

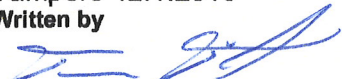




Elements of DiD architecture	DiD levels				
	Normal operation: Prevent deviations and failures	Operational occurrences: Abnormal situation management	Postulated events: Control of accidents within design basis	Severe accidents: Limit off-site releases	Significant releases: Mitigate consequences
Society & regulator	Regulatory oversight	Event reporting	Emergency management		
Management	Safety management				
O&M personnel	Periodic tests	Plant operations	EOPs		
ICT	Displays	Alarm handling	Diagnostics	Communications	
I&C	Process control	Protection		Measurements	
Barriers and process systems		Confinement			
Siting	Availability of ultimate heat sink				

# Challenges in Defence in Depth and I&C architectures

Authors: Teemu Tommila and Nikolaos Papakonstantinou

Confidentiality: Public

<b>Report's title</b>	
Challenges in Defence in Depth and I&C architectures	
<b>Customer, contact person, address</b>	<b>Order reference</b>
Ministry of Trade and Industry/Nuclear Waste Management Fund, Jorma Aurela	SAFIR 5/2015
<b>Project name</b>	<b>Project number/Short name</b>
Integrated safety assessment and justification of nuclear power plant automation	102392 / SAUNA_2015
<b>Author(s)</b>	<b>Pages</b>
Teemu Tommila and Nikolaos Papakonstantinou	54 p. + app. 5 p.
<b>Keywords</b>	<b>Report identification code</b>
Defence in Depth, Instrumentation and Control, architecture	VTT-R-00090-16
<b>Summary</b>	
<p>This report discusses the terminology and modelling concepts related to the design and analysis of Defence in Depth (DiD) and I&amp;C architectures in nuclear power plants. The purpose is to collect ideas for further research in the SAFIR2018 programme towards model-based and tool-supported systems engineering. The interpretations of the current practices and suggestions for new directions are based on available literature, discussions with several domain experts and previous research carried out in the SAFIR2014 programme.</p> <p>According to the literature review, DiD continues to be a major design principle for nuclear power plants. There is, however, a debate going on regarding its scope and interpretations. The concrete challenge is to find good technical solutions and practices for their development and assessment. Unfortunately, many of the terms related to DiD, system properties seem to be defined in rather vague ways. Different standards and guidelines give often different and sometimes even contradictory definitions. This situation does not provide a good basis for model-based engineering and design automation. On the basis of these observations, the following are suggested as potential topics for further research:</p> <ul style="list-style-type: none"> <li>• Further development of modelling concepts and taxonomies related to DiD and I&amp;C architecture</li> <li>• Refinement of a systems engineering process for developing a plant-level I&amp;C architecture</li> <li>• Criteria and review methods for assessing DiD and I&amp;C architectures as part of the licensing and qualification processes</li> <li>• Structured multidisciplinary methods and tools for modelling and analysis of I&amp;C architectures.</li> </ul>	
<b>Confidentiality</b>	Public
Tampere 12.1.2016	
<b>Written by</b>	<b>Reviewed by</b>
	
Teemu Tommila, senior scientist	Atte Helminen, senior scientist
	<b>Accepted by</b>
	
	Riikka Virkkunen, head of research area
<b>VTT's contact address</b>	
Teemu Tommila, PL 1300, FI-33101 Tampere; teemu.tommila@vtt.fi	
<b>Distribution (customer and VTT)</b>	
SAFIR2018 programme	
<p><i>The use of the name of VTT Technical Research Centre of Finland Ltd in advertising or publishing of a part of this report is only permissible with written authorisation from VTT Technical Research Centre of Finland Ltd.</i></p>	

## Preface

---

This research report is a deliverable of task T1.2, “Description and analysis of the Defence in Depth architecture” in the research project “Integrated safety assessment and justification of nuclear power plant automation” (SAUNA, 2015 – 2018). The SAUNA project is part of the Finnish Research Programme on Nuclear Power Plant Safety 2015 – 2018 (SAFIR2018), focusing especially on its research area “plant safety and systems engineering”.

During the first project year 2015, the aim of task T1.2 was to review the literature and recommendations on the approaches to model and analyse overall architectures of complex, critical systems in nuclear power and other relevant safety-critical domains. Starting from plant level, the task focused on the design and analysis of I&C architectures. In addition, the purpose was to define next steps to be taken in SAUNA towards structured representation, analysis and assessment of the safety architecture in nuclear power plants with respect to independence, robustness, security, etc.

The SAUNA project was monitored and guided by Reference Group 1 (Automation, organisation and human factors) of the SAFIR2018 programme. In this research report, the authors’ interpretations of the current practices and suggestions for new directions are based on available literature, previous research in the SAFIR2014 programme and on discussions with the regulator and three utilities (13 persons altogether). The authors thank the Reference Group for guiding the work and the domain experts for valuable discussions.

Tampere 12.1.2016

*Authors*

## Contents

---

Preface.....	2
Contents.....	3
1. Introduction.....	4
2. Challenges of overall safety.....	4
3. DiD concepts, history and problems.....	5
3.1 Definition.....	5
3.2 History.....	6
3.3 Structure of DiD.....	7
3.4 Recent challenges.....	8
4. Key concepts in an overall DiD architecture.....	9
4.1 Postulated initiating events.....	10
4.2 Plant states.....	11
4.3 On dependencies between NPP systems.....	14
4.3.1 Redundancy.....	15
4.3.2 Diversity.....	16
4.3.3 Physical separation.....	18
4.3.4 Functional isolation.....	18
4.4 Definitions of faults and failures revisited.....	19
4.5 Classifying failure modes.....	22
4.6 On active failures of intelligent systems.....	24
4.7 Resilience for managing the unexpected.....	27
5. Modelling of I&C architecture.....	29
6. Design process.....	33
7. Analysis methods and tools.....	38
7.1 Guidance for Diversity and Defence-in-Depth (D3) analysis.....	40
7.2 Risk analysis techniques.....	43
7.3 Functional Failure Identification and Propagation framework (FFIP).....	45
7.4 Architecture Description Languages.....	47
8. Summary and conclusions.....	49
References.....	50
Appendix A: Acronyms and abbreviations.....	55
Appendix B: Glossary.....	56

## 1. Introduction

---

The concept of Defence in Depth (DiD) is the cornerstone of nuclear safety. However, recently the need has arisen to reconsider its interpretations and the ways of implementing it in actual plants (WENRA 2013). In particular, unintended complex interactions across discipline and system boundaries may threaten safety in case of multiple faults and extreme conditions. A further challenge is created by human and organisational factors (including safety culture) which by their very nature are never independent of each other – nor of the technical components. A sociotechnical system such as a nuclear power plant is characterised by dynamic relationships between the system elements. The emergent properties – such as safety – created by these dynamic relationships are difficult to capture by traditional linear and component based analysis methods. When looking at the safety of the overall architecture it is not enough to limit the analysis on aggregation of component or even subsystem level inputs. A multidisciplinary model is needed that takes into account the relations between different elements of the sociotechnical system and how these affect the Defence in Depth architecture.

This report reviews the literature and recommendations on the approaches to model and analyse overall architectures of complex, critical systems in nuclear power. In the context of plant-level safety the report focuses on the I&C architecture. Due to the multidisciplinary character of DiD and conceptual design in general, the surrounding process and electrical systems, as well as human operators are also considered, for example in the form of a *Concept of Operations* (ConOps). Important terms related to DiD, e.g. the meaning of functional isolation and active failures, are discussed and defined in Appendix B. In addition, the purpose is to define next steps to be taken in the SAUNA project towards structured representation, analysis and assessment of the architecture of nuclear power plant I&C. In the first place, the target is in manual practices but also the model-driven approach and computer tools for assessing DiD and I&C designs are foreseen.

## 2. Challenges of overall safety

---

Nuclear power has long traditions in safety engineering, and countermeasures are in place for single failures and anticipated hazardous scenarios. The remaining challenges are mostly related to new kinds of hazards, such as earthquakes, and to the inherent complexity of modern technology, e.g. digital I&C. Recent experiences have shown that the capabilities of human organisations and individuals are critical for the prevention and management of disasters. While proven technologies and extensive V&V ensure quality of individual plant items, unintended dependencies on system and plant level have turned out to be a source of vulnerabilities.

Safety is an emergent feature depending on the quality and collaboration of all NPP elements including technical systems and structures, human organisations and the operational environment. The plant must be reliable in normal operation and anticipated occurrences but also resilient, when unexpected situations are encountered. Whereas conventional risk management approaches are based on hindsight and emphasise failure probabilities, resilience engineering looks for solutions that are robust but also flexible (Kadambi 2013). Since communication, interactions and collaboration are important for the overall performance, plant systems and organisations should be developed using an integrated design process and a shared plant model as a boundary object between various disciplines.

When safety is concerned, this boils down to the concept of Defence in Depth (DiD). Recently, the exact meaning and scope of DiD have been discussed in the nuclear community. We claim here that, there is a need for structured and multi-disciplinary ways to describe the overall DiD architecture and methods to analyse its safety performance. The

most important decisions are made early during the design process. In addition, the DiD architecture and the regulatory requirements behind it are an important source of safety requirements both for the organisational structure and the I&C architecture. Therefore, multi-disciplinary modelling concepts and working practices on the plant and system level are a relevant issue for requirements definition.

In particular, I&C systems integrate the viewpoints of several disciplines. Hazard analysis often leads to a safety-related performance requirement or a function, e.g. protection or alarm, added to the control system. For eliciting operational requirements, process engineers and human operators are the most important collaborators. The goals, constraints and control tasks required by the process system should be identified and allocated to humans and I&C systems in an optimal way. Even if co-design of process equipment and control has been the goal for a long time, a problem often encountered in the process industry is that process engineering solutions are fixed before control engineers are involved. In nuclear power, integration of Human Factors Engineering (HFE) and the design of technical systems is a well-known but still unsolved problem.

The reasons for working in isolation are partly in different backgrounds and training. But more importantly the problem is in the lack of sound and shared concepts, representations and working practices. As a cure we suggest adoption of the idea of *Concept of Operation* (ConOps) that is used in many areas of Systems Engineering (SE) as a high-level description shared by all participants (see Tommila, Laarni & Savioja 2013). In the case of nuclear power, ConOps should be combined with the concept of DiD in order to provide a practical boundary object to work with in a collaborative way.

### 3. DiD concepts, history and problems

---

#### 3.1 Definition

For decades the concept of Defence in Depth (DiD) has been the most important strategy to ensure nuclear safety for nuclear plants. According to IAEA (2007), DiD means “hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of anticipated operational occurrences and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive materials and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions”. The US Nuclear Regulatory Commission (NRC, see <http://www.nrc.gov/reading-rm/basic-ref/glossary.html>) defines defence in depth in a similar way as “an approach to designing and operating nuclear facilities that prevents and mitigates accidents that release radiation or hazardous materials. The key is creating multiple independent and redundant layers of defence to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon. Defence in Depth includes the use of access controls, physical barriers, redundant and diverse safety functions and emergency response measures”. So, the core of DiD is in several independent and consecutive solutions, “defence lines”, to prevent accidents. DiD includes both functional and physical solutions and covers both technical and organisational means to ensure plant safety.

DiD is usually divided into five levels of protection and four physical barriers as shown in Figure 1. Should one level fail, the subsequent level comes into play (IAEA 2005). Boundaries between the levels are, however, not quite clear. *Barriers* are physical means to prevent the progression of a fault by preventing or inhibiting the movement of people, material or some other phenomenon (e.g. fire) (IAEA 2007, ONR 2014). For typical reactors, the barriers that confine radioactive material include the fuel matrix, fuel cladding, pressure boundary of the coolant system and the containment.

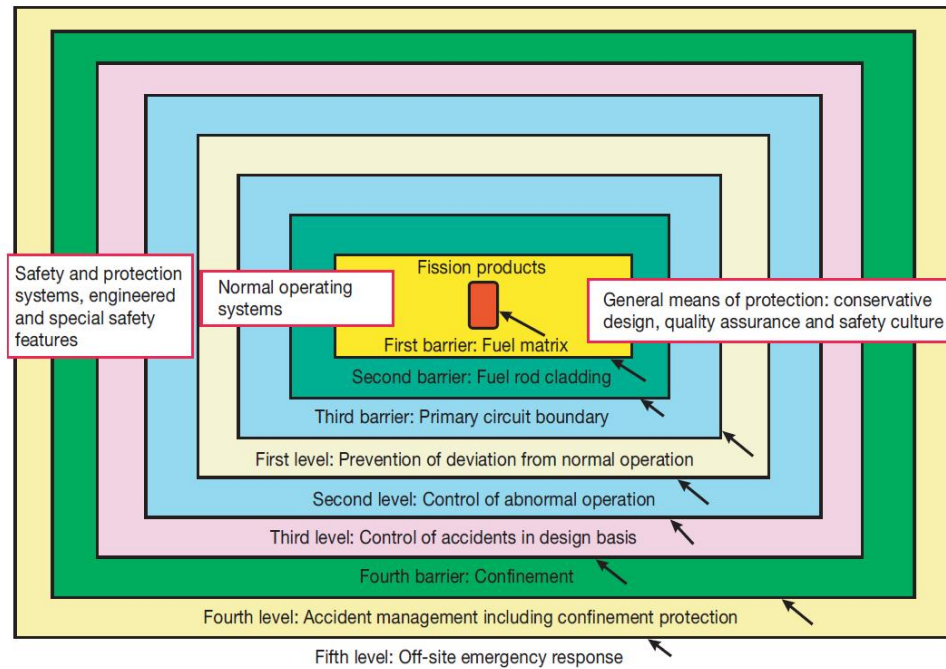


Figure 1. Interrelationship between physical barriers and levels of protection in defence in depth (IAEA 2005).

We understand that DiD is an overall safety philosophy rather than a specific architectural solution. Defence in Depth should be applied to all safety related activities, whether organisational, behavioural or design related, and whether in full power, low power or various shutdown states (WENRA 2013). So, the basic idea is applicable to both the safety architecture of the power plant and to the design process producing it. For example, independent design reviews can be understood as a defence line against design errors.

### 3.2 History

The term Defence in Depth referred originally to a military strategy but is now used in many areas of engineering and commerce. In the field of nuclear safety the concept was introduced in the early 1970s. First DiD included three levels for normal operation, *Anticipated Operational Occurrences* (AOO) and *Design Basis Accidents* (DBA) (WENRA 2013). Incidents and accidents were postulated on the basis of single initiating events. The concept was gradually refined to take into account severe situations not explicitly addressed in the original design (hence called “beyond design conditions”). These developments led to two additional levels for severe accidents and mitigation of significant releases (WENRA 2013). At present the concept includes a more general structure of multiple physical barriers and complementary means to protect the barriers themselves, the so-called “levels of defence” (Figure 1).

Recently, construction of new nuclear power plants has begun or is being envisaged in several European countries. Also the lessons learned from the Fukushima Dai-ichi accident have created the need to be prepared for situations that have been considered “beyond design” for existing plants. According to WENRA (2013), DiD is a key to safety also for new nuclear power plants. WENRA expects new nuclear power plants to be designed and operated with the objective of “enhancing the effectiveness of the independence between all levels of defence in depth.”

### 3.3 Structure of DiD

New reactor designs should consider complex situations, such as multiple failure events and core melt accidents, called *Design Extension Conditions* (DEC) (WENRA 2013). The phenomena involved in accidents with core/fuel melt (severe accidents) differ radically from those which do not involve a core melt. Therefore, it has been proposed to treat the multiple failure events as part of the 3rd level of DiD, but with a clear distinction between means and conditions (sub-levels 3.a and 3.b). The refined structure of DiD proposed by the WENRA Reactor Harmonization Working Group (RHWG) is shown in Figure 2.

Levels of defence in depth	Objective	Essential means	Radiological consequences	Associated plant condition categories
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation, control of main plant parameters inside defined limits	No off-site radiological impact (bounded by regulatory operating limits for discharge)	Normal operation
Level 2	Control of abnormal operation and failures	Control and limiting systems and other surveillance features		Anticipated operational occurrences
Level 3 <sup>(1)</sup>	3.a Control of accident to limit radiological releases and prevent escalation to core melt conditions <sup>(2)</sup>	Reactor protection system, safety systems, accident procedures	No off-site radiological impact or only minor radiological impact <sup>(4)</sup>	Postulated single initiating events
	3.b	Additional safety features <sup>(3)</sup> , accident procedures		Postulated multiple failure events
Level 4	Control of accidents with core melt to limit off-site releases	Complementary safety features <sup>(3)</sup> to mitigate core melt, Management of accidents with core melt (severe accidents)	Off-site radiological impact may imply limited protective measures in area and time	Postulated core melt accidents (short and long term)
Level 5	Mitigation of radiological consequences of significant releases of radioactive material	Off-site emergency response Intervention levels	Off site radiological impact necessitating protective measures <sup>(5)</sup>	-

Figure 2. The refined structure of the levels of DiD (WENRA 2013).

Defence in Depth is often defined at the overall plant level and is not focused specifically on I&C. However, EPRI (2014) suggests refinements to WENRA's definitions to make them better applicable to integrated digital systems (Figure 3). The adaptations include addition of the roles of human and I&C systems on each level of defence (i.e. the degree of automation, which is a key issue also in HFE and ConOps) and clarifying the differences between Levels 2 and 3 with regard to mitigation of AOs.



Levels of Defense in Depth	Associated Plant Conditions	Objective	Essential Means		Radiological Consequences
			Systems (Additive) <sup>1</sup>	Human Role <sup>2</sup>	
Level 1	Normal operation, with plant conditions remaining within normal operating limits	Prevention of abnormal operation and failures	Control systems <sup>3</sup> used to maintain plant within normal operating limits, associated indications, SPDS, and other surveillance features	Monitor and, if necessary, take control actions to maintain plant parameters within defined limits using normal operating procedures (NOPs <sup>4</sup> ); monitor plant safety status; monitor safety system availability; perform maintenance and surveillance tests per surveillance test procedures (STPs)	Within regulatory operating limits for radiological discharge (no abnormal off-site radiological impact)
Level 2	Anticipated operational occurrences (AOOs), with plant conditions remaining within reactor trip limits	Control of abnormal operation and failures to avoid exceeding reactor trip limits	Limitation systems <sup>5</sup>	Perform actions specified by abnormal operating procedures (AOPs <sup>4</sup> ); monitor and control plant parameters to within reactor trip limits; monitor critical safety functions; monitor safety system availability; perform manual shutdown if required	
Level 3	Level 3.a Postulated single initiating events <sup>6</sup>	Control of event to limit radiological releases and prevent escalation to core melt conditions	Reactor protection system, auxiliary supporting systems, post-accident monitoring instrumentation	Perform manual actions credited in the safety analysis and prescribed in emergency operating procedures (EOPs); monitor critical safety functions; select and implement manual safety and non-safety success paths as required per EOPs	No off-site radiological impact or only minor radiological impact
	Level 3.b Postulated multiple failure events		Diverse manual and automatic actuation systems and associated indications, other safety features needed for postulated multiple failure events (risk reduction systems)	Perform manual actions to mitigate consequences of the event (e.g., actions credited in a Diversity and Defense in Depth or D3 analysis)	

Figure 3. Proposed definition of levels of defence to support I&C architecture design (EPRI 2014, levels 4 and 5 not included).

In a nuclear power plant, the three fundamental *safety functions* (control of reactivity, heat removal from the fuel and confinement of radioactive materials) have to be performed in all situations. Each of fundamental safety function may be divided into several subsidiary safety functions (IAEA 2005). Safety functions can be accomplished using Systems, Structures and Components (SSC) and also with prepared staff actions. The role of a structure, system or component in performing safety functions is the basis for its safety classification. Safety functions can be challenged by various situations and causal mechanisms. The aim of “provisions” is to protect the barriers by preventing hazardous events and to mitigate the consequences if the barriers are damaged. The provisions include inherent plant safety features, systems, procedures, availability and training of staff, safety management and safety culture measures. An example of a safety function is prevention of unacceptable reactivity increase that can be caused by erroneous control rod withdrawal. Provisions to prevent that include, for example, monitoring rod positions and limiting the speed of rod withdrawal (IAEA 2005).

The levels of defence are intended to be independent to the extent practicable. In practice, however, some sort of interdependence between the levels exists. The containment is an example of a structure which is used on different levels of defence. A problem may also be that both the main and backup systems control the same actuators. Dependencies weaken the DiD concept and should therefore be identified and analysed for possible implications (WENRA 2013). Attention shall be paid to the design of I&C, electrical power supply, cooling systems and other potential cross cutting systems. Situations in which all barriers are not available (e.g. during shutdown) also necessitate special attention. The adequacy of the achieved independence shall be justified (WENRA 2013).

### 3.4 Recent challenges

In general, it is expected in nuclear engineering that, if the commonly shared safety principles are adequately applied, nuclear power plants should be very safe, even though absolute freedom of risk can't be guaranteed (IAEA 2005). A new challenge is related to the risks associated with extreme external events and complex failure combinations, such as the problems encountered during the Fukushima accident. These rare but severe situations are

beyond conventional safety design practices and have given rise to lively debate about research needs (e.g. SNETP 2013 and NUGENIA 2013). This highlights the importance of emergent, system-level phenomena. The traditional, technology-driven concept of Defence in Depth (WENRA 2013, IAEA 2005) should be given an extended meaning and its use reinforced. For example, there have been suggestions to extend DiD outside the plant to cover company management, regulatory activities and even the international community as a whole (Weightman 2013). On the other hand, a precise definition of such a design philosophy may not be necessary. As suggested by Kadambi (2013), shifting the focus from definitions to the risk-informed and performance-based practical application of Defence in Depth might lead to more immediate safety improvements.

We focus here on the design of I&C systems. Also in that area DiD would need some clarifications. For example, integration of Human Factors Engineering (HFE) to the design of technical systems is still a problem. A multidisciplinary way should be found for representing, discussing and analysing the implementation of the DiD concept as a practical, plant-specific safety architecture. In this sense, the current understanding of DiD seems to have some weaknesses. In general, DiD looks like a technical approach to protect the plant from hazards, including errors made by humans. The most important elements in a DiD architecture are the *Systems, Structures and Components* (SSCs) important to safety that according to IAEA (2007) are “items which contribute to protection and safety, except human factors”. On the other hand, it is said in (IAEA 1996) that safety functions can be accomplished using systems, components or structures and also with staff actions. The types of DiD provisions include also procedures, availability and training of staff, safety management and safety culture measures. Moreover, experiences have shown that the capabilities of human organisations become critical in complex and unforeseen situations. Even today accident procedures shall be in place to define the management of the safety features and to give guidance on necessary human actions. In analysing risks of multiple failure events, the time available for necessary human actions should be considered. An important lesson from the Fukushima Dai-ichi accident was the importance of a control room and emergency response centre to be adequately protected against external hazards. The accessibility of local control points required for manual actions has also to be ensured. Finally, security has gained growing importance with the introduction of digital systems. In addition to information security, physical security is an important component of defence in depth. As is well known, the human organisation is often the weak point when security concerned. So, the definitions of DiD seem to be somewhat ambivalent with respect to human factors. Solutions tend to focus on technology, and humans come into play in complex situations beyond the capabilities of technical systems. Normally prescriptive procedures are applied, but in severe situations all available plant equipment may be used.

DiD is still the cornerstone of NPP safety, but recently the need has arisen to reconsider its interpretations and ways of implementing it in actual plants (WENRA 2013). Unintended interactions may threaten safety in case of multiple faults and extreme conditions. Digital automation with its failure mechanisms and cross-cutting role is one source of increased complexity. A further challenge is created by human and organisational factors (e.g. safety culture). The emergent properties created by many dynamic dependencies are difficult to capture by traditional methods. A model is needed that takes into account the relations between different elements of the sociotechnical system. A consensus standard on Defence in Depth would take into consideration a wider perspective than just hardware or software issues and include also operational and organisational issues (Kadambi 2013).

#### **4. Key concepts in an overall DiD architecture**

---

Defence in Depth is a design principle aiming at the prevention and management of undesired events and mitigating their consequences. In our understanding DiD includes two key dimensions: 1) coverage of all functions ranging from prevention to mitigation; and 2)

implementation of required functions by several independent, consecutive solutions. Figure 4 shows an outline of an extended DiD architecture where various functions needed for DiD are mapped to DiD levels and elements on different architectural levels. Allocating safety functions to plant systems and structures and to human organisations and procedures on various DiD levels is a difficult design task encountered already during the conceptual design stage. A robust design based on DiD with sizeable safety margins and diverse means for delivering the safety functions, as well as operator response plans, will help to protect against unanticipated situations (WENRA 2013). However, organisational behaviour needs also to be taken into account, as well as the overall, common-cause, influence of safety culture on all organisational processes.

	DiD levels				
	Normal operation: Prevent deviations and failures	Operational occurrences: Abnormal situation management	Postulated events: Control of accidents within design basis	Severe accidents: Limit off-site releases	Significant releases: Mitigate consequences
Society & regulator	Regulatory oversight		Event reporting	Emergency management	
Management	Safety management				
O&M personnel	Periodic tests	Plant operations	EOPs		
ICT	Displays	Alarm handling	Diagnostics	Communications	
I&C	Process control	Protection		Measurements	
Barriers and process systems	Confinement				
Siting	Availability of ultimate heat sink				

Figure 4. An outline of an extended DiD architecture where functions needed on various DiD levels are allocated to technical systems, organisations and processes/procedures.

DiD can be implemented in different ways. In any case, clear and sound modelling concepts are needed for describing the concrete safety architecture in an understandable way. Clarifications can perhaps be found by considering some related terms in more detail. This chapter discusses a few key concepts on the basis of the reviewed literature and the discussions with domain experts.

## 4.1 Postulated initiating events

The concept of initiating events was introduced in the United States by NRC in 1975 together with the event tree methodology and a set of common event types (IAEA 1993). The term initiating event (initiator) refers to an unintended occurrence that leads to *Anticipated Operational Occurrences* (AOO) or accident conditions. It is used, e.g., for reporting events that have actually occurred<sup>1</sup>. (IAEA 2007, YVL B.1 2013)

During design stage, the term *Postulated Initiating Event* (PIE) is a hypothetical event capable of leading to AOOs or accident conditions. The primary causes of postulated initiating events may be equipment failures, operator errors or natural phenomena, both within and external to the nuclear facility (IAEA 2007). Designers have two objectives in controlling the risk level, a) to limit the probability of the PIE and; b) to ensure that plant systems can handle the situation (STUK 2014).

<sup>1</sup> Please note that the term “event” may have various meanings and does not necessarily mean an instantaneous change of state.

The determination of initiating events is an important starting point of design. The frequency of IEs has a direct impact on the results for core damage frequency, as well as on the importance of individual components or actions (IAEA 1993). Candidate initiating events and frequencies can be found, e.g., by analysis of plant systems (FMEA, etc.), reference to previous PRAs or by using operating experience and event lists for similar plants (e.g. INL 2015) or by expert opinion on rare events (IAEA 1993). Examples of initiating events are given below:

- Internal events
- Uncontrolled control rod withdrawal
- Leakage in primary system
- Sudden opening of steam relief valves
- Loss of off-site power (LOOP)
- Loss of instrument-air
- Spurious manual or automatic trip
- Fire in control room
- External events
- External floods and fires
- Airplane crash
- Seismic event
- Extreme winds and/or tornados
- Release of chemical or toxic gas

Traditionally, safety analysts have been modelling plants assuming full power operation. Several incidents involving loss of decay heat removal during shutdown have pointed out the vulnerability of the plant in the shutdown mode. Also new types of initiators have been identified in shutdown mode, e.g. due to equipment being out of service and increased human activities. (IAEA 1993)

For each of the initiating events, an event tree, depicting possible plant responses (accidents and successes) should be made. Some of the initiating events would induce the same or a similar plant response. In that respect, the different events are grouped in order to decrease the amount of analyses required for PRA. (IAEA 1993)

In addition, postulated initiating events and associated transients should be grouped into categories (see next section). Currently, the most common approach is to group initiating events and their associated transients according to the expected frequency of the initiating events. The second approach is to group according to the frequency of the accident scenarios. (IAEA 2009b)

## 4.2 Plant states

Plant states are categorised according to the severity of the situation. The IAEA glossary (2007) gives the following definitions:

- *Normal operation*: Operation within specified *Operational Limits and Conditions* (OLC). This state includes startup, power operation, shutting down, shutdown, maintenance, testing and refuelling.
- *Anticipated Operational Occurrence* (AOO): An operational process deviating from normal operation which is expected to occur at least once during the operating lifetime

of a facility but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions.

- *Design Basis Accident (DBA)*: Accident conditions against which a facility is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorised limits.
- *Severe Accident*: Accident conditions more severe than a design basis accident and involving significant core degradation.

Alternative definitions can be found in the European Utility Requirements (EUR 2012) that define a *Design Basis Condition (DBC)* as a situation (of internal origin) for which the plant is designed according to established design criteria and conservative methodology. In a similar fashion, YVL B.1 (2013) defines a set of *Design Basis Categories (DBC)*. *Anticipated operational occurrence (DBC 2)* is such a deviation from *normal operation (DBC 1)* that can be expected to occur once or several times during any period of a hundred operating years. *Accident* includes postulated accidents, design extension conditions and severe accidents. In YVL, the DBCs are mapped to the DiD levels as shown in Figure 5.

Level 1	Normal operation (DBC 1)	
Level 2	Anticipated operational occurrences (DBC 2)	$f > 10^{-2}/a$
Level 3a	Postulated accidents Class 1 (DBC 3)	$10^{-2}/a > f > 10^{-3}/a$
	Postulated accidents Class 2 (DBC 4)	$f < 10^{-3}/a$
Level 3b	Design extension conditions (DEC)	Multiple failures DEC A – CCF combined with DBC2 / DBC3 DEC B – Complex failure combination DEC C – Very rare external event
Level 4	Severe accidents (SA)	Safety goals CDF $< 10^{-5}/a$ ; LRF $< 5 \times 10^{-7}/a$

Figure 5. DiD levels, event categories and frequencies (source: STUK).

DBC's are usually classified into categories "according to their expected frequency". At first sight, this kind of definition doesn't make sense, since a rare but harmless deviation should obviously not be considered as an accident. The basic idea is, however, to design the plant so that regulatory requirements are fulfilled. For each DBC, regulations set requirements related to radioactive releases, failure criteria (N+1, N+2) and diversity. Some requirements also limit acceptable event frequencies. The applicant's combination of event frequencies and consequences should be balanced and reasonable. Otherwise, the solution might not be accepted, or it might be economically infeasible due to low availability or high investment cost.

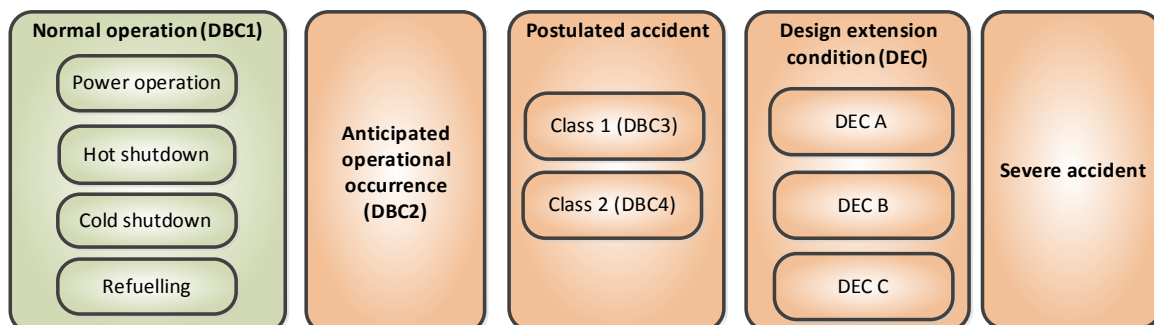


Figure 6. Classification of plant states according to YVL B.1 (2013).

As described above, a PIE triggers the transition from normal operation to an Anticipated Operational Occurrence (or even directly to an accident). The main responsibility of plant systems and personnel is to keep the plant within its safe envelope and when disturbances occur, to bring it to a *controlled state* and finally to a *safe state*. According to YVL B.1 (2013), *controlled state* is a state where a reactor has been shut down and the removal of its decay heat has been secured. *Safe (shutdown) state* in turn is a state where the reactor has been shut down and is non-pressurised, and removal of its decay heat has been secured. According to EUR (2012), controlled and safe states are defined only in incident or accident conditions or in certain DEC. Obviously, a PIE can occur in any of the plant operational states during normal operation. Figure 7 illustrates the relations between DBCs, operational states in DBC1 and controlled and safe states

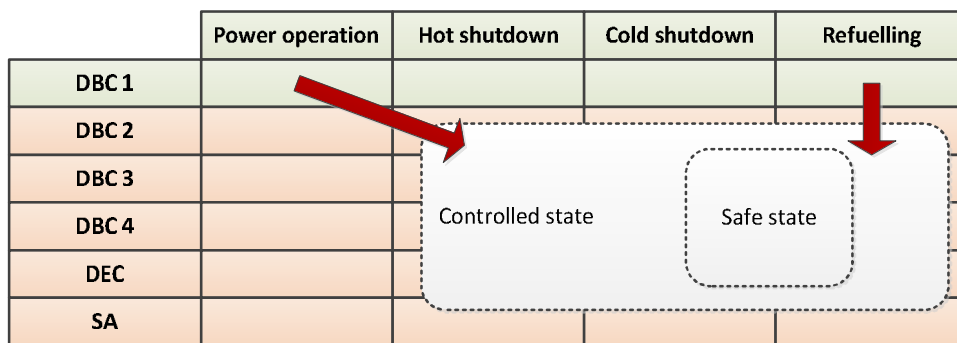


Figure 7. Relations of initial operational states, resulting design basis conditions and controlled/safe states.

To conclude the discussion above, Figure 8 summarises the key terms and relationships discussed above. The definitions and Finnish counterparts can be found in appendix B.

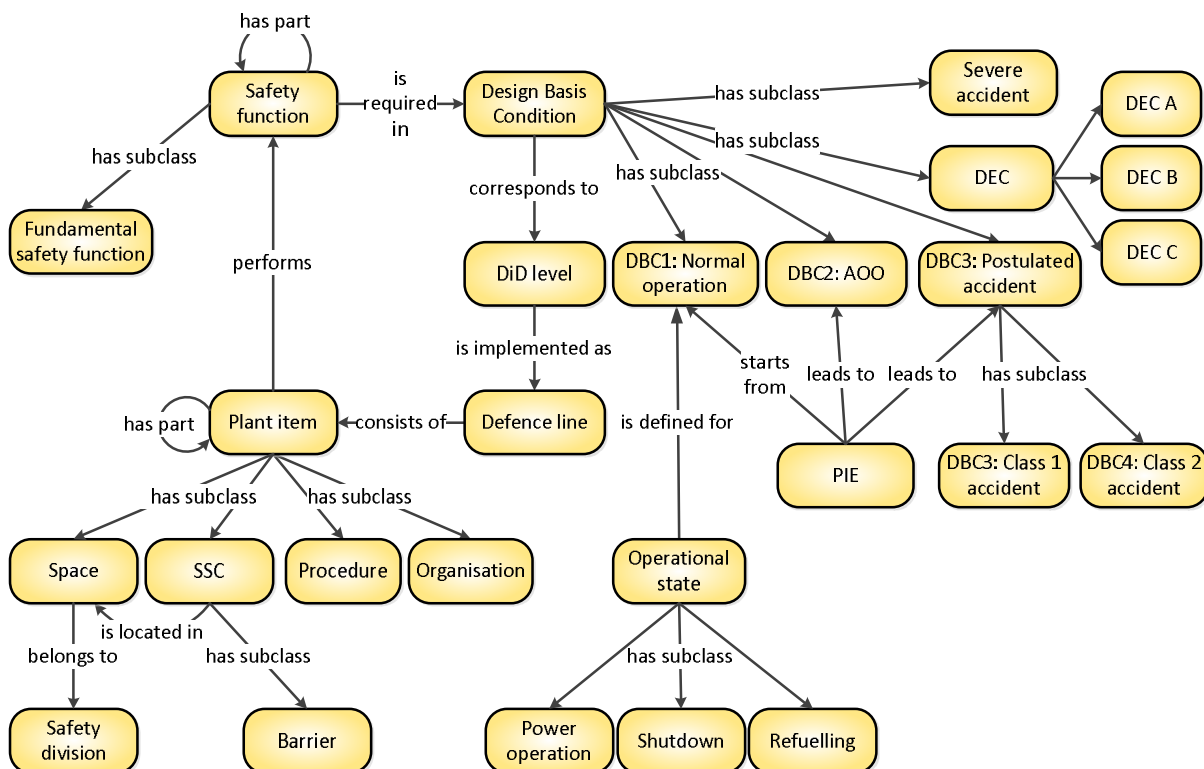


Figure 8. Main concepts related to plant-level DiD.

### 4.3 On dependencies between NPP systems

Dependencies are a major source of complexity in man-made systems. Dependencies can be intended or unintended, concern both physical plant items and their functions and caused by direct interactions or reliance on a common element. While interactions are necessary for desired system functionality, unnecessary and potentially dangerous dependencies must be identified and removed early in the design process. Redundancy, diversity and separation are examples of principles widely applied to avoid such dependencies. The definitions given in guidelines and regulations are often rather abstract. The aim of this section is to clarify some of the terms closely related to DiD and I&C architectures.

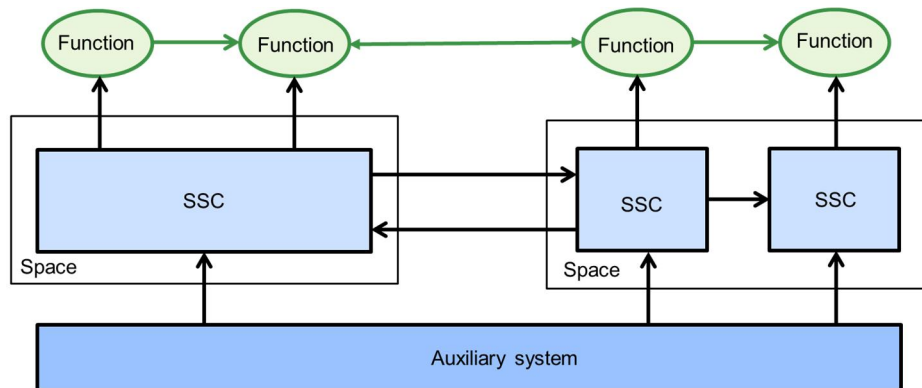


Figure 9. The functions performed physical plant items make things happen.

To do this, also certain very basic terms must be first defined. Figure 9 illustrates our way of looking at I&C systems (see Tommila & Alanen 2015). A nuclear power plant consists of physical plant items that are *Systems, Structures or Components* (SSC) located in various *spaces* (rooms, outdoor areas) and connected to each other. As suggested by Tommila & Alanen (2015), *functions* are understood as specifications of capabilities of plant items, for example as control loops performed by an I&C system. These interconnected functions generate all the behaviours that can occur, including malfunctions caused by design errors. For SSCs to operate, they must be supported by various auxiliary systems such as power supplies and cooling facilities.

In I&C systems, binary and analogue signals are the typical way to connect individual functions together. In addition to the value, the communicated data items can contain a time stamp and quality information. The specified I&C functions are implemented as software components (e.g. function blocks) executed by the control equipment (e.g. distributed controllers and smart field devices) in cyclical or event-driven mode. In general, however, modern software-based systems can interact also with more complex data structures, services and messages. So, the outputs of a digital system can provide structured data, events and services to be accessed by other systems, typically via the communication middleware of the control platform.

There are many types of dependencies between various plant elements, for example:

- SSC → function: One or more systems are needed to perform a function (in a role). Faults in an SSC affect the performance of the function or make it fully unavailable. SSCs are also dependent on auxiliary systems. Shared support systems are a source of Common Cause Failure (CCF).
- Function → function: Interacting functions exchange material, energy or information via a physical resource (e.g. a shared memory or communication link). Execution of independent functions must be synchronised, e.g., by an event.

- SSC → SSC: Plant items are intentionally connected by wires, pipelines, etc. The state (e.g. voltage level or pressure) of a component may affect the state of another component.
- Space → SSC: Environmental conditions, e.g. temperature, have impacts on plant items installed in a space. Physical phenomena originating from other SSCs in the space (e.g. radiation) are mediated by the space.

Notice that *traceability* is related to dependencies between engineering artefacts describing the system itself. In addition to the safety of the final system, dependencies are relevant for synchronising the development activities performed by various engineering disciplines and teams. So, in the broadest sense, the issue of dependencies in engineering design includes interdependencies in real-world system, its engineering artefacts and the processes and human organisations for system development, operation and maintenance. If dependencies are not carefully considered, the dependencies will often be revealed at integration tests (Torry-Smith et al. 2014), which is quite obviously too late.

#### 4.3.1 Redundancy

In general, redundancy refers to the existence of more than one means for performing a required function (IEC 60050-192 2015). For example, duplicated components and parity bits in communicated data are forms of redundancy.

By definition, redundancy leads to two or more system elements capable of performing a function. Often only one of them is active while others provide a readily available reserve in standby mode. In systems with memory, such as I&C systems, the internal state of the spare parts must be synchronised with the active element in order to provide a rapid and bumpless switch-over. When several system elements are active, their outputs must be combined in a suitable way. For example, a load balancing control allows three cooling water pumps, each having a 50 % capacity, to be run in parallel. For inputs and outputs of I&C systems, a voting unit must be added to drop outliers and to produce one validated signal. When more complex software-based functions are concerned, the principles of failure tolerance, reconfiguration and loosely coupled systems come into play. Typical solutions can be defined as high-availability architectural design patterns. A common example is the “m out of n” (m oo n) structure, wherein at least m of the total n items must be functioning to meet a requirement.

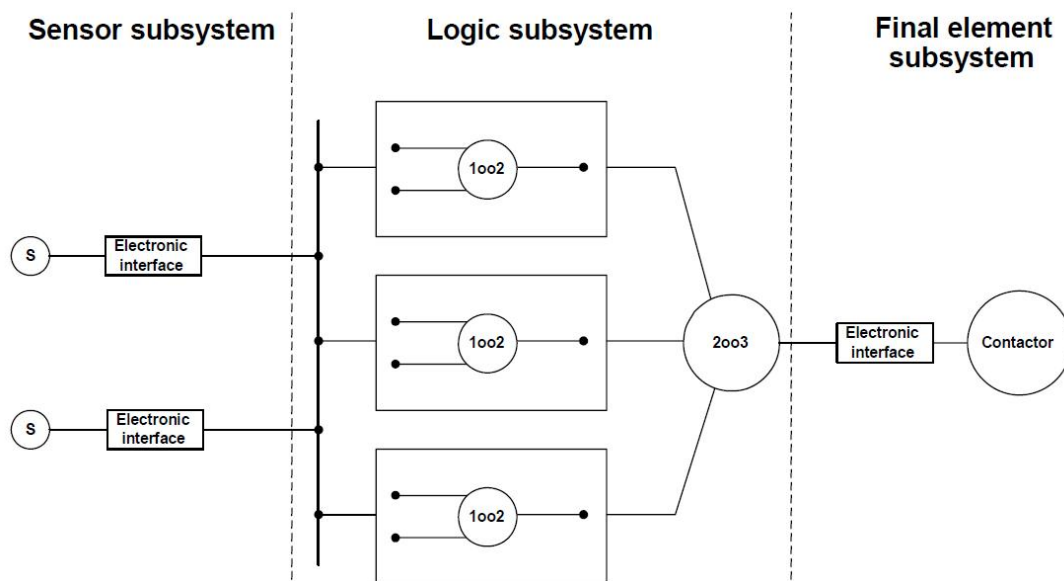


Figure 10. A system architecture with two sensors with 1oo2 voting and a three-redundant logic subsystem in a 2oo3 configuration (IEC 61508-6 2010).



In the context of nuclear safety, IAEA (2007) and YVL B.1 (2013) give a slightly narrower definition as “provision of alternative (identical or diverse) structures, systems or system components, so that any one of them can perform the required function regardless of the state of operation or failure<sup>2</sup> of any other”. This definition is limited to SSCs as the means and doesn’t explicitly consider degraded performance levels or various combinations of SSCs in performing a function. This is probably a good approach for safety-critical systems and anticipated abnormal situations. For unexpected, beyond the design basis conditions, a broader interpretation of redundancy might be useful (see the overview of resilience in Section 4.7).

Redundancy is used primarily to improve reliability or availability. Extra elements also provide flexibility in testing and maintenance operations. Redundancy may also be used to minimise spurious actions through architectures such as 2oo3 (IEC 61508-4 2010). The disadvantages include increased investment cost and additional complexity of the system.

#### 4.3.2 Diversity

In general, diversity refers to a kind of variety, i.e. to the condition of being composed of differing elements (see [www.merriam-webster.com/dictionary/diversity](http://www.merriam-webster.com/dictionary/diversity)). The term is used in many areas, e.g. in natural sciences, technology, business and sociology. In the development of safety critical systems, such as nuclear power plants, diversity is complementary to DiD as an approach for addressing CCF vulnerabilities.

As defined in YVL B.1 (2013), diversity refers to the backing up of functions through systems or components having different operating principles or differing from each other in some other manner, with all systems or components able to implement a function separately. In a similar way, the IAEA glossary (2007) characterises diversity as presence of two or more systems or components to perform an identified function, where the systems or components have different attributes so as to reduce the possibility of common cause failure. NUREG/CR-6303 (1994) describes six basic types of diversity:

- Human diversity: Different design teams or maintenance personnel.
- Design diversity: Different approaches, e.g. different technologies or architectures, to solve a problem.
- Equipment diversity: Different equipment to perform safety functions.
- Software diversity: Different programs designed and implemented by different development groups to accomplish the safety goals.
- Functional diversity: Different underlying principles or mechanisms (e.g. gravity versus pumping).
- Signal diversity: Use of different process parameters to initiate protective action.

---

<sup>2</sup> Tolerance of misbehaving (malfunctioning) system elements is obviously hidden in the definition of failure and in the expression “state of operation”. According to IAEA, an SSC is considered to fail when it becomes incapable of functioning, whether or not this is needed at that time. IEC 61508-4 (2009) defines failure as termination of the ability of a functional unit to provide a required function or operation of a functional unit in any way other than as required.

Diversity attribute	Strategy <sup>a</sup>		
	A	B	C
<b>Design</b>			
Different technologies	x	–	–
Different approach—same technology	–	x	–
Different architectures	i	i	x
<b>Equipment Manufacturer</b>			
Different manufacturer—different design	x	x	–
Same manufacturer—different design	–	–	–
Different manufacturer—same design	–	–	x
Same manufacturer—different version	–	–	–
<b>Logic Processing Equipment</b>			
Different logic-processing architecture	i	i	x
Different logic-processing versions in same architecture	–	–	–
Different component integration architecture	i	x	x
Different data-flow architecture	i	–	–
<b>Functional</b>			
Different underlying mechanisms	i	i	–
Different purpose, function, control logic, or actuation means	x	x	x
Different response-time scale	–	–	–
<b>Life-cycle</b>			
Different design organizations/companies	x	x	x
Different management teams within same company	–	–	–
Different design/development teams (designers, engineers, programmers)	i	i	i
Different implementation/validation teams (testers, installers, or certification personnel)	i	i	i
<b>Logic</b>			
Different algorithms, logic, and program architecture	i	x	x
Different timing or order of execution	i	i	–
Different runtime environment	i	i	x
Different functional representation	i	i	x
<b>Signal</b>			
Different parameters sensed by different physical effects	x	x	x
Different parameters sensed by same physical effects	x	x	x
Same parameter sensed by a different redundant set of similar sensors	x	x	x

Figure 11. Diversity strategies of NUREG/CR 7007 (2009). Intentional diversity (x), inherent diversity (i), not applicable (–).

A more detailed list is shown in Figure 11. Typically, several types of diversity should exist (NRC 2012). Two issues must be addressed by the design team: (1) how much diversity is required and (2) what combinations of diversities are most effective in avoiding CCF vulnerability (NUREG/CR 7007 2009). The number of possible combinations is large. As a solution, NUREG/CR 7007 (2009) presents three strategies: (A) different technologies; (B) different approaches within the same technology; and (C) different architectures within the same technology.

So, the key in diversity seems to be that several and different means are applied to achieve certain safety goals. The purpose is to improve system dependability by limiting the risk of Common Cause Failures caused by dependencies in the technology basis and development practices. Use of several means in the implementation introduces some redundancy by definition thus having an impact on availability also. The means can be different to a certain degree, such as is the case in the three strategies in Figure 11. Furthermore, the differences between the means can be in their functions, implementation or in the life-cycle activities and the organisations and tools used for them. Introducing the separation as early as possible in the development chain is probably the most powerful approach. For example, looking for functional diversity and fundamentally different operating principles is the most common and strongly recommended approach (NUREG/CR 7007 2009). Similarly, having requirements defined by two independent teams might be more effective than two groups of programmers during the implementation phase.

### 4.3.3 Physical separation

According to YVL B.1 (2013), physical separation refers to the separation of systems or components from one another by means of adequate *barriers*, distance or placement, or combinations thereof. ONR (2014) uses a different term “segregation” defined as physical separation of structures, systems or components by distance or by some form of barrier that reduces the likelihood of common cause failures.

As can be seen, YVL gives only solutions while ONR indicates the purpose also, in a very broad sense however. In our opinion, neither of the definitions catches the key idea of physical separation. As with *barrier*, the purpose of separation is to prevent propagation of any type of physical phenomenon that may be harmful to physical parts or operation of other SSCs (and thereby cause their functions to fail). The harmful effect can be triggered, e.g., by misbehaviour of a function, hardware fault or by an external event damaging several redundant components. Examples of harmful effects include water hazards from water sprays, flooding, fire, missiles, steam jets, pipe whip and chemical explosions (IAEA 2014a).

These examples are mostly mechanical, but we would also include other mechanisms like radiation and heat. In addition, electricity can be considered as a physical phenomenon. For example, IAEA (2014a) uses the term *electrical isolation*. Adverse interactions can be caused by factors such as electromagnetic interference, electrostatic pickup, short circuits or application of the maximum credible voltage. Examples of provisions for electrical isolation include circuit breakers, optical isolation, cable shielding, separation distance and mechanical structures. For example, an optical isolator is a barrier against electrical pulses but also prevents information flow in the wrong direction (see functional isolation below).

### 4.3.4 Functional isolation

In YVL B.1 (2013) functional isolation refers to the isolation of systems from one another so that the operation or failure of one system does not adversely affect another system. In YVL, functional isolation also covers electrical isolation and isolation of the processing of information between systems. IAEA (2007) gives the definition as prevention of influences from the mode of operation or failure of one circuit or system on another. WNA-PS-00016-GEN also includes allocation of related functions to separate hardware to ensure that upon failure no more than one of the functions is affected.

So, the purpose of functional isolation is to remove or reduce unnecessary and unintended dependencies (information flows, timing issues, CCFs) between *functions* (i.e. “separation of functions”, see Figure 9). When function A is lost or when it misbehaves (spuriously or in other wrong ways), function B should not be affected (too much). The means can be purely functional (no signals), software-based (protocols) or physical (barriers or no signal paths). Possible methods to achieve this are:

- B does not use A at all (no engineered communication)
- The link between A and B provides diagnostics and replacements (loose coupling, e.g. a voting unit)
- The link limits the information flows (rate, direction, values) to reduce the effects on B’s behaviour (e.g. opto-coupler allowing information flow in one direction only)
- B detects the failure and behaves accordingly (defensive behaviour)
- A and B are dependent on or performed by independent resources (no common cause failures, e.g. separate power supplies)

“Operation” and “failure” are functional terms and therefore different from the harmful physical phenomena considered in physical separation. So, physical separation is about physical dependencies between physical system elements (hardware) while functional

isolation is related to the functional model of the system. As with physical separation, functional isolation is not a black-and-white issue. Instead, there is a certain degree of “functional coupling” between two system functions.

To give some examples, Figure 12 shows two I&C functions allocated to two physical controllers. The controllers are physically separated by locating them in different rooms. Also the optical isolator separates the controllers electrically. Moreover, some physical separation from the power supply (and between controllers) is provided by the overvoltage protecting devices.

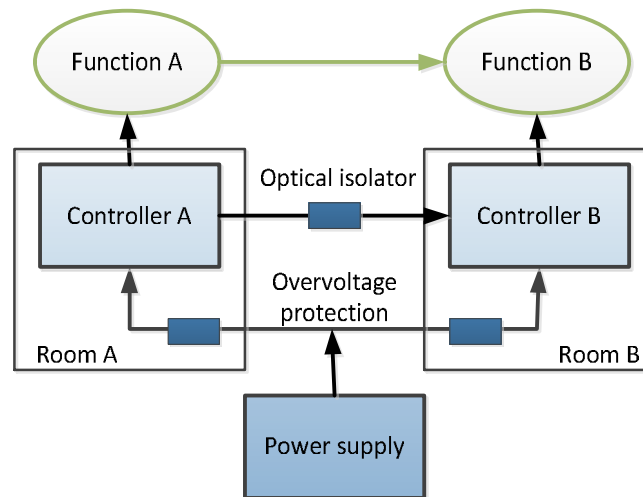


Figure 12. Examples of physical separation and functional isolation.

As far as functional isolation is concerned, functions A and B are clearly connected by an information flow. However, the optical isolator should allow communication only in one direction thereby making A functionally isolated from function B. But the power supply is a source of common cause failure since both functions are dependent on their controllers and they are in turn functionally dependent on electrical power. If the power supply fails to perform its “provide power” function, both functions A and B are lost.

We can now sum up the discussion on dependencies between NPP systems in Section 4.3. The purpose of the discussion is to clarify some terms and to proceed towards structured system models and methods that can be used to identify potentially harmful dependencies early in the design process. Our conceptual basis starts from functions performed by physical resources, i.e. SSCs and human operators. For a function to be available, at least a sufficient combination of possibly redundant SSCs must be able perform their own partial (service) functions. For this to be possible, the resources may need certain auxiliary functions (e.g. supply of power) to be available. This leads to complex network of functions and resources describing, what is needed for the top-level safety functions to be successful.

In our understanding, physical separation tries to limit the propagation of unwanted physical phenomena between SSCs while functional isolation considers links between abstract system functions. The terms physical separation and functional isolation are related to dependencies embedded into the design solutions while diversity attempts to limit the dependencies caused by the development practices and technologies used.

#### 4.4 Definitions of faults and failures revisited

Due to the complex failure mechanisms of software-based systems, unintended and random behaviour of control systems has become a concern in the nuclear domain. In Section 4.6, we will give some interpretations for the common expressions “active failure” and “spurious

actuation”. But before that, the basic concepts like fault, failure and failure mode need to be discussed in this and the next section.

There are many interpretations for terms *fault*, *error* and *failure* (Randell 2003, Avizienis et al. 2004, Uder, Stone & Tumer 2004). Most definitions found in safety standards are based on IEC’s electrotechnical vocabulary IEC 60050-192 (2015), often with some modifications. In it, fault is inability of an item to perform as required, due to an internal state. Failure refers to the loss of ability to perform as required. According to IEC 61513 (2011), equipment is considered to fail when it becomes incapable of functioning, whether or not it is needed at that time. Fault is defined as a defect in a hardware, software or system component, i.e. as a possible cause of inability. In both standards, error is a discrepancy between an observed real value and the correct, specified value. While error looks like a state, *human error* (mistake) is a human action that produces an unintended result.

With this definition, failure is an event transferring the system to a “faulty” state. Fault is an abnormal condition, i.e. a state, that may cause a reduction in, or loss of, the capability of a system to perform a function. One confusing thing with these definitions is that a failure may not be externally observable if the system or its function is not needed the time of the event. Many authors understand failure differently as an instance in time when a system displays behaviour (at system boundary and visible to users) that is contrary to its specification (e.g. Randell 2003, Avizienis et al. 2004, <http://en.wikipedia.org/wiki/Dependability>, Haapanen & Helminen 2002). Also IEC 60880 (2006) defines failure as deviation of the delivered service from the intended one. Furthermore, a consequence of considering faults as internal problems is that a system can’t be said to fail, if only its inputs are wrong. In practice, however, “faults are propagated” between systems. It would be quite natural to say that “a system fails”, when the correct input signal is lost.

So, there seems to be some variation and confusion in the basic terminology. In fact, some standards even seem to use their own definitions in an inconsistent way, and IEC 60812 (2006) uses the terms fault and failure interchangeably “for historical reasons”. Obviously existing definitions familiar to nuclear practitioners should be preserved as far as practical. Some refinements and new terms can, however, be proposed. Below we give some interpretations in the context of digital I&C systems.

If faults and failures are, by definition, internal events and states, there is no agreed word for “externally visible misbehaviour”. Failure mode defined as “manner in which failure occurs” (IEC 60050-192 2015) is close but with the word “mode” looks like a term suitable for classification of misbehaviours. So, we suggest introducing the term “malfunction” as a deviation in the behaviour of a system. Figure 13 gives an example of a temperature controller supposed to follow a pre-defined ramp within given safety margins. Three malfunctioning periods can be seen in the figure, first a spontaneous rise of the signal, then a delayed reaction to the rise of the setpoint and finally the temperature drifting out of the specified region.

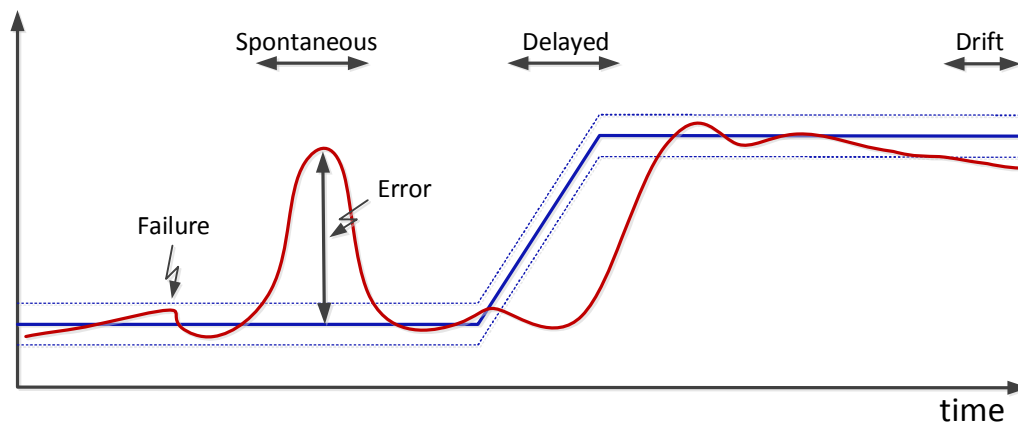


Figure 13. A malfunctioning temperature control.

Now, the key terms can be interpreted as follows (Figure 14):

- **Fault:** Reason for the inability (state) of *system element* to perform its intended *function(s)*, due to an internal state. Faults include, for example, damaged hardware, software defects and wrong configuration data. If not properly handled by fault tolerant solutions, a fault may lead to immediate or delayed *malfunctions* when triggered by a demand.
- **Defect:** Kind of fault, used for discrepancy in the static structure of a system element, e.g. a hardware fault or design flaw.
- **Error:** Kind of fault due to a discrepancy in the (dynamic) state of the system element, e.g. wrong data values in the memory or outputs.
- **Failure:** Termination (event, sometimes also termed as “failure event”) of the ability of a system element to perform an intended function. The transition of an item from state “ok” to a faulty state. A new fault can have an impact on only some of the functions. Therefore, it is more correct to say that a “function of a system fails”, when it becomes unavailable or degraded.
- **Common Cause Failure (CCF):** Refers to failures of multiple items, which would otherwise be considered independent of one another, resulting from a single cause (IEC 60050-192 2015). As defined in (EPRI 2014), the failures are assumed to be concurrent and occur over a time interval during which it is not plausible that the failures would be corrected.
- **Demand:** An external request (e.g. a signal combination or command) asking a system element to do something.
- **Malfunction:** Unintended (unwanted) externally visible behaviour caused by a fault in the system. Malfunctioning of a function can be triggered only in specific situations like a received start command (demand) and certain input data combinations. These kinds of malfunctioning have their origin in system design, e.g. in requirements, functional specifications or software implementation. In addition, malfunctions can be directly caused by random physical failures, such as a suddenly damaged output transistor.

- *Failure mode*: Type of malfunction used for characterising different kinds of failure malfunctions<sup>3</sup>, e.g. “loss of function”, “wrong output” and “delayed signal” (see NEA 2015). Note that failure mode could also refer to physical phenomena, such as over-voltage or catching fire.
- *Failure effect*: Physical or functional consequence of the malfunction. Can lead to a new fault that causes failure of other functions (i.e. fault propagation within and between systems).

In the first place, a system can be seen as a single unit so that errors, malfunctions and failure effects are visible at the external system boundary. However, a system consists of several system elements, and each of them can fail separately. The effects are not necessarily seen outside. So, we can speak about internal and externally visible failures, faults, errors, malfunctions, etc. To be specific, we should always define the domain of discourse by saying “failure of system/component/function X”.

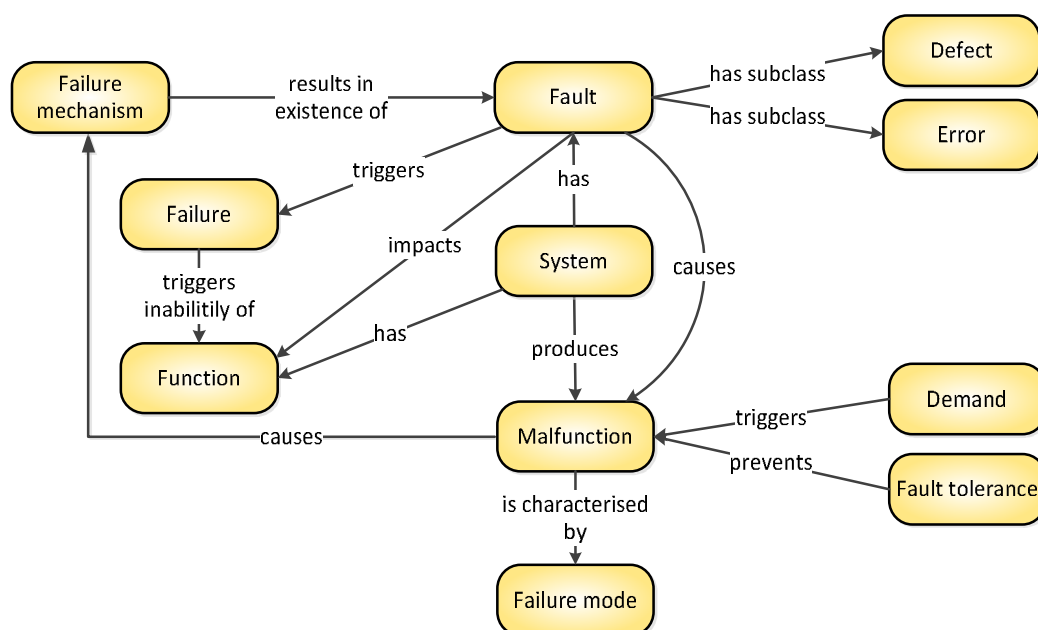


Figure 14. Suggested main failure concepts.

## 4.5 Classifying failure modes

As illustrated in Figure 14, malfunctions are here understood as externally visible misbehaviours of system elements. The possibilities are countless and dependent on the application, element type and particular situation. To make things easier, various failure modes can be defined and used to categorise the malfunctions. An agreed taxonomy of failure modes could be a way to support

- communication between various stakeholders, e.g. in requirements definition
- identification and analysis of potential problems, e.g. in FMEA
- analysis and reporting of occurred abnormal events
- development of software tools for risk analysis and systems engineering.

<sup>3</sup> The term “failure mode” is actually inconsistent with the other definitions since it is used here to describe malfunctions not failure events. However, it has been preserved just to be compatible with the existing terminology used in reliability and safety engineering.

In fact, several taxonomies of failure modes and related concepts have been suggested in the literature (e.g. by Avizienis et al. 2004, Li et al. 2006, O'Halloran, Stone & Tumer 2012). In the nuclear domain, the Working Group on Risk Assessment (WGRisk) of OECD/NEA has recently published a failure mode taxonomy in particular for probabilistic risk assessment (PRA) of digital I&C systems (NEA 2015).

After many years of debate, there obviously is no commonly accepted agreement. As discussed above, even the basic concepts are a source of confusion. Current taxonomies don't necessarily have the properties of a good taxonomy, such as a hierarchical structure from general to particular, clear criteria of classification, full coverage of the domain (completeness) and avoidance of overlaps between different classes (disjointness). In addition, the taxonomy and its terms should be understandable so that various malfunctions are classified in the same way by all stakeholders. We try to add something to the discussion with regard to concepts related to DiD (e.g. functional isolation and physical separation).

First of all, several criteria can be used to classify system faults and failures, for example fault location, life-cycle phase, type of misbehaviour, detectability, etc. There is, however, the danger of mixing up malfunctions and their causes. We try to avoid this with the interpretation of malfunction as unwanted behaviour of a system element seen as a black box. In spite of this focus, there are more than one classification criteria, for example the content and timing of system outputs (Aviezienis et al. 2004). This leads to the idea that each actual malfunction can be categorised in several independent (orthogonal) dimensions. In other words, an abnormal event report can specify several attributes, one or more in each dimension, that together characterise the way system actually malfunctioned (see O'Halloran, Stone & Tumer 2012). Here, we suggest the following classification dimensions:

- Functional vs. physical: An I&C system is a physical object consisting of hardware and software (see Tommila & Alanen 2015). Its elements, in particular software components (e.g. function blocks in a PLC), implement the intended (abstract) I&C functions (e.g. measurements and protections). Now, functional failure modes characterise how the system behaviour deviates from the expectations defined, e.g., by I&C functions. Quite obviously, this has something to do with the idea of functional isolation in section 4.3.4. Physical failure modes are in turn related to the physical impacts that the I&C hardware might have, for example due to over-voltage or excessive heat generation. Physical separation in section 4.3.3 is a way to limit the consequences of physical failure modes.
- Content: A digital I&C system has a set of outputs providing data (basic signals and more complex data), event notifications (alarms) and services (request/reply protocols). When a malfunction with wrong output occurs, the content or part of it is missing or erroneous in some way.
- Timing: An I&C system is expected to deliver its outputs within certain time limits and possibly in a specific order/sequence. Not obeying these constraints can be classified as a timing failure.

Note that a system can exhibit several malfunctions at the same time. Moreover, several system elements can misbehave simultaneously, e.g. due to a common cause. Especially malfunctions caused by unsuccessful coordination and synchronisation are associated with several system elements or systems. However, on a higher level of system decomposition, this means a combined misbehaviour of more than one system outputs. Anyway, we might speak about "combined failure modes". For example, when a computer stops fully due to loss of electrical power, its failure mode "halt" includes both missing content and infinitely late timing (adapted from Avizienis et al. 2004).

To take an example from process and plant engineering, we can consider a crack in a cooling water pipe. From the functional viewpoint, the pipe loses its ability to transfer cooling



water to the reactor. Physically it misbehaves by releasing water to its environment thereby potentially causing damage of nearby electrical equipment.

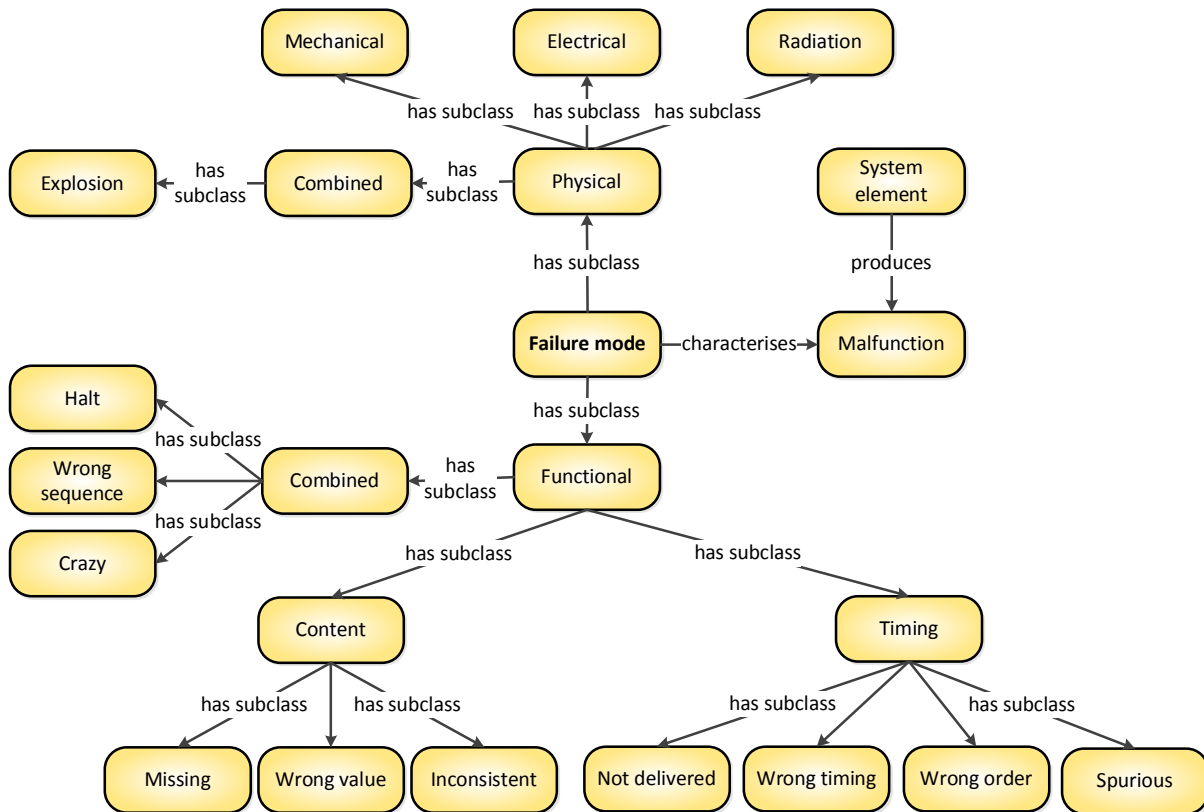


Figure 15. Partial classification of failure modes.

Figure 15 illustrates the top-level classification of failure modes with some more specific examples. The first distinction is made between functional and physical failure modes. Functional modes are divided into problems in the content and timing of I&C system outputs. Physical modes are classified according to the kind of unwanted impact spread to its environment by a misbehaving system element. Both main classes can have terms for combined failure modes for frequently encountered combinations. It is not the aim of the report to elaborate this issue any further. However, this reminds us of the old idea of a shared taxonomy and sets of common failure modes for various types of functions and devices. For example, an internet-based repository would allow the designer or safety analyst to query the potential failure modes for each particular function (Uder, Stone & Tumer 2004).

#### 4.6 On active failures of intelligent systems

With this background we can now look at active failures in more detail. “Passive failure” is the term usually referring the unavailability of a system or function. In short, “active failure” means that a system unexpectedly does something it shouldn’t do in the given situation. In nuclear I&C, the more specific term “spurious actuation” refers to changing the state of process equipment, e.g. opening a valve, without a demand. In digital systems, the possibilities for misbehaviour are endless. What can be explicitly required, specified and tested represents a negligible portion of possible behaviours. Active failures are unpredictable and therefore often considered more difficult than passive ones. The question is how to ensure that active failures don’t compromise safety?

In engineering, “active components” are usually understood as devices that require external power, e.g. fuel or electricity, to operate. Traditionally, active functions and components have been associated with mechanical motion or a change of state, e.g., closing a relay or change

in state of a transistor. In electrical engineering, the IEC electrotechnical vocabulary (<http://www.electropedia.org/>) describes active failure as a failure of an item which causes the operation of the protection devices around it and results in the opening of one or more circuit breakers or blowing of one or more fuses. This definition clearly includes two ideas: unwanted spontaneous action and having an effect on the surrounding world. In YVL B.1 (2013), *active failure* is defined in a rather general way as failure mechanisms other than passive failure mechanisms (such as malfunctions). As its complement, *passive failure* means a mode of failure that can be treated as an operability deficiency (such as a total or partial lack of a device or operability).

Existing definitions of active failures may be sufficient for traditional, signal-oriented control systems. Also in digital I&C systems, individual signals play an important role in spurious actuations. In general, however, modern programmable I&C systems are kind of “intelligent agents” comparable to human actors. They can perform several I&C functions implemented as *software components* (e.g. function blocks) and executed by the control equipment (e.g. distributed controllers and smart field devices) in cyclical or event-driven mode. In addition to signals, these systems interact with their environment with complex services and messages. Therefore, more elaborate and general definitions may be needed. The discussion below is an attempt into this direction.

In standard language, “being active” means bringing about of an alteration by force or through a natural agency, or an act of will (<http://www.merriam-webster.com>). The first part matches well with the traditional interpretations above while the second part, “act of will”, brings us to the domain of intelligent agents. Some ideas can be borrowed from action theory, an area in philosophy concerned with the processes causing human bodily movements caused by desires and beliefs (see e.g. <http://plato.stanford.edu/entries/action/>). An *action* is something which is intentionally done by an agent in order to have an effect on the state of the environment or the agent itself. So, an active entity, an “actor”, needs to have the means to manipulate the state of the world, not only for changing states-of-affairs but also for maintaining them (Lind 2005). So, a temperature controller can be considered as an active entity. It operates in a continuous mode (IEC 61508-4 2010), while safety-relevant protective functions in nuclear power plants are typically activated only on demand (low demand mode). In addition to physical effects (e.g. movement or voltage change), deciding to do something can be seen as a mental action changing the mental state of the actor itself. In fact, deciding not to do something, e.g. letting things happen, is an action as well (see Lind 2005). Also intending and unsuccessfully trying can be considered as actions.

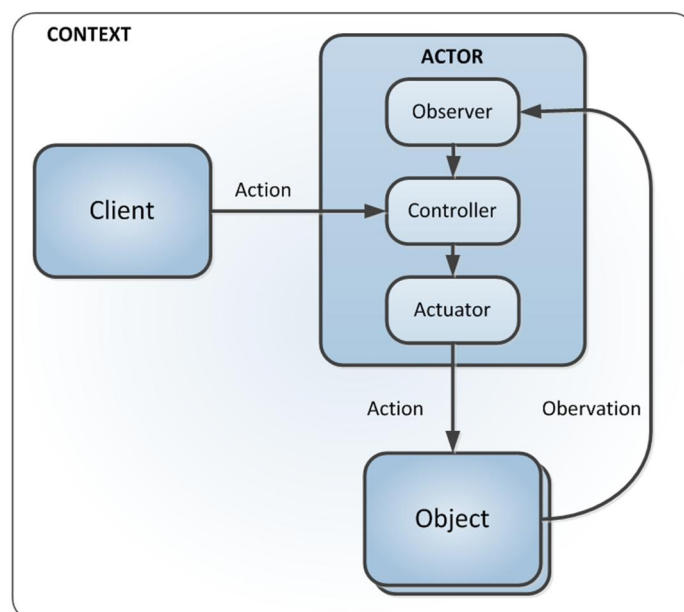


Figure 16. Model of an “intelligent actor”.

Thinking about the functions<sup>4</sup> of digital I&C, Figure 16 shows a model of an actor (I&C system) receiving information and commands from a client (e.g. operator or another computer system) and controlling some objects (process equipment). How should the term active failure be understood in this context? We can try to answer the question by combining the ideas and definitions above. This much can be said at this stage:

- In digital I&C, one system output can be controlled by several functions either at different times or coordinated by a priority or voting unit.
- A system or function is “on” if it is performing or ready to perform its tasks.
- Being “active” means that the I&C system (“acts”) changes its outputs, e.g. by changing a binary signal from false to true or by issuing an alarm message.
- Also continuously keeping (cyclically updating) the same output value can be regarded as acting?
- When the I&C system is “active” when it is not expected to be, it is said to “malfunction actively”.
- Spurious activation is a type of active malfunction where an I&C system unexpectedly without a demand triggers an external function, e.g. starts or stops a pump.
- The creation (event) of a new fault possibly leading to an “active malfunction” might be called an “active failure”. This is confusing but preserves the idea of inability of function irrespective of the current demand.
- Similarly, we might introduce terms for “active fault” and “active failure mode”.
- Decisions made by a controller are actions, and a decision not to act is also an action.
- So, when a software component in the I&C system decides not to react to an alarm or refuses to obey a command given by the operator (client), an active failure of the component occurs.
- However, at the system boundary this looks like a passive failure since the intended function of the I&C system is not available on demand. But, if the system clearly indicates its negative response, it behaves actively.
- In addition to software, hardware components can fail actively, e.g. due to a faulty transistor in an output module turning a signal on. These situations are not directly associated with I&C functions or software components. However, a faulty hardware component can make the I&C function fail and malfunction actively later in a specific situation.
- If the control system performs an intended action slightly too early, its performance is degraded. But beyond a certain limit, the situation can be regarded as a result of an active failure.
- Similarly, a passive failure occurs when action is delayed too much. But if it is delayed to a distant future (e.g. spooled to job queue), it becomes an active failure because it is not expected any more.

---

<sup>4</sup> Physical effects like over-voltage or heat are not considered here. See the discussion on physical separation in Section 4.3.3 and failure modes in Section 4.5.

- The intended output of an I&C function can include several signals, messages and services in parallel or as a timed sequence. There might be extra signals and messages as an indication a “partial active failure”.
- An analogue signal can oscillate or gradually drift out of specified limits. Should this be regarded as active or passive malfunction?

There seems to be many kinds of causes and internal mechanisms leading to malfunctions in digital I&C systems. Therefore, it is probably easier to define active failures with respect of what is expected by an external observer. These expectations should, in principle, be available in system specifications, for example in the form of functional requirements and logic diagrams. Expectations concerning active failures are, however, more difficult to define. They might be found in “negative requirements (“system shall not ...”) and failure tolerance requirements.

To sum up, “active failure” seems to be a fuzzy term boiling down to the general problem of I&C systems behaving randomly or “going crazy”. In general, safety experts seem to think that active failures are not a big problem in existing I&C systems (IAEA 2009a, Bäckström et al. 2005). Spurious actuations due to software failures are usually not modelled in PSA. Active failures are, however, a relevant issue, for example in failure tolerance analysis where worst case behaviours of I&C outputs should be considered. The important thing would be to develop ways to detect, analyse, avoid and tolerate the possibilities of chaotic behaviour in I&C systems.

## 4.7 Resilience for managing the unexpected

A major challenge of the nuclear industry is associated with extreme external events and complex failure combinations, such as the ones encountered in the Fukushima accident. These severe and unanticipated situations are beyond conventional safety design practices and have given rise to lively debate about research needs within the nuclear community (e.g. SNETP 2013 and NUGENIA 2013).

To cope with unexpected situations the human and technical elements of a nuclear power plant need to be optimally combined, proactive and flexible in their actions. In addition to functioning reliably, each element should react appropriately to external events and failures of other plant elements. Moreover, during the course of a transient or an accident, plant elements should co-operate and take advantage of all opportunities to prevent further escalation of the problem and to reach a safe plant state.

The notion of *resilience* has been proposed as an expression of such responses of a system. The term was originally used as a material’s ability to rebound or spring back after being deformed elastically. Later the term has been extended and used in many disciplines, e.g. in psychology and sociology, business and ecology. Resilience can be considered in many time scales from climate change and ageing of components to sudden tsunamis or loss of electrical power. In systems engineering resilience is related to the ability of a system to cope with change or failure and still maintain its functions. INCOSE (2015) uses the definition “ability to prepare and plan for, absorb or mitigate, recover from, or more successfully adapt to actual or potential adverse events”. One of the most cited definitions of resilience by Erik Hollnagel (2011) states that “resilience is the intrinsic ability of a system to adjust its functioning, prior to or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions.”

In recent years, resilience has become an important issue in many areas outside nuclear power, for example in critical infrastructures, air traffic management, transport networks and built environments. A notable amount of publications on resilience engineering exist. There are consortia and online networks working around the topic, for example the Resilience Engineering Association (<http://www.resilience-engineering-association.org/>), and

conferences are organised (e.g. <http://www.rea-symposium.org>). So, there is a lot of existing knowledge that might be taken as a starting point and adapted to the needs of the nuclear industry.

Resilience looks like a general concept that combines many more concrete features like reliability, robustness, maintainability, flexibility, learning and adaptation. Furthermore, cohesion is a key attribute of a resilient system, meaning the ability of its elements to operate together (INCOSE 2015). Consequently, resilience is an emergent and even nondeterministic feature of an entire socio-technical system, and not only that of the human or the technical part. This means that in a nuclear power plant resilient features should be designed into the process equipment, electrical systems, buildings and structures, operation and maintenance organisations and into the I&C systems. Clearly, many of the aspects of resilience are already covered by the nuclear design practices in the form of redundancy, diversity and separation of plant systems and functions. Also maintaining a safe plant state during operational occurrences, low-power operation and maintenance requires certain amounts of reconfigurability from plant systems. The allowed operating envelopes are defined in the *Operational Limits and Conditions* (OLC).

However, the proactive character of resilience emphasises the role of forward-looking situation awareness and built-in capabilities to operate in a wide range of circumstances and in various configurations. Therefore, we claim here that the new feature of a “resilient nuclear power plant” would be its multi-purpose functions and equipment that can be combined and used in more than one way.

To some extent, this idea is analogous to batch process control (IEC 61512-1 1997) in the chemical industry. There the design is based on pre-defined equipment procedures, e.g. for heating, cooling and transferring the product batch. In a product recipe these basic operations are parameterised and combined into a manufacturing sequence. Even if the available equipment units are slightly different, their procedures are functionally compatible. So, the recipe can be run on more than one unit or production line. In a nuclear power plant, recipes could correspond, for example, to alternative strategies for managing beyond design basis accidents.

With new plant concepts and upgrades of existing plants, digital information technology has become increasingly important. The question is what resilience would mean for I&C systems. In general, I&C systems can contribute to plant resilience in two main ways: firstly, by helping operators and other systems to act in a resilient way and secondly by being internally resilient. The first way would, for example, require the I&C system to provide relevant information and control options to human operators. The second way to contribute would mean capabilities to survive internal faults and external threats. Beyond normal reliability and robustness, I&C systems should have ability to recover from failures. Control systems should also be able to operate in all process conditions (including the extreme ones). In particular, the idea of reconfigurable equipment capabilities above would mean that I&C functions are from the beginning designed as “services” provided by various functional units operating in different operational states and operating modes, including both normal and abnormal situations. Flexible reconfiguration requires that the systems and functions are loosely coupled but interoperable. These decisions are essential elements of the I&C architecture discussed in Chapter 5. The purpose of resilience engineering is to determine an architecture and system characteristics that anticipate, survive and recover from disruptions (INCOSE 2015).

The dark side is that safety-relevant I&C systems and the overall I&C architecture need to be designed and verified according to strict engineering rules and regulatory requirements. Clearly, there is the risk that resilience increases complexity and contradicts with the requirement for critical I&C to be predictable. But on the other hand, providing relevant data for human users and dimensioning the equipment also for extreme conditions is needed in any case. Flexibility and the freedom to use it are a more difficult issue. Well-structured

functions and equipment can provide some flexibility without extra cost. One option is to design in a certain amount of resilience and to relax the operational constraints according to the current plant condition. During normal operation, prescriptive rules are in force but in severe accidents also creative solutions can be allowed. In addition to the capabilities of the technical systems, the human organisations must have the knowledge and procedures to use them. In order to manage the unexpected, engineering guidance and assessment methods should be developed for the resilience of the plant-level DiD and I&C architecture beyond normal failure tolerance and robustness features.

## 5. Modelling of I&C architecture

---

In common language, architecture refers to the way in which the components of a system are organised and integrated. In systems and software engineering (according to ISO/IEC/IEEE 42010 2011), architecture comprises fundamental concepts of a system in its environment embodied in its elements, relationships, and in the principles of its design. The description should record also the rationale for the decisions that have been made. Architecture is described according to several *viewpoints* each expressing the architecture from the perspective of specific concerns of the stakeholders. The standard does not require any particular viewpoints to be used. However, some typical examples of viewpoints found in the literature are requirements, functional, information, physical, process, operational, performance, security and development viewpoints.

Within nuclear I&C, the complexity of digital systems has resulted in difficulties in regulatory approval of I&C designs and thereby increases in costs and uncertainties faced by vendors and utilities (EPRI 2014). I&C plays an important role on all levels. Its architecture should be defined in the context of the plant's overall concept of defence in depth (EPRI 2014).

IEC 61513 (2013) defines *I&C architecture* as organisational structure of the I&C systems of the plant which are important to safety. The organisational structure specifies the main functions, class and boundaries of each system, the interconnections and independence between systems, the priority and voting between concurrently acting signals, and the HMI. With its focus on safety, the standard considers only a subset of the "whole I&C architecture of the plant" omitting unclassified systems and equipment. As part of the overall I&C architecture, an *I&C system architecture* defines the organisational structure of an individual I&C system. *I&C function* is also one of the key terms defined as a system function to control, operate and/or monitor a defined part of the process. In its recommendations for developing I&C architectures, EPRI (2014) adopts the definition given in IEC 61513 (2013) but extends it to encompass non-classified I&C systems as well. In our opinion, this is a reasonable generalisation, just like is considering the role of human organisations in the overall DiD architecture.

In practice the ideal situation with completely separate levels of defence is not typically realisable (EPRI 2014). For example, human-system interfaces or sensors and actuators may need to be shared between systems on different levels of defence (Figure 17). To minimise the dependencies, signal branching is provided at the sensor level and priority logic as close to the actuators as possible.

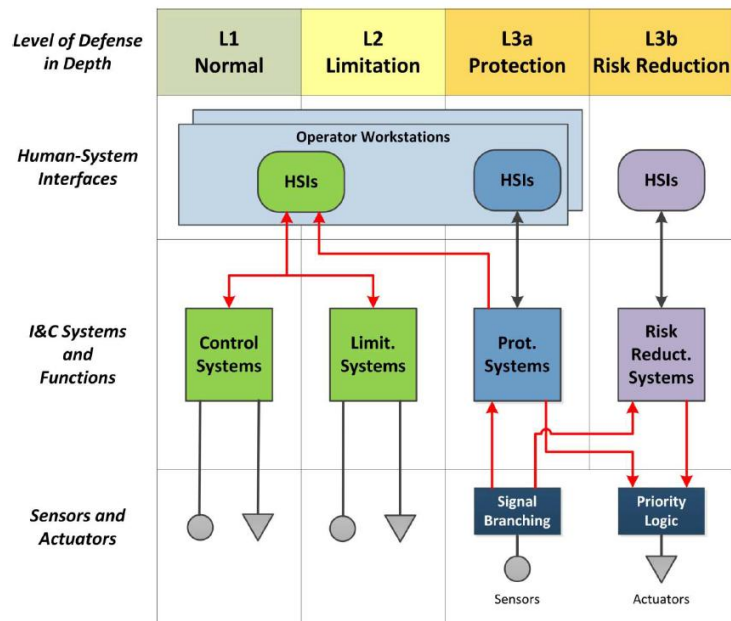


Figure 17. An I&C architecture and Defence in Depth (EPRI 2014).

So, what does all this mean for modelling nuclear I&C architecture? Firstly, though not explicitly stated the term architecture obviously refers to an overall description omitting unnecessary details, except perhaps the most critical ones. As systems are hierarchically decomposed, we can see architectures on the levels of the whole “system of systems”, individual systems, subsystems and even on the level of components. The boundary of a “system” depends on the viewpoint. Even though the descriptions of different levels should be compatible and linked to each other, the concepts and representations may be slightly different.

Secondly, a system interacts with its environment. For nuclear I&C systems, the interfaces to process equipment, electrical systems, human users, other I&C and information systems and to the operational environment should be part of the architecture description.

Thirdly, an architecture description should consider all relevant concerns and aspects of the system. We might make a distinction between the functional and physical (implementation) architectures. As described in EPRI (2014), functional architecture refers to the functions that need to be performed and how they should be structured, prior to assigning functions to specific I&C systems. While the term “function” has no clear definition in nuclear power, we understand a system *function* as a specification of a system’s behavioural capability (Tommila & Alanen 2015). In I&C, this means measurement and control “loops”, protections, control room displays and alarms, reports, etc. So, we can use the definition from IEC 61513 (2013) and say that a functional architecture specifies the *I&C functions* and their interactions, including the necessary data structures. On the level of basic process control, the function block paradigm, extended with the concepts of SysML, could be a basis for domain-specific architecture modelling language. Even if I&C functions are intended to be independent from their implementation, they are structured in a way that can be easily mapped to the (SW or HW) components<sup>5</sup> of the system. So, it makes sense to say that I&C functions are allocated to one or more I&C systems and their components (e.g. PLC controllers, smart sensors and actuators).

<sup>5</sup> An I&C function can be implemented, for example, as a function block instance or network, as a FPGA circuit or as a traditional hard-wired electronic or relay circuit.

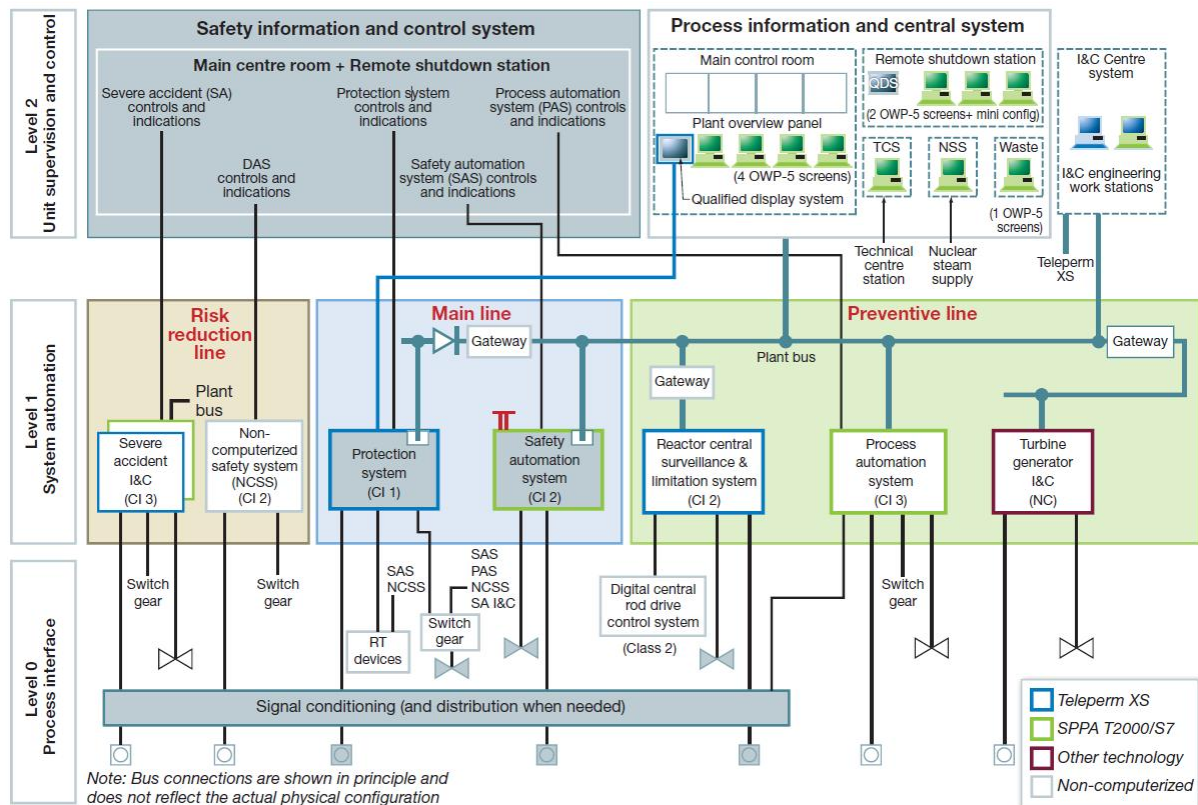


Figure 18. Example of an I&C architecture (Areva 2013).

The physical architecture describes system structure in terms of hardware and software. The hardware architecture would be a description of physical sensors, controllers, actuators and human interface devices, as well as the communication and signal paths connecting them. Figure 18 shows one example focusing on hardware but indicating also other aspects like DiD levels, tasks and control platforms. Support systems such as power supplies and engineering workstations are also part of the picture. Moreover, the hardware architecture should describe the locations of the devices in the operational environment. Relationships to co-located systems, e.g. to air conditioning systems, may be essential. The role of software architecture would be to define the organisation of system and application software and the relations of software elements to I&C functions and hardware resources. Finally, the operational view could be realised as a Concept of Operations (ConOps) describing how the functions and elements of the system and the entities in its environment communicate and collaborate in order to achieve the stated goals of the system (Tommila, Laarni & Savioja 2013).



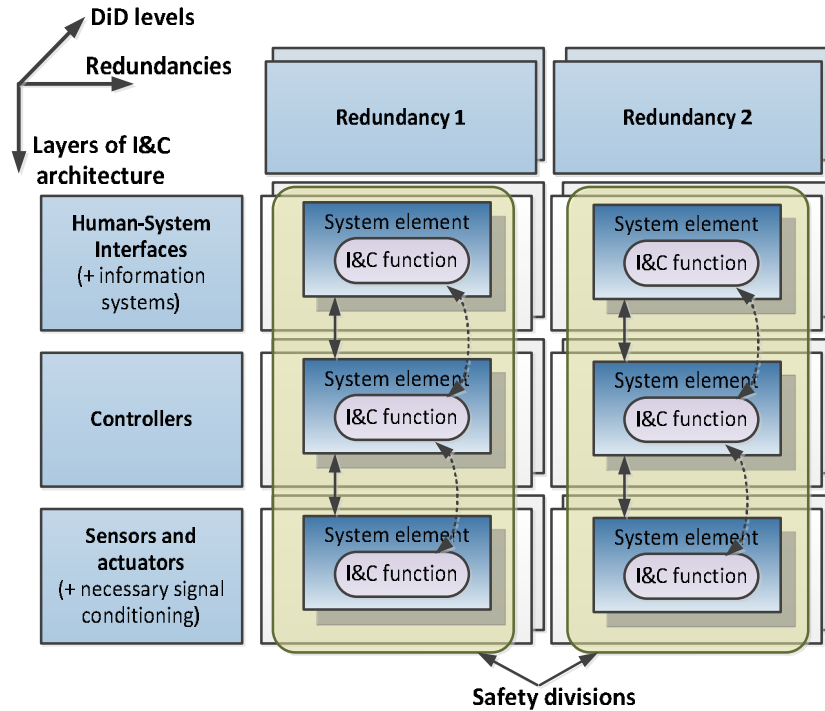


Figure 19. Elements of I&C architecture with the functional architecture shown as a layer on top of the physical architecture.

Figure 19 tries to illustrate the main elements of I&C architecture in three dimensions. Vertically the physical architecture can be organised as layers from field equipment to control room devices. In the horizontal direction the figure shows the “redundancies”, i.e. the redundant parts of the I&C systems in all vertical layers. The third dimension covers the levels of Defence in Depth. As can be seen, I&C system elements are connected by physical communication paths and perform I&C functions that are specified to exchange information using the services of the underlying control platform. In nuclear I&C, safety is a primary concern requiring a dedicated viewpoint, concepts and representations. This safety architecture view highlighting, e.g., hazards, failure modes, fault propagation paths and mitigations, is in the core of DiD. Systems are usually structured as 3 or 4 redundant “trains” each located in its own *safety division*. Physical separation can be implemented between the redundancies, between DiD levels or both (Figure 20).

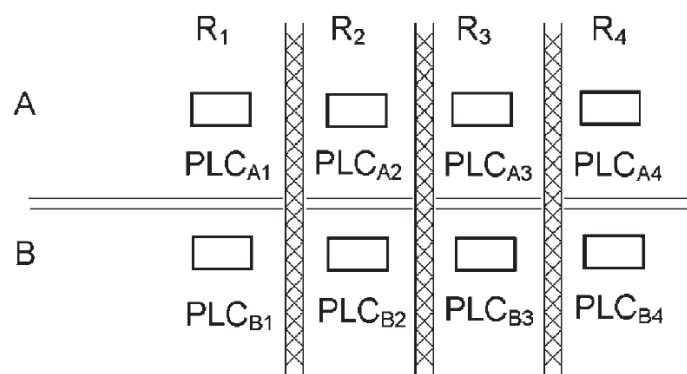


Figure 20. In a physical I&C architecture separation of programmable logic controllers can be applied between DiD levels (A, B) and between redundancies ( $R_1 \dots R_4$ ) (IAEA 2009a).

Figure 21 tries again to summarise the discussion above. A question for further research is, what kind of modelling concepts and representations would be needed to support design and communication of architectural solutions and, in particular, computer-aided analysis of their safety properties, such as physical and functional dependencies and the amount of diversity.

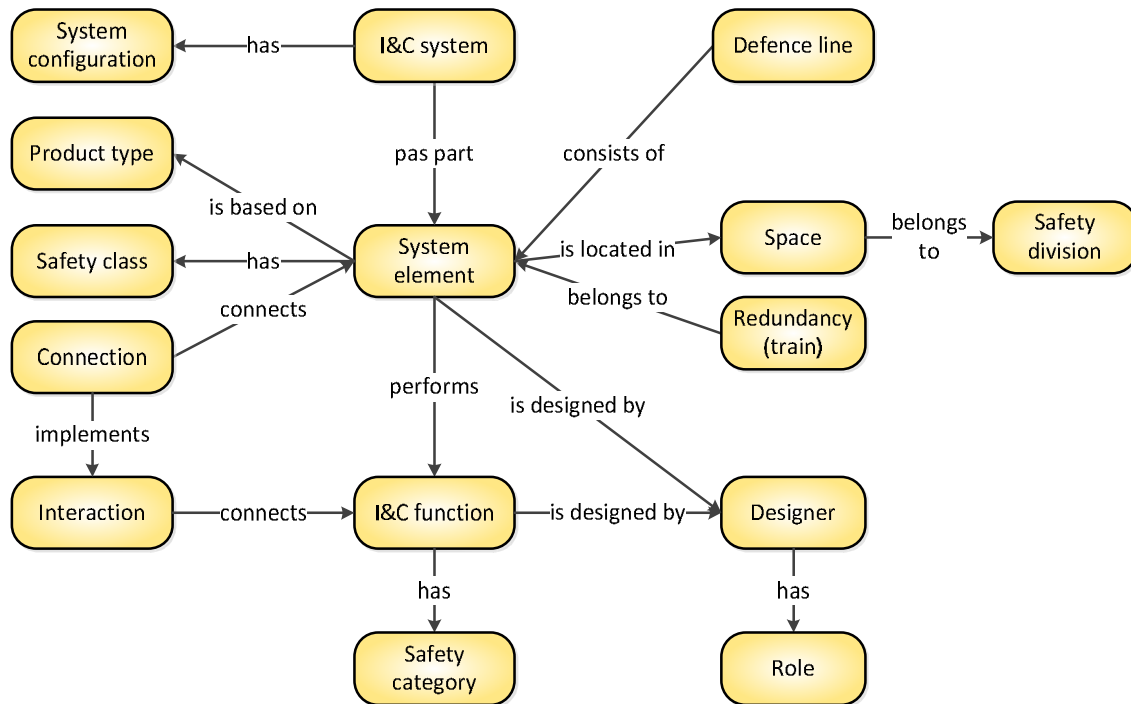


Figure 21. Modelling concepts for I&C architecture.

## 6. Design process

The previous chapters aimed to clarify some terms and modelling concepts that designers use in describing the overall DiD and I&C architectures. The purpose of this chapter is to discuss the design process, first in general and then especially focussing on I&C systems.

As suggested above in Chapter 5, an I&C system architecture can be described in terms of its physical elements (HW & SW), functions and locations. When the term architecture is understood as an overall description, architectures can be found on all levels of decomposition from plant-wide I&C to individual components. In general, design proceeds in an iterative fashion from overall system concepts to detailed solutions. After each iteration (life-cycle phases), solutions are evaluated and decisions made concerning next design steps (milestones). When solutions are corrected and further refined, the amount of design information increases. Figure 22 illustrates the idea as a spiral model. Solution concepts emerge from an analysis of the operational environment and needs and constraints of the stakeholders. During the first life-cycle phase, perhaps only the idea of a new I&C system and its main functions is suggested as a replacement of the existing obsolete instrumentation. Once the existence of a future system is specified, it is possible to define the high-level system requirements. Later on, details of the system context, structure, functions and layout (locations and physical form) are added. The interplay of various “players”, e.g. systems, functions and their human users can be tested and represented in the form of scenarios. As a result, also more detailed requirements are identified<sup>6</sup>.

<sup>6</sup> Note that the figure seems to show requirements and their solutions in an unconventional order. The reason is that it is not possible to express a meaningful requirement without its target being defined at some level (see Tommila & Alanen 2015). The same holds for control system functions. Incoming requirements to a design step actually originate from the previous iteration or from stakeholders’ need and various constraints, such as regulations and existing systems.

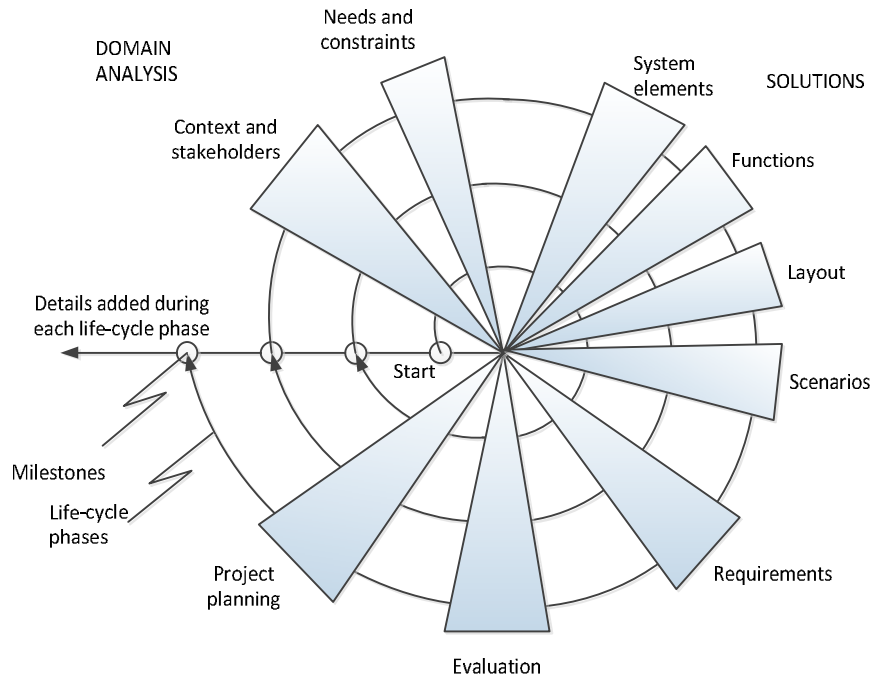


Figure 22. Spiral model of the design process.

In nuclear power, safety design starts from the plant concept and postulated initiating events (PIE) included in the design basis (see Section 4.1). For each identified event, the plant response should be analysed to see the potential consequences and thereby the DBC category of the resulting plant state (see section 4.2). In this way also initiating events can be classified by associating them with the DBC category of the expected plant state. If the initial analysis shows that the PIEs would occur too often or regulatory requirements can't be met, redesign of the plant concept should be considered. Then necessary countermeasures must be engineered for each PIE. To protect the plant against the identified PIEs, additional safety functions must be defined (Figure 23) and allocated to systems, structures and components. The associated DBC, among other things (e.g. safety classes and regulatory requirements), determines many requirements set for those SSCs. In addition to process equipment, this holds for plant engineering. Finding a good and technically feasible plant layout with buildings, spaces, component placement, separation of divisions, etc. is not simple in practice.

	SG <sub>1</sub>	SG <sub>2</sub>	...	SG <sub>j</sub>		
DBE <sub>1</sub>						
DBE <sub>2</sub>						
DBE <sub>j</sub>				{MF1, MF2, MF3, ...}		

Figure 23. Design basis events (DBE) threatening selected safety goals (SG) create the need for mitigating functions (MF). (IAEA 2009a)

We can suppose that there is a plant concept covering, e.g., main process systems (process and nuclear engineering) and architectural design (plant engineering). The iterative design tasks can then be outlined as:

- identification of initiating events
- analysis of the plant response
- estimation of event frequencies
- categorisation of initiating events and scenarios
- definition of required safety functions
- allocation of functions to systems and structures
- definition of I&C architecture
- analysis of dependencies, diversity, failure tolerance, etc.
- safety demonstration.

The new safety guides by IAEA (IAEA 2014a and 2014b) provide more detailed recommendations on the design of instrumentation and control (I&C) and electrical systems. The design of the overall I&C architecture establishes:

- I&C systems that comprise the overall architecture
- allocation of I&C functions to these systems;
- interconnections across the I&C systems and the respective interactions
- design constraints (including prohibited interactions and behaviours)
- definition of the boundaries among the various I&C systems.

The architectural design of individual I&C systems refines the composition-decomposition through all levels of integration down to individual components.

EPRI (2014) recommends more specific principles that can be used to design I&C architectures. Instead of adjusting an existing architecture, the approach is to design the I&C architecture from the beginning as part of the plant's overall DiD concept. In modifications and upgrades, it is important to first understand how the existing levels of defence in depth are supported by the current I&C architecture.

A suggested process for developing and evaluating the I&C architecture is shown in Figure 24. As can be seen, the regulatory requirements and standards are used as a basis for defining application-specific design rules (requirements). In addition, there are inputs and constraints from other engineering disciplines, e.g. from safety analysis and PRA, operations and maintenance and HFE. Functional requirements for I&C systems come primarily from the process designers. In addition, process designers and safety analysts should identify the safety classification of the functions and the level of defence that they support in the plant's overall DiD concept. In the opposite direction, also I&C designers may provide inputs and place constraints on other design areas. The rules and possible exceptions (concerning for example the independence of DiD levels) need to be justified. Moreover, additional criteria used to evaluate alternative architectures are identified covering, for example, reliability, operability, maintainability, licensing risks and cost. (EPRI 2014)

A functional I&C architecture is then defined by assigning I&C functions to different levels of defence and identifying any shared instrumentation and other dependencies. The functional decomposition can be based on the safety goals (e.g. reactivity control, residual heat removal), the design basis events challenging the goals and the necessary mitigating functions. The safety categories of I&C functions are determined and functions assigned to I&C systems within each level of defence. Then system platforms can be selected and

provisions specified for redundancy, diversity and physical separation. From the physical perspective, the architecture can use programmable logic controllers (PLC) in four redundancies that are spatially separated and isolated by barriers. (EPRI 2014, IAEA 2009a)

The characteristics of each system element must be understood for the analysis of the I&C architecture, including for example (IAEA 2009a):

- functions and data, including interactions and timing characteristics (e.g. real-time behaviour and clock synchronization);
- internal architecture, e.g. HW/SW components, platform products and pre-developed components
- functional and physical connections to external systems (including auxiliary systems)
- safety classification
- operational conditions
- failure behaviour and self-diagnostics.

Typically, functions are first assigned to a safety category, and then one can derive the safety class of the systems that implement those functions (EPRI 2014). According to YVL B.2 (2013), only systems are classified into safety Classes 1, 2, and 3 and Class EYT (non-nuclear safety) on the basis of their significance in performing the safety functions of the plant. In addition, systems, structures and components shall be assigned to three seismic categories. In practice, today's digital I&C systems implement many functions and only some of them may be needed to handle an event. So, it is often economically beneficial to classify equipment instead of whole systems.

The specified I&C architecture is assessed according to the attributes established earlier and corrected if necessary. The architecture of the I&C systems and associated information systems and human-system interfaces needs to consider the planned concepts for operating and maintaining the plant, for example the level of automation, staffing levels, degree of centralisation of functions in the main control room versus local stations, and operating crew structure and assignment of responsibilities in normal, abnormal and emergency situations. (EPRI 2014)

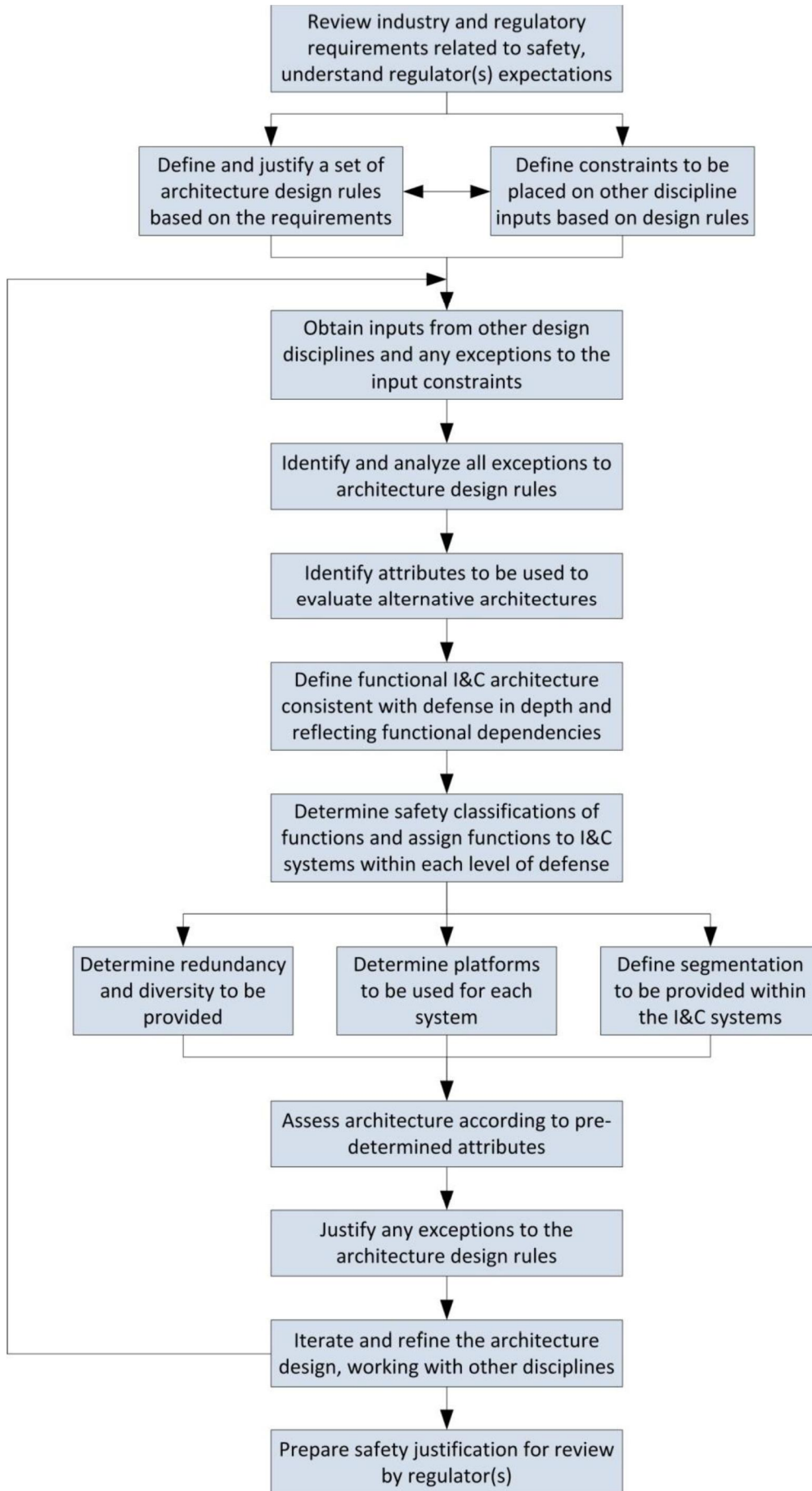


Figure 24. Process for Developing and Evaluating the I&C Architecture (EPRI 2014).

As stated in (YVL B.1 2013 and STUK 2014), failure tolerance analyses, considering all failure modes (including human errors) of one “functional complex” (systems performing safety functions and relevant auxiliary systems) at a time, shall be carried out to demonstrate that when an initiating event occurs

- all systems performing safety functions and their auxiliary systems satisfy the specified failure criteria
- systems assigned to different levels of defence according to the defence in depth approach have been functionally isolated from one another
- a common cause failure in any single component type will not prevent the plant from being brought to a controlled state and further to a safe state.

For example, failure tolerance analysis shall consider the effects of initiating events on devices (components lost in the beginning), common cause failures and propagation of failures due to dependencies between various systems. In failure tolerance/robustness analysis, each of the main systems is seen as a black box and worst case behaviour is assumed. For example, all items in a division are assumed to behave in an unpredictable way in a fire situation. Critical process parameters are identified and then the functions and systems having an effect on these parameters (due to possible actuations). It is then checked that the other systems can handle each of the initiating events in the design basis.

In general, it is expected in nuclear engineering that, if the commonly shared safety principles are adequately applied, nuclear power plants should be very safe (IAEA 2005). However, a documented safety justification is required for confidence in system quality (Common position 2014). Therefore, the information collected during architecture development and assessment is used to prepare a safety justification of the I&C architecture for discussion with the regulator(s) (EPRI 2014).

## 7. Analysis methods and tools

---

Supposing that the I&C architecture has been defined in a structured or even formal way, this chapter discusses the possibilities to analyse its safety properties and vulnerabilities, either manually or with computer tools. Since we are interested in the multi-disciplinary plant-level DiD, we focus here on the overall I&C architecture rather than on the architecture of individual I&C systems.

The I&C architecture should be based on the safety functions that need to be performed, including their safety significance and required reliability. An important issue is the robustness to failure of other systems. Consideration needs to be given also to long-term maintenance of system capabilities. Rigorous definition of the overall system architecture, including assignment of functions to systems and definition of interface and independence requirements, assists with the safety demonstration of the plant I&C (ONR 2011). I&C architecture assessment should consider many safety-related design features, such as:

- defence-in-depth and failure management, including CCF
- safety classifications
- independence between lines of defence, safety classes and redundancies
- provision for automatic and manual safety actuation
- appropriateness of platforms and equipment types.

To be safe in general, plant I&C should implement the correct functions (including both normal and abnormal situations) in a dependable way. So, when assessing an I&C architecture, we can look at the following main safety aspects:

- **Feasibility:** As a starting point, the assessor needs to build sufficient understanding and overall picture of the domain of discourse. As part of this, various characteristics required from a “good” solution can be observed to assess the overall adequacy of the solutions, e.g. in terms of cost, human factors, applied safety principles and implications to other engineering disciplines.
- **Reliability:** Ability of individual I&C systems to perform to their required tasks as specified under given operational conditions assuming that the necessary external resources are provided.
- **Independence:** Avoiding unnecessary and unintended interactions in order to remove hazardous fault propagation paths, e.g. by using functional isolation, diversity and physical separation.
- **Robustness:** Tolerance of external hazards, loss of resources, and misbehaving system elements, including, for example, failure tolerance, abnormal situation management (e.g. alarms and procedures) and resilience in unexpected situations.

As described in Chapter 5, we can make a distinction between several viewpoints to the I&C architecture, in particular the functional and physical architecture, the latter one comprising the physical HW and SW structure and the geographical layout. Combining these two dimensions we end up with the overall assessment landscape outlined in Table 1. More detailed lists of assessment topics and criteria can be found in many standards, regulations and guidelines. A possible topic for further research would be to develop a set of criteria and systematic working methods for assessing the overall I&C architecture.

*Table 1. Examples of assessment topics grouped according to architectural viewpoints and top-level assessment criteria.*

Architecture viewpoints	Aspects			
	Feasibility	Reliability	Independence	Robustness
<b>Functional</b>	ConOps degree of automation states and operating modes alarming concept	self-diagnostics	functional isolation functional/data/ signal diversity	spurious actuations reconfiguration
<b>System structure</b>	long-term support for selected platform(s)	redundancy	electrical isolation electromagnetic interference equipment and software diversity power supplies	equipment dimensioning security
<b>Layout</b>	available space ventilation	accessibility for maintenance and repair	physical separation diversity of physical location	environmental conditions access control

Even if I&C architecture concerns primarily the technical solution, its assessment should consider also relevant life-cycle activities to build confidence in its safety. Therefore, the assessment should cover, as far as practical, the methods, artefacts and resources of the Systems Engineering (SE) and Operations and Maintenance (O&M) activities. For example, the review should consider diversity of development and V&V practices (methods, tools, programming languages) as well as the diversity and independence of participating project organisations.



The assessment of I&C architecture should be carried out in systematic way by an reasonably independent team. IAEA (2011) gives some general ideas for reviewing I&C designs in nuclear power plant. A review team can use five steps to acquire the information needed to develop their observations and recommendations:

1. review of written material and / or presentations
2. discussion and interviews
3. direct observation of programme implementation and the status of the i&c systems
4. discussions among the review team
5. discussion of evaluations/tentative conclusions with developers.

The use of review criteria (e.g. standards and regulations), working practices and assessment techniques should be planned in advance. Formulation of observations and possible recommendations should be based on the identified problems, i.e. *issues*. Multiple cycles of document review, interviews and discussions may be required for clarification and resolution of complex issues and observations. (IAEA 2011)

One objective of analysing a proposed I&C architecture is to find possible weaknesses and to suggest improvements to the developers themselves. In addition, the results of the assessment are important input to the *safety demonstration* and qualification of the plant I&C. Therefore, assessment results must understandable, traceable and unarguable. In addition to the identified issues and conclusions, the selected assessment criteria, working methods and the resources used must be justified. So, the structured safety case approach based on claims, evidence and arguments (Common position 2014, ISO/IEC 15026-2 2011) can be applied also in various safety assessment tasks.

In the rest of this chapter, we represent a few methods that can be used to assess DiD and I&C architectures. Many approaches are today based on manual work and expert judgement. In the future however, Model Based Systems Engineering (MBSE) will become more commonplace also in nuclear power. Structured and even formal system models allow for computer-based design support and analysis, for example complexity measures, simulation and formal model checking. The set of approaches described below is not meant to be exhaustive. It rather contains examples of techniques that seem to give useful inputs to further research in the SAUNA project.

## 7.1 Guidance for Diversity and Defence-in-Depth (D3) analysis

Digital I&C increases the risk of software-related CCF and enhances the need to ensure that the plant has sufficient D3 capabilities. Because of the critical role of DiD, the design principles and architectural solutions must be assessed throughout the system life-cycle, starting as early as possible. And since application of DiD is required by the regulators, the fulfilment of their requirements must be demonstrated in a documented manner. So, there is a need for efficient assessment methods. In our literature review we were able to find a few approaches for evaluating Diversity and Defence in Depth (D3) capabilities. While progress has been made in using probabilistic methods, the approaches are mostly deterministic (IAEA 2005). A couple of examples are described below.

IAEA safety report no. 46 (IAEA 2005) provides guidance primarily for self-assessment by plant operators but it can be used also by regulators and independent assessors. The approach is applicable to all life-cycle phases except decommissioning.

The elements of the approach are illustrated in 68 different objective trees structured as shown in Figure 25. For each safety objective on each DiD level, a set of challenges potentially endangering the safety functions are identified, and the mechanisms leading to the challenges are determined. A broad spectrum (e.g. equipment, procedures, personnel,

safety culture) of possible provisions helping to prevent the mechanisms from occurring is listed in the report. For making an inventory of DiD capabilities one should identify all challenges and mechanisms and then determine whether relevant provisions exist. The IAEA report does not give preference to the provisions, so their adequacy must be determined by the user. The method is deterministic in nature and can also be used without PRA. PRA can, however, be used to justify the adequacy of the DiD architecture and contribution of provisions to risk reduction. The review method was originally tested at two units of one nuclear power plant. It was then considered as a good method for periodic safety review (IAEA 2005). Other indications of its applicability or new versions (e.g. taking into account the Fukushima accident) were, however, not found in our review.

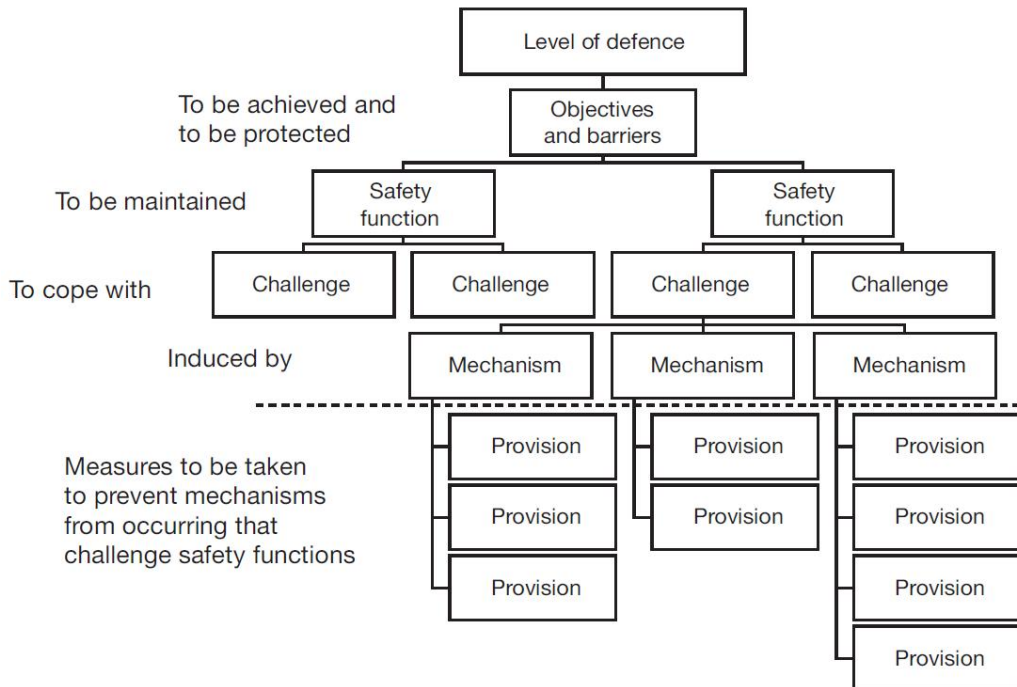


Figure 25. The structure of objective trees (IAEA 2005).

In United States, the Nuclear Regulatory Commission (NRC) has established regulatory guidance for assessing the diversity and defence-in-depth (D3) in an I&C architecture. The guidance is included in Branch Technical Position BTP 7-19, “Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems” (NRC 2012) within Chapter 7, “Instrumentation and Controls” of NUREG-0800. (NUREG/CR 7007 2009)

The applicant shall assess the defence in depth and diversity of the proposed I&C system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed (NRC 2012). The analysis methods are documented in NUREG/CR-6303 (1994). The assessment involves identification of common elements, interdependencies and diversities (NUREG/CR 7007 2009). The purpose of BTP 7-19 is to provide guidance for evaluating an applicant’s D3 assessment and design solutions to ensure that adequate diversity and DiD have been provided and that critical displays and controls are diverse from the digital systems (Figure 26).

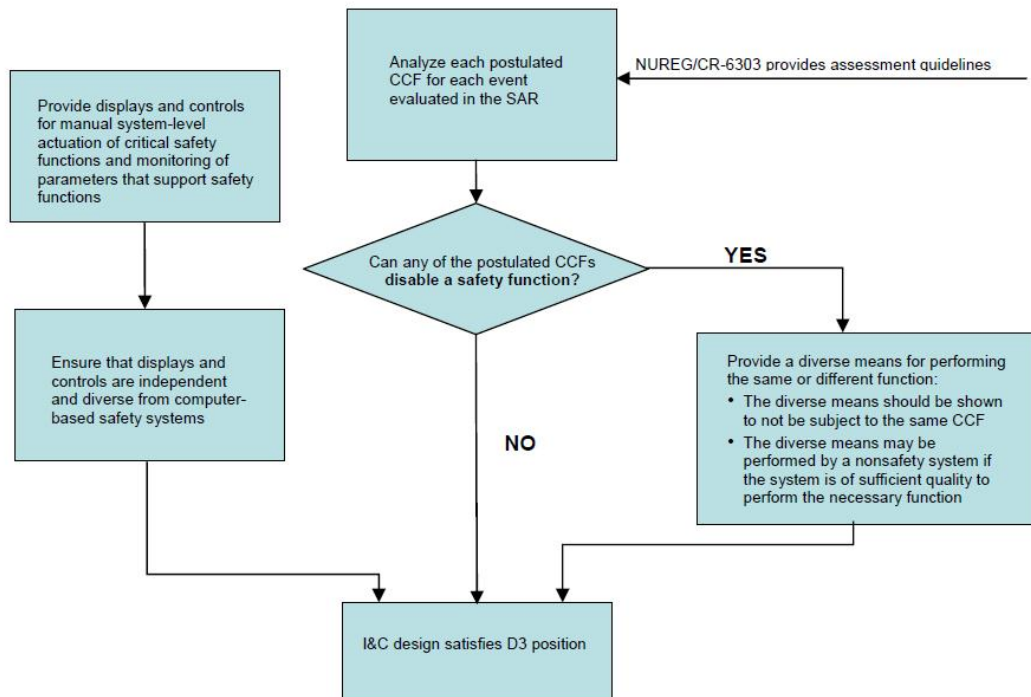


Figure 26. Assessment approach for satisfying D3 regulatory requirements (NUREG/CR 7007 2009).

As a third example of DiD assessment approaches, we take EPRI's technical report 1002835 (EPRI 2004). Its purpose is to shift the focus towards risk-informed methods. The earlier NRC recommendations above have mostly based on deterministic approaches and not considered sufficiently the safety significance of various events and systems. Therefore, the idea of this guide is to extend existing guidelines with risk-informed approaches to digital upgrades. Three alternative methods for D3 evaluation are presented:

- extended deterministic is based on BTP 7-19 but with risk insights applied
- standard risk-informed uses a PRA model modified to reflect the new I&C
- simplified risk-informed uses data from the existing unmodified PRA.

The guide lists sets of defensive measures to be applied in functional specifications, implementation with programmable equipment and use of smart devices. These measures can help designers to avoid and tolerate faults and to cope with unanticipated situations. So, they can also be credited in the D3 evaluations. In addition, such recommended solutions, including the provisions in (IAEA 2005), can be used as criteria in independent D3 assessments.

The use of PRA in analysing the DiD capabilities of digital I&C has been considered by others also, for example (NEA 2015) and (Hellström 2015). Quantitative methods need probability values that are not always available during early stages or for software components. However, EPRI (2004) believes that valuable insights can be obtained by using high-level models and sensitivity analysis. Some common estimates are available for qualified equipment. Estimates can also be adjusted by considering various factors like standard development practices, operational experience and applied defensive measures, including operator's actions. Moreover, the level of diversity and structure of DiD can have a greater impact on the overall risk than the estimated probabilities (EPRI 2004). So, the combination of deterministic and probabilistic methods would be beneficial also in the analysis of overall I&C architectures.

## 7.2 Risk analysis techniques

There are two basic types of safety analysis approaches required in nuclear power: deterministic safety analysis and Probabilistic Safety Analysis (PSA) (IAEA 2009b). Deterministic safety analyses, such as Failure Mode and Effects Analysis (FMEA), are performed to identify hazards, failure modes, plant responses to initiating events and possible accident scenarios. PRA complements the results of deterministic analyses, generally for low-probability and high-consequence events. As part of PRA, Human Reliability Analysis (HRA) is used to quantify human errors. Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) are widely applied in modelling dependencies and scenarios. While usually thought of as PRA tools, FTA and ETA are first used deterministically and then quantified. In addition to estimating accident probabilities, PRA is best suited for determining the safety significance of various plant items and sensitivities of the estimates to input data uncertainties and as a decision support tool for comparing design alternatives.

Single events are the easiest to analyse. For example, in FMEA each failure mode is treated as independent (IEC 60812 2006). So, its ability to analyse CCF is quite limited. Another deficiency of FMEA is its inability to describe interactions and dynamics of a system. Where multiple failures and sequential effects need to be studied, FTA and ETA are more suitable. However, difficulties still arise when several elements of a complex system interact in unintended ways. And this is what is critical in plant-level DiD and I&C architectures, especially in abnormal situations. For example, software has been a challenge to the PRA community. It is not clear, whether a fault tree model adequately captures all dependencies and how software failures should be included in a reliability model (NEA 2015). So, there seems to be a need for methods and tools to analyse interdependencies and to integrate all information in a traceable way. Below we describe two potential approaches, Matrix FMEA and STPA.

In FMEA, the failure effects identified at a lower level may become failure modes at a higher level (IEC 60812 2006). This is the basic idea of “Matrix FMEA” introduced already in the 1970ies. Matrices can be applied also in the horizontal direction. Starting from failure modes of a system, failure effects can be propagated as causes of faults to the neighbouring system. Connected FMEA forms can integrate the analysis results of various engineering disciplines, systems and levels of plant hierarchy. This kind of matrix approach might have a role, for example, in the failure tolerance analysis required by the YVL guides. However, manual FMEA forms would force the analyst to repeat many pieces of text and generate lots of documentation that is difficult to maintain. So, software tools are needed. Figure 27 shows an example, where the basic FMEA elements are maintained in several linked matrices.

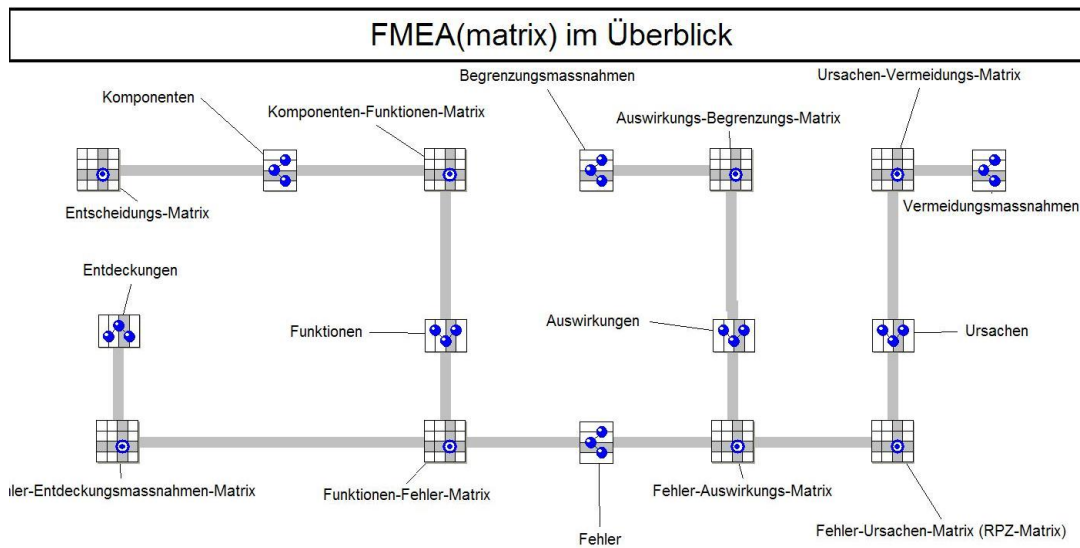


Figure 27. Matrix FMEA links functions, components, failure modes and countermeasures as a network of matrices (<http://www.qfd.de>).

STPA (Systems-Theoretic Process Analysis) is a new hazard analysis technique based on the STAMP (Systems-Theoretic Accident Model and Processes) accident causality model (Leveson 2011). STPA relies on systems thinking rather than on reliability theory. In contrast to traditional techniques, STPA is claimed to be more powerful in identifying causal factors and hazardous scenarios, particularly those related to software, system design and human behaviour (Leveson et al. 2015). Traditional techniques were designed to prevent component failure accidents. STPA addresses also interaction accidents, where no components “fail” but accidents are caused by unsafe interactions and specification errors. A key concept in STAMP is the “safety control structure” (sometimes called the safety management system). Its goal is to enforce safety constraints on various levels from technical systems and organisations to governmental and regulatory practices. Accidents occur when enforcement of the safety constraints fails due to control actions that are, e.g., wrong for the situation, missing, delayed or not obeyed (Figure 28). Quite obviously, hierarchical control structures have something in common with the extended DiD concept in the beginning of Chapter 4. Also the importance of interactions makes STPA a potential candidate for assessing DiD and I&C architectures.

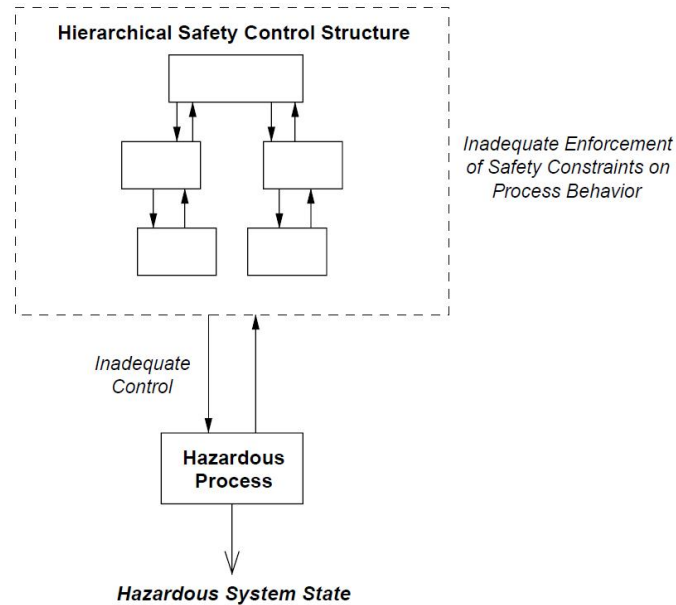


Figure 28. According to the STAMP causality model, accidents occur because of inadequate enforcement of the safety constraints (Leveson et al. 2015).

### 7.3 Functional Failure Identification and Propagation framework (FFIP)

As presented in Chapters 3 and 4, it is necessary to model the interactions between different actors of the sociotechnical system in a holistic manner. Unintended dependencies between NPP systems or between different engineering disciplines can enable failure propagation and circumvent the DiD barriers. For example, if we consider two redundant safety-critical systems, a maintenance person having access to both of them leaves space for human error. Thus, there is a need for multidisciplinary methods for early assessment of system safety, and different system aspects cannot be assessed separately when DiD is concerned. Having a decomposition with two main views of the system, one functional and one with the system components, facilitates the identification of dependencies between safety functions.

The Functional Failure Identification and Propagation (FFIP) framework is a risk assessment method designed to improve the safety of complex systems and can be applied early in the system development process. FFIP method can be used to identify faults which can transverse the automation, electromechanical and structural aspects of the system (Kurtoglu and Tumer 2008; Kurtoglu, Tumer et al. 2010; Tumer and Smidts 2011; Sierla, Tumer et al. 2012).

In FFIP, the functions of the system are described in a functional model and mapped to the physical system components modelled as a Configuration Flow Graph (CFG). Figure 29 gives a simple example with a water tank and a control loop to regulate the water flow. The components in the CFG have behavioural logic and can be simulated. In this case, the CFG has been built with the Apros process simulation software (<http://www.apros.fi/en/>), but also other tools, e.g. Matlab, can be used. The functions in the functional model include Functional Failure Logic that is able to reason the health of the functions based on the simulation results. The granularity and complexity of the functional model depend on the needs of the analysis. The reasoner can run "online" as part of the simulation model, or the functional failure logic is calculated afterwards using the results of the simulation. For example, after a PIE is injected to the simulation, the failure propagation at a functional level can be calculated.

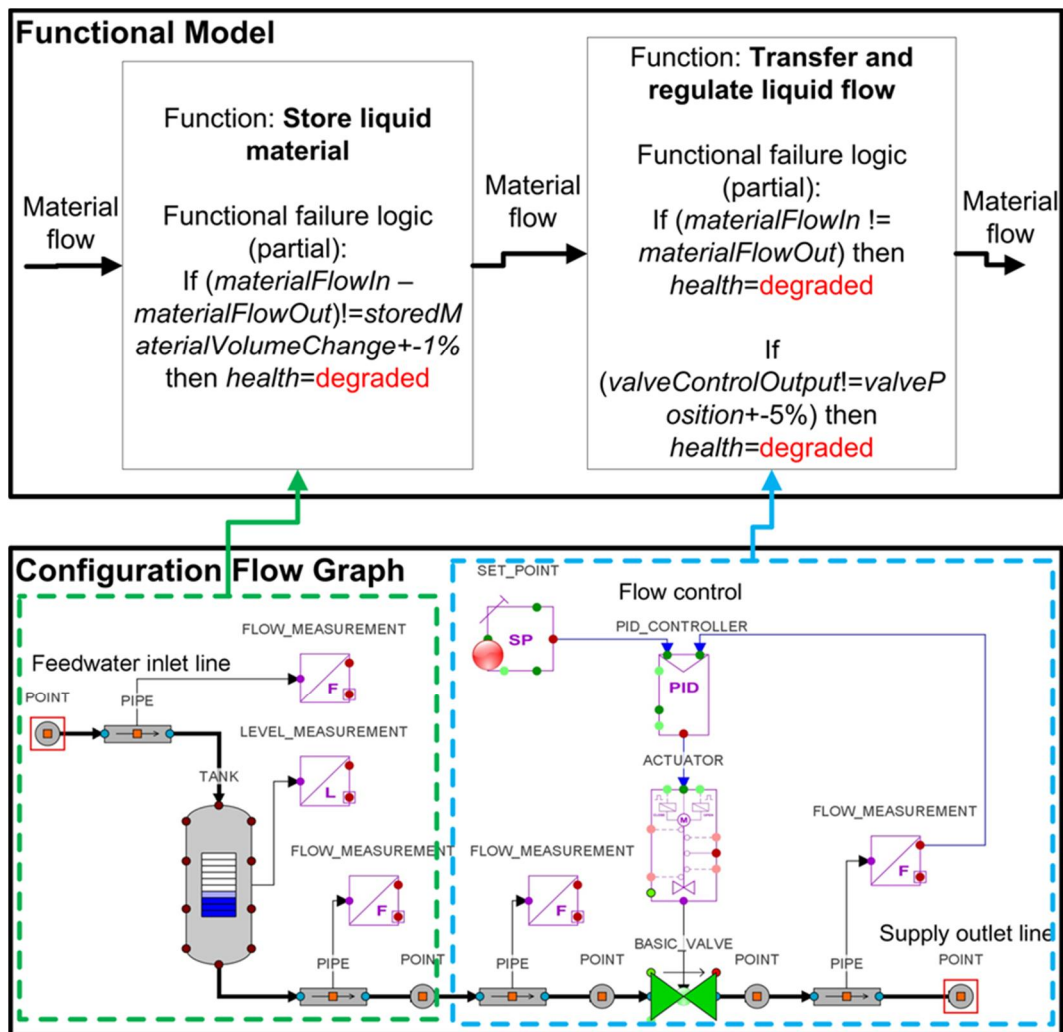


Figure 29. An example of the FFIP framework. The system functions (upper part) are mapped to components of a Configuration Flow Graph (lower part) which can be simulated. The functional failure logic reasons the health of the related function.

One way to use FFIP is to run many scenarios (e.g. using genetic algorithms) and to select the ones with serious consequences for further analysis. Another application is to start from an initiating event and intentionally disable safety functions, for example to generate event trees (below) or to compare different system designs.

The FFIP framework has been extended to support sensitivity analysis of early designs of complex systems (Papakonstantinou, Jensen et al. 2011), safety evaluation of alternative system configurations (Papakonstantinou, Sierla et al. 2012), automatic generation of event trees for critical event scenarios (Papakonstantinou, Sierla et al. 2013) and the compilation of training and testing data sets to be used as inputs for data based quantitative fault detection and identification methods (utilising machine learning – data mining algorithms) (Papakonstantinou, Proper et al. 2014).

To give an example, FFIP has been utilised to automatically generate event trees based on simulation of early system designs (Papakonstantinou, Sierla et al. 2013). In that research the UML metamodel presented in Figure 30 was developed to describe event tree models. The different scenarios were generated by the selective forced failure of safety functions, resulting in event trees with branches for every combination of safety functions working properly or failing to activate.

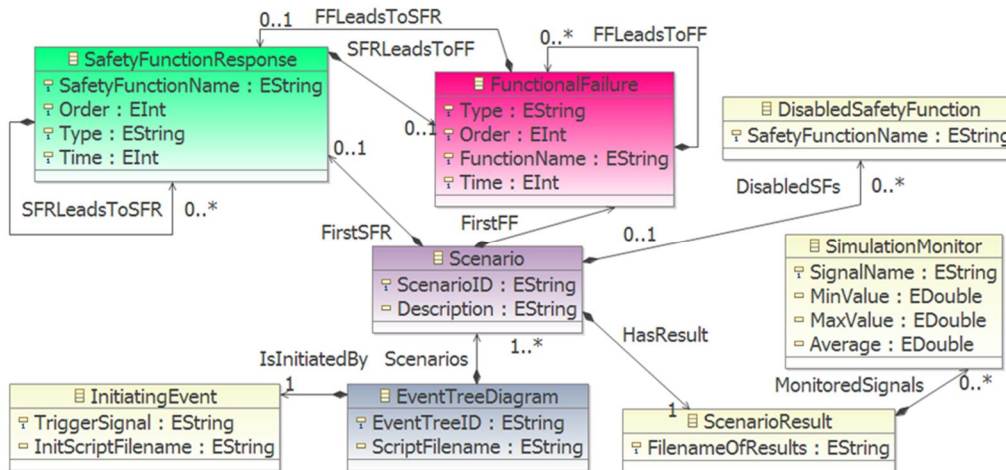


Figure 30. A metamodel of event tree models which include functional failure (Papakonstantinou, Sierla et al. 2013).

There is a clear relation between the components of the CFG of the FFIP method with their mapping to system functions and the system decomposition presented in Section 4.3 (system components related to functions). Since FFIP can be used to identify functional failure propagation for PIEs crossing disciplinary boundaries, its results can be useful for overall DiD safety assessment.

## 7.4 Architecture Description Languages

The elements of nuclear I&C architectures were introduced above in Chapter 5. Here we discuss standards that could be used to build architectural models in formal ways allowing their analysis with computer tools.

The standard ISO/IEC/IEEE 42010 (2011) defines an Architecture Description Language (ADL) as "any form of expression for use in architecture descriptions". With this definition even natural language and symbols in traditional drawings could be considered as an ADL. However, ADLs are usually more structured or even formal, and therefore closely related to Model-Based Systems Engineering (MBSE). In fact, SysML and UML are commonly used for architectural descriptions. The ACME language developed by the Carnegie Mellon University and the Architecture Analysis & Design Language (AADL) by the Society of Automotive Engineers (SAE) are examples of dedicated architecture description languages.

Architecture description languages (ADLs) are used in several disciplines (within information technology), such as systems and software engineering and enterprise modelling. To be useful, the language should:

- be accepted by system developers and analysts,
- support communicating the architecture, looked from various viewpoints, to all relevant parties
- allow for early analysis and validation of architectural decisions
- provide sufficient information for implementation and support for automatic generation of more detailed specifications or software.

Today's ADLs have typically a graphical and textual form with formal syntax and semantics for representing hierarchical levels of system structure and functions. There are differences in their purpose and ability to incorporate design knowledge, behaviour and timing issues, as well as in available tool support.



To give an example, ACME is a small and simple language (<http://www.cs.cmu.edu/~acme/>). Its key concepts are system, component, connector and port. A system is constituted by components connected by connectors (Figure 31). The Acme project began already in 1995. Currently, the ACME language and tools provide a generic, extensible infrastructure for developing and analysing software architecture descriptions.

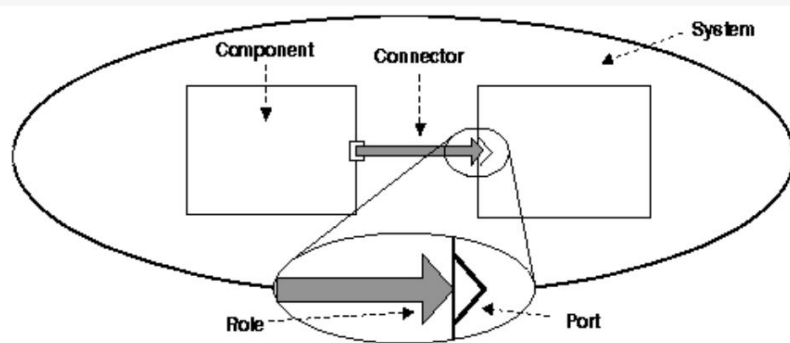


Figure 31. Basic ACME model constructs (<http://www.di.univaq.it/malavolta/al/>).

The Architecture Analysis & Design Language (AADL) is an example of a large and complete language. Version 2.1 of the standard was published by the Society of Automotive Engineers (SAE) in 2012. AADL is supported by multiple tools, both open-source and commercial. An AADL specification can be expressed textually and graphically, or as Extensible Markup Language (XML) (Feiler, Gluch & Hudak 2006).

AADL is intended for the design of both hardware and software of a system. Systems are modelled as hierarchical collections of interacting application components (processes, threads, subprograms, events, data) and a set of platform components (processors, memory, buses, devices). The AADL standard defines runtime semantics, including, for example, message and events, synchronised access to shared components, thread scheduling and timing requirements. In addition, dynamic reconfiguration of runtime architectures can be specified using operational modes and mode transitions. The core language can be extended with new properties and modelling elements. For example, the Error Model Annex published by SAE complements the core language with dependability modelling, including, for example, error models (Figure 32), fault and repair assumptions, fault-tolerance mechanisms and stochastic parameters. In this way, the AADL architectural model can be used for various analyses, e.g. dependability analysis, formal verification, scheduling and analysis of deadlocks. These characteristics make AADL suitable for model-based specification and analysis of safety-critical real-time embedded systems. (Feiler, Gluch & Hudak 2006, Rugina et al. 2008)

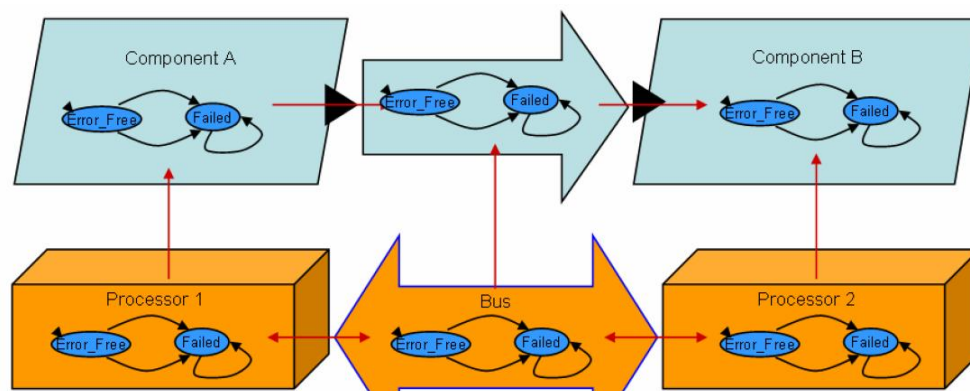


Figure 32. Fault propagation between error models based on application component interactions and execution platform bindings (Feiler & Rugina 2007).

The short overview above indicates that Architecture Description Languages like SysML, ACME and AADL might have applications also in nuclear I&C. A formal description would allow us to evaluate the correctness of the I&C architecture at a high level of abstraction early during the development process. In the context of DiD, the interesting questions would be, for example the diversity and independence of DiD levels, defence lines and redundant systems in various safety classes. For overall safety, the architectural models should cover several disciplines as suggested in Chapter 5. Computer tools could, for example, help designers in identifying unintended dependencies and exceptional fault propagation paths and in checking that the design satisfies certain (regulatory) requirements. Executable models and simulation, such as FFIP in the previous section, are one option. In addition, rule-based reasoning on the model elements, their connections and properties can give answer to several questions. For example, PLC devices connected with an Ethernet cable or located in the same room are not fully independent. Clearly there is the need to adapt existing ADL standards and tools to the practices, terminology and tools of the nuclear domain. So, analysis tools should be integrated to existing design environments in a way that allows access to design data and automatic generation of the analysis models and associated requirements.

## 8. Summary and conclusions

---

In this report we have discussed the terminology and reviewed some literature related to the design and analysis of overall Defence in Depth (DiD) and I&C architectures. The purpose has been to collect ideas for further research towards model-based and tool-supported systems engineering.

In our understanding, DiD continues to be a major design principle for nuclear power plants. There is, however, a debate going on its scope and interpretations concerning, for example, human and organisational factors and extreme conditions. DiD is accepted as an abstract idea that can be implemented in many ways. So, the concrete challenge is to find good technical solutions and practices for their development and assessment. Unfortunately, many of the terms related to DiD, system properties (e.g. physical separation, functional isolation and diversity) and failure behaviour (fault, failure, etc.) seem to be defined in rather vague ways. Different standards and guidelines give often different and sometimes even contradictory definitions. This situation does not provide a very good basis for model-based engineering and design automation.

On the basis of these observations, the following seem to be potential topics for further research in the SAUNA project:

- Further development of modelling concepts and taxonomies related to DiD and I&C architecture including, for example, functions, physical system elements, geographical layout, classifications and failure modes. The foreseen result would be a clarified terminology and a structured information model to be used as basis for systematic design and assessment practices and, in particular, development of software tools.
- Refinement of a systems engineering process for developing a plant-level I&C architecture starting from process engineering and safety requirements and taking into account also the interfaces to other engineering disciplines. In particular, the Concept of Operations (ConOps) could be the tool for interfacing with human factors engineering and end-users.
- Criteria and review methods for assessing DiD and I&C architectures as part of the licensing and qualification processes. Following the idea of structured safety demonstrations, relevant regulatory requirements can be interpreted and rephrased

as a pool of claims and combined into a hierarchical argument structure according to the properties of the particular application. Various review and analysis methods can then be recommended as ways to collect the necessary evidence for or against the selected claims.

- Structured multidisciplinary I&C models and analysis algorithms. Due to the complexity of plant I&C and its links to other disciplines, computer tools are needed for identifying unexpected behaviours and fault propagation paths. A description of the I&C architecture should preferably be automatically generated from design data and support better integration of the I&C models with the safety functions and safety analysis of the plant. Structured cross-disciplinary models would allow the use of simulation and reasoning algorithms for analysing critical safety properties of the solution at early stages of development.

The work presented in this research report will focus in 2016 on the first and last topic above with the aim to develop model-based safety assessment methodologies for Defence in Depth and I&C architectures. In fact, also many other elements of the suggested topics are present in various tasks of the SAUNA project plan. In addition, there are links to other projects in the SAFIR 2018 programme. Therefore, taking advantage of the existing synergies would be highly beneficial.

## References

---

- Areva 2013. The UK EPR digital I&C system. Nuclear Engineering International, April 2013. Available at: [www.neimagazine.com/features/featurethe-uk-eprtm-digital-ic-system/](http://www.neimagazine.com/features/featurethe-uk-eprtm-digital-ic-system/).
- Avizienis, A., Laprie, J-C., Randell, B. & Landwehr, C. 2004. Basic Concepts and Taxonomy of Dependable and Secure Computing. University of Maryland, Institute for Systems Research, technical report TR 2004-47, 37 p.
- Bäckström, O., Holmberg, J.-E., Jockenhövel-Barttfeld, M., Porthin, M., Taurines, A. & Tyrväinen, T. 2015. Software reliability analysis for PSA: failure mode and data analysis. Nordic nuclear safety research (NKS), report NKS-341, 85 p.
- Common position 2014. Licensing of safety critical software for nuclear reactors - Common position of seven European nuclear regulators and authorised technical support organisations.
- EPRI 2004. Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital I&C Upgrades – Applying Risk Informed and Deterministic Methods. Electric Power Research Institute, Inc. (EPRI), technical report 1002835, 96 p.
- EPRI 2014. Principles and Approaches for Developing Overall Instrumentation and Control Architectures that Support Acceptance in Multiple International Regulatory Environments. Electric Power Research Institute, Inc. (EPRI), technical report 3002002953, 366 p.
- EUR 2012. European utility requirements for LWR nuclear power plants - Volume 1, Main policies and objectives - Appendix B, Definitions.
- Feiler, P., Gluch, D. & Hudak, J. 2006. The Architecture Analysis & Design Language (AADL): An Introduction. Carnegie Mellon University, technical note CMU/SEI-2006-TN-011, 144 p.

- Feiler, P. & Rugina, A. 2007. Dependability Modeling with the Architecture Analysis & Design Language (AADL). Carnegie Mellon University, technical note CMU/SEI-2007-TN-043, 86 p.
- Haapanen, P. & Helminen, A. 2002. Failure mode and effects analysis of software-based automation systems. STUK-YTO-TR 190. Helsinki 2002. 35 p + Appendices 2 p.
- Hellström, P. 2015. DID-PSA: Development of a Framework for Evaluation of the Defence-in-Depth with PSA. Swedish Radiation Safety Authority (SSM), report 2015:04, 96 p., available at: <http://www.stralsakerhetsmyndigheten.se/>.
- Hollnagel, E. 2011. Prologue: The Scope of Resilience engineering. In: Hollnagel, E., Paries, J., Woods, D. and Wreathall, J., (Eds.) 2011. Resilience engineering in practice: a guidebook. Farnham, Ashgate.
- IAEA 1993. Defining initiating events for purposes of probabilistic safety assessment. IAEA-TECDOC-719, 152 p.
- IAEA 1996. Defence in depth in nuclear safety (INSAG-10). International Safety Advisory Group (INSAG), 48 p., available at [http://www-pub.iaea.org/MTCD/publications/PDF/Pub1013e\\_web.pdf](http://www-pub.iaea.org/MTCD/publications/PDF/Pub1013e_web.pdf).
- IAEA 2005. Assessment of Defence in Depth for Nuclear Power Plants. IAEA Safety Reports Series no. 46.
- IAEA 2007. IAEA safety glossary – Terminology used in nuclear safety and radiation protection 2007 edition, 238 p.
- IAEA 2009a. Protecting against common cause failures in digital I&C systems of nuclear power plants. IAEA Nuclear Energy Series No. NP-T-1.5, 65 p.
- IAEA 2009b. Deterministic Safety Analysis for Nuclear Power Plants. Vienna, International Atomic Energy Agency (IAEA), Specific Safety Guide no. SSG-2, 84 p.
- IAEA 2011. Preparing and Conducting Review Missions of Instrumentation and Control Systems in Nuclear Power Plants. Vienna, International Atomic Energy Agency (IAEA), IAEA-TECDOC-1662, 89 p.
- IAEA 2014a. Design of Instrumentation and Control Systems for Nuclear Power Plants. International Atomic Energy Agency (IAEA), draft safety guide DS431, 133 p.
- IAEA 2014b. Design of Electrical Power Systems for Nuclear Power Plants. International Atomic Energy Agency (IAEA), draft safety guide DS430, 95 p.
- IEC 60050-192 2015. International electrotechnical vocabulary - Part 192: Dependability. Geneva, International Electrotechnical Commission (IEC), 239 p., definitions available at: <http://www.electropedia.org/>.
- IEC 60880 2006. Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions. Geneva, International Electrotechnical Commission (IEC), 218 p.
- IEC 60812 2006. Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA), edition 2.0. Geneva, International Electrotechnical Commission (IEC), 98 p.

- IEC 61508-4 2010. Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations. Geneva, International Electrotechnical Commission (IEC), 68 p.
- IEC 61508-6 2010. Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3. Geneva, International Electrotechnical Commission (IEC), 237 p.
- IEC 61512-1 1997. Batch control - Part 1: Models and terminology. Geneva, International Electrotechnical Commission (IEC), 177 p.
- IEC 61513 2011. Nuclear power plants - Instrumentation and control important to safety - General requirements for systems, 98 p.
- INCOSE 2015. Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities, version 4.0. Hoboken, NJ, USA: John Wiley and Sons, Inc.
- INL 2015. Initiating Event Rates at U.S. Nuclear Power Plants 1988–2013. Idaho National Laboratory, report INL/EXT-14-31428, Revision 1, 23 p.
- ISO/IEC 15026-2 2011. Systems and Software Engineering — Systems and Software Assurance — Part 2: Assurance Case. 10 p.
- ISO/IEC/IEEE 15288 2015. Systems and software engineering – System life cycle processes. 108 p.
- ISO/IEC/IEEE 42010 2011. Systems and software engineering — Architecture description. 37 p.
- Kadambi, N. 2013. Defence in depth in nuclear safety. Nuclear Engineering International, 30 January 2013. Available at <http://www.neimagazine.com/features/featuredefence-in-depth/>.
- Kurtoglu, T. and Tumer, I. 2008. A Graph-Based Fault Identification and Propagation Framework for Functional Design of Complex Systems. Journal of Mechanical Design 130(5).
- Kurtoglu, T., Tumer, I. et al. 2010. A functional failure reasoning methodology for evaluation of conceptual system architectures. Research in Engineering Design 21: 209-234.
- Leveson, N. 2011. Engineering a Safer World – Systems Thinking Applied to Safety. MIT Press, Cambridge.
- Leveson, N. et al. 2015. An STPA Primer, version 1, August 2013 (updated June 2015). 91 p.
- Li, B., Li, M., Chen, K. & Smidts, C. 2006. Integrating Software into PRA: A Software-Related Failure Mode Taxonomy. Risk Analysis, Vol. 26, No. 4, 2006, 16 p.
- Lind, M. 2005. Modeling Goals and Functions of Control and Safety Systems – theoretical foundations and extensions of MFM. Nordic nuclear safety research, report NKS-114, 45 p.
- Malavolta, I., Lago, P., Muccini, H., Pelliccione, P. & Tang, A. 2013. What Industry Needs from Architectural Languages: A Survey. IEEE Transactions on software engineering, vol. 39, no. 6, June 2013.

- NEA 2015. Failure Modes Taxonomy for Reliability Assessment of Digital Instrumentation and Control Systems for Probabilistic Risk Analysis. The OECD Nuclear Energy Agency (NEA), Committee on the Safety of Nuclear Installations (CSNI). NEA/CSNI/R(2014)16, 135 p.
- NRC 2012. Guidance for evaluation of diversity and defense-in-depth in digital computer-based instrumentation and control systems – review responsibilities. U.S. Nuclear Regulatory Commission, branch technical position 7-19, 28 p.
- NUGENIA 2013. NUGENIA Roadmap (2013). Nuclear GENERation II & III Association (NUGENIA, <http://nugenia.org>), 56 p.
- NUREG/CR-6303 1994. Method for performing diversity and defense-in-depth analyses of reactor protection systems. U.S. Nuclear Regulatory Commission, 52 p.
- NUREG/CR 7007 2009. Diversity strategies for nuclear power plant instrumentation and control systems. U.S. Nuclear Regulatory Commission, 251 p.
- O'Halloran, B., Stone, R. & Tumer, I. 2012. A Failure Modes and Mechanisms Naming Taxonomy. IEEE, proceedings of the Annual Reliability and Maintainability Symposium (RAMS), 23-26 Jan. 2012, 6 p.
- ONR 2011. Generic Design Assessment – New Civil Reactor Build - Step 4 Control and Instrumentation Assessment of the EDF and AREVA UK EPRTM Reactor. Office for Nuclear Regulation (ONR), assessment report: ONR-GDA-AR-11-022, 182 p.
- Papakonstantinou, N., Jensen, D. et al. 2011. Capturing interactions and emergent failure behavior in complex engineered systems and multiple scales. ASME IDETC/CIE. Washington, DC, USA.
- Papakonstantinou, N., Proper, S. et al. 2014. Simulation Based Machine Learning For Fault Detection In Complex Systems Using The Functional Failure Identification And Propagation Framework. ASME CIE. Buffalo NY, USA.
- Papakonstantinou, N., Sierla, S. et al. 2012. Using Fault Propagation Analyses for Early Elimination of Unreliable Design Alternatives of Complex Cyber-Physical Systems. ASME IDETC/CIE 2012. Chicago, Illinois, USA.
- Papakonstantinou, N., Sierla, S. et al. 2013. A Simulation Based Approach to Automate Event Tree Generation for Early Complex System Designs. ASME IDETC/CIE 2013. Portland, Oregon, USA.
- Randell, B. 2003. On Failures and Faults. In: Araki, K., Gnesi, S. & Mandrioli, D. (Eds.): Proceedings of the International Symposium of Formal Methods Europe (FME 2003), Pisa, Italy, September 8-14, 2003. Berlin Heidelberg, Springer-Verlag, LNCS 2805, pp. 18–39.
- Rugina, A., Feiler, P., Kanoun, K. & Kaâniche, M. 2008. Software Dependability Modeling Using An Industry-Standard Architecture Description Language. Proceedings of the 4th International Congress on Embedded Real-Time Systems, 10 p.
- Sierla, S., Tumer, I. et al. 2012. Early integration of safety to the mechatronic system design process by the functional failure identification and propagation framework. *Mechatronics* 22(2): 137-151.
- Sierla, S., O'Halloran, B. M., Karhela, T., Papakonstantinou, N. & Tumer, I. Y. 2013. Common cause failure analysis of cyber–physical systems situated in constructed environments. *Research in Engineering Design* 24(4): 375-394.

- SNETP 2013. Identification of Research Areas in Response to the Fukushima Accident. Sustainable Nuclear Energy Technology Platform, <http://www.snetp.eu>, 48 p.
- STUK 2014. Justification memorandum 27.01.2014, YVL B.1, Safety design of a nuclear power plant (in Finnish), 34 p.
- Tommila, T., Laarni, J. & Savioja, P. 2013. Concept of operations (ConOps) in the design of nuclear power plant instrumentation & control systems. VTT, working report of the SAREMAN project, version 2, 68 p.
- Tommila, T. & Alanen J. 2015. Conceptual model for safety requirements specification and management in nuclear power plants. VTT Technology 238, 120 p. + app. 26 p. Available at: <http://www.vtt.fi/inf/pdf/technology/2015/T238.pdf>.
- Torry-Smith, J., Mortensen, N. & Achiche, S. 2014. A proposal for a classification of product related dependencies in development of mechatronic products. Res Eng Design (2014) 25:53–74.
- Tumer, I. Y. and Smidts, C. S. 2011. Integrated Design and Analysis of Software-Driven Hardware Systems. IEEE Transactions on Computers 60(8): 1072-1084.
- Uder, S., Stone, R. & Tumer, I. 2004. Failure analysis in subsystem design for space missions. Proceedings of DETC '04 2004 ASME Design Engineering Technical Conferences and Computers and Information in Engineering Conference September 28 – October 2, 2004, Salt Lake City, Utah, 17 p.
- WENRA 2013. Safety of new NPP designs - Study by Reactor Harmonization Working Group RHWG. March 2013. 52 p.
- Weightman, M. 2013. Fukushima – A Failure of Institutional Defence in Depth. International Conference on Topical Issues in Nuclear Installation Safety: Defence in Depth, 21-24 October 2013, Vienna. Presentation slides, available at <http://www-pub.iaea.org/iaeameetings/cn205p/Wednesday/Weightman.pdf>.
- YVL A.1 2013. Regulatory oversight of safety in the use of nuclear energy. 22 November 2013, 43 p.
- YVL B.1 2013. Safety design of a nuclear power plant. 15 November 2013, 46 p.
- YVL B.2 2013. Classification of systems, structures and components of a nuclear facility. 15 November 2013, 9 p.

## Appendix A: Acronyms and abbreviations

---

ADL	Architecture Description Language
AOO	Anticipated Operational Occurrence
CCF	Common Cause Failure
ConOps	Concept of Operations
D3	Diversity and Defence-in-Depth
DBC	Design Basis Condition
DBC	Design Basis Category
DEC	Design Extension Condition
DiD	Defence in Depth
FMEA	Failure Mode and Effects Analysis
FTA	Fault Tree Analysis
HFE	Human Factors Engineering
I&C	Instrumentation and Control
IEC	International Electrotechnical Commission
IAEA	International Atomic Energy Agency
NEA	Nuclear Energy Agency
MBSE	Model Based Systems Engineering
NRC	U.S. Nuclear Regulatory Commission
OECD	Organisation for Economic Co-operation and Development
OLC	Operational Limits and Conditions (previously Technical Specifications)
PIE	Postulated Initiating Event
PLC	Programmable Logic Controller
PRA	Probabilistic Risk Analysis
PSA	Probabilistic Safety Analysis
SE	Systems Engineering
SSC	Systems, Structures and Components
STUK	Säteilyturvakeskus, Radiation and Nuclear Safety Authority
V&V	Verification and Validation



## Appendix B: Glossary

---

This appendix contains in alphabetical order definitions of the most important terms used in this report. The definitions have been adopted from relevant standards and guidelines whenever appropriate. Some of them have, however, been given a new meaning consistent with our approach (see Tommila & Alanen 2015).

For interested readers it is probably worthwhile to know about these freely available collections of definitions:

- Software and Systems Engineering Vocabulary (SEVOCAB): <http://pascal.computer.org>
- IEC's Online Electrotechnical Vocabulary (Electropedia): <http://www.electropedia.org>
- Definitions used in the YVL guides: <https://ohjeisto.stuk.fi/YVL/YVL-maaritelmat.xls>

**Accident** (onnettomuus): Includes *postulated accidents*, *design extension conditions* and *severe accidents* (YVL B.1 2013).

**Active failure** (aktiivinen vikaantuminen): A *failure* that causes a system to carry out spontaneous actions ("active malfunction") without a demand.

**Anticipated operational occurrence** (odotettavissa oleva käyttöhäiriö): A deviation from normal operation that can be expected to occur once or several times during any period of a hundred operating years (YVL B.1 2013).

**Barrier**: A physical obstruction that prevents or inhibits the movement of people, radionuclides or some other phenomenon (e.g. fire), or provides shielding against radiation (IAEA 2007).

**Common Cause Failure** (yhteisvika): A failure of two or more structures, systems and components due to the same single event or cause (YVL B.1 2013).

**Concept of Operations** (toimintakonsepti): An overall specification describing how the functions and elements (technical and human) of a system and the entities in its environment communicate and collaborate in order to achieve the stated goals of the system (modified from Tommila, Laarni & Savioja 2013).

**Defence line, line of defence** (puolustuslinja): Set of plant items (systems, structures, etc.) to protect people and environment against radiation. *Physical defence lines* refer to the barriers between active material and environment, i.e. to fuel matrix, fuel cladding, primary circuit boundary and the containment. *Functional defence lines* consist of systems (e.g. I&C and process systems, procedures and people) controlling the plant with the purpose to protect the physical barriers and to transfer the plant to a controlled and safe state. Each defence line is dedicated for certain plant conditions (DBC, DEC, SA). For example, the functional defence lines might include:

- normal process control and preventive limitation systems
- reactor protection system and engineered safety features
- diverse actuation system
- severe accident management system.

**Defence in Depth level** (puolustustaso): Group of plant *functions* and *systems* intended to control the plant in a kind of situation ranging from normal operation to severe accidents.

- Level 1: prevention of abnormal situations during normal plant operation
- Level 2: Control of abnormal situations
- Level 3: Control of accidents
- Level 4: Control of core melt accidents
- Level 5: Mitigation of consequences of significant releases of radioactive material

**Design Basis Condition:** A situation for which the plant has been designed.

**Design Basis Category** (suunnitteluperusteluokka): A class of *Design Basis Condition* defined according to the expected frequency and severity of the situation. Each DBC category is associated with a specific DiD level:

- DBC 1: Normal operation (level 1)
- DBC 2: Anticipated Operational Occurrence (level 2)
- DBC 3: Postulated accident, class 1 (level 3a)
- DBC 4: Postulated accident, class 2 (level 3a)

**Design Extension Condition** (oletetun onnettomuuden laajennus): A specific set of accident situations that goes beyond DBCs. In YVL B.1 (2013) DEC has three subclasses:

- DEC A: accident where an anticipated operational occurrence or class 1 postulated accident involves a common cause failure in a system required to execute a safety function
- DEC B: accident caused by a combination of failures identified as significant on the basis of a probabilistic risk assessment
- DEC C: accident caused by a rare external event and which the facility is required to withstand without severe fuel failure (DEC C).

**Diversity** (erilaisuus): Backing up of functions through systems or components having different operating principles or differing from each other in some other manner, with all systems or components able to implement a function separately (YVL B.1 2013).

**Electrical isolation** (sähköinen erottelu): Subtype of *physical separation* used to prevent unwanted electrical phenomena, e.g. voltage transients, electro-magnetic fields and electrostatic discharges, in one system from affecting connected systems. Examples of provisions for electrical isolation include absence of electronic connections, optical isolation and use of separation by distance or electrical insulators (modified from IAEA 2014a).

**Failure** (vikaantuminen): An event that results in a fault of a system element and consequently loss of its ability to perform as required (adapted from IEC 60050-192 2015).

**Failure criterion** (vikakriteeri): A requirement on system behaviour in failure situations<sup>7</sup>. YVL B.1 (2013) defines two important failure criteria:

- N+1: it must be possible to perform a safety function even if any single component designed for the function fails.
- N+2: it must be possible to perform a safety function even if any single component designed for the function fails and any other component or part of a redundant

---

<sup>7</sup> IEC 60050-192 (2015) gives a different definition as a pre-defined condition for acceptance as conclusive evidence of failure, e.g. a limit beyond which it is deemed to be unsafe to continue operation.

system – or a component of an auxiliary system necessary for its operation – is simultaneously out of operation due to repair or maintenance.

**Failure mode** (vikaantumistapa): Manner in which a *malfunction* occurs (modified from IEC 60050-192 2015<sup>8</sup>).

**Function** (toiminto): A capability of a *system* to generate one or more intended behaviours of the system and/or effects on the system environment (Tommila & Alanen 2015). A function, e.g. a specification of a start-up sequence, is an abstract concept used only in the system model. In the real-world system, functions are implemented in the form of devices and software components.

**Fault** (vika): Internal state (e.g. defect or design error) of system element causing its inability to perform one or more of its intended *functions* (adapted from IEC 60050-192 2015).

**Functional isolation** (toiminnallinen erottelu): Isolation of system *functions* from one another so that the (normal or abnormal) behaviour of one function does not adversely affect another function. Functional isolation can be achieved, for example, by avoiding exchange of information (and electrical power) between systems. (modified from YVL B.1 2013)

**I&C architecture** (automaatioarkkitehtuuri): Organisational structure of the *I&C systems* of the plant (modified from IEC 61513 2011).

**I&C function** (automaatio toiminto): *Function* to control, operate and/or monitor a defined part of the process (IEC 61513 2011).

**I&C system** (automaatiojärjestelmä): *System*, based on electrical and/or electronic and/or programmable electronic technology, performing I&C functions as well as service and monitoring functions related to the operation of the system itself (IEC 61513 2011).

**Issue**: An identified concern or an area for improvement, which has been identified during the assessment of a system (modified from IAEA 2011).

**Malfunction** (virhetoiminta): Unintended (unwanted) externally observable misbehaviour of a system.

**Operational Limits and Conditions** (turvallisuustekniset käyttöehdot): The technical and administrative requirements for ensuring the plant's operation in compliance with the design bases and safety analyses; the requirements for ensuring the operability of systems, structures and components important to safety; and the limitations that must be observed in the event of component failure (YVL A.1 2013).

**Passive failure** (passiivinen vikaantuminen): A *failure* causing a system *function* to be unavailable and degraded on demand (passive malfunction).

**Physical separation** (fyysinen erottely): Separation of systems, structures and components (SSC) from one another by *barriers* (e.g. distance, structure or device) that prevent propagation of physical phenomenon that may be harmful to physical parts or operation of other SSCs.

**Postulated accident** (oletettu onnettomuus): A deviation from normal operation which is assumed to occur less frequently than once over a span of one hundred operating years, excluding design extension conditions; and which the nuclear power plant is required to withstand without sustaining severe fuel failure, even if individual components of systems important to safety are rendered out of operation due to servicing or faults (YVL B.1 2013). Postulated accidents are grouped into two classes on the basis of the frequency of their

---

<sup>8</sup> IEC's definition is in the form "manner in which failure occurs".

initiating events: a) Class 1 postulated accidents (DBC 3), which can be assumed to occur less frequently than once over a span of one hundred operating years, but at least once over a span of one thousand operating years; b) Class 2 postulated accidents (DBC 4), which can be assumed to occur less frequently than once during any one thousand operating years.

**Postulated Initiating Event** (oletettu alkutapahtuma): A hypothetical event identified during design capable of leading to anticipated operational occurrences or accident conditions.

**Redundancy** (rinnakkaisuus): Provision of alternative (identical or diverse) structures, systems and components, so that anyone can perform the required function regardless of the state of operation or failure of any other (IAEA 2007)<sup>9</sup>.

**Safety category**: One of four possible safety assignments (A, B, C, unclassified) of *I&C functions* resulting from considerations of the safety relevance of the function to be performed (IEC 61513 2011).

**Safety class** (turvallisuusluokka): One of four possible assignments (1, 2, 3, unclassified) of *I&C systems* important to safety resulting from consideration of their requirement to implement *I&C functions* of different safety importance (IEC 61513 2011)<sup>10</sup>.

**Safety division** (turvallisuuslohko): Premises and the components and structures contained therein, where one of the redundant parts of each safety system is placed (YVL B.1 2013).

**Safety function** (turvallisuustoiminto): A specific *function* that must be accomplished by a system for safety (modified from IAEA 2007).

**Severe reactor accident** (vakava reaktorionnettomuus): An accident in which a considerable part of the fuel in a reactor loses its original structure (YVL B.1 2013).

**Space** (tila): An area or volume (e.g. room) bounded actually (e.g. by walls) or theoretically (by coordinates).

**Spurious activation**: Type of active *malfunction* where an I&C system unexpectedly without a demand triggers an external function, e.g. starts or stops a pump.

**System** (järjestelmä): Combination of interacting *system elements* organised to achieve one or more stated purposes (ISO/IEC/IEEE 15288 2015). In this report system elements are considered to be real-world (physical) entities like machines, structures, people, software or data (see Tommila & Alanen 2015).

---

<sup>9</sup> Informally, the term can also refer to the redundant "trains" of plant equipment.

<sup>10</sup> In Finland, only systems, structures and components are grouped into the Safety Classes 1, 2, and 3 and Class EYT ( non-nuclear safety) (YVL B.2 2013).