NKS-302
ISBN 978-87-7893-378-2

Guidelines for reliability analysis of digital systems in PSA context — Phase 4 Status Report

Stefan Authén[1]

Jan-Erik Holmberg[1]

Linda Lanner[1]

Tero Tyrväinen[2]

[1]Risk Pilot AB, Sweden

[2]VTT, Finland

March 2014

Abstract

DIGREL develops practical guidelines for analysis and modelling of digital systems in probabilistic safety assessment (PSA) for nuclear power plants. The project consists of three interrelated activities. A taxonomy for failure modes of digital I&C systems has been developed by a task group of OECD/NEA Working Group RISK. In the parallel Nordic activity, a fictive digital I&C PSA-model has been developed for the demonstration and testing of modelling approaches. The third activity has been to develop a method for the quantification of software reliability in the context of PSA, which is reported in another publication.

The failure modes taxonomy is based on a failure propagation model and a definition of five levels of abstraction: 1) system, 2) division, 3) I&C unit, 4) I&C unit module, 5) basic component. The failure propagation model constitutes of the following elements: fault location, failure mode, uncovering situation, failure effect and the end effect.

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. I&C unit-level and module-level modelling were compared. Modelling on the I&C unit level of abstraction can result in large conservatisms that may produce misleading results e.g. regarding dominating core damage sequences and significance of I&C failure modes. Both undetected and detected failures contribute significantly to the PSA result, indifferently of the assumed fault tolerant design.

Two different modelling approaches were compared. In RiskSpectrum the system failure logic is represented by graphical fault trees while in FinPSA a so called communication network representation was applied. Same minimal cut sets were obtained except some differences in CCF calculations and truncation of minimal cut sets with small probabilities.

Key words

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

NKS-302
ISBN 978-87-7893-378-2

Electronic report, March 2014

NKS Secretariat
P.O. Box 49
DK - 4000 Roskilde, Denmark
Phone +45 4677 4041
www.nks.org
e-mail nks@nks.org

NKS Report NKS-302

Guidelines for reliability analysis of digital systems in PSA context

Phase 4 Status Report

Stefan Authén[1]
Jan-Erik Holmberg[1]
Linda Lanner[1]
Tero Tyrväinen[2]

[1]Risk Pilot AB, Parmmätargatan 7, SE-11224 Stockholm, Sweden
[2]VTT, P.O.Box 1000, FI-02044 VTT, Finland

March 2014

Table of contents

Abbreviations

A/D	Analog/digital
ACP	AC power system
AIM	Analog input module
ALOCA	Large loss-of-coolant accident
AOM	Analog output module
APU	Acquisition and processing unit
APU-AS	APU application-specific software modules
BWR	Boiling water reactor
CCF	Common cause failure
CCI	Common cause initiator
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	Diverse protection system
DCS	Data communication software
DCU	Data communication unit
DLC	Data link configuration
DPS	Diverse protection system
ECC	Emergency core cooling system
EDF	Électricité de France
EFW	Emergency feedwater system
ENEL	Ente Nazionale per l'Energia eLettrica, Italy
ESFAS	Engineered safety features actuation system
ET	Event tree
FMEA	Failure mode and effects analysis
FC	Fractional contribution
FT	Fault tree
FTD	Fault tolerant design
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 institute 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
MU	Manual control unit (I&C unit for main control room operations)
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
RDF	Risk decrease factor
RIF	Risk increase factor
RHR	Residual heat removal system
RPS	Reactor protection system
RT	Reactor trip
SAFIR	Finnish Research Programme on Nuclear Power Plant Safety
SCM	Signal conditioning module
SUR	Subrack incl. power supply
SW	Software
SWS	Service water system
SyS	System software
TXP	Teleperm XP (now SPPA T2000), product of Siemens AG
TXS	Teleperm XS, product of AREVA
VU	Voting unit
VU-AS	VU application-specific software modules
VU-FRS	VU functional requirements specification modules
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.

The failure modes taxonomy based on a hierarchical definition of five levels of abstraction: 1) system level, 2) division level, 3) I&C unit level, 4) I&C unit modules level, 5) basic components level. This structure corresponds to a typical reactor protection system architecture. The main feature of the taxonomy is to describe the failure propagation using a failure model. The failure model and the taxonomy consist of the following elements: fault location, failure mode, uncovering situation, failure effect and the end effect. The purpose of the taxonomy is to support PRA, and therefore it focuses on high level functional aspects rather than low level structural aspects. This focus allows handling of the variability of failure modes and mechanisms of I&C components. It reduces the difficulties associated with the complex structural aspects of software in redundant distributed systems.

In a parallel Nordic activity, a comparison of Nordic experiences and a literature review on main international references was performed in 2010 (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. In 2011–12, 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 (reports NKS-261, NKS-277). In 2013, the model was complemented with software fault basic events and additional tests of modelling features have been made.

A comparison was made between the I&C unit-level and module-level modelling. Modelling on the I&C unit level of abstraction can result in large conservatisms that may produce misleading results e.g. regarding dominating core damage sequences and significance of I&C failure modes. The evaluation of the example PSA also shows that both undetected and detected failures contribute significantly to the PSA result, indifferently of the assumed fault tolerant design. This stresses the importance of not excluding detected failures from the reliability model without thorough investigations. Similar conclusion can be drawn from the test of using different CCF parameters for undetected and detected failures. Finally, SW faults have a non-negligible effect on results. Attention needs to be paid on the quantification of software faults and the assessment of degree of diversity between subsystems of the reactor protection system.

Two different modelling approaches were compared. In RiskSpectrum the system failure logic is represented by graphical fault trees while in FinPSA a so called communication network representation was applied. Since the fundamental failure logic was same in both models, very similar minimal cut sets were obtained. There are only some differences in CCF calculations and truncation of minimal cut sets with small probabilities.

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 is 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.

Disclaimer

The views expressed in this document remain the responsibility of the author(s) and do not necessarily reflect those of NKS. In particular, neither NKS nor any other organization or body supporting NKS activities can be held responsible for the material presented in this report.

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 shows 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 takes 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 taxonomies and suggested definitions should be considered proposals and not as a PSA community consensus thoughts. The status of WGRISK/DIGREL activities has been presented in several events [3–10]. The 2011 interim report presented the preliminary failure modes taxonomy and the first version of the example PSA model for digital I&C [11]. In the 2012 interim report, the failure modes taxonomy and the example PSA model were developed further [12].

---

[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.

This 2013 interim report summarises the taxonomy proposal of the WGRISK/DIGREL task and reports the results of experiments with the example model. Software reliability quantification is reported in NKS report [13].

1 Scope and objectives

The objective of 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 abstraction in system analysis and screening of components, failure modes and dependencies
3. Develop an approach for modelling and quantification of CCF between components
4. Develop an approach for modelling and quantification of software (reported in [13]).

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.

2 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 digital I&C system risk. The focus of this WGRisk activity was on current experiences with reliability modelling and quantification of these systems in the context of PSAs of NPPs. Two workshops were organised to share and discuss experiences with modelling and quantifying digital I&C 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 of the new task called DIGREL are

- To develop technically sound and feasible failure modes taxonomy (or taxonomies if needed to address variations in modelling 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 (among other things):

- 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 guide the work, meaning e.g. that the (digital) system and its failures are studied from their functional significance point of view. This was considered a meaningful way to approach the problem.

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

The activity has taken 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 organised and public seminars have been organised annually [14, 15, 16].

A final draft was prepared for WGRISK in 2013 [17]. After that the taxonomy report shall go through an external review and then the acceptance steps of WGRISK, CSNI Programme Review Group and the CSNI itself.

The following organisations in the preparation of the taxonomy report: 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 International Common-cause Failure Data Exchange (ICDE) Project
- OECD/NEA Computer-based Systems Important to Safety (COMPSIS) Project (included December 2011 in ICDE)
- 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".

3 General approach for the development of the taxonomy

3.1 Definitions

Detected failure: A failure detected by (quasi-) continuous means, e.g. online detection mechanisms, or by plant behaviour through indications or alarms in the control room.

Detection mechanism: The means or methods by which a failure can be discovered by an operator under normal system operation or can be discovered by the maintenance crew by some diagnostic action [18].

There are two categories of detection mechanisms:

- Online detection mechanisms. Covers various continuous detection mechanisms.
- Offline detection mechanisms. E.g. periodic testing and also other kind of controls (e.g. maintenance).

Fail safe: Pertaining to a functional unit that automatically places itself in a safe operating mode in the event of a failure [19]; “system or component” has been replaced with “functional unit”) Example: a traffic light that reverts to blinking red in all directions when normal operation fails. Note: In general fail safe functional units do not show fail safe behaviour under all possible conditions.

Failure: Termination of the ability of a product to perform a required function or its inability to perform within previously specified limits [20]. "Failure" is an event, as distinguished from "fault" which is a state.

Failure effect: Consequence of a failure mode in terms of the operation, function or status ([21] “of the system” removed).

Failure mode: The physical or functional manifestation of a failure [20].

Failure mechanism: Relation of a failure to its causes.

Fatal failure: The I&C unit or the hardware module ceases functioning and does not provide any exterior sign of activity. Fatal failures may be subdivided into:

> **Ordered fatal failure:** The outputs of the I&C unit or the hardware module are set to specified, supposedly safe values. The means to force these values are usually exclusively hardware.
>
> **Haphazard fatal failure:** The outputs of the I&C unit or the hardware module are in unpredictable states.

Fault: Defect or abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function ([22]; “defect” added).

Fault tolerance: The ability of a functional unit to continue normal operation despite the presence of failures of one or more of its subunits. Note: Despite the name this definition refers to failures, not faults of subunits. It is therefore distinct from the definition in [19]. Possible means to achieve fault tolerance include redundancy, diversity, separation and fault detection, isolation and recovery.

Non-fatal failure: The I&C unit or the hardware module continues to generate outputs. Non-fatal failures may be subdivided into:

> **Failures with plausible behaviour:** An external observer cannot determine whether the I&C unit or the hardware module has failed or not. The unit is still in a state that is compliant to its specifications, or compliant to the context perceived by the observer.
>
> **Failures with implausible behaviour:** An external observer can decide that the I&C unit or the hardware module has failed. The unit is clearly in a state that is not compliant to its specifications, or not compliant to the context perceived by the observer.

Spurious actuation: An actual failure event where an actuation occurred that should not have occurred.

Systematic failure: Failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors [22].

Uncovering situation: The context where the failure becomes visible. The failure may become visible through dedicated "detection mechanisms" (see above), or failures may be discovered by a process event. The latter case includes failures revealed by spurious actuation or revealed (or triggered) by demand.

Undetected failure: A failure detected by offline detection mechanisms or by demand. Also called latent failure or hidden failure.

3.2 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 [3].

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 abstraction 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.

3.3 Types of I&C systems

A clear distinction can be made between the treatment of protection systems, i.e., reactor trip (RT) and engineered safety features actuation system (ESFAS) functions 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 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. DIGREL primarily considers protection systems since they are considered more important for PSA and it is considered conceivable target for the activity.

Protection systems (Figure 1) are composed of redundant divisions 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 software 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.

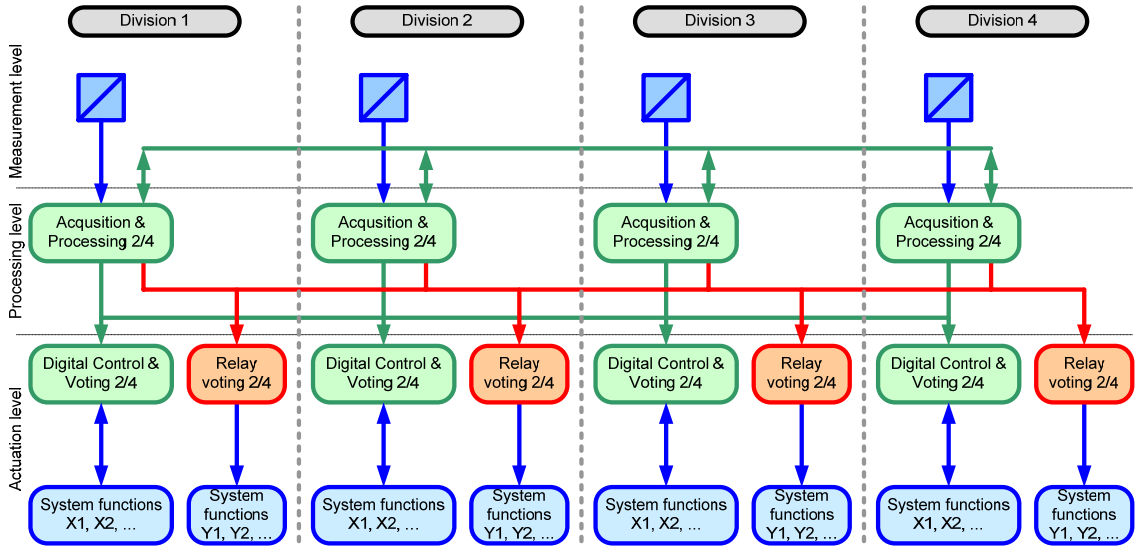

Figure 1. Example of a four-redundant digital I&C protection system architecture.

3.4 Requirements

The development of a taxonomy is dependent on the overall criteria and prerequisites since they will set boundary conditions e.g. for the needed level of abstraction of hardware resp. software components and for the structure of the failure modes. A different set of criteria may result in a different taxonomy, and the criteria are partly conflicting, in which case some balance needs to be found.

In the context of failure modes taxonomy, the main possible conflict in the requirements is same as with the PSA: the wish to have a realistic and complete taxonomy (or PSA model) and on other hand to have a practical, usable and understandable taxonomy (or PSA model). There is a pressure both towards perfectionism and towards simplifications between which targets a balance must be decided.

A related question is to what extent the plausibility of a failure mode is a criterion for defining the taxonomy. On one hand, we may define all theoretically possible failure modes regardless of their likelihood, and let the user of the taxonomy to decide (e.g. based on available data) which are relevant for the application. This approach is however problematic since our imagination may produce a large set of failure modes which is impractical basis for the use of the taxonomy. The plausible failure modes approach could be thus preferred, but it may be difficult to generally define which failure modes are relevant for certain components.

As a conclusion, the used approach to develop a taxonomy compromises between the simplicity and completeness targets.

Following the general principles of taxonomy construction and the particular requirements set by the domain of study, i.e. failure modes for digital instrumentation and control systems for application to PSA practice, the following set of criteria has been defined:

- Criterion 1: Defined unambiguously and distinctly

  There should be a clear definition of each failure mode with distinct characteristics which allow the analyst to clearly distinguish one failure mode from another. This criterion will ensure repeatable classification and hence help to ensure the quality of the information (e.g. failure data) collected.

- Criterion 2: Form a complete/exhaustive set

  This criterion stems from the need to cover all possible types of failures of software-based digital instrumentation and control systems so as to not leave potential risk contributors unidentified.

- Criterion 3: Be organized hierarchically

  This criterion allows easy organization of the taxonomic information and retrieval of the information. It also allows access to multiple levels of modelling.

- Criterion 4: Be mutually exclusive

  This criterion ensures that each failure mode will belong to one and only one taxonomic class at each taxonomic level. This is important for the failure data classification and consistent estimation of failure rates.

- Criterion 5: Data to support the taxonomy should be available now or in the future

  This criterion stems from the planned usage of the taxonomy and data collected on failure modes for PSA quantification. This criterion states that, if such a system does not yet exist, one should be able to put in place a data collection system that would allow accurate reporting of occurrence of such failure modes as well as number of opportunities for such occurrence. Presently data collection is seen problematic especially with regard to software faults. This taxonomy aims to support better data collection in future.

- Criterion 6: There should be analogy between failure modes of different components

  This criterion aims to develop a more consistent and complete failure mode taxonomy by comparing the failure modes of different components. On the other

hand, for many components there is a natural decomposition of the failure modes.

- Criterion 7: At the very least, the lowest level of the taxonomy should be sufficient to pinpoint existing dependencies of importance to PSA modelling

  Dependencies between components may lead to dependent failures that are potentially high impact risk contributors. The taxonomic levels should be such that one or multiple levels of the taxonomy allow accurate representation of such dependencies. This criterion is challenging in the sense that the number of potential faults in digital I&C is very high and we have a limiting ability to identify all dependencies and event propagation paths.

- Criterion 8: Should support PSA practice, and fulfil PSA requirements and conditions

  This criterion comprises of a wide range of aspects, which vary between PSA projects, e.g.

  1. Be a feasible analysis for PSA experts to perform
  2. Possible to implement into existing tools
  3. Possible to review by a PSA-expert
  4. Allow living PSA, e.g. possible to maintain and update with reasonable resources
  5. Available and maintainable failure data, i.e., allows collection and evaluation of operational events
  6. Support PSA applications.

- Criterion 9: Should capture defensive measures against fault propagation (detection, isolation and correction) and other essential design features of digital I&C

  The larger part of the failures within a digital I&C RPS will be detected by monitoring features such as self-surveillance, open circuit monitoring, cross channel comparison etc., while a small part only will be detected by periodic tests or actual need of the equipment. There are many fault tolerant features implemented at different levels of detail that may be platform and application specific. The failure parameters (i.e., failure rates and coverage) need to accurately capture the fault tolerant features.

3.5 Levels of abstraction

A failure modes taxonomy is based on an architecture structure that provides a hierarchical view on the system and its parts. Different levels of abstraction may be defined and failure modes can be defined from a function point of view or from a component point of view.

With regard to the analysis and modelling of protection systems, the following levels of details are distinguished (Figure 2):

- System level: a collection of equipment or platforms (subsystems) that is configured and operated to serve some specific plant function as defined by terminology of each utility. For a digital protection system, at the system level, the software consists of the collection of software running on various

microprocessors of the system and failure modes can be defined at this highest level.

- Division level: the system can be carried out in redundant or diverse divisions. In this case, a division may consist of the pathway(s) from sensor(s) to generation of an actuation signal. One such pathway is designated as a channel. The actuation signal can be sent to multiple actuators. A division can be decomposed further in I&C units. For the redundant or diverse divisions of a digital protection system, the collection of software running on the microprocessors of a single division may also fail and cause the failure of that division.
- I&C unit level: a division consists of one or more I&C units that perform specific tasks or functions that are essential for a system in rendering its intended services. I&C units consist of one or more modules. There is a limited number of I&C unit categories in a protection system.
- Module level: an I&C unit can be decomposed into modules that carry out a specific part of the process. For example, input/output-cards, motherboard, and communication cards, etc. An I&C unit may contain only a subset of these modules. The software program running on a particular microprocessor is also decomposed into modules (see Table 1).
- Basic component level: a module is composed of a set of basic components bounded together on a circuit board in order to interact. Consequently, the states of a module are the set of the combined (external) states of its basic components. Failure modes defined at the basic component level should be independent of design or vendor. Basic component level decomposition is only considered for hardware modules. For software it is not considered meaningful to go beyond the module level indicated in Table 1.

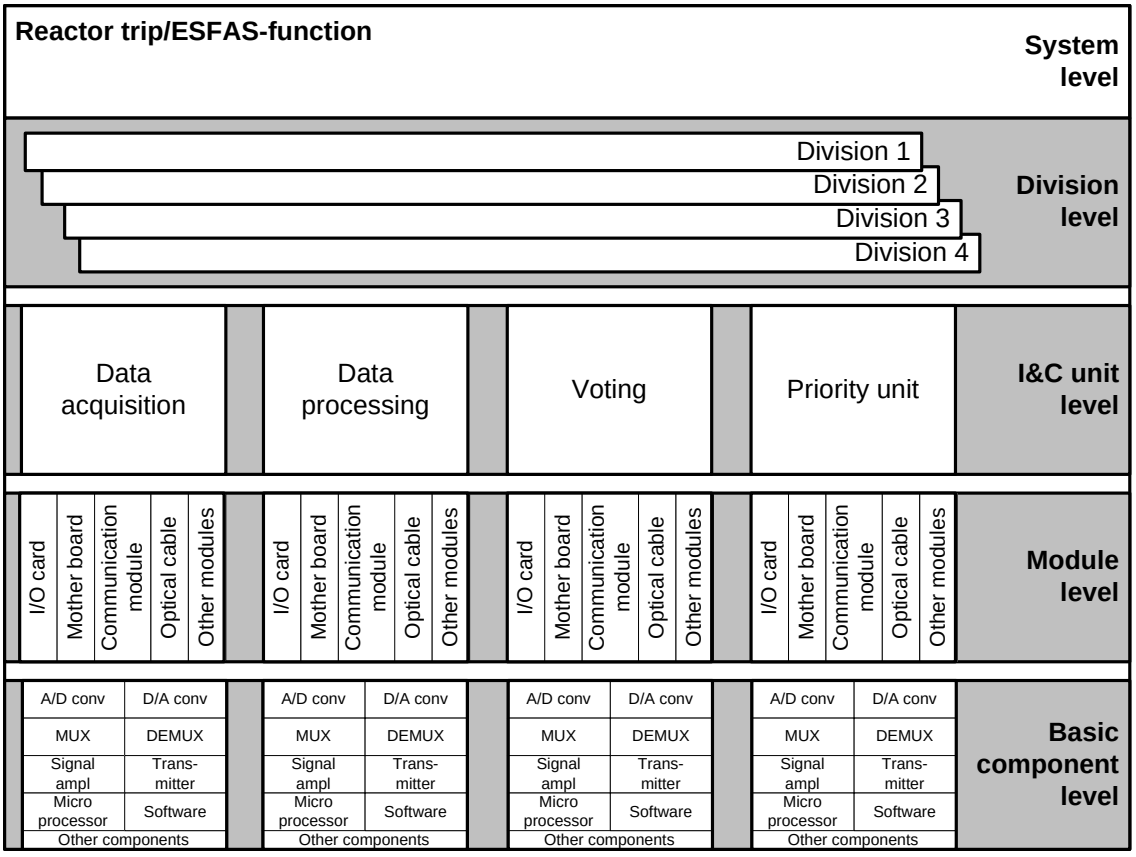

Figure 2. Principal structuring of safety I&C into different levels of details.

Table 1. Software modules in I&C units.

Unit	Software modules
I&C unit • Acquisition and processing unit (APU) • Voting unit (VU)	• System software • Application specific software • Elementary functions • Functional requirements specification (virtual software)
Data communication unit (DCU)	• System software • Data communication software • Data link configuration • Functional requirements specification (virtual software)
Potentially any kind of I&C unit (case by case assessment to be done)	• Proprietary SW modules (specific pieces of software present in hardware modules)

4 Failure modes taxonomy

4.1 Basic principles

This chapter describes a taxonomy that supports the representation of digital I&C protection systems in PSA, and the taxonomy is further modified in next chapter to be applicable for PSA modelling. This chapter discusses the failure mode taxonomy in generic terms in order to provide an exhaustive basis for the failure analysis. The

discussion presented here is a summary of the draft WGRISK/DIGREL failure modes taxonomy report [17].

The purpose of the taxonomy is to support PSA, and therefore it focuses on high level functional aspects rather than low level structural aspects. This focus allows handling of the variability of failure modes and mechanisms of I&C components. It reduces the difficulties associated with the complex structural aspects of software in redundant distributed systems.

The main approach is to define failure modes hierarchically and functionally. Hierarchical approach means that failure modes are considered both from top-down and bottom-up perspective. The top-down structuring starts from the actuator functions, identifies failure modes failing the functions and associated I&C functions and continues down to units, modules and even to basic components, if so wished.

In the bottom-up view the failure modes of the sub-units are defined and then the failure effects are considered at the higher level. The result is a set of mappings between failure modes and effects between two levels of hierarchy. The PSA practitioner has to choose suitable level of abstraction for each individual PSA and its application.

The taxonomy aims to be complete at system, division, I&C unit and module levels. The module level (both hardware and software) seems to be sufficient to analyse dependencies important to PSA, at least for protection systems. In specific cases, basic component level analysis may be needed, but it is not considered reasonable to fully deepen the taxonomy in that level.

The functional approach means that failure modes are defined in relation to the functional effect. In the system, division and I&C unit levels, no distinction is made between hardware or software aspects. At lower levels, the taxonomy is divided into hardware and software related failure modes.

The main feature of the taxonomy is to describe the failure propagation using a failure model. The important elements of the failure model, on which the taxonomy focuses, stand out:

- fault location,
- failure mode,
- uncovering situation,
- failure effect,
- the end effect.

These concepts are applied, in particular, to define the relationship between a fault in hardware or software modules (*module level failure modes*) and the end effect on I&C units (*I&C unit level failure modes*). In the analysis, a fault is postulated in a hardware or software module (fault location). For hardware modules, different failure modes are explicitly defined. Software module failure modes are directly associated with the failure effect. Uncovering situation describes when, where and how the module failure is significant at the I&C unit level. Failure effect is a simple but exhaustive way to categorise the effect of wrong output in a module.

The end effect describes the final propagation of the failure, taking into consideration all these elements of the failure model. In this consideration, a distinction can be made between the “maximum possible end effect”, when fault tolerance design (FTD) is not

effective or does not exist, and the “most likely end effect”, assumes that FTD features are present and efficient.

A comprehensive description of the failure model can be found in [17], and is illustrated in Figure 3. Failure propagation is the path from a “locally” postulated fault to a system or plant level end effect. The propagation can be considered at different levels of abstraction following the I&C architecture. The most interesting part is though the propagation between module and I&C unit levels. The ”context” is a concept, consisting of concepts “plant condition”, “initiating event” and “activation conditions”, and is a necessary part of the analysis of the failure propagation in PSA.

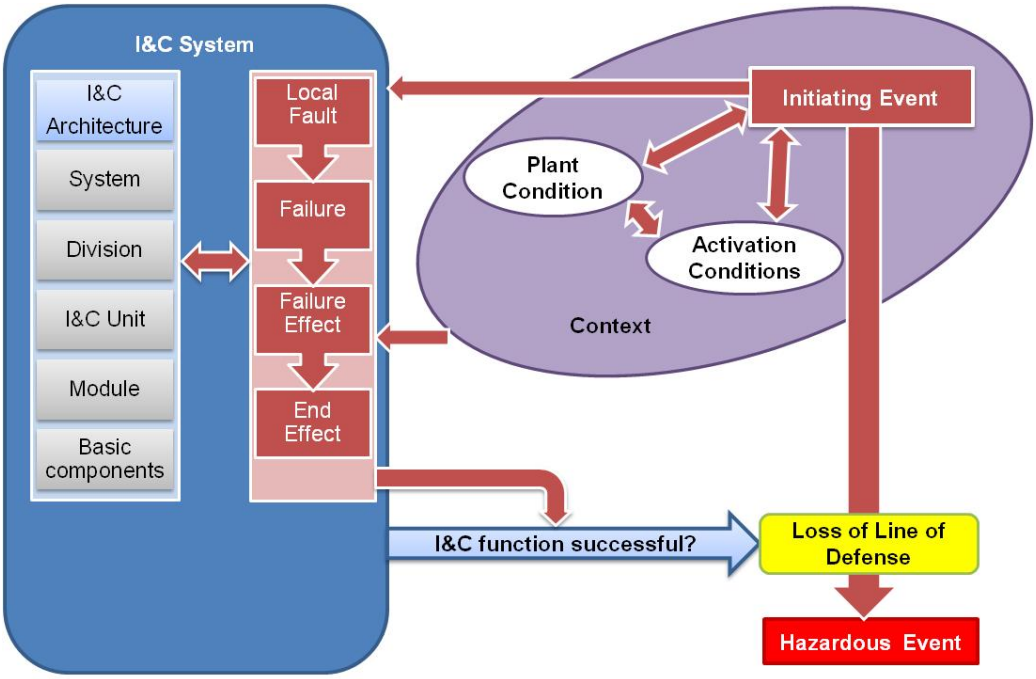

Figure 3. Representation of the Failure Propagation in an I&C system [17].

4.2 System and division levels

Practically, the safety-related function of the system is defined as the generation of safety-related actuation signal in a predefined time interval only when required. Since the “division” designates the division of the protection system which is responsible of controlling the actuators in the corresponding division, the function of a division is same as for a system. Thus, the failure modes in the division level are similar with those of the system level, which are

- failure to actuate the function (including late actuation),
- spurious actuation.

4.3 I&C unit and module levels

The key part of the digital I&C failure modes taxonomy is in the I&C unit and module levels where the fundamental functionality of the system can be discussed, e.g., the defensive measures against faults. It is practical to keep these two levels together in the

taxonomy since the meaning is to define dependency between failure modes of an I&C unit and the modules of it.

In the analysis, the existence of faults is postulated in the modules (hardware or software), and the question is to determine 1) how the unit is affected and 2) how other units that communicate with the defected unit are affected. In order to answer to these questions, the following issues need to be defined:

- The fault location: In which hardware or software module the fault is located?
- Failure effect:
    - Fatal, ordered failure (generation of outputs ceases, outputs are set to specified, supposedly safe values)
    - Fatal, haphazard failure (generation of outputs ceases, outputs are in unpredictable states)
    - Non-fatal, plausible behaviour (generation of outputs continues, an external observer cannot determine whether the I&C unit or the hardware module has failed or not)
    - Non-fatal, implausible behaviour (generation of outputs continues, an external observer can decide that the I&C unit or the hardware module has failed).
- Uncovering situation:
    - Online detection. Covers various continuous detection mechanisms.
    - Offline detection. E.g. periodic testing, and also other kind of periodic controls which can be credited in PSA.
    - Latent revealed by demand. The element considered was not correct before the demand, but the failure was not detected. This category can be divided into two parts: 1) failures which could have been detected by periodic testing but were not because the demand occurred prior to the test, 2) failures which cannot be detected by periodic testing.
    - Triggered by demand. The demand itself causes the failure of the element that had not experienced a failure before the demand. There was an existing fault which was activated by the demand, or a deviation in the demand that initiate the failure.
    - Revealed by spurious actuation. The occurrence of the failure immediately triggers spurious actuation. There are two categories:
        - Spurious actuation due to failure of online detection
        - Spurious actuation due to another I&C failure and correct action from online detection.

The combination of fault location, failure effect, uncovering situation together with the fault tolerant design (FTD) of the system are usually sufficient to determine the functional end effect in the I&C unit (APU/VU). Determination must be done case by case and is the essential part of the failure analysis. Examples are provided in next chapters.

An important issues is that it is neither necessary nor reasonable to assume all possible combinations, which considerably reduces the number of relevant failure modes (see Table 2).

Table 2. Relevance of the combinations of failure effects and detection situations.

	Uncovering situation				
Failure effect	Online detection	Offline detection	Revealed by spurious action	Latent revealed by demand	Triggered by demand
Fatal, ordered	**R**	**NR**	**R**	**NR**	**R**
Fatal, haphazard	**NR**	**R**	**R**	**R**	**R**
Non-fatal, plausible behaviour	**NR**	**R**	**R**	**R**	**R**
Non-fatal, implausible behaviour	**R**	**NR**	**R**	**NR**	**R**

R: Combination relevant for further analysis of end effects
NR: Combination not relevant for the analysis of the effects. Non-relevance is due to logical considerations.

First the combinations of failure effect and uncovering situations are considered. With regard to the fatal failures, haphazard failures can be ignored. It is unlikely that modules of the reactor protection system can fail in an unknown state, i.e., if the module crashes then the outputs are set to specified values. Fatal (ordered) failures are detected by online detection or by spurious effect.

Non-fatal failures are more dangerous since any detection situation may be possible. In case of implausible behaviour, failure is detected by online detection or by spurious effect. Plausible behaviour is not detected by online detection.

In the analysis of functional impacts on I&C units, we distinguish between the impact on a single I&C unit and impact on multiple I&C units. The latter is especially important when analysing the impacts of software faults (systematic fault in the system design).

From a single I&C unit point of view, the following functional failure modes can be considered:

- Loss of all functions (outputs) of the I&C unit,
- Loss of a specific function,
- Spurious function.

The above list is not exhaustive, and, e.g., for voting units or in case of intelligent validation of input signals the functional end effect may be more complex (e.g. degraded voting logic). Diesel load sequencer is also an example of a rather complex I&C function, for which a large number of failure modes may be assumed (but it can be sufficient to model only few of them in PSA).

The failure extent among multiple I&C units depends on the system architecture. In order to cover a variety of failure extents, including CCF between diverse systems, the system architecture shown in Figure 4 is considered. The protection system consists of two diverse subsystems A and B, both divided into four physically separated divisions. In the example PSA discussed in chapter 6 and Appendix A, the subsystems A and B are called RPS (reactor protection system) and DPS (diverse protection system), respectively.

The extent of diversity between A and B may vary, but we may generally assume that they perform different functions. The platforms are assumed to be identical, in order to include the platform CCF in consideration. The number of APU:s and VU:s per each subsystem and division may vary, too, but in Figure 4 we assume that there can be more than one APU/VU per each subsystem and division. In addition, there may be dedicated I&C units for operator actions.

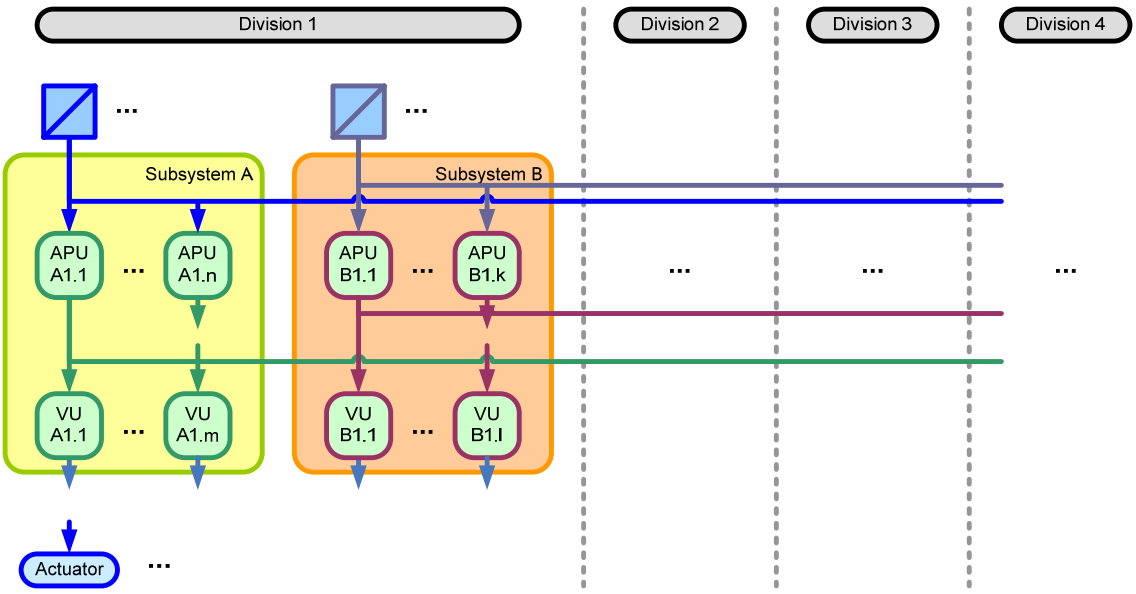

Figure 4. Example I&C system architecture.

In the above I&C architecture, the following end effects of a failure can be assumed:

- Failure of a single I&C module or basic component (single point failure)
- Failure of one application function including elementary function (or more) in one subsystem
- Failure of one Function (or more) in only one division in one subsystem
- Failure of one application function including elementary function (or more) in all subsystems
- Failure of one group of redundant similar APUs in all divisions
- Failure of multiple groups of redundant similar APUs in only one subsystem
- Failure of multiple VUs in only one subsystem
- Failure of multiple DCUs in only one subsystem
- Failure of only one subsystem
- Failure of multiple groups of redundant similar APUs in both subsystems. Possible system failure, depending on the allocation of application software modules.
- Failure of one subsystem and of group(s) or redundant similar APUs in all divisions in the other subsystem. Likely system failure.
- Failure of both subsystems.

The combinations of hardware module failures or software faults, detection situations and their functional impacts are further discussed in next subchapters.

4.3.1 Hardware modules

Table 3 lists a number of typical hardware modules in APU:s and VU:s and examples of failure modes. The list of failure modes is not exhaustive but it is rather representative. For each failure mode, the generic failure mode type, detection situation and functional impact on a single I&C unit are defined.

Table 3. Failure mode examples for hardware modules.

Hardware module	Failure mode examples	Failure effect	Uncovering situation	Functional impact on I&C units
Processor module	Hang	Fatal, ordered	Online detection	Loss of APU/VU functions (all)
	Communication dropout	Non-fatal, implausible	Online detection	Loss of APU/VU functions (all)
	Delayed signal	Non-fatal, plausible	Offline detection	Loss of APU/VU functions (all)
	Random behaviour	Non-fatal, plausible	Offline detection	Loss of APU/VU functions (all)
		Non-fatal, implausible	Online detection	Loss of APU/VU functions (all)
			Spurious effect	Spurious APU/VU function(s)
Analog input module	Signal fails high/low	Non-fatal, implausible	Online detection	Loss of all module application functions
	Signal drifts	Non-fatal, implausible	Online detection	Loss of all module application functions
	Signal hangs/freezes	Non-fatal, plausible	Offline detection	Loss of all module application functions
		Non-fatal, implausible	Online detection	Loss of all module application functions
Digital input module, single channel	Signal stuck to current value	Non-fatal, plausible	Offline detection	Loss of specific module application function
		Non-fatal, implausible	Online detection	Loss of specific module application function
	Signal fails to opposite state	Non-fatal, implausible	Spurious effect	Spurious module application function
Digital output module, single channel	Signal stuck to current value	Non-fatal, implausible	Online detection	Loss of specific module application function
		Non-fatal, plausible	Offline detection	Loss of specific module application function
	Signal fails to opposite state	Non-fatal, implausible	Spurious effect	Spurious module application function

4.3.2 Software modules

The approach is to successively postulate a single software fault in each software module regardless of the likelihood of such faults, and to determine the maximum possible extent of the failure, regardless of the measures taken by design or operation to limit that extent.

The following list of software modules is considered:

- System software (SyS).
- Elementary functions (EFs). Elementary functions are library SW modules used in the design of application software modules. A fault in EF is unlikely. However, misuse of complex EF in the application-specific SW (AS) modules is

a fault mode which may be relevant consider. Use of common EFs in AS modules is a potential source of common cause failures between AS modules.

- APU functional requirements specification modules (APU-FRS). There is one such module per application function required of an APU. Their purpose is to allow the representation of errors in functional requirements specifications of the acquisition and processing functions.
- APU application-specific software modules (APU-AS). There is one such module per application function implemented by an APU. Their purpose is to allow the representation of errors in the implementation of application-specific acquisition and processing software. If desired, a virtual module may be used to represent postulated errors in the data tables specifying the hardware configuration and the data communication of the APU.
- VU functional requirements specification modules (VU-FRS). There is one such module per voting function required of a VU. Their purpose is to allow the representation of errors in functional requirements specifications of the voting functions.
- VU application-specific software modules (VU-AS). There is one such module per voting function implemented by a VU. Their purpose is to allow the representation of errors in the implementation of application-specific voting software. If desired, a virtual module may be used to represent postulated errors in the data tables specifying the hardware configuration and the data communication of the VU.
- Data communication software (DCS).
- Data link configuration (DLC). There is one such module per network in the system.
- Proprietary SW in I&C modules (Propr. SW). Specific pieces of software present in hardware modules in APU, DCU, VU or any other module of the system (e.g. power supply) other than SyS and AS.

Given the taxonomy of end effects at I&C level, the Table 4 summarises the maximum failure extent of a postulated software fault in each of the software modules. In the next section (5.1.2), a limited number of cases are considered for the example PSA. For more discussion on software faults, see also [13].

Table 4. End effects of software module faults [13].

	SW fault location									
Effect	**SyS**	**EF (in APU)**	**APU-FRS**	**APU-AS**	**Propr. SW**	**VU-FRS**	**VU-AS**	**EF (in VU)**	**DCS**	**DLC**
FF-1SS	R	R	R	R	NR	R	R	R	NR	NR
FF-1D-1SS	R	R	R	R	NR	NR	NR	NR	NR	NR
FF-AllSS	R	R	NR	NR	NR	NR	NR	NR	NR	NR
1APU	R	R	R	R	R	NR	NR	NR	NR	NR
1VU	R	NR	NR	NR	NR	R	R	R	NR	NR
MAPU-1SS	R	R	NR	NR	R	NR	NR	NR	NR	NR
1SS	R	R	R	NR	R	R	R	R	R	R
MAPU-AllSS	R	R	NR	NR	R	NR	NR	NR	NR	NR
1SS-APU	R	R	NR	NR	R	NR	NR	NR	NR	NR
SYSTEM	R	R	NR	NR	R	R	R	R	R	NR

R: Relevant.
NR: Not Relevant. Non relevance is due to logical considerations.

- FF-1SS: Failure of one Function (or more) in one subsystem. This extent applies to non-fatal software failures that result in the misbehaviour of one or more I&C functions in one subsystem. The I&C functions that are dependent on the failed functions could also fail. Those dependent functions are necessarily in the same subsystem.
- FF-1D-1SS: Failure of one Function (or more) in only one division in one subsystem. This extent applies to non-common cause, non-fatal software failures of I&C functions without vote.
- FF-AllSS: Failure of one Function (or more) in all subsystems.
- 1APU: Failure of one set of redundant APUs. This extent applies to fatal software failures affecting only one set of redundant APU:s (necessarily in the same subsystem).
- MAPU-1SS: Failure of multiple sets of redundant APUs in only one subsystem.
- 1SS: Loss of one subsystem.
- MAPU-AllSS: Failure of multiple sets of redundant APUs in both subsystems.
- 1SS-APU: Loss of one subsystem and of one or more sets of redundant APU:s in the other subsystem.
- SYSTEM: Loss of both subsystems.

4.4 Basic components

Regardless of vendors, the functions of individual basic components of digital systems are well-defined, e.g., A/D converter is always used to convert analog signals to digital ones. This facilitates the definition of failure modes for individual components, similar to those of hardware modules. Also, a consistent set of failure modes can be applied to components of the same type, even if they are of different makes or models.

Failure modes for basic components are not further discussed in this context, since from the PSA point of view, the main analytical and modelling questions are solved at the module level. Basic component level may have though relevance in the determination of reliability parameters for modules (e.g. the failure rate of a module is a function of

failure rates of its basic components) and in the analysis of common cause failures (if two modules have similar basic components, there is a potential for CCF).

5 PSA Modelling

The main purpose of the developed failure mode taxonomy is to serve as basis for the modelling of digital I&C reliability in PSA:s. The intent of this chapter is to demonstrate the usage of the developed taxonomy for PSA modelling. Another purpose of this chapter is to address the different challenges in performing a reliability model of a digital reactor protection system (RPS), and to give guidance in aspects vital for achieving a sound PSA.

The task of incorporating a reliability model of a digital I&C based RPS into a traditional PSA model meets a number of challenges due to the specific features of digital I&C, e.g. features such as functional dependencies, signal exchange and communication, fail-safe design and treatment of degraded voting logic. This requires both new modelling approaches and new fault tree structures, which are to be incorporated within the existing PSA model structure. Another challenge due to the complexity and number of components within a digital I&C RPS is to keep the PSA model comprehensive at a reasonable size, e.g., number of FT:s and basic events, and to meet requirements regarding realism, quality assurance, maintainability, etc.

In order to demonstrate the taxonomy and to present and support modelling recommendations, a number of test cases have been performed by using the example PSA model presented in Appendix A.

The example PSA model was first developed in 2011 as a Master's Thesis at Royal Institute of Technology (KTH) in cooperation with the NKS/DIGREL project [23]. The example was based on RiskSpectrum example model (EXPSA). The model has been further developed in order to better describe a generic BWR [12]. The improvements cover among other things diversity of safety functions, four-redundant front line safety systems and a diversified reactor protection system. The digital I&C reliability model has been updated with new ESFAS and scram functions, and adapted to the hardware taxonomy presented in chapter 6.1 below.

The main objectives of the test cases are:

- Demonstrate the developed taxonomy and verify the usability for PSA purpose
- Produce and verify recommendations regarding
    - Level of detail of the reliability model
    - System, division, I&C unit and module level
    - Fault tolerant design
    - E.g. modelling of default values at detected failures and different voting logics
    - Hardware failure modes
    - Critical equipment, risk contribution of detected and undetected failures, etc.
    - Modelling of CCF
    - Software failure modes

- Software failures are modelled as CCF, with different impact depending on the fault location.

Since the dominating tool for performing state-of-the-art PSA is fault tree/event tree analysis, it will be the focus of this chapter. It is however recognised that other, more advanced, can be considered and that these tools in certain situations may be better suited for reliability analysis of digital I&C than traditional fault tree/event tree analysis. It should be noted that the developed taxonomy does not exclude the use of other tools than fault tree/event tree analysis.

5.1 Taxonomy for PSA modelling

Chapter 5 presented generic failure mode taxonomies at different levels of abstraction. The required level of abstraction to apply in the PSA depends as earlier discussed on several factors such as complexity of the digital I&C design and the RPS architecture, purpose of the PSA, diversity of the reactor protection system and safety systems in general.

The purpose here is to demonstrate the taxonomy and to evaluate different modelling aspects, among others the required level of abstraction, why a detailed level of abstraction is required in the example PSA. Hence, the failure mode taxonomy for the module level will be applied for the example PSA. The detailed level of abstraction is necessary initially to classify the basic failure modes of each digital I&C module into one of the defined generic failure modes, in order to decide the effect of the failure on a functional level.

5.1.1 Hardware failure modes

From the PSA modelling perspective, it is more beneficial to define the failure modes by functional effect rather than failure effect, since this not only will keep down the number of events and the model size, but also will simplify the modelling efforts and make the fault tree structure and the dependencies more comprehensible to the PSA user.

Based on the above reasons it is preferable to perform the grouping at as a high functional level as possible, taking into account failure characteristics vital for the functional effect. Such characteristics that must be considered for a digital RPS are in general means of failure detection since this decides whether or not the failure will be covered by the fault tolerant design and also the actions taken accordingly. Other characteristics that may need to be considered when defining the failure mode groups are differences in test intervals, CCF categorization and failure mode timing issues.

The described approach has been used for the example PSA to further categorize and group failures of the different digital I&C modules to achieve a more simple and PSA adapted failure modes taxonomy.

The main steps in developing the taxonomy for the example PSA are:

1. Failure effect according to the failure modes taxonomy at the module level (Table 3) is assigned to the failure modes of the digital RPS example system hardware modules presented in Appendix A, see Table A-8. Then the uncovering situation and functional impact on I&C units can be defined for the example system.

2. Compressed failure modes describing the functional impact on I&C unit level are defined based on the functional impact on I&C units and uncovering situation for the failure modes. The compressed failure modes distinguish between failures detected by the fault tolerant design (detected failures) and failures that are not detected by the fault tolerant design (undetected/latent failures). The categories for failure detection are also further developed in order to provide information on the location of detection, and also adapted to Nordic PSA terminology, by defining generic failure detection means. See Table 5.
3. Based on the knowledge of functional impact on I&C unit level, whether detected failure will be covered by the fault tolerant design or not and the location of the detection, it is possible to define the failure end effect, i.e. the impact on RT/ESFAS actuation signals for a given module failure, see Table 6.
4. The last step in defining the failure mode taxonomy for the digital RPS of the example PSA is to group all basic failure modes of an I&C module that have the same attributes for compressed failure mode, generic failure detection and failure end effect. The PSA adapted taxonomy is presented in Table 7.

Table 5. Demonstration of the taxonomy for the example PSA, step 1.

Hardware module	**Failure mode examples**	**Failure effect**	**Uncovering situation**	**Functional impact on I&C units**
Processor module	Hang	Fatal, ordered	Online Detection	Loss of APU or VU functions (all)
	Communication dropout	Non-fatal, implausible	Online Detection	Loss of APU or VU functions (all)
	Delayed signal	Non-fatal, plausible	Latent revealed by demand	Loss of APU or VU functions (all)
	Random behaviour	Non-fatal, plausible	Latent revealed by demand	Loss of APU or VU functions (all)
		Non-fatal, implausible	Online Detection	Loss of APU or VU functions (all)
			Spurious effect	Spurious APU/VU function(s)
Analog input module	Signal fails high/low	Non-fatal, implausible	Online Detection	Loss of all Module Application Functions
	Signal drifts	Non-fatal, implausible	Online Detection	Loss of all Module Application Functions
	Signal hangs/freezes	Non-fatal, plausible	Latent revealed by demand	Loss of all Module Application Functions
		Non-fatal, implausible	Online Detection	Loss of all Module Application Functions
Digital input module, single channel	Signal stuck to current value	Non-fatal, plausible	Latent revealed by demand	Loss of specific Module Application Function
		Non-fatal, implausible	Online Detection	Loss of specific Module Application Function
	Signal fails to opposite state	Non-fatal, implausible	Spurious effect	Spurious Module Application function
Digital output module, single channel	Signal stuck to current value	Non-fatal, implausible	Online Detection	Loss of specific Module Application Function
		Non-fatal, plausible	Latent revealed by demand	Loss of specific Module Application Function
	Signal fails to opposite state	Non-fatal, implausible	Spurious effect	Spurious Module Application function

Table 6. Demonstration of the taxonomy for the example PSA, steps 2 and 3.

Hardware module	**Uncovering situation**	**Functional impact on I&C units**	**Compressed failure mode**	**Failure detection**	**Failure end effect (RT or ESFAS)**
Processor module	Online detection	Loss of APU or VU functions (all)	Loss of function	Monitoring[1]	All outputs of APU or VU acc. to FTD
	Latent revealed by demand	Loss of APU or VU functions (all)	Latent loss of function	Periodic test[2]	Loss of all APU/VU outputs
	Spurious effect	Spurious APU/VU function(s)	Spurious function	Self-revealing	Spurious APU/VU output(s)
Analog input module	Online detection	Loss of all module application functions	Loss of function	Self-monitoring[3]	1oo4 conditions of specific[4] APU/VU outputs acc. to FTD
	Latent revealed by demand	Loss of all module application functions	Latent loss of function	Periodic test	Loss of 1oo4 conditions of specific APU/VU outputs
Digital input module, single channel	Latent revealed by demand	Loss of all module application functions	Latent loss of function	Periodic test	Loss of 1oo4 conditions of specific APU/VU outputs
	Online detection	Loss of all module application functions	Latent loss of function	Self-monitoring	1oo4 conditions of specific APU/VU outputs acc. to FTD
	Spurious effect	Spurious module application function	Spurious function	Self-revealing	Spurious 1oo4 conditions of specific APU/VU outputs
Digital output module, single channel	Online detection	Loss of all module application functions	Loss of function	Self-monitoring	Specific APU/VU output acc. to FTD
	Latent revealed by demand	Loss of all module application functions	Latent loss of function	Periodic test	Loss of specific APU/VU output
	Spurious effect	Spurious module application function	Spurious function	Self-revealing	Spurious APU/VU output
Communication module	Online detection	Loss of specific application functions	Latent loss of function	Self-monitoring	1oo4 conditions of specific APU/VU outputs acc. to FTD
Backplane	Online detection	Loss of APU or VU functions (all)	Loss of function	Monitoring	All outputs of APU or VU acc. to FTD
Power supply	Online detection	Loss of APU or VU functions (all)	Loss of function	Monitoring	All outputs of APU or VU acc. to FTD
Measurement	Online detection	Loss of specific application functions	Loss of function	Monitoring	1oo4 conditions of specific APU/VU outputs acc. to FTD
	Latent revealed by demand	Loss of specific application functions	Latent loss of function	Periodic test	Loss of specific APU/VU output

[1]Detected by monitoring functions in the next level of I&C-units, i.e. units communicating with the faulty unit.
[2]Periodic tests according to Technical Specifications
[3]Detected by the self-monitoring functions implemented in the module, or by monitoring mechanisms, provided by controlling modules
[4]The end effect of the failure is restricted to outputs dependent on the failed module
Offline detection is not considered here since it is only relevant with regard to unavailability due to corrective maintenance

Table 7. Demonstration of the PSA adapted taxonomy for the example PSA, step 4.

Hardware module	Compressed failure modes	Failure detection	Failure end effect (RT or ESFAS)
Processor module	Loss of function	Monitoring[1]	All outputs of APU or VU acc. to FTD
	Latent loss of function	Periodic test[2]	Loss of all APU/VU outputs
	Spurious function	Self-revealing	Spurious APU/VU output(s)
Analog input module	Loss of function	Self-monitoring[3]	1oo4 conditions of specific[4] APU/VU outputs acc. to FTD
	Latent loss of function	Periodic test	Loss of 1oo4 conditions of specific APU/VU outputs
Digital input module	Latent loss of function	Periodic test	Loss of 1oo4 conditions of specific APU/VU outputs
	Latent loss of function	Self-monitoring	1oo4 conditions of specific APU/VU outputs acc. to FTD
Digital output module	Loss of function	Self-monitoring	Specific APU/VU output acc. to FTD
	Latent loss of function	Periodic test	Loss of specific APU/VU output
Communication module	Loss of function	Monitoring[1]	1oo4 conditions of specific APU/VU outputs acc. to FTD
Backplane	Loss of function	Monitoring	All outputs of APU or VU acc. to FTD
Power supply	Loss of function	Monitoring[1]	All outputs of APU or VU acc. to FTD
Measurement	Loss of function	Monitoring[3]	1oo4 conditions of specific APU/VU outputs acc. to FTD
	Latent loss of function	Periodic test	Loss of 1oo4 conditions of specific APU/VU outputs

[1]Detected by monitoring functions in the next level of I&C-units, i.e. units communicating with the faulty unit.
[2]Periodic tests according to Technical Specifications
[3]Detected by the self- monitoring functions implemented in the module, or by monitoring mechanisms, provided by controlling modules
[4]The end effect of the failure is restricted in outputs dependent on the failed module
Offline detection is not considered here since it is only relevant with regard to unavailability due to corrective maintenance

5.1.2 Software failure modes

Table 4 summarises software faults which ideally could be considered in PSA. In PSA it is reasonable to consider a limited number of end effects. The selection should however be large enough to cover all relevant cases (i.e. end effects).

Firstly, the selection of postulated software faults is dependent on the system architecture why not all end effects are of interest to take into account. A natural simplification is to assume large end effect and ignore smaller end effects since they are covered by the larger case. Large end effects include complete CCF of the system (SYSTEM), and CCF of one subsystem (1SS).

Secondly, the selection of postulated software faults is dependent on the SW quantification method. In most cases, SW fault probability is based on a simple engineering judgement and as long as it is impossible to refine the probability judgement, it is meaningless to refine the set of modelled software faults.

Table 8. Screening of SW faults cases for the example PSA. Cases 1–4 are explained below.

	SW fault location									
Effect	**SyS**	**EF (in APU)**	**APU-FRS**	**APU-AS**	**Propr. SW**	**VU-FRS**	**VU-AS**	**EF (in VU)**	**DCS**	**DLC**
FF-1SS			4a	4a		4b	4b			
FF-1D-1SS			4c	4c						
FF-allSS										
1APU/1VU			3a	3a		3b	3b			
MxU-1SS										
1SS	2a	2a	2a		2a	2a	2a	2a	2b	2b
MAPU-AllSS										
1SS-APU										
SYSTEM	1	1			1	1	1	1	1	

- Case 1: A complete CCF covering faults located in SyS. The end effect of the fault is loss of both RPS and DPS (SYSTEM). This is a fatal failure discovered by online detection. Both APUs and VUs are affected and no outputs are generated as a consequence. This CCF is represented in the example model by a single basic event.
- Case 2: A complete CCF where all APUs and VUs fail (2a) or all communication fails (2b) due to failure of a common software module. The end effect of the fault is loss of one of the two subsystems: RPS or DPS (1SS). This is a fatal failure discovered by online detection.
    a. Case 2a: Both APUs and VUs are affected and no outputs are generated as a consequence. This CCF is represented in the example model by two basic events, one representing failure of APUs and VUs in RPS and the other failure of APUs and VUs in DPS.
    b. Case 2b: All communications between the APU and VU fails. The outputs are set to specified default values. This CCF is represented in the example model by two basic events, one representing failure of the communications in RPS and the other failure of communication in DPS.
- Case 3: A CCF causing failure of all redundant APUs (3a) or VUs (3b) due to failure of a common software module. The end effect of the fault is loss of one of the two subsystems: RPS or DPS (1APU, 1VU). This is a fatal failure discovered by online detection.
    a. Case 3a: All APUs in one subsystem are affected. VUs replace the inputs from the APU with default values. This CCF is represented in the example model by two basic events, one representing failure of APUs in RPS and the other failure of APUs in DPS.
    b. Case 3b: All VUs in one subsystem are affected and no outputs are generated as a consequence. This CCF is represented in the example model by two basic events, one representing failure of VUs in RPS and the other failure of VUs in DPS.
- Case 4: A CCF causing failure of redundant APUs (4a) or VUs (4b) due to failure of a common software module. The end effect of the fault is loss of one application function in one of the two subsystems: RPS or DPS (FF-1SS). This is a non-fatal failure that leads to failure to actuate or spurious actuation.

a. One application function in redundant APUs in one of the subsystem is affected. The CCF is modelled by application function and failure mode specific basic events.

b. One application function in redundant VUs in one of the subsystem is affected. The CCF is modelled by application function and failure mode specific basic events.

The postulated software faults of the digital RPS and DPS systems in the example system are summarised in Appendix A, Table A-10. Software fault probability is derived from [13] and listed in Table A-13.

5.2 PSA model structure

5.2.1 Introduction

The complex design with failure detection, default values and degraded voting significantly increases the effort of fault tree modelling, the complexity and the size of the model, compared to a model of an old relay-based RPS. These issues can to some extent be managed by the use of *modelling blocks* and *standardized fault tree structures*.

The purpose of the modelling blocks is to group events required for several different actuation signals, and events that have the same impact at failure on the actuation signals and can be modelled in the same positions of the fault tree structure. This procedure will minimize the number of fault trees and the number of event occurrences in the fault trees. It will also lead to a harmonisation of the fault trees and the fault tree structures, and hence increase the model clarity.

5.2.2 RiskSpectrum modelling

In order to achieve the goal stated in subsection 6.2.1, a number of new standardized fault tree types have been created. Table 9 describes the applied fault tree structures and modelling blocks. The fault tree structure allows the model to describe a voting that combines failures in I&C hardware with failures of measurements, compared to the more commonly used and simplified approach where votings of these failures are modelled separately. The importance of this difference in the PSA quantification have not yet been evaluated, though it will likely have impact when considering area events and common cause initiators (CCI) in power supply.

Table 9. RPS and DPS digital I&C fault tree structure.

Fault Tree Type	Fault Tree Description
Safety Function	The FT models failure of a Safety Function by transfer to one or several System Function FT:s.
System Function	The FT models System Function success criteria and transfers to FT:s of System Divisions.
System Division	The FT models System Division failures by transfers to FT:s of critical components.
Component (actuator)	The FT models basic events for mechanical component failures and functional dependencies by transfers to FT:s of e.g. Actuator Signal and power supply
Actuator Signal	The FT models signal dependencies for specific component failure mode by transfers to FT:s of voltage supply, Output Module failure and RPS Actuation Signal.
Output Module[1]	The FT models Actuator Signal failure due to failure in transfer of RPS Actuation Signal from Voting Unit via an Output Module. Output Module failure is modelled by basic events and failure of Voting Unit by transfer to VU fault tree page.
RPS actuation signal[2]	The FT models failure in the processing and voting of RPS Actuation Signals, and failures in signal exchange of RPS Protection Function status between VU and APU. SW failure modes type 1, 2a and 4b are modelled by basic events. Transfers are made to FT:s of RPS Protection Functions and to FT:s of failures in communication between VU:s and APU:s.
RPS protection function[2]	The FT models failure in the acquisition and processing of process measurements into RPS Protection Functions, and signal exchange of these values between APU:s. SW failure modes type 4a are modelled by basic events. Transfers are made to FT:s of Process Measurement and APU to APU communication failures. Transfer may also be modelled to FT:s of sub-functions of an RPS Protection Function.
Communication VU-APU[1]	The FT models failure in the signal exchange of RPS Protection Functions from APU:s to VU:s, by modelling failure of the communication module and SW failure modes type 2b by basic events and failure of sending APU by transfer to specific APU FT.
Communication APU-APU[1]	The FT models failure in the signal exchange of Process Measurement values between specific APU:s, by modelling failure of the communication module and SW failure modes type 2b by basic events and failure of sending APU by transfer to specific APU FT.
Process measurement[1]	The FT models failure in the Process Measurements and the acquisition of these signals via Input Modules. Failure of sensors is modelled by basic events and failure of Input Module by transfer to specific FT.
Acquisition & processing unit, APU[1]	The FT models failure of APU processor and subrack by basic events, SW failure modes type 3a and voltage supply failure by a FT transfer.
Voting unit, VU[1]	The FT models failure of VU processor and subrack by basic events, SW failure modes type 3b and voltage supply failure by a FT transfer.
Input module[1]	The FT models failure of Input Module by basic events

[1] Separate FT:s for latent and detected failures in order to account for effects of default values.
[2] One FT per division and RPS Actuation Signal or Protection Function.

Based on the taxonomy developed in section 6.1 and the safety I&C protection functions and fault tolerant design defined in Appendix A, the fault tree model of the example PSA with digital I&C has been developed by applying the fault tree structure of Table 9. The main tasks of the procedure (in a bottom-up perspective) are:

- Grouping of module failures into modelling blocks taking into account:
    - Possible failure modes
    - Possible default values at detected failure.

- Allocation of modelling blocks for each specific RPS/DPS safety protection functions (Table A-3) with regard to
    - Failure mode of the function
    - The consequence of applied default values at detected failure
    - Type of voting logic.
- Allocation of modelling blocks for each specific RPS/DPS actuation signal (Table A-2) with regard to
    - Failure mode of the actuation signal
    - The consequence of applied default values at detected failure
    - Type of voting logic.
- Allocation of modelling blocks for each actuator with regard to
    - Failure mode of the actuator
    - Fail-safe state of the actuator.

The reliability model has been developed with a somewhat expanded fault tree structure in order to increase the flexibility and to make it possible to evaluate different modelling aspects. The model of the digital I&C currently consists of 500 fault trees pages, 360 basic events and 90 hardware CCF groups. Software faults are modelled with a total of 39 CCF groups. The developed I&C model follows a generic coding system for fault trees and events.

5.2.3 FinPSA model structure

FinPSA model is otherwise similar to RiskSpectrum model except that I&C systems are modelled using I&C modelling feature of FinPSA [24]. In FinPSA, I&C model is built using success logic instead of failure logic. The system is described as a communication network so that each line of the model code represents a simple dependency structure: the element of the left hand side of the equation needs the elements of the right hand side of the equation to function. The model is written in a text file using operands '*', '+' and 'K/N', which are presented in Table 10, to define the dependencies.

Table 10. Operands of I&C model.

Operand	Example	Possible interpretation
*	S1 = C1 * C2 * C3	Signal S1 is TRUE if components C1, C2 and C3 work.
+	S2 = C1 + C2	Signal S2 is TRUE if component C1 or C2 works.
K/N	S3 = <2 C1 + C2 + C3>	Signal S3 is TRUE if two of components C1, C2 and C3 work.

The I&C model is fully integrated to other PSA model parts. Fault trees contain links to I&C model and I&C model includes links to fault trees. I&C model also uses the same data base as fault trees. When minimal cut sets are generated for the PSA model, the I&C model is automatically transformed into fault trees which are linked to LIC gates in fault trees. This transformation does not increase the calculation time much.

The I&C modelling feature is an alternative and complementary to fault tree modelling. Benefits of I&C modelling are the compact and simple representation and ease of making modifications. Model can also be imported using simple copy and paste. This makes, for example, changing of fail-safe principle simple and efficient.

The I&C model replaces Actuator Signal, RPS actuation signal and RPS protection function fault trees of the RiskSpectrum model (Table 9). The general structure of the I&C model text file is from top to bottom:

1. Inputs to APU voting
2. APU votings
3. Dependencies between signals
4. Inputs to VU voting
5. VU votings
6. Actuation signals

The I&C model mainly consists of links to fault trees and I&C model elements which are defined in their own I&C model equations. Basic events appear only in fault trees (with two exceptions).

Different I&C model parts are described in the following subsections.

5.2.3.1 Inputs to APU voting

An APU voting has always four inputs. An input is TRUE if the measurement sensor works and the communication link between this APU and the APU from the sensor's division works. If the measurement comes from the same division, only the measurement sensor needs to function. Example:

```
RPS30PU001I0002_2_I = RPS21PU001VL002_F_S * RPS32LLPU1PU1--_F_S,
```

where `RPS30PU001I0002_2_I` is an input to APU voting, `RPS21PU001VL002_F_S` is a measurement sensor and `RPS32LLPU1PU1--_F_S` is a communication link. Failures of measurement sensors and communication links are modelled in fault trees. Hence, `RPS21PU001VL002_F_S` and `RPS32LLPU1PU1--_F_S` are names of fault trees. Failures of APU analog input modules are modelled in the fault trees of measurement sensors as in the RiskSpectrum model (Table 9).

5.2.3.2 APU votings

An APU voting is typically 2 out of 4 voting as in the following example:

```
RPS30PU001I0002_V_I
= <2 RPS30PU001I0002_1_I + RPS30PU001I0002_2_I + RPS30PU001I0002_3_I + RPS30PU001I0002_4_I>
```

All the inputs are I&C model elements that are defined in 'Inputs to APU voting' section.

5.2.3.3 Dependencies between signals

Some signals are combined after the APU votings. For example, signals I002 and I005 are combined to form I000. Example equation:

```
RPS30PU001I0000_V_I = RPS30PU001I0002_V_I + RPS30PU001I0005_V_I,
```

where `RPS30PU001I0002_V_I` and `RPS30PU001I0005_V_I` are defined in APU votings. The equation means that I000 signal is TRUE if I002 or I005 is TRUE.

5.2.3.4 Inputs to VU voting

A VU voting has always four inputs. An input is TRUE if signal from APU (e.g. I000) is TRUE and the communication between this VU and the APU works. Example:

```
RPS40PU002AC001_3_I + RPS40PU002EC001_3_I = RPS30PU001I0000_V_I * RPS34LLPU1PU2--_F_S,
```

where RPS40PU002AC001_3_I is an input to ACP related VU voting, RPS40PU002EC001_3_I is an input to VU voting of ECC pump start signal, RPS30PU001I0000_V_I is I000 signal defined in 'Dependencies between signals' section and RPS34LLPU1PU2--_F_S is a communication link between APU 3 and VU 4. The equation means that these two inputs are TRUE if I000 is TRUE and the communication link works. The failure of the communication link is modelled in a fault tree named RPS34LLPU1PU2--_F_S. The equation includes both an input to ACP related VU voting and input to VU voting of ECC pump start signal because they are same. They could also be defined in separate equations but the model is more compact this way.

5.2.3.5 VU votings

A VU voting is typically 2 or 3 out of 4 voting. Example:

```
RPS40PU002EC001_S_I
= <2 RPS40PU002EC001_1_I + RPS40PU002EC001_2_I + RPS40PU002EC001_3_I + RPS40PU002EC001_4_I>
```

All the inputs are I&C model elements that are defined in 'Inputs to VU voting' section.

5.2.3.6 Actuation signals

An actuation signal is typically TRUE if the voting result in VU is positive, the digital output module of VU works and a DC power system bus works. Example:

```
ECC40PM001AS001_S_I + ECC40VM002AS001_S_I
= RPS40PU002EC001_S_I * RPS40PU002DO003_A_S * DCP41BT001DG001_G_S,
```

where ECC40PM001AS001_S_I is an ECC pump start signal, ECC40VM002AS001_S_I is an ECC valve open signal, RPS40PU002EC001_S_I is a VU voting result, RPS40PU002DO003_A_S is a digital output module and DCP41BT001DG001_G_S is a DC power system bus. The actuation signals for the pump and the valve are same. RPS40PU002EC001_S_I is defined in VU votings and the failures of the digital output module and the DC power system bus are modelled in fault trees named RPS40PU002DO003_A_S and DCP41BT001DG001_G_S. Fault trees of ECC pump and valve include LIC gates with names ECC40PM001AS001_S_I and ECC40VM002AS001_S_I. When minimal cut sets are generated, fault trees of the actuation signals are created and linked to LIC gates.

5.3 Comparison of RS – FinPSA results

The most significant difference between RiskSpectrum and FinPSA is in CCF related probability calculations as programs interpret the basic event probabilities given in the data bases differently. In RiskSpectrum, the basic event probability that is defined in the data base is the total probability that includes both the probabilities of CCFs and the single failure. The single failure probability is obtained when the portion of CCFs is multiplied out. In FinPSA, the basic event probability that is defined in the data base is the probability of the single failure. The total probability is calculated from it by adding

the CCF portion. Because of this difference, exactly same probability calculations cannot be performed using these two programs.

The minimal cut set results of RiskSpectrum and FinPSA are very similar. There are only some differences in CCF calculations and truncation of minimal cut sets with small probabilities. Common cause failure groups with over six basic events cannot be modelled in FinPSA except with beta-factor model. Because of this, FinPSA results are missing some minimal cut sets. In FinPSA, there can be a CCF between a group of basic events only if they all appear in a fault tree. In the analysed case, one of the main feedwater pumps is not in operation, and hence, FinPSA results include only a CCF of the two pumps that are in operation, while RiskSpectrum results include also a CCF of all three pumps.

5.4 Evaluation of modelling aspects

The example PSA model has been designed in a dynamic manner to allow major changes of the modelling of different digital I&C aspects. The model changes are mainly performed by the use of boundary condition sets in the consequence analysis cases.

Since the model and the data are fictive, it is not meaningful to draw conclusions from numerical results. The evaluation have instead been made by comparing importance measures such as risk increase factor (RIF), risk decrease factor (RDF) and sensitivity factors, and by qualitative analysis of minimal cut sets (number, rank, why a minimal cut set, which are missing, etc.), for different configurations of design and modelling aspects.

All initiating events as presented in Appendix A (Table A-1) have been analysed, but conclusions are mainly made based on the analysis of the initiating event “general transient” since this event will give the most unbiased results. The other initiating events all have impact on one or more core damage barriers, which will affect the importance of the digital I&C equipment.

The modelling aspects that have been addressed in this project are:

- Hardware failure modes. Relative importance of digital I&C modules and hardware failure modes (detected vs. undetected failures).
    - Level of detail. System level vs. I&C unit level vs. module level.
    - Default values. Importance of default value modelling.
    - CCF parameter importance.
- Software failures modes. Relative importance of digital I&C units and software failure modes (detected vs. undetected failures).

The results from the evaluation of these aspects are stated below.

5.4.1 Hardware failure modes

The fault tree model has been developed at module level of abstraction with modules and failure modes according to Table 7. Importance measures have been calculated for each module type and combined failure mode.

The results show that both undetected and detected failures contribute significantly to the result, in fact detected failures have almost 13 times higher fractional contribution

than undetected failures. The contribution is almost exclusively given by CCF events both for detected and undetected failures.

The reason to the high contribution from the detected failures is found in the fault tolerant design of the RPS and DPS, where several RPS/DPS safety functions (mainly isolation signals) apply a default value of 1 (i.e. 1-o-o-4 conditions tripped) at a detected failure in the APU:s, see Appendix A (Tables A-6, A-7). With failure in more than one division, e.g., by a CCF, this will lead to a spurious VU activation of one or several RPS/DPS actuation signals, which in turn may cause stop of one or several safety systems. The main contributor to the detected failures is the subrack module which affects the complete I&C unit and also has a relatively high failure probability compared to the other I&C modules. The contribution to detected failures from digital output modules is small since these only can affect a single system function.

The contribution from undetected failures was found to be of the same magnitude for the different modules. No module or failure mode was found to have insignificant contribution to the plant risk.

The results stress the importance of *not* excluding detected failures from the reliability model.

5.4.1.1 Level of detail

In order to evaluate the effect on plant risk measures of performing the digital I&C reliability model at different levels of detail, the example model has been developed with the possibility to evaluate the reliability of the digital protection system at I&C unit level.

This is performed by applying the hardware taxonomy of section 5.3 for the I&C unit level and modelling corresponding failure modes as exchange events for the basic events of processor failure modelled at module level. All other basic events at the module level receive a failure probability of 0. SW failure modes are however unchanged since they already represent I&C unit level and are modelled according to section 6.4.2.

One important task for the I&C unit level modelling is to calculate realistic failure rates and probabilities with regard to the number of sub-components (i.e. modules) critical for the I&C units function and the test interval of the I&C unit. For the purpose of evaluating modelling aspects in this project, where the impact with regard to simplifications in modelling of dependencies rather than conservatisms in reliability data is the objective, the failure rate is calculated as the sum of failure rates and failure probabilities for one piece of each module in the I&C unit. This gives the lowest possible failure rate for the I&C unit and the differences in results compared to the module level reliability model will to a larger extent be the result of simplifications in functional dependencies. The test interval for undetected failures is assumed to be the same as for the processor module, i.e., one year.

When results from the general transient event tree analysis case in the example model at the I&C unit level are compared to the results from the module level model, a CDF increase of a factor 1,8 is observed for the I&C unit level case.

The importance of the RPS and the DPS systems increases with a factor 4. These systems gain the highest fractional contributions among the modelled safety systems. The largest increase in importance is found for the undetected failures where the fractional contribution increases with a factor 44 while the increase factor for detected failures is less than 2. At I&C unit level undetected failures also have a higher risk

contribution than detected failures by a factor 2, whereas in the module level of abstraction the detected failures had a 13 times higher risk contribution than the undetected failures. This shows that the modelling at a higher level of abstraction (less details) may produce misleading results which in turn may lead to erroneous risk informed decisions.

One reason for the large increase in the importance of undetected failures is that a test interval of 1 year is applied to the I&C unit, while in the module level of abstraction the test interval for digital outputs is assumed to be 4 weeks, i.e. the failure probability of a single digital output is increased with a factor of 13 (all other modules have in the module level a test interval of 1 year). The results show however also that a large increase can be found due to the simplifications of dependencies to input and output modules, and also communication modules, that are applied when modelling at I&C unit level.

The rather low increase in the importance of detected failures is due to that the subrack is by far the largest contributor to detected failures. The failure probability of the complete I&C unit is a factor 2 compared to that of the subrack, which implies that the impact of modelling detected failures on a higher level of abstraction is negligible, i.e. the increase found is solely due to increase in the failure probability. The reason for this result is that failure of the subrack has the same impact as a failure of a complete I&C unit in combination with the subrack dominating the contribution from detected failures. In a case with lower failure probability of the subrack a larger relative increase in importance of detected failures when modelling at I&C unit level should be expected.

By comparing the cut set lists of the I&C unit and module level major differences can be observed. The list at module level is dominated by sequences with loss of offsite power as a post transient event in combination with failure of backup power resulting in a station blackout. The dominating events causing these sequences are unrelated to digital I&C. Cut sets containing digital I&C have a low individual contribution to the top frequency and the highest contribution is given by cut sets with CCF of emergency feedwater pumps and loss of RPS system due to software failure of communication modules (fault case 2b), and from cut sets containing software failures that affect emergency feedwater (fault case 4a or 4b) and software failure of RPS communication modules (fault case 2b).

The cut set list at the I&C unit level is not dominated by the station blackout sequences as in the module level, though these sequences are still high ranked. In addition the I&C unit level cut set list contains a large number of cut sets containing threefold CCF for undetected failure of RPS and DPS APU:s respectively. The sequence leads to the failure of reactor scram, which in comparison is a core damage sequence with quite low importance in the module level PSA. There are two major reasons for the increase in importance. The first is that dependencies for individual scram conditions to different input and output modules are not considered when modelling on the I&C unit level, i.e. they all fail at the same time. The second reason is that correct test intervals of the digital outputs for the reactor scram cannot be applied at I&C unit level modelling, which incorrectly results in a high risk contribution from reactor scram sequences.

It should be noted that the chosen approach for the I&C unit failure rate estimation produces lowest possible failure rate and that a more realistic approach should be expected to produce much higher results than presented here. A more realistic treatment of test intervals by calculating a mean value would decrease the results, but the differences described above would still be evident, only somewhat smaller.

5.4.1.2 Impact of default values

As described in Appendix A and discussed in previous sections, the assumed fault tolerant design of the example digital I&C systems apply default values of 1 in case of detected failures for some safety functions and actuator signals. This has the effect that spurious signals can occur and affect the safety systems availability, which is also reflected in the results of the evaluation of the modelling aspects performed on the reference model in sections 6.3.1 and 6.3.2. It is hence relevant to also evaluate the impact of the digital I&C for a fault tolerant design with a minimum of spurious signals.

For this purpose the example PSA has been evaluated under the assumption that a default value of 1 is applied to detected failures only for the reactor scram safety function. For all the other safety functions a default value of 0 is applied to detected failures, which means that no spurious signals can be caused by the digital I&C and detected failures instead contribute to loss of actuator signals.

The evaluation shows a small decrease in the core damage frequency at the module level of abstraction, which means that the decrease of the probability of spurious signals has bigger effect than the increase of the probability for failure to actuate caused by detected failures. The importance of detected failures decreases significantly compared to the reference model, and also the importance of undetected failures decreases because cut sets containing combinations of detected and undetected CCF events are no longer valid. The fractional contribution (FC) is of the same size for detected failures as for undetected failures.

When evaluating this case at the I&C unit level of abstraction one major difference is observed compared to the module level. The importance of undetected failures is still very high while the importance of detected failures decreases significantly. The FC of undetected failures is a factor 100 higher than the FC for detected failures. The reason for this is the increased importance of the event sequences related to failure of the scram system which was observed in section 6.3.2 when the I&C unit level of abstraction was applied, and also is observed here. Since the scram safety function in this case still applies a default value of 1 at detected failures, the conservatism applied for undetected failures when modelling on the I&C unit level comes even more evident in this case. Compared to the FC of undetected failures at the module level of abstraction, the I&C unit level of abstraction FC is a factor 100 higher.

5.4.1.3 Sensitivity of CCF parameters of detected faults

The evaluation results show that the contribution from hardware failures is almost exclusively given by CCF events both for detected and undetected failures which are expected due to the design and redundancy of the digital I&C systems.

The assigned CCF parameters will of course have large impact on the importance of the digital I&C for the plant safety, and in the example model the same CCF parameters have been assigned for both detected and undetected failures. CCF parameter values of digital I&C units and hardware modules are found in Appendix A, Table A-12. For the example model generic values have been used due to lack of I&C specific values.

It can be questioned if it is reasonable to use the same CCF parameter values for both detected and undetected failure modes, e.g. with regard to time factors. It is often argued that the likelihood of CCF for detected failures should be smaller than for undetected failures. If calculated CCF parameters for conventional equipment are studied, e.g. NUREG/CR-5496, no evidence for this can be found. The comparison is however not completely accurate and it could still be the case for digital I&C.

Since the results show that detected failures have a significantly higher fractional contribution than undetected failures (13 times higher), it is reasonable to perform a sensitivity analysis where the values of the CCF parameters for detected failures are significantly lowered. The sensitivity analysis therefore applies values up to ten times lower than the parameters of the undetected failures. Assumed CCF parameters are presented in Table 11.

Table 11. Assumed CCF parameters for digital I&C units and hardware modules.

Failure Mode	**Alpha 2/3**	**Alpha 2/4**	**Alpha 3/3**	**Alpha 3/4**	**Alpha 4/4**
Detected Failure in sensitivity analysis	1,0E-2	1,0E-2	1,0E-3	1,0E-3	1,0E-4
Detected Failure in original analysis	5,0E-2	5,0E-2	1,0E-2	1,0E-2	1,0E-3
Undetected Failure in original and sensitivity analyses	5,0E-2	5,0E-2	1,0E-2	1,0E-2	1,0E-3

The results from the sensitivity analysis show that lowering the CCF parameters of the detected failures have a significant impact on the results. The total core damage frequency decreases with 10 %. The results however show that detected failures still have a significantly higher fractional contribution compared to undetected failures, i.e. by more than a factor 3.

Once again, this stresses the importance of *not* excluding detected failures from the reliability model. Also relevant CCF parameters are of interest in order to achieve a relevant result.

5.4.2 Software failure modes

The results show that software faults have a significant impact on the overall result. Software faults in total have a fractional contribution of about 9%.

A comparison of the different software fault cases shows that software fault case 2 has the highest fractional contribution of 6%, followed by fault case 4, fault case 3 and finally software fault case 1, in that order (see Table 8 for fault cases).

Fault case 2b has a significant impact on the core damage frequency. This is due to that the VU:s applies default values to the outputs at failure of the communication software. In the example model it causes the main feedwater pumps to stop due to spurious actuation. The fault case also causes malfunction of the open signal of the automatic depressurisation system relief valves.

It should be remembered that the failure probability differs between different fault cases. Fault case 1 that has the worst end effect has a relatively low fractional contribution of 1%, and also the lowest failure probability. If however the failure probability is increased by a factor 100 to 1E-05, the core damage frequency increases with 30%. The impact of the different software fault cases is hence, and naturally, highly dependent on the assigned failure probabilities.

The impact of spurious signals is large which is shown when default values of 0 instead of 1 are applied in accordance with section 6.4.1.2. In this case the fractional contribution of software faults in total is 1%, e.g. the same magnitude as for hardware failures, and the fractional contribution of fault case 2b is reduced to 0.5%.

Based on the above, it can be concluded that software faults in general have a non-negligible effect on the results and should be considered in a digital I&C PSA.

Quantification of software faults and the assessment of the degree of diversity between subsystems can therefore be significant from the overall PSA results point of view.

5.4.3 Conclusions

The evaluation of the example PSA shows that both undetected and detected failures of hardware and software contribute significantly to the PSA result, indifferently of the assumed fault tolerant design. In the case where spurious signals can occur due to that default values of 1 are applied at detected failures, detected failures can even dominate the contribution from digital I&C to the plant risk. This stresses the importance of not excluding detected failures from the reliability model without thorough investigations.

The results show that the choice of level of abstraction for the modelling of digital I&C is of high importance for the result. Modelling at the I&C unit level can result in large conservatism that may produce misleading results e.g. regarding dominating core damage sequences and significance of I&C failure modes with regard to the plant risk, which in turn may lead to erroneous risk informed decisions.

SW faults have a non-negligible effect on the results due to their functional impact on all divisions — one or more safety functions can be lost. Therefore attention needs to be paid to the quantification of software faults and the assessment of the degree of diversity between the subsystems of the reactor protection system.

The received results are based on the specific design of the example plant and example I&C system and also the assumed failure data of the digital I&C and assumed CCF parameters. The results of this study should therefore not directly be generalised to other designs.

6 Next steps

In 2014, the focus is on dissemination of the results of the previous years' work. Besides the finalisation of the WGRISK taxonomy report and the software reliability quantification method, the main effort is to summarise the previous years' work into "Nordic guidelines on the reliability analysis of digital I&C in PSA" (tentative work name of the report).

Milestones 2014

Start	**1.1.2014**
T + 3 M	WGRISK/DIGREL task group meeting, finalisation of the taxonomy report
T + 6 M	PSAM12 conference papers
T + 10 M	Final draft of the NKS report and seminar (covering all activities 2010–14)
T + 13 M	NKS final report on guidelines of the reliability analysis of digital I&C systems in PSA

7 Conclusions

Failure modes taxonomy is a framework of describing, classifying and naming failure modes associated with a system. Main uses of the failure modes taxonomy is 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 has been 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 set boundary conditions e.g. for the needed level of abstraction of hardware components and for the structure of the failure modes. The following overall requirements for the hardware taxonomy have been agreed upon:

- forms a complete/exhaustive set, mutually exclusive failure modes,
- organized hierarchically,
- data to support the taxonomy should be available,
- analogy between failure modes of different components,
- the lowest level of the taxonomy should be sufficient to pinpoint existing dependencies of importance to PSA modelling,
- supports PSA practice, i.e. appropriate level for PSA, and fulfil PSA requirements/conditions,
- captures defensive measures against fault propagation and other essential design features of digital I&C.

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

(1) the entire system

(2) divisions

(3) processing units (and cabinets)

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

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

The evaluation of the example PSA has demonstrated the developed taxonomy and verified that it is suitable for PSA purpose. The evaluation shows that the choice of the level of abstraction for the modelling of digital I&C is of high importance for the results. The most suitable level of abstraction is found to be the "module level" which concurs with the level of abstraction of the general PSA state of the art. The module level makes it feasible to perform, maintain and review a PSA of digital I&C with

reasonable resources while capturing critical dependencies. It is also possible to capture fault tolerant features of the digital system and the safety functions' impact on the reliability.

Modelling on the I&C unit level of abstraction can result in large conservatisms that may produce misleading results e.g. regarding dominating core damage sequences and significance of I&C failure modes with regard to the plant risk, which in turn may lead to erroneous risk informed decisions.

The evaluation of the example PSA also shows that both undetected and detected hardware and software failures contribute significantly to the PSA results, indifferently of the assumed fault tolerant design. This stresses the importance of not excluding detected failures from the reliability model without thorough investigations. Similar conclusion can be drawn from the test of using different CCF parameters for undetected and detected failures.

SW faults have a non-negligible effect on the results due to their functional impact on all divisions — one or more safety functions can be lost. Therefore attention needs to be paid to the quantification of software faults and the assessment of the degree of diversity between the subsystems of the reactor protection system.

Two modelling approaches were compared. In RiskSpectrum the system failure logic is represented by graphical fault trees while in FinPSA a so called communication network representation is applied. Since the fundamental failure logic was same in both models, very similar minimal cut sets were obtained. There are only some differences in CCF calculations and truncation of minimal cut sets with small probabilities.

The received results are based on the specific design of the example plant and example I&C system and also the assumed failure data of the digital I&C and assumed CCF parameters. The results of this study should therefore not directly be generalised to other designs. Differences in conclusions may of course be found for different designs and failure data.

In order to develop a realistic fault tree model for a digital I&C protection system it is vital that the chosen fault tolerant design is fully understood and correctly described in the model. The treatment of faulty inputs and degraded voting logic sets the foundation of the fault tree analysis. In general, modelling of digital I&C significantly increases the effort of failure mode analysis, dependency analysis and fault tree modelling. The amount of resource involved in such a task should not be underestimated, neither should the task of quality assurance.

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.
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.
3. 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.

4. Holmberg, J.-E., Authén, S., Amri, A., Development of best practice guidelines on failure modes taxonomy for reliability assessment of digital I&C systems for PSA, Proc. of 11th International Probabilistic Safety Assessment and Management Conference & The Annual European Safety and Reliability Conference, Helsinki, 25-29.6.2012, 10-Th4-1.
5. Smidts, C., Kim, M.C., Identification of failure modes of software in safety-critical digital I&C systems in nuclear power plants, Proc. of 11th International Probabilistic Safety Assessment and Management Conference & The Annual European Safety and Reliability Conference, Helsinki, 25-29.6.2012, 10-Th4-2.
6. Piljugin, E., Authén, S., Holmberg, J.-E., Proposal for the taxonomy of failure modes of digital system hardware for PSA, Proc. of 11th International Probabilistic Safety Assessment and Management Conference & The Annual European Safety and Reliability Conference, Helsinki, 25-29.6.2012, 10-Th4-3.
7. Chu, T.L., Yue, M., Postma, W., A summary of taxonomies of digital system failure modes provided by the DigRel Task Group, Proc. of 11th International Probabilistic Safety Assessment and Management Conference & The Annual European Safety and Reliability Conference, Helsinki, 25-29.6.2012, 10-Th4-4.
8. Holmberg, J.-E., Authén, S., Gustafsson, J., Nordic experience and experiments of modelling digital I&C systems in PSA, Proc. of the 8th International Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies, NPIC & HMIT 2012, San Diego, 22-26.7.2012, American Nuclear Society, LaGrange, Park, Illinois, USA, pp. 278-290.
9. Kim, M.C., Stiller, J.C., Smidts, C.S., Discussion on definitions of terms in reliability analysis of digital I&C systems, Proc. of the 8th International Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies, NPIC & HMIT 2012, San Diego, 22-26.7.2012, American Nuclear Society, LaGrange, Park, Illinois, USA, pp. 291–295.
10. Holmberg, J.-E., Authén, S., Amri, A., Sedlak, J., Thuy, N., Best practice guidelines on failure modes taxonomy for reliability assessment of digital I&C systems for PRA, Proc. of the 8th International Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies, NPIC & HMIT 2012, San Diego, 22-26.7.2012, American Nuclear Society, LaGrange, Park, Illinois, USA, pp. 724-732.
11. Authén, S., Gustafsson, J., Holmberg, J.-E., Guidelines for reliability analysis of digital systems in PSA context — Phase 2 Status Report, NKS-261 Nordic nuclear safety research (NKS), Roskilde, 2012.
12. Authén, S., Holmberg, J.-E., Guidelines for reliability analysis of digital systems in PSA context — Phase 3 Status Report, NKS-277, Nordic nuclear safety research (NKS), Roskilde, 2013.
13. Authen, S., Bäckström, O., Holmberg, J.-E., Jockenhövel, M., Porthin, M., Taurines, A., Software reliability analysis for PSA. Draft report to be published in NKS series.
14. 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.

15. Proceedings of the DIGREL seminar, Development of best practice guidelines on failure modes taxonomy for reliability assessment of digital I&C systems for PSA, November 6, 2012, VTT-M-07735-12, Espoo, 2012.
16. Proceedings of the NKS-R DIGREL 2013, Seminar on reliability analysis of digital systems in PSA context, November 26, 2013, VTT-M-08815-13, Espoo, 2013.
17. Failure modes taxonomy for reliability assessment of digital I&C systems for PRA, Report prepared by a OECD/NEA Working Group RISK Task group DIGREL, draft November 2013.
18. Procedures for performing a failure mode, effects and criticality analysis, MIL STD 1629A, US Department of Defense, Washington D.C., 1984.
19. Systems and software engineering – Vocabulary, ISO/IEC/IEEE 24765:2010, International Electrotechnical Commission, Geneva, 2010.
20. Software engineering -- Software product quality requirements and evaluation (SQuaRE) -- Guide to SQuaRE, ISO/IEC 25000:2005, ISO/IEC, Geneva, 2005.
21. Analysis techniques for system reliability, Procedure for failure mode and effects analysis (FMEA), International standard IEC 60812:2006(E), Second edition, International Electrotechnical Commission (IEC), Geneva, 2006.
22. 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.
23. Gustafsson, J., Reliability analysis of digital protection system of a nuclear power plant, Master's Thesis, KTH, Stockholm, May 2012.
24. Niemelä, I., Isolation of I&C model from PRA fault tree model. Proc. of 11th International Probabilistic Safety Assessment and Management Conference & The Annual European Safety and Reliability Conference, Helsinki, 25–29.6.2012, 10-We3-4.

Appendix A. Description of the example system

Overview of the front-line safety systems

The example PSA-model represents a fictive boiling water reactor (BWR), which has four-redundant safety systems. The example model includes the following systems:

- ACP – AC power system
- ADS – Automatic depressurisation system
- CCW – Component cooling water system
- ECC – Emergency core cooling system
- EFW – Emergency feedwater system
- FCV – Filtered containment venting system
- HVA – Heating, venting and air conditioning system
- MFW – Main feedwater system
- RHR – Residual heat removal system
- RSS – Reactor scram system
- SWS – Service water system.

Figure A-1 and A-2 show a simplified flow diagram and line diagram related to the safety systems relevant to the example. It should be noted that this example must not be interpreted as a representative boiling water reactor, but rather as an example for demonstrating the reliability analysis of representative nuclear safety I&C.

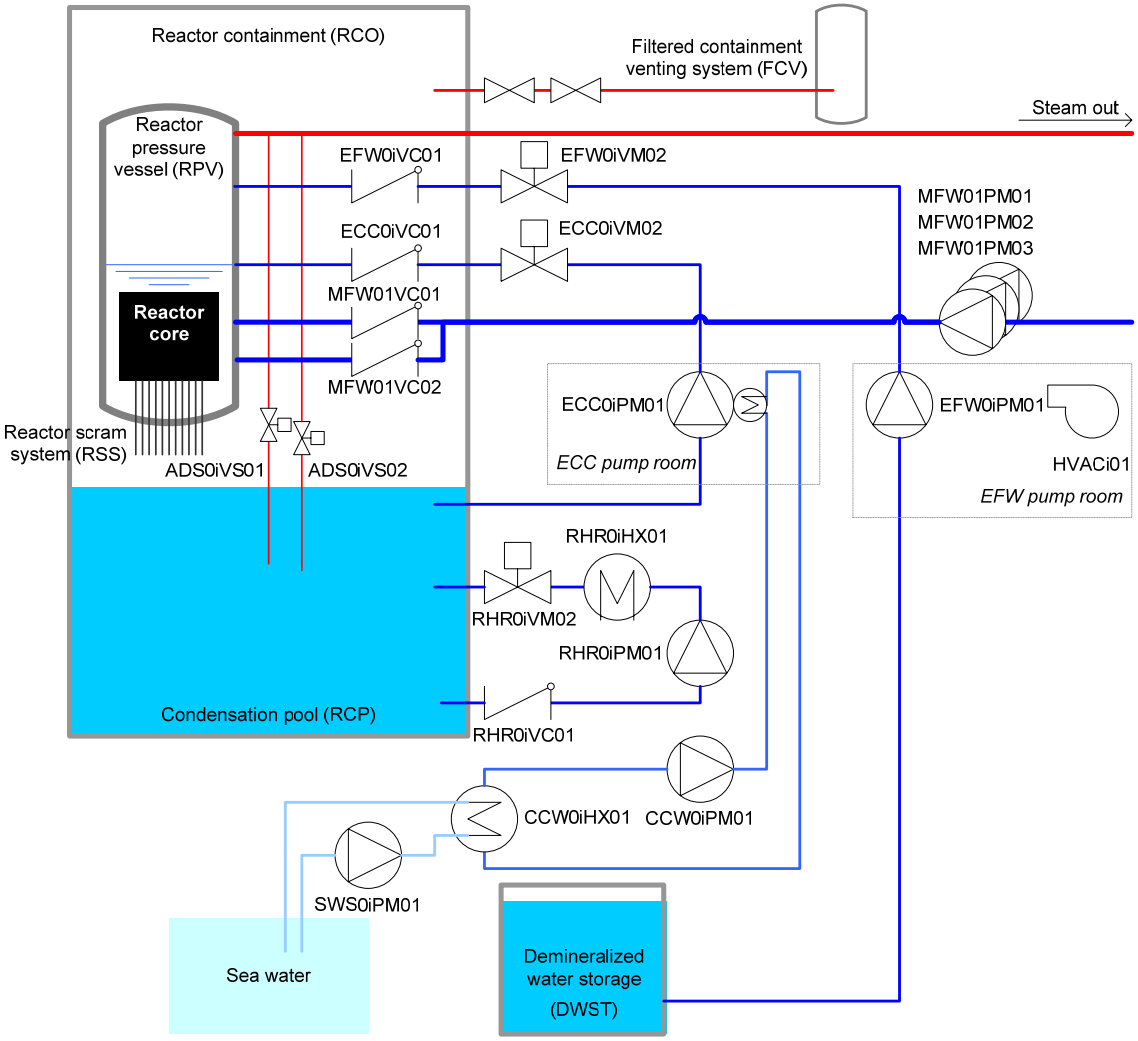

Figure A-1. Flow diagram of one train of the example NPP.

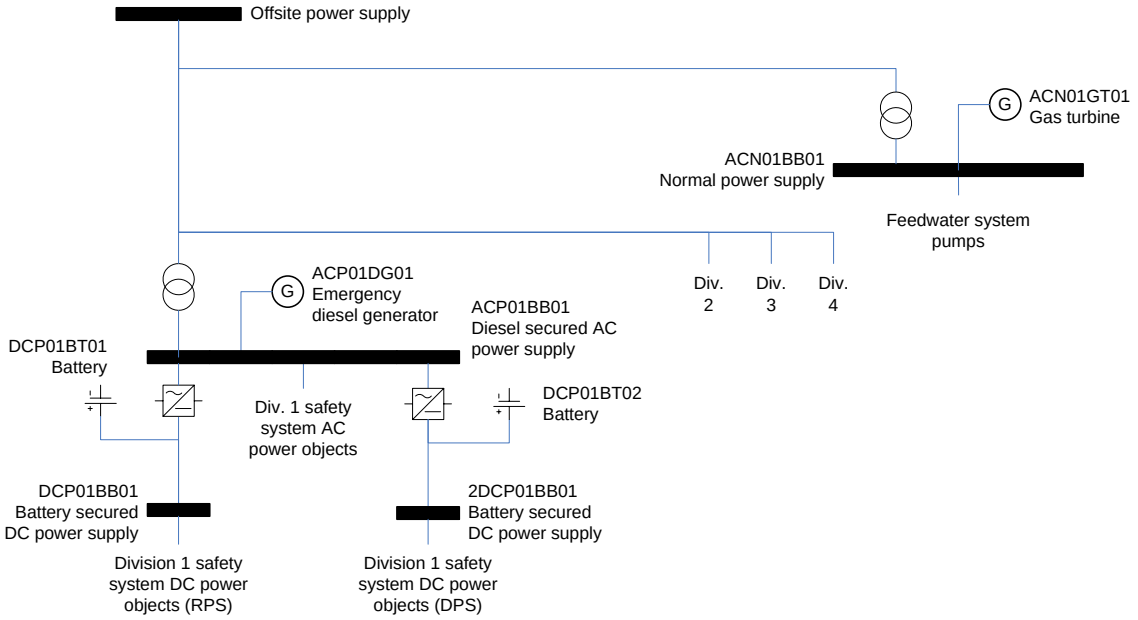

Figure A-2. Example NPP electric system line diagram.

Five initiating events are considered, see Table A-1. Depending on the initiating event there are different success criteria for the front line safety systems.

Table A-1. Front line safety system success criteria.

Initiating event	**MFW**	**EFW**	**ADS**	**ECC**	**RHR**
ALOCA – Large Loca	No credit	No credit	Not required	1oo4	1oo4
LMFW – Loss of main feedwater	No credit	1oo4	4oo8	1oo4	1oo4
LOOP – Loss of offsite power	2oo3	1oo4	4oo8	1oo4	1oo4
TRAN – General transient	2oo3	1oo4	4oo8	1oo4	1oo4
CCI DCP – Common cause initiator loss of DC power bus bar	2oo3	1oo4	4oo8	1oo4	1oo4

Safety I&C architecture and fault tolerant design

The architecture of the safety I&C is presented in Figure A-3. The protection system is divided into two subsystems, called RPS (reactor protection system) and DPS (diverse protection system). In addition to the APU:s and VU:s, the I&C architecture includes an I&C unit for operator actions (only for RPS), abbreviated by MU. This I&C unit is relevant for the manual actuation of the primary circuit depressurization and manual actuation signal of main feedwater pumps.

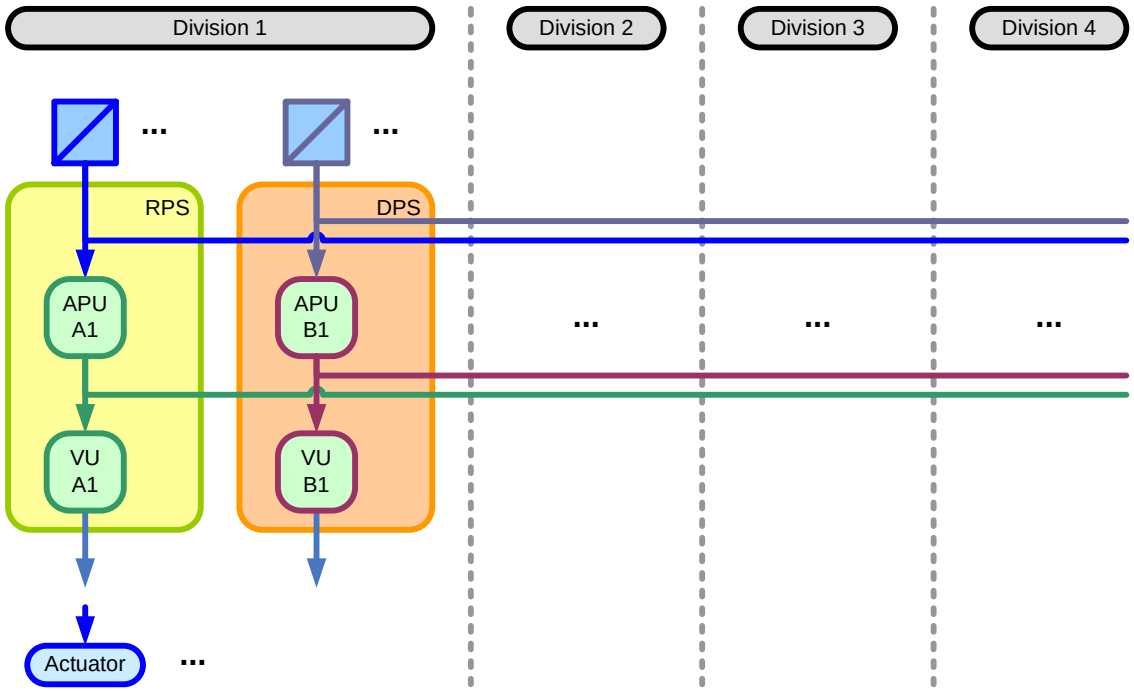

Figure A-3. I&C architecture.

The example PSA Digital I&C protection system is designed with fault tolerant features (fault tolerant design), which provides means to detect failures and mark faulty signals, e.g. self-surveillance, dynamic self-test, open circuit monitoring, cross channel comparison etc. Fault processing is implemented in the design of the hardware circuits and the software logic, and it can be 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. In general, the following applies for detected failures of the example I&C protection system:

- Detected failure in input signals, in intra I&C unit signal processing or in inter I&C unit signal exchange will cause corresponding signals to be replaced by a default value of 0 or 1.
- Complete, or fatal, failure of an I&C unit, e.g. processor failure or power supply failure, will cause all output channels of the I&C unit to 0 and controlled actuators will go to the predefined fail-safe state.

There are different solutions for voting applied in the safety I&C system for actuation signals to the actuators:

- Hardwired 2/4 voting by relays or pilot valves (e.g. scram)
- Software 2/4 voting performed in VU:s with possible treatment of degraded voting logic as follows:
    - **Logic 1:** The faulty signal is not set (0) to tripped condition, i.e. 2/4 degrades to 2/3 at first faulty input, 2/2 at second and fails at third faulty input.
    - **Logic 2:** The faulty signal is set (1) to tripped condition, i.e. 2/4 degrades to 1/3 at first faulty input, and trips at second faulty input.
    - **Logic 3:** One or more faulty signals are ignored, e.g. 2/4 degrades to 1/3 at first faulty input, and to 1/2 at second and 1/1 at third faulty input.

The fail-safe actions are separately defined for each RPS/DPS Safety Function and for each actuation signal. Safety Functions using the same inputs, may apply different default values and different types of voting logic.

Safety I&C protection functions

The general principle is that the EFW is controlled by the DPS and the ECC and ADS are controlled by the RPS. Pumps and valves in the respective system have same actuation signals. Also the support systems needed for cooling of the systems have same actuation signals.

In case of loss of feedwater transient, the normal consequence is the reactor scram actuated e.g. by the protection signal on low level in reactor pressure vessel (signal ID SS04), which is actuated both by the RPS (RSS04) and the DPS (DSS04). DSS04 will also actuate the EFW by starting the pump and opening the valve for the emergency feedwater injection.

If the emergency feedwater injection fails, the extreme low level protection signal will actuate (signal ID I002), also both by the RPS (RI002) and the DPS (DI002). I002 will in turn actuate the containment isolation protection signal I000, which is the start signal of the ECC (RI000). On the other hand DI000 is a secondary start signal for the EFW, if DSS04 has failed.

ECC will not be able to inject water to the RPV without depressurization of the primary circuit. The pressure relief valves of the ADS are actuated by the protection signal RTB00. RTB00 requires two subconditions two be actuated RTB01 and RTB02. The relief valves are actuated by solenoid valves which receive actuation signals from APU:s. Each APU controls two ADS valve lines.

Table A-2. Actuators and their actuation signals (i = division 1, 2, 3 or 4).

System	Actuator	Control	Condition for control type	VU Signal ID[1]	APU Signal ID[1]	DFLT[2]
ACP	Diesel generator	Start	Reactor scram due to containment isolation or low voltage in respective bus bar	RACP1 + DACP1	RSS12 + RZ00*i* + DZ00*i*	0
		Stop	Manual stop and not active start signal	RACP2 + DACP1	NOT(RSS12 + RZ00*i* + DZ00*i*) * MAN-0*i*DG01	1
ADS	Pressure relief valve	Open	Depressurisation signal	–	RADS1 {RTB0}	0
		Close	Manual close and not active depressurisation signal	–	RADS2 {NOT(RTB00) * MAN-ADS*j*, *j* = 1-8}	1
CCW	Pump	Start	Reactor scram or high temperature in the condensation pool	RCCW1	RSS00 + RX003	0
		Stop	Manual stop and not active start signal	RCCW2	NOT(RSS00 + RX003) * MAN-CCW0*i*PM01	1
ECC	Pump	Start	Containment isolation and no water leakage in the respective pump room	RECC1	NOT(RH00*i*) * RI000	0
		Stop	Water leakage in the respective pump room	RECC2	RH00*i*	0
ECC	Motor-operated valve	Open	Containment isolation and no water leakage in the respective pump room	RECC1	NOT(RH00*i*) * RI000	0
		Close	Water leakage in the respective pump room	RECC2	RH00*i*	0
EFW	Pump	Start	Feedwater system isolation, reactor scram due to low water level in reactor or containment isolation and no water leakage in the respective pump room	DEFW1	NOT(DH00*i*) * (DSS04 + DI000)	0
		Stop	Water leakage in the respective pump room	DEFW2	DH00*i*	1
EFW	Motor-operated valve	Open	Reactor scram due to low water level in reactor, diverse low water level condition or very low water level condition and no water leakage in the respective pump room	DEFW3	NOT(DH00*i*) * (DSS04 + DX001 + DI002)	0
		Close	Water leakage in the respective pump room or very high water level in reactor	DEFW4	DH00*i* + DSS05	1
HVA	AC cooler	Start	Start EFW	DEFW1	NOT(DH00*i*) * (DSS04 + DI000)	0
		Stop	Manually	DHVA1	DH00*i* + MAN-HVA0*i*AC01	1

System	Actuator	Control	Condition for control type	VU Signal ID[1]	APU Signal ID[1]	DFLT[2]
MFW	Pump	Start	Manual start and not active stop signal	RMFW1	NOT(RM000 + RSS05) * MAN-MFW*i*, *i* = 1, 2, 3	0
		Stop	Feedwater system isolation or very high water level in reactor	RMFW2	RM005 + RSS05	1
RHR	Pump	Start	Reactor scram or high temperature in the condensation pool and no water leakage in the respective pump room	RRHR1	RSS00 + RX003	0
		Stop	Manual stop and not active start signal	RRHR2	NOT(RSS00 + RX003) * MAN-RHR0*i*PM01	0
RHR	Motor-operated valve	Open	Reactor scram or high temperature in the condensation pool and no water leakage in the respective pump room	RRHR1	RSS00 + RX003	0
		Close	Manual stop and not active start signal	RRHR2	NOT(RSS00 + RX003) * MAN-RHR0*i*VM02	0
SWS	Pump	Start	Reactor scram or high temperature in the condensation pool	RRHR1	RSS00 + RX003	0
		Stop	Manual stop and not active start signal	RRHR2	NOT(RSS00 + RX003) * MAN-RHR0*i*VM02	0
RSS	Control rods		Reactor scram	–	RSS {RSS00} + DSS {DSS00}	1

[1] Fictive IDs used as identifiers in the coding of elements in the PSA model

[2] Default value applied at loss of communication signal between VU and APU

Table A-3. RPS- and DPS safety functions (i = division 1, 2, 3 or 4).

Signal	Description	Condition[1]	DFLT[2]
RPS			
RH00*i*	Isolation of the ECC pump room *i*	ECC*i*0CL001-H1 + ECC*i*0CL002-H1	1
RI000	Containment isolation	2/4*(RI002-*i* + RI005-*i*)	1
RI002	Containment isolation due to extremely low level in RPV	2/4*(RPV*i*0CL002-L4)	1
RI005	Isolation due to high pressure in containment	2/4*(RCO*i*0CP001-H1)	1
RM000	Feedwater isolation	2/4*(RM005-*i*)	1
RM005	Feedwater isolation due to high temperature in feedwater system compartment	2/4*(MFW*i*0CT001-H1)	1
RSS00	Reactor scram	2/4*(RSS04-*i* + SS05-*i* + SS12-*i* + SS13-*i*)	1
RSS04	Reactor scram due to low water level in RPV	2/4*(RPV*i*0CL001-L2)	1
RSS05	Reactor scram due to high water level in RPV	2/4*(RPV*i*0CL001-H2)	1
RSS12	Reactor scram due to containment isolation (I- or M-isolation)	2/4*(RI000-*i* + RM005-*i*)	1
RSS13	Low pressure before feedwater pump	2/4*(MFWi0CP001-L1)	1
RTB00	Depressurisation of the primary circuit	RTB01 * RTB02	0
RTB01	Depressurisation of the primary circuit condition 1: extreme low level in reactor (same as I002)	2/4*(RPV*i*0CL002-L4)	0
RTB02	Depressurisation of the primary circuit condition 2: high pressure in containment (same as I005) or manual actuation	RTB03 + 2/4*(RCO*i*0CP001-H1)	0
RTB03	Manual TB	MAN-TB	0
RX003	High temperature in condensation pool	2/4*(RCO*i*0CT001-H1)	1
RZ00*i*	Low voltage in AC bus bar *i*	ACP*i*0CE001-L1	1
DPS			
DH00*i*	Isolation of the EFW pump room *i*	EFW*i*0CL001-H1 + EFW*i*0CL002-H1	1
DI000	Containment isolation	2/4*(DI002-*i* + DI005-*i*)	1
DI002	Containment isolation due to extremely low level in RPV	2/4*(RPV*i*0CL002-L4)	1
DI005	Isolation due to high pressure in containment	2/4*(RCO*i*0CP001-H1)	1
DSS00	Reactor scram	2/4*(DSS04-*i* + SS05-*i* + SS12-*i* + SS13-*i*)	1
DSS04	Reactor scram due to low water level in RPV	2/4*(RPV*i*0CL001-L2)	1
DSS05	Reactor scram due to high water level in RPV	2/4*(RPV*i*0CL001-H2)	1
DSS12	Reactor scram due to containment isolation (I- or M-isolation)	2/4*(DI000-*i* + DM000-*i*)	1
DX001	Extra low level in RPV	2/4*(RPVi0CL002-L3)	1
DZ00*i*	Low voltage in AC bus bar *i*	ACP*i*0CE001-L1	1

[1] + = OR, * = AND, 2/4 = 2-o-o-4

[2] Default value applied by APU at loss of input signal from measurement or other APU:s

RPS and DPS have partly different input signals but they also share several measurements, see Table A-4.

Table A-4. Measurements (i = division 1, 2, 3 or 4).

Measurement	Component ID	Limit		Purpose	RPS	DPS
RPV water level, fine level	RPV*i*1CL001	L2	Low level	Core cooling protection	RSS04	
	RPV*i*2CL001	H2	Extra high level	RPV overfilling protection		DSS05
	RPV*i*2CL001	L2	Low level	Core cooling protection		DSS04
RPV water level, coarse level	RPV*i*1CL002	L4	Extremely low level	Core cooling protection	RI002 RTB01	
	RPV*i*2CL002	L3	Extra low level	Core cooling protection		DX001
	RPV*i*2CL002	L4	Extremely low level	Core cooling protection		DI002
Feedwater system pump suction pressure	MFW*i*0CP001	L1	Low pressure before feedwater pump	Loss of feedwater supervision		DSS13
Feedwater system room temperature	MFW*i*0CT001	H1	High room temperature	Leakage supervision		DM005
Containment pressure	RCO*i*1CP001	H1	High pressure in containment	Leakage supervision	RI005 RTB02	
	RCO*i*2CP001	H1	High pressure in containment	Leakage supervision		DI005
Condensation pool temperature	RCO*i*0CT001	H1	High temperature in condensation pool	Residual heat removal	RX003	
Water level in the ECC pump room	ECC*i*0CL001	H1	Water on the floor	Leakage supervision	RH00*i*	
Water level in the EFW pump room	EFW*i*0CL001	H1	Water on the floor	Leakage supervision		DH00*i*
AC power voltage bus bar ACP-*i*	ACP*i*1CE001	L1	Low voltage on bus bar ACP-*i*	Loss of offsite power supervision	RZ00*i*	
	ACP*i*2CE001	L1	Low voltage on bus bar ACP-*i*	Loss of offsite power supervision		DZ00i

Front line safety system failure modes

Table A-5 describes failure modes of the systems EFW, ECC and ADS related to the initiating event LOFW. Support system failure modes are not included in the table. Since EFW and ECC are similar from the failure modes and effects analysis point of view, they are shown in the same lines in this table. I&C failures are further in the next chapter.

Table A-5. Failure modes and effects analysis of EFW, ECC and ADS.

System/component (*i* = division)	Failure modes	Failure cause	Failure effect
EFW (ECC)	Failure to provide coolant injection		No water to RPV
EFW division *i* (ECC division *i*)	Failure to provide coolant injection		EFW (ECC) train *i* unavailable for coolant injection
EFW*i*0PM01 (ECC*i*0PM01)	Failure to start Spurious stop	Mechanical failure Power supply I&C failure Component cooling failure Maintenance Alignment error	EFW (ECC) train *i* unavailable for coolant injection
EFW*i*0VM02 (ECC*i*0VM02)	Failure to open Spurious closure	Mechanical failure Power supply I&C failure Maintenance Alignment error	Train *i* unavailable for coolant injection
EFW*i*0VC01 (ECC*i*0VC01)	Failure to open Spurious closure	Mechanical failure	Train *i* unavailable for coolant injection
ADS	Failure to depressurize the primary circuit		ECC cannot inject water to RPV
ADS valve line *j* (8 valve lines)	Failure to open		Valve line unavailable for depressurization
ADS*i*0VS01, VS02	Failure to open	Mechanical failure Power supply I&C failure Operator error	Valve line unavailable for depressurization

I&C system failure modes

Complete failures of RPS and DPS are not meaningful failure modes to be considered, but the relevant failure modes of I&C can be analysed from the actuator failure modes point of view (see Table A-10). Therefore in practice, the failure modes of RPS and DPS are either failure on demand or spurious actuation of critical RPS- and DPS-signals for the actuators.

For instance, the relevant I&C failure modes related to the pump EFW*i*0PM01 are

- failure to start on DEFW1 signal
  - failure-on-demand to actuate DSS04-signal
  - failure-on-demand to actuate DI000-signal
- spurious stop on DEFW2 signal
  - spurious actuation of DH00*i*-signal.

The next step is to analyse which I&C units can contribute to these failure modes, in other words a failure analysis in the I&C unit level.

I&C unit failure modes

As an example, the failure modes related to the pump EFW*i*0PM01 are analysed.

Voting units are assumed to fail to provide EFW1 and EFW2 signal if power supply fails or if there is an internal I&C unit failure (i.e. the default value is 0). At loss of communication between VU and APU due to detected failure in the APU, EFW1 will fail to activate in a 3/4 condition and EFW2 will activate spuriously in an 2/4 condition.

In case of APU safety functions, detected failures of DI000 and DSS04 input signals from measurements or from other APU:s cause an actuation (i.e. the default value is 1) in an 2/4 condition. Internal I&C unit failures are analysed in the module level.

Table A-6. Failure modes and causes of the I&C units.

Unit	**Failure modes**	**Failure causes**
VU	Failure to actuate EFW1 to EFW*i*0PM001	VU internal failure - undetected failure - detected failure Power supply failure No EFW actuation signal from APU:s (3-o-o-4)
	Spurious stop signal EFW2 to EFW*i*0PM001	VU failure causing spurious signal - detected failure VU-APU communication link failure - detected failure Spurious stop signal from APU:s (2-o-o-4)
APU	No EFW1 actuation signals from APU	APU internal failure - undetected failure Failure of DI000 and DSS04
	Failure to actuate DI000	Failure of DI002
	Failure to actuate DI002	Failure of DI002 actuation from APU:s (3-o-o-4) - undetected failure Failure of measurements for I002 - undetected failure
	Failure to actuate DSS04	Failure of DSS04 actuation from APU:s (3-o-o-4) - undetected failure Failure of measurements for SS04 - undetected failure
	Spurious DH00*i*	APU internal failure - detected failure APU-APU communication link failure Failure of DH00*i* actuation from APU:s (3-o-o-4) - detected failure Failure of measurements for DH00*i* - undetected failure - detected failure

Single I&C unit failure is typically not critical but a CCF is required to have an effect on safety functions. This is analysed in Table 7.

Table A-7. Failure effects of I&C units on front line safety systems.

I&C unit failure (RPD/DPS)	**Safety system failure effect**		
	EFW (DPS)	**ADS (RPS)**	**ECC (RPS)**
VU failure detected or undetected	no start	-	no start
CCF between communication links APU-VU 2/4 detected	spurious close of valves	-	-
3/4 detected	no start, spurious close of valves	-	-
CCF between APU:s 1/4 detected	-	no open of 2 valves	-
1/4 undetected	-	no open of 2 valves	-
2/4 detected	spurious close of valves	no open of 4 valves	-
2/4 undetected	-	no open of 4 valves	-
3/4 detected	no start, spurious close of valves	no open of 6 valves	no start
3/4 undetected	no start	no open of 6 valves	no start
4/4 detected	no start, spurious close of valves	no open of 8 valves	no start
4/4 undetected	no start	no open of 8 valves	no start
CCF between communication links APU-APU 12/12 detected	no start, spurious close of valves	no open of 8 valves	no start
MU failure Detected or undetected	-	no manual open	-
CCF between communication links MU-APU Detected or undetected	-	no manual open	-

Hardware modules and failure modes

The hardware modules of an I&C unit are presented in Figure A-4. The hardware modules and corresponding basic failure modes that are included in the example PSA model are presented in Table A-8.

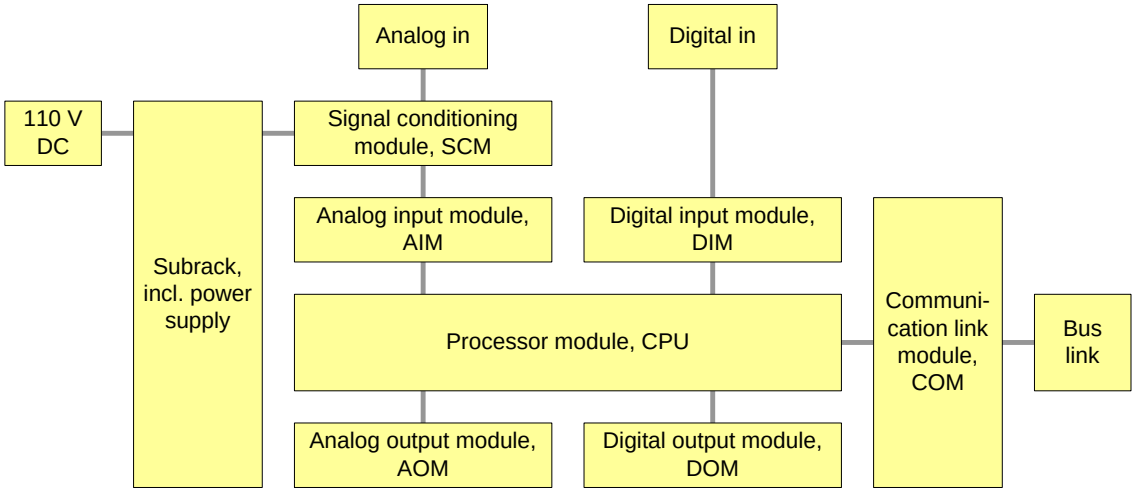

Figure A-4. Modules included in the example PSA I&C unit.

Table A-8. Hardware modules and basic failure modes.

Hardware component	**Failure mode**
Processor module	Hang
	Communication dropout
	Delayed signal
	Random behaviour
Analog input module	Signal fails high/low
	Signal drifts
	Signal hangs/freezes
Digital input module	Signals stuck to current value
Digital output module	Signals stuck to current value
Communication module	Failure to establish communication
Backplane	Loss of backplane
Power supply	Interruption
	Short circuit
	Ground contact
Measurement	Fails high
	Fails low
	Drift of value
	Freeze of value

Software failure modes

Assumed software failure modes for the example PSA are presented in Table A-9.

Table A-9. Assumed software failure modes for digital I&C units.

	SW fault location									
End effect	**SyS**	**EF (in APU)**	**APU-FRS**	**APU-AS**	**Propr. SW**	**VU-FRS**	**VU-AS**	**EF (in VU)**	**DCS**	**DLC**
FF-1SS			4a	4a		4b	4b			
FF-1D-1SS										
FF-allSS										
1APU			3a	3a		3b	3b			
MxU-1SS										
1SS	2a	2a	2a		2a	2a	2a	2a	2b	2b
MAPU-AllSS										
1SS-APU										
SYSTEM	1	1			1	1	1	1	1	

1 Failure cases are represented in the Fault Trees by SyS failure etc., both subsystems are failing, i.e. RPS and DPS.

2a Failure cases are represented in the Fault Trees by SyS failure etc.

2b Failure cases are represented in the Fault Trees by DLC failure.

3a Failure cases are represented in Fault tress by APU-AS/FRS failures.

3b Failure cases are represented in Fault tress by VU-AS/FRS failures.

4a Failure cases are represented in the Fault Trees by APU-AS/FRS failure. One of the functions in one subsystem is failing. Two common cause failure modes are possible: Failure of actuation or spurious function.

4b Failure cases are represented in the Fault Trees by VU-AS/FRS failure. One of the functions in one subsystem is failing. Two common cause failure modes are possible: Failure of actuation or spurious function.

Assumed software basic events for the example PSA are presented in table A-10. Basic events leading to the same end effect have been merged together. Common cause failure is assumed between application software basic events based on (practically) identical software modules in RPS and DPS.

Table A-10. Assumed software fault basic events (i = division 1, 2, 3 or 4).

CCF software group	Failed func. or I&C unit	Failure modes description	Fault cases	Uncovering situation	FTD APU	FTD VU
RPS/DPS-CCF_SW1	SyS	Complete CCF covering faults in SyS of both subsystem. Fatal failure.	1	Online Detection	Outputs to 0	Outputs to 0
RPS-CCF_SW2A DPS-CCF_SW2A	APU & VU	All APU and VU fails due to a failure of an common SW module. Fatal failure.	2a	Online Detection	Outputs to 0	Outputs to 0
RPS-CCF_SW2B DPS-CCF_SW2B	DCS or DLC	All communication fails due to a failure of an common SW module. Fatal failure.	2b	Online Detection	DFLT-values	DFLT-values
RPS-CCF_SW3A DPS-CCF_SW3A	APU	Loss of all functions in APU due to failure of SW module. Fatal failure.	3a	Online Detection	DFLT-values	-
RPS-CCF_SW3B DPS-CCF_SW3B	VU	Loss of all functions in VU due to failure of SW module. Fatal failure.	3b	Online Detection	-	Outputs to 0
RPS-CCF_SW4A_ADS1	RADS1	Failure to actuate RADS1 due to failure of SW module. Non-fatal failure.	4a	Latent revealed by demand	No	-
RPS-CCF_SW4A_H00*i* DPS-CCF_SW4A_H00*i*	RH00*i* DH00*i*	Spurious actuation xH00i due to failure of SW module. Non-fatal failure.	4a	Spurious effect	No	-
RPS-CCF_SW4A_I002 DPS-CCF_SW4A_I002	RI002 DI002	Failure to actuate xI002 due to failure of SW module. Non-fatal failure.	4a	Latent revealed by demand	No	-
RPS-CCF_SW4A_I005 DPS-CCF_SW4A_I005	RI005 DI005	Failure to actuate xI005 due to failure of SW module. Non-fatal failure.	4a	Latent revealed by demand	No	-
RPS-CCF_SW4A_M005	RM005	Spurious actuation RM005 due to failure of SW module. Non-fatal failure.	4a	Spurious effect	No	-
RPS-CCF_SW4A_SS04 DPS-CCF_SW4A_SS04	RSS04 DSS04	Failure to actuate xSS04 due to failure of SW module. Non-fatal failure.	4a	Latent revealed by demand	No	-
RPS-CCF_SW4A_SS05 DPS-CCF_SW4A_SS05	RSS05 DSS05	Spurious actuation xSS05 due to failure of SW module. Non-fatal failure.	4a	Spurious effect	No	-
RPS-CCF_SW4A_SS12 DPS-CCF_SW4A_SS12	RSS12 DSS12	Failure to actuate xSS12 due to failure of SW module. Non-fatal failure.	4a	Latent revealed by demand	No	-
RPS-CCF_SW4A_SS13	RSS13	Failure to actuate RSS13 due to failure of SW module. Non-fatal failure.	4a	Latent revealed by demand	No	-
RPS-CCF_SW4A_TB01	RTB01	Failure to actuate RTB01 due to failure of SW module. Non-fatal failure.	4a	Latent revealed by demand	No	-

CCF software group	Failed func. or I&C unit	Failure modes description	Fault cases	Uncovering situation	FTD APU	FTD VU
RPS-CCF_SW4A_TB02	RTB02	Failure to actuate RTB02 due to failure of SW module. Non-fatal failure.	4a	Latent revealed by demand	No	-
RPS-CCF_SW4A_TB03	RTB03	Failure to actuate RTB03 due to failure of SW module. Non-fatal failure.	4a	Latent revealed by demand	No	-
DPS-CCF_SW4A_X001	DX001	Failure to actuate DX001 due to failure of SW module. Non-fatal failure.	4a	Latent revealed by demand	No	-
RPS-CCF_SW4A_X003	RX003	Failure to actuate RX003 due to failure of SW module. Non-fatal failure.	4a	Latent revealed by demand	No	-
RPS-CCF_SW4A_ZS00*i* DPS-CCF_SW4A_ZS00*i*	RZ00*i* DZ00*i*	Failure to actuate xZ00i due to failure of SW module. Non-fatal failure.	4a	Latent revealed by demand	No	-
RPS-CCF_SW4B_ACP1 DPS-CCF_SW4B_ACP1	RACP1 DACP1	Failure to actuate xACP1 due to failure of SW module. Non-fatal failure.	4b	Latent revealed by demand	-	No
RPS-CCF_SW4B_CCW1	RCCW1	Failure to actuate RCCW1 due to failure of SW module. Non-fatal failure.	4b	Latent revealed by demand	-	No
RPS-CCF_SW4B_ECC1	RECC1	Failure to actuate RECC1 due to failure of SW module. Non-fatal failure.	4b	Latent revealed by demand	-	No
RPS-CCF_SW4B_ECC2	RECC2	Spurious actuation RECC2 due to failure of SW module. Non-fatal failure.	4b	Spurious effect	-	No
RPS-CCF_SW4B_MFW1	RMFW1	Failure to actuate RMFW1 due to failure of SW module. Non-fatal failure.	4b	Latent revealed by demand	-	No
RPS-CCF_SW4B_MFW2	RMFW2	Spurious actuation RMFW2 due to failure of SW module. Non-fatal failure.	4b	Spurious effect	-	No
RPS-CCF_SW4B_RHR1	RRHR1	Failure to actuate RRHR1 due to failure of SW module. Non-fatal failure.	4b	Latent revealed by demand	-	No
DPS-CCF_SW4B_EFW1	DEFW1	Failure to actuate DEFW1 due to failure of SW module. Non-fatal failure.	4b	Latent revealed by demand	-	No
DPS-CCF_SW4B_EFW2	DEFW2	Spurious actuation DEFW2 due to failure of SW module. Non-fatal failure.	4b	Spurious effect	-	No
DPS-CCF_SW4B_EFW3	DEFW3	Failure to actuate DEFW3 due to failure of SW module. Non-fatal failure.	4b	Latent revealed by demand	-	No
DPS-CCF_SW4B_EFW4	DEFW4	Spurious actuation DEFW4 due to failure of SW module. Non-fatal failure.	4b	Spurious effect	-	No

Failure data

- Safety system equipment
- Generic data (T-book)
- IE frequencies
- Assumed based on Nordic operating experience
- Digital I&C hardware
- Fictive data, engineering judgement, see Table A-11
- Digital I&C hardware CCF
- Generic data (NUREG/CR-5496) , see Table A-12
- Digital I&C software
- Assumed based on engineering judgement [13], see Table A-13

Table A-11. Assumed hardware failure rates for digital I&C units.

I&C modules		**Failure rate Total**	**Detection coverage**	**Rate undetected failures**	**Rate detected failures**
Type	**Description**	[/h]	[%]	[/h]	[/h]
CPU[1]	Processor module	2,0E-6	99%	2,0E-8	2,0E-6
COM	Communication link module	7,5E-6	100%	0,0E+0	7,5E-6
DIM	Digital input module	1,7E-6	75%	4,2E-7	1,3E-6
DOM	Digital output module	4,4E-6	91%	4,0E-7	4,0E-6
AIM	Analog input module	2,3E-6	65%	7,9E-7	1,5E-6
AOM	Analog output module	4,0E-6	87%	5,3E-7	3,5E-6
SUR	Subrack incl. power supply	1,0E-5	100%	0,0E+0	1,0E-5

I&C units[2]		**Failure rate Total**	**Detection coverage**	**Rate undetected failures**	**Rate detected failures**
Type	**Description**	[/h]	[%]	[/h]	[/h]
APU	Acquisition and processing unit	2,6E-5	95%	1,2E-6	2,5E-5
VU	Voting unit	2,4E-5	98%	4,2E-7	2,3E-5
MU	Manual control unit	2,1E-5	98%	4,4E-7	2,1E-5

I&C modules[3]		**#Items in I&C Unit**		
Type	**Description**	APU	VU	MU
CPU	Processor module	1	1	1
COM	Communication link module	8	4	4
DIM	Digital input module	0	0	1
DOM	Digital output module	3	4	0
AIM	Analog input module	6	0	0
AOM	Analog output module	0	0	0
SCM	Signal conditioning module	0	0	0
SUR	Subrack incl. power supply	1	1	1

[1] Includes two processors for data processing and communication
[2] Failure rates includes 1 of each relevant module
[3] Number of items equals the number modelled items at the module level

Table A-12. Assumed CCF parameters for hardware modules.

Failure Mode	**Alpha 2/3**	**Alpha 2/4**	**Alpha 3/3**	**Alpha 3/4**	**Alpha 4/4**
Detected Failure	5,0E-2	5,0E-2	1,0E-2	1,0E-2	1,0E-3
Undetected Failure	5,0E-2	5,0E-2	1,0E-2	1,0E-2	1,0E-3

Table A-13. Assumed CCF failure data for software modules [13].

SW failure end effect	**SW CCF Case**	**Probability**
SYSTEM: Loss of both subsystems, fatal CCF	1	1,0E-7
1SS: Loss of one subsystem, fatal CCF	2a	1,0E-6
1SS: Loss of DCUs in one subsystem, fatal CCF	2b	1,0E-5
APU-1SS/VU-1SS: Loss of redundant APUs/VUs in one subsystem, fatal CCF	3	1,0E-6

FF-1SS: Failure of one (or more) application function (Spurious actuation or Failure to actuate), fault in AS module causing a non-fatal CCF	4a, 4b	1,0E-5

Bibliographic Data Sheet **NKS-302**

Title	Guidelines for reliability analysis of digital systems in PSA context — Phase 4 Status Report
Author(s)	[1]Stefan Authén, [1]Jan-Erik Holmberg, [1]Linda Lanner, [2]Tero Tyrväinen
Affiliation(s)	[1]Risk Pilot AB, Sweden, [2]VTT, Finland
ISBN	978-87-7893-378-2
Date	March, 2014
Project	NKS-R DIGREL (Contract: AFT/NKS-R(13)86/3)
No. of pages	60
No. of tables	11+13
No. of illustrations	4+4
No. of references	24

Abstract
max. 2000 characters

DIGREL develops practical guidelines for analysis and modelling of digital systems in probabilistic safety assessment (PSA) for nuclear power plants. The project consists of three interrelated activities. A taxonomy for failure modes of digital I&C systems has been developed by a task group of OECD/NEA Working Group RISK. In the parallel Nordic activity, a fictive digital I&C PSA-model has been developed for the demonstration and testing of modelling approaches. The third activity has been to develop a method for the quantification of software reliability in the context of PSA, which is reported in another publication.

The failure modes taxonomy is based on a failure propagation model and a definition of five levels of abstraction: 1) system, 2) division, 3) I&C unit, 4) I&C unit module, 5) basic component. The failure propagation model constitutes of the following elements: fault location, failure mode, uncovering situation, failure effect and the end effect.

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. I&C unit-level and module-level modelling were compared. Modelling on the I&C unit level of abstraction can result in large conservatisms that may produce misleading results e.g. regarding dominating core damage sequences and significance of I&C failure modes. Both undetected and detected failures contribute significantly to the PSA result, indifferently of the assumed fault tolerant design.

Two different modelling approaches were compared. In RiskSpectrum the system failure logic is represented by graphical fault trees while in FinPSA a so called communication network representation was applied. Same minimal cut sets were obtained except some differences in CCF calculations and truncation of minimal cut sets with small probabilities.

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