V&V of FPGA Based Systems for Nuclear Applications

By: Sergio A. Russomanno

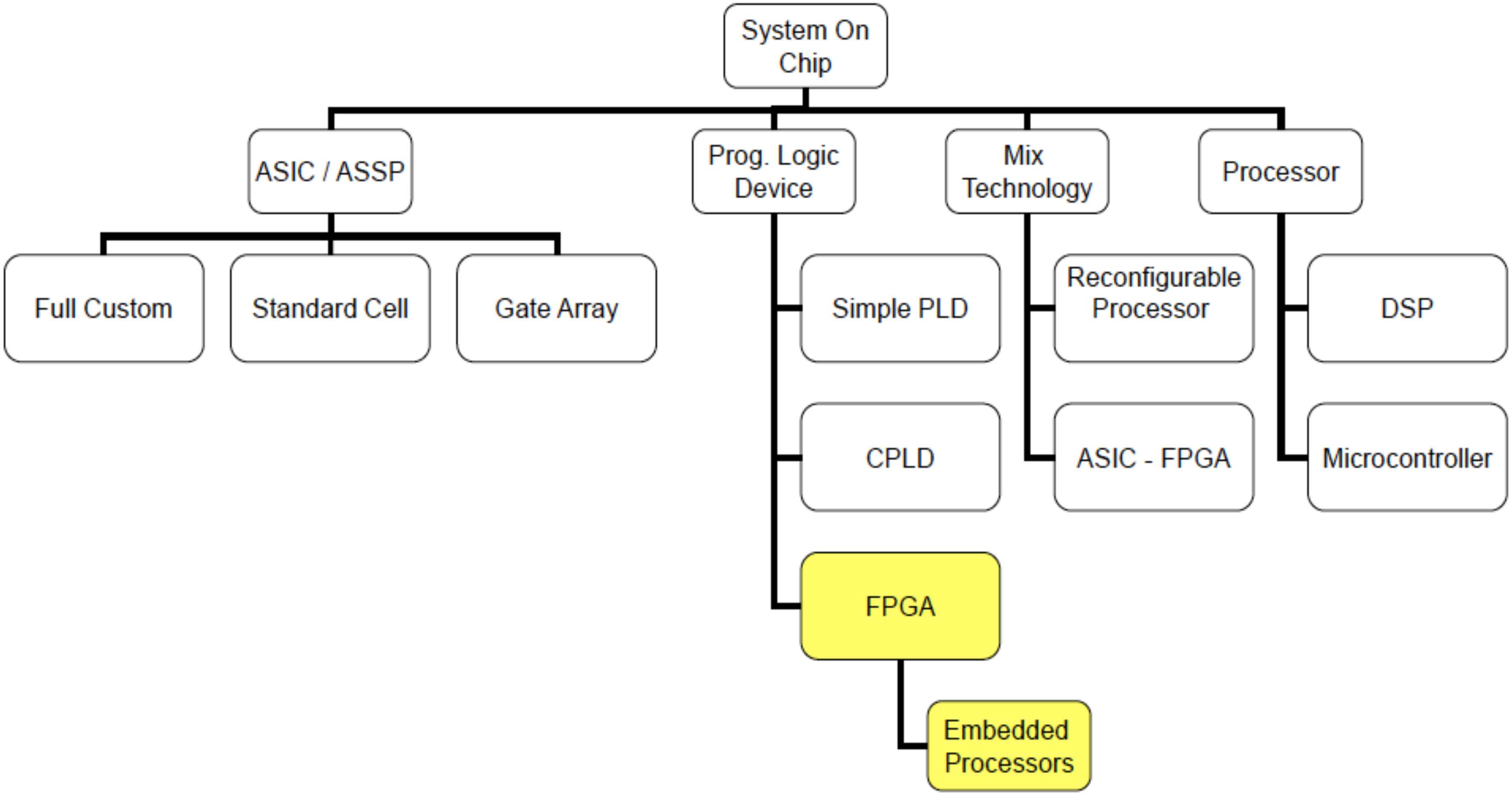
Presented at the March 4th to 7th IAEA National Workshop ARG2013 on Obsolescence issues and Digital I&C modernization approaches

Sunport
Connecting Forward

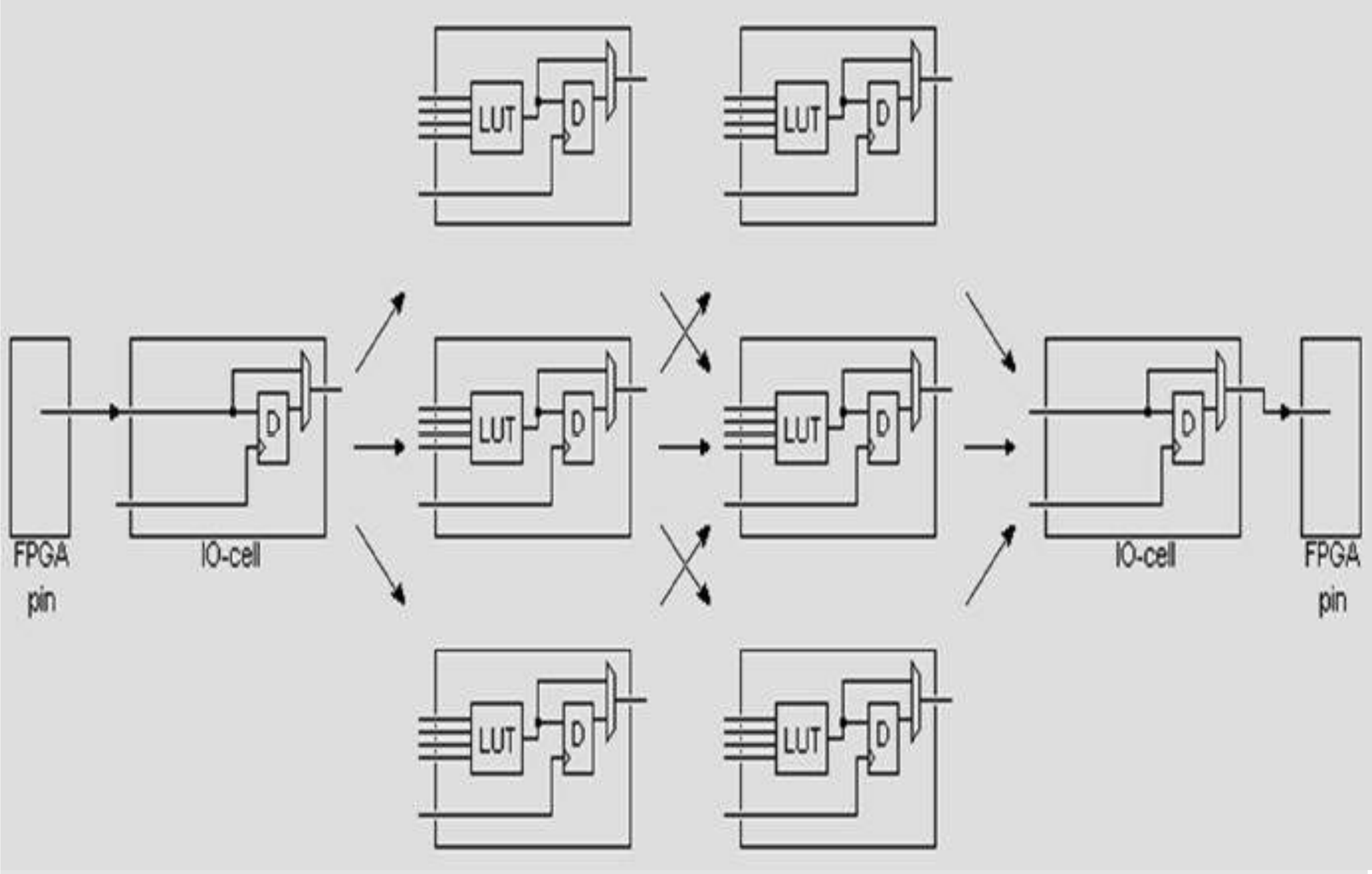
Outline

1. Applications
2. What is and why do we perform V&V
3. Basis and criteria for the establishment of V&V processes
4. FPGA platform Safety life cycle, associated processes and V&V activities

FPGAs in the overall scenario

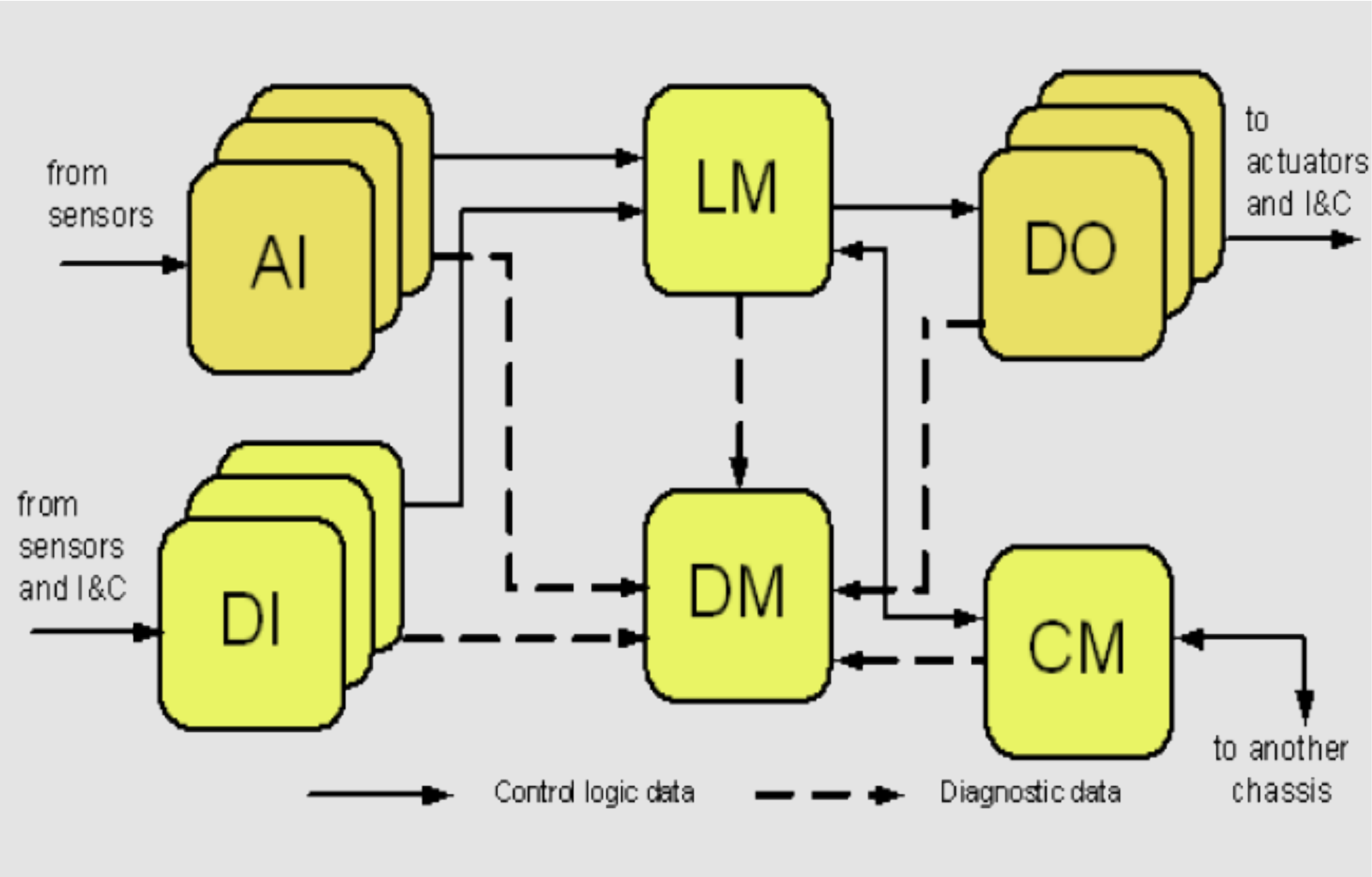


Inside the FPGA Chip



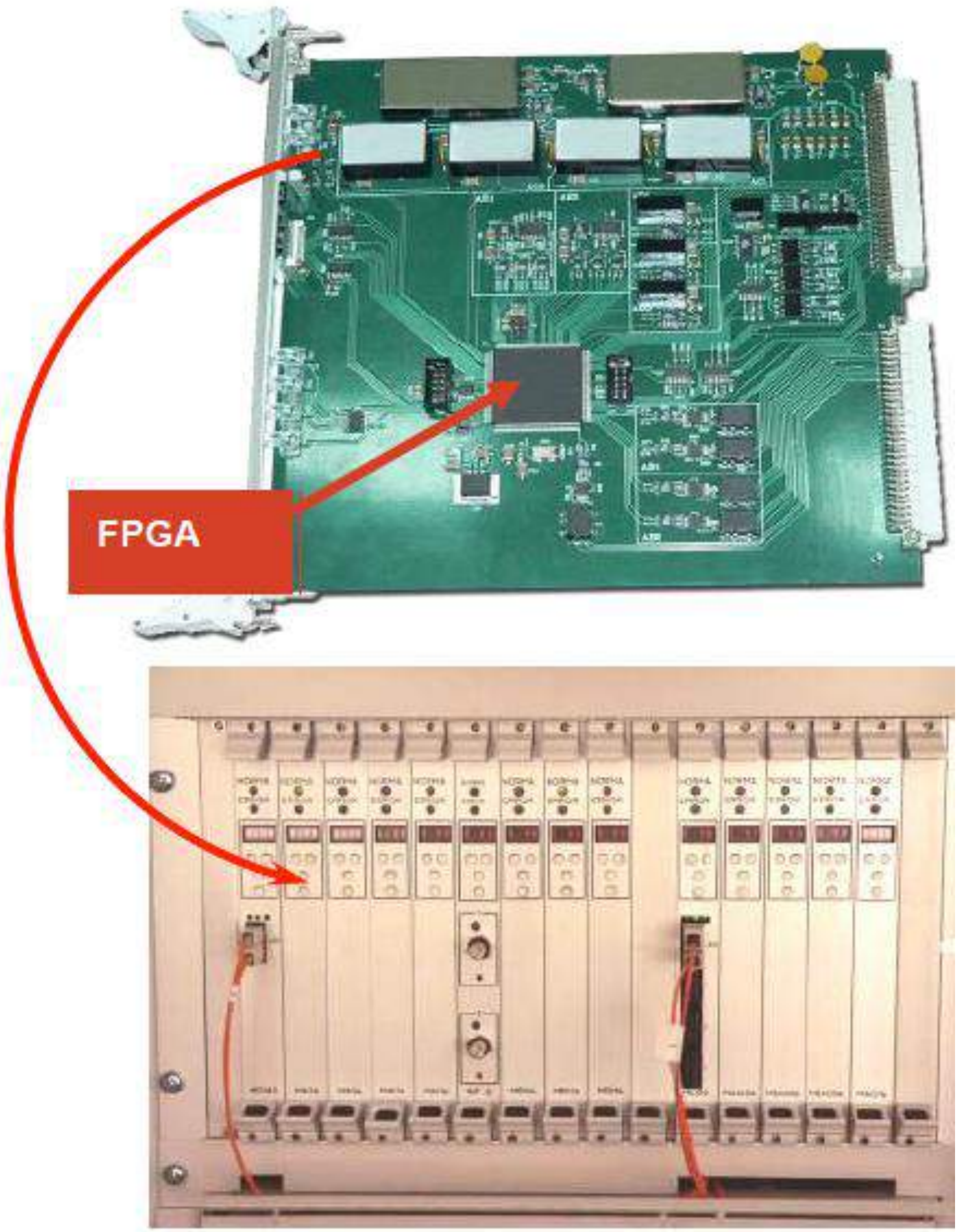
Sun*port*

Basic FPGA system architecture



Applications

- FPGA-based I&C platform
- Safety related systems
- Process control systems in research reactors
- Electric power supply equipment
- Main Control Room panels
- Fire alarm and suppression systems
- Seismic monitoring systems



Safety Systems Applications

Sun port

Main Control Room Applications

Why V&V?

Today's FPGAs platforms are used in applications that ***involve millions of gates*** running at increasing clock speeds.

Synthesis tools perform optimizations that drastically change design implementation structures.

Given the complex nature and criticality of many of the applications, it is important that we adopt a ***rigorous approach to V&V*** in compliance with widely recognized standards.

Why V&V?

Also, from a project perspective, V&V:

Facilitates early detection and correction of design errors;

Enhances management insight into process and product risk; and

Supports the development life cycle processes to ensure compliance with program performance, schedule, and budget requirements

What is V&V?

An objective assessment of products and processes ***throughout their life cycle*** to demonstrate that requirements are correct, complete, accurate, consistent, and testable.

Basis for the establishment of V&V processes and procedures

Suppliers to implement a V&V program in full compliance with processes defined in:

IEC 61508. Functional safety of electrical/ electronic/ programmable electronic safety-related systems;

IEC 62566 Requirements specific to FPGA design for NPP I&C systems;

IEC60880. Nuclear power plants. Instrumentation and control systems important to safety;

IEEE Std 1012. Software Verification and Validation;

Basis for the establishment of V&V processes and procedures

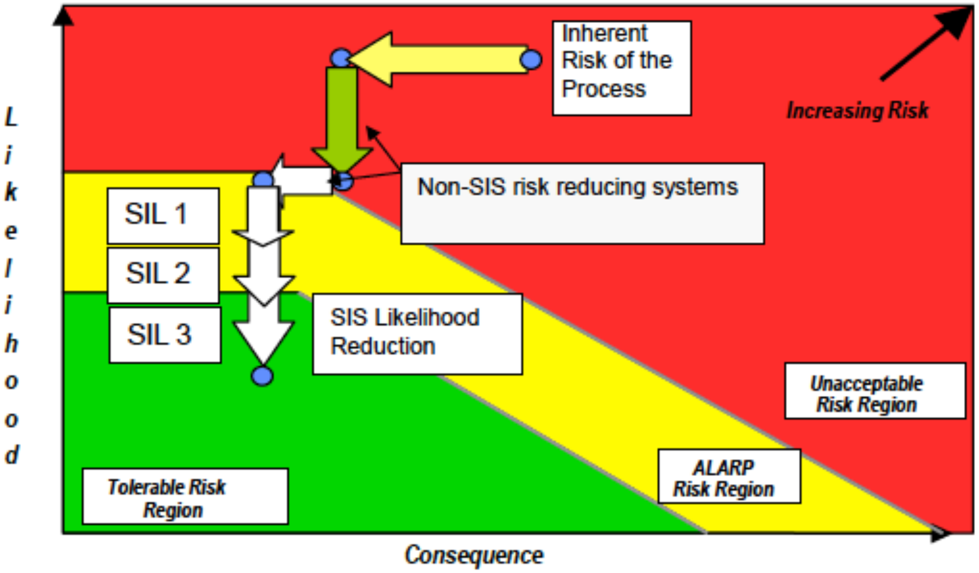
IEEE 1012 uses a software integrity level (SIL) approach to quantify software criticality;

SIL is based on the consequence and likelihood of the event to be mitigated;

V&V processes and procedures are based on SIL level.

Criteria used in IEC 61508 to select SIL – Safety Integrity Level. (applies to both hardware and software)

- Establish Tolerable Risk (tolerable level of consequence);
- Establish likelihood of initiating events;
- Determine probability of success of existing effective mitigating systems;
- Calculate mitigated risk;
- Compare to tolerable risk:
  - Determines Risk Reduction Factor
  - Defines SIL

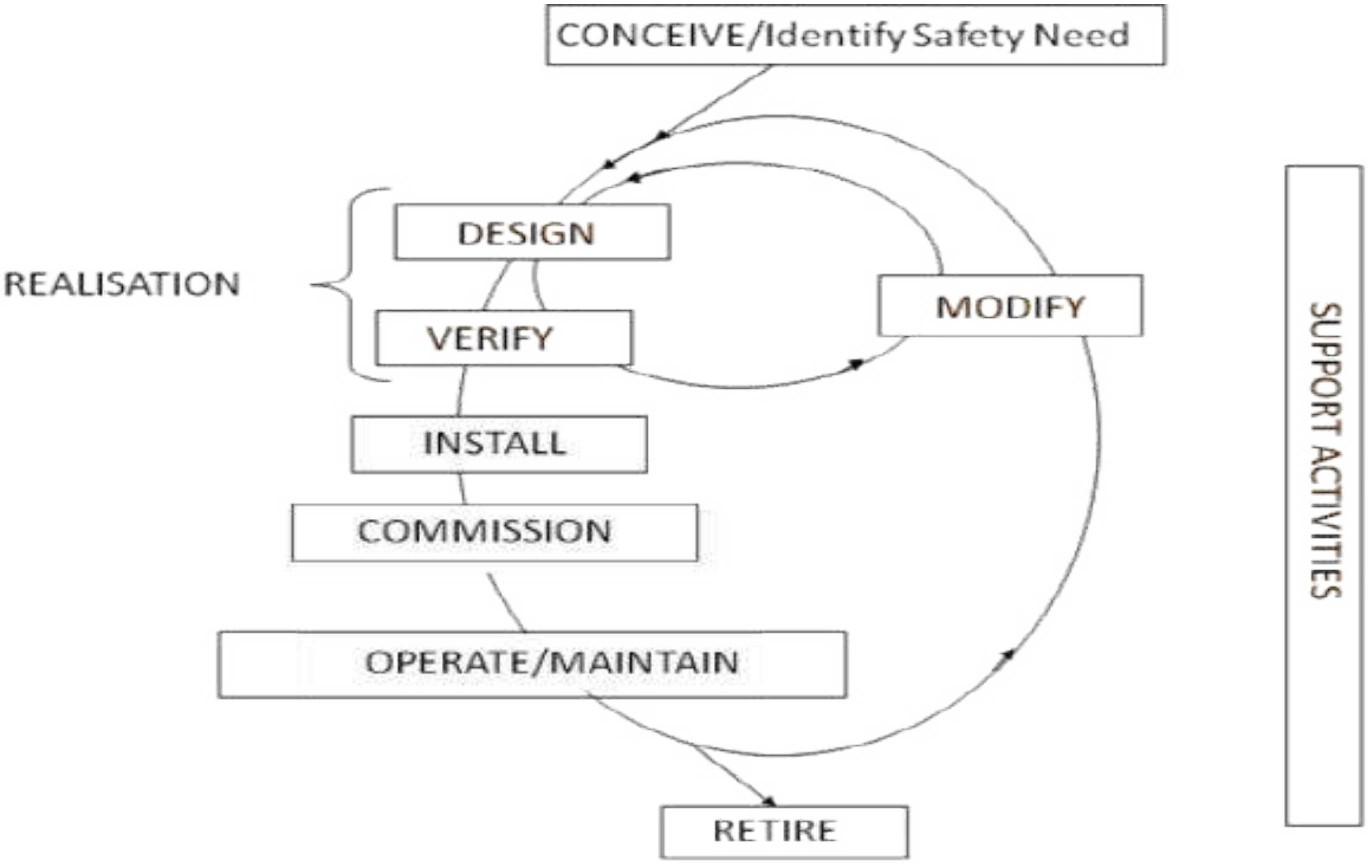


Comparison of Key V&V Issues of Various Standards

	IEC 61508	IEC 60880	IEEE 1012
Verification at every stage in Safety Life Cycle	✓	✓	✓
Independence of this Verification		✓	✓
Validation at the end of the Safety Life Cycle	✓	✓	✓
Independence of this Validation		✓	✓
Independent assessment of all activities at the end, before use	✓	✓	✓
Requires proof of coverage (tracing):			
from stage to stage in design (e.g. SRS→PAD, PAD→ITP)	✓	(✓)	✓
in testing of design/implementation	✓		
Specific test coverage requirements (e.g. branch, MC/DC)	✓	✓	
Fault injection testing to demonstrate coverage claimed in FMEDA	✓		

Sun port

Safety Life Cycle



Life Cycle processes and associated V&V approach

1. **Management:**

   i. Overview and support of all below listed activities;

   ii. V&V activities consist in the auditing (work processes and documentation review by an independent organization).

2. **Supply:**

   i. Includes activities such as deciding to reply to an acquirer's request for proposal and determination of procedures and resources needed to plan and execute the project;

   ii. V&V via R&C, inspection and audits to ensure that all that will be supplied for the completion of the final product is adequate, complete and meets clients and regulatory requirements.

Life Cycle processes and associated V&V approach Cont…

3. **Acquisition:**
   1. Spans from the definition of the need to acquire a product or service to the acceptance of the same;
   2. Verified mostly via R&C, Inspection and audits to ensure that all that will be supplied for the completion of the final product is adequate, complete and meet clients and regulatory requirements.
4. **Development:**
   1. The development process includes concept and detail requirements definition, detail design, implementation and installation activities;
   2. Dealt with in the next slides.

V&V activities

- V&V activities are conducted throughout the system lifecycle:
  - Management process;
  - Supply process;
  - Acquisition process;
  - Development process;
- Verification activities consist of a combination of different techniques such as review, inspection, analysis or testing;
- Validation activities consist mostly of testing.

V&V techniques applied to the Suppliers Management Process

- Safety Systems suppliers must establish and support an internal organization and management structure responsible for the implementation and oversight of all V&V activities associated with the entire lifecycle of the product.
- Management processes must be V&V'd by an external organization.

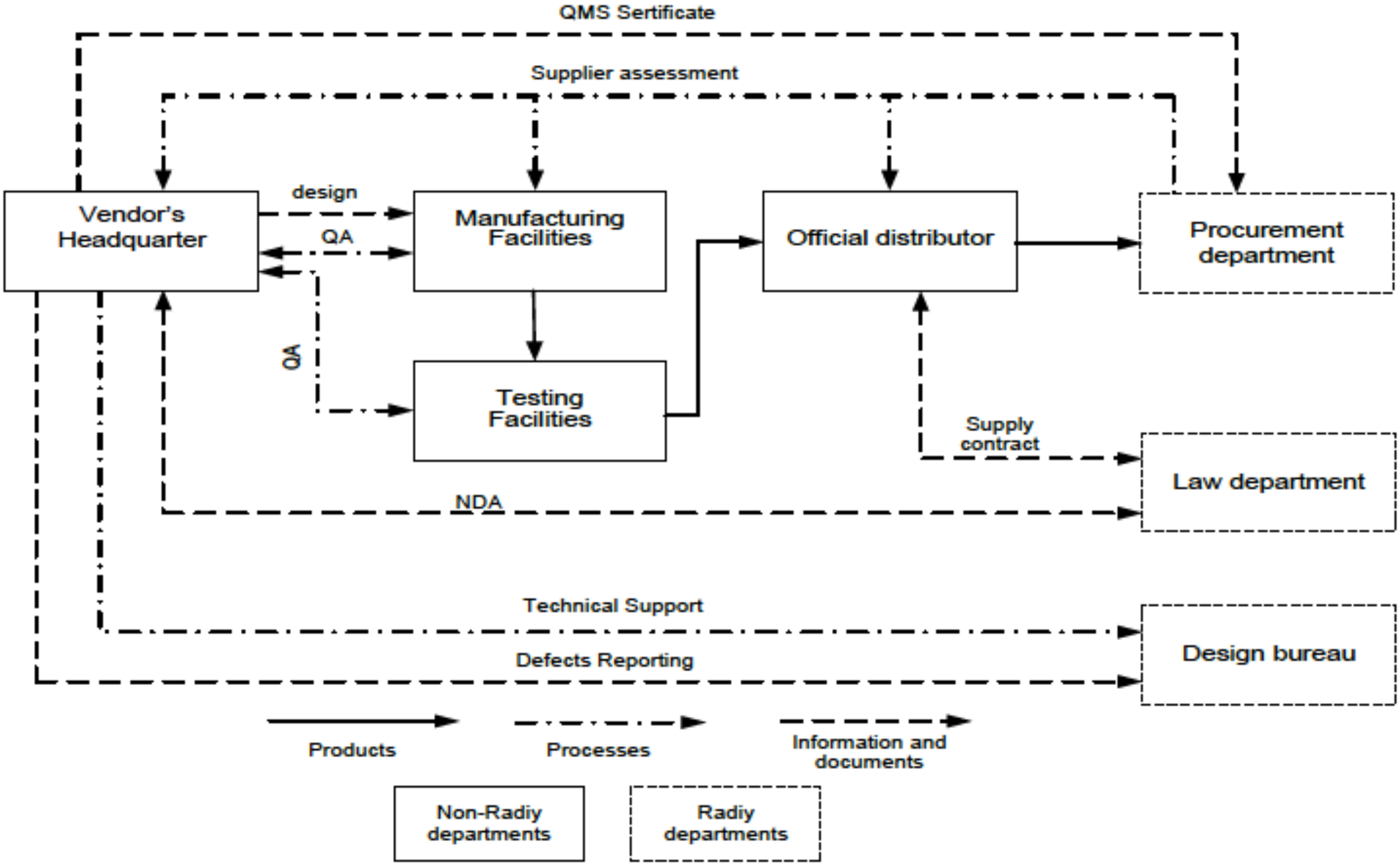
V&V techniques applied to the Supply process

- Clients and regulators impose requirements on manufacturers products and these should be reflected in their work processes.
- Above requirements are normally reflected in Request for Proposals and other documents that are part of the bidding process.
- Suppliers and stake holders within the utilities should engage in early discussions to ensure that requirements are understood in sufficient detail and early enough to be able to reflect them in the suppliers work processes and thus devise V&V mechanisms to ensure that such requirements are met.

V&V techniques applied to the Acquisition process

- The Acquisition process is verified mostly via R&C, inspection and audits of vendors 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.

Qualification of vendor's ability to meet regulatory expectations: Analysis of FPGA components supply chain



V&V techniques applied to the Development process

- FPGA based systems main components requiring their own set of V&V activities and associated techniques are:
  - Hardware modules;
  - VHDL code of Functional Block Library (FBL);
  - VHDL code of FPGA Electronic Designs (ED) of Hardware modules;
  - Configuration Tools.

- All above parts should be subjected to a suite of V&V techniques which involve, as applicable, review, inspection, analysis and/or testing.

Development process. Stages and associated V&V activities

1. **Product concept definition (requirements at the system level) :**

   - Identification of requirements and platform architecture;
   - Definition of applicable standards;
   - Type of FPGA technology and associated development and testing tools,
   - Amount and type of self testing;
   - Assignment of safety and non safety functions in order to minimize and simplify V&V activities are made at this stage.

   V&V activities are designed to ensure completeness, correctness, testability and consistency of the above 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.

Development process. Stages and associated V&V activities

2. **Requirements definition (hardware, software, subsystems):**

- Functional, performance and safety requirements;
- Diagnostics;
- Human Factors;
- Interfaces with external components;
- Communication requirements.

Implementation of above requirements are V&V'd to ensure that:

- Requirements are consistent with those specified in higher level doc's;
- Every possible branch of the logic that implements the above requirements results in the desired outcome (White Box testing);
- Inputs result in the desired outputs independently of implementation details (Black Box testing).

Development process. Stages and associated V&V activities

3. Detail design:

- Requirements are translated into an architecture involving software and hardware components;
- Product Architecture Design. Functionality allocated to hardware and software modules of the product;
- Software Architecture Design: Software functionality allocated to the different modules and developed. The output of this activity is commented VHDL code and associated design description;
- Electronic Architecture Design.

V&V includes testing in a simulated environment.

Development process. Stages and associated V&V activities

4. Implementation:

- Translation of the chosen architecture and functionality assigned to the different software and hardware modules into database structures, communication protocols and related machine executable representations.

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

Development process. Stages and associated V&V activities

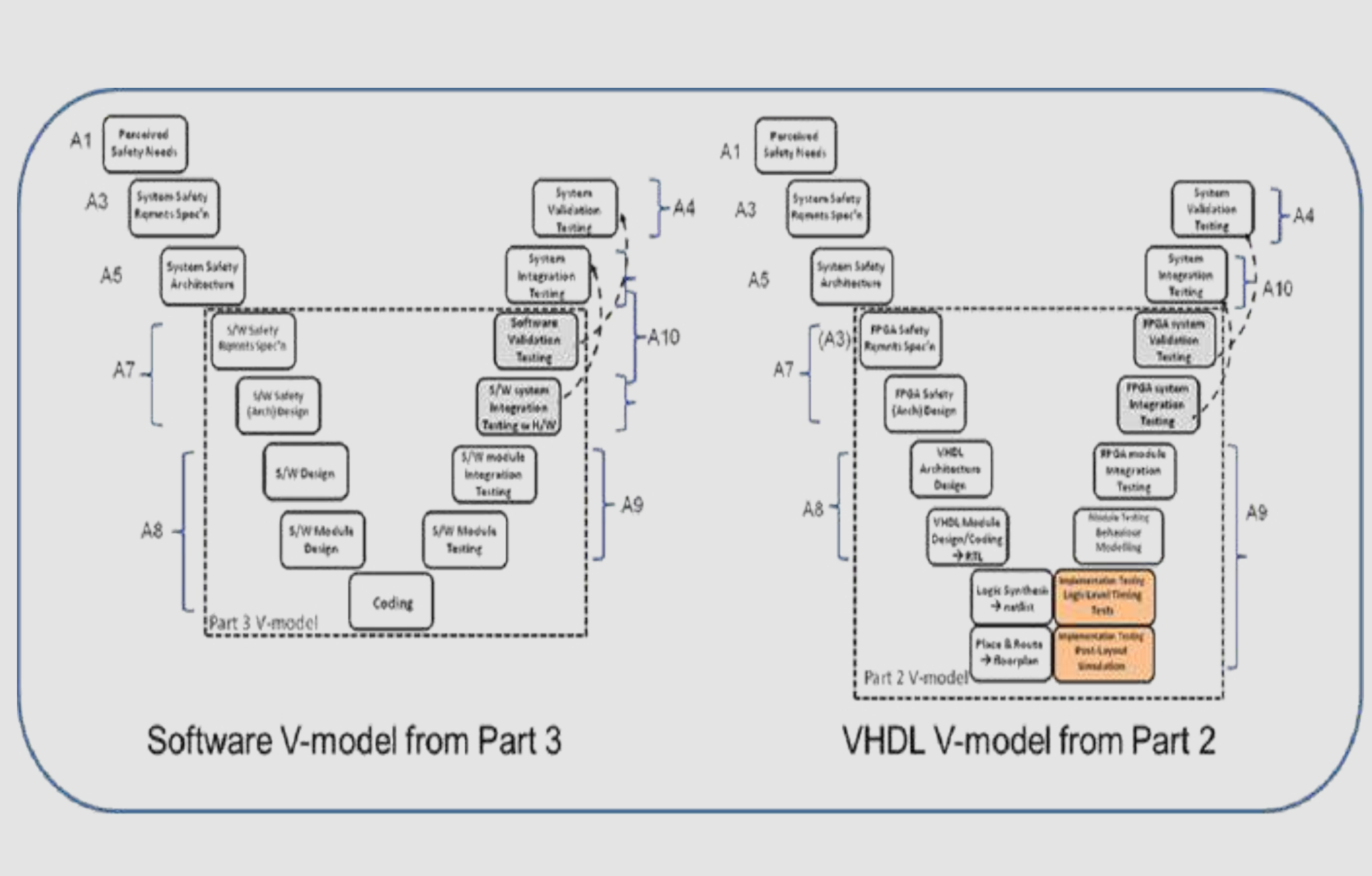
5. **Installation of the different components into a final integrated platform:**

    - Embedding functionality in the target environment.

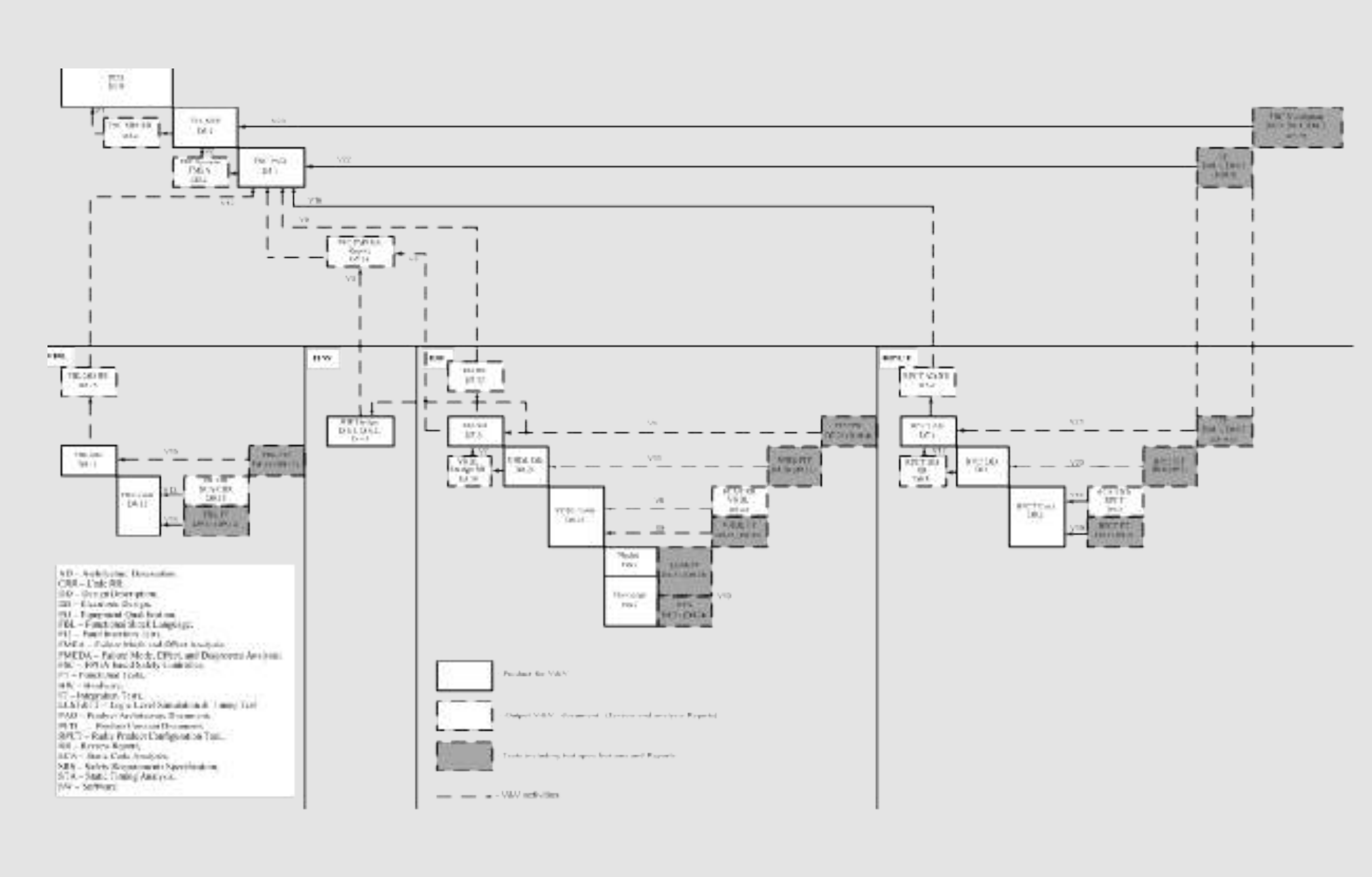
V&V involves reviewing and testing of the platform composed of final components as a clearly defined and configured product. Includes verification that the correct and intended versions of all components are pre-tested, verified and installed in the platforms prior to execution of the different levels of system testing.

Configuration and change control should continue after systems are delivered to site. After product acceptance, final users become responsible for the establishment of their own processes, procedures and tools.

Integrated Development/V&V activities. S/W and E-design.

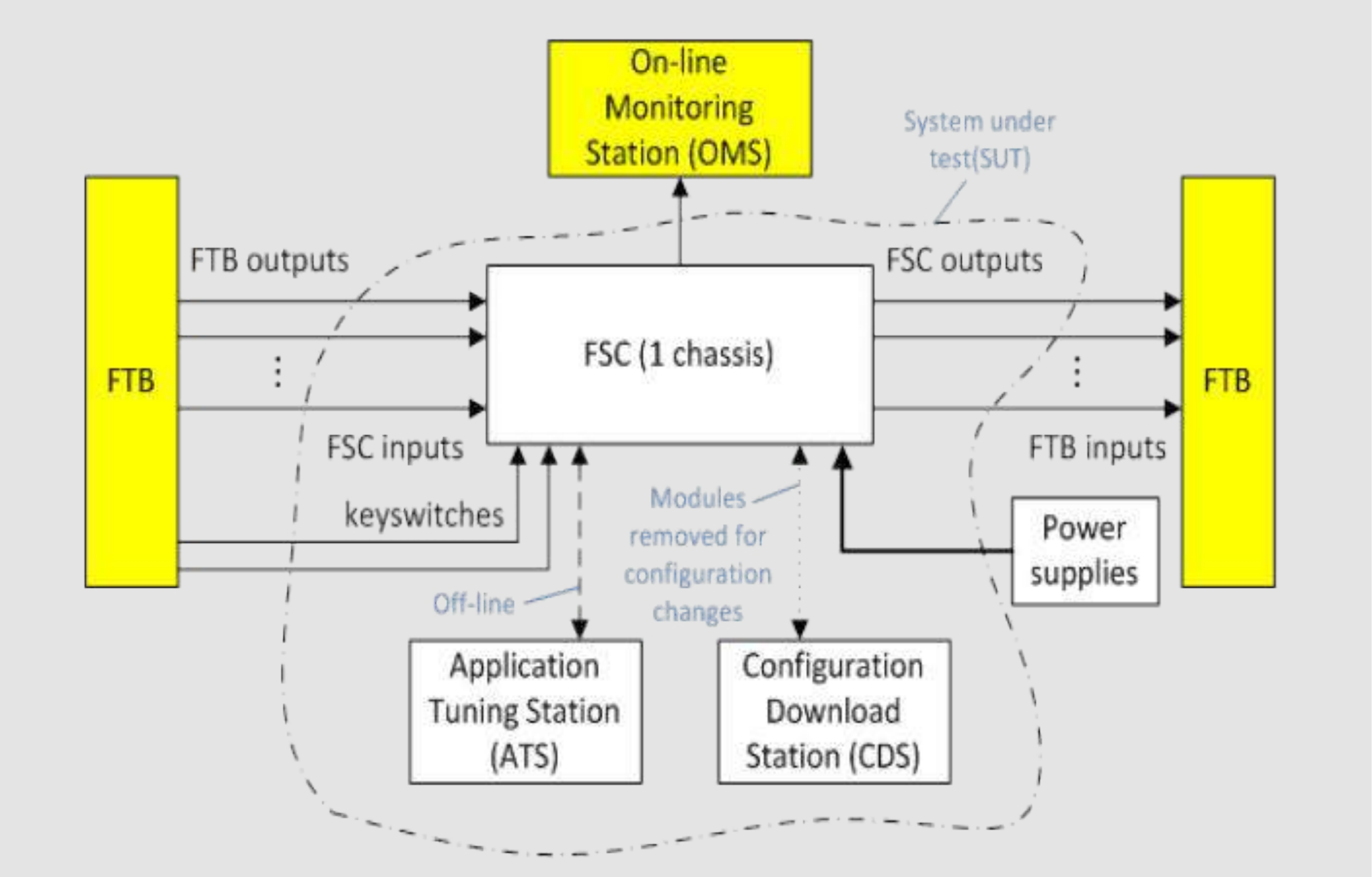

A1
Perceived Safety Needs
A3
System Safety Rqmnts Spec'n
A5
System Safety Architecture
A7
S/W Safety Rqmnts Spec'n
S/W Safety (Arch) Design
A8
S/W Design
S/W Module Design
Coding
Part 3 V-model
S/W Module Testing
S/W module Integration Testing
A9
S/W system Integration Testing w H/W
Software Validation Testing
A10
System Integration Testing
System Validation Testing
A4
Software V-model from Part 3
A1
Perceived Safety Needs
A3
System Safety Rqmnts Spec'n
A5
System Safety Architecture
A7
(A3)
FPGA Safety Rqmnts Spec'n
FPGA Safety (Arch) Design
A8
VHDL Architecture Design
VHDL Module Design/Coding → RTL
Logic Synthesis → netlist
Place & Route → floorplan
Part 2 V-model
Implementation Testing Post-Layout Simulation
Implementation Testing Logic Level Timing Tests
Module Testing Behaviour Modelling
FPGA module Integration Testing
A9
FPGA system Integration Testing
FPGA system Validation Testing
System Integration Testing
A10
System Validation Testing
A4
VHDL V-model from Part 2

Integrated Development/V&V activities. S/W, E-design, FBL and tools.


FBL
HW
SW
RPCT
AD – Architecture Description
CRR – Unit 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 Diagnostic Analysis
FT – Functional Tests
HW – Hardware
IT – Integration Tests
PAD – Product Architecture Document
RPCT – Radio Product Configuration Tool
RR – Review Report
SCA – Static Code Analysis
SRS – Safety Requirement Specification
STA – Static Timing Analysis
SW – Software
Product for V&V
Output V&V document (Review and analysis Reports)
Tools including fault injection and Reports
V&V activities

Sunport

Validation Configuration Platform


On-line Monitoring Station (OMS)
System under test(SUT)
FTB
FTB outputs
FSC outputs
FSC (1 chassis)
FTB
FSC inputs
FTB inputs
keyswitches
Modules removed for configuration changes
Power supplies
Off-line
Application Tuning Station (ATS)
Configuration Download Station (CDS)

Types of tests carried out as part of the V&V process

1. Functional Tests:

- The lowest level of software testing;
- “white-box” approach. Testers are familiar enough with the coding to stimulate the software through all logic paths;
- Applied to the design of the Function Blocks Library, HDL code and suppliers proprietary tools.

Types of tests carried out as part of the V&V process

2. Fault Insertion Tests:

- PCB extenders and devices used to inject single or combination of faults to stimulate self checks and diagnostic functions;
- To demonstrate the correct implementation of above functions so that when faults are detected the system is taken to the safe state within the required time;
- Applied to the design of the Function Blocks Library, HDL code and suppliers proprietary tools.

Types of tests carried out as part of the V&V process

3. Logic and Timing Simulation Tests:

- Involve simulations to verify the operation of digital circuits;
- VHDL components treated as equivalent to hardware design so they are subjected to logic and timing testing;
- VHDL components tested at the gate level to ensure that correct outputs result from all combinations of inputs;
- Applied to the Netlist and Floor Plan Files.

Types of tests carried out as part of the V&V process

4. System Integration Tests:

- Performed after low level testing and analysis are complete;
- All h/w and s/w sub-systems tested in an integrated fashion;
- Testing is usually black box;
- Applied to h/w modules, VHDL code of Functional Block Library (FBL), VHDL code of FPGA Electronic Design (ED) of Hardware modules and Configuration Tools;
- Test cases developed against representative configurations of the application as defined in the V&V Plan.

Types of tests carried out as part of the V&V process

5. Validation Tests:

- Conducted separately on the integrated h/w and s/w;
- Designed to ensure compliance with black box requirements;
- Applied to h/w modules, VHDL code of Functional Block Library (FBL), VHDL code of FPGA Electronic Design (ED) of Hardware modules and Configuration Tools;
- Except for some requirements which are being validated via analytic techniques, testing is the primary validation technique;
- Validation test cases are developed against representative configurations as defined in the Validation Plan.

Verification activities carried out as part of the V&V process

1. Review and Comments (R&Cs):

- A recorded check of a document’s contents and correctness that does not follow an analytic process or use a tool;
- Reviewers must not have taken part of the preparation of the document;
- Reviewers selected based on their knowledge or association with the product;
- The resulting output is an R&C report.

In general, applicable documents associated with the Product Concept Definition, coding guidelines, Test Plans, Specifications and Reports are subject to verification via the R&C process.

Verification activities carried out as part of the V&V process

2. Requirements traceability:

- To ensure that all and only the necessary requirements are implemented and tested;
- Must be supported by tools to help demonstrate completeness and detect requirements conflicts in different documents;
- Safety requirements status documented in a Requirements Tracing Matrix (RTM), a cross-reference list indicating where requirements appear in the different documents and are allocated to the different components in the platform;
- All documents including test specifications are being reviewed to ensure that requirements are complete, necessary, unambiguous and consistent among documents.

Verification activities carried out as part of the V&V process

3. Document Inspection (DI):

- Formal process carried out according to a defined procedure. The resulting output is a Review Report (RR);
- Inspection shall include the tracing and confirm consistency between requirements of the previous level and implementation at the next level;
- Applied to:
  - System FMEA and FMEDA documents, reviewed because they are used as design or design evaluation documents;
  - Product Hardware and Software design documents (Software DD, Product SRS, modules ED and AD);
  - Verification of System architecture documents (PAD);
  - Verification of FBL DD and code;
  - Verification of RPCT AD, DD and code.

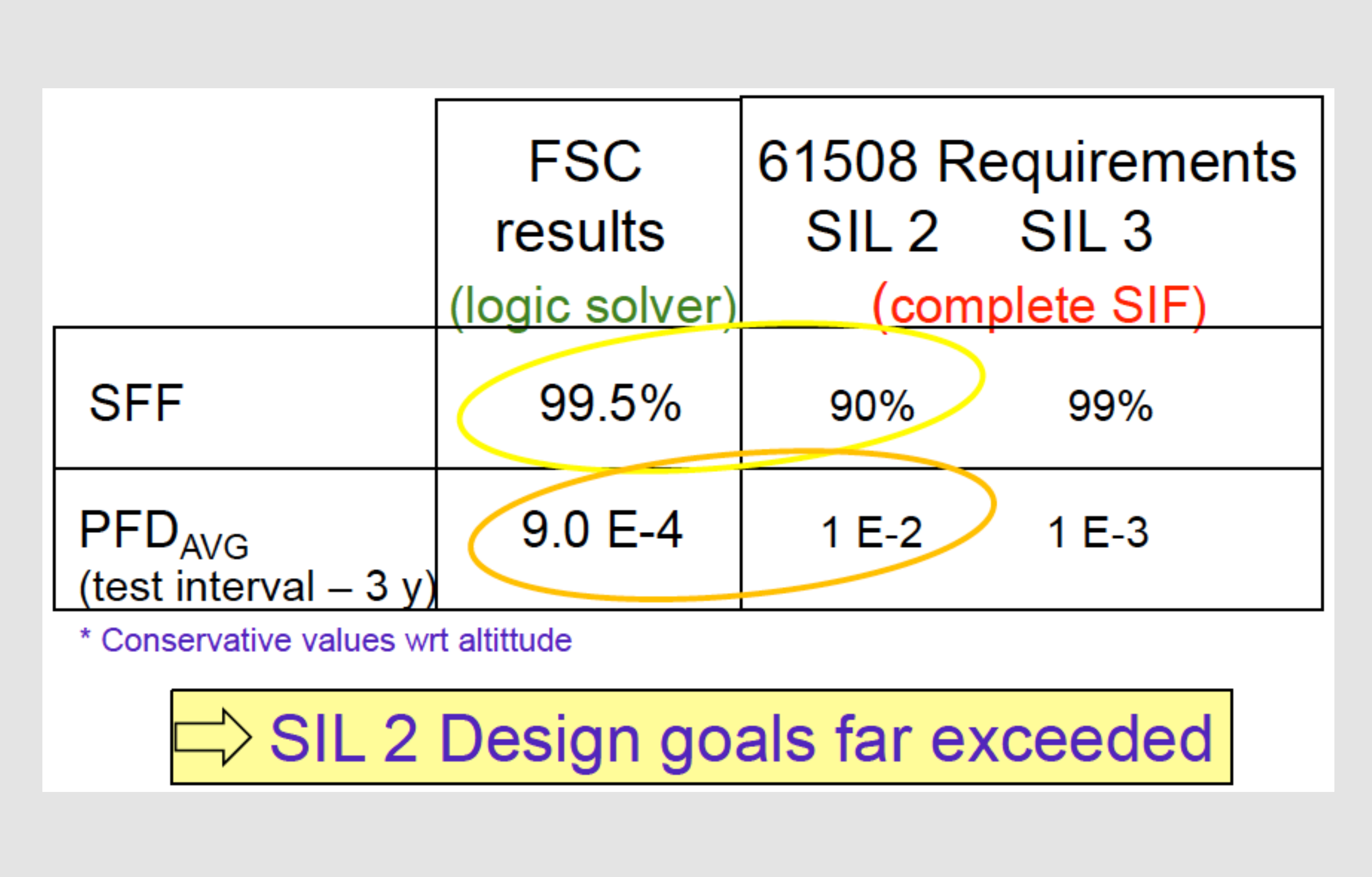
Verification activities carried out as part of the V&V process

4. Analysis:

Examples, FMEA, FMEDA, criticality analysis, static timing and static code analysis. Definitions of each of these:

- **Failure modes and effects analysis (FMEA).** Technique used during the conceptual phase of the design for analysis of potential failure modes within a system based on past experience with similar products, 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.
- **Failure Modes Effects and Diagnostic Analysis (FMEDA)** is a systematic technique to obtain product level failure rates, failure modes and diagnostic capability. This technique is used during the detail design phase of the design.

FMEDA Results for the FSC*



	FSC results (logic solver)	61508 Requirements SIL 2	SIL 3 (complete SIF)
SFF	99.5%	90%	99%
PFD_{AVG} (test interval – 3 y)	9.0 E-4	1 E-2	1 E-3

* Conservative values wrt altittude

⇨ SIL 2 Design goals far exceeded

Verification activities carried out as part of the V&V process

4. Analysis Cont’d:

- **System Criticality Analysis (SCA)**. To identify modules of lower criticality in which to allow design and verification methodologies corresponding to a lower SIL level.
- **Static Timing Analysis (STA)**. To compute the expected timing of circuits to find worst-case delays at the different stages over all possible input combinations and parameters fluctuations.
- **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.

Summary and Conclusions

1. Based on the criticality of FPGA applications Suppliers and users must institute V&V programs in compliance with IEC 61508, IEC 60880 and processes defined in IEEE Std 1012.
2. Starting from the SIL assignment, down to the processes and procedures mandated by SIL3 level for nuclear applications.
3. V&V applied to all phases of the product life cycle. Suppliers to support customers in applying all necessary processes procedures and tools required throughout the rest of their products' lifecycle.

Summary and Conclusions

4. Whereas Validation consists mostly of testing, Verification may be done by review, inspection, analysis or testing.
5. There is considerable parallellism between development and V&V activities. These follow the sequence illustrated in the right branch of the IEC 61508 V-Model.
6. Levels of independence between those carrying out development and safety assessments of safety related systems. depend on the SIL.

Sunport

Connecting Forward

www.sunport.ch

SunPort SA

LaCite Business Nucleus Avenue
De l'Universite 24 CH-1005
Lausanne, Switzerland
t: +41 213 123 901