Evolution of safety design approaches.

Radiy's experience.

Kostiantyn Leontiiev, Technical Director

9th International Workshop on Application of FPGA in NPP
October 3-6, 2016, Lyon, France




Agenda

- RadICS Platform history and overview;
- Main design principles;
- Application design approaches;
- Tools support (RPCT);
- Platform validation methods;
- Conclusions

RPC Radiy's products evolution

1995

Started development and supply of the equipment for NPP I&C systems

Replacement of obsolete NPP I&C modules

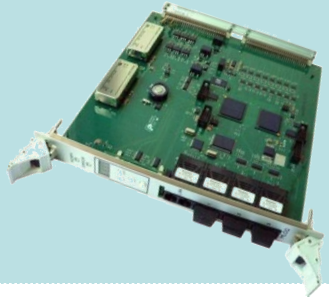
1998

First generation of equipment for NPP I&C systems

FPGA-based I&C systems for NPP

2002

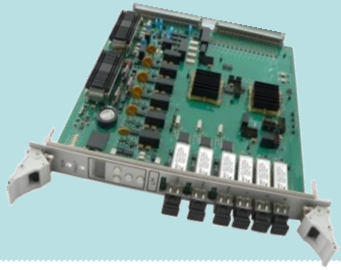
Second generation of equipment for NPP I&C systems



FPGA-based I&C platform for NPP

2011-2014

Third generation of equipment for NPP I&C systems

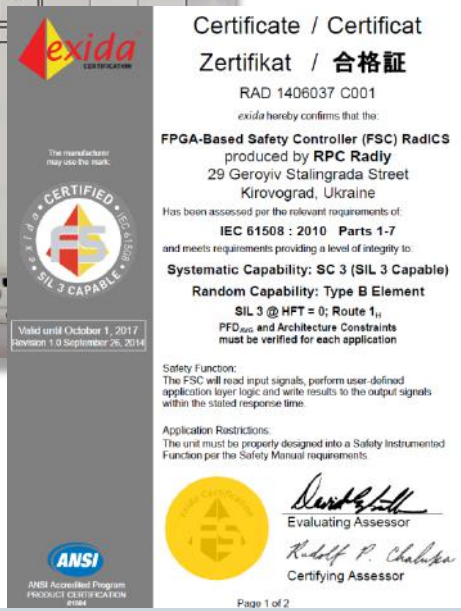


SIL3 certified FPGA-based I&C platform for NPP

RadICS Platform Overview

Product Highlights

- FPGA-based
- IEC 61508:2010 SIL 3 architecture (in one chassis)
- **Designed for Nuclear Safety I&C**
- **High reliability, functional safety and cyber-security**
- Comprehensive, tried-and-tested I/Os
- **Flexible redundancy management**
- Comprehensive multilevel on-line diagnostic (>99% coverage)
- Fast response time (5 ms)
- Hot-swapping of modules (if needed)
- High resistance to external impacts


exida

Certificate / Certificat

Zertifikat / 合格証

RAD 1406037 C001

exida hereby confirms that the:

FPGA-Based Safety Controller (FSC) RadICS

produced by **RPC Radiy**

29 Geroyiv Stalingrada Street

Kirovograd, Ukraine

Has been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-7

and meets requirements providing a level of integrity to:

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 3 @ HFT = 0; Route 1_H

PFD_{AVG} and Architecture Constraints must be verified for each application

Safety Function:
The FSC will read input signals, perform user-defined application layer logic and write results to the output signals within the stated response time.

Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements

Evaluating Assessor

Certifying Assessor

Page 1 of 2

CERTIFIED IEC 61508 SIL 3 CAPABLE

Valid until October 1, 2017
Revision 1.0 September 26, 2014

ANSI

FPGA technology benefits:

- **Diversity with PLC-based equipment**;
- Transparency, parallelism, and determinism of design;
- High speed performance (relevant for some reactor types, i.e. Candu);
- **Absence of system software;**
- **High level of cybersecurity;**
- Resilience to obsolescence due to the portability of the Hardware Description Language (HDL) code between various FPGA-chips produced by different manufacturers;
- Fit for reverse engineering;

Main design principles

Main design principles

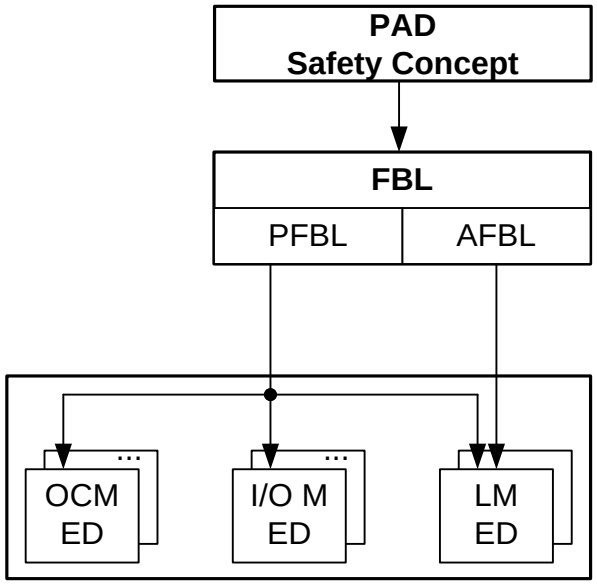
- Safety concept is a base for requirements specifications and detailed design;
- Use optimal design decomposition;
- Organize well-structured libraries (HW, FPGA EDs, TBs);
- Use verified, analyzed and proven in use components library in the platform design;
- Do not increase library components quantity without necessity (reuse is important);
- Describe the design in the way that could be understood by noninvolved person;

Design: HW

- Use components intended for safety applications or proven in use components (FPGA's qualified for SIL3);
- Operation experience and vendor safety recommendations are used in the process of components selection;
- Use principle of sufficiency for the chips selection (plan required capacity, avoid unnecessary embedded features);
- Local HMI to provide details on current HW status;
- Comprehensive HW behavior simulation;

Design: FPGA Electronic Design (Platform)

- Do not use third-party IP Cores (blackboxes) at all in safety-critical parts;
- Avoid asynchronous design;
- Do not create one process for a complex component (code transparency, readability);
- Coding Guides following is mandatory;



Design: FPGA Electronic Design (Application)

- Provide End-User with libraries for Application Design based on IEC 61131 list of components and our experience in Nuclear I&C systems development and supporting process;
- Application level receives all needed diagnostic information;
- Application Functional Block Library (AFBL) components perform defensive measures to protect the application from “bad data”;
- Each AFBL Component signals the “error” condition to the application via special pinouts and allow the End User decide what to do (safe state for the whole system or for the particular board, announcing etc.);

Design: Application design flows

Provide End-user with a means to implement Application logic Design diversity (two different design flows are available):

1. User Application Logic (UAL) is a part of FPGA-design. UAL-designer operates with AFBL components directly;

2. UAL is a bitstream generated by RadICS Platform Configuration Toolset (RPCT), stored in the Logic Module external EEPROM and processed by special AFB Controller inside the module FPGA each work cycle. UAL-designer operates with AFBL components via RPCT;

Design: FPGA Electronic Design (AFB Controller features)

- **AFB Controller is FSM** which performs operations in accordance with UAL bitstream generated by RPCT and stored in external EEPROM;
- **AFB Controller doesn't have branches or cycles;**
- **AFB Controller doesn't have interruptions;**
- AFB Controller provides determined processing time;

Design: FPGA Electronic Design (AFB Controller features)

- AFB Controller operates with determined set of AFBL Components;
- AFB Controller is not able to modify UAL bitstream or any input data;
- AFB Controller performs self-diagnostics to detect possible failures (SEU and user errors);

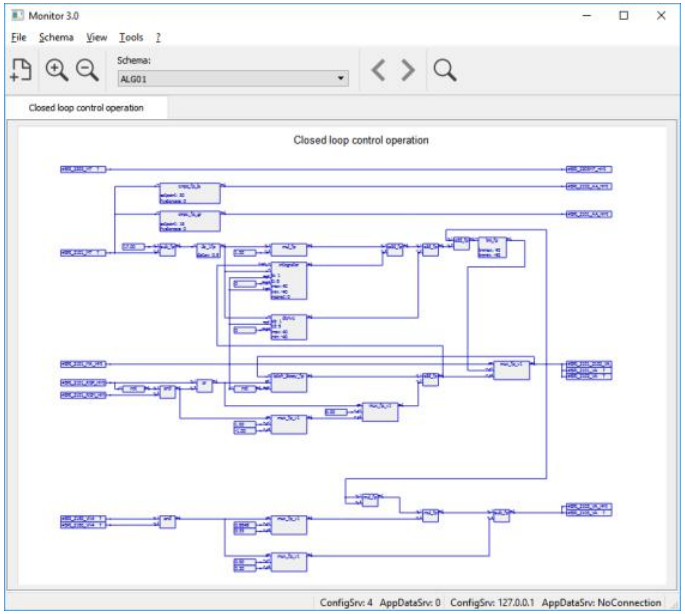
FPGA project recompilation is not required to change application logic;

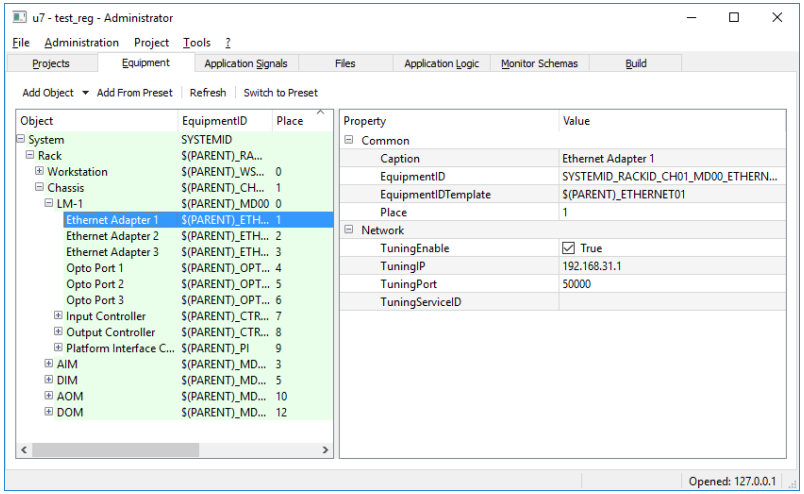
Design: Application Design Flows (Comparison Table)

Two different approaches of UAL execution in the platform	
FPGA only	**FPGA (Controller) + external EEPROM (Logic)**
Features	
Full parallelism is available	Only serial execution for application logic
UAL capacity depends on FPGA resources usage	UAL capacity depends on external EEPROM size
UAL change means FPGA ED recompilation	Frozen FPGA ED design.
FPGA vendor design tools are used to create and simulate UAL	RPCT
UAL V&V scope includes activities related to FPGA (LLS, STA, TS etc.)	UAL V&V process is simpler.
UAL designers have to be qualified in the field of HDL programming and be familiar with Logic Module ED architecture	Qualification requirements for designers are lower

RPCT Overview

➞ Integrated Development Environment (IDE)





➞ Monitoring and Tuning System (MATS)

RPCT Integrated Development Environment

Functions:

- Configure hardware architecture of FPGA-based Safety System (FSS);
- Define Application Signals which will be used in UAL;
- Design UAL using AFB items – representatives of corresponding AFB Components in FPGA;
- Configure MATS;
- Perform build, generate FPGA-based Safety Controllers (FSCs) and MATS configuration files;

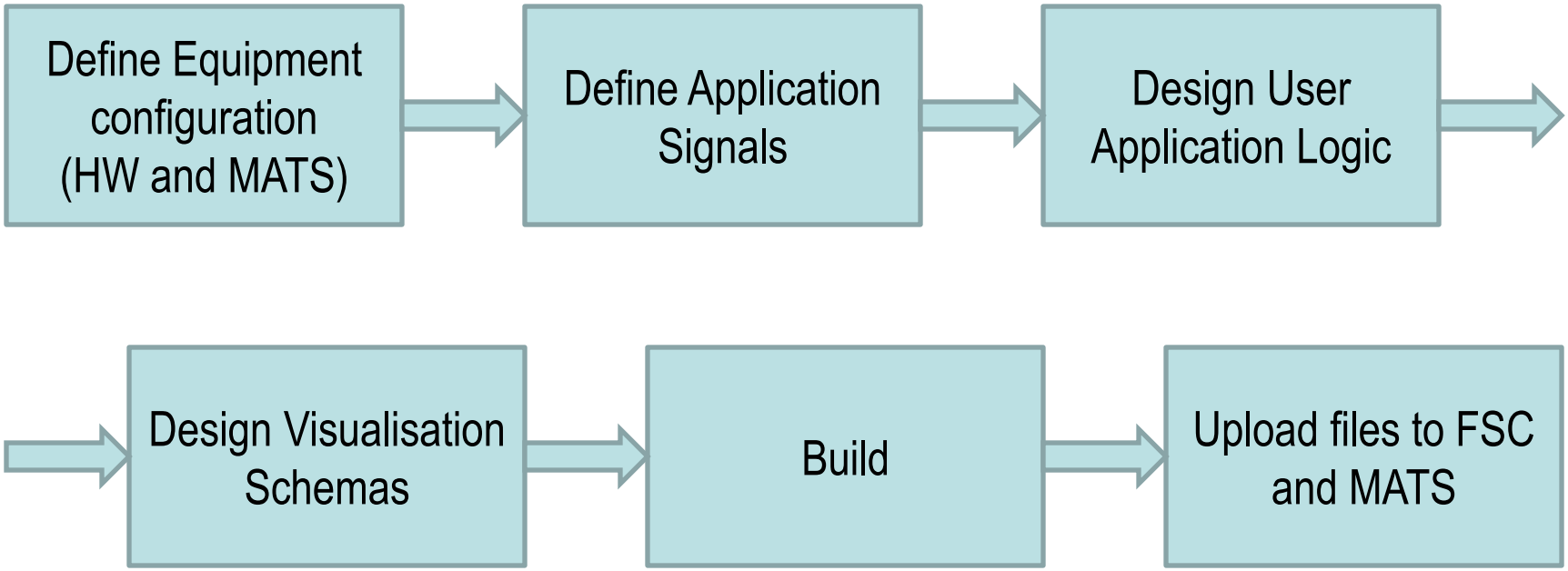
RPCT Integrated Development Environment (Cont.)

Features:

- Homemade;
- Client-server architecture;
- Multiuser access to project database;
- Version control system;
- Running on Windows or Linux OS;

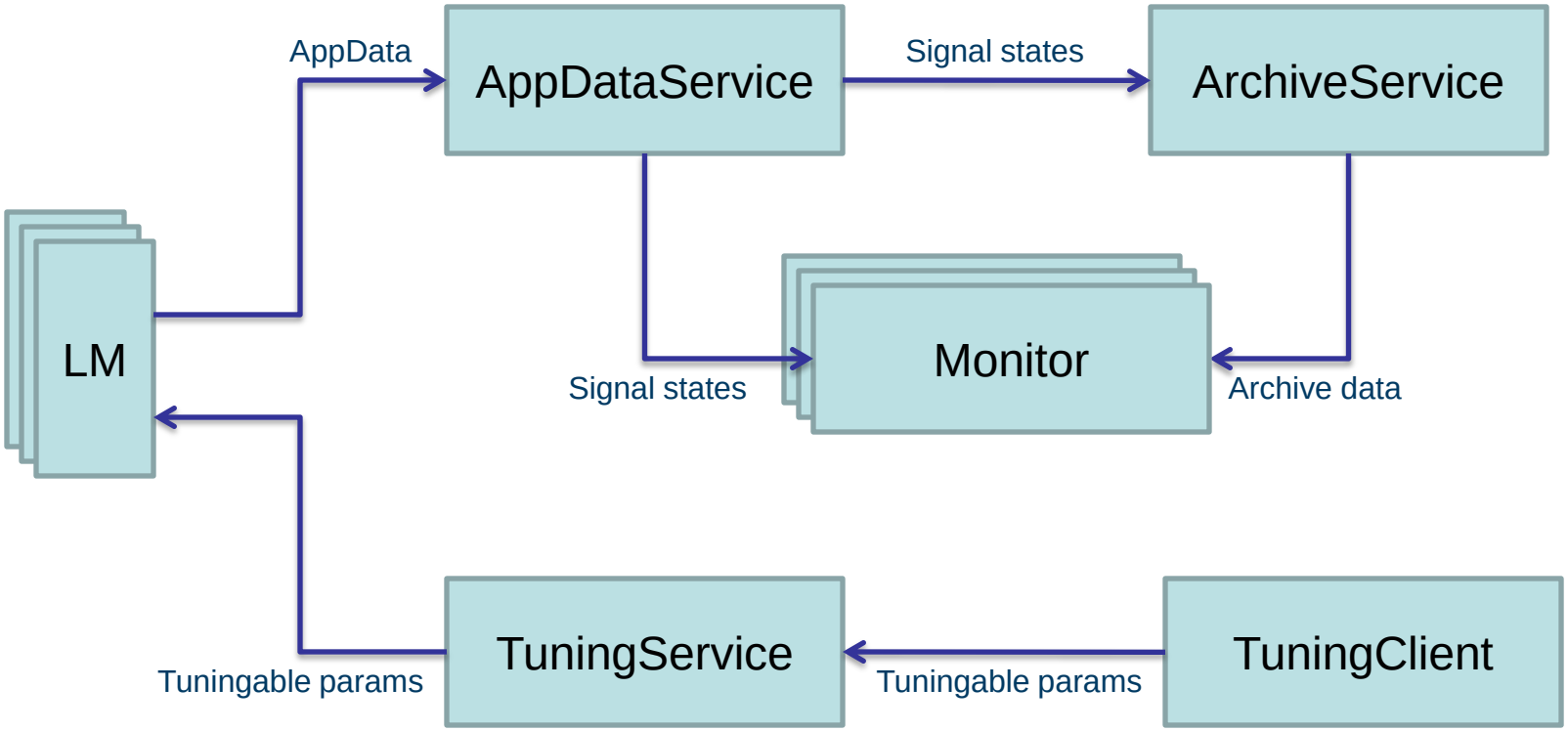
RPCT Integrated Development Environment (Cont.)

Project Design workflow:



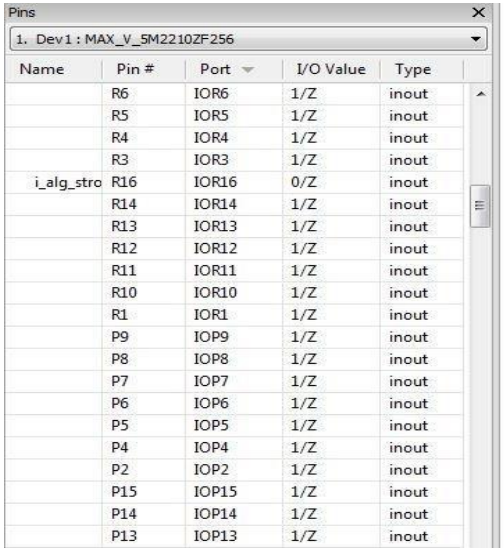
Monitoring and Tuning System (MATS)

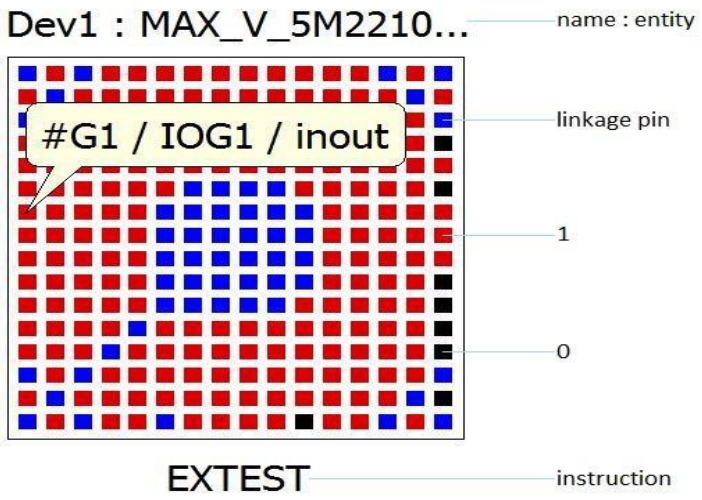
MATS Dataflow



Platform validation

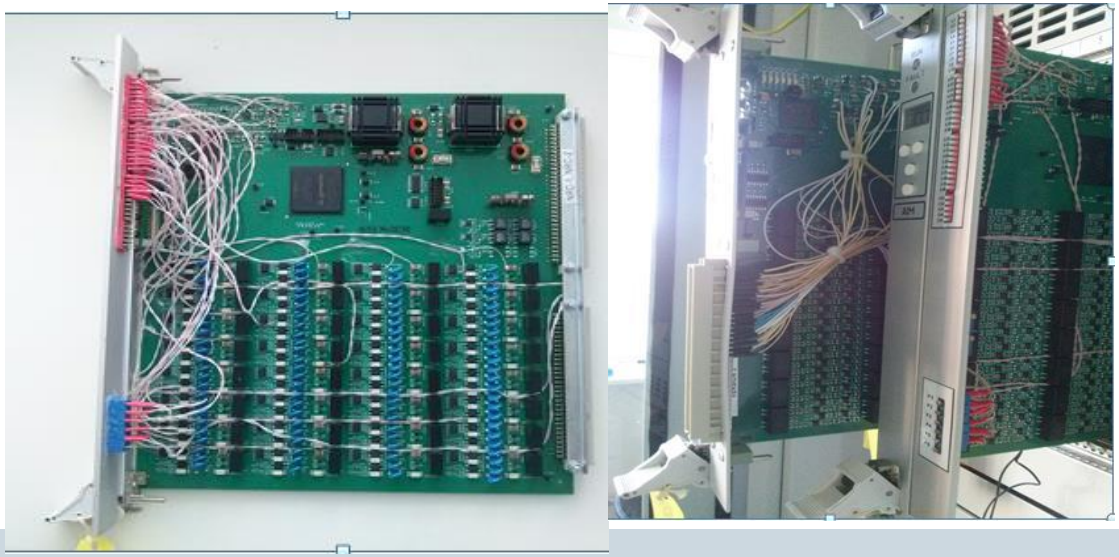
- Analytic Tests to check schematic design components critical characteristics;
- FPGA is a main focusing point (special tool is used to check pinouts health, usage etc.);





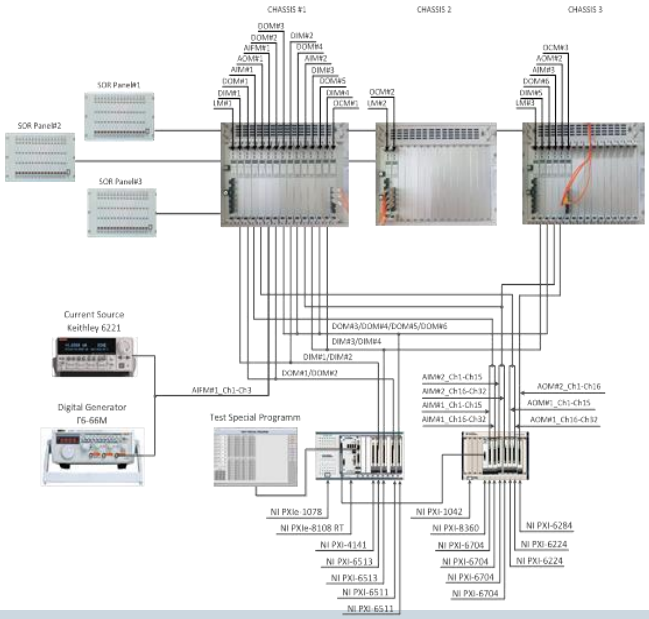
Platform validation (cont.)

- Fault insertion tests are based on FMEDA done by external experts (exida);
- FIT approaches - Diagnostic reaction of each object (module under test) is as important as reaction of the whole system;
- Faults are injected in circuits as well as in FPGA and in EEPROM(s) of the module;



Platform validation (cont.)

- Try to overstress our system under test (SUT) as much as possible (fully filled chassis, all modules are fully loaded, load is changed dynamically etc.);
- Automate our tests as much as we can (NI + LV are used);



Conclusions

- Platform provides sufficient flexibility in terms of I&C systems architecture design:
  - redundancy management;
  - diversity management;
  - two UAL design flows;
- FPGA technology and adapted design process ensures the high level of Cyber Security;
- We continuously improve our design technics and approaches;

We've started RadICS Platform US NRC Certification process (Topical Report submitted September 2016);

Safety products and applications make safety world!

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