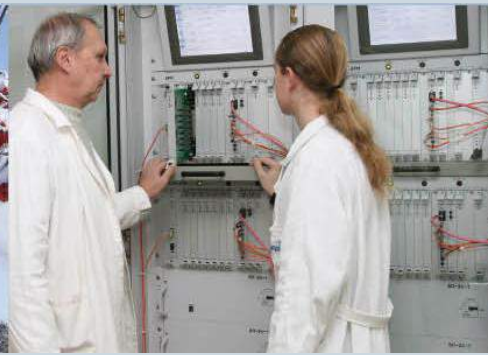
Panel Discussion on V&V and Testing in the FPGA Development Process

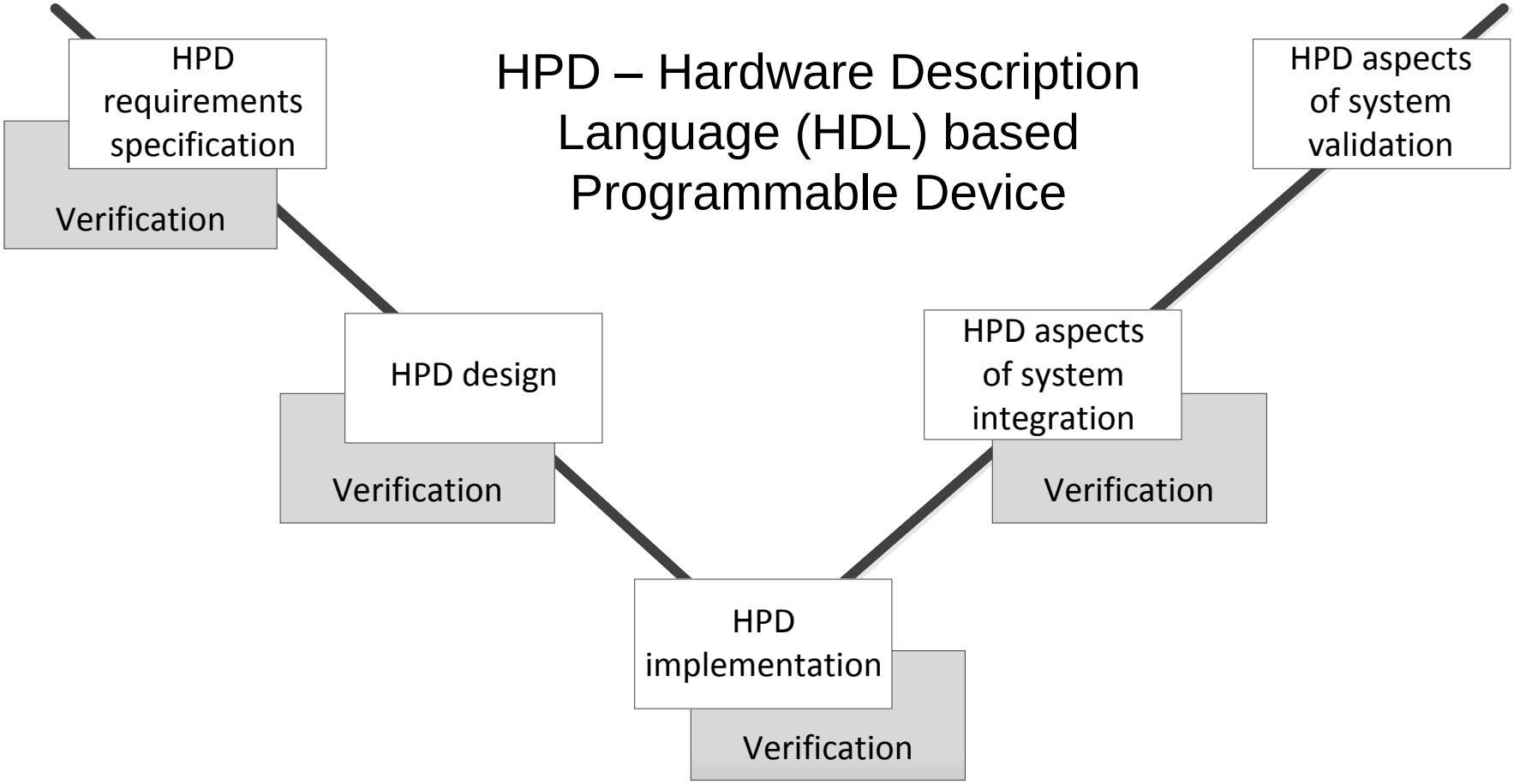
Vladimir Sklyar, Technical Director

8th International Workshop on the Application of FPGAs in NPPs
13-16 October 2015, Shanghai, China



Safety Life Cycle of FPGA-based Application (IEC 62566)



V&V techniques

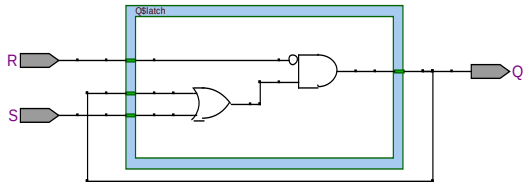
- Documents Review
- Failure and Mode Effect Analysis (FMEA)
- Static Code Analysis and Code Review
- HDL Code Functional Testing
- Logic Level Simulation, Timing Simulation and Static Timing Analysis (for FPGA Electronic Design)
- Reports Review of Synthesis, Place and Route, Bitstream Generation (for FPGA Electronic Design)
- Fault Insertion Testing (FIT) for the platform level
- Integration Testing, Validation Testing

Static Code Analysis and Code Review

Tools

Aldec ALINT
Mentor Graphics HDL Designer

```
TrigProc:
process (R, S) is-- Violation, asynchronous combination logic
begin
      if R = '1' then
            Q <= '0';
      elsif S = '1' then
            Q <= '1';
      end if;
end process TrigProc;
```



ALINT - D:/eth_moduleV0/Communication/TxBuffer.vhd

File Edit View Linting Tools Window Help

alint.avdb TxBuffer.vhd

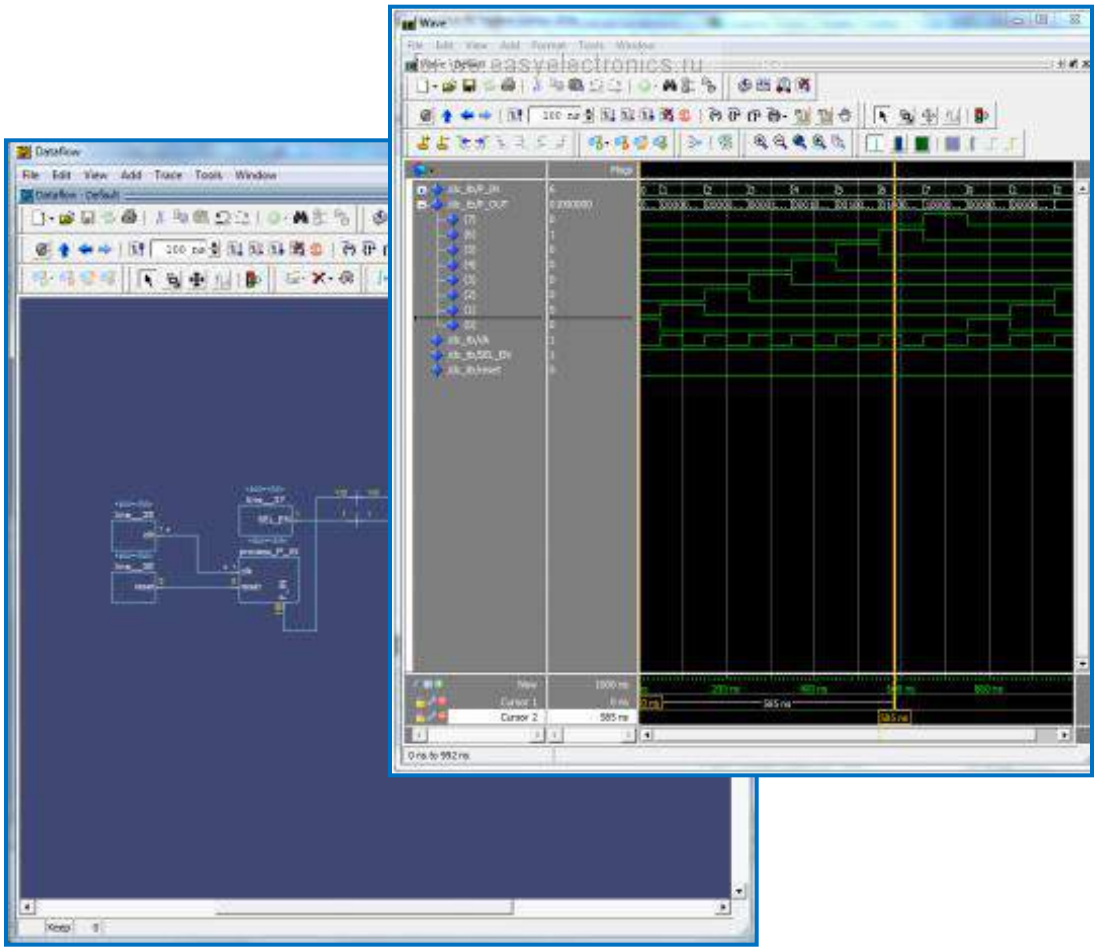
```
48              end if;
49
50      --      if(i = 0)then
51      --          InitVal(0) := to_unsigned(257,oD'length);
52      --      end if;
53          end loop;
54          return(InitVal);
55      end InitRamFunc;
56
57      signal RAM : RAM_TYPE := InitRamFunc;
58  begin
59      process(clkWr)is
60      begin
61          if(clkWr'event)and(clkWr = '1')then
62              if(wr = '1')then
63                  Ram(to_integer(unsigned(addrWr))) <= "00"&unsigned(iD);
64              end if;
65          end if;
66      end process;
67
68      process(clkRd)is
69      begin
70          if(clkRd'event)and(clkRd = '1')then
71              oD <= std_logic_vector(Ram(to_integer(unsigned(addrRd))));
72          end if;
73      end process;
74
75      process(clkWr)is
76          constant RepTmp : RAM_TYPE := InitRamFunc;
77          variable tmp,t1,t2 : integer;
78          variable iDataCRC : unsigned(15 downto 0);
79          variable RegCRCm : unsigned(15 downto 0);
```

Default Console Documents Policy Ruleset

Functional Testing of RTL

Tools

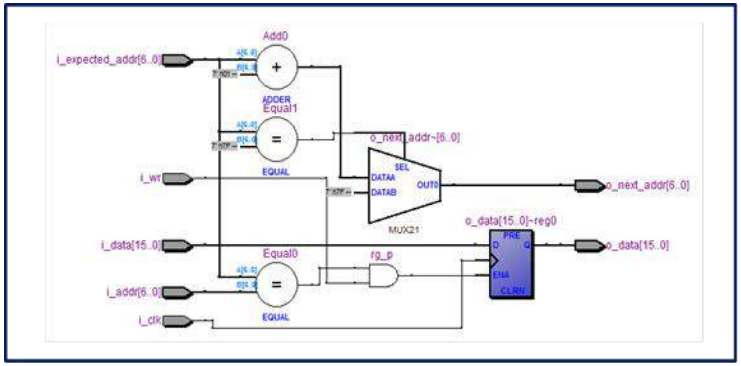
Vendor	Name
Aldec	Active-HDL, Riviera-PRO
Mentor Graphics	ModelSim, Questa
Cadence	Incisive Enterprise Simulator/Verifier
Synopsys	VCS и Verdi3



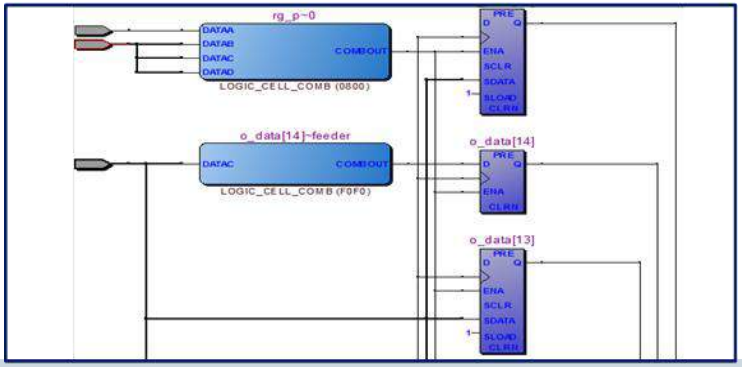
Logic Level Simulation, Timing Simulation

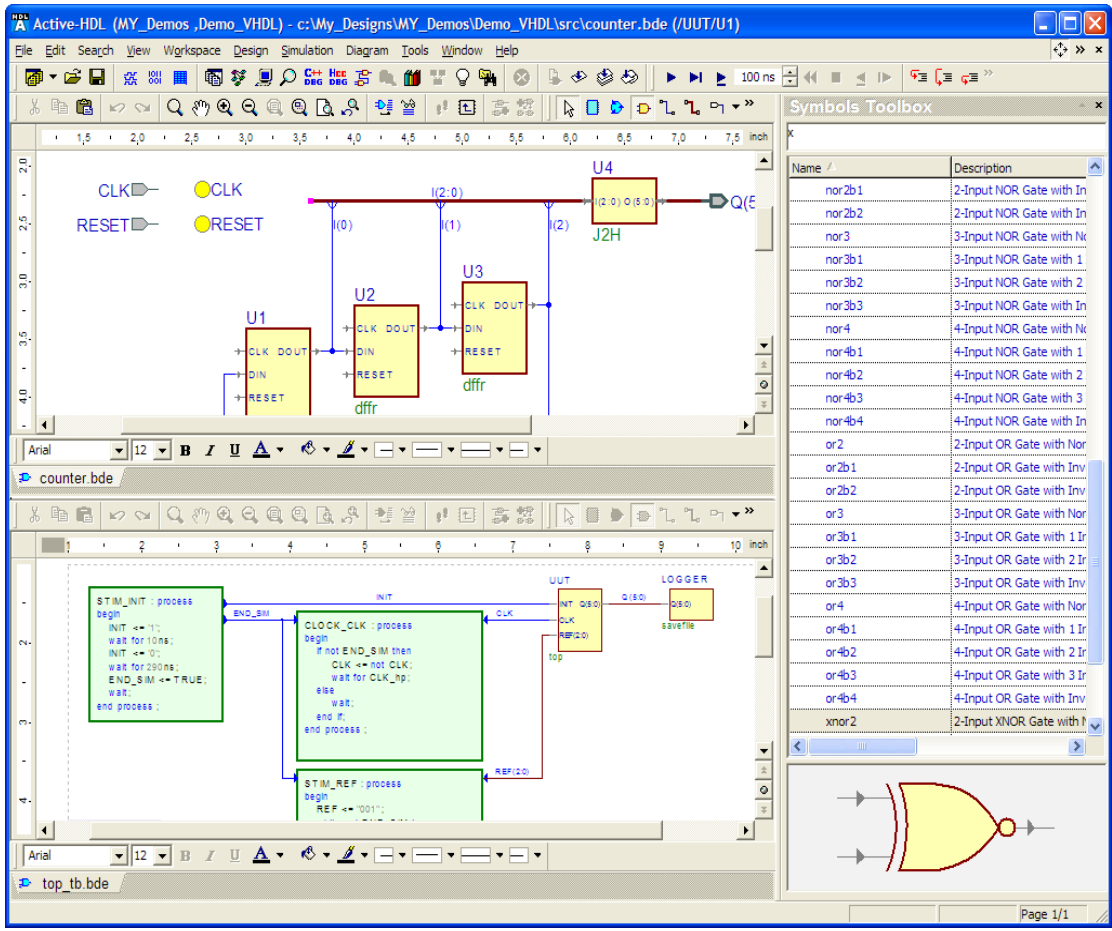
Tools

The same as for FT



Синтез

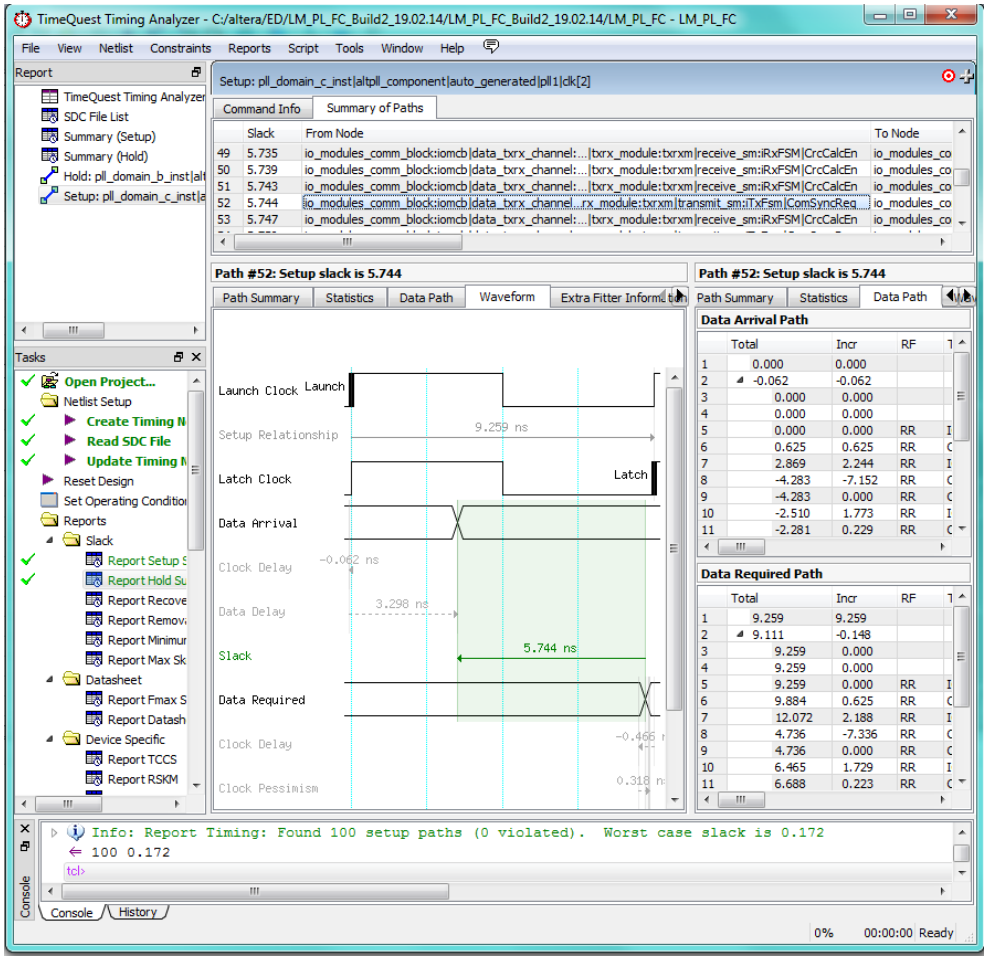




Static Timing Analysis

Tools

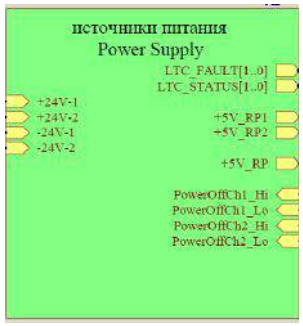
Vendor	Name
Microsemi	SmartTime
Xilinx	Vivado Static Timing Analysis
Altera	TimeQuest Timing Analyzer
Cadence	TempusTiming Signoff Solution
Synopsys	PrimeTime Suite



Example of FIT implementation for FPGA-based I&C Platform RadICS

1. Analysis of the fault:

- **To define the module**
- **To define the unit**
- **To define the symptom**

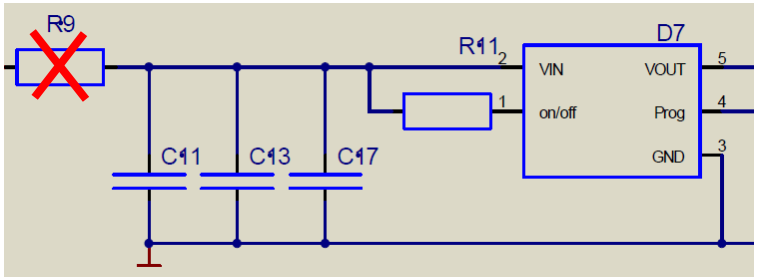


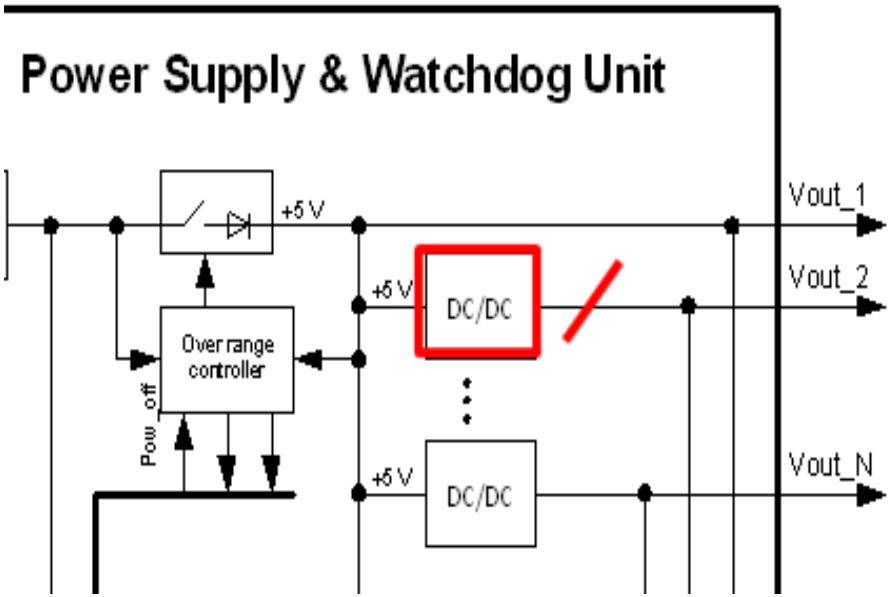
Test Case RID	Unit	Test descriptor detectable symptom	Chassis config'n	Insertion required	Module's MODE	Auto'd Test
FIT.DOM.01	PS	IO.PS VCCINT 1.2V lost.	DOM	open cct	RUN, STARTUP	manual
FIT.DOM.2	PS	IO.PS 3.3v lost	DOM	open cct	RUN, STARTUP	manual
FIT.DOM.3	PS	IO.PS VCCA 2.5v lost.	DOM	open cct	RUN, STARTUP	manual
FIT.DOM.4	PS	IO.PS 2.5v BANK5 lost	DOM	open cct	RUN, STARTUP	manual
…	…	…	…	…	…	…

Example of FIT implementation for FPGA-based I&C Platform RadICS (continued)

2. Unit circuit analysis:

- **To define the element of the unit (VCCA 2.5V)**
- **To define the action on the element (VCCA 2.5V <u>Lost</u>)**
- **To define the method of the fault realization in scheme**





Example of FIT implementation for FPGA-based I&C Platform RadICS (continued)

3. Requirements to tool for FIT:

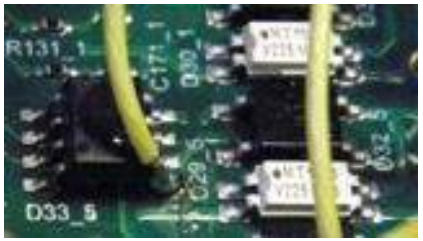
- **Making multiple faults at the same time**
- **Monitoring the changes**
- **Representativity**
- **Ergonomic design**

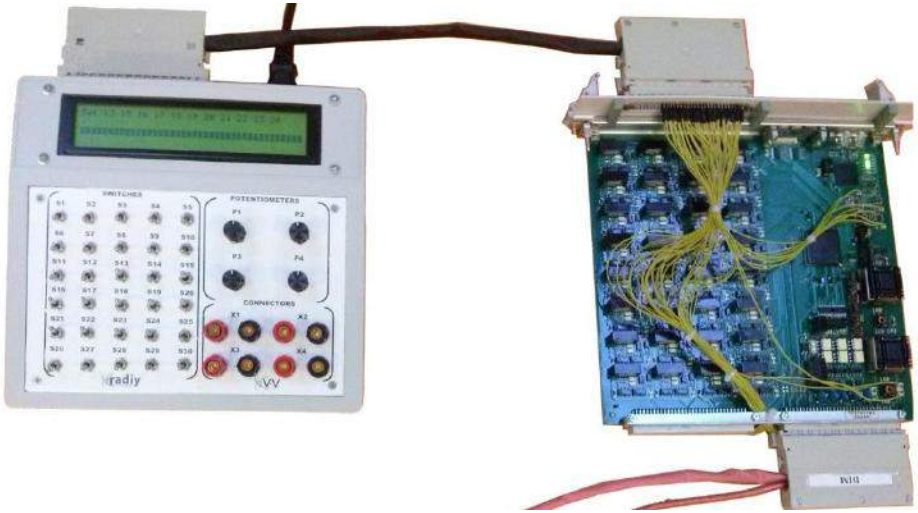
FIT Panel

Example of FIT implementation for FPGA-based I&C Platform RadICS (continued)

4. Implementation FIT hardware:

- **Fault insertion (soldering)**
- **FIT Panel connection to the module**

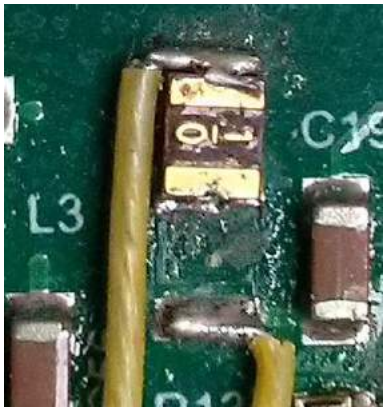




Example of FIT implementation for FPGA-based I&C Platform RadICS (continued)

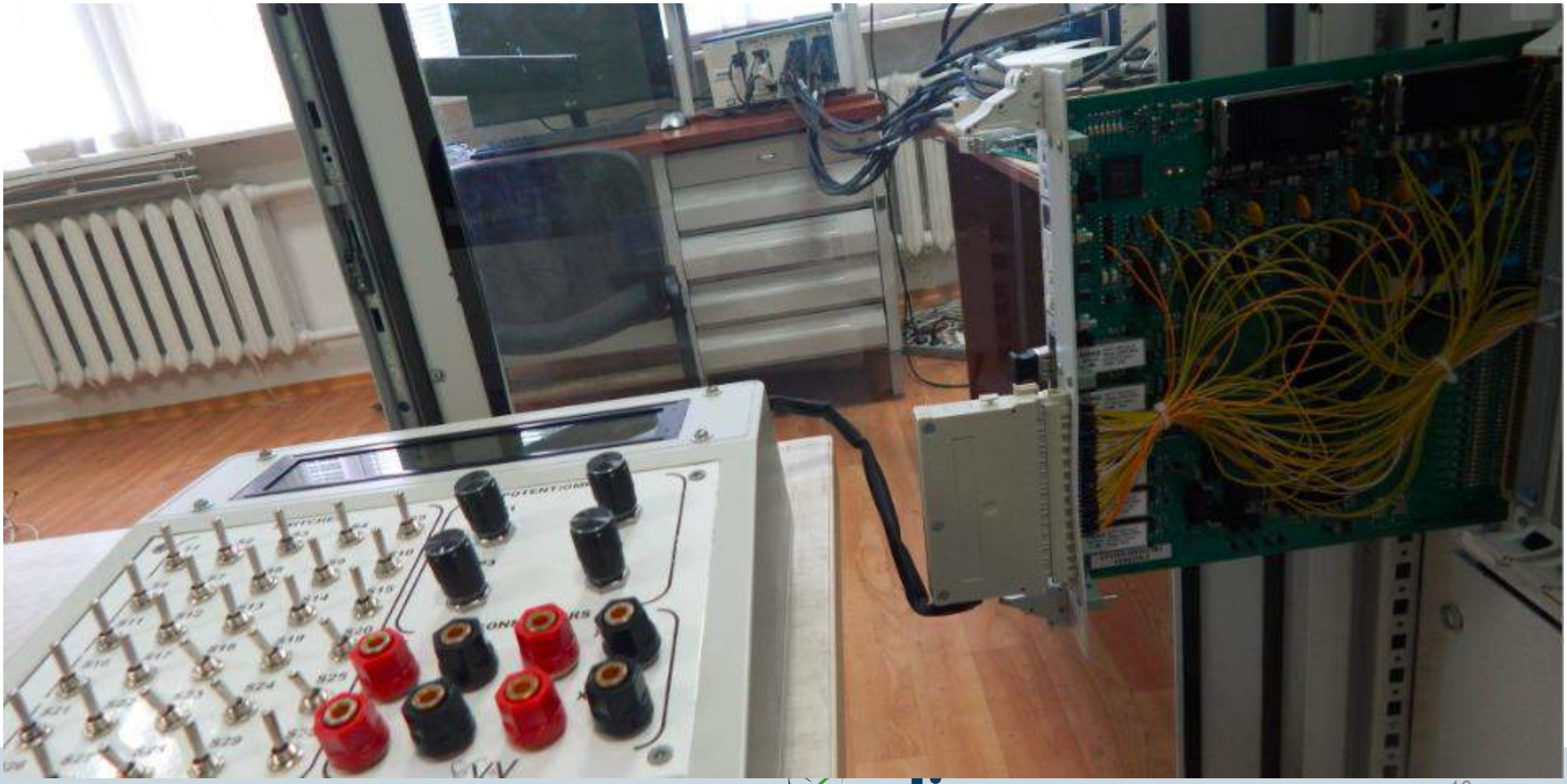
Analysis results of module self-diagnostics

IO.PS VCCINT 1.2V Lost

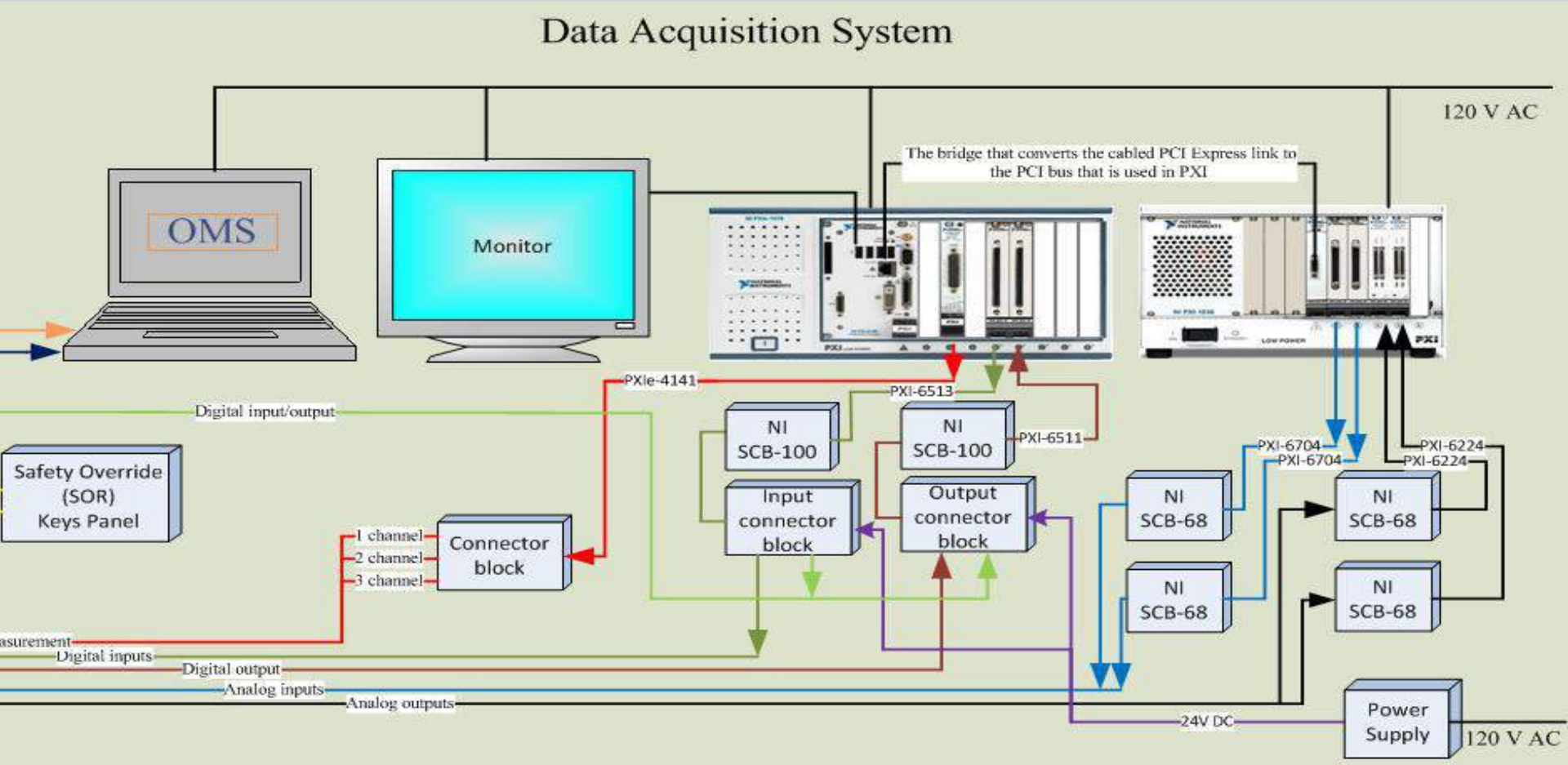


39 Injected faults for Logic Module

- Each power supply: loss / high / low
  - Clock failure (A,B,C), etc.



Integration and Validation testing:
DAS on the base of NI PXI controller and LabView



Expected issues to discuss: General approach to organize V&V

- → Completeness and adequacy of the used techniques and tools set
- → Requirement management and tracing
- → Coverage criteria
- → Tests automation approach
- → FIT for the FPGA chip
- → Best practices
- → Experience transfer from non-safety IT industry: focus on Project Management and Human Factor, agile methodologies etc.

Expected issues to discuss: Formal verification and Static Code Analysis methods

- → Any relevant experience
- → Models and specification which can be useful
- → Model checking approach
- → Relevant Static Code Analysis methods
- → Tools for Static Code Analysis available at the market

Thank you for your attention!

Research & Production Corporation Radiy
29, Geroyiv Stalingrada Street, Kirovograd 25006, Ukraine
e-mail: v.sklyar@radiy.com
http://www.radiy.com