



BME

Budapest University of Technology and Economics



KHJIT

Faculty of Transportation Engineering and Vehicle Engineering

Department of Control for Transportation and Vehicle Systems

Nuclear I&C Systems Safety

The Principles of Nuclear Safety for
Instrumentation and Control Systems

Legal and Regulatory Framework

Legal framework, regulatory bodies and main standards of Nuclear Power Plants

Legal Framework

- Act CXVI of 1996 on Atomic Energy (Atomic Act)
- Govt. Decree 118/2011. (VII. 11.) on the nuclear safety requirements of nuclear facilities and on related regulatory activities (Nuclear Safety Code)
 - Volume 1. Nuclear safety authority procedures of nuclear facilities
 - Volume 2. Management systems of nuclear facilities
 - Volume 3. Design requirements of nuclear power plants
 - Volume 3a. Design requirements of nuclear power plants (new installation)
 - Volume 4. Operation of nuclear power plants
 - Volume 5. Design and operation of research reactors
 - Volume 6. Interim storage of spent nuclear fuel
 - Volume 7. Site survey and assessment of nuclear facilities
 - Volume 8. Decommissioning of nuclear facilities
 - Volume 9. Requirements for the construction of a new nuclear installation
 - Volume 10. Nuclear Safety Code definitions
- Govt. Decree 190/2011. (IX. 19.) on physical protection requirements for various applications of atomic energy, and on the corresponding system of licensing, reporting and inspection

Regulatory Body (Licensor)

Hungarian Atomic Energy Authority

- Responsible for the regulatory tasks in connection with
 - the use of atomic energy exclusively for peaceful purposes,
 - the safety of nuclear facilities and transport containers,
 - the security of nuclear and other radioactive materials and associated facilities.
- With the consideration of the relevant legal requirements, authorizes the licensee to perform activities in connection with the use of atomic energy.
- Regularly reviews and assesses the operation of the licensees, and the safety and security performance of the facilities. If observes any non-compliance, then it takes or order measures to its elimination.



International Guidance and Coordination

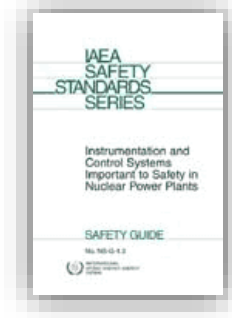
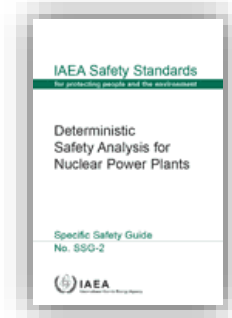
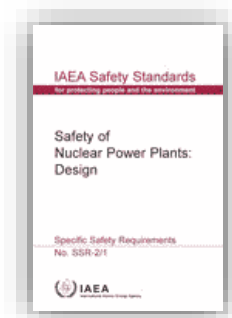


International Atomic Energy Agency

- The IAEA is the "Atoms for Peace" organization within the United Nations family.
- Set up in 1957 as the world's centre for cooperation in the nuclear field, the Agency works with its Member States and multiple partners worldwide to promote the safe, secure and peaceful use of nuclear technologies.
- **Main Work Areas**
 - Nuclear Technology & Applications
 - to help countries use nuclear and isotopic techniques to promote sustainable development objectives.
 - Nuclear Safety & Security
 - to provide a strong, sustainable and visible global nuclear safety and security framework, protecting people and the environment from the harmful effects of ionizing radiation.
 - Safeguards & Verification
 - to fulfil the duties and responsibilities of the IAEA as the world's nuclear inspectorate.

IAEA Main I&C Related Standards

Deprecated		New
IAEA Safety Standards Series NS-R-1 (2000), Safety of Nuclear Power Plants: Design	Requirements	IAEA Safety Standards Series SSR-2/1 (2012), Safety of Nuclear Power Plants: Design Specific Safety Requirements
IAEA Safety Standards Series NS-R-2 (2000), Safety of Nuclear Power Plants: Operation		IAEA Safety Standards Series SSR-2/2 (2011), Safety of Nuclear Power Plants: Commissioning and Operation
		IAEA Safety Standards Series SSG-2 (2010), Deterministic Safety Analysis for Nuclear Power Plants
IAEA Safety Standards Series NS-G-1.1 (2000), Software for Computer Based Systems Important to Safety in Nuclear Power Plants	Safety Guide	IAEA Safety Standards Series SSG-39 (2016), Design of Instrumentation and Control Systems for Nuclear Power Plants (supersedes NS-G-1.1 and NS-G-1.3)
IAEA Safety Standards Series NS-G-1.3 (2002), Instrumentation and Control Systems Important to Safety in Nuclear Power Plants		



Other IAEA I&C Related Guides

Budapest University of Technology and Economics

Faculty of Transportation Engineering and Vehicle Engineering

Department of Control for Transportation and Vehicle Systems

IAEA Safety Standards Series **SSG-30** (2014), Safety Classification of Structures, Systems And Components in Nuclear Power Plants

IAEA Nuclear Energy Series **NP-T-3.12** (2011), Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants

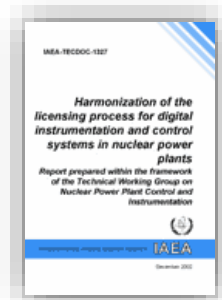
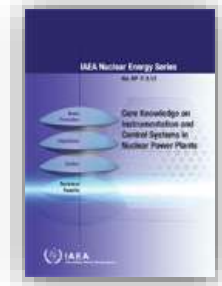
IAEA Nuclear Security Series **NSS-17** (2011), Computer Security at Nuclear Facilities

IAEA Nuclear Energy Series **NP-T-1.5** (2009), Protecting Against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants

IAEA Nuclear Energy Series **NP-T-1.4** (2009), Implementing Digital Instrumentation and Control Systems in the Modernization of Nuclear Power Plants

IAEA **TECDOC-1389** (2004), Managing modernization of nuclear power plant instrumentation and control systems

IAEA **TECDOC-1327** (2002), Harmonization of the licensing process for digital instrumentation and control systems in nuclear power plants



Nuclear Standards: Differences from IEC 61508

- Mixed deterministic/probabilistic approach
 - Safety functions are classified into categories according to their impact on plant safety
 - Systems are classified into categories according to the safety functions they provide
 - Requirements are assigned to categories
 - Requirements are drawn from the plant safety design base
- Many requirements are explicitly deterministic
 - Design for reliability
 - Single failure criterion → Redundancy
 - Common cause failure criterion → Independence → Diversity
 - Lack of backlash from lower category equipment

Nuclear I&C Safety Principles

Principles, Terms and Concepts of Safety in
Nuclear Instrumentation and Control Systems

Safety Classification of I&C Functions

- The safety classification is usually performed using a combination of deterministic methods, probabilistic methods and engineering judgment taking into consideration:
 - The safety function(s) to be performed (to take action in response to some plant event, or to not fail in a way that would cause a hazardous event);
 - The probability of, and the safety consequences that could result from, a failure of the function;
 - The probability that the function will be needed to provide safety.
 - If the function is needed:
 - how quickly the function must respond and for how long the function must be performed;
 - the timeliness and dependability of alternative actions.
- Once I&C functions are classified, systems and components are assigned to classes according to the highest level function that they must perform.

Comparison of Different Classification Systems

Nat. or intl. standard	Classification of the importance to safety				
IAEA NS-R-1	Systems Important to Safety			Systems Not Important to Safety	
	Safety	Safety Related			
IEC 61226 Functions Systems	Systems Important to Safety			Unclassified	
	Category A Class 1	Category B Class 2	Category C Class 3		
Canada	Category 1	Category 2	Category 3	Category 4	
France N4	1E	2E	SH	Important to Safety	Systems Not Important to Safety
EUR	F1A (Aut.)	F1B (A./M.)	F2		Unclassified
Russian Fed.	Class 2		Class 3		Class 4 (N/I. to Safety)
USA and IEEE	Systems Important to Safety			Non-nuclear Safety	
	SR / Class 1E	(No name assigned)			
R. of Korea	IC-1		IC-2		IC-3

Main Principles of NPP I&C Design

- 1) **Specification of performance requirements** for I&C actions is necessary to ensure that these functions are achieved over the full range of measured variables to be accommodated, with the characteristics (e.g., accuracy, response time) to produce the necessary output signal.
- 2) **Design for reliability** of I&C systems important to safety is necessary to prevent undue challenges to the integrity of the plant physical barriers provided to limit the release of radiation and to ensure the reliability of engineered protective systems.
 - a. Compliance with the single failure criterion
 - b. Redundancy
 - c. Diversity
 - d. Independence
- 3) **Consideration of equipment failure modes** (fail safe principle) is given in the design of I&C systems to make their functions more tolerant of expected failures of systems or components. The design of systems and equipment should strive to ensure that the range of possible failure modes is predictable and that the most likely failures will always place the system in a safe state.

Main Principles of NPP I&C Design

- 4) **Control of access to I&C equipment** important to safety must be established to prevent unauthorized operation or changes and to reduce the possibility of errors caused by authorized personnel.
- 5) **Set point analysis** is performed to ensure that I&C functions that must actuate to ensure safety do so, before the related process parameter exceeds its safe value (safety limit).
 - An analysis is necessary to calculate the point at which the I&C system must act to accomplish this. The difference between the safety limit and the set point must account for errors and uncertainties that cause a difference between the measured value acted upon by the I&C system and the actual value of the physical process.
- 6) **Design for optimal operator performance** is the practice of applying human factors engineering to minimize the potential for operator errors and limit the effects of such errors.
 - Human factors engineering is applied to ensure that operators have the information an controls needed for safe operation and to provide an operator friendly interface for operation, maintenance, and inspection of systems important to safety.

Main Principles of NPP I&C Design

- 7) **Equipment qualification** is a process for ensuring that the systems and equipment important to safety are capable of performing their safety functions. This process involves the demonstration of the necessary functionality under all service conditions associated with all plant design states.
- 8) **Quality in the design and manufacturing** of systems and equipment important to safety is necessary to demonstrate that they will perform their assigned safety functions.
- 9) **Design for electromagnetic compatibility** is necessary to ensure that installed systems and equipment will withstand the electromagnetic environment in a nuclear power plant.
 - This involves making appropriate provisions for the grounding, shielding and decoupling of interference.
 - The qualification of equipment for operation in the electromagnetic environment is important and is a part of equipment qualification.

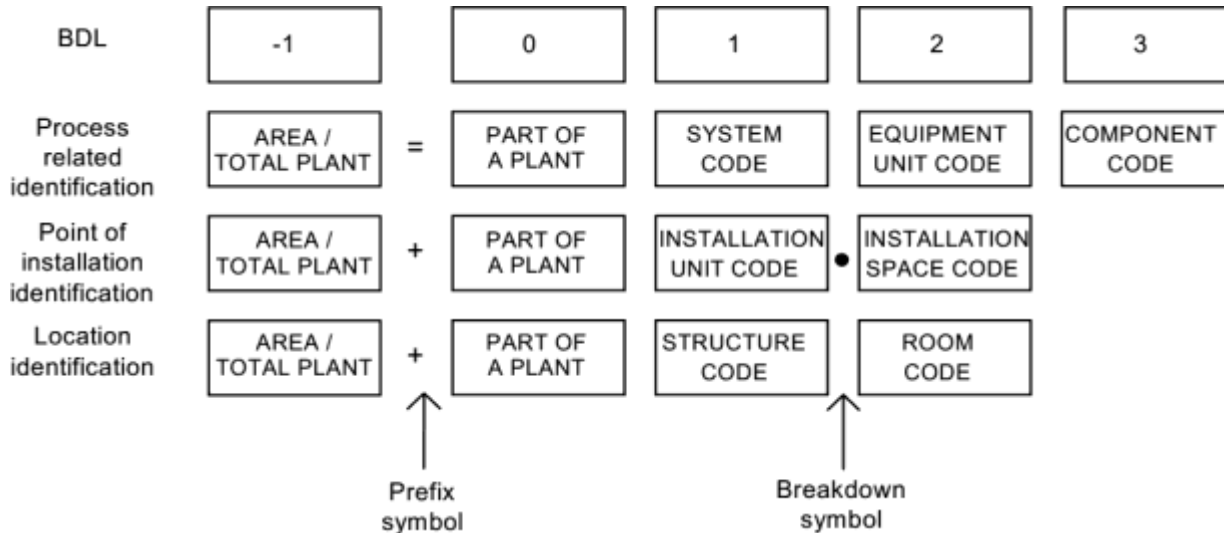
Main Principles of NPP I&C Design

- 10) **Testing and testability** provide assurance that I&C systems and equipment important to safety remain operable and capable of performing their safety tasks.
 - This principle includes both the need to provide a design that facilitates testing, calibration, and maintenance, and the establishment of programs to appropriately schedule, conduct, and learn from these activities.
- 11) **Maintainability** is the principle of designing I&C systems and equipment important to safety to facilitate timely replacement, repair, and adjustment of malfunctioning equipment.
 - A consequence of design for testability and maintainability is the provision of additional redundancy so that the single failure criterion continues to be met while one redundancy is removed for maintenance or testing.
- 12) **Documentation of I&C functions, systems, and equipment** is necessary to ensure that the plant operating organization has adequate information to ensure safe operation and maintenance of the plant and to safely implement subsequent plant modifications.
- 13) **Identification of I&C functions, systems, and equipment** important to safety is required to ensure that these items are properly treated during the design, construction, maintenance and operation of the plant.
 - Both the physical items, and documentation of these items should unambiguously identify their safety significance.

KKS (Kraftwerk Kennzeichnen System)

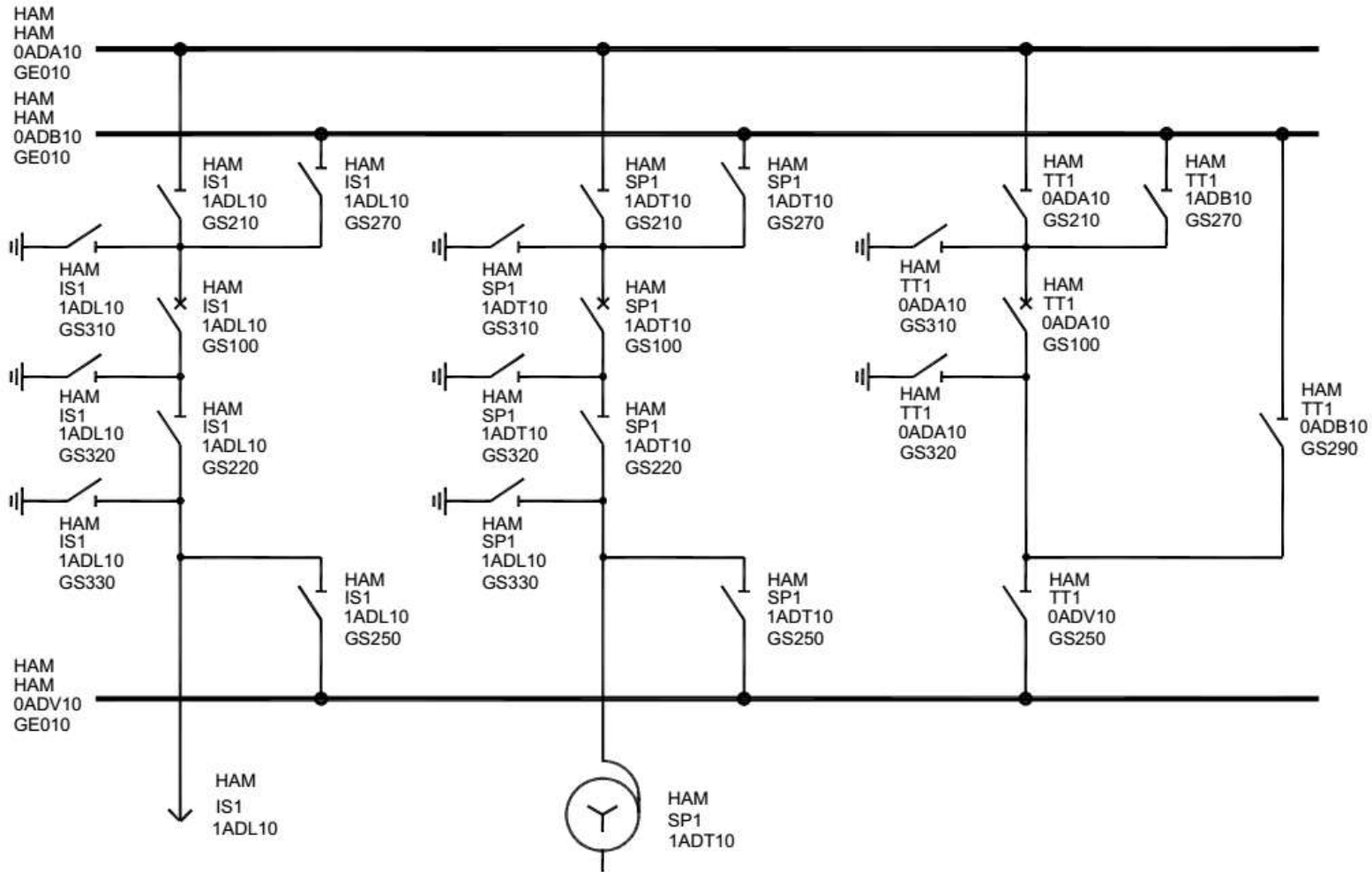
The KKS code consists of alpha letters (A) and numbers (N). The code is divided in 4 (0-3) BDL's in the process related code and in 3 (0-2) BDL's in the point of installation code and the location code.

BDL	0			1					2				3						
Definition	Part of a plant			System code					Equipment unit code				Component code						
Name	G			F ₀	F ₁	F ₂	F ₃	F _N	A ₁	A ₂	A _N		A ₃	B ₁	B ₂	B _N			
Type of key	A/N	A/N	A/N	N	A	A	A	N	N	A	A	N	N	N	A	A	A	N	N



Source: LANDSNET KKS HANDBOOK, December 2008, Edition: 07

KKS Coding Example



Source: LANDSNET KKS HANDBOOK, December 2008, Edition: 07

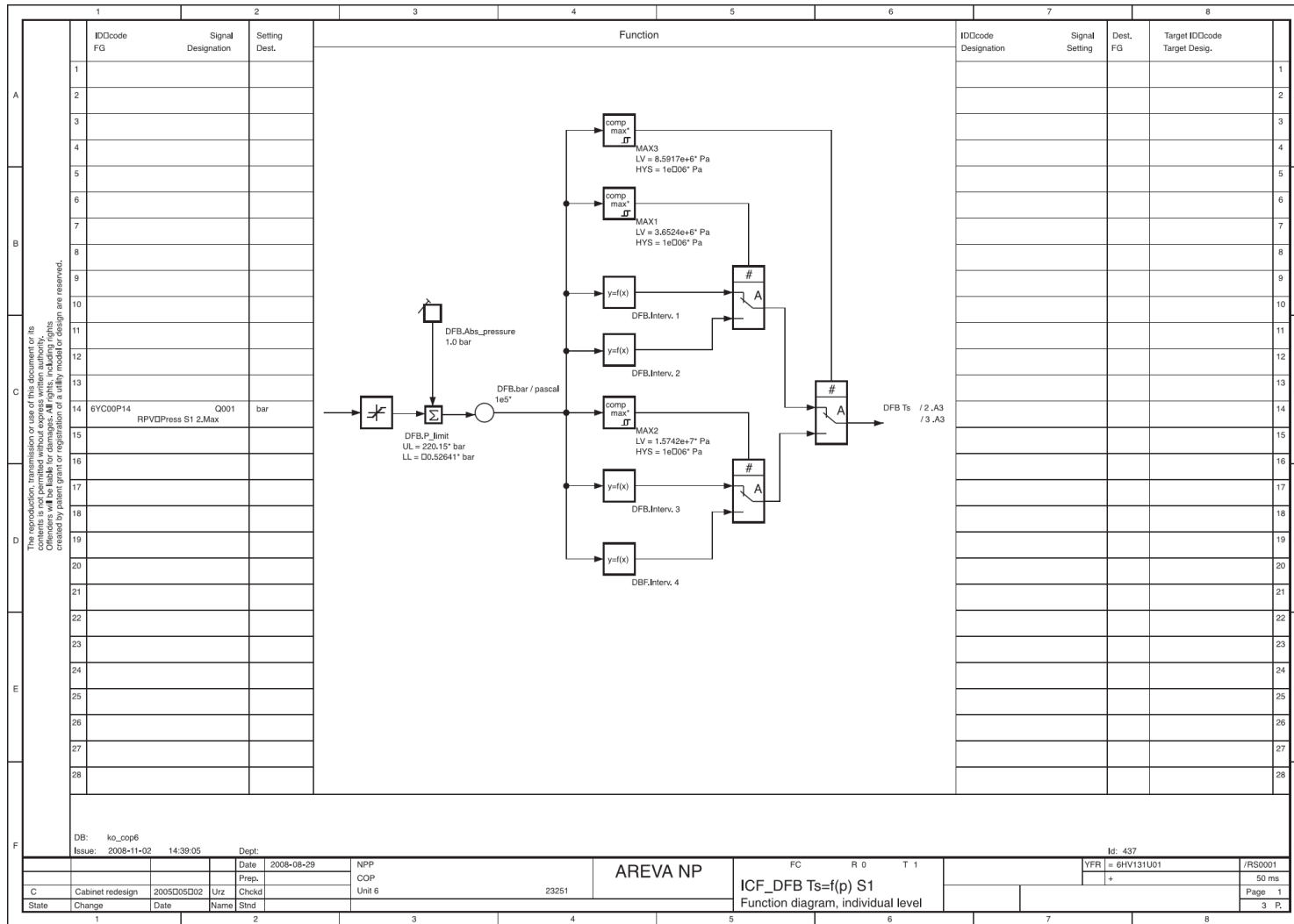
Example of coding line- and transformer bays, two busbars and one spare

I&C System Functional Description

Budapest University of Technology and Economics

Faculty of Transportation Engineering and Vehicle Engineering

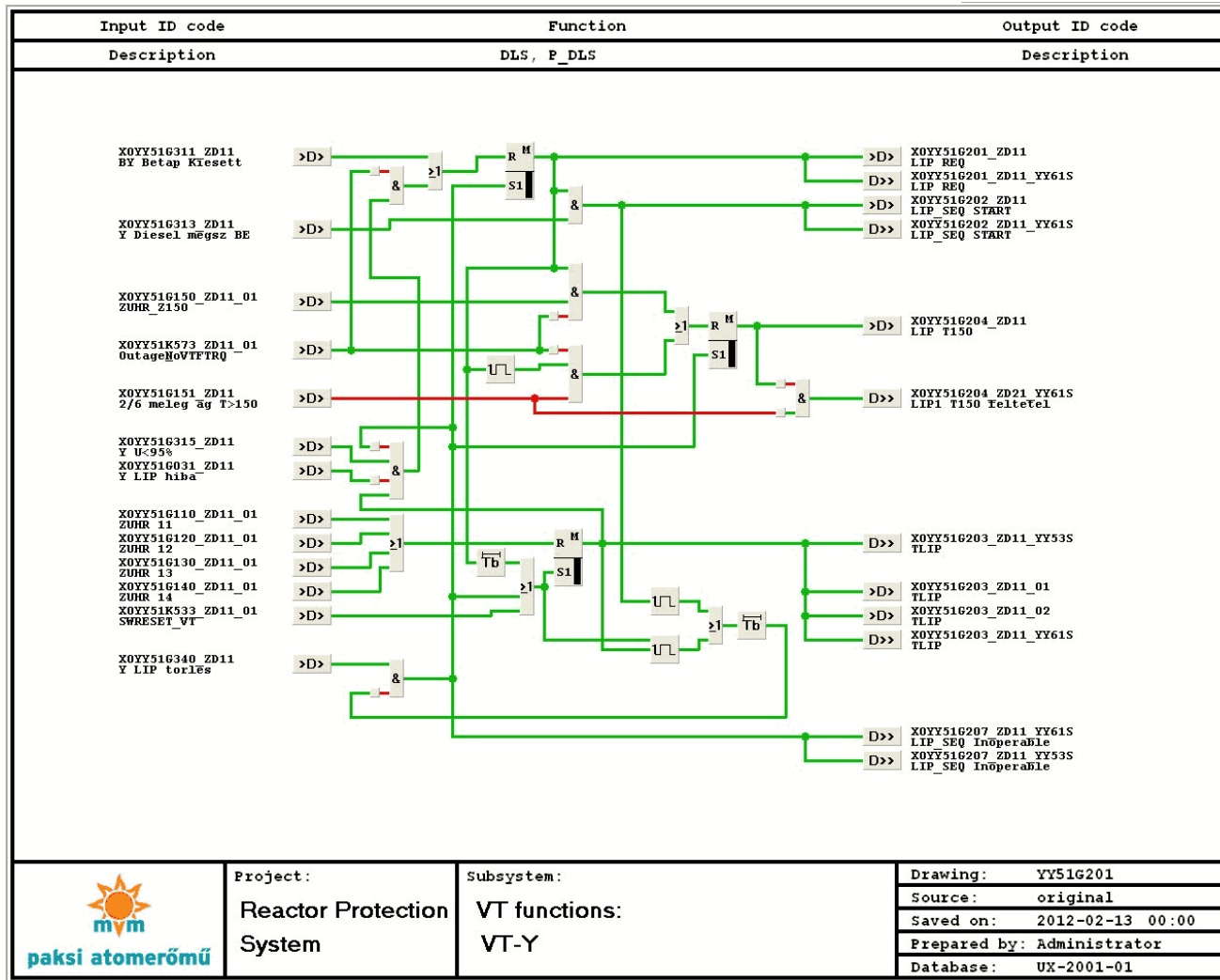
Department of Control for Transportation and Vehicle Systems



Source: Instrumentation and Control, TELEPERM® XS System Overview (Areva, 2012)



I&C Functional Specification in the Paks NPP



Defence in depth

Definition and Comments	Relationships	Examples
A 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 material and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions.	Provides	
	The primary means of preventing accidents in a nuclear power plant and mitigating the consequences of accidents if they do occur is the application of the concept of defence in depth	
	Requires	I&C Systems
	<ul style="list-style-type: none">• 5 levels• 3 layers• active, passive and inherent safety features	<ul style="list-style-type: none">• Control Systems• Limitation Systems• Protection Systems• ESFAS

Current Recent Concept of Defence-in-Depth in NPPs

Levels of defence in depth	Objective	Essential means	Associated plant condition categories
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation	Normal operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features	Anticipated operational occurrences
Level 3	Control of accident within the design basis	Engineered safety features and accident procedures	Design basis accidents (postulated single initiating events)
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management	Multiple failures Severe accidents
Level 5	Mitigation of radiological consequences of significant releases of radioactive material	Off-site emergency response	

Design for reliability of I&C systems important to safety

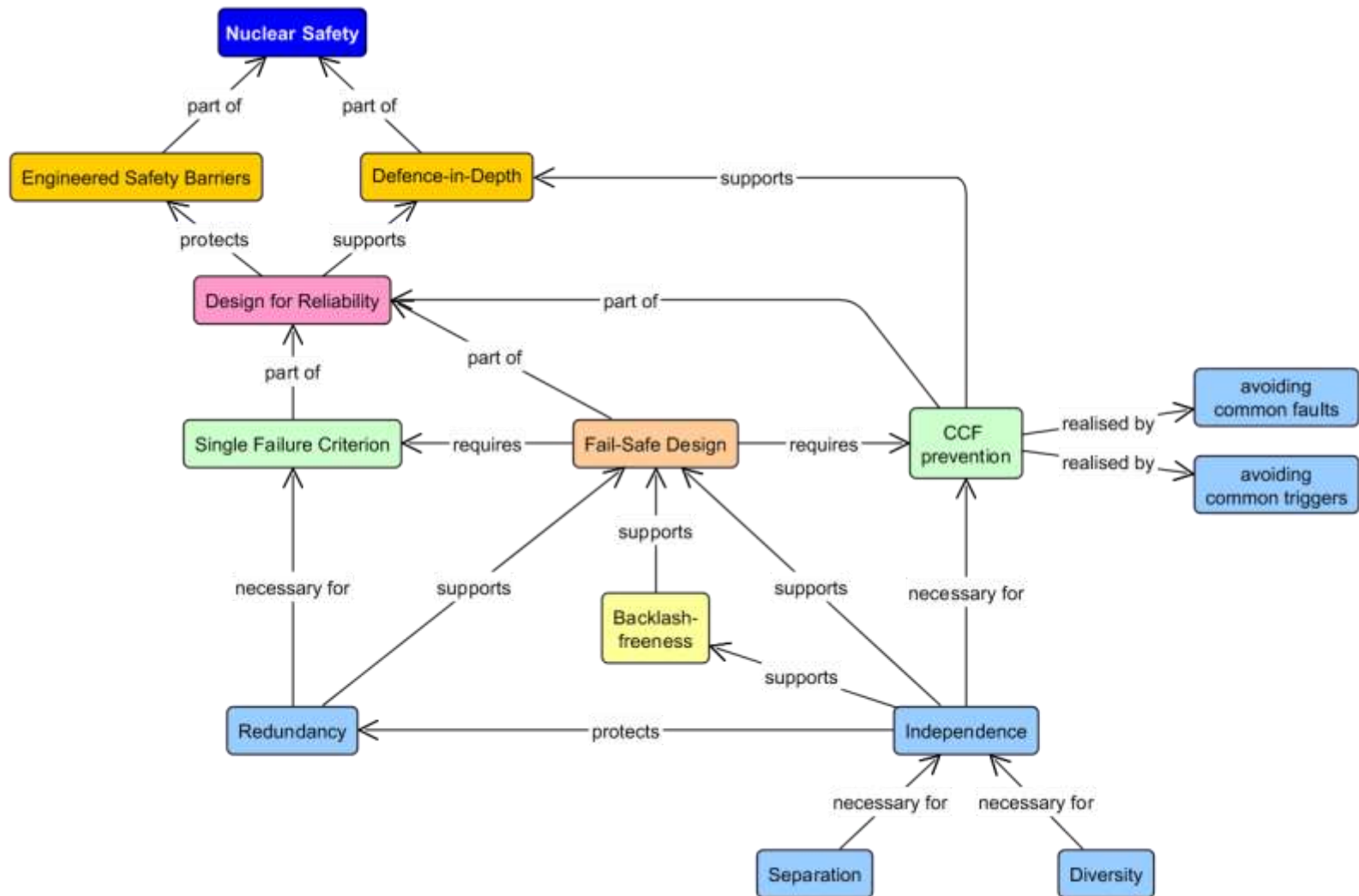
Necessary to prevent undue challenges to the integrity of the plant physical barriers, and to ensure the reliability of engineered protective systems.

- Compliance with the **single failure criterion** is a deterministic approach to ensuring that I&C systems can tolerate a random failure of any individual component, taking into account both the direct consequences of such a failure and any failures caused by events for which the system must function.
- **Redundancy** is the provision of multiple means of achieving a given function. It is commonly used in I&C systems important to safety to achieve system reliability goals and/or conformity with the single failure criterion.
 - For redundancy to be fully effective the redundant systems must be independent of each other.

Design for reliability of I&C systems important to safety

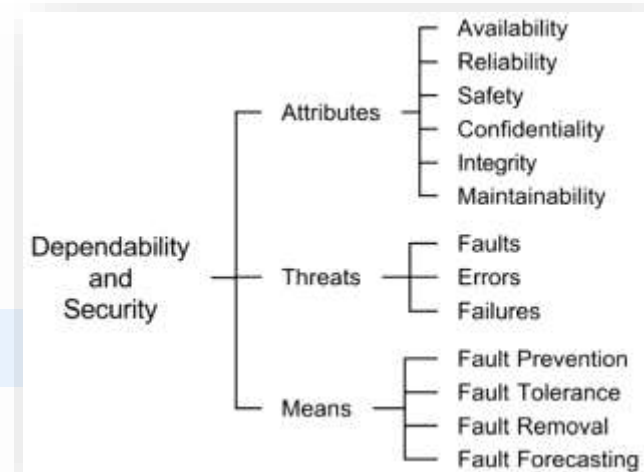
- **Independence** prevents propagation of failures — from system to system, between redundant elements within systems, and caused by common internal plant hazards.
 - Independence can be achieved through physical separation, isolation, remote location, etc.
- **Diversity** in I&C systems is the principle of monitoring different parameters, using different technologies, different logic or algorithms, or different means of actuation in order to provide several ways of achieving an I&C function. Diversity provides defence against common cause failures (CCF).
 - It is complementary to the plant design principle of defence in depth.
- Consideration of equipment failure modes (**fail safe principle**) is given in the design of I&C systems to make their functions more tolerant of expected failures of systems or components.
 - The design should ensure that the range of possible failure modes is predictable, and that the most likely failures will always place the system in a safe state.

Design for Reliability Principles



Design for reliability

Definition and Comments	Relationships	Examples
<p>All structures, systems and components that are items important to safety be designed such that their quality and reliability are commensurate with their classification.</p>	<p>Design features</p> <ul style="list-style-type: none">• Tolerance of random failure• Tolerance of common cause failures• Fail-safe design• Independence of equipment and systems• Selection of high quality equipment• Testability and maintainability	<p>Graded approach</p> <p>Safety measures are applied proportional to the potential consequences of a failure.</p>
<p>A suitable combination of probabilistic and deterministic design criteria should typically be applied.</p>	<p>Requires</p> <ul style="list-style-type: none">• Safety objective• Safety principles• Requirements and measures	



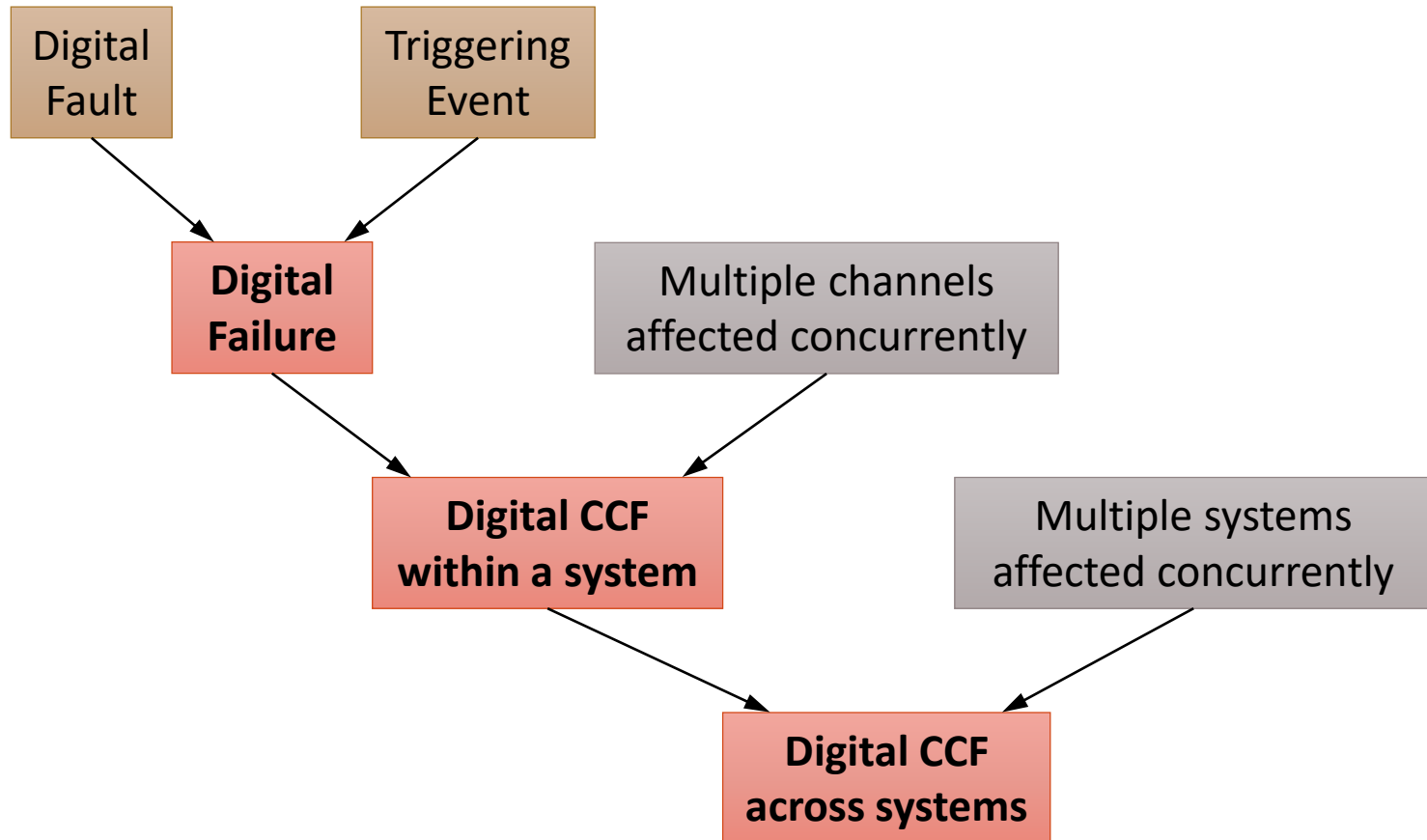
Fail-safe design

Definition and Comments	Relationships	Conformance
The concept of fail-safe design shall be incorporated, as appropriate, into the design of systems and components important to safety.	<p>I&C systems</p> <p>I&C systems for items important to safety shall be designed for high functional reliability and periodic testability commensurate with the safety function(s).</p>	<p>Verification and validation</p> <ul style="list-style-type: none">• Formal methods• Deterministic safety assessment• Testing
Systems and components important to safety shall be designed for fail-safe behaviour, as appropriate, so that their failure or the failure of a support feature does not prevent the performance of the intended safety function.	<p>Requires</p> <ul style="list-style-type: none">• Single failure tolerance• Common cause failure avoidance• Redundancy• Independence• Diversity	<p>Evidence</p> <ul style="list-style-type: none">• Safety case

Common cause failure

Definition and Comments	Relationships	Causes
<p>Failure of two or more structures, systems and components due to a single specific event or cause.</p> <p>For example, a design deficiency, a manufacturing deficiency, operation and maintenance errors, a natural phenomenon, a human induced event, saturation of signals, or an unintended cascading effect.</p>		<p>Origin</p> <ul style="list-style-type: none">• Human error• (Common) dependence• Environmental
	<p>Means</p> <ul style="list-style-type: none">• Independence• Diversity	<p>Constituents</p> <ul style="list-style-type: none">• (Common) fault/error• (Common) trigger
	<p>Common mode failure</p> <p>Failure of two or more structures, systems and components in the same manner or mode due to a single event or cause.</p>	<p>Supported by</p> <ul style="list-style-type: none">• Deterministic safety assessment• Formal methods

Conditions required to create a digital CCF



Independence

Definition and Comments	Relationships	
<p>Safety systems should be independent of safety related and non-safety systems.</p> <p>Independence should be provided between redundant parts of safety systems and safety-related systems.</p> <p>Appropriate independence should be provided between diverse functions.</p>	<p>Provides</p> <p>Prevents:</p> <ol style="list-style-type: none">(1) propagation of failures from system to system or(2) propagation of failures between redundant parts within systems, and(3) common cause failures due to common internal plant hazards.	<p>Examples</p> <ul style="list-style-type: none">• Separate locations (rooms)• Independent cabling (paths)• Analogue / Digital technology
<p>Interference between safety systems or between redundant elements of a system shall be prevented by appropriate means.</p>	<p>Means</p> <ul style="list-style-type: none">• Physical separation• Electrical isolation• Functional independence• Independence of communication (data transfer)	

Diversity

Definition and Comments	Relationships	
<p>The presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure, including common mode failure.</p>	<p>Types</p> <ul style="list-style-type: none">• Human diversity• Design diversity• Software diversity• Functional diversity• Signal diversity• Equipment diversity• System diversity	<p>Diversity</p> <ul style="list-style-type: none">• When are two systems diverse enough?
<p>Examples: different operating conditions, different working principles or different design teams, different sizes of equipment, different manufacturers, types of equipment that use different physical methods.</p>	<p>Requires</p> <ul style="list-style-type: none">• Independence	<p>Examples</p> <ul style="list-style-type: none">• Heterogeneity• N-version programming• Recovery Blocks

Single failure criterion

Definition and Comments

A criterion (or requirement) applied to a system such that it must be capable of performing its task in the presence of any single failure.

The double contingency principle is, for example, such that the design for a process must include sufficient safety factors that an accident would not be possible unless at least two unlikely and independent changes in process conditions were to occur concurrently.

Relationships

Provides

Assessment is often aimed at quantifying performance measures for comparison with criteria.

Requires

- Redundancy
- Independence

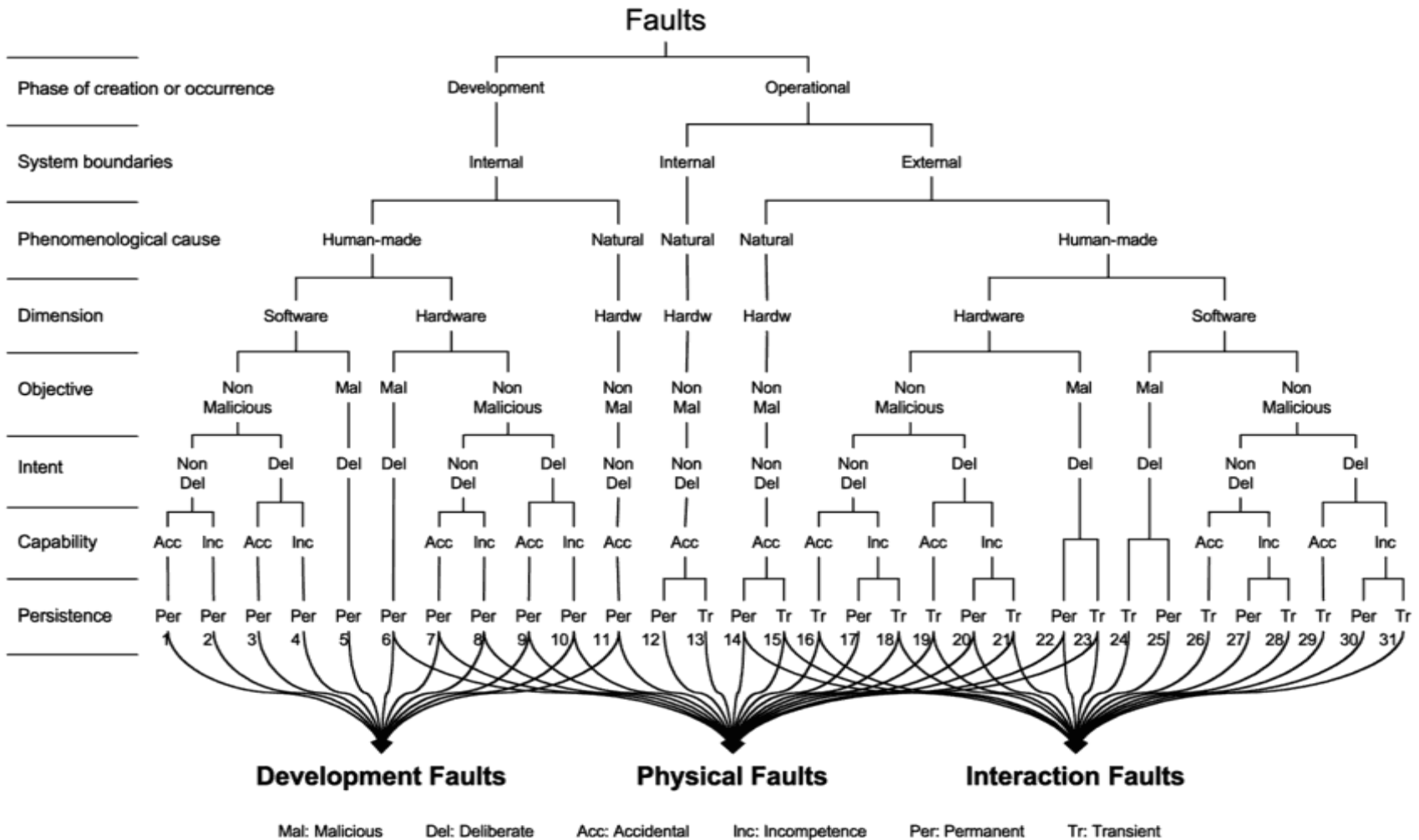
Supported by

- Deterministic safety assessment

Applies to

Systems important to safety

Classification of Faults



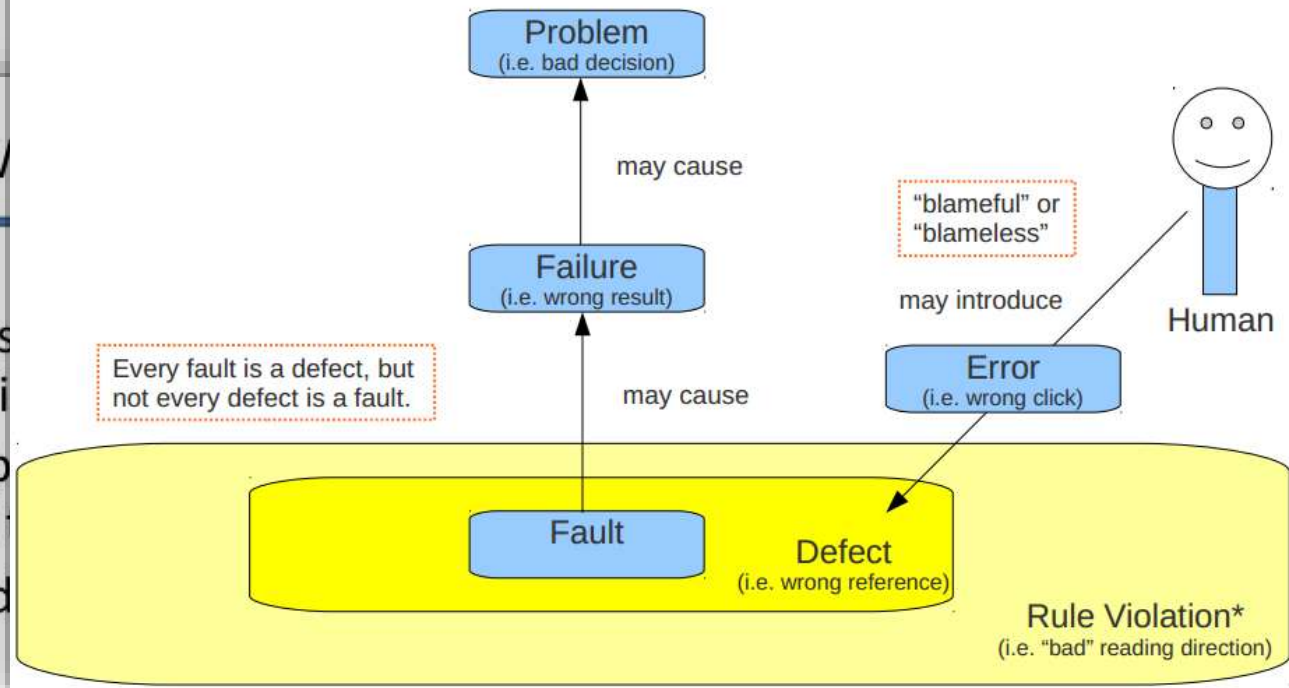
Fault – Error – Failure – Problem

(according to IEEE Std 1044-2009)



IFIP W

- **Failure** occurs longer compli
- **Error** is that p liable to lead
- **Fault** is adjud error.



Faults are the cause of errors that may lead to failures



Safety assessment

Definition and Comments

The process, and the result, of analysing systematically and evaluating the hazards associated with sources and practices, and associated protection and safety measures.

Assessment is often aimed at quantifying performance measures for comparison with criteria.

- Deterministic safety assessment
- Probabilistic safety assessment

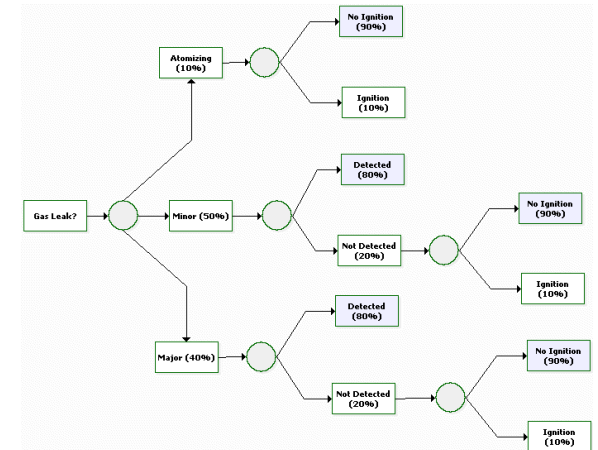
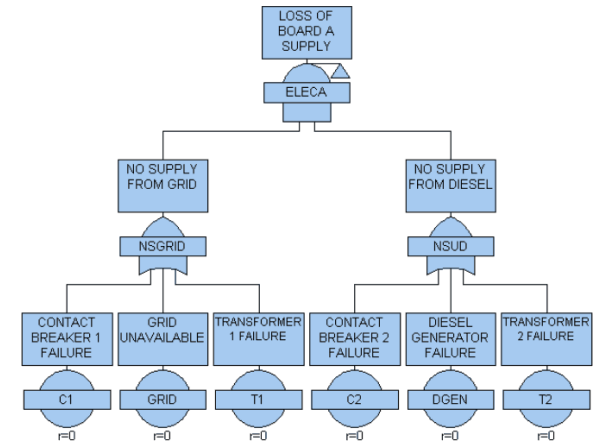
Relationships

Supports

- Safety case

Requires

- Risk assessment
- Failure modes
- Basic event probabilities
- Safety case
- Safety arguments and evidence



Safety case

Definition and Comments

A collection of arguments and evidence in support of the safety of a facility or activity.

Property-based, vulnerability aware, standards-informed and is described by the safety justification triangle.

Relationships

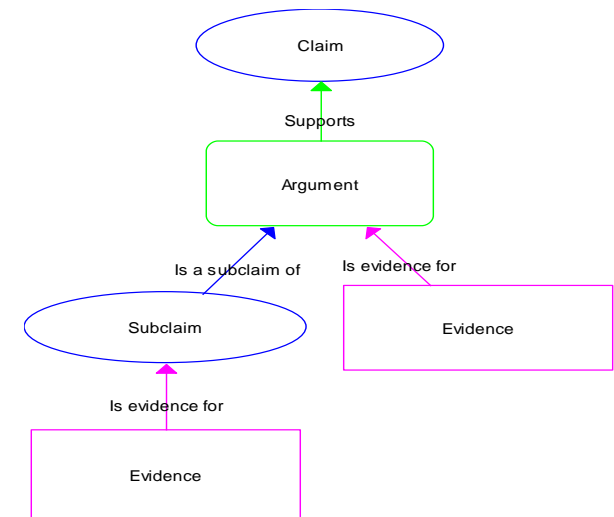
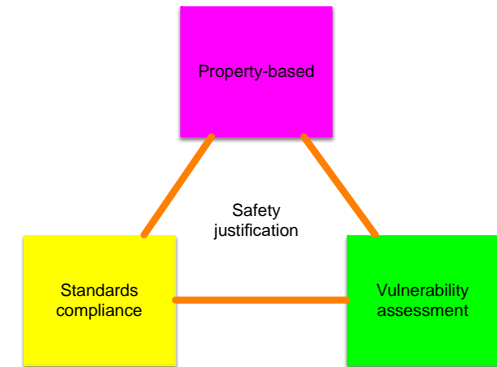
Types of claims

- Reliability-functionality
- Safety-robustness
- Safety-fail safe
- Rule compliance
- Vulnerability assessment

Sources of evidence

E.g. Functionality:

- Random testing
- Statistical testing
- Functional testing
- Model-based testing
- Development metrics
- Static analysis
- Formal verification
- Modelling and simulation



Verification and validation

Definition and Comments	Relationships	
<p>Validation</p> <p>The process of determining whether a product or service is adequate to perform its intended function satisfactorily.</p>	<p>Validation is broader in scope, than verification.</p> <ul style="list-style-type: none">• Computer system validation: testing and evaluation of the integrated computer system to ensure compliance with the requirements.	<p>Examples</p> <ul style="list-style-type: none">• Simulation• Emulation• Testing
<p>Verification</p> <p>The process of determining whether the quality or performance of a product or service is as stated, as intended or as required.</p>	<p>Verification is closely related to quality assurance and quality control.</p> <ul style="list-style-type: none">• Computer system verification: ensuring that a phase in the system life cycle meets the requirements imposed on it by the previous phase.	<p>Examples</p> <ul style="list-style-type: none">• Specification analysis• Static analysis• Model-based development• Formal verification