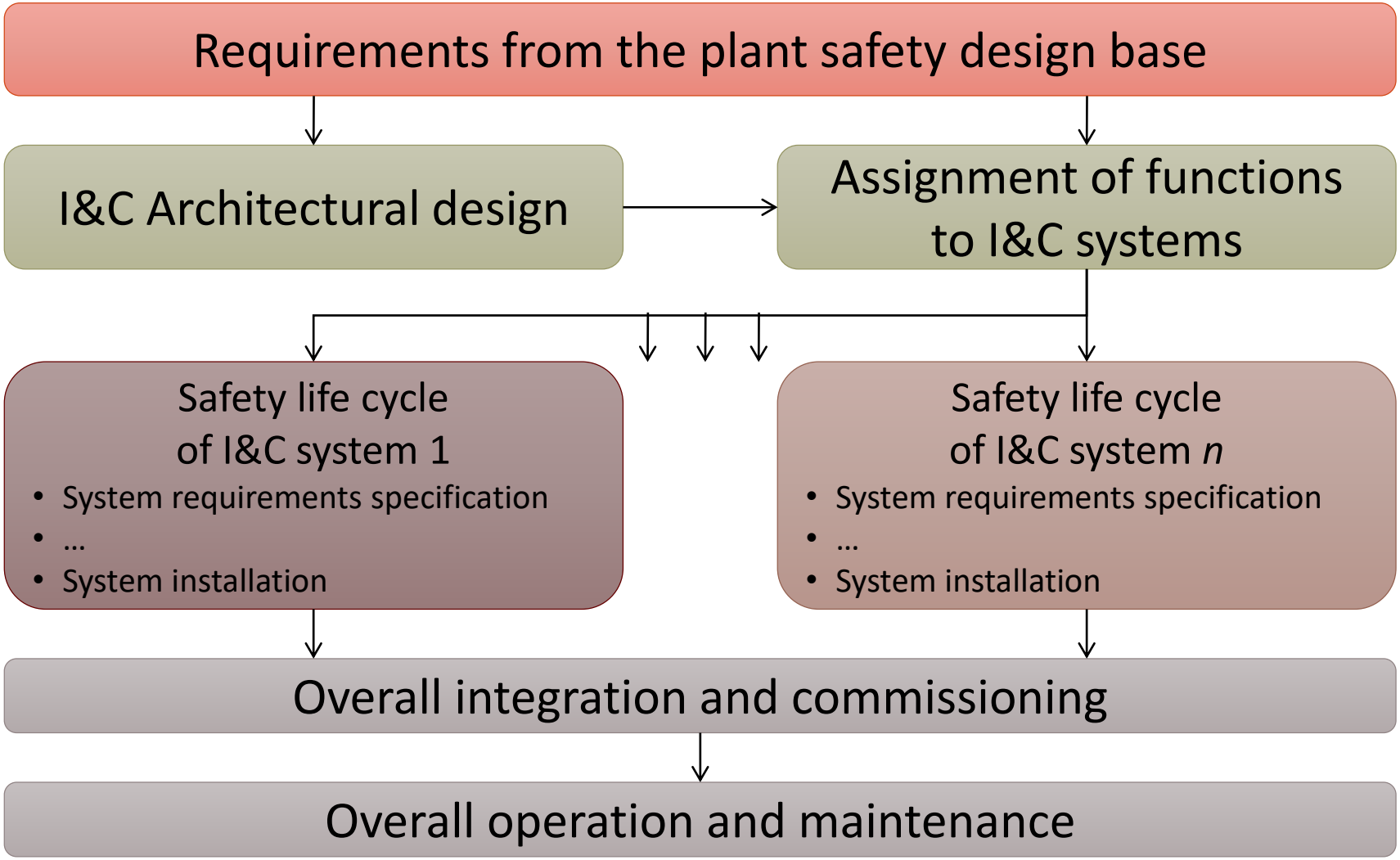
Budapest University of Technology and Economics
Faculty of Transportation Engineering and Vehicle Engineering
Department of Control for Transportation and Vehicle Systems

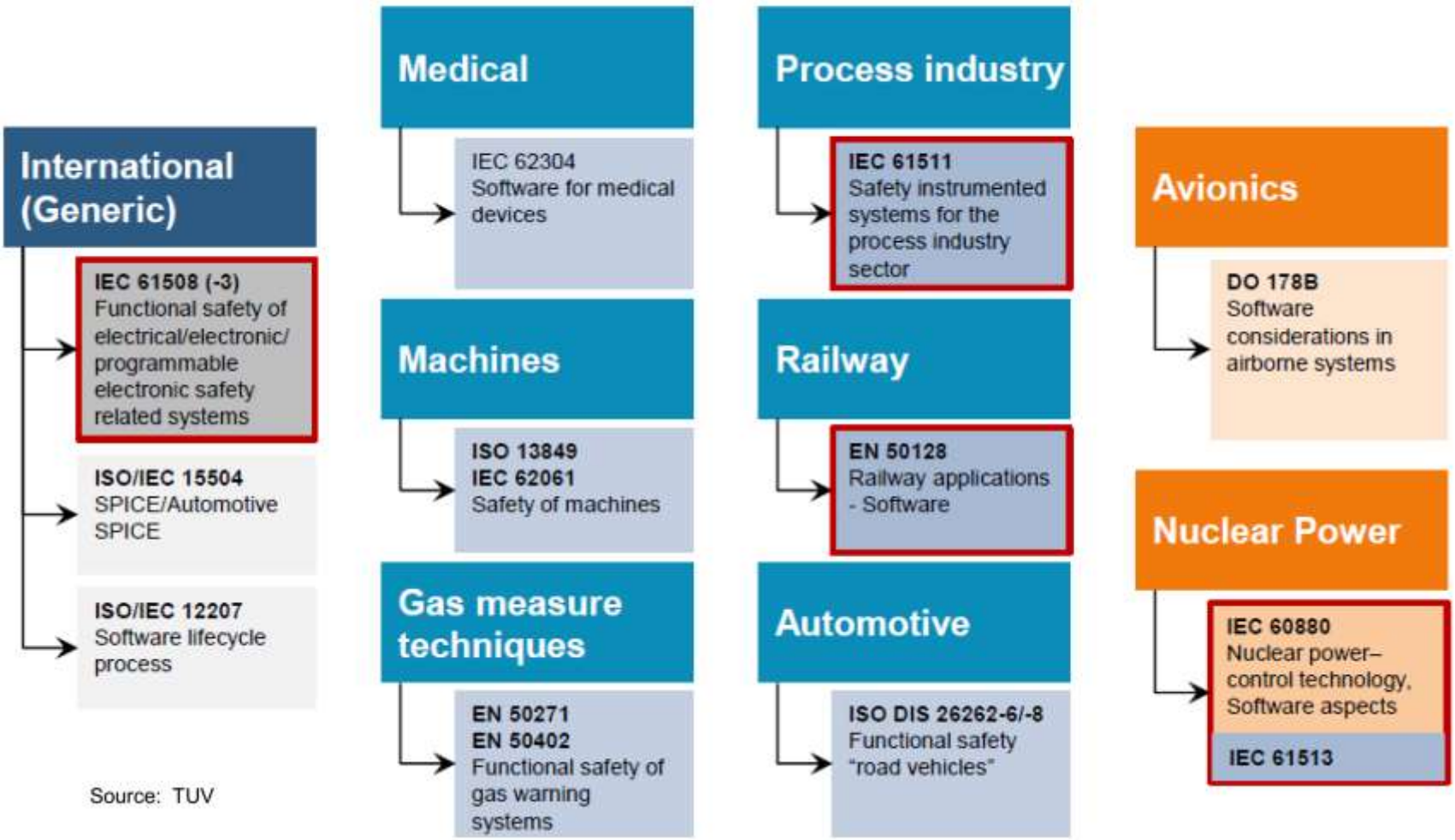
Nuclear I&C Design

Design Process and Requirements of Nuclear Instrumentation and Control Systems

Simplified I&C Safety Life-Cycle



Safety Standards for Different Fields



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

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

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

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

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.

Overall Requirements: IEC Class 1

- Single (random) failure criterion
  - robustness with respect to errors
- Low complexity
  - defensive design against CCF
- Deterministic behavior for computer-based systems:
  - cyclic behavior
  - preferably stateless behavior
  - load independent of external conditions
  - static resource allocation
  - guaranteed response times
- Software developed according to stringent nuclear industry standards (e.g. IEC 60880)

Overall Requirements - Class 2

- Controlled complexity
- Confidence based in particular on analysis of system design
- High quality software
  - IEC 61238 is usually required for new development
  - not necessarily developed according to nuclear industry standards (e.g. pre-developed software)

Overall Requirements - Class 3

- No specific limit for complexity
- Confidence mainly based on:
  - proven application of quality standards
  - global demonstration of fitness
- Specific demonstrations may be required on identified topics

Consistency with System-Level Constraints

- Predictable behavior (Classes 1 & 2):
  - precise specification of component behavior
  - documented conditions of use in system
- Deterministic behavior (Class 1):
  - static resource allocation
  - static parameterization
  - preferably stateless behavior
  - clear-box (with limited exceptions)
  - proven maximum response time
  - proven robustness against consequences of errors