Recent developments in IEC standards and the use of FPGAs at EDF

EDF
Nuclear Engineering and New Build Projects Division
Design and Technology Branch

Alexander Wigg CEng MIET
alexander-john.wigg@edf.fr

CHANGER L'ÉNERGIE ENSEMBLE

- Regulatory context
- RCC-E 2016
- New standard development
- Current and future work at EDF

CHANGER L'ÉNERGIE ENSEMBLE

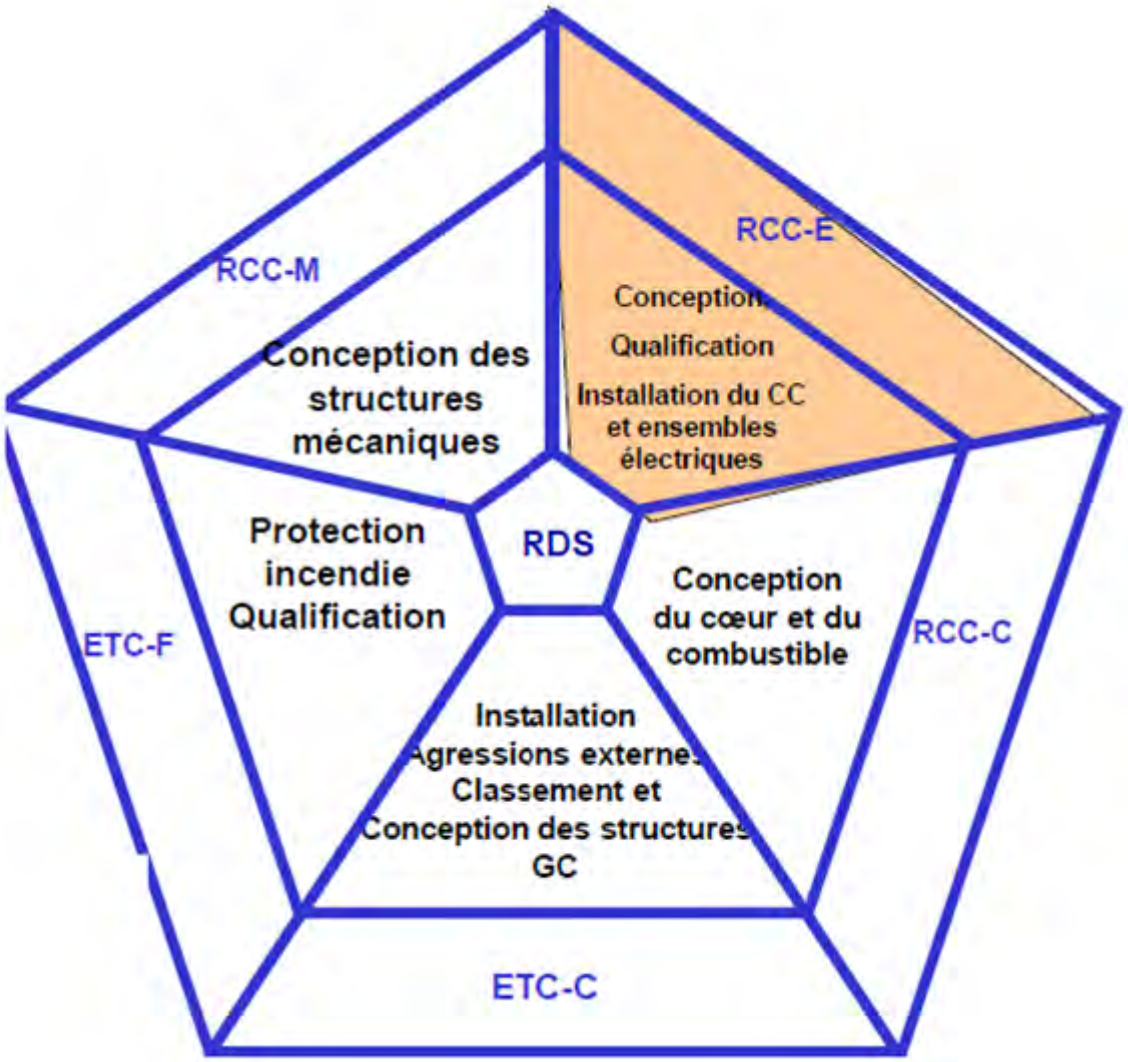
Regulatory context for HPD use

AFCEN : French Association for Design, Construction and Operational Rules for Nuclear Power Plants

RCC-E: Design and Construction Rules for Electrical Equipment of Nuclear Islands

Evaluated and approved by the French Regulator

Concerns the design, qualification and installation of electrical equipment.



RCC-E : Design and Construction Rules for Electrical and I&C Systems and Equipment

- History of the RCC-E, the *"Electrician's Rulebook"*:
  - First edition published in 1981,
  - Purpose : to set requirements for safety classified equipment through supplier contracts,
  - Takes into account industrial experience,
  - Completed with project-specific requirements,
  - Technological developments have been gradually taken into account through the introduction of chapters specific to digital I&C equipment.

RCC-E 2016 : Design and Construction Rules for Electrical and I&C Systems and Equipment

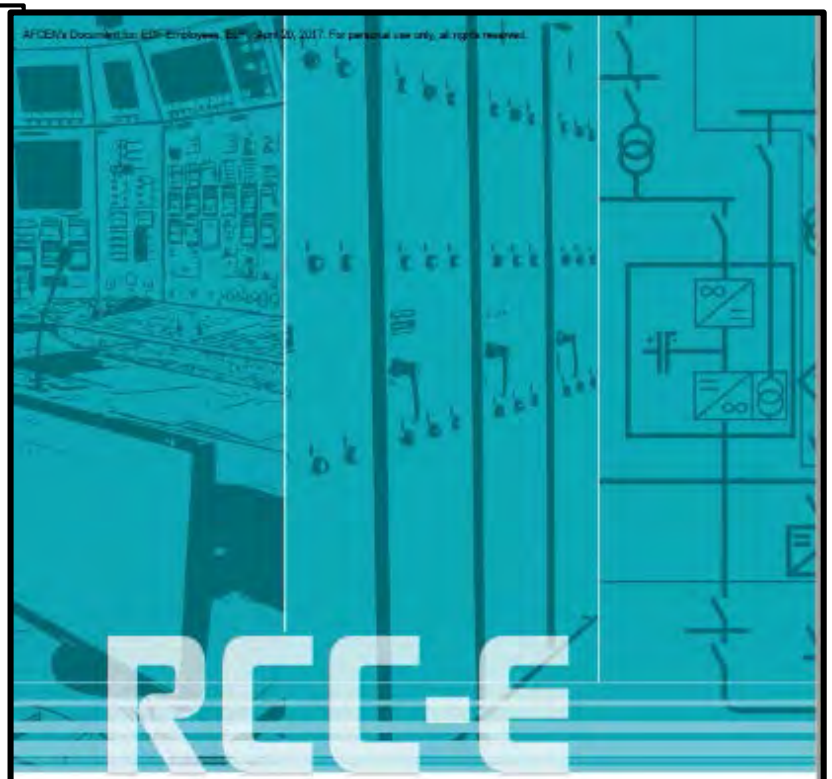
DESIGN AND CONSTRUCTION RULES
FOR ELECTRICAL AND I&C SYSTEMS AND
EQUIPMENT

RCC-E

French Association
for design, construction and in-service inspection rules
for nuclear island components

afcen

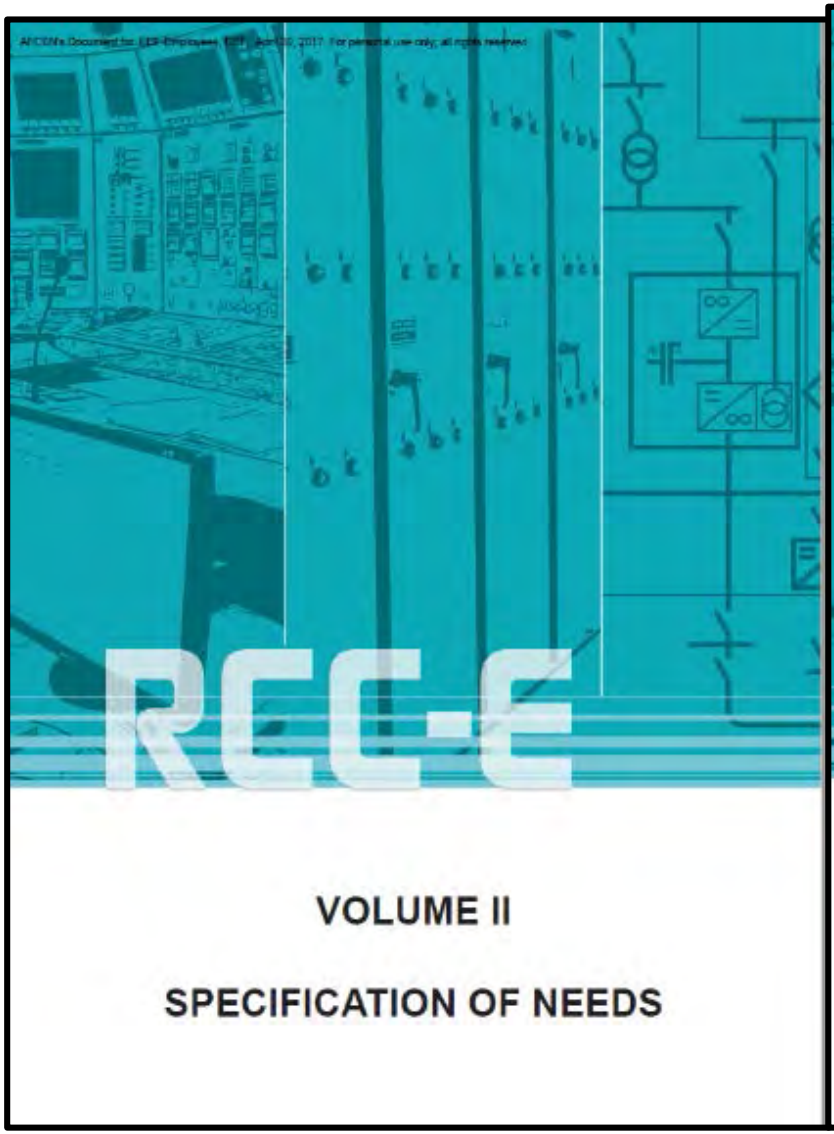
December 2016 Edition

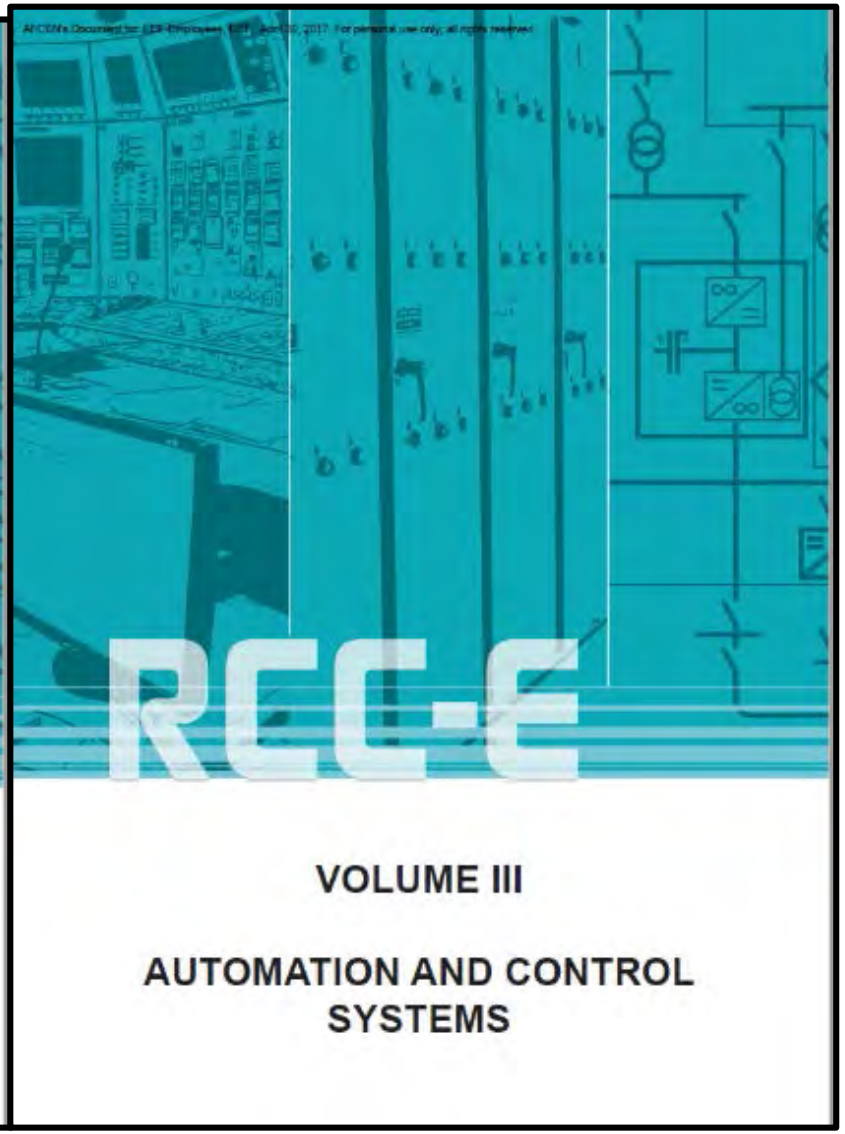


VOLUME I

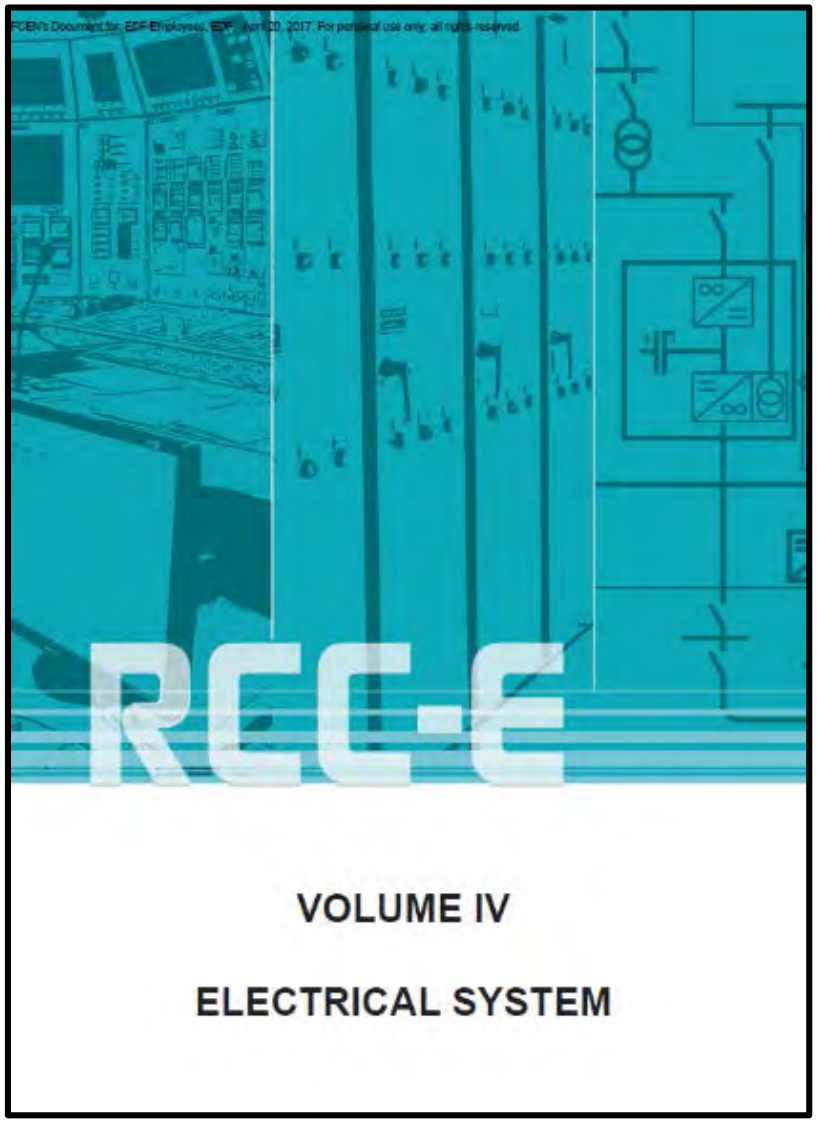
GENERAL AND QUALITY
ASSURANCE

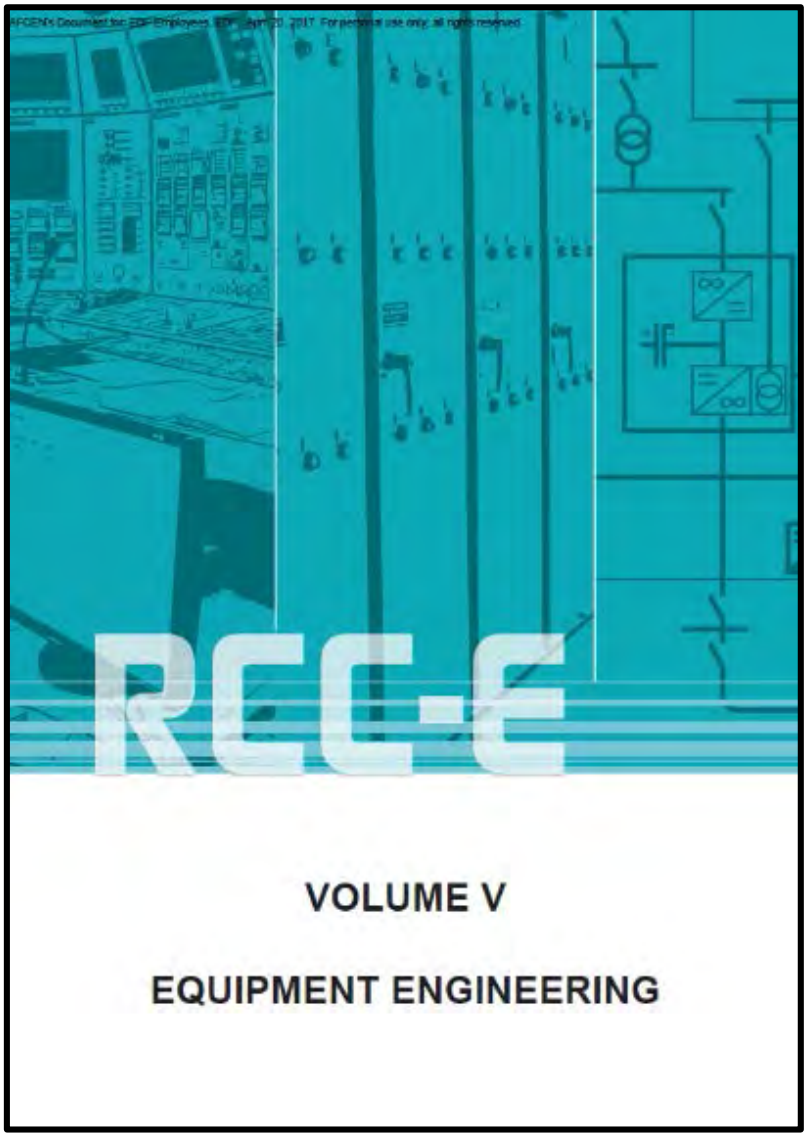
RCC-E 2016 : Design and Construction Rules for Electrical and I&C Systems and Equipment



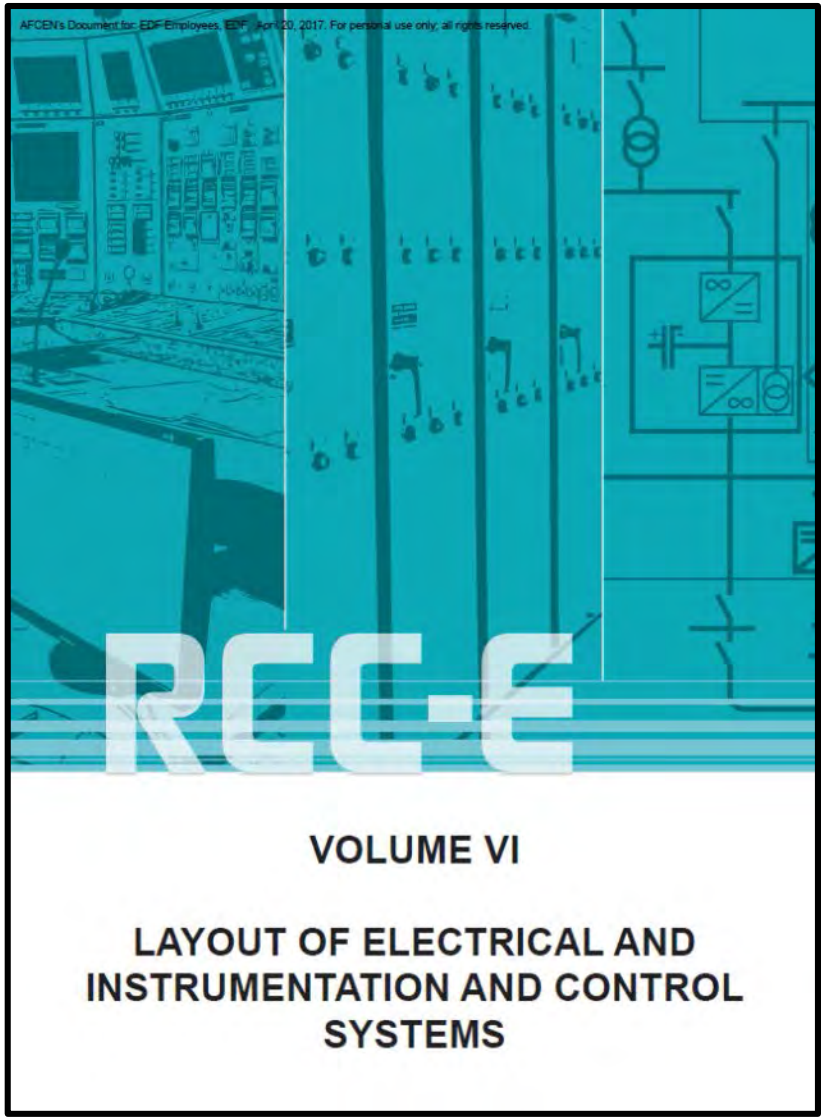


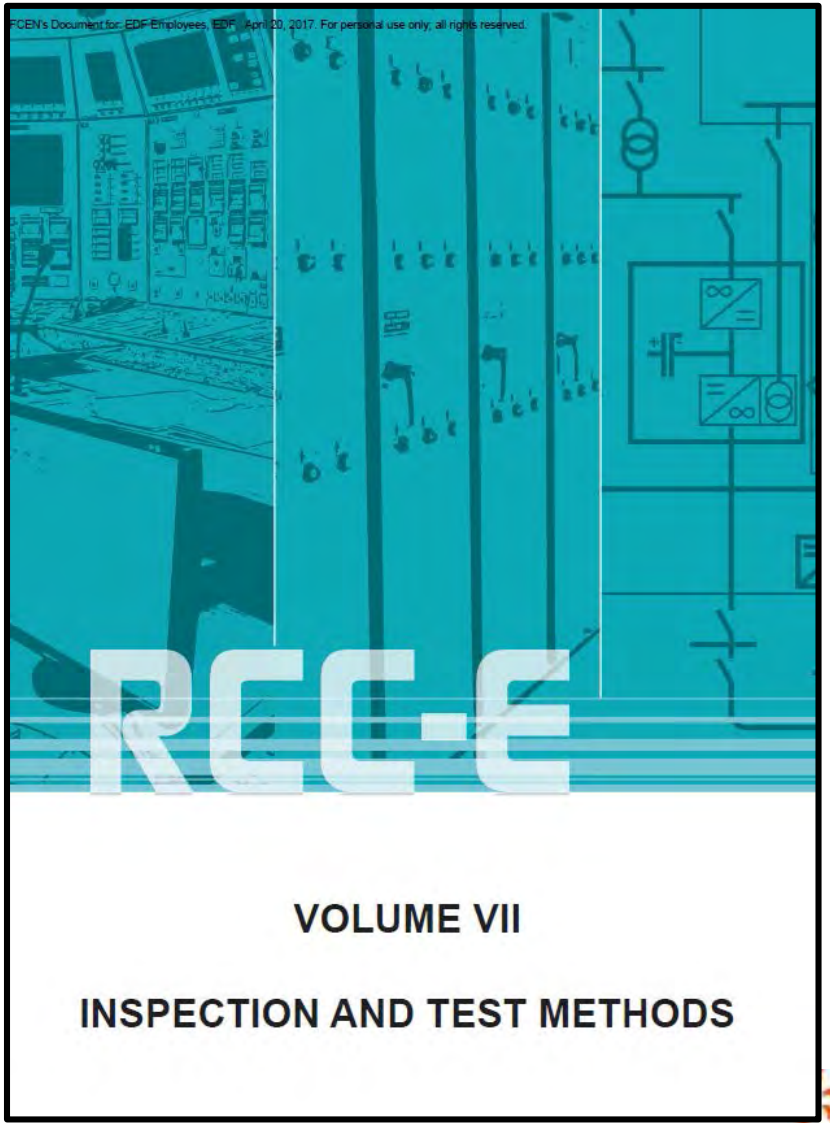
RCC-E 2016 : Design and Construction Rules for Electrical and I&C Systems and Equipment



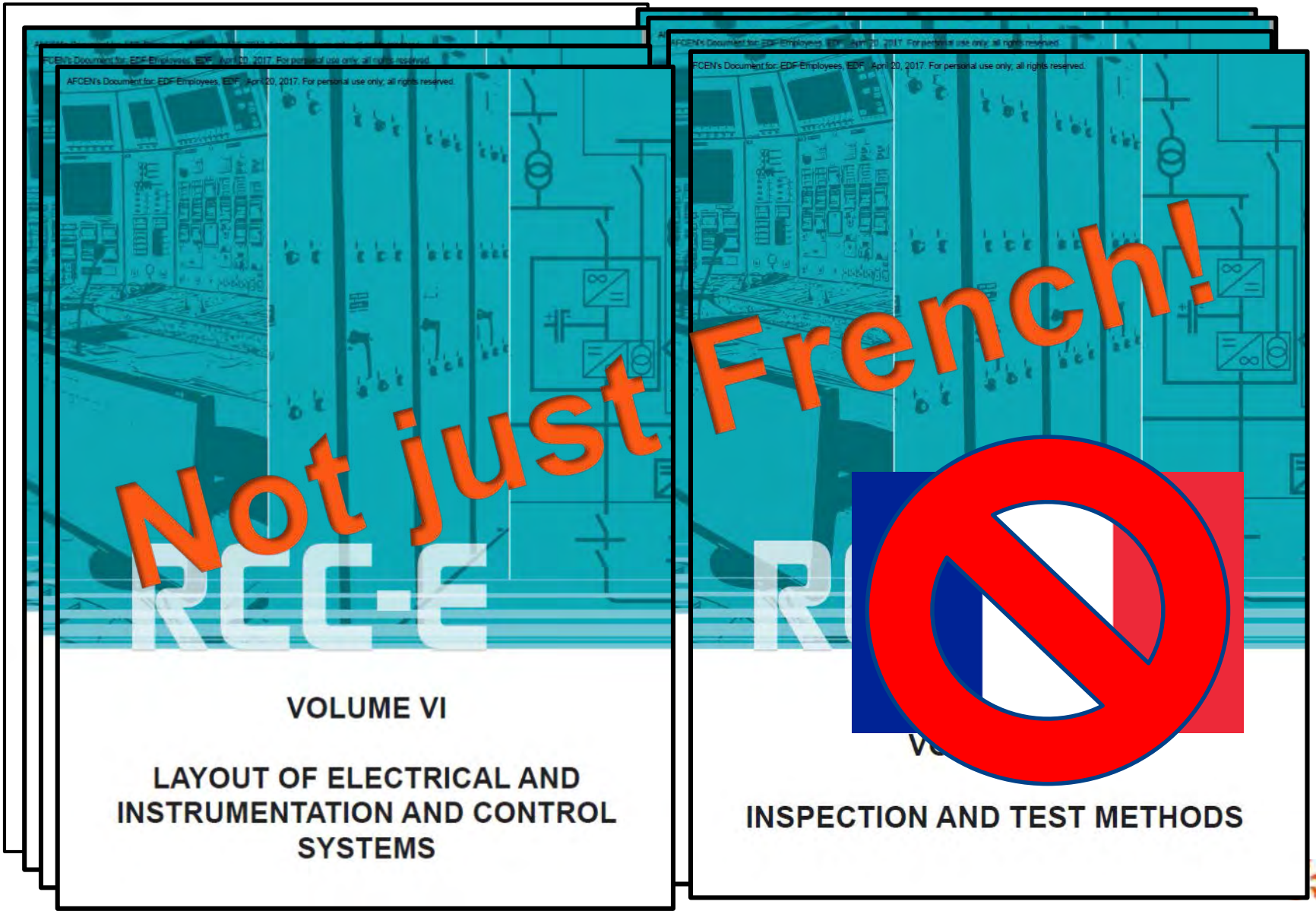


RCC-E 2016 : Design and Construction Rules for Electrical and I&C Systems and Equipment





RCC-E 2016 : Design and Construction Rules for Electrical and I&C Systems and Equipment



RCC-E 2016 : Volume III – Automation and Control Systems

Overall automation and control architecture : Part B excluding §6

Automation and control system *n* : Part B §6

Topic		System classification		
		Class 1	Class 2	Class 3
Hardware	New	Part C excluding§ 6.8		Part D
	Pre-existing	Part C excluding§ 6.2 à § 6.7		
Software	New	Part E	Part F § 6 excluding§ 6.2	Part F § 5 excluding§ 5.2
	Pre-existing	Same requirements as for new software	Part F § 6.2	Part F § 5.2
HPD (FPGA, CPLD etc.)	New	Part G excluding§ 7	Requirements defined in the Book of Project Data	
	Pre-existing	Part G § 7		

System n out of N systems in total

Reference to IEC 62566(-1) with amendments and precisions

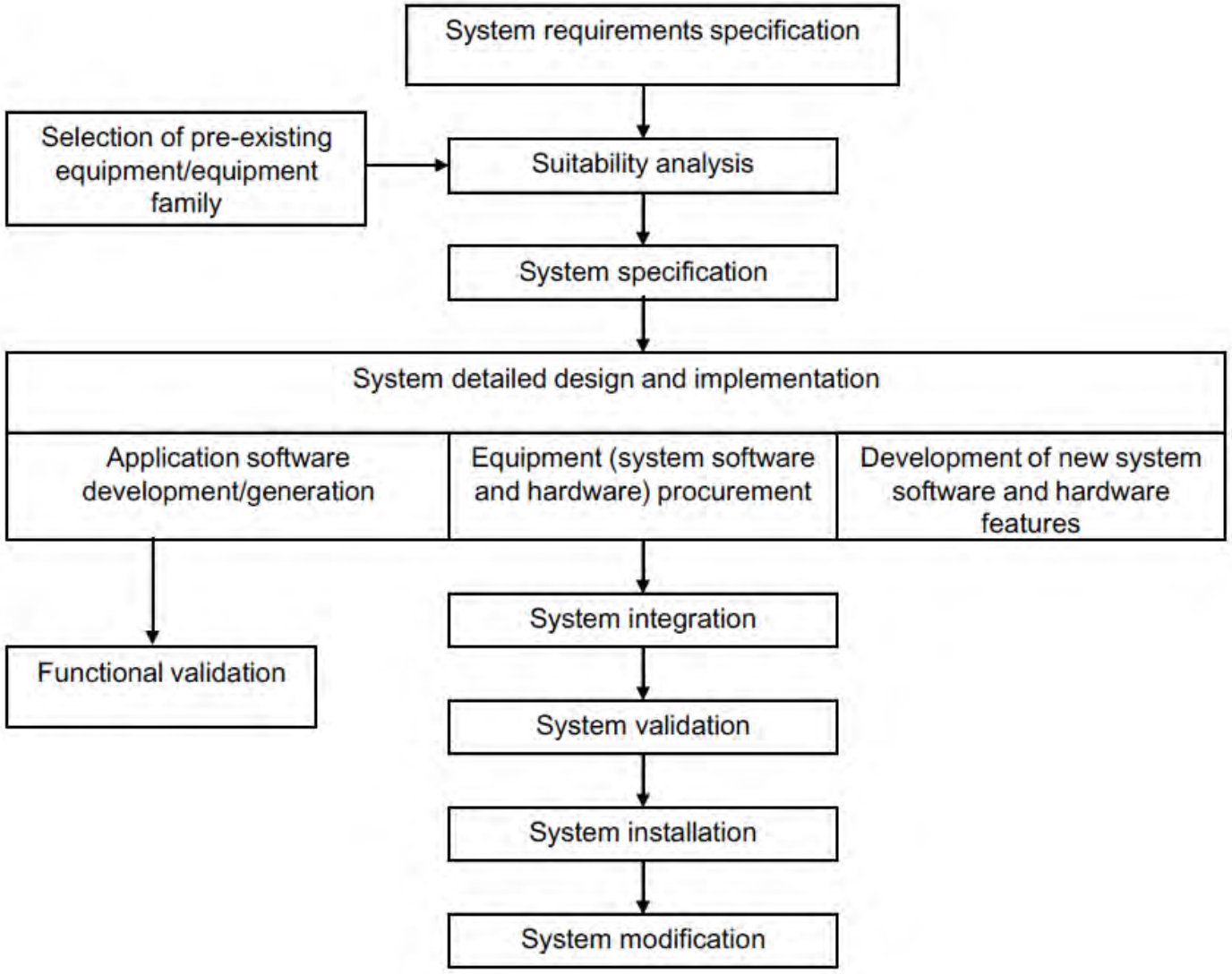
Future reference to IEC 62566(-2) with amendments and precisions if necessary

Digital Devices of Limited Functionality (DDLF) *m*

DDLF	Part H
DDLF with acceptable IEC 61508 certification	Part I

DDLF m out of M DDLFs in total

IEC 61513 : System-level requirements



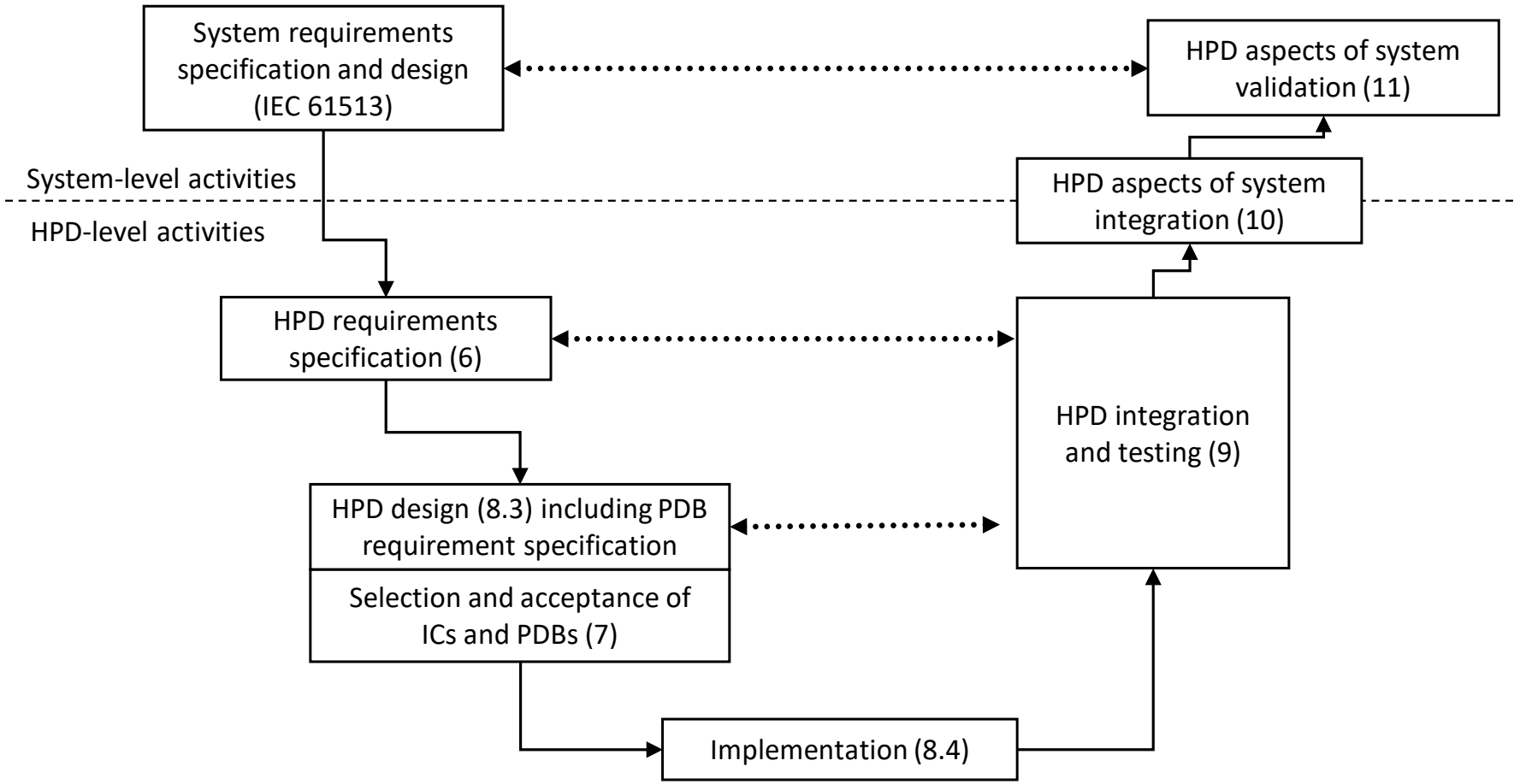
IEC 62566-2 : Class 2 and 3 HPD requirements – some fundamental decisions

- 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.
  - With a few exceptions, such as verification requirements and the structure of chapter 7 for the selection and acceptance of predeveloped components.
- Coherence with IEC 62138 in terms of requirement severity
  - This ensures that the severity of requirements does not impact the technological choices.
- Introduction of gradation principles as per IEC 62138
  - To provide coherent and appropriate differentiation between class 2 and 3 as per software standards.
- Reference to IEC 62138 for general requirements
  - IEC rules dictate that when requirements are taken from other standards, they should be referenced instead of copied.
  - However, this proved very difficult to implement in practice.

IEC 62566-2 : Class 2 and 3 HPD requirements – further developments

- Removal of requirements concerning deterministic design
  - Such requirements would need to be taken into account from the initial design stages, and for predeveloped items would result in the need for very detailed information about the internal operation of the component and probably the need for design modifications.
- Maintaining requirements concerning predictable design for class 2, removal of such requirements for class 3
  - Such clauses require detailed design information and cannot reasonably be expected for class 3. In certain cases, requirements might be downgraded to recommendations for class 3.
- Conservation of requirements which simply reflect good industrial practice
  - Even if there is no equivalent in IEC 62138 and as long as they are not too penalizing in terms of cost or time.

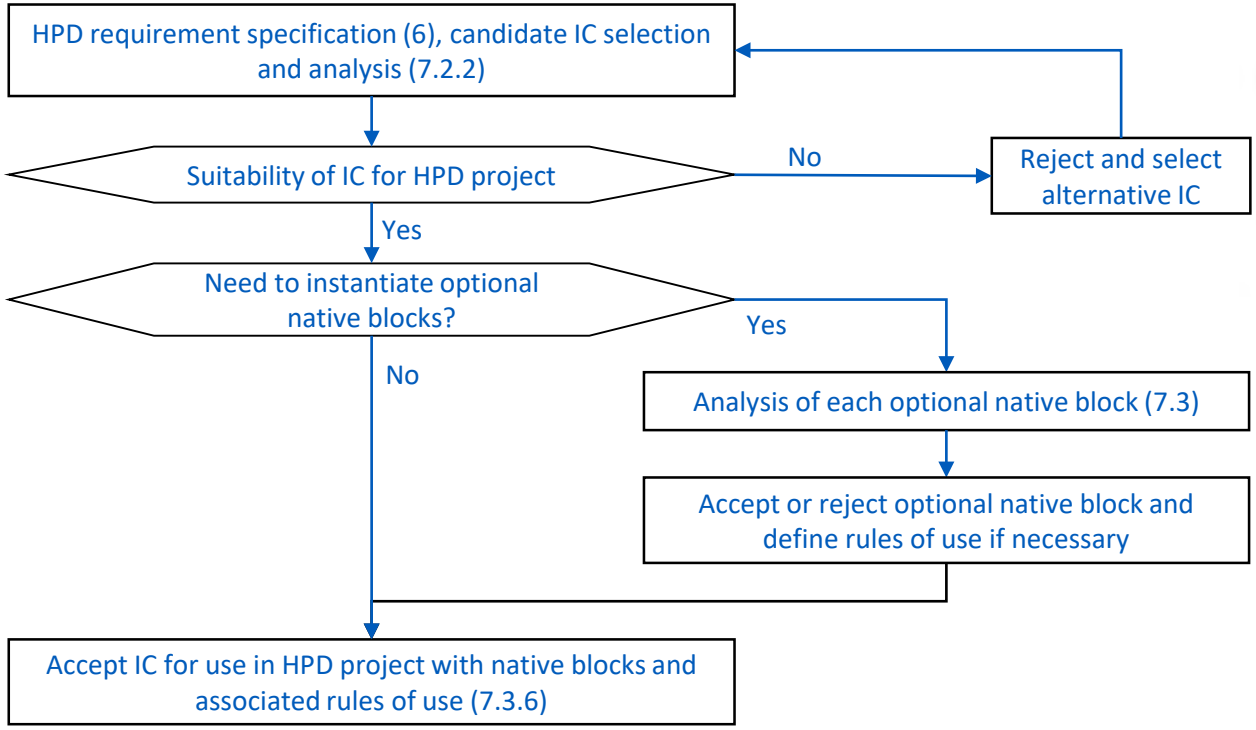
IEC 62566-2 : Class 2 and 3 HPD lifeycle requirements



IEC 62566-2 : Class 2 and 3 HPD requirements – Acceptance process for pre-developed items

- §7: Acceptance process for programmable integrated circuits, native blocks and pre-developed blocks.
  - The need for pre-developed items will increase significantly due to the nature of the functions that are likely to be implemented in class 2 or class 3 systems.
  - Separation of requirements concerning selection and acceptance of blank integrated circuits from requirements concerning the selection and acceptance of pre-developed blocks (IP cores etc.)
  - Introduction of 2 flow charts describing the acceptance processes for pre-developed items (blank integrated circuits and pre-developed blocks).

IEC 62566-2 : Class 2 and 3 HPD requirements – Recommended acceptance process for blank ICs



IEC 62566-2 : Class 2 and 3 HPD requirements – Recommended acceptance process for PDBs

PDB requirement specification (8.3.1), candidate PDB selection and functional suitability (7.3.2)

Suitability of PDB for HPD project

No

Reject and select alternative PDB

Yes

Type of PDB

PDB provided as an RTL description

PDB provided as a netlist

PDB using optional native block(s)

Design documentation (7.3.4.2)

Certification (7.3.4.4)

Operational experience (7.3.4.3)

Generation of supporting Documentation for Safety

Sufficient evidence of correctness?

No

Complementary means (additional tests, audits, analysis) (7.3.5)

Yes

Yes

Adequacy of complementary means

No

Accept PDB for general use or for use in specific IC subject to configuration, integration and validation requirements

Reject PDB

IEC 62566-2 : Class 2 and 3 HPD requirements – specific examples of structural or content changes

- §9 : HPD verification and validation
  - Need to separate verification and validation requirements.
  - Verification requirements are taken from IEC 62138. Requirements from IEC 62566 are too severe, in particular the level of independence between design and verification teams.
  - General verification requirements moved to the beginning of the standard, even if a small amount of structural coherence with IEC 62566-1 is lost.
- §10 : HPD aspects of system integration and §11 : HPD aspects of system validation :
  - Need for reduced emphasis on unit testing and integration testing as per IEC 62138.
  - Adoption of content without modification from IEC 62138.

IEC 62566-2 : Class 2 and 3 HPD requirements – specific examples of structural or content changes

- §15 : Software tools for the development of HPDs
  - Simplification of the content of chapter 15 which was inherited from IEC 62138 but which, for the purposes of HPDs, was too heavily oriented towards the selection and use of system-level design tools that are used with PLCs.
  - The content is now much more suited to the lower-level tools associated with the development of HPDs such as: functional simulation tools, synthesis and P&R tools delivered with the blank chips etc.

IEC 62566-2 : Class 2 and 3 HPD requirements – project timeline

- NWIP presented at the IEC SC45A meeting in Gyeongju in the Republic of Korea in March 2016.
- Working Draft distributed within the WGA3 group in January 2017.
- CD1 circulated among National Committees in April 2017.
- CD1 discussed at IEC SC45A meeting in Shanghai in October 2017.
- Following intermediate meeting in March 2018, CDV finalized and currently circulating among NCs for a period of 5 months.
- FDIS will be prepared for comment towards the end of 2018.
- Circulation of FDIS towards the beginning of 2019 and discussion of comments at the next IEC SC45A meeting in Paris in April 2019 (WGA3 meeting on 4th - 5th April).
- Publication hoped for Q3 2019.

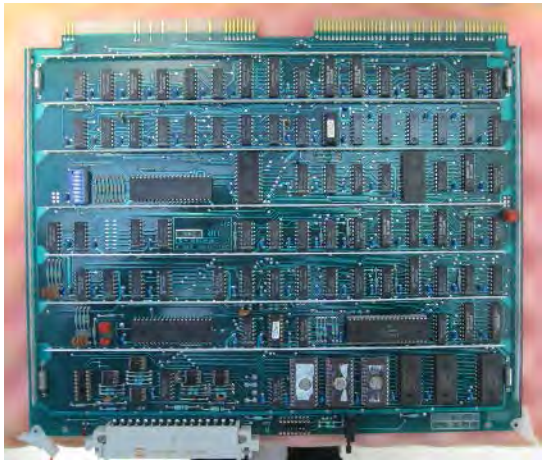
Automation and control system *n* : Part B §6

Topic		System classification		
		Class 1	Class 2	Class 3
Hardware	New	Part C excluding§ 6.8		Part D
	Pre-existing	Part C excluding§ 6.2 à § 6.7		
Software	New	Part E	Part F § 6 excluding§ 6.2	Part F § 5 excluding§ 5.2
	Pre-existing	Same requirements as for new software	Part F § 6.2	Part F § 5.2
HPD (FPGA, CPLD etc.)	New	Part G excluding§ 7	Part XXX	
	Pre-existing	Part G § 7		

- FPGA development requirements (all safety classes) :

Current and future work at EDF

- Class 1 CPLD-based primary pump speed measurement module



- Class 2 redesign of a Controbloc electronic module using FPGAs

Functional suitability

Tools

Diversity requirements

Cybersecurity requirements

Thank you for your attention

CHANGER L'ÉNERGIE ENSEMBLE