Licensing of FPGA-based Safety Platform RadICS: Case Study

Anton Andrashov, Head of International Projects Division

10th International Workshop on the Application of FPGAs in NPPs
December 4-6 2017, Gyeongju, Republic of Korea

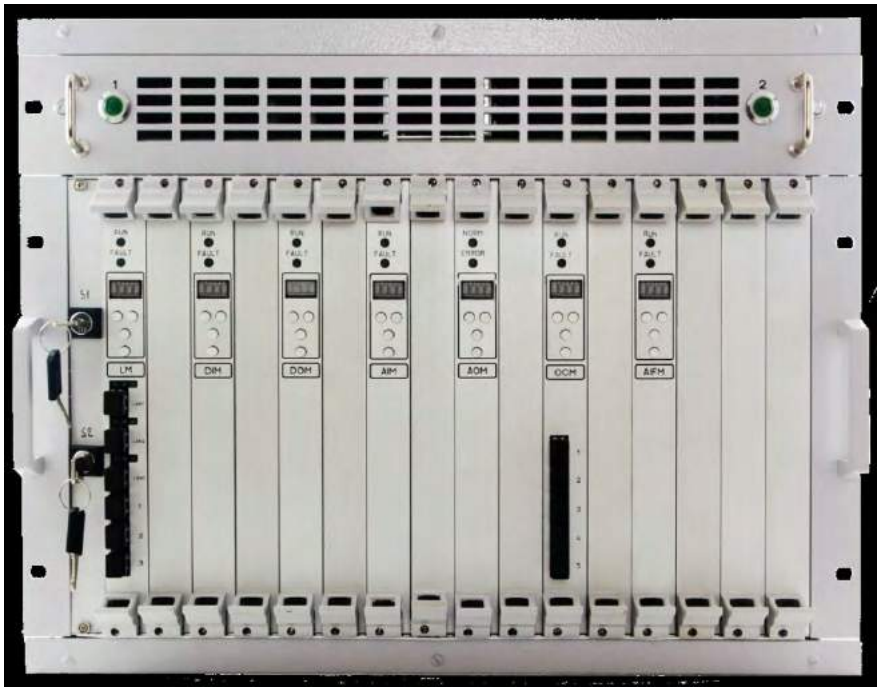
Agenda

- Introduction
- IEC 61508 Certification
- US NRC Licensing
- Conclusions

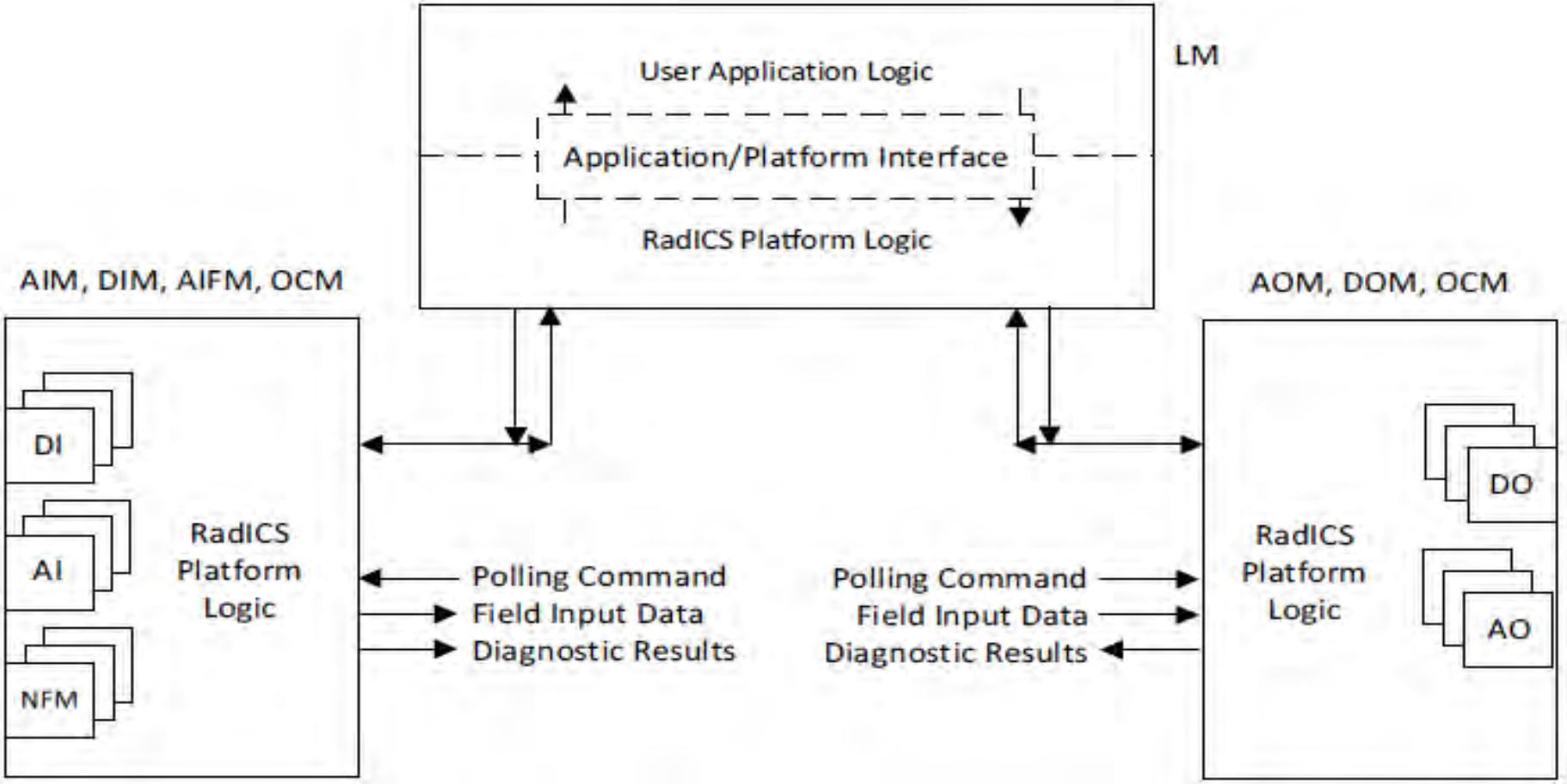
Introduction

Introduction (1)

- RPC Radiy is a vendor of FPGA-based I&C Platform/Systems for NPPs
- Main product is RadICS Platform SIL-3 (single channel) certified as per IEC 61508:2010
- Topical Report for the RadICS Platform is under the U.S. NRC review



Introduction (2)

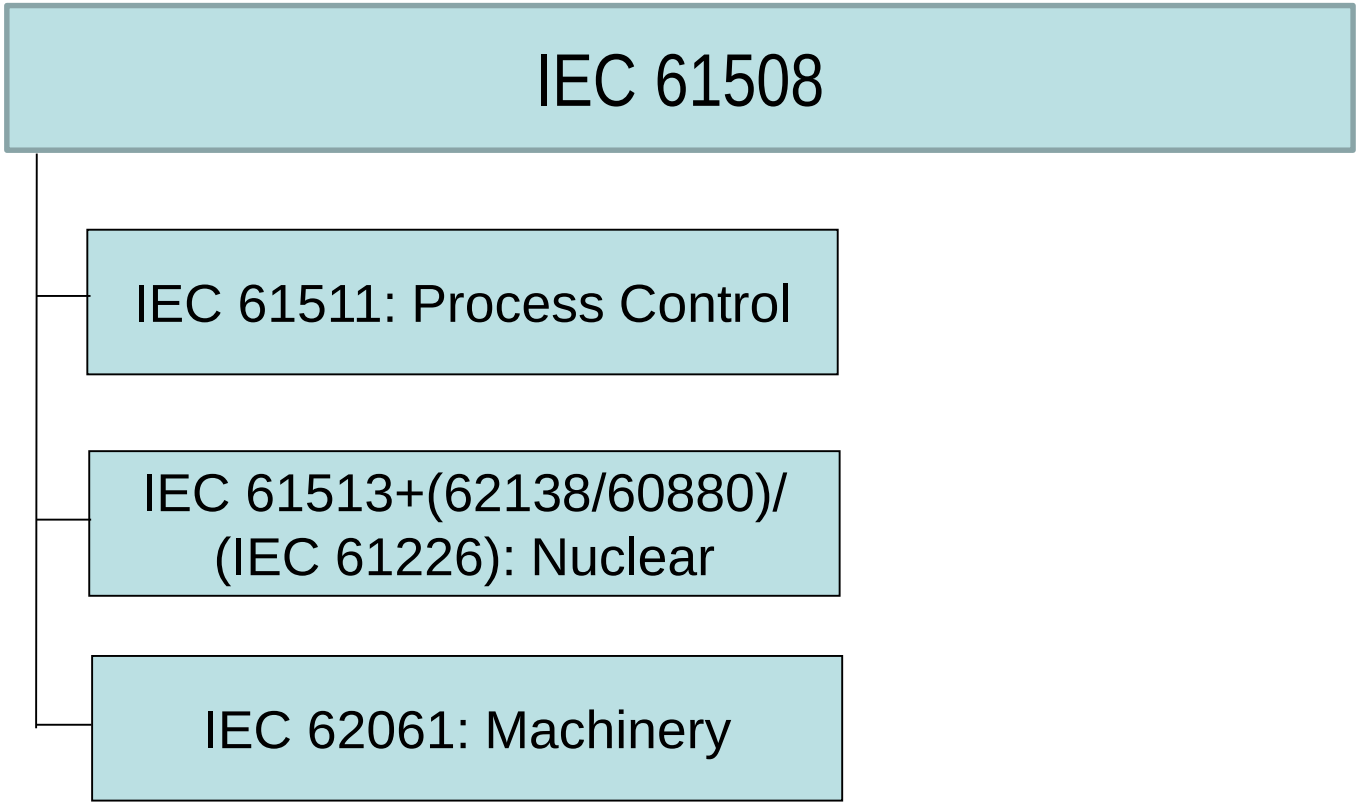


Introduction (3)

- ➞ 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 1 (Category A) system
- ➞ 2010-2014: RadICS platform SIL3 certification (IEC 61508)
- ➞ 2013-2014: Canada, Argentina, Window Annunciators, Pump Motor Speed Measuring Devices, Category 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 62566) licensing case study for FPGA-based systems
- ➞ 2016: Topical Report for RadICS Platform submitted to the US NRC

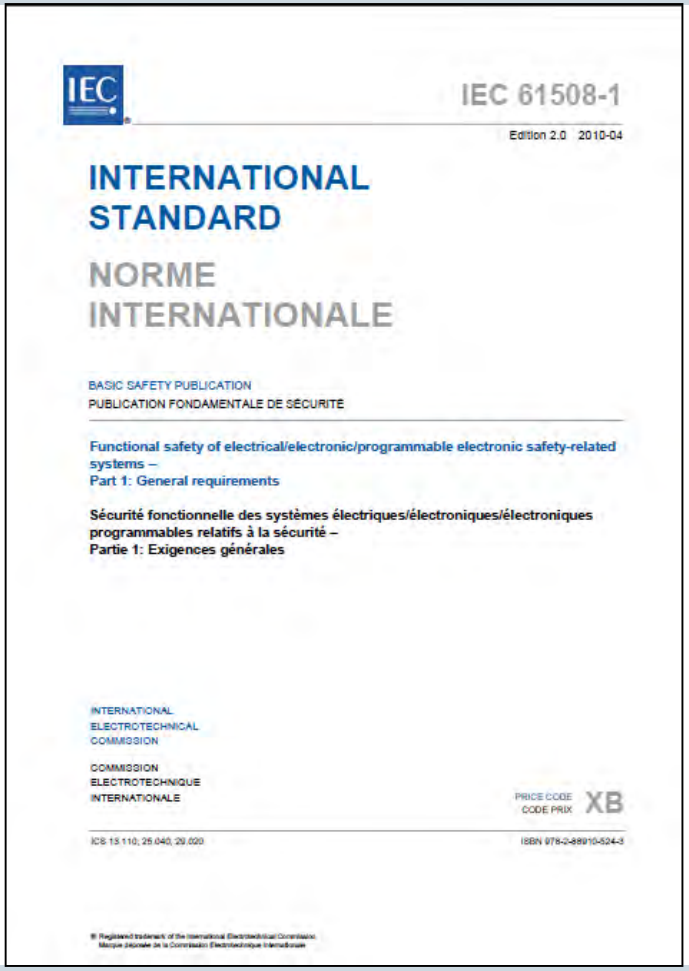
IEC 61508 Certification

IEC 61508 Certification (1)



IEC 61508 Certification (2)

- The first edition was issued in 1998-2000;
- The second edition has been issued in April 2010;
- IEC 61508 includes 7 parts with 594 pages;
- IEC 61508 bases on SIL 1-SIL 4 concept for specifying the safety integrity requirements of the safety functions;
- In some countries (for example, Canada) IEC 61508 is mandatory for NPP I&C systems.


IEC

IEC 61508-1

Edition 2.0 2010-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

BASIC SAFETY PUBLICATION
PUBLICATION FONDAMENTALE DE SÉCURITÉ

Functional safety of electrical/electronic/programmable electronic safety-related systems –
Part 1: General requirements

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité –
Partie 1: Exigences générales

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE CODE PRIX XB

ICS 13.110; 25.040; 29.020

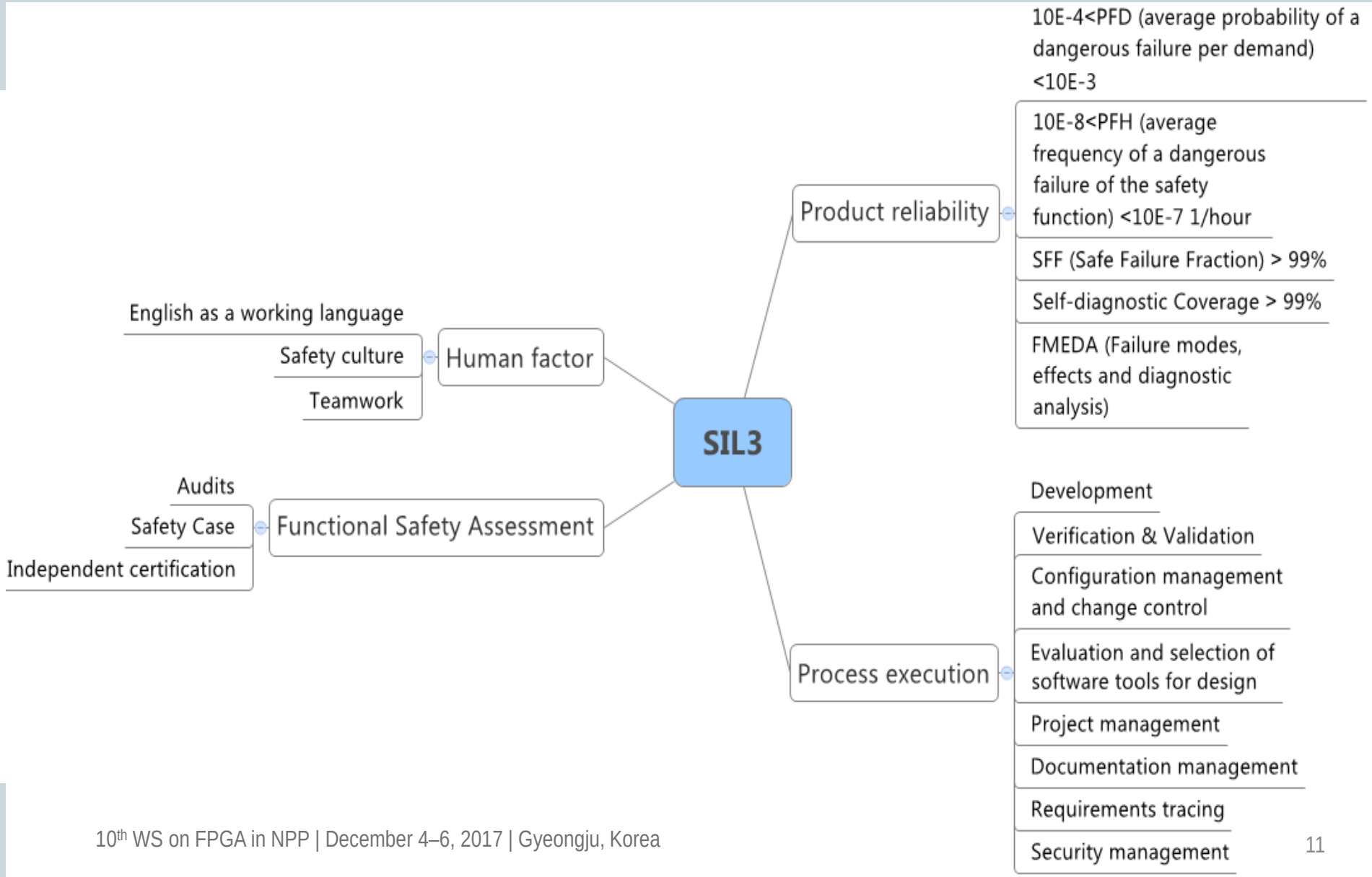
ISBN 978-2-88910-524-3

IEC 61508 Certification (3)

SIL (safety integrity level)

SIL Safety Integrity Level	**PFDavg** Average probability of failure on demand per year (low demand)	**(1-PFDavg)** Safety availability	**RRF** Risk Reduction Factor	**PFDavg** Average probability of failure on demand per hour (high demand)
SIL 4	**$\geq 10^{-5}$ to $< 10^{-4}$**	**99.99 to 99.999 %**	**100000 to 10000**	**$\geq 10^{-9}$ to $< 10^{-8}$**
SIL 3	**$\geq 10^{-4}$ to $< 10^{-3}$**	**99.9 to 99.99 %**	**10000 to 1000**	**$\geq 10^{-8}$ to $< 10^{-7}$**
SIL 2	**$\geq 10^{-3}$ to $< 10^{-2}$**	**99 to 99.9 %**	**1000 to 100**	**$\geq 10^{-7}$ to $< 10^{-6}$**
SIL 1	**$\geq 10^{-2}$ to $< 10^{-1}$**	**90 to 99 %**	**100 to 10**	**$\geq 10^{-6}$ to $< 10^{-5}$**

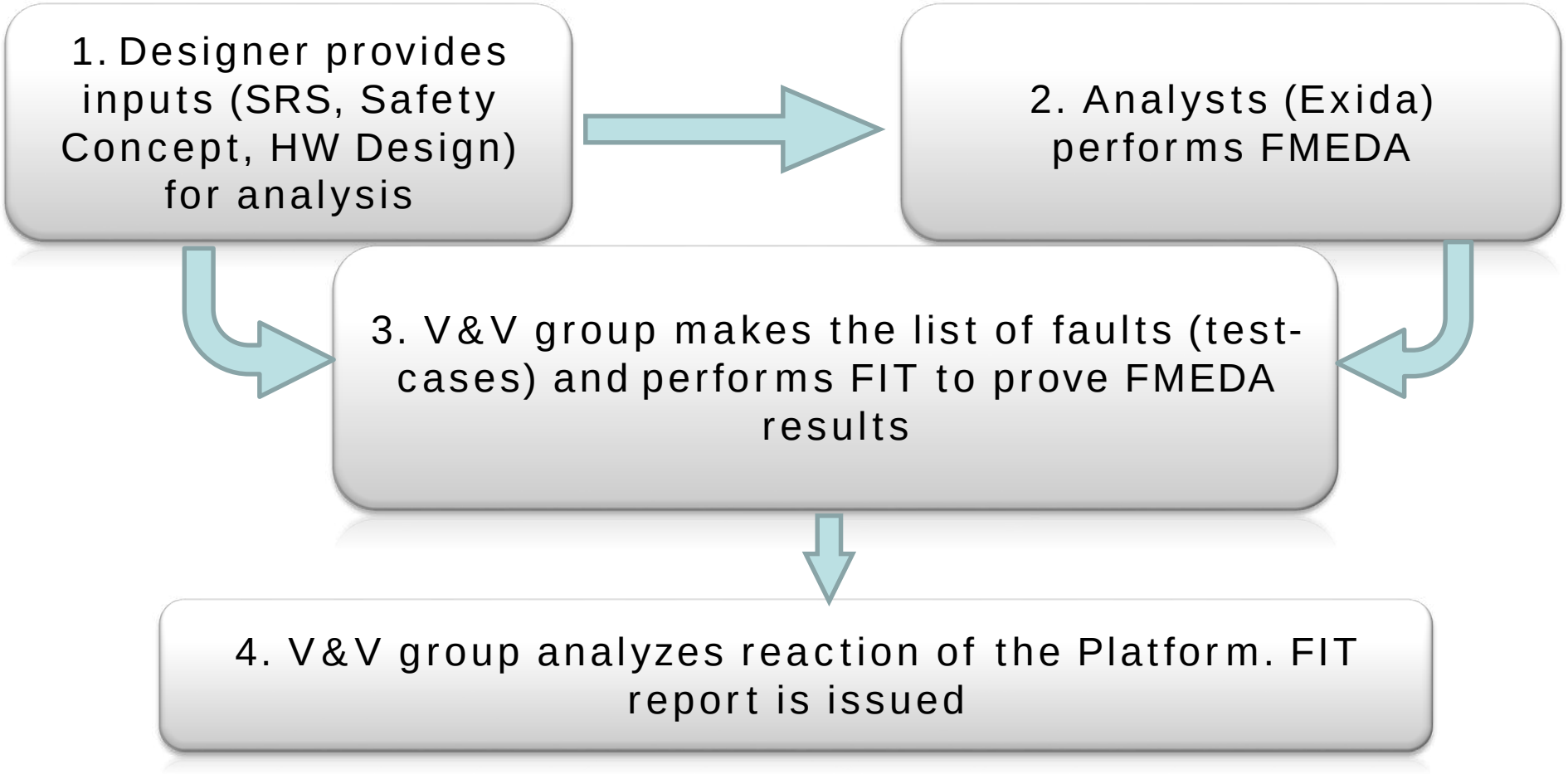
IEC 61508 Certification (4)



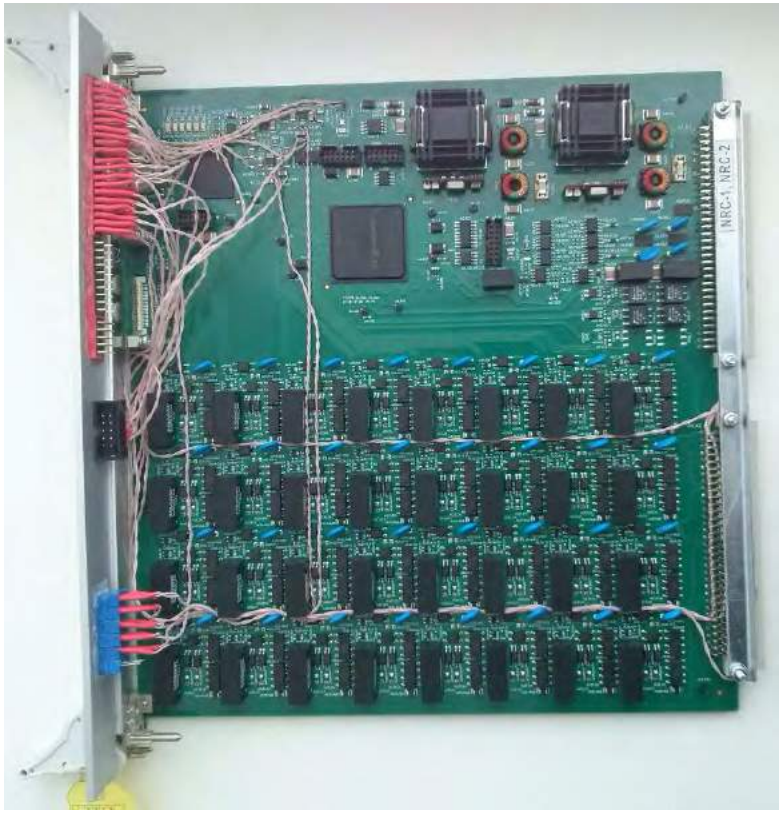
IEC 61508 Certification (5)

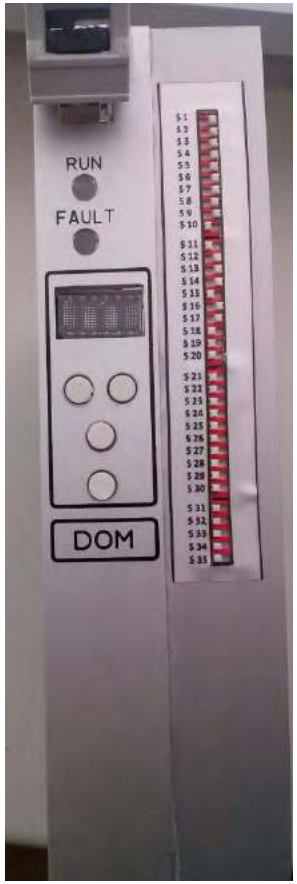
- Documents Review
- Failure and Mode Effect Diagnostic Analysis (FMEDA)
- Static Code Analysis and Code Review
- HDL Code Functional Testing
- Logic Level Simulation, Timing Simulation and Static Timing Analysis (for FPGA Electronic Design)
- Reports Review of Synthesis, Place and Route, Bitstream Generation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

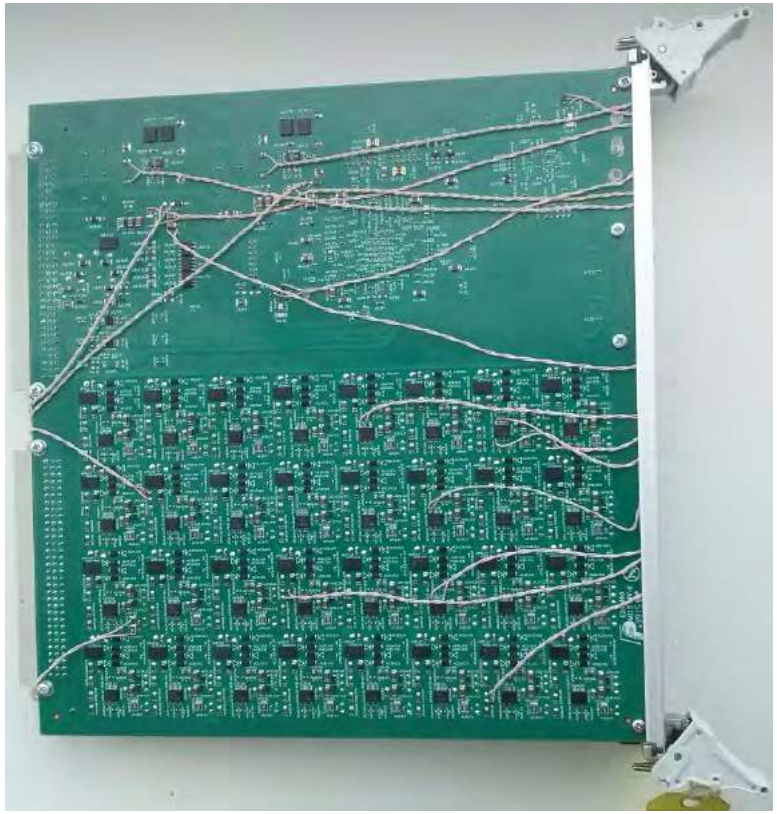
IEC 61508 Certification (6)



IEC 61508 Certification (7)

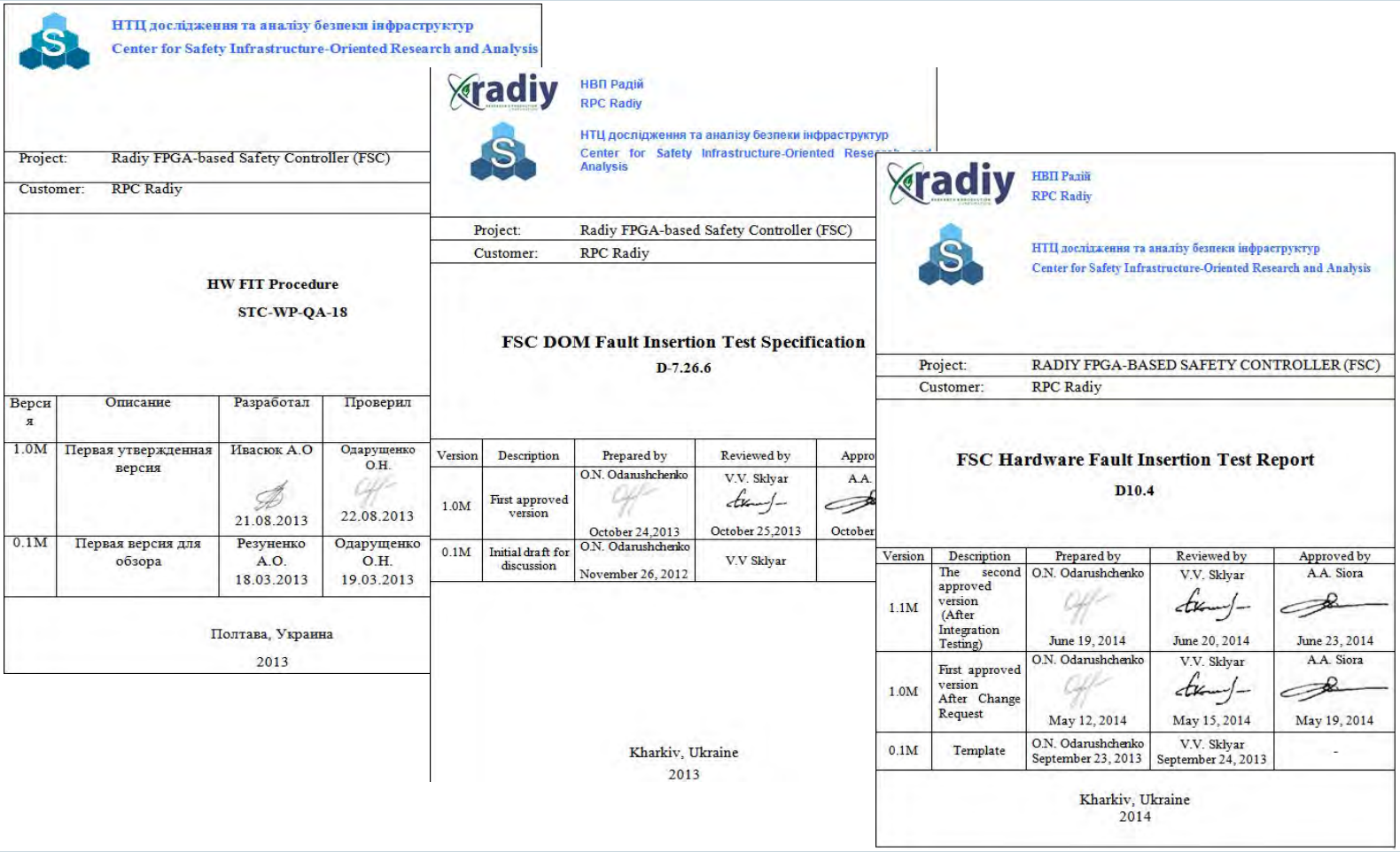






IEC 61508 Certification (8)

IEC 61508 Certification (9)



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

Project:	Radiy FPGA-based Safety Controller (FSC)
Customer:	RPC Radiy

HW FIT Procedure

STC-WP-QA-18

Версия	Описание	Разработал	Проверил
1.0M	Первая утвержденная версия	Ивасюк А.О 21.08.2013	Одарущенко О.Н. 22.08.2013
0.1M	Первая версия для обзора	Резуненко А.О. 18.03.2013	Одарущенко О.Н. 19.03.2013

Полтава, Украина
2013

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 DOM Fault Insertion Test Specification

D-7.26.6

Version	Description	Prepared by	Reviewed by	Appro
1.0M	First approved version	O.N. Odarushchenko October 24,2013	V.V. Sklyar October 25,2013	A.A. October
0.1M	Initial draft for discussion	O.N. Odarushchenko November 26, 2012	V.V Sklyar	

Kharkiv, Ukraine
2013

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
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
0.1M	Template	O.N. Odarushchenko September 23, 2013	V.V. Sklyar September 24, 2013	-

Kharkiv, Ukraine
2014

IEC 61508 Certification (10)

- 737 requirements of IEC 61508 standard
- Approximately 200 documents produced (totally 50 thousands pages)
- One year (2010-2011) for preparation and 3 years (2011-2014) for execution
- Up to 70 people were working on the project in different time periods
- Project Core Team: 7 people in design team, 10 people in V&V team, 5 people in PM team and safety assessment team, 2 people in infrastructure support team
- Total project effort is more than 50 man/years

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

The manufacturer may use the mark:

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

ANSI Accredited Program
PRODUCT CERTIFICATION
#1004

FPGA-Based Safety Controller (FSC) RadICS

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

IEC 61508 Certification (11)

- Vendor's benefits:
  - 3rd Party revirew of the product
  - FMEDA + FIT
- Customer's benefits
  - Reliability numbers for product (PFD)
  - Warranty of the use of rigorous safety lifecycle processes for the product design
  - Safety Manual for product
- Regulator's benefits:
  - 3rd party review by competent (certified) experts
  - Additional evidence for the decision making

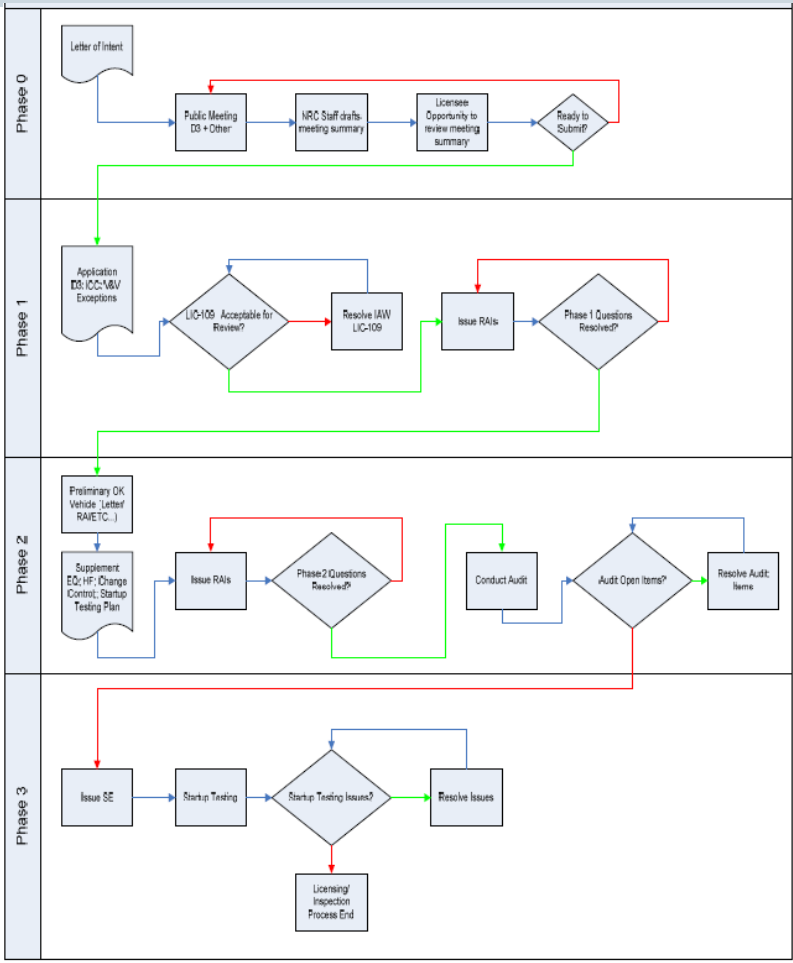
US NRC Licensing

US NRC Licensing (1)

- 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
- DI&C-ISG-06, Revision 1, Licensing Process
- BTP 7-14, Revision 5, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems

US NRC Licensing (2)

- Licensing strategy is based on Digital I&C-ISG-06
- Consist of
  - Phase 0
  - Phase 1
  - Phase 2
  - Phase 3



US NRC Licensing (3)

- Pre-Application Activities (Phase 0) - Goal is to reach general agreement with NRC that:
  - RadICS conceptual design is acceptable
  - Equipment qualification plans are appropriate
  - Commercial grade dedication strategy is acceptable
  - Document submittal plans are understood
  - Overall RadICS project schedule is reasonable
- RadICS Phase 0 Activities
  - Topical Report preparation
  - Equipment qualification plan development
  - Commercial grade dedication plan development
  - 10 CFR Part 50 Appendix B QA Plan certification and implementation

US NRC Licensing (4)

- RadICS Topical Report Submittal (Phase 1) - Goal is to have application accepted for review and get early feedback on acceptability of EQ Plan:
  - RadICS Topical Report
  - RadICS Equipment Qualification Plan
  - RadICS Commercial Grade Dedication Plan
  - DI&C-ISG-06 Phase 1 Submittals
- RadICS Phase 1 Activities
  - Topical Report review support
  - Equipment qualification plan implementation
  - Commercial grade dedication plan implementation
  - Respond to NRC Round 1 requests for additional information
  - Prepare Phase 2 Documents for submittal

US NRC Licensing (5)

- Pre-Application Activities (Phase 2) - Goal is to provide timely responses and have successful audits :
  - RadICS Equipment Qualification Summary Report
  - RadICS Commercial Grade Dedication Summary Report
  - DI&C-ISG-06 Phase 2 Submittals
- Radiy Phase 2 Activities
  - Topical Report review support
  - Support NRC audits, as necessary
  - Respond to NRC Round 2 requests for additional information
  - Prepare Final Topical Report Update
  - Review draft safety evaluation report for proprietary information

US NRC Licensing (6)

- Pre-Application Activities (Phase 3) - Goal is to provide timely issuance of approved RadICS Topical Report:
  - RadICS Topical Report (–A Versions)
- Radiy Phase 3 Activities
  - None, project complete

US NRC Licensing (7)

- 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

US NRC Licensing (7)

- Topical Report submitted on Sep 21, 2016
- Acceptance review letter received on Apr 5, 2017
- Topical Report Review will start in Aug, 2017
- RAI will be issued in March, 2018
- Safety Evaluation report draft will be issued by June, 2019

Conclusions

Conclusions

Criteria	SIL (IEC 61508)	U.S. NRC
Quality Management System	Doesn't say about QMS, ISO9001 is usually applicable	10 CFR50, Ap. B
Equipment Qualification	Doesn't say about EQ levels, it is an applicant choice	EPRI TR 107330
Safety Life Cycle	IEC 61508, Part 2	NUREG 0800
Reliability and Availability Analysis	Probability (Frequency) of a Dangerous Failure, FME(D)A, Safe Failure Fraction, Diagnostic Coverage	FMEA, Reliability and Availability indexes
Final document	Functional Safety Assessment Report by Certification Body	Safety Evaluation Report by U.S. NRC

Thank you for your attention!

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