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

DIGREL Seminar

Drawn up by: Jan-Erik Holmberg & Tero Tyrväinen VTT, Stefan Authén, Risk Pilot, December 13, 2012
Date: November 6, 2012
Place: Swedish Radiation Safety Authority, Solna Strandväg 96, Stockholm, Sweden

Participants:

Name	Organisation	Country
Stefan Authén	Risk Pilot	Sweden
Jan-Erik Holmberg	VTT	Finland
Linda Lanner	Risk Pilot	Sweden
Tomas Jelinek	SSM	Sweden
Ralph Nyman	SSM	Sweden
Tsong-Lun Chu	Brookhaven National Laboratory	USA
Stefan Eriksson	RAB	Sweden
Cilla Andersson	RAB	Sweden
Jiri Sedlak	Nuclear Research Instute Rez	Czech Republic
Ming Li	NRC	USA
Kaisu Leino	Fortum/NKS	Finland
Emil Ohlson	FKA	Sweden
Johan Gustavsson	FKA	Sweden
Tero Tyrväinen	VTT	Finland
Jan Nirmark	Vattenfall Research & Development	Sweden
Keisuke Kondo	JNES	Japan
Atte Helminen	TVO	Finland
Hannu Tuulensuu	TVO	Finland
Herve Bruneliere	Areva	France
Gilles Deleuze	EDF	France
Ewgenij Piljugin	GRS	Germany
Carol Smidts	The Ohio State University	USA

1 Opening of the seminar

Stefan Authén, Risk Pilot, opened the seminar and welcomed the participants.

Ralph Nyman, SSM, also welcomed the participants. Ralph is the Swedish contact person of OECD/ICDE common cause failure data collection project. OECD/ICDE has taken over the task of COMPSIS to collect data from digital I&C related component failures.

The agenda of the seminar was accepted (Att. 1). The presentation of SSM's perspective will take place in the workshop next day by Bo Liwång.

Participants presented themselves.

2 Overview of DIGREL

Jan-Erik Holmberg, VTT, presented the objectives and scope of the WGRISK DIGREL task and the corresponding Nordic NKS research activity. He gave also an introduction to the development of the taxonomy (Att. 2). Two failure mode examples were discussed by participants.

3 Definitions

Carol Smidts, OSU gave an introduction to terms and definitions related to DIGREL task. She made a comparison of terms used in IEEE and IEC standards (Att. 3) and pointed out differences.

4 Collection of failure mode taxonomies

Tsong-Lun Chu, BNL, presented a summary of taxonomy inputs from the Task group member organisations (Att. 4). Eleven organisations provided input. The results are presented in two tables: one for hardware failure modes and one for software failure modes.

5 Example system

Ewgenij Piljugin, GRS, presented an example of a generic digital I&C system (Att. 5) and a tentative failure modes and effects analysis for such system. The system description is decomposed into system architecture, hardware structure, and software architecture.

6 General approach to the taxonomy

Gilles Deleuze, EDF, presented the general approach to define the failure modes taxonomy (Att. 6). The approach follows a functional model of faults, failures, activation conditions, failure propagation, etc. Taxonomy is defined at several levels: system, division, I&C unit, module, basic component. Taxonomy takes into account features such as failure detection and failure extent.

7 Nordic Test Case: Evaluation of the modelling aspects and application of the taxonomy

Stefan Authén, Risk Pilot, demonstrated how the proposed taxonomy can be applied in PSA (Att. 7). The demonstration was based on an example digital I&C PSA model in the Nordic part of DIGREL.

8 Discussion, conclusions of the seminar

A round table discussion was carried out. Among others following issues were raised by the seminar participants:

- The gap between PRA and I&C experts needs to be closed
- Challenges with the data collection. Data collection and reliability data estimation are beyond the scope of the WGRISK/DIGREL task. However the aim of the taxonomy is to support data collection. One problem with data collection is that the lifetime of I&C technology is short. It can be questionable to use data from previous generation devices. Vendors should have data, but the data proprietary restriction may hinder wider use of data. In practice, hardware data estimation is based on partly operating/testing experience and on theoretical consideration following standards.
- Consensus is needed in the definitions
- The failure modes taxonomy must be validated against the requirements
- Importance of recognising dependencies in the system was pointed out

Attachments

1. Agenda
2. Status of NKS/NPSAG DIGREL project, overview of the activities
3. WGRISK TG DIGREL, guideline development, overview, requirements for the taxonomy
4. Definitions
5. Presentation of collected Taxonomies
6. Example system
7. General approach to the digital I&C failure modes taxonomy
8. Nordic Test Case: Evaluation of the modelling aspects and application of the taxonomy

DISTRIBUTION Seminar participants, WGRISK DIGREL Task Group members

Attachment 1. Agenda

Tuesday November 6, 2012 **NKS/DIGREL seminar**		
09:00	*Coffee, registration*	
09:30	Opening of the seminar	Stefan Authén, Risk Pilot
09:45	Nordic regulator perspective	Ralph Nyman, SSM
10:15	Status of NKS/NPSAG DIGREL project, overview of the activities	Jan-Erik Holmberg, VTT
10:30	*Break*	
10:45	WGRISK TG DIGREL, guideline development, overview, requirements for the taxonomy	Jan-Erik Holmberg, VTT
11:15	Definitions	Carol Smidts, OSU
11:45	Presentation of collected Taxonomies	Tsong-Lun Chu, BNL
12:30	*Lunch*	
13:30	Example system	Ewgenij Piljugin, GRS
14:15	General approach to the digital I&C failure modes taxonomy	Gilles Deleuze, EDF
15:00	*Break*	
15:15	Nordic Test Case: Evaluation of the modelling aspects and application of the taxonomy	Stefan Authén, Risk Pilot
16:00	Discussions and conclusions of the seminar	All
16:30	Adjourn	

Risk Pilot
Your Risk Navigator

NKS/DIGREL Seminar
November 6 2012

Introduction

Stockholm November 6, 2012
Stefan Authén, Risk Pilot AB

Seminar Agenda

Tuesday November 6, 2012 **NKS/DIGREL seminar**		
09:00	*Coffee, registration*	
09:30	Opening of the seminar	Stefan Authén, Risk Pilot
09:45	Nordic regulator perspective	Ralph Nyman, SSM
10:15	Status of NKS/NPSAG DIGREL project, overview of the activities	Jan-Erik Holmberg, VTT
10:30	*Break*	
10:45	WGRISK TG DIGREL, guideline development, overview, requirements for the taxonomy	Jan-Erik Holmberg, VTT
11:15	Definitions	Carol Smidts, OSU
11:45	Presentation of collected Taxonomies	Tsong-Lun Chu, BNL
12:30	*Lunch*	
13:30	Example system	Ewgenij Piljugin, GRS
14:15	General approach to the digital I&C failure modes taxonomy	Gilles Deleuze, EDF
15:00	*Break*	
15:15	Nordic Test Case: Evaluation of the modelling aspects and application of the taxonomy	Stefan Authén, Risk Pilot
16:00	Discussions and conclusions of the seminar	All
16:30	Adjourn	

Meeting logistics

- Meeting room “Kungsholmen”

- Coffee breaks in the entrance hall
- Lunch in restaurant KANTIN, next building

- WLAN available

- Taxi: ask the reception personnel to order

Business from technology

Status of NKS/NPSAG DIGREL project, overview of the activities

DIGREL seminar, November 6, 2012, SSM, Stockholm, Sweden

Jan-Erik Holmberg, VTT

DIGREL Project aim

- The objective with the project is to provide guidelines to analyse and model digital systems in PSA context
  - International OECD/NEA WGRISK task
    - focused on failure modes taxonomy
  - Nordic “NKS/NPSAG” effort
    - aims to cover wider scope of issues

DIGREL task background

- 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)
- Task report NEA/CSNI/R(2009)18, OECD/NEA/CSNI, Paris, 2009 http://www.oecd-nea.org/nsd/docs/2009/csni-r2009-18.pdf

- A new task (abbreviated DIGREL) was started 2010

Nordic project background

- Variety of experience of analysing digital I&C in PSA context
  - Most plants do not yet have digital RPS, but will have in future
  - Turbine plant I&C and diverse other safety-related systems are already digital, but have minor role in PSA context
  - New-builts (in Finland) will have complete digital I&C
- No common approach (yet)
  - However, there is a tradition to try find harmonised approaches for PSA and its applications
- Generally strong interest to find solutions and guidelines how assess safety and reliability of digital I&C and how to meet regulatory requirements

DIGREL Task objectives

- To develop technically sound and feasible failure modes taxonomy for reliability assessment of digital I&C systems for PSA
- To provide guidelines on the use of taxonomy in modelling, data collection and quantification of digital I&C reliability

WGRISK/DIGREL Task Group (TG)

DIGREL task scope

- 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**

- **Needs of PSA are addressed**

Overall working approach of the DIGREL task

- Collection, comparison and analyses of failure modes taxonomies for hardware and software of digital components from the member countries
- Development of generic I&C system example for demonstration and benchmarking purposes
- Guidelines regarding level of detail in system analysis and screening of components, failure modes and dependencies
- Working meetings

Combination of PSA and I&C experts' perspectives

PSA expert

- Follows the needs of PSA modelling
  - to capture **relevant dependencies**
  - to find **justifiable reliability parameters**
- Estimation of the system reliability P
- Level of details can be kept in rather high level

I&C expert

- Focused on **failure mechanisms** and their **recovery means**
  - to demonstrate that the system **fulfil the safety and reliability requirements**, including P < P* (residual risk is acceptably low)
- Needs to analyse failure initiation possibilities and failure propagation methods in a far more comprehensive manner

WGRISK/DIGREL achievements so far

- Failure mode taxonomies collected
- Concepts defined
- Example system defined
- Tentative taxonomy prepared
  - However several important open issues exists
- Guidelines under preparation

DIGREL Guidelines

Chapter	Title
	List of Acronyms
	Executive Summary
1	Objective and Scope
2	Motivation
3	Uses of the Taxonomy within PRA
4	Definition of Terms
5	Approach and Assumptions, including description of the example
6	Taxonomies
7	Example(s), demonstration of taxonomy
8	Possible Data Sources and Data Collection Needs
9	Open Issues- Limitations
10	User Guidelines
11	Conclusion and Recommendations
12	References
	Appendix-Detailed example taxonomies
	Appendix-Detailed example system description

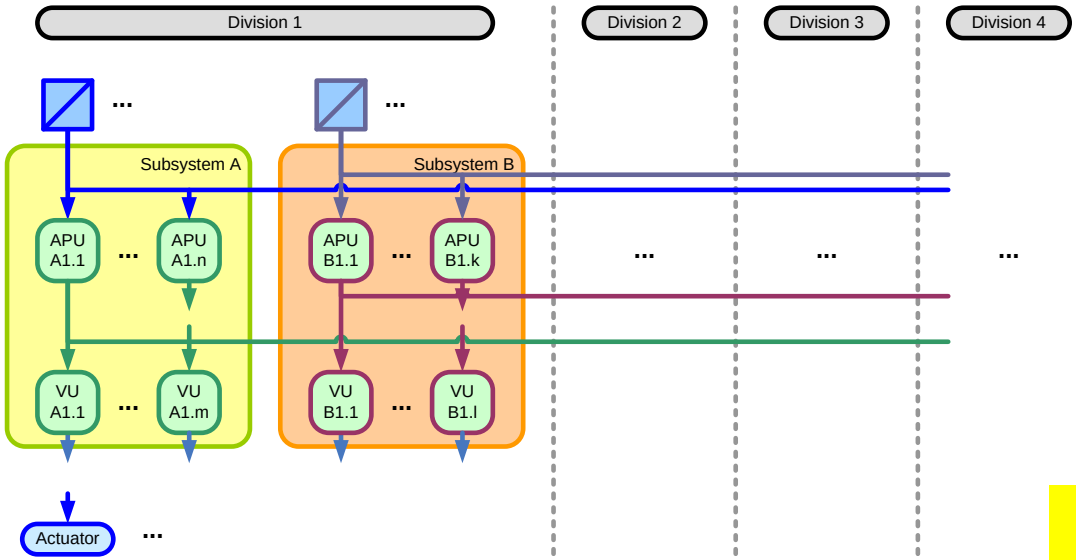
Dissemination of results

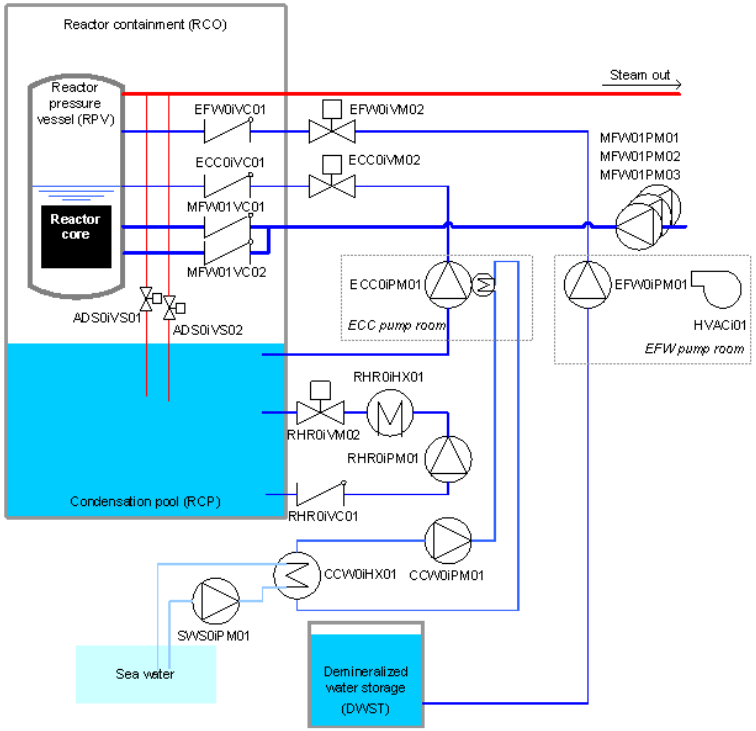
- WGRISK guidelines: draft 2012, final 2013 (WGRISK approval March 2013, CSNI meeting June 2013)

- Conference papers
  - PSAM11 (June 2012)
  - NPIC-HMIT (July 2012)
  - …
- Journal papers
  - Nuclear Engineering and Technology, Vol. 44, No. 5, 2012
  - …
- Nordic annual work reports NKS-230, NKS-261 (www.nks.org)

Nordic DIGREL achievements so far

- Nordic survey on state-of-the-art
- Example digital I&C PSA model prepared
  - Simple version 2011 as a MSc thesis
  - More complex version 2012 under preparation
- Interim reports prepared annually (2010, 2011) covering also modelling and data related issues





To be further discussed in the afternoon

Business from technology

WGRISK TG DIGREL, guideline development, overview, requirements for the taxonomy

DIGREL seminar, November 6, 2012, SSM, Stockholm, Sweden

Jan-Erik Holmberg, VTT

DIGREL Task objectives

- To develop technically sound and feasible failure modes taxonomy for **reliability assessment of digital I&C systems for PSA**
- To provide guidelines on the use of taxonomy **in modelling, data collection and quantification** of digital I&C reliability

Failure modes taxonomy in general

- Failure mode
  - manner in which failure occurs
  - may be defined by the function lost or the state transition that occurred
  - describes the function the components failed to perform (e.g., fail to run, fail to open, fail to close, fail to change position ...etc.)

- Taxonomy
  - The science of finding, describing, classifying and naming organisms
  - The classification in a hierarchical system

Purposes of FMEA and failure modes taxonomy

- Failure modes taxonomy is a framework of describing, classifying and naming failure modes associated with a system
- Main uses are in the performance of reliability analyses and in the collection of operating experience (failure data)
- The taxonomy is applied in FMEA and in the fault tree modelling
  - Combination of TOP-DOWN and BOTTOM-UP approaches

Generic failure modes

- Failure modes are always defined with respect to a certain function
- Therefore there are basically only two failure modes:
  - Failure to function
    - Failure to actuate, failure to perform the action, omission error, failure to change state, …
  - Spurious function
    - Spurious actuation, spurious change of state, …

Generic failure modes and operational status

- A component can have basically two operational modes:
  - In operation
  - Stand-by

Operational mode	State after: no function	State after: function
In operation	Spurious stop to function	Does not stop to function when demanded
Stand-by	Failure to start when demanded	Spurious start to function

- In principle, the above taxonomy should be sufficient

Generic failure modes and von Wright's elementary actions

- An elementary action: an action effecting **a change** or a **not-change** in the physical world
  - An elementary change: a succession in time of two contradictorily opposed states in the physical world
  - An elementary not-change again that a given state remains, stays on over a succession, stretch, in time

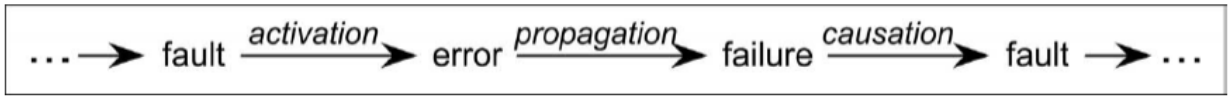
Elementary action	State before	State after	Failure mode
Productive	Stand-by	In operation/ changed status	Spurious start to function
Destructive	In operation	Not in operation	Spurious stop to function
Suppressive (preventive)	Stand-by	Not in operation/ not changed status	Failure to start when demanded
Sustaining	In operation	In operation	Does not stop to function when demanded

Why the previous simple, generic failure modes taxonomy is not always sufficient (is not used)?

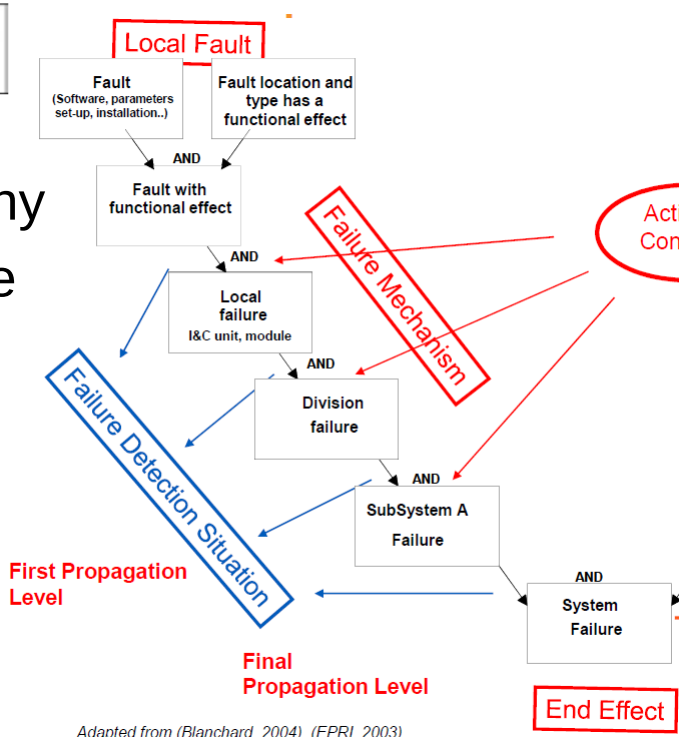
- For many components we are used to use more descriptive failure modes and more than two failure modes
  - More informative
  - Could match better with available data/quantification methods
  - However often the definitions used are ambiguous, mixes up with failure mechanisms, failure causes, failure effects, etc., do not explicitly address the failed function
- We need to consider interactions
  - Component 1 – Component 2
  - System – Component – Subcomponent
- From the PSA modelling point of view, we need to take into account more issues

Interactions – propagation of the failure

- Failure cause -> Failure -> Failure effect
- Failure propagation between components
  - Alternatively fault -> error -> failure (Algirdas Avizienis et al 2004)



- Failure analysis at different levels of the system hierarchy
  - The effect of the component failure is a cause of the system failure
  - Local effect w.r.t global effect



Adapted from (Blanchard, 2004), (EPRI, 2003)

Definitions will be further discussed in next presentations

Some other important dimensions of failure modes

- Time point of the failure w.r.t. the initiating event
  - Type A: before the initiating event
  - Type B: causing the initiating event
  - Type C: after the initiating event
- Failure detection
  - Detected
  - Undetected (latent)
- Criticality
  - Critical
  - Repair-critical
  - Non-critical
- System level
  - Full vs. partial failure
  - Single vs. multiple function failure

Example a
Failure modes for the system/signal level

1. Failure to generate signal in time (omission failure)
2. Spurious signal
3. Adverse effects on other functions (systems, operators)

- What do you think about this?

Example 2
Failure modes used for the microprocessor level

1. Hang
2. Abort
3. Missing operation
4. Extra operation
5. Erroneous operation

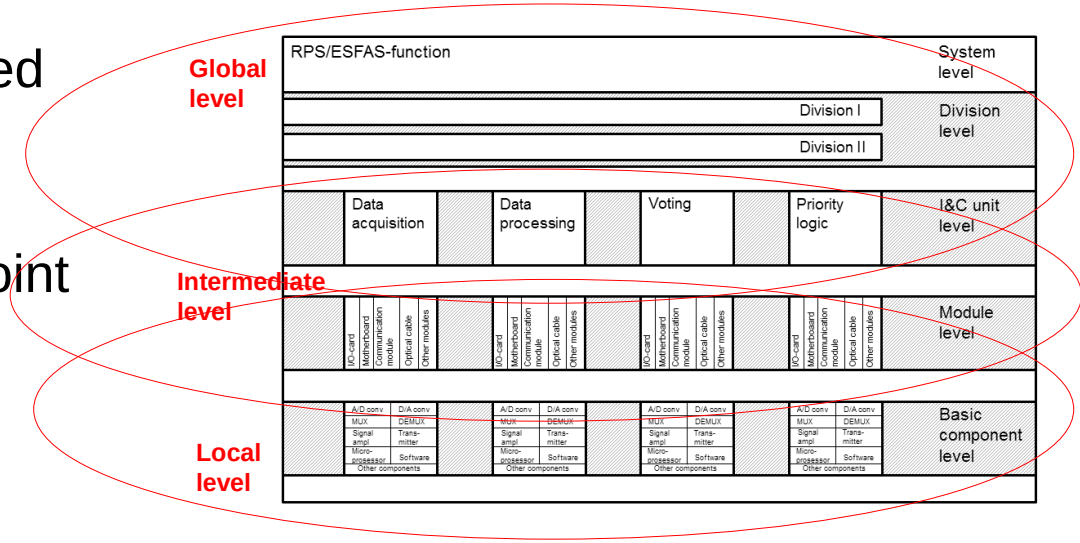
- What do you think about this?

DIGREL considerations
Requirements and desirable properties of the failure modes taxonomy

- 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 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 fault tolerant features and other essential design features of digital I&C

DIGREL
Failure modes taxonomy principles

- Hierarchical approach
  - Five levels defined
- At global level, failure modes considered only from the functional point of view
- At local level, failure modes are considered only from the local effect point of view
- In between there is the interesting intermediate level where the specific features of I&C system are considered
- Special attention to software failure modes
- CCF is not a failure mode



To be further discussed in the afternoon

DIGREL Example I&C system
Basis for the development of the taxonomy

- The design of the digital I&C of the safety important systems can be implemented on the basis of very different technologies
  - The differences may be significant
  - But, the stringent safety requirements lead to recognizable similarities of the architecture
- The example is assumed to representative enough for the taxonomy
  - Typical architecture
  - Typical hardware components
  - Typical operation modes (maintenance, testing, etc. not considered)
  - Typical means and features for failure detection and recovery
  - Typical majority voting for actuation

To be further discussed in the afternoon

DIGREL failure modes taxonomy summary

- DIGREL develops a failure modes taxonomy jointly by PSA and I&C experts — A “meeting point” needs to be defined
- DIGREL taxonomy principles
  - Requirements for the taxonomy
  - Material collected from member countries
  - Representative I&C system example (RPS) defined
- DIGREL taxonomy structure
  - Different levels of details of failures modes defined
  - Can either be based on a function view or a component view
  - At system/division/I&C unit level failure modes are considered only from the functional point of view
  - At module/basic component level failure modes divided into hardware and software related failure modes

Discussion on Definitions of Terms in Reliability Analysis of Digital I&C Systems

Man Cheol Kim[a], Jan C. Stiller[b], Carol S. Smidts[c]

[a] Korea Atomic Energy Research Institute, Daejeon, Korea

[b] Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Deutschland

[c] The Ohio State University, Columbus, Ohio, USA
Nuclear Engineering Program, DOE Academic Center of Excellence (ACE),
Instrumentation, Control and Safety

Outline

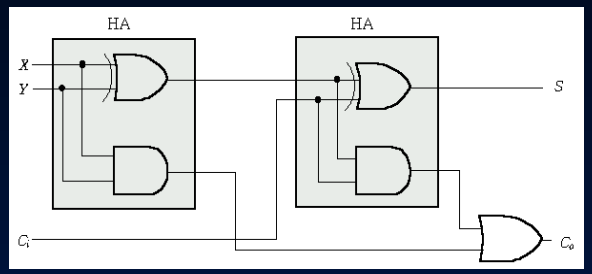
1. Introduction
2. Digital System
3. Main Standards Reviewed
4. Fault, Error, and Failure
5. Safety Classification
6. Dependencies
7. Conclusions

1. Introduction

- OECD/NEA WGRISK DIGREL Task Group
  - Project/Activity Title
    - Development of best practice guidelines on **failure modes** taxonomy for reliability assessment of **digital I&C systems** for PSA
- Terminology/Definitions
  - Support to the activity
  - Terms should be defined unambiguously to avoid a “Babel effect”
  - Particularly challenging because:
    - Spans a variety of countries
    - Spans a variety of disciplines
      - Computer Science (Digital Systems Software)
      - Electrical Engineers (Digital Systems Hardware)
      - Nuclear Engineers (Application Environment)
      - Risk Analysts (PRA Developers)
      - Regulators (Users of PRA)

2. Digital System

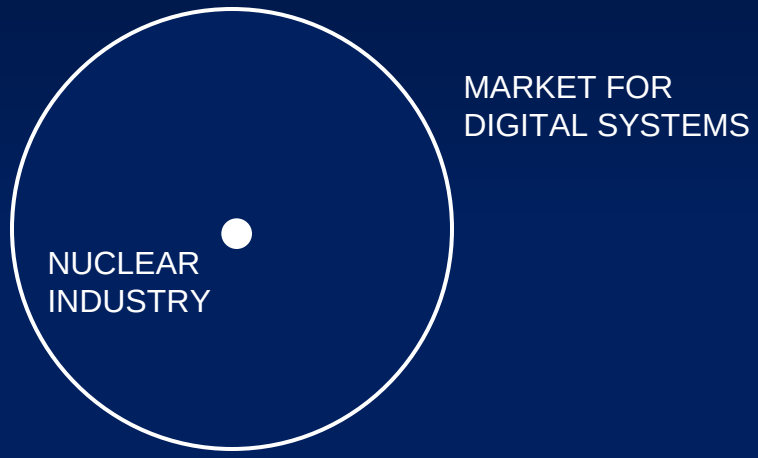
- Uses discrete values to represent information
- Incorporates a wide variety of systems



SIMPLE DIGITAL CIRCUIT

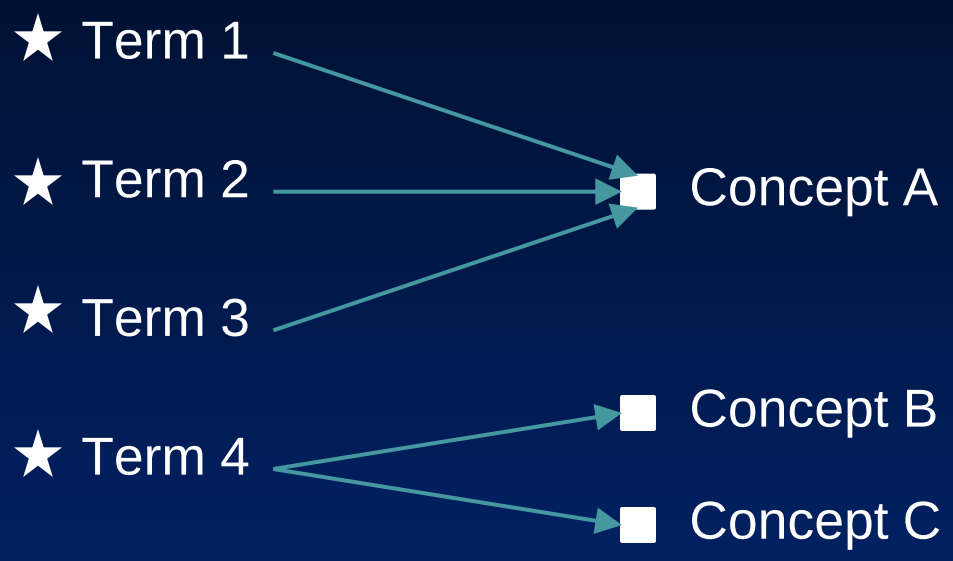
SUPERCOMPUTER

- The nuclear industry is a minor player in the market for digital systems



2. Digital System

- Findings from review of the literature (standards in particular) indicate:
  - A one-to-many and a many-to-one relationship exists between terms and concepts



3. Main Standards Reviewed

- IEC Standards
  - IEC 61508
    - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
  - IEC 61513
    - Nuclear Power Plants - Instrumentation and Control for Systems Important to Safety - General Requirements for Systems
- IEEE Standards
  - IEEE Std 603-1998
    - IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations
  - IEEE Std 7-4.3.2-2003
    - IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations

4. Fault, Error, and Failure

The most common terms used in system reliability analysis an

- Fault

Standard	tion
IEC 61508	abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function
IEC 62340 IEC 61513	defect in a hardware, software or system component
IEEE Std 7-4.3.2-2003 IEEE Std 610.12-1990	device or component; for example, a wire. 2. An incorrect step, process, or data definition in a computer program. (Note) This definition is used primarily by the fault tolerance discipline. In common usage, the terms "error" and "bug" are used to express this meaning.

May be questionable for software

No definition for software/hardware interactions

Defines faults using a new term which remains undefined

4. Fault, Error, and Failure

- Error

Standard	Definition
IEC 61508	discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition
IEEE Std 7-4.3.2-2003 IEEE Std 610.12-1990	1. The difference between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition. For example, a difference of 30 meters between a computed result and the correct result. (error) 2. An incorrect step, process, or da incorrect instruction in a compu ct result. For example orrect result is 10. (failure) ction that produces an incorrect result. For example, an incorrect action on the part of a programmer or operator. (mistake)

Narrow definition

Software reliability practice error ≡ human error that produces a fault

IEC uses error and mistake. Mistake is for human error

4. Fault, Error, and Failure

- Standard may recognize that at some point the component may become unable to perform its function

Implies a specific reliability model—may not be applicable to software, i.e., failure occurs when incorrect software is installed

	D
IEC 61508	termination of the ability of a functional unit to perform a required function
IEC 62340	ynamic. The definition istinguish between d permanent failures
IEEE Std 7-4.3.2-2003 IEEE Std 610.12-1990	the inability of a system or component to perform its required functions within specified performance requirements (NOTE) The fault tolerance discipline distinguishes between a human action (a mistake), its manifestation (a hardware or software fault), the result of the fault (a failure), and the amount by which the result is incorrect (the error).

event

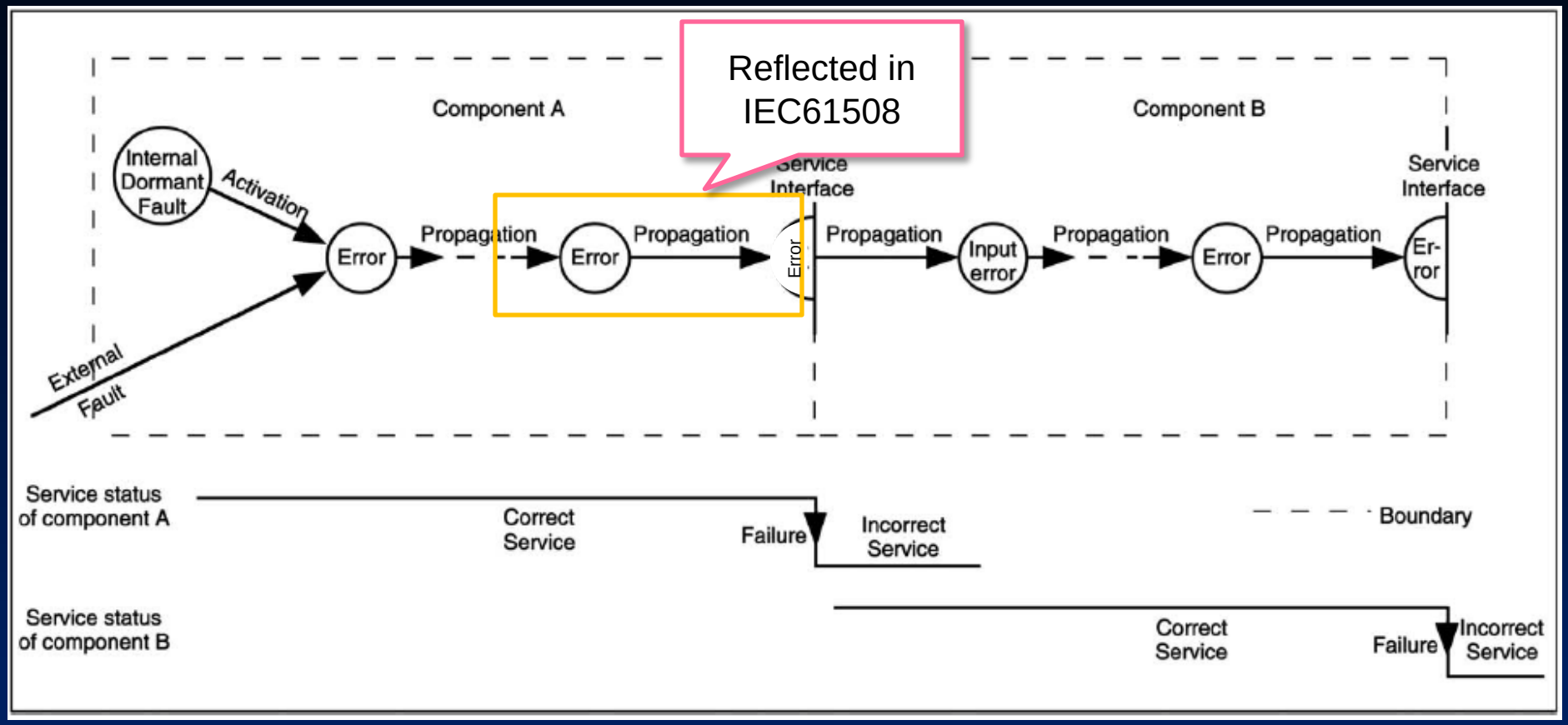
state

NO CONSENSUS

4. Fault, Error, and Failure

- Fault-error-failure chain

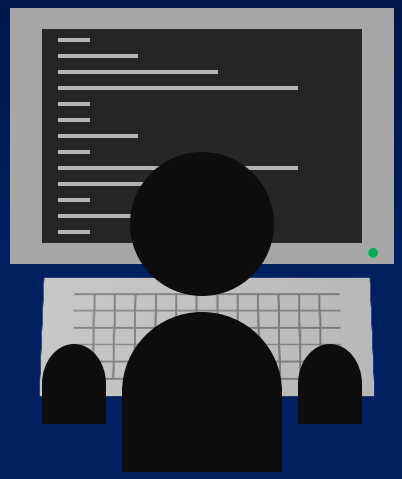
(Source: Algirdas Avizienis et al., 2004)

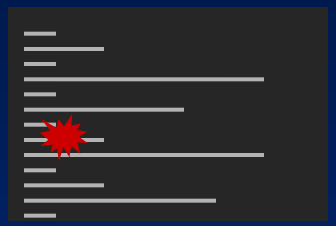


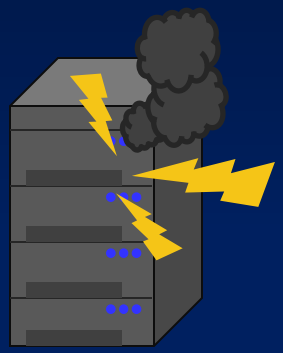
4. Fault, Error, and Failure

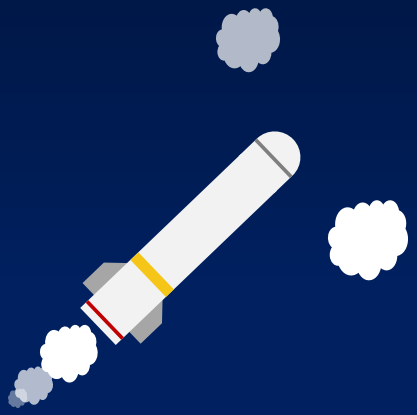
Reflected in IEEE7.4.3.2-2003

- Error-fault-failure chain
  - Error
    - An actual human error
  - Fault
    - The physical manifestation in the code, requirements, or design
  - Failure
    - What is experienced from the system perspective or mission perspective









5. Safety Classification

- The following terms are used to indicate the importance of a system relative to safety:
  - Safety system
  - Safety-related system
  - Safety-critical system
  - System important to safety

5. Safety Classification

Term	Standard	Definition
safety system	IEEE Std 603-1998	A system that is relied upon to remain functional during and following design basis events
	IEEE Std 7-4.3.2-2003	

Notes in IEEE Std 603-1998

1. The electrical portion of the safety systems, that perform safety functions, is classified as Class 1E.
2. This definition of “safety system” agrees with the definition of “safety-related systems” used by the American Nuclear Society (ANS) and IEC 60231A (1969-01).
3. Users of this standard are advised that “Class 1E” is a functional term. Equipment and systems are to be classified Class 1E only if they fulfill the functions listed in the definition.

5. Safety Classification

Term	Standard	Definition
safety system	IEEE Std 603-1998 IEEE Std 7-4.3.2-2003	A system that is relied upon to remain functional during and following design basis events
safety-related system	10 CFR 50.2	
	IEC 61508	designated system that both • implements the required safety functions necessary to achieve or maintain a safe state for the EUC; and • is intended to achieve … the necessary safety integrity for the required safety functions

Notes from NUREG/CR-6101

"The term *safety critical* refers to a system whose failure could cause an accident."

5. Safety Classification

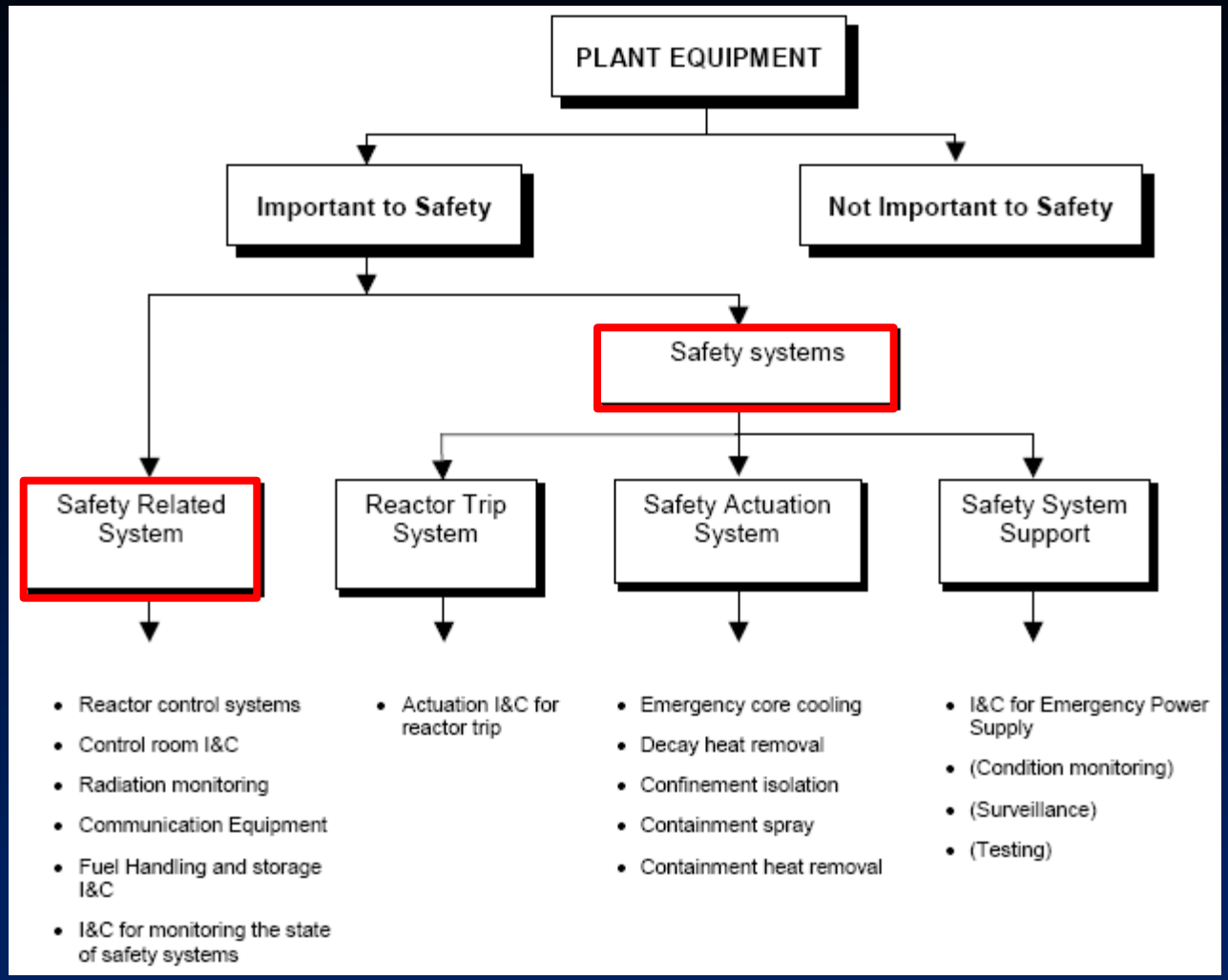
Source: IAEA-TECDOC-1402

ORGANIZATIONS AND/OR COUNTRIES	CLASSIFICATION			
IAEA	Systems Important to Safety		Systems not important to safety	
	Safety system	Safety related system		
IEC	Category A	Category B	Category C	Unclassified
France	1E	2E	IFC/NC	
European Utilities Requirements (EUR)	F1A (Automatic)	F1B (Automatic and Manual)	F2	Not Classified
UK	Category 1	Category 2	Not classified	
USA	1E	Non-nuclear safety		

Safety classification of important functions in nuclear power plants

5. Safety Classification

Source: IAEA-TECDOC-1402



Breakdown of safety equipment of a nuclear power plant

6. Dependencies

- Another interesting distinguishing feature between the IECstandards and the IEEE standards appears when one studies dependencies b etween items defined.

- If one considers IEC 61508 and IEEE Std 7-4.3.2-2003
- , we note that:

  - In the IEC standard, items are defined acyclicly;

  - In the IEEE standard, items are defined cyclicly;

- The end result is different- while the IEC standard may be clearer, the IEEE standard builds comprehensive relations between items defined.
- The IEC standard uses many isolated constructs (18/81) compared to the IEEE standard (3/52)

7. Conclusions

- Different definitions on the terms
  - Different definitions by different standards
    - IEC standards
    - IEEE standards
  - Different definitions by different disciplines
    - Fault tolerance discipline (fault-error-failure chain)
    - Software engineering discipline (error-fault-failure chain)
  - ISO/IEC/IEEE 24765-2010(E)
    - Systems and software engineering - Vocabulary
    - Mainly based on IEEE standards

→ Common understanding of basic concepts is important

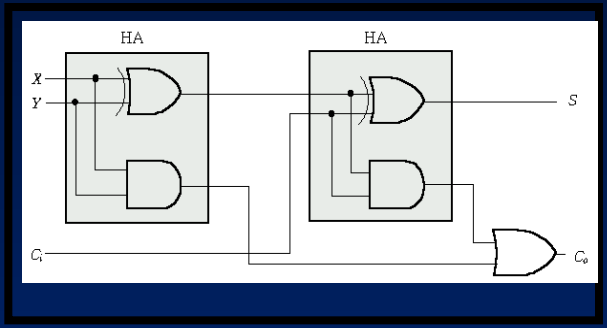
Questions?

Appendix

- OECD/NEA WGRISK DIGREL Task Group
  - Project/Activity Title
    - Development of best practice guidelines on **failure modes** taxonomy for reliability assessment of **digital I&C systems** for PSA

RTS : Reactor Trip System
ESFAS : Engineered Safety Features Actuation System

- Question
  - How should the target system (RTS/ESFAS) be called?
    - Safety-critical digital I&C system
    - (Digital) computer-based safety system
    - Digital computer in safety systems
    - Software-based safety system
    - Programmable system
    - Electric equipment important to safety
    - Class 1E digital computer system



A Summary of Taxonomies of Digital System Failure Modes Used in Recent Studies

NKS/DIGREL Seminar, Stockholm

November 6, 2012

Tsong-Lun Chu
Nuclear Science and Technology Department
(631-344-2389, Chu@BNL.GOV)

BROOKHAVEN NATIONAL LABORATORY

a passion for discovery

Office of Science
U.S. DEPARTMENT OF ENERGY

Outline of Presentation

- Background
- Collection of failure mode information from the participants
- Levels of detail of digital systems
- Summary of failure modes from participants
- Conclusions and ongoing work

Background and Objective

- In 2007, the OECD/NEA CSNI directed the Working Group on Risk Assessment (WGRisk) to set up a task group to coordinate activities in digital system reliability.
- Task report NEA/CSNI/R(2009)18, OECD/NEA/CSNI, Paris, 2009 http://www.oecd-nea.org/nsd/docs/2009/csni-r2009-18.pdf summarizes research activities of participating countries/organizations and recommendation of future research.
- One of the recommendations was to develop a taxonomy of failure modes of digital systems for the purposes of probabilistic safety assessment (PSA).
- A new task group (abbreviated as DIGREL) was started 2010 with the goal of developing a failure mode taxonomy or taxonomies.
- This presentation summarizes the inputs provided by participants of the project.

Collection Of Failure Modes Information

- The first workshop of the DIGREL TG was held on May 16-19, 2011 in Bethesda, Maryland, U.S.A. During the workshop, participants presented information on their failure mode work and ideas on the development of a failure mode taxonomy.
- In addition, the participants provided some written information about their research in this area including hardware and software failure modes, FMEAs, and modelling methods.
- The failure mode inputs from the participants are summarized according to the different levels of detail agreed upon by the participants.

Hardware Levels of Detail

- **System level:** A collection of equipment that is configured and operated to serve some specific plant function as defined by terminology of each utility.
- **Division level:** A system can be carried out in redundant or diverse divisions. A division may consist of the pathway(s) from sensor(s) to generation of an actuation signal. The actuation signal can be sent to multiple actuators. A division can be decomposed further into I&C units.
- **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.
- **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.
- **Basic components 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.

Software Levels of Detail

- **System level:** For a digital reactor protection system (RPS), 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:** For the redundant or diverse divisions of an RPS, 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.
- **Module level/microprocessor level:** For the software program running on a particular microprocessor, the software is treated as an individual component like the microprocessor of a module.
- **Sub-module level:** 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.

Hardware Failure Modes

- The failure modes are often defined in terms of the functions, e.g., failure to actuate and spurious actuation. Some failure modes are more descriptive (and like failure causes), e.g., round-off/truncation/sampling rate errors and setpoint corruptions.
- Some failure modes are defined as detectable and non-detectable.
- Some failure modes are in terms of the value of the signals being processed, e.g., many of those at the basic component level.

Software Failure Modes

- At system level, the failure modes are the same as those of hardware functional failures, and timing of load sequencer and specific actuation signals of ESFAS are also used in the definition.
- Due to the common assumption that divisions running the same software would fail together and cause a system failure (i.e., they are effectively system failure modes), no specific division level failure modes was defined.
- At module level, function specific failure modes were defined, e.g., incorrect voting. At microprocessor level, generic failure modes were defined, e.g., software stalls, software aborts.
- At sub-level, functional failure modes associated with signals to valves and pumps were defined.

Conclusions and Going Forward

- The taxonomy of failure modes summarized here represents preliminary results collected from participants. The working group is developing a consensus failure mode taxonomy for both hardware and software based on the input of the participant and the discussions during the workshops. Other presentations of DIGREL provide information about the progress made so far.
- The taxonomy needs to be defined and maintained at various levels of detail to provide options to PRA analysts and/or I&C system designers such that the taxonomy at a particular level of detail can be selected based on their own FMEA and/or reliability modelling need.
- It is generally agreed that a modelling method needs to capture dependencies and fault tolerant features, use meaningful failure modes, and propagate failure effects.

WGRISK TG DIGREL

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

Topic:
Example System

Ewgenij Piljugin, GRS

2012-11-06

NKS/DIGREL Seminar, Stockholm, Sweden

Introduction

- General remarks
- The Example System Architecture
  - Basis for the development
  - Architecture of the hardware
  - Overall software architecture
- Concept for identification of generic FMs of the hardware
- Outlook

Disclaimer

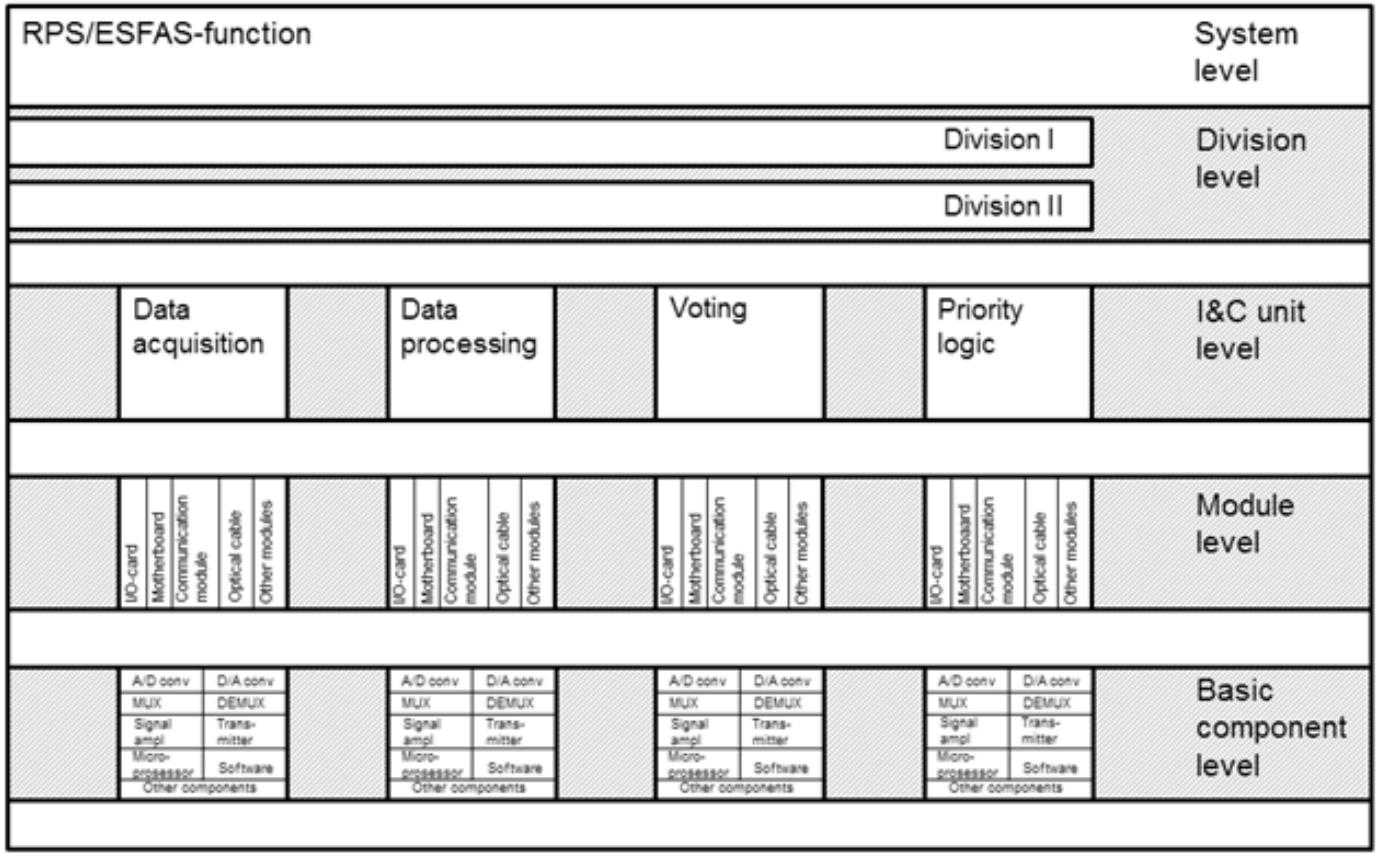
Note! The results presented here are preliminary and the slides reflect discussions in the DIGREL Task Group, but are not necessarily agreed by the task group

General remarks (1)

- Several modern technical standards and guidelines determine the methodology of the state-of-the-art FMEA of electronic equipment, e.g.
  - IEC 60812. Analysis techniques for system reliability - Procedures for failure mode and effect analysis (FMEA),
  - IEC 60300-1. Dependability management - Part 1: Dependability management systems,
  - SAE ARP 5580. Recommended Failure Modes and Effects Analysis (FMEA) Practices for Non-Automobile Applications
- Application of the FMEA to a technical system or an equipment requires initially
  - Definition of the system (equipment) and its functional breakdown,
    - Preparation of functional block diagrams of the system (equipment) including internal and external signal and data flows,
    - Determining the level of details (e.g. function→unit →module)
  - Establishing of basic rules and assumptions including mission requirements (e.g. control or monitoring functions)
    - Description of the operational modes of the equipment (e.g. continuous mission, stand-by, cyclic operation, maintenance, failure detection).

General remarks (2)

Principal decomposition of a safety I&C function into different levels of details.



General remarks (3)

- Actual challenges by application of the FMEA Methodology for a complex digital I&C system :
  - Appropriate decomposition of the system (e.g. modules, basic components) for identification of all relevant functions and of all relevant failure modes (FMs)
  - Consideration of the software
    - Boundaries of the software modules
    - Consideration of dependencies
    - Definition of the FMs
    - Identification of the failure effects (comprehensibility?)
  - Consideration of the fault tolerance features (e.g. network communication) by evaluating of the FMs
    - failure detection means
    - fault handling possibilities
    - fail safe principles

General remarks (4)

- The following aspects of the hardware of digital I&C should be considered in the DIGREL taxonomy approach:
  - typical architecture of digital I&C systems performing safety functions (e.g. Reactor Protection 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 of failure recovery,
    - typical majority voting for actuation of RPS/ESFAS functions.
  - Evaluation of the failure modes under consideration
    - Spurious actuation,
    - Loss of operability (required function) on demand,
    - Failure to operate at the proper time,
    - Failure to stop operating at the proper time,
    - Loss of output,
    - Degraded output or reduced operational capability.

General remarks (5)

- The level of detail for the decomposition of the hardware of a generic digital I&C system (Example System) shall
  - support PSA practice,
  - capture all critical dependencies and design features,
  - be appropriate for safety-important systems,
  - support modeling of CCF at necessary level.
- With regard to the analysis and modeling of the safety-important I&C functions in the PSA, the following levels of detail can be distinguished:
  - 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. basic components of modules.
- The most suitable level of detail was identified to be the module level which concurs with the level of detail of PSA methodology state of the art.

Basis for the development of the Example System (1)

- Digital I&C architectures are deployed in several reactors worldwide, e.g.
  - NPPs Chooz B (France), Sizewell B (UK), Ringhals-1 and -2 (Sweden), Temelin-1/2 (Czech Republic), Tianwan-1 and -2 (China),
  - also new designs, e.g. the EPR (AREVA), the APWR (MHI), ESBWR (GEH) demonstrate the recent state concerning digital I&C architectures in NPPs.
- In general the design of the safety-important digital I&C systems could be implemented in different reactor design on the basis of different technologies and architectures and platforms of the digital I&C.
  - The dissimilarities between different I&C platforms may be significant, e.g. equipment, design, fault tolerant features and voting logic.
  - However the stringent safety requirements on design, manufacturing and operating of the safety-important systems in the nuclear power plants lead consequently to recognizable similarities of the architecture of several digital safety-important I&C systems and of their functions.

Basis for the development of the Example System (2)

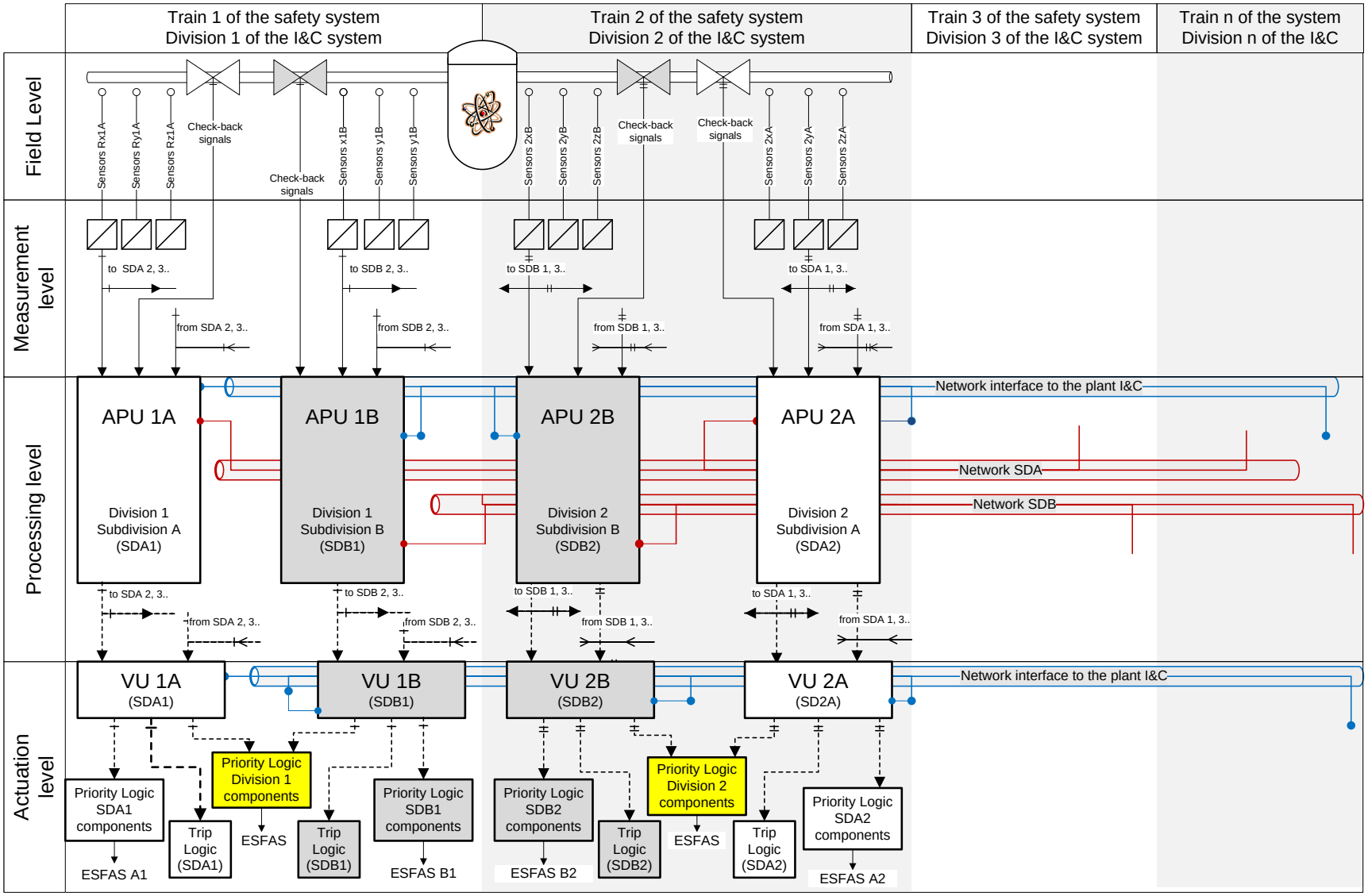
- The development of a generic digital I&C system (EDICS) was inspired by some examples of the implementation of the following different platforms of digital I&C for safety functions:
  - Teleperm XS, e.g.
    - EPR reactor design, modernization projects in several NPPs,
  - Common Q / Advant AC160 system, e.g.
    - AP1000 reactor design,
  - Westinghouse Eagle 2000/ Westinghouse Ovation, e.g.
    - Sizewell-B, Temelin 1 & 2.

Basis for the development of the Example System (3)

- Main evaluation steps of the Example Digital I&C System (EDICS)
  - draw up a flexible generic architecture of a simplified model of a typical DIC system
    - the overall architecture of the safety importantI&C system,
    - the divisions: redundant structure of the signal processing, consideration of the internal redundant structure of the divisions
  - break down a simplified model of the generic DIC system into generic parts (components) of the hardware
    - I&C units: computerized unit dedicated to data acquisition, processing, voting and actuator control (APU, VU, …)
    - modules: modules of I&C units (PMM, AIM, AOM, DCU…)
    - basic components: basic parts (elements) used to build a digital system, unit, module

Architecture of the hardware of the Example System (1)

Overall architecture of the EDICS



Architecture of the hardware of the Example System (2)

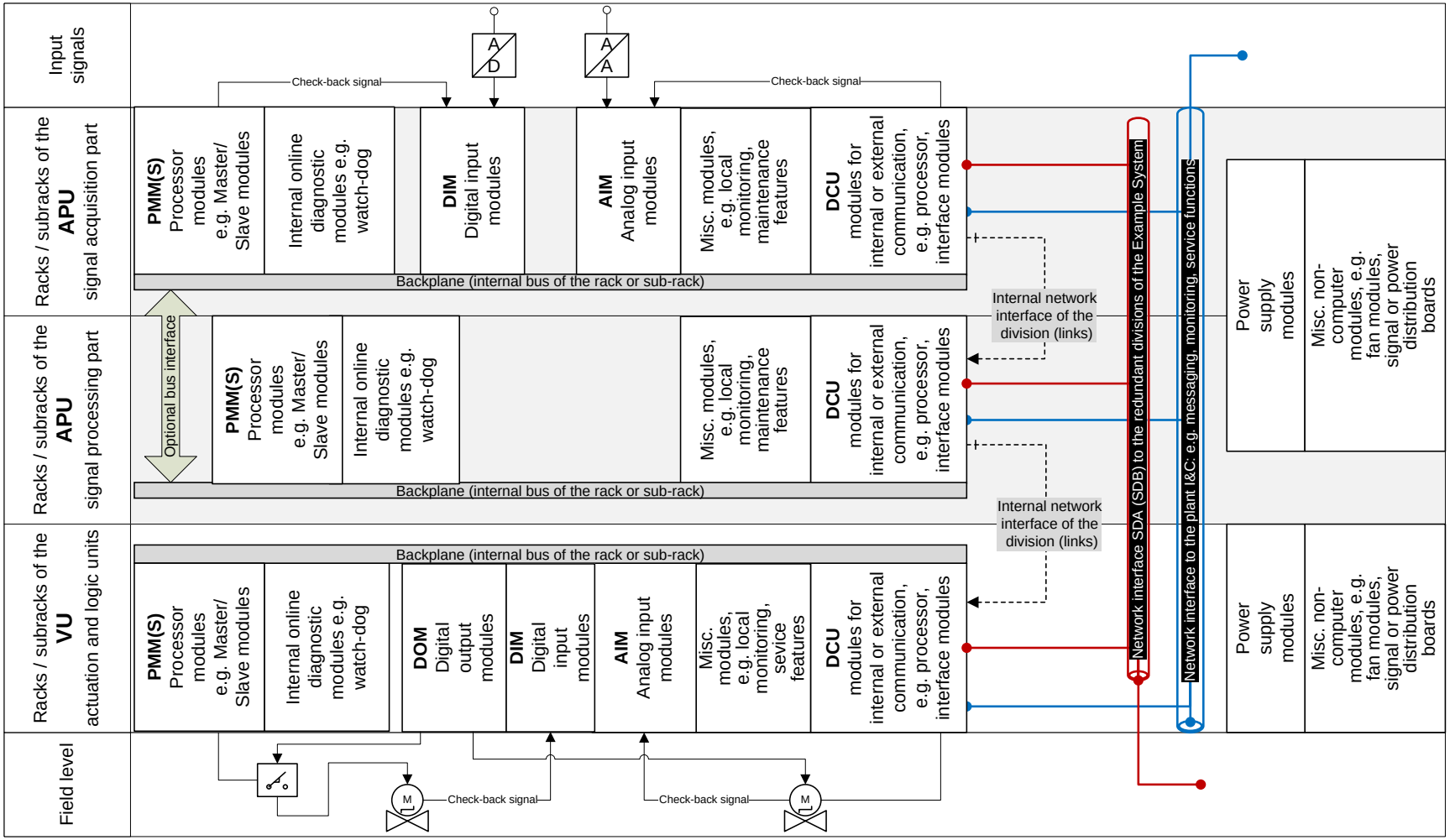
- The architecture can consider various different architectures of the safety-important DIC systems regarding evaluation of the FMEA:
  - In one case the sub-divisions Div. 1, 2, ...(A) and Div. 1, 2, …(B) of the EDICS can be interpreted as implementation of the functional diversity (functions A and B) inside one division based on a common I&C platform,
  - In the other case the sub-divisions Div. 1, 2, ...(A) and Div. 1, 2, …(B) of the EDICS can be interpreted also as diverse redundant divisions of the diverse I&C systems A and B based on different I&C platforms, e.g. the redundant channels of a primary and of a secondary (diverse) protection system.

Architecture of the hardware of the Example System (3)

- The generic architecture of the hardware of the entire signal processing of the EDICS consists of the following kinds of hardware (functional units of a generic hardware platform):
  - Processor modules for signal processing,
  - Communication modules, cables, optical links,
  - Input and output modules of digital or analog signals,
  - Electrical items such as electrical connections, cables and power supply modules.
  - Mechanical components such as racks, fans and cabinets for housing the above modules.

Architecture of the hardware of the Example System (4)

Module level architecture of the APU and of the VU units inside the divisions of the EDICS



Architecture of the software of the Example System (1)

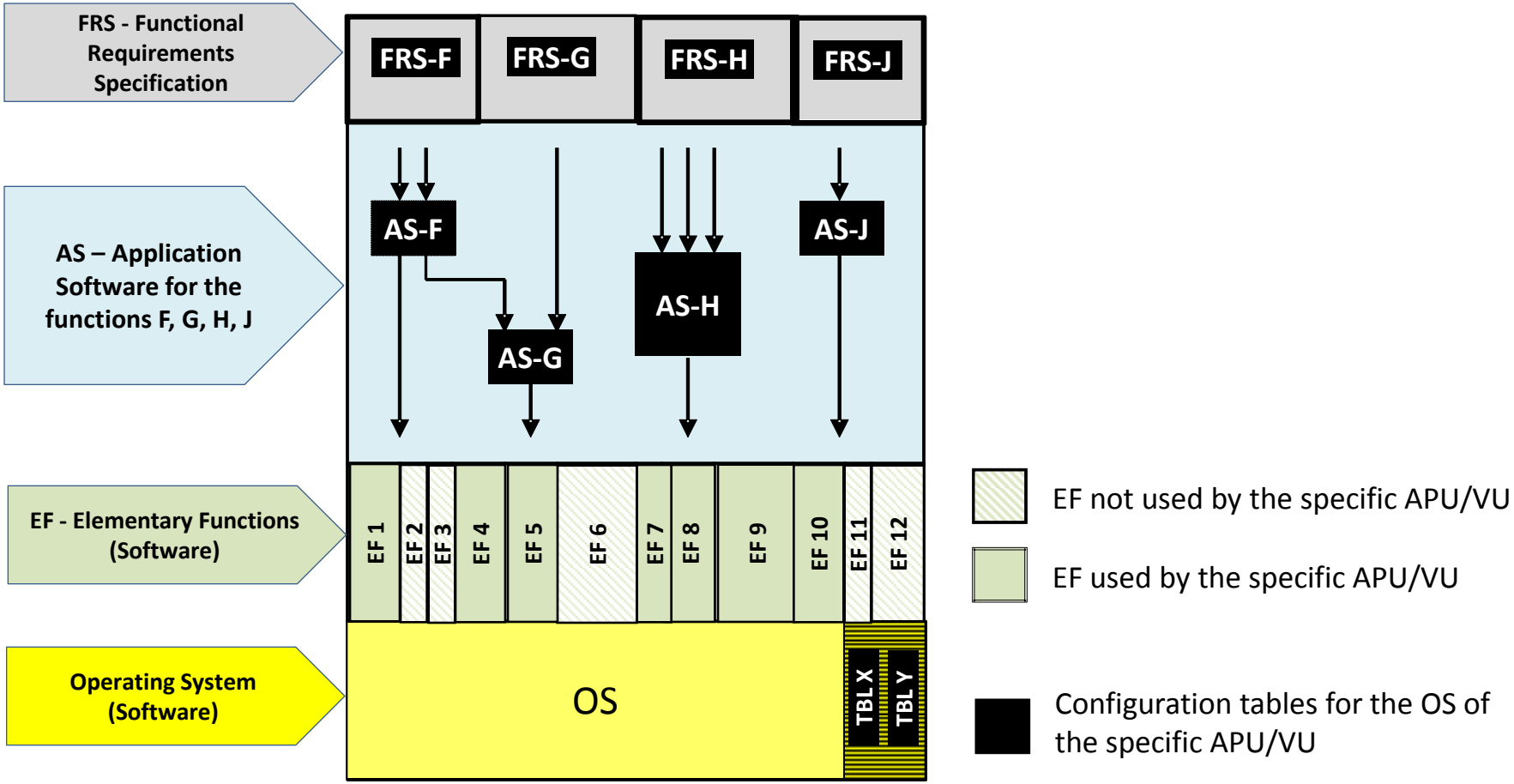
- The software of an APU of the Example System can be decomposed into the following software modules:
  - Operating System (OS):
    - this module controls the overall functioning of the APU. It is a part of the I&C platform software.
  - Elementary Functions (EFs):
    - these modules provide readily useable standard functions such as mathematical functions or delays. They are a part of the I&C platform software.
  - Application-specific Software (AS):
    - typically, an APU supports multiple application functions, and the specific software for each of these functions is an AS module. Homologous APUs in redundant divisions have principally the same sets of AS modules.

Architecture of the software of the Example System (2)

- The organisation of the software of a DCU modules can be decomposed into the following software modules:
  - Operating System (OS):
    - the OS of a DCU is the same as the OS of the APUs and VUs
  - Data Communication Software (DCS):
    - this module implements the data communication protocol. It is part of the platform software
  - Data Link Configuration (DLC):
    - this module is provided in the form of a data table.

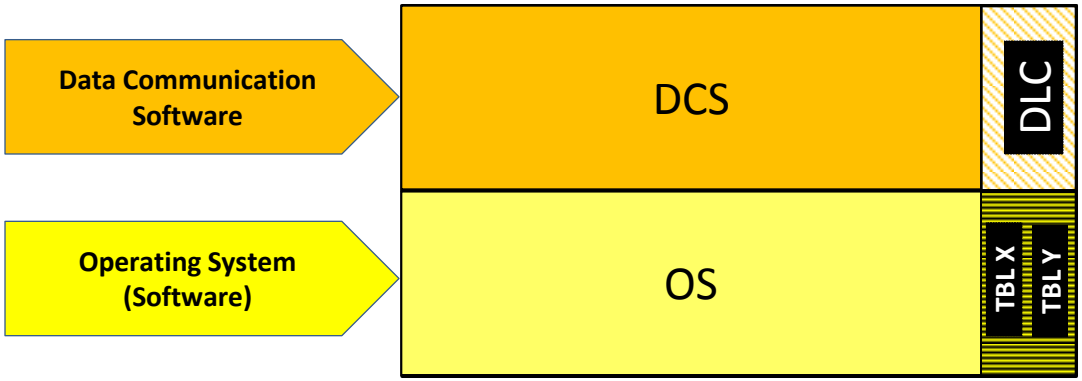
Architecture of the software of the Example System (3)

Software architecture of the processing modules of an APU or VU



Architecture of the software of the Example System (4)

Software architecture of the communication modules (DCU) of an APU or VU



Configuration tables for the OS of the specific APU/VU

Concept for evaluation of generic FMs of hardware

Proposal of a FMEA Worksheet of the signal processing units APU/VU

Decomposition of the specific I&C system into hardware modules on the basis of the EDICS	Examples			
	Failures modes of hardware modules FM	Failure effect of the function of the next module / unit	Detection of the failure: e.g. monitoring, test	Relevance regarding execution of the SW
Processing Unit Module	PMM1: CPU stalls	loss of signal processing	watchdog message	no execution
Digital Input Module	undefined output of Ch.1	PM: loss of information from Ch.1	APU message „Input Ch.1 failed“	no impact
Analog Input Module	output of Ch.2 fails to low	PM: loss of information from Ch.2	APU message “out of range“	no impact
Digital Output Module	output of Ch. fails to 1	APU: spurious actuation	message „Drive ON“	no impact
Analog Output Module	?	?	?	?
Communication Module	loss of one telegram DCU1 to DCU2	DCU:disturbance of one cycle of communication	DCU monitor: message „one telegramm lost“	APU: no impact
Misc. Modules e.g. fans, power supply modules, backplane.	loss of fan function	temperature inside of the APU cabinet will be increased	APU messages: „APU cabinet temperature to high“	?

Outlook

- The DIGREL task group intends, in a next step,
  - to complete the development of the architecture of the Example System (EDICS),
  - to finalize the evaluation of the generic failure modes of the hardware and
  - to accomplish the draft of the DIGREL guidelines report.

Digital I&C Failure Modes Taxonomy

General Approach

Gilles DELEUZE, Electricité de France

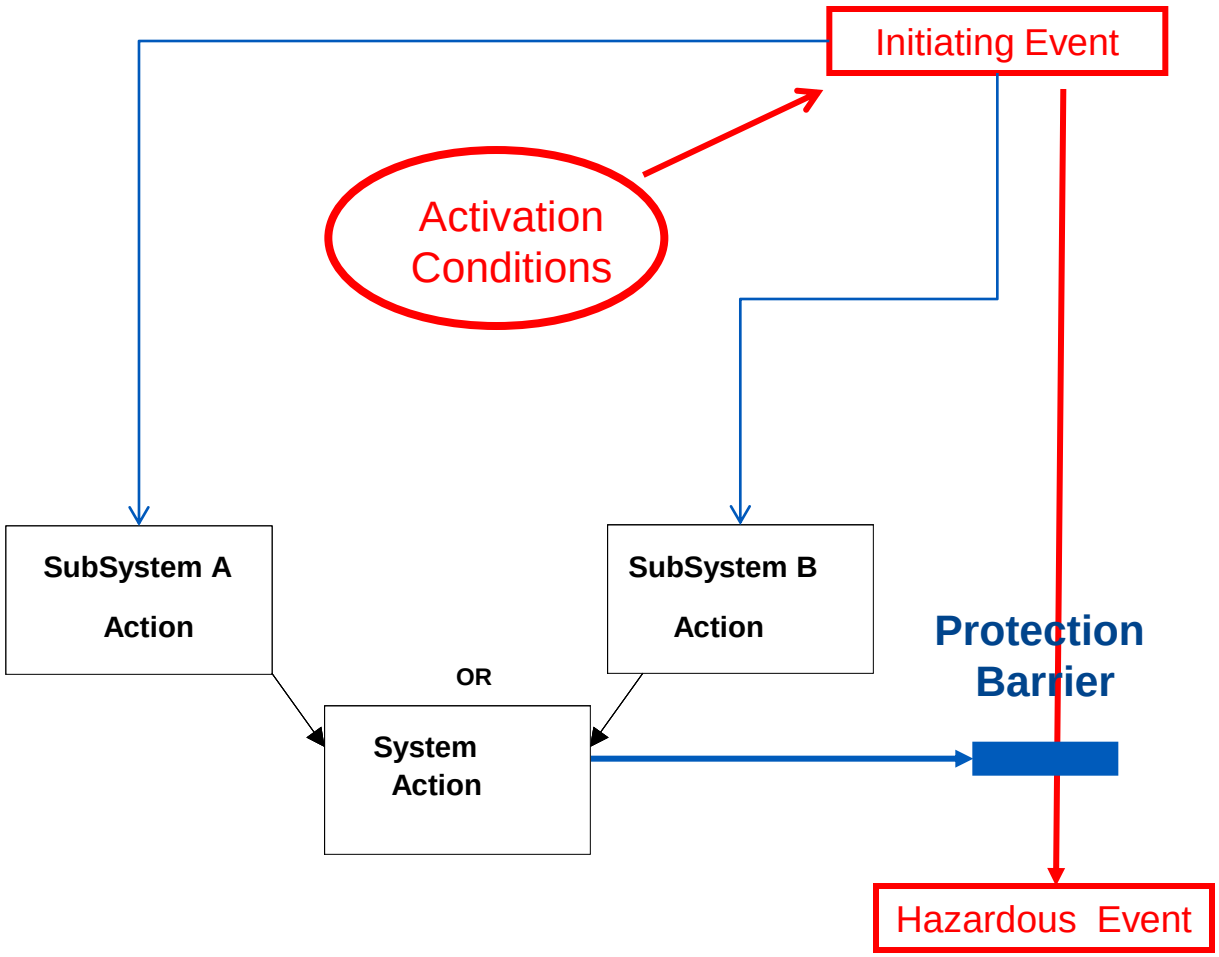
WGRisks DIGREL Meeting

Stockholm, 6 November 2012

Summary

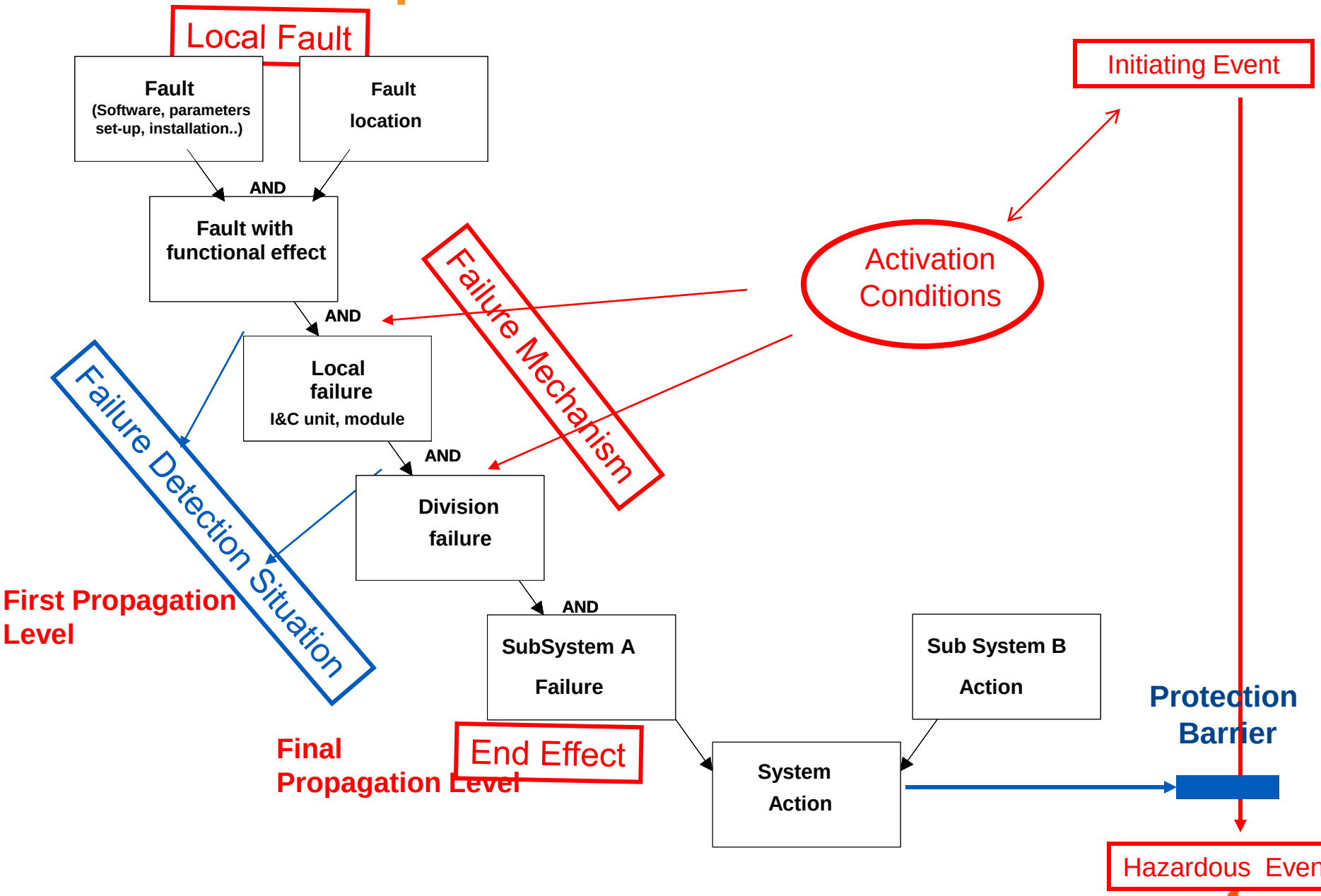
- General Principles
- Taxonomies at various Architecture Levels
- Taxonomy and PSA

General Principles – The fonctional model



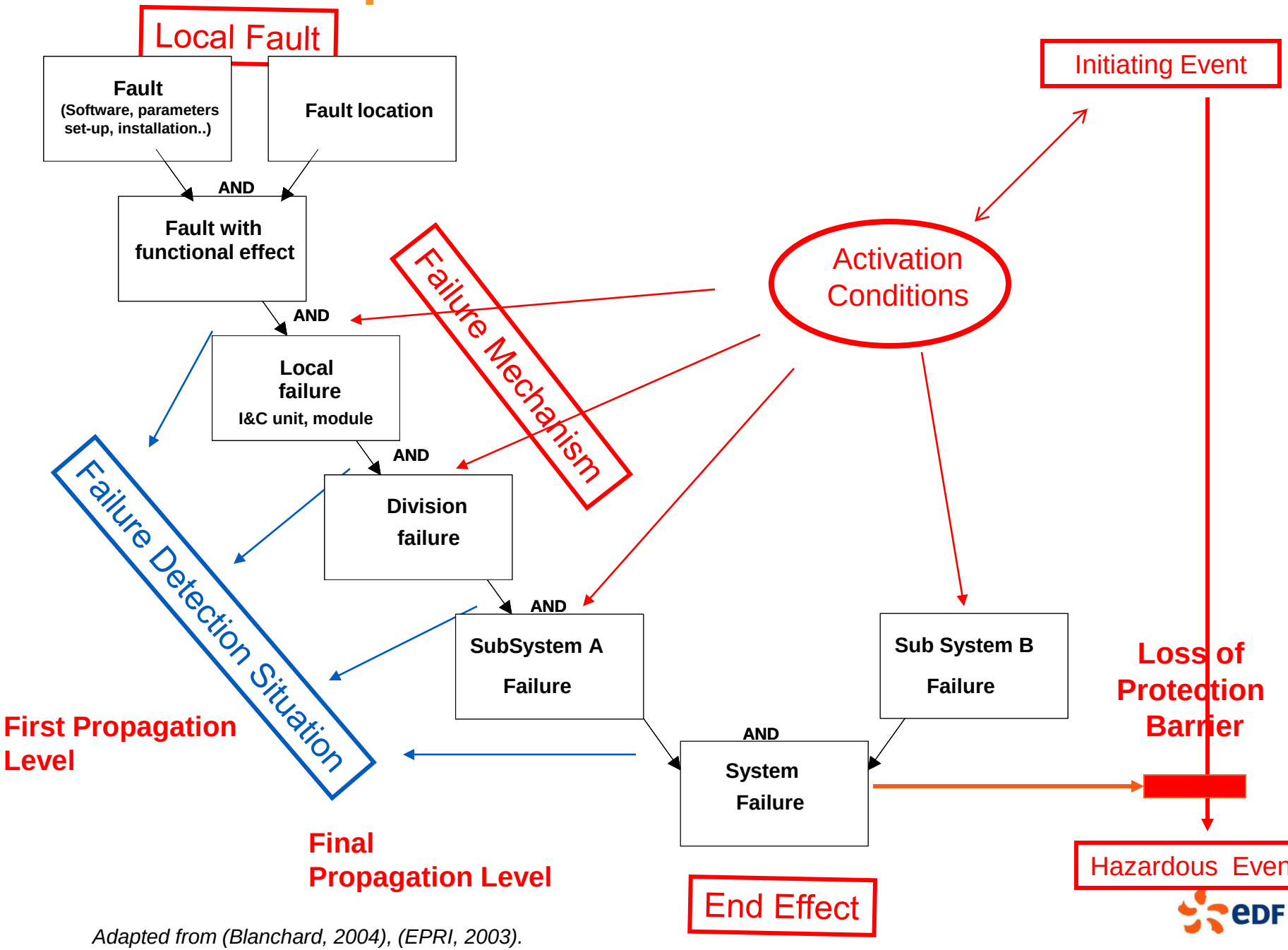
Adapted from (Blanchard, 2004), (EPRI, 2003).

General Principles – The failure model



Adapted from (Blanchard, 2004), (EPRI, 2003).

General Principles – The failure model



Adapted from (Blanchard, 2004), (EPRI, 2003).

Taxonomies at various Architecture Levels

- System Level taxonomy
- Division Level taxonomy
- I&C Unit Level taxonomy
- Module Level taxonomy
- Basic Component Level taxonomy

Taxonomies at various Architecture Levels

- System Level taxonomy
- Division Level taxonomy
- I&C Unit Level taxonomy
- Module Level taxonomy
- Basic Component Level taxonomy

Functional point of view.
No difference between hardware or software aspects.

Taxonomies at various Architecture Levels

- System Level taxonomy
- Division Level taxonomy
- I&C Unit Level taxonomy

Functional point of view.
No difference between hardware or software aspects.

- Module Level taxonomy
- Basic Component Level taxonomy

Various points of view.
Differences between hardware or software aspects.

System Level taxonomy

- Safety function = generation of safety actuation signal in a predefined time interval only when required

- Four possible combinations

Required output / System output	Actuation	No actuation
Actuation	Success	Failure (Spurious actuation)
No actuation Late actuation Partial actuation	Failure (Failure-on-demand)	Success

Failure modes at system level

- Relevant for protection systems that are not under continuous demand
- Failure modes independent of the architecture, DiD and diversity strategies of the protection systems.

Division Level taxonomy

- A system may have redundant or diverse divisions.
- Safety function = generation of safety actuation signal in a predefined time interval only when required

Required output / System output	Actuation	No actuation
Actuation	Success	Failure (Spurious actuation)
No actuation Late actuation Partial actuation	Failure (Failure-on-demand)	Success

Failure modes at division level

- Relevant for protection systems that are not under continuous demand
- Failure modes independent of the architecture, DiD and diversity strategies of the protection systems.

Taxonomies at various Architecture Levels

- System Level taxonomy
- Division Level taxonomy
- I&C Unit Level taxonomy
- Module Level taxonomy
- Basic Component Level taxonomy

I&C Unit Level taxonomy

- More complex than System and Division levels
  - A division (or a system with no division) consists of one or more I&C units.
  - I&C units perform various functions. Some are necessary (*critical*) at division or system levels.
- FMEA at I&C Units level require a Failure Model and inputs (taxonomies)
  - I&C Units categories
  - I&C Units faults/defects Locations
  - I&C Units failures modes
  - I&C Units failures Detection Situations

I&C Unit Level
I&C Units Categories

- Acquisition & Processing Unit (APU)
- Voting Unit (VU)
  - Some systems have no VU
- Data Communication Unit

Dependent of the architecture of the protection system

I&C Unit Level

Faults /defects locations in I&C Units

- Permits to assume where faults/defects can be located in the various I&C units of the protection system

I&C unit category	Possible defect locations at I&C Unit level
Acquisition & Processing Unit (APU)	Operating System Elementary Functions (APU) Application Specific Software (APU) Functional Requirements Specification (APU) APU input module hardware APU processing module hardware APU subrack hardware
Voting Unit (VU)	Operating System Elementary Functions (VU) Application Specific Software (VU) Functional Requirements Specification (VU) VU output module hardware VU processing module hardware VU subrack hardware
Data Communication Unit	Operating System Data Communication Software Application Specific Software (Data Link Configuration) Link module Hardware DCU subrack hardware Network wires APU/DCU Interface

I&C Unit Level

I&C Units Failure Modes

- Every critical fault/default location is now assumed to cause a failure.
- The analyst has first to determine its effects *where it occurs*

Failure Modes		Local Effect	Note
Functional Effect	Fatal/ hang	• Defined output, ordered output • The outputs of the I&C unit are set to specified, supposedly safe values. The means to force these values are usually exclusively hardware	In the situation of Fatal Failures, the I&C unit ceases functioning and does not provide any exterior sign of activity.
		• Undefined output, Haphazard behaviour* • The outputs of the I&C unit or the hardware module are in unpredictable states	Fatal, haphazard failures are very unlikely on protection systems.
	Non Fatal (example: intermittent operation)	• Plausible Behavior (Exple: stuck to current value , significant delay) • It is difficult for an external observer to determine whether the I&C unit or the hardware module has failed or not • Non Plausible Behavior (Exemple: non consistent alarms, haphazard successive spurious actions...) . An external observer can rapidly decide that the I&C unit or the hardware module has failed	In the situation of Non Fatal Failures, the I&C unit or the hardware module continues to generate outputs
No Functional Effect		Various effects	Not to be considered in FMEA or PSA

- Relevant for a protection system, that is not under continuous demand
- The failures originate from hardware, or software, or software/hardware interactions.

I&C Unit Level

I&C Units Failure Modes

- Examples of Failure Modes at I&C Unit level

Failure modes and local effects	Examples
Ordered Fatal Failures	Divisions by zero or illegal access to memory (e.g., writes to ROM or read/writes to inexistent memory addresses) will be trapped by the microprocessor exception mechanisms; the usual action is then to halt the microprocessor so that hardware watchdogs can force the outputs to the specified, safe values.
Haphazard Fatal Failures	Not relevant for safety systems. Defensive measure: watchdogs are purely based on hardware.
Failures with Plausible Behaviour	Inadequate requirements specification for a given I&C unit function is likely to be non-fatal and could lead to a faulty but plausible behaviour. The other functions of the I&C unit may remain unaffected and behave correctly, unless they are functionally dependent on the failed function.
Failures with Non-plausible Behaviour	Activation of a software implementation error could lead to outputs that are not in the expected range of values Drift of an analog component

I&C Unit Level

I&C Units Detection Situations

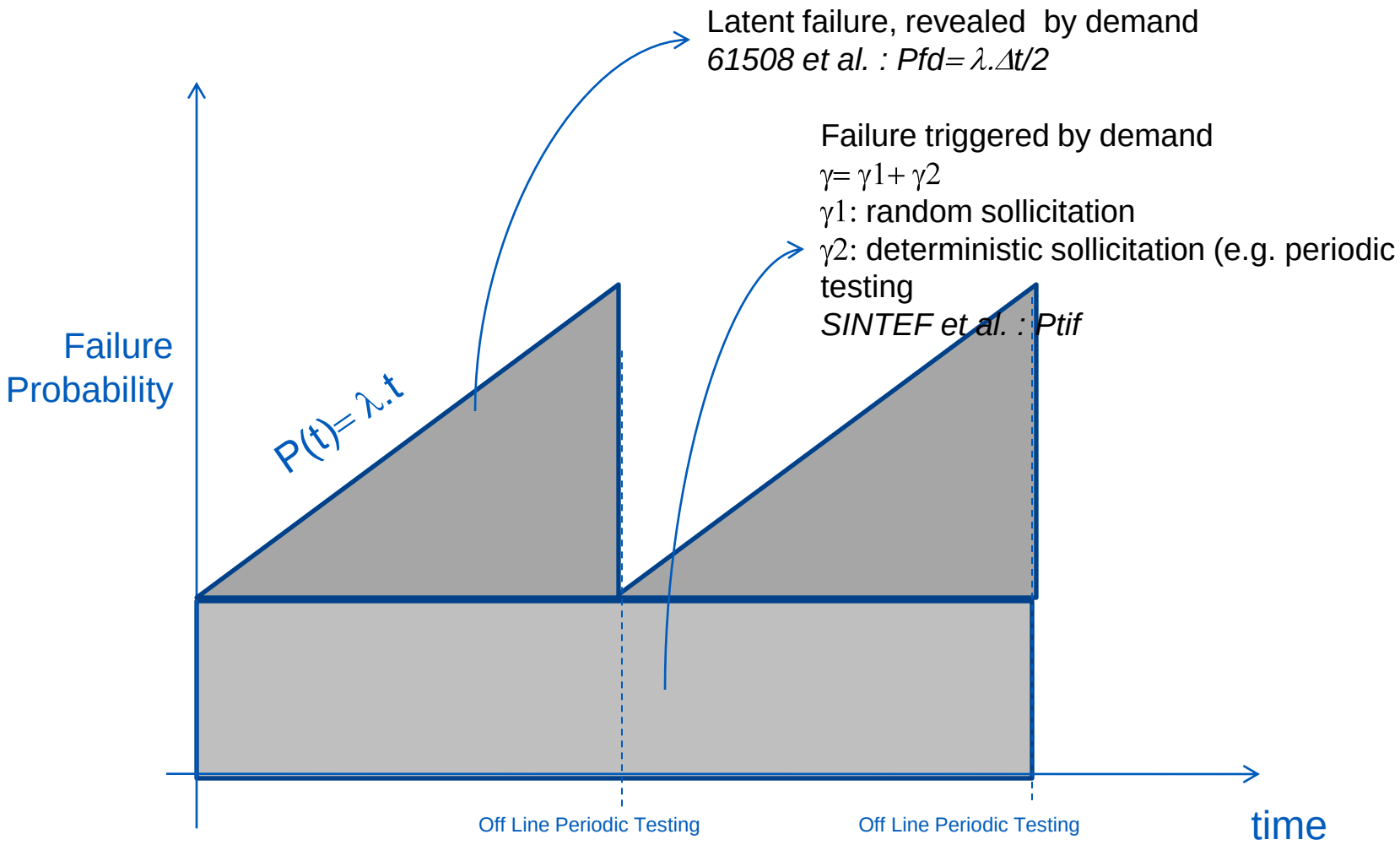
Five Detection Situations

- On line Detection Mechanisms.
  - Covers various continuous detection mechanisms (e.g. Watchdogs)
- Off line Detection Mechanisms.
  - Periodic testing and various mechanisms (maintenance...).
- **These detection Mechanisms are designed to lead to safe states.**

- Other mechanisms
  - Latent revealed by demand
  - Triggered by demand
  - Spurious
- **Failures discovered in these situations may lead to unsafe or hazardous states.**

I&C Unit Level

I&C Units Detection Situations



Assumptions: No wear out, As Good As New after repair or periodic test

I&C Unit Level

I&C Units Detection Detection Situations

Detection Situation	Note
On line Detection Mechanisms	Lead to safe states. Exc: Spurious. Estimated by failure rate and repair time
Off line Detection Mechanisms	Lead to safe states Estimated by failure rate and test interval
Latent revealed by demand	May lead to unsafe states Estimated by a Pfd
Triggered by demand	May lead to unsafe states (Initiates a spurious or other effect.) Estimated by a Conditional Probability
Spurious	May lead lead to unsafe or hazardous states Estimated by a Frequency

I&C Unit Level

Detection Situations and Failure Modes at I&C Unit leve

- Detection Situations Detection Situations combine with Failure Modes & Local Effects
  - 20 combinations, from which 10 are irrelevant or very unlikely, and 10 are relevant.

Relevance of local effects and detection situations

Local Effect	**Detection Situation**				
	Online Detection	Offline Detection	Revealed by Spurious Action	Latent, revealed by demand	Triggered by demand.
Fatal, ordered	**R**	**X**	**R**	**X**	**R**
Fatal, Haphazard	**Very Unlikely**	**Very Unlikely**	**Very Unlikely**	**Very Unlikely**	**Very Unlikely**
Non Fatal, Plausible Behavior	**X**	**R**	**R**	**R**	**R**
Non Fatal, Non Plausible Behavior	**R**	**X**	**R**	**X**	**R**

X: Excluded. Combination not relevant for the analysis of the effects due to logical considerations
R: Combination relevant for further analysis of end effects
Very Unlikely: Combination practically not relevant, due to a very low likelihood

Taxonomies at various Architecture Levels

- System Level taxonomy
- Division Level taxonomy
- I&C Unit Level taxonomy
- Module Level taxonomy
- Basic Component Level taxonomy

Module Level taxonomy

3 points of view

- **Intrinsic failure**
  - Considers the failure within the component.
  - Mostly HW focused, considers some SW aspects
  - Has to distinguish modules with digital outputs and with analog outputs...
- **SW failure**
  - Focused on SW faults propagation
  - Include « virtual » modules to represent design and specification issues
- **Functional effect**
  - Considers component failures with regard to their functional effect.
  - Relevant for both SW and HW,
  - Links Module level and I&C Unit level
    - Functional effects already defined in I&C unit taxonomy (fatal, ordered; fatal, haphazard; non fatal, plausible; non fatal, non plausible)

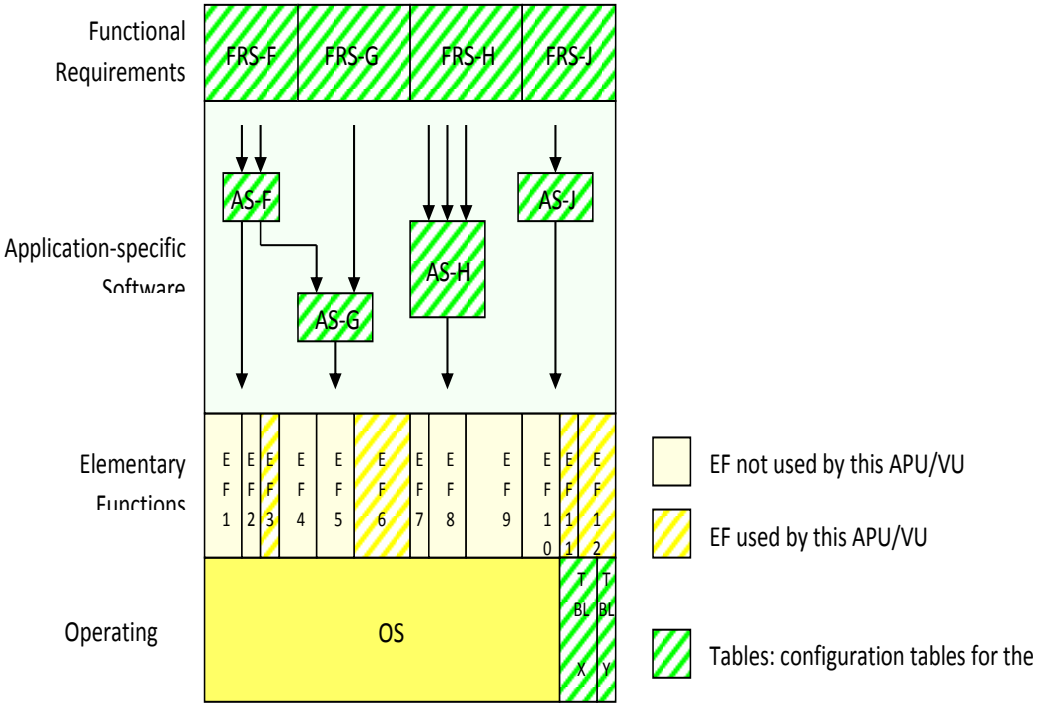
Module Level taxonomy
Intrinsic Failures

Failure modes of modules with digital and analog outputs

	Modules with digital outputs	Modules with analog outputs
Module Catgories	Digital input modules, digital output modules, processing modules, network modules...	Analog input modules, analog output modules...
Failure modes	• Signal fails to 1 • Signal fails to 0 • Signal stuck to current value • Signal goes to the opposite state • Hang • Delayed signal • Random behaviour	• Signal fails to MAX • Signal fails to MIN/0 • Signal is stuck to current value • Signal fails to an erroneous value • Hang • Delayed signal • Random behaviour • Drifted signal

Module Level taxonomy
SW Failures

- Operating System and Functional software modules
- Communication software modules
- « Virtual » software modules



Module Level taxonomy

SW Modules Categories

- Operating System and Functional software modules

SW Module Category	Note
Operating System (OS)	One per platform. Controls the overall functioning of the APUs, DCUs and VUs
Elementary Functions (EFs).	Relevant for APUs and VUs Readily useable standard functions (mathematical functions, delays...). There is one set of EFs, platform dependent, for all the APUs and VUs of the System. A specific APU or VU use only a specific subset of all available EFs.
APUs Application-specific Software (APU-AS).	Represent errors in the implementation of application-specific acquisition and processing software. An APU supports multiple application functions, and the specific software for each of these functions is an AS module. Homologous APUs in redundant divisions have the same sets of AS modules.
VUs Application-specific Software (VU-AS).	Represent errors in the implementation of application-specific voting software. The VU-AS modules implement the specific voting logics required for the subsystem. The subsystems use different voting logics: AS modules in VUs from different Subsystems tend to be different.

Module Level taxonomy
SW Modules Categories

- « Virtual » software modules
  - Represent errors in Functional Requirements Specifications (FRS) or errors in Data Tables

SW Module Category	Note
APUs Functional Requirements Specification (APU-FRS).	Represent errors in FRS of the acquisition and processing functions. One APU-FRS module per application function of an APU. May also represent errors in the data tables specifying the hardware configuration and the data communication of the APU.
VUs Functional Requirements Specification (VU-FRS).	Represent errors in FRS of the voting functions. One APU-FRS module per voting logic of a VU. May also represent errors in the data tables specifying the hardware configuration and the data communication of the VU

Module Level taxonomy
SW Modules Categories

- Communication software modules

SW Module Category	Note
Data Communication Software (DCS).	Represent errors in the DCS, e.g. data communication protocol. All DCUs of a platform have the same DCS
Data Link Configuration (DLC).	DLC is a data table that specifies the nodes of a given network, and the data messages that can be exchanged. The two subsystems use different networks: the DLCs of their DCUs are different.

Module Level taxonomy
Functional point of view

- Considers module failure mechanisms with regard to their functional effect

Module Functional Failure Mechanism	Functional Effect (Module level)	Functional effects (I&C unit level)
Output module failure leading to a APU failure	Failure of the specific application function inside the APU	Fatal, ordered Fatal, haphazard Non fatal, plausible Non fatal, non plausible
Processing module failure leading to a APU failure	Failure of the specific application function inside the APU	
Output module failure leading to VU failure	Failure of all functions inside the VU	
Processing module failure leading to VU failure	Failure of all functions inside the VU	
Subrack failure leading to VU failure	Failure of all functions inside the VU	
Link module failure leading to DCU failure	Failure of all functions inside the DCU	
Subrack failure leading to DCU failure	Failure of all functions inside the DCU	
Input module failure leading to A1, A2 or A3 failure	Failure of the specific application function inside the APU	
Processing module failure leading to A1, A2 or A3 failure	Failure of the specific application function inside the APU	
Input module failure leading to APU failure	Failure of all functions inside the APU	
Processing module failure leading to APU failure	Failure of all functions inside the APU	

Taxonomies at various Architecture Levels

- System Level taxonomy
- Division Level taxonomy
- I&C Unit Level taxonomy
- Module Level taxonomy
- Basic Component Level taxonomy

Basic Component Level taxonomy

- Mostly Hardware Focused
- May be useful, but is not necessary in most cases

Failure modes taxonomy for Basic Components (Example)

Components	Failure Modes	Failure Mode Detection	Failure Effects on the Module
Microprocessor	The microprocessor seems to be running normally but sends erroneous output	No	Undetectable Failure of the module.
	The microprocessor stops updating output	FTD dependent	Depending on FTDs of the module such as a WDT.
Internal Bus	Loss of internal bus	FTD dependent	Depending on FTDs of the module such as a WDT.
RAM	Loss of RAM	FTD dependent	Depending on FTDs of the module such as a WDT.
Current Loop	Fail (drift) high or fail (drift) low of current loop device	FTD dependent	1. Signal and FTD dependent if the current loop is for an input signal. 2. If the current loop is for an output, then the analog output of the module will fail (drift) high or fail (drift) low.

FDT: Fault Tolerance Design
WDT: WatchDog Timer. WDT detectable means the update of the toggling signal to WDT is stopped

Summary

- General Principles
- Taxonomies at various Architecture Levels
- Taxonomy and PSA

Taxonomy and PSA

- CCF assessment: from local failure to system failure

- From Taxonomy to PSA

Link

- Taxonomy of failure mechanisms at I&C Units (or lower) levels

To

- Base events used in the PSA

Taxonomy and PSA
CCF assessment: from local failure to system failure

- The analyst assesses CCF on the basis on three inputs:

  - I&C Failures Modes
    - At least at I&C Unit level
    - Analysis at I&C module, or even Basic Component levels, may be necessary
  - Detection Situations
    - Combination of Failures Modes and Detection Situations
  - CCF effect
    - The taxonomy provide the maximum possible end effect
    - Further analysis to assess the end effect, given architecture, activation conditions, defensive measures

Taxonomy and PSA
CCF maximum possible end effect

- Example: SW Module Failure point of view
  - Successively postulate a single software fault in each software module
    - Regardless of the likelihood of such faults
  - Determine the maximum possible extent of the failure
    - Regardless of the measures taken by design or operation to limit that extent
  - Further analysis to assess the most plausible end effect, given architecture, activation conditions, defensive measures

Taxonomy and PSA
SW Module Failure point of view

Maximum CCF end effect of a fault in a SW Module

End Effect	SW Module Category							
	OS	EF	APU-FRS	APU-AS	VU-FRS	VU-AS	DCS	DLC
FF-1D-1SS	R	R	R	R	NR	NR	NR	NR
FF-1SS	R	R	R	R	R	R	NR	NR
FF-2SS	R	R	NR	NR	NR	NR	NR	NR
1APU	R	R	NR	R	NR	NR	NR	NR
MAPU-MSS	R	R	NR	NR	NR	NR	NR	NR
1SS	R	*	*	NR	*	R	R	R
1SS-APU	R	*	NR	NR	NR	NR	NR	NR
SYSTEM	R	*	NR	NR	NR	NR	R	NR

SS: SubSystem, MAPU: Multiple APU, FF: Functional Failure, D: Division

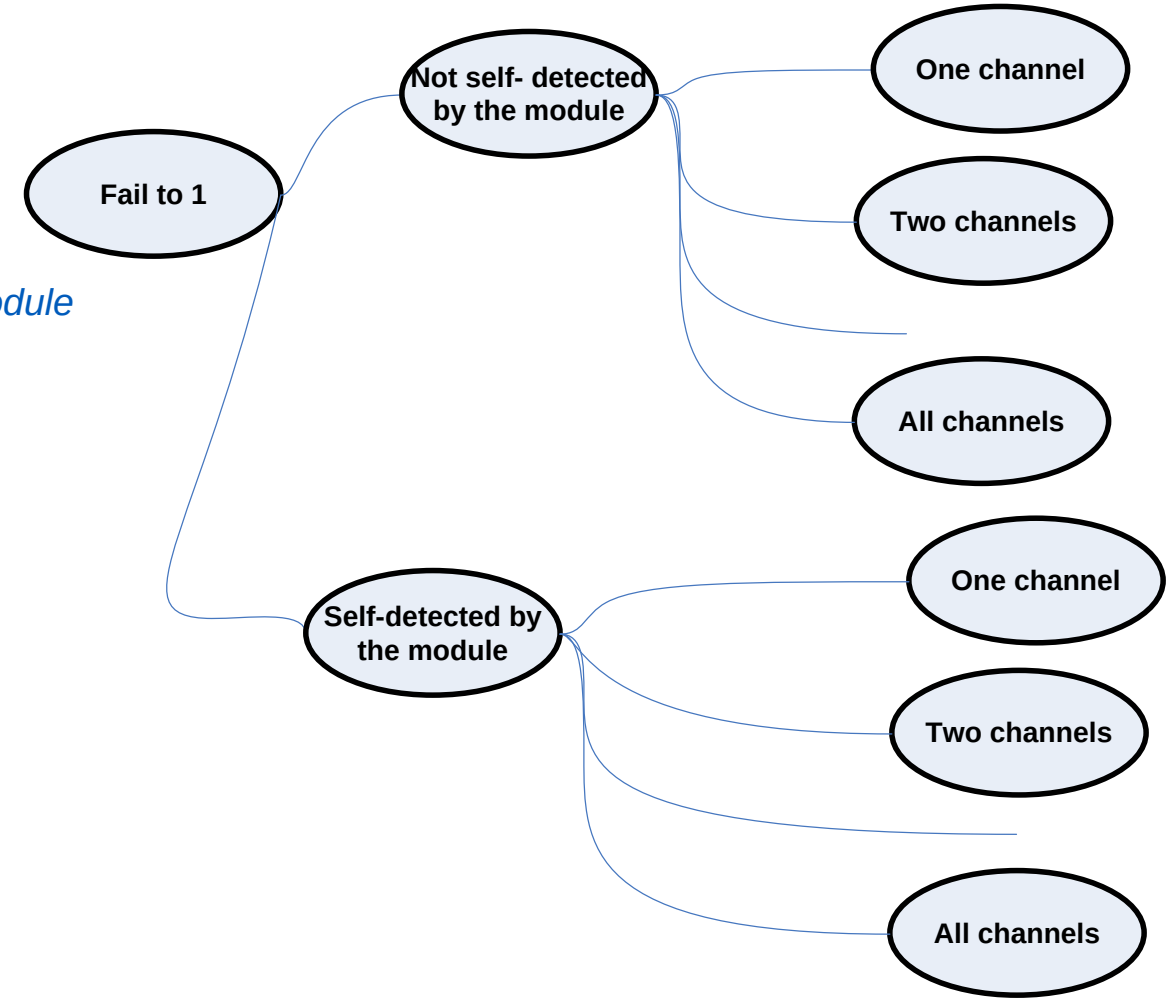
R: Combination relevant for further analysis of end effects
**: Combination that may be relevant in some situations*
NR : Combination not relevant due to logical considerations or due to a very low likelihood (PNR)

Taxonomy and PSA

Module Failure Intrinsic point of view

Maximum CCF end effect of an HW failure at Module level

Failure modes of module



May require an analysis at Basic Component Level

I&C Unit Level
CCF End Effects

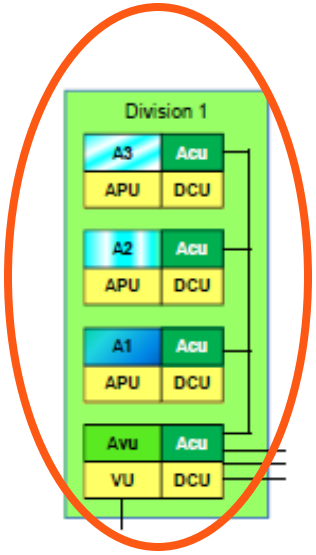
Example of possible end effects, various initial fault localisations

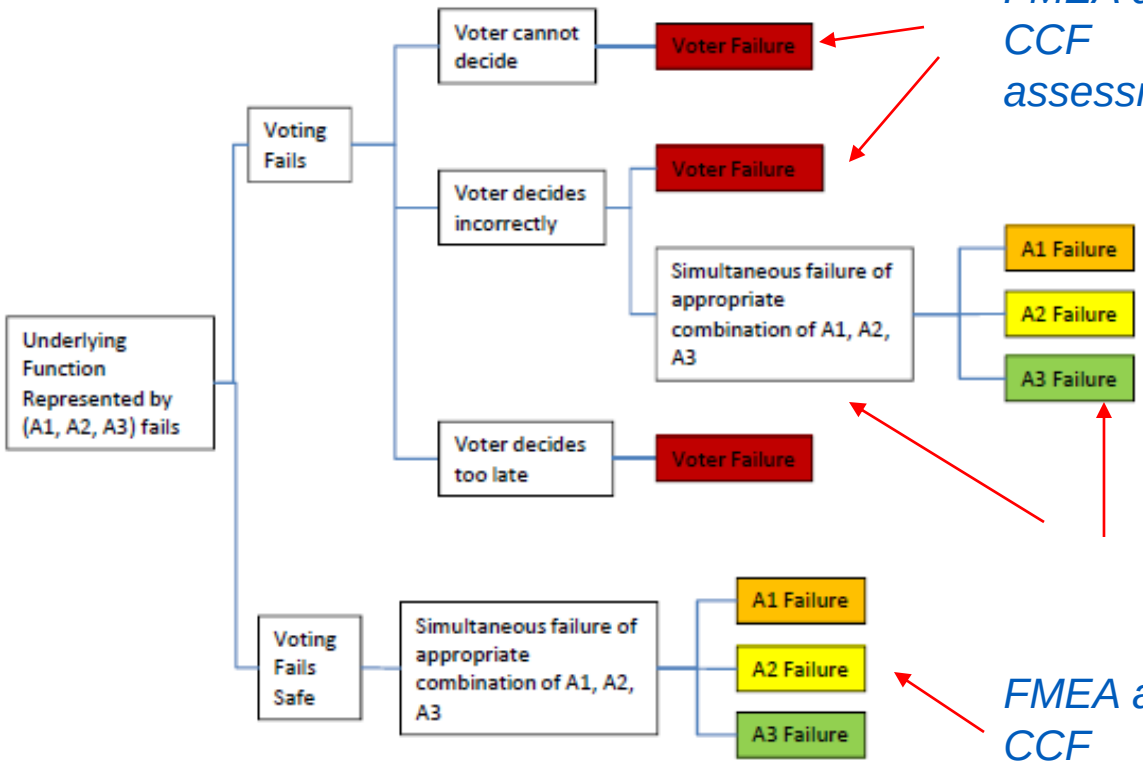
Inital Failure (Example)	End Effect	
	First Extent of Initiating Failure	Final Possible Extent of Initiating Failure
APU, DCU or VU Hardware failure	Affects one APU/DCU	Same as first Extent
	Affects one set of redundant APU/DCU	Affects one Channel
	Affects multiple sets of redundant APU	Affects one subsystem or multiple/all subsystems
	Affects one VU	Affects one Channel
	Affects multiple VU/DCU	Affects one subsystem or multiple/all subsystems
Function Failure (Ai) Voting Function Failure (A) Communication Function Failure (A)	Affects only one APU	Same as first Extent
	Affects one set of redundant APU	Affects one Channel
	Affects multiple sets of redundant APU	Affects one subsystem or multiple/all subsystems
	Affects multiple DCU/VU	Affects one subsystem or multiple/all subsystems
Fault in the Operating System of a platform, in an Elementary Function used in VU, CCF affecting Data Communication Hardware	Affects one subsystem Affects one subsystem and one set of redundant APU in another subsystem Affects multiple subsystems Affects all subsystems	Same as first Extent

Further analysis assesses the most plausible end effect, given architecture, activation conditions, defensive measures

From Taxonomy to PSA

- Link failure mechanisms at I&C Units levels and base events used in the PSA
- Example. End Effect= Failure of a protective action at division level





FMEA and CCF assessment

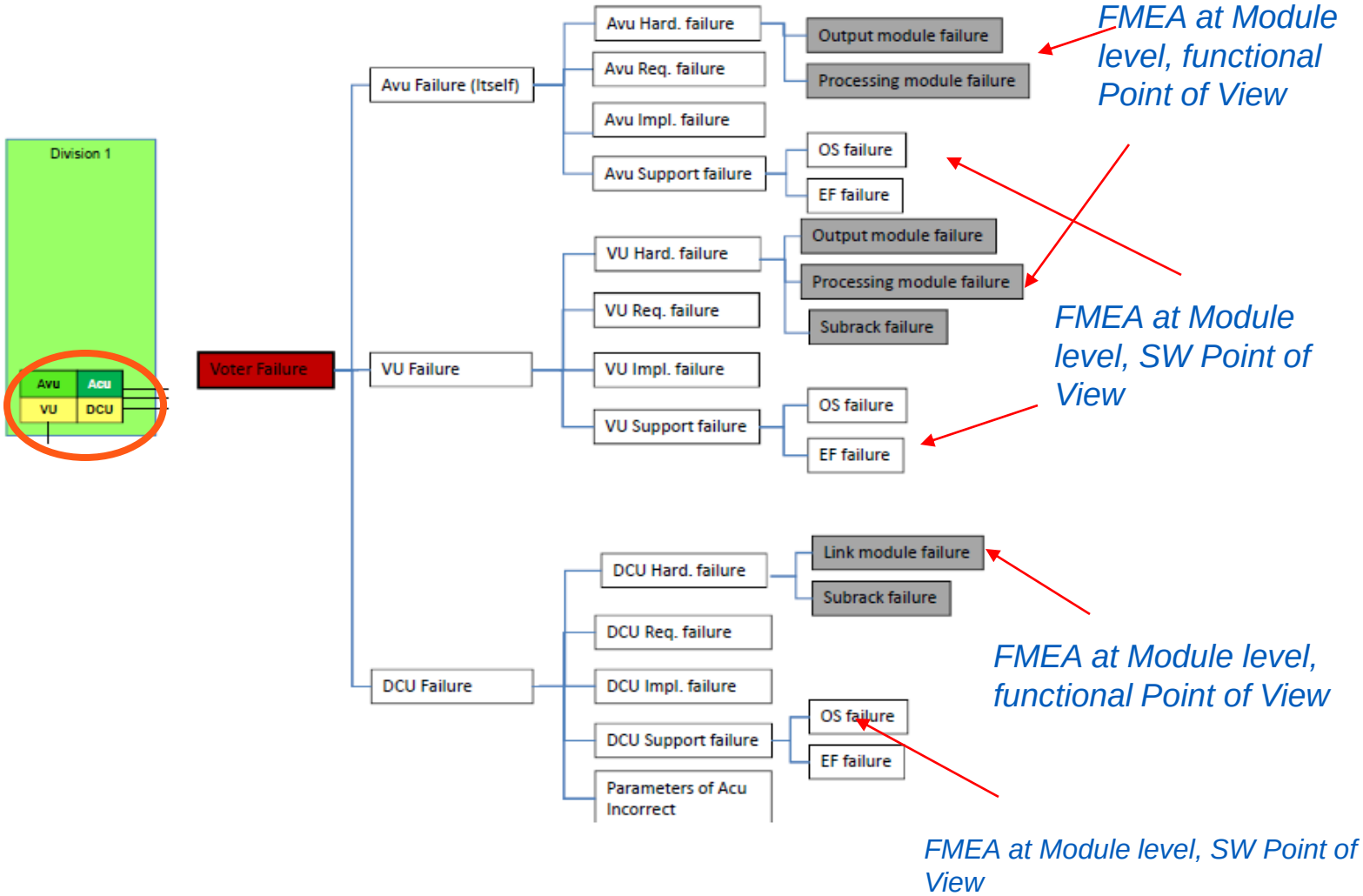
Relevant Failure for PSA

FMEA and CCF assessment

Classification Tree

From Taxonomy to PSA

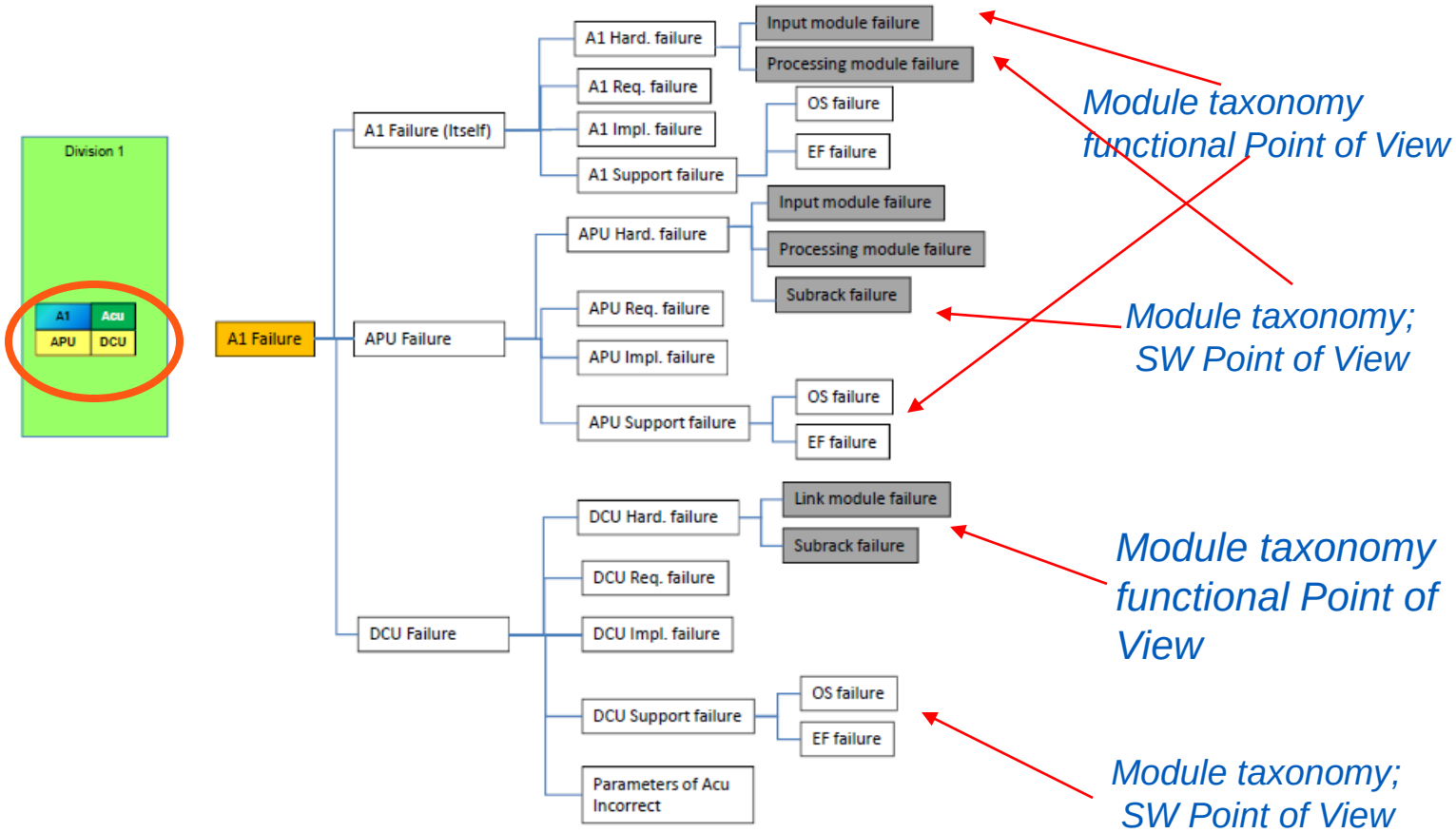
- Link failure mechanisms at I&C Units levels and base events used in the PSA
- Expl: Failure of a Voting Unit



Boxes with the same label may be found in various locations: Common Cause Failures.

From Taxonomy to PSA

- Link failure mechanisms at I&C Units levels and base events used in the PSA
- Exple: Failure of Application Specific Function 1



Boxes with the same label may be found in various locations: Common Cause Failures.
Same tree structure for failure of other functions A2 and A3.

From Taxonomy to PSA

- Some cases require a specific analysis.
  - Safety related systems used also in continuous operation conditions.
    - Failure taxonomies at system, division and I&C units levels have to be adapted.
    - Failure on Demand has to be replaced by a Failure Rate.
  - Some systems have complex, non simple Boolean outputs
    - Example Diesel Load Sequencers
    - 4 trains, independent, not subject to vote
    - Loss of one 1PU has effects at I&C system level
  - …

Thank You for your attention

Risk Pilot
Your Risk Navigator

NKS/DIGREL Seminar

Nordic Test Case

Evaluation of the modelling aspects and application of the taxonomy

Stockholm November 6, 2012

Stefan Authén, Risk Pilot AB

Background

- The recommendations in NKS/DIGREL guideline will be backed up by practical test cases
- An example digital I&C PSA model was developed 2011 as a Master's Thesis at Royal Institute of Technology (KTH) in cooperation with the NKS/DIGREL project
- The example PSA-model was based on Risk Spectrum example model (EXPSA)
- The model has now been further developed and will be used for the test cases

Objectives of the Test Case

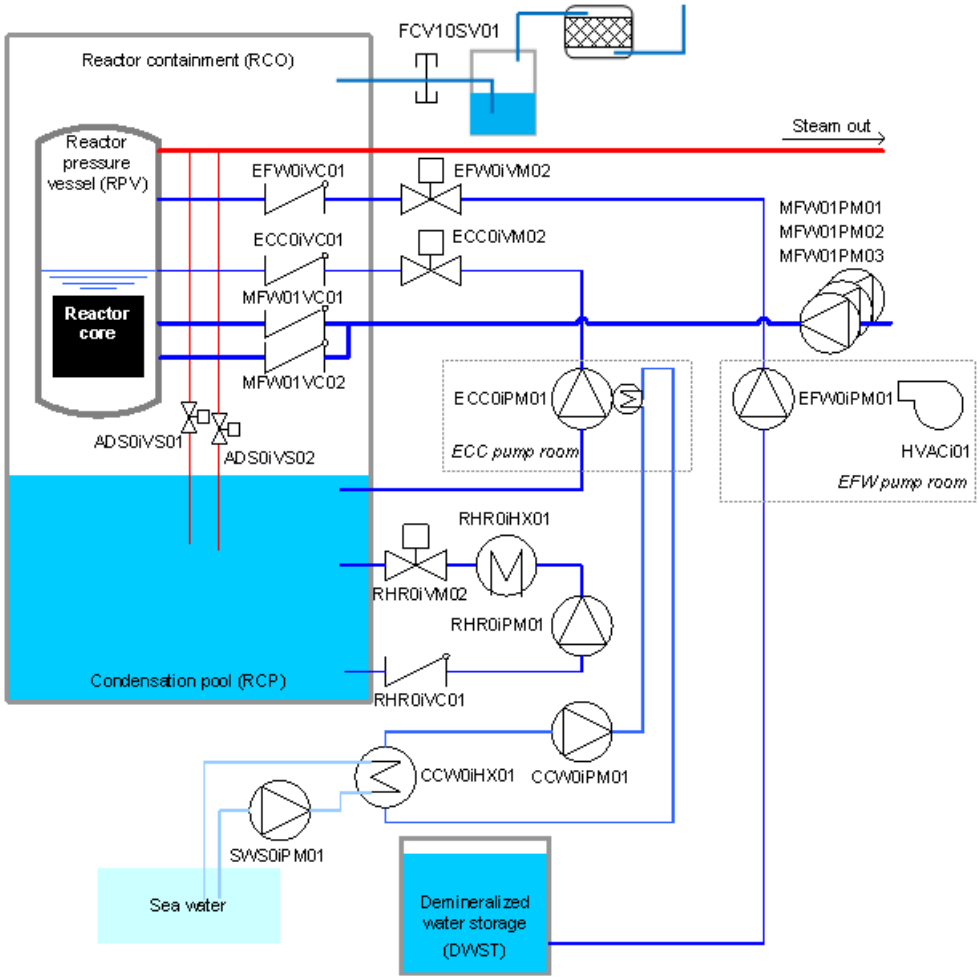
- V&V of the developed taxonomy
- Produce/verify recommendations regarding
  - Taxonomy
  - Level of detail
  - Critical dependencies
  - Modeling of digital I&C specific features
  - Modeling of software
  - Modeling of CCF
- Produce insights regarding design issues
  - Fault Tolerant Design
  - Diversification
- Serve as reference/test model for the financiers of the NKS/DIGREL project.

Plant Design

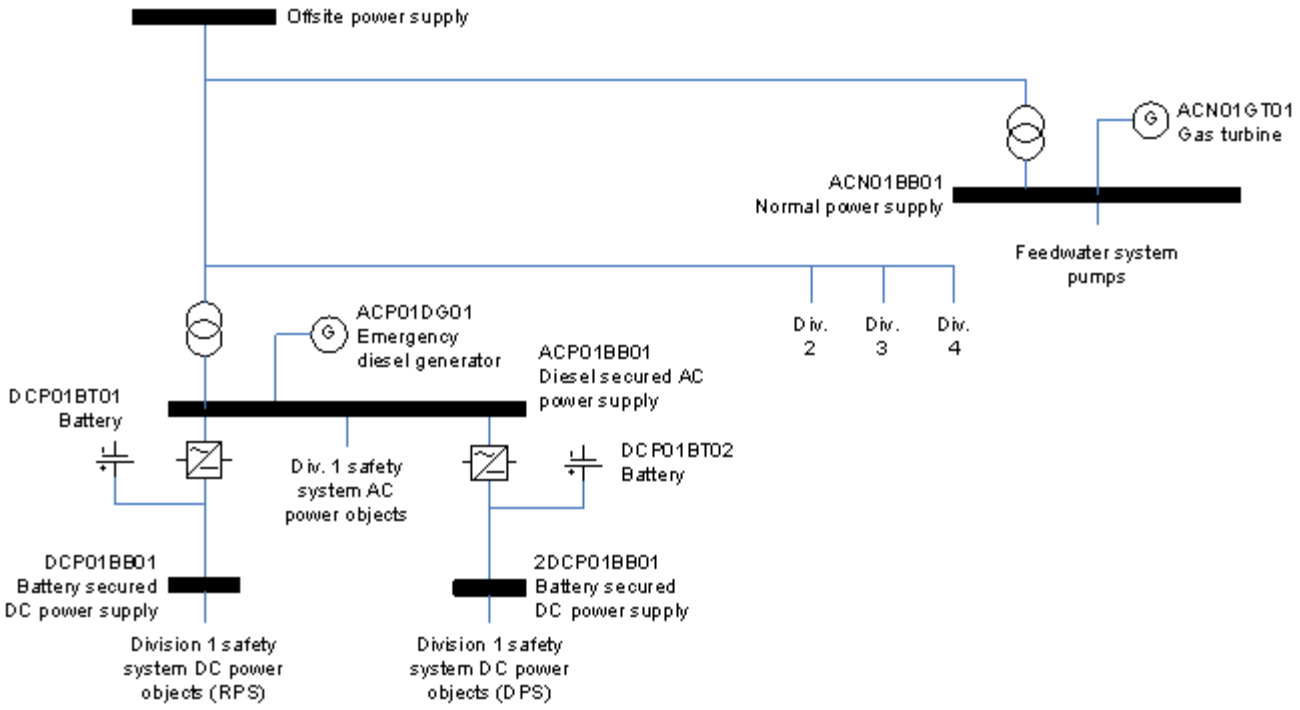
- A fictive boiling water reactor (BWR)
- Not a representative BWR,
  - only an example for demonstrating the reliability analysis of representative nuclear safety I&C

- Four-redundant safety systems
  - Reactor Protection
    - RPS, Reactor Protection System
    - DPS, Diversified reactor Protection System
  - Reactor Scram
    - RSS, Reactor Scram System
  - Water Inventory Control
    - MFW, Main Feedwater System.
    - ECC, Emergency Core Cooling system
    - EFW, Emergency Feedwater System, 3 trains
    - ADS, Automatic Depressurisation System, 8 trains
  - Residual Heat Removal
    - RHR, Residual Heat Removal system
    - FCV, Filtered Containment Venting (Passive System), 1 train
  - Support Systems
    - ACP, Diesel backed AC power system
    - DCP, Battery backed DC power system
    - CCW, Component Cooling Water system
    - SWS, Service water system
    - HVA, Heating, Ventilation and Air conditioning system

Safety Systems



Power Supply



Initiating events and system success criteria

Initiating Event	MFW	EFW	ADS	ECC	RHR
ALOCA	No credit	No credit	Not req.	1oo4	1oo4
LMFW	No credit	1oo4	2oo8	1oo4	1oo4
LOOP	2oo3	1oo4	2oo8	1oo4	1oo4
Transient	2oo3	1oo4	2oo8	1oo4	1oo4
CCI DCP	2oo3	1oo4	2oo8	1oo4	1oo4

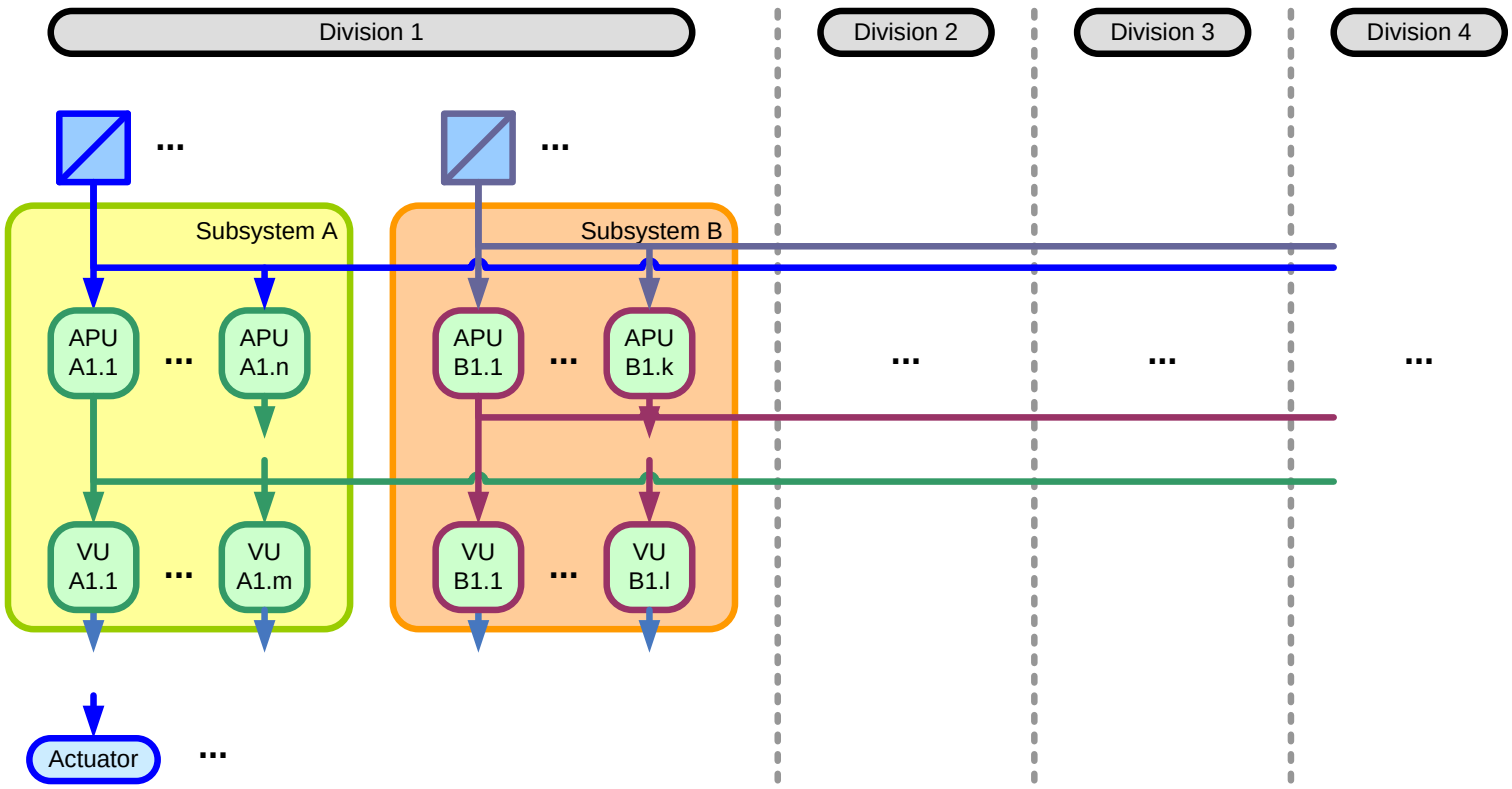
Protection System Design

- The general architecture the same as the generic structure presented in the WGRISK example system

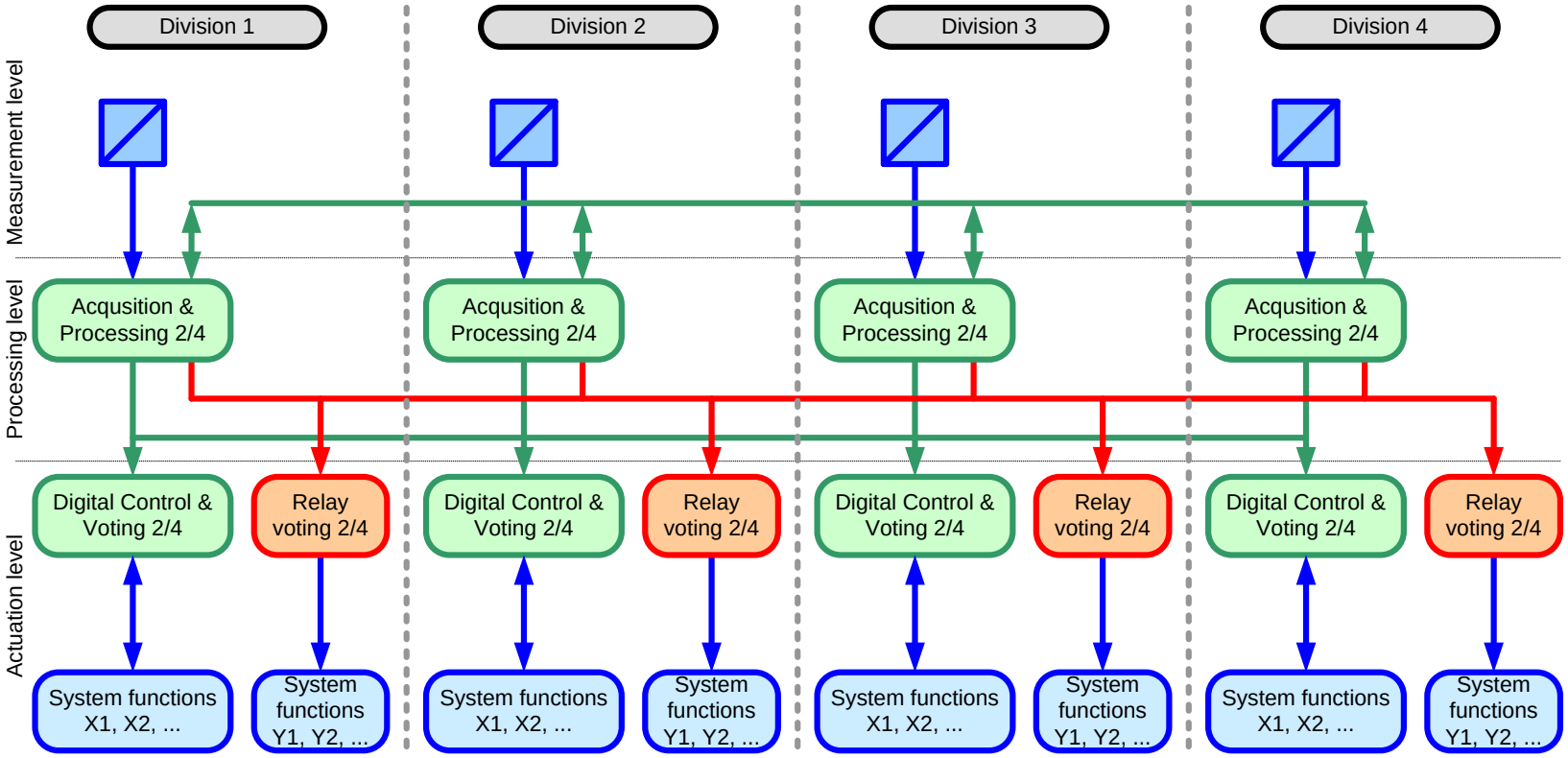
- Two subsystems, RPS and DPS
  - RPS controls ECC, RHR, ADS, CCW and SWS systems
  - DPS controls MFW, EFW, CVS and HVA systems
  - Joint control of ACP DG:s and RSS

- Control and protection signals based on a typical BWR design

RPS & DPS Design



RPS & DPS Design



Equipment Control signals

System	Actuator	Control	Condition for control type	VU Signal ID	APU Signal ID	DFLT
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	1
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	1
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

Protection functions

Signal	Description	Condition	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	I isolation due to high pressure in containment	2/4*(RCOi0CP001-H1)	1
RM000	Feedw ater isolation	2/4*(RM005-i)	1
RM005	Feedw ater isolation due to high temperature in feedw ater 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 w ater level in RPV	2/4*(RPVi0CL001-L2)	1
RSS05	Reactor scram due to high w ater 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 feedw ater 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	I isolation due to high pressure in containment	2/4*(RCOi0CP001-H1)	1
DM000	Feedw ater isolation	2/4*(DM005-i)	1
DM005	Feedw ater isolation due to high temperature in feedw ater system compartment	2/4*(MFWi0CT001-H1)	1
DSS00	Reactor scram	2/4*(DSS04-i + SS05-i + SS12-i + SS13-i)	1
DSS04	Reactor scram due to low w ater level in RPV	2/4*(RPVi0CL001-L2)	1
DSS05	Reactor scram due to high w ater 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
DSS13	Low pressure before feedw ater pump	2/4*(MFWi0CP001-L1)	1
DX001	Extra low level in RPV	2/4*(RPVi0CL002-L3)	1

Sensors

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

Taxonomy

- Requirements on the taxonomy for the Test Case:
  - Support evaluation of design and modeling aspects
    - fault tolerant design, failure detection, critical dependencies, different levels of detail, software failures, CCF:s, spurious functions, tests, maintenance etc.
  - Concur with the detailed taxonomy developed within WGRISK TG Digrel
  - As simple as possible
    - Realistic approach
    - Keep down the size of the model
    - Lower ”learning threshold”

Hardware Taxonomy

Hardware Components	Module Failure Examples	Local Functional Impact	Local Detection	Generic Failure Modes	Generic Failure Detection	Failure End Effect (RT or ESFAS)
Processor module	Hang/stalls Delayed signal Random behaviour Round-off/ truncation/ sampling rate errors Communication dropout etc.	Loss of all APU/VU functions	Online Detection	Loss of function	Monitoring[1]	All APU/VU outputs acc. to FTD
	"	"	Latent revealed by demand	Latent loss of function	Periodic test[2]	Loss of all APU/VU outputs
	Random behaviour	Spurious APU/VU function(s)	Spurious effect	Spurious function	Self revealing	Spurious APU/VU output(s)
Analog Input Module	Signal fails high/low Signal drifts	Loss of all Module Application Functions	Online Detection	Loss of function	Self-Monitoring[3]	1oo4 conditions of specific APU/VU outputs acc. to FTD
	Signal hangs/freeze	Loss of all Module Application Functions	Latent revealed by demand	Latent loss of function	Periodic test	Loss of 1oo4 conditions of specific APU/VU outputs
Digital Input Module	Signals stuck to current value	Loss of all Module Application Functions	Online Detection	Loss of function	Self-Monitoring	1oo4 conditions of specific APU/VU outputs acc. to FTD
	"	"	Latent revealed by demand	Latent loss of function	Periodic test	Loss of 1oo4 conditions of specific APU/VU outputs
Digital Output Module	Signals stuck to current value	Loss of all Module Application Functions	Online Detection	Loss of function	Self-Monitoring	Specific APU/VU outputs acc. to FTD
	"	"	Latent revealed by demand	Latent loss of function	Periodic test	Loss of specific APU/VU outputs
Communication module	Failure to establish communication	Loss of specific APU/VU Application Functions	Online Detection	Loss of function	Monitoring	1oo4 conditions of specific APU/VU outputs acc. to FTD
Backplane	Loss of backplane	Loss of all APU/VU functions	Online Detection	Loss of function	Monitoring	All APU/VU outputs acc. to FTD
Power supply	Interruption Short circuit Ground contact etc.	Loss of all APU/VU functions	Online Detection	Loss of function	Monitoring	All APU/VU outputs acc. to FTD
Measurement	Fails high Fails low Drift of value	Loss of specific Module Application Function	Online Detection	Loss of function	Monitoring	1oo4 conditions of specific APU/VU outputs acc. to FTD
	Freeze of value	Loss of specific Module Application Function	Latent revealed by demand	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

Software Taxonomy

	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
- Digital I&C Hardware CCF
  - Generic data (NUREG/CR-5496)
- Digital I&C Software
  - Fictive data, engineering judgement

PSA Model

- Developed in Riskspectrum software
  - Benchmarking with FinPSA software
- Follows a generic coding system
- Follows a generic FT structure
- Developed with expanded FT structure
  - Flexible and more easy to follow

- Digital I&C model statistics:
  - 460 Fault Trees, 280 Basic Events, 66 CCF groups

PSA Model

- Based on the taxonomy the fault tree model of the digital I&C is developed by three stages:
  - Mapping of possible detected and undetected failures for each component.
  - Assignment of possible default values for detected failures and grouping of components into modeling blocks.
  - Allocation of modeling blocks for each specific RPS/DPS Control Signal or Protection Function with regard to
    - the failure mode of the sequence (Loss of Function or Spurious Function),
    - type of degraded voting logic
    - and the consequence of applied default values at detected failure of components critical for the sequence.

Generic Fault Tree Structure

Fault Tree Type	Basic Event	Transfer to FT	Modeling block	Comment
Safety Function				
System Function				
System Division				
Active Equipment	Active Equipment			
Equipment Signal	-	Output Module, RPS Control Signal		
Output Module	Output Module	Voting Unit	Signal from Output Module	FT undetected / detected
Voting Unit, VU	VU		Signal from Output Module	FT undetected / detected
RPS Control Signal	-	RPS Protection function, Communication VU-APU		Modeling of voting
Communication VU-APU	Communication module	Accuisition & Processing Unit	Communication VU-APU	FT undetected / detected
RPS Protection function	-	RPS Protection function, Communication APU-APU Process measurement		Separate FT:s by division
Communication APU-APU	Communication module	APU unit	Communication VU-APU	FT undetected / detected
Accuisition & Processing Unit, APU	APU		Communication VU-APU Communication APU-APU	
Process Measurement		Input Module	Measurement signal	FT undetected / detected
Input Module	Input Module		Measurement signal	FT undetected / detected

Test Case Evaluation

- Evaluation aspects
  - Level of detail
    - System, Division, I&C Unit and Module level
  - Fault Tolerant Design
    - e.g. default values at detected failures and different voting logics
  - Hardware failure modes
    - Equipment, detected/undetected failures, etc.
  - Software failure modes
  - Common Cause Failures
  - Diversity aspects
    - Protection system, measurements etc.

- Model changes will be performed by use of boundary conditions

Test Case Evaluation

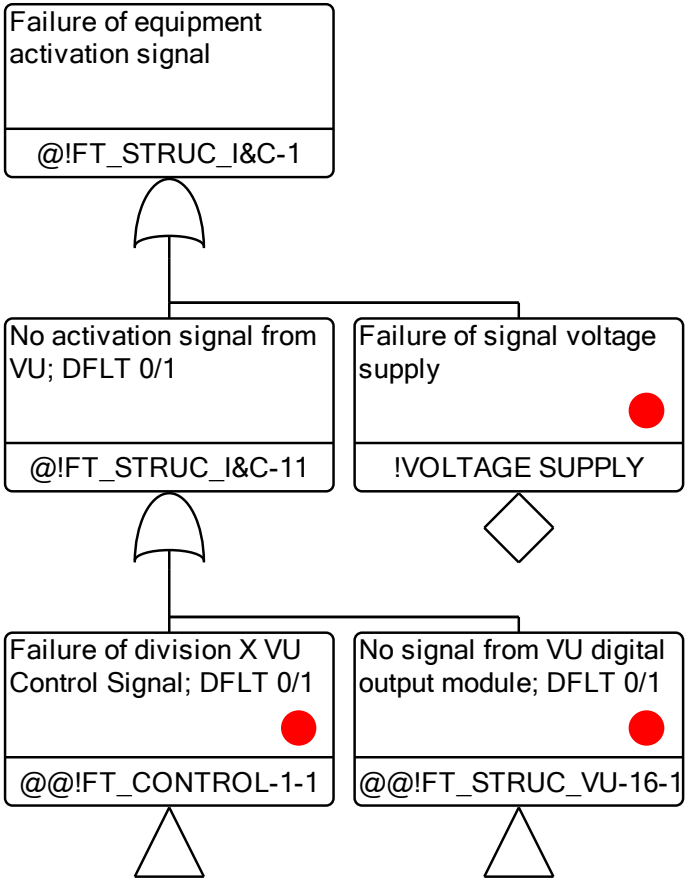
- Since the model and the data are fictive, it is not meaningful to draw conclusions from the numerical results

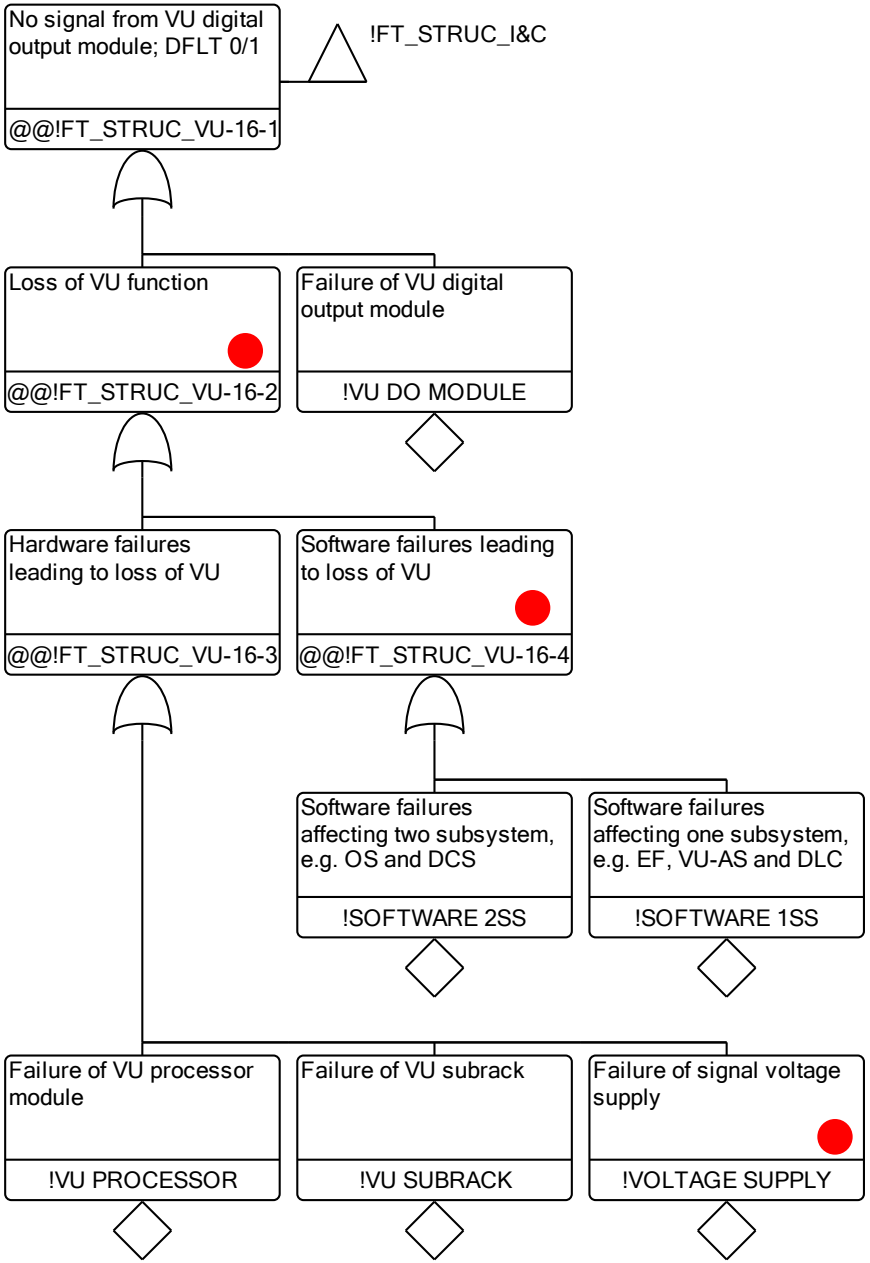
- Evaluation will be made by
  - comparing importance measures such as RIF, RDF and sensitivity factors,
  - by qualitative analysis of minimal cut sets (number, rank, why a minimal cut set, which are missing, etc.),

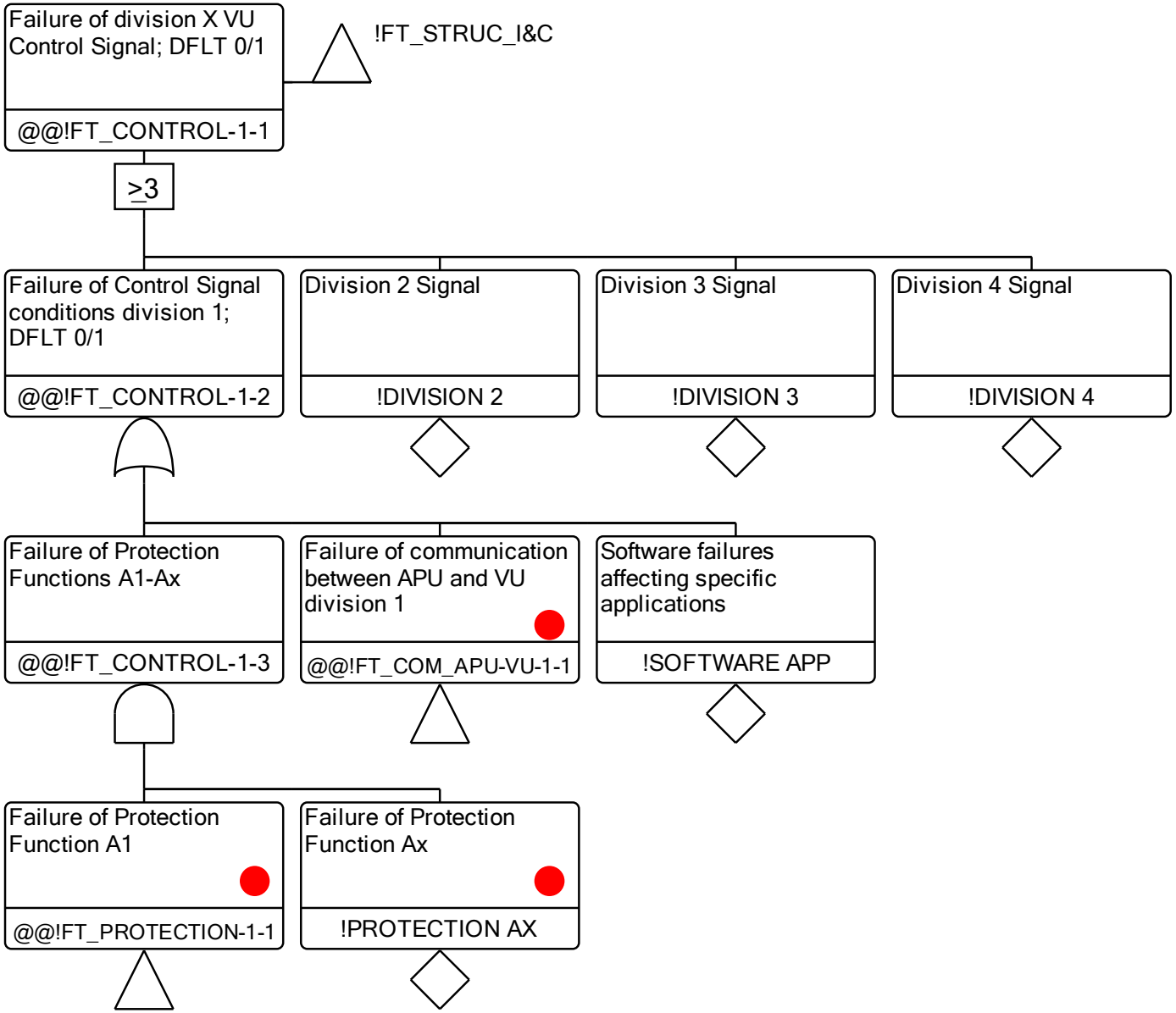
  for different configurations of design and modeling aspects

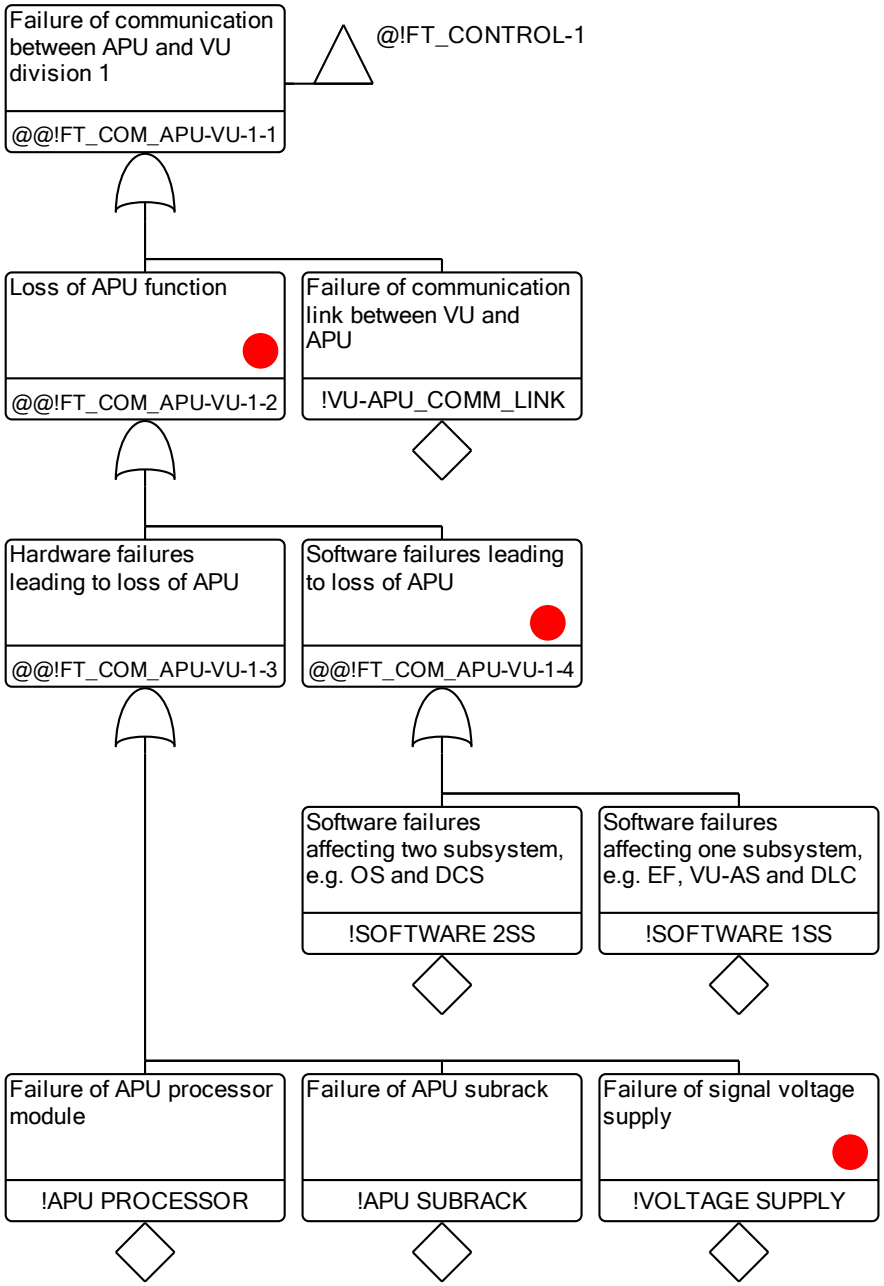
Current Status and next step

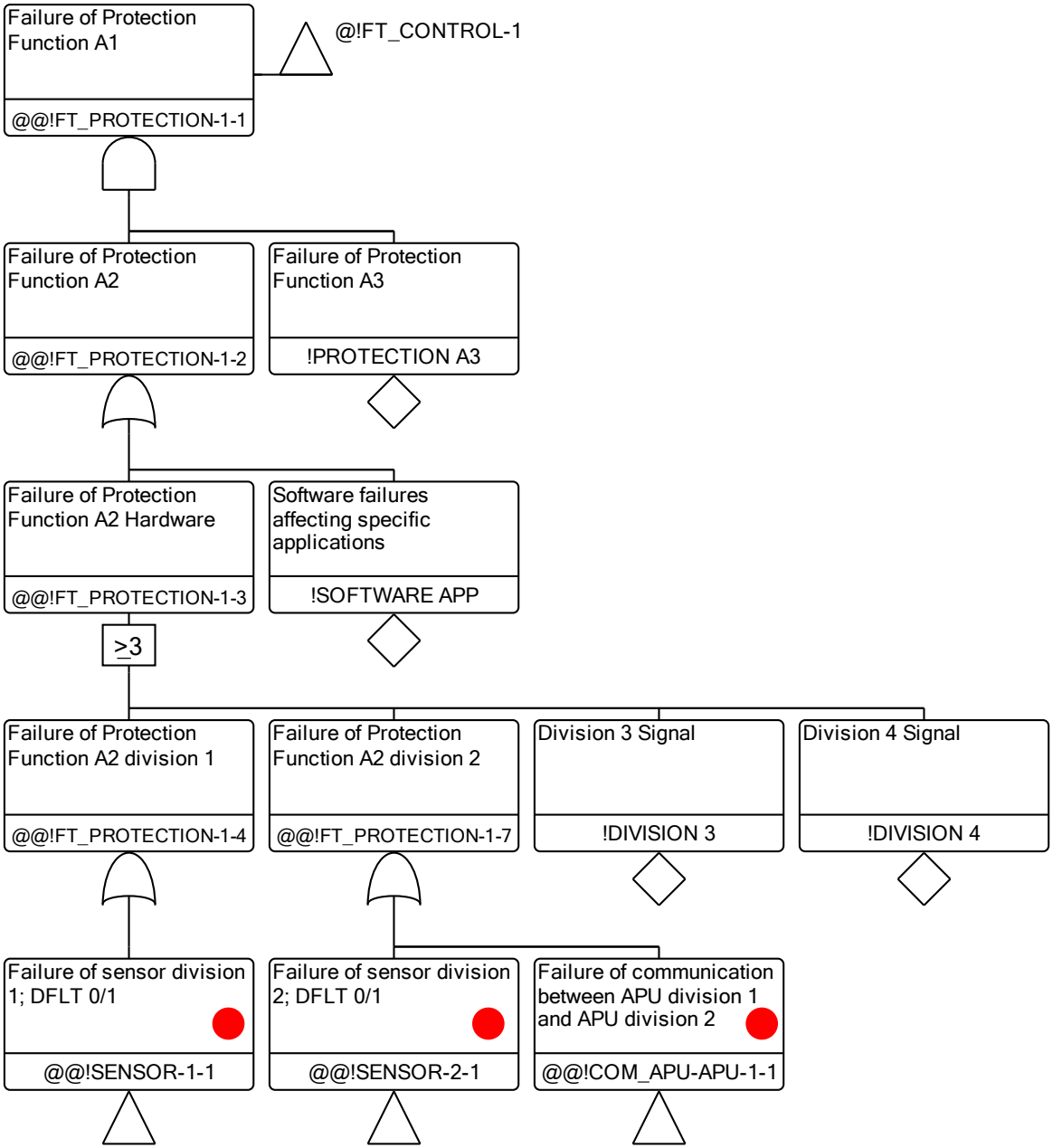
- The PSA model is completed
  - Some additional work with setting up boundary conditions for test cases remains
- Test cases will be quantified during November
- Results will be included in the 2012 NKS Status Report (Phase 3)
- Evaluation of Software failures and FinPSA benchmarking will be performed 2013

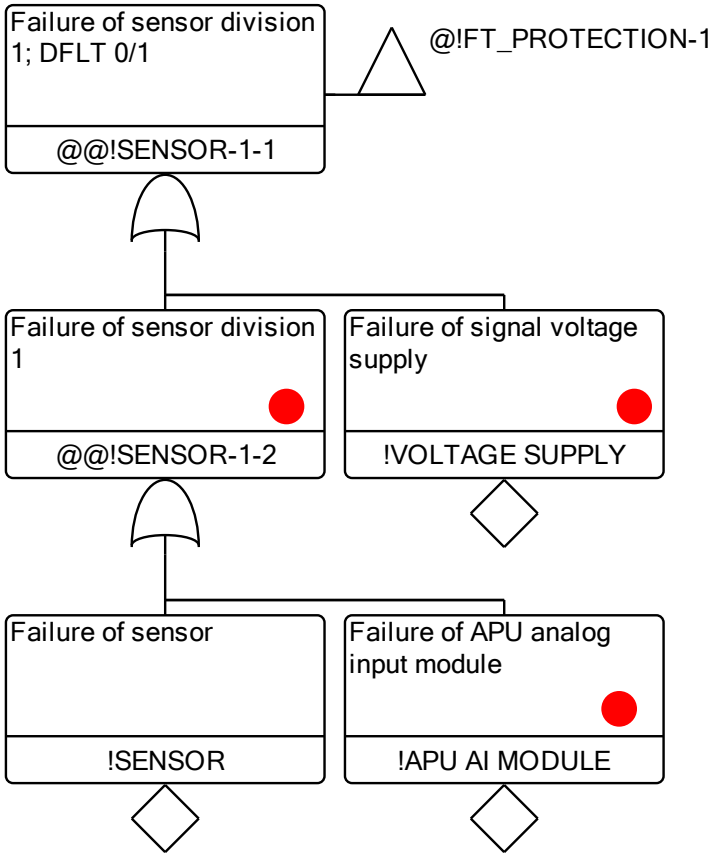

Failure of equipment activation signal
@!FT_STRUC_I&C-1
No activation signal from VU; DFLT 0/1
@!FT_STRUC_I&C-11
Failure of signal voltage supply
!VOLTAGE SUPPLY
Failure of division X VU Control Signal; DFLT 0/1
@@!FT_CONTROL-1-1
No signal from VU digital output module; DFLT 0/1
@@!FT_STRUC_VU-16-1

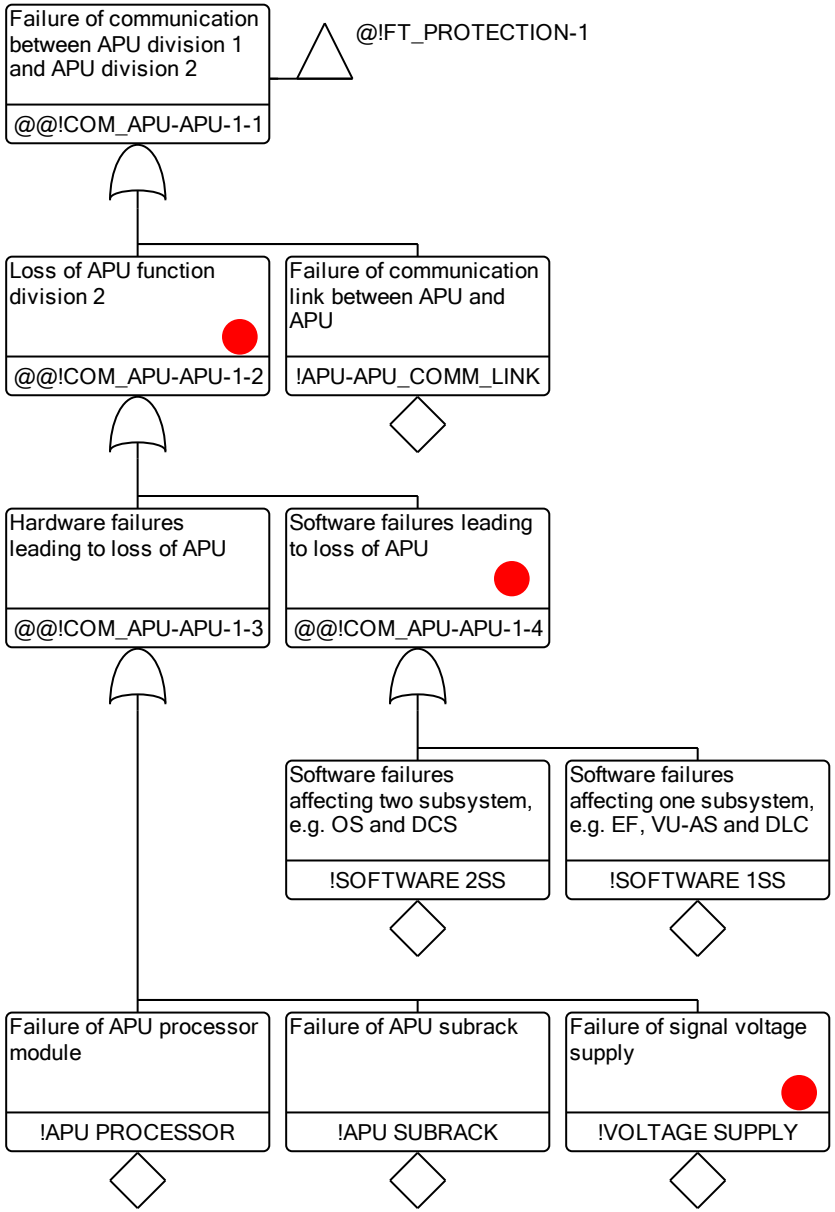

No signal from VU digital output module; DFLT 0/1
@@!FT_STRUC_VU-16-1
!FT_STRUC_I&C
Loss of VU function
@@!FT_STRUC_VU-16-2
Failure of VU digital output module
!VU DO MODULE
Hardware failures leading to loss of VU
@@!FT_STRUC_VU-16-3
Software failures leading to loss of VU
@@!FT_STRUC_VU-16-4
Software failures affecting two subsystem, e.g. OS and DCS
!SOFTWARE 2SS
Software failures affecting one subsystem, e.g. EF, VU-AS and DLC
!SOFTWARE 1SS
Failure of VU processor module
!VU PROCESSOR
Failure of VU subrack
!VU SUBRACK
Failure of signal voltage supply
!VOLTAGE SUPPLY


Failure of division X VU Control Signal; DFLT 0/1
@@!FT_CONTROL-1-1
!FT_STRUC_I&C
≥3
Failure of Control Signal conditions division 1; DFLT 0/1
@@!FT_CONTROL-1-2
Division 2 Signal
!DIVISION 2
Division 3 Signal
!DIVISION 3
Division 4 Signal
!DIVISION 4
Failure of Protection Functions A1-Ax
@@!FT_CONTROL-1-3
Failure of communication between APU and VU division 1
@@!FT_COM_APU-VU-1-1
Software failures affecting specific applications
!SOFTWARE APP
Failure of Protection Function A1
@@!FT_PROTECTION-1-1
Failure of Protection Function Ax
!PROTECTION AX


Failure of communication between APU and VU division 1
@@!FT_COM_APU-VU-1-1
@!FT_CONTROL-1
Loss of APU function
@@!FT_COM_APU-VU-1-2
Failure of communication link between VU and APU
!VU-APU_COMM_LINK
Hardware failures leading to loss of APU
@@!FT_COM_APU-VU-1-3
Software failures leading to loss of APU
@@!FT_COM_APU-VU-1-4
Software failures affecting two subsystem, e.g. OS and DCS
!SOFTWARE 2SS
Software failures affecting one subsystem, e.g. EF, VU-AS and DLC
!SOFTWARE 1SS
Failure of APU processor module
!APU PROCESSOR
Failure of APU subrack
!APU SUBRACK
Failure of signal voltage supply
!VOLTAGE SUPPLY


Failure of Protection Function A1
@@!FT_PROTECTION-1-1
@!FT_CONTROL-1
Failure of Protection Function A2
@@!FT_PROTECTION-1-2
Failure of Protection Function A3
!PROTECTION A3
Failure of Protection Function A2 Hardware
@@!FT_PROTECTION-1-3
Software failures affecting specific applications
!SOFTWARE APP
≥3
Failure of Protection Function A2 division 1
@@!FT_PROTECTION-1-4
Failure of Protection Function A2 division 2
@@!FT_PROTECTION-1-7
Division 3 Signal
!DIVISION 3
Division 4 Signal
!DIVISION 4
Failure of sensor division 1; DFLT 0/1
@@!SENSOR-1-1
Failure of sensor division 2; DFLT 0/1
@@!SENSOR-2-1
Failure of communication between APU division 1 and APU division 2
@@!COM_APU-APU-1-1


Failure of sensor division 1; DFLT 0/1
@@!SENSOR-1-1
@!FT_PROTECTION-1
Failure of sensor division 1
@@!SENSOR-1-2
Failure of signal voltage supply
!VOLTAGE SUPPLY
Failure of sensor
!SENSOR
Failure of APU analog input module
!APU AI MODULE


Failure of communication between APU division 1 and APU division 2
@@!COM_APU-APU-1-1
@!FT_PROTECTION-1
Loss of APU function division 2
@@!COM_APU-APU-1-2
Failure of communication link between APU and APU
!APU-APU_COMM_LINK
Hardware failures leading to loss of APU
@@!COM_APU-APU-1-3
Software failures leading to loss of APU
@@!COM_APU-APU-1-4
Software failures affecting two subsystem, e.g. OS and DCS
!SOFTWARE 2SS
Software failures affecting one subsystem, e.g. EF, VU-AS and DLC
!SOFTWARE 1SS
Failure of APU processor module
!APU PROCESSOR
Failure of APU subrack
!APU SUBRACK
Failure of signal voltage supply
!VOLTAGE SUPPLY