



BME



KHJIT

Budapest University of Technology and Economics

Faculty of Transportation Engineering and Vehicle Engineering

Department of Control for Transportation and Vehicle Systems

Nuclear I&C Systems Safety

The Requirements of Nuclear Safety for
Instrumentation and Control Systems

Legal and Regulatory Framework

Legal framework, regulatory and international bodies for 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.



Hierarchy and characteristics of requirement sources

Requirement source		Compliance	Nature	Examples
Legal	Law	Due to the mandatory nature of the legislation, their application can not be waived and the lack of knowledge of the law does not exempt from the consequences.	Mandatory	Act CXVI of 1996 on Atomic Energy
	Govt. decree			118/2011. Kr. (NSC) 190/2011. Kr.
Standard	International	Standards are not binding on their own. Among other things, their relevance is that their application becomes mandatory if prescribed in the contract.	Voluntary, but ... becomes mandatory if prescribed in a law or contract	IEC 62645:2014 IAEA SSR-2/1
	National			MSZ EN 61513:2011 MSZ EN 61226:2011
Guide	IAEA guidance	Helps to comply with the requirements, the HAEA regards it as normative.	Voluntary	IAEA SSG-30 IAEA SSG-39
	HAEA guide	Following it is voluntary, but guarantees a simplified licensing procedure.	Voluntary	HAEA guide A3.35 HAEA guide N3a.36

International Guidance and Coordination

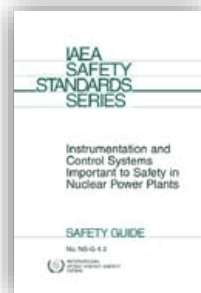
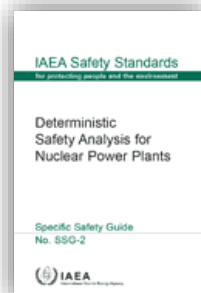
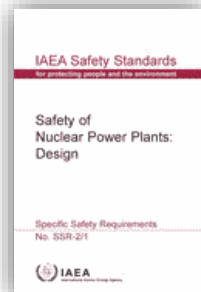


International Atomic Energy Agency

- 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
	Safety Guide	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		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

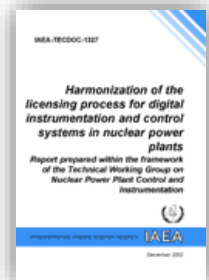
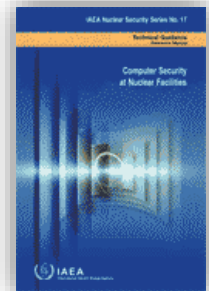
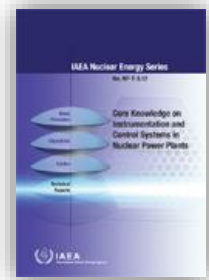
IAEA Nuclear Security Series **NSS-17** (2011), Computer Security at Nuclear Facilities

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 I&C Standards

International standards for the nuclear industry, and their use in the development process

NSC requirements regarding the use of standards

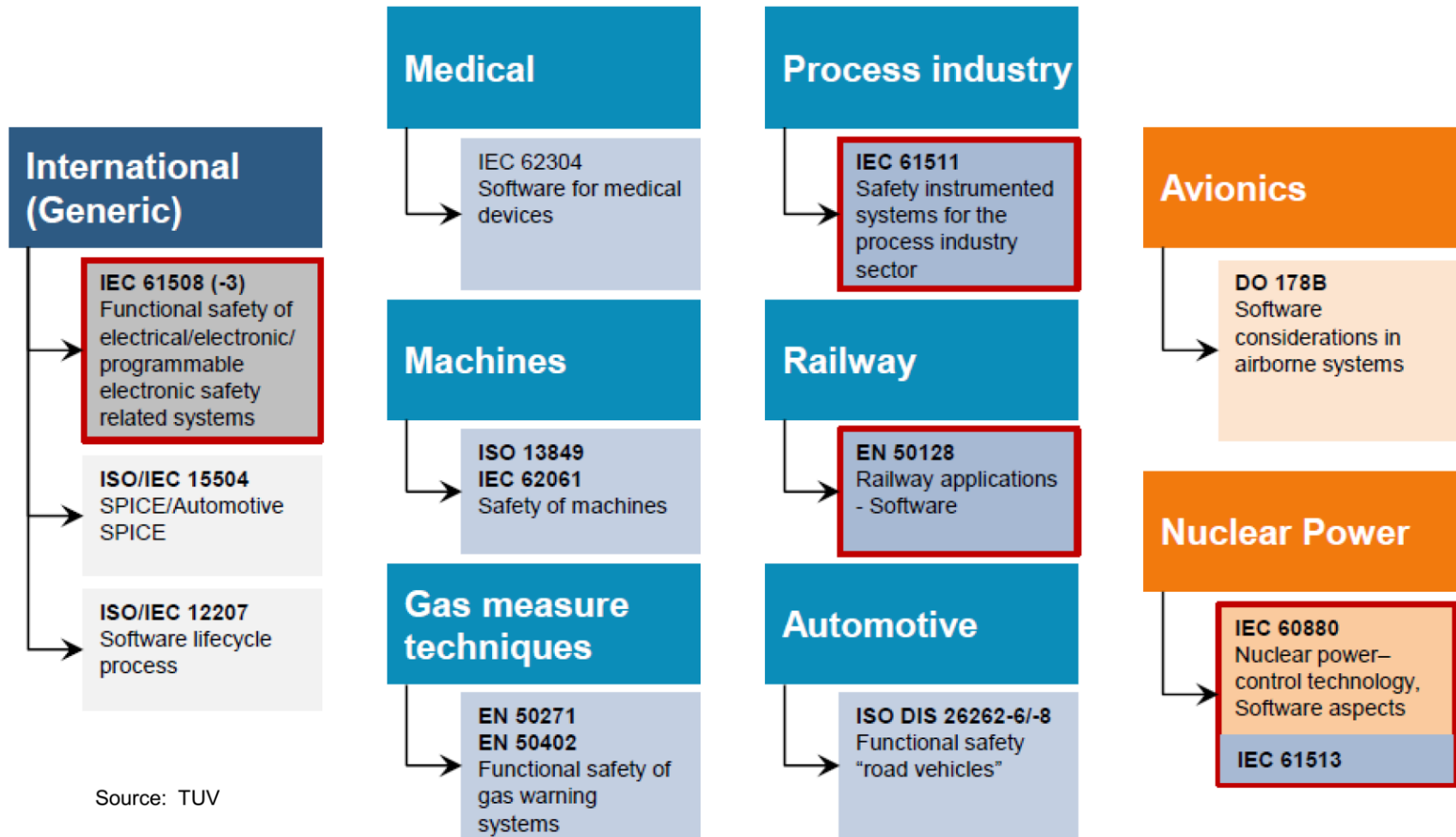
„Systems, structures and components that are **important to safety** shall be designed **according to proven standards of nuclear industry**. The standards selected for the design process shall be preliminarily defined, their applicability shall be justified. (NSC 3.2.1.2100)

„**Design requirements based on national and international standards** and proven engineering practices **shall be assigned to the safety classes** of systems, structures and system components and shall be consistently applied.” (NSC 3.2.2.2165)

„For each operating condition, a set of design limits shall be determined for the physical parameters of the nuclear safety related systems, structures and system components. The **design limits shall be consistent with the nuclear safety requirements and applied standards**.” (NSC 3.2.2.2500)

„The design and implementation of the instrumentation and control systems and system components shall be carried out in **accordance with the selected standards applicable to systems and system components of the relevant safety class and differentiated requirements**.” (NSC 3.4.5.2000)

Safety Standards for Different Fields



Source: TUV

IEC Nuclear I&C Standards

IEC No.	MSZ No.	Title
IEC 61226:2009	MSZ EN 61226:2011	Nuclear power plants - Instrumentation and control important to safety - Classification of instrumentation and control functions
IEC 61513:2011	MSZ IEC 61513:2013	Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems
IEC 60987:2007	MSZ EN 60987:2015	Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems
IEC 60880:2006	MSZ EN 60880:2010	Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions
IEC 62138:2004	MSZ EN 62138:2009	Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions

IEC Nuclear I&C Standards

Budapest University of Technology and Economics

Faculty of Transportation Engineering and Vehicle Engineering

Department of Control for Transportation and Vehicle Systems

IEC No.	MSZ No.	Title
IEC 61227:2008	MSZ IEC 61227:2011	Nuclear power plants - Control rooms - Operator controls
IEC 61225:2005	MSZ IEC 61225:2011	Nuclear power plants - Instrumentation and control systems important to safety - Requirements for electrical supplies
IEC 62340:2007	MSZ EN 62340:2011	Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF)
IEC 60709:2004	MSZ EN 60709:2011	Nuclear power plants - Instrumentation and control systems important to safety - Separation
IEC 60780:1998	MSZ IEC 60780:2011	Nuclear power plants - Electrical equipment of the safety system - Qualification
IEC 61500:2009	MSZ IEC 61500:2011	Nuclear power plants - Instrumentation and control important to safety - Data communication in systems performing category A functions
IEC TR 61000 ser.	MSZ EN 61000 ser.	Electromagnetic compatibility requirements

The Use of IEC Standards in the Design Process

Requirements from the plant safety design base

IEC 61226: Classification of I&C functions

I&C Architectural design

Assignment of functions to I&C systems

IEC 61513: General requirements for systems

Design and
Implementation
of the I&C Hardware

Design and Implementation
of the I&C Software

IEC 60987: Hardware
design requirements

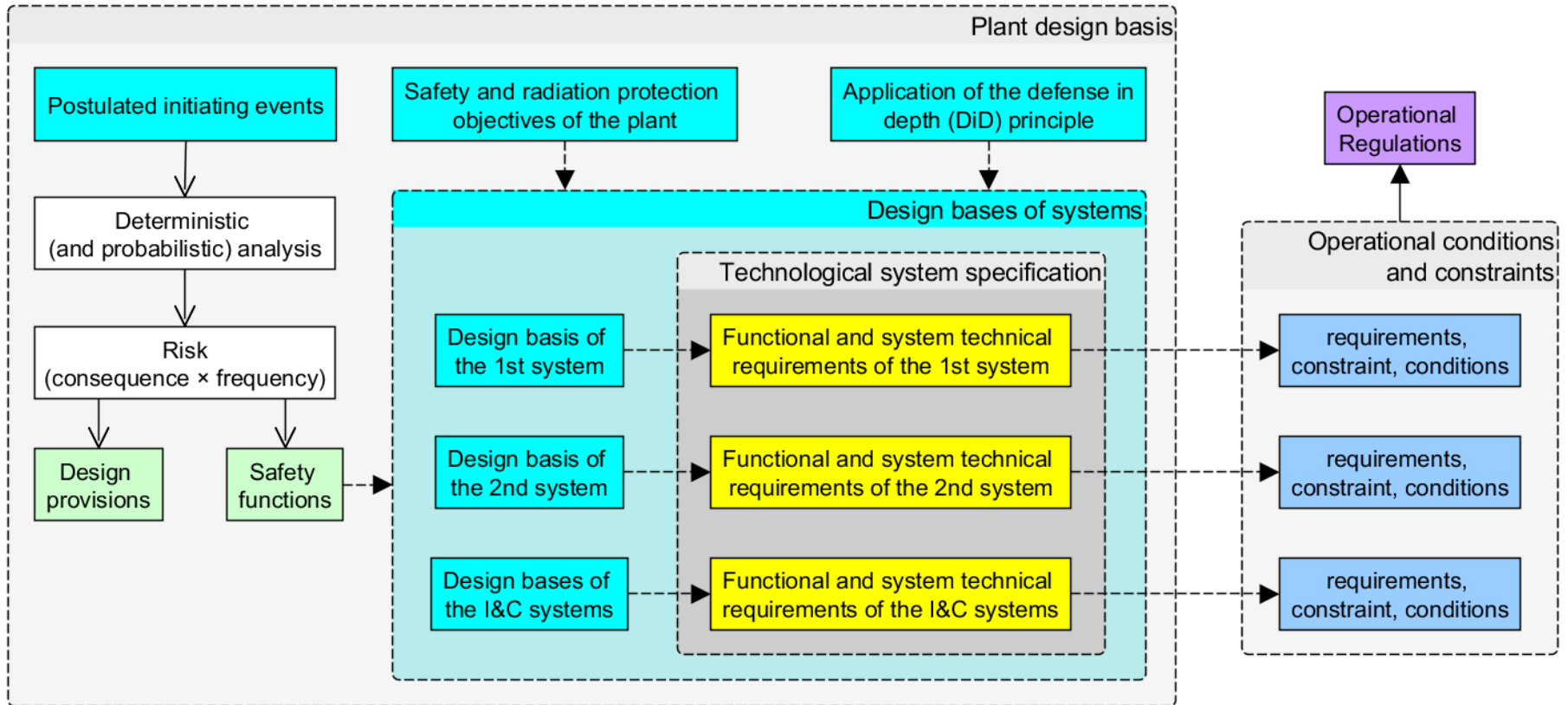
IEC 60880: Software
aspects for computer-
based systems performing
category A functions

IEC 62138: Software
aspects for computer-
based systems performing
category B or C functions

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

Connection between the plant and the I&C system design bases



Connection with the plant design basis

The process functional specification of the instrumentation and control systems shall comply with the following requirements:

- a) it shall identify the control task in accordance with the technological purposes and requirements,
 - b) it shall assign an unambiguous identification code to each control task,
 - c) it shall classify the management tasks in functional safety levels on the basis of the importance of the given task to safety and shall assign them to the appropriate level of defense in depth,
 - d) it shall determine the independence criteria associated with the functions, including diversity requirements,
 - e) it shall determine the response times associated with the functions,
- (continued, NSC 3a.4.5.3200)

Connection with the plant design basis

- g) it shall determine the tasks that require operator intervention in the TA1-4 and TAK1 operating conditions of the nuclear power plant in such a way that the operating personnel are able to perform them,
- h) in addition to a description in a human language, it shall use an appropriately structured, formal language description method,
- i) it shall design an automated system for their formal monitoring and verification,
- j) it shall contain the information necessary to perform operator tasks and the monitoring of automatic tasks,
- k) it shall set accuracy requirements for operating limits and the display of analogue values,
- l) it shall determine the expected reliability requirements, and
- m) in the case of programmable instrumentation and control systems included in the Safety Class ABOS 2, it shall determine simulation methods for their functional monitoring and validation.

(NSC 3a.4.5.3200)

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)			
Rep. of Korea	IC-1		IC-2	IC-3	

I&C Systems by Importance to Safety (IAEA old scheme)

Plant equipment

Items important to safety

Items not
important to safety

Safety systems

Safety related items or systems

Protection system **Initiation I&C** for:

- Reactor trip
- Emergency core cooling
- Decay heat removal
- Confinement isolation
- Containment spray
- Containment heat removal

Safety actuation system **Actuation I&C** for:

- Reactor trip
- Emergency core cooling
- Decay heat removal
- Confinement isolation
- Containment spray
- Containment heat removal

Safety system support features I&C for:

- Emergency power supply

- Reactor control systems
- Plant control systems
- Control room I&C
- Fire detection and extinguishing I&C
- Radiation monitoring
- Communication equipment
- Fuel handling and storage I&C
- Radiation monitoring
- I&C supporting the operation of the safety systems
- I&C for monitoring the state of the safety systems
- Access control systems

Safety categorization of I&C functions (relevant in Hungary)

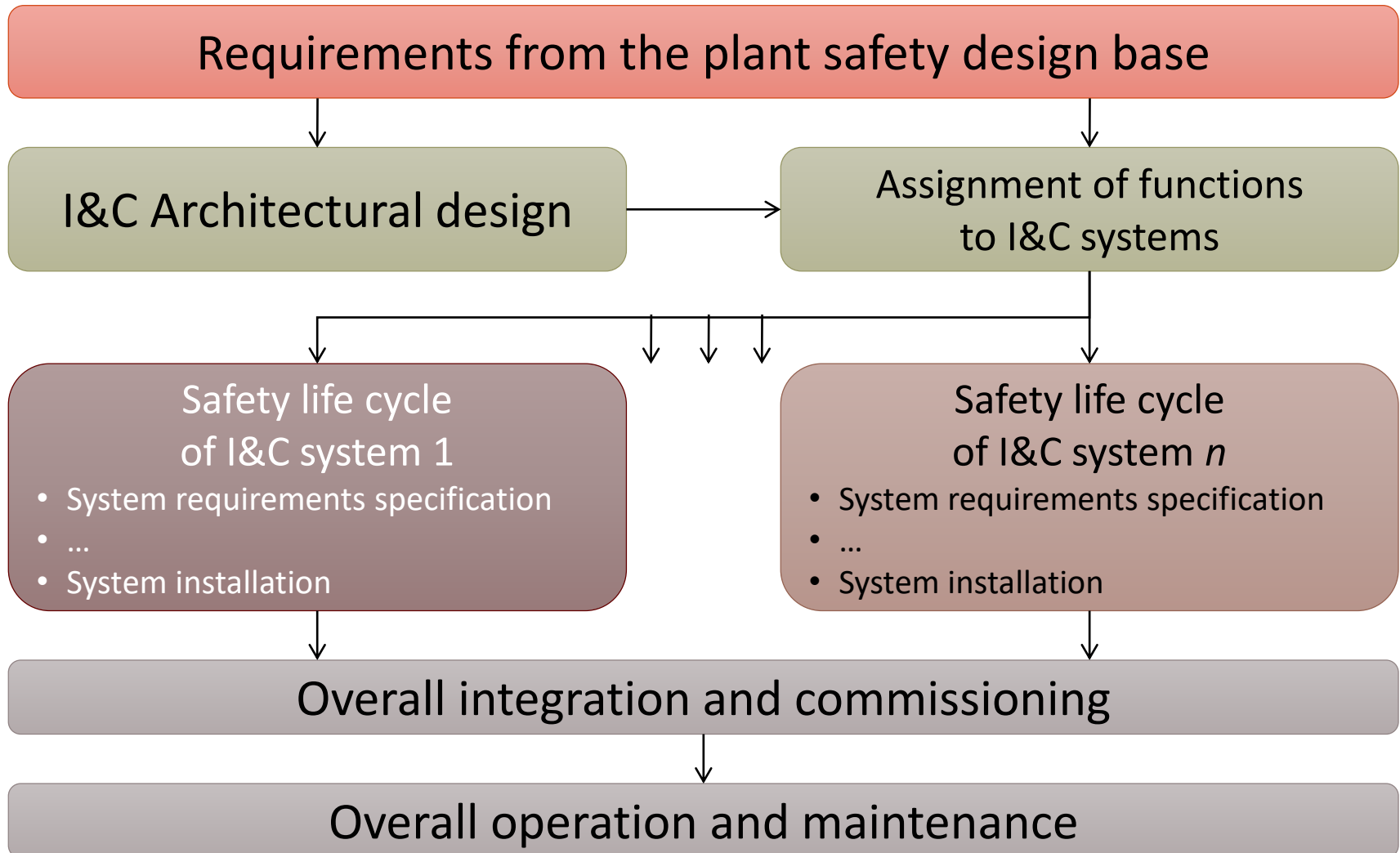
IAEA SSG-30	Function	Safety category 1	Safety category 2	Safety category 3	Systems not important to safety	
	Equipment	Safety class 1	Safety class 2	Safety class 3		
IEC 61226	I&C function	Category A	Category B	Category C	NC (not classified)	
	I&C equipment	Class 1	2. class	3. class		
EUR Rev. D	Function	F1A	F1B	F2	-	
	Equipment	L1A	L1B	L2		
NSC 3/A. (new builds)	Function	F1A	F1B	F2	-	
	Equipment	ABOS 1	ABOS 2	ABOS 3	ABOS 4	
NSC 3. (operating)	Active function / I&C equipment	Safety class 2		Safety class 3		Class 4 (non-safety)

Correlation Between IEC Classes and Categories

Categories of I&C functions important to safety (according to IEC 61226)			Corresponding classes of I&C systems important to safety (according to IEC 61513)
A	(B)	(C)	1
	B	(C)	2
		C	3

- I&C functions of category A may be implemented in class 1 systems only
- I&C functions of category B may be implemented in class 1 and 2 systems
- I&C functions of category C may be implemented in class 1, 2, and 3 systems

Simplified I&C Safety Life-Cycle



System Architecture

The architecture of the system is constrained by the category of functions to be implemented within the system and the defence in-depth concept.

- a) The system **may implement** functions of the highest category allowed for its class and **functions of lower categories**:
 - 1) the design requirements for each subsystem **shall not be lower than those required by the function of the highest category** implemented by the subsystem;
 - 2) the design of the system shall ensure that the requirements of the subsystems or equipment of the higher classes **are satisfied in case of failure of the equipment of the lower class**.
- b) The design of the system shall include redundancy and other features necessary to provide tolerance to failure and to accommodate the functions important to safety.
 - The system may also include redundancy to fulfil availability requirements. The need for such redundancies is defined at the level of system design.
- c) The design of the system shall satisfy any independence requirements to
 - prevent propagation of failures from systems of lower importance to safety;
 - prevent propagation of failures between redundant trains providing category A functions.
- d) The design of class 1 systems shall include sufficient redundancy to meet the single-failure criterion for category A functions **during operation and maintenance**.

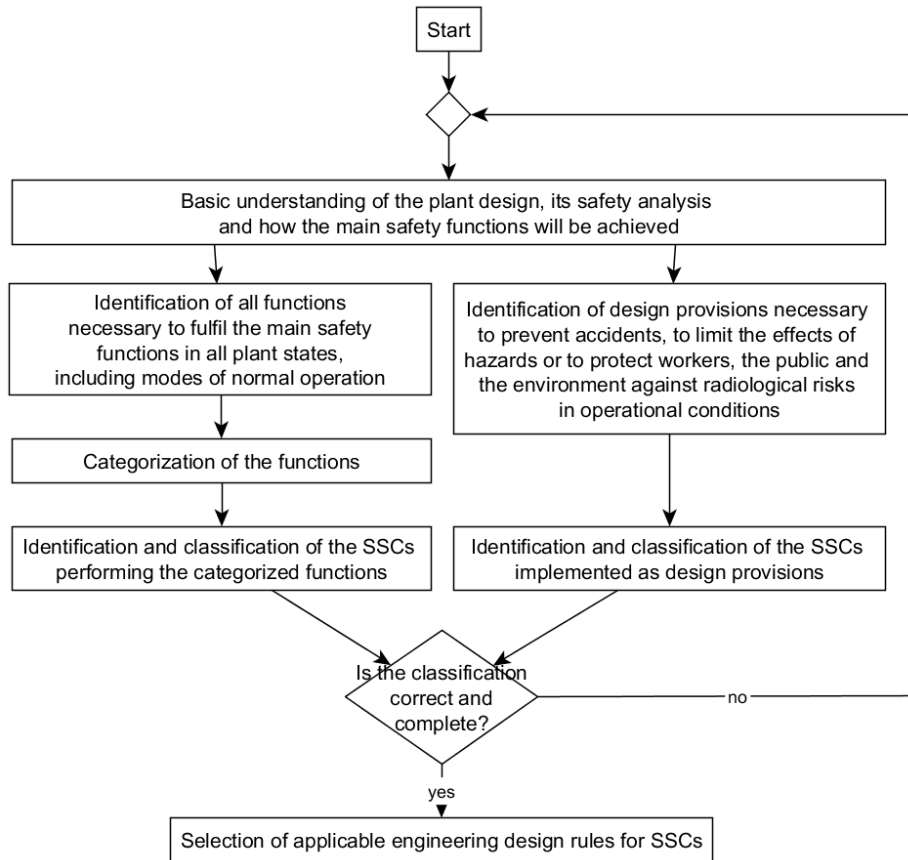
Nuclear I&C Safety Principles

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

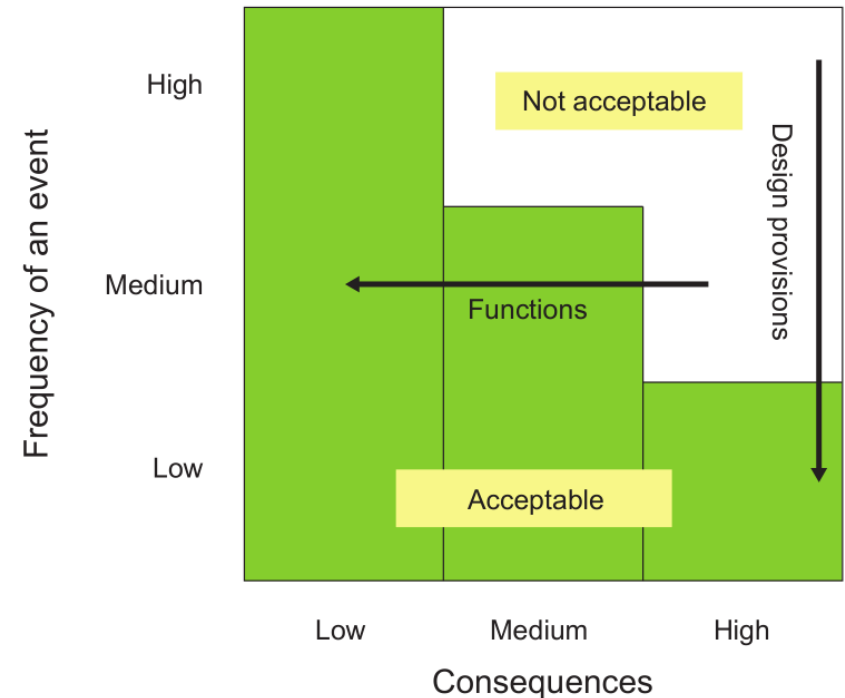
Safety Classification of I&C Functions

- 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.

IAEA (SSG-30) categorization and classification process



The basic principle of frequency versus consequences



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.

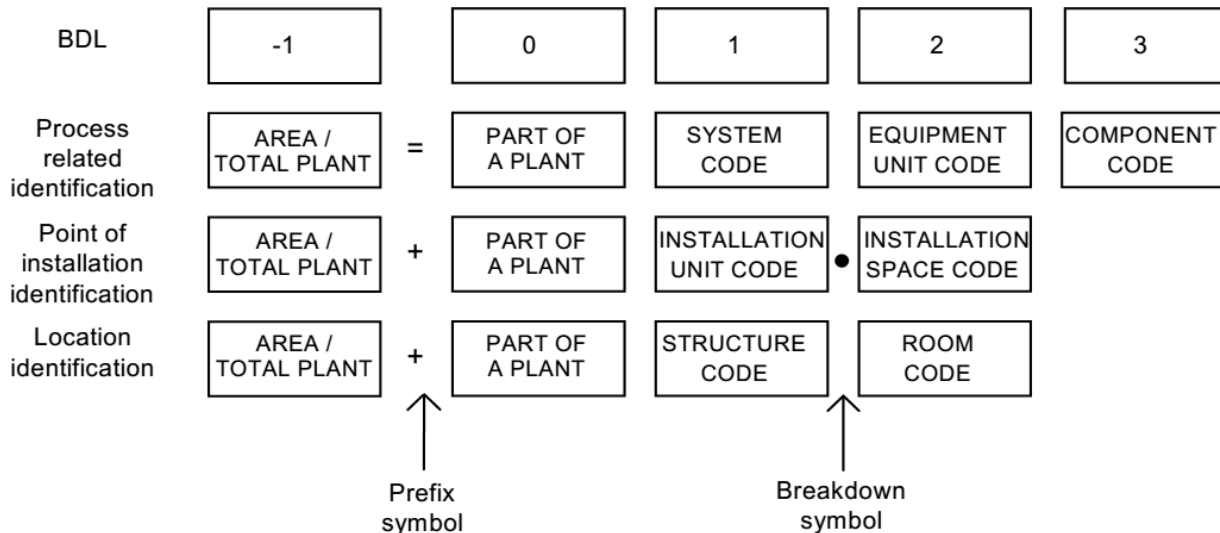
Main Principles of NPP I&C Design

- 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)

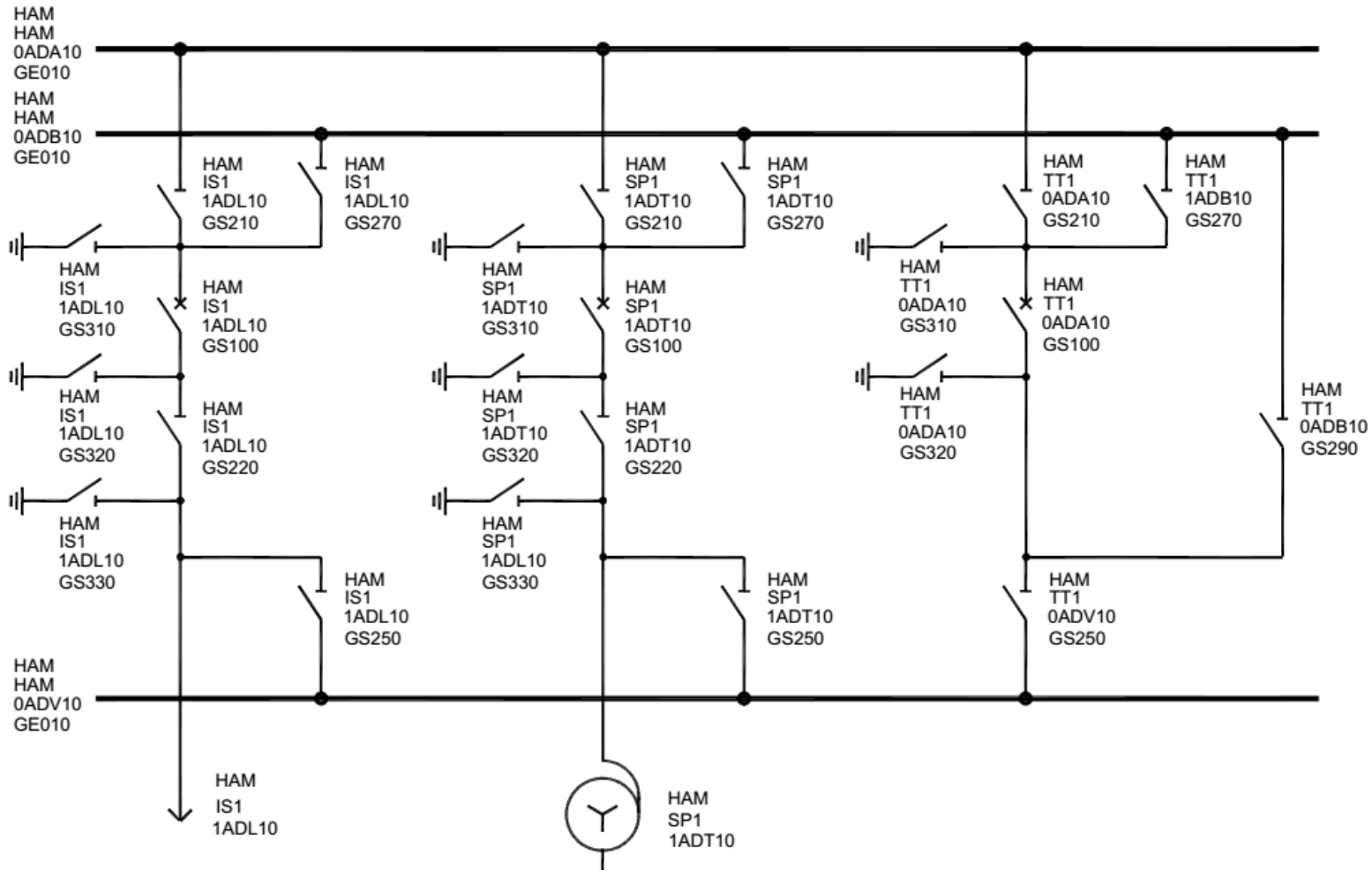
The KKS code consists of alpha letters (A) and numbers (N). The code is divided in 4 (0-3) BDL's in the process related code and in 3 (0-2) BDL's in the point of installation code and the location code.

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

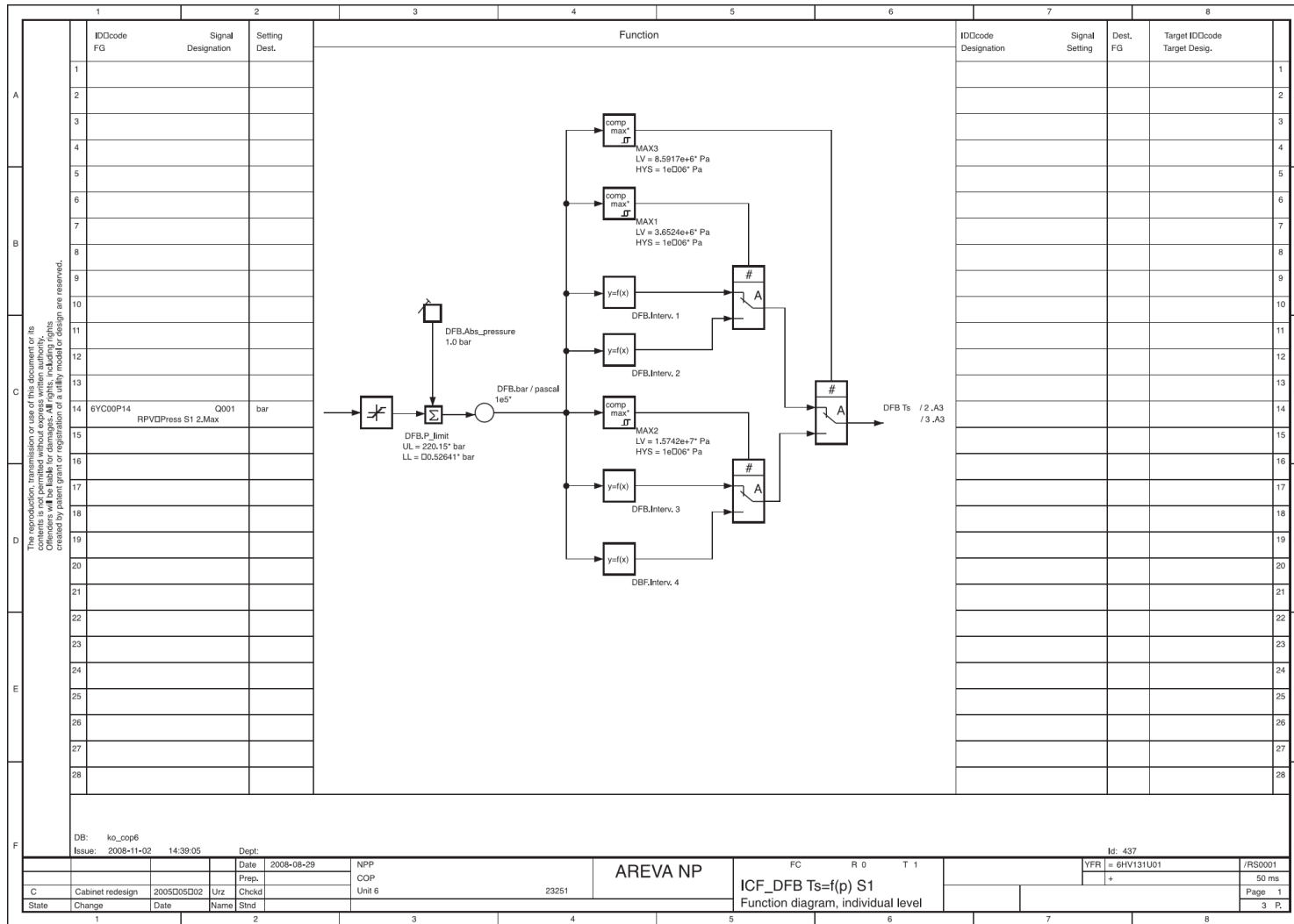
Example of coding line- and transformer bays, two busbars and one spare

I&C System Functional Description

Budapest University of Technology and Economics

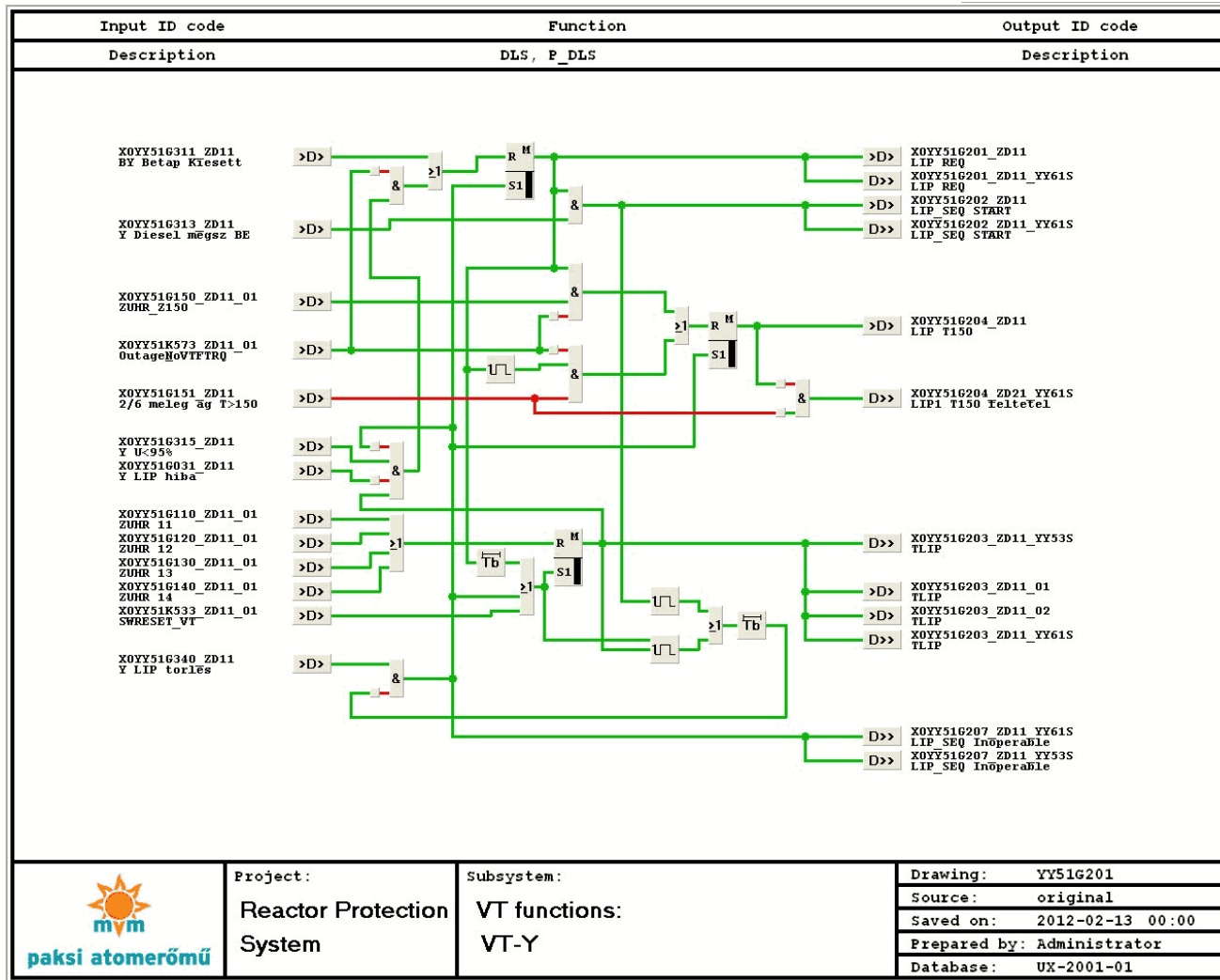
Faculty of Transportation Engineering and Vehicle Engineering

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<ul style="list-style-type: none">• 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	

Defense in Depth layers (1–3.) for Paks I. and II. (NSC Vol. 3. and 3a.)

DiD layer	Paks I. operating units (INSAG-10)		Paks II. new units (WENRA 2013)		Relevant oper. condition
	Objective	Essential means	Objective	Essential means	
1.	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation	Deviations from the normal operating condition and prevention of failures	Conservative design, implementation and operation to a high standard; maintaining the main operating parameters between the prescribed limits	Normal operation (DB1)
2.	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features	Management of deviations from the normal operating condition and failures	Control and safety protection systems; other surveillance methods	Anticipated operational occurrences (TA2)
3.	3.a.	Control of accident within the design basis	Management of design basis accidents in order to limit radioactive releases and to prevent fuel melting	Safety systems, emergency operating procedures	Design basis accident (TA3-4)
	3.b.	(Earlier this operating condition and the corresponding means (systems) were on DiD level 4.)		Added safety features for the elimination of complex accidents, emergency operating procedures, on-site emergency response measures	Complex accidents (Postulation of multiple failures) (TAK1)

Plant states – according to IAEA SSR 2/1 / IEC 61226 / NSC

Operational states		Accident conditions (AC)			
IAEA SSR-2/1, IAEA SSG-30					
Normal operation	Anticipated operational occurrences	Design basis accidents (DBA)		Design extension conditions (DEC)	
		Design extension		-	Significant degradation of the reactor core
IEC 61226 (Ed. 4 - Draft)					
Normal operation	Design basis event (DBE)			Design extension conditions (DEC) ...	
	Anticipated operational occurrences	- (AC not explicitly considered as design basis accident)	Design basis accidents (DBA)	w/o significant fuel degradation	with core melt
NSC Volume 3. (operating units)					
DBC1 (normal operation)	Operational states considered as part of the design basis (DBC)			Design extension conditions (DEC)	
	DBC2 (anticipated operational events)	DBC4 (design basis incidents)		DEC1 (complex malfunctions without fuel melt)	DEC2 (serious accidents involving significant fuel melt)

Correlation between DiD levels and allocation of events/PIEs

IAEA SSR 2/1		Operational States (OS)		Accident Conditions (AC)			
		Normal Operation	Anticipated operational occurrences	Design basis accidents (DBA)		Design Extension Conditions	
						(without significant fuel degradation)	Severe accidents (with core melting)
WENRA	DiD Level 1	Prevention of Abnormal operation and failure					
	DiD Level 2		Control of Abnormal operation and failure				
	DiD Level 3.a			Control of accident to limit radiological releases and prevent escalation to core...			
	DiD Level 3.b					...damage conditions	
	DiD Level 4					Control of accidents with core melt to limit offsite releases	
	DiD Level 5						
Design Base Conditions / Design Extension Conditions	DBC-1	DBC-2	DBC-3	DBC-4		DEC-A	DEC-B
	Transients related to normal operation	Anticipated operational occurrences	Infrequent accidents	Limiting accidents (higher frequency) (lower frequency)		Reduction of risk and prevention of core meltdown	Reduction of risk and control of core meltdown
Frequency	Each event in this category is expected to occur frequently or regularly during operation	Each PIE in this category should be expected to occur one or a few times during plant lifetime	No individual PIE in this category is expected to occur during the plant lifetime, but one or a few PIE within this category should be expected during plant lifetime	PIEs in this category are considered to be possible but are believed to be excluded by the design. Nevertheless, they are considered on order to understand the radiological consequences of limiting accidents		PIEs in this category are not considered to be sufficiently credible to include as design basis events but are nevertheless considered in the design process in order to ensure radioactive releases are kept within acceptable limits should they occur.	
	f > 1/a	f < 10 ⁻¹	10 ⁻² /a < f < 10 ⁻³ /a	f < 10 ⁻³ /a		10 ⁻⁴ /a < f < 10 ⁻⁶ /a	CDF < 10 ⁻⁵ /a; LRF < 5 * 10 ⁻⁷ /a

Source: Safety Classification for I&C Systems in Nuclear Power Plants – Current Status & Difficulties – CORDEL Digital Instrumentation & Control Task Force

Design for reliability of I&C systems important to safety

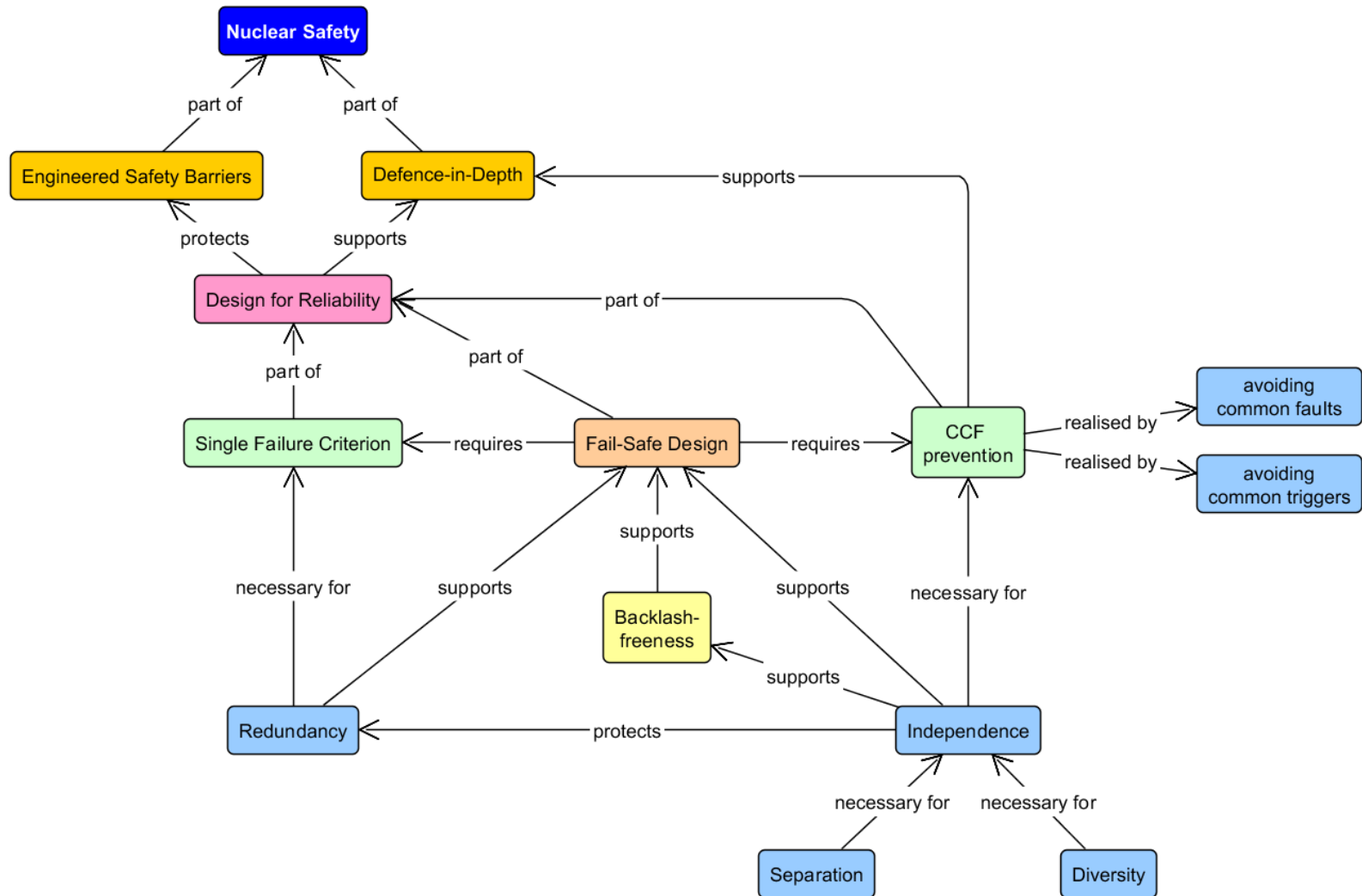
Necessary to prevent undue challenges to the integrity of the plant physical barriers, and to ensure the reliability of engineered protective systems.

- 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.

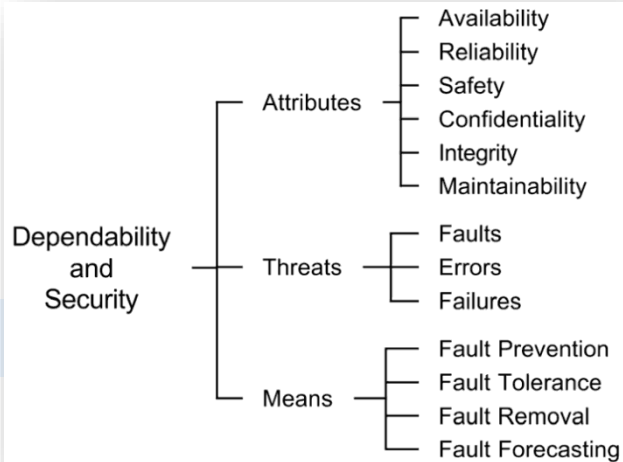
Design for reliability of I&C systems important to safety

- **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 	 <pre> graph LR A[Dependability and Security] --- B[Attributes] A --- C[Threats] A --- D[Means] B --- B1[Availability] B --- B2[Reliability] B --- B3[Safety] B --- B4[Confidentiality] B --- B5[Integrity] B --- B6[Maintainability] C --- C1[Faults] C --- C2[Errors] C --- C3[Failures] D --- D1[Fault Prevention] D --- D2[Fault Tolerance] D --- D3[Fault Removal] D --- D4[Fault Forecasting] </pre>

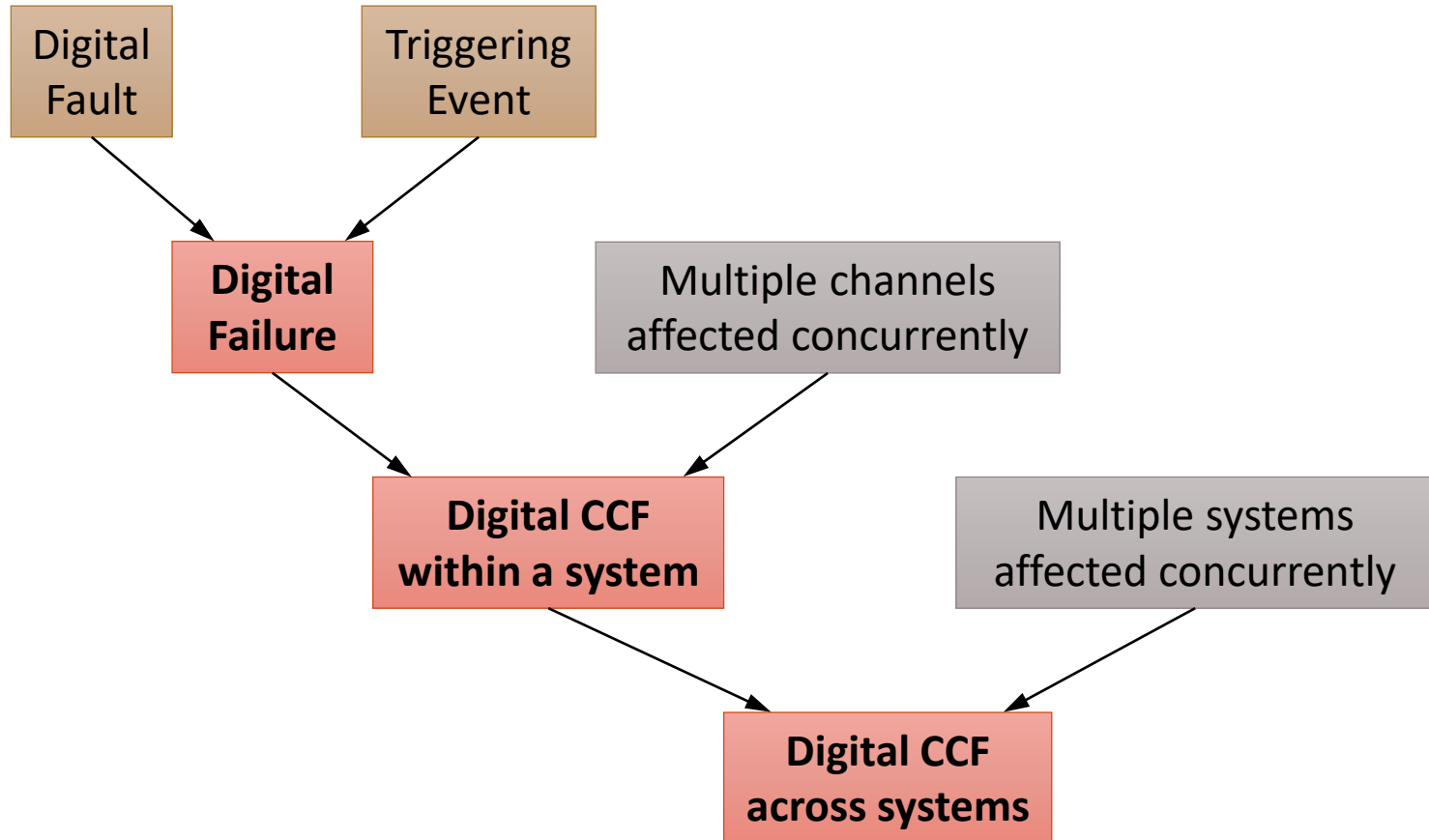
Fail-safe design

Definition and Comments	Relationships	Conformance
<p>The concept of fail-safe design shall be incorporated, as appropriate, into the design of systems and components important to safety.</p>	<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
<p>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>	<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>Means</p> <ul style="list-style-type: none"> • Independence • Diversity 	<p>Origin</p> <ul style="list-style-type: none"> • Human error • (Common) dependence • Environmental <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> <ul 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

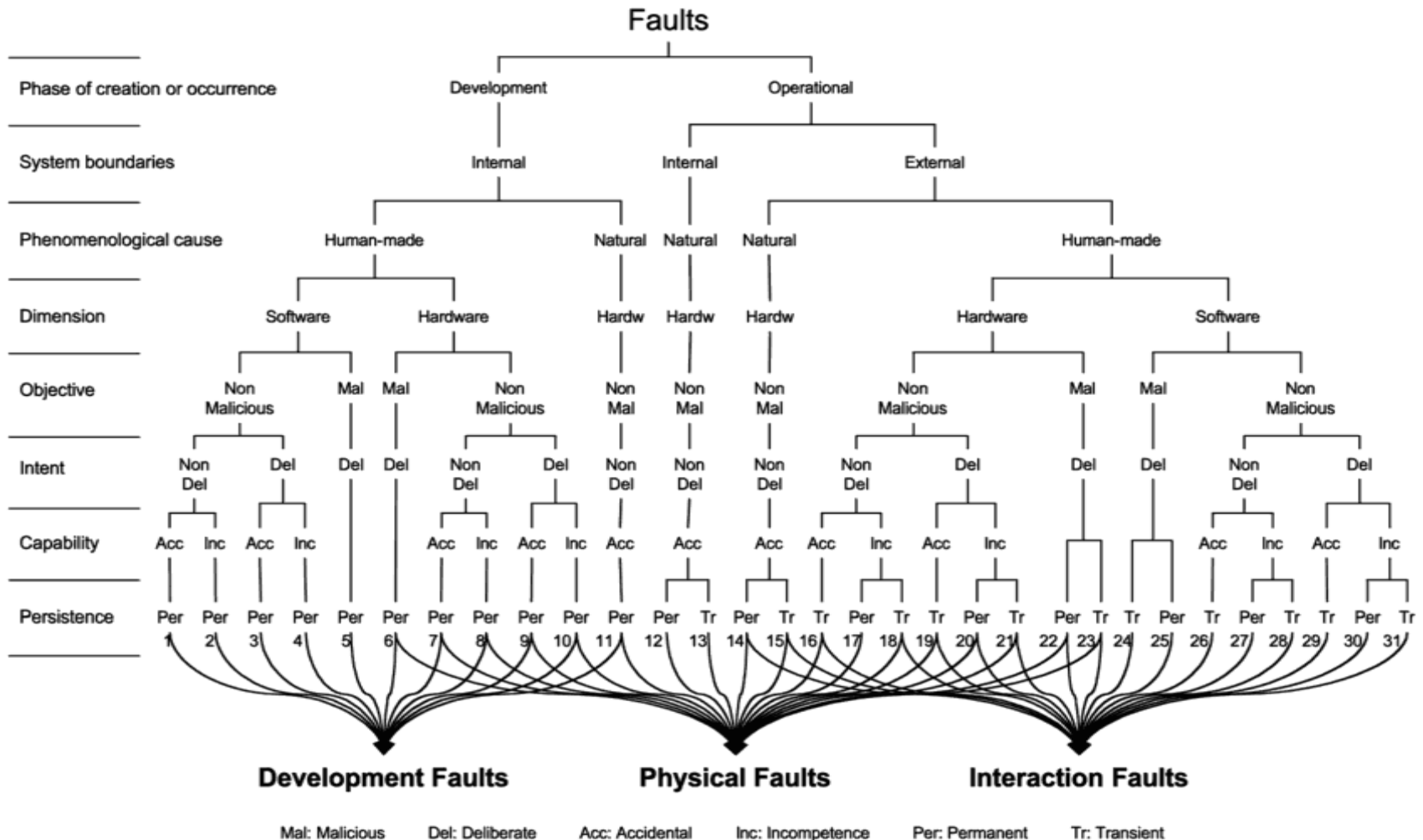
Supported by

- Deterministic safety assessment

Applies to

Systems important to safety

Classification of Faults



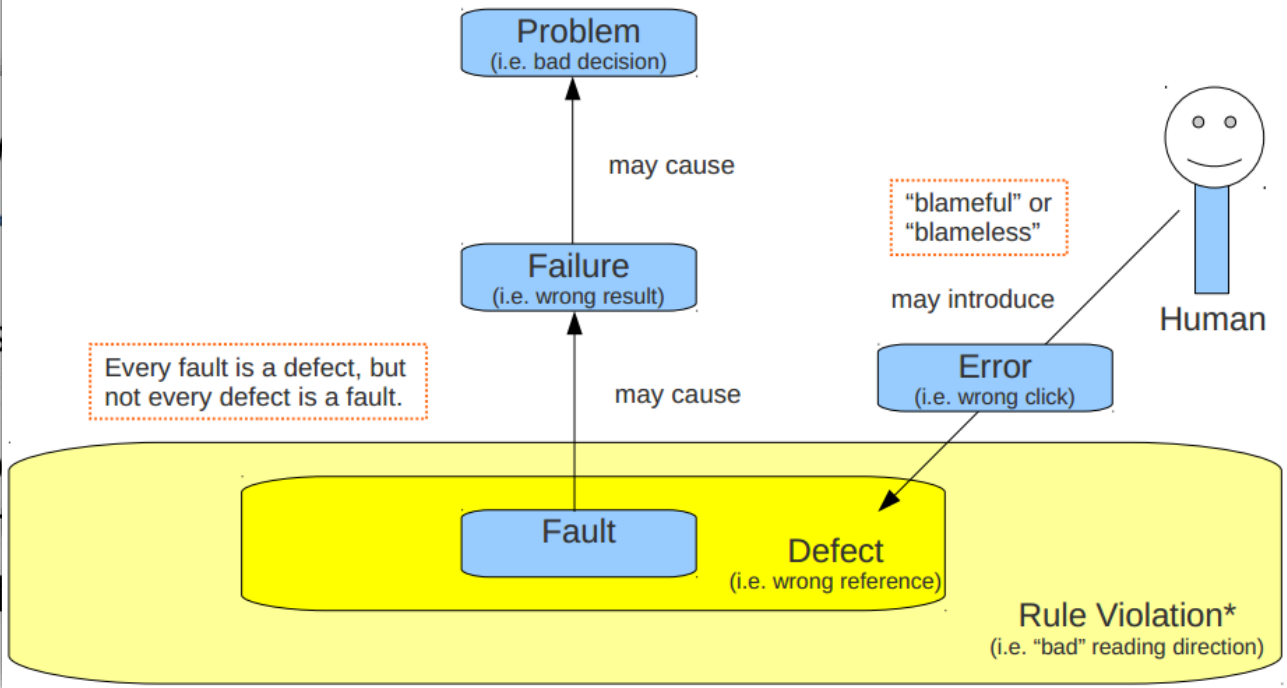
Fault – Error – Failure – Problem

(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

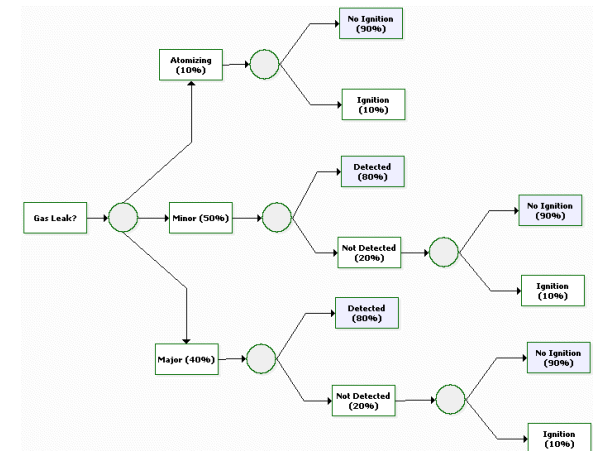
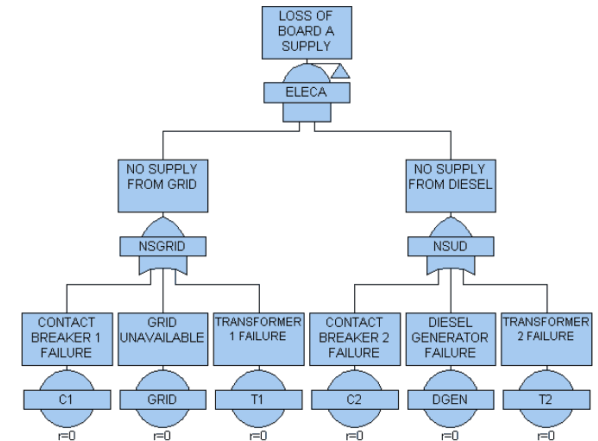
Relationships

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

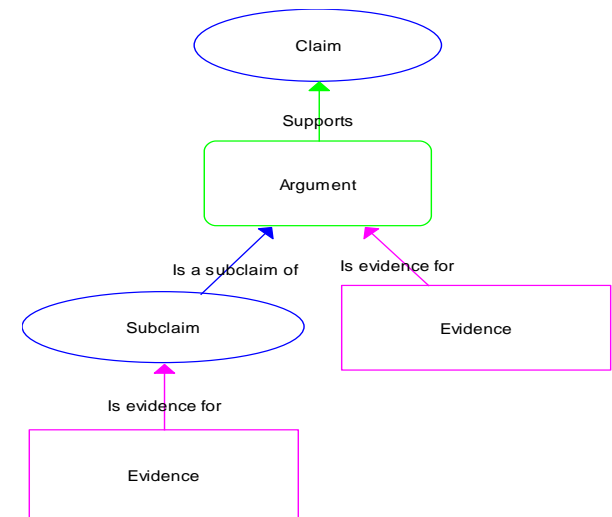
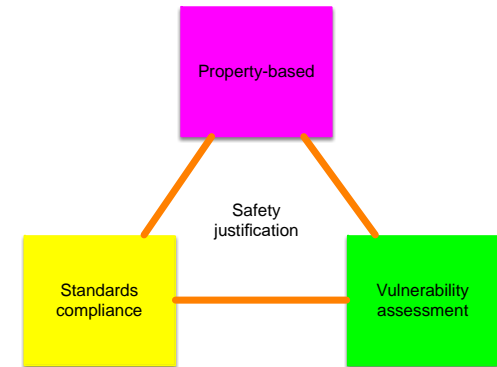
Types of claims

- 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