NKS-277
ISBN 978-87-7893-352-2

Guidelines for reliability analysis of digital systems in PSA context — Phase 3 Status Report

Stefan Authén[1]

Jan-Erik Holmberg[2]

[1]Risk Pilot AB, Sweden

[2]VTT, Finland

March 2013

Abstract

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 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.

This an interim report of the project. A draft guidelines document on the failure modes taxonomy has been developed. The taxonomy is rather complete covering all levels from the system level down to module and basic component level failure modes, including hardware and software aspects. There are still open issues to be resolved by the task group, especially related to I&C unit and module level taxonomy.

In a parallel Nordic activity, a comparison of Nordic experiences and a literature review on main international references has been performed. 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. An existing simplified PSA model has been complemented with fault tree models for a four-redundant distributed protection system in order to study and demonstrate the effect of design features and modelling approaches. The model has been used to test the effect of CCF modelling, fail-safe principle and voting logic. A comparison has been made between unit-level and module-level modelling.

Key words

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

NKS-277
ISBN 978-87-7893-352-2

Electronic report, March 2013
NKS Secretariat
P.O. Box 49
DK - 4000 Roskilde, Denmark
Phone +45 4677 4041
www.nks.org
e-mail nks@nks.org

NKS-277
ISBN 978-87-7893-352-2

Guidelines for reliability analysis of digital systems in PSA context

Phase 3 Status Report

Stefan Authen[1]
Jan-Erik Holmberg[2]

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

March 2013

Table of contents

Tables

Figures

Abbreviations

A/D	Analog/digital
ACP	AC power system
AIM	Analog input module
ALOCA	Large loss-of-coolant accident
AOM	Analog output module
APU	Acquistion and processing unit
CCF	Common cause failure
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	Depressurisation valve system
ECC	Emergency core cooling system
EDF	Électricité de France
EFW	Emergency feedwater system
ENEL	Ente Nazionale per l'Energia eLettrica, Italy
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 insitute of technology in Stockholm
LMFW	Loss of main feedwater
LOCA	Loss-of-coolant accident
LOOP	Loss-of-offsite power
MCR	Main control room

MFW	Main feedwater system
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
SAFIR	Finnish Research Programme on Nuclear Power Plant Safety
SCM	Signal conditioning module
SWS	Service water system
TXP	Teleperm XP (now SPPA T2000), product of Siemens AG
TXS	Teleperm XS, product of AREVA
V&V	Verification and validation
VEIKI	Institute for Electric Power Research, Hungary
VTT	Technical Research Centre of Finland
WGRISK	OECD/NEA CSNI Working Group on Risk Assessment

Summary

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

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, 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 (report NKS-261). The model was used to test the effect of CCF modelling, fail-safe principle and voting logic.

In 2012, a draft guidelines document on the failure modes taxonomy has been developed by the WGRISK/DIGREL task group. The taxonomy is rather complete covering all levels from the system level down to module and basic component level failure modes, including hardware and software aspects. There are still open issues to be resolved by the task group, especially related to I&C unit and module level taxonomy. Also the the approach to handle software faults needs to be agreed on. The example PSA-model has been expanded to represent a plant with four redundant front line safety systems and a diversified reactor protection system. A comparison has been made between unit-level and module-level modelling.

Acknowledgements

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

1 Introduction

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

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

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

DIGREL task 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 includes hardware and software related failure modes, for which purpose example taxonomies have been collected. A representative fictive digital protection system example has been developed to be used as a reference in the application and demonstration of the taxonomy.

This report presents the *interim* results from the WGRISK and Nordic activities. The presented taxonmies and suggested definitions should be considered preliminary proposals and not as a PSA community consensus thoughts. The status of WGRISK/DIGREL activities has been presented 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 this 2012 interim report, the failure modes taxonomy and the example PSA model have been developed further. Chapter 2 summarises the objectives of the project. Chapter 3 gives an overview to the international WGRISK/DIGREL task group activity

[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.

on failure modes taxonomy. Chapter 4 lists a number of essential definitions used in the project. Chapter 5 describes a failure modes taxonomy for digital I&C systems. In chapter 6, the modelling aspects are discussed, including the application of the taxonomy. Chapter 7 provides a summary of state-of-the art regarding failure data for digital systems. Chapter 8 outlines next actions in the project, and chapter 9 concludes the report. In the appendix, the example PSA model and the underlying fictive nuclear power plant with digital reactor protection system are described.

2 Scope and objectives

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

1. Develop a taxonomy of hardware and software failure modes of digital components for common use
2. Develop guidelines regarding level of detail in system analysis and screening of components, failure modes and dependencies
3. Develop approach for modelling of common cause failures (CCF) between components, including software.
4. Develop an approach for modelling and quantification of software. This objective will be addressed in 2013–14.

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

3 WGRISK task group DIGREL

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

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

- To develop technically sound and feasible failure modes taxonomy (or taxonomies if needed to address variations in 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 (but not limited to):

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

There are many different digital I&C failure mode taxonomies. An activity focused on development of a common taxonomy of failure modes was seen as an important first step towards standardised digital I&C reliability assessment techniques for PSA. Needs from PSA guides the work, meaning e.g. that the (digital) system and its failures are studied from their functional significance point of view. This 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 define a structure for data collection. The results of the activity can be directly used in the review of PSA studies.

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

A series of working meetings have been organised to develop best practice guidelines on the topic, to share information and to plan future activities. Public seminars have been organised annually [12, 13].

A final draft will be prepared for WGRISK in 2013. After that the guidelines shall go through an external review and then the acceptance steps of WGRISK, CSNI Programme Review Group and the CSNI itself.

The following organisations form presently (January 2013) the task group, being responsible for planning and organisation of work meetings and preparation of the best practice guidelines: VTT, Finland (leader); Risk Pilot, Sweden; IRSN, France; EDF, France; AREVA, France; GRS, Germany; KAERI, Korea; NRC, USA; Ohio State University, USA; NRI, Czech; JNES, Japan; VEIKI, Hungary; ENEL, Italy; NRG, the Netherlands; RELKO, Slovakia and CSNC, Canada.

The task has relation at least to the following projects:

- OECD/NEA 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".

4 General approach for the development of the taxonomy

4.1 Definitions

Defect: The following definition is specific to software: An incorrect step, process, or data definition in a computer program (called also software development or implementation error).

Detected failure: a failure detected by (quasi-) continuous means, e.g. on line 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 [17].

There are two categories of detection mechanisms:

- On line detection mechanisms. Covers various continuous detection mechanisms.
- Off line 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 [18]; “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 [14]. "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 (IEC 60812, “of the system” removed).

Failure mode: the physical or functional manifestation of a failure [14].

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 ([15]; “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 [18].

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 Non-plausible Behaviour:** An external observer can decide that the I&C unit or the hardware module has failed. The unit is still 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 [15].

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

4.2 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 details in the fault tree modelling can be kept in a high level as long as relevant dependencies are captured and reliability data can be found.

4.3 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.

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

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

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

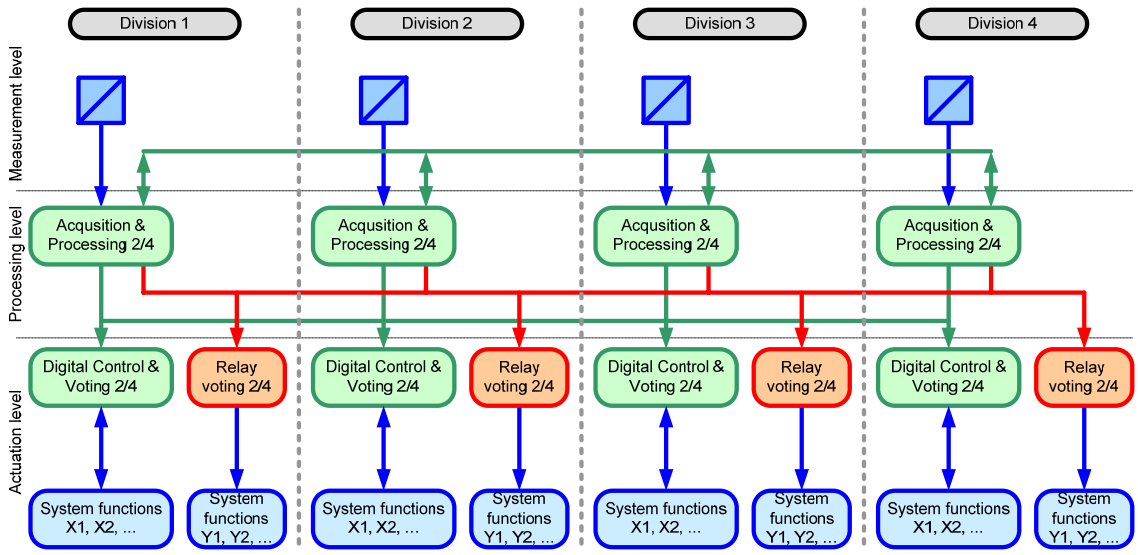

Figure 1. Example of a four-redundant digital I&C protection system architecture.

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

4.4 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 detail 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 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. Plausibility arguments have also been used to exclude some failure modes.

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 have 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 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/conditions, e.g.
  - Be a feasible analysis for PSA experts to perform.
  - Possible to implement into existing tools
  - Possible to review by a PSA-expert
  - Allows living PSA, e.g. possible to maintain and update with reasonable resources
  - Available and maintainable failure data, i.e., allows collection and evaluation of operational events
  - 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, dynamic self-test, open circuit monitoring, cross channel comparison etc., while a small part only will be detected by periodic tests or actual need of the equipment. 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 coverages) need to accurately capture the fault tolerant features.

4.5 Levels of details

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

The taxonomies are based on the generic digital I&C architecture and hardware configuration presented in chapter 4 together with corresponding general approach and assumptions. The taxonomies are also based on the collected taxonomies [7].

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 group of divisions controlling a same actuator(s) is a train. 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. Failure modes of all software belonging to a single division can be defined at this level as division level failure modes.
- 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 treated as an individual component like the microprocessor of a module (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. The software that runs on a microprocessor may be complicated enough such that it can be further decomposed, to a so-called sub-module level.

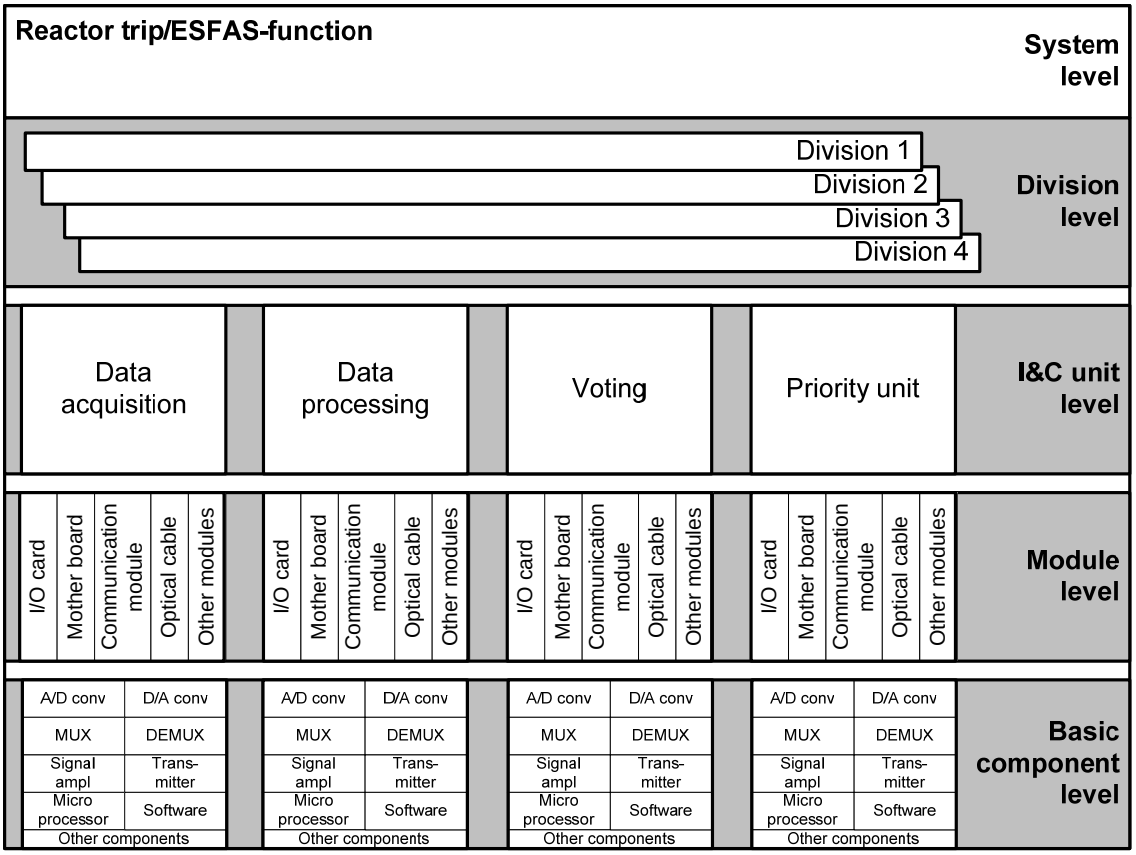

Figure 2. Principal structuring of safety I&C into different levels of details.

Table 1. Software modules in I&C units.

Unit	Software modules
I&C unit • Acquisition and processing unit (APU) • Voting unit (VU)	• Operating system • Application specific software • Elementary functions
Data communication unit	• Operating system • Data communication software • Data link configuration

5 Failure modes taxonomy

5.1 Basic principles

This chapter describes an “analytical failure modes taxonomy” which 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. In chapter 6, a simpler taxonomy is provided based on the fault tree modelling approach.

The main approach is to define failure modes hierarchically and functionally. Hierarchical approch 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 detail 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 hardware failure mode taxonomy is developed for the two lowest levels of detail (modules and basic component level).

For the software failure mode taxonomy a “software fault scope” analysis based approach is proposed. This approach is based on identifying critical software modules (Table 1) and associated fault scopes (which are common cause failures) given a fault in the software module (see ch. 5.3.2).

It is important to note that the software failure mode taxonomy is actually referring to the systematic faults in that part of the system where the safety functions are designed and implemented. In this report, a distributed microprocessor-based protection system is assumed, meaning that systematic faults appear in software. If the protection system is based on hard-wired technology or FPGA:s (field programmable gates), systematic faults should be considered for the hardware design in similar manner.

5.2 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.

5.3 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?
- Generic failure mode type:
    - 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, non-plausible behaviour (generation of outputs continues, an external observer can decide that the I&C unit or the hardware module has failed).
- Detection 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.
    - Revealed only by demand. The fault remains undetected and failure cannot be detected by periodic testing.
    - Spurious effect. Detection by plant behaviour. This may be consequence of a failure detected by online detection.

The combination of fault location, local effect, detection 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 local effects and detection situations.

	Detection Situation			
Local effect	Online detection	Offline detection	Spurious effect	Latent, revealed by demand
Fatal, ordered	**R**	LNR	**R**	LNR
Fatal, haphazard	PNR	PNR	PNR	PNR
Non-fatal, plausible behaviour	LNR	**R**	**R**	**R**
Non-fatal, non-plausible behaviour	**R**	LNR	**R**	**R**

R: Combination relevant for further analysis of end effects
LNR: Combination not relevant for the analysis of the effects. Non-relevance is due to logical considerations. For example, a failure detected by continuous detection has not to be considered in combination with the periodic texting.
PNR: Combination practically not relevant, due to a very low likelihood, compared to other likelihoods (for example haphazard fatal failure of a protection system).

First the combinations of local effect and detection 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 non-plausible 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 extens, including CCF between diverse systems, the system architecture shown in Figure 3 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 here we assume that there can be more than one APU/VU per each subsystem and division.

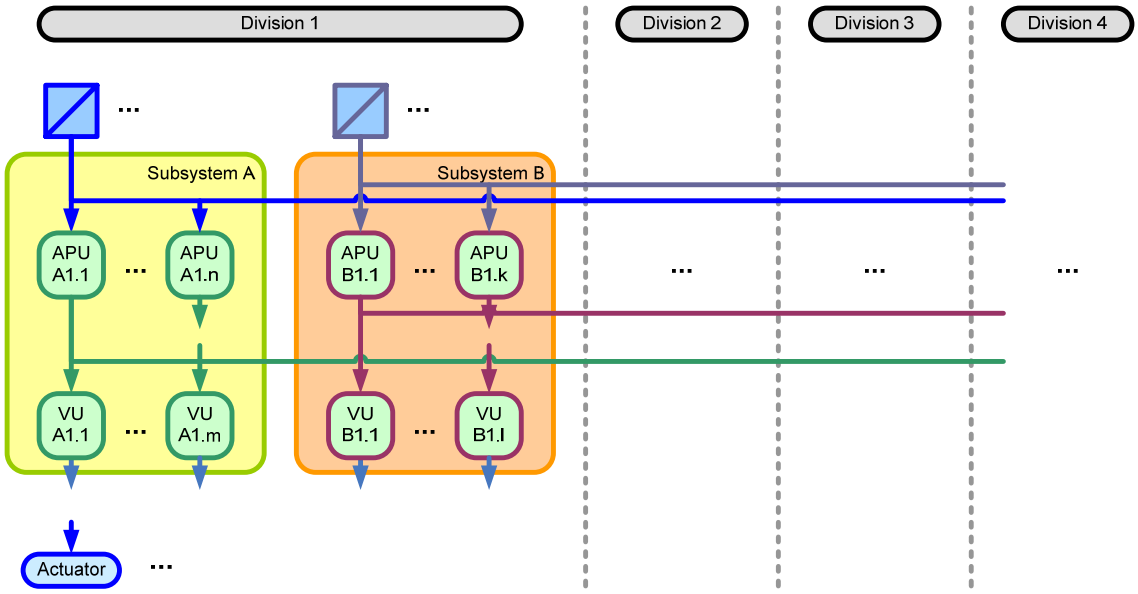

Figure 3. Example I&C system architecture.

In the above I&C architecture, the following failure extents can be assumed

- Only one I&C unit is affected. This is usually only relevant for hardware modules failures
- One set of redundant APU:s/VU:s is affected (i.e., one APU/VU per division)
- Multiple sets of redundant APU:s/VU:s in one subsystem are affected. This can be relevant for some specific software fault (i.e., more than one APU/VU per division)
- Multiple sets of redundant APU:s/VU:s in both subsystems are affected. This can be relevant for some specific software fault
- One subsystem is affected
- One subsystem and one or more sets of redundant APU:s in the other subsystem are affected
- Both subsystems are affected.

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

5.3.1 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 mode type	Detection situation	Functional impact
Processor module	Hang	Fatal, ordered	Online detection[1]	Loss of all APU/VU functions
	Communication dropout	Non-fatal, non-plausible	Online detection	Loss of all APU/VU functions
	Delayed signal	Non-fatal, plausible	Offline detection[2]	Loss of all APU/VU functions
	Random behaviour	Non-fatal, plausible	Offline detection[2]	Loss of all APU/VU functions
		Non-fatal, non-plausible	Online detection	Loss of all APU/VU functions
			Spurious effect	Spurious APU/VU function(s)
Analog input module	Signal fails high/low	Non-fatal, non-plausible	Online detection[3]	Loss of all module application functions
	Signal drifts	Non-fatal, non-plausible	Online detection	Loss of all module application functions
	Signal hangs/freeze	Non-fatal, plausible	Offline detection[2]	Loss of all module application functions
		Non-fatal, non-plausible	Online detection	Loss of all module application functions
Digital input module, single channel	Signal stuck to current value	Non-fatal, plausible	Offline detection[2]	Loss of specific module application function
		Non-fatal, non-plausible	Online detection	Loss of specific module application function
	Signal fails to opposite state	Non-fatal, non-plausible	Spurious effect	Spurious module application function
Digital output module, single channel	Signal stuck to current value	Non-fatal, non-plausible	Online detection	Loss of specific module application function
		Non-fatal, plausible	Offline detection[2]	Loss of specific module application function
	Signal fails to opposite state	Non-fatal, non-plausible	Spurious effect	Spurious module application function

[1] Detected by monitoring functions in the next level of I&C-units, i.e. units communicating with the faulty unit
[2] Tech.Spec. periodic tests
[3] Detected by the self-monitoring functions implemented in the module, or by monitoring mechanisms, provided by controlling modules

5.3.2 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 are considered:

- Operating system (OS).
- Elementary functions (EFs). There is one such module per EF. A virtual EF could be created for each hardware module for which one wants to consider failures due to its software and / or hardware design.
- 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.

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:

- Functions failure in one division and one subsystem (FF-1D-1SS): this extent applies to non-common cause, non-fatal software failures of I&C functions without vote.
- Functions failure in one subsystem (FF-1SS): 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.
- Functions failure in both subsystems (FF-2SS): this extent applies to non-fatal software failures that result in the misbehaviour of I&C functions in both subsystems. As in the previous case, the I&C functions that are dependent on the failed functions could also fail.
- Loss of one set of redundant APU:s (1APU): this extent applies to fatal software failures affecting only one set of redundant APU:s (necessarily in the same subsystem).
- Loss of multiple sets of redundant APU:s in one subsystem (MAPU-1SS): this extent applies to fatal software failures affecting multiple sets of redundant APU:s in the same subsystem.
- Loss of multiple sets of redundant APU:s in both subsystems (MAPU-2SS): this extent applies to fatal software failures affecting multiple sets of redundant APU:s in the two subsystems.
- Loss of one subsystem (1SS).
- Loss of one Subsystem and of one or more sets of redundant APU:s in the other subsystem (1SS-APU).
- Loss of both subsystems (SYSTEM).

Table 4. Maximum failure extent of a postulated software fault in a software modules.

Extent	OS	EF	APU-FRS	APU-AS	VU-FRS	VU-AS	DCS	DLC
FF-1D-1SS	✓	✓	✓	✓				
FF-1SS	✓	✓	✓	✓	✓	✓		
FF-2SS	✓	✓	??		??			
1APU	✓	✓	?	✓				
MAPU-1SS	✓	✓						
MAPU-2SS	✓	✓						
1SS	✓	?	?		?	✓	✓	✓
1SS-APU	✓	?						
SYSTEM	✓	?					✓	

✓ = postulated software fault possible
? = uncertain if the postulated software fault is possible (it may be possible to screen out the software fault)

?? = depends on the level of diversity between the subsystems. If both subsystems use same FRS for some parts, CCF over the subsystems may be possible.

For most application I&C functions implemented by the APU:s, the VU:s will perform a vote to reduce the potential for spurious actuation and provide protection against random failures. For such functions, only CCF involving multiple divisions will have system/subsystem consequences. Voting is feasible mainly for functions where the output is a single, latched Boolean signal. Functions with more complex outputs, like for example diesel load sequencers, are not subject to vote and need to be considered regardless of their potential for CCF.

5.4 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).

6 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. The demonstration will at this stage be limited to the hardware taxonomy, while the software taxonomy will be demonstrated in the next project phase.

Another purpose of this chapter is to address the different challenges in performing a reliability model of a digital 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 has 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 [16]. The example was based on Risk Spectrum example model (EXPSA). The model has during 2012 been further developed in order to better describe a generic BWR NPP. 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 software
    - Modelling of CCF.

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 of chapter 5 does not exclude the use of other tools than fault tree/event tree analysis.

6.1 Taxonomy for PSA modelling

Chapter 5 presents generic failure mode taxonomies at different level of details. The required level of detail 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 detail, why a high level of detail is required in the example PSA. Hence, the failure mode taxonomy for the module level will be applied for the example PSA.

As mentioned initially in chapter 5, the taxonomies presented are of an “analytical” nature and the chapter 5 taxonomy for the module level will in most cases be of unneccassary high level of detail to apply in a PSA model. The high level of detail 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 (for reference see Table 2).

From the PSA modelling perspective, it is more beneficial to define the failure modes by functional effect rather than local 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 stucture 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 accordingingly. 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 mode types according to the failure modes taxonomy at the module level (Table 3) is assigned to the basic failure modes of the digital RPS example system hardware modules presented in Appendix A, see Table A-9. Then the means of detection and local functional impact can be defined for the example system.
2. Generic failure modes describing the functional impact on I&C unit level are defined based on the local functional impact and means of detection for the basic failure modes. The generic failure modes distinguish between failures detected by the fault tolerant design (detected failures) and failures that are not (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, makes it 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 a I&C module that have the same attributes for generic 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 Components	Failure Mode Examples	Failure Mode Type	Failure Mode Detection	Local Functional Impact
Processor module	Hang	Fatal, ordered	Online Detection	Loss of all APU/VU functions
	Communication dropout	Non fatal, non-plausible	Online Detection	Loss of all APU/VU functions
	Delayed signal	Non fatal, plausible	Latent revealed by demand	Loss of all APU/VU functions
	Random behaviour	Non fatal, plausible	Latent revealed by demand	Loss of all APU/VU functions
	"	Non fatal, non-plausible	Online Detection	Loss of all APU/VU functions
	"	"	Spurious effect	Spurious APU/VU function(s)
Analog Input Module	Signal fails high/low	Non fatal, non-plausible	Online Detection	Loss of all Module Application Functions
	Signal drifts	Non fatal, non-plausible	Online Detection	Loss of all Module Application Functions
	Signal hangs/freeze	Non fatal, plausible	Latent revealed by demand	Loss of all Module Application Functions
	"	Non fatal, non-plausible	Online Detection	Loss of all Module Application Functions
Digital Input Module	Signals stuck to current value	Non fatal, non-plausible	Online Detection	Loss of all Module Application Functions
	"	Non fatal, plausible	Latent revealed by demand	Loss of all Module Application Functions
Digital Output Module	Signals stuck to current value	Non fatal, non-plausible	Online Detection	Loss of all Module Application Functions
	"	Non fatal, plausible	Latent revealed by demand	Loss of all Module Application Functions
Communication module	Failure to establish communication	Non fatal, non-plausible	Online Detection	Loss of specific APU/VU Application Functions
Backplane	Loss of backplane	Fatal, ordered	Online Detection	Loss of all APU/VU functions
Power supply	Interruption	Fatal, ordered	Online Detection	Loss of all APU/VU functions
	Short circuit	Fatal, ordered	Online Detection	Loss of all APU/VU functions
	Ground contact	Fatal, ordered	Online Detection	Loss of all APU/VU functions
Measurement	Fails high	Non fatal, non-plausible	Online Detection	Loss of specific Module Application Function
	Fails low	Non fatal, non-plausible	Online Detection	Loss of specific Module Application Function
	Drift of value	Non fatal, non-plausible	Online Detection	Loss of specific Module Application Function
	Freeze of value	Non fatal, plausible	Latent revealed by demand	Loss of specific Module Application Function
Offline detection not considered here since it is only relevant with regard to unavailability due to corrective maintenance				

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

Hardware Components	Failure Mode Detection	Local Functional Impact	Generic Failure Modes	Generic Failure Detection	Failure End Effect (RT or ESFAS)
Processor module	Online Detection	Loss of all APU/VU functions	Loss of function	Monitoring[1]	All APU/VU outputs acc. to FTD
	Online Detection	Loss of all APU/VU functions	Loss of function	Monitoring	All APU/VU outputs acc. to FTD
	Latent revealed by demand	Loss of all APU/VU functions	Latent loss of function	Periodic test[2]	Loss of all APU/VU outputs
	Latent revealed by demand	Loss of all APU/VU functions	Latent loss of function	Periodic test[2]	Loss of all APU/VU outputs
	Online Detection	Loss of all APU/VU functions	Loss of function	Monitoring	All APU/VU outputs acc. to FTD
	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 APU/VU outputs acc. to FTD
	Online Detection	Loss of all Module Application Functions	Loss of function	Self-Monitoring	1oo4 conditions of specific 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
	Online Detection	Loss of all Module Application Functions	Loss of function	Self-Monitoring	1oo4 conditions of specific APU/VU outputs acc. to FTD
Digital Input Module	Online Detection	Loss of all Module Application Functions	Loss of function	Self-Monitoring	1oo4 conditions of specific 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 Output Module	Online Detection	Loss of all Module Application Functions	Loss of function	Self-Monitoring	Specific APU/VU outputs acc. to FTD
	Latent revealed by demand	Loss of all Module Application Functions	Latent loss of function	Periodic test	Loss of specific APU/VU outputs
Communication module	Online Detection	Loss of specific APU/VU Application Functions	Loss of function	Self-Monitoring	1oo4 conditions of specific APU/VU outputs acc. to FTD
Backplane	Online Detection	Loss of all APU/VU functions	Loss of function	Monitoring	All APU/VU outputs acc. to FTD
Power supply	Online Detection	Loss of all APU/VU functions	Loss of function	Monitoring	All APU/VU outputs acc. to FTD
	Online Detection	Loss of all APU/VU functions	Loss of function	Monitoring	All APU/VU outputs acc. to FTD
	Online Detection	Loss of all APU/VU functions	Loss of function	Monitoring	All APU/VU outputs acc. to FTD
Measurement	Online Detection	Loss of specific Module Application Function	Loss of function	Monitoring	1oo4 conditions of specific APU/VU outputs acc. to FTD
	Online Detection	Loss of specific Module Application Function	Loss of function	Monitoring	1oo4 conditions of specific APU/VU outputs acc. to FTD
	Online Detection	Loss of specific Module Application Function	Loss of function	Monitoring	1oo4 conditions of specific APU/VU outputs acc. to FTD
	Latent revealed by demand	Loss of specific Module Application Function	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]Tech.Spec periodic tests

[3]Detected by the self- monitoring functions implemented in the module, or by monitoring mechanisms, provided by controlling modules

FTD: Fault Tolerant Design

Offline detection 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 Components	Generic Failure Modes	Generic Failure Detection	Failure End Effect (RT or ESFAS)
Processor module	Loss of function	Monitoring[1]	All APU/VU outputs 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 APU/VU outputs acc. to FTD
	Latent loss of function	Periodic test	Loss of 1oo4 conditions of specific APU/VU outputs
Digital Input Module	Loss of function	Self-Monitoring	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
Digital Output Module	Loss of function	Self-Monitoring	Specific APU/VU outputs acc. to FTD
	Latent loss of function	Periodic test	Loss of specific APU/VU outputs
Communication module	Loss of function	Self-Monitoring	1oo4 conditions of specific APU/VU outputs acc. to FTD
Backplane	Loss of function	Monitoring	All APU/VU outputs acc. to FTD
Power supply	Loss of function	Monitoring	All APU/VU outputs acc. to FTD
Measurement	Loss of function	Monitoring	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]Tech.Spec periodic tests

[3]Detected by the self- monitoring functions implemented in the module, or by monitoring mechanisms, provided by controlling modules

FTD: Fault Tolerant Design

Offline detection not considered here since it is only relevant with regard to unavailability due to corrective maintenance

6.2 PSA model structure

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.

In order to achieve this, a number of new standardized fault tree types have been created. Table 8 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 voting 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 8. 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	The FT models basic events for mechanical component failures and functional dependencies by transfers to FT:s for e.g. Actuator Signal and power supply
Actuator Signal	The FT models signal dependencies for specific component failure mode by transfers to FT:s for 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 modeled by basic events and failure of Voting Unit by transfer to VU fault tree page.
RPS Actuatation 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. Transfers are made to FT:s of RPS Protection Functions and to FT:s for failures in communication between VU:s and APU:s.
RPS Protection function[2]	The FT models failure in the accuisition and processing of process measurements into RPS Protection Functions, and signal exchange of these values between APU:s. Transfers are made to FT:s of Process Measurement and APU to APU communication failures. Transfer may also be modeled 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 modeling failure of the communication module by a basic event 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 modeling failure of the communication module by a basic event and failure of sending APU by transfer to specific APU FT.
Process Measurement[1]	The FT models failure in the Process Measurements and the accuisition 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, and voltage supply failure by a FT transfer.
Voting Unit, VU[1]	The FT models failure of VU processor and subrack by basic events, 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, digital I&C has been developed by applying the fault tree structure of Table 8. 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. The developed I&C model follows a generic coding system for fault trees and events.

6.3 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 as mentioned in section 6. 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 adressed in this project phase are:

- Hardware failure modes
  - Relative importance of digital I&C modules and 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.

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

6.3.1 Hardware failure modes

The fault tree model has been developed at module level of detail 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 a more than 8 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). At 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 where 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. This stresses the importance of *not* excluding detected failures from the reliability model.

6.3.2 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 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 modeled at module level. All other basic events at the module level receive a failure probability of 0.

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.

There are several different approaches that may be chosen for this task, whereof the three most obvious ones are described here:

1. Calculate the sum of failure rates and failure probabilities for all modules of the I&C unit. This approach will include modules that are critical as well as non-critical for the actuator signals under consideration, e.g. input and output modules. The result will be a highly conservative failure probability of the I&C unit that will have a large impact on the reliability of actuator signals and on the probability for spurious signals.
2. Identify the I&C modules that are required for performing the specific actuations modeled in the PSA and calculate the sum of failure rates and failure probabilities for these. This approach will require extensive information regarding the I&C design, RPS safety functions and RPS actuation signals. The result will still be conservative since in reality only certain modules are required for certain functions and signals.
3. Calculate the sum of failure rates and failure probabilities for one piece of each module of the I&C unit. With this approach it will be assumed that only one specific I&C module, e.g. input module, will be required for a specific RPS safety function or actuator signal. This will in most cases be a non-conservative assumption since, e.g., safety functions often include several sub-conditions dependent on different input modules. It may however still produce conservative reliability estimates on system level since when modelling on I&C unit level, all RPS safety functions or RPS actuation signals in a given division will fail at the same time.

Test intervals for the calculation of failure probabilities of undetected failures may in the above cases either be conservatively chosen as the longest of the modules or as a calculated mean of the considered modules test interval. The first approach will produce very conservative results, while the second will require extensive input data and may be difficult to perform.

One important aspect to consider in the choice of approach is hence the amount and level of detail in system and design information necessary for the approach in relation to the purpose of the reliability model and the level of conservatism that can be accepted.

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, approach number 3 have been applied. 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 is compared to the results from the module level model, a CDF increase of a factor 2,5 is observed for the I&C unit level case.

The importance of the RPS and the DPS systems increases with a factor 10 and gains the highest fractional contributions among the modeled safety systems. The largest increase in importance is found for the undetected failures where the fractional contribution increases with a factor 50 while the increase for detected failures is a factor 2. At I&C unit level undetected failures also have a higher risk contribution than detected failures by a factor of 6, whereas in the module level of detail the detected

failures had a 8 times higher risk contribution than the undetected failures. This shows that the modelling at a higher level of detail may produce misleading results which in turn may lead to erronous risk informed decisions.

One reason for the large increase of undetected failures importance is due to that a test interval of 1 year is applied for the I&C unit, where in the module level of detail the test interval for digital outputs is assumed to 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, a factor of 8, can be found due to the simplifications of dependencies to input and output modules, but also communication modules, that are applied when modelling at I&C unit level.

The rather low increase of the detected failures importance 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 detail is negligeble, 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 have 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 cutset 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. Cutsets containing digital I&C have a low individual contribution to the top frequency and the highest contribution is given by cutsets resulting in loss of emergency feedwater due to loss of DPS actuator signals and loss of feedwater system due to spurious RPS isolation signals and loss of emergency core cooling system due to failure of the depressurisation signal. The contributing I&C events to these sequences are CCF:s containing detected failure of DPS subracks in combination with CCF:s of RPS subracks.

The cutset 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, the cutset list contains a large number of cutsets containing threefold CCF for undetected failure of RPS APU:s in combination with threefold CCF for undetected failure of DPS APU:s. 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 can not 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 approaches 1 and 2 for the I&C unit failure rate estimation would 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.

6.3.3 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 section 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 at detected failures only for the reactor scram safety function. For all the other safety functions a default value of 0 will be applied at detected failures, which means that no spurious signals can be caused by the digital I&C and detected failures will instead contribute to loss of actuator signals.

The evaluation shows a small decrease in the core damage frequency at the module level of detail, 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 due to that cutsets containing combinations of detected and undetected CCF events are no longer valid. The risk 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 detail 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 detail 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 detail, the I&C unit level of detail FC is a factor 100 higher.

6.3.4 Conclusions

The evaluation of the example PSA shows that both undetected and detected failures 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 detail 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 erronous risk informed decisions.

It should be noted that these conclusions are preliminary and further work and validation is planned during 2013. The received results is due to the specific design of

the example plant and example I&C system and also due to 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.

7 Failure data

7.1 Hardware reliability data

Usually, hardware failure data is provided by the vendor of the equipment. This is standard requirement in the contract between the utility and the vendor. The data provided by the supplier sets the limit for the detail of the PSA, i.e., it is not feasible to model in more detail due to lack of reliability data. Two kinds of failure data may provided by vendors: 1) based on operating experience, 2) based on a part counting method followed by a standard like Siemens SN 29500 [19] or generic data bases such as the reliability prediction database the Military Handbook for "Reliability Prediction of Electronic Equipment" (MIL-HDBK-217) [20]. MIL-HDBK-217 contains failure rate models for the various part types used in electronic systems, such as integrated circuits, transistors, diodes, resistors, capacitors, relays, switches, and connectors. These failure rate models are based on mathematical models derived from empirical field failure rates that are gathered for different parts and systems. Those models respect ambient conditions, level of stress, and type of applications.

Failure data is typically provided in terms of failure rate (1/time unit). From the PSA modelling point of view it is necessary to distinguish between detected and undetected failures, which depends on the failure detection features of the I&C units. The judgement of the share of detected vs. undetected failure rates needs to be provided by the vendor.

A second important reliability parameter needed for PSA is CCF failure rates. CCF parameters are sometimes derived from some generic values, but as an alternative IEC 61508-6 [15] has been used, e.g., in [21].

7.2 Software reliability data

Sophisticated software reliability estimation methods presented in the academic literature are not applied in real industrial PSAs. Instead, the numbers are some kind of engineering judgments for which justifications may be hard to find.The engineering judgement approaches can be divided into the following categories depending on the argumentation and evidence they use [22]:

- screening out approach
- screening value approach
- expert judgement approach
- operating experience approach.

The reliability model used for software failures is practically always the simple “probability of failure per demand”, denoted here by the parameter q.

Screening out approach means that software failures are screened out from the model. The main arguments to omit software are that 1) the contribution of software failures is

insignificant or that 2) no practical method to assess the probability of software failure (systematic failure).

Screening value approach means that some reliability number, like q = 1E-4, is chosen without detailed assessment of the reliability, and it is claimed that this is a conservative number for a software CCF. The screening value is taken from a reference like IEC 61226 [23]. Accordingly,the reference [24] states that reliability claims "q < 1E-4" for a single software based system important to safetyshall be treated with extreme caution. This derives partly due to the fact that demonstrating lower probabilities, e.g., by statistical testing is very laborious.

Expert judgement approach relies on the assessment of the features of the software system which are assumed to have correlation with the reliability. The two questions are 1) which features should be considered and 2) what is the correlation between the features and the reliability. This kind of approaches are used extensively in PSA, e.g., in human reliability analysis. Such models are difficult to validate.

Operating experience approach means an assessment based on operational data. In reality, operating experience approach is like the expert judgement approach since operational data need to be interpreted in some way to be used for reliability estimation. Especially if the reliability estimation is not carried out explicitly using well-defined data and reliability models.

Generally, only common cause failures are modelled in PSA. One reason for this is that there has not been a methodology available to correctly describe and incorporate software failures into a fault tree model.The only reliability model which is applied is constant unavailability (q) and this is used to represent the probability of CCF per demand. Spurious actuations due to software failures are not modelled or no need to consider software failure caused spurious actuations has been concluded.

Software CCF is usually understood as the application software CCF or its meaning has not been specified. Software CCF is generally modelled between processors performing redundant functions, having the same application software and on the same platform. One of the exceptions is the design phase PSA made for the automation renewal of the Loviisa NPP, where four different levels of software failures are considered: 1) single failure, 2) CCF of a single automation system, 3) CCF of programmed systems with same platforms and or software, and 4) CCF of programmed systems with different platforms and or software [22].

With regard to the reliability numbers used in PSA, it is difficult to trace back where they come from — even in the case of using operating experience. The references indicate the sort of engineering judgement but lacks supporting argumentation. To overcome the shortcomings of the present approaches for software failure rate estimation, an analytical approach is provided in [25].

8 Next steps

In 2013, the main activities will be to finalize the WGRISK guidelines and to work with software reliability modelling and quantification. The preliminary ideas to develop the approach to software reliability quantification are presented in papers [22, 25, 26].

In addition, the example PSA model will be developed further in order to match with the final guidelines on failure modes taxonomy and to test and demonstrate the software reliability quantification and modelling.

In 2014, the focus is on dissemination of results of previous years work.

Milestones 2013–14

Start	**1.1.2013**
T + 1 M	Kick-off meeting on software modelling and quantification
T + 3 M	WGRISK task group meeting and WGRISK annual meeting in Paris
T + 9 M	PSA2013 conference and tentative WGRISK task group meeting
T + 10 M	Final draft of the WGRISK guidelinessubmitted to external review
T + 11 M	NKS (Nordic) seminar on software modelling and quantification
T + 12 M	NKS report on software modelling and quantification
T + 14 M	Final WGRISK guidelines
T + 20 M	Final draft of the NKS report and seminar (covering all activities 2010–14)
T + 24 M	NKS final report on guidelines of reliability analysis of digital I&C systems in PSA

9 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 will set boundary conditions e.g. for the needed level of detail of hardware components and for the structure of the failure modes. The following overall requirements for the hardware taxonomy have been agreed upon:

- 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 details can be distinguished from the hardware point of view:

(1) the entire system

(2) a division

(3) processing units (and cabinets)

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

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

The evaluation of the example PSA have demonstrated the developed taxonomy and verified it is suitable for PSA purpose. The evaluation shows that the choice of level of detail for the modelling of digital I&C is of high importance for the results. The most suitable level of detail is found to be the “module level” which concur with the level of detail of the general PSA state of the art. The module level will make it feasible to perform, maintain and review a PSA of digital I&C with reasonable resources while capturing critical dependencies. It will also be possible to capture fault tolerant features of the digital system and the impact on the reliability of safety functions.

Modelling on the I&C unit level of detail 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 erronous risk informed decisions.

The evaluation of the example PSA also shows that both undetected and detected failures contributes 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.

It should be noted that the conclusions from the example PSA are preliminary and further work and validation is planned during 2013. The received results is due to the specific design of the example plant and example I&C system and also due to 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.

10 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, 25-29.6.2012, Helsinki, 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, 25-29.6.2012, Helsinki, 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, 25-29.6.2012, Helsinki, 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, 25-29.6.2012, Helsinki, 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. 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.
13. 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.
14. Software Engineering -- Software product Quality Requirements and Evaluation (SQuaRE) -- Guide to SQuaRE , ISO/IEC 25000:2005, ISO/IEC, Geneva, 2005.
15. 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.
16. Gustafsson, J. Reliability analysis of digital protection system of a nuclear power plant. Masters Thesis, KTH, Stockholm, May 2012.
17. Procedures for Performing a Failure Mode, Effects and Criticality Analysis, MIL STD 1629A, US Department of Defense, Washington D.C., 1984.
18. Systems and software engineering – Vocabulary. ISO/IEC/IEEE 24765:2010, International Electrotechnical Commission, Geneva, 2010.
19. Failure Rates of Components, SN 29500. Siemens AG, CT SR SI, Otto-Hahn-Ring 6, D-81739 Munich, Germany.
20. Reliability Prediction of Electronic Equipment, Notice 2, MIL-HDBK-217F(2), US Department of Defense, Washington D.C., 1995.
21. Authén, S., Wallgren, E., Eriksson, S., Development of the Ringhals 1 PSA with Regard to the Implementation of a Digital Reactor Protection System, 10th International Probabilistic Safety Assessment & Management Conference, PSAM 10, Seattle, Washington, June 7–11, 2010, paper 213.
22. Bäckström, O., Holmberg, J.-E. Use of IEC 61508 in Nuclear Applications Regarding Software Reliability, Proc. of 11th International Probabilistic Safety Assessment and Management Conference & The Annual European Safety and Reliability Conference, 25-29.6.2012, Helsinki, 10-Th2-4.
23. Nuclear power plants. Instrumentation and control important to safety. Classification of instrumentation and control functions, IEC 61226, Ed. 3.0, International Electrotechnical Commission, Geneva, 2009.
24. Licensing of safety critical software for nuclear reactors – Common position of seven European nuclear regulators and authorized technical support organisations. SSM Report 2010:01, Stockholm, January 2010.
25. Estimating Failure Rates in Highly Reliable Digital Systems. EPRI TR-1021077, Electric Power Research Institute, Inc., Palo Alto, CA (2010). Limited distribution.
26. Holmberg, J.-E., Bishop, P., Guerra, S., Thuy, N., Safety case framework to provide justifiable reliability numbers for software systems, Proc. of 11th International Probabilistic Safety Assessment and Management Conference & The Annual European Safety and Reliability Conference, 25-29.6.2012, Helsinki, 10-Th2-2.

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.

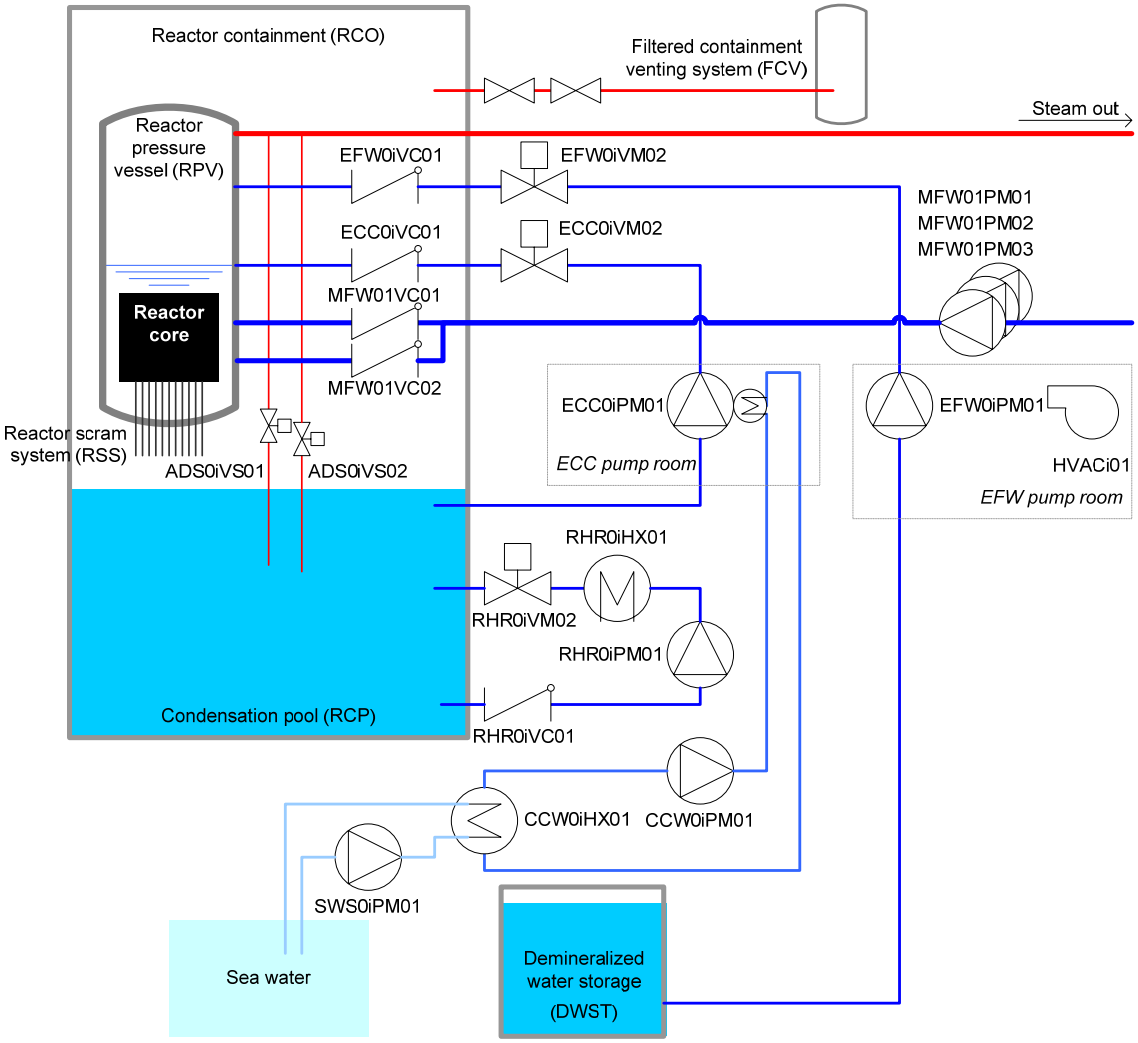

Figure A-1. Flow diagram of one train of the example NPP.

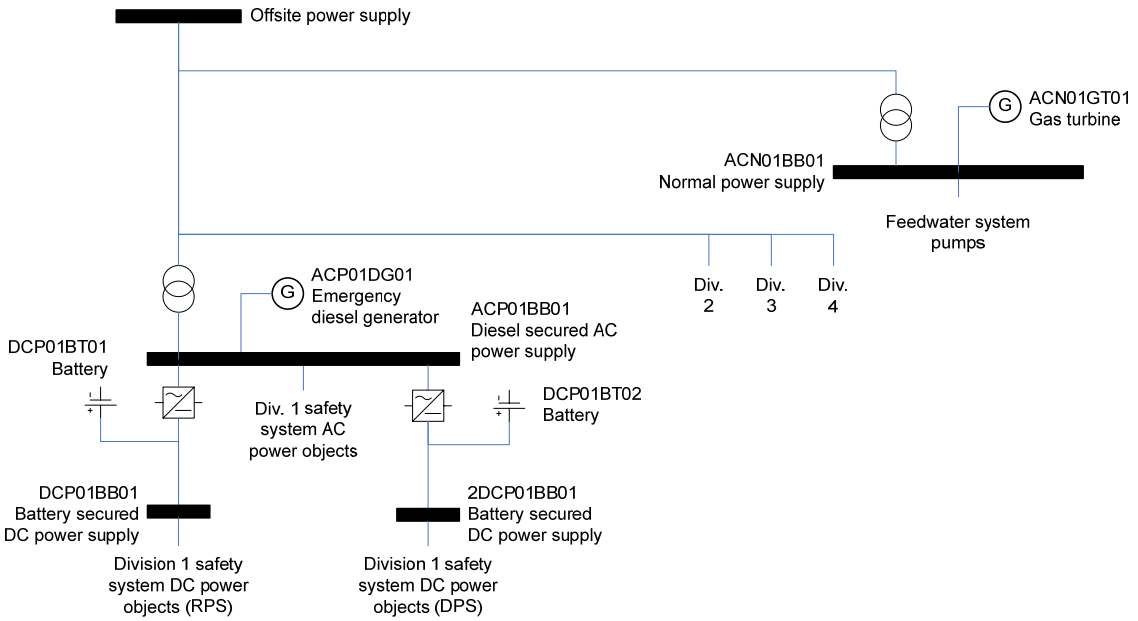

Figure A-2. Example NPP electric system line diagram.

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, abbreviated by MU. This I&C unit is relevant for the manual actuation of the primary circuit depressurization.

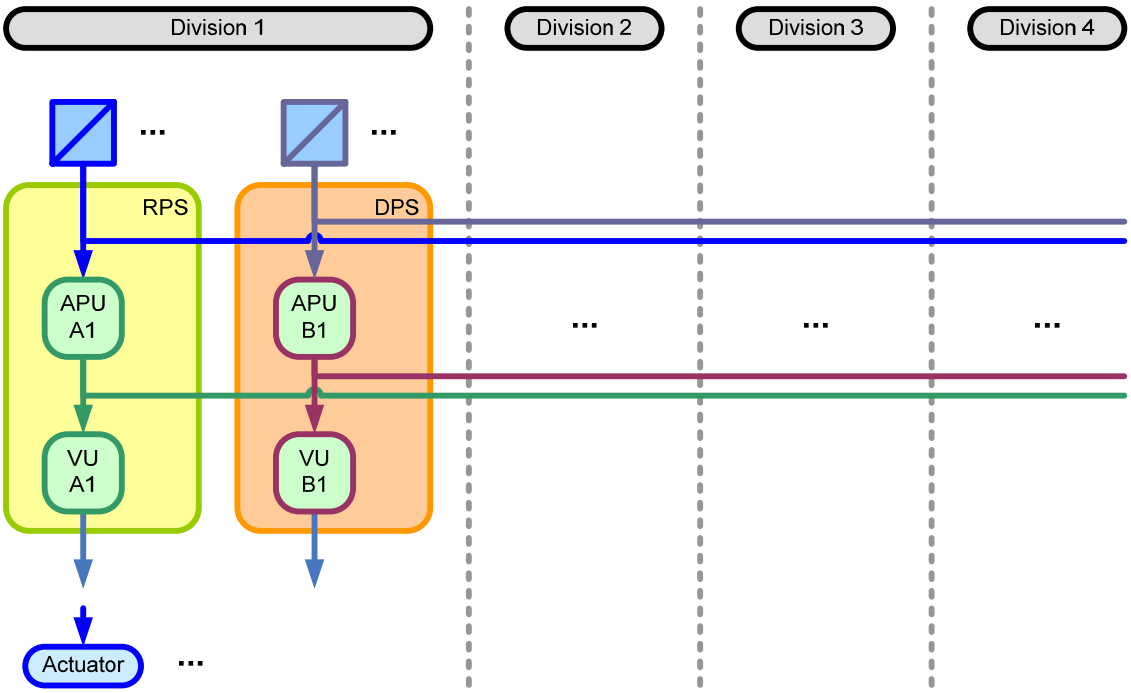

Figure A-3. I&C architecture.

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 is 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 actuations 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.

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 + RZ00i + DZ00i	0
		Stop	Manual stop and not active start signal	RACP2 + DACP1	NOT(RSS12 + RZ00i + DZ00i) * MAN-0iDG01	1
ADS	Pressure relief valve	Open	Depressurisation signal	–	RADS1 {RTB0}	0
		Close	Manual close and not active depressurisation signal	–	RADS2 {NOT(RTB00) * MAN-ADSi, i = 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-CCW0iPM01	1
ECC	Pump	Start	Containment isolation and no water leakage in the respective pump room	RECC1	NOT(RH00i) * RI000	0
		Stop	Water leakage in the respective pump room	RECC2	RH00i	0
ECC	Motor-operated valve	Open	Containment isolation and no water leakage in the respective pump room	RECC1	NOT(RH00i) * RI000	0
		Close	Water leakage in the respective pump room	RECC2	RH00i	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(DH00i) * (DM000 + DSS04 + DI000)	0
		Stop	Water leakage in the respective pump room	DEFW2	DH00i	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(DH00i) * (DSS04 + DX001 + DI002)	0
		Close	Water leakage in the respective pump room or very high water level in reactor	DEFW4	DH00i + DSS05	1
HVA	AC cooler	Start	Start EFW	DEFW1	NOT(DH00i) * (DM000 + DSS04 + DI000)	0
		Stop	Manually	DHVA1	MAN-HVA0iAC01	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-MFWi, i = 1, 2, 3	0
		Stop	Feedwater system isolation or very high water level in reactor	RMFW2	RM000 + 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-RHR0iPM01	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-RHR0iVM02	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-RHR0iVM02	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.

Signal	Description	Condition[1]	DFLT
RPS			
RH00i	Isolation of the ECC pump room i	ECCi0CL001-H1 + ECCi0CL002-H1	1
RI000	Containment isolation	2/4*(RI002-i + RI005-i)	1
RI002	Containment isolation due to extremly low level in RPV	2/4*(RPVi0CL002-L4)	1
RI005	Isolation due to high pressure in containment	2/4*(RCOi0CP001-H1)	1
RM000	Feedwater isolation	2/4*(RM005-i)	1
RM005	Feedwater isolation due to high temperature in feedwater system compartment	2/4*(MFWi0CT001-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*(RPVi0CL001-L2)	1
RSS05	Reactor scram due to high water level in RPV	2/4*(RPVi0CL001-H2)	1
RSS12	Reactor scram due to containment isolation (I- or M-isolation)	2/4*(RI000-i + RM000-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*(RPVi0CL002-L4)	0
RTB02	Depressurisation of the primary circuit condition 2: high pressure in containment (same as I005) or manual actuation	RTB03 + 2/4*(RCOi0CP001-H1)	0
RTB03	Manual TB	MAN-TB	0
RX003	High temperature in condensation pool	2/4*(RCOi0CT001-H1)	1
RZ00i	Low voltage in AC bus bar i	ACPi0CE001-L1	1
DPS			
DH00i	Isolation of the EFW pump room i	EFWi0CL001-H1 + EFWi0CL002-H1	1
DI000	Containment isolation	2/4*(DI002-i + DI005-i)	1
DI002	Containment isolation due to extremly low level in RPV	2/4*(RPVi0CL002-L4)	1
DI005	Isolation due to high pressure in containment	2/4*(RCOi0CP001-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*(RPVi0CL001-L2)	1
DSS05	Reactor scram due to high water level in RPV	2/4*(RPVi0CL001-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
DZ00i	Low voltage in AC bus bar i	ACPi0CE001-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.

Measurement	Component ID	Limit		Purpose	RPS	DPS
RPV water level, fine level	RPVi1CL001	L2	Low level	Core cooling protection	RSS04	
	RPVi2CL001	H2	Extra high level	RPV overfilling protection		DSS05
	RPVi2CL001	L2	Low level	Core cooling protection		DSS04
RPV water level, coarse level	RPVi1CL002	L4	Extremly low level	Core cooling protection	RI002 RTB01	
	RPVi2CL002	L3	Extra low level	Core cooling protection		DX001
	RPVi2CL002	L4	Extremly low level	Core cooling protection		DI002
Feedwater system pump suction pressure	MFWi0CP001	L1	Low pressure before feedwater pump	Loss of feedwater supervision		DSS13
Feedwater system room temperature	MFWi0CT001	H1	High room temperature	Leakage supervision		DM005
Containment pressure	RCOi1CP001	H1	High pressure in containment	Leakage supervision	RI005 RTB02	
	RCOi2CP001	H1	High pressure in containment	Leakage supervision		DI005
Condensation pool temperature	RCOi0CT001	H1	High temperature in condensation pool	Residual heat removal	RX003	
Water level in the ECC pump room	ECCi0CL001	H1	Water on the floor	Leakage supervision	RH00i	
Water level in the EFW pump room	EFWi0CL001	H1	Water on the floor	Leakage supervision		DH00i
AC power voltage bus bar ACP-i	ACPi1CE001	L1	Low voltage on bus bar ACP-i	Loss of offsite power supervision	RZ00i	
	ACPi2CE001	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* = train)	Failure modes	Failure cause	Failure effect
EFW (ECC)	Failure to provide coolant injection		No water to RPV
EFW train *I* (ECC train *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 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, which is 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 is presented in Figure A-4. The corresponding basic failure modes of individual hardware modules are presented in Table A-8.

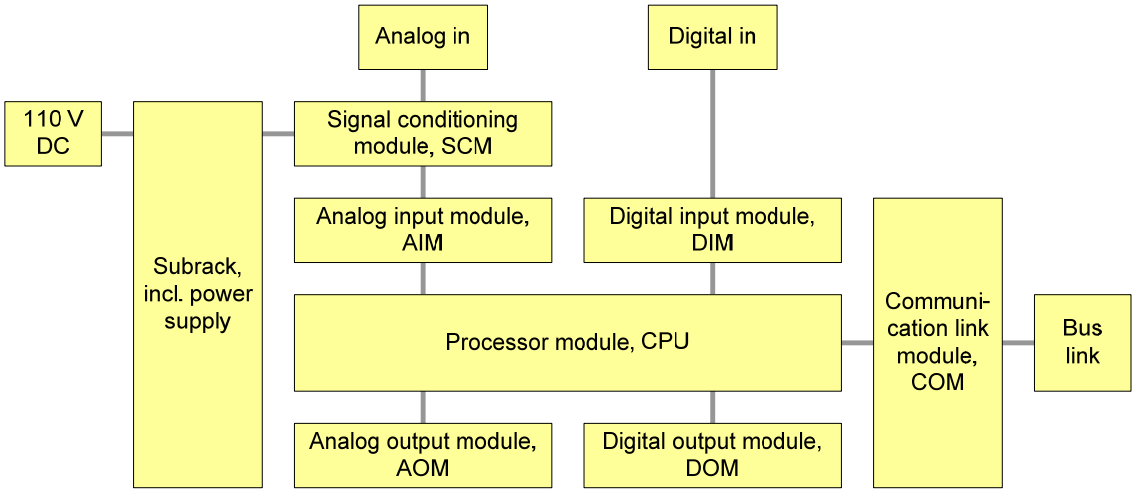

Figure A-4. Modules included in the example PSA I&C unit

Table A-8. Assumed hardware failure modes for digital I&C Units.

Hardware Components	Failure Modes
Processor module	Hang
	Communication dropout
	Delayed signal
	Random behaviour
Analog Input Module	Signal fails high/low
	Signal drifts
	Signal hangs/freeze
Analog Input Module, Single channel	Signal fails high/low
	Signal drifts
	Signal hangs/freeze
Analog Output Module	Signal fails high/low
	Signal drifts
	Signal hangs/freeze
Analog Output Module, Single channel	Signal fails high/low
	Signal drifts
	Signal hangs/freeze
Digital Input Module	Signals stuck to current value
Digital Input Module, Single channel	Signal stuck to current value
	Signal fails to opposite state
Digital Output Module	Signals stuck to current value
Digital Output Module, Single channel	Signal stuck to current value
	Signal fails to opposite state
Signal Conditioning Module	Signal fails high/low
	Signal drifts
	Signal hangs/freeze
Communication module	Failure to establish communication
Watch-Dog Timer	Fails to activate
	Activates without computer failure
Backplane	Loss of backplane
Power supply	Interruption
	Short circuit
	Ground contact
Measurement	Fails high
	Fails low
	Drift of value
	Freeze of value

The example PSA will in this project phase only consider the main modules of the I&C unit, i.e. modules necessary for the performance of several actuation signals. Hardware components only affecting the actuation signal of an individual actuation signal or safety system component will hence be neglected. This concerns failure of single channels of I/O modules and failure of signal conditioning module. Also, the reliability of the watch-dog timer is excluded from the analysis, as is analog output modules since no analog control signals has been defined for the example safety systems. These excluded components will be adressed for the example PSA model during the next project phase (2013).

The hardware modules and corresponding basic failure modes that are included in the example PSA model is presented in Table A-9.

Table A-9. Hardware modules and basic failure modes considered for digital I&C Units in the example PSA model.

Hardware Components	Failure Modes
Processor module	Hang
	Communication dropout
	Delayed signal
	Random behaviour
Analog Input Module	Signal fails high/low
	Signal drifts
	Signal hangs/freeze
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 digital I&C RPS is presented in table A-10. Software failure modes will however not be included in the example PSA model until next project phase (2013).

Table A-10. Assumed software failure modes for digital I&C Units.

	OS	EF	APU-FRS	APU-AS	VU-FRS	VU-AS	DCS	DLC
FF-1D-1SS	✓	✓	✓	✓				
FF-1SS	✓	✓	✓	✓	✓	✓		
FF-2SS	✓	✓						
1APU	✓	✓	?	✓				
MAPU-1SS	✓	✓						
MAPU-2SS	✓	✓						
1SS	✓	?	?		?	✓	✓	✓
1SS-APU	✓	?						
SYSTEM	✓	?					✓	

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
  - Fictive data, engineering judgement

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 paramaters for digital I&C units and 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

Title	Guidelines for reliability analysis of digital systems in PSA context — Phase 3 Status Report
Author(s)	Stefan Authén[1], Jan-Erik Holmberg[2]
Affiliation(s)	[1]Risk Pilot AB, Sweden, [2]VTT, Finland
ISBN	978-87-7893-352-2
Date	March 2013
Project	NKS-R / DIGREL
No. of pages	54
No. of tables	8 + 12
No. of illustrations	3 + 4
No. of references	26

Abstract

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 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.

This an interim report of the project. A draft guidelines document on the failure modes taxonomy has been developed. The taxonomy is rather complete covering all levels from the system level down to module and basic component level failure modes, including hardware and software aspects. There are still open issues to be resolved by the task group, especially related to I&C unit and module level taxonomy.

In a parallel Nordic activity, a comparison of Nordic experiences and a literature review on main international references has been performed. 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. An existing simplified PSA model has been complemented with fault tree models for a four-redundant distributed protection system in order to study and demonstrate the effect of design features and modelling approaches. The model has been used to test the effect of CCF modelling, fail-safe principle and voting logic. A comparison has been made between unit-level and module-level modelling.

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