Licensing and Certification Issues of FPGA-based Platform and Applications

Vladimir Sklyar, Technical Director

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

Licensing Documents

- Safety Product Quality Plan
- Quality Assurance Program
- Technical Specification
- Reliability Analysis Report (PSAR, FMEA as specific parts)
- Software Verification Plan and Software Verification Report
- Equipment Qualification Plan and Equipment Qualification Report
- Validation (FAT) Plan and Validation (FAT) Report
- SAT Plan and SAT Report
- Safety Evaluation Report

IEC standards applicable to FPGA-based NPP I&C systems

- IEC 61508 Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-related Systems
- IEC 61513 Nuclear power plants - Instrumentation and control important to safety - General requirements for systems
- IEC 62566 Nuclear power plants - Instrumentation and control important to safety - Development of HDL-programmed integrated circuits for systems performing category A functions
- IEC 60880 Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions
- IEC 62138 Nuclear power plants - Instrumentation and control important for safety - Software aspects for computer-based systems performing category B or C functions
- IEC 60987 Nuclear power plants - Instrumentation and control important to safety - Hardware design requirements for computer-based systems
- IEC 60780 Nuclear power plants - Electrical equipment of the safety system – Qualification

IEEE standards (endorsed by the U.S. NRC), EPRI and the U.S. NRC documents applicable to FPGA-based NPP I&C systems

- IEEE Std 603-1991, Criteria for Safety Systems for Nuclear Power Generating Stations
- IEEE Std 7-4.3.2-2003, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations
- IEEE Std 323-2003, IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations
- EPRI TR-107330, Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, December 1996
- DI&C-ISG-04, Revision 1, Highly Integrated Control Rooms - Digital Communication Systems
- BTP 7-14, Revision 5, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems

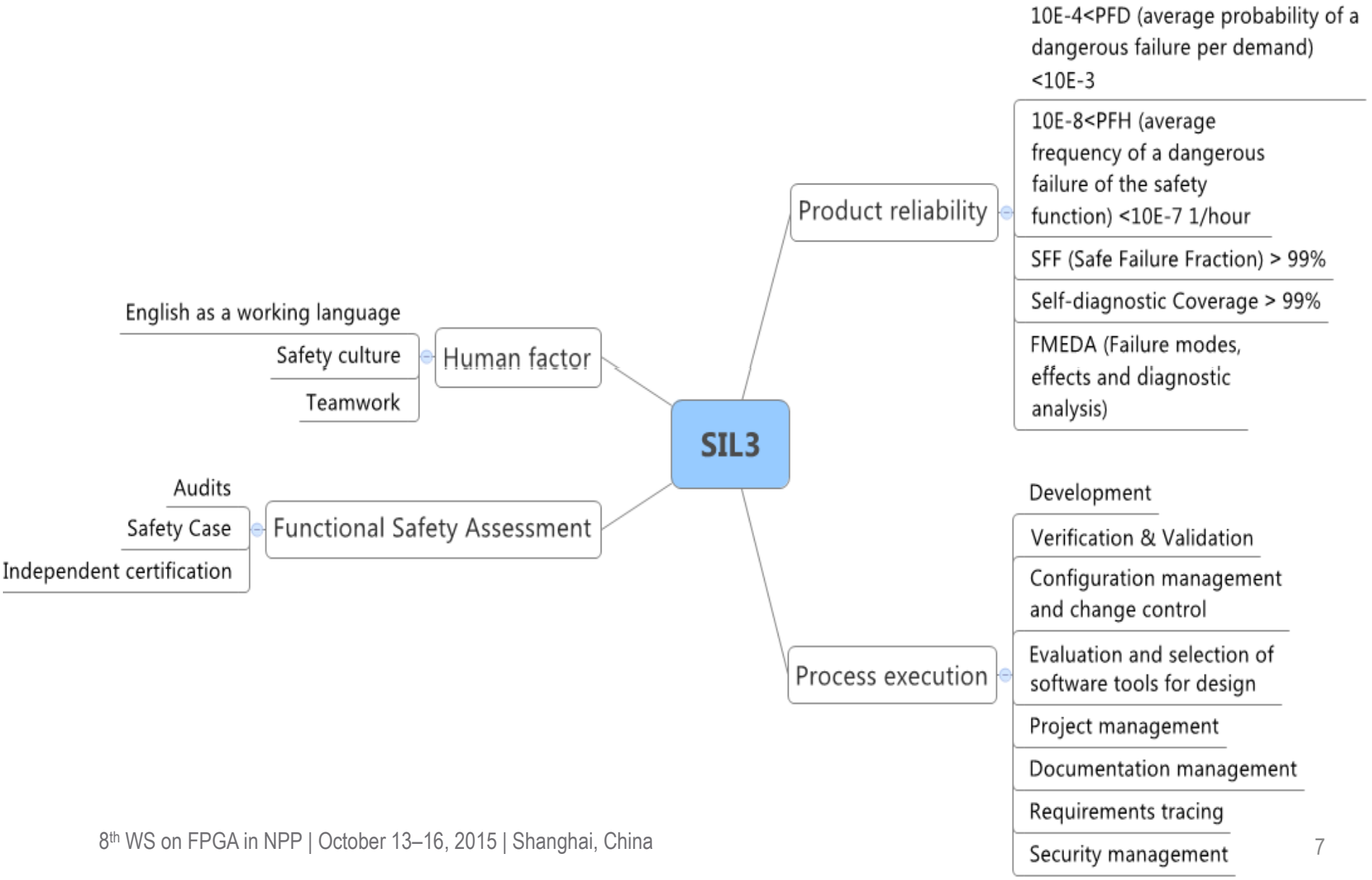
Radiy's experience in licensing of FPGA-based applications

- Since 1998: safety and safety-related I&C systems for Ukrainian NPPs (IEC and IAEA standards set with national requirements)
- 2008-2010: Bulgaria, 6 ESFAS' for Kozloduy NPP (IEC and IAEA standards set), Safety Class 2 (Category A) safety systems
- 2010-2014: RadICS platform SIL3 certification (IEC 61508), ***exida*** was a Certification Authority
- 2013-2014: Canada, Argentina, Window Annunciators, Pump Motor Speed Measuring Devices, Category A functions safety systems (IEC 61508, IEC 61226, IEC 61513)
- 2015: EdF, I&C Test Platform for R&D project (IEC 61226, IEC 61508, IEC 61513, IEC 60880, IEC 62566), licensing case study for Category A functions FPGA-based systems
- Since 2009: Radiy has been represented in IEC TC45A "Instrumentation, control and electrical systems of nuclear facilities" and has participated in standards development
- Analysis of national regulatory requirement of Finland, France, Slovakia, Hungary and other
- Since 2015: Preparation to QMS certification against 10CFR50, Appendix B and introducing Radiy to U.S. NRC

FPGA-based safety controller: RadICS Platform

LM DIM AIM AIFM DOM AOM OCM

Safety Integrity Level (SIL) 3 Certification Framework



exida CERTIFICATION

The manufacturer may use the mark:

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

ANSI Accredited Program
PRODUCT CERTIFICATION
#1004

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

Rudolf P. Chalupa
Certifying Assessor

Page 1 of 2

FPGA-Based Safety Controller (FSC) RadICS

exida CERTIFICATION

64 N Main St
Sellersville, PA 18960

T-002, V3R4-3

Certificate / Certificat / Zertifikat / 合格証

RAD 1406037 C001

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

Systematic Capability :

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.
A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.

Random Capability:

The SIL limit imposed by the Architectural Constraints must be met for each element.

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of average Probability of Failure on Demand (PFD_{AVG}), or Probability of Failure per hour (PFH), considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

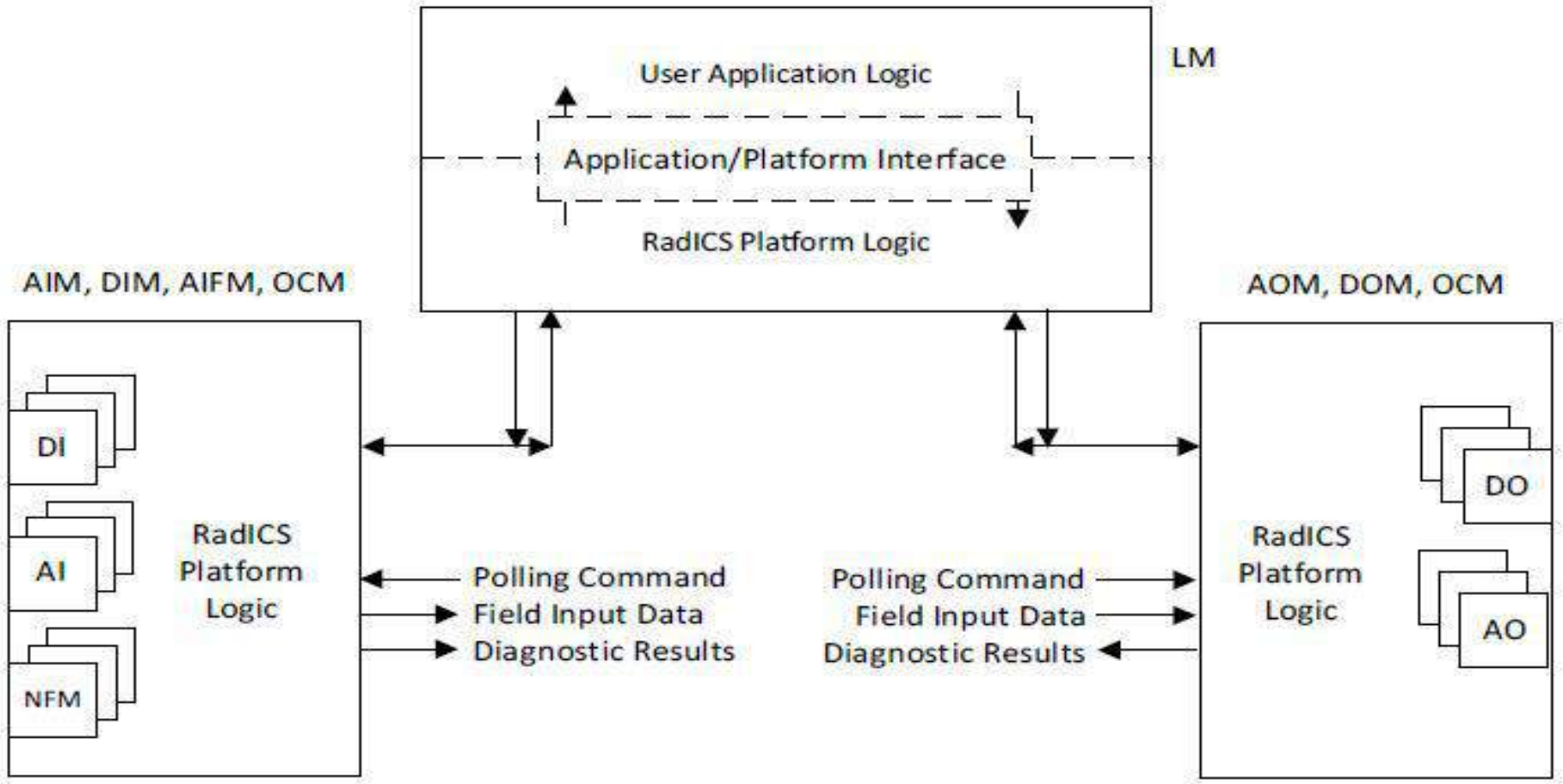
The following documents are a mandatory part of certification:

Assessment Report: RAD 14-06-037 R002 V1R0 61508 Assessment - FSC

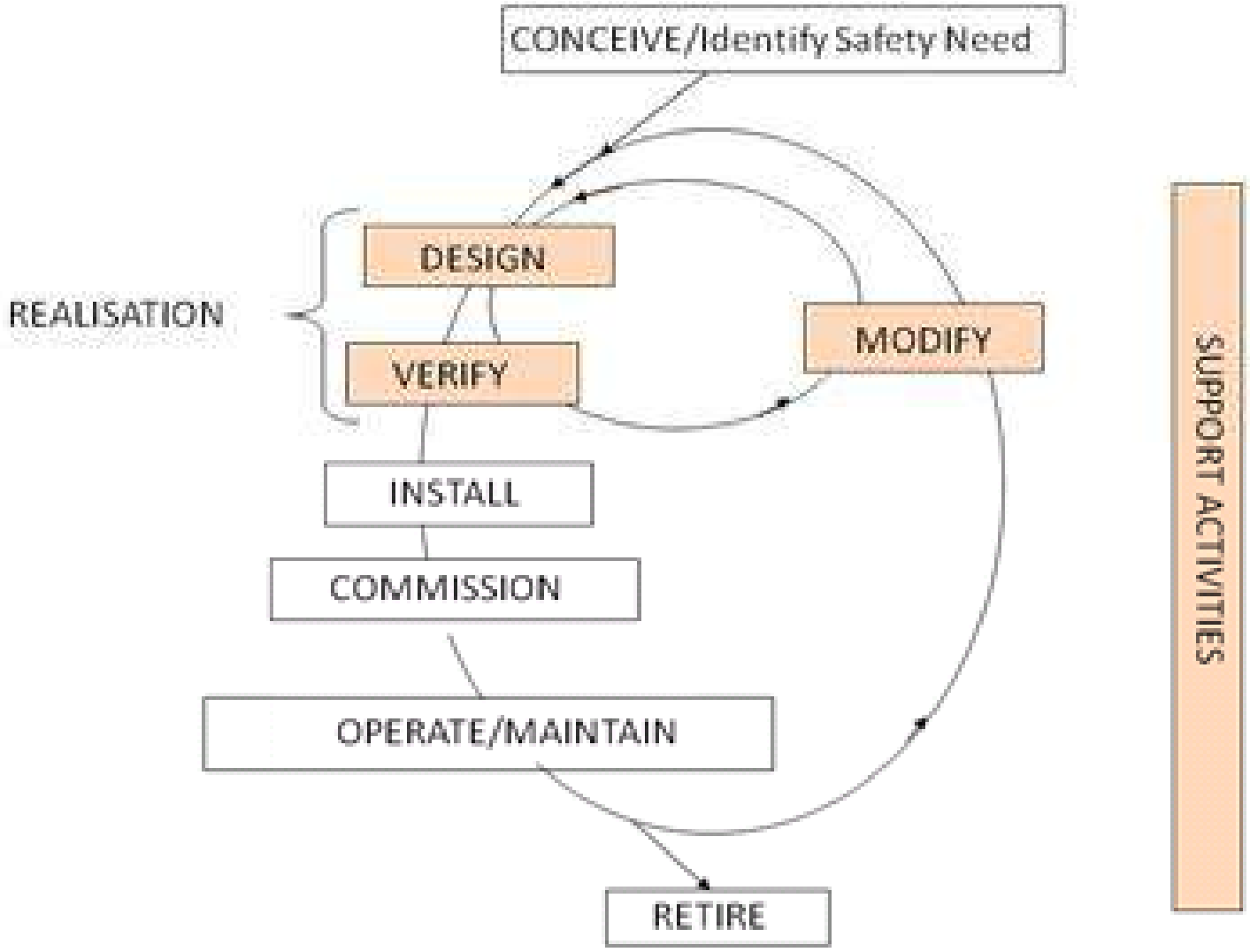
Safety Manual: D11.1 - Radiy FSC Product Safety Manual V1R2

Page 2 of 2

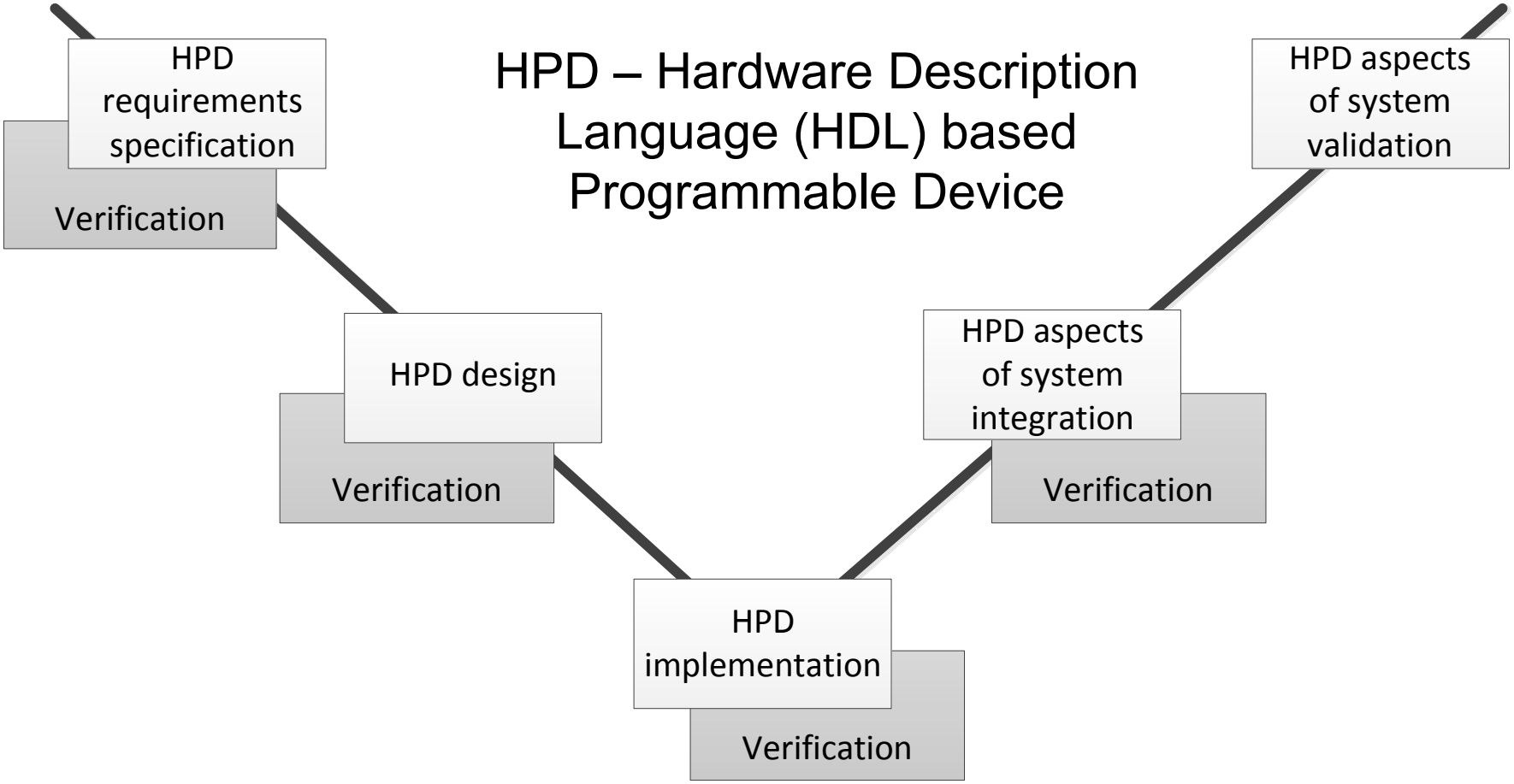
RadICS Platform: Modules connection into the chassis



Safety Life Cycle Concept



Safety Life Cycle based on pre-qualified platform (IEC 62566)



V&V technics

- → 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

Supporting life cycle processes and Project Management Activities

- Safety Case
- Functional Safety Management
- Functional Safety Audits
- Requirement Tracing
- Personnel Management
- Documentation Management
- Action Tracking
- Configuration Management and Change Control
- Tools Selection and Evaluation
- Security Management and Assessment

Equipment Qualification: IEC standards

- IEC 60780:1998 ed.2.0 Nuclear power plants - Electrical equipment of the safety system - Qualification
- IEC 60068-1:2013 ed.7.0 Environmental testing - Part 1: General and guidance
- IEC 60980:1989 ed.1.0 Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations
- IEC 62003:2009 ed.1.0 Nuclear power plants - Instrumentation and control important to safety - Requirements for electromagnetic compatibility testing
- IEC 61000-4-x. Electromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques

Equipment Qualification: EMC testing

- IEC 61000-4-2:2008 ed.2.0 Electrostatic discharge immunity test
- IEC 61000-4-3:2006 ed.3.0 Radiated, radio-frequency, electromagnetic field immunity test
- IEC 61000-4-4:2012 ed.3.0 Electrical fast transient/burst immunity test
- IEC 61000-4-5:2014 ed.3.0 Surge immunity test
- IEC 61000-4-6:2013 ed.4.0 Immunity to conducted disturbances, induced by radio-frequency fields
- IEC 61000-4-8:2009 ed.2.0 Power frequency magnetic field immunity test
- IEC 61000-4-9:1993 ed.1.0 Pulse magnetic field immunity test
- IEC 61000-4-10:1993 ed.1.0 Damped oscillatory magnetic field immunity test
- IEC 61000-4-11:2004 ed.2.0 Voltage dips, short interruptions and voltage variations immunity tests
- MIL-STD-461E, DOD Interface Standard Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment

Equipment Qualification: IEEE

- IEEE Std 323-2003, IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations
- IEEE Std 344-2004, IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations
- IEEE Std 384-1992, Standard Criteria for Independence of Class 1E Equipment and Circuits
- EPRI TR-107330, Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, December 1996

Software Requirements: IEEE

- BTP 7-14, Revision 5, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems
- IEEE Std 730-1998, IEEE Standard for Software Quality Assurance Plans
- IEEE Std 828-2005, IEEE Standard for Software Configuration Management Plans
- IEEE Std 829-2008, IEEE Standard for Software Test Documentation
- IEEE Std 830-1998, IEEE Recommended Practice for Software
- IEEE Std 1008-1987, IEEE Standard for Software Unit Testing
- IEEE Std 1012-2004, IEEE Standard for Software Verification and Validation Plans
- IEEE Std 1028-2008, IEEE Standard for Software Reviews and Audits
- IEEE Std 1074-2006, IEEE Standard for Developing Software Life Cycle Processes

Protection against Common Cause Failure (CCF)

- IEC 62340:2007 ed.1.0 Nuclear power plants - Instrumentation and control systems important to safety - Requirements for coping with common cause failure (CCF)
- Using independence principle in RadICS platform and in I&C applications design
- Using self diagnostic to discover components failures
- Diversity principle implementation

Independence principle

- Physical separation of system channels
- Galvanic isolation of I/Os in one hardware module
- Independent power supply
- Avoidance of failure propagation via communications paths (one direction digital communications only from controller to HMI)

Self diagnostic

- Diagnostic of hardware units on modules boards
- Each of the module is equipped with a watchdog independent from FPGA
- Diagnostic of FPGA's RAM and Electronic Design integrity
- Diagnostic of data transition with CRC64
- Transition of I&C system to the safe state (outputs de-energize to trip) in case of critical failure appearance

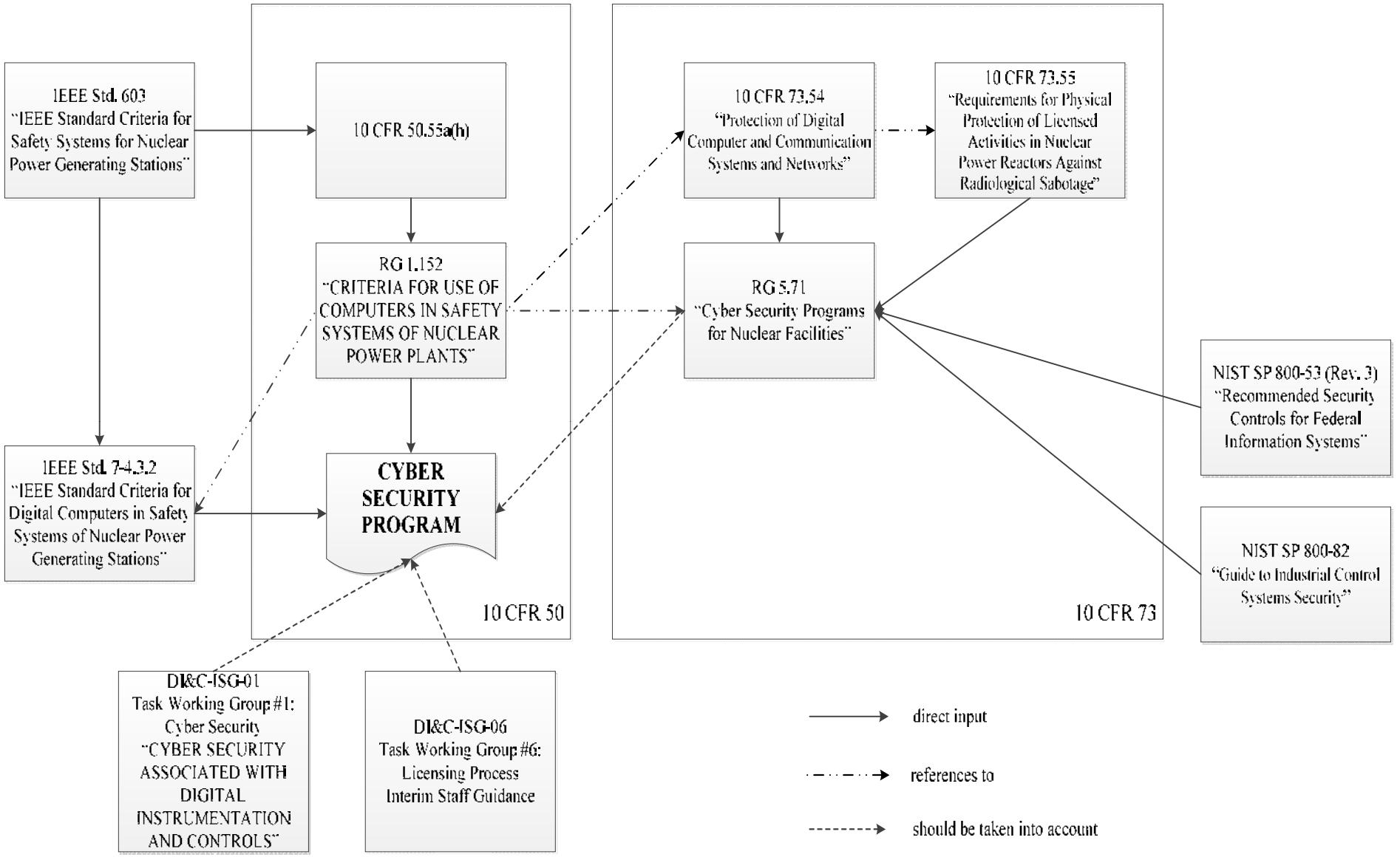
Diversity types (NUREG/CR-6303-1994, NUREG/CR-7007-2008)

- Design Diversity – different technologies and architectures
- Equipment Diversity – different hardware
- Functional Diversity – different control logic
- Human Diversity – different teams of designers and/or verificators
- Signal Diversity – different physical parameters and sensors
- Software Diversity – different source code implementation

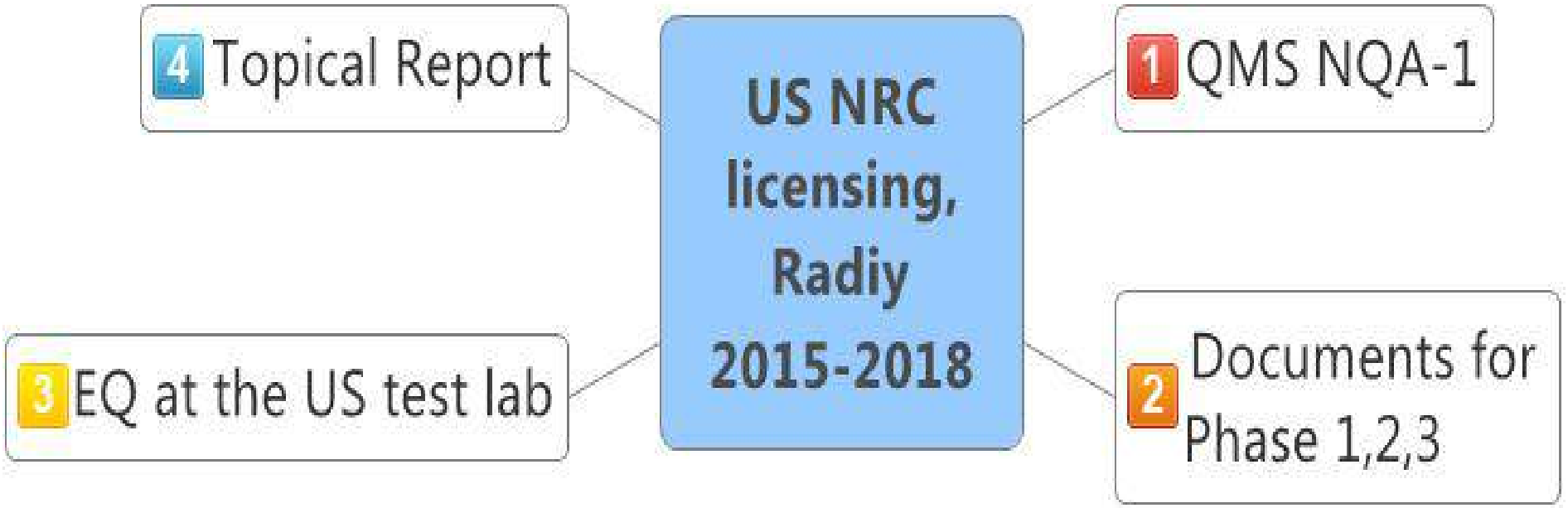
Diversity types implementation opportunities with FPGAs

- FPGA vs PLC
- FPGAs based systems from different vendors
- FPGAs based systems from the same vendor with different hardware using different FPGA chips programmed with different design tools
- All six diversity types can be implemented with FPGA-based systems

Security aspects in accordance with US NRC requirements



RadICS Platform Certification against the U.S. NRC expectations



QMS NQA-1

- In 2015, Radiy started work to fully align Radiy's QMS, implementing procedures, and training with 10 CFR Part 50, Appendix B, ASME NQA-1-2008, 10 CFR 21 in preparation for submittal of RadICS Topical Report to NRC
  - QA Program document
  - Implementing procedures for 18 criteria of Appendix B
  - Training program for RadICS personnel on QA Program document and implementing procedures
  - Lead auditor and inspector qualifications and training
  - Support activities for commercial grade dedication work supporting RadICS Topical Report

Commercial Grade Dedication Strategy

- EPRI TR-106439 is used to structure the CGD effort
  - Compliance with EPRI TR-106439 process will be demonstrated using a checklist, which provided a mapping that shows where the elements of the dedication process are addressed in licensing documentation
- RadICS CGD plan uses a combination of three acceptance methods described in EPRI TR-106439 to verify the adequacy of the platform:
  - Method 1: Special Tests and Inspections of the equipment
  - Method 2: Commercial Grade Survey of hardware and electronic design development processes
  - Method 4 (additional): Acceptable Performance Record of the RadICS platform

Qualification Test Plan

- Factory Acceptance Testing
- Pre-Qualification Acceptance Testing
- Radiation Exposure Withstand Testing
- Environmental Testing
- Seismic Testing
- Electromagnetic Compatibility Testing
- Electrical Fast Transient Testing
- Surge Withstand Testing
- Electrostatic Discharge (ESD) Testing
- Class 1E to Non-Class 1E Isolation Testing
- Performance Proof Testing
- Operability Testing
- Prudency Testing

Conclusions: Licensing and Certification Issues of FPGA-based Platform and Applications

- Safety life cycle with V&V – mostly related with FPGA technology
- Computer Security – related with FPGA technology
- Diversity – related with FPGA technology
- Self diagnostics – related with FPGA technology
- Independence principle
- Equipment Qualification
- QMS and Commercial Grade Dedication

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