Status of IEC 62566-2 and V&V experiences

TÜV-Rheinland ISTec GmbH, October 2019

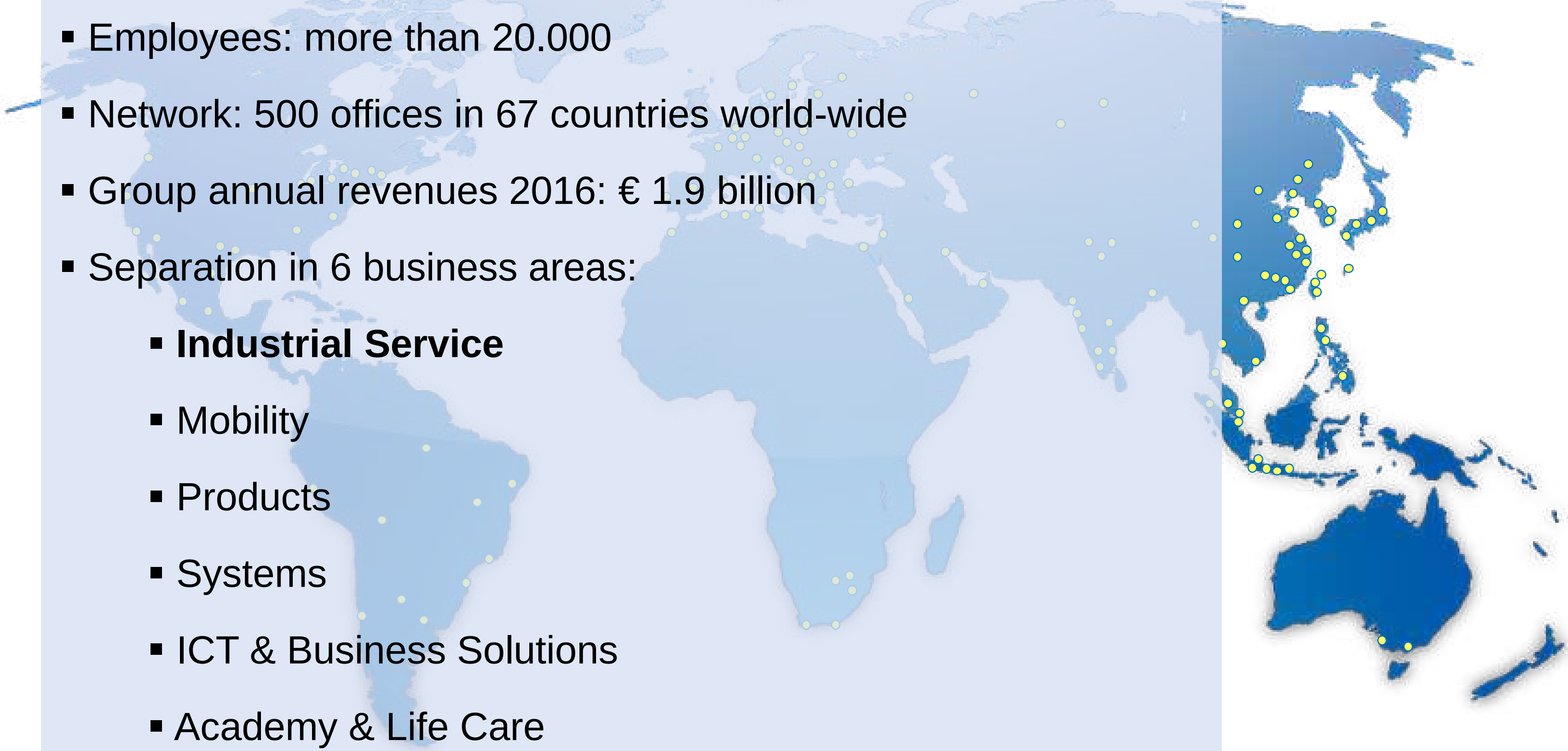
Foto: shutterstock, Robert Caucino

TÜVRheinland®
Genau. Richtig.

Content

- TR - Industrial Services and Responsibilities
- Current state of revised nuclear IEC Standards
- IEC 62566-2 : Class 2 and 3 HPD requirements – some fundamental decisions
- Technical background, main issues and organisation of the Standard
- Life cycle according IEC 62566-2 for HDP
- Overview of the chapters of IEC 62566-2
- Post-route simulation/analysis

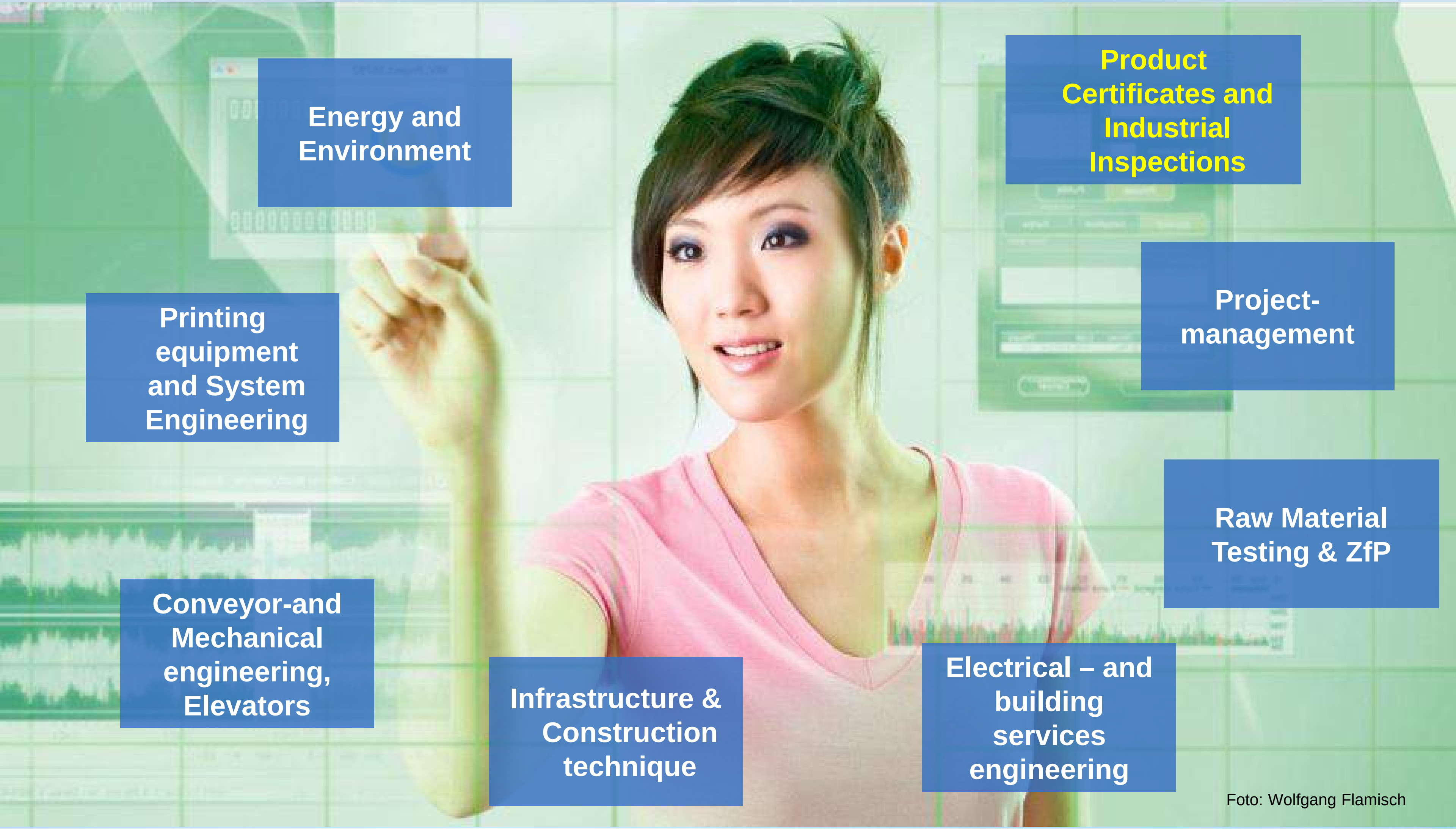
TÜV-Rheinland - Overview



- A leading provider of test, inspection and conformity services worldwide
- Founded in 1872 and headquartered in Cologne (Germany)
- Employees: more than 20.000
- Network: 500 offices in 67 countries world-wide
- Group annual revenues 2016: € 1.9 billion
- Separation in 6 business areas:
  - **Industrial Service**
  - Mobility
  - Products
  - Systems
  - ICT & Business Solutions
  - Academy & Life Care

TÜVRheinland®
Genau. Richtig.

Business segments of the Industrial Service



Energy and Environment

Product Certificates and Industrial Inspections

Printing equipment and System Engineering

Project-management

Raw Material Testing & ZfP

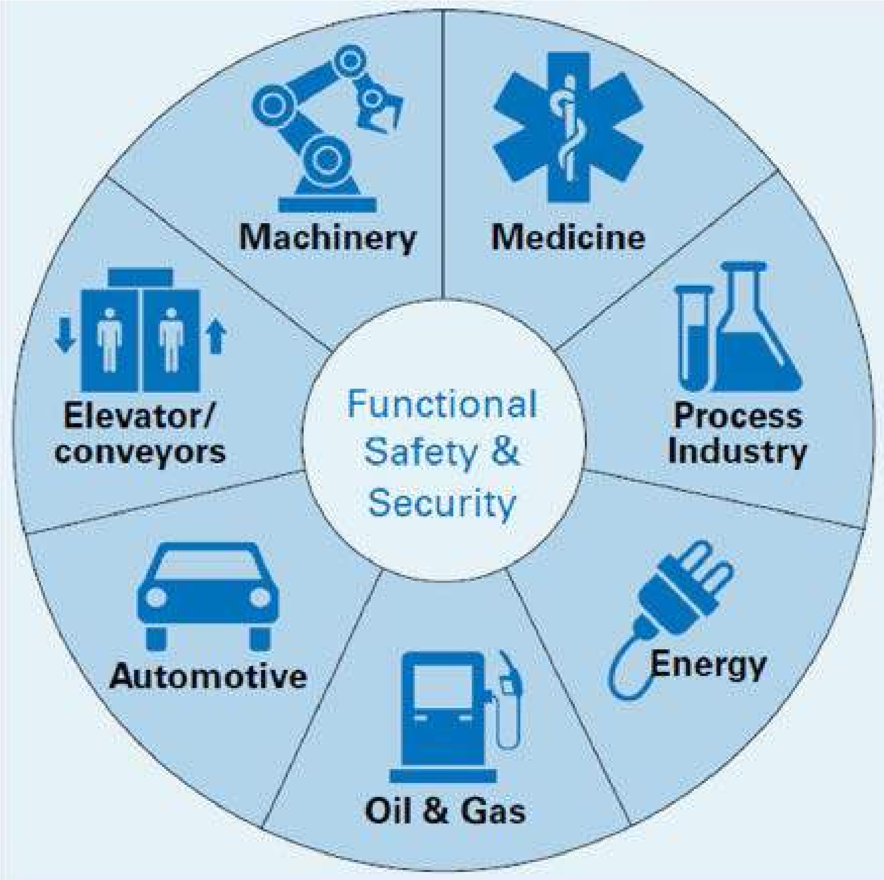
Conveyor-and Mechanical engineering, Elevators

Infrastructure & Construction technique

Electrical – and building services engineering

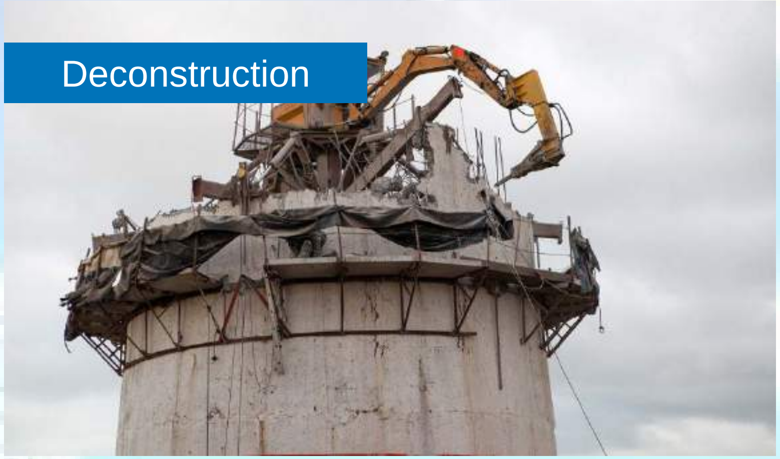
Foto: Wolfgang Flamisch

Functional Safety and Cyber Security



Responsibilities – Power Generation and Nuclear Energy

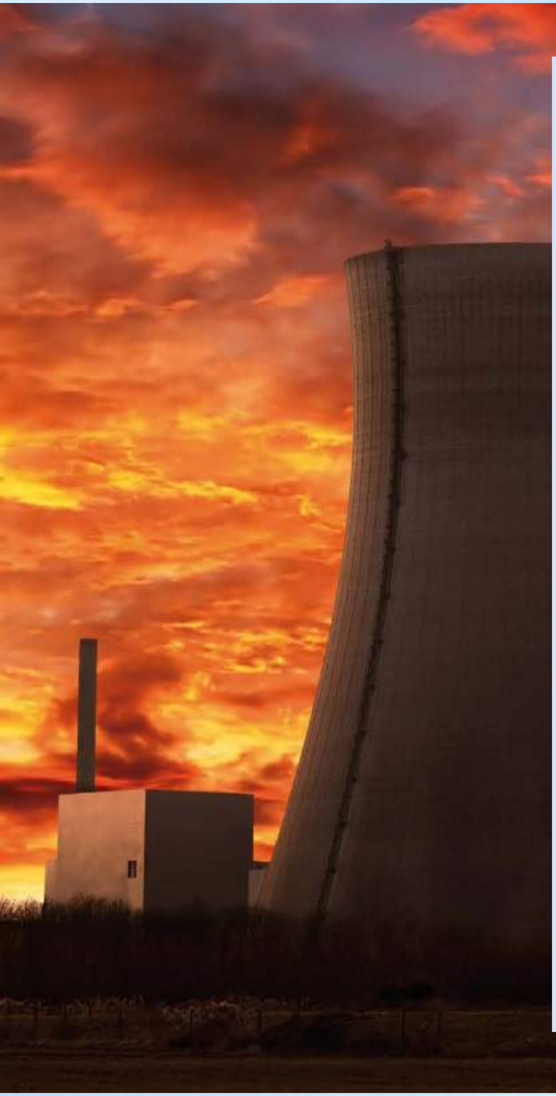
Nuclear Energy



Deconstruction

Radiation Protection

Nuclear Project Experiences - I&C / Functional Safety



Services and Products:

- Type Approvals with optional certification
- Hardware, Software and System Tests
- Environmental Laboratory Testing (Temperature, Climate, Mechanical Strength, EMV, etc.)
- Analysis of the safety and reliability levels
- Software Review (User Software, Compiler)
- Quality Assurance during design
- In-house Trainings and Workshops Functional Safety Engineer, Training Program
- Development of automatic test devices and check routine programs
- Quality assurance during system implementation
- **International standard and regulation work**

Foto: Fotolia, Smileus

Current state of revised nuclear IEC Standards

IEC 62566-2 Ed.1.0 -, Nuclear power plants - Instrumentation and control systems important to safety - Development of HDL-programmed integrated circuits - Part 2: HDL-programmed integrated circuits for systems performing category B or C functions

- Currently CDV-Status
- Intermediate meeting in Lyon (Spring 2018)
- EN (CENELEC) Standard could be expected in Dec 2021
- FDIS will be circulated to National Committees for approval in November 2019
- Structure is similar to IEC62566 and IEC 62138 (IEC 62138 is conform to IEC 60880),

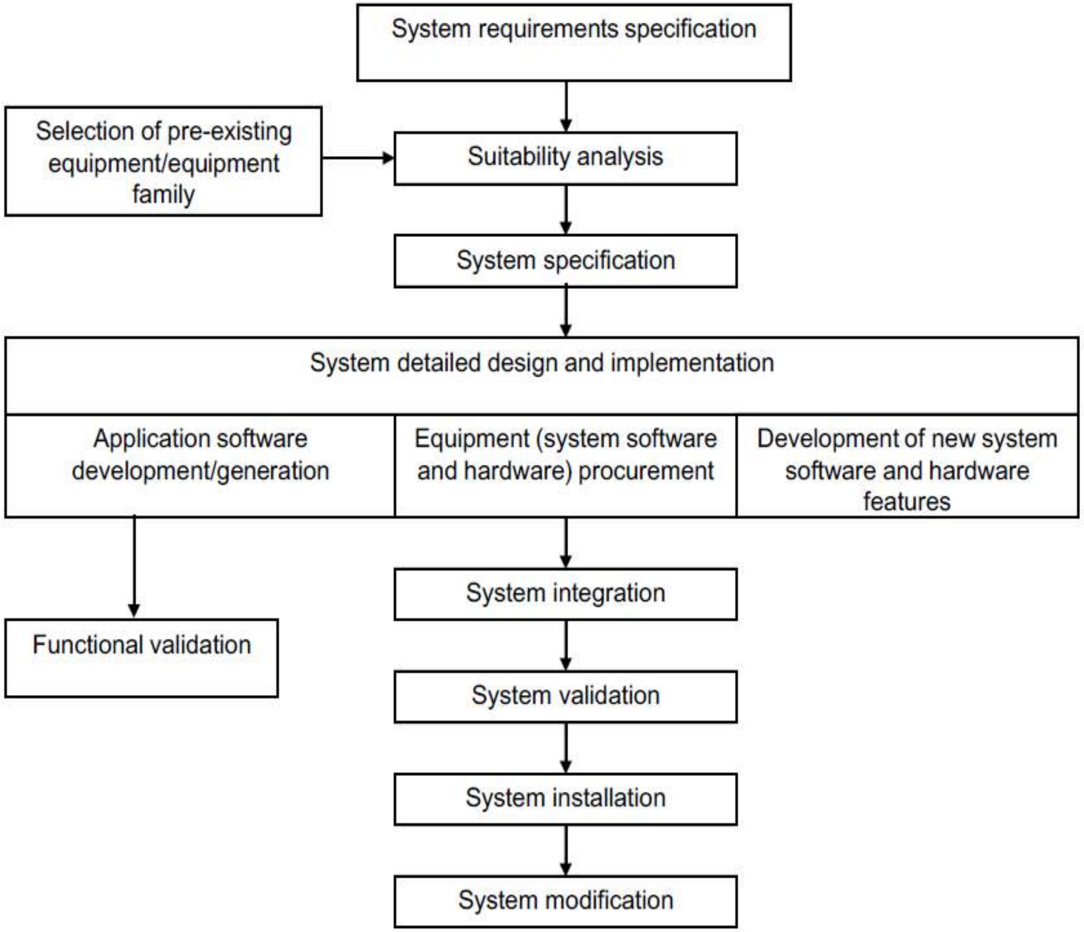
IEC 62566-2 : Class 2 and 3 HPD requirements – some fundamental decisions

- **Conservation of the structure of IEC 62566**
  - This ensures that the difference in severity of requirements is clear and also that a structure oriented around the specificities of the HPD development process are maintained.
- **Coherence with IEC 62138 in terms of requirement severity**
  - This ensures that the severity of requirements does not impact the technological choices made by the developer.
- **Introduction of graduation principles as per IEC 62138**
  - To provide coherent and appropriate differentiation between class 2 and 3 compared to software standards.
- **Reference to IEC 61513 and IEC 62138 for general requirements which are independent of the technological specificities of HPD developments (quality assurance, project management etc.)**
  - IEC rules dictate that when requirements are taken from other standards, they should be referenced instead of copied.

Technical background, main issues and organisation of the Standard

The system life-cycle of IEC 61513 is complemented in

- IEC 60880 (for category A functions),
- IEC 62138 (for category B and C functions) for software development;
- IEC 62566 (for category A functions),
- **IEC 62566-2 (for category B and C functions) for HPD development;**
- IEC 60987 for hardware development of class 1 and 2 computer-based systems. (next revision will also cover class 3)


System requirements specification
Selection of pre-existing equipment/equipment family
Suitability analysis
System specification
System detailed design and implementation
Application software development/generation
Equipment (system software and hardware) procurement
Development of new system software and hardware features
Functional validation
System integration
System validation
System installation
System modification

Technical background, main issues and organisation of the Standard

- Electronic systems performing category B and C functions (according to IEC 61226) used in nuclear power plants need to be fully validated and qualified according to their safety class.
- The function of an integrated circuit such as FPGAs or similar technologies is not defined by the supplier of the physical component or micro-electronic technology but by the I&C designer.
- The specific integrated circuits addressed by this standard are:
  a) based on pre-developed micro-electronic technologies,
  b) developed within an I&C project,
  c) developed in Hardware Description Languages (HDL) by using appropriate and compatible development tools
- This standard provides requirements for the development of class 2 or 3 HDL programmed devices performing category B or C functions as defined by IEC 61226.
- It complements IEC 62566 which provides requirements for the development of HDL-Programmed Devices (HPDs) performing category A functions.

Technical background, main issues and organisation of the Standard

This standard does not put requirements on the development of the micro-electronic technologies, which are usually available as "commercial off-the-shelf" items and are not developed under nuclear quality assurance standards.

The standard addresses the developments made with these micro-electronic technologies in an I&C project with HDLs and related tools.

It provides guidance to avoid as far as possible latent faults remaining in HPDs, and to reduce the susceptibility to single failures as well as to potential Common Cause Failures (CCFs).

The standard provides therefore requirements on:

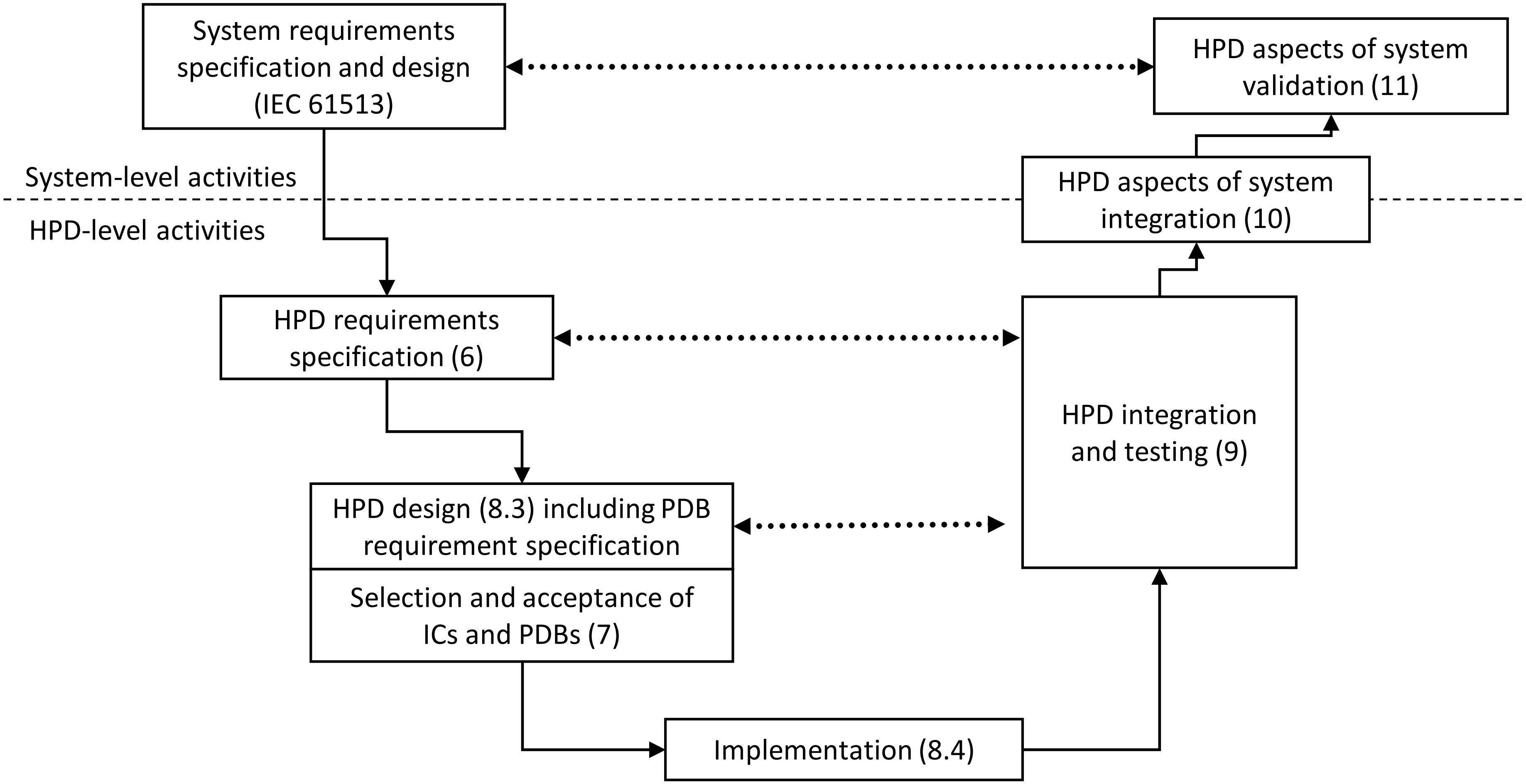
a) a dedicated HPD life-cycle addressing each phase of the development of HPDs, including specification of requirements, design, implementation, integration and validation, as well as verification activities associated with each phase,

b) planning and complementary activities such as modification and production,

c) selection of pre-developed components. This includes micro-electronic technologies and Pre-Developed Blocks (PDBs),

d) tools used to design, implement and verify HPDs.

Life cycle according IEC 62566-2 for HDP



System requirements specification and design (IEC 61513)

HPD aspects of system validation (11)

System-level activities

HPD-level activities

HPD aspects of system integration (10)

HPD requirements specification (6)

HPD integration and testing (9)

HPD design (8.3) including PDB requirement specification

Selection and acceptance of ICs and PDBs (7)

Implementation (8.4)

Overview of the chapters of IEC 62566-2

Introduction chapters are the general IEC chapters.

§5 General requirements for HPD projects

- The clause first places the HPD within the context of the I&C system as described by IEC 61513. Then it describes the HPD life-cycle which structures the HPD project. Finally it provides requirements for HPD projects, for quality assurance and for configuration management, many of which are common with those of software development processes and are taken from IEC 62138 and which are supplemented by HPD specific requirements if needed.

§6 HPD requirements specification

- The clause completes and adds precision to the requirements of IEC 61513 related to the requirement specification of HPD in general, for functional aspects, fault detection, fault tolerance, and Electronic System Level tools.

§7 Acceptance process for programmable integrated circuits, native blocks and Pre-Developed Blocks

- The clause described the acceptance process for blank programmable integrated circuits and their included native blocks related to functional suitability, documentation for safety, complementary means, rules of use, and modification for acceptance.

Overview of the chapters of IEC 62566-2

§8 HPD design and implementation

-The clause provides requirements and recommendations based on good practice for design and implementation to meet appropriate safety features such as fault-free as possible and amenability to verification. It contains requirements related to the HDL, the related tools, the design, the implementation, and the system level tools and automated code generation

§9 HPD integration and testing

-In this clause requirements of the HPD integration and testing related test-benches for HPD functional simulation, test coverage, and test execution are presented. The HPD integration and testing described by the clause is completely distinct from the HPD aspects of system-level integration and validation described by clauses 10 and 11.

§10 HPD aspects of system integration

- The present clause complements subclauses 6.2.5, 6.3.4 and 6.4.5 of IEC 61513:2011 by providing additional requirements specific, or of particular importance, to HPDs related to the system integration.

Overview of the chapters of IEC 62566-2

§11 HPD aspects of system validation

- The present clause complements 6.2.6, 6.3.5 and 6.4.6 of IEC 61513:2011 by providing additional requirements specific, or of particular importance, to HPDs related to the system validation.

§12 Modification

-The HPD modification is subject to the requirements of 6.2.8 and 6.4.7 of IEC 61513:2011. The present clause provides additional requirements specific, or of particular importance, to HPDs related to modification.

§13 HPD production

-This clause presents requirements to the production of HPDs. “Production” is designates as the final step before delivering the integrated circuit ready for use in the I&C system.

§14 HPD aspects of installation, commissioning and operation

- The present clause provides additional requirements specific, or of particular importance related to the installation of HPDs.

§15 Software tools for the development of HPDs

- This clause gives requirements for software tool which can aid or automate the development of HPDs.

Overview of the chapters of IEC 62566-2

§16 Design segmentation or partitioning

-This clause recognizes that it might be possible with specific design measures and partitioning of the HPD to ensure that auxiliary or support functions are independent of those of category B or C and cannot inappropriately interfere with them. In such cases requirements are provided in in this clause, else they shall be developed, implemented and verified according to the requirements of rest of this standard.

§17 Defences against HPD Common Cause Failure

-This clause provides links to requirements SC45A standards to minimise the potential for CCF.

§ Annex A Documentation

- This annex identifies typical documentation for each of the main clauses of this standard

§ Annex B Development of HPDs

- This annex gives additional information to ease the understanding of the corresponding clauses of this standard.

V&V experiences

Questions of clients of TÜV Rheinland:

Is the post-route simulation required or can it be covered by other verification measures?

Up to now

The post-route simulation was required for class 1.

For class 2 in the standard IEC 62566 there were no distinct requirements related to the post-route simulation and other verification measures.

Therefore, there was a kind of freedom regarding the verification of the integrated circuit such as FPGAs or similar technologies.

The TÜV Rheinland had always strongly recommended to do the post-route simulation and other verification measures (e.g. static timing analysis) for good practice.

V&V experiences

With the new standard IEC 62566

The post-route simulation is required for class 1 and 2 and recommended for class 3. Because other verification measures do not cover the full scope of verification that the P&R process took place correctly.

In addition:

The finite state machine analysis is required for class 2 and 1, recommended for class 3

and

The static timing analysis is required for class 2 and 1, recommended for class 3

Now the TÜV Rheinland has the basis to claim the prior strongly recommended verification measures.

Any questions or remarks?