MANGAN INC.
SAFETY INSTRUMENTED SYSTEMS

DESIGN CONSIDERATIONS

SAFETY INSTRUMENTED FUNCTION (SIF)

SAFETY REQUIREMENTS SPECIFICATION (SRS)

SAFETY INSTRUMENTED SYSTEM (SIS)

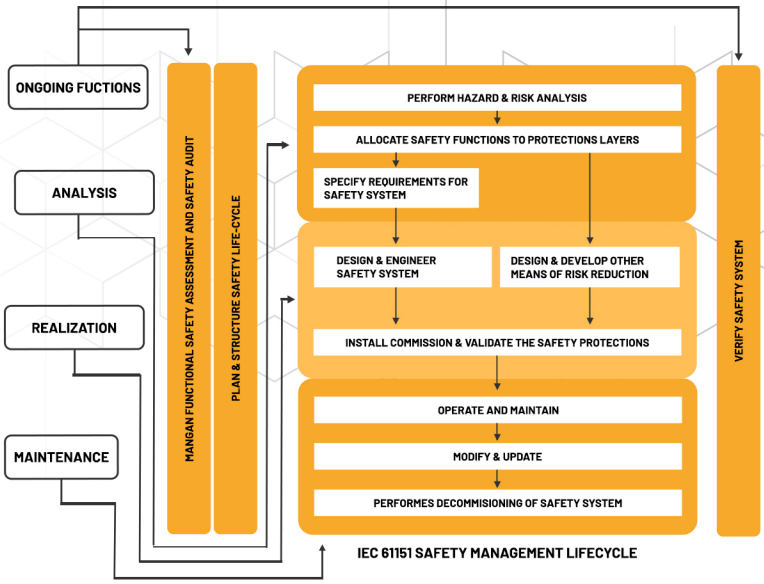
HTTPS://MANGANSIS.COM/

MANGAN INC.
SAFETY INSTRUMENTED SYSTEMS

FUNCTIONAL SAFETY LIFECYCLE OVERVIEW

Functional safety engineering is a vital aspect of process control safety systems design. It ensures the safety of both personnel, assets and the environment in industries that utilize and/or involve hazardous materials. Mangan Functional Safety Engineering has decades of experience in assisting our clients develop and maintain a Functional Safety program that incorporates Operational and Maintenance criteria in the associated design of mitigation systems.

One of the primary components of functional safety engineering is compliance with the International Electrotechnical Commission (IEC) 61511 ed.2 and ISA 84.00.01 standard. This standard lays out the requirements for the implementation, operation, and design of Safety Instrumented Systems (SIS) for the process industry. Mangan Functional Safety Engineering has significant experience assisting our clients comply with IEC 61511 Performance based or Prescriptive standards.



ANALYSIS

The first stage of the Safety Lifecycle program involves a Hazard and Risk Assessment to evaluate the different kinds of risk, causes, and consequences present in a plant's processing environment. A Process Hazard Analysis (PHA) and Layers of Protection Analysis (LOPA) process is conducted to identify and quantify the unmitigated identified risk, allocate credit for existing protection layers and determine a target Safety Integrity Level (SIL) required to achieve the organization's corporate defined tolerable risk. This process is know as a SIL determination/study/assessment where Safety Instrument Functions (SIF) will be allocated to mitigate any remaining risk as corresponding with the SIL level, Risk Reduction Factor (RRF), and Mean Time to Fail Spuriously (MTTFS) defined for each SIF in this phase.

The Conceptual/Process Safety Requirement Specification (SRS) is then developed as defined by IEC 61511 ed.2 and ISA 84.00.01 requiring that a SRS be prepared for each SIS with the requirements specified in Clause 10. The SRS documents the Functional and Safety Integrity requirements for each SIS and SIF (including sensor, logic solver, final element, and sources of power) required to adequately identify the presence of a hazard and return the process to a safe state according to the defined acceptable risk guidelines.

The Stage 1 Functional Safety Assessment (FSA-1) is then carried out before starting the SRS Design phase to identify systematic deficiencies before they develop into potential hazards and ensure appropriate assignment of safety mitigation measures.

DESIGN & IMPLEMENTATION

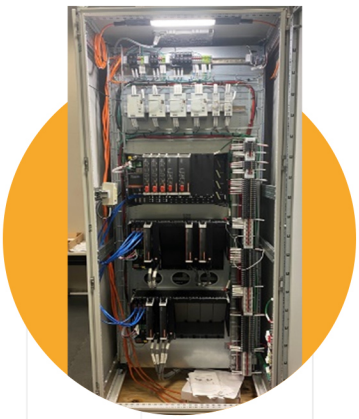
The Design phase of the Safety Lifecycle includes the technology selection (sensors, logic solvers, valves and actuators) certified for the required SIL, and architecture definition (independence, redundancy, and diversity). Each element selected is certified for the required SIL or justified through "proven in use" data.

The design will have to demonstrate its capability in accordance with IEC 61508 and IEC 61511 through a SIL Verification ensuring each SIF complies with the SIL, RRF, MTTFS requirements as defined in the Conceptual SRS. This includes considerations of random hardware failures/Dangerous failure (Probability of Failure on Demand (PFD)), Hardware Safety Integrity (Safe Failure Fraction (SFF), Hardware Fault Tolerance (HFT)), Systematic Capability (SC), and Common Cause Failure (CCF).

The SIL Verification is carried out using various methods (Reliability Block Diagram (RBD), Fault Tree Analysis (FTA), Failure Mode and Effect Analysis (FMEA)) and commercially available software packages.

Once the SIFs are verified against their SILs and acceptable Proof Test Procedure (PTP) frequencies the Design SRS can be finalized.

The SIS can then be procured, integrated, and configured for each of the SIFs according to the Design SRS. The system is then Validated per IEC 61511 clause 15 through a combination of the Factory Acceptance Test (FAT) and Site Acceptance Test (SAT) and a Stage 2 and 3 FSA-2, FSA-3 are conducted after the FAT and SAT accordingly.



OPERATION AND MAINTENANCE

The Operation and Maintenance phase of the Safety Lifecyle is to ensure that the integrity of all SIFs are maintained. This involves conducting Proof Test Procedures (PTP) at defined intervals and monitoring the performance of all SIFs. A strategy to improve this testing process involves optimizing the offline vs. online testing as much as possible and streamlining the PTP based on trips. Performance of the SIFs in terms of demand rate or any parameter used in calculating the Probability of Failure on Demand are monitored and recorded. Any change in the SIF that degrades its performance below the assigned SIL must be addressed.

Modifications to SIFs are per guidelines laid out in IEC 61511 Clause 17.

Stage 4 FSA-4 are conducted at defined intervals in the Safety Lifecycle to review Operate and Maintain (O&M) procedures, training, PTP practice and the collection and assessment of SIS performance data. Stage 5 FSA-5 are conducted when modifications to a SIS and prior to decommissioning of a SIS.

SRS DEVELOPMENT

Safety Requirements Specification (SRS) plays an essential role in functional safety engineering. It sets the foundation for the design, implementation, and operation of Safety Instrumented Functions (SIF) and Safety Instrumented Systems (SIS). The guidelines for the SRS are set in IEC 61511/ISA 84 Clause 10 and focus on five areas of requirements listing 29 elements.

01 Hazard Prevention – the hazard each SIF prevents and the function the SIF performs

02 Operation Modes – who and when SIFs are put into service and are required to be available, bypass requirements

03 SIF Performance – Probability of Failure on Demand (PFD) and Spurious Trip Rate (STR)

04 Functional Requirements – SIF and SIS

05 Design Requirements – SIF and SIS

06 Operation and Maintenance

The SRS in simple terms is a document that provides a mechanism to ensure that safety systems can achieve the set performance goals and mitigate potential risks to a safe state. An SRS should be used as an input and to guide detailed design and subsequently verify the design meets the requirements. A project that does not complete the SRS prior to detailed design is not following a good RAGAGEP and will likely experience high project cost during the design phase.

THE STEP-BY-STEP PROCESS OF SRS DEVELOPMENT

The methodology for developing an SRS involves starting with the Process Hazard Analysis (PHA) and Layer of Protection Analysis (LOPA) to document the risk and conceptual mitigation requirements into a Conceptual SRS. The SRS is updated once detailed design and SIL Verification is complete to incorporate any changes or validate initial requirements.

01 **Conceptual System SRS:** The process starts by identifying the risk that need to be mitigated through a PHA/HAZOP process. Safety Integrity Levels (SIL) are then determined to adequately mitigate the risk to an acceptable level. Safety instrumented functions (SIFs) are then allocated as protection layers that either achieve the SIL or as specified in Prescriptive Owner Requirements Specifications.

The Hardware/ Architecture & Software SIS requirements, general and specific SIF requirements are then documented in the SRS including parameters such as the following:

- Purpose and Scope
- General Project Information and Standards used
- Independent protection layer risk reduction allocations.
- Define risk reduction assumptions
- Safety Integrity level of each SIF
- SIF Architecture
- Redundancy or voting logic
- Sensor & transmitter accuracy
- Bypass procedure
- Safe state of the process
- Process inputs and trip points
- Process outputs and actions
- Functional relationships, failure modes
- Manual shutdown and reset requirements
- Maintenance/bypassing requirements
- Response time requirements
- Human machine interface requirements; and
- Cybersecurity

02 **Design SRS:** A SIL Verification process is conducted for the final SIFs Design that is based on the conceptual SRS and includes associated functional and operational (ex: proof test procedure interval) parameters. If the Target Safety Integrity level is not achieved then proof test intervals , input-output relationships and redundancy options might have to be adjusted. These changes are updated in the Design SRS.

03 **Risk Analysis:** A thorough risk assessment is done for each SIF to ascertain its SIL. Important factors considered include the potential process hazards, the likelihood of these hazards occurring, and the effectiveness of current protection layers.

04 **Documentation:** Keeping track of every decision, assumption, and rationale during the SRS development is essential. This thorough documentation aids in transparent communication, and it becomes invaluable during any future system reviews or audits.

BENEFITS OF AN EFFECTIVE SRS DEVELOPMENT

- **Enhanced System Reliability:** A well-detailed SRS ensures the development of robust safety systems capable of effectively mitigating process risks.
- **Compliance with Standards**: A good SRS aligns with global safety standards, ensuring operations are both safe and compliant.
- **Operational Efficiency:** An SRS serves as the foundation for efficient system design, significantly reducing the chances of system failures and operational downtimes.

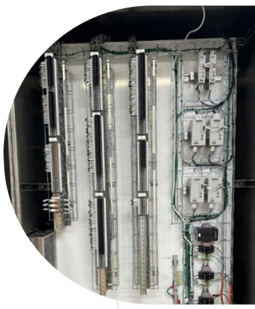
Developing a comprehensive SRS is critical in the realm of functional safety engineering. A well-prepared SRS not only safeguards assets and operations but also serves as a guidepost for system designers, operators and implementation of the SIS.

SIS IMPLEMENTATION

Through our integration facilities in Houston, TX and Gonzales, LA; Mangan can build/integrated and configure the SIS panels as defined in the SRS. This includes a full set of complement Safety, Control and Design engineering services to compete required engineering deliverables.

- SIS Instrument Index
- C&E Development
- Start-up/Reset Sequence Development
- SIF Data Sheets
- SIL Verification
- SRS IFD
- SIS Hardware layout design
  - SIS, Marshalling, Panel layout & BOM
  - SIS, Marshalling and Panel wiring
  - Heat load / power calculations

- Systems Engineering
  - DCS mapping
  - HMI Configuration
  - SIS Configuration



- Procedure Development
  - On-line / Off-line maintenance procedures
  - Logic FAT/SAT procedures
  - Hardware FAT/SAT procedures
  - Proof Test Procedure (PTP)
- Systems Integration
  - SIS, Marshalling, Power Supply Enclosures
  - Unit Local Control Panels
- Acceptance Testing
  - SIS Factory Acceptance Test (FAT)
  - SIS/DCS Integrated Factory Acceptance Test (iFAT)
  - Site Acceptance Testing (SAT)