Concepts for the architecture of digital I&C systems in NPPs and approaches for their assessment

Robert Arians, Dagmar Sommer

GRS mbH, Schwertnergasse 1, D-50667 Cologne

Abstract:
In recent years, many I&C systems of NPPs were replaced by software-based I&C systems.Due to the more complex structure, software-based I&C equipment shows the potential for new failure mechanisms and an increasing number of failure possibilities, including the potential of common cause failures. To assess the reliability of this equipment, methods for a reliability assessment need to be worked out. To fulfil the requirements given by different authorities the architectures of digital I&C systems have to be designed to prevent and control potential common cause failures. In this paper, some examples for international requirements concerning the design of software-based I&C systems in safety systems of NPPs, some methods for a reliability assessment of I&C systems and examples for software-based architectures are given.

1INTRODUCTION

The equipment of I&C systems in German NPPs is often in use since their commissioning in the 1970ies/1980ies. Thus, an increasing amount of equipment of I&C systems has to be replaced reaching its end of lifetime. Procurement of the spare parts for these systems is getting more and more difficult. Consequently, a replacement with identical equipment is not always possible or even not wanted as modern equipment allows optimisation of processes. Thus, an increasing amount of equipment is replaced with software-based equipment.

Software-based equipment shows specific characteristics differing remarkably from the characteristics of conventional analogue I&C equipment, e. g. a more complex structure, additional properties, changed failure mechanisms and failure behaviour, and a changed man-machine interface. An additional contribution to this more complex realisation of the equipment is the use of specific development tools. Due to the use of software or programmable logic (e. g. FPGA)modern I&C equipment shows the potential for new failure mechanisms and consequently an increasing number of failure possibilities. Concerning single failures software-based equipment is deemed to have a higher reliability in comparison to analogue equipment as additional self-testing and failure detection routines are in place. But another important aspect of the reliability of a software-based I&C system is its robustness against common cause failures (CCF).Systematic failures of software may occur if programming errors which always can exist latently in any software are triggered by a certain, randomly arising system status or combination of parameters, thus leading to an unknown failure mechanism. One additionally important aspect of new failure mechanisms is the possibility of manipulation of software-based equipment by malware having a remarkable contribution to the potential of CCF.

The reliability of software-based and programmable equipment has to be investigated and assessedconsidering its specific characteristics. It has to be decided which requirements have to be fulfilled to allow the installation of this equipment in safety I&C systems of NPPs. In this paper, the positions in selected countries concerning measures to prevent CCF and concerning requirements to control CCF are outlined. Further, examples of architectures of digital I&C systems realised are shown and its characteristics for CCF prevention and control are discussed.

2INTERNATIONAL REQUIREMENTS CONCERNING THE DESIGN OF SOFTWARE-BASED I&C SYSTEMS IN SAFETY SYSTEMS

The probability of common cause failures in software-based I&C systems and measures to control an occurring CCF are highly discussed as well nationally as internationally. In the following it is outlined which requirements are made by different authorities and TSOs concerning prevention and especially control of CCF in safety I&C systems in NPPs. Therefore, the requirements made by IAEA, NRC, HSE, European nuclear regulators and the German federal authority and TSOs (VdTÜV) are outlined.

IAEA

The main guideline of IAEA concerning design of I&C systems in NPPs is NS-G-1.3 “Instrumentation andControl SystemsImportant to Safety inNuclear Power Plants“. /1/ It contains the following statements:

- … design features such as tolerance of random failure, tolerance of common cause failures, fail-safe design, independence of equipment and systems, selection of high quality equipment, testability and maintainability should be considered as appropriate.
- Diversity provides defence against common cause failures, is complementary to the principle of defence in depth and increases the chance that safety tasks will be performed when necessary. …Types of diversity that may be considered include human diversity,design diversity, software diversity, functional diversity, signal diversity, equipment diversity and system diversity.
- Additional conservatism should be provided where the necessary demonstration of system reliability is not feasible, e.g. where the reliability of a multiple redundant system will be limited by such factors as common cause failures or uncertainties in the design. Specific difficulties may arise in demonstrating the reliability of computer based systems, for example. Diversity is a way to include conservatism in order to compensate for the difficulty of demonstrating the necessary level of reliability.

Concerning CCF in digital I&C systems more details are given in the IAEA technical report /2/ “Protecting against Common Cause Failures in Digital I&C Sysems of Nuclear Power Plants”. Here the following measures for I&C design against CCF are proposed:

- Minimizing faults in structures, systems and components
- Avoiding common faults
- Avoiding concurrent activation
- Avoidance of failure propagation
- Avoidance of common subsystems
- Fault tolerance.

Minimizing faults includes fault avoidance during design and development and fault detection and removal during verification and validation activities in the development process.
Concerning avoiding common faults the following statements are given:

- Despite the measures taken to eliminate faults from I&C designs (quality aspects), it is still postulated that there remain residual faults. For systems that are supposedly independent from one another, it is important to ensure that common faults do not exist or are not triggered at the same time. Diversity is the principle means of achieving this.

Concerning diversity attributes as types of system diversity are considered human diversity, functional diversity and design diversity.

- Human diversity is the employment of several people with different background, experience, etc to solve the same problem.
- Functional diversity is in place if two systems performing different physical functions have an overlapping safety effect.

- Design diversity is the use of different solutions to solve the same problem or separate instances of the same problem. The rationale of design diversity is that the different, independent solutions obtained through design diversity are expected to have different faults and different failure modes, thus reducing the potential for a CCF.
  Summing up, it is stated that a single type of diversity helps, but usually does not guarantee, to avoid CCFs. Incorporating several types of diversity may be most effective in dealing with this limitation.

U.S. NRC

The U.S. NRC refers to the Standard Review Plan (SRP) which gives in chapter 7 guidance for review of I&C for nuclear power plants. In chapter 7.8, Rev. 5 the review process and acceptance criteria for the diverse instrumentation and control (I&C) systems and equipment provided for the expressed purpose of protecting against potential common-cause failures of protection systems is described. /3/ It is stated that:

- For plants with a digital reactor trip system(RTS) or an engineered safety features actuation system(ESFAS), the NRC position on diversity and defense-in-depth(D3) should be especially noted. This position is contained in Item II.Q, “Defense Against Common-Mode Failures in Digital Instrument and Control Systems,” of the Staff Requirements Memorandum (SRM) on SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs.” SRM requirements applicable to diverse I&C functions are as follows:
  - “If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure [as the safety system], shall be required to perform either the same function [as the safety system function that is vulnerable to common mode failure] or a different function [that provides adequate protection]. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary functions under the associated event conditions.”

Further, in the regulatory guide 1.152 “Criteria for use of Computers in Safety Systems of Nuclear Power Plants”, Rev3, 2011 it is stated that /4/:

- With the introduction of digital systems into plant safety system designs, concerns have emerged aboutthe possibility that a design error in the software in redundant safety system channels could lead to a common-cause failure or common-mode failure of the safety system function. Conditions may exist under which some form of diversity may be necessary to provide additional assurance beyond that provided by the design and quality assurance (QA) programs that incorporate software QA and verification and validation (V&V). The design techniques of functional diversity, design diversity, diversity in operation, and diversity within the four echelons of defense in depth (provided by the reactor protection, engineered safety features actuation, control, and monitoring I&C systems) can be applied as defense against common-cause failures. Manual operator actuations of safety and nonsafety systems are acceptable, provided that the necessary diverse controls and indications are available to perform the required function under the associated event conditions and can be completed within the acceptable time.
- The NRC does not endorse the concept of quantitative reliability goals as a sole means of meeting its regulations for reliability of digital computers used in safety systems. The NRC’s acceptance of the reliability of computer systems is based on deterministic criteria for both hardware and software. Quantitative reliability determination, using a combination of analysis, testing, and operating experience, can provide an added level of confidence in the reliable performance of computer systems.

TheBranch Technical Position (BTP) 7-19, “Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems,”, Rev6, 2012 in NUREG-0800, “Standard Review Plan,” Section 7, “Instrumentation and Controls,” provides additional guidance /5/:

- There are two design attributes that are sufficient to eliminate consideration of software based or software logic based CCF:
    - Diversity - If sufficient diversity exists in the protection system, then the potential for CCF within the channels can be considered to be appropriately addressed without further action.

      Example: An RPS design in which each safety function is implemented in two channels that use one type of digital system and another two channels that use a diverse digital system. If a D3 analysis performed consistent with the guidance in NUREG/CR-6303 determines that the two diverse digital systems are not subject to a CCF, then,in this case, no additional diversity would be necessary in the safety system.
    - Testability - A system is sufficiently simple such that every possible combination of inputs and every possible sequence of device states are tested and all outputs are verified for every case (100% tested).

Summing up, U.S. NRC does not accept quantitative reliability goals only for a digital I&C system in safety systems of NPPs but claims for deterministic criteria for hardware and software.To eliminate the consideration of a CCF in software based systems,according to U.S. NRC sufficient diversity in the systems and testability of the systems have to be realised. Concerning the question if a certain system has sufficient diversity, U.S. NRC requires an analysis applying the guidance of NUREG/CR-6303. /15/

HSE (UK)

In the “Generic Design Assessment – New Civil Reactor Build; Step 4, Control and Instrumentation Assessment of the EDF and AREVA UK EPR^{TM} Reactor”, Rev0, 2011 from the Office for Nuclear Regulation it is stated that /6/:

- The use of various forms of diversity within systems performing protection functions is important to minimise the risk of simultanous failure on demand of those systems.
- A review of the diversity of those systems implementing reactor protection functionality was completed. The systems included in the diversity review were the protection system (PS) (TXS) and the safety automation system / process automation system (SAS / PAS) (Siemens SPPA-T2000). The approach included consideration of various forms of diversity, including:
    - Equipment diversity (including diversity of platform);
    - Diversity of verification and validation;
    - Diversity of physical location (segregation);
    - Software diversity;
    - Functional / data / signal diversity;
    - Diversity of design / development; and
    - Diversity of specification.

EUROPE

The report “Licensing of safety critical software for nuclear reactors – Common position of seven European nuclear regulators and authorised technical support organisations”, Revision 2010 from BEL V (Belgium), BfS (Germany), CSN (Spain), ISTec (Germany), NII (United Kingdom), SSM (Sweden), and STUK (Finland) gives the following information about their opinion concerning software design diversity /7/:

- In order to achieve high reliability, use is typically made of redundant systems and components. While identical redundancy is effective in guarding against random hardware failures, a common cause failure possibility arises from systematic failures, e.g. specification, design, implementation and maintenance errors etc. Diversity may be introduced to provide protection against common cause failures.

- One approach typically adopted during architecture design, to protect against the possibility of common cause failure, is to consider the use of multiple, possibly diverse, systems. Also consideration of the need for defence in depth such that a failure in one layer is compensated for in the overall systems architecture may lead to the need for diverse, possibly software based, systems.
- The number of systems, components or channels required, the degree of diversity between them, the apportionment of reliability targets and the selection of the technology for each of them have to be addressed. One approach that may be adopted for one-out-of two systems where one of them is a computer based system is to employ a simple non-computer based secondary system.Where multiple computer based systems, channels or components are employed, the issue of software diversity has to be considered.

GERMANY

In the Revision D of the “Safety Criteria for Nuclear Power Plants” /8/ of the German Federal Ministry for the Environment, Nature Conservation and Nuclear Safety the following statements are given:

- Safety installations for which potentials for common-cause failures were identified are designed according to the principle of diversity as far as feasible and technically reasonable.
- The nuclear power plant is equipped with reliable instrumentation and control installations with functions on level of defence 3 (reactor protection system) whose instrumentation and control functions initiate protective actions as soon as defined response levels are reached. These installations are designed according to the following principles:
    - redundant design of components, sub-assemblies and sub-systems,
    - physical separation of installations corresponding to the impact range of possible postulated initiating events,
    - diversity,
    - automatic failure monitoring,
    - adaption of the components to the possible ambient conditions,
    - simple software structure,
    - limitation of the functional scope to the necessary safety-related degree,
    - use of fault-preventing, fault-detecting and fault-controlling measures and installations.
- The design of the instrumentation and control installations executing instrumentation and control functions of Category A (the instrumentation and control functions of Category A comprise all I&C functions necessary to control events assigned to level of defence 3) provides measures against systematic failures of the software-based instrumentation and control installations including systematic software failure in such a way that the systematic failure is controlled.
- For software-based instrumentation and control, dissimilar instrumentation and control installations are used as a matter of principle.
- For protective actions not being safety oriented for every plant condition, a 2-fold or 3-fold dissimilar design of the software-based instrumentation and control is used in dependence of the effects of passive or active systematic failures in the instrumentation and control installations executing instrumentation and control functions of Category A.

TheGerman VdTÜV (all German TSOs) has given an opinionto the necessary preventive measures against systematic failures of digital instrumentation and control systems in nuclear facilities that execute instrumentation and control functions of Category A. /9/ In this opinion the following statements are given:

- The principally precautionary measures that have to be taken according to the state of science and technology include the full range of measures for fault avoidance as well as the failure controlling measures.

- Only the failure controlling measures in view of dissimilar installations from redundant channels or strands or subsystems are treated. … Dissimilar means in that case sufficiently different hardware, software, development tools, development teams, manufacturing, and testing and maintenance, so that a systematic failure of mutually dissimilar installations is sufficiently unlikely.
- For protective actions not being safety oriented for every plant condition, a 2-fold or 3-fold dissimilar design of the digital instrumentation and control should be used.

CONCLUSION

The requirement of diversity for software-based systems is different in clarity between the different authorities, but the unanimous opinion of all cited authorities and TSOs is that diversity provides defence against CCF. Especially the U.S NRC and the German VdTÜV require diversity for software-based I&C systems. Thereby, an effective diversity is required which is not only given by one attribute. A further investigationof the diversity attributes of I&C systems is necessary to show if effective diversity is given.

3METHODS FOR RELIABILITY ASSESSMENT OF I&C SYSTEMS

Before installation of software-based safety I&C systems in NPPs the following questions are essential:

- Is the planned I&C system sufficiently robust?
- Is the design of the I&C equipment sufficiently diverse?
- How large is the probability that a software CCF occurs?

To find an answer to these questions considering the equipment reliability, adequate methods for a reliability assessment of software based I&C systems have to be worked out.

The methods for a software reliability assessment are used to estimate failure rates from software-based components or systems and to specify failure probabilities. Principally two different failure modes have to be distinguished:

- Failure to generate a signal when it is needed (failure to trip)
- Generation of a signal when it is not needed (spurious trip)

For software-based I&C systems such as a reactor protection system the probabilities for both failure modes have to be estimated. Therefore, different reliability methods may need to be used depending on the failure mode of interest, a failure-rate based method or a failure-on-demand based method.

Some methods for the assessment of the reliability of software-based equipmenthave been developed in recent years. These are for example:

- Failure mode and effects analysis
- Fault tree analysis
- Markov processes methodology and Petri net methodology
- Dynamic flow graph methodology
- Simulation and or test-based methods
- Bayesian belief network methods
- Software reliabilitygrowthmethods

Especially for the installation of a homogenous, software-based safety I&C system, the requirements relating to the accuracy of a method to show the system reliability are very high. On the other hand, the assumptions which have to be taken as a basis for an appropriate assessment method are inevitably fraught with uncertainties. Therefore, the fundamental question that arises is if any of the methods under discussion is capable of making a sufficiently reliable statement concerning the installation of a singlesoftware-based safety I&C system in a NPP. The proof of a high reliability of a I&C system would be required if it should be installed as a single homogenous I&C system without providing additional measures to improve reliability.

A discussion by experts at the PSAM11 in Helsinki 2012 revealed that this problem will probably remain unsolved. If a solution cannot be given by a proof of the reliability of a single homogenous software-based I&C system, then those high requirements for reliability of the I&C system have to be solved by a system design considering all potential CCFs in software as well as in hardware. Therefore diversity may be introduced to provide means to control common cause failures.

4EXAMPLES FOR SOFTWARE-BASED ARCHITECTURES

In many German and international NPPs software-based I&C equipment is already implemented or its implementation is planned for the near future. In the following, some examples are given.

GERMANY

In nearly all German NPPs software-based equipment in I&C systems is installed. The software-based I&C equipment is almost exclusively used in operational systems. These are for example:

- Process computer to evaluate the operating condition and to record the process parameters
- Control and limitation equipment for carrying out the specified normal operation of the plant
- Digital measuring devices, for example neutron flux instrumentation
- Control systems of the refueling machine
- Control and protection systems of the turbine

In no German NPP software-based equipment is installed in the reactor protection system.

In the following, some examples for the refitting on software-based I&C equipment in German NPPs is given:

- NPP Biblis: reactor control (Teleperm XS)
- NPP Brokdorf: reactor control (Teleperm XS)
- NPP Brunsbüttel: reactor control (Teleperm XS)
- NPP Emsland: reactor control (Teleperm XS)
- NPP Grafenrheinfeld: core monitoring (Teleperm XS)
- NPP Grohnde: power distribution monitoring (Teleperm XS)
- NPP Gundremmingen: additional coolant tower water treatment (Symphony Melody)
- NPP Isar-1: reactor limitation and control (Symphony Melody)
- NPP Neckarwestheim-2: process computer (Teleperm XS)
- NPP Philippsburg-2: reactor power limitation and reactor control (Teleperm XS)
- NPP Unterweser: reactor limitation and control (Teleperm XS)
- NPP Philippsburg-1: independent emergency system USUS (Teleperm XS)
- NPP Brunsbüttel: refueling machine(Simatic S5/S7)

INTERNATIONAL

With the modernisation of international NPPs software-based I&C equipment is already used in the safety related I&C. For the design of new NPPs the use of software based I&C systems for all automation tasks is generally taken into account. In the following some examples for software-based I&C equipment used in international NPPs are given:

- NPPs Darlington-1 and -2, Canada
  - In the NPPs Darlington two functionally independent fast shutdown systems (SDS) are used. /10/ SDS1 works with control rods, SDS2 works with boric

acid. Both shutdown systems are build up triply redundant. They use different software-based system platforms, that means a different manufacturer, a different chip family and board layout and different development software, compiler and programmer. /10/ SDS1 uses a General Automation (GA) model 220 computer with a GA-16/220 microprocessor which is programmed in FORTRAN and GA-assembler. SDS2 uses a Digital Equipment Corporation (DEC) computer with a LSI-11/23 microprocessor which is programmed in PASCAL and MACRO-assembler. /10/

- NPP Sizewell-B, Great Britain
    - In the NPP Sizewell-B two protection systems are used. /10/ The primary protection system (PPS) includes the reactor trip and other safety relevant functions. The secondary protection system (SPS) is a diverse backup system. Both systems are designed four-fold redundant. /10/For the PPS the software-based Westinghouse Integrated Protection System (IPS) is used. In each of the four redundancies two functionally diverse subsystems are implemented which work with different activation criteria. For the SPS the Laddic technology from British Energy is used. It is based on hardwired magnetic core logic elements. /10/
- NPP Chooz-B1, France
    - In the NPP Chooz-B1 two systems in the safety I&C are used, the primary protection system for the reactor trip and the emergency cooling function and the diverse backup system. /10/ The primary protection system is based on the SPIN platform from AREVA NP, EdF and DS&S. A SPIN-N4 platform with a Motorola 68000 microprocessor (programmed in C) is used. The diverse backup system uses the Contronic-E platform from Hartmann & Braun. It is based on an Intel 80286 microprocessor with Intel 80287 co-processor and is programmed with a proprietary graphical programming language. /10/
- NPP Tianwan, China
    - In the NPP Tianwan a software-based safety I&C based on the AREVA Teleperm XS system is used. /10/ According to /11/, already in the planning phase two different physical criteria were defined for each initiating event. In the safety I&C of the reactor protection system two part-strands A and B are realized. The computers of both strands do not work synchronous and there is no data transfer between strand A and B. Additionally to the software-based system a hard-wired backup for the reactor protection system is used. /11/
- NPPs Loviisa-1 and -2, Finland (planned)
    - For the NPPs Loviisa a comprehensive retrofit of the entire I&C equipment is planned. /12/ The planned software-based safety I&C system is based on the AREVA Teleperm XS system. The planned operational I&C and the planned automatic backup system of the reactor protection system is based on SPPA T2000 from Siemens. Additionally some hard-wired components for a manual backup of the reactor protection system are planned. /12/
- NPPs Oconee-1 and -2, USA (planned)
    - For the NPPs Oconee a refitting of the existing hard-wired safety I&C to software-based I&C is planned. The planned software-based safety I&C is based on Teleperm XS by AREVA. /13/ The safety I&C comprises the reactor protection system (RPS) and the engineered safety protective system (ESPS). The RPS is planned as a four-fold redundant system with four electrically independent and physically separated channels. The ESPS consists of two redundant sub-systems, each of them with three input channels. /14/ To master a software CCF two additional systems which use conventional analogue limit switches will be installed. These are a diverse system for low pressure injection (DLPIAS) in case of a large leak and a diverse system for high pressure injection (DHPIAS) in case of a small leak. /14/ Additionally, two already existing diverse systems will be used which are based on another system platform (programmable logic controllers from Schneider). These are the AMSAC (ATWS Mitigation System) to control the ATWS with simultaneous

loss of main feedwater and the DSS (Diverse Scram System) for a diverse excitation of a reactor scram. /14/

These examples show different approaches to realise system diversity of different extent, ranging from some diverse backup functions up to two diverse reactor protection systems.

5 CONCLUSION

An increasing amount of hardwired I&C equipment of NPPs is already or will be replaced by software-based equipment which shows the potential for new failure mechanisms and an increasing number of failure possibilities due to its more complex structure, especially an increasing potential for CCF. The potential of a Common Cause Failure due to the possibility of a manipulation of the software-based equipment is one important new failure mechanism.Therefore, the robustness of a software-based I&C system against a CCF is an important aspect of the reliability of such a system.Due to this fact, the reliability of software-based I&C systems has to be investigated and assessed.

The methods for a reliability assessment of software-based I&C systems that have been developed in recent years have all one problem:to perform an appropriate assessment some assumptions have to be taken as a basis for this. These assumptions are inevitably fraught with uncertainties. Due to this problem, experts discuss if any of the assessment methods is capable of making a sufficiently reliable statement concerning the reliability of a I&C system. Up to today, no final solution is found and the problem will probably remain unsolved.

If a solution can’t be given by a proof of the reliability of a single, homogenous I&C system, then the adequate design of the I&C system must solve the problem. Therefore, different authorities made requirements concerning the prevention and control of a CCF in safety I&C systems in NPPs. We have outlined the requirements made by IAEA, NRC, HSE, European nuclear regulators and Germany. The unanimous opinion of these authorities is that diversity provides defence against CCF. Eventually various types of diversity should be used to minimise the risk of a simultaneous failure.To show that systems are effectively diverse further investigations have to be performed. In the opinion of the German TSOs (VdTÜV) diversity is an inevitable means to control an occurring CCF. The given examples of architectures of software-based I&C systems show the different approaches to reach diversity. The examples show that diversity is not only the theoretic requirement of some authorities and TSOs but furthermore it is also practicably feasible.

6 REFERENCES

/1/ IAEA safety guide NS-G-1.3, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, International Atomic Energy Agency, March 2002

/2/ IAEA nuclear energy series NP-T-1.5, Protection against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants, International Atomic Energy Agency, November 2009

/3/ U.S. NRC Standard Review Plan NUREG-0800, Section 7.8, Revision 5, Diverse Instrumentation and Control Systems, U.S. Nuclear Regulatory Commission, March 2007

/4/ U.S. NRC regulatory guide 1.152, Revision 3, Criteria for use of Computers in Safety Systems of Nuclear Power Plants, U.S. Nuclear Regulatory Commission, July 2011

/5/ U.S. NRC Standard Review Plan NUREG-0800, Branch Technical Position 7-19, Revision 6, Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems, U.S. Nuclear Regulatory Commission, July 2012

/6/ ONR-GDA-AR-11-022, Generic Design Assessment – New Civil Reactor Build, Step 4, Control and Instrumentation Assessment of the EDF and AREVA UK EPR^{TM} Reactor, Revision 0, Office for Nuclear Regulation (An agency of HSE), November 2011

/7/ Licensing of safety critical software for nuclear reactors, Common position of seven European nuclear regulators and authorised technical support organisatons, Revision 2010, BEL V (Belgium), BfS (Germany), CSN (Spain), ISTec (Germany), NII (United Kingdom), SSM (Sweden), STUK (Finland), 2010

/8/ Safety Criteria for Nuclear Power Plants, Revision D, German Federal Ministry for the Environment, Nature Conservation and Nuclear Safety, June 2009

/9/ Stellungnahme des VdTÜV zu den erforderlichen Vorsorgemaßnahmen gegen systematisches Versagen von digitalen leittechnischen Einrichtungen in kerntechnischen Anlagen die Leittechnikfunktionen der Kategorie 1 ausführen (Opinion of the VdTÜV to the necessary preventive measures against systematic failures of digital instrumentation and control systems in nuclear facilities that execute instrumentation and control functions of Category 1), VdTÜV, March 2008

/10/ U.S. NRC NUREG/CR-7007, Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems, U.S. Nuclear Regulatory Commission, February 2010

/11/ Design Optimization and Operational Experiences of Digital Safety I&C in Tianwan NPP / China, Xu, X., Li, Y. and Ding, Y., 2. Symposium Digital Safety I&C, September 2010

/12/ VTT Technical Research Centre of Finland, J. Valkonen, Current Affairs in the Finnish Nuclear Sector, IAEA Technical Working Group on Nuclear Power Plant Control & Instrumentation, May 2007

/13/ Nuclear Engineering International, H.M. Hashemian, Instrumentation and control – Digital I&C – USA's first fully digital station, November 2010

/14/ Duke Energy: License Amendment Request for Reactor Protective System/Engineered Safeguards Protectice System Digital Upgrade, Technical Specification Change Number 2007-09, January 2008

/15/ U.S. NRC NUREG/CR-6303, Method for Performing Diversity and Defence-in-Depth Analyses of Reactor Protection System, U.S. Nuclear Regulatory Commission, December 1994