Approach adopted by RPC Radiy for the Verification and Validation (V&V) of FPGA based platforms for nuclear safety applications.

Vladimir Sklyar and Sergio A. Russomanno
Research and Production Corporation (RPC) Radiy
v.sklyar@radiy.com
S.russomanno@radiy.com

Abstract

In order to maximize stakeholders' confidence that design implementations meet all requirements, it is of paramount importance that design organizations and suppliers of FPGA platforms to be utilized in nuclear safety applications adopt rigorous V&V processes and techniques in compliance with widely recognized industry standards.

The above challenge has been fully embraced by RPC Radiy in the form of a V&V plan that is in general compliance with IEC 61508 for platforms to be used in nuclear safety applications in North America.

This paper describes details of the above program which is designed to evolve and adapt to meet further challenges as we advance in our working relations and seek to meet specific requirements of utilities, regulators and design organizations in the Americas, Asia and Europe.

1. Introduction

Today's FPGAs platforms have reached Application Specific Integrated Circuits (ASIC) proportions, with millions of gates running at increasing clock speeds. In addition, as part of their specific functions, Synthesis tools perform optimizations that drastically change design implementation structures.

Given the complex nature of these platforms and the criticality of many of the applications in which RPC Radiy is using them within the nuclear industry, the implementation of a rigorous approach to V&V in compliance with widely recognized standards is considered by management and the company's technical community an important measure to be taken in order to ensure compliance with requirements posed by utilities and regulators.

RPC Radiy's approach was to institute a V&V program in full compliance with processes defined in IEEE Std 1012, "IEEE Standard for Software Verification and Validation", starting from the criteria established in the above standard for the definition of the System Integrity Level (SIL), down to the processes and procedures mandated by the SIL level that are necessary to provide supporting evidence that the software complies with requirements.

In applying the criteria described in Clause 4 of IEEE Std 1012, Radiy, in conjunction with external regulators and under advice from experts in the nuclear industry, has established that the integrity level required for nuclear safety applications is SIL3. The sections that follow in this paper include the following:

1. A brief description of a typical Radiy FPGA platform used in nuclear safety applications, hereinafter referred to as FSC (FPGA Based Safety Controller)

2. Background on the processes that result from the application of IEEE Std 1012 and IEC 61508 to platforms such as Radiy’s FSC system, that must be certified in Canada to SIL3 and how they fit in a typical lifecycle for products used in safety applications.

3. A description of the main elements of the program instituted by Radiy for the implementation of V&V processes and activities that satisfy the requirements on FSCs posed by the above standard.

4. A description of the structure and contents of the technical Safety documentation and the activities that drive the preparation and contents of the resulting V&V documentation.

2. Typical Radiy FPGA platform used in nuclear safety applications Ref [1].

The digital I&C platform developed by Radiy is composed of multiple modules based on the use of field programmable gate arrays (FPGAs) as a computational engine for each module.

The basic platform configuration consists of a rack containing one Logic Module (LM) and one Diagnostic Module (DM) plus up to 14 other of any mix of module types (I/O and optic communication). The basic set of I/O modules comprise analog inputs (AI), digital inputs (DI), Analog outputs (AO) and digital output (DO) modules. There are also special purpose I/O boards such as RTD, thermocouple, ultra-low voltage AI boards (used for neutronics instrumentation), actuator controller modules, and a fiber-optic communication module that can be used to extend the system to multiple chassis. It is also possible to provide inter-channel communications between 2, 3 or 4 channels via fiber-optic communications directly between logic modules.

LMs gather input data from input modules, execute user configured logic, and update the value driving the output modules. DMs gather diagnostic and general health information from all I/O Modules and the Logic Module. The I/O modules provide interfaces with other devices (e.g., sensors, actuators). The functionality of each module is driven by the logic implemented in the on-board FPGA(s).

The platform backplane provides external interfaces to power, process I/O, communications links, and local inputs and indicators. Internal backplane interfaces facilitate connections to the various modules that are installed within the chassis by means of dedicated, isolated, point-to-point low-voltage differential signaling. The basic configuration of Radiy’s Platform is shown in Figure 1.

Examples of applications are:

- Reactor Trip System (RTS),
- Reactor Power Control and Limitation System (RPCLS),
- Engineering Safety Features Actuation System (ESFAS),
- Rods Control System (RCS),
- I&C for Research Reactors.

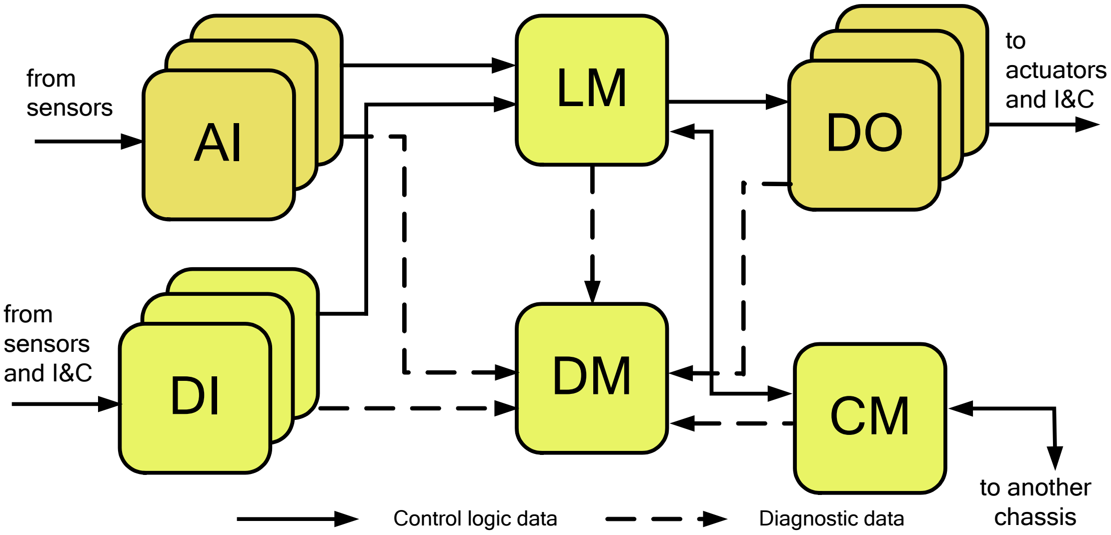


Figure 1. Basic configuration of Radiy's FPGA platform

3. Safety Life Cycle

Radiy has adopted the concept of a "Safety Life Cycle" (SLC), common to all modern standards associated with functional safety. Figure 2 below shows a model that covers the cradle-to-grave life of a safety product or system. As explained in more detail in sections to follow, V&V activities are applied throughout the lifecycle of the system, except at the "Retire" phase.

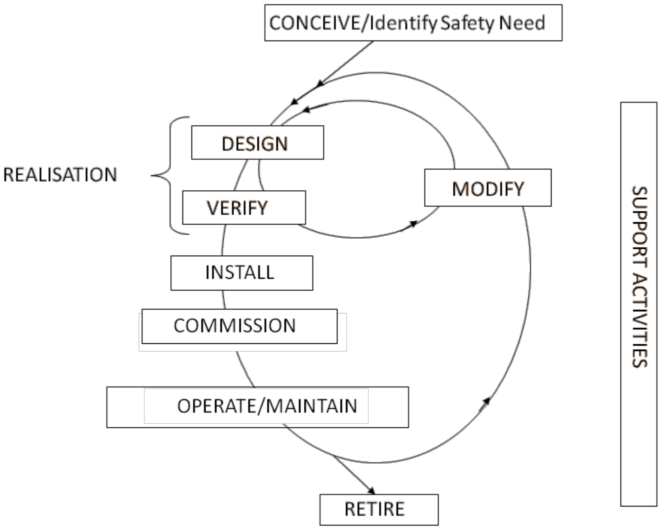


Figure 2. Safety Life Cycle

4. Process

A further breakdown into processes, of the phases that are part of the Safety Life Cycle model shown in Figure 2 is necessary in order to be able to describe V&V activities planned at RPC Radiy to fulfill SIL3 requirements. These are as follows:

4.1 Management. RPC Radiy has established a management structure responsible for the overview and support of all V&V activities associated with the different processes listed in sections 4.2 to 4.6 below.

4.2 Acquisition. V&V activities associated with the acquisition process are instituted in order to attain the required degree of assurance that all the supplied parts, materials, services, test facilities and tools required for the completion of the final product are adequate and complete. Measures undertaken to attain the above are described in section 5.

4.3 Supply. Clients and regulators impose requirements on RPC Radiy's products that must be considered in the implementation of our work processes. Normally, these are requirements of the type that would be included in Request for Proposals and other documents that are part of the supply process; however, when allowed by clients policies and procedures, Radiy's approach is to engage in early discussions with potential users to ensure that we understand their requirements in sufficient detail and early enough to be able to reflect them in our work processes and thus devise V&V mechanisms to ensure that such requirements are met.

4.4 Development. As shown in section 6 below, V&V processes at Radiy are applied to the entire product lifecycle. Particularly, Development and V&V activities are mostly conducted in parallel, this allows us to uncover and remove problems early in the process, thus reducing costs and minimizing risks to the schedule.

Although Verification and Validation techniques and objectives are complementary in that they are both designed to ensure compliance of the product with requirements, they are also viewed at Radiy as different processes. The following are definitions for each of these two activities as included in IEEE Std 1012:

> *The **verification** process provides supporting evidence that the software and its associated products:*
>
> 1) *Comply with requirements (e.g., for correctness, completeness, consistency, accuracy) for all life cycle activities during each life cycle process (acquisition, supply, development, operation, and maintenance);*
> 2) *Satisfy standards, practices, and conventions during life cycle processes; and*
> 3) *Establish a basis for assessing the completion of each life cycle activity and for initiating other life cycle activities**.***
>
> *The **validation** process provides supporting evidence that the software satisfies system requirements allocated to software, and solves the right problem (e.g., correctly models physical laws, or implements system business rules).*
>
> In accordance with the IEC 61508 V-Model at RPC Radiy, we extended the above definitions in IEEE Std 1012 to cover hardware as well as software V&V activities.
>
> The following subsections provide a general description of the approach adopted by Radiy in conducting V&V activities at each stage of the development process.

4.4.1 Product Concept Definition

The Product Concept definition process consists in identifying the FSC requirements and platform architecture that will remain common to each application. Also part of this phase is the definition of standards based on which the FSC will be developed, in this case IEEE Std 1012, IEC 61508, applicable parts of IEC 60880 and the current draft of IEC 62566. In addition, decisions such as the type of FPGA technology and associated development and testing tools, the amount and type of self testing and overall assignment of safety and non safety functions in order to minimize and simplify V&V activities are made at this stage.
Therefore, V&V activities are designed to ensure completeness, correctness, testability and consistency of the above set of requirements, the suitability of the system architecture and, to identify and correct any potential undesirable outcomes that could result from the development or usage of the system.

4.4.2 Requirements Definition

While the Product Concept Definition phase is mostly associated with requirements at the system level, this phase deals with requirements as allocated to the hardware, software, and FPGA/VHDL subsystems. The type of requirements defined at this stage of the development process are mostly functional, performance and safety requirements (including fault avoidance requirements as specified in IEC 61508) and interfaces with components external to the software such as data exchange and human factors requirements.

Requirements can be further subdivided into black-box and white-box types as follows:

White-box requirements include details on the internal logic of the smallest testable units, for example, a software module, a function or procedure, in testing these requirements it is ensured that every possible branch of the logic results in the desired outcome.

Black-box requirements are independent from implementation details. In testing these requirements it is ensured that inputs result in the desired outputs independently of implementation details.

V&V activities in this phase are designed to ensure the correctness, completeness, accuracy, testability, and consistency of the above requirements.

4.4.3 Detail design

In this phase of the product development process, requirements are translated into an architecture involving software and hardware components.

This design phase can be further subdivided into the following activities:

1. **Product Architecture Design**. At this stage, functionality is allocated to the major hardware and software modules of the product.
2. **Software Architecture Design:** Software for the functionality allocated to the different modules is developed at this stage. The output of this activity is commented code and associated design description.
3. **Electronic Architecture Design:** This activity is carried out for the hardware architecture in an analogous manner as activity 2 above is carried out for the software architecture. The analogy's validity is strengthened by the need to carry out VHDL development which, process and outputs wise, is comparable to software development.

4.4.4 Implementation

The Implementation V&V activity consists in translating the functionality assigned to the different software and hardware modules and the architecture chosen to have all the above modules interconnected and communicating with each other during the design phase into code, database structures, communication protocols and related machine executable representations.

The objectives of V&V are to verify and validate that these transformations are correct, accurate, and complete and to demonstrate that the design is a correct, accurate, and complete transformation of the software and hardware requirements into the intended functionality. The V&V process also ensures that no unintended features are introduced in the design.

4.4.5 Installation of the different components into a final integrated platform

This activity is associated with the installation of the software and hardware components in the target environment and the final users' acceptance review and testing of the platform composed of the above components as a clearly defined and configured product.

At RPC Radiy we have established processes, procedures and tools to ensure that our products are under rigorous configuration and change control until they are delivered to our customers. This includes verification that the correct and intended versions of all components are installed in our platforms throughout the different cycles of the development process and in particular prior to the execution of the different levels of testing (see section 4.4.6 below).

The V&V process also includes activities to ensure that the hardware and software components installed as part of the platform to be delivered corresponds to the components that were subjected to V&V.

Configuration and change control should continue after the platforms are delivered to the different sites, at which time, final users become responsible for the establishment of their own processes, procedures and tools after our products are installed in their facilities. We provide our customers with all the information required to implement their processes safely and effectively and where the need arises, we support their effort in ensuring proper configuration and change control of our platforms.

4.5. V&V activities

V&V activities are conducted throughout the FSC lifecycle. Verification activities are conducted via a combination of different techniques such as review, inspection, analysis or testing, whereas Validation activities consist mostly of testing. Section 5 below includes a brief description of the different V&V techniques and how they are applied to the different stages in the FSC lifecycle.

4.6. Installation, Operation and Maintenance at site

Final users are responsible for the establishment of their own processes, procedures and tools after our products are installed in their facilities to ensure that the FSC platforms continue to be under rigorous configuration and change control through their remaining lifecycle.

At RPC Radiy we prepare a Product Safety Manual which includes or references all documentation and guides needed by the users for safe installation, testing, maintenance, operation, and modification of our products at site, and where the need arises, we work with our customers in establishing and applying all the necessary processes procedures and tools that must be in place throughout our products' lifecycle.

5. V&V Techniques

The following subsections describe V&V techniques applied to each of the stages described under section 4 above.

5.1 V&V techniques applied to the Acquisition and Supply processes

The Acquisition and Supply processes are verified mostly via R&C, Inspection and audits to ensure that all the supplied parts, materials, services, test facilities and tools required for the completion of the final product are adequate, complete and meet clients and regulatory requirements.

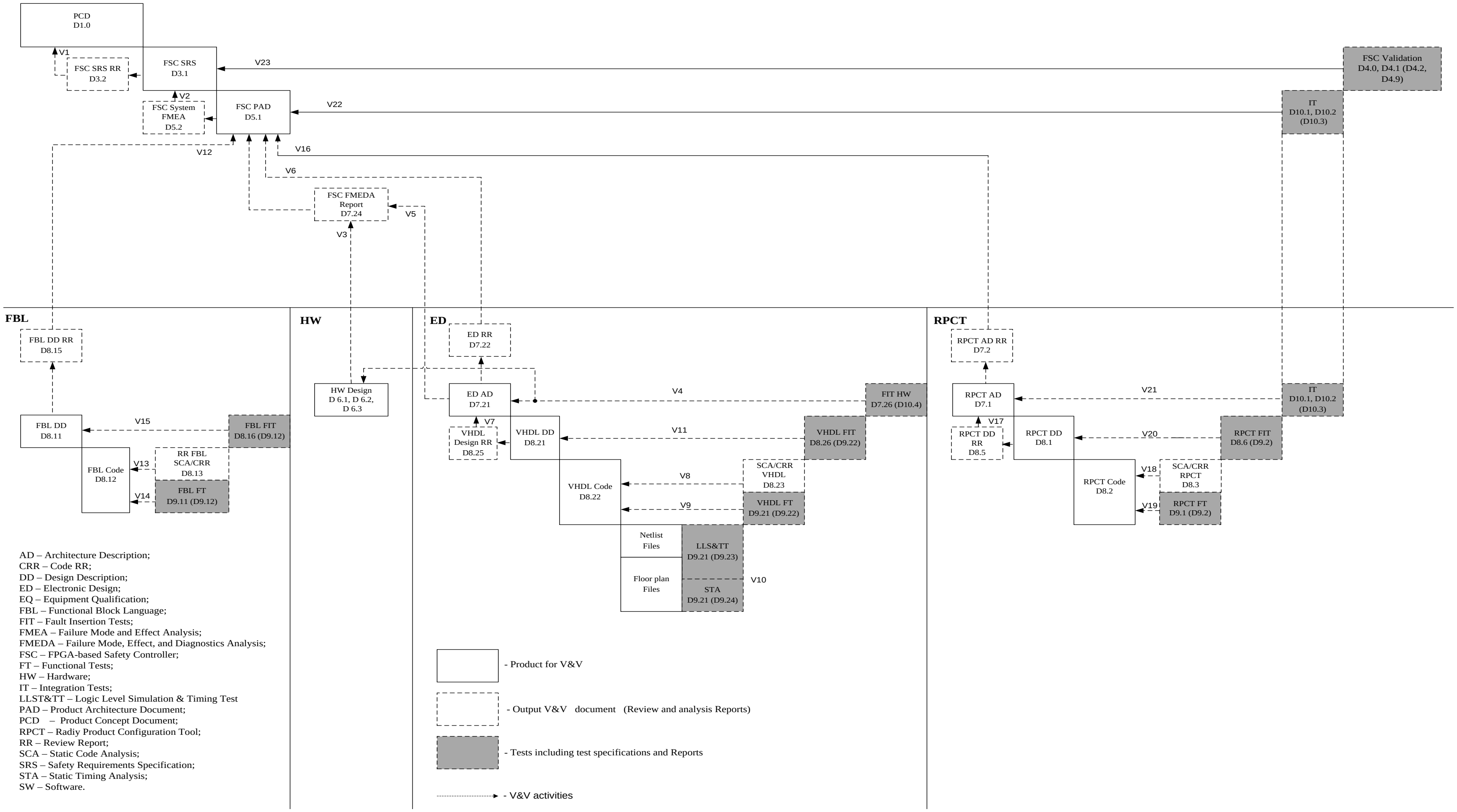
5.2 V&V techniques applied to the Development process

The FSC has a number of identifiable parts (each requiring its own set of V&V activities and associated techniques) as follows:

1. Hardware modules;
2. VHDL code of Functional Block Library (FBL);
3. VHDL code of FPGA Electronic Designs (ED) of Hardware modules;
4. Radiy Platform Configuration Tools (RPCT); and
5. Custom tools used with the FSC product.

The above parts are subjected to a complete suite of V&V techniques. V&V may be done by review, inspection, analysis or testing.

The integration of development and V&V activities for the five parts of the FSC listed above is shown in Figure 3 below followed by a brief description of the different V&V techniques applied at each stage of the development process.



AD – Architecture Description;
CRR – Code RR;
DD – Design Description;
ED – Electronic Design;
EQ – Equipment Qualification;
FBL – Functional Block Language;
FIT – Fault Insertion Tests;
FMEA – Failure Mode and Effect Analysis;
FMEDA – Failure Mode, Effect, and Diagnostics Analysis;
FSC – FPGA-based Safety Controller;
FT – Functional Tests;
HW – Hardware;
IT – Integration Tests;
LLST&TT – Logic Level Simulation & Timing Test
PAD – Product Architecture Document;
PCD – Product Concept Document;
RPCT – Radiy Product Configuration Tool;
RR – Review Report;
SCA – Static Code Analysis;
SRS – Safety Requirements Specification;
STA – Static Timing Analysis;
SW – Software.

Figure 3. V-Shaped Lifecycle model showing all V&V activities in association with development activities

The solid boxes in Figure 3 above represent development phases subject to V&V activities. Each of the above activities is also associated with one of the development categories referred to in section 4.4 above. For example, the System Requirements Specification results from the execution of the Requirements definition process described in section 4.4.2 above and incorporates elements of all the FSC identifiable parts, whereas the VHDL DD is part of the Detail Design Process described in section 4.4.3 above and it is specific to the Electronic Design part (item 3 in section 5.2 above)

The shaded boxes in Figure 3 represent all V&V tests associated with each of the above described development activities.

The following is a description of each of the test types referred to in the above mentioned shaded boxes:

1. **Functional Tests.** These comprise the lowest level of software testing and they follow a "white-box" approach, in that the testers are familiar enough with the coding to stimulate the software through the different possible logic paths to ensure that low level functional requirements are met in every case.
2. **Fault Insertion Tests (FITs).** The purpose of FITs is to demonstrate that the implementation of safety functions in the FSC platform hardware and software is correct and complete, unaffected by faults and for cases that they might be affected, that the failure is detected and the system is taken to the safe state within the required time specified in the SRS.
   At RPC Radiy, we instrument our PC boards with relays and make extensive use of card extenders so that individual and combination of faults can be injected in order to observe components response.
3. **Logic and Timing Simulation Tests.** VHDL components are treated as the equivalent of hardware design and as a result they require both logic and timing robustness testing. These types of tests involve simulations to verify the operation of digital circuits, in this case of the Netlist and Floor Plan Files for each VHDL component, in order to verify their logical and post layout timing correctness. The logic of the VHDL components are tested at the gate level to ensure the correct outputs result from all possible combination of inputs.
4. **System Integration Tests.** After low level testing and analysis are complete, all hardware and software sub-systems identified in section 5.2 are tested as an integrated system to expose faults in the interfaces and in the interaction between lower level integrated components. Testing is usually black box as the code is not directly checked for errors.

Unlike most products developed and certified to IEC 61508, the FSC is a very general product, which can be deployed in a vast number of configurations and may be configured with any combination of I/O modules in up to 14 slots, where the application logic can be any practical combination of hundreds of blocks selected from over 20 of these in the Function Block Library. System Integration test cases are developed against representative configurations as defined in the Verification and Validation Plan.

5. **Validation Tests.** These tests are conducted separately on the integrated hardware and software and are designed to ensure compliance, in this case of the separately integrated hardware and software, with their respective black box requirements (see section 4.4.2 above).
   Scope of validation tests encompasses all components identified in section 5.2.
   Except for some requirements which are being validated via analytic techniques, testing is the primary technique adopted by RPC Radiy for the validation of our FSC platforms.

   For the same reasons as described above for System Integration tests, Validation test cases are developed against representative configurations as defined in the Validation Plan.

The dashed lined boxes in Figure 3 represent verifications performed via analysis, review or inspection associated with the development process. The above figure provides an indication of which document types are subject to each or a combination of the above approaches to verification by referring to associated outputs. The following is a description of each of the verification activities and document types that they apply to.

1. **Review and comment (R&C).** This is a recorded check of a document's contents and correctness that does not follow an analytic process or use a tool. Individuals in the RPC Radiy development organization who did not take part of the preparation of the document, based on their knowledge or association with the product, are selected as reviewers of the document's contents for completeness, correctness, clarity and consistency with other documents in the project. The resulting output is an R&C report. In general, all documents associated with the Product Concept Definition phase (section 4.4.1), coding guidelines as well as Test Plans, Specifications and Reports are subject to verification via the R&C process.
2. **Requirements traceability.** The purpose of requirements tracing is to ensure that all and only the necessary product requirements are implemented and tested.
   The RPC Radiy FSC development project implements requirements tracing based on IEC 61508 Edition 2 and all nuclear standards.

   This tracing is required to be supported by tools capable of analysing the design and verification documents, demonstrating completeness and helping to detect conflicts.

The implementation status of the safety requirements are being documented in a Requirements Tracing Matrix (RTM), in which the tracing information is given by means of a cross-reference list indicating how requirements defined in the different documents paragraphs are allocated to the FSC platform components. All documents including test specifications at the system and product level are being reviewed to ensure that requirements included in them are complete, unambiguous, consistent among documents and that all unnecessary requirements are excluded.

3. **Document Inspection (DI).** This is a formal process of document verification, according to a defined procedure. The resulting output is a Review Report (RR). This technique is applied to the following document types:

    a. Documents that are outputs of phases where the requirements tracing process does not manage requirements. For these cases the inspection shall include the tracing and confirm consistency between requirements of the previous level and implementation at the next level.
    b. System FMEA. System FMEA and FMEDA documents. Even though these are "verification documents" (see below), they are reviewed because they are used later as design or design evaluation documents.
    c. Product Hardware and Software design documents (Software DD, Product SRS, modules ED and AD)
    d. Verification of System architecture documents (PAD)
    e. Verification of FBL DD and code
    f. Verification of RPCT AD, DD and code

4. **Analysis** involves a discipline analysis or use of a tool. Examples are FMEA, FMEDA, system criticality analysis, static timing analysis and static code analysis. The following are brief definitions of each of these:

    a. Ref. [2]. Failure modes and effects analysis (FMEA) is a systematic technique used during the conceptual phase of the design for analysis of potential failure modes within a system. The main objective is to identify potential failure modes based on past experience with similar products or processes, allowing developers to design those failures out of the system fairly in advance thus reducing development time and costs. Failures are classified according to their consequences, frequency of occurrence and ease of detection.

b. Ref. [2]. Failure Modes Effects and Diagnostic Analysis (FMEDA) is a systematic technique to obtain product level failure rates, failure modes and diagnostic capability.

c. System Criticality Analysis (SCA). The objective of SCA is to identify modules of lower criticality in which to allow design and verification methodologies corresponding to a lower SIL level.

d. Static Timing Analysis (STA). This method is used to compute the expected timing of the different circuits by analysis. The objective is to find the worst-case delay of the electronic circuits at the different steps and stages over all possible input combinations and parameters (such as temperature and voltage) fluctuations.

e. Static Code Analysis. The purpose of this analysis is to verify the code by examining, without executing, via manual or automated means, every possible branch within each module.

6. V&V related documentation

General platform requirements at RPC Radiy are documented as “Perceived Safety Needs” in a document entitled “Product Concept Document” (not a formal safety related document). The concept that is documented in the PCD will be the basis for the top-level formal design documents, i.e. the Safety Requirements Specification (SRS), the Product Architecture Document (PAD) and all derived safety requirements included in lower level documents.

The structure of testing documentation is in general developed following the principles of IEEE 1012, which includes a Test Plan, a Test Specification, a Test Procedure (if such detail is required) and a Test Report for each test activity. IEC 61508 requires that the test documentation cover the same material, but is not prescriptive as to the document set.

7. Summary and conclusions

Given the criticality of many of the applications in which RPC Radiy is using FPGA platforms within the nuclear industry, our approach was to institute a V&V program that is in general compliance with IEC 61508 and processes defined in IEEE Std 1012, “IEEE Standard for Software Verification and Validation”, starting from the criteria established in the above standard for the definition of the System Integrity Level (SIL), down to the processes and procedures mandated by the adopted SIL3 level for nuclear applications.

V&V activities at RPC Radiy cover all phases of the development portion of the life cycle until the equipment is released to the customer. We prepare documentation and work with our customers to support them in their effort to establish and apply all the necessary processes procedures and tools that must be in place throughout the rest of our products' lifecycle.

The V&V plan established by RPC Radiy mandates the adoption of appropriate techniques to ensure compliance with all system requirements as well as the adequacy of user documentation at all stages of the product life cycle. V&V techniques and associated documentation for all the above stages and all identifiable FSC parts are described in sections 5 and 6 respectively. The above parts are subjected to a complete suite of V&V techniques. Whereas Validation consists mostly of testing, Verification may be done by review, inspection, analysis or testing. V&V and development activities are conducted in parallel and follow the sequence illustrated in the right branch of the IEC 61508 V-Model, where the left branch shows, in a top-down fashion, the sequence of development activities and the right branch, in a bottom-up fashion, the sequence of V&V activities. The integration of development and V&V activities for the different parts of the FSC is shown in Figure 3.

IEC 61508 establishes minimum levels of independence between those carrying out development and functional safety assessments of safety related systems. These depend on the consequences of system failure and integrity levels and could be, from the least to the most critical applications, at the person, department or, as mandated by SIL 3 certification, at the organizational levels.

8. References

[1] V. Sklyar, I. Bakhmach, V.Kharchenko, A.Andrashov and O.Baranova, "Advanced instrumentation and control systems for CANDU refurbishment". Proceedings of the 9th CNS International Conference on CANDU® Maintenance
Toronto, Ontario, Canada, December 4-6, 2011

[2] J. Grebe and Dr. W. Goble, "FMEDA – accurate product failure metrics"