Multinational Design Evaluation Programme
Generic Common Position
DICWG No5 – PUBLIC USE

Date: 13 march 2013
Validity: **until next update or archiving**
Version A

MDEP Generic Common Position No DICWG-05

Related to: Digital Instrumentation and Controls Working Group activities

COMMON POSITION ON THE TREATMENT OF HARDWARE DESCRIPTION LANGUAGE (HDL) PROGRAMMED DEVICES FOR USE IN NUCLEAR SAFETY SYSTEMS

Participation

Countries involved in the MDEP working group discussions:	Canada, Finland, France, India, Japan, People's Republic of China, Republic of Korea, Russian Federation, South Africa, the U.A.E., the U.K. and the U.S.
Countries which support the present common position	Canada, Finland, France, India, Japan, People's Republic of China, Republic of Korea, Russian Federation, South Africa, the U.A.E., the U.K. and the U.S.
Countries with no objection:	
Countries which disagree	
Compatible with existing IAEA related documents	Yes

Multinational Design Evaluation Programme

Digital Instrumentation and Controls Working Group

GENERIC COMMON POSITION DICWG NO5 : COMMON POSITION ON THE TREATMENT OF HARDWARE DESCRIPTION LANGUAGE (HDL) PROGRAMMED DEVICES FOR USE IN NUCLEAR SAFETY SYSTEMS

Summary:

The Digital Instrumentation and Controls Working Group (DICWG) has agreed that a common position on this topic is warranted given the increase of use of Digital I&C in new reactor designs, its safety implications, and the need to develop a common understanding from the perspectives of regulatory authorities. This action follows the DICWG examination of the regulatory requirements of the participating members and of relevant industry standards and IAEA documents. The DICWG proposes a common position based on its recent experience with the new reactor application reviews and operating plant issues[1].

Context:

Following other industries, the nuclear industry developed increasing interest in the use of programmable logic components that are implemented using hardware description language (HDL) such as such as FPGAs[2], CPLDs[3] or ASICs[4]. HDL programmed devices (HPD) has both characteristics of software and hardware. Therefore applications using HPDs has many similarities with the traditional software (in particular the design may be affected by errors) and characteristics of traditional electronic design (e.g. electronic-level timing and electrical issues). However, due to the unique nature of HPDs, there exist several differences between HPDs and traditional software. Some key differences include:

- HPDs use parallel processing with dedicated hardware for each function instead of executing instructions sequentially as in the case of traditional software.
- Safety critical software uses imperative languages which specify each instruction of the program whereas HPDs use declarative languages.
- The target of software is a microprocessor, which guarantees properties such as memory consistency after each instruction. Such properties are not inherent in HPDs and thus the design process needs different steps to build and guarantee behavioural properties.

[1] The goal of MDEP is not to independently develop new regulatory standards. Common Positions are not legally binding and do not constitute additional obligations for the regulators or the licensees but are guidelines, recommendations, or assessments that the MDEP participants agree are good to highlight during their safety reviews of new reactors. Any MDEP member may decide to implement the common positions through its national regulatory process.

[2] Field Programmable Gate Array

[3] Complex Programmable Logic Device

[4] Application Specific Integrated Circuit

- Translation of the HDL description to bitstreams in HPDs is much more involved than the translation of source code to binary in software compilation. In the HPD case, this process is not fully automatic, and therefore designer must guide the tools, which may result in undetectable errors.

Figure 1 shows the typical development life cycle of HPDs that may be undertaken in parallel with the development of other components (software or hardware) of the system, but integrated at the integration and validation phases of the system life cycle. The HPD requirements specification is typically derived from the overall system requirements. During HPD design, the requirements specifications are translated to HDL code (e.g. VHDL source code). In HPD implementation, a netlist is synthesized from the HDL code, which provides a description of the connections and gate structure of the logic. Place and route operation maps the design onto the device architecture by creating the physical layout. The output of the place and route is the configuration file. This configuration file is used to configure the actual device. Lastly, the HPD is integrated with the rest of the system.

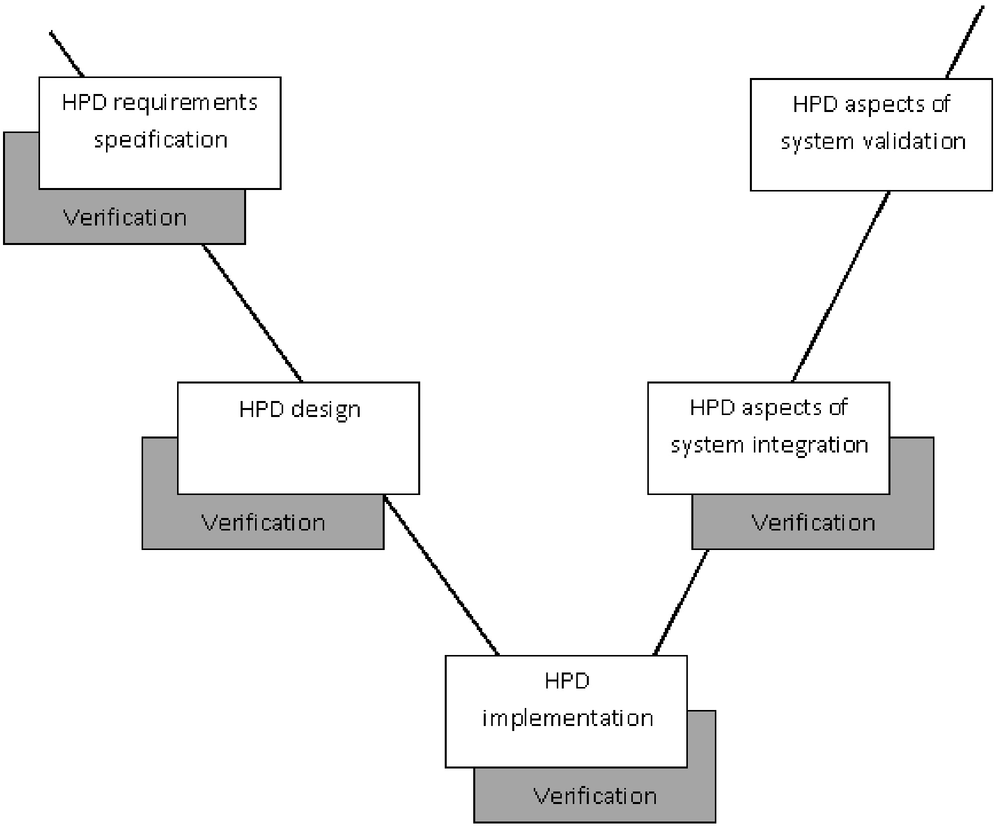
HPD requirements specification
Verification
HPD aspects of system validation
HPD design
Verification
HPD aspects of system integration
Verification
HPD implementation
Verification

Figure 1: Typical development life cycle of HPDs

The safety systems of nuclear power plants need to be of the highest quality to minimize the likelihood of failure. When their logic is implemented in HPDs the correctness of this logic has to be ensured. However, as it is the case for software, no simple solution exists to build and demonstrate the correctness of non-trivial HDL designs.

Definition of terms:

HDL-Programmed Device (HPD): a HPD is an integrated circuit configured for Nuclear Power Plants I&C systems, with Hardware Description Languages and related software tools. Typical examples of such integrated circuits are FPGAs, CPLDs and ASICs.

Safety System: a system important to safety provided to ensure the safe shutdown of the reactor or the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents [IAEA Safety glossary].

Requirements: expression in the content of a document conveying criteria to be fulfilled if compliance with the document is to be claimed and from which no deviation is permitted [IEC 61513].

Metastability: condition in which a two-states digital element oscillates between its two states for arbitrarily long times.

Scope:

This common position applies to the development of HPDs for use in safety systems at nuclear power plants. This common position does not provide guidance on the development of the micro-electronic component, which are usually available as “commercial off-the-shelf” items.

Generic Common Position on the Treatment of HPDs:

1) The development process associated with the use of HPDs should follow a safety life cycle, be duly documented and include verification:

    a. the safety life cycle should be defined before the beginning of the development and structured in phases having defined inputs, activities and outputs,

    b. the HPD should be developed under a nuclear safety system quality assurance program in accordance with a previously defined quality assurance plan,

    c. a comprehensive documentation of the development activities should justify each technical decision and make it understandable by a third party,

    d. the outputs of the development phases of the HPD should be verified and the HPD specific aspects of the system validation should be addressed,

        i. verification & validation (V&V) should be performed and documented according to a previously defined plan including the verification objectives and procedures.

        ii. V&V should include 1) HPD specific aspects of the system validation with respect to the system requirements and 2) verification of each development phase (including at least the specification of requirements, the design, and implementation) with respect to its own inputs,

iii. V&V should confirm that 1) the HPD requirement specification fulfils the system requirements assigned to the HPD and 2) the HPD design specification and HDL description fulfil the HPD requirement specification (including confirmation that no hidden circuits exist to affect the functions of the HPDs),

iv. V&V should be performed by technically qualified individuals in an appropriately independent group who has not been engaged in the design & development of the HPD.

e. The adequacy and the coverage of the verification process should be analysed and justified.

f. the post-route analysis should demonstrate the compliance of the design and implementation with the technology rules defined by the supplier of the design and implementation tools,

g. the implementation plan for HPDs should define the means to ensure that each produced part complies with the design,

h. the process of integrating the HPD design should be part of the overall system development process. A separate plan for integration and testing may be prepared to integrate the HPD to the overall system,

i. configuration management of HPDs should be conducted according to a previously defined plan and should cover design products and development/verification environments.

2) Clear, consistent and complete requirements should be established and be the basis for the design activities. Additionally, the design process associated with HPDs should ensure that:

a. behaviour of the HPDs is deterministic (e.g. using internal synchronous design) in order to favour correctness (avoidance of metastability issues) and testability and to make the best use of the design and verification tools. As such,

i. timing analysis and simulation are performed,

ii. design requirements for HPDs include timing requirements, such as gate delays and setup times,

iii. all signal paths in the HPDs are tested during development.

b. standardized HDLs are used to program the HPDs. In addition, qualified and compatible tools are used.

c. the design is restricted to HDL structures having well-defined implementation and behavioural properties. If feasible, such implementation and properties should be capable of using verification techniques based on mathematical theorem proving,

d. the design explicitly handles all possible cases of logic and all operating modes of the HPD such as reset, power-on and normal operation. The design should be correct for all possible timing cases resulting from bounding variations in supply voltages, temperature and microelectronic process.

e. each function implemented in the HPD is testable.

3) The selection of pre-developed items (such as the programmable integrated circuit to be used, e.g. antifuse vs. SRAM based devices, libraries and Intellectual Property (IP) cores) to be included in the final product should follow a defined and documented process to guarantee their suitability.

a. The use of IP cores in HPDs should be avoided or additional verification of the core should be performed.

i. If use of IP cores cannot be avoided, the IP cores used should be obtained from qualified vendors, who followed high quality IP-cores development process, including a rigorous engineering process, well-defined and useful documentation, and ease of integration.

ii. Evaluations should be performed to determine potential introduction of hazards.

b. If modifications of the pre-developed item are necessary to achieve acceptance, they should be specified, designed, implemented, and verified before the acceptance review. These modifications should be performed and documented through acceptable safety system life cycle process.

c. If the HPD includes auxiliary features (e.g., built-in self-test), their suitability in contributing to the performance of a safety function should be determined by evaluation of various elements including their development process (including verification process) and of their design.

d. Equipment qualifications and analyses should demonstrate that the inclusion of pre-developed items or auxiliary features does not degrade the ability of safety systems to perform their safety functions.

References

IEC 60880 Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions, 2006

IEC 61513 Nuclear power plants - Instrumentation and control important to safety - General requirements for systems, 2011

IEC 60987 Nuclear power plants - Instrumentation and control important to safety - Hardware design requirements for computer-based systems, 2007

IEC 62566 Nuclear power plants - Instrumentation and control important to safety - Development of HDL-programmed integrated circuits for systems performing category A functions, 2012

Gassino, J. Introduction of Programmable Electronic Devices in Nuclear Safety Systems: A new Challenge in Assessment. In: EUROSAFE 2009: Safety Implications of an Increase Demand for Nuclear Energy, Brussels, 2-3 November.

Ranta. J. The Current State of FPGA Technology in the Nuclear Domain. Espoo 2012. VTT Technology 10. 62p

NRC 2010b. Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems. U.S. NRC, NUREG/CR-7006, (ORNL/TM-2009/20), 2010.

IAEA Safety glossary, 2007