OECD/NEA WGRISK task on failure modes taxonomy for digital I&C – DIGREL

Abdallah Amri[a], Stefan Authén[b], Herve Bruneliere[c], Gilles Deleuze[d], Gabriel Georgescu[e], Jan-Erik Holmberg[f*], Man Cheol Kim[g], Keisuke Kondo[h], Ming Li[i], Ewgenij Piljugin[j], Wietske Postma[k], Jiri Sedlak[l], Carol Smidts[m], Jan Stiller[j], and Nguyen Thuy[d]

[a]OECD/NEA, Paris, France
[b]Risk Pilot AB, Stockholm, Sweden
[c]AREVA, Paris, France
[d]EDF R&D, Paris, France
[e]Institut de Radioprotection et de Sûreté Nucléaire, Paris, France
[f]Risk Pilot AB, Espoo Finland
[g]Chung-Ang University, Seoul, Korea
[h]Nuclear Regulation Authority, Japan
[i]United States Nuclear Regulatory Commission, USA
[j]Gesellschaft für Anlagen- und Reaktorsicherheit, Germany
[k]Nuclear Research and consultancy Group, the Netherlands
[l]ÚJV Řež, Husinec - Řež, Czech Republic
[m]Ohio State University, USA

Abstract: The OECD/NEA CSNI Working Group on Risk Assessment (WGRisk) has set up a task group called DIGREL to develop a taxonomy of failure modes of digital components for the purposes of probabilistic risk analysis (PRA). The failure modes taxonomy is based on a failure propagation model and a definition of five levels of abstraction: 1) system level, 2) division level, 3) I&C unit level, 4) I&C unit modules level, 5) basic components level. This structure corresponds to a typical reactor protection system architecture. The failure propagation model consists of the following elements: fault location, failure mode, uncovering situation, failure effect and the end effect. These concepts are applied to define the relationship between a fault in hardware or software modules (module level failure modes) and the effect on I&C units (I&C unit level failure modes). The purpose of the taxonomy is to support PRA, and therefore focuses on high level functional aspects rather than low level structural aspects. This focus allows handling of the variability of failure modes and mechanisms of I&C components. It reduces the difficulties associated with the complex structural aspects of software in redundant distributed systems.

Keywords: Probabilistic risk analysis, digital I&C, failure mode, taxonomy

1. INTRODUCTION

Digital protection and control systems appear as upgrades in older Nuclear Power Plants (NPP), and are commonplace in new NPP. To assess the risk of NPP 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 (e.g., functions are implemented by software, units of the system interact in a communication network, faults can be identified and handled online), a number of modelling and data collection challenges exist, and international consensus on the reliability modelling 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

* jan-erik.holmberg@riskpilot.se

taxonomy of failure modes of digital components for the purposes of Probabilistic Risk Assessment (PRA) [1]. This resulted in a follow-up task group called DIGREL. 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 PRA. Standard technological equipment of NPP process systems, like pumps, are either in the running or standby mode. On the opposite, computer based systems are typically always in the running mode – the difference in the modes is that they process different sets of input parameters and consequently solve different branches of algorithms. The need of specific taxonomy establishment is hence obvious.

The paper will give an overview of the digital I&C failure modes taxonomy, which will be published as an OECD/NEA working report in 2014. Results presented here should be considered preliminary proposals and not as the task group consensus thoughts.

2. GENERAL APPROACH

2.1. Introduction

A failure modes taxonomy is a framework of describing, classifying and naming failure modes associated with a system. One of the main uses of digital I&C failure modes taxonomy is to support the performance of reliability analyses and to unify the operational experience data collection of digital I&C systems. In the work of the DIGREL task, needs from PRA have guided the definition of the taxonomy, meaning, e.g., that I&C system and its failures are studied from their functional significance point of view.

In PRA, a failure modes taxonomy is applied in the systems analysis, including the performance of FMEA (failure modes and effects analysis) and the fault tree modelling. In PRA, the definitions for the failure modes and the related level of details of abstraction in the fault tree modelling can be kept in a high level as long as relevant dependencies are captured and reliability data can be found.

The DIGREL task has taken advantage from recent and on-going R&D activities carried out in the member countries in this field. This knowledge has been merged by inviting experts in the field to contribute to the activity. Example taxonomies have been collected from the member countries, and analysed, and the conclusions from the taxonomy examples and workshop discussions have been taken into account when considering principles for the taxonomy [2]. This material showed some variety in the handling of I&C hardware failure modes, depending on the context where the failure modes have been defined. Regarding the software part of I&C, failure modes defined in NPP PRAs have been simple – typically a software CCF failing identical processing units.

The taxonomy has been developed jointly by PRA and I&C experts which have slightly different views and needs on defining the failure modes. The PRA experts' perspective follows the needs of PRA 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. verification and validation (V&V) measures. An important aspect in the development of the taxonomy has been for PRA and I&C experts to define the "meeting point" for the two perspectives. The "meeting point" means both agreeing on common terminology and defining the issues and levels of abstraction which the taxonomy shall address.

2.2. 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 targets for the taxonomy have been defined by the task group:

- Defined unambiguously and distinctly

- 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 abstraction of the taxonomy should be sufficient to pinpoint existing dependencies of importance to PRA modelling
- Supports PRA practice, i.e. appropriate level for PRA, and fulfil PRA requirements/conditions
- Captures defensive measures against fault propagation and other essential design features of digital I&C.

2.3. Example system

The taxonomy is focused on the reliability analysis of the reactor protection system, which reduces the scope of failure modes and failure effects considerably. This limitation can be justified by several arguments. Firstly, there is a general consensus that protection systems (reactor trip & Engineered Safety Feature Actuation Systems (ESFAS)) shall be included in PRA, 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 quite different basis for the reliability analysis and modelling. Thirdly, the I&C of the control systems is versatile having both on demand and continuous functions and they do not necessarily have a redundant structure. Even if the taxonomy is focused on the protection systems, it can be useful for control systems, too.

A representative fictive digital protection system example has been developed to be used as a reference in the application and demonstration of the taxonomy. Though there are technical differences between solutions provided by different vendors, many of the features of protection systems are similar for all vendors. Therefore the example is considered representative enough for the failure modes taxonomy purposes

The simplified model takes into account the following:

- Typical architecture of digital I&C systems performing safety functions of the Reactor trip system (RTS) and the ESFAS, jointly called hereafter Reactor Protection System (RPS) functions
- Typical hardware components of the digital I&C platforms
- Typical operation modes of the RPS: ready to actuate a safety function on demand (maintenance, testing, etc. modes are not considered)
- Typical means and features for failure detection and recovery
- Typical majority voting for actuation of RTS and ESFAS functions.

The example system implements I&C safety functions (of Category A according to [3], of Class 1E according to [4]). The overall system architecture describes its organisation in terms of divisions and I&C units.

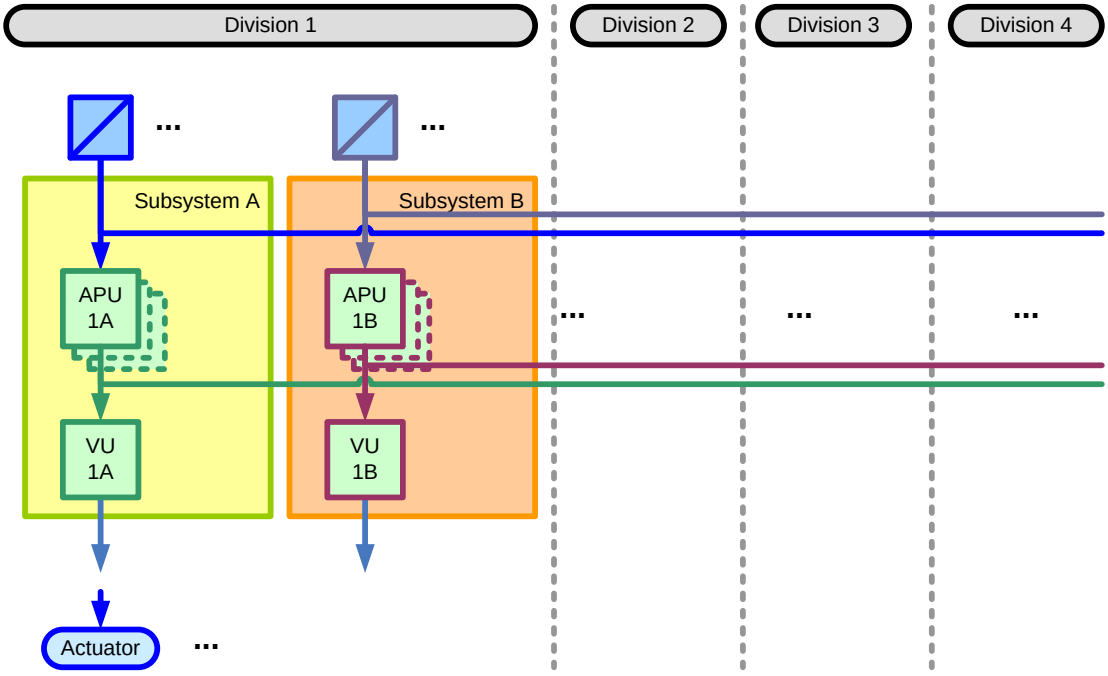
The architecture of a digital I&C system is established primarily by hardware (e.g. analog and digital circuit boards/modules, units, cabinets) and their communication paths (e.g. direct wired connections, network communications, signal distribution boards). The architecture determines essentially the propagation paths of the probable failures of the hardware and of the software.

The example system is organised into two separated subsystems A and B, which are based on the same I&C platform, but implement functions that are diverse. The two subsystems do not exchange information, and for shared actuators, their outputs are fed to simple hardwired logic to determine system-level outputs.

The overall example system architecture can thus be summarised as shown in Figure 1. Each subsystem is itself organised into four redundant divisions, each division of subsystem being composed of different types of I&C units, namely:

- Acquisition and processing units (or APUs): these units acquire process-related information from sensors, and perform calculations to determine the division outputs.
- Voting units (or VUs): these units receive the results determined by the APUs of their division and subsystem and for which voting is required.
- Data Communication Units (or DCUs): these units allow APUs and VUs to communicate with one another. DCUs are integral parts of APUs and VUs, and therefore not shown in the figure below.

Figure 1: Example protection system architecture.



2.4. Levels of abstraction

The DIGREL task group has defined five levels of abstraction for the consideration of failure modes. The levels were identified when comparing examples of taxonomies used by different organisations [2], and are:

1) system level (complete reactor protection system),
2) division level,
3) I&C unit level,
4) I&C unit modules level,
5) basic components level.

This structure corresponds to a typical reactor protection system architecture, which is the scope of the DIGREL work. To handle complexity at the level of system, division and I&C units, failure modes are considered as much as possible only from the functional point of view. No significant distinction is made between hardware or software aspects at these levels. At the module and basic component levels, the taxonomy differentiates between hardware and software related failure modes.

3. FAILURE MODES TAXONOMY FOR DIGITAL I&C

3.1. Basic principles

The main approach is to define failure modes hierarchically and functionally. Failure modes are considered both from top-down and bottom-up perspective. The top-down structuring starts from the failure modes of the actuator functions (e.g. a pump fails to start, a valve fails to open), identifies 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 are defined at low level of abstraction (typically at the module level or the basic component level) 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 PRA practitioner has to choose suitable level of abstraction for each individual PRA and its application.

The taxonomy is developed using a specific conceptual model of failure and failure propagation. The important elements of the failure model are:

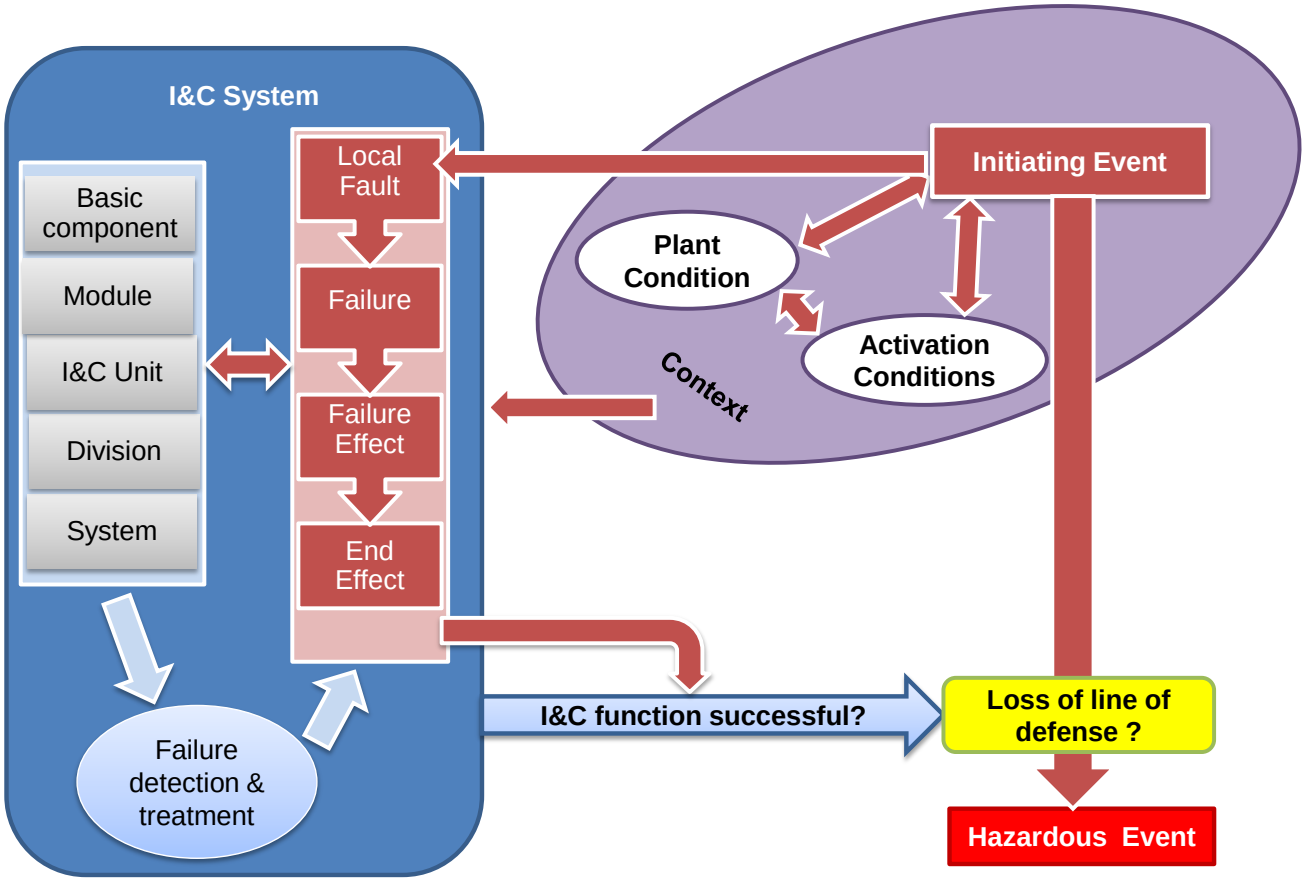
- fault location,
- failure mode,
- uncovering situation,
- failure effect,
- end effect.

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

The *end effect* describes the final propagation of the failure, taking into consideration all these elements of the failure model. In this consideration, a distinction can be made between the “maximum possible end effect”, when fault tolerance design (FTD) is not effective or does not exist, and the “most likely end effect”, assumes that FTD features are present and effective. FTD is effective only when the fault is detected by online monitoring, which is one of the uncovering situation categories.

A comprehensive description of the failure model can be found in [5], and is illustrated in Figure 2. Failure propagation is the path from a “locally” postulated fault to a system or plant level end effect, and it is dependent on the “context”, which defined by the “plant condition”, “initiating event” and “activation conditions”. The propagation can be considered at different levels of abstraction following the I&C architecture. The most interesting part for PRA modelling is though the propagation between module and I&C unit levels.

Figure 2: Failure model [5].



This general approach has been developed in the course of the DIGREL project. Its applicability and usefulness need to be assessed in further research efforts.

3.2. Failure mode taxonomy at 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 for controlling the actuators in the corresponding division, the function of a division is the 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.

3.3. Failure mode taxonomy at 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 the relation between failure modes of an I&C unit and the modules.

In the analysis, the existence of faults is postulated in the modules (hardware or software), and the question is to determine 1) how the unit is affected and 2) how other units that communicate with the

defected unit are affected. In order to answer to these questions, the following issues need to be defined:

- The fault location: In which hardware or software module the fault is located?
- Failure effect:
  - *Fatal, ordered failure*: generation of outputs ceases, outputs are set to specified, supposedly safe values. Halt/abnormal termination of function with clear message.
  - *Fatal, haphazard failure*: generation of outputs ceases, outputs are in unpredictable states. Halt/abnormal termination of function without clear message.
  - *Non-fatal, plausible behaviour*: I&C runs with wrong results that are not evident. An external observer cannot determine whether the I&C unit or the hardware module has failed or not.
  - *Non-fatal, non-plausible behaviour*: I&C runs with evidently wrong results. An external observer can decide that the I&C unit or the hardware module has failed.
- Uncovering situation:
  - *Online detection*. Covers various continuous detection mechanisms.
  - *Offline detection*. E.g. periodic testing, and also other kind of periodic controls which can be credited in PRA.
  - *Revealed by demand.*
    - Latent failure, revealed by demand. A failure is present that is not detectable by online or offline mechanisms (test independent failure).
    - Failure triggered by demand. A specification error causes a failure on demand in an unexpected context.
  - *Revealed by spurious actuation*. The activation of the fault triggers spurious actuation before any FTD has time to take place. This situation covers two variants:
    - Spurious actuation due to functional failure, incl. voting logic
    - Spurious actuation due to failure of detection mechanism.

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

An important issue is that it is neither necessary nor reasonable to assume all possible combinations, which considerably reduces the number of relevant failure modes (see Table 1). Fatal haphazard failures are not considered in this analysis, because here it is assumed that modules of the reactor protection system do not fail in an unknown state. Fatal failures are ordered and are detected by online detection or by spurious effect.

Non-fatal failures are more dangerous since any uncovering situation may be possible. In case of non-plausible behaviour, failure is detected by online detection or by spurious effect. “Plausible behaviour” refers to the case where the failure is not detected by online detection.

Table 1: Relevance of the combinations of local effects and detection situations

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

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

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 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 output (one function),
- Spurious output (all functions).

The above list is not exhaustive, and, e.g., for voting units 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 PRA).

In the example I&C architecture (Figure 1), the following end effects of a failure can be assumed:

- Failure of one function (or more) in one subsystem,
- Failure of one function (or more) in only one division in one subsystem,
- Failure of one function (or more) in both subsystems,
- Failure of one set of redundant APUs/VUs,
- Failure of multiple sets of redundant APUs/VUs in only one subsystem,
- Loss of one subsystem,
- Failure of multiple sets of redundant APUs/VUs in both subsystems,
- Loss of one subsystem and of one or more sets of redundant APUs in the other subsystem,
- Loss of both subsystems.

At the module level, a distinction is made between the treatment of hardware and software related failure modes. The taxonomy report [5] includes comprehensive list of hardware module failures which are associated with the failure effect and uncovering situations, and this is sufficient to determine the functional impact on I&C units. For instance, one of the failure modes of the processor module is that the processor stops execution of code, which is a fatal ordered failure and is detected by the online detection. The functional impact is loss of all APU/VU functions according to FTD. See [5] for more examples.

The approach for software modules 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). This module controls the overall functioning of the I&C unit (APU/VU/DCU), and is the same for all the units of all divisions or of all subsystems of the example system.
- Elementary functions (EFs). These modules provide readily useable standard (library) functions such as Boolean logic, mathematical functions or delays. They are the same for all units of the example system. However, an important difference with respect to the OS is that a specific APU/VU will use only a specific subset of all available EFs.
- Application-specific software modules (AS). These modules implement specific I&C functions in APUs and VUs. Homologous APUs (resp. VUs) in redundant divisions have the same sets of AS modules.
- Functional requirements specification modules (FRS). These are virtual software modules associated with application functions. There is one such module per application function required of an APU or a VU. The purpose to consider FRS modules is to allow the representation of errors in functional requirements specifications, which by operating experience has been shown to be not uncommon [6].
- Data communication software (DCS). This module implements the data communication protocol. It is part of the platform software, and all DCUs of the example system have the same DCS.
- Data link configuration (DLC). This module specifies the nodes that can be part of a given network, and the data messages that can be exchanged between the nodes of the network. The two subsystems use different networks, and therefore the DLCs of their DCUs are different.
- SW in COTS-modules (Commercial off-the-shelf). These modules are specific pieces of software present in hardware modules in APU, DCU, VU or any other module of the system (e.g. power supply) other than OS and AS. The implementation in software belongs to a commercial company, and the source code is not freely nor publicly available. It is restricted from use, such as modification or V&V, for the end user.

4. CONCLUSION

Due to the many unique attributes of digital systems, a number of modelling and data collection challenges exist, and international consensus has not yet been reached regarding their modelling in PRA. Currently in PRA, computer-based systems are mostly modelled by using simple approaches, and the primary goal is to model dependencies (I&C systems' support systems). There is a general consensus that protection systems shall be included in PRA, while control systems can be treated in a limited manner, depending on the importance on the plant safety.

The objective of OECD/NEA DIGREL task was to develop a failure mode taxonomy for reliability assessment of digital I&C systems for use in PRA. The I&C failure mode taxonomy has been developed to support modelling and quantification efforts. It will also help define a structure for data collection and to review PRA studies.

The proposed failure mode taxonomy has been developed by first collecting examples of taxonomies provided by the task group organisations. This material showed some variety in the handling of I&C hardware failure modes, depending on the context where the failure modes have been defined. Regarding software part of I&C, failure modes defined in nuclear power plant PRAs have been simple — typically a software related CCF failing identical processing units.

The failure modes taxonomy is based on a failure propagation model and a definition of five levels of abstraction: 1) system level, 2) division level, 3) I&C unit level, 4) I&C unit modules level, 5) basic components level. This structure corresponds to the typical reactor protection system architecture, which was the scope of the taxonomy researched in this document. The failure propagation model consists of the following elements: fault location, failure mode, uncovering situation, failure effect and

the end effect. These concepts are applied to define the relationship between a fault in hardware or software modules (module level failure modes) and the effect on I&C units (I&C unit level failure modes). To handle complexity, at the level of system, division and I&C units, failure modes are considered as much as possible only from the functional point of view. No significant distinction is made between hardware or software aspects at these levels. At the module and basic component levels, the taxonomy differentiates between hardware and software related failure modes.

This approach has been developed in the course of the DIGREL project. Its applicability and usefulness need to be assessed in further research efforts. The purpose of the taxonomy is to support PRA, and therefore focuses on high level functional aspects rather than low level structural aspects. This focus allows handling of the variability of failure modes and mechanisms of I&C components. It reduces the difficulties associated with the complex structural aspects of software in redundant distributed systems.

Acknowledgements

Opinions presented are those of the authors and not necessarily those of the organisations of the authors or of other members of the DIGREL task group.

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. 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 paper possible. Work by GRS has been funded by the German Federal Ministry for the Environment, Nature Conservation, Building and Nuclear Safety

References

[1] "*Recommendations on assessing digital system reliability in probabilistic risk assessments of nuclear power plants*", NEA/CSNI/R(2009)18, OECD/NEA/CSNI, 2009, Paris.

[2] W. Postma, T.-L. Chu, M. Yue, "*Observations and discussion from the taxonomies of digital system failure modes provided by the DIGREL task group*", ANS PSA 2013 International Topical Meeting on Probabilistic Safety Assessment and Analysis, Columbia, SC, September 22–26, 2013, on CD-ROM, American Nuclear Society, 2013, LaGrange Park, IL. Paper 91.

[3] "*Nuclear power plants — Instrumentation and control important to safety — Classification of instrumentation and control functions*", IEC 61226, ed. 3.0 International Electrotechnical Commission, 2009, Geneva.

[4] "*IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations*", IEEE Std. 323-2003, Institute of Electrical and Electronics Engineers, 2003.

[5] "*Failure modes taxonomy for reliability assessment of digital I&C systems for PRA*", Report prepared by OECD/NEA Working Group RISK Task group DIGREL, draft March 2014.

[6] "*Estimating Failure Rates in Highly Reliable Digital Systems*", EPRI 1021077, Electric Power Research Institute, 2010, Palo Alto (limited distribution).