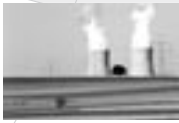
İLK

INTERNATIONALE
LÄNDERKOMMISSION
KERNTECHNIK

Baden-Württemberg · Bayern · Hessen



ILK Recommendation

on the Avoidance of Dependent Failures of Digital I&C Protection Systems

Für deutsche Fassung bitte umdrehen!

September 2003
No.: ILK-15 E

Foreword

The International Committee on Nuclear Technology (Internationale Länderkommission Kerntechnik, ILK) was established by the three German states of Baden-Württemberg, Bavaria and Hesse in October 1999. It is currently composed of 13 scientists and experts from Germany, France, Sweden, Switzerland and USA. The ILK acts as an independent and objective advisory body to the German states on issues related to the safety of nuclear facilities, radioactive waste management and the risk assessment of the use of nuclear power. In this capacity, the Committee's main goal is to contribute to the maintenance and further development of the high, internationally recognised level of safety of nuclear power plants in the southern part of Germany.

Commensurate with advances in technology, the last years have seen an increasing application of digital safety instrumentation and control (I&C) systems in nuclear power plants. The ILK views this approach as being particularly important in terms of safety and has thus, with the support of a third party expertise, dealt extensively with the aspect of avoiding dependent failures in the use of digital I&C systems. The present ILK recommendation was adopted at the 25th ILK meeting on September 15th, 2003 in Stuttgart. For re- and backfits with digital safety I&C systems the ILK recommends measures that, given a relatively simple system structure are necessary to allow the assessment of a dependent failure as being sufficiently improbable. The recommendation is directed at licensees and the regulatory authorities.

The Chairman

Dr. Serge Prêtre

ILK - Geschäftsstelle beim Bayerischen Landesamt für Umweltschutz

Bürgermeister-Ulrich-Str. 160
D-86179 Augsburg
Telefon: +49-173-65 707-11/-10
Telefax: +49-173-65 707-98/-96
E-Mail: info@ilk-online.org
http://www.ilk-online.org

1 Statement of affairs

1. In German nuclear power plants, the instrumentation and control (I&C) technology with the highest importance for safety is essentially hard-wired. In future, digital I&C systems will be put into use as a result of their manifold and sufficiently known advantages.

For this reason, the German Reactor Safety Commission (Reaktorsicherheitskommission, RSK) published guidelines [1] on digital safety instrumentation and control in 1996. In these guidelines, the process-engineering requirements on safety I&C systems are called I&C-functions. Their implementation in executable software represents the application software. Depending on their importance for safety, these I&C functions are assigned to one of three categories with graded requirements on their development, manufacture, qualification and operation. I&C functions of category 1 are given the highest importance for safety and constitute the protection system. For this reason, functions relating to the reactor protection system such as tripping the reactor or activating the engineered safety features actuation system are largely found in category 1. In the case of low expected damage impacts, protective limitations are used. These are thus assigned to category 2. Categories 1 and 2 of the I&C functions are independent of each other and are implemented in associated equipment that is subject to the same level of equipment requirements. Due to their low importance for safety, category 3 I&C functions receive no further mention here.

2. Next to the provisions for controlling accidents through the safety system, internal accident management measures have been planned that are able to control beyond design basis events or that can attenuate their impact. These measures are basically manual measures. I&C devices are necessary in order to obtain the necessary information and to initiate the corresponding measures. For this purpose, equipment of the operational I&C systems may be used in agreement with regulations applying to internal accident management. Due to the low probability of occurrence of such events, these devices do not have to satisfy the requirements placed on safety I&C systems, especially as far as dependent failures are concerned.

A dependent failure refers to a system failure that is based on a latent design or manufacturing fault with the potential of causing, through the occurrence of a single initiating event, correlated coincidental failures of redundant components or system functions.

Recommendation

The above-mentioned RSK guidelines [1] influenced the licensing procedure for digital I&C re- and backfits for nuclear power plants (NPP) Neckarwestheim 1 and Unterweser in 1998. These involved implementing, amongst other things, category 2 I&C functions in digital automation devices. While the consideration of the dependent failure does not represent a stringent design requirement in this category, it was nevertheless given due significance in the licensing process.

It should be recalled that up to now, there is no generally accepted methodology in the field of probabilistic analyses to take account of failures caused by software. For this reason, individual measures are prone to subjective assessments in terms of their effectiveness in preventing dependent failures. The present recommendation by the ILK should thus act as signpost to help both licensees and licensing authorities for assessing such re- and backfits.

The ILK initiated an investigation [2] with the objective of assessing the effectiveness of known measures for preventing dependent failures of a digital safety I&C system.

3. In order to make the likelihood of I&C dependent failures sufficiently improbable, commonalities between the redundant I&C installations should be avoided as far as possible. This requires giving consideration to the entire signal processing path from the sensors to the actuator.

No simple rules exist for determining concrete measures. Instead, as the review of international practice sketched below shows, the approach taken thus far has been to develop specific solutions suited to the circumstances of individual nuclear power plants. The frequency of incidents to be controlled as well as the consequences of an assumed failure of I&C have played an important role in this approach. Additionally, the consequences of such an I&C failure can be counteracted within the defence-in-depth concept by other installations of the nuclear power plant. General rules for evaluating measures for avoiding dependent failures exist in the USA [3] and also in the UK [4] where these rules also include the postulated probabilities of occurrence of dependent failures; a review is given in [2].

4. CANDU plants (Canada) have two diversified shut-down systems with threefold redundancy that process measurement signals independently of each other from the sensor to the actuator. Either shut-down rods or gadolinium nitrate are used for the shut-down procedure. A primary and secondary protection system is installed in Temelin (Czech Republic) and in Sizewell B (UK), where, in the case of Temelin, both systems operate digitally. The secondary protection system in Sizewell is not

redundant with the primary protection system, but for probabilistic reasons initiates countermeasures for incidents that are assumed to be more frequent. Among the French N4-plants (Chooz, Civaux), the digital SPIN (Système de Protection Intégré Numérique) is supplemented by a correspondingly graded qualified I&C system by the same manufacturer as SPIN, also for probabilistic reasons. In this way, for anticipated transients without scram (ATWS), measures such as [isolating the steam generator, activating emergency feed, de-energizing control rod drivers, turbine trip, safety injection] are initiated independently of the SPIN system. In Beznau (Switzerland), the existing hardwired separate emergency system was extended while backfitting the protection system to digital I&C technology. Kashiwasaki-Kariwa 6 and 7 (Japan), Bohunice (Slovakia) and Paks (Hungary) all have a digital protection system without diversified hardware. The one in Paks, for instance, consists of three redundant trains, each with two diversified groups of actuating criteria.

5. Diversified design represents a technical measure for achieving independence among I&C devices. Essentially, there are two kinds of diversity for the hardwired reactor protection system: Functional diversity describes physically diversified actuating criteria that serve the same purpose. Wherever different actuating criteria do not exist, at least diversity in the peripheral equipment of the reactor protection system most at risk (namely, the measuring devices and actuators) is used. These normally remain unaffected by a digitalization of the central I&C systems. Hardware diversity is limited to the central part of the complete signal processing path.

6. Diversified hardware in digital automation equipment is usually also taken to provide for the use of mutually independent system software. This includes the functions of the operating systems, the compiler and the communication system for the individual automation devices. Since the number of digital safety I&C systems is very low, economic arguments weigh against the complete and costly development and servicing of corresponding specialized equipment whose functionality is also needed elsewhere. Thus, one needs to at least occasionally revert to using industrial off-the-shelf products that were not designed with nuclear engineering guidelines in mind.

For this reason, there is a tendency to demand the use of diversified hardware especially during the introduction of digital safety I&C systems when experience with these systems is still being built up. Diversified hardware, due to the ensuing diversity of the system software that it essentially entails, is able to counteract design- and implementation errors. However, diversified hardware cannot counter specification errors of the application software.

Recommendation

On the other hand, an equipment platform usually also includes a software development environment. For diversified hardware, this fact translates into the need to maintain and administer at least two equipment platforms as well as their corresponding development environments. Since, in the case of two platforms, a situation could conceivably arise where each arrives at different results, the demand for a minimum of three separate equipment platforms could be made. When compared to existing reactor protection systems, a deterministic argument of this kind would evidently lead to excessive design requirements which could be effectively countered by employing probabilistic methods.

Experience shows that hardware weaknesses and errors can frequently be compensated by software measures. Moreover, digital electronic modules generally show a higher reliability than analog, hardwired ones due especially to their considerably increased failure detection mechanisms.

7. For the sake of completeness, the following design features of a digital safety I&C system are mentioned. These partly result from RSK guidelines [1] which must be complied with in German plants:

(1) The computers belonging to the safety I&C system periodically process their programs in a fixed sequence. This leads to constant processor and communication loads. [according to RSK-LL 7.3.2 (13), 7.6.1.1 (4)]

(2) The computers of two mutually redundant trains have not been temporally synchronized. Furthermore, the starting points of the computers in the individual trains are consciously chosen to differ. This makes a simultaneous access to erroneous operating system resources given identical (time-)counter reading less likely. [according to RSK-LL 7.3.5 (2)]

(3) Operator actions and maintenance work for redundant automation devices are not undertaken at the same time. [RSK-LL 7.2.1 (12), 7.3.9 (4)]

(4) Only highly qualified hardware and software is used. [RSK-LL 7.3.6.2 und 7.3.7]

2 Assessment

1. The ILK welcomes the willingness of NPP licensees to digitalize safety I&C systems. The ILK expressly endorses the approach taken whereby I&C functions with graded importance for safety are digitalized first in order to gain experience with this new technology. The ILK sees this as a responsible contribution to the safe operation of NPPs. In this way, the foundation for the correct assessment of the potential for dependent failures can be laid.

2. Due to the very low number of known incidents in the use of a digital safety I&C system, the ILK cannot make definitive statements on the probable initiating events for dependent failures. The incidents do, however, reflect experiences that are well-known from software development where peculiarities not covered by the specification as well as a number of operating situations, such as inspections and maintenance procedures with numerous possibilities of intervention, present special problems.

Diversified hardware is unable to avoid these potential causes of dependent failures.

3. The ILK points out that one of the times in which diversified hardware in a digital safety I&C system is used is whenever probabilistic objectives are to be achieved as a proof for the high level of safety. To date, no *generally accepted* methodology exists for including failures caused by erroneous software in a probabilistic analysis. Currently, great efforts are being undertaken to take account of human factors.

4. The ILK is fully aware of the increase in system complexity and resulting higher susceptibility to errors, e.g. during maintenance, associated with the use of different types of hardware.

5. The ILK judges the functional diversity to be more effective than hardware diversity, also because diversified hardware only covers a part of the entire signal processing path: Functional diversity means diversified I&C functions and thus leads to independent parts of the application software.

6. For this reason, the ILK views the use of a single equipment platform as a more effective precondition for avoiding dependent failures if, within the defence-in-depth concept, functional diversity as well as different "system ages" in the mutually redundant I&C trains are used in the safety I&C system. Different kinds of application software that are executed on similar but physically separate hardware are based on diversified functions. Different "system ages" reinforce the independence of individual I&C trains in terms of the functions requested with the same (time) counter reading of the system software.

7. The investigation into CONVOY plants showed that the actuating criteria of a reactor scram are fully functionally diversified. In contrast, the actuating criteria for the engineered safety features actuation system have only been halfway functionally diversified. Functional diversity could be increased by formulating modified or additional I&C functions. The implementation of corresponding I&C functions in digital technology is free of the restrictions placed on the functionality of qualified electronic modules of hardwired technology. However, also in this case due regard should always be given to the principle that the design of the safety I&C systems of category 1 should be simple [RSK-LL 7.3.2 (4), 7.6.1.2.1 (2,3)].

Recommendation

3 Recommendations

Beyond the requirements laid out by the RSK-guidelines [1], the ILK recommends the following approach especially towards re- and backfits with digital safety I&C systems of category 1, excluding their measurement equipment and actuators, as a necessary precondition in order to make dependent failures sufficiently unlikely. The failure of category 1 safety I&C systems represents a beyond-design-basis incident.

1. Different approaches should be taken in the definition and validation of I&C functions. The considerations should be characterized by diversified starting points. For instance, the starting points could be described using word pairs (event-oriented, safety goal-oriented) or (bottom-up, top-down) or alternatively (inductive-deductive).

2. The requirement specification of a safety I&C system [RSK-LL 7.3.3 (1)] should in particular fully cover its maintenance as well as the plant components it communicates with for all plant operating conditions.

3.1 If the objective pursued is to initially only *partly* digitalize category 1 safety I&C systems, then the part that is to be digitally implemented should ideally be configured in such a way that the functionality of the remaining hardwired part is diverse from the new digital part.

3.2 If this is not the case for individual I&C functions, then they should have functional diversity [RSK-LL 7.3.4 (2)]. Functional diversity can either be implemented solely in the new digital part or should exist - within the framework of the defence-in-depth concept - in corresponding I&C functions of category 2.

4.1 In case the category 1 safety I&C systems are to be *entirely* digitalized, then the activation of the engineered safety feature actuation system, especially for not unequivocally safety-related measures, should be carried out in a functionally diversified way. For this purpose, physically diversified actuating criteria should be used [RSK-LL 7.3.4 (2)].

4.2 Should this turn out not to be purposeful in a technical sense, then equivalent measures should be taken. For instance, a category 2 I&C function can be implemented in order to take credit from the defence-in-depth concept within safety I&C systems.

5. Diversified I&C functions should be processed by physically separate equipment.

Literature

[1] RSK-Leitlinien für Druckwasserreaktoren, Stand 15.11.1996, BAnz Nr. 158a vom 23.08.1996, 4. Änderung: Berichtigung (BMU-Bekanntmachung vom 29.10.1996) BAnz Nr. 214 vom 15.11.1996

[2] M. Baleanu, E.-W. Hoffmann, M. Kersken, A. Lindner, J. Märtz, E. Sädtler, G. Schnürer und D. Wach, „Empfehlungen zur Systemarchitektur und zur Anwendung von Hardware-Diversität zur Vermeidung gemeinsam verursachter Ausfälle bei Nutzung einer digitalen Sicherheits-Leittechnik“ ISTec - A - 723, April 2003

[3] NUREG-0800, Standard Review Plan, Appendix 7-A, Branch Technical Position HICB - 19, “Guidance for Evaluation of Defence-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems”, Rev. 4 - June 1997, US-NRC, Washington, USA

[4] Safety Assessment Principles for Nuclear Plants, 1992
ISBN 0118820435, HSE Books, P Box 1999,
Sandbury, Suffolk C010 2 WA oder www.hse.gov.uk/nsd/saps.htm

1. **Prof. Dr. George Apostolakis, USA**
   Professor of Nuclear Engineering and Engineering Systems at the Massachusetts Institute of Technology (MIT) in Cambridge, USA

2. **Prof. Dr. phil., Dr.-Ing. E.h. Adolf Birkhofer, Germany**
   Managing Director of ISaR Institute for Safety and Reliability GmbH
   Holder of the Chair for Reactor Dynamics and Reactor Safety at the Technical University of Munich

3. **Ms. Annick Carnino, France**
   Former Director of the Division of Nuclear Installations Safety at the IAEA

4. **Prof. Dr.-Ing. Dr.-Ing. E. h. Dr. techn. h. c. Josef Eibl, Germany**
   Former Director of the Institute for Massive Construction and Building Material Technology at the University Karlsruhe

5. **Prof. Dr.-Ing. habil. Hans Dieter Fischer, Germany**
   Holder of the Chair for Communication Theory at the Ruhr-University Bochum

6. **Ing. Bo Gustafsson, Sweden**
   Former Managing Director of SKB International Consultants AB founded in 2001 as the international branch of SKB

7. **Prof. Dr. rer. nat. habil. Winfried Hacker, Germany**
   Former Professor for General Psychology at the Technical University of Dresden

8. **Prof. Dr.-Ing. habil. Wolfgang Kröger, Switzerland**
   Holder of the Chair for Safety Technology at the ETH Zurich

9. **Ing. Marcel Lallier, France**
   Former Head of Operations of the “EPR“ (European Pressurized Reactor) Project

10. **Dr.-Ing. Erwin Lindauer, Germany** (Vice Chairman)
    Chief Executive Officer of the GfS Gesellschaft für Simulatorschulung mbH
    Chief Executive Officer of the KSG Kraftwerks-Simulator-Gesellschaft mbH

11. **Dr. Serge Prêtre, Switzerland** (Chairman)
    Former Director of the Swiss Nuclear Safety Inspectorate
    (HSK, Hauptabteilung für die Sicherheit der Kernanlagen)

12. **Prof. Dr.-Ing. habil. Eberhard Roos, Germany**
    Holder of the Chair for Material Testing, Material Science and Material Properties at the University Stuttgart
    Director of the State Materials Testing Institute, University Stuttgart

13. **Prof. Dr. Frank-Peter Weiß, Germany**
    Professor of Plant Safety at the Technical University Dresden
    Director of the Institute for Safety Research at the Research Centre Rossendorf

(Members are listed in alphabetical order)

ILK Publications:

ILK-01 ILK Statement on the Transportation of Spent Fuel Elements and Vitrified High Level Waste (July 2000)

ILK-02 ILK Statement on the Final Storage of Radioactive Waste (July 2000)

ILK-03 ILK Statement on the Safety of Nuclear Energy Utilisation in Germany (July 2000)

ILK-04 ILK Recommendations on the Use of Probabilistic Safety Assessments in Nuclear Licensing and Supervision Processes (May 2001)

ILK-05 ILK Recommendation on the Promotion of International Technical and Scientific Contacts of the Nuclear Safety Authorities of the German States (October 2001)

ILK-06 ILK Statement on the Draft Amendment dating from the July 5 2001 to the Atomic Energy Act (October 2001)

ILK-07 ILK Statement on Reprocessing of Spent Fuel Elements (November 2001)

ILK-08 ILK Statement on the Potential Suitability of the Gorleben Site as a Deep Repository for Radioactive Waste (January 2002)

ILK-09 ILK Statement on the General Conclusions Drawn from the KKP 2 Incidents associated with the Refueling Outage of 2001 (May 2002)

ILK-Publications

ILK-10 ILK Statement on the Handling of the GRS Catalog of Questions on the "Practice of Safety Management in German Nuclear Power Plants" (July 2002)

ILK-11 ILK Recommendation on Performing International Reviews in the Field of Nuclear Safety in Germany (September 2002)

ILK-12 Internal ILK-Report on the Intentional Crash of Commercial Airliners on Nuclear Power Plants (March 2003)

ILK-13 ILK Statement on the Proposals for EU Council Directives on Nuclear Safety and on Radioactive Waste Management (May 2003)

ILK-14 ILK Statement on the Recommendations of the Committee on a Selection Procedure for Repository Sites (AkEnd) (September 2003)

ILK-15 ILK Recommendation on the Avoidance of Dependent Failures of Digital I&C Protection Systems (September 2003)

ILK-CD CD with all presentations held at the ILK Symposium "Opportunities and Risks of Nuclear Power" in April 2001