Certificazione di un sistema HIPPS

18 Febbraio 2016

G. Picciolo

Associazione Italiana Strumentisti

ISA Italy Section

Move Forward with Confidence

BUREAU VERITAS

Agenda

- Scope of the Certification as a Third Party (Notified Body)
- Conformity assessment criteria and techniques
  - Data & Information
  - The Safety Plan
  - Verification
  - Validation & Test

Scope of the Certification by a Third Body (the Third Party - Certifier)

- VERIFY AND VALIDATE, BY DOCUMENTED EVIDENCE, THE HIPPS CONFORMS WITH IEC 61511 & IEC 61508 MANDATORY REQUIREMENTS
- The System Integrator will ensure that all end-to-end IEC 61511 /IEC 61508 requirements for the HIPPS SIL elements are fulfilled to demonstrate a SIL3 delivery into the Safety Analysis Report, covering the life full lifecycle process.

Data & Information

- Data & Information shall be available at the onset of the “Certification” “ process, before the Contract:
  - A Functional Safety Management organization (skilness, tools, etc) in place by the Integrator
  - Independent functional safety review Department
  - In case of lack, Certifier might provide the intended support for achieving functional safety (**NO design**!)

The Functional Safety Management Plan (FSMP)

- The FSMP describes how the Functional Safety for the HIPPS System will be performed, ensuring the expedition, follow-up and resolution of functional safety related activities. The plan is subject to change as the project progresses; all changes will be updated in the SIL planning in due course. The FSMP integrates activities and documentation into an overall Management Plan for the HIPPS, including the following core activities:
- Demonstration of SIL compliance using FMEDA (mandatory)
- Demonstration of SIL compliance against PFD target for HIPPS system elements
- Quantitative Analysis to ensure that architectural constraints are satisfied
- Qualitative Analysis for the control and avoidance of systematic failures
- Verification and Validation reporting
- External Safety Auditing: Functional Safety Assessment

The Functional Safety Management Plan (FSMP)

- The FSMP will provide relevant steps for Certifier's verification and review; namely:
  - SRS content and completeness (typically related to demand rate, valves tight shutoff leakage rate)
  - Safety related equipment documentation (SIL certificates, FMEDA reports, etc.) and datasheets (valves pipe connection: flanged, welded, testing devices, etc.)
  - End User's Operation and Maintenance constraints (diagnostics, proof test interval and procedures)
  - Reliability block diagram and PFDavg preliminary calculations
  - Hardware Fault Tolerance (HFT) Verification
  - Systematic capability (SC) verification
  - Safety Manual

The Safety Requirements (SRS)

►The SRS shall been produced using the FEED Safety Requirements Specification and following the risk analysis outcomes that allocated a High Integrity Pressure Protection System (HIPPS) Safety Instrumented System (SIS) as a protective layer for the Process Control System.

►The SRS is the reference document for use throughout the Safety Lifecycle controlling the design, verification and validation of the HIPPS during build and commission, and HIPPS performance monitoring during the operating lifetime, and final de-commissioning.

►The document will be kept current and updated throughout the design and build process of the system, as the precise performance and detail of the SRS cannot be fully defined in the early phases of project execution; significant engineering change will be controlled by a management of change process.

Safety Equipment

- A statement that the item is to be used in a Safety Instrumented System including:
  - A Safety Manual has to be part of the purchase order agreement
  - A list of mandatory safety documents
  - The SIL requirement to be achieved
  - A clear statement that the item of equipment is to be formally SIL certified or a fully documented proven in use or prior use record, based on similar equipment in a similar operating environment to satisfy IEC 61508/ 61511 requirements

The Functional Safety Assessment

- Functional safety assessment in the context of IEC 61508 and IEC 61511 implies performing independent reviews and audits at predefined stages of the safety lifecycle (“independent 3rd party verifications”).
- The safety analysis will confirm that the system is designed and built to satisfy the requirement of the HIPPS SIL3 SRS quantitative target, response time and the qualitative requirements; in accordance with IEC 61511, documenting:
  - Confirmation that the HIPPS meets the SIL3 PFD threshold and specified PFD target
  - Compliance with hardware safety integrity constraints achieved by implementing the Hardware Fault Tolerance and Safe Failure Fraction (route 2H) assessment versus the safety equipment employed
  - Effectiveness of the measures and techniques for the Control and Avoidance of Systematic Failures against SIL 3 level

The SAR (Safety Analysis Report)

- The Safety Analysis Report (SAR) shall be prepared from technical safety information supplied by Contractor's Suppliers (End User)
- The SAR is generated using component level analysis documenting how the equipment satisfies the SIL requirements, and how the equipment / components fulfil its assigned SIL for the SIS. The SAR also provide failure data for the SIL calculations (PFD calculations and documentation of the architectural constraints) within the sub-system architecture.
- The HIPPS Safety Analysis Report is delivered at a system level to demonstrate that the entire HIPPS has complied with the four SIL requirements:
  - Assessment of the probability that a safety instrumented function failing to respond to a potentially dangerous condition meets the required SIL level;
  - Compliance with hardware safety integrity constraints achieved by verifying the Hardware Fault Tolerance and Safe Failure Fraction criteria (route 2H);
  - Control and Avoidance of Systematic Failures.
  - *Control and Avoidance of Systematic Failures* throughout the design, build and testing phases.

Typical SAR Content

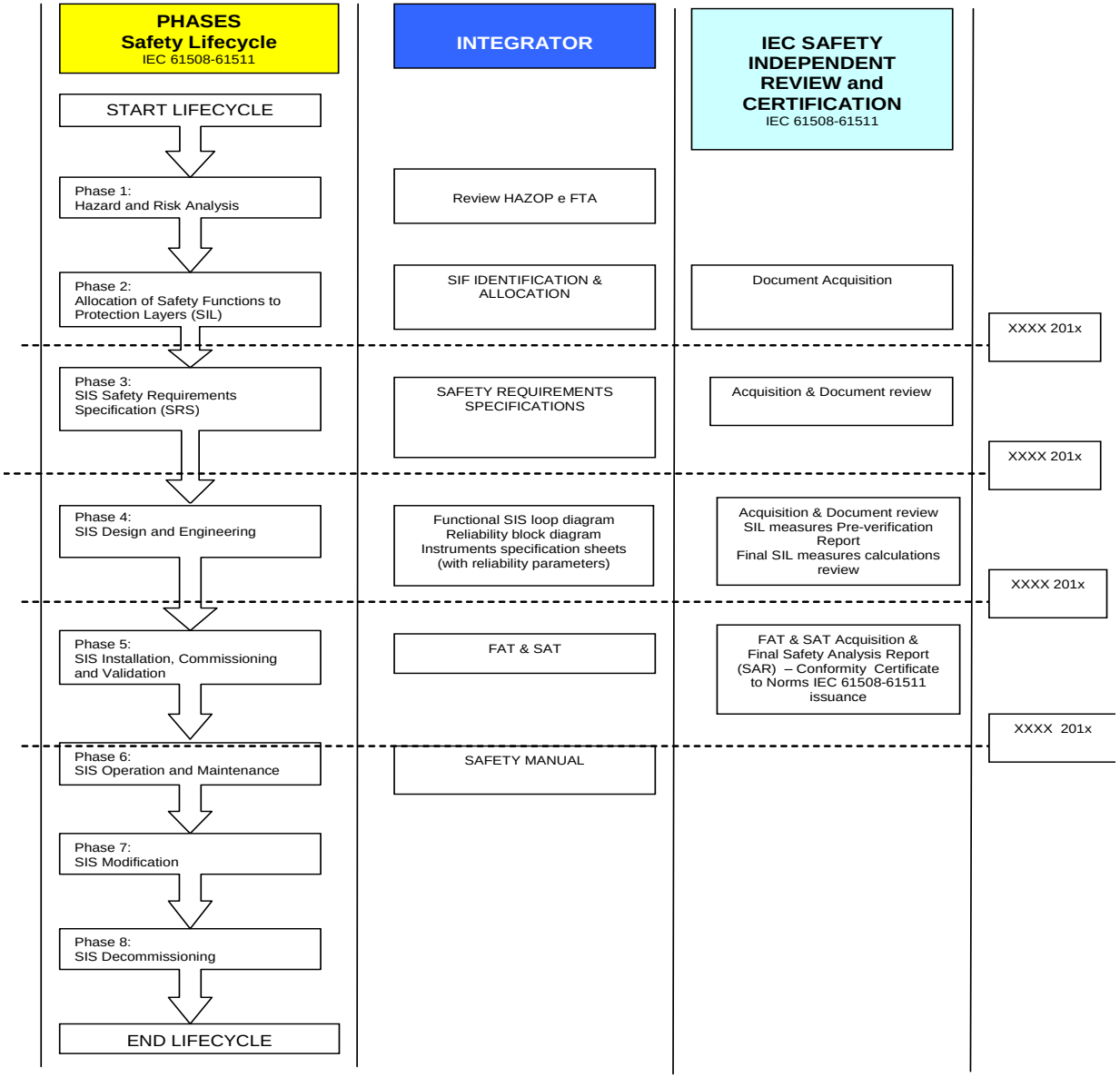
I Abbreviations
II References
III Summary

1. Introduction
2. System Description
3. System Topology and Block Diagram
4. Operational description of the system (including modes of operation)
5. Assumptions
6. Failure rate of the components
7. Common Cause failures (CCF)
8. Diagnostic Coverage & Safe Failure Fraction
9. Behaviour of system/components on detection of a fault
10. Factory testing
11. Proof testing
12. Architectural Constraints
13. Avoidance and Control of Systematic Failures
14. Effective time to repair
15. Software documentation
16. Results

Appendices

Safety Instrumented System Certification Process

SAFETY INSTRUMENTED SYSTEM CERTIFICATION - PROCESS



BUREAU
VERITAS

Move Forward with Confidence