Radiy experience with RadICS Platform SIL 3 certification:

adaptation of FPGA V-model to IEC 61508 requirements

and using FIT to validate FMEDA results.

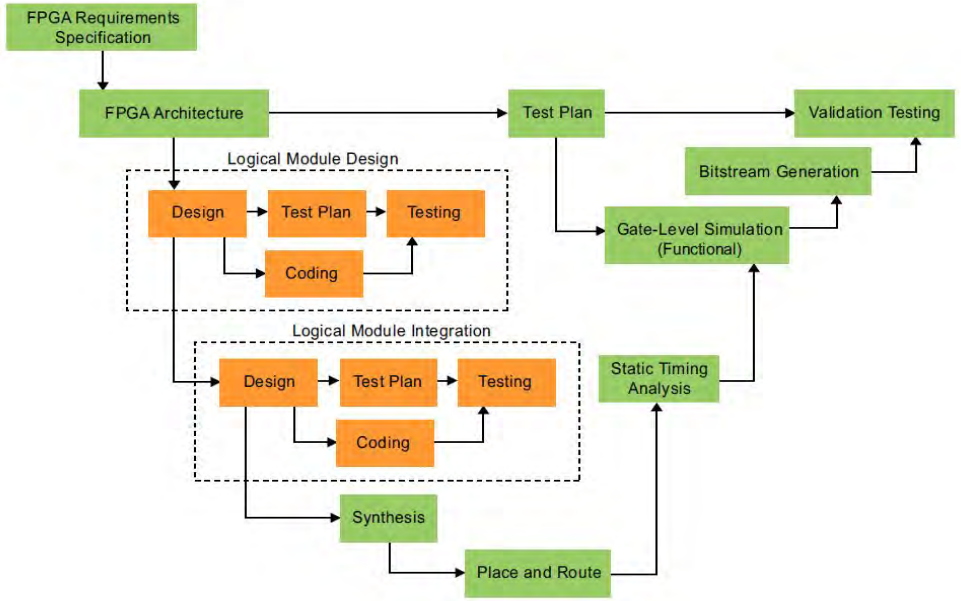
Kostiantyn Leontiiev, Technical Director

October, 2018, Dallas, USA 11th International FPGA Workshop

Agenda

- FPGA V-Model adaptation
- HW Fault Insertion Testing (FIT)
- SW FIT
- Conclusions

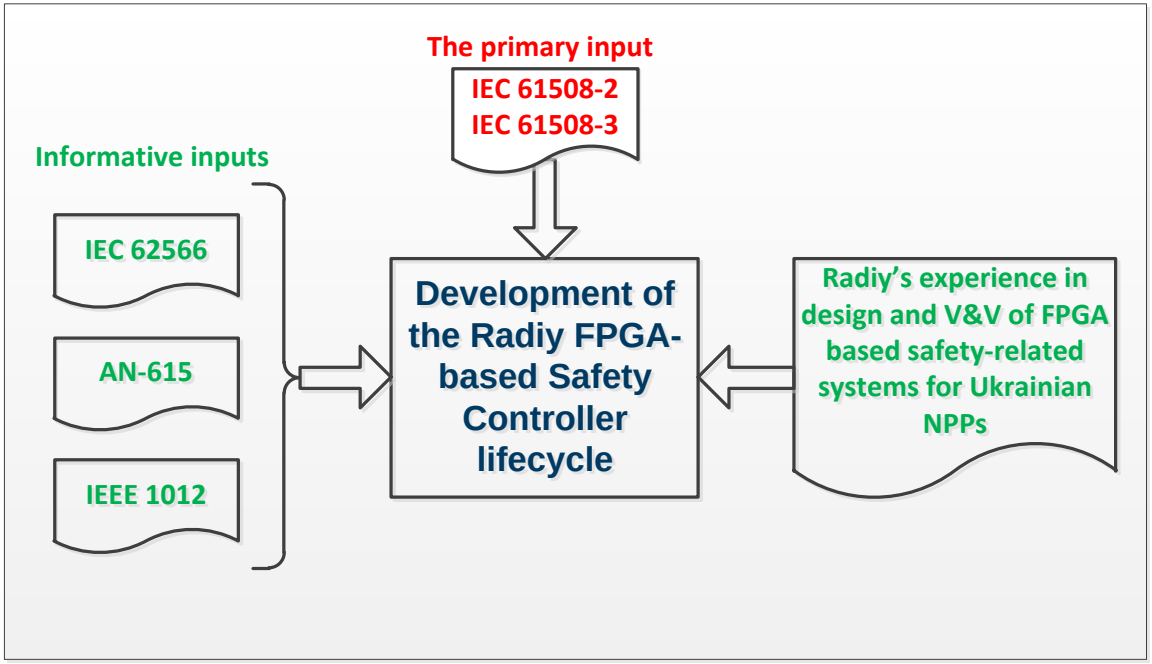
FPGA development V-model adaptation



IEC 61508 – requirements to system safety lifecycle model

IEC 61508 **defines** a lifecycle for safety-related systems, but we needed to adopt it for our product.

See:
IEC 61508-2, Section 7.1.3
IEC 61508-3, Section 7.1.2



IEC 61508 – recommendations for FPGA based system safety lifecycle

IEC 61508 provides a reference lifecycle model of the ASIC development lifecycle (see IEC 61508-2, Figure 3).

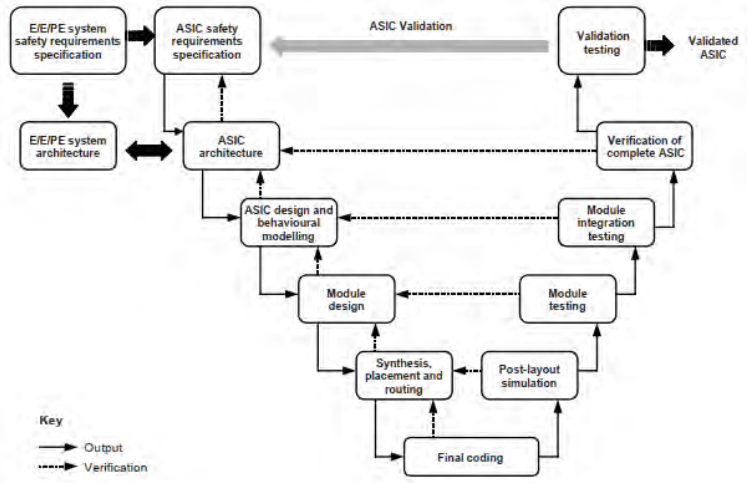


Figure 3 – ASIC development lifecycle (the V-Model)

IEC 61508 defines techniques and measures to avoid introducing faults during design with user programmable integrated circuits - FPGA/PLD/CPLD (see IEC 61508-2, Annex F).

Table F.2 – Techniques and measures to avoid introducing faults during ASIC design and development: User programmable ICs (FPGA/PLD/CPLD) (see 7.4.6.7)

Design phase	Ref	Technique/Measure	See IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
Design entry	1	Structured description	E.3	HR high	HR high	HR* high	HR* high
	2	Design description in (V)HDL (see Note)	E.1	HR high	HR high	HR* high	HR* high
	3	Schematic entry	E.2	– high	– high	NR	NR
	4	Design description using boolean equations		R high	R high	NR	NR
	5a	For circuit descriptions that use boolean equations: manual inspection in designs with limited (low) complexity		HR high	HR high	HR* high	HR* high
	5b	For circuit descriptions that use boolean equations: simulation of state transitions in designs with higher complexity		HR high	HR high	HR* high	HR* high
	6	Application of a proven in use design environment	E.4	HR high	HR high	HR* high	HR* high
	7	Application of proven in use (V)HDL simulators (see Note)	E.4	HR high	HR high	HR* high	HR* high
	8	Functional test on module level (using for example (V)HDL test benches) (see Note)	E.6	HR high	HR high	HR* high	HR* high

IEC 62566 – recommendations for FPGA based system safety lifecycle

IEC 62566 defines strict process and technical requirements for the development of Hardware Description Languages Programmed Devices in order to achieve the reliability required for safety I&C systems.

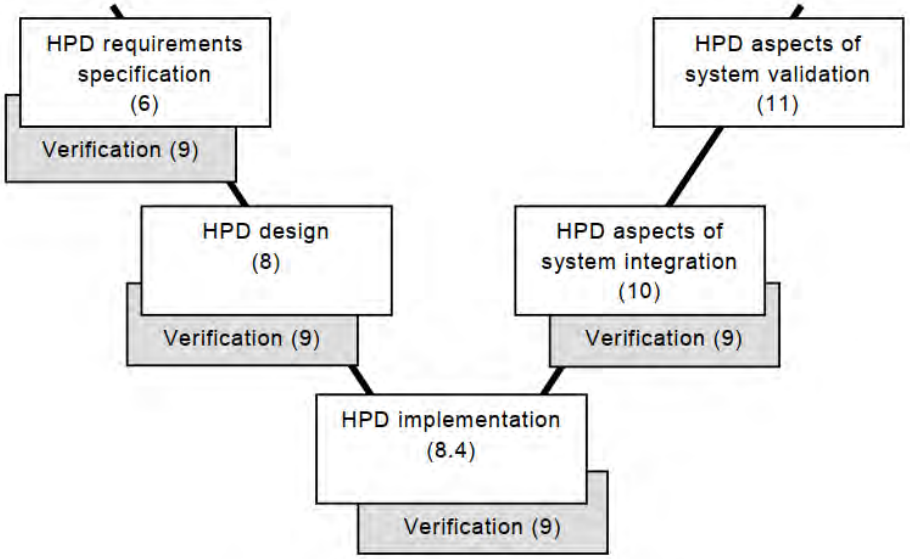
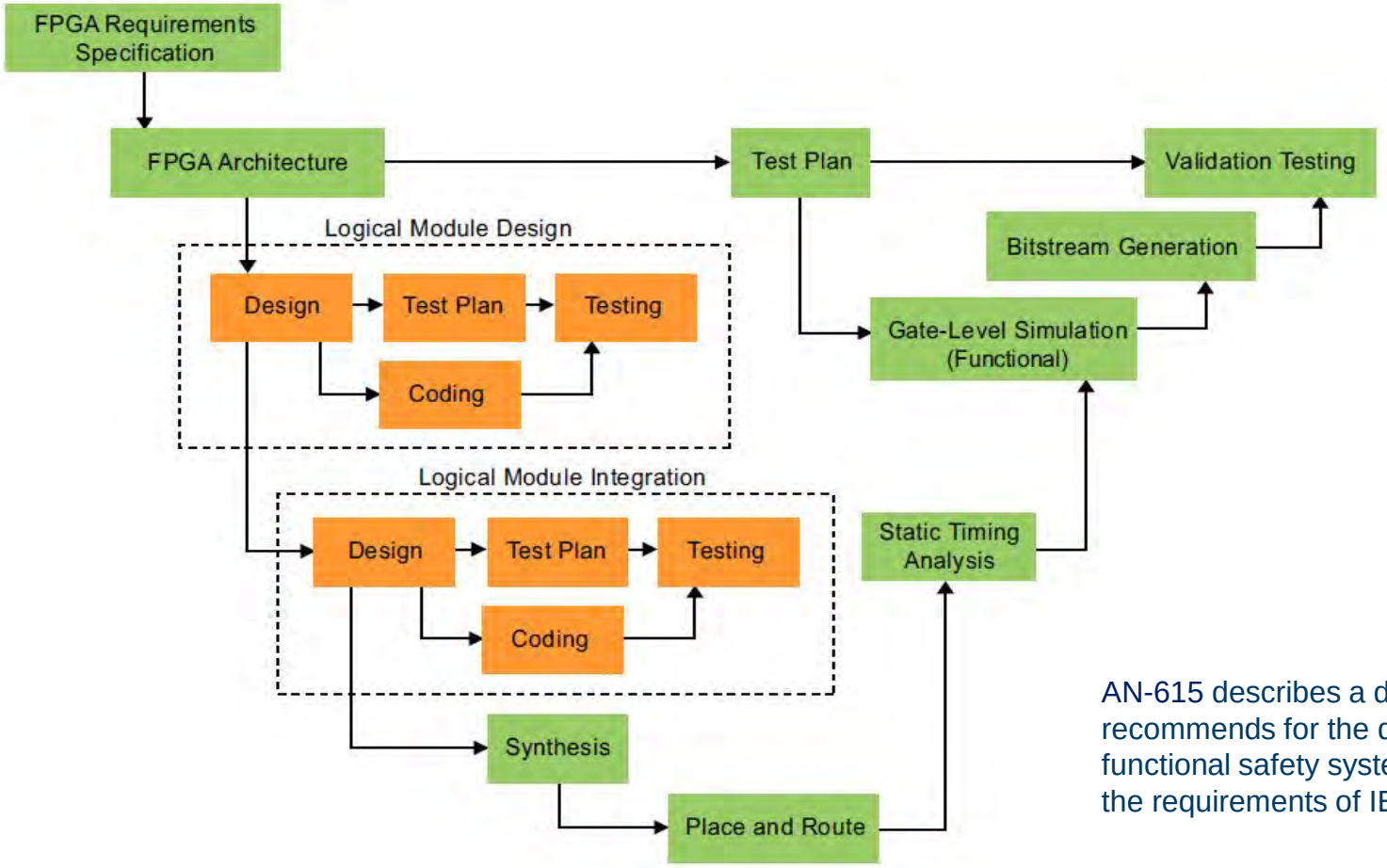


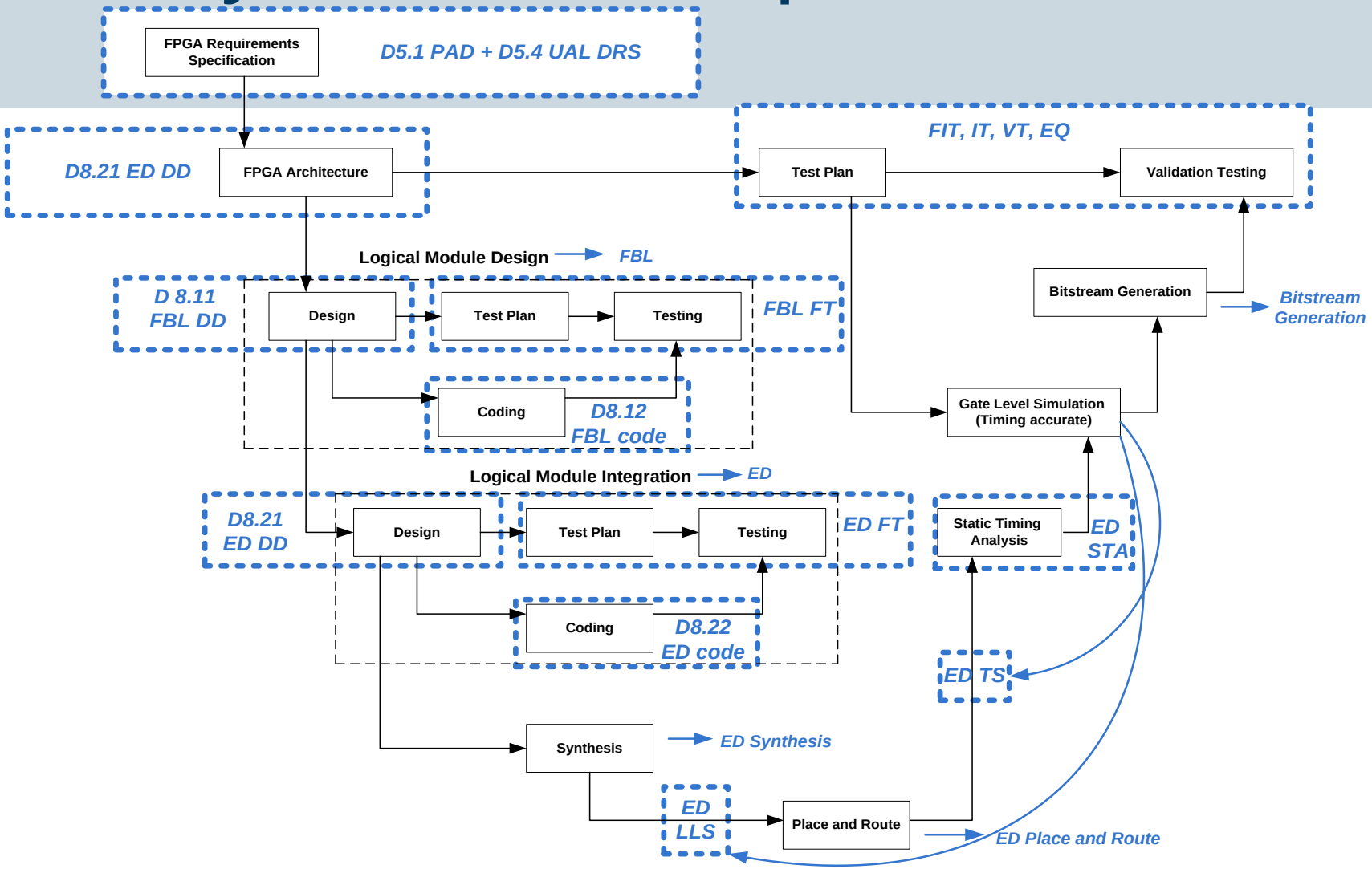
Figure 2 – Development life-cycle of HPD

Altera FPGA Development V-model

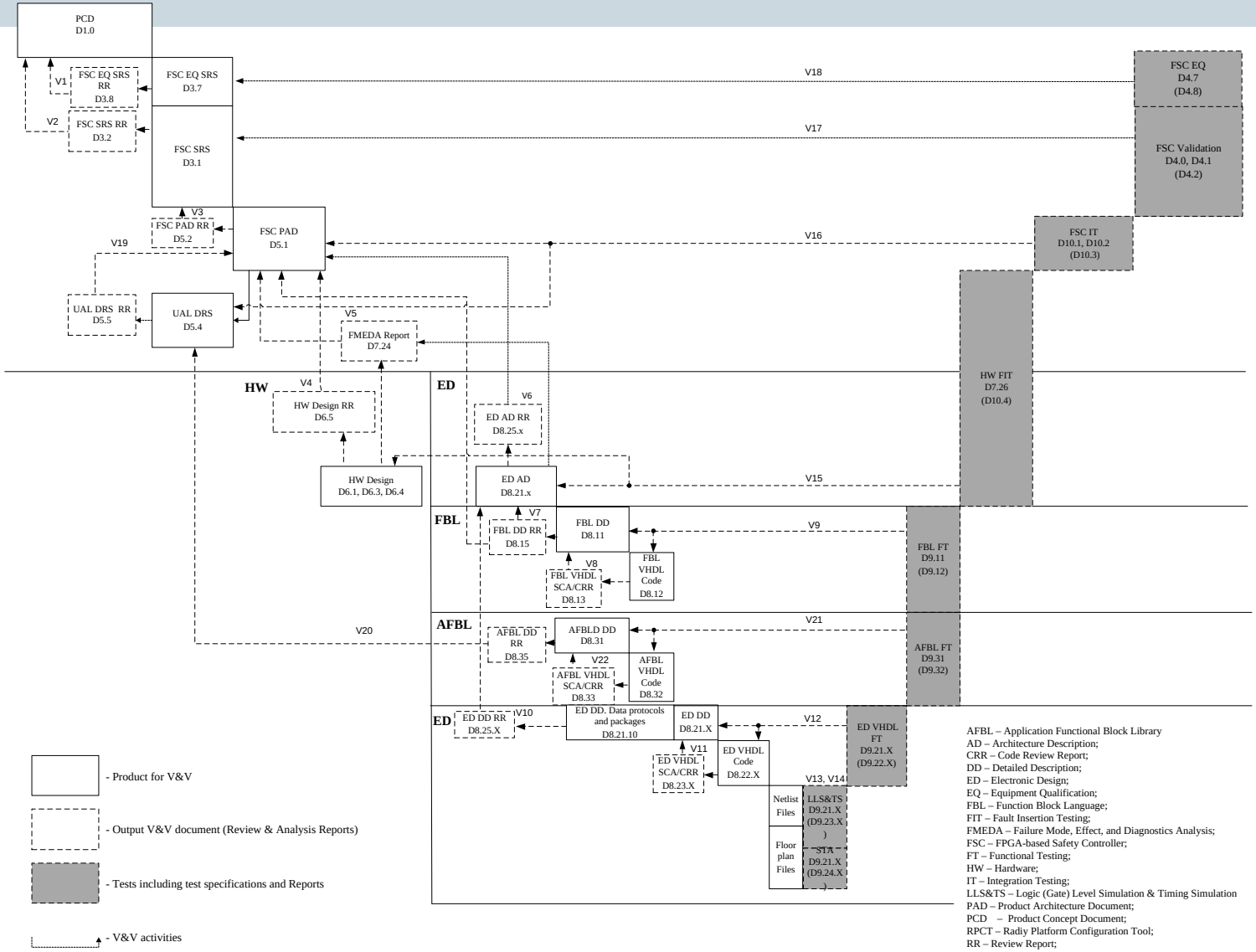


AN-615 describes a design flow that Altera recommends for the development of functional safety systems in order to satisfy the requirements of IEC61508

Radiy FPGA Development V-model

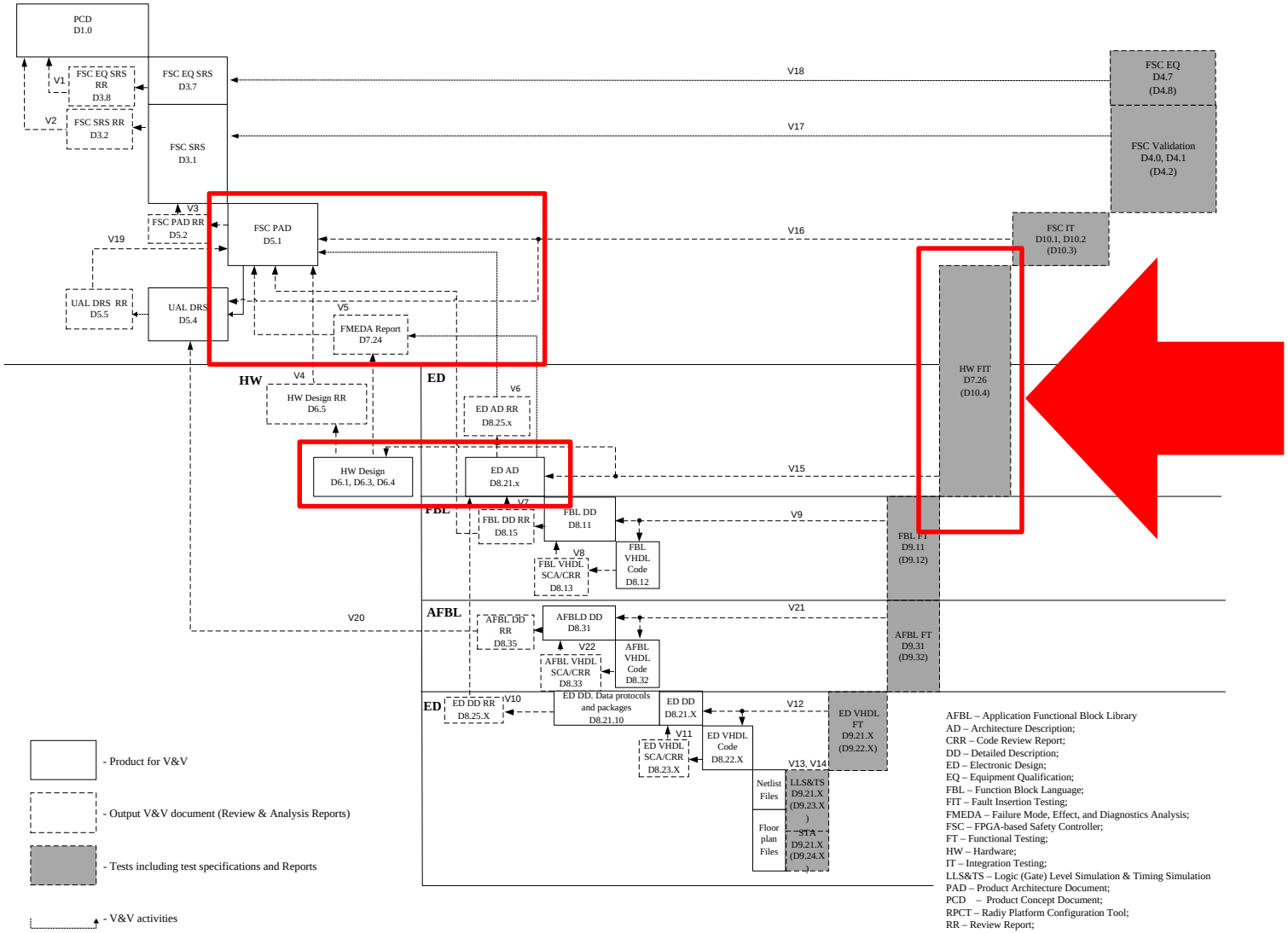


Radiy FPGA-based Safety Controller lifecycle



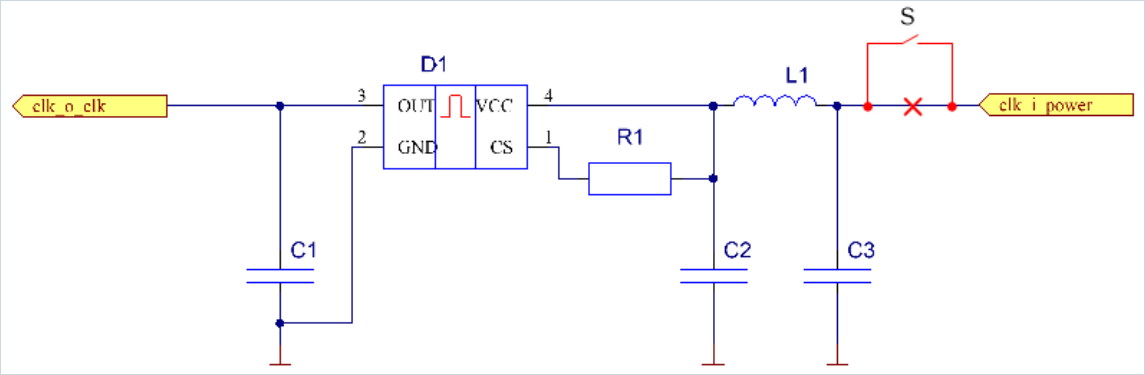
AFBL – Application Functional Block Library
AD – Architecture Description;
CRR – Code Review Report;
DD – Detailed Description;
ED – Electronic Design;
EQ – Equipment Qualification;
FBL – Function Block Language;
FIT – Fault Insertion Testing;
FMEDA – Failure Mode, Effect, and Diagnostics Analysis;
FSC – FPGA-based Safety Controller;
FT – Functional Testing;
HW – Hardware;
IT – Integration Testing;
LLS&TS – Logic (Gate) Level Simulation & Timing Simulation
PAD – Product Architecture Document;
PCD – Product Concept Document;
RPCT – Radiy Platform Configuration Tool;
RR – Review Report;
SCA – Static Code Analysis;
SRS – Safety Requirements Specification;
STA – Static Timing Analysis;

Radiy FPGA-based Safety Controller lifecycle



AFBL – Application Functional Block Library
AD – Architecture Description;
CRR – Code Review Report;
DD – Detailed Description;
ED – Electronic Design;
EQ – Equipment Qualification;
FBL – Function Block Language;
FIT – Fault Insertion Testing;
FMEDA – Failure Mode, Effect, and Diagnostics Analysis;
FSC – FPGA-based Safety Controller;
FT – Functional Testing;
HW – Hardware;
IT – Integration Testing;
LLS&TS – Logic (Gate) Level Simulation & Timing Simulation
PAD – Product Architecture Document;
PCD – Product Concept Document;
RPCT – Radiy Platform Configuration Tool;
RR – Review Report;
SCA – Static Code Analysis;
SRS – Safety Requirements Specification;
STA – Static Timing Analysis;

HW FIT



HW FIT (1)

Goal:

- To confirm\test FMEDA results;
- to check the functionality of system self-diagnostics through detection or non-detection of inserted fault;
- to check behavior of the module after fault insertion (mode of operation, information on the indication board unit);

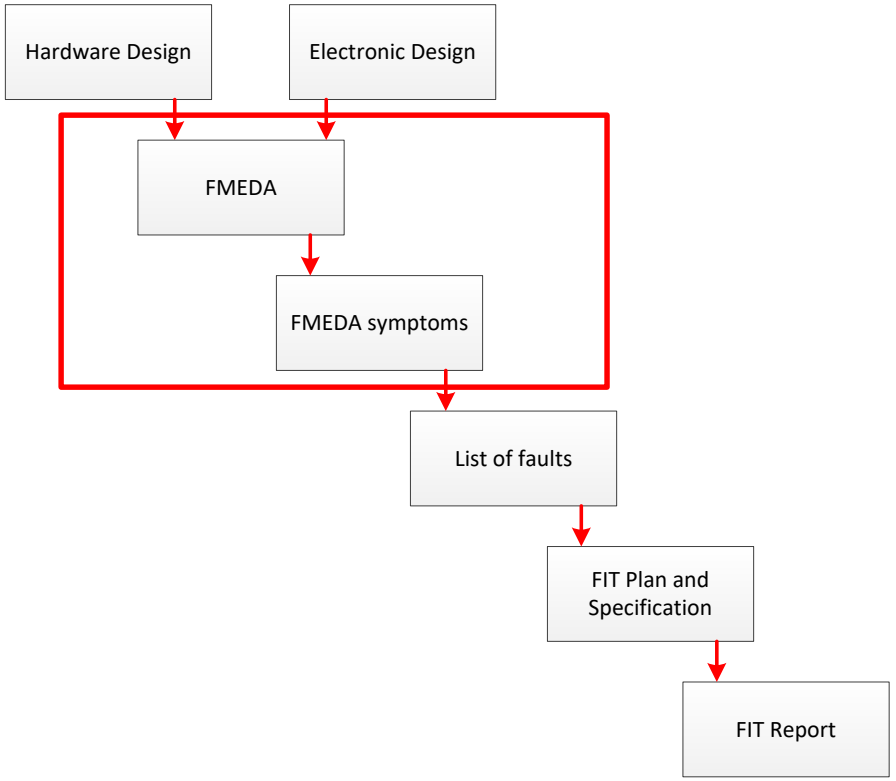
Approach:

- FIT is based on the FMEDA results which are transferred to the FIT Specification for each module.

Inputs:

- STC-WP-QA-18 Hardware FIT Procedure;
- Circuit Diagrams;
- Bills of materials;
- Mechanical and Assembly drawings;
- FSC module.

Fault Insertion Testing includes next steps:



HW FIT (2)

An example of FIT test case for DIM (Test Case: FIT.DIM.05).

FIT Test Specification and Report. All FIT cases are traceable to FMEDA.

Test Case RID	FIT.DIM.05	**Test Case TID**	DIM.05.01
Test Case TN	[IO Clock B failure]		
Test Case description	Test: IO Clock B failure Tracing: D7.24.X		
Test Designed by	Bulba E.	**Test Designed date**	April 12, 2017
SUT Configuration	SUT.DIM.01	**TB Configuration**	TB.01
Requirements related to the test			
DIM ED DD	DIM_ED.01, DIM_ED.02, DIM_ED.03, DIM_ED.05, DIM_ED.06, DIM_ED.07, DIM_ED.11, DIM_ED.12, DIM_ED.13		
PSWD ED DD	PSWD_ED.01, PSWD_ED.02, PSWD_ED.04, PSWD_ED.06, PSWD_ED.07, PSWD_ED.12, PSWD_ED.13		
FBL DD	DDC.04, DDC.05, DDC.06, DDC.07, DDC.10, DDC.11, IBUC.01, IBUC.02, IBUC.03, IBUC.04, IBUC.04a, IBUC.04b		
Test			
Pre-conditions	1. Solder the switch between the raised pin of the element AA1.L1 and vacated contact pad (Figure DIM.05.01.01). 2. Activate SUT in accordance with subsection 2.4 (UAL developed in accordance with Appendix C, Figure C.1 is uploaded). 3. Activate TB in accordance with subsection 2.3. 4. Initial state of DIM in accordance with Appendix C, Table C.1.		

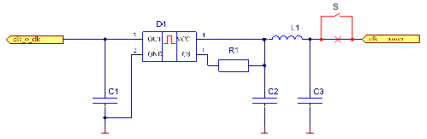


Figure DIM.05.01.01 – Symptom realization

Test Case Steps	1. No fault. Register state of all safety outputs in Chassis using LabVIEW software and MATS. 2. Insert fault (activate switch S). Register state of all safety outputs in Chassis using LabVIEW software and MATS. 3. Check the state of DIM. Register the error code/codes on the IBU/PSWD LEDs of DIM. 4. Register the error code/codes on the IBU of LM. 5. Remove fault (deactivate switch S). Register the state of all safety outputs in the chassis using LabVIEW software and MATS. 6. Remove DIM from Chassis and put it back without fault.

Expected result		Actual result		Pass/Fail
LED "RUN"	OFF	**LED "RUN"**	OFF	Pass
LED "FAULT"	ON	**LED "FAULT"**	ON	Pass
PSWD LEDs	010010	**PSWD LEDs**	010010	Pass

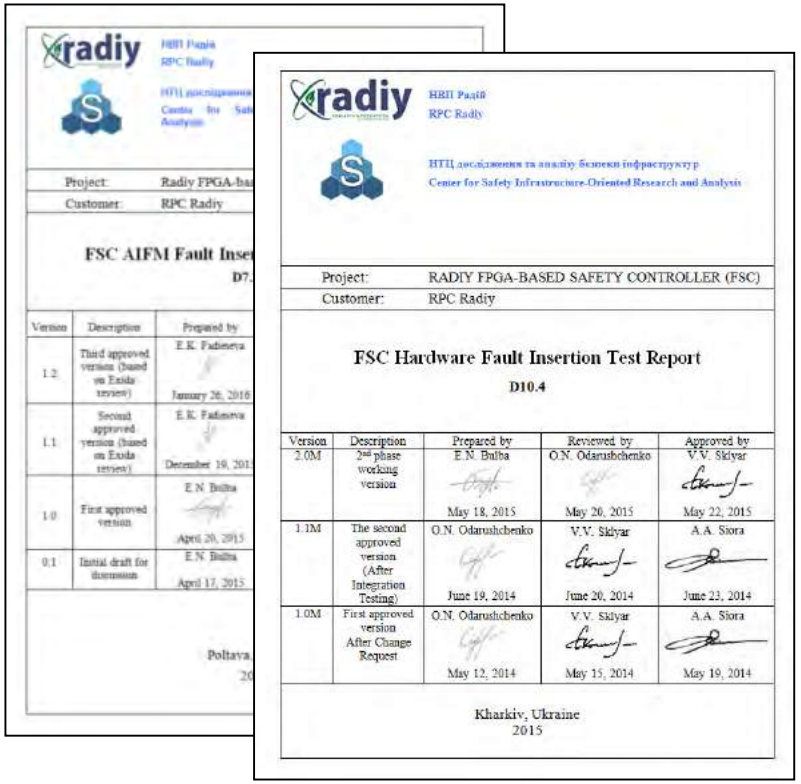
Figure FIT.DIM.05.01.01

LM state [Step 4] (See Figure FIT.DIM.05.01.02)

Expected result		Actual result		Pass/Fail
LED "RUN"	ON	**LED "RUN"**	ON	Pass
LED "FAULT"	Flashing	**LED "FAULT"**	Flashing	Pass
IBU state	#014, #088, #08A, #08C, #1DB, #1DC, #1DD, #1DE, #1DF	**IBU state**	#014, #088, #08A, #08C, #1DB, #1DC, #1DD, #1DE, #1DF	Pass

Figure FIT.DIM.05.01.02

Acceptance criterion	1. "Pass" – when all values from expected result is equal all values from actual result; 2. Test successful when all values are Pass. Else – test unsuccessful.
Summary of Test Results (Pass/Fail)	Test successfully PASSED.
Summary of all test anomalies and the CRs raised	Anomalies are not detected.
Justification unresolved bugs	
Justification from designer	Justification from verifier



radiy

НВП Радій
RPC Radiy

НТЦ дослідження та аналізу безпеки інфраструктур
Center for Safety Infrastructure-Oriented Research and Analysis

Project: RADIY FPGA-BASED SAFETY CONTROLLER (FSC)
Customer: RPC Radiy

FSC Hardware Fault Insertion Test Report

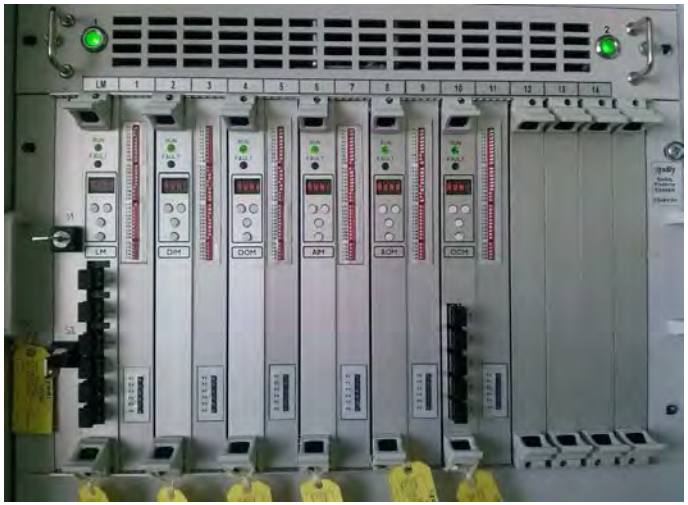
D10.4

Version	Description	Prepared by	Reviewed by	Approved by
2.0M	2nd phase working version	E.N. Bulba May 18, 2015	O.N. Odarushchenko May 20, 2015	V.V. Sklyar May 22, 2015
1.1M	The second approved version (After Integration Testing)	O.N. Odarushchenko June 19, 2014	V.V. Sklyar June 20, 2014	A.A. Siora June 23, 2014
1.0M	First approved version After Change Request	O.N. Odarushchenko May 12, 2014	V.V. Sklyar May 15, 2014	A.A. Siora May 19, 2014

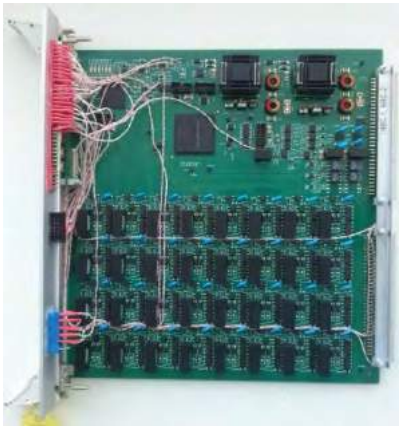
Kharkiv, Ukraine
2015

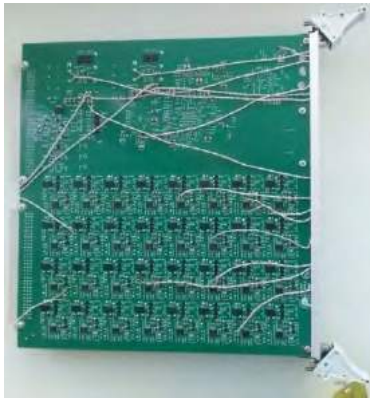
HW FIT (3)

Example of FIT testing

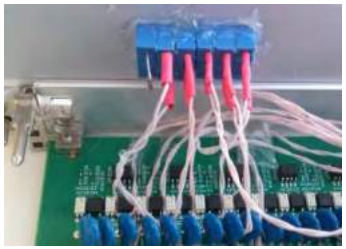


Module with inserted faults

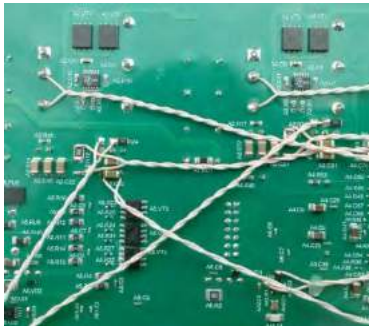


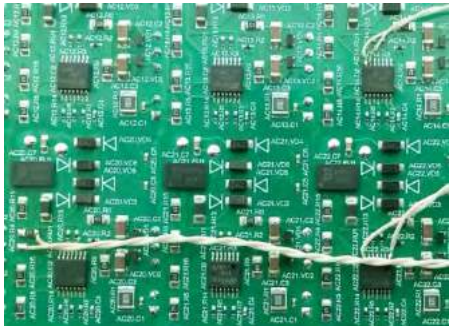


Control Panel for faults activation



Example of inserted faults





SW FIT

Fragment of a human readable description of the Application Logic

```
"z_description_channel_01": {
        "desc fields": "Version;IsCommand;Address;BinCode;MnemoCode;Comment",
        "desc00000000": "1;true;0000;8440000C;APPSTART  12;",
        "desc00000001": "1;false;;;;FB's initialization code",
        "desc00000002": "1;false;;;;Initialization of or (fbtype LOGIC, opcode 1, instance 0, opCode:1:params:2:1:2, non RAM)",
        "desc00000003": "1;false;;;;OperandCount (i_oprd_quant) = 2",
        "desc00000004": "1;false;;;;BusWidth (i_bus_width) = 1",
        "desc00000005": "1;false;;;;Config (i_conf) = 2",
        "desc00000006": "1;true;0002;DA8100000002;WRFBC     OR.0[0], #2;i_oprd_quant <= 2",
        "desc00000007": "1;true;0005;E28100010001;WRFBC     OR.0[1], #1;i_bus_width <= 1",
        "desc00000008": "1;true;0008;7A8100020002;WRFBC     OR.0[2], #2;i_conf <= 2",
        "desc00000009": "1;false;;;;End of FB's initialization code section",
        "desc00000010": "1;true;000B;60C0;STOP      ;set address of application logic code start",
```

Human redable description is NOT uploaded into LM

Data frame is uploaded into LM

Corresponding data frame

```
"z_frame_0003": {
        "data0000": "8440 000c da81 0000 0002 e281 0001 0001 7a81 0002 0002 60c0 61c0 b402 0000 0000",
        "data0010": "89c0 b402 0001 0001 cac1 0003 0076 0000 7ac1 0004 0076 0001 7881 0000 6301 0014",
        "data0020": "b403 0000 7180 b400 0000 33c0 b400 0076 0000 fbc0 b400 0076 0101 f100 d2c4 b400",
        "data0030": "5140 d2c5 b403 0001 5980 d2c6 0000 cbc0 d2c6 b403 0000 f900 3200 d2c6 a180 e1b6",
        "data0040": "0000 60c0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000",
        "data01f0": "0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 44e2 54b4 3022 d53f",
        "frameIndex": 3
    },
```

CRC64 checksum

SW FIT (1)

Goal:

- to ensure that the FSC Logic Module (LM) detects errors in configuration data uploaded into FSC using diagnostics subsystem and appropriate actions are performed in accordance with error types;
- to ensure that the RPCT Outputs Verification Tool (ROVT) detects and reports errors in configuration data during UAL Build verification before uploading configuration data into FSC;

Approach:

- FIT is based on the FSC FMEDA and RPCT FMEA results.

Inputs:

- UAL DRS;
- RPCT SRS;
- FSC module.

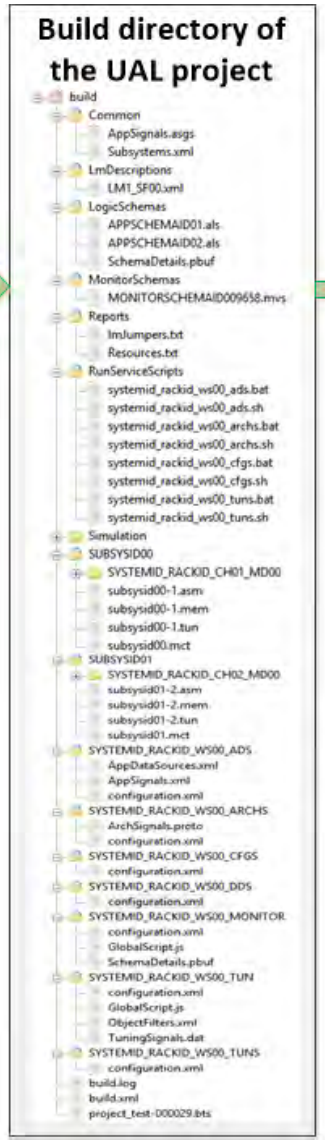
SW FIT (2)

Radiy IDE

RPCT

UAL project design

Build directory of the UAL project



LM configuration file (*.BTS)

RadICS Platform

FCS LM

Fault insertion

ROVT analysis

ROVT reports

Consistency of a build directory is protected with MD5 hashing algorithm.

MD5 checksum is calculated for the each file in the build.

SW FIT (3)

8. Find and Replace the selected command with the command that contains SE in the Data Frame:

Fragment of the configuration file before error seeding

wt_verification-000050.bts

```
z_frame_0003": {
    "data0000": "8440 000c da81 0000 0002 e281 0001 0001 7a81 0002 0002 60c0 61c0 b402 0000 0000",
    "data0010": "89c0 b402 0001 0001 cac1 0003 0076 0000 7ac1 0004 0076 0001 7881 0000 6301 0014",
    "data0020": "b403 0000 7180 b400 0000 33c0 b400 0076 0000 fbc0 b400 0076 0101 f100 d2c4 b400",
    "data0030": "5140 d2c5 b403 0001 5980 d2c6 0000 cbc0 d2c6 b403 0000 f900 3200 d2c6 a180 e1b6",
    "data0040": "0000 60c0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000",
    "data01f0": "0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 44e2 54b4 3022 d53f",
    "frameIndex": 3 }
```

Fragment of the configuration file after error seeding

wt_verification-000050.bts

```
z_frame_0003": {
    "data0000": "8440 000c da81 0000 0002 e281 0001 0001 7a81 0002 0002 60c0 61c0 b402 0000 0000",
    "data0010": "89c0 b402 0001 0001 cac1 0003 0076 0000 7ac1 0004 0076 0001 3001 0000 6301 0014",
    "data0020": "b403 0000 7180 b400 0000 33c0 b400 0076 0000 fbc0 b400 0076 0101 f100 d2c4 b400",
    "data0030": "5140 d2c5 b403 0001 5980 d2c6 0000 cbc0 d2c6 b403 0000 f900 3200 d2c6 a180 e1b6",
    "data0040": "0000 60c0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000",
    "data01f0": "0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 44e2 54b4 3022 d53f ",
     "frameIndex": 3 }
```

Conclusions

- SLC model shall be adopted for FPGA-based product and justified
- Require full understanding of the product from the independent expert and V&V team members
- Take into account reaction of the whole system when you insert fault
- FIT activities take a lot of time but brings good results

RadICom Platform Overview

Product Highlights

- FPGA-based
- Developed for non-1E systems
- Based on SIL 3 certificated RadICS digital I&C Platform
- Cost-effective solution
- Modules are compatible with RadICS Platform (same dimensions, connectors, latches…)
- Comprehensive, tried-and-tested I/Os
- Flexible redundancy management
- Comprehensive on-line diagnostic (SIL2)
- Fast response time (5 milliseconds)
- RPCT support . Possibility to change application logic configuration online via Tuning interface.

Thank you for your attention!

Public Company «Research and Production Corporation «Radiy»
29 Geroyiv Stalingrada Street, Kirovograd, Ukraine, 25009
e-mail: ksleontiev@radiy.com
http://www.radiy.com