Title	Development of best practice guidelines on failure modes taxonomy for reliability assessment of digital I&C systems for PSA
Author(s)	Holmberg, Jan-Erik; Authén, Stefan; Amri, Abdallah
Citation	11th International Probabilistic Safety Assessment and Management Conference & The Annual European Safety and Reliability Conference, pp. 10-TH4-1
Date	2012
Rights	Reprinted from 11th International Probabilistic Safety Assessment and Management Conference & The Annual European Safety and Reliability Conference. This article may be downloaded for personal use only

Development of best practice guidelines on failure modes taxonomy for reliability assessment of digital I&C systems for PSA

Jan-Erik Holmberg[a*], Stefan Authén[b], Abdallah Amri[c]
[a]VTT, Espoo, Finland
[b]Risk Pilot AB, Stockholm, Sweden
[c]OECD/NEA, Paris, France

Abstract: 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 the many unique attributes of digital systems, a number of modelling and data collection challenges exist, and consensus has not yet been reached. The OECD/NEA CSNI Working Group on Risk Assessment (WGRisk) has set up a task group called DIGREL to develop a taxonomy of failure modes of digital components for the purposes of probabilistic safety assessment (PSA). An activity focused on development of a common failure modes taxonomy is seen as a step towards standardised digital I&C reliability assessment techniques. 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 modelling and quantification efforts. It will also help to define a structure for data collection and to review PSA. DIGREL will take advantage from R&D activities, actual PSA applications as well as experience related to digital systems. The scope of the taxonomy includes both protection and control systems, though primary focus is on protection systems. The taxonomy is divided into hardware and software related failure modes, for which purpose example taxonomies have been collected from the member countries. A representative fictive digital protection system example has been developed to be used as a reference in the demonstration of the taxonomy. With regard to the hardware failure modes taxonomy, the main issue is to define a feasible level of details. Module level, i.e., subcomponents of processing units, seems to be the most appropriate from the PSA modelling point of view. The software failure modes taxonomy is focused on identifying and defining which common cause failures are reasonable to postulate. The plan is to publish guidelines in 2013.

Keywords: PRA, PSA, digital I&C, failure modes taxonomy

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 the 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 into a follow-up task group called DIGREL. This paper describes an overview of the DIGREL task and a preliminary outline of the taxonomy.

2. OVERVIEW OF THE DIGREL TASK

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

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

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

There exist many different digital I&C failure modes 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 will guide the work, meaning e.g. that the (digital) system and its failures are studied from their functional significance point of view. This is considered a meaningful way to approach the problem.

The taxonomy will be the basis of future modelling and quantification efforts. It will also help define a structure for data collection. The results of the activity can be directly used in the review of PSA studies. The activity takes advantage from recent and on-going R&D activities carried out in the 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 comparison of failure modes taxonomies has been made in 2011 [3].

A series of working meetings have been and will be organised in order to develop best practice guidelines on the topic, to share information and to plan future activities. For instance, in 2011, two workshops were organised. A public seminar was organised in connection to the second workshop in October 2011 [4]. The aim is to prepare the draft guidelines by the end of 2012. A final draft will be prepared for WGRISK in the beginning of 2013. After that the guidelines shall go through the acceptance steps of WGRISK, PRG and CSNI.

The following organisations form presently (January 2012) 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.

3. OUTLINE OF THE FAILURE MODES TAXONOMY

3.1. General approach

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.

From PSA point of view, failure modes taxonomy is applied in the systems analysis, including the performance of FMEA (failure modes and effects analysis) and the fault tree modelling. Systems analysis 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, the 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, 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.

In PSA, 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.

3.2. Types of digital I&C systems

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

Protection systems 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 software packages 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.

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

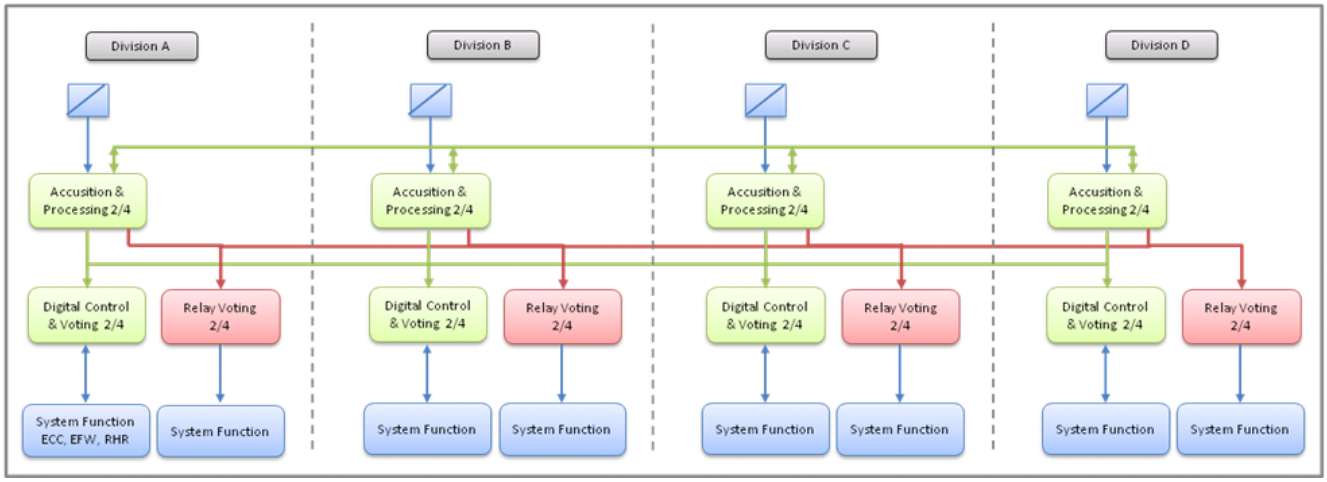

Figure 1. Example of the architecture of a digital I&C protection system

3.3. Levels of details

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

(1) the entire system
(2) a division
(3) processing units (and cabinets)
(4) modules, i.e. subcomponents of processing units
(5) generic components, i.e. subcomponents of modules.

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

The reactor protection system consists of redundant divisions that provide inputs to voting modules that determine if an actuation signal should be generated. The divisions may be of the same or different architectures but in general all perform the same functions. Each division comprises an entity from power supply and physical separation point of view, although some cross-connections of power supply between divisions may be applied for certain components. From the PSA modelling point of view, a usual simplification is to assume a loss of complete division in case of a hazard affecting the division. Loss of AC or DC power supply is also division wide functional failures to be considered in PSA.

Each division consists of one or more processing units and data buses between them. Processing units may be dedicated to data acquisition, processing, voting and actuator control. In Figure 1, each division has two processing units: an acquisition & processing unit (APU) and a digital control & voting unit (DCV). Processing units may be sometimes doubled (within each division) to increase the availability of the system. Processing units are installed in cabinets, each of which has a specific power supply route and condition monitoring. Cabinet level is the most detailed level from the power supply and room dependency point of view.

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

Modules and channels are the most detailed level from the hardware functional dependency point of view. Also the software components can be associated with the modules.

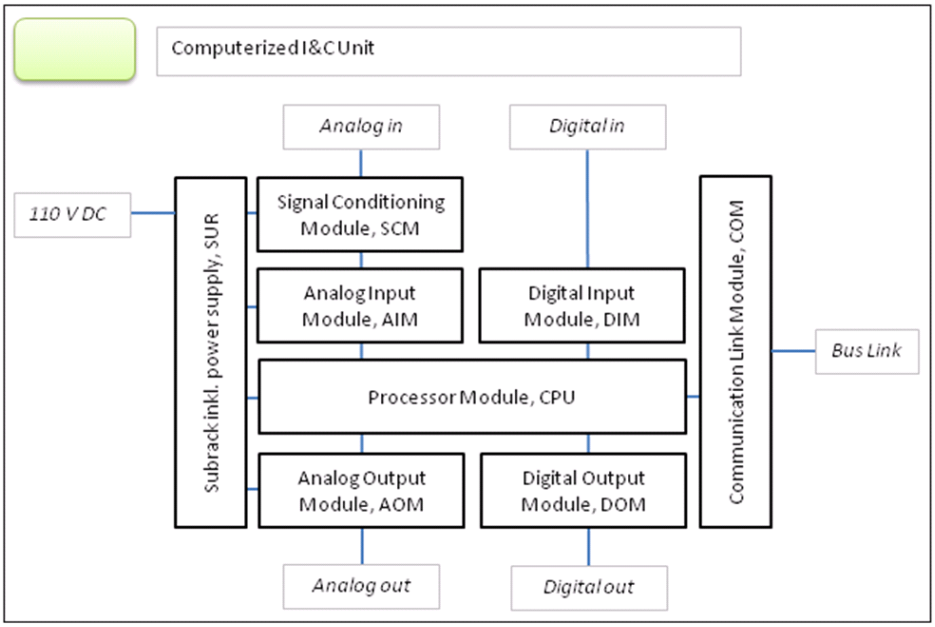

Figure 2. Example of modules included in a computerized I&C unit

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

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

3.3. Requirements for the taxonomy

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

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

Same requirements can be applied to software failure modes, too.

With regard to the hardware failure modes taxonomy, module level seems to be the most appropriate from the PSA modelling point of view. The module level concurs with the level of detail of general PSA state of the art and it will make it feasible to perform, maintain and review a PSA of digital I&C with reasonable resources while capturing critical dependencies. It will also be possible to capture fault tolerant features of the digital system and the impact on the reliability of safety functions.

The software failure modes taxonomy is still an open issue. From PSA point of view a set of principally critical failure events associated with software faults can be defined. It is for the I&C experts to judge which of the failure events, being typically common cause failures (CCF), that are reasonable to postulate.

3.4. Hardware failure modes taxonomy

The hardware taxonomy failure modes can either be based on a function view or a component view. The function view considers component failures with regard to their impact on the function that the component supports, e.g. “loss of function to actuate”, while the component view is more descriptive and considers component failures with regard to the manifestation of the failure within the component, e.g. “freeze of value” or “set point corrupted”.

From the PSA point of view it is desirable to group failure modes with regard to their functional consequence to as high extent as possible, in order to simplify the fault tree analysis. See also the pre-study report [2], taxonomy comparison [3] and the DIGREL seminar 2011 [4] for examples of failure modes used in practice. At generic level, the two main failure modes are:

- Loss of function, loss of communication, no actuation signal when demanded
- Spurious function, spurious actuation signal.

If applicable other failure modes, such as erratic output, may be considered, but in practical PSA applications it may be difficult to consider more ambiguous events than “failure to actuate” or “spurious actuation”.

Failure detection is an important aspect of the failure mode. Firstly, failure detection determines the choice of the component reliability model (constant unavailability, monitored, repairable, standby component). Secondly — specifically for I&C systems — failure detection is a relevant attribute from the failure effect point of view. Detected failure may cause a spurious actuation signal or change the voting logic, depending on the design. To accurately model the effect of detected failures may be a laborious task in practice, but failure detection should be analysed and considered at least in FMEA. The following categories of failure detection are possible:

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

Development of the hardware failure modes taxonomy in DIGREL is further discussed in [5].

3.5. Software failure modes taxonomy

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

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

The PSA perspective follows the functions of the system, e.g., RPS, and considers the critical failure modes of the system. Knowing the functions of a processing unit, the following possible functional failure modes may be considered:

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

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

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

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

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

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

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

Development of the software failure modes taxonomy in DIGREL is further discussed in [6].

4. CONCLUSION

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 the many unique attributes of digital systems, a number of modelling and data collection challenges exist, and consensus has not yet been reached.

An activity focused on development of a common taxonomy of failure modes is 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 of PSA studies.

The scope of the taxonomy will include both protection and control systems of a nuclear power plant, though primary focus is on protection systems. The taxonomy is divided into hardware and software related failure modes, for which purpose example taxonomies have been collected from the member countries. A representative fictive digital protection system example has been developed to be used as a reference in the application and demonstration of the taxonomy.

With regard to the hardware failure modes taxonomy, the main issue is to define a feasible level of details. Module level, i.e. subcomponents of processing units, seems to be the most appropriate from the PSA modelling point of view. The software failure modes taxonomy is focused on identifying and defining which common cause failures are reasonable to postulate.

Acknowledgements

Contributions from the WGRISK/DIGREL task group members are acknowledged. The Finnish and Swedish 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.

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] Chu, T-L, Yue, M. A Comparison of Taxonomies of Digital System Failure Modes. 11th International Probabilistic Safety Assessment & Management Conference, PSAM 11, Helsinki, June 25–29, 2012.

[4] 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.

[5] Authén, S., Piljugin, E. Proposal for the Taxonomy of Failure Modes of Digital System Hardware for PSA. 11th International Probabilistic Safety Assessment & Management Conference, PSAM 11, Helsinki, June 25–29, 2012.

[6] Smidts, C., Kim, M.C. Identification of Failure Modes of Software in Safety-Critical Digital I&C Systems in Nuclear Power Plants. 11th International Probabilistic Safety Assessment & Management Conference, PSAM 11, Helsinki, June 25–29, 2012.