



Digital I&C Qualification and Licensing Issues

Anton Andrashov, Head of International Projects Division, RPC Radiy

Innovations in Nuclear Technology 2012 – Brazil: Challenges and Opportunities
(INT2012) | December 10–11, 2012 | Sao Paulo, Brazil



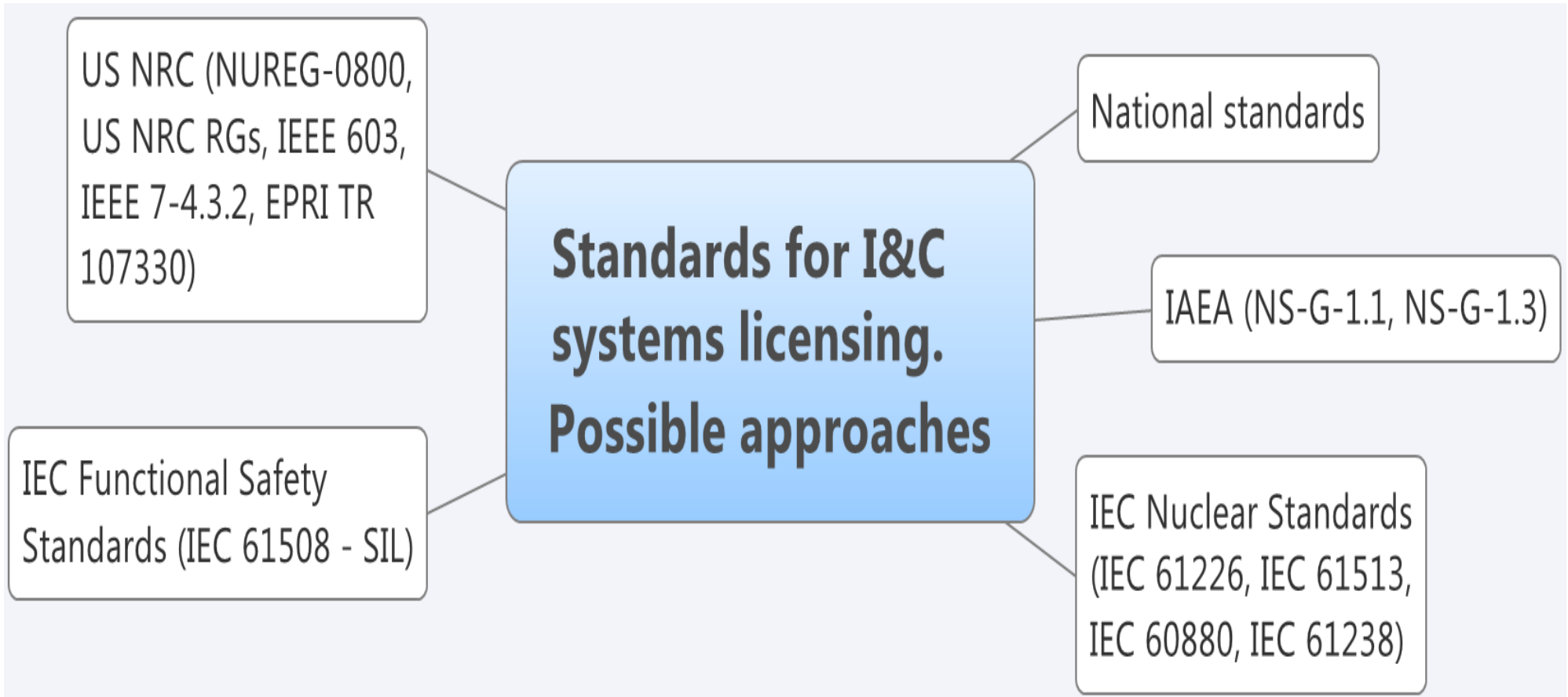
Agenda

- General licensing framework for digital I&C platforms and systems
- U.S. NRC approach to qualify FPGA-based safety I&C platform
- SIL (IEC 61508) approach to qualify FPGA-based safety I&C platform
- Conclusions

General licensing framework for digital I&C platforms and systems



General licensing framework for digital I&C platforms and systems



U.S. NRC approach to qualify FPGA-based safety I&C platform

US NRC Regulatory Requirements for I&C systems

NUREG-8000, Standard Review Plan, Chapter 7, I&C – Overview of Review Process

RG 1.28, Quality Assurance Program Requirements (Design and Construction)

ANSI/ASME NQA-1, Quality Assurance Program Requirements for Nuclear Facilities

RG1.152, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants

IEEE Std 7-4.3.2, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used In Safety Systems of Nuclear Power Plants

IEEE Std 1012, IEEE Standard for Software Verification and Validation

IEEE Std 1028, IEEE Standard for Software Reviews and Audits

US NRC Regulatory Requirements for I&C systems

Cont'd

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

IEEE Std 828, IEEE Standard for Configuration Management Plans

IEEE Std 1042, IEEE Guide to Software Configuration Management

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

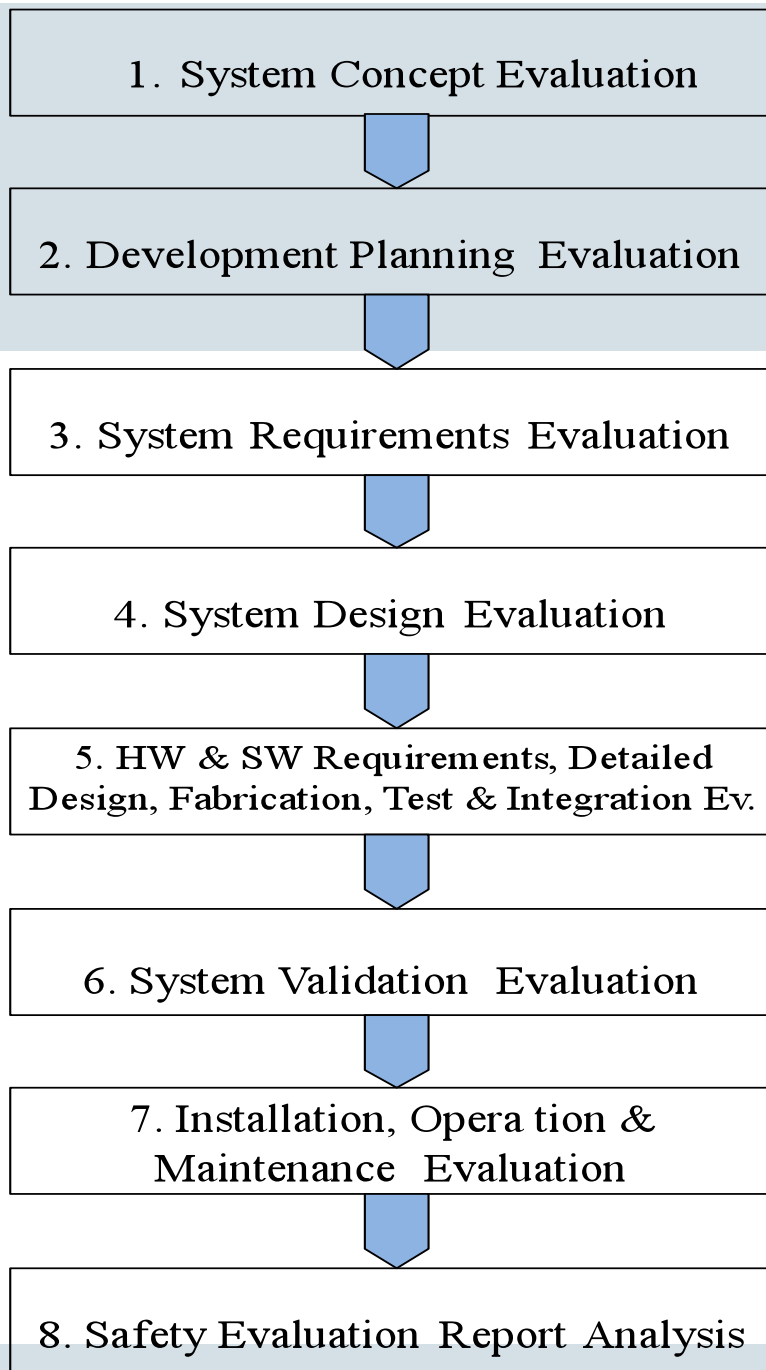
IEEE Std 829, IEEE Standard for Software Test Documentation

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

IEEE Std 1008, IEEE Standard for Software Unit Testing

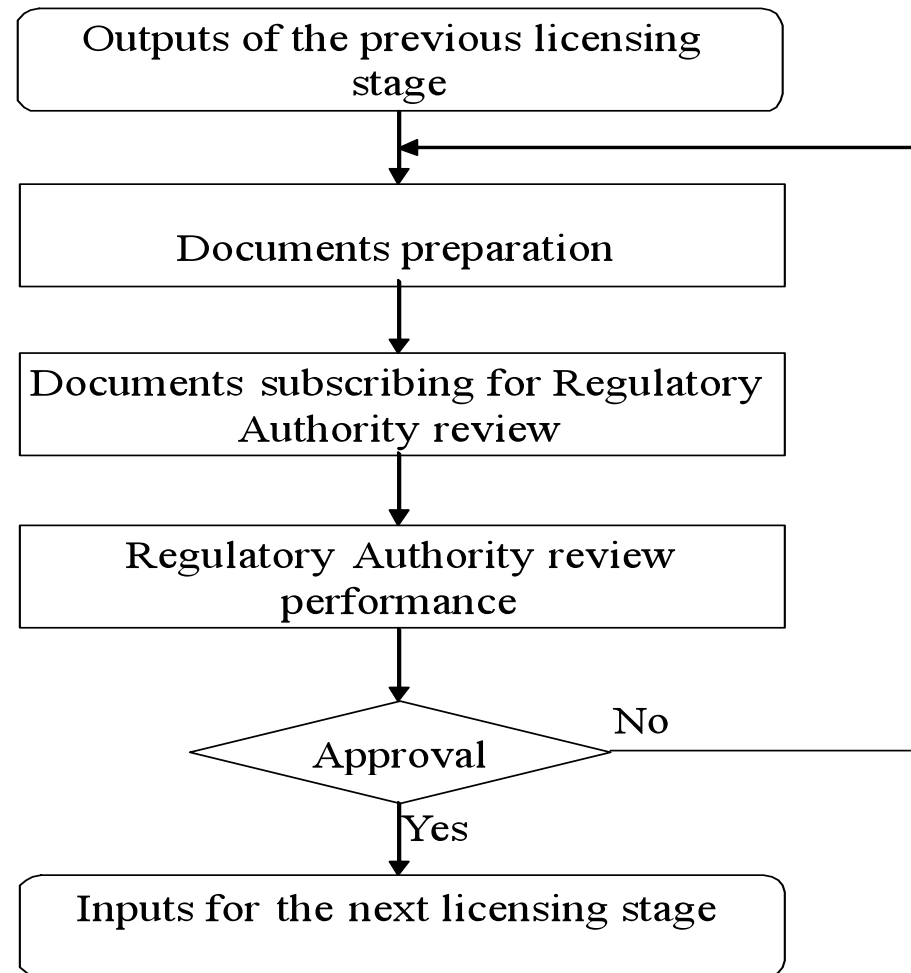
RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

IEEE Std 830-1993, IEEE Recommended Practice for Software Requirements Specifications

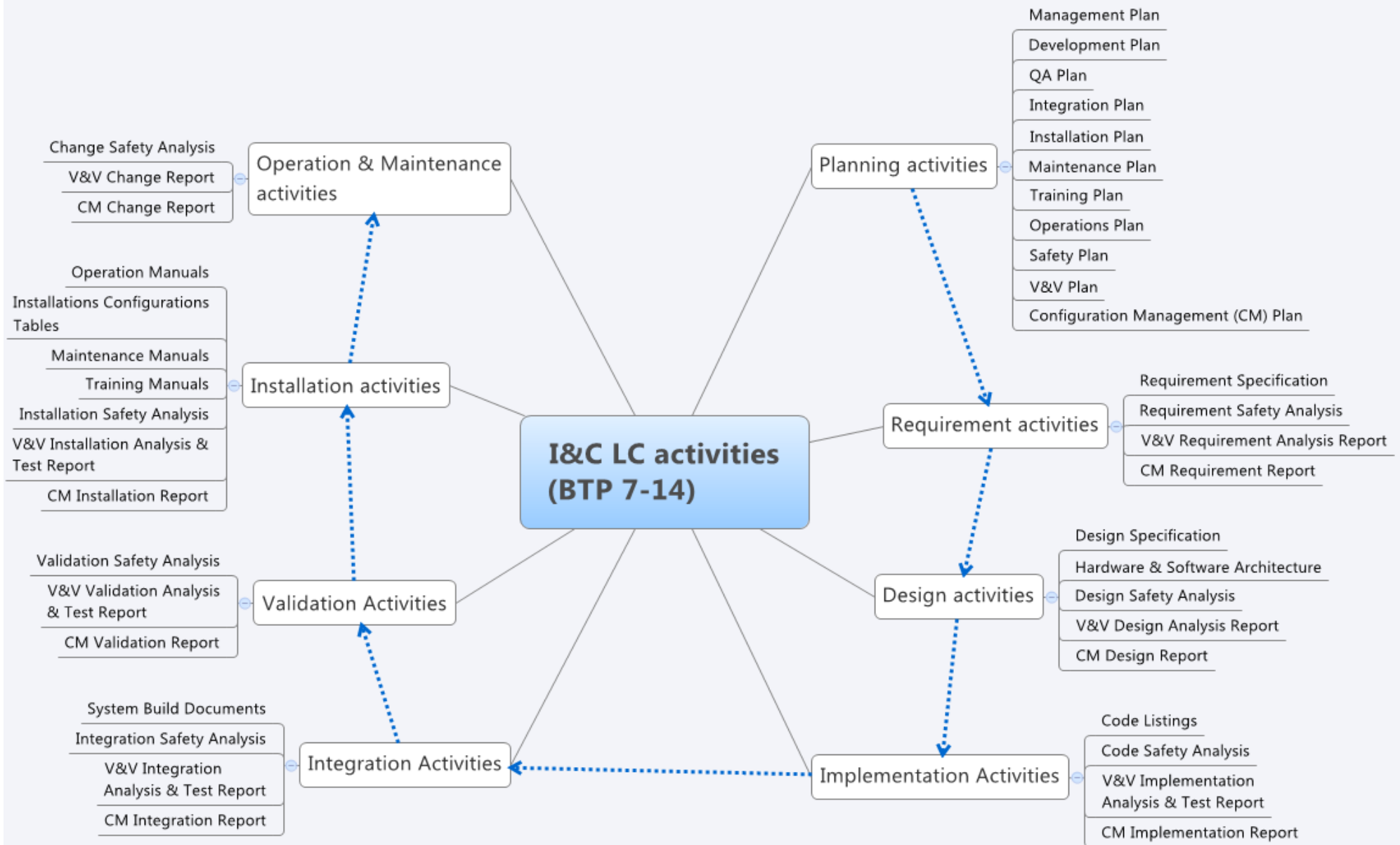


Licensing approach harmonized with US NRC (NUREG 0800)

Typical regulatory review of documents during one licensing stage



I&C systems life cycle activities (NUREG-0800)



Equipment Qualification Requirements

Radiation Exposure Withstand test

based on EPRI TR-107330 and IEEE 323 requirements

Environmental tests

based on EPRI TR-107330

Seismic and Vibration conditions tests

based on EPRI TR-107330-1996, include IEEE-344 procedures – 5 OBE-level and 1 SSE-level simulation tests, resonance search test, vibrational aging tests

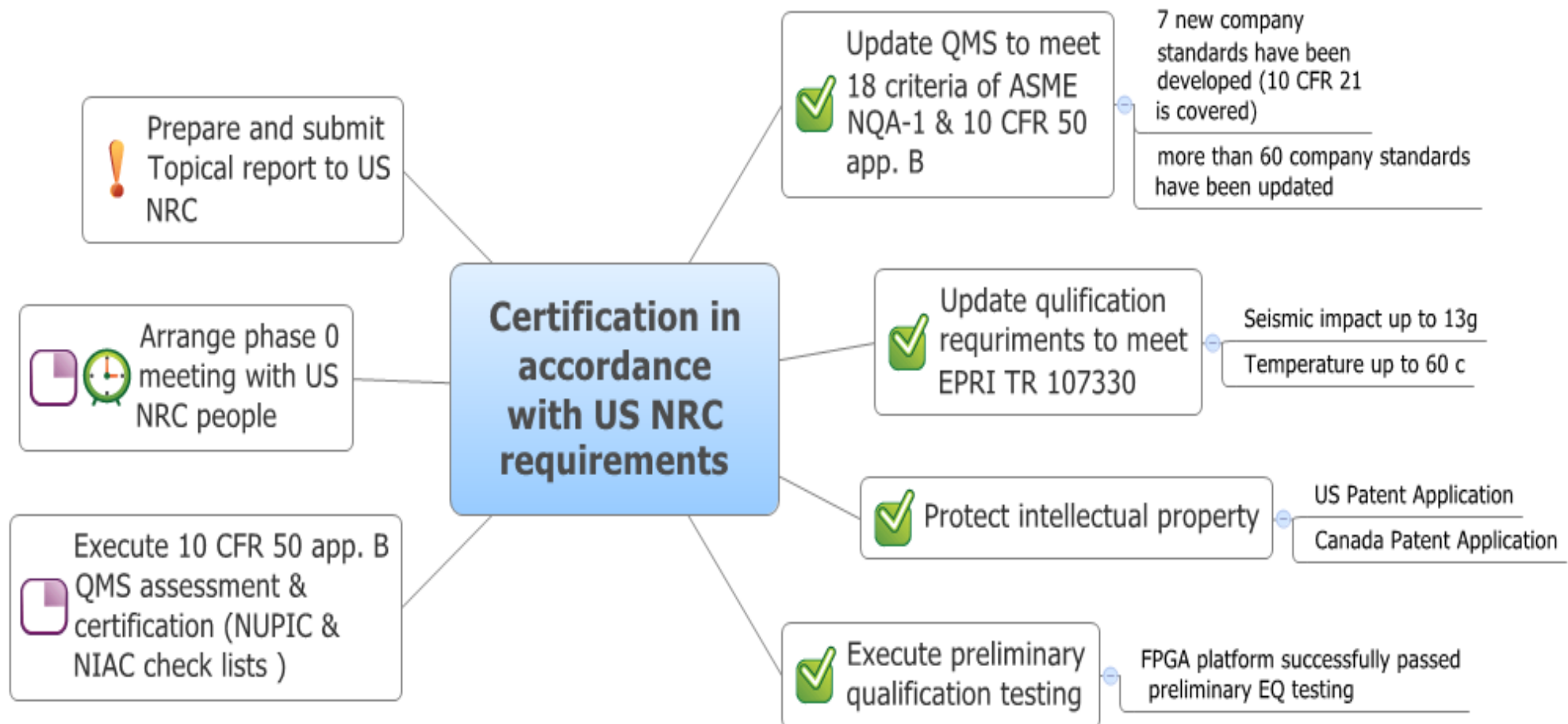
Electromagnetic Compatibility & Electric Insulation tests

based on the EPRI TR-102323 rev. 3 - using of IEC 61000-4 (Parts 1-16) and MIL-STD 461 E procedures (CE 101-102, RE 101-102) with 2 – 3 (5) test levels requirements

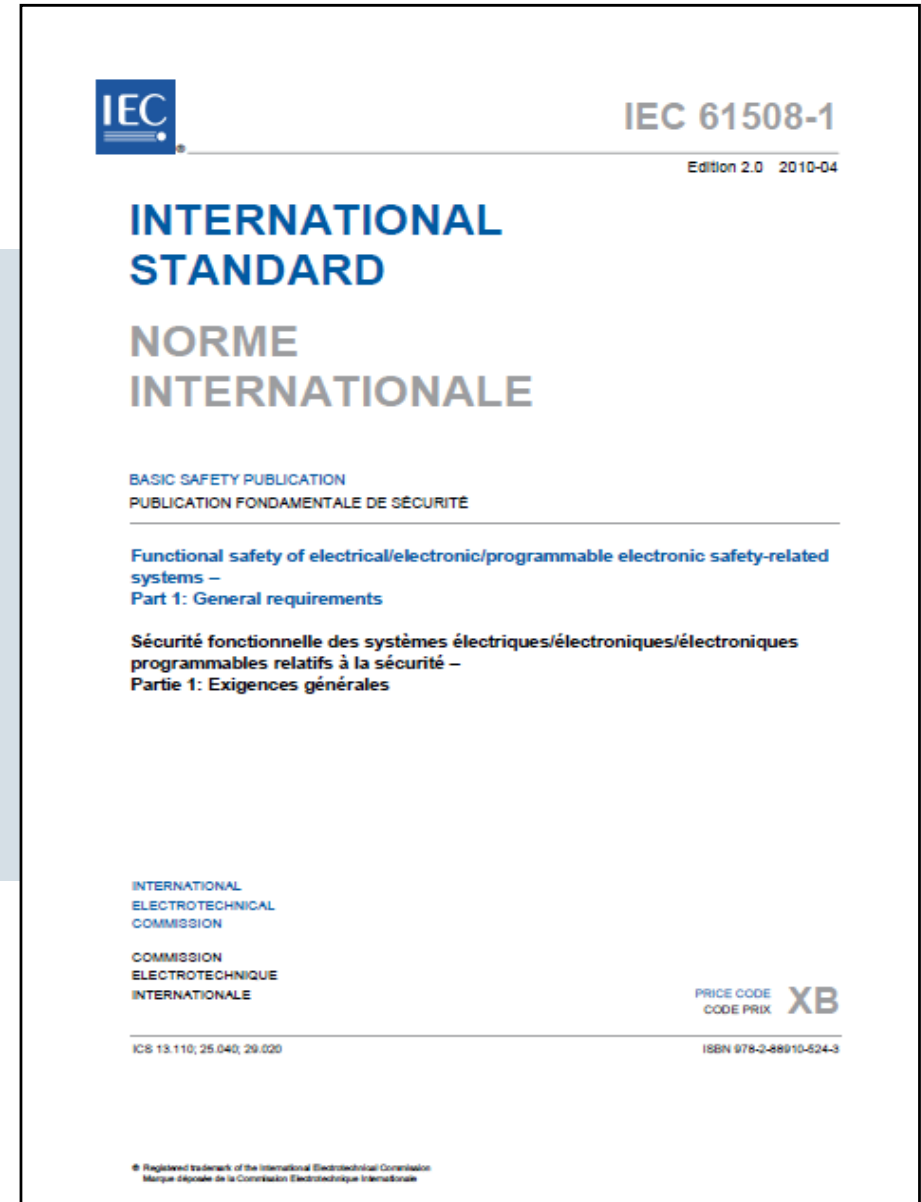
Electric Power Supply tests

based on EPRI TR-107330 and EPRI TR -102323

General approach to meet U.S. requirements



SIL (IEC 61508) approach to qualify FPGA-based safety I&C platform



Overview of international standard IEC 61508 (1)

- 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 SIL1-SIL4 conceptions for specifying the safety integrity requirements of the safety functions;
- IEC 61508 is approved by the most part of Nuclear Community;
- In some countries (for example, Canada) IEC61508 is mandatory for NPP I&C systems.



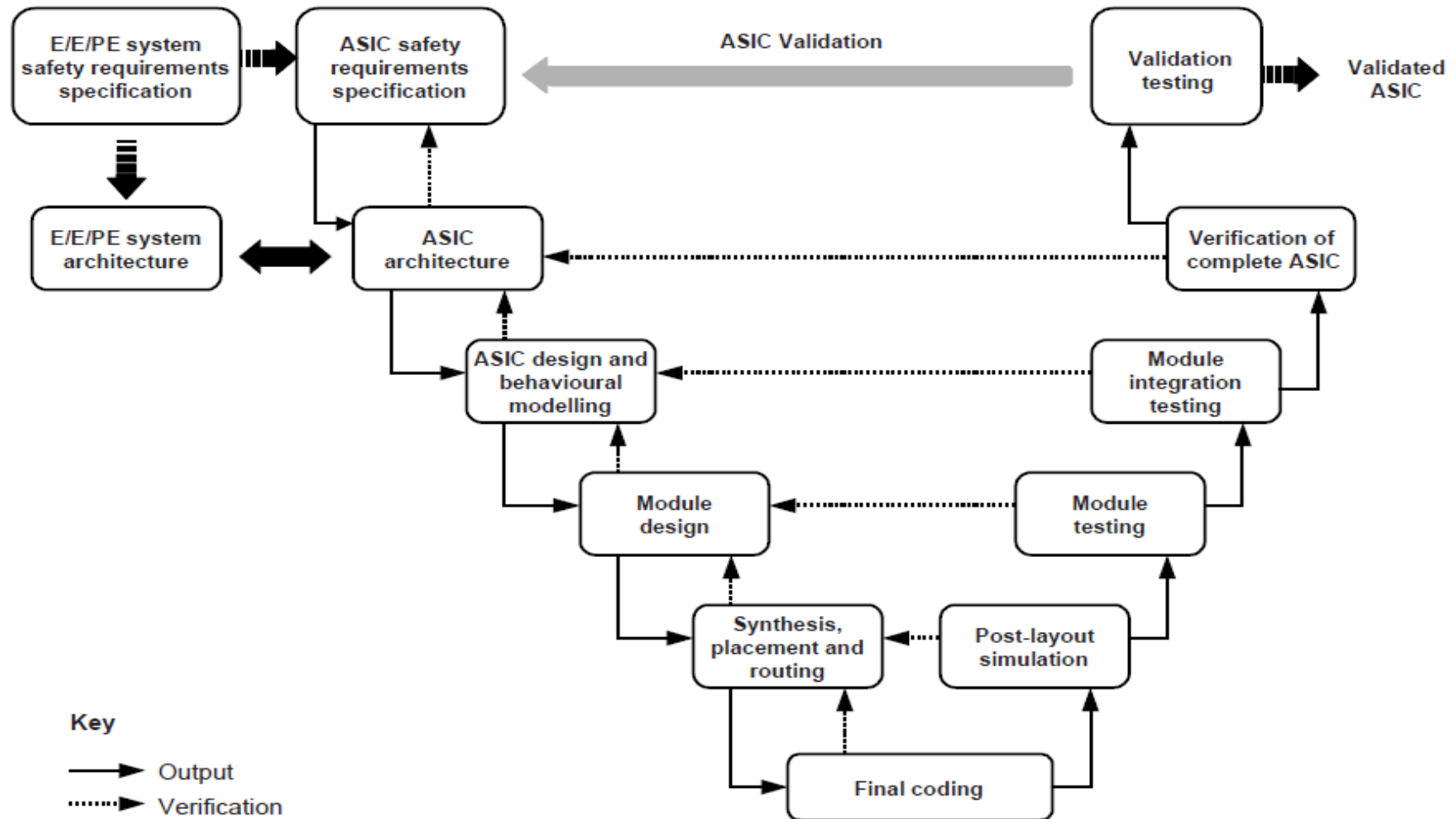
Overview of international standard IEC 61508 (3)

SIL (safety integrity level) discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

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 $< 10^{-5}$

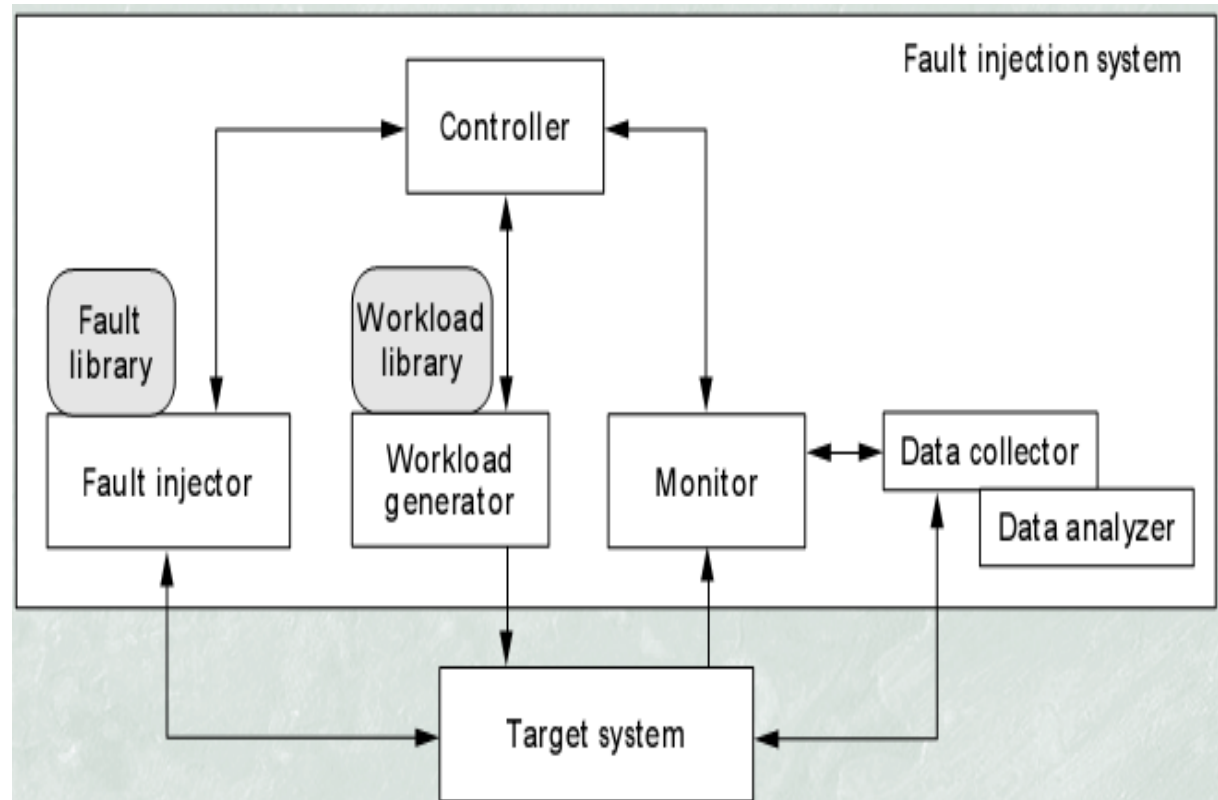
FPGA Technology for NPP I&C Systems

Design Flow & Life Cycle (IEC 61508-2)

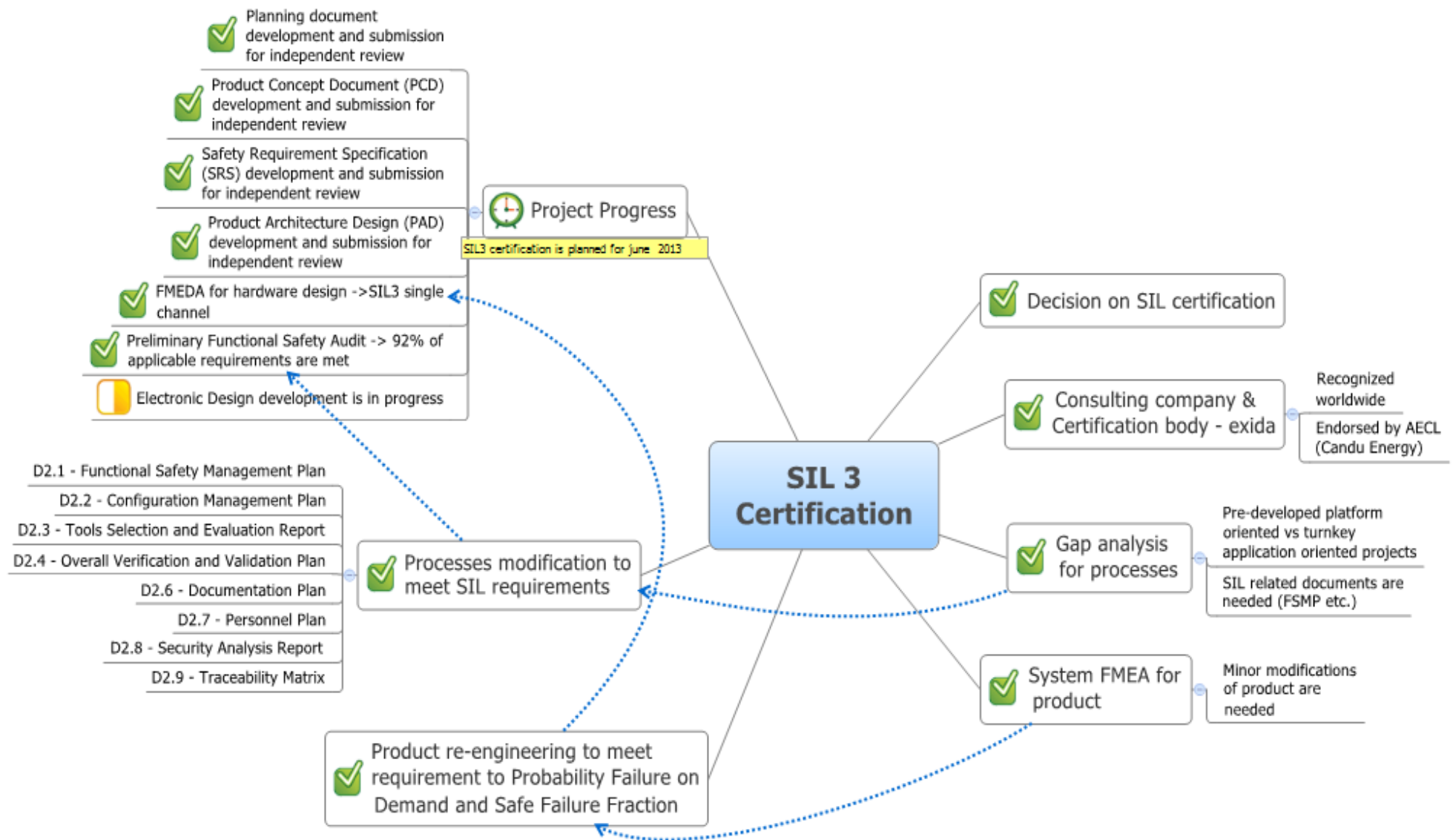


Fault Injection Testing

- To confirm FMEDA results
- To check self-diagnostics under worst case conditions
- To provide confidence in fault tolerance features of the platform



General approach to meet SIL (IEC 61508) requirements



Conclusions



Conclusion. Qualification approaches differences

Criteria	U.S. NRC	SIL (IEC 61508)
Quality Management System	10 CFR50, Ap. B	Doesn't say about QMS, ISO9001 is usually applicable
Equipment Qualification	EPRI TR 107330	Doesn't say about EQ levels, it is an applicant choice
Safety Life Cycle	NUREG 0800	IEC 61508, Part 2 (for ASIC)
Planning Activity	11 plans	6 plans (complete coincidence with U.S. NRC in 2 plans)
Reliability and Availability Analysis	FMEA, Reliability and Availability indexes	Probability (Frequency) of a Dangerous Failure, FME(D)A, Safe Failure Fraction, Diagnostic Coverage
Final document	Safety Evaluation Report by U.S. NRC	Functional Safety Assessment Report by Certification Body

Conclusions

- **Licensing** of digital I&C systems might be an **issue**
- Licensing **framework** may differ from **case to case**
- **Early dialog** established within all the parties involved may help to **make the process smoother**
- Clear **understand** of the licensing **requirements** and licensing **experience** help to overcome the problems
- Radiy has accumulated **extensive experience** in licensing of digital I&C systems and **providing this experience** to its **customers** on a regular basis



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>

