5) further specifies how the requirement for a 'reliable reactor protection system' within the meaning of the safety criterion can be met:

> *„As means for the reliable design of the reactor protection system, the following shall, preferably, be applied:*
>
> - *redundant design of components, structural assemblies and subsystems, physically separated installation corresponding to the effective range of possible events leading to a failure,*
> - *use of different types of equipment (principle of diversity),*
> - *largely automatic monitoring with respect to system failure,*
> - *adjustment of components to possible environmental conditions."*

Chapter 7.3 of the **RSK Guidelines for Pressurized Water Reactors** deals with instrumentation and control systems important to safety, with the instrumentation and control system functions divided into three categories. The functions of the reactor protection system fall within category 1. With regard to the prevention or mitigation of systematic failures, the following requirements for instrumentation and control systems important to safety of category 1 should be noted:

> *„Chapter 7.3.2 General Requirements*
>
> *(4) The structure of the instrumentation and control technology of category 1 should be simple. It should reliably enable the necessary demonstrations for qualifying the system.*
>
> *(5) Provisions are to be taken against systematic failures in the design of the instrumentation and control systems important for safety of category 1.*
>
> *(6) It is to be demonstrated that the instrumentation and control systems important for safety of category 1 also fulfil their function if an incidental failure and a systematic failure and consequential failures occur in addition to the accident. A systematic failure does not have to be assumed here if sufficient measures for its prevention are demonstrated. During a case of maintenance, an accident is also to be assumed. Within a period of 100 h the systematic failure and the incidental failure need not be superimposed.*

(9) Incorrect triggering of the safety system is to be prevented considering the failure combinations according to 7.3.2 (6) if accidents having intolerable effects can occur thereby.

(10) The instrumentation and control systems important for safety must not determine the non-availability of the safety system.“

KTA 3501 “Reactor Protection System and Monitoring Equipment of the Safety System” further specifies the requirements for the reactor protection system. With regard to the prevention or control of systematic failures, the following requirements in particular must be observed (requirements that are identical to those in the RSK guidelines are not repeated):

Chapter 4 Design Principles for the Reactor Protection System
4.4 Failure combinations
4.4.1 Basic assumptions

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

a) a random failure	*Z,*
b) plus one common-mode failure (if it cannot be precluded as specified under para (5))	*S,*
c) plus secondary failures.	*F*

(3) During specified normal operation of the reactor plant the failure combination shown in Figure 4-1 regarding occurring design-basis accidents shall be 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.

(5) The effects of systematic failures in the reactor protection system shall be analysed. Depending on the results of the analyses, additional measures shall be taken to reduce the probability of systematic failures or their effects.

N o t e:
The probability of systematic failures can, for example, be reduced through the selection of suitable equipment systems, test cycles and limit load tests to such an extent that the systematic failures in the failure combination referred to in Section 4.4.1(2) no longer need to be taken into account. Mitigating the effects may require additional measures outside the reactor protection system.

4.4.3.2 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 4.4.1, 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 fulfil the required safety-related tasks.

(3) With regard to erroneous actuations of not clearly safety-oriented partial protective actions caused by random failures, the requirements of Section 4.4.1 para. (5) shall be applied.

N o t e:

In designing this part of the reactor protection system, 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.

4.4.4 Erroneous actuations of protective actions

Considering the basic assumptions specified in Section 4.4.1, 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 reactor protection system shall not lead to design-basis accidents with sequential damages.

The test requirements defined in the national regulations at equipment level

- KTA 3503 “Type Testing of Electrical Modules for the Instrumentation and Control System Important to Safety“, 11.2005

- KTA 3506 “System Testing of the Instrumentation and Control Equipment Important to Safety of Nuclear Power Plants“, 11.1984

do not consider the topic area of CCF.

5.2 Overview of regulatory requirements in the IEC, DIN IEC and DIN EN standards regarding the life cycle of computer-based instrumentation and control systems important to safety

In recent years, the IEC-SC45A series of standards has been developed to provide a comprehensive set of regulations governing the use of instrumentation and control systems for safety-related applications, particularly in nuclear power plants. The top-level document for the IEC-SC45A series of standards is IEC

61513 [5.1]. It sets out the general requirements for instrumentation and control systems and equipment used to perform safety-related functions in nuclear power plants.

IEC 61513 “Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems” is a first-level standard that refers to other standards in the IEC-SC45A series which cover general topics such as the categorisation of functions and the classification of systems, software requirements, hardware aspects of computer-based systems, qualification, system separation, measures against common-cause failure, and control room design (second-level standards). The third-level standards of the IEC-SC45A series deal with specific equipment, technical methods or specific activities.

The introductory sections of the IEC SC45A series of standards state that the requirements contained therein are based on the principles and fundamental safety aspects of the IAEA Code for the Safety of Nuclear Power Plants and the IAEA Safety Series. In particular, the requirements NS-R-1 “Safety of Nuclear Power Plants: Design” [5.2] and Safety Guide NS-G-1.3 “Instrumentation and control systems important to safety in Nuclear Power Plants” [5.3] are cited specifically. In the IEC-SC45A series of standards, the terminology and definitions correspond to those used by the IAEA.

The IEC-SC45A series of standards has been incorporated into German standards as DIN-IEC standards, and currently also as DIN-EN standards, by the DKE committee UK 967.1, which acts as the national mirror committee for IEC-SC45A.

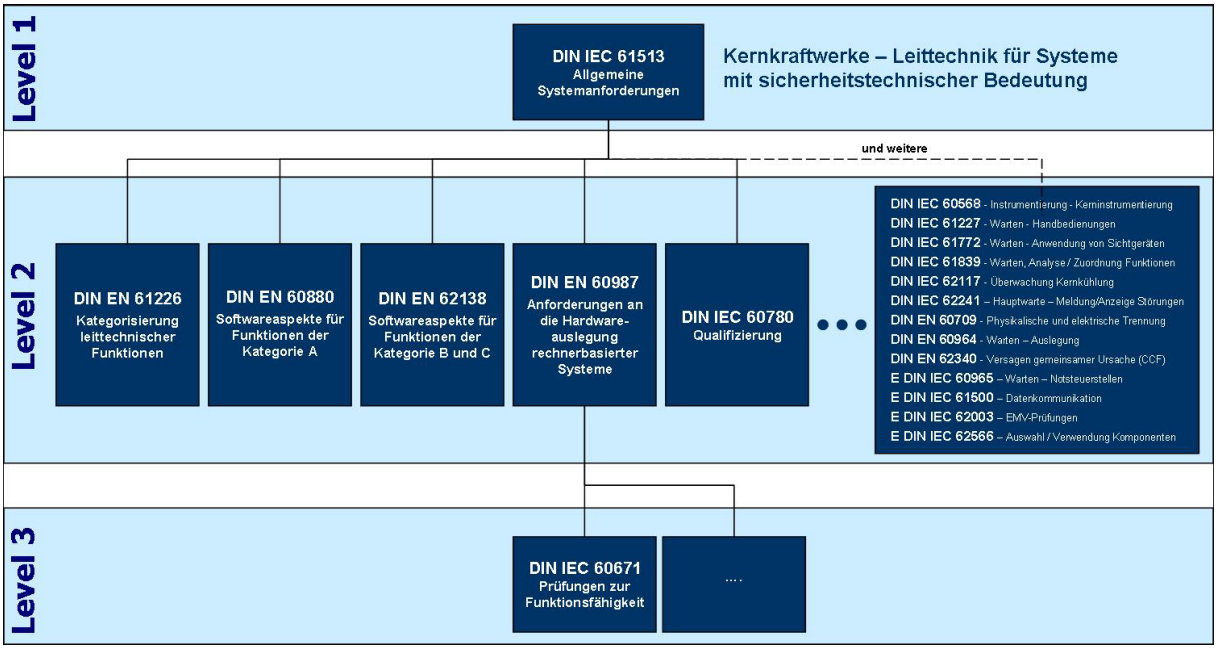

Figure 1: Overview of the DIN-IEC and DIN-EN standards applicable in Germany relating to instrumentation and control systems for safety-related systems in nuclear power plants

The IEC standards series IEC-SC45A, which has been or is being transposed into German standards via DIN-IEC and DIN-EN standards, sets out comprehensive requirements for the design and documentation of the safety lifecycle of computer-based instrumentation and control systems with safety-related functions in

nuclear power plants. These standards contain basic requirements for the prevention and control of CCF in computer-based instrumentation and control systems.

5.3 Need for amendments to German regulations

Due to their position in the hierarchy of regulations, the national regulations mentioned do not specify detailed verification procedures or associated requirements.

When implementing computer-based instrumentation and control systems, it remains necessary – given the complexity of the equipment used and the system design – to assess whether the diversity or dissimilarity incorporated into the instrumentation and control architecture is sufficient to prevent and control CCF as the regulatory framework does not contain any specific assessment criteria or detailed verification requirements in this regard. Of particular significance to the discussion regarding the design of computer-based instrumentation and control systems is the fact that it is not possible to demonstrate that systems are completely error-free and that latent errors cannot, in principle, be ruled out. Since a CCF cannot therefore be ruled out for computer-based instrumentation and control systems, the requirements contained in the regulations regarding analyses and verification must be met in order to sufficiently reduce the probability of a CCF occurring within a subsystem and to limit the occurrence of a CCF to subsystems through a suitable overall architecture, thereby controlling it.

Measures at equipment level and for quality assurance are designed to minimise CCF by ensuring high quality and robustness. By contrast, measures to control CCF are primarily appropriate at system level, meaning that corresponding amendments to the aforementioned system-related regulations RSK Guidelines and KTA 3501 are required.

The nuclear standards of IEC, DIN-IEC and DIN-EN provide a framework for addressing CCF and specify preferred countermeasures. These primarily involve defence-in-depth and the application of functional diversity together with measures to prevent fault propagation. With their proposed measures, they remain at the system level and do not adequately address the identification of potential common cause (CC) initiators and vulnerabilities at equipment level.

However, to ensure an optimal and verifiable CCF design at system level, the specific CC initiators and CC vulnerabilities at equipment level that are to be addressed by the system must also be known as far as possible. In this regard, the ERL working group considers it necessary to apply procedures that go beyond the current state of the art in the standards of the nuclear regulatory framework (see Chapter 5.4). As outlined above, the test requirements defined in the national regulations at equipment level

- KTA 3503 “Type Testing of Electrical Modules for the Instrumentation and Control System Important to Safety“, 11.2005

- KTA 3506 “System Testing of the Instrumentation and Control Equipment Important to Safety of Nuclear Power Plants“, 11.1984

do not consider the topic area of CCF. Although it is common practice to include system characteristics relevant to the CCF issue in type testing in addition to simply testing the components, this practice has not yet been incorporated into national regulations. Under the current regulatory framework, additional requirements are therefore necessary. A corresponding amendment must also be taken into account as part of the forthcoming revision of KTA 3503. This is discussed further in Chapter 12.

If the approach based on equipment dissimilarity is adopted, this requires an assessment of the appropriate level of dissimilarity. Consequently, the existing scope of verification must be supplemented by an examination and assessment of the differences in equipment technology; like type testing, this requires in-depth system information at the development level from the user’s perspective. The relevant requirements for this still need to be defined.

5.4 CCF Analysis

Effective measures to prevent or control CCF require a systematic analysis of the potential CCF mechanisms and common-cause initiators for the respective operating conditions. The aim of the analyses should be to gain a better understanding of the potential common-cause mechanisms and initiators and, on that basis, to make targeted and effective use of i.a. functional and/or equipment diversity. CCF analyses can be used as both a verification and a design method.

Overall, the following findings and recommendations emerge regarding the performance of CCF analyses:

- CCF Analysis: Each redundant system configuration must be analysed as part of a CCF analysis to assess its behaviour in relation to potential common-cause initiators (CCI), regardless of whether the system configuration is homogeneously redundant or diversely redundant.

- Analysis guidelines: The nuclear regulatory framework currently contains no requirements regarding CCF analysis. The ERL working group therefore recommends that, in order to establish a basis for a standardised approach, guidelines for conducting CCF analyses at the equipment and system levels be developed in the near future, bringing together the individual methods specified in various standards: FTA (Fault Tree Analysis), FMEA and CCA. In addition to the nuclear standards of the IEC regulations, standards [5.4] to [5.9] in particular should be consulted in this regard.

- CCI catalogue: As a basis for CCF analyses, a catalogue of initiators for software and hardware CCFs that must be considered as a minimum should be compiled within this framework. The catalogue should be based on the current state of knowledge regarding potential CCI. Experience with instrumentation and control systems used in nuclear engineering should also be taken into account. The catalogue is to be kept up to date by a body appointed for this purpose. To this end,

information on potential CCI is to be collected and evaluated. Service letters issued by manufacturers of computer-based instrumentation and control systems important to safety used in German plants are to be taken into account.

- HALT tests: In the aviation industry, the HALT (Highly Accelerated Lifetime Testing) procedure has been introduced to determine the resilience of a subsystem when subjected to a multitude of external influences simultaneously. The tests are usually carried out until the first components fail. For computer-based systems intended for use in reactor protection applications, the HALT test should be applied unless no additional insights are expected to be gained from it. To assess whether HALT tests are necessary, the test results from type testing and the aforementioned CCI catalogue should be consulted. The component-specific stressors to be considered in the HALT tests should be derived from the aforementioned CCI catalogue.

- Monitoring of operating experience: For computer-based instrumentation and control systems and field devices used in Germany for Categories A and B, it is important – in order to ensure the required high level of reliability – that operating experience and system information are made available to authorities and authorised experts in a secure information exchange so that the implementation of any necessary measures is ensured. This information is generally communicated by the manufacturer to their customers in the form of product notifications. A suitable procedure must be established for the exchange of information, e.g. in the form of regular system reports from the operators, or reports triggered when required, containing the product information provided by the manufacturer and the measures derived from this information in the plant.

6 Aspects of CCF prevention

6.1 Aspects of the operation of computer-based instrumentation and control systems important to safety that perform Category A functions

The IEC standards require computer-based instrumentation and control systems important to safety to operate in a manner that ensures the system is robust against initiating events originating from the process. According to DIN IEC 61513 (Section 5.3.1.5) [6.1], class 1 instrumentation and control systems and their auxiliary systems must be designed to be independent of factors influencing the processes of the plant. Furthermore, DIN IEC 61513 (Section 6.1.1.2.2) stipulates i.a. that specific development techniques must be applied to class 1 equipment in order to ensure a high degree of reliability with regard to deterministic behaviour.[2] In DIN EN 62340 [6.2], Section 8.1 requires that instrumentation and control systems performing Category A functions must not be dependent on the requirement profile in their operation and functioning. This overarching requirement is underpinned by individual requirements.

[2] "c) In order to provide a high degree of assurance of deterministic behaviour, class 1 systems should be developed using techniques such as those of appendix B of IEC 60880 (notably B2.d on execution time and B2.e on interrupts). Techniques using static scheduling of operations (see note 2) are preferable to those using interrupts."

Software-based digital automation devices for reactor protection systems designed in accordance with IEC standards are therefore intended to operate sequentially and cyclically and to demonstrate a high degree of reliability in terms of deterministic behaviour. These requirements of the IEC standards apply to all instrumentation and control systems that perform Category A functions, which includes:

- measured data acquisition for the reactor protection system;
- reactor protection system;
- priority control, including priority unit protection;
- instrumentation and control systems for the necessary auxiliary systems (e.g. emergency power supply).

It should be noted that, in practice, outside the central instrumentation and control system (reactor protection system), equipment that does not meet all the requirements of the IEC standards is used in individual cases, even for Category A functions. The reason for this is that equipment designed in accordance with IEC standards is not available for all applications, and it is therefore necessary to rely on standard industrial products. This gives rise to the following requirements:

- For the execution of Category A functions, equipment must always be used that meets the requirements of the IEC standards governing the operation of computer-based instrumentation and control systems performing Category A functions (in particular IEC 61513, 60880 and 62340). In particular, all computer-based devices in Category A instrumentation and control systems (central units, peripherals) must be based on strictly sequential and cyclical software processing and demonstrate a high degree of reliability in terms of deterministic behaviour (predictability). Interventions in the timing of processing and in the processing sequence, such as those caused by interrupts or other hardware units, and interventions in data by other hardware units must be justified and controlled by additional safety measures.
- Where in individual cases no equipment technology is available for Category A functions that complies with the requirements of the IEC standards regarding the operation of computer-based instrumentation and control systems, any deviations in the mode of operation must be documented and it must be demonstrated that this mode of operation and the associated CCF cannot result in any impermissible safety-related consequences within the plant.

6.2 Aspects of fundamental quality requirements at the process engineering/instrumentation and control interface

DIN EN 62340 [6.2] attaches great importance to the use of functional diversity as a means of ensuring independence and managing CCF. The rationale is that, by assigning different tasks, functional diversity helps to mitigate the effects of the following two types of error:

a) error in the task formulation;
b) error in the implementation of the task (relates to the application software).

The implementation of functional diversity is only possible to a limited extent in existing German plants.

As high quality in the formulation and implementation of the task specification is a key factor in minimising the likelihood of a CCF, quality assurance measures aimed at preventing the aforementioned types of errors take on added importance. To this end, the task specification should be formulated such that it is both unambiguous and equally understandable to both instrumentation and control engineers and process engineers. In addition, further efforts are required to detect errors, such as extended testing procedures, closed-loop simulations and simulations incorporating process engineering. The following general requirements can be derived from this:

- The completeness and correct implementation of the process-based task formulation must be ensured through high-quality preparation of the specification and its processing at the interface between instrumentation and control engineering and process engineering as well as through appropriate test procedures and simulations.

  The process-based task formulation must therefore:

  - take all safety-related features into account (completeness);
  - be unambiguous and specified in a formalised manner;
  - be simple, so that a full inspection is possible;
  - also include test cases and the expected test results, which can be used to verify the correctness of the implementation.

  Suitable test procedures and simulations to ensure the completeness and correct implementation of the task include, in particular:

  - closed-loop simulations (‘knowing tests’) that take into account feedback from the process (e.g. staggered excitation of components);
  - system testing in the test environment (integration test).

It should furthermore be noted that all system states must be adequately taken into account in the specification. This means that special states which may occur in the systems (e.g. disconnections) must also

be considered in sufficient detail. The process-related task must therefore contain explicit statements with regard to

- in which operating states the relevant function must be available,
- what states at the interfaces need to be taken into account as a result of inspection and repair work.

With regard to error type b), having different development teams implement the task independently using different development environments can reduce the likelihood of identical implementation-related errors. This is the case, for example, when different hardware is used alongside application software developed by different manufacturers.

7 Diversity as a contribution to CCF prevention / control

7.1 Diversification of internal states of computers

Errors arising from specific internal states of computers can be controlled by limiting them to a small number of computers, provided that sufficiently different internal states of the computers are enforced. The DIN IEC standard requires that independent instrumentation and control systems be operated with different signal paths (DIN IEC 61513 [7.1] – Clause 5.3.1.5). The rationale behind this requirement is to avoid identical internal states of the computers. According to DIN IEC 61513, this can be ensured through diversity (e.g. equipment diversity or functional diversity).

DIN IEC 62340 (clause 5.5) [7.2] states that the allocation of diverse functions to independent instrumentation and control systems can be used as a means of ensuring different signal paths when operating the instrumentation and control systems. Section 7.3.1 requires that functional diversity must be applied to diversify the 'input signal' component of the signal paths.

Essentially, the safety functions determine the internal states of the respective computers. They represent the loads on the hardware and the operating system. Viewed macroscopically across the entire system, there are no changes in load; however, viewed microscopically in relation to the individual CPUs, there certainly are. The chain "different safety functions → different loads at the microscopic level → different internal states of the computers" forms the basis for classifying functional diversity as a possible means of mitigating a CCF by diversifying the internal states of the computers.[3] As already noted, the implementation of functional diversity in existing German plants is only possible to a limited extent. Therefore, other measures are

[3] **Comment by Dr. Graf:**
Diversifying the internal states serves to rule out a potential CCF for non-cyclical load cases. For services used purely cyclically (HW + SW), a CCF can be ruled out once a cycle has elapsed, as there is no initiator. However, there are also non-cyclic load cases in the application. As the measuring signals from the process do not change cyclically, the memory area in which the derived calculation results are stored e.g. is occupied by constantly varying values. It is precisely for these non-cyclically used services that the diversification required by the IEC comes into play.

required to diversify the internal states of the computers. The following minimum requirements are derived from this:

- Where there is a lack of functional diversity, the diversification of the internal states of the computers must be achieved through instrumentation and control technology or equipment diversity. Suitable measures for diversifying internal states in the case of homogeneous equipment technology may include, in particular:

    - different configurations of the input/output channels,
    - different processing sequences for the instrumentation and control functions,
    - different standardisation of the measuring signals used,
    - asymmetric implementation of additional monitoring functions,
    - different implementations of the functions.

It must be demonstrated that the measures implemented are sufficiently effective in terms of diversifying internal states.

If different equipment technology with different operating systems is used, the internal states of the various computers will differ due to their design.

1. Comments by the advocates of Architecture 1: *Description of the architecture: see Chapter 8*

In contrast to the significant benefits of functional diversity for error types a) and b) in Section 6.2 within the application software, the effect of enforcing different states for the system hardware and software is not considered effective.

Diversification of the internal states of the system hardware and software (i.e. not in the application software, which constitutes the technical implementation of the functional specifications) is not feasible due to the properties required by DIN EN 60880. Thus, the required strictly cyclical operation of the system software – which is to be independent of the influencing factors of the plant process and separate from the application software – and the invariance of processing and communication load conflict with the intended influence on the internal states of the system hardware and software by the measuring signals of the plant process. This applies both to functional diversity and to the use of diverse measuring instruments. It should be noted here that, when using diverse measuring instruments for the same physical measurand, only sensor technologies based on different physical measuring principles are employed. Analogue transducers generally output a signal of 0/4–20 milliamps, which is then converted in most cases into a 0–10 V signal. However, the different measuring principles and the signal conversion do not result in the signal trajectories differing. The substitute measures listed in the bullet list generally result in even less diversification of the input signals. This means that it is not possible to demonstrate the effectiveness of the proposed diversification measures with regard to preventing CCF.

Section 5.5 of DIN EN 62340 already identifies both functional diversity and equipment diversity (referred to here as 'dissimilarity') as measures for ensuring different signal trajectories (which, by definition, also encompass the internal states of the computer system). Similarly, in 7.3, the effect of functional diversity is restricted to the 'input signal' component of the signal path, and it is pointed out that the other parts of the path, such as the internal states, must also be considered. An effect for enforcing different internal states can only result from the use of proven dissimilar processing levels.

1. Comments by the advocates of Architecture 2 *Description of the architecture: see Chapter 8*

The system properties required by DIN IEC 62340 ensure that the vast majority of a computer's internal states either do not change or change cyclically and therefore cannot initiate a CCF. However, a few internal states remain that are influenced by the calculated functions, as e.g. the results of a function's calculation are also stored in memory areas and are thus a subset of the internal states. To mitigate a CCF that could be initiated via these few influenceable internal states, DIN IEC 62340 requires that diverse functions be implemented in independent instrumentation and control systems. The rationale behind avoiding CCF in this context is that a latent, possibly undetected systematic error would need to be triggered simultaneously in different trains in order to result in a CCF. Accordingly, the aim is to ensure that identical numbers, combinations of numbers and sequences will not occur simultaneously in the independent subsystems. For this measure to be effective, it is entirely irrelevant whether physically diverse functions are actually

implemented or whether the same functions are implemented in different ways. Both approaches result in the few internal states of the computers that can be influenced by these functions being different.

7.2 A comparison of architectures implemented in the USA, France, Japan and Finland with regard to the use of diverse systems

This chapter outlines the solutions for digital instrumentation and control systems important to safety in nuclear power plants that have been accepted by regulatory authorities in various countries and have been implemented or are currently being implemented on this basis. The presentation focuses on the architecture principles and their integration into the safety concept as well as on the use of a diverse design for instrumentation and control systems assigned to identical or different levels of defence. The term "instrumentation and control systems important to safety" is used here to encompass reactor protection as well as other instrumentation and control installations for controlling accidents involving the superposition of CCF.

USA

The retrofit of the reactor protection system at the Oconee nuclear power plant, Units 1 to 3, for which a licence was granted by the US NRC in January 2010, is cited as an example of a design approach accepted in the USA for digital instrumentation and control systems important to safety. The following description is based on this licence [7.3].

The new reactor protection system at the Oconee nuclear power plant consists of a combination of a primary, redundant digital reactor protection system and diverse redundant backup systems of different technical designs.

The primary digital instrumentation and control system important to safety is divided into the Reactor Protection System (RPS), which initiates reactor scram (RESA), and the Engineered Safeguards Protection System (ESPS), which activates the safety systems. The RPS has a four-channel configuration (2-out-of-4 selection), whilst the ESPS comprises two subsystems, each with three channels (2-out-of-3 selection). One ESPS subsystem is implemented on the hardware components of three channels of the RPS, whilst the other ESPS subsystem is implemented on its own components. The ESPS subsystems are implemented on identical hardware with identical software, i.e. without diversity features.

The diverse backup functions for managing design-basis accidents with a simultaneous software-based CCF are distributed across several systems. On the one hand, an existing two-channel ATWS system (PLC technology) is used to cover transients; on the other hand, a hard-wired, three-channel system (with 2-out-of-3 selection) has been retrofitted to manage small- and large-scale loss-of-coolant accidents. The backup systems are constantly active and have their own actuation criteria. They meet quality requirements based on the requirements for standard industrial systems. Manual actions are only taken into account (with one exception assessed by the NRC) if they are not required within the first 30 minutes after the occurrence of the accident.

The overall design of the instrumentation and control systems important to safety thus comprises a redundant reactor protection system combined with diverse backup systems, the functional scope of which, when implemented in a redundant configuration, provides comprehensive coverage of the spectrum of events under consideration.

France

This section outlines French practice with regard to the design of the instrumentation and control system important to safety at the Chooz B nuclear power plant, which was commissioned in 1996 and belongs to the N4 reactor series.

According to the descriptions in NUREG/CR-7007 [7.4], the instrumentation and control system important to safety of the N4 consists of a primary reactor protection system and a diverse backup system; both systems are software-based digital instrumentation and control systems.

The primary reactor protection system is fundamentally designed as a four-channel system with 2-out-of-4 selection circuits and in some sections as a dual four-channel system. Elements of functional diversity and different signal paths are achieved within the primary reactor protection system through the use of diverse process variables, supported by the implementation of computational circuits for different functions on separate processors.

The secondary backup system (ATWS system) controls a limited range of initiating events. In accordance with NUREG/CR-7007, it is actuated exclusively by the ‘steam generator level low’ criterion, which covers the most frequent transients identified by probabilistic analyses. The backup system is implemented on hardware that differs from the primary reactor protection system and uses a different programming language at the application level. The system is subject to - graded - quality requirements.

In essence, this results in an integrated system featuring a high degree of redundancy in the primary reactor protection system and a reduced scope of functions for the instrumentation and control system of the diverse backup system.

Japan

This description is also based on the information provided in NUREG/CR-7007 [7.4], in this case for the Kashiwazaki-Kariwa 6 and 7 reference plants, the first Advanced Boiling Water Reactors (ABWRs) commissioned in 1996 and 1997, respectively.

The instrumentation and control systems important to safety of these nuclear power plants consist of a primary digital reactor protection system and a hard-wired backup system (ATWS system).

The primary reactor protection system is designed with four-fold redundancy using 2-out-of-4 selection circuits based on digital technology. Functional diversity is employed in the reactor protection system

wherever possible. In doing so, diverse technical implementations are utilised for several safety functions (e.g. two different high-pressure injection systems). The introduction of digital technology in the reactor protection system was preceded by a long-standing process of introducing digital instrumentation and control systems in Japanese nuclear power plants, initially at the operational level and subsequently in the control of safety systems. Based on this long-standing experience and the use of proven software development tools, the potential for CCF in Japan is considered to be low.

The diverse backup system (ATWS system), which is hard-wired, has a limited range of functions. It can trigger reactor scram via a diverse mechanism and shut down the forced-circulation pumps. In addition, provision is made for the manual actuation of safety functions. For this purpose, a separate, hard-wired instrumentation and control system is installed, enabling staff to actuate a number of selected safety functions from the control room via hardware switches and logic circuits. The actuation paths are independent of and diverse to the digital protection system.

The design of the instrumentation and control systems important to safety at the Kashiwazaki-Kariwa Units 6 and 7 in Japan thus combines redundancy in the reactor protection system, utilising functional diversity, with a diverse backup system with a limited scope of functions.

Finland

The EPR in Finland also employs, in accordance with NUREG/CR-7007 [7.4], a combination of a redundant primary digital reactor protection system and a backup system of a different technical design for the instrumentation and control systems important to safety.

The primary reactor protection system, which utilises digital technology, consists of two subsystems, each of which is configured with four-fold redundancy. In accordance with NUREG/CR-7007, functional diversity is applied to the subsystems by using different parameters and functional relationships for the initiating events. It is intended that this will result in differently programmed application software whilst using identical hardware and an identical operating system.

The backup system consists, for one, of a digital instrumentation system with hardware and software that is different from the reactor protection system, designed to control the more frequent initiating events. In addition, there is a hardware backup system with programmable logic devices (PLD technology) which serves to provide a redundant actuation for reactor scram as well as the option to manually actuate protective actions. The digital backup system is configured with dual redundancy, whilst the hardware backup system is four-channel (2-out-of-4 selection).

This results in an overall system featuring diversity characteristics at the level of the reactor protection system, combined with a diverse (in this case, even twofold diverse) backup system with a limited scope of functions.

8 Presentation of two architectures for controlling CCF within the framework of the defence-in-depth concept

The ERL working group has conducted an in-depth discussion of two architecture approaches for the use of computer-based technology in reactor protection systems. The first approach is based on the use of dissimilar equipment, whilst the second approach is based on the use of two independent reactor protection subsystems with diverse characteristics, as well as "additional instrumentation and control systems" (*zusätzliche leittechnische Einrichtungen* - ZLE). Furthermore, other architectures are conceivable, but these were not discussed by the ERL working group.

In the opinion of the ERL working group, the following applies to both approaches with regard to the need for diversity to control CCF:

- For a (largely) homogeneous, redundantly configured and computer-based system, the occurrence of a CCF cannot be considered so unlikely that it need not be assumed when the system is used for reactor protection on level of defence 3. Therefore, at least two independent (sub)systems must be used to control CCF.[4]

- Diversity is a necessary (but not sufficient) means of ensuring an independent failure behaviour of subsystems within the instrumentation and control system important to safety. To control the CCF potential of computer-based systems, the use of diverse subsystems is required within the overall architecture.

- Diversity should be applied in a targeted manner, taking into account potential CCF mechanisms (i.e. diversity decisions appropriate to the intended objective must be made). To this end, relevant CCF analyses must be carried out (see DIN IEC 61513 and associated standards).

- It cannot be entirely ruled out that CCF analyses may fail to identify previously unknown error types or initiators that could lead to a CCF.

Regarding a suitable overall instrumentation and control system architecture, there are differing views within the ERL working group. These stem from differing assessments of the robustness of the results of CCF analyses – that is, the probability that CCF mechanisms not taken into account in the analyses will come into play – as well as the robustness of evidence regarding the effectiveness of implemented functions in ensuring a controlled malfunctional behaviour (for this key aspect, see Chapter 9). This gives rise to two different approaches to the overall architecture.

Architecture 1 does not focus solely on the quality of the equipment as demonstrated during type testing as it is considered impossible to achieve the same level of in-depth understanding of all the equipment's characteristics in modern equipment technology, as was possible with previous technology. For this reason, supplementary architecture-related approaches involving the use of dissimilar equipment technologies within

[4] Requirements for independent instrumentation and control systems are set out i.a. in sections 7.1 and 7.2 of the IEC 62340 standard.

a coordinated overall architecture are deemed necessary. The assessment of adequate dissimilarity – i.e. an examination and assessment of the differences in equipment technology – must be added to the existing scope of demonstrations, with information from the type tests being used in the assessment of dissimilarity. As with type testing, information on equipment development is required for this assessment in order to determine the differences in functional and implementation principles as well as the absence of commonalities, e.g. in algorithms, hardware and software components, and tools.

Architecture 1 requires the use of at least two independent and dissimilar reactor protection subsystems. Depending on the potential consequences of active functional failure, certain functions may require three independent and dissimilar reactor protection subsystems, as well as a selection circuit (voter), or implementation using hard-wired technology based on discrete components (see Chapter 9). A CCF caused by the equipment technology that affects more than one reactor protection subsystem is considered so unlikely as a result of the dissimilar design that it is practically excluded. In the event of a CCF in one of the reactor protection subsystems, the dissimilar subsystem (or subsystems) is therefore always available for event control. No additional measures are required on level of defence 4 as CCF control must already be achieved through the measures provided on level of defence 3.

2. Comments by the advocates of Architecture 2:

To manage active functional failures, Architecture 1 requires three dissimilar reactor protection subsystems linked via a selection circuit (voting). It is precisely in this interconnection of the three different device systems at the system level that a significant risk of new and even more complex failure modes with the potential for CCF failure is identified. On the one hand, the selection circuit creates dependencies between the dissimilar reactor protection subsystems by triggering protection challenges only when they are present in at least two of the three reactor protection subsystems, and on the other hand because as a result, they simultaneously alter the timing behaviour of the protection challenges.

There is no operating experience worldwide in the field of nuclear technology with such system architectures in reactor protection applications, so the advantage of this new system architecture over the globally proven backup solutions is not apparent.

Architecture 1 is justified as follows:

- Complexity of modern equipment technology; The introduction of computer-based control systems has led to a significant concentration of instrumentation and control functions into just a few modules. Furthermore, the hardware of computer-based instrumentation and control systems offers greater functionality and flexibility compared to hardwired systems. Furthermore, due to the transition to serial processing and the incorporation of new development and manufacturing technologies - including highly integrated commercial-off-the-shelf (COTS) components and software elements - into modern equipment technology, the development effort required is significantly greater than with previous technology. This leads overall to a significant increase in complexity within the equipment technology and thus to behaviour that is more difficult to

predict in the event of failures or malfunctions which cannot be adequately addressed by the previous type testing procedure alone.
These arguments are not invalidated even when simple functional principles are used. Even though in equipment technology functional principles are implemented in the system software in line with the requirements of the IEC standards (see Chapter 6.1), thereby achieving greater robustness, the issues outlined - such as complexity and limitations on testability - still persist. With regard to potential CCF, the assessment of equipment technology cannot be reduced to these "simple functional principles" and the technology consequently classified as "simple" in the same way as the hard-wired technology used.

- Short innovation cycles; Given the rapid pace of innovation and the high complexity of computer-based technology, a demonstration of proven operating experience is now only of limited use.

- Testability; The COTS components used in computer-based equipment technology often cannot be assessed in detail (due to the lack of relevant development documentation, etc.). This applies to the equipment manufacturer, the operator and the authorised experts alike. The associated difficulties are illustrated using the example of the authorised expert but also apply to the other parties involved in the process. Furthermore, the almost unmanageable variety of processor types, computer architectures, operating systems, programming languages, engineering tools, specific controller modules, communication protocols, etc., means that inspectors can only go into relatively shallow detail. Experience shows that these checks ultimately serve to ensure that documents remain compliant with regulations, to verify that the basic functional requirements are met, and to confirm that authorised bodies have carried out the necessary environmental assessments. Software checks, such as code inspections or even very extensive tests on the machine itself to rule out systematic errors, cannot be replicated in a finished product in the long term. The practice of review and testing throughout the development process, which was often advocated in the past, is no longer feasible under today's market conditions. This situation is exacerbated in the case of type-change tests, which, due to the rapid innovation cycles of COTS components and the practical impossibility of verifying the absence of retroactive effects from minor changes, exhibit an even greater imbalance between the required testing effort and the available testing time.

- Modifications; The addition of potential new errors as part of future changes is becoming increasingly important due to the complexity involved, particularly when the system's original developers are no longer available.

- CCF analyses; The conclusiveness of CCF analyses is insufficient to rule out CCF on level of defence 3 on this basis. This is because such a profound understanding of the system cannot be achieved for computer-based instrumentation and control systems[5] and because systems can only be designed to counter known CCF mechanisms. An evaluation of operating experience across

[5] This applies to both the manufacturer and the authorised expert (the four-eyes principle).

various technical fields shows that new mechanisms continue to emerge which have not previously been observed in global experience.

- Controlled malfunctional behaviour; The effects of a CCF cannot be narrowed down through analysis of the system's properties to such an extent that a malfunction deviating from an implemented, controlled malfunctional behaviour on level of defence 3 no longer needs to be assumed. Reasons for this include, for example, malicious software (malware), hardware faults, or manufacturing defects.

Architecture 2 focuses on a deep understanding of the system, complemented by the use of diversity within the framework of a tiered overall architecture.

Architecture 2 requires the use of two independent reactor protection subsystems with diversity features as well as additional instrumentation and control systems. The diversity features of the reactor protection subsystems are derived within the framework of the CCF analysis, i.e. (at least) the level of diversity required to control the CCI under consideration is implemented. Each reactor protection subsystem has a full range of functions. A CCF affecting one reactor protection subsystem is assigned to level of defence 3 and is controlled by the second reactor protection subsystem. Based on the CCF analysis, a CCF affecting both reactor protection subsystems is considered so unlikely that it can be assigned to level of defence 4.[6]

2. Comments by the advocates of Architecture 1:

The proposal for Architecture 2 stipulates that the CCF of both reactor protection subsystems must be assigned to level of defence 4. This would only be permissible if it were practically impossible for the CCF to affect both subsystems. Such practical impossibility would be established if the probability of this event occurring were less than 10^{-7}/a, as is the case for the hard-wired reactor protection system currently in use. As there is currently no probabilistic method for assessing the reliability of computer-based instrumentation and control systems, such an exclusion cannot be demonstrated. Nor can such values for the CCF be derived from operating experience. Ultimately, this means that the equipment for the additional instrumentation and control functions must be assigned to level of defence 3.

3. Comments by the advocates of Architecture 2:

The statement that there is currently no probabilistic analytical method for assessing the reliability of computer-based instrumentation and control systems applies to both architectures. This also concerns the voter problem (see comment 2).
However, it is certainly possible to derive estimates of reliability or failure rates from operating experience. This approach is also used internationally to conclude that the probability of a CCF is less than 10^{-x}.
Naturally, when evaluating operating experience, any changes to components or systems must be assessed to determine whether these changes could be relevant in terms of CCF potential, which in turn requires an

[6] The quality of the CCF analysis and the CCF guidelines as well as the completeness of the CCI catalogue (see Chapter 5.4) are therefore of great importance.

understanding of the system with regard to possible CCF mechanisms. However, this is nothing out of the ordinary as such an understanding of the system with regard to possible CCF mechanisms is also required, for example, for a dissimilarity check.

In the event that a CCF affects both reactor protection subsystems, additional instrumentation and control systems are available to prevent breaches of fundamental safety functions in the event of an assumed CCF in the reactor protection system. The additional instrumentation and control systems should preferably be implemented using a different technology to that of the reactor protection subsystems (e.g. hardware-based) so that they are not affected by software changes. They are technically characterised as follows:

- The additional instrumentation and control systems are subject to verifiable quality requirements, which are yet to be defined.

- The additional instrumentation and control systems are to be designed to come into effect in the event of a CCF affecting the entire reactor protection system and must not impair accident control, provided the reactor protection system is functioning correctly (non-interaction). Non-interaction can be ensured

    - either by specifying that the additional instrumentation and control systems will only be activated redundancy-wise upon a CCF in the reactor protection system following the shutdown of the associated redundant trains of the reactor protection system triggered by the combined action of all monitoring devices (internal and external monitoring). This requires monitoring equipment on the reactor protection system computers that can detect a CCF in the reactor protection system with a high degree of certainty and reliably activate the additional instrumentation and control systems;
    - or by specifying for additional instrumentation and control systems that are constantly active (activating components when downstream limit values are reached) that their active functional failure can be ruled out or will not have any unacceptable consequences. Activation via a CCF monitoring system is not required.

- They are designed to be “simple” in structure, thereby ensuring a high degree of reliability and a low error rate. Compared to the reactor protection system, this results in a reduced scope of functions:

    - no analysis boundary conditions for level of defence 3 (in particular, no application of the single-failure concept);
    - control of parts of the event spectrum by ensuring vital functions (see Chapter 9.3).

3. Comments by the advocates of Architecture 1:

The fundamental problem with additional instrumentation and control systems, particularly when they meet lower quality and design requirements, is that, on the one hand, the function is supposed to be

activated when required (CCF in reactor protection), but, on the other hand, there should be no unintended side effects.

Two options are mentioned for additional instrumentation and control systems. In the first option, in addition to the reactor protection subsystems, external monitoring is also required for each subsystem. By deactivating the additional instrumentation and control systems during normal operation, feedback effects are reliably prevented; however, there remains the problem of reliably detecting an active or passive erroneous activation in reactor protection solely by monitoring reactor protection (not the process!). Currently, there are no specific details regarding the scope of the external monitoring test function (see footnote 10 in Chapter 9.2).

In the other variant, the additional instrumentation and control systems are always in operation. It is unclear how "an active functional failure" is to be technically "excluded", particularly with equipment that is subject to quality requirements that are less stringent than those for the reactor protection system. A necessary but not sufficient requirement for this would be that the additional instrumentation and control systems must at least meet the single-failure criterion and that the quality requirements corresponding to those for the reactor protection system must be met. Further comments: see remarks on Chapter 9.2 Architecture 2.

Architecture 2 is justified as follows:

- Complexity of modern equipment technology; Deliberate avoidance of those features of modern device technology that contribute to its complexity (including the avoidance of concurrent processes and process-induced interrupts). Use of an equipment system with simple and verifiable operating principles which exhibits all the characteristics of continuously and deterministically operating systems in its operational and failure behaviour, performing the same functions in the same manner during both normal operation and in the event of a malfunction. This is accompanied by a correspondingly simple hardware design that preserves the essential characteristics of proven reactor protection systems.
  Maintaining a straightforward task specification for instrumentation and control systems important to safety in nuclear power plants and supporting the design process with problem-oriented design tools offering extensive verification and testing capabilities. These design tools allow for a much more thorough verification of the task specification than would be possible with hard-wired equipment.

- Short innovation cycles; Deliberate renunciation of continuous manufacturing processes – with their resulting short innovation cycles – and a shift to batch production with the associated inventory management so that innovations can be planned and implemented in a targeted manner.

- Testability; The testability of a piece of equipment is defined by the achievable level of thoroughness of testing, which in turn is largely determined by its internal operating principles. By making targeted use of equipment with simple operating principles, it is therefore possible to achieve an extremely high level of thoroughness of testing with regard to safety functions, which

even exceeds the achievable level of thoroughness of testing for hard-wired equipment. For example, during a test, it is not only possible to monitor the input and output signals; all internal registers and signals of a function can also be monitored externally during the test, meaning that faults which do not initially affect the output signals can also be detected. A key advantage over hard-wired equipment is that “installed on site” is practically the same as “designed and set up in the test environment”, thereby minimising wiring faults that can sometimes be difficult to locate during on-site installation. This applies in particular to wiring modifications that need to be carried out on site.

- Modifications; In principle, all the project engineering and testing tools used in the design of the systems are also available for making modifications. Consequently, modifications can be carried out to the same high standard as the design of the systems themselves. The use of an approach based on standardised equipment technology offers significant advantages in terms of the man-machine interface. This applies, for example, to the consistency of documentation, staff training, or the standardisation of signals in the control room.

- CCF analyses; By restricting the system to simple operating principles, the potential impact of latent faults is also significantly reduced. When carried out appropriately, the informative value of a corresponding CCF analysis is sufficient to rule out, on this basis, a CCF on level of defence 3 that would lead to the malfunction of both reactor protection subsystems. The in-depth understanding of the system required for this can be achieved even for computer-based instrumentation and control systems when limited to correspondingly simple operating principles. A CCF of the reactor protection system leading to the malfunction of both reactor protection subsystems is to be assigned to level of defence 4 and is controlled via a suitable overall architecture using the additional instrumentation and control systems.

- Controlled malfunctional behaviour; By limiting the system to simple operating principles, the effects of a CCF can be contained to such an extent that a malfunction deviating from an implemented, controlled malfunctional behaviour need not be assumed. These simple operating principles make it possible to analyse the malfunctional mechanisms sufficiently. Based on the known malfunctional mechanisms, effective monitoring mechanisms can be implemented to detect such malfunctions and then bring the affected equipment to a defined state. Furthermore, targeted measures can be implemented to diversify potential triggering system states, thereby limiting the scope of a potential dependent failure to a group of otherwise identical devices.

9 The impact of CCF postulates at the instrumentation and control/process engineering interface

If, in the event of a CCF in the reactor protection system, reactor protection signals are not generated (passive failure) or are generated incorrectly (active failure), this has consequences for the operational processes of the plant.

An active functional failure resulting from a CCF in subsystems of the reactor protection system may lead to

- the generation of faulty reactor protection signals or

- the fact that excitations requiring coordination are executed in such a way that there is no longer any coordination, resulting in damage to safety equipment (e.g. a pump is started but the associated lubricating oil pump is not).

Active functional failure can occur both during normal operation and in the course of controlling events initiated elsewhere.

Passive functional failure resulting from a CCF in subsystems of the reactor protection system only comes into play in the event of events initiated elsewhere, in that these subsystems fail to perform the necessary reactor protection functions. Passive functional failure therefore does not initiate transients or accidents. The control of passive functional failure requires that the remaining instrumentation and control functions are sufficient for event control.

9.1 Consequences of falsely generated reactor protection signals

Falsely generated reactor protection signals (active functional failure) can initiate plant transients and, in some cases, accidents.

This also applies to short-term false signals. With a few exceptions, such as control operators, triggered actuators will move away from their original position (OPEN or CLOSED) and will only stop once they reach the end position (CLOSED or OPEN). Similarly, most circuit breakers for pumps, ventilators and generator circuit breakers for emergency diesel generators will remain switched on. In most cases, manual intervention or the activation of the unit protection system is only possible once the relevant reactor protection signal has ceased.

If only some of the available process redundancies are affected by the false signals, the others remain available to control the initiated event. To what extent event control is influenced, exacerbated, or hindered depends

- on the plant type (PWR or BWR),
- on the instrumentation and control and the process engineering design of the plant,
- on the combination of false signals,
- on the duration for which the false signals persist,
- on the kind and scope of the equipment affected by the false signals, and
- on the technical options and time constraints for manual actions that are independent of the reactor protection system.

This also applies if it is assumed that, in subsystems of the reactor protection system, a CCF with active functional failure occurs in addition to an event sequence initiated by other causes.

With regard to uncoordinated control signals, it should be noted that the reactor protection system in a typical Siemens PWR has approximately 40 trip signals, which control roughly 600 to 800 component functions (ON/OFF or OPEN/CLOSED). For a number of functions, multiple components must be controlled in a coordinated manner (typically in relation to the individual process trains). To date, this coordination of control signals for safety systems primarily takes place in the reactor protection system (control level), allowing the in-service inspection for the corresponding instrumentation and control measures to be integrated into the in-service inspection of the RPS. Assuming that, in the event of a hypothetical active functional failure, the components associated with a trip signal are actuated differently, damage to safety-related components cannot be ruled out.

When considering these cases, it is also relevant whether or not they must be controlled under analysis boundary conditions applying to level of defence 3. Demonstrating event control under the boundary conditions of level of defence 3 means, amongst other things, that the loss-of-offsite-power scenario must be assumed (if unfavourable) and the single-failure concept must be applied.

9.2 Control of active and passive functional failures in the context of different architectures

Architecture 1 assumes that, for modern computer-based equipment technologies, CCF analyses are not sufficiently conclusive to rule out CCF on level of defence 3 on this basis. Since, according to Approach 1, in the event of a CCF, a malfunction deviating from an implemented, controlled malfunctional behaviour on level of defence 3 must be assumed, the occurrence of active and passive functional failures must be assumed in homogeneous computer-based subsystems and controlled by means of a suitable overall architecture utilising dissimilar subsystems. This means:

- Process engineering analysis: A process engineering analysis must be carried out to determine the consequences of active and passive functional failures.

- Consideration of malfunction: If a passive or active malfunction leads to unacceptable consequences, even when taking into account possible manual actions independent of the reactor protection system and the 30-minute criterion, it must be possible to perform the function using dissimilar subsystems. Otherwise, implementation using homogeneous equipment, such as the hard-wired design of the reactor protection system currently in place at the plants, is considered appropriate, taking into account the required measures for fault avoidance.
  If both active and passive malfunctions were to be taken into account for individual functions, this would require three dissimilar subsystems when using modern computer-based technology. The triggering/activation of the components would then have to be carried out via a voter (2-out-of-3), with sufficient safety against CCF having to be achieved for the voter. Instead, in view of the requirement for simplicity in reactor protection, it is preferable to implement the function

using homogeneous hard-wired technology based on discrete components which can be tested in the same way as in the previous procedure.

4. Comment by advocates of Architecture 2: see 2nd comment.

- Assignment of dissimilar equipment to the redundant subsystems: Instead of processing functions in parallel across dissimilar subsystems followed by voting, a design involving the assignment of dissimilar equipment on a train-by-train basis (e.g. 2x2) can also be used for functions that activate components train-by-train (e.g. 4 pumps). This ensures that the effects of a CCF in one subsystem are reliably limited to only one part of the process trains. In view of the necessary coordination of the actuation of multiple components in different trains, this is an advantageous and simple implementation solution. However, the following aspects must be considered:

  - Combination of CCF in the reactor protection system with the single-failure concept: According to the current version of KTA 3501, the combination of CCF and malfunction due to single failures or maintenance cases must be controlled in addition to the accident scenario. However, the current plant design is based on the exclusion of CCF from reactor protection, meaning that this combination did not have to be considered. If such an interaction were to be considered, this would lead to highly complex implementations involving three or four dissimilar subsystems. In this regard, it should be noted that a fault leading to systematic malfunction, provided the instrumentation and control technology is designed to meet the requirements, represents a very rare special case of a single failure and therefore should not be assumed to be a simultaneous single failure. The reasoning behind this is that, given a design intended to prevent malfunction due to single failures and the high-quality measures in place to control and prevent systematic malfunction, the simultaneous occurrence of both malfunctional mechanisms is to be regarded as sufficiently unlikely, provided that appropriate administrative measures are taken to reduce the time taken to detect and rectify faults. This should be viewed in particular in the context of the highly developed self-monitoring measures, which ensure that errors detectable by self-monitoring persist in digital instrumentation and control systems for only a short period of time.

  - Data exchange between redundant trains: In most plants, the existing reactor protection system concept stipulates that, for individual trip signals, not only train-specific detection, processing and actuation are required but also data exchange between redundant trains (e.g. for shut-off trip signals such as DAF 2 > max). As these links between redundant trains limit their required independence, the necessity of these links between redundant trains must be assessed on a plant-specific basis when assigning them on a train-by-train basis. Where cross-redundancy signal exchange is necessary, analyses of the coupling of dissimilar subsystems are required, e.g. regarding signal propagation times, possibilities of fault propagation, etc.

The requirements arising from this approach are set out in the VdTÜV statement on the necessary precautionary measures against systematic malfunction of digital instrumentation and control systems [9.1] and in the BMU's 'Safety Criteria for Nuclear Power Plants, Module 5', Chapter 3.2 (11).

Architecture 2 assumes that the effects of a CCF can be mitigated to such an extent that a malfunction deviating from an implemented, controlled malfunctional behaviour need not be assumed. The controlled malfunctional behaviour presupposes the effectiveness of internal and, where applicable, additional external monitoring by equipment that is physically separate from the software-controlled computers of the reactor protection system. The monitoring processes take a finite amount of time to ensure that a defined state is established at the outputs. With TELEPERM XS, this is achieved by switching off the load power supply to the signal outputs. In the case of computer-related (internal) monitoring functions that operate within a processing cycle, it can generally be assumed that incorrect triggering (active functional failure) will not occur. In the case of an external monitoring function[7], which may monitor several computers on a module carrier, the disconnection of the load power supply may only be ensured after more than one processing cycle. Short-term (<< 1 s) fault signals in the period until the monitoring functions respond cannot therefore be ruled out.

7 Explanation of the manner of operation of external monitoring: Experience has shown that hardware failures or the triggering of faults, including those with the potential to cause CCF, ultimately result in the cyclic operation of the automation device being interrupted. This interruption is reliably detected by the multi-stage internal monitoring systems so that the load power supply to the output module is switched off and a defined state is ensured. If, despite experience, it is postulated that a fault is of such a nature that cyclic operation is not interrupted but leads to an impact on the reactor protection instrumentation and control system functions, there must in any case be a corresponding change in the hardware, software, or internal states.
The external monitoring concept stipulates that, during each processing cycle, a signal sequence from the external monitoring system is fed into the relevant monitored module assembly frame of the reactor protection system, processed by a special test function, and the result of this processing is compared with the signal expected during normal operation. The test function utilises all hardware and software components that are also used for the actual reactor protection functions and for which the potential for a CCF cannot be sufficiently ruled out. If a change is assumed in these components which, whilst not affecting cyclic operation, does influence the result of the instrumentation and control system functions, this must also lead to changes in the result of the test functions that deviate from the expected result. This deviation would then lead to the shutdown of the module's load power supply and thus to a defined state, i.e. an active functional failure would also be prevented in this case.
The external monitoring system is part of the reactor protection system and is subject to the relevant quality and design requirements.

4. Comments by advocates of Architecture 1 on footnote 10:
For the highly effective detection of a subsystem failure required here - based solely on device behaviour and internal states - the monitoring functions mentioned are far from sufficient. To achieve this, comprehensive and in-depth monitoring measures would need to be developed on the basis of detailed CCF analyses of all hardware and software components.

5. Comments by advocates of Architecture 2 on footnote 10:
Based on a sufficient understanding of the system, combined with the necessary CCF analyses, it can certainly be demonstrated that adequate monitoring can be demonstrated with compact monitoring functions in the external unit that complement the internal monitoring system.

Overall, this has the following implications for Architecture 2 with regard to the instrumentation and control/process engineering interface:

- Delay in tripping: In principle, it is possible to prevent false tripping due to transient faulty signals by delaying the activation of all instrumentation and control systems (with the exception of reactor scram) by approximately 1 s (outside the reactor protection system computers). Although this requires accident analyses to be carried out with a 1-second delay for the process functions, this is not expected to cause any problems in meeting the criteria in the verifications. However, such a general solution would be quite complex given the approximately 600 to 800 components controlled by the reactor protection system. If this solution cannot be applied appropriately, the functions must be assessed individually for short-term incorrect activation as part of a process engineering analysis, taking into account the instrumentation and control components used.

- Process engineering analysis: It must be investigated whether or not incorrectly tripped functions will lead to impermissible effects. Impermissible effects are avoided if, although incorrect control signals may initiate transients, these are controlled by the reactor protection subsystem (level of defence 3) not affected by the CCF or if breaches of protection objectives in the event of a CCF of the entire reactor protection system (level of defence 4) are controlled by additional, diverse instrumentation and control equipment. A favourable factor here is that, due to the state defined at the outputs - which is ensured by monitoring at intervals of fractions of a second - activation is no longer pending. For example, damage can thus be prevented by unit protection. Suitable countermeasures must be defined to address impermissible effects resulting from momentary faulty activations.

- Passive malfunction: Passive malfunction of a reactor protection subsystem due to CCF (level of defence 3) is mitigated by the second reactor protection subsystem. Passive malfunction of both reactor protection subsystems due to CCF (level of defence 4) is controlled by additional instrumentation and control systems for part of the event spectrum (definition of vital functions).

- Active malfunction: Given the controlled malfunctional behaviour, active malfunction beyond short-term false tripping need not be assumed. Short-term false tripping is controlled either by means of 1-second time delays or by demonstrating as part of the process engineering analysis (supplemented where necessary by individual countermeasures) that ultimately only passive malfunction needs to be controlled.

- Train-by-train design: As the CCF of a reactor protection subsystem is assigned to level of defence 3 and is also to be controlled in accordance with the analysis boundary conditions of level of defence 3, each reactor protection subsystem must be capable of controlling all four redundant trains (by controlling the components via an OR gate that combines the signals from the respective outputs of the two quadruple-redundant, independent reactor protection subsystems). Otherwise, the CCF combined with the single-failure concept would not be controlled. Furthermore, the existing reactor protection system concept in most PWR plants

provides not only for train-by-train-specific detection, processing and triggering of individual trip signals but also for data exchange between redundant trains (e.g. for shutdown trip signals such as DAF 2 > max), albeit with data exchange taking place only between the redundant trains of the respective quadruple-redundant reaction protection subsystem.

- Combination of CCF in the reactor protection system with the single-failure concept: The combination of a CCF in a reactor protection subsystem (level of defence 3) with the single-failure concept is controlled for all design basis accidents.

9.3 Derivation of vital functions

For Architecture 1, the selection of the functions to be implemented in a dissimilar manner is determined from the total set of functions to be implemented by means of a process analysis and an examination of passive and active functional failures (see Chapter 9.2).

Architecture 2 requires the specification of the functional scope of the additional instrumentation and control systems, hereinafter referred to as “vital functions”. The task of the so-called “vital” system functions is to stabilise the plant in the short term in the event of a postulated malfunction of the reactor protection system due to CCF of both reactor protection subsystems (level of defence 4) in such a way that, taking into account measures subsequently initiated by plant personnel, impermissible effects on the environment are avoided. In this context, an active functional failure of the reactor protection subsystems with prolonged malfunctions of process engineering systems is not assumed (see Chapter 9.2).

The triggering of a plant transient by short-term false signals resulting from CCF in subsystems of the reactor protection system (CCF as the initiator of the event) is to be controlled by a subset of the vital functions - in the case of the PWR, these are reactor scram/turbine trip heat as well as removal via the main steam valves.

Vital system functions are defined as those process functions that are necessary to deal with combinations of events within 30 minutes in order to meet the protection objectives. The selection of vital system functions depends on the accident control concept for the plant in question. Since, for example, the accident control concept for Siemens pressurised water reactors (PWRs) is similar, the scope of the vital system functions is also similar. One possible approach to identifying vital functions for PWRs is based on the results of safety status analyses (SSA) - as illustrated in [9.2].

10 Compilation of consequences for development, implementation and operation arising from the implementation of the two architectures for controlling CCF

For both architectures, the required reliability of the reactor protection system or the overall system (reactor protection system and additional instrumentation and control systems) cannot be ensured by the chosen architecture alone but must also be demonstrated for the equipment technology employed. This requires i.a. a

high quality of the equipment system, which must be demonstrated in a suitable type test, and a CCF analysis (see Chapter 5.4). In summary, Architecture 2 achieves a lower degree of diversity between the two reactor protection subsystems than Architecture 1 (dissimilarity); on the other hand, in Variant 2, the additional instrumentation and control systems are planned for level of defence 4. Each variant has specific implications for the design, installation, operation and maintenance of the instrumentation and control systems.

If **Architecture 1** is implemented, this will have the following significant consequences:

- It is assumed that events can be controlled entirely or in part by means of computer-based systems.

- The use of dissimilar reactor protection subsystems requires different equipment technologies for the subsystems. The operator has to ensure the overall planning of the reactor protection system - comprising dissimilar subsystems - as required by IEC 61513, the overall integration of the reactor protection subsystems into an overall instrumentation and control system, and the commissioning of the overall system.

- Any faults, omissions or ambiguous requirements identified in the specifications for the reactor protection subsystems must be communicated between the individual manufacturers and the person responsible for overall planning. In doing so, the independence of the individual manufacturers' development work must not be compromised.

- The entire development process, including the associated potential for errors (e.g. when implementing specifications), must be performed twice, or in some cases three times, for the reactor protection subsystems. Consequently, a higher overall number of faults can be expected compared to Architecture 2; however, the likelihood of "identical" faults occurring in both subsystems is expected to be lower.

- The use of dissimilar reactor protection subsystems requires a dissimilarity analysis. To this end, suitable criteria for assessing dissimilarity must be developed in advance. The effectiveness of the individual diversities implemented in terms of mitigating CCF mechanisms must be justified so that the simultaneous malfunction of dissimilar subsystems due to CCF on level of defence 3 can be practically ruled out.

- During operation, operating experience from the plant itself and from other plants as well as other new findings regarding the control of CCF mechanisms must be monitored and any necessary measures taken (see Chap. 5.4).

- Verification and assessment must be carried out twice or, where necessary, three times for the different reactor protection subsystems.

- The diversity/dissimilarity realised in the design must be maintained throughout the operational life of products from different manufacturers. Maintenance expertise is required for reactor protection subsystems from different manufacturers, with the advantage that this reduces the occurrence of CCF errors during maintenance and modifications whilst also providing protection against malware with CCF potential.

- The nuclear applications must be implemented twice or, where necessary, three times for the dissimilar reactor ptotection subsystems. The dissimilar systems must operate in such a way as to ensure reliable triggering within a specified time frame through the overlapping triggering of the subsystems. Alternatively, in view of the requirement for simplicity in reactor protection, the function may be implemented using homogeneous hard-wired technology based on discrete components (see Chapter 9.2).

If **Architecture 2** is implemented, this will have the following significant consequences:

- If the additional instrumentation and control systems are implemented hardware-based, systems employing different technologies are available to ensure vital functions (compliance with protection objectives in the event of a CCF of the entire reactor protection system for part of the event spectrum).

- It must be demonstrated that the additional instrumentation and control systems will be effective in the event of a CCF of the reactor protection system. The CCF of the reactor protection system must not prevent the additional instrumentation and control systems from intervening.

- The development of computer-based reactor protection subsystems with diversity features may, where appropriate, be carried out by a single manufacturer using different development teams and in-house diversity management. A decision must be made as to whether the additional instrumentation and control systems should be sourced from a different manufacturer. The operator must ensure the overall planning of the complete system comprising the reactor protection system and the additional instrumentation and control systems, as required by IEC 61513, as well as the overall integration and commissioning of the overall system.

- Any errors, omissions or ambiguous requirements identified in the specifications for the reactor protection subsystems must, where necessary, be communicated only within a single manufacturer between different development teams in such a way that the independence of their development work is not called into question.

- The entire development process, including the associated potential for errors (e.g. when implementing specifications), is not carried out in full twice for the reactor protection subsystems. Consequently, fewer errors are generally expected overall than in Architecture 1; however, there is also a higher likelihood that “identical” errors will occur in both reactor protection subsystems.

- The diversity characteristics of the two reactor protection subsystems must be defined in a targeted manner, taking into account possible CCF mechanisms. To this end, suitable criteria for diversity decisions must be developed in advance. The effectiveness of the individual diversity characteristics with regard to the control of CCF mechanisms must be justified as a simultaneous malfunction of both reactor protection subsystems due to CCF on level of defence 3 is not assumed.

- During operation, operating experience gained from the plant itself and from other plants as well as other new findings regarding the control of CCF mechanisms must be monitored and any necessary measures taken.

- The additional instrumentation and control systems are subject to a different set of specifications, which covers only some of the functions (vital functions).

- The controlled malfunctional behaviour of the reactor protection subsystems is of critical importance in terms of safety, which is why the verification requirements in this regard are extremely stringent. At the subsystem level, the malfunctional behaviour of the subsystems must be determined and it must be demonstrated that each subsystem assumes a predefined safe state. Faults which, in conjunction with possible common-cause initiators, do not lead to such a safe state of the reactor protection subsystems and the additional instrumentation and control systems must be identified and rectified with a high degree of reliability. Any potential temporary false signals from the reactor protection system must be controlled (in the event of a CCF in one reactor protection subsystem, by the other reactor protection subsystem; in the event of a CCF affecting the entire reactor protection system, by the additional instrumentation and control systems; and by other instrumentation and control systems, such as unit protection, as well as - subject to appropriate grace periods - by manual intervention). If an approach is adopted whereby the additional instrumentation and control systems are not only enabled following the shutdown of the relevant redundant components of the reactor protection system but are always engaged – for example, using a downstream limit value – the requirements for a controlled malfunctional behaviour must also be met for the additional instrumentation and control systems.

- The diversity/dissimilarity incorporated in the design must be maintained throughout the operational life of a manufacturer’s reactor protection subsystems. Maintenance expertise is required for a manufacturer’s reactor protection subsystems. Additional maintenance expertise is required for the additional instrumentation and control systems.

For both architectures, even when installed in existing systems, a complete specification of requirements must be available or, where necessary, drawn up, including the assumed electrical ambient conditions and other environmental factors. It must be demonstrated that the new technology is compatible with worst-case conditions.

For both architectures, it must be investigated whether there are any environmental factors to which the new computer-based technology is more sensitive than the conventional reactor protection technology used to

date (e.g. voltage fluctuations, EMC and radiation that can lead to data corruption (soft errors)). If this is the case, appropriate countermeasures must be taken.

11 Maintenance and modification measures

Maintenance and modification work can introduce errors into computer-based systems. As part of the system lifecycle, maintenance and modification measures on instrumentation and control systems are subject to the requirements of the DIN IEC 61513 series of standards.

To prevent errors from occurring during maintenance and modification measures, the following general requirements must be met:

- All maintenance and modification measures must be carried out by trained personnel in accordance with the plant-specific procedural regulations governing maintenance and modifications. This requires knowledge of both plant engineering and the equipment systems. Depending on the potential impact of the maintenance measures or modifications, the required plant condition (full load, partial load or shutdown) must be established before work commences. The loaded software must undergo an identity and consistency check.

- A formalised change and configuration management system must be implemented so that it is possible at any time to trace when the system was operated in which configuration.

- Recurring maintenance measures, such as in-service inspections or parameter changes (e.g. for stretch-out operation) should be supported by ergonomically designed input screens. Inputs must be checked for correct syntax (comma; full stop; invisible control character) and correct value entries (decimal places; value changes). The selection of predefined setting options is preferable to the specification of alphanumeric values.

- Recurring maintenance measures must be carried out by trained specialist personnel in accordance with approved procedures, with the measures taking into account the current condition of the plant.

- Where there are availability requirements for the instrumentation and control system in question, maintenance measures must, as a general rule, be confined to a single redundancy section. A switch to the next redundancy section triggered by maintenance operations requires verification that the work has been carried out correctly and that the previously serviced redundancy section is operational. This also includes monitoring and analysing system error messages and warnings. Should maintenance measures affecting multiple redundancy sections become necessary, appropriate safety and security measures must be put in place, in particular ensuring that such measures are carried out whilst the system is in a state where there is no requirement for the affected system to be operational. These measures must be planned in terms of timing and technical requirements in such a way that any previously undetected fault in the modified plant

system or in the testing and programming equipment used is, as far as possible, detected as early as possible during introduction into the first redundant train and before introduction into the subsequent redundant trains.

- Before maintenance measures are carried out for the first time or before modified components are used for the first time, the potential for unintended interactions with other components must be analysed, tested in practice and, where necessary, ruled out by taking appropriate measures.

- It should be checked whether the maintenance regulations or other operating documents need to be amended in line with the above requirements.

International operating experience shows that modifications to computer-based instrumentation and control systems in particular are a significant source of (additional) errors. This gives rise to the following requirements:

- The number and scope of future modifications should be minimised through appropriate planning, design, and corresponding procurement and manufacturing strategies. In particular, this means that continuous manufacturing processes – and the resulting short innovation cycles – should be avoided. Instead, batch production with appropriate stockholding should be adopted, so that innovations can be better scheduled.

To prevent errors from being introduced when changes are nevertheless necessary, the following principles in particular should be applied:

- In order to implement modifications, including testing and clearance, responsibilities must be defined for at least the following activities:

    - proposal for a modification,
    - review of the proposal for the modification,
    - decision on the implementation of the modification,
    - implementation of the modification,
    - verification of the correct implementation of the modification.

    Here, it must be ensured that the body carrying out the verification is independent of the body making the proposal or carrying out the work, and that the body taking the decision is independent of the body making the proposal.

- Modifications must be carefully planned, with sufficient time allowed for development and implementation, assessment, and testing.

- The justification, the objective and the boundary conditions for the modification must be clearly set out.

- The modification requires an analysis of the impact on the computer-based system concerned, on the (computer-based) systems linked to it, and on the process engineering system to be controlled.

- The tests and simulations to be carried out must be defined and justified.

- It must be evaluated which parts of the type and qualification test need to be carried out again.

- Modifications are only permitted following prior verification in a suitable simulation environment or on the plant itself under appropriate operating conditions. In doing so, not only must the modified intended functionality be tested but also the continued integrity of the unmodified functionalities (e.g. regression testing, tests derived from the analysis of the impact of the modification).

- The documentation of the modification must be included in the documentation of the computer-based system.

12 Qualification and complexity; distinction between type testing and qualification testing

The current version of KTA 3503, “Type Testing of Electrical Modules for the Safety Related Instrumentation and Control Systems” (version: November 2005) requires updating with regard to suitable test procedures for computer-based equipment. At the same time, the complexity of computer-based instrumentation and control systems important to safety places new and increased demands on type and qualification testing.

As part of a type test, verification must be provided that sufficient measures were taken during development to meet the requirements set out in the regulations and that the specified functions are included and have been verified accordingly through practical tests. The qualification of the component for the intended use is assessed as part of qualification testing, taking the type test into account.

To date, type testing in accordance with the regulations has been purely a component test. As part of qualification testing, the system-specific configuration (system functionality) and the interaction between components are tested.

If the type tests do not provide sufficient verification of relevant system characteristics, supplementary tests should be carried out.

To this end, tests must be carried out on the relevant system characteristics and the interaction between components that are functionally related. This applies to characteristics such as timing behaviour, controlled malfunctional behaviour, and the effectiveness of self-monitoring.

So-called field devices (such as measuring transducers, switching devices and protective devices) must be qualified in accordance with the nuclear regulatory framework, taking into account CCF issues, in the same way as the instrumentation and control components.

The qualification test is generally carried out by an authorised expert different to the one who conducted the type test. To ensure the qualification test is carried out effectively, it is important that the scope and depth of the tests performed as part of the type test can be reproduced. To ensure that a type test carried out by one authorised expert is subsequently recognised by the authorised expert conducting the qualification test, it is necessary for the depth and scope to be agreed between the authorised experts. To this end, Directive 35 [12.1] was drawn up by the TÜV Nuclear Coordination Office. Important information in the type test documentation includes, amongst other things:

- a detailed description of the test object, including the associated devices, configurations, functions and interfaces

- the manufacturer's requirements for the test object and a detailed description of how these requirements are implemented technically

- information contained in the manufacturer's documents on which the test is based

- a specific list of the requirements from the applicable test standards that have been taken into account; when selecting the normative requirements relevant to the test, it may be useful to employ a database tool that allows for the preliminary filtering of the most important requirements to be covered and that contains examples of acceptable solutions

- a detailed description of the scope of testing (e.g. functional safety, basic safety (electrical, mechanical), EMC, security, availability); this should also include software testing and testing to ensure that non-safety-related components/subsystems will not adversely affect safety-related components

- full details of the test methods and test procedures

- a full presentation of the results of the individual tests, such as

    - how concretely the requirements for the test object were implemented (see safety case in accordance with IEC 61508)
    - whether the specified functionality is maintained
    - whether the quality requirements specified in the standards (including those for software) are fulfilled[8]
    - what kind of failure behaviour the tested component exhibits.

[8] It should be noted here that there is no uniform assessment standard setting out quality criteria for software components. For hardware components, KTA 3503 serves as the standard.

- in some cases, the failure behaviour of an assembly - particularly of software components - can only be identified in the runtime environment or at system level; in such cases, a note to this effect should be included in the type-test documentation

- full representation of compliance / non-compliance with the relevant normative requirements.

Any additional findings arising from the qualification test that indicate shortcomings in type testing should be taken into account when further developing the type testing procedures (experience feedback).

Given the complexity of computer-based safety instrumentation and control system and in order to avoid any future ambiguities, it would be advisable for the relevant testing institutions to agree on uniform testing standards. Furthermore, it would be advisable to draw up a testing guideline for computer-based instrumentation and control systems that sets out the specific requirements for type testing in accordance with KTA 3503.

This matter should be addressed and taken forward within the Committee on Electrical Installations.

Referenced documents

Chapter 1

[1.1] RSK-Ausschuss ELEKTRISCHE EINRICHTUNGEN; Positionspapier: „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“; 04.06.2009

Chapter 2

[2.1] DIN 40 041; Zuverlässigkeit: Begriffe; Dezember 1990

[2.2] VDI-Richtlinie 4001 Blatt 2: Begriffsbestimmungen zum Gebrauch des VDI-Zuverlässigkeitshandbuchs (Teil des VDI-Zuverlässigkeitshandbuchs); Juni 1986

[2.3] NTG- Empfehlung 3004: Zuverlässigkeitsbegriffe im Hinblick auf komplexe Software und Hardware, NTZ, 35(5):428-443, 1982

[2.4] E DIN IEC 61513; Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen; Entwurf Fassung 2010-04

[2.5] DIN EN 62340: Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen zur Beherrschung von Versagen aufgrund gemeinsamer Ursache; Fassung 2010-12

[2.6] VDI/VDE 3528: Regelung und Steuerung von Kernreaktoren; Spezielle Begriffe und Benennungen; 1972

[2.7] DIN EN 61226; Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Kategorisierung leittechnischer Funktionen; Fassung 2010-08

[2.8] DIN EN 60880: Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A, Fassung 2010-03

Chapter 5

[5.1] IEC 61513; Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems; Fassung 2001-03

[5.2] IAEA Safety Standards Series No. NS-R-1; Safety of Nuclear Power Plants: Design – Requirements; Fassung 2000

[5.3] IAEA Safety Standards Series No. NS-G-1.3; Instrumentation and control systems important to safety in Nuclear Power Plants; Safety Guide; Fassung 2002

[5.4] IEC 61508; Functional safety of electrical/electronic/programmable electronic safety-related systems; Fassungen 1998 und Entwurf 2010

[5.5] EN 50128, prEN 50128:2008; Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems

[5.6] ISO DIS 26262; Road vehicles — Functional safety; Fassung 2009

[5.7] ISO 13849; Safety of machinery — Safety-related parts of control systems; Fassung 2006

[5.8] RTCA DO 178B bzw. ED-12B; Software Considerations in Airborne Systems and Equipment Certification; Fassung 1992

[5.9] ECSS-Q-80-03A; Space product assurance – Methods and techniques to support the assessment of software dependability and safety; Fassung Draft 2006

Chapter 6

[6.1] E DIN IEC 61513; Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen; Entwurf Fassung 2010-04

[6.2] DIN EN 62340: Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen zur Beherrschung von Versagen aufgrund gemeinsamer Ursache; Fassung 2010-12

Chapter 7

[7.1] E DIN IEC 61513; Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen; Entwurf Fassung 2010-04

[7.2] DIN EN 62340: Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen zur Beherrschung von Versagen aufgrund gemeinsamer Ursache; Fassung 2010-12

[7.3] U.S. NRC; Duke Energy Carolinas, LLC; Docket No. 50-269; Oconee Nuclear Station, Unit 1; Amendment to renewed facility operating license; 28.01.2010

[7.4] U.S. NRC; Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems; NUREG/CR-7007

Chapter 9

[9.1] VdTÜV; Stellungnahme des VdTÜV zu den erforderlichen Vorsorgemaßnahmen gegen systematisches Versagen von digitalen leittechnischen Einrichtungen in kerntechnischen Anlagen, die Leittechnikfunktionen der Kategorie 1 ausführen; 22.01.2008

[9.2] Ulrich Waas; Auswirkungen von CCF-Postulaten an der Schnittstelle Leittechnik/Verfahrenstechnik; Textbeitrag vom 10. November 2010

Chapter 12

[12.1] Weisungsbeschluss 35 der TÜV-Leitstelle Kerntechnik bei der VdTÜV: Prüfung von Serienbauteilen für Kernkraftwerke im Rahmen atomrechtlicher Genehmigungs- und Aufsichtsverfahren, Fassung 03.2004

Appendix

to the statement „Computer-based instrumentation and control (I&C) systems important to safety for use in the highest safety category in German nuclear power plants“ – Presentation of the consultation results from the RSK working group on USE OF COMPUTER-BASED INSTRUMENTATION AND CONTROL SYSTEMS

Course of the discussion

The working group discussed the matter at a total of nine meetings. At its 1st meeting on 21 May 2010 /1.1/, the working group commenced its work in accordance with the task assignment formulated by the RSK (426th meeting on 20 May 2010) /1.2/ and, on the basis of the proposal /1.8/ and taking into account /1.3–1.7/, the comments /1.9/ and the relevant discussions, drew up a schedule for further deliberations. A schedule /1.10/ set out the allocation of tasks to the working group members and other experts.

At the 2nd meeting on 21 - 22 June 2010 /2.1/, the main focus of the discussions was on the current international situation regarding the use of computer-based systems in instrumentation and control systems important to safety in nuclear power plants, divided into three topic areas:

1. description of different safety philosophies and concepts, and the integration of architectures of instrumentation and control systems important to safety into the safety concept;
2. diversity characteristics / independence characteristics as well as controlled / uncontrolled failure behaviour;
3. NUREG CR 7007 with reference to NRC BTP 7-19.

In his presentation /2.2/, Mr Verstegen outlined the CCF postulates to be established from VdTÜV’s perspective for computer-based instrumentation and control systems and the reasons underlying these postulates. He then outlined the general principles governing the design of instrumentation and control systems important to safety in US nuclear power plants. In his presentation /2.3/, Mr Waas described the safety principles for the technical design of a computer-based protection system in accordance with event classes and levels of defence. He outlined protection concepts against common-cause initiators and the implications for instrumentation and control systems important to safety.

Regarding the second topic, Ms Bühler /2.4/ provided an overview of implementations at foreign plants based on information from NUREG/CR-7007 /2.5/. With regard to the distinction between the terms “dissimilarity” and “diversity”, reference was made to the definition in /2.6/. As a practical example, Mr Verstegen reported on 11 ASN/GPR requirements for the Flamanville 3 EPR /2.7/. Furthermore, Dr Fischer /2.8, slides 16 and 17/ explained the basic principles of plant safety and the defence-in-depth concept.

With regard to the third topic area, GRS /2.9/ outlined the NRC’s requirements for diversity as a safeguard against common-cause failures in computer-based instrumentation and control systems important to safety. In doing so, the key requirements from BTP 7-19 /2.10/ and DI&C-ISG-02 /2.11/ as well as NUREG/CR-

6303 /2.12/ were addressed. The diversity aspects from NUREG CR 7007 /2.5/ were explained and compared with those from /2.12/. As an example of the implementation of these rules, GRS briefly discussed the licensing procedure for the conversion of instrumentation and control systems important to safety to Teleperm XS (TXS) at the US nuclear power plant in Oconee. Dr Graf provided a detailed description of the Oconee project /2.13/. He first described the regulatory requirements in the US for computer-based instrumentation and control systems with regard to CCF /2.10, 2.13, 2.14/. In addition, the defence-in-depth and diversity analyses, including the assumed CCF failure modes and the required quality of the backup measures derived from them were explained.

After the meeting, on the basis of the reports presented and with reference to a presentation /2.15/ and to NUREG/CR 7007 /2.5/, Section 4, the Chair compiled a systematic overview of the various realisations comparing aspects such as diversity and dissimilarity /2.16/.

At the 3rd meeting on 5 - 6 July 2010 /3.1/, an overview of international standards and regulations was provided with regard to existing requirements for the prevention and control of a CCF. In particular, the discussion focused on whether the requirements were comprehensive.

Dr Riekert explained /3.2/ the assessment of digital instrumentation and control technology within the OECD NEA's MDEP process and the key content of the IAEA reports /3.3 and 4/. Dr Lindner explained that the SC 45A standards implement the principles of the IAEA Safety Guides into technical rules /3.5/. He provided an overview of the IEC's work. He also explained the CDV (Committee Draft for Voting) IEC 61513 /3.6/ with regard to dealing with a CCF. Furthermore, he referred to /3.7/ in relation to a probabilistic assessment for a software-based system. In Great Britain, the probability of malfunction of a software-based system when challenged must not be less than 10^{-4} /3.8/. In the ensuing discussion, reference was made to a comparison of digital instrumentation and control applications in foreign nuclear power plants /3.7/, in which four different diversity design approaches for software-based instrumentation and control systems important to safety were identified. The documents /3.9/ and /3.10/ were consulted in the discussion.

Mr Schröder described how the CCF is incorporated into the IEC 61513 series of standards and its subordinate standards /3.11/. In connection with his comments on the draft DIN EN 62340, he referred to /3.12/.

In his presentation, Mr Faller described standards from other industries relating to the treatment of the CCF /3.13, 3.14/. In addition to the IEC standards IEC 61508 and IEC 61511, he concluded by referring to aerospace analysis techniques /3.15/ and to HAZOP studies /3.16, 3.17/. He also explained the stress-strength conceptual model, which forms the basis in most industries.

In a further presentation, Mr Waas discussed the interface between instrumentation and control and process engineering, using a PWR plant as an example /3.18/.

To conclude, the working group discussed possible instrumentation and control system architectures, taking into account the previous discussions /2.16, 3.19/.

At the 4th meeting on 16 - 17 August 2010 /4.1/, individual topics were examined at greater length. In his presentation, Dr Graf described the feasibility of functional diversity, particularly on the basis of DIN IEC 62340 /4.2/. Dr Lindner explained the significance and effectiveness of the external monitoring device (ExtÜ) intended for TXS, which forms part of the VGB concept /4.3/. The topic of diversity was also touched upon in this context. Mr Waas reported on the consequences of prolonged control errors dependent on the postulate of controlled or uncontrolled failure behaviour /4.4/. The working group then summarised the findings from the presentations, which were to be incorporated into the statement. On the basis of a proposal /4.5, 4.6/, the working group defined the objectives and key content of the statement and drew up a timetable /4.7/.

At the 5th meeting on 27 September 2010 /5.1/, following a brief discussion on a current security issue (the 'Stuxnet' malware), the working group began discussing the 1st DRAFT/statement /5.2/. On the basis of a proposed structure /5.3/, contributions from the working group members /5.4 – 5.14/ had been agreed upon for a first draft of a statement.

At the 6th meeting on 13 October 2010 /6.1/, the discussion on the DRAFT/Statement /6.2/ continued; further comments and additions /6.3 – 6.8/ had been incorporated in the meantime. The document /6.9/ was also available.

At the 7th meeting on 8 - 9 December 2010 /7.1/, the working group was briefed by Dr Haake of TÜV Nord and Dr Lindner of ISTec on the type testing of the TXS system /7.2, 7.3/. The working group then continued its discussion of the DRAFT/statement, which had been revised in the meantime by Mr Brettner, taking into account contributions from the working group members. No consensus could be reached regarding the text and scope /7.15/. The key points of the DRAFT/statement are to be summarised in an executive summary and adopted as a joint paper by the working group. The full version of the text is to be approved by only part of the working group and submitted to the RSK.

At its 8th meeting on 9 February 2011, the working group briefly discussed the topic of 'Redesign of assemblies' /8.2–8.4/ and concluded that further discussions should take place within the Committee on Electrical Installations. The working group then continued its discussion on the statement. The draft discussed at the 7th meeting (hereinafter referred to as the "long version") /7.15/ has since been revised /8.5, 8.6/. The key points are to be summarised in an executive summary and adopted as a joint paper by the working group.

The subject of the discussion was the draft summarised as an Executive Summary (hereinafter referred to as the 'summary') /8.7, 8.8/. Taking into account further documents /8.9–8.11/ as well as additional comments and amendments, the working group revised the summary of the statement /8.12/. Following the meeting, the draft was revised to incorporate the agreements reached at the 8th ERL working group meeting and the comments and textual revisions received /8.13/ as a consultation document for the 9th and final meeting.

At the 9th meeting on 7 September 2011, in addition to document /8.13/, comments were received from Ms Bühler and Mr Verstegen /9.1/, Dr Riekert /9.2/, and Mr Waas and Dr Graf /9.3/. Following discussion, the working group adopted the current version.

Documents

/1.1/ Kurzprotokoll der RSK-Ad-hoc-Arbeitsgruppe Einsatz Rechnerbasierter Leittechnik (ERL) der 1. Sitzung am 21.05.2010 (EP_AG-ERL1.doc)

/1.2/ M. Brettner, Vorschlag für die Aufgabenstellung für die RSK Ad-hoc-Arbeitsgruppe „Einsatz Rechnerbasierter Sicherheitsleittechnik“ (AG ERL), 426. RSK-Sitzung am 20.05.2010 (Vorschlag Aufgabenstellung AG ERL 100518.doc)

/1.3/ M. Brettner, „RSK AG Einsatz rechnerbasierter Sicherheitsleittechnik der höchsten Sicherheitskategorie: Eingrenzung des Beratungsbedarfs abgeleitet aus einem Abgleich bestehender Anforderungen in RSK LL DWR, Modul 5 und Positionspapier RSK Ausschuss EE“, 11.05.2010, (Eingrenzung Beratungsbedarf 11-5-2010.doc)

/1.4/ BMU, „ Sicherheitskriterien für Kernkraftwerke, REVISION D, APRIL 2009 (modulerevisiond020709.pdf)

/1.5/ RSK-Leitlinien für Druckwasserreaktoren, Ursprungsfassung (3. Ausgabe vom 14. Oktober 1981) mit Änderungen vom 15.11.1996 (RSK_LL96.pdf)

/1.6/ RSK418, Info-7, „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ - Positionspapier des Ausschusses ELEKTRISCHE EINRICHTUNGEN“ einschließlich 9 Anlagen, (RSK418_Info-7_RSK418 inkl. Anhang 1-9.pdf)

/1.7/ R. Faller, „Ad-hoc AK ERL Einsatz rechnerbasierte Leittechnik, SILT Diskussion“ (AdHoc AK ERL.pdf)

/1.8/ M. Brettner, Vorschlag Beratungsgegenstände (hier nur CCF) für 1. Sitzung der AG ERL am 21.05.2010 (e-mail_Brettner_19.05.2010_Vorschlag_Beratungsgegenstände hier_nur_CCF für 1. Sitzung.pdf)

/1.9/ C. Verstegen, Kommentare /Änderungswünsche zum Vorschlag Beratungsgegenstände für 1. Sitzung der AG ERL am 21.05.2010 (VorschlagBrettnerKomVer-1.doc)

/1.10/ Anhang zum Kurzprotokoll der 1. Sitzung Arbeitsgruppe ERL am 21.05.2010 (Anhang EP_AG-ERL1_Ablaufplan der Beratungen.doc)

/2.1/ Kurzprotokoll der 2. Sitzung der RSK-Ad-hoc-Arbeitsgruppe Einsatz Rechnerbasierter Leittechnik (ERL) am 21./22.06.2010 (EP_AG-ERL2.doc)

/2.2/ C. Verstegen, Fehlerpostulate und Grundlagen der Auslegung in US KKW, 2. Sitzung AG ERL, 21./22.06.2010 (Verstegen, GRS, Fehlerpostulate.ppt)

/2.3/ U. Waas, Einordnung von Sicherheitsleittechnikarchitekturen in das Sicherheitskonzept, Foliensatz ,(RSK-AG_DSILT_20100621-ang.ppt)

/2.4/ Cornelia Bühler, TÜV SÜD Industrie Service GmbH, Vorsorgemaßnahmen gegen CCF, Beispiele zum internationalen Stand basierend auf NUREG/CR-7007, RSK-Arbeitsgruppe ERL 21./22.06.2010, Foliensatz (ERL internationaler Stand.ppt)

/2.5/ US NRC, NUREG/CR 7007, Diversity Strategies für Nuclear Power Plant Instrumentation and Control Systems, published February 2010 (NUREGcr7007.pdf)

/2.6/ Cornelia Bühler, TÜV SÜD Industrie Service GmbH, Digitale Leittechnik im Reaktorschutz Vorsorgemaßnahmen gegen CCF Die Anforderungen der Sachverständigen im VdTÜV, Symposium des TÜV Nord am 29. – 30.09.2009 in Hamburg (09 Bühler_Symposium TÜV Nord 9 2009.pdf)

/2.7/ C. Verstegen, GRS, Forderungen der ASN zur geplanten Architektur der softwarebasierten Leittechnik im französischen EPR Flamanville 3 – „Réacteurs nucléaires à eau sous pression Projet EPR-Flamanville 3 – Architecture générale du contrôle-commande et des plateformes associées“ von der französischen Aufsichtsbehörde (Autorité de Sureté Nucléaire ASN) an die EDF (15.10.2009), 21./22. Juni 2010, Foliensatz (RSK ERL_170610.ppt)

/2.8/ Dr.-Ing. Erwin Fischer, Technische Leitung Kernkraftwerk Isar, Sicherer Langzeitbetrieb von Kernkraftwerken – ein Widerspruch?, 3. VdTUV-Forum Kerntechnik 2010, Berlin 15.-16- Marz 2010 (25_Fischer-Langzeitbetrieb.pdf)

/2.9/ J. Stiller, D. Sommer, C. Verstegen, GRS, Anforderungen der NRC an Diversität als Vorkehrung gegen gemeinsam verursachte Ausfälle softwarebasierter Sicherheitsleittechnik, 2. Sitzung der Ad-hoc-Arbeitsgruppe „Einsatz Rechnerbasierter Leittechnik“ (ERL) der RSK, Foliensatz (GRS-Vortrag Stiller.ppt)

/2.10/ US NRC, BTP 7-19, Branch Technical Position 7-19, Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems (BTP19_rev5.pdf)

/2.11/ US NRC, DI&C-ISG-02, Task Working Group #2: Diversity and Defense-in-Depth Issues, Interim Staff Guidance, Revision 2 (TWG #2 ISG R2.pdf)

/2.12/ NUREG/CR-6303, Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, published Dezember 1994 (NUREGCR-6303.pdf)

/2.13/ Arnold Graf, I&C Architecture Design Authority, AREVA, CCF Behandlung im Genehmigungsverfahren Oconee, 2010-06-14, Foliensatz (Oconee Licensing.ppt)

/2.14/ Answers to questions (Answers to Questions.doc)

/2.15/ Arndt Lindner, Institut für Sicherheitstechnologie (ISTec) GmbH, Anforderungen an rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken, Bonn 18./19.02.2008 (RSK-Workshop “Digitale Leittechnik”), 2 Foliensätze (RSK-Workshop-Vortrag04-Lindner_RSK Workshop_1.ppt, RSK-Workshop-Vortrag04- Lindner_RSK Workshop_2.ppt)

/2.16/ M. Brettner, RSK Ad-Hoc Arbeitsgruppe „Einsatz Rechnerbasierter Leittechnik (AG ERL)“ Darstellung möglicher Leittechnikarchitekturen unter Einbeziehung des bisherigen Diskussionsstandes in der AG, Bremen, 30.06.2010 (Strukturierung von Leittechnikarchitekturen_30-6-2010.doc)

/3.1/ Kurzprotokoll der 3. Sitzung der RSK-Ad-hoc-Arbeitsgruppe Einsatz Rechnerbasierter Leittechnik (ERL) am 05./06.07.2010 (EP_AG-ERL3.doc)

/3.2/ Dr. Thomas Riekert, RSK, Überblick über internationale Normen und Regelwerk: MDEP OECD NEA, IAEA, Foliensatz, (Vortrag DrRi.ppt)

/3.3/ IAEA Nuclear Energy Series, No NP-T-1.4, Implementing Digital Instrumentation and Control Systems in the Modernization of Nuclear Power Plants (IAEA_Implementing digital I and C.pdf)

/3.4/ IAEA Nuclear Energy Series, No NP-T-1.5, Protecting against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants (Pub1410_web.pdf)

/3.5/ Dr. Lindner, IEC/SC45A Standards, Tabelle (IEC_SC45A Standards.docx)

/3.6/ Arndt Lindner, Institut für Sicherheitstechnologie (ISTec) GmbH, 3. Sitzung der Ad-hoc-Arbeitsgruppe „Einsatz Rechnerbasierter Leittechnik“ (ERL) der RSK, Foliensatz (IEC61513-CCF.pptx)

/3.7/ Arndt Lindner, Institut für Sicherheitstechnologie (ISTec) GmbH, Anforderungen an rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken Bonn 18./19.02.2008, Digitale Sicherheitsleittechnik – Anwendungen in ausländischen Kernkraftwerken (modifiziert für 3. Sitzung der Ad-hoc-Arbeitsgruppe „Einsatz Rechnerbasierter Leittechnik“ (ERL) der RSK), Foliensatz (RSK-WS_mod.ppt)

/3.8/ B. Littlewood et. al., Modelling Softwaredesign diversity: a review, (Bev Littlewood et al, Modelling software design diversity.pdf)

/3.9/ Stellungnahme des VdTÜV zu den erforderlichen Vorsorgemaßnahmen gegen systematisches Versagen von digitalen leittechnischen Einrichtungen in kerntechnischen Anlagen, die Leittechnikfunktionen der Kategorie 1 ausführen, 06.03.2008 (Erforderliche_Vorsorgemaßnahmen_digitale_Sicherheitsleittechnik.pdf)

/3.10/ B. Littlewood, The use of proof in diversity arguments, (Diversity_and_logic.pdf)

/3.11/ M. Schröder, Behandlung CCF in DIN IEC 61513, 3. Sitzung der Ad-hoc-Arbeitsgruppe „Einsatz Rechnerbasierter Leittechnik“ (ERL) der RSK am 05./06.07.2010 (100605-ERL-Behandlung_CCF_in_DIN_IEC_61513.ppt)

/3.12/ Anhang 9 des Positionspapiers des Ausschusses ELEKTRISCHE EINRICHTUNGEN 8 EE200_Positionspapier-Anhang9.doc)

/3.13/ R. Faller, Ad-hoc AK ERL Einsatz Rechnerbasierter Leittechnik, (AdHoc AK ERL R2 CCA.ppt),
einschließlich:
P.G. Bishop, Adelard, Review of Software Design Diversity
Bev Littlewood et al, Modelling software design diversity
Susan Brilliant, John Knight, Nancy Leveson, Analysis of Faults in an N-Version Software Experiment

/3.14/ Tabelle zu /3.13/, (Tabelle von AdHoc AK ERL R2 CCA.xls)

/3.15/ Draft ECSS-Q-80-03, Space product assurance Methods and techniques to support the assessment of software dependability and safety, 1 March 2006 (Draft-ECSS-Q-80-03A(1March2006).pdf)

/3.16/ Ministry of Defence, Defence Standard 00-58, HAZOP Studies on Systems Containing Programmable Electronics, Part 1 Requirements, Issue 2 Publication Date 19 May 2000 (DStan 00-58-1-Hazop Teil1.pdf)

/3.17/ Ministry of Defence, Defence Standard 00-58, HAZOP Studies on Systems Containing Programmable Electronics, Part 2 General Application Guidance, Issue 2 Publication Date 19 May 2000 ((DStan 00-58-1-Hazop Teil2.pdf)

/3.18/ U. Waas, Schnittstelle Verfahrenstechnik/Leittechnik am Beispiel einer DWR-Anlage (RSK-AG-ERL_vitale_20100706.PPT)

/3.19/ /2.16/ mit Änderungen aus der 3. Sitzung (Strukturierung von Leittechnikarchitekturen_30-6-2010 Änderung.doc)

/4.1/ Kurzprotokoll der 4. Sitzung der RSK-Ad-hoc-Arbeitsgruppe Einsatz Rechnerbasierter Leittechnik (ERL) am 16./17.08.2010 (EP_AG-ERL4.doc)

/4.2/ Dr. Graf, „Umsetzbarkeit funktionaler Diversität", (Funktionale Diversitaet_fin.pptx)

/4.3/ Arndt Lindner, Institut für Sicherheitstechnologie (ISTec) GmbH, 4. Sitzung der Ad-hoc-Arbeitsgruppe „Einsatz Rechnerbasierter Leittechnik" (ERL) der RSK, Wirksamkeit der externen Überwachungseinrichtung, (ERL_WEUE.pptx)

/4.4/ U. Waas, „Konsequenzen von länger anstehenden Fehlansteuerungen", RSK-AG-ERL, 16.08.2010 (RSK-AG_DSILT_CCF-LT-VT_20100816.ppt)

/4.5/ M. Brettner, „Strukturvorschlag für die Darstellung der Beratungsergebnisse der RSK AG ERL", Bremen, den 16. Juli 2010 (Strukturvorschlag Beratungsergebnisse AG ERL 16-7-2010.doc)

/4.6/ Dr. Riekert, „Vorschlag für eine Gliederung der Empfehlung zur digitalen Sicherheitsleittechnik für den Reaktorschutz", (Riekert_Vorschlag fuer Gliederung_15.07.2010.doc)

/4.7/ Strukturvorschlag für die Darstellung der Beratungsergebnisse der RSK AG ERL, in der 4. Sitzung am 17.08.2010 überarbeitet (Strukturvorschlag Beratungsergebnisse AG ERL 4.Sitzung-17.08.2010.doc)

/5.1/ Kurzprotokoll der 5. Sitzung der RSK-Ad-hoc-Arbeitsgruppe Einsatz Rechnerbasierter Leittechnik (ERL) am 27.09.2010 (EP_AG-ERL5.doc)

/5.2/ RSK-Information Nr. ERL5, ENTWURF/Stellungnahme „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken" – Ergebnisse der RSK-Arbeitsgruppe ERL", 27.09.2010 Dr. Graf, „Umsetzbarkeit funktionaler Diversität", (ERL-Stellungnahme_27-09-2010_Sitzung_5)

/5.3/ M. Brettner, „Strukturvorschlag für die Darstellung der Beratungsergebnisse der RSK AG ERL", überarbeitet in 4. Sitzung AG ERL, 17.08.2010 (Strukturvorschlag Beratungsergebnisse AG ERL 4.Sitzung-17.08.2010)

/5.4/ M. Brettner, „Begriffe", Abschnitt 2, (Entwurf zu Abschnitt 2 - Begriffe.doc)

/5.5/ Dr. Lindner, Kommentare zu /2/, Abschnitt 2, (Entwurf zu Abschnitt 2 - Begriffe_Kommentare Lindner.doc)

/5.6/ W. Fischer, „Software basierte Sicherheitsleittechnik –Prinzipielle Vor- und Nachteile – Sicherheitstechnischer Nutzen/Gewinn", 19.09.2010, Abschnitt 4 (Vor u Nachteile softwarebasierter Lettechnik_v02_RSK.doc)

/5.7/ Dr. Riekert, „5. Übergeordnete Anforderungen im bestehenden deutschen Regelwerk und Anpassungsnotwendigkeiten", Kurzfassung, 08.09.2010, Abschnitt 5 (Kapitel 5 DrRi 06092010 Kurzfassung)

/5.8/ Dr. Riekert, „5. Übergeordnete Anforderungen im bestehenden deutschen Regelwerk und Anpassungsnotwendigkeiten", 08.09.2010, (Kapitel 5 DrRi 06092010)

/5.9/ M. Schröder, „6. Übersicht über Ansätze im internationalen Regelwerk zum Lebenszyklus rechnerbasierter Sicherheitsleittechnik, 6.1 Allgemeine Übersicht über Regelungsinhalte im IEC und DIN-IEC-Regelwerk", 20.09.2010, Abschnitt 6.1 (Kapitel_6 1_Regelungsinhalte_IEC_DIN-IEC_05.doc)

/5.10/ Dr. Graf, „Diversität als Maßnahme zur CCF Vermeidung / Beherrschung", 14.09.2010, Abschnitt 7 (Diversität als Massnahme.pdf)

/5.11/ M. Brettner, „Diversitätsentscheidungen und Diversität im Ausfallverhalten", 19.09.2010, Abschnitt 7 (7b_Entwurf zu Abschnitt 7)

/5.12/ H. Faller, „Vorschlag für Ergänzungen der Qualifizierungsanforderungen an Rechner in Cat A Funktionen", 13.09.2010, Abschnitt 8 (RSK ERL R002 V0R2.docx)

/5.13/ U. Waas, „Auswirkungen von CCF-Postulaten an der Schnittstelle Leittechnik/Verfahrenstechnik", 21.09.2010, Abschnitt 9 (RSK-Beratung_SILT_CCF-Postulate_LT-VT_20100918.doc)

/5.14/ M. Brettner, „Abschnitt 10 der Darstellung der Beratungsergebnisse der RSK AG ERL", 15.09.2010, Abschnitt 10 (Entwurf Abschnitt 10 Beratungsergebnisse AG ERL 15-09-2010.doc)

/6.1/ Kurzprotokoll der 6. Sitzung der RSK-Ad-hoc-Arbeitsgruppe Einsatz Rechnerbasierter Leittechnik (ERL) am 13.10.2010, ENTWURF (EEP_AG-ERL6.doc)

/6.2/ RSK-Information Nr. ERL6, ENTWURF/Stellungnahme „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in

deutschen Kernkraftwerken“ Fassung 12.10.2010 (ERL-Stellungnahme_Sitzung_6_12-10-2010.doc)

/6.3/ Ergänzung zu Abschnitt 10, Dr. Riekert, 27.09.2010 (e-mail_Riekert_27.09.2010_AW AG ERL Unterlagen.pdf)

/6.4/ Ergänzungen und Kommentierungen zu Abschnitt 7a, H. Verstegen, 07.10.2010 (7_Verstegen_07.10.2010_Kap. 7a)

/6.5/ Ergänzungen und Kommentierungen zu Abschnitt 9.1, H. Verstegen, 07.10.2010 (9_Verstegen_07.10.2010_Kap. 9-1.doc)

/6.6/ Ergänzungen und Kommentierungen zu Abschnitt 10, H. Verstegen, 07.10.2010 (10_Verstegen_07.10.2010_Kap. 10.doc), 07.10.2010

/6.7/ Ergänzung zu Abschnitt 6.2, Dr. Riekert, 11.10.2010 (6.2_Riekert_Kapitel 6_2 DrRi 22092010.doc)

/6.8/ Kommentierung Abschnitt 7a, Dr. Graf, 12.10.2010 (7a_Graf_12.10.2010_Kap. 7a_gr.doc)

/6.9/ Kommentierung Abschnitt 9, H. Waas, 12.10.2010 (9_Waas_12.10.2010_Wa_Verstegen_Kap. 9.doc)

/7.1/ Kurzprotokoll der 7. Sitzung der RSK-Ad-hoc-Arbeitsgruppe Einsatz Rechnerbasierter Leittechnik (ERL) am 08./09.12.2010, ENTWURF (EPV_AG-ERL7.doc)

/7.2/ Dr. D. Haake, TÜV-Nord SysTec GmbH & Co. KG, „Aspekte zur Typprüfung TXS“, 8. Dezember 2010 (RSK_DLT_20101208_Haa2)

/7.3/ Dr. Lindner, „Software-Prüfungen“, 08.11.2010 (SW-Pruefungen)

/7.4/ U. Waas, Anmerkungen zu Kapitel 9, 07.11.2010 (Kap. 9_2010-11-10.doc)

/7.5/ RSK-Information „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ – Darstellung der Beratungsergebnisse der RSK-Arbeitsgruppe ERL (ENTWURF/Stellungnahme), Stand 19.11.2010 (ERL-Stellungnahme_neu_19-11-2010.doc)

/7.6/ R. Faller, Anmerkungen zu „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ – Darstellung der

Beratungsergebnisse der RSK-Arbeitsgruppe ERL (ENTWURF/Stellungnahme), Stand 19.11.2010 (ERL-Stellungnahme_neu_19-11-2010_RF.doc)

/7.7/ Cornelia Bühler, „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ – Darstellung der Beratungsergebnisse der RSK-Arbeitsgruppe ERL, Stand: 19.11.2010 - Generelle übergeordnete Kommentare zu den einzelnen Kapiteln, 07.12.2010

/7.8/ C. Bühler, C. Verstegen, Ergänzung zu 10.3, Seite 44, (Textauszug Abschnitt 9.3_Architektur 1bue_ver.doc)

/7.9/ C. Verstegen, Kommentare zu „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ – Darstellung der Beratungsergebnisse der RSK-Arbeitsgruppe ERL (ENTWURF/Stellungnahme), Stand 19.11.2010, (Verstegen_ERL-Stellungnahme_neu_19-11-2010.doc)

/7.10/ RSK-Information „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ – Darstellung der Beratungsergebnisse der RSK-Arbeitsgruppe ERL (ENTWURF/Stellungnahme), Stand 06.12.2010 (ERL-Stellungnahme_neu_06-12-2010.doc)

/7.11/ RSK-GS, Waldorf, Anhang zu „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ – Darstellung der Beratungsergebnisse der RSK-Arbeitsgruppe ERL (ENTWURF/Stellungnahme), Stand 06.12.2010, „3. Beratungsverlauf“ (3_ERL-Stellungnahme_Anhang 3 Beratungsgang.doc)

/7.12/ HSE Health and Safety Executive, “Out of control, Why control systems go wrong and how to prevent failure”, ISBN 978 0 7176 2192 7 (hsg238.pdf)

/7.13/ R. Faller, exida, “Common Cause Analysis for Integrated Circuits with On-Chip Redundancy”, Safetronic 2010 (Safetronic exida IC CCA V3R1.pdf)

/7.14/ Nuclear Engineering International, “USA’s first fully digital station”, November 2010 (Nucl.Eng.Oconee_stuxnet.pdf)

/7.15/ RSK-Information „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ – Darstellung der Beratungsergebnisse der RSK-Arbeitsgruppe ERL (ENTWURF/Stellungnahme), Stand 06.12.2010 (7.Sitzung ERL-Stellungnahme_09-12-2010.doc)

/8.1/ Kurzprotokoll der 8. Sitzung der RSK-Ad-hoc-Arbeitsgruppe Einsatz Rechnerbasierter Leittechnik (ERL) am 09.02.2011, ENTWURF (EPV_AG-ERL8.doc)

/8.2/ Vereinigte Elektronikwerkstätten GmbH, „REDESIGN, NACHFERTIGUNG, NEUENTWICKLUNG“, Schreiben vom 07.01.2011 an das BMU, H. Fabian (Brief Bundesministerium f. Umwelt Fabian 07.01..doc) einschließlich Prospekt (_Prospekt-VEW-Bremen.pdf), Referenzen (_ausgewaehlte-Referenzen_VEW-Bremen.pdf) und Anzeige aus VGB PowerTech 12/2010, Seite 15

/8.3/ VGB PowerTech 10/2010, Hentschel et al, „Alterungsmanagement der Elektro- und Leittechnik in Kraftwerken der RWE Power“, (_Hentschel_et_al-2010_Alterung-EuLT_VGB-Powertech.pdf)

/8.4/ A: Graf; „Redesigns Programmable Logic Devices”, Foliensatz, (PLD_Redesign.ppt)

/8.5/ RSK-Information ERL7/Info_HP, „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ - „Zwischen den AG ERL Mitgliedern Brettner, Faller, Fischer, Graf, Riekert, Schröder und Waas abgestimmtes Hintergrundpapier zur gemeinsam getragenen Darstellung der Beratungsergebnisse der RSK-Arbeitsgruppe ERL“”, Entwurf vom 26.01.2011 (7.Sitzung ERL-Langfassung_26-01-2011.doc)

/8.6/ Kommentare von H. Schröder zu /2.2/ vom 07.02.2011 (7.Sitzung ERL-Langfassung_26-01-2011_Anmerkungen_Sch.doc)

/8.7/ RSK-Information ERL7/Info 1, “„Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ Darstellung der Beratungsergebnisse der RSK-Arbeitsgruppe ERL”, Entwurf vom 14.01.2011 (7.Sitzung ERL-Stellungnahme_14-01-2011_Kurzfassung.doc)

/8.8/ RSK-Information ERL7/Info 1, “„Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ Darstellung der Beratungsergebnisse der RSK-Arbeitsgruppe ERL”, Entwurf vom 17.01.2011 (7.Sitzung ERL-Stellungnahme_17-01-2011_Kurzfassung.doc)

/8.9/ C. Bühler, C. Verstegen, „gekürzte Fassung der RSK-Information ERL7/Info 1 vom 14.01.2011“, 21.01.2011 (7 Sitzung ERL-Stellungnahme_14-01-2011_Kurzfassung gekuerzt.doc)

/8.10/ Dr. Riekert, „Anmerkungen zur RSK-Information ERL7/Info 1 vom 17.01.2011“, 06.02.2011 (ERL-Stellungnahme_17-01-2011_Kurzfassung_DrRi.doc)

/8.11/ U. Waas, „Kapitel 14: Zusammenstellung abgeleiteter Anforderungen und Empfehlungen“, 04.02.2011 (7 Sitzung ERL-Stellungnahme_Kap.14_20110204.doc)

/8.12/ RSK-Information ERL8/Info 1, “„Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ Darstellung der Beratungsergebnisse der RSK-Arbeitsgruppe ERL”, Entwurf vom 09.02.2011 (ERL-Stellungnahme_Kurzfassung_09.02.2011.doc)

/8.13/ RSK-Information ERL9/Info 1, “„Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ Darstellung der Beratungsergebnisse der RSK-Arbeitsgruppe ERL”, Entwurf vom 09.02.2011 (ERL-Stellungnahme_Kurzfassung_09.03.2011.doc)

/9.1/ /8.13/ mit Kommentare von Frau Bühler und Herrn Verstegen, 16.08.2011 (ERL-Stellungnahme_16-08-2011_VER_BUE an Brettner.doc)

/9.2/ /9.1/ mit Kommentare von Herrn Dr. Riekert, 03.09.2011 (ERL-Stellungnahme_16-08-2011_VER_BUE Struktur DrRi.doc)

/9.3/ /9.1/ mit Kommentare von Herrn Dr. Riekert, 03.09.2011 (ERL-Stellungnahme_16-08-2011_VER_BUE an Brettner_gr+wa.doc)