Safety Integrity Level Certification Efficacy for Nuclear Power

MP3 Public Meeting

David Hooten
Principal Investigator
EPRI Nuclear I&C Program

July 12, 2018

For more info contact: David Hooten, david.hooten@imperiaep.com
Matt Gibson, mgibson@epri.com

Texas City Refinery Explosion

Introduction/Background

- Nuclear industry is not unique regarding its potential to kill and injure people and severely damage facilities.

- How do other industries address this potential with respect to instrumentation and control (I&C) systems?
  - There exists an entire ecosystem of safety-related electrical, electronic, and programmable electronic (E/E/PE) systems.
  - These systems are certified to accepted industry standards by third parties rather than by regulatory bodies.

Introduction/Background (cont.)

- EPRI is investigating the methods, assumptions, and processes used to certify E/E/PE equipment to the Safety Integrity Levels (SILs) described in IEC 61508/61511.

- EPRI is obtaining reliability data on SIL certified programmable logic controllers and process controllers (a.k.a. “logic solvers” within SIL certification circles).

Project Objectives

- Develop an understanding of SIL certification process.
- Develop an understanding of SIL certification aging.
- Develop an understanding of SIL certifier accreditation and oversight.
- Develop statistically valid conclusions of the efficacy of SIL certifications to establish hardware and software reliability of certified equipment at the scope of the certification without additional analysis.
- Establish if SIL certifications are an accurate indicator of hardware and software reliability.

Project Objectives (cont.)

- In summary, determine the efficacy of using existing SIL Certifications (via IEC 61508/61511) as surrogates for some of the existing design and review processes.
- Engaging Certifiers and Vendors to harvest a large data set of in-situ performance of SIL certified systems for analysis.

Commoditizes Safety/Critical Systems

- **Allows Platform Selection in Design Phase and Expands Vendor Market**
- **Could Ease Regulatory Interface**
- **Data Gathering In Progress**
  - **Certifiers Engaged - 1 billion hrs. of platform reliability data so far (no CCF!)**
  - **International Members Interviewed for OE**
- **Future Expansion Envisioned to a Full Transition to SIS Methods**
- **Coordinated Development with NEI 17-06**

Governing Standard – IEC 61508 (2010)

- "Functional safety of electrical/electronic/programmable electronic safety-related systems"
  - Part 1: General requirements
  - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
  - Part 3: Software requirements
  - Part 4: Definitions and abbreviations
  - Part 5: Examples of methods for the determination of safety integrity levels
  - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
  - Part 7: Overview of techniques and measures

Governing Standard – IEC 61508 (cont.)

- The standard has thousands of requirements (i.e., sentences including “shall” or “must”).
- The requirements generally fall into one of two groups, which relate to the two fundamental concepts of IEC 61508:
  - Safety Lifecycle, a detailed engineering design process, intended to reduce or eliminate failures due to systematic errors
  - Probabilistic failure performance analysis, quantified in order of magnitude levels (i.e., SILs), intended to address random failures
- These requirements help designers create systems that work correctly or fail in a predictable manner.

Companion Standard – IEC 61511 (2016)

- "Functional safety – Safety instrumented systems for the process industry sector"
  - Part 1: Framework, definitions, system, hardware and application programming requirements
  - Part 2: Guidelines for the application of IEC 61511-1:2016
  - Part 3: Guidance for the determination of the required safety integrity levels

(Note: ISA-84.00.01-2004 is nearly equivalent to IEC 61511.)

SILs and Risk Reduction

- IEC 61508 uses a performance-based approach, and the SILs correspond to orders of magnitude of risk reduction.

SIL	Average probability of failure on demand (Low Demand mode of operation)	Probability of dangerous failure per hour (Continuous or High Demand mode of operation)
4	≥10–5 to <10–4	≥10–9 to <10–8
3	≥10–4 to <10–3	≥10–8 to <10–7
2	≥10–3 to <10–2	≥10–7 to <10–6
1	≥10–2 to <10–1	≥10–6 to <10–5

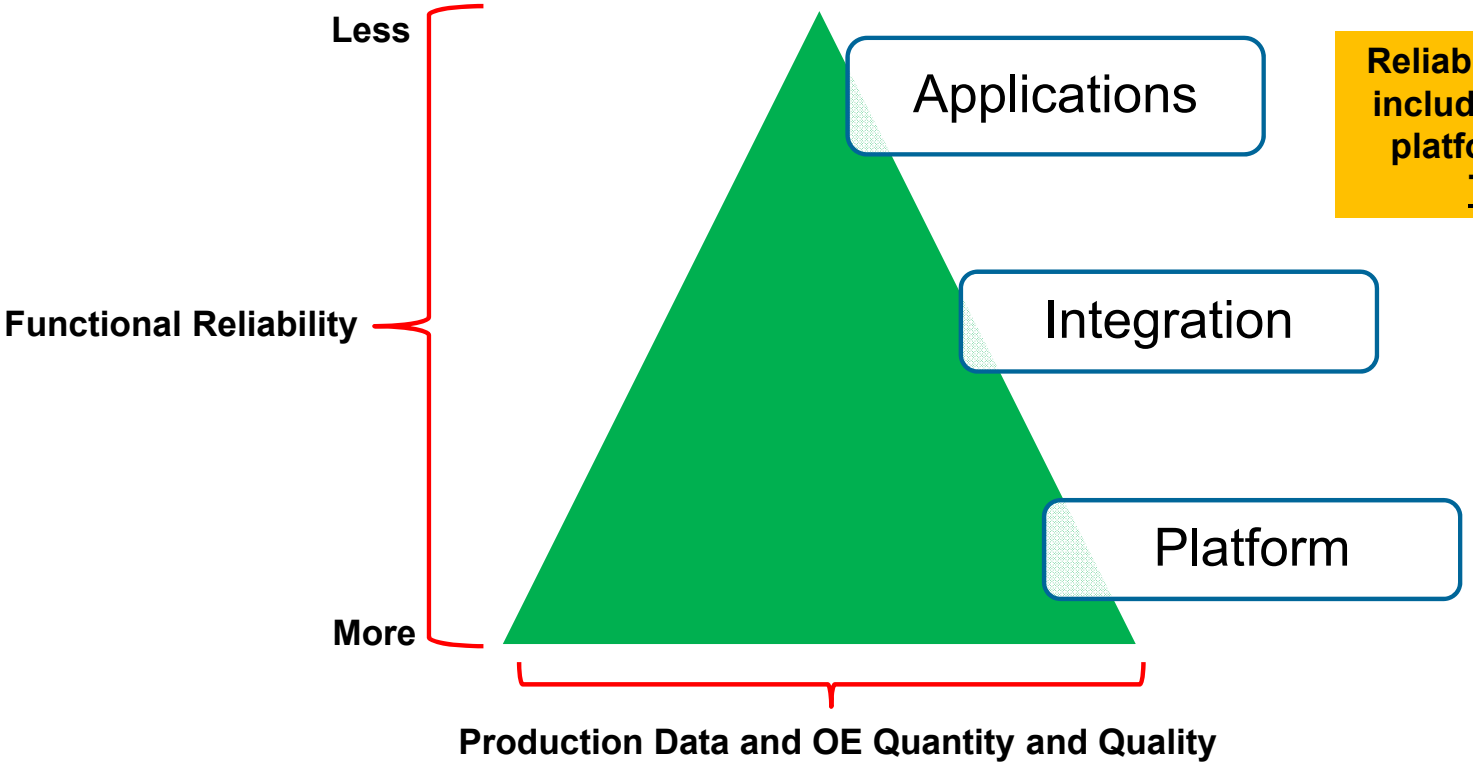
SILs and Risk Reduction

- SIL 4 involves the greatest rigor and the most requirements, but it is almost never used.
- SIL 1 involves the least rigor and the fewest requirements
- Most equipment certifications are done to SIL 3 or SIL 2.

(Note: A “Safety Instrumented Function” utilizing SIL 3 certified equipment will not necessarily achieve SIL 3.)

Platform vs. Integration vs. Application Reliability

- Emphasis on Platform issues likely misplaced.



Reliability, especially software reliability, including CCF, should be segmented by platform, integration, and application. Then Considered Separately

Third-Party Certifiers of E/E/PE Equipment

- Bureau Veritas
- exida
- TÜV NORD
- TÜV Rheinland
- TÜV SÜD

Of these, exida and TÜV Rheinland have performed the most E/E/PE equipment certifications to IEC 61508/61511 criteria. (This is especially true for logic solvers.)

Example Certifier Assessment Activities

- Assess development process through an audit and review of a detailed safety case against a certification scheme that includes the relevant IEC 61508 SIL 3 requirements.

- The safety case must:
  - show all requirements with an argument for each as to how the system/product meets it (e.g., design arguments, verification activities, test cases, etc.)
  - provide a link to the evidence documentation that supports each argument

Example Certifier Assessment Activities (cont.)

- Review and assess a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the equipment to document the hardware architecture and failure behavior.

- Review the manufacturing quality system.

Development Process – Areas Examined

- Documentation Management
- Configuration Management
- Functional Safety Management
- Safety Requirements
- Safety Validation Test Planning
- System Architecture Design
- Hardware Design
- Software Design
- Implementation
- Integration and Safety Validation Test Execution
- Modification Procedure
- Verification

Example Certifier Assessment Conclusions

- "The … development process, as tailored and implemented …, complies with the relevant safety management requirements of IEC 61508 SIL 3."

- "… is certified for use in de-energize-to-trip SIL 3 applications in low demand mode, or high demand mode, when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual (including requirements for proof testing, maintenance, hardware architecture constraints, etc.), and when using the versions specified …"

Equipment Reliability Data

EPRI is in the process of obtaining field failure data for SIL certified PLCs and process controllers.

- Equipment Manufacturers are highly sensitive to the confidentiality of their products' field failure data.
- One certifier obtains and analyzes field failure data as part of product recertification process.
- Agreement obtained to have certifier preserve OEM/product anonymity by collecting and analyzing the data and providing summary results to EPRI.
- Expect to end up with a dozen (or so) sets of field failure data.

Failure Rate Estimation Techniques

- Industry Databases (e.g., OREDA)
  - Data not available for many years on new design products
  - OREDA 2015 only had a population of 10 controllers with 2 failures
- End User Field Failure Data Studies
  - Some have high quality data collection/analysis, but many have low quality (e.g., data not collected on all failures) or none at all
  - Published data only available for field devices, not logic solvers
- Manufacturer Field Return Data Studies
  - Valuable source of data
  - Limits to usage

Is Failure Data Estimation Good Enough?

- Lots of data is available when things fail often; however, reliability has improved over the years …
- By the time enough data is gathered about a product, it may be obsolete.
- Failure rate estimation is, by itself, insufficient.

Failure Rate Prediction Techniques

- MIL-HNBK-217
  - Based on design strength analysis using a component database that predicts total failure rates
  - Parts Count method and Parts Stress method
  - Results are usually pessimistic (in 4X to 20X range)
- FMEDA
  - Uses a component database that accounts for design strength versus a predefined environment and accounts for failure modes, diagnostic coverage, and useful life
  - Can be applied to a newly designed device

Combine Failure Rate Estimation and Prediction

- Realistic results can be produced
  - FMEDA component database is calibrated/validated with field failure data from end users in a similar environment/application.
  - The results should match. If not, one or both methods are flawed.

- exida's Calibrated FMEDA™ has been refined for 15 years.

- An FMEDA standard is being developed by exida, TÜV Rheinland, and others.

Combine Failure Rate Estimation and Prediction (cont.)

- Obtain shipping records and warranty return information
  - Categorize returns (i.e., failure vs not a failure)
  - Assume equipment placed in service 6 months after shipment
  - Choose return rate assumption (based on criteria)
- Calculate point estimate of total failure rate, (%) confidence factor failure rate, and upper/lower bounds
- Compare results to FMEDA prediction
  - Typically, return data calculation is lower than FMEDA results
  - If return data calculation is higher, a more detailed audit is triggered

Certifier Accreditation

A “Certification Body” (i.e., certifier) is accredited by a national “Accreditation Body” (i.e., accreditor).

- In the United States, the American National Standards Institute (ANSI) is the national Accreditation Body.
- In the Federal Republic of Germany, the Deutsche Akkreditierungsstelle (DAkkS) is the national Accreditation Body.
- Accreditation is awarded when a company passes a detailed multi-day audit where all requirements of ISO/IEC 17065, “Conformity Assessment – Requirements for Bodies Certifying Products, Processes, and Services”, are successfully met.

Preliminary Research Learnings

- Manufacturing process issues are more frequent contributors to systematic failures than are software errors.

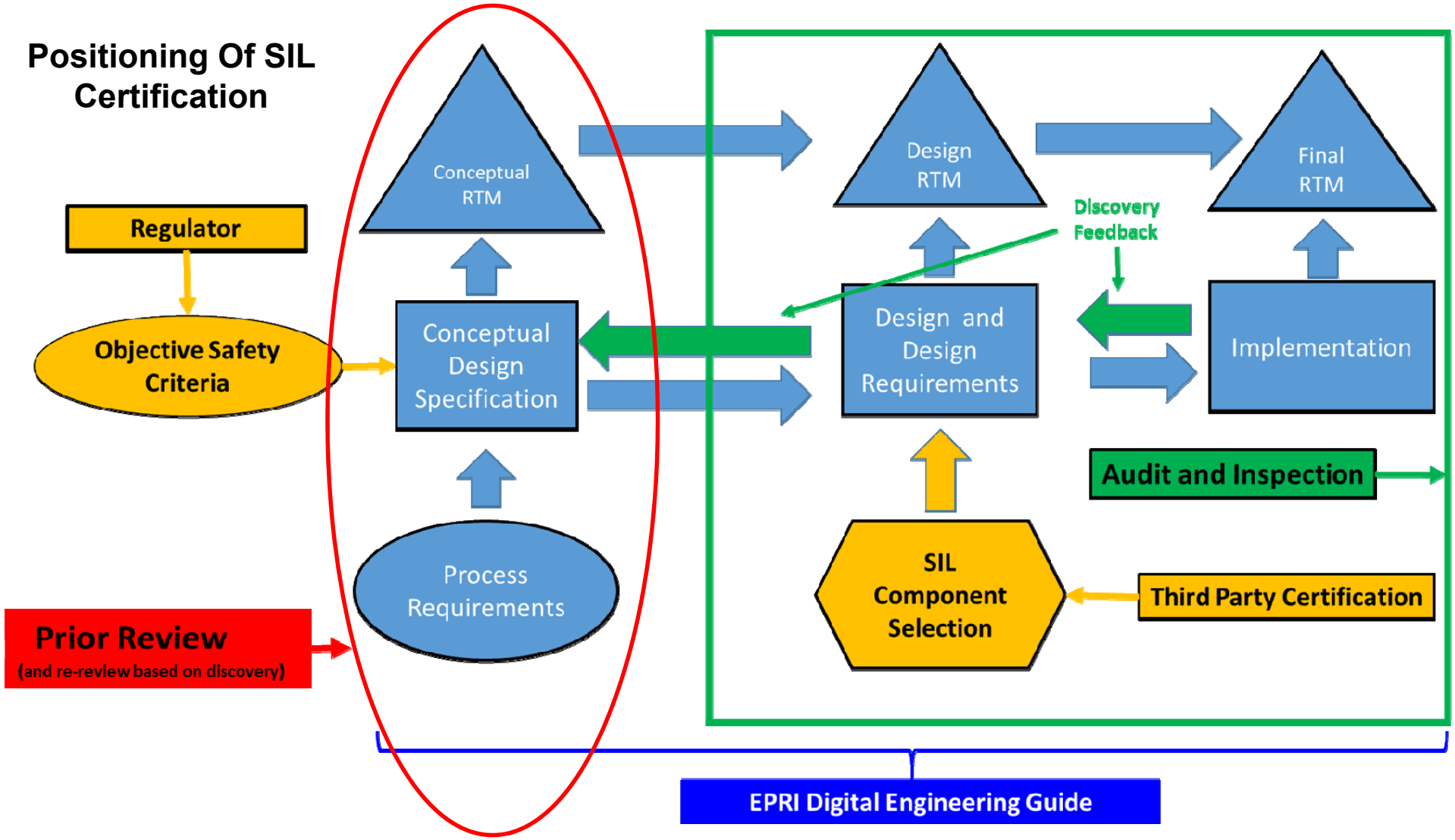
- Differences between SIL certified and non-SIL certified equipment performance is driven by differences in systematic errors and diagnostic coverage, not by differences in random hardware failures.

- SIL certification is valid only for the duration of the product's useful life (published in the safety manual).

Preliminary Research Learnings (cont.)

- SIL certified equipment is widely used for safety-related applications in oil & gas and chemical process plants.
- SIL 3 certification process is rigorous enough that equipment often does not achieve SIL 3 certification without needing a design change (e.g., related to diagnostic coverage).
- Some certifiers are more transparent than others regarding their processes and documentation.

Positioning Of SIL Certification



Together…Shaping the Future of Electricity