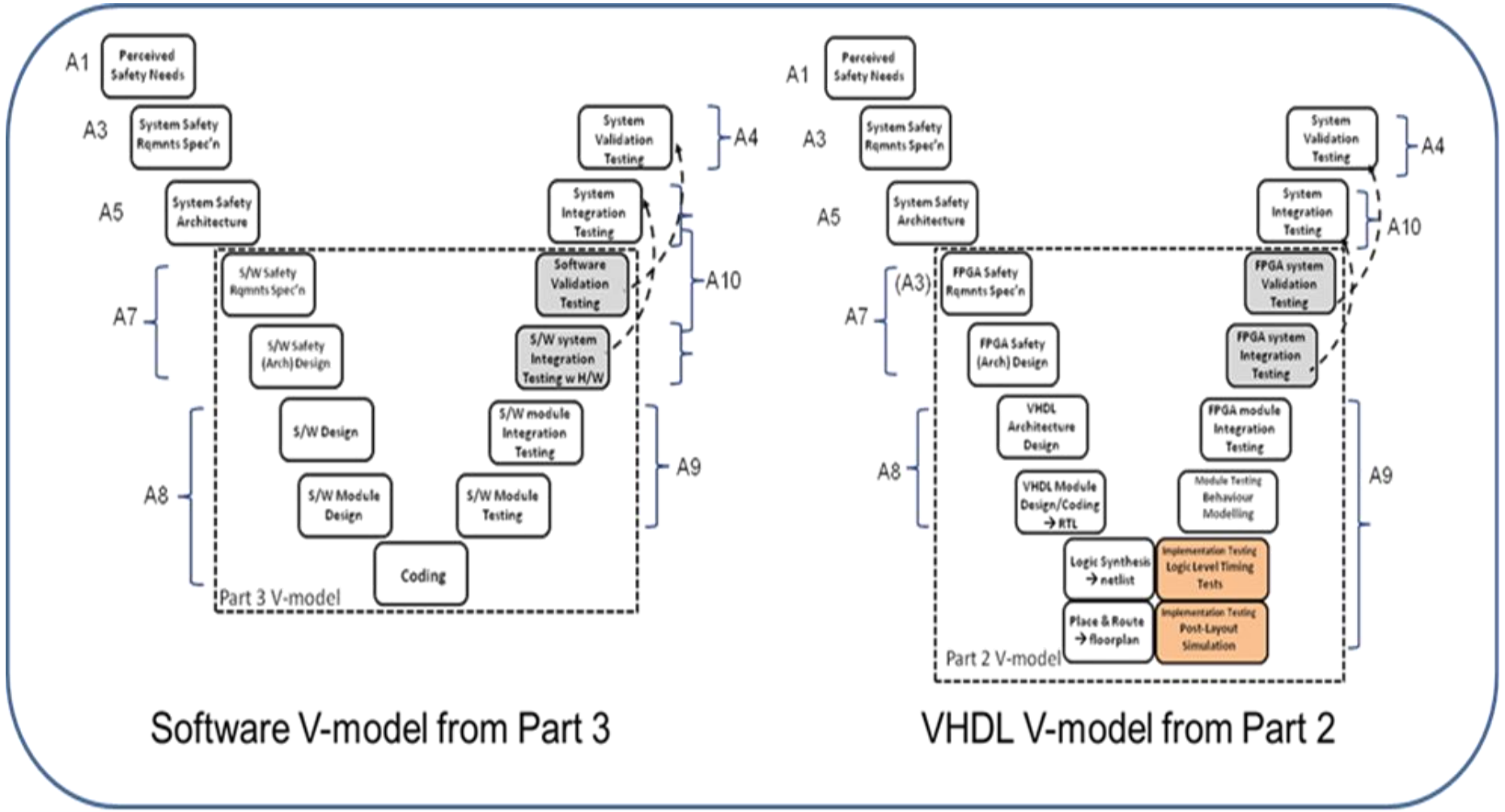
Panel Discussion. Development Tools and Processes

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



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 Cont…

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 Cont…

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 Cont…

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 appliation as defined in the V&V Plan.

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

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 Cont….

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 Cont….

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 Cont….

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

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.