NKS-261
ISBN 978-87-7893-333-1

Guidelines for reliability analysis of digital systems in PSA context - Phase 2 Status Report

Stefan Authén (1)
Johan Gustafsson (2)
Jan-Erik Holmberg (3)

1. Risk Pilot AB, Sweden
2. Royal Institute of Technology, Sweden
3. VTT, Finland

February 2012

Abstract

The OECD/NEA CSNI Working Group on Risk Assessment (WGRisk) has set up a task group called DIGREL to develop a taxonomy of failure modes of digital components for the purposes of probabilistic safety assessment (PSA). A parallel Nordic activity carried out a pre-study where a comparison of Nordic experiences and a literature review were performed. The study showed a wide range of approaches and solutions to the challenges given by digital I&C.

In 2011, a proposal for the failure modes taxonomy was defined. This is based on a set of requirements agreed on the purpose of the taxonomy. The following levels of details can be distinguished from the hardware point of view: (1) the entire system, (2) a division, (3) processing units (and cabinets), (4) modules, i.e. subcomponents of processing units and (5) generic components, i.e. subcomponents of modules. Module level seems to be the most appropriate from the PSA modelling point of view. The software failure modes taxonomy is still an open issue.

An existing simplified PSA model has been complemented with fault tree models for a four-redundant distributed protection system in order to study and demonstrate the effect of design features and modelling approaches. The example shows that even rather simple I&C design leads to rather complex model despite of the fact that many things have been simplified and only a few protection signals are considered. One lesson from the example is that the Alpha factor model should be used to model common cause failures instead of the Beta factor model. Two options were developed to the comparison of different fail-safe principles. The role of detectable and undetectable failure modes with respect to the failed versus spurious actuations can be clearly seen in the results, showing the importance to model these features in PSA.

Key words

Digital I&C system, probabilistic safety assessment, reliability, nuclear power plant safety

NKS-261
ISBN 978-87-7893-333-1

Electronic report, February 2012

NKS Secretariat
P.O. Box 49
DK - 4000 Roskilde, Denmark

Phone +45 4677 4041
www.nks.org
e-mail nks@nks.org

NKS-261 Report

Guidelines for reliability analysis of digital systems in PSA context

Phase 2 Status Report

Stefan Authen[1]
Johan Gustafsson[2]
Jan-Erik Holmberg[3]

[1]Risk Pilot, Parmmätargatan 7, SE-11224 Stockholm, Sweden
[2]Royal Institute of Technology, Stockholm, Sweden
[3]VTT, P.O.Box 1000, FI-02044 VTT, Finland

January 2012

Table of contents

Tables

Figures

Abbreviations

A/D	Analog/digital
ACP	AC power system
AIM	Analog input module
ALOCA	Large loss-of-coolant accident
AOM	Analog output module
APU	Acquistion and processing unit
CCF	Common cause failure
CCW	Component cooling water system
CDF	Core damage frequency
COM	Communication link module
COMPSIS	OECD/NEA Computer-based Systems Important to Safety Project
CPU	Central processing unit
CSNC	Canadian Nuclear Safety Commission
CSNI	Committee on the Safety of Nuclear Installations (OECD/NEA)
DCV	Digital control and voting unit
DFLT	Default value
DIM	Digital input module
DOM	Digital output module
DPS	Depressurisation valve system
ECC	Emergency core cooling system
EDF	Électricité de France
EFW	Emergency feedwater system
ENEL	Ente Nazionale per l'Energia eLettrica, Italy
FMEA	failure mode and effects analysis
GRS	Gesellschaft für Anlagen- und Reaktorsicherheit, Germany
I&C	Instrumentation and control
I/O	Input/output
IAEA	International Atomic Energy Agency
IAEA NE-ICT	IAEA Network of Excellence for Supporting the Use of I&C Technologies for the Safe and Effective Operation of NPPs
ICDE	OECD/NEA International Common-cause Failure Data Exchange Project
IEC	International Electrotechnical Commission
IRSN	Institut de Radioprotection et de Sûreté Nucléaire, French Institute for Radiological Protection and Nuclear Safety
JNES	Japan Nuclear Energy Safety Organization
KAERI	Korea Atomic Energy Research Institute
KTH	Kungliga tekniska högskolan, Royal Insitute of Technology in Stockholm
LMFW	Loss of main feedwater
LOCA	Loss-of-coolant accident
LOOP	Loss-of-offsite power
MCR	Main control room
MFW	Main feedwater system
NEA	OECD Nuclear Energy Agency
NKS	Nordic nuclear safety research
NPIC-HMIT	Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies conference

NPP	Nuclear power plant
NPSAG	Nordic PSA Group
NRC	U.S. Nuclear Regulatory Commission
NRG	Nuclear Research & consultancy Group, the Netherlands
NRI	Nuclear Research Institute Rez plc
OECD	Organisation for Economic Co-operation and Development
PSA	Probabilistic safety assessment
PSAM	Probabilistic Safety Assessment and Management conference
RHR	Residual heat removal system
RPS	Reactor protection system
SAFIR	Finnish Research Programme on Nuclear Power Plant Safety
SCM	Signal conditioning module
SWS	Service water system
TXP	Teleperm XP (now SPPA T2000), product of Siemens AG
TXS	Teleperm XS, product of AREVA
V&V	Verification and validation
VEIKI	Institute for Electric Power Research, Hungary
VTT	Technical Research Centre of Finland
WGRISK	OECD/NEA CSNI Working Group on Risk Assessment

Summary

Digital protection and control systems appear as upgrades in older plants, and are commonplace in new nuclear power plants. To assess the risk of nuclear power plant operation and to determine the risk impact of digital systems, there is a need to quantitatively assess the reliability of the digital systems in a justifiable manner. In 2007, the OECD/NEA CSNI directed the Working Group on Risk Assessment (WGRisk) to set up a task group to coordinate an activity in this field. One of the recommendations was to develop a taxonomy of failure modes of digital components for the purposes of probabilistic safety assessment (PSA), resulting in a follow-up task group called DIGREL. Needs from PSA will guide the work. The taxonomy will be the basis of future modelling and quantification efforts. It will also help define a structure for data collection and to review PSA studies.

A parallel Nordic activity carried out in 2010 a pre-study where a comparison of Nordic experiences and a literature review were performed (report NKS-230). The study showed a wide range of approaches and solutions to the challenges given by digital I&C, and also indicated that no state-of-the-art currently exists. There are some areas where the different PSAs agree, giving a basis for development of a common taxonomy for reliability analysis of the digital I&C. A distinction can be made between the treatment of protection and control systems. There is a general consensus that protection systems shall be included in PSA, while control systems can be treated in a limited manner.

In 2011, a proposal for the failure modes taxonomy was defined. This is based on a set of requirements agreed on the purpose of the taxonomy. With regard to the hardware failure modes taxonomy, the main issue is to define a feasible level of details. The following levels of details can be distinguished from the hardware point of view: (1) the entire system, (2) a division, (3) processing units (and cabinets), (4) modules, i.e. subcomponents of processing units and (5) generic components, i.e. subcomponents of modules. Module level seems to be the most appropriate from the PSA modelling point of view. The software failure modes taxonomy is still an open issue. From PSA point of view a set of principally critical failure events associated with software faults can be defined. It is for the I&C experts to judge which of the failure events, being typically common cause failures (CCF), are reasonable to postulate. More work is still needed to integrate the PSA and I&C expert perspectives.

Another major effort in 2011 was the development of a fictive PSA model to study and demonstrate the effect of I&C design features and modelling approaches. The model is based on a simple example originally included in the PSA tool RiskSpectrum. In this study, I&C fault trees have been developed for the example representing a four-redundant distributed protection system. It has been used to test the effect of CCF modelling, fail-safe principle and voting logic. The example shows that even rather simple I&C design leads to rather complex model despite of the fact that many things have been simplified and only a few protection signals are considered. One lesson from the example is that the Alpha factor model should be used to model CCF:s instead of the Beta factor model. Two options were developed to the comparison of different fail-safe principles. The role of detectable and undetectable failure modes with respect to the failed versus spurious actuations can be clearly seen in the results, showing the importance to model these features in PSA.

Acknowledgements

The work has been financed by NKS (Nordic nuclear safety research), SAFIR2014 (The Finnish Research Programme on Nuclear Power Plant Safety 2011–2014) and the members of the Nordic PSA Group: Forsmark, Oskarshamn Kraftgrupp, Ringhals AB and Swedish Radiation Safety Authority. Part of the input to the report are contributions from the WGRISK/DIGREL task group members. NKS conveys its gratitude to all organizations and persons who by means of financial support or contributions in kind have made the work presented in this report possible.

1 Introduction

Digital protection and control systems appear as upgrades in older plants, and are commonplace in new nuclear power plants. To assess the risk of nuclear power plant operation and to determine the risk impact of digital systems, there is a need to quantitatively assess the reliability of the digital systems in a justifiable manner. Due to many unique attributes of digital systems, a number of modelling and data collection challenges exist, and consensus has not yet been reached.

In 2007, the OECD/NEA CSNI directed the Working Group on Risk Assessment (WGRisk) to set up a task group to coordinate an activity in this field. One of the recommendations was to develop a taxonomy of failure modes of digital components for the purposes of probabilistic safety assessment (PSA) [1]. This resulted in a follow-up task group called DIGREL. An activity focused on development of a common taxonomy of failure modes was seen as an important step towards standardised digital I&C reliability assessment techniques for PSA. Needs from PSA will guide the work, meaning e.g. that I&C system and its failures are studied from their functional significance point of view. The taxonomy will be the basis of future modelling and quantification efforts. It will also help define a structure for data collection and to review PSA studies.

A parallel Nordic activity financed by NKS, SAFIR and Ringhals AB carried out a pre-study where a preliminary comparison of Nordic experiences was performed, and a literature review on main international references was presented [2].[1] The study showed a wide range of approaches and solutions to the challenges given by digital I&C, and also indicates that no state-of-the-art currently exists. The study showed some areas where the different PSA:s agree and gave a basis for development of a common taxonomy for reliability analysis of digital I&C.

DIGREL task will take advantage from ongoing R&D activities, actual PSA applications as well as analyses of operating experience related to digital systems in the OECD/NEA member countries. The scope of the taxonomy includes both protection and control systems of a nuclear power plant, though primary focus is on protection systems. The taxonomy is divided into hardware and software related failure modes, for which purpose example taxonomies have been collected. A representative fictive digital protection system example has been developed to be used as a reference in the application and demonstration of the taxonomy.

This report presents the *interim* results from the WGRISK and Nordic activities. The presented taxonmies and suggested definitions should be considered preliminary proposals and not as a PSA community consensus thoughts. The status of WGRISK/DIGREL activities has been presented also in an NKS seminar in October 2011 [3]. This interim report focuses on the failure modes taxonomy requirements, preliminary proposals for the failure modes taxonomies and the example PSA model developed in 2011.

---

[1] The ongoing stage of the Nordic activity has been financed by NKS, SAFIR and Nordic PSA group (NPSAG): Forsmark, Oskarshamn Kraftgrupp, Ringhals AB and Swedish Radiation Safety Authority.

2 Scope and objectives

The objective with the project is to provide guidelines to analyse and model digital systems in PSA context, using traditional reliability analysis methods (failure mode and effects analysis, fault tree analysis). Based on the pre-study questionnaire and discussions with the end users in Finland, Sweden and within the WGRISK community, the following focus areas have been identified for the activities:

1. Develop a taxonomy of hardware and software failure modes of digital components for common use
2. Develop guidelines regarding level of detail in system analysis and screening of components, failure modes and dependencies
3. Develop approach for modelling of common cause failures (CCF) between components, including software.

The project covers the whole scope of I&C systems important to safety at nuclear power plants (e.g. protection systems and control systems), both hardware and software aspects as well as different life cycle phases of the systems and plant: design/development, testing, commissioning, operation and maintenance.

3 WGRISK task group DIGREL

In 2007, the OECD/NEA CSNI directed the Working Group on Risk Assessment (WGRisk) to set up a task group to coordinate an activity on DIC system risk. The focus of this WGRisk activity was on current experiences with reliability modeling and quantification of these systems in the context of PSAs of NPPs. Two workshops were organised to share and discuss experiences with modeling and quantifying DIC systems. The participants recognized that several difficult technical challenges remain to be solved. One of the recommendations was to develop a taxonomy of hardware and software failure modes of digital components for the purposes of PSA [1].

As a continuation, a new task proposal was made to WGRISK, which was accepted by WGRISK and CSNI in Spring 2010. The objectives with the new task called DIGREL is

- To develop technically sound and feasible failure modes taxonomy (or taxonomies if needed to address variations in modeling methods or data availability) for reliability assessment of digital I&C systems for PSA
- To provide best practice guidelines on the use of taxonomy in modelling, data collection and quantification of digital I&C reliability.

The activity focuses on failure modes taxonomy and its application to modelling, data collection and impacts on quantification. The following items will be considered (but not limited to):

- Protection systems and control systems,
- Hardware and software,
- Development, operation and maintenance,
- Failure detection and recovery means.

There are many different digital I&C failure mode taxonomies. An activity focused on development of a common taxonomy of failure modes was seen as an important first step towards standardised digital I&C reliability assessment techniques for PSA. Needs from PSA guides the work, meaning e.g. that the (digital) system and its failures are studied from their functional significance point of view. This is considered a meaningful way to approach the problem.

The taxonomy will be the basis of future modelling and quantification efforts. It will also help define a structure for data collection. The results of the activity can be directly used in the review of PSA studies.

The activity takes advantage from recent and ongoing R&D activities carried out in the OECD/NEA member countries in this field. More PSA applications including digital I&C systems have been or are being prepared. Efforts to analyse operating experience from digital systems are in progress. This knowledge will be merged by inviting experts in the field to contribute to the activity.

A series of working meetings have been and will be organised in order to develop best practice guidelines on the topic, to share information and to plan future activities. For instance, in 2011, two workshops were organised. A public seminar was organised in connection to the second workshop in October 2011 [3].

The aim is to prepare the draft guidelines by the end of 2012. A final draft will be prepared for WGRISK in the beginning of 2013. After that the guidelines shall go through the acceptance steps of WGRISK, CSNI Programme Review Group and the CSNI itself.

The following organisations form presently (December 2011) the task group, being responsible for planning and organisation of work meetings and preparation of the best practice guidelines: VTT, Finland (leader); Risk Pilot, Sweden; IRSN, France; EDF, France; AREVA, France; GRS, Germany; KAERI, Korea; NRC, USA; Ohio State University, USA; NRI, Czech; JNES, Japan; VEIKI, Hungary; ENEL, Italy; NRG, the Netherlands; RELKO, Slovakia and CSNC, Canada.

The task has relation at least to the following projects:

- OECD/NEA Computer-based Systems Important to Safety (COMPSIS) Project (finished December 2011)
- OECD/NEA International Common-cause Failure Data Exchange (ICDE) Project
- IAEA NE-ICT activities (Network of Excellence for Supporting the Use of I&C Technologies for the Safe and Effective Operation of NPPs)
- Nordic NKS project on "Development of guidelines for reliability analysis of digital systems in PSA context".

4 Reliability analysis of digital I&C systems in the PSA context

4.1 Failure modes taxonomy

Failure modes taxonomy is a framework of describing, classifying and naming failure modes associated with a system. Main uses of failure modes taxonomies are in the performance of reliability analyses and in the collection of operating experience (failure data) of technological systems. In the DIGREL, the taxonomy is developed jointly by PSA and I&C experts which have slightly different views and needs on defining the failure modes [4].

The fault tree modelling and systems analysis in PSA is a combination of top down and bottom up approaches. Fault tree modelling is a top down method starting from the top level failure modes defined for the system. In the system level, the two main failure modes are 1) failed function and 2) spurious function. For the failed function more descriptive definitions may be given such as “no function”, “not sufficient output”, “no state transition”, “broken barrier”, “loss of integrity”, etc, depending on the nature of the system. In the fault tree analysis, the system level failure modes are broken down further into sub-system and component level failure modes. The system level failure modes appear thus as fault tree gates in the PSA model, while component level failure modes appear as basic events.

Basically, same failure modes taxonomy can be applied for components as at the system level (failed function, spurious function), but the definitions are usually more characterising, e.g., “sensor freeze of value”, and are closer related to the failure mechanisms or unavailability causes. The component level failure modes are applied in the performance of the FMEA (failure modes and effects analysis) which is a bottom-up analysis approach. The analysis follows the list of components of the system and for each component failure modes, failure causes (mechanisms) and associated effects are identified. FMEA precedes the fault tree modelling but it needs the definitions of the system functions and associated failure modes.

From the PSA point of view, the definitions for the failure modes and the related level of details in the fault tree modelling can be kept in a high level as long as relevant dependencies are captured and reliability data can be found.

4.2 Types of I&C systems

A clear distinction can be made between the treatment of protection systems (reactor trip and ESFAS (engineered safety features actuation system) functions and control systems controlling e.g. the turbine plant. Firstly, there is a general consensus that protection systems shall be included in PSA, while control systems can be treated in a limited manner. Secondly, the system architecture and the mode of operation of protection systems versus control systems are different, which creates different basis for the reliability analysis and modelling.

Protection systems (Figure 1) are composed of redundant divisions (also called subsystems, trains, channels or redundancies) running in parallel microprocessors and they actuate functions on demand (e.g. when process parameter limits are exceeded).

Control systems are versatile having both on demand and continuous functions and they do not necessarily have a redundant structure. Different roles of the protection and control systems are also reflected in the safety classification, meaning different safety and reliability requirements.

The differences between different I&C platforms and softwares may be significant, not only the physical design but also the functional, e.g. fault tolerant features and voting logic. Figure 1 represents an example of a typical digital I&C protection system.

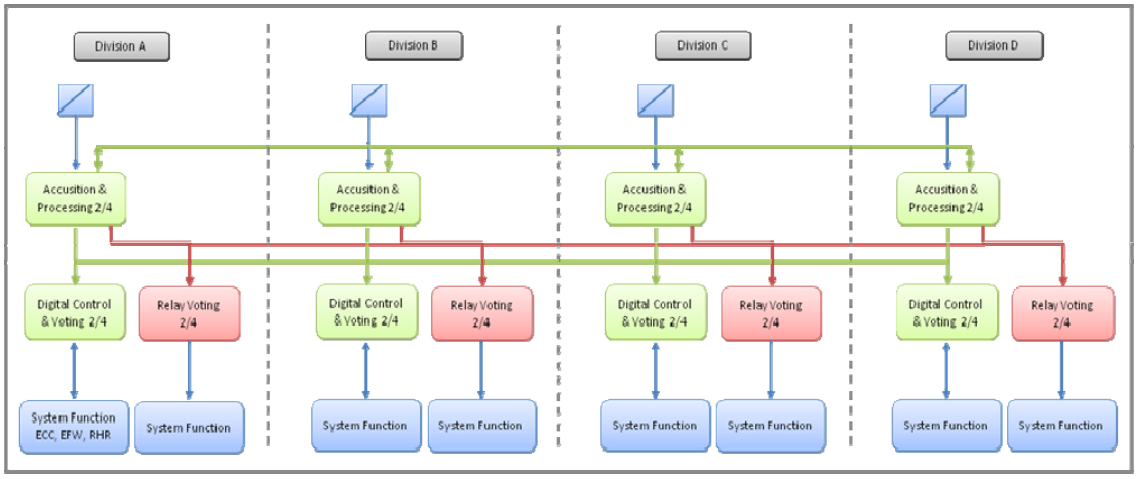

Figure 1. Example of a digital I&C protection system.

DIGREL will primarily consider protection systems since it considered more important for PSA and it is considered conceivable target for the activity. The aim is, however, to discuss even failure modes taxonomy for control systems, once the taxonomy has been defined for protection systems. This report only considers protection systems.

4.3 Levels of details

4.3.1 Hardware

With regard to the analysis and modelling of protection systems, the following levels of details can be distinguished from the hardware point of view:

(1) the entire system

(2) a division

(3) processing units (and cabinets)

(4) modules, i.e. subcomponents of processing units

(5) generic components, i.e. subcomponents of modules.

A safety system is the entity performing a safety function or part of it. In PSA context, reactor protection system is never treated as a black box, but the analysis is always broken down into the protection function and at least the divisional level.

The reactor protection system consists of redundant divisions that provide inputs to voting modules that determine if an actuation signal should be generated. The divisions may be of the same or different architectures but in general all perform the same

functions. Each division comprises an entity from power supply and physical separation point of view, although some cross-connections of power supply between divisions may be applied for certain components. From the PSA modelling point of view, a usual simplification is to assume a loss of complete division in case of a hazard affecting the division. Loss of AC or DC power supply are also division wide functional failures to be considered in PSA.

Each division consists of one or more processing units and data buses between them. Processing units may be dedicated to data acquisition, processing, voting and actuator control. In Figure 1, each division has two processing units: an acquisition & processing unit (APU) and a digital control & voting unit (DCV). Processing units may be doubled (within each division) to increase the availability of the system.

Processing units are installed in cabinets, each of which has a specific power supply route and condition monitoring. Cabinet level is the most detailed level from the power supply and room dependency point of view.

A processing unit is a computerised system designed to receive input signals, perform computing and send output. It consists of modules such as input module, processing module, communication module and output module. Modules may be further broken down into generic components such as an analog/digital converter, a multiplexer, a microprocessor and its associated components, a demultiplexer, an A/D converter and channels of an I/O module (see Figure 2), e.g., depending on the available failure data. Modules and channels are the most detailed level from the hardware functional dependency point of view. Also the software components can be associated with the modules.

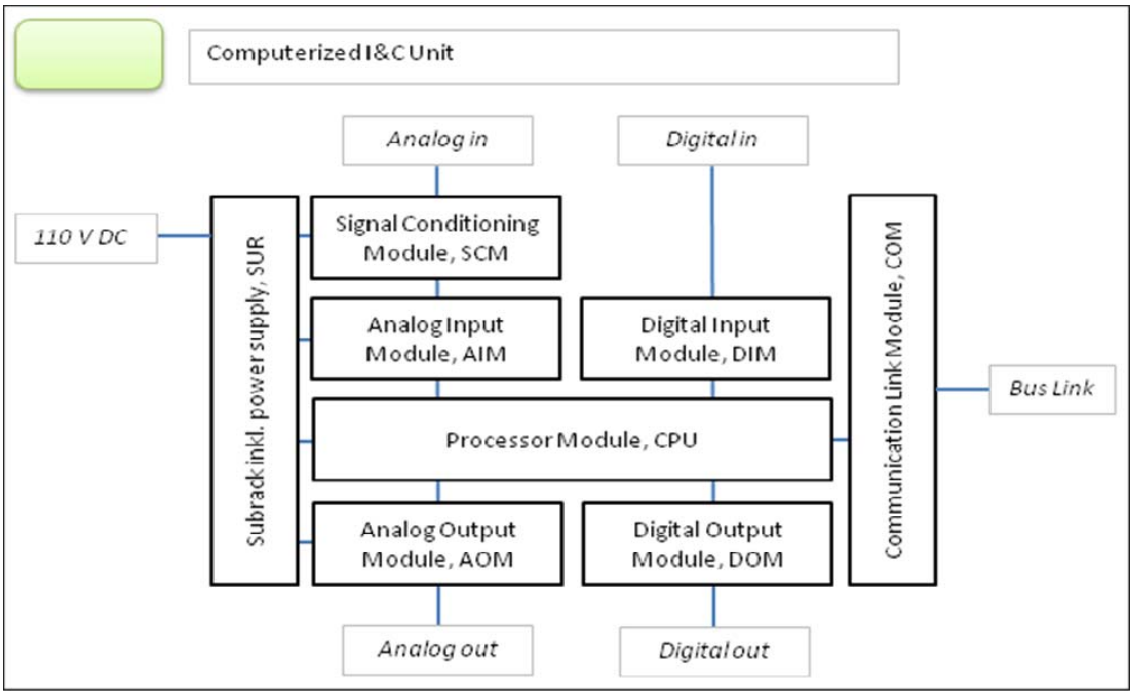

Figure 2. Example of modules included in a computerized I&C unit.

4.3.2 Software

In the case of safety critical programmable systems in nuclear power plants (so called cat. A systems), at least the following kind of software components can be identified:

- In processing units
    - Operating system
    - Application specific software
    - Elementary functions
- In communication units
    - Communication firmware
    - Network specific communication patterns.

The same levels of detail is in general applicable for the software failure modes as for the hardware failure modes. This is also desirable from the PSA modelling point of view.

4.3.3 State-of the art in PSA

In current PSA:s, a “super-component” modelling approach is mostly followed. A super-component contains multiple modules that perform input, output, processing, subrack etc. FMEA:s (failure modes and effects analysis) can sometimes be more detailed, especially if they have been prepared by the vendor who needs to perform detailed reliability analyses on a subcomponent level. Normally it is difficult for the utilities to perform detailed FMEA due to lack of detailed specifications and I&C expert competence regarding specific platforms [2].

As basic events CPU failures, application failures and CCF:s between identical components are generally modelled.

However, it is not clear which failure modes or system parts CCF:s should be postulated for. The primary goal is to model dependencies, which will be limited by the chosen level of detail. The possibilities to reflect important system behaviour such as treatment of faulty signals and complex voting logic will also depend on the level of detail in the model. Different applications of a PSA will put different requirements on the needed level of detail, and the taxonomy to be developed must consider this while ensuring that vital dependencies and system behaviour are covered.

In industrial PSA:s, FMEA and fault tree modelling are the main approaches to evaluate the reliability of digital I&C. It should be noted that the number of PSA:s worldwide including reliability models of digital I&C systems, e.g., of a digital reactor protection system (RPS), are very few. More dynamic approaches are still in trial stage and can be difficult to apply in full scale PSA-models.

4.4 Hardware failure modes taxonomy

The development of a hardware taxonomy is dependent on the overall requirements and prerequisites since they will set boundary conditions, e.g., for the needed level of detail of hardware components and for the structure of the failure modes. A different set of requirements may result in a different taxonomy.

4.4.1 Overall requirements

The following overall requirements for the hardware taxonomy have been agreed upon within the WGRISK task group DIGREL, and will also be applied here:

- Shall support PSA practice, i.e. appropriate level for PSA, fulfill PSA requirements/conditions
- Shall cover undetected and detected failures
- Shall capture all critical dependencies and design features
- Shall be appropriate for safety related systems
- Shall support definition of failure modes, not mechanisms
- Shall be based on function view, not component
- Shall support modeling of CCF:s at necessary level.

The impact of these on the choice of level of detail and failure modes for the hardware taxonomy is discussed below.

4.4.2 Level of detail

To find the proper level of detail the overall requirements are broken down into detailed requirements that are interpreted with regard to the impact on choice of level of details.

Shall support PSA practice

The taxonomy shall be aimed at support of PSA practice rather than being a support for the vendors and I&C experts. To support PSA practice the taxonomy needs to meet at least the following conditions:

- Be a feasible analysis for PSA experts to perform.
  The PSA:s will be performed by PSA experts where I&C experts will provide input when needed. The level of detail in the taxonomy should hence correspond to a system knowledge that is realistic to require of PSA experts, without at the same time requiring them to be I&C experts. Modelling on the generic component level requires I&C expert knowledge, why the proper level of detail is the module level or higher.
- Possible to implement into existing tools (fault tree/event tree).
  PSA:s are today performed by use of tools based on fault tree and event tree techniques. The taxonomy must hence be on a level such that it can be incorporated in a PSA by use of the same tools. This does, however, not exclude the use of more dynamic tools in order to produce input to the fault tree/event tree analysis. This implies that the generic component level or higher should be applied, but that complex behaviours and relations, e.g., hardware/software interactions and time dependencies, should be analysed outside and prior to the PSA modelling. It also means that properties related to specific tools other than fault tree/event tree tools does not need to be considered in the taxonomy.
- Possible to review by a PSA-expert.
  Mainly the same reasons as for being a feasible analysis for PSA-experts to perform, but from the perspective of verifying that the model is a correct and sufficient description of the design. The level of detail should also be in such a level that the review can be performed with reasonable efforts.

- Allows living PSA, e.g. possible to maintain and update with reasonable resources.
  The PSA:s are in general required to be continuosly maintained and uppdated with regard to plant changes and new data in order to describe the plant as built, and also in order to keep up to date with various findings and progress in PSA methodology. To make this process feasible the amount of time and resources required needs to be on an acceptable level, which is directly related to the details needed in terms of inputs and modelling. This requires the taxonomy to be at the module level or higher.

- Available and maintainable failure data, i.e., allows collection and evaluation of operational events.
  Presently failure data are in general only available from the vendors, and then based on theoretical calculations. It is therefore desirable to facilitate collection and evaluation of operational data with the objective to produce generic and platform specific failure data. This requires that the level of detail corresponds with the level at wich maintenance of the equipment is performed, which in general is the module level.

- Support PSA applications.
  Besides safety demonstration, PSA is used for a number of different applications such as risk follow up, evaluation of design changes and power uprates, evaluation of techniqual specifications, maintenance policies, etc. This puts requirements on the general level of detail within the PSA model, and hence also on the digital I&C. For the larger part of the applications the module level is sufficient and in some cases, e.g. evaluation of allowed outage times, also necessary.

Cover undetected and detected failures

The larger part of the failures within a digital I&C RPS will be detected by monitoring features such as self-surveillance, dynamic self-test, open circuit monitoring, cross channel comparison etc., while a small part only will be detected by periodic tests or actual need of the equipment. It has been common in PSA:s of digital I&C only to considered the latter types of failures motivated by that the contribution to unavailability from detected failures is insignificant. It has however been shown that the detected failures will in some cases have a significant contribution, [4], why these failure modes need to be included in the taxonomy. This will have quite a large impact on the requirements on the taxonomy:

- Fault detection, treatment of faulty signals and complex voting logic needs to be considered in the model.
  The effect of detected failures will depend on applied fail safe criteria and voting logic for each of the RPS functions, so in order to correctly model the impact of detected failures it is needed to also model the means for treatment of faulty signals. Different RPS functions will possibly not only engage different sets of processing units, but also engage specific sets of I&C modules within each processing unit. Since the coverage of failure detection depends on the type of I&C module addressed, the taxonomy needs to be on the module level.

- Spurious activation of safety functions due to detected failure of components needs to be covered.
  Detected failures may due to applied fail safe principles significantly contribute to the occurrence of spurious activation of RPS functions.

Capture critical dependencies/features

Critical dependencies and features of a digital I&C RPS needs to be covered in the PSA and will hence affect the format of the taxonomy. The following main dependencies and features have been identified for the digital I&C hardware:

- Functional dependencies including voltage and signaling dependencies.
- Area dependencies, i.e. fire, flooding and missiles.
- Treatment of faulty equipment/signals. Fault detection, default values, output control.
- Voting logic, e.g. Ignore, Trip, No trip, 2:nd max, 2:nd min, etc.
- Coverage of failure detection.
- Tests, corrective and preventive maintenance.
- Effects due to hardware/software interaction.
- Interaction with software taxonomy.

Regarding functional dependencies and room dependencies the processing unit level is sufficient since the modules of a processing unit in general is installed in the same cabinet. However to cover the issues related to the treatment of faulty equipment/signals, voting logic and HW/SW interaction, the taxonomy in general needs to be on the module level. Also, tests and maintenance are most often defined on the module level and will differ between the modules.

Coverage of the failure detection is most conviniently defined on the module level, but the calculation requires input from the lower level of the generic components. The calculation of coverage is normally performed by the vendor as a part of the system reliability data, why the taxonomy can be defined for a higher level.

The module level is judged to be sufficient in order to capture vital dependencies in our case, though this depends to some part on the specific digital I&C design and it should be verified for each case.

Appropriate for the safety related systems

The level of detail of the taxonomy shall be appropriate with regard to state of the art modelling of safety related systems within a PSA. This means that the level of detail should be high and correspond with the general level of a detailed PSA, e.g., modelling of process equipment, electrical equipment and dependencies. Simplifications as for operational systems will in general not be acceptable, unless for use in a preliminary design or equivalent PSA.

That the taxonomy shall be developed for safety related systems also means that issues specific for digital I&C control functions will not be considered in the taxonomy.

This requirement implies that the taxonomy should at least be defined at the processing unit level, but not higher than the module level. The generic component level is in comparison in much higher detail than general PSA state of the art, and will require unreasonable resources and significantly increase model size.

Support modelling of CCF

CCF:s can be modeled at any level, where only the degree of conservatism will differ. The grouping will be decided by the safety functions and the controlled equipment, where the allocation of modules will differ between safety functions and also for control of components within safety systems.

Further on, the level of detail should be such that CCF parameters are available or possible to estimate, e.g., by the use of [5].

With regard to state of the art the module level will be most appropriate, since the effect of module allocation, and failure of these, for the different RPS functions then will propagate in the fault tree model. It is also a level suitable for estimation of parameters and for collection of operational data.

In some designs the test interval of an individual I/O channel will differ from the test interval of a complete I/O module, and in these cases it should be considered to model CCF at I/O channel level.

A draw back of choosing the module level is that CCF:s may exist on the generic component level causing failure of the same cause for different types of modules. It is however not required by a state of the art PSA to consider intra component or intra system CCF:s.

Conclusions on taxonomy level of detail

The most suitable level of detail is the module level which concur with the level of detail of general PSA state of the art. The module level will make it feasible to perform, maintain and review a PSA of digital I&C with reasonable resources while capturing critical dependencies. It will also be possible to capture fault tolerant features of the digital system and the impact on the reliability of safety functions.

Though the module level will not fulfill all requirements. Failure data and coverage of failure detection is currently calculated at a higher level of detail, i.e. the generic Component level, and needs to be supplied by the vendor. But in a longer perspective it is desirable that these data is derived from operational data, where it is not reasonable to expect that data is collected on a higher level of detail than the module level. It also needs to be verified for each digital RPS design that all critical dependencies are captured at the module level, e.g. failures due to common causes.

The next lower level of detail, the processing unit level, fulfills many but not all of the requirements of a state of the art PSA, why this level may be suitable for a preliminary design PSA while not for an as-built PSA. For this purpose, the taxonomy developed at the module level can be aggregated to and used at the processing unit level.

The generic component level is usually where the vendor performs reliability analyses in order for system licensing or as part of deliverables to customers. Implementing the generic component level into a PSA is not seen as reasonable as this will require large amounts of resources, both in short and long term, and significantly increase model size without significant quality increase in the PSA results. This level of detail may be considered for the purpose of using the PSA for specific applications.

4.4.3 Failure modes

The hardware taxonomy failure modes can either be based on a function view or a component view. The function view considers component failures with regard to their impact on the function that the component supports, e.g. “loss of function to actuate”,

while the component view is more descriptive and considers component failures with regard to the manifestation of the failure within the component, e.g. “freeze of value” or “setpoint corrupted”. Descriptive failure modes is of use in a more detailed level when deciding the consequence of the failure at a higher level.

From the PSA point of view it is desirable to group failure modes with regard to their functional consequence to as high extent as possible, in order to simplify the fault tree analysis. See also the pres-study report [2] and the DIGREL seminar 2011 [3] for examples of failure modes used in practice.

When defining failure modes, a certain entity of a system is taken under consideration. In digital systems, the entity may be generally called as a functional unit consisting of hardware or software, or both, capable of accomplishing a specified purpose [6]. A functional unit can be anything from a computer to a generic component of a module. The definition for the failure mechanism, failure mode, failure effect and detection depend thus on which functional unit that is considered and what its role is from the system point of view.

There are two perspectives when structuring a system into functional units:

1. hierarchical structure in which larger units are composed of sub-units, sub-units of sub-sub-units etc.
2. network structure, in which the units are in an signal exchange relation (input-output relation).

From the hierarchical structure point of view, the failure effects of the lower level components constitute the failure causes of failure modes of the upper level components. Hierarchical approach of defining failure modes and effects is practical for generic components and modules. From the network structure point of view, the input-output relation between the functional units determines how the failures are propagated in the system. The failures in the output from the sending unit constitute the failure modes of the receiving unit (e.g. “no input” or “spurious input”). Network approach of defining failure modes and effects is applicable for analysing interactions between the processing units.

The input-output relation between functional units offers a simple, generic way of defining failure modes for digital units with Boolean output (1 or 0), which is typical for protection functions. “1” means an actuation signal or an condition for it, and “0” is the opposite state. The two basic failure modes are:

- 0 instead of 1, i.e., no actuation signal when demanded.
- 1 instead of 0, i.e, spurious actuation signal.

If applicable other failure modes, such as too late output or erratic output, may be considered, but in practical PSA applications it may be difficult to model these more complicated and dynamic events.

In case of multifunctional units, it may be necessary to further distinguish between the case when the unit is totally “crashed” and does not send any signal and the case when the unit fails to send a specific actuation signal.

The network perspective also raises the important question of what is actually meant by failure detection. The failure may be detected by the unit itself who sends (or does not send) the signal or it is detected by the unit receiving (or not receiving) the signal. In the FMEA, it is important that the definition of the failure mode includes the failure

detection of the unit itself, while what happens to the next unit is not a feature of the failure mode but a failure effect, i.e., failure effect describes what happens on the next level for the safety function, i.e., in the functional unit receiving the signal (or not receiving a signal).

The following categories of failure detection are possible:

- Demand (no periodic test detects the failure)
- Periodic test
- Monitoring
    - Self-monitoring (online monitoring of the module itself)
    - Monitoring by another module

Category of failure detection determines the choice of the component reliability model (constant unavailability, monitored, repairable, standby component).

Failure detection is a most relevant attribute from the failure effect point of view, since the digital I&C system will apply fail-safe principles when a failure is detected. Whether a failure is detected or not will hence decide the effect of the failure, and subsequently set the failure mode at the next higher level in the system hierarcy or in the network structure. The following effects may be considered:

- Loss of function (loss of protective action, loss of communication)
- Spurious function
- Effect on voting logic/fail safe default value depending on the design.

Failure modes of sensors and transmitters is considered to be out of the scope of the DIGREL task. These components do not bring additional considerations from the digital I&C point of view. Focus of DIGREL is thus in the data acquisition, processing and voting units and communication between them. It should, however, be noted that the failure detection within the RPS also covers failures in transmitters.

4.5 Software failure modes taxonomy

The overall requirements for the hardware taxonomy presented in the previous chapter are applicable to software failure modes, as well. The way of defining of software failure modes is, however, somewhat different due to the nature software. Software cannot be decomposed into components in so straightforward manner as it can be done for the hardware part. Secondly software failures are in general mainly caused by systematic errors, and not on random errors, which emphasises the need to consider CCF. In addition, the failure effect of software fault may be difficult assess.

In the DIGREL task, the software failure modes taxonomy is still an open issue, and the work will be continued in 2012. The taxonomy has been approached from two perspectives: PSA and software engineering. The main attention is put on the possible faults in the operating system and application software running in the processing units.

The PSA perspective *functional* failure modes may be considered in similar manner as for hardware, i.e.:

- loss of all functions (no output from the processing unit)
- loss of one function (no actuation signal)
- spurious actuation signal.

Other more complex functional failures may be naturally imagined, but then the analysis goes beyond what is reasonable in PSA. Simultaneous actuation of more than one spurious signal is, for instance, considered an event which does not need to be assumed.

The next relevant issue is to analyse CCF, i.e., between which processing units the functional failure can appear at the same time. The following CCF cases could be postulated:

- redundant units within the division
- redundant units in redundant divisions
- all units with same platform
- units with different platform.

Based on the list of possible functional failures and the CCF options, we get a set of principally possible basic events associated with software faults, either in the operating system or in the application software of the processing units. Which of these "software basic events" are reasonable to assume and which of them are fully unreasonable to postulate is a judgement task for the software system expert.

The present praxis in PSA:s is to consider a very small number of software related events, typically a single CCF causing loss of all functions in all redundant units in redundant divisions or all units with same platform. The aim of DIGREL is to go beyond the state-of-the-art. In order to do that the software engineering expertise is taken into account.

The software engineering perspective follows the design of the software and its development process including V&V activities. Based on this knowledge, some faults may be judged to be impossible while others may not be ruled out. As e.g. discussed in the DIGREL seminar 2011 [3], the highest safety class (Cat. A) software systems have strict design principles and they go through a rigirous V&V process, which gives well-justified arguments to rule out a number of software fault types, e.g., software is designed to behave cyclically time-based and not event-based, and the operating system is designed not to be affected by the plant conditions.

Figure 3 presents a preliminary taxonomy for software faults. The main concern is in the specification faults of the application software, but it is hard to proof that the operating system is faultless. The challenge for DIGREL is to see to how the knowledge about the possibility of different software *faults* (as e.g. listed in Figure 3) can be used to decide which kind of software *failure events* should be modelled in PSA.

	Specification Faults	Software Faults	Faults in SW / HW Interactions
Application	•Incorrectness •Incompleteness •Out-of-date •Ambiguity	•Forgotten requirements •Inadequate algorithms or design •Programming faults •Incorrect SW version & configuration management •Translation tools faults •Non-compliance to claimed structural properties	•Insufficient system HW resources •Inconsistent system HW configuration
I&C Platform	•Noise •Over-specification •Excessive ambition		•Inadequate handling of HW failures •Insufficient detection of HW faults

Figure 3. Preliminary taxonomy for software faults [3]. Application and I&C platform are subject to the same types of faults, but possibly with different interpretations.

4.6 Fail-safe principle

The digital I&C provides means to detect and mark faulty signals, e.g. self-surveillance, dynamic selftest, open circuit monitoring, cross channel comparison etc. Fault processing is implemented in the design of the hardware circuits and the software logic, and it is defined on a case-by-case basis how the logic shall react if invalid input signals are present, and how output signals shall be set in case of faulty logic signals:

- Input signals marked as faulty will be replaced by a default value of 0 or 1, or be ignored.
- In case of a fault in the system, e.g. loss of controlling processor, an output will either trip a function or remain in normal status. [5]

The fail-safe design sets the following general conditions for the fault tree analysis of the RPS functions (see Table 1). Failure modes and data need to thus distinguish between detected failures and undetected failures, i.e., latent failures. Considerations need to be done case by case since a specific measurement or input can have different default values in different RPS functions.

Table 1. Treatment of fail-safe design in different component failure modes.

Component failure mode	**Function fail-safe design**	**Function failure mode**
Latent	Default value 1	Failure to trip
Latent	Default value 0	Failure to trip
Detected	Default value 1	Spurious trip
Detected	Default value 0	Failure to trip

A second issue to be accounted for in the modelling is the effect of failure to the majority voting and different types of degraded voting logic in combination with a detected invalid measurement (called also intelligent validation). Table 2 shows some treatment principles which may be applied. In reality, different principles can be applied depending on the function. If these principles are implemented in the PSA model, the model easily becomes very complex, since several variants of logic tree structures need to be developed. An issue for further research is to find a feasible level of modelling the realistic behaviour of intelligent validation.

Table 2. Examples of different principles to treat invalid input signal, when the voting logic 2-o-o-4.

Validation principle	**New logic after 1. fault**	**New logic after 2. fault**
Invalid input is always set to tripped	1-o-o-3	tripped
Invalid input is always ignored	2-o-o-3	2-o-o-2
First invalid input is tripped, second is ignored	1-o-o-3	1-o-o-2

4.7 Failure data

Failure data for hardware failures is developed by the manufacturer or this is at least expected to be the case. Generic failure data and operational experience is very scarce, why existing failure rates are derived from theoretically calculations.

The software reliability estimates are engineering judgments based on some common understanding rather than a proper reference. A general opinion is that it is sufficient (and even meaningful) to only model software CCF and omit “single” software failures. It is an open issue in which way software failure modes should be defined and in which level of details. This issue will be further discussed in the DIGREL task.

5 Example

5.1 Overview of the example digital I&C PSA model

An example digital I&C PSA model was developed as a Master’s Thesis at Royal Insitute of Technology (KTH). Details of the model are presented in [8]. The basis of the example PSA-model is taken from an example prepared by Scandpower Lloyd’s Register (originally Relcon AB). The model is a very simple example of a PSA-model for a nuclear power plant made for illustration purposes to demonstrate basic elements of the risk and reliability analysis software Risk Spectrum (trademark of Scandpower Lloyd’s Register) [9].

The example PSA-model represents a boiling water reactor (BWR), which has two-redundant safety systems. The example model includes system fault trees for the following systems:

- ACP – AC power system
- CCW – Component cooling water system
- ECC – Emergency core cooling system

- EFW – Emergency feedwater system
- DPS – Depressurisation valve system
- RHR – Residual heat removal system
- SWS – Service water system
- MFW – Main feedwater system.

The example model includes only a few main components these system as illustrated in the flow diagram and electric system line diagram (Figure 4 and Figure 5). It should be noted that the locations of the objects in the diagram do not reflect any actual NPP design but only represent the reliability structure of the systems included in the example PSA model (i.e. the diagram could be read as a reliability block diagram).

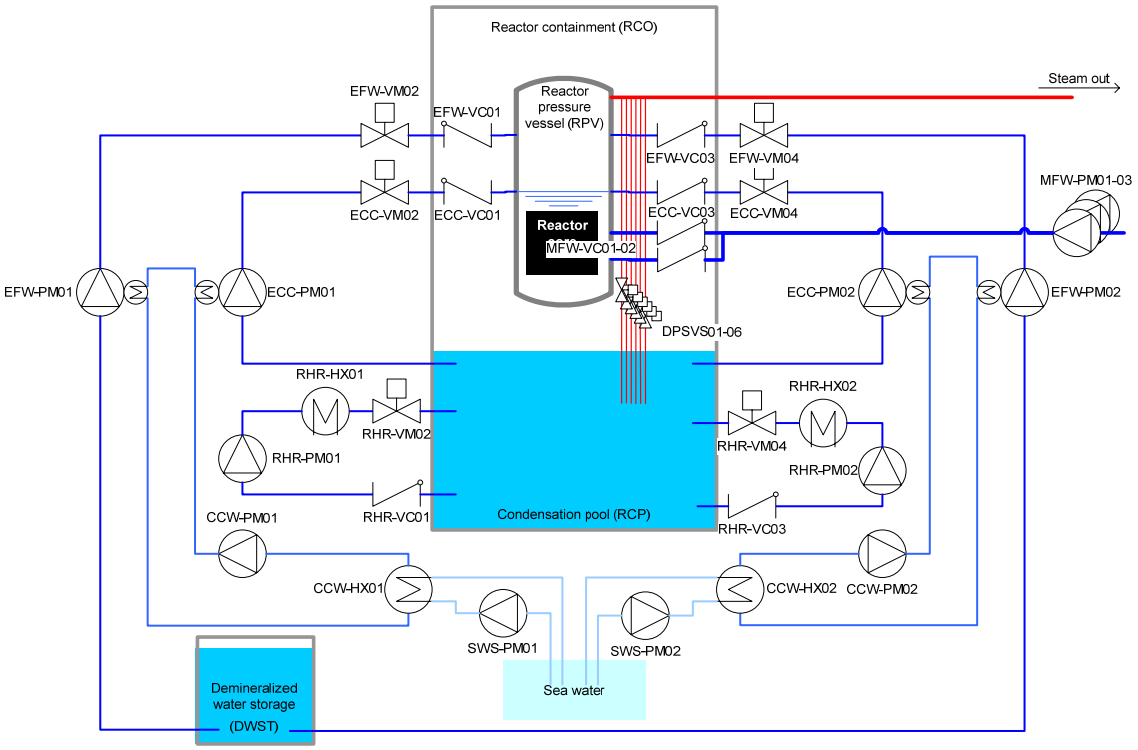

Figure 4. Example NPP safety system flow diagram.

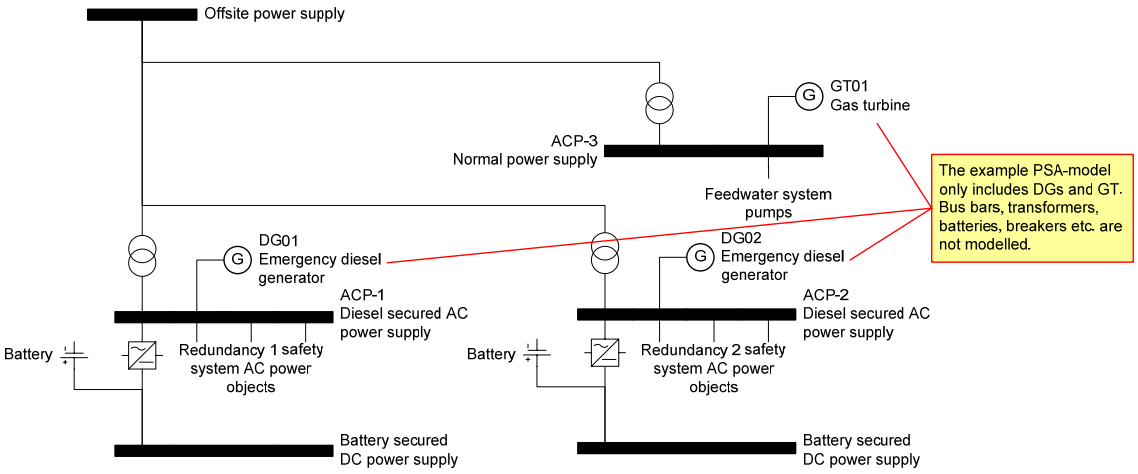

Figure 5. Example NPP electric system line diagram.

There are four initiating events considered in the example PSA-model:

- Large loss-of-coolant accident (ALOCA)
- Loss of main feedwater (LMFW)
- Transient
- Loss-of-offsite power (LOOP)

The initiating events set different success criteria for the safety systems. Success criteria of the systems providing coolant to the reactor are given in Table 1. These are the front-line safety systems together with the residual heat removal system (RHR). Coolant must be provided to reactor either by the main feedwater system, emergency feedwater system or emergency core cooling system. Emergency core cooling system requires a depressurisation of the primary circuit in case of LOOP or transient.

Table 3. Success criteria of the front line safety systems.

Initiating event	**Main feedwater system (MFW)**	**Emergency feedwater system (EFW)**	**Depressurisation valves (DPS)**	**Emergency core cooling (ECC)**	**Residual heat removal (RHR)**
ALOCA	Not credited	Not credited	Not needed	1-o-o-2 trains	1-o-o-2 trains
LMFW	Not credited	1-o-o-2 trains	5-o-o-6 valves	1-o-o-2 trains	1-o-o-2 trains
LOOP	2-o-o-3 trains	1-o-o-2 trains	5-o-o-6 valves	1-o-o-2 trains	1-o-o-2 trains
Transient	2-o-o-3 trains	1-o-o-2 trains	5-o-o-6 valves	1-o-o-2 trains	1-o-o-2 trains

The successful operation of the front-line safety systems requires that support systems functions as well. Respective EFW or ECC train is cooled by the component cooling water system (CCW) train, which is cooled by the corresponding service water system (SWS) train.

All pumps and motor-operated valves require power supply. Power supply is provided by off-site electric grid (which is lost by definition in LOOP) or by diesel generators. Main feedwater system pumps cannot be supplied by diesel generators but there is a gas turbine which may be started if the off-site power is lost. Only diesel generator and gas turbine failures have been modelled.

5.2 Automation functions

The original example PSA-model described above did not include any automation functions or associated I&C system fault trees. For the purpose of the Master's Thesis a number of automation functions are assumed for the operation of the front-line and support systems. In general terms, the assumed automation functions resemble some typical protection functions of a boiling water reactor. It should be noted that this example includes only very few protection functions compared to real NPPs. The purpose has been just to define so many protection functions, which is necessary to study the importance of redundancy, diversity and different fail-safe principles. In most cases, the actuation is based on 2-out-of-4 measurement sensor values exceeding a critical limit value.

Table 4. Automation functions of the example PSA.

Protection function	**Process consequence**
Isolation of the emergency pump room 1 resp. 2	Stop of corresponding EFW and ECC pumps
Containment isolation	Start EFW and ECC
Containment isolation due to extremely low level in RPV	As above + open EFW regulation valves + subcondition for primary circuit depressurisation
Containment isolation due to high pressure in containment	As Containment isolation + subcondition for primary circuit depressurisation
Feedwater system isolation	Stop MFW and start EFW pumps
Feedwater isolation due to high temperature in feedwater system compartment	As above
Reactor scram	Start RHR and SWS pumps, open RHR valves
Reactor scram due to low water level in RPV	As above + start EFW pumps and open EFW regulation valves
Reactor scram due to high water level in RPV	Stop MFW and close EFW regulation valves
Reactor scram due to containment isolation	Start ECC and EFW pumps, open ECC valves
Low pressure before feedwater pump	Start EDGs
Depressurisation of the primary circuit	Open DPS valves
Extra low level in RPV	Open EFW regulation valves
High temperature in condensation pool	Start RHR and SWS pumps, open RHR valves
Low voltage in AC bus bar 1 resp. 2	Start corresponding EDG

The actuation of protection signals depends on the initiating event. The following categories of actuation can be distinguished:

- The condition for the protection signal is assumed with certainty. For instance, a LOCA will cause actuation of the containment isolation due to high pressure in the containment.
- The condition for the protection signal is assumed with a probability. For instance, a LOCA may cause an actuation of the high level in RPV.
- Protection signal is not actuated by the initiating event. Spurious actuation, due to I&C system failures, is taken into account, since it may have harmful effect on safety functions. For instance, a CCF of sensor may cause an isolation of the emergency pump room.
- Manual actuation of the protection signal is taken into account.

5.3 I&C architecture

The I&C system is divided in to redundant divisions A, B, C, D. In each division there is an acquisition and processing unit (APU) and a digital control and voting unit (DCV). An APU receives measurement signals and checks whether limiting conditions are exceeded. The actuation signals are sent to DCV units, which build the actuator (valve, pump, diesel generator) specific control signals.

In addition there is a processing unit for operator actions denoted as MCR-unit (main control unit). The operability of the MCR-unit is necessary for successful operator actions.

There is a comprehensive signal exchange between both APU and DCV units in order to ensure the reliability of the system. On the other hand, logic is built independently in each unit. Each APU unit receives the measurement signal from its division and builds

the actuation signal if the condition is fulfilled (e.g. low level in RPV). This signal is exchanged by all APU units. Each APU unit checks if 2-o-o-4 condition (or some other condition) is fulfilled, and if this is true the relevant RPS-signal is sent to all DCV units (e.g. SS04).

Since there are two front-line trains there are only two DCV units in this example. Each DCV unit receives signals from all four APUs and usually performs 2-o-o-4 voting to decide whether to send to control signal to the actuator (e.g. start pump X).

Figure 6 illustrates the I&C architecture with an example where RPS-xxxx signal controls the ECC-pumps. The condition for RPS-xxxx is actuation of 2-o-o-4 LL-level signals from the sensors PMS-xxxy.

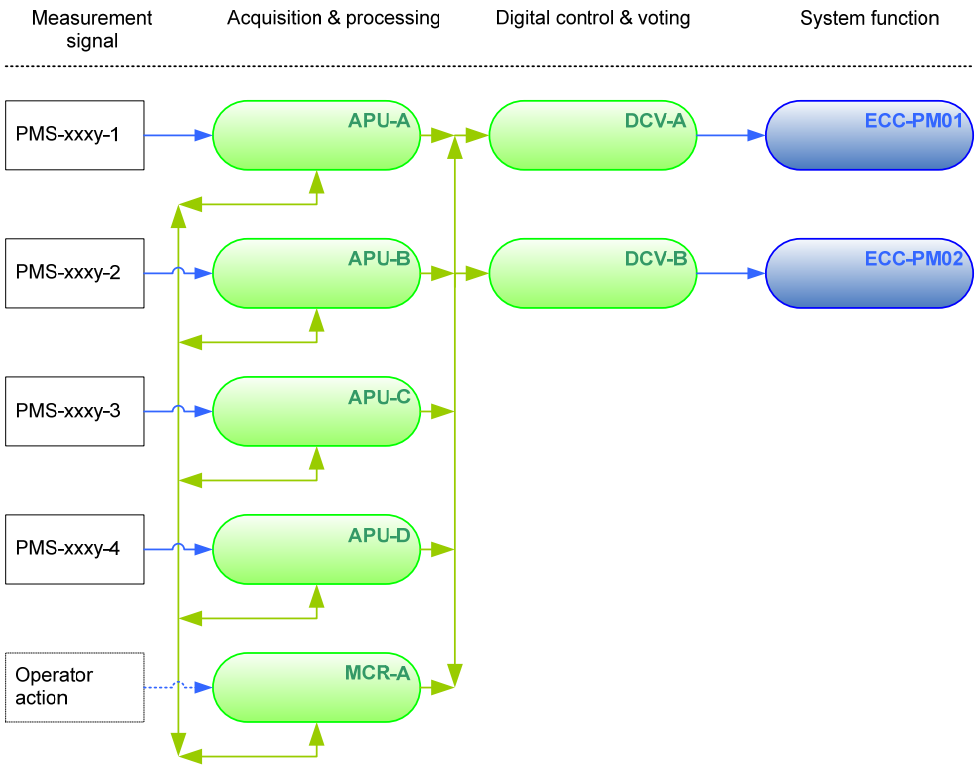

Figure 6. Example I&C system architecture.

This kind of redundant digital I&C system with lots of signal exchange is capable of handling many fault situations, e.g., to detect faulty signals or loss of individual units in the system. The fail-safe actions are, as mentioned above, separately defined for each RPS sequence and for each controlled safety function. Since different RPS sequences often uses the same inputs, though by different input channels, this results in that a given input can receive a default value of 0 in the voting for one RPS sequence, and default value 1 in the voting for another RPS sequence. Further complexity could be added when these RPS sequences are actuated by different types of voting logic, but this is not considered in this example.

From the PSA modelling point of view, “DFLT 0” cases need to be considered as causes to fail to trip both with respect to detectable and undetectable failure modes “DFLT 1” cases will cause spurious trip when the fault is detectable and failure to trip when the failure mode is undetectable.

A processing unit is a computerised system designed to receive input signals, perform computing and send output. It consists of modules. The following subcomponents are considered here:

- processor including software
- input and output modules (analog or digital) which are interfaces between the units and communication links
- subrack including all subcomponents needed for the power supply (within the unit)

In addition, each link between the units is considered as a communication link component.

5.4 Modelling assumptions

The PSA-model is simplified in several manners, as follows:

- Unavailability due to repair of detected failures during normal operation is not modelled.
- Only few failure modes have been considered for each component.
- Channels of the I/O modules are not modelled.
- Software failures are modelled as CCF:s one overall basic event for DCV units respectively APU units, both causing loss of all functions of DCVs respectively APUs (failure to trip).
- Hardware common cause failures are generally considered between all identical, redundant components with active failure modes. CCF:s are not modelled between DCV and APU levels, since they would not provide additional impact on the failure of RPS.
- Power supply to I&C is not modelled. Generally all hardware within the same division have the same dependencies to power supply.

5.5 Modelling options

Four model alternatives are considered:

1. Reference case as described above.
2. Simplified CCF-model for hardware failures. Alpha-factor is replaced by the Beta-factor model [10]. In the Beta-factor model there are only single failures and failure of the whole CCF group. The purpose is to study the importance of the partial CCF:s.
3. Signal for which ”DFLT 1” is assumed are changed to “DFLT 0”. The purpose is to study the the importance of the fail-safe design and spurious signals.
4. Intelligent validation. In this option, it is assumed that the first detected failure is ignored in the voting, i.e., 2-o-o-4 becomes 2-o-o-3. The fault trees are modified as follows:

    i) In case of “failure to trip” and “DFLT 1”, a detected failure in combination with a 2-o-o-3 failure of remaining channels is also a critical failure.

ii) In case of “spurious trip” and “DFLT 1”, 3-o-o-4 failure is a critical failure (instead of 2-o-o-4).

iii) For “DFLT 0” functions, there is no need to change the fault trees.

Option 2 studies the effect of a modelling approach in PSA. Options 3 and 4 are kind of sensitivity studies between different I&C architectures.

5.6 Results

Since the model and the data are fictive, it is not meaningful to draw conclusions from the numerical results. Therefore the analysis of the results is made qualitatively by studying the minimal cut sets which include I&C system basic events. The analysis were done in a comparative manner: 1) comparing the reference model with the original one without I&C and 2) the options are compared against the reference model. The numerical results, most important minimal cut sets and basic event importance can be found in [8].

5.6.1 Reference model

The minimal cut sets which include I&C failures can be summarised into the following categories:

- Any transient and a detected double (or more) CCF in APU processors. Spurious “high water level in RPV” and “feedwater isolation” will stop the water injection with MWF and EFW. Depressurisation fails in those trains which are controlled by failed APUs.
- Loss-of-feedwater transient (or LOCA) and detected or undetected CCF in DCV processors. DCV processors are vital to control EFW, ECC, RHR and SWS systems.
- Loss-of-feedwater transient and undetected CCF between level measurement sensors. Level measurement sensor CCF causes failure to actuate EFW and ECC.
- Loss-of-feedwater transient, CCF between EFW trains and failure of manual depressurisation (human error or I&C failure). There is no means to inject water to reactor.
- Loss-of-feedwater transient, CCF between EFW trains and failure of APU unit in division B or D. The APU units B and D both control two depressurisation valves. Since the success criterion is 5-o-o-6, a single failure in these units is a critical failure.
- LOCA and triple or quadruple CCF:s in APU causing failure to actuate the containment isolation which is the actuation signal of ECC.
- LOCA and double or quadruple CCF:s in APU causing spurious isolation of emergency pump rooms.

The rest of the minimal cut sets are longer.

The results are well understandable and can be explained by the lack of diversity at the plant. Such designs are not allowed in reality. In can also be noticed that no single failure of a I&C component in combination with an initiating event causes a core damage.

5.6.2 Option 2

In the option 2, the Alpha factor model for CCF:s is replaced by the Beta factor model, which is much simpler. In the Beta factor model, there are only single failure basic events and full CCF basic events, which is obviously reflected in the minimal cut set list.

The numerical difference between option 2 and the reference model depends on the relative contribution of partial CCF:s and on the beta factors used. In this example, the quantitative difference is clear, since double and triple CCF:s have quite high contribution. This also highlights the importance of accuracy in the parameter estimation and in transfer between different CCF models.

Another important observation was that when using the Beta-factor model some critical failure combinations and also modelling errors may not be observed. A fault tree for a four-redundant protection system with different fail-safe principles has easily a complex structure, which is prone to modelling errors. In this case, some modelling errors could be identified in the results of the reference model but not in the option 2 model.

5.6.3 Option 3

In option 3, detected I&C failures cannot cause spurious actuations. This has two effects on the reliability of the safety functions, when comparing to the reference case. Probability of failure to trip should increase (for those functions which were originally “DFLT 1” in the reference case), since detected failures are also critical. On the other hand, the probability of spurious actuation should decrease.

In the example model, the decrease of the probability of spurious actuation has bigger effect, i.e. a decrease in the total CDF is observed. The main difference is that a CCF between 2 out of 4 APU units does not in the case of detected failures cause spurious actuation of certain protection signals in option 3. A reversed example is the CCF of the communication links between APU and DCV, which is a critical failure in option 3, but not in the reference model. In the reference model, the fail-safe design would have given the actuation signal. All in all, option 3 results in a fewer number of minimal cut sets compared to the reference model.

It should be noted that result is due to the specific design of the example I&C system and cannot directly be generalised to other designs. One important feature of the design was that the fail-safe principle “DFLT 1” is implemented only in the APU level, but not in DCV level. Effect of option 3 is seen only in the importance of the failures of APU units. In addition, in this design there are two critical spurious signals which can make the core cooling unavailable.

5.6.4 Option 4

Option 4 evaluates the impact of so called intelligent validation, instead of ordinary trip/no trip validation.

Similar to option 3, the probability of failure to trip should increase and the probability of spurious actuation should decrease for those function which are “DFLT 1”.

The result is similar to option 3 so that the most important effect is that a double CCF of APU units after a transient is not anymore a minimal cut set. A difference from the option 3 is that triple detected CCF of APU after a transient is a minimal cut set.

5.6.5 Conclusions from the example

The example model shows that even rather simple I&C design leads to rather complex model despite of the fact that many things have been simplified and only a few protection signal are considered.

A lesson from the model option 2 is that Alpha factor model should be used to model CCF:s. Beta factor model may be sufficient in some cases, but an obvious benefit of using Alpha factor model is that it provides better means to identify critical failure combinations and to verify the correctness of the fault tree modelling. Existence (or non-existence) of double and triple CCF:s in minimal cut sets provides valuable insights into the reliability structure of the design.

Options 3 and 4 illustrate examples of comparing different I&C architectures. This example is simple enough to understand the effect of different designs on the overall reliability. However, the example is too simple to draw further conclusions on how detailed a PSA model should be and what benefits and drawbacks of different designs are. In order to be more realistic, there should be more diversity in the safety functions and e.g. the front line systems as well as DCVs could be four-redundant.

6 Plan for next phases 2012–13

6.1 Content, methods and phases

The project will consist of two closely interrelated activities:

1. WGRISK activity focusing on the development of best practice guidelines on failure modes taxonomy for reliability assessment of digital I&C systems for PSA.
2. The complementary Finnish-Swedish activity covering also objectives 2 and 3 (see ch. 2).

In 2012, the WGRISK activity will focus on finalising the failure modes taxonomy and to prepare a draft guidelines. A preliminary list of contents agreed in October 2011 is shown in Table 5.

Table 5. Preliminary list of contents of the WGRISK/DIGREL guidelines on the failure modes taxonomy

0 List of Acronyms
00 Executive Summary
1. Objective and Scope
2. Motivation
3. Uses of the taxonomy within PRA
4. Definition of terms
5. Approach and Assumptions
   - 5.1. General approach
   - 5.2. Hardware Assumptions
   - 5.3. Software Assumptions
6. Taxonomies
   - 6.1. General principles
   - 6.2. Collection of taxonomies
   - 6.3. Hardware taxonomy
   - 6.4. Software taxonomy
7. Example System
   - 7.1. Hardware Architecture
   - 7.2. Software Architecture
8. Demonstration of the Taxonomies Using the Example Systems
   - 8.1. System level example
   - 8.2. Module level example
9. Possible Data Sources and Data Collection Needs
   - 9.1. Current Data Sources
   - 9.2. Collection Needs/Methods
10. Open Issues- Limitations
11. User Guidelines
12. Conclusion and Recommendations
13. References

Appendix-Detailed Taxonomies

The complementary Finnish-Swedish activity will additionally focus on the following topics in 2012

- Failure data including CCF.
- Further studies related to the appropriate level of modelling based on experiments with the generic I&C system example created in 2011. The preliminary plan is to prepare a complete four-redundant plant and to have some diversity in the design.

In 2013, the work will be focused on the finalisation of the WGRISK guidelines and the NKS final report. Table 6 presents the milestones as planned in December 2011.

Table 6. Milestones of the NKS/DIGREL project (2012–13).

T=1.1.2012	Start
T + 2 M	WGRISK task group meeting in Paris
T + 5 M	WGRISK/DIGREL workshop in Berlin
T + 6 M	PSAM-11 conference in Helsinki, presentation of the activity
T + 7 M	ANS NPIC & HMIT 2012 conference in San Diego, presentation of the activity
T + 9 M	NKS (Nordic) workshop
T + 9 M	Draft guidelines on failure modes taxonomy (WGRISK)
T + 12 M	Interim report for NKS
T + 15 M	WGRISK task group meeting
T + 18 M	Final guidelines on failure modes taxonomy (WGRISK)
T + 24 M	NKS final report

6.2 Results and deliverables

The final result of the WGRISK activity will be a document “Best practice guidelines on failure modes taxonomy for reliability assessment of digital I&C systems for PSA”.

The result of the parallel NKS activity will be a document which has a broader scope: “Guidelines for reliability analysis of digital systems in PSA context.”

In addition, an interim work report will be prepared in the end of 2012 and workshops will be arranged to the end users to disseminate the results. Conference papers will be prepared to events such as PSAM (www.psam11.org) and NPIC-HMIT (http://meetings.ans.org/npic-hmit).

7 Conclusions

Failure modes taxonomy is a framework of describing, classifying and naming failure modes associated with a system. Main uses of failure modes taxonomies are in the performance of reliability analyses and in the collection of operating experience of technological systems. Due to the many unique attributes of digital systems, a number of modelling and data collection challenges exist, and consensus has not yet been reached.

In the DIGREL task, the taxonomy will be developed jointly by PSA and I&C experts which have slightly different views and needs on defining the failure modes. The PSA experts’ perspective follows the needs of PSA modelling in order to capture relevant dependencies and to find justifiable reliability parameters. I&C experts are focused on failure mechanisms and their recovery means, e.g., V&V measures. An important aspect in the development of the taxonomy is for PSA and I&C experts to define the “meeting point” for the two perspectives.

A clear distinction can be made between the treatment of protection and control systems controlling e.g. the turbine plant. There is a general consensus that protection systems shall be included in PSA, while control systems can be treated in a limited manner. The aim of DIGREL is first to define a common taxonomy for protection system type of digital systems. This is considered a conceivable target for the task, while the treatment of control systems may remain as an open issue.

The development of a hardware taxonomy is dependent on the overall requirements and prerequisites since they will set boundary conditions e.g. for the needed level of detail of hardware components and for the structure of the failure modes. The following overall requirements for the hardware taxonomy have been agreed upon:

- Shall support PSA practice, i.e. appropriate level for PSA, fulfill PSA requirements/conditions
- Shall cover undetected and detected failures
- Shall capture all critical dependencies and design features
- Shall be appropriate for safety related systems
- Shall support definition of failure modes, not mechanisms
- Shall be based on function view, not component
- Shall support modeling of CCF:s at necessary level.

With regard to the analysis and modelling of protection systems, the following levels of details can be distinguished from the hardware point of view:

(1) the entire system

(2) a division

(3) processing units (and cabinets)

(4) modules, i.e. subcomponents of processing units

(5) generic components, i.e. subcomponents of modules.

The most suitable level of detail is the “module level” which concur with the level of detail of general PSA state of the art. The module level will make it feasible to perform, maintain and review a PSA of digital I&C with reasonable resources while capturing critical dependencies. It will also be possible to capture fault tolerant features of the digital system and the impact on the reliability of safety functions.

The example model developed in the Nordic study [8] shows that even rather simple I&C design leads to rather complex model despite of the fact that many things have been simplified and only a few protection signal are considered. The example can be used to study the effect of detectable vs. undetectable failure modes. One lesson from the example is that alpha factor model should be used to model CCF:s instead of beta factor model. Two options were developed to illustrate the comparison of different fail-safe principles. The role of detectable and undetectable failure modes with respect to the failed versus spurious actuations can be clearly seen in the results, showing the importance to model these features rather accurately in PSA. At next stage, the example needs to be developed more complex to study the effect of diversity.

8 References

1. Recommendations on assessing digital system reliability in probabilistic risk assessments of nuclear power plants, NEA/CSNI/R(2009)18, OECD/NEA/CSNI, Paris, 2009. http://www.nea.fr/nsd/docs/2009/csni-r2009-18.pdf
2. Authén, S, Björkman, K., Holmberg, J.-E., Larsson, J. Guidelines for reliability analysis of digital systems in PSA context — Phase 1 Status Report, NKS-230

Nordic nuclear safety research (NKS), Roskilde, 2010. http://www.nks.org/scripts/pdfsearchbackend.php?Mode=getpdf&id=111010000275036&hash=055eaeac4b879aa3845cd9e798a899c7

3. Proceedings of the DIGREL seminar “Development of best practice guidelines on failure modes taxonomy for reliability assessment of digital I&C systems for PSA”, October 25, 2011, VTT-M-07989-11, Espoo, 2011. http://www.nks.org/download/nks_r_digrel_25th_oct_2011/vttm0798911_digrel_2011october_2011_vtt_proceedings.pdf
4. Holmberg, J-E, Authén, S., Failure modes taxonomy for digital I&C systems — common framework for PSA and I&C experts. In Proc. of Nordic PSA Conference - Castle Meeting 2011, Johannesbergs Slott, Gottröra, Sweden, 5–6 September, 2011. http://www.npsag.org/upload/userfiles/file/CastleMeeting2011/Papers/21%20-%20Paper.pdf
5. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 6: Guidelines on the application of IEC 61508:2 and IEC 61508:3. International Electrotechnical Commission, Geneva, 2000.
6. Information technology — Vocabulary — Part 1: Fundamental terms. ISO/IEC 2382-1:1993.
7. Authén, S., Wallgren, E., Eriksson, S., Development of the Ringhals 1 PSA with Regard to the Implementation of a Digital Reactor Protection System, 10th International Probabilistic Safety Assessment & Management Conference, PSAM 10, Seattle, Washington, June 7–11, 2010, paper 213.
8. Gustafsson, J. Reliability analysis of digital protection system of a nuclear power plant. Masters Thesis, KTH, Stockholm. January 2012. Manuscript.
9. RiskSpectrum PSA version 1.1.4 http://www.riskspectrum.com/en/risk/
10. RiskSpectrum Professional, Theory Manual, Relcon AB, 2001.

Title	Guidelines for reliability analysis of digital systems in PSA context — Phase 2 Status Report
Author(s) Affiliation(s)	Stefan Authén (1), Johan Gustafsson (2), Jan-Erik Holmberg (3) 1. Risk Pilot AB, 2. Royal Institute of Technology, 3. VTT
ISBN	978-87-7893-333-1
Date	February 2012
Project	NKS-R / DIGREL
No. of pages	32
No. of tables	6
No. of illustrations	6
No. of references	10

Abstract

The OECD/NEA CSNI Working Group on Risk Assessment (WGRisk) has set up a task group called DIGREL to develop a taxonomy of failure modes of digital components for the purposes of probabilistic safety assessment (PSA). A parallel Nordic activity carried out a pre-study where a comparison of Nordic experiences and a literature review were performed. The study showed a wide range of approaches and solutions to the challenges given by digital I&C.

In 2011, a proposal for the failure modes taxonomy was defined. This is based on a set of requirements agreed on the purpose of the taxonomy. The following levels of details can be distinguished from the hardware point of view: (1) the entire system, (2) a division, (3) processing units (and cabinets), (4) modules, i.e. subcomponents of processing units and (5) generic components, i.e. subcomponents of modules. Module level seems to be the most appropriate from the PSA modelling point of view. The software failure modes taxonomy is still an open issue.

An existing simplified PSA model has been complemented with fault tree models for a four-redundant distributed protection system in order to study and demonstrate the effect of design features and modelling approaches. The example shows that even rather simple I&C design leads to rather complex model despite of the fact that many things have been simplified and only a few protection signals are considered. One lesson from the example is that the Alpha factor model should be used to model common cause failures instead of the Beta factor model. Two options were developed to the comparison of different fail-safe principles. The role of detectable and undetectable failure modes with respect to the failed versus spurious actuations can be clearly seen in the results, showing the importance to model these features in PSA.

Key words Digital I&C system, probabilistic safety assessment, reliability, nuclear power plant safety

Available on request from the NKS Secretariat, P.O.Box 49, DK-4000 Roskilde, Denmark.
Phone (+45) 4677 4041, e-mail nks@nks.org, www.nks.org