Title	Proposal for the taxonomy of failure modes of digital system hardware for PSA
Author(s)	Piljugin, Ewgenij; Authén, Stefan; Holmberg, Jan-Erik
Citation	11th International Probabilistic Safety Assessment and Management Conference & The Annual European Safety and Reliability Conference, pp. 10-TH4-3
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

Proposal for the Taxonomy of Failure Modes of Digital System Hardware for PSA

Ewgenij Piljugin[a*], Stefan Authén[b], Jan-Erik Holmberg[c]
[a]Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Forschungszentrum, Garching, Germany,
[b]Risk Pilot AB, Stockholm, Sweden, [c]VTT, Espoo, Finland

Abstract: Currently a new taxonomy approach is developed by the DIGREL task group, established by the Working Group on Risk Assessment of OECD/NEA, in order to support the modelling of digital I&C systems in the framework of PSA for nuclear power plants (NPP). It should improve the identification of potential failure modes of hardware as well as software. It is based on generic experience with different types of digital I&C systems. Also it should help to define the structure of data to be collected and support the quantification of PSA models.
The DIGREL task group has decided to separate the evaluation of the taxonomy approaches of digital I&C systems into two parts: a taxonomy of the failure modes of hardware and a taxonomy of the failure modes of software.
This paper presents a proposal for a generic structure of the hardware of a digital I&C system with safety-functions relevant to safety. The hardware failure mode taxonomy approach is based on decomposition of a particular digital I&C system according to a generic hardware structure. It is assumed that this generic decomposition is sufficient to identify generic issues of the specific I&C systems, components and functions.
The decomposition of the hardware into modules is based on the current practice of data collection from operating experience of analog and digital I&C to be applied in PSA. The simplified model takes into account the typical design features of digital I&C systems in the NPP e.g. redundant signal processing, network communication and voting of the actuation signal. Furthermore, a concept (methodology) is presented for the identification of generic issues with regard to failure modes of hardware of a digital I&C system and to probable effects by propagation of the failure modes through each level of signal processing (local, next higher assembly and system level).

Keywords: Digital I&C, failure modes taxonomy, hardware, PSA

1. INTRODUCTION

In 2010, the Working Group on Risk Assessment of OECD/NEA CSNI established a task group DIGREL [1]. The activities of DIGREL focus on development of a generic taxonomy approach for identifying failure modes of digital instrumentation and control (I&C) equipment. The main objective of the DIGREL task is to prepare a basis for future modelling (e.g. FTA – Fault Tree Analysis) of the digital I&C in PSA, particularly to support a failure mode and effect analysis (FMEA).

The industry-wide and technology-wide established methodology of the FMEA is used for identifying of all parts of a system with relevance for reliability or for safety, and their associated failure modes. The FMEA can also support a comprehensible assessment of the causes and effects of each failure mode in the framework of PSA.

The presented taxonomy approach [1] should support evaluation of the FMEA of a specific digital I&C on the basis of generic sources. One important topic of the DIGREL taxonomy approach is the determination of generic issues regarding identifying failure modes of the hardware and of the software on the basis of various I&C systems, components and functions. Therefore, it was initially necessary to develop a generic model of digital I&C such that all the relevant properties of a specific systems can be captured comprehensibly.

The abstraction level of a generic model was chosen in such a way that the commonalities in signal processing between different types of I&C systems remain recognizable and the differences of specific attributes of the particular hardware components do not predominate the evaluation of failure modes.

This paper presents a proposal of the generic architecture of the hardware of a digital I&C system with safety-relevant functions. A complementary work will be done by a separate DIGREL working team regarding identification of failure modes of software of digital I&C systems relevant to safety in nuclear power plants [2].

2. GENERAL APPROACH

2.1. Application of the FMEA Methodology for Digital I&C

The state-of-the-art FMEA of electronic equipment should be performed in accordance with internationally established requirements for usage of the FMEA methodology, e.g.:

- IEC 60812: 2006, "Procedure for failure mode and effect analysis" [3],
- IEC 60300-3-1: 2003, Dependability management - Part 3-1: Application guide - Analysis techniques for dependability [4].

Generally, the application of FMEA to a technical system is preceded by a hierarchical decomposition of a system into basic elements. An analyst performing a FMEA applying a functional approach must be able to define and identify each system function and its associated failure modes for each functional output. Therefore, an analyst needs the following information to perform a FMEA [3], [5]:

- Definition of the equipment and its functional breakdown,
- Reliability block diagrams[1] or functional block diagrams[2] of the equipment including internal and external signal and data flows,
- Description of the operational modes of the equipment (e.g. continuous mission, stand-by, cyclic operation, maintenance, failure detection),
- Basic rules and assumptions including mission requirements (control and monitoring functions of different actuators, e.g. motor or solenoid valves, drives),
- Specification of the hardware and software of the equipment.

In practice, a FMEA of a complex digital I&C system or of a complex hardware module is an iterative process. The FMEA team can principally use either a bottom-up approach (e.g. hardware modules approach) or a top-down approach (e.g. functional approach for identifying of the associated modules) depending on what works best for them (see Figure 1).

The typical FMEA starts usually with lowest level elements. A failure effect at a lower level may become a failure cause of a failure mode of an item in the next higher level. The analysis proceeds in a bottom-up approach until the end effect on the system has been identified.

[1] A reliability block diagram is a graphical method for showing how component reliability contributes to the success or failure of a complex system

[2] A function block diagram is a block diagram that describes a function between input variables and output variables. A function is described as a set of elementary blocks. Input and output variables are connected to blocks by connection lines.

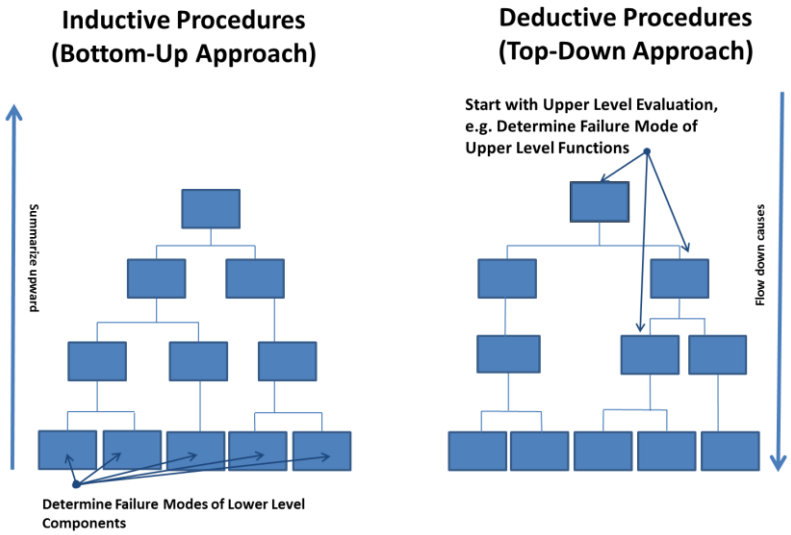

Figure 1. Bottom-up approach (typically FMEA) and top-down approach (typically FTA - Fault Tree Analysis)

As described above, the application of an FMEA follows a systematic workflow. Such a typical FMEA workflow is presented in Figure 2.

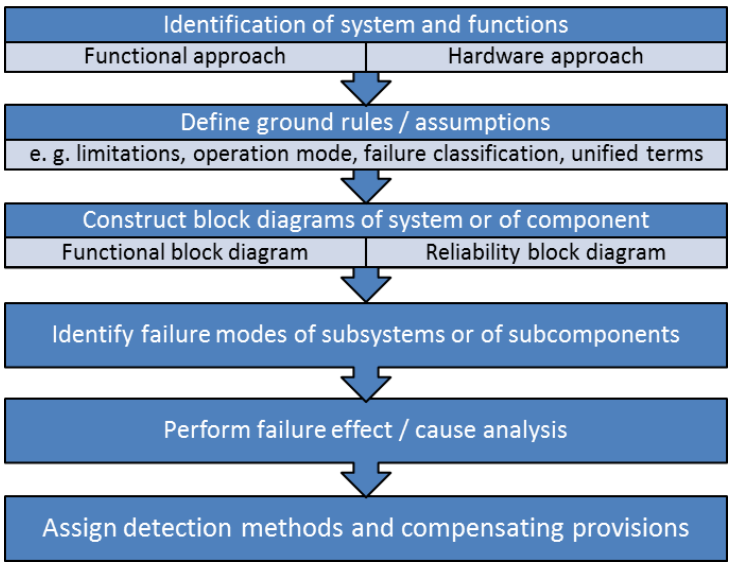

Figure 2. Main steps of performing a FMEA

To ensure that a complete analysis has been performed, each component failure mode and/or output function should be examined covering the following conditions [5]:

- Spurious actuation,
- Loss of output,
- Degraded output or reduced operational capability,
- Failure to operate at the proper time,
- Failure to stop operating at the proper time.

The FMEA should also identify the means and the procedures by which occurrence of a failure of the hardware and/or of its malfunction will be detected. The states of detection means can be characterized as follows [5]:

- An indication that the system (or function, or module) is operating as required,
- An indication that the system (or function, or module) has malfunctioned or failed,

- An erroneous indication that a malfunction has occurred when actually there is no fault. Conversely, an indication that the system is operating normally when, in fact, there is a failure.

2.2 Assumptions

The approach presented in this paper focuses on the failure modes taxonomy of the hardware and its application to modelling and to the quantification task. The following items are considered:

- Typical architecture of digital I&C systems, performing safety functions (e.g. RPS – Reactor Protection System or ESFAS - Engineered Safety Features Actuation System)
- Typical components of the hardware of the digital I&C platforms,
- Typical operation modes of the digital I&C,
- Typical means and features of failure detection and recovery,
- Typical majority voting for actuation of RPS and ESFAS functions.

With regard to the analysis and modeling of the I&C of safety and safety-related systems in the PSA, the following levels of details can be distinguished from the hardware point of view [1]:

- Failure modes of the entire system,
- Failure modes of a division and/or subdivisions,
- Failure modes of processing modules or racks of cabinets or whole cabinets,
- Failure modes of the modules, i.e. subcomponents of processing units,
- Failure modes of the generic components, i.e. subcomponents of modules.

The presented proposal for the decomposition of the hardware of the I&C system has been developed based on proven practice with respect to data collection of the operating experience with analog I&C for the purpose of PSA.

The level of detail for the decomposition of the generic digital I&C system was decided, to the level of modules based on an interpretation of the overall requirements for the hardware taxonomy whereof the most important are:

- Shall support PSA practice,
- Shall capture all critical dependencies and design features,
- Shall be appropriate for safety related systems,
- Shall support modeling of CCF at necessary level.

Also additional aspects such as feasibility of PSA modeling and quality assurance, implementation into existing PSA tools (using fault tree and event tree techniques), maintainability of data and model and usage of the PSA for various applications, where taken into consideration [6]. The most suitable level of detail was identified to be the module level which concurs with the level of detail of general PSA state of the art. The module level will make it feasible to perform, maintain and review a PSA of digital I&C with reasonable resources while capturing critical dependencies. It will also be possible to capture fault tolerant features of the digital system and the impact on the reliability of safety functions.

In the presented approach the evaluation of the model of generic digital I&C regarding measures of the failure detection is limited

- to the detection of malfunction or failure of generic modules during normal operation or on demand, and
- to the determination of the failure identification methods of generic modules by testing.

3. DEVELOPMENT OF A GENERIC MODEL OF DIGITAL SAFETY-RELATED I&C

3.1. Basis for Evaluation

In the last decades a variety of different safety-related digital I&C systems were developed and implemented in nuclear installations and facilities around the world. Digital I&C architectures are deployed in several reactors worldwide [7], [8] such as Chooz B (France), Sizewell B (United Kingdom), Ringhals-1 and -2 (Sweden), Temelin-1 and -2 (Czech Republic), Tianwan (China). Also new designs, e.g. the EPR developed by AREVA, the APWR by Mitsubishi Heavy Industries, Ltd. (MHI) and the ESBWR by General Electric - Hitachi (GEH) also demonstrate the recent state concerning digital I&C architectures in NPPs. The entire I&C architecture of the above designs can usually divided into:

- Process interface level,
- System automation level,
- Unit supervision and control level.

The first level of signal processing presents the physical interface between system automation level (e.g. systems, subsystems) and sensors, actuators, and switchgear (e.g. measurements, control signals, check-back signals). The system automation level of a nuclear power plant consists usually of the reactor protection system, the safety automation system, the process automation system, and actuation and control equipment. The supervision and control level consists of the displays, workstations and panels of the control rooms (e.g. main and emergency control room) and of the process information and control system. Each level of signal processing may contain both safety-related and non-safety-related systems and equipment.

The safety standards define requirements regarding design for reliability of structures, systems and components. The highest quality of and best practices for hardware and software shall be used for digital I&C of safety systems, considering the following criteria [8], [9]:

- Compliance with single failure criterion,
- Robustness concerning common cause failures,
- Principle of fail-safe design.

The architecture, the equipment (hardware) and software of the digital safety-related I&C (I&C platform) are designed to meet all safety-related I&C requirements in nuclear power plants. The dissimilarities between different I&C platforms may be significant. Not only the physical design but also the functional design, e.g. fault tolerant features and voting logic, may differ. However the stringent safety requirements on design, manufacturing and operating of the safety systems and safety-related systems in the nuclear power plants lead consequently to recognizable similarities of the architecture of several digital safety-related I&C systems and of their functions.

3.2. Proposal of Overall Architecture of Generic Digital Safety-Related I&C

The development of a generic digital I&C system was based on examples of the implementation of the following different platforms of digital I&C systems for safety functions:

- Teleperm XS (e.g. EPR reactor design, modernisation projects of the I&C in several NPPs),
- Common-Q/Advant AC160 system (e.g. AP1000 reactor design),
- Tricon PLC system (e.g. ESBWR reactor design).

Figure 3 presents a proposal of a simplified architecture of a generic digital safety-related I&C system. The signal processing of each redundant division of the digital safety-related I&C systems is divided in two separate sub-systems (subdivisions) Red. 1, 2, ...(A) and Red. 1, 2, …(B). Thus, the generic structure presented here can consider various different architectures of the digital safety-related I&C systems, e.g.

- In one case the sub-systems Red. 1, 2, ...(A) and Red. 1, 2, …(B) can be interpreted as implementation of the functional diversity inside of one system based on a common platform,

- In the other case the sub-systems Red. 1, 2, ...(A) and Red. 1, 2, …(B) can be interpreted also as redundant channels of the diverse I&C systems based on different platforms (diverse hardware), e.g. the redundant channels of a primary and of a secondary (diverse) protection system.

The signal processing from sensors to actuators in Figure 3 is extremely simplified, for the reason that it should help to identify main features of the architecture of the digital I&C systems (items of hardware and their functions) and main signal pathways (e.g. networks) inside and outside of the divisions and subdivisions. For reasons of clarity it was renounced to present the connections in the Figure 3 with the external systems (e.g. connection to the plant network, messaging and service interface).

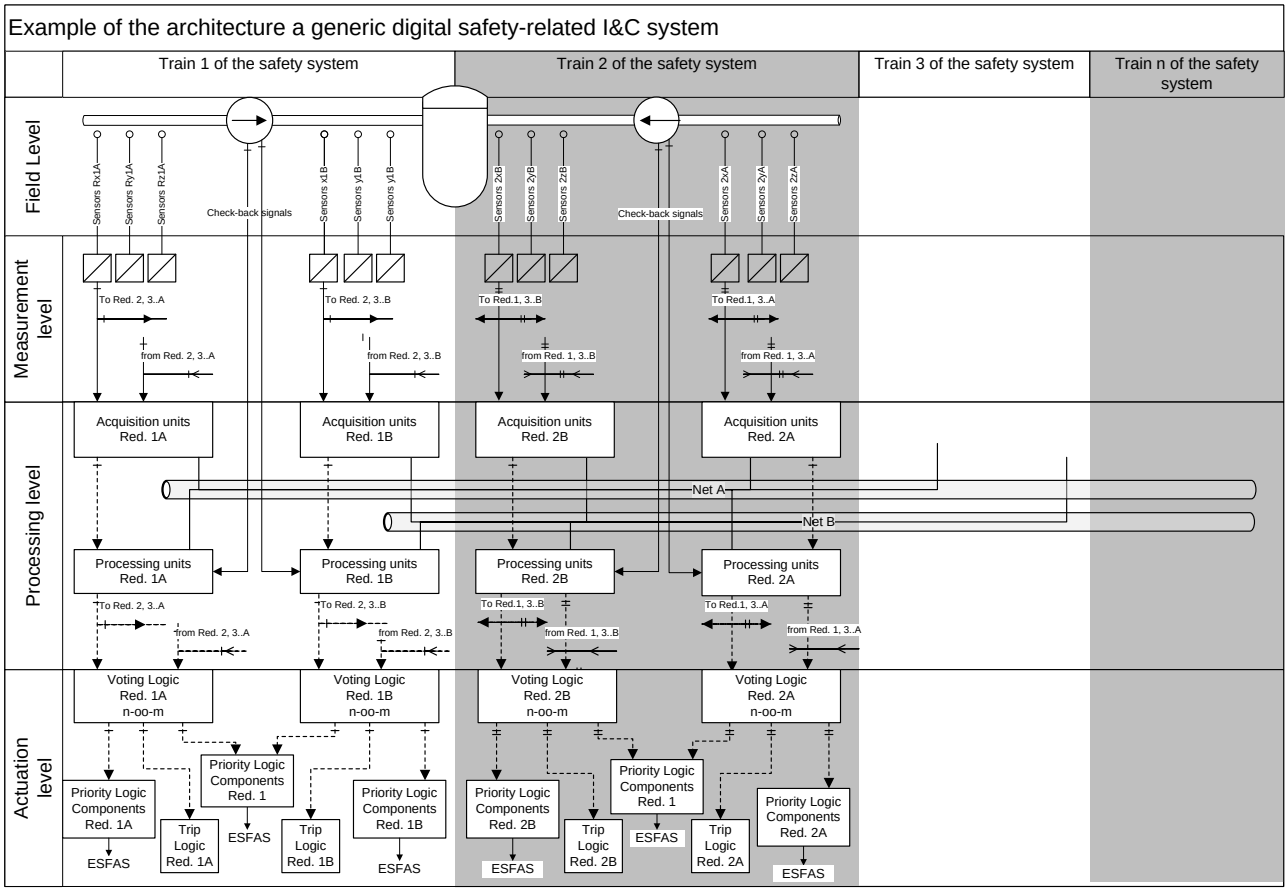

Figure 3. Proposal of architecture of generic digital safety-related I&C

In the report [10] it is ascertained that the I&C function of the new design NPPs extensively depend on network communications to transmit data within and among various control and safety digital I&C systems. The network of the particular digital I&C systems can be configured as any one of several topologies leading to the result of successful transmission of data from source to one or more receivers. Network topology refers to the graph properties of the connections among network nodes, independent of the medium, transmission speed, and other properties. The network can be implemented as different types of topology:

- Physical topology - the physical connections among the nodes,
- Signal topology - paths taken by the physical network signals among the nodes, and
- Logical topology - the flow of information between the nodes.

The topology of a network of digital I&C can have significant influence on the network's failure modes, fault propagation, and fault handling properties. The relevant features of the networks (see Figure 3: Net A, Net B, signal and data links) should be identified in the framework of the taxonomy of the hardware.
It is necessary also within the scope of taxonomy to identify the structure and the technologies of the internal and external communication (e.g. platforms, topologies, protocols, wired or optical fiber) between the parts of a digital I&C system and between the different systems or equipment too.

Table 1 presents a proposal for identification of the communication features for each sub-system (level) of the digital I&C.

Table 1. Examples for the identification of the communication features of the digital I&C

Level of signal processing (see Figure 3)	Means and features of the internal communication / inside of a node (e.g. division, subdivision, rack)	Means and features of the external communication (e.g. Net A and B) between nodes (e.g. redundant divisions)	Means and features of the external communication to the other systems
Measurement Level	e.g. hard-wired connection, optical fiber cable, HART-link to data acquisition unit	e.g. hard-wired, optical fiber cable, no connections	e.g. hard-wired, optical fiber cable, no connections
Signal Acquisition Level	e.g. hard-wired or optical fiber cable input, internal bus (e.g. backplane), point-to-point network connection	e.g. point-to-point network connection, local area network, no connections	e.g. local area network, no connections
Signal Processing Level	e.g. internal bus (backplane) hard-wired output, point-to-point connection, PROFIBUS link, local area network	e.g. point-to-point connection, local area network, no connections	e.g. local area network (monitoring & service interface to plant bus), no connections
Actuation Logic Level	e.g. hard-wired, point-to-point, PROFIBUS link, local area network	e.g. point-to-point connection, local area network, no connections	e.g. local area network (monitoring & service interface to plant bus), no connections

3.3. Proposal of Structure of Generic Hardware of Digital Safety-Related I&C

The proposal for the decomposition of the hardware of the I&C system (see Figure 4) was developed on the basis of established practice of fault tree modelling of analog and digital I&C (hardware) in the PSA [6].

The generic structure of the hardware of the entire signal processing consists of the following kinds of hardware components [8]:

- Processor modules for signal processing,
- Communication modules,
- Input and output modules of digital or analog signals,
- Electrical items such as electrical connections, cables and power supply modules,
- Mechanical components such as subracks, fans and cabinets for housing the above modules.

The processor modules for signal processing usually implement on the basis of various components (e.g. central processing unit, memory chips, clock generator, on-board controllers) the following tasks:

- Execution of the system software and application software (e.g. I&C functions),
- Data accesses to the input and output modules, to the interface modules,
- Monitoring features.

The components for communication provide signals, data and information transfer through wires or fibre optics by using networks with digital data protocols [8], [10]. Typical components are:

- Communication processor modules,
- Communication modules (e.g. interface modules),
- Server and gateways.

The analog or digital input/output modules can provide following analog input/output capabilities:

- Single or multiple analog input/output channels,

- Connection features to the internal bus,
- Integrating measuring principle,
- Power supply of the sensors,
- Isolation (decoupling) features.

The I&C cabinets provide mechanical and electrical parts for the installation of the racks (subracks). The cabinets and the racks can comprise:

- Internal computer bus,
- Internal power supply for the I&C modules from the external power supply,
- Packaging system with the mechanical installation features for the I&C modules,
- Cooling system (e.g. natural convection and/or forced ventilation by fans),
- Monitoring equipment (e.g. alarm, power supply, temperature).

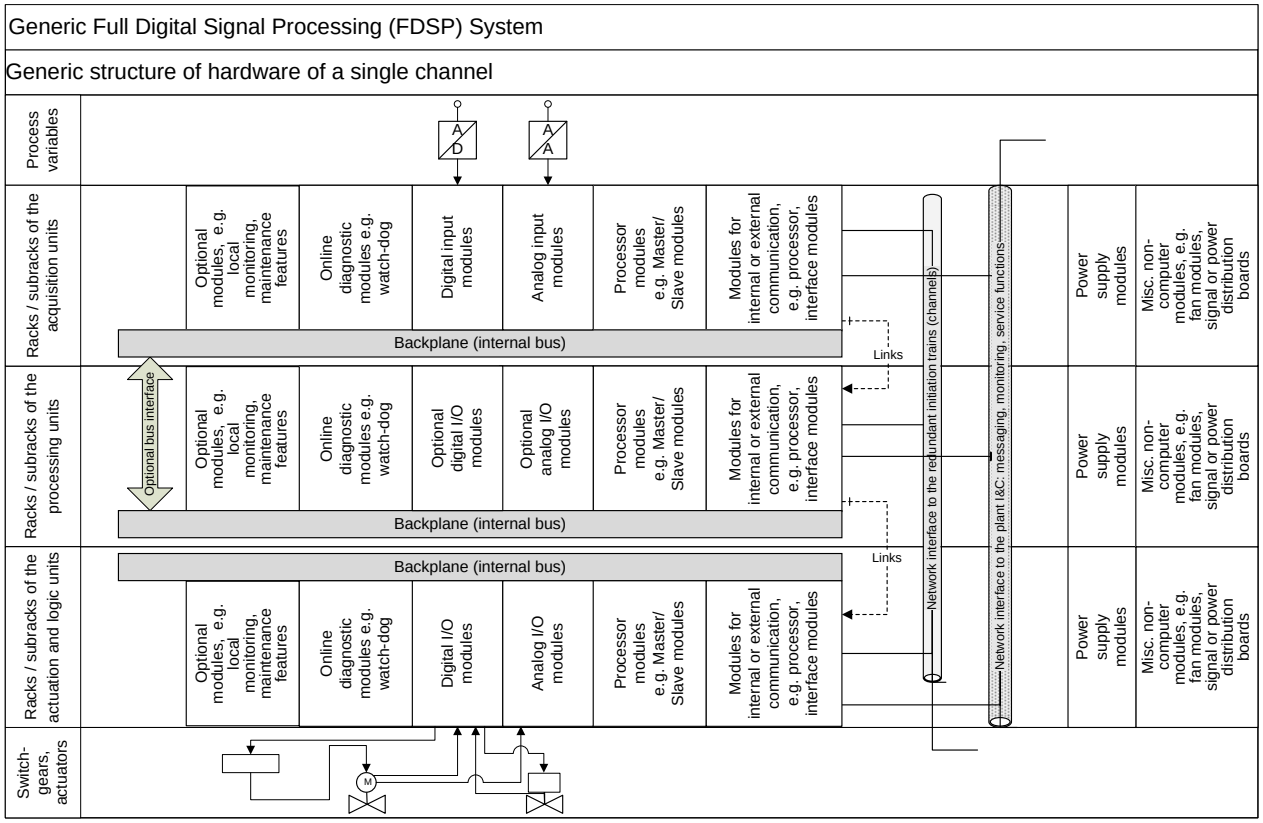

Figure 4. Proposal of structure of generic hardware of digital safety-related I&C

Table 2 presents a draft of FMEA worksheet for evaluation of the failure modes of the hardware modules of generic digital safety-related I&C systems.

Table 2. Worksheet for the evaluation of the failure modes of the generic modules of the digital I&C systems

Hardware modules of the generic signal processing units (e.g. rack, subrack) (see figure 4)	Failure modes of hardware module	Failure effect of the function of the unit (e.g. output signals)	Failure identification features: e.g. on-line monitoring, periodical test	Relevance regarding execution of software of the unit
Backplane (internal bus)				
Processor Modules				
Digital Input/Output modules				
Single Channel of Digital Input/Output Module				

Hardware modules of the generic signal processing units (e.g. rack, subrack) (see figure 4)	Failure modes of hardware module	Failure effect of the function of the unit (e.g. output signals)	Failure identification features: e.g. on-line monitoring, periodical test	Relevance regarding execution of software of the unit
Analog Input/Output Modules				
Single Channel of Analog Input/Output module				
Communication Modules				
Online diagnostic modules, e.g. watchdog				
Optional HMI modules, e.g. local monitoring, maintenance features				
Misc. modules (non-computer equipment e.g. power supply, fan, signal distribution board)				

4. CONCLUSION

The recent activity of the DIGREL task group initiated by WGRisk is focused on development of a common taxonomy of failure modes of digital I&C to support reliability assessment in the frame of PSA. This paper presents a proposal of the generic structure of the hardware of a digital I&C system with functions relevant to nuclear safety. The hardware failure mode taxonomy should support evaluation of a particular digital I&C system according to a generic hardware structure. It is assumed that the proposed structure and decomposition of the generic digital I&C system is appropriate to identify generic issues of specific I&C systems, components and functions.

The DIGREL task group intends, in a next step, to complete the proposal regarding structure of the generic digital I&C and to continue the evaluation of the generic failure modes of the hardware on the basis of the proposed FMEA worksheet.

Acknowledgements

Contributions from the WGRISK/DIGREL task group members are acknowledged. Parts of this work were sponsored by the Federal German Ministry of Economics and Technology (BMWi) within the frame of corresponding R&D projects. 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] 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. 11th International Probabilistic Safety Assessment & Management Conference, PSAM 11, Helsinki, June 25–29, 2012.

[2] 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.

[3] International Electrotechnical Commission (IEC). Analysis techniques for system reliability, Procedure for failure mode and effects analysis (FMEA), International standard IEC 60812:2006(E), Second edition 2006-01.

[4] International Electrotechnical Commission (IEC). Dependability management, Application guide – Analysis techniques for dependability – Guide on methodology, International standard IEC 60300-3-1:2003, Part 3-1.

[5] Department of the Army, TM 5-698-4, Failure Modes, Effects and Criticality Analyses (FMECA) for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities, 29 September 2006

[6] Authén, S., Gustafsson, J., Holmberg, J.-E., Guidelines for reliability analysis of digital systems in PSA context, Phase 2 Status Report, NKS Report, January 2012.

[7] United States Nuclear Regulatory Commission. Instrumentation and Controls in Nuclear Power Plants: An Emerging Technologies Update. NUREG/CR-6992, 2009

[8] International Atomic Energy Agency. Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants. IAEA Nuclear Energy Series No. NP-T-3.12. Vienna, Austria, 2011.

[9] International Atomic Energy Agency. Safety Standards Series No. NS-R-1, SAFETY OF NUCLEAR POWER PLANTS: DESIGN, Safety Requirements, Vienna, 2000.

[10] Kisner, R. et al. Safety and Non-Safety Communications and Interactions in International Nuclear Power Plants, Guidelines for the Design of Highly Integrated Control Rooms, ORNL/NRC/LTR-07/05, Prepared for the U.S. Nuclear Regulatory Commission, August 2007.