DEVELOPMENT OF A NEW IEC STANDARD FOR HDL-PROGRAMMED DEVICES PERFORMING CATEGORY B OR C FUNCTIONS

Alexander Wigg and Ludovic Pietre-Cambacedes
EDF SEPTEN
12-14 Avenue Dutriévoz,
69628 Villeurbanne, France
alexander-john.wigg@edf.fr; ludovic.pietre-cambacedes@edf.fr

Frédéric Daumas and François Cheriaux
EDF R&D
6 Quai Watier – BP 49
78401 Chatou, France
frederic.daumas@edf.fr; francois.cheriaux@edf.fr

Rémy Delhomme
EDF DPN
1 Place Pleyel,
93200, France
remy.delhomme@edf.fr

ABSTRACT

This paper presents an ongoing project within IEC[1] SC45A regarding the development of a new standard addressing the development of HDL[2]-Programmable Devices (HPDs) carrying out category B or C functions. This paper initially presents the context and the approach that was adopted for the development of the initial proposal, presented at the IEC SC45A meeting in the Republic of South Korea in March 2016. The objective of this paper is to present the current state of progress of the new standard, which has now been allocated the project number IEC 62566-2. A number of key points and topics for discussion in the coming months are presented. It is hoped that the standard will be published in 2019, completing the body of normative requirements for all function categories and for all technological families currently addressed by the IEC SC45A set of standards. The final content of the standard will be based on a necessary compromise between the need to maintain coherence with the SC45A set of standards, in particular with requirements imported from IEC 62566 and IEC 62138, and the need to perfect requirements specific to class 2 and 3 HPD developments. A number of conclusions and recommendations are made, especially the need to encourage the use of HPDs when they are well suited to the target application, even if no standards currently exist. It is only through such experiences that relevant, industrially-applicable standards can be developed. In order to harmonize requirements between countries and increase the competitively of nuclear power, stakeholders should be encouraged to contribute to, and endorse standards where they are available.

Key words: Standards, IEC, HPD, FPGA, licensing.

1. INTRODUCTION

For a number of years, the use of HDL-Programmable Devices (HPDs) has been increasing in the nuclear sector. Certain suppliers have chosen to develop complete instrumentation and control platforms that are entirely based on such technologies, which include, among others, FPGA[3]s and

[1] International Electrotechnical Commission
[2] Hardware Description Language
[3] Field Programmable Gate Array

CPLD[4]s. These strategic choices were even made before the publication of the first IEC standard that specifically addresses this family of technologies, IEC 62566 [1], published in 2012, which concerns the development of HPDs performing category A functions.

It was initially intended that IEC 62566 address the development of HPDs for all safety categories. As the project progressed, this objective proved extremely difficult to achieve in practice, and would have resulted in an extremely long and complicated document that would have been difficult to implement in real projects. It was therefore decided to limit the scope of IEC 62566 to HPDs performing category A functions only. After a relatively long development process, IEC 62566 was published as an international IEC standard in 2012. This long-awaited and very complete standard finally provided normative requirements and recommendations for the suppliers and operators that chose to adopt such technologies. It also allowed nuclear safety authorities around the world to objectively evaluate the development processes that were adopted by suppliers, therefore assisting in the qualification of class 1 systems employing HPD technologies.

Due to the reduced scope of IEC 62566 with regards to the original objectives of the standard development group, its publication left a very obvious gap in the subjects covered by the standards within the 45A sub-commission of the IEC, notably the development requirements for HPDs performing category B or C functions. In the absence of suitable standards, operators can be reluctant to adopt certain technologies if the development requirements are not clearly set by regulators, even if they are well suited to the application, therefore introducing significant licensing risks. On the other hand, nuclear safety authorities can be reluctant to provide specific guidance or requirements concerning the development process for technologies that are relatively new in the nuclear sector.

However, standards, by definition, do not themselves constitute national or international regulation. Standards are used to drive the adoption of new technologies and harmonize practices in an international marketplace by allowing stakeholders everywhere (manufacturers, consumers, regulators, government, certification laboratories etc.) to establish, on the basis of consensus, uniform technical criteria, methods processes. The use of standards is voluntary, unless their implementation is specifically required through government legislation or business contracts. The development of good standards therefore requires significant input based on real world experience about what constitutes appropriate industrial practice.

The absence of standards should therefore not discourage suppliers from adopting particular technologies if those technologies are well suited to the needs of the project and the target system being considered. In France, software-based reactor protection systems were qualified and installed well before nuclear software development standards existed. The industrial experience associated with the adoption of new technologies is in fact essential for the development of standards that contain suitable requirements and recommendations and which are therefore truly relevant and applicable in a real-world environment.

Following the acceptance of the New Work Item Proposal (NWIP) in South Korea in March 2016, and the subsequent positive Result of Vote on New Work Item Proposal (RVN), the draft of the standard was reworked and the development of the first Committee Draft (CD1) is underway. The CD1 will be presented at the next IEC SC45A meeting in Shanghai in October 2017.

This paper presents a high-level vision of the content of the current version of the new standard, in addition to an explication of the approach used to develop it. The detailed content of requirements is bound to evolve over the coming months and years, and the focus of this paper therefore remains on the general approach to the development of HPDs including selection and acceptance of PDBs. Chapter 2 addresses the initial approach to the development of the NWIP. Chapters 3, 4 and 5 address certain aspects of the content of the standard, respectively general requirements for HPD projects, selection and acceptance of predeveloped items, and HPD integration and functional validation.

[4] Complex Programmable Logic Device

Chapter 6 presents a number of conclusions regarding the structure and content of IEC 62566-2 in addition to a number of general points relating to the development, use, and endorsement of standards.

2. INITIAL APPROACH TO THE DEVELOPMENT OF IEC 62566-2

In the absence of a suitable IEC standard for HPDs performing category B and C functions, for a number of years EDF has been working closely with one of its suppliers to re-design an existing class 2 module using FPGA technology. The development of the re-designed module is based on a suitable set of requirements which are derived from IEC 62566 and based on engineering judgment, analysis and rational negotiation with the supplier.

The development of IEC 62566-2 could be argued to be relatively simple compared to other standards due to the fact that much of the input data exists already within other standards. IEC 62566, addressing the development of HPDs carrying out category A functions, constitutes one possible starting point for the development of IEC 62566-2. IEC 62566 presents a development lifecycle specific to HPDs which integrates into the system lifecycle described by IEC 61513. It is important that the new standard is, first and foremost, a document which addresses the development of HPDs as a technology, rather than a document which addresses the development HPDs as class 2 or 3 components. The standard will be used by HPD designers, not software designers. Therefore, the structure needs to be similar, if not the same as that of IEC 62566, allowing the difference in requirement severity to be easily identifiable, and also maintaining coherence between development practices for different safety classes.

A second possible approach would have been to use IEC 62138 [2] as a starting point. Such an approach would have been in line with the IEC software standards, where the structure differs significantly between the two standards. Although the initial decision may still be a subject for discussion, the reasons for the approach are justified. As long as the severity of requirements is reduced to a level which is compatible with IEC 62138, there is no reason to adhere to the structure of a standard which addresses software development. As explained previously, standards simply reflect good industrial practice, it is therefore equally important that the severity of the requirements within IEC 62566-2 is compatible with IEC 62138. This is to ensure that the content of the standards does not influence the technological choices of equipment suppliers and plant operators. Technologies should be chosen according to their suitability for the given application within a system, not according to the ease of demonstrating compliance to a given standard.

The initial NWIP presented in March 2016 was very heavily based on IEC 62566. A certain number of requirements were deleted as they were deemed to be too severe for class 2 and 3 applications. Other requirements were downgraded and/or made specific to either class 2 or class 3 developments. Requirements which reflect good industrial practice were maintained, and few importations were made from IEC 62138 at this stage. A number of topics requiring significant developments or discussions were identified, in particular the requirements concerning the selection and acceptance of PDB[5]s.

At this stage, it was decided not to make reference to requirements within other standards, but rather to import the text itself. This was important in the initial stages as it increases readability and facilitates discussions on the content of the standard, especially in cases where changes need to be made to imported requirements. In reality, in cases where requirements are imported from other standards without modification, IEC rules impose that the requirement is referenced rather than copied into the new standard. Furthermore, the development of IEC 62566-2 must ensure that the overall structure of the IEC SC45A body of standards is maintained, and that the new standard integrates seamlessly with the existing normative documents. Once the structure and the overall approach have been discussed and agreed upon with all National Committees, the details regarding the precise content of the requirements will need to be open for discussion. In particular, a compromise will have

[5] Pre-Developed Blocks, for example Intellectual Property (IP) cores.

to be found between the need to maintain the existing content and wording of imported requirements for the sake of coherence with other IEC standards, and the need to modify the content and wording of imported requirements for the sake of improvement.

The following paragraphs describe some of the main developments and areas for work regarding the development of IEC 62566-2.

3. GENERAL REQUIREMENTS FOR CLASS 2 OR 3 HPD PROJECTS

The requirements of IEC 62566-2, as is the case with IEC 62566 and software standards, are to be read as a complement to the system-level requirements defined in IEC 61513. General lifecycle requirements for HPD projects, as presented in the current working draft, are based heavily on the equivalent requirements for software. In cases where HPD project activities are not specific in any way compared to software projects, the requirements can be easily adapted from IEC 62138. This is the case for requirements relating to project management, quality assurance, configuration management and verification.

Furthermore, the gradation principles currently defined in IEC 62138 are perfectly applicable to HPD developments. For software and for HPDs, the principles followed are the same in order to ensure that neither technology is penalized by having stricter requirements associated with it. For class 3, regardless of the technology that is employed, the principles upon which the requirements are based on are:

- Quality assurance;
- Adequate contribution to safety functions and the assurance that the HPD cannot adversely affect safety functions;
- Detection of errors and failures and making this information available to operators;
- Adequate documentation of HPD-specific activities.

For safety class 2, the following principles are applicable in addition to those defined for class 3:

- Justification based on test and design that the performance specifications are met in all conditions (for example, through a demonstration of predictable behavior through HPD modeling);
- More stringent requirements for the selection and acceptance of pre-developed blocks and native blocks;
- More stringent requirements for functional validation (for example through behavioral simulations at the level of individual entities or modules, rather than on the HPD-level for class 3);
- More stringent requirements for verification and the selection and use of development tools;
- Explicit requirements for simplicity, clarity, precision, verifiability and testability.

Verification requirements for class 2 and 3 HPDs are presented within the chapter concerning general requirements, contrary to IEC 62566 where verification activities were presented as part of the functional validation phase involving test bench simulations. In reality, verification is not a single phase within a lifecycle as chapter 9 of IEC 62566 could lead to believe, but an activity that is carried out after each phase in order to ensure that that activity has been performed correctly with respect to its inputs. For this reason, the modification with respect to the structure of IEC 62566 was deemed justified.

An updated version of the HPD lifecycle process has been proposed for the new standard. In the initial draft presented in March 2016, a new figure based on Figure 4 from IEC 62138, presenting development activities for software, was proposed. This format had the advantage of differentiating between different types of HPD implementation, notably HPDs implemented using HDLs, HPDs implemented using application-oriented languages or system-level tools and the implementation and

configuration of PDBs and native blocks. Such a distinction was deemed important because of an expected increase in the number of PDBs that would be used for class 2 and 3 applications.

After further discussions, Figure 1 as shown below represents the current state of work and provides an overall view of the HPD lifecycle development process.

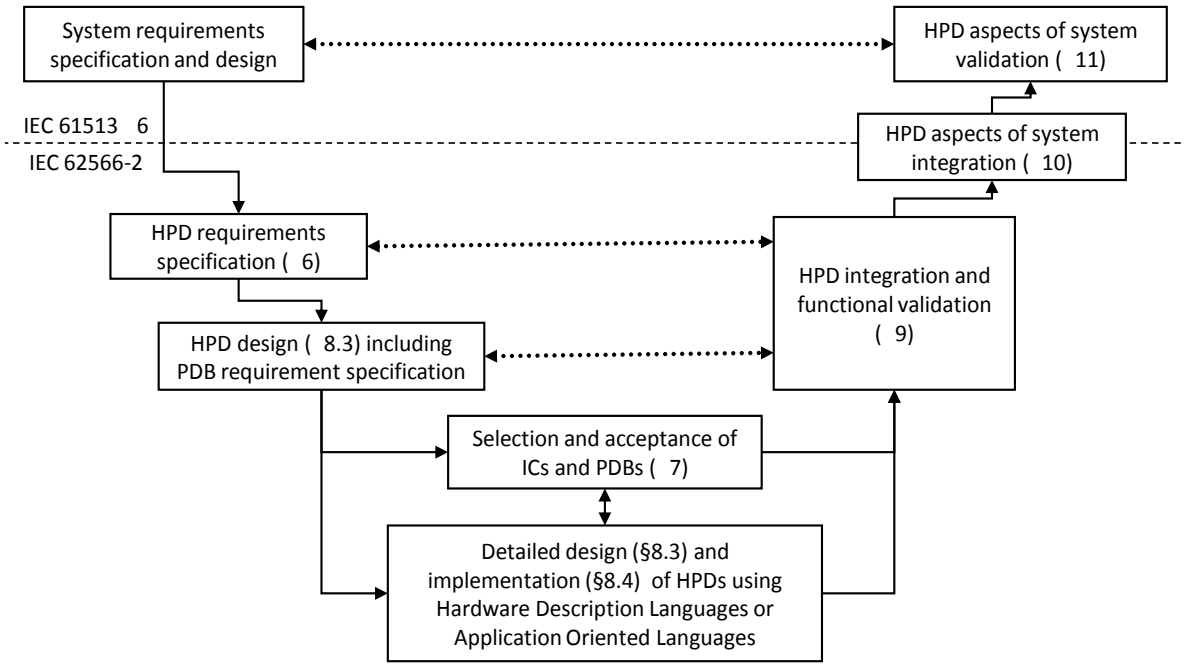

Figure 1 : HPD lifecycle

The newly proposed figure presents the following main differences compared to the equivalent figures in IEC 62566 and 62138:

- It clearly presents the boundary between system-level and HPD-level activities.
- It differentiates between the preliminary design phase and subsequent detailed design and implementation phases. The preliminary design and PDB requirement specification phase involves the initial high-level design of the HPD and the associated allocation of requirements to different modules and entities within the HPD. The detailed design and implementation phase demonstrates the parallel nature of these activities, which involve the selection, acceptance and configuration of blank circuits and PDBs on one side, and the development of new modules and entities on the other side using HDLs or application-oriented languages.
- It demonstrates the activities specific to HPDs which occur during the rising phase of the V-shaped lifecycle, notably the HPD integration and functional validation activities which primarily consist of behavioral simulations and functional validation carried out on test benches at increasing levels of integration.

The proposed figure is an active subject for discussion and it will certainly be subject to future modifications and improvements.

4. ACCEPTANCE PROCESS FOR PROGRAMMABLE INTEGRATED CIRCUITS, NATIVE BLOCKS AND PRE-DEVELOPED BLOCKS

The use of pre-developed blocks and native blocks within chosen integrated circuits can be expected to be significantly higher in class 2 and 3 systems due to the more complex nature of applications. One of the objectives for the new standard was therefore to significantly develop this

chapter by providing additional guidance for the selection and acceptance of such pre-developed items, taking into account the different natures of these components.

The new standard draft firstly distinguishes a dedicated selection and acceptance process for the blank integrated circuit that is to be used (PLD, CPLD, FPGA, etc.), along with the native blocks that are included with the circuit. Candidate integrated circuits are to be selected according to the requirements derived from the overall HPD requirements specification. The integrated circuits are to be chosen based on the results of a suitability analysis, the minimum content of which is given in the standard, which includes factors such as the circuit technology, the configuration technology, the number of logic elements and input/output pins and the maximum operating frequency.

The acceptance of a particular integrated circuit does not imply the acceptance of any of its included native blocks, which are not analyzed during the suitability analysis. The chosen circuit can be used without accepting any native blocks, provided that the native blocks are not instantiated in the design. A separate acceptance process is presented in the standard for cases where native blocks are to be used, although the rejection of native blocks according to this selection process does not imply that the integrated circuit itself cannot be used. Native blocks are in fact to be analyzed and accepted according to the same criteria as hard core PDBs, as presented in the following paragraphs.

The overall process for the selection and acceptance of integrated circuits and included native blocks is shown in Figure 2.

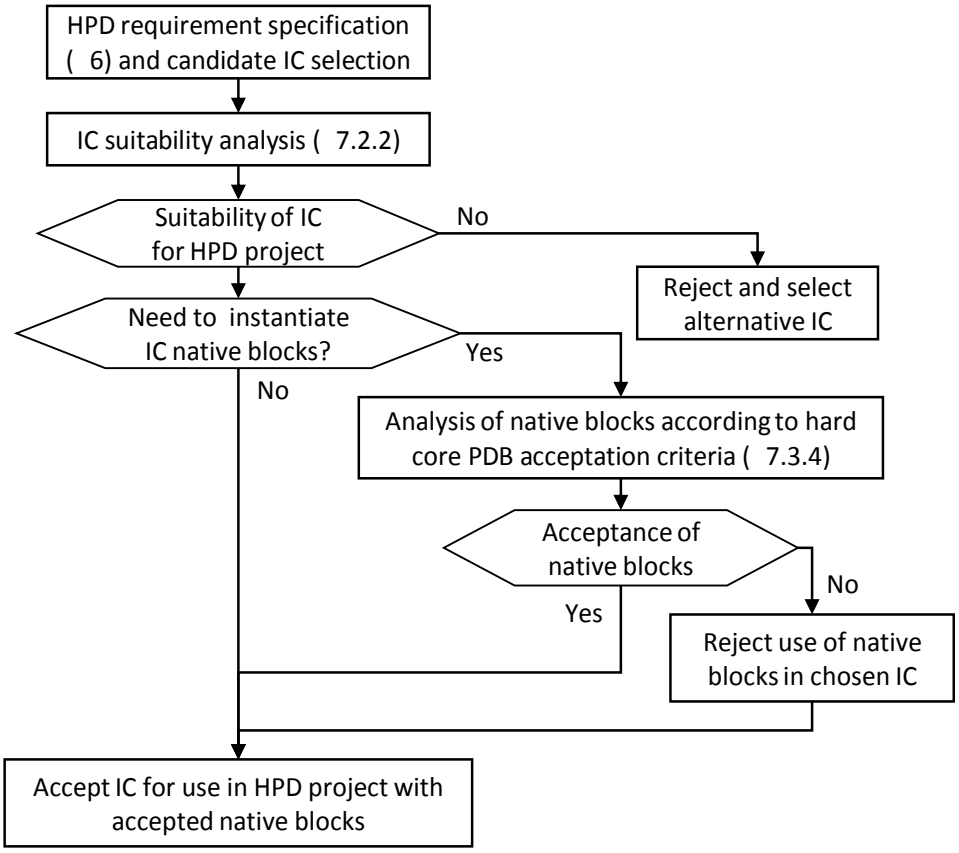

Figure 2 : Recommended selection and acceptance process for blank integrated circuits and included native blocks

The selection and acceptance process for PDBs follows the same principles as for pre-developed software in IEC 62138. The objective of PDB acceptance is to demonstrate that the PDB is correct with respect to its documentation for safety. This demonstration can take a number of forms depending

on the nature of the PDB that is being analyzed. Three categories of PDBs are identified in the new standard: soft-core PDBs provided in the form of HDL code, soft-core PDBs provided in the form of synthesized code and hard-core PDBs, representing function blocks included with the chosen integrated circuit. Soft-core PDBs are to be understood as blocks which can be integrated into a design using any circuit, whereas hard-core blocks are provided as part of the integrated circuit.

The overall recommended selection and acceptance process for PDBs is presented below in Figure 3.

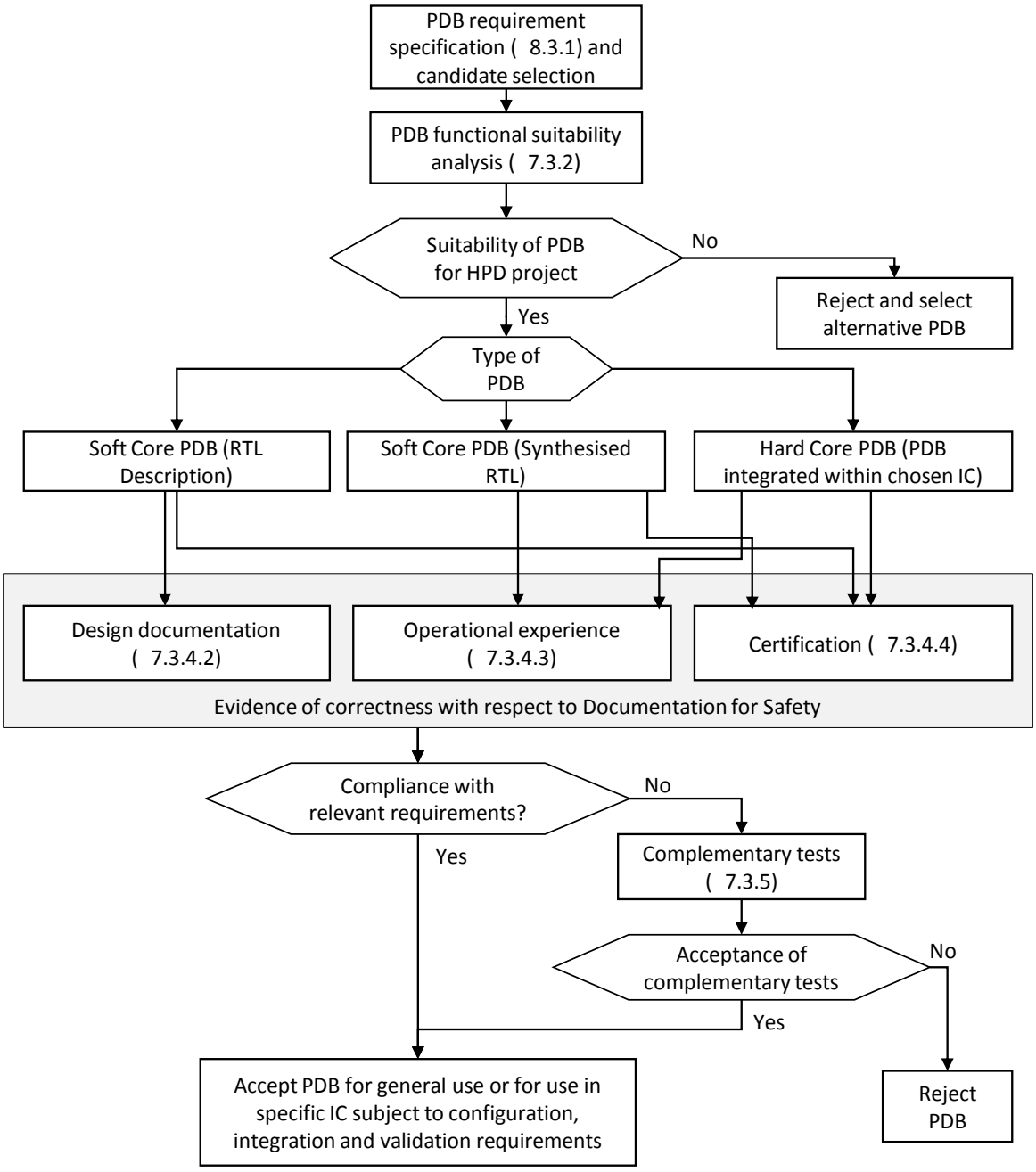

Figure 3 : Recommended selection and acceptance process for PDBs

Whatever the type of PDB which is being analyzed, the objective is to demonstrate its correctness with respect to its documentation. Three possibilities are offered for making this demonstration; design documentation, operational experience and certification. Although certain methods are recommended for certain types of PDBs, it was decided within the standard, as is the case within IEC 62138, not to give strict requirements on the method to be used, but rather to make

recommendations. This is because the method will need to be adapted according to the quantity and the nature of information that is available for a given PDB. In certain cases, a combination of approaches may be necessary. In all cases, there is the possibility of performing complementary tests through behavioral simulation of PDBs where sufficient evidence of correctness cannot be provided by other means. The content of the requirements of each approach are comparable with those for software. It is also to be noted that for the selection and acceptation of blank integrated circuits and PDBs, the gradation in requirements between class 2 and class 3 HPDs does not appear in the general figures reproduced here. The overall approach is common to both safety classes and the distinction between class 2 and class 3 appears within the text of the requirements.

It is to be noted that the selection and acceptance process explicitly mentions the possibility of performing a generic acceptance of PDBs rather than acceptance for use in one specific integrated circuit or project. Such a generic acceptance would of course be subject to configuration, integration and validation requirements that are specific to each HPD project.

5. HPD INTEGRATION AND FUNCTIONAL VALIDATION

The title and the scope of chapter 9 have been modified from IEC 62566 as previously mentioned. General verification activities, previously covered by chapters 9.1, 9.2, 9.3 and 9.4, have been moved to chapter 5 concerning general requirements for HPD projects. Such requirements are in fact distinct from simulation and test bench activities, covered by chapter 9.5 and onwards, and are general requirements that apply during the entire length of the project whenever verification activities are carried out.

The reader is reminded that verification and validation are two distinct activities with different objectives. Definitions for “verification” and “system validation” are common to all IEC SC45A standards and are defined within IEC 61513 [3]. The current organization of IEC 62566 can therefore be a source for confusion and the project therefore deemed that a modification is justified. Consequently, the title of chapter 9 was modified in order to better reflect its content which addresses specifically the gradual integration of components and entities within the HPD and their behavioral simulation at progressively higher levels for the purposes of functional validation. Such functional validation through behavioral simulation requires the development of test benches and test scenarios, typically described using HDLs. Good industrial practice dictates that simulations first take place on the lower levels, including down to the level of individual HDL entities if necessary, followed by a progressive integration of entities and modules and an appropriate set of test bench simulations and recuperation of output signals at each stage allowing the design to be sufficiently exercised at each level.

The requirements given by chapter 9 simply reflect good industrial practice, whilst formalizing the need for a suitable simulation strategy and test program which are to be documented. Specific requirements relate to the need to develop specific test scenario in order to sufficiently exercise PDBs when they are used in the design, especially in cases where additional behavioral simulation is to be carried out as part of complementary testing for the acceptance of PDBs. A number of requirements are specific to class 2 developments, in particular the need to define and document suitable test coverage criteria, without defining any particular metric (structural, functional, branch coverage etc.).

6. CONCLUSIONS

The objective of this paper was to describe the approach that was adopted for development of the current working draft of IEC 62566-2 addressing the development of HPDs performing category B or C functions. This paper also presents a general view of some issues within the future standard and a number of topics for discussion.

The IEC SC45A body of standards must continue to remain a coherent set of documents that complement and complete each other. However, standards are never perfect, they set guidelines and should be used to encourage coherence and harmonize practices between stakeholders. Standards are the result of years of negotiations between stakeholders that represent the interests of their respective countries and which are therefore subject to national regulations. As a result, standards within all industries can contain ambiguities and imperfections.

Consequently, the development of a new standard that relies heavily on the content of existing standards demands that a compromise is found. It is necessary to find a suitable equilibrium between the need to maintain coherence with existing standards, both in terms of content and in terms of structure, and the need to modify and improve existing requirements for the specific purposes of a project. The examples presented in this paper primarily represent cases where modifications are deemed justified, but that they have been implemented whilst conserving the spirit of the existing standards. The main principles adopted for the standard have been accepted, although the way in which they will be implemented has yet to be discussed in detail within SC45A. The devil is likely to be in the details, in particular the rules which are used to determine how existing requirements are imported or referenced and in which cases requirements cannot be modified for the purposes of coherence with other SC45A standards, even when modifications are technically justified within the context of IEC 62566-2.

The current work program plans for publication of IEC 62566-2 in 2019. However, in the intervening years, the absence of this standard should not discourage operators from using HPDs for class 2 and class 3 systems in cases where HPDs are an appropriate technical solution with respect to the system requirements. It should also be noted that, contrary to popular belief, the decision to use any particular technology does not intrinsically guarantee that required system properties can be achieved. Although particular technologies may have underlying properties, it is primarily the supplier's proficiency in the design and implementation of a given technology that will lead to the production of safe and reliable systems. Reference [4] presents a number of arguments to this effect and encourages the need for critical analysis and open discussion regarding the most appropriate technological choices for a given system.

Standards cannot, and should not, provide guidance regarding which technology should be used and when, and the absence of a standard should not prevent a suitable technology from being used when appropriate. Any future use of HPDs in the forthcoming years, before the publication of IEC 62566-2, could prove to be valuable input data for the future development and revision of HPD standards. Regulators and operators should actively contribute to the development of standards, and not discourage the adoption of new technologies in cases where no standards exist. HPDs have been used for decades in other industries because they are extremely well suited to certain applications. To implement barriers against the use of new, proven technologies, even in cases where no specific standard exists, could be to contribute to the degradation of safety in aging systems.

The contribution to, and the endorsement of standards is to encourage harmonization of practices and promote a situation where a qualification in one country might be recognized in another. In cases where standards represent a suitable minimum set of requirements, regulators, suppliers and operators should not hesitate to adopt them.

7. ACKNOWLEDGEMENTS

The authors would like to thank all active contributors to the development of IEC 62566-2 for their continued feedback and support.

8. REFERENCES

1. IEC[6] 62566:2012: *Nuclear Power Plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions*
2. IEC 62138:2004: *Nuclear Power Plants – Instrumentation and control important to safety – Software aspects for computer-based systems performing category B or C functions*
3. IEC 61513:2011: *Nuclear Power Plants – Instrumentation and control important to safety – General requirements for systems*
4. A. Wigg and L. Pietre-Cambacedes, "FPGA-Based I&C Systems: Unraveling myths from reality (position paper)", *Proceedings of the 9th International Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies,* Charlotte, USA, February 23-26 2015.

[6] As explained on its website, "the International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The objective of the IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides. Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation (this includes the ISO, the IEEE or the AIEA for instance). The standard presented in this paper is being developed by the Subcommittee 45A (SC45A) of the IEC, addressing Instrumentation and control (I&C) of nuclear facilities. SC45A has issued many worldwide recognized references on different issues with respect to I&C, in particular for I&C systems important to safety (see [1,2,3] for instance).