D. Sommer (GRS)

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

Outline

- Introduction
- International requirements concerning the design of software-based I&C systems in safety systems
- Methods for reliability assessment of I&C systems
- Examples for software-based I&C architectures
- Conclusion

Introduction (1 / 2)

- In Germany, the equipment of I&C systems is often in use since their commissioning in the 1970ies / 1980ies
  - Equipment reaches its end of lifetime
  - Procurement of spare parts is getting more and more difficult
    - ⇒ Extensive replacement of equipment is expected
- A replacement with identical equipment is not always possible or even not wanted
  - Modern software-based equipment is applied
- Software-based equipment shows specific characteristics differing from characteristics of conventional analogue equipment
  - More complex structure
  - Additional properties
  - Changed failure mechanisms and failure behaviour
  - Changed man-machine interface

Introduction (2 / 2)

- Modern I&C equipment:
  potential for new failure mechanisms and an increasing number of failure possibilities in due to use of software or programmable logic (e.g. FPGA)

- Robustness of the modern equipment influenced by
  - Single failures
    - ➢ Possibly higher reliability than analogue equipment due to additional self-testing and failure detection routines
  - Common cause failures (CCF)
    - ➢ Software-CCF may occur especially if latently existing programming errors are triggered by a certain, randomly arising system status or combination of parameters
    - ➢ Possibility of manipulation of software-based equipment by malware has a remarkable contribution to the potential of CCF

- CCF has an important contribution to reliability of the equipment

- Reliability of software-based and programmable equipment has to be investigated and assessed

Outline

- Introduction
- International requirements concerning the design of software-based I&C systems in safety systems
- Methods for reliability assessment of I&C systems
- Examples for software-based I&C architectures
- Conclusion

International requirements concerning the design of software-based I&C systems in safety systems

- Screening of selected international requirements of authorities
  - IAEA
  - NRC
  - HSE
  - STUK
  - European nuclear regulators
  - German Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU)
  - German VdTÜV
- Focus: methods to control CCF in software-based I&C systems

IAEA safety guide NS-G-1.3

- Statements from NS-G-1.3 “Instrumentation and Control Systems Important to Safety in Nuclear Power Plants”
  - … design features such as tolerance of random failure, **tolerance of common cause failure** … should be considered as appropriate
  - **Diversity provides defence against common cause failures** … and increases the chance that safety tasks will be performed when necessary
  - **Types of diversity** that may be considered:
    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** … Specific difficulties may arise in demonstrating the reliability of computer based systems … **Diversity is a way to include conservatism**

IAEA nuclear energy series NP-T-1.5

- Statements from NP-T-1.5 “Protection against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants”, 2009
  - **Despite the measures taken to eliminate faults from I&C designs**, 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.
  - diversity attributes as types of system diversity:

    human diversity, functional diversity and design diversity
  - … 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 Standard Review Plan NUREG-0800

- Statements from NUREG-0800, chapter 7.8 “Diverse instrumentation and control systems”, 2007
  - 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].

U.S. NRC regulatory guide 1.152

- Statements from regulatory guide 1.152 “Criteria for use of Computers in Safety Systems of Nuclear Power Plants”, 2011
  - **With the introduction of digital systems** into plant safety system designs, concerns have emerged about the 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** …
  - **Design techniques** as defence against common-cause failures: functional diversity, design diversity, diversity in operation, and diversity within the four echelons of defence in depth can be applied
  - The NRC’s acceptance of the reliability of computer systems is based on **deterministic criteria for both hardware and software**.
  - Quantitative reliability determination … can provide an added level of confidence in the reliable performance of computer systems.

U.S. NRC Branch Technical Position 7-19

- Statements from BTP 7-19 “Guidance for Evaluation of Diversity and Defence-in-Depth in Digital Computer-Based Instrumentation and Control Systems”, 2012
  - 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: A reactor protection system 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.
    - **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).

HSE (United Kingdom)

- Statements from “Generic Design Assessment – New Civil Reactor Build; Step 4, Control and Instrumentation Assessment of the EDF and AREVA UK EPR^{TM} Reactor”, 2011
  - **Use of various forms of diversity within systems performing protection functions is important** to minimise the risk of simultaneous failure on demand of those systems.
  - The approach included consideration of various forms of diversity
    - 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
    - Diversity of specification

STUK (Finland)

- Statements from presentation
  “Safety and regulation of nuclear power plants – regulatory project management for a new build”, 2012
  - It is impossible to show the correctness of a software based system by testing or analyses, software based systems and equipment are normally too complicated
  - The possibility of a CCF effecting to multiple parallel redundant systems can’t be ruled out with software based systems
    - CCFs are activated by some triggering events and these triggering events are normally so complex that they are very hard to find in testing or verification phases

    ⇒ You must ensure adequate diversity in HW and SW

    ⇒ You must ensure adequate separation between systems and redundant channels

German Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU) (1 / 2)

- Statements from Revision E of the “Safety Criteria for Nuclear Power Plants”, October 2012
  - The nuclear power plant have to be equipped with reliable I&C installations with functions on level of defence 3 (reactor protection system).
  - These I&C installations must designed according to the following principles
    - Redundant design of components, sub-assemblies and sub-systems
    - Physical separation of installations
    - Diversity
    - Automatic failure monitoring
    - Simple software structure
    - Limitation of the functional scope to the necessary safety-related degree
    - Use of fault-preventing, fault-detecting and fault-controlling measures

German Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (2 / 2)

- Statements from Revision E of the “Safety Criteria for Nuclear Power Plants”, October 2012
  - The design of the I&C installations executing I&C functions of Category A has to provide **measures against systematic failures** of the I&C installations in such a way that the systematic failure need not to be considered .
- Statements from Revision D of the “Safety Criteria for Nuclear Power Plants”, Modul 5 “Instrumentation and Control”, April 2009
  - For software-based I&C, dissimilar I&C installations have to be used as a matter of principle
  - For protective actions … a 2-fold or 3-fold dissimilar design of the software-based I&C is used in dependence of the effects of passive or active systematic failures in the I&C installations executing I&C functions of Category A
- At the moment revision of main part and of the detailed modules of the “Safety Criteria for Nuclear Power Plants” is in process

German TÜV and GRS

- Statements from “Opinion of the VdTÜV to the necessary preventive measures against systematic failures of digital I&C systems in nuclear facilities that execute I&C functions of Category A”, 2008
    - The principally precautionary measures that have to be taken … include the **full range of measures for fault avoidance** as well as the **failure controlling measures**
    - For protective actions not being safety oriented for every plant condition a 2-fold or 3-fold dissimilar design of digital I&C should be used
    - Dissimilar means in that case sufficiently different hardware, software, development tools, development teams, manufacturing, and testing and maintenance, so that the systematic failure of mutually dissimilar installations is sufficiently unlikely

Summary – International requirements

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

Outline

- Introduction
- International requirements concerning the design of software-based I&C systems in safety systems
- Methods for reliability assessment of I&C systems
- Examples for software-based I&C architectures
- Conclusion

Reliability assessments for I&C systems

- Before installation of software-based I&C systems in NPPs the following questions are essential
  - Is the planned I&C system sufficiently robust?
  - How large is the probability that a software CCF occurs?

➢ Adequate methods for a reliability assessment of software based I&C systems have to be worked out

- 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 safety I&C systems (e. g. RPS) the probabilities for both failure modes have to be estimated

Software reliability assessment methods (1 / 2)

- Some methods for the assessment of the reliability of software-based equipment have been developed in recent years
  - 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 networks
  - Software reliability growth methods

Software reliability assessment methods (2 / 2)

- For the installation of a software-based I&C system high requirements relating to the accuracy of a method to show the system reliability

- Uncertainties of the assumptions which have to be taken as a basis for an assessment method

- Question
  - Is any of the methods capable of making a sufficiently reliable statement concerning the installation of a software-based I&C system in a NPP?

- Probably this problem will remain unsolved
  - A solution cannot be given by a proof of the reliability of a I&C system

  ⇒ The 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

  ⇒ Diversity may be introduced to provide means to control a CCF

Outline

- Introduction
- International requirements concerning the design of software-based I&C systems in safety systems
- Methods for reliability assessment of I&C systems
- Examples for software-based I&C architectures
- Conclusion

International

- With the modernisation of international NPPs software-based 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

NPPs Darlington-1 and -2, Canada

- Two functionally independent fast shutdown systems (SDS)
  - Control rods (SDS1)
  - Boric acid (SDS2)
- Both triply redundant
- Both shutdown systems use different software-based system platforms
  - Different manufacturer
  - Different chip family and board layout
  - Different development software, compiler, programmer
- SDS1
  - General Automation (GA) model 220 computer (GA-16/220 microprocessor)
  - Programming in FORTRAN and GA-assembler
- SDS2
  - Digital Equipment Corporation (DEC) computer (LSI-11/23 microprocessor)
  - Programming in PASCAL and MACRO-assembler

NPP Sizewell-B, Great Britain

- Two protection systems
  - Primary Protection System (PPS): reactor trip and other safety relevant functions
  - Secondary Protection System (SPS): diverse backup system
- Both four-fold redundant
- PPS
  - Software-based Westinghouse Integrated Protection System (IPS)
  - In each of the four redundancies are two functionally diverse subsystems implemented which work with different activation criteria
- SPS
  - Laddic technology from British Energy
  - Based on hardwired magnetic core logic elements

NPP Tianwan, China

- Software-based safety I&C based on AREVA Teleperm XS
  - Two different physical criteria were defined for each initiating event already in the planning phase
  - In the safety I&C of the reactor protection system two part-strands A and B are realized
  - The computers of both strands did not work synchronous
  - No data transfer between strand A and B
- Additionally a hard-wired backup for the reactor protection system is used

NPPs Oconee-1, -2 and -3, USA (planned)

- Refitting of existing hard-wired safety I&C to software-based safety I&C (based on AREVA Teleperm XS) is planned
- Four-fold redundant reactor protection system (RPS)
  - Four electrically independent and physically separated channels
- Engineered Safety Protective System (ESPS)
  - Two redundant sub-systems, each with three input channels
- To master a software CCF two additional systems which use conventional analogue limit switches will be installed
  - A diverse system for low pressure injection (DLPIAS) in case of a large leak
  - A diverse system for high pressure injection (DHPIAS) in case of a small leak
- Additionally, two already existing diverse systems will be used which are based on another system platform (programmable logic controllers (PLCs) from Schneider)
  - AMSAC (ATWS Mitigation System) to control the ATWS with simultaneous loss of main feedwater
  - DSS (Diverse Scram System) for a diverse excitation of a reactor scram

Outline

- Introduction
- International requirements concerning the design of software-based I&C systems in safety systems
- Methods for reliability assessment of I&C systems
- Examples for software-based I&C architectures
- Conclusion

Conclusion (1 / 2)

- An increasing amount of hardwired I&C equipment of NPPs is already or will be replaced by software-based equipment
  - Potential for new failure mechanisms and an increasing number of failure possibilities
  - Increasing potential for a CCF due to the possibility of a manipulation of the software-based equipment
  - Robustness against a CCF is an important aspect of the reliability of such a system
- Methods for a reliability assessment of software-based I&C system have all one problem
  - The assumptions that have to be taken as a basis for the assessment are inevitably fraught with uncertainties
  - It is questionable whether one of the assessment methods is capable of making a sufficiently reliable statement concerning the reliability of an I&C system
  - Up to today, no final solution is found

Conclusion (2 / 2)

- If a solution cannot be given by a proof of the reliability of a single, homogeneous I&C system, then the adequate design of the I&C system must solve the problem

- Different authorities made requirements concerning the prevention and control of a CCF in safety I&C systems in NPPs
  - The unanimous opinion of these authorities is that diversity provides defence against CCF
  - In the opinion of the German TSOs diversity is an inevitable means to control an occurring CCF
  - Eventually various types of diversity should be used to minimise the risk of a simultaneous failure

- Examples of architectures of software-based I&C systems show different approaches to reach diversity
  - Diversity is not only the theoretic requirement of some authorities and TSOs but furthermore it is also practically feasible