Safety Requirements Specifications

Safety Lifecycle Manager

Conformance to IEC61511

MANGAN Software Solutions

Safety Requirements Specifications

SLM Overview

SLM® Safety Lifecycle Manager

www.Mangansoftware.com

Table of Contents

Table of Contents

1 Introduction

IEC 61511-1 2016, Clause 10, requires that a Safety Requirements Specification (SRS) be prepared for all Safety Instrumented Systems. The Clause presents a number of items that shall be covered by the SRS but provides little or no guidance on how an SRS should be developed, organized or maintained. The end results are that Operating Companies, SIS Consultants and Engineering Companies have produced a variety of SRS's that vary widely in format, content and quality. In practice, these SRS's have become extremely expensive to produce and maintain, and really don't meet the intended functionality and value.

This White Paper will review the purpose and usage of an SRS, some of the issues that have been observed in SRS's produced by various organizations, provide some practical suggestions for SRS preparation, and discuss the advantages of a Data-Driven SRS. This paper also is the first part of multiple white papers that will provide a user with a reference on the details and best practices for development of Safety Requirements Specifications and management of SIS's, SIF's and Input and Output using SLM.

2 Reference Papers

As mentioned above, this paper is the first in a series of White Papers that describe how to use SLM to develop and manage, SRS's, SIS's, SIF's and related data. These papers are:

1. SRS's with SLM – Overview (This paper)
2. The SLM SIS Object
3. The SLM SIF Object
4. SLM Input and Outputs – Voting Groups and Assets
5. Minimizing SRS Development Time with Cloning and Linking
6. SLM SIL PFD Calculations
7. An Overview of SRS Data and the Operate-Maintain Module

3 SRS Requirements

3.1 IEC 61511 and ISA 84.00.01

The first edition of IEC 61511-1 2004 and ISA 84.00.01-2004 Part 1 Clause 10, contained the basic requirements for an SRS. An update to IEC 61511 was issued in 2016, with an amended version issued in 2017 to fix some errors in the original release. ISA has adopted the standard and issued it as ANSI/ISA 61511-1-2018 and has withdrawn ISA 84.00.01-2004 Part 1.

3.2 Whats Missing

The requirements for an SRS are a result of findings by various studies, including a British Health and Safety Executive study, of major incidents in the processing industries. The BHE study found that 44% of the incidents were attributable to incorrect and incomplete specification of the Safety Functions. The SRS requirements in IEC 61511 and ISA 84.00.01-2004 were developed to address this fundamental gap by defining the minimum requirements for specification of functional and basic design requirements that are to be included in an SRS that is prepared prior to detailed design, installation and operation. Table 2 of IEC 61511-1 2016 shows that the SRS is to be prepared prior to Design and Engineering of the SIS.

In the new version of IEC 61511-1 the SRS basic requirements in Clause 10 have been expanded upon to further clarify what information is intended to be presented and to tighten some requirements by changing previous usage of “should” to “shall”. The SRS requirements are being enhanced by the addition of more detailed requirements for proof testing and expanding the requirements for application programming. These are summarized in Figure 1.

IEC 61511-1 is a performance standard that is focused on assuring that SIS’s and their SIF’s are designed to meet a required Availability requirement. Availability is the measure of whether a SIF will perform its intended function. However, the Standards do not address the other side of the coin – what is the Reliability of the SIS and its SIF’s? Reliability is a measure of the ability of a design to not cause false trips due to failures or mis-operation and to be maintainable and consistent with local practices.

As far as IEC 61511 is concerned, Reliability concerns are not part of their scope. It is the responsibility of the User to provide that information. It’s considerably simpler to develop an SRS without addressing the Reliability aspect of the SIS and SIF designs. The result can be an SRS that specifies an SIS that is highly available, but which has an entirely unacceptable Reliability, or which is extremely hard to maintain. Section 5 of this paper discusses the additional things that should go into an SRS beyond the minimum IEC 61511 requirements.

Figure 1: IEC 61511-1 2016 SRS Required Items

- a description of all the safety instrumented functions necessary to achieve the required functional safety
- a list of the plant input and output devices related to each SIF which is clearly identified by the plant means of equipment identification (e.g., field tag list);
- requirements to identify and take account of common cause failures for each identified SIF, such that a stable state has been achieved and the specified hazardous event has been avoided or sufficiently mitigated
- a definition of the safe state of the process for each identified SIF, such that a stable state has been achieved and the specified hazardous event has been avoided or sufficiently mitigate
- a definition of any individually safe process states which, when occurring concurrently, create a separate hazard (for example, overload of emergency storage, multiple relief to flare system)
- the assumed sources of demand and demand rate on the safety instrumented function
- requirement for proof-test intervals
- requirements relating to proof test implementation
- response time requirements for each SIF to bring the process to a safe state within the process safety time
- the required SIL and mode of operation (demand/continuous) for each SIF
- a description of SIS process measurements, range, accuracy and their trip points
- a description of SIF process output actions and the criteria for successful operation, e.g., leakage rate for valves
- the functional relationship between process inputs and outputs, including logic, mathematical functions and any required permissives for each SIF
- requirements for manual shutdown for each SIF
- requirements relating to energize or de-energize to trip for each SIF
- requirements for resetting each SIF after a shutdown (e.g., requirements for manual, semi-automatic, or automatic final element resets after trips)
- maximum allowable spurious trip rate for each SIF
- failure modes for each SIF and desired response of the SIS (e.g., alarms, automatic shut-down)
- any specific requirements related to the procedures for starting up and restarting the SIS
- all interfaces between the SIS and any other system (including the BPCS and operators)

Figure 1 Continued

- any specific requirements related to the procedures for starting up and restarting the SIS
- all interfaces between the SIS and any other system (including the BPCS and operators)
- a description of the modes of operation of the plant and requirements relating to SIF operation within each mode
- the application program safety requirements as listed in 10.3.3
- requirements for bypasses including written procedures to be applied during the bypassed state which describe how the bypasses will be administratively controlled and then subsequently cleared
- the specification of any action necessary to achieve or maintain a safe state of the process in the event of fault(s) being detected in the SIS, taking into account of all relevant human factors
- the mean repair time which is feasible for the SIS, taking into account the travel time, location, spares holding, service contracts, environmental constraints
- identification of the dangerous combinations of output states of the SIS that need to be avoided
- identification ofthe extremes of all environment conditions that are likely to be encountered by the SIS during shipping, storage, installation and operation. This may require consideration of the following: temperature, humidity, contaminants, grounding, electromagnetic interference/radio frequency interference (EMI/RFI), shock/vibration, – 52 – IEC 61511-1:2016 □ IEC 2016 electrostatic discharge, electrical area classification, flooding, lightning, and other related factors
- identification of normal and abnormal process operating modes for both the plant as a whole (e.g., plant start-up) and individual plant operating procedures (e.g., equipment maintenance, sensor calibration or repair). Additional SIF's may be required to support these process operating modes
- definition of the requirements for any SIF necessary to survive a major accident event, e.g., time required for a valve to remain operational in the event of a fire

4 Observations from the Wild

Mangan Inc. has had an opportunity to review numerous SRS's produced by a variety of Operating Companies, Safety Systems Consultants and Suppliers and Engineering Companies. These SRS's have exhibited wide variations in format, content and quality, but all of share number of common issues.
When Functional Safety Assessments (FSA's) have been performed for the SIS's, there are almost always numerous substantial findings relative to SRS completeness. In most cases assessment of the SRS's has required addition time to dig through attachments or referenced documents to identify if a required item has been addressed.

One overall conclusion though, is that all of the organizations observed are clearly struggling with figuring out the content of an SRS and its role in the Safety Life Cycle. It is apparent that a lot of money is being spent on these documents, much of it unnecessarily, and that the SRS's are not really meeting their intended value.
Some of the issues commonly observed are described below:

4.1 SRS Format

Almost all of the SRS's that Mangan has seen are in some type of Microsoft Word format, often with attached Microsoft Excel based data sheets. These documents are often very large and, in some cases, have other files embedded in them or just have embedded references to a local network drive location.

Often the documents are issued in a pdf format, which makes the embedded files inaccessible to readers that do not have the source document.

It has been observed, that even with a basic Word document format, the final documents vary widely in their details, often with parallel SRS's produced by the same organization varying in their organization, content and quality.

4.2 SRS Work Process

It is clear from the SRS's reviewed that the organizations producing them are having difficulties in incorporating SRS's into their project execution processes. The Safety Life Cycle defined in IEC-61511 intends that the SRS to be produced prior to the commencement of detailed design and procurement. Based upon observation of the SRS's produced by various organizations, this does not appear to be practiced.

It's been observed that in almost all cases, SRS's are being produced either as an afterthought, typically when a Functional Safety Engineer points out to a Project Engineer that an SRS is required or may have been started but never really completed before detailed design was started. SRS's appear to never to be actually finished with many formal revisions occurring to attempt to capture design developments.

The above observations indicate that there has not yet been general adoption of the SRS's position in the Safety Life Cycle. The SRS is not being treated as the key document that defines functional and design requirements that is prepared, completed and issued before detailed design activities are started. Instead the SRS has been incorrectly treated as a post design document or has become an attempt to document the design as it progresses.

4.3 SRS Content

The requirements for an SRS are a result of findings by various studies, including a British Health and Safety Executive study, of major incidents in the processing industries. The BHE study found that 44% of the incidents were attributable to incorrect and incomplete specification of the Safety Functions. The SRS requirements in IEC 61511 and ISA 84.00.01-2004 were developed to address this fundamental gap by defining the minimum requirements for specification of functional and basic design requirements that are to be included in an SRS that is prepared prior to detailed design, installation and operation. Table 2 of IEC 61511-1 2016 shows that the SRS is to be prepared prior to Design and Engineering of the SIS.

In the new version of IEC 61511-1 the SRS basic requirements in Clause 10 have been expanded upon to further clarify what information is intended to be presented and to tighten some requirements by changing previous usage of “should” to “shall”. The SRS requirements are being enhanced by the addition of more detailed requirements for proof testing and expanding the requirements for application programming. These are summarized in Figure 1.

- clear, precise, verifiable and maintainable and feasible
- written to aid comprehension and interpretation by those who will utilize the information at any phase of the safety life-cycle

In reality, the SRS’s observed are generally not well organized, and where they exist, key requirements are not clearly described.

Often the basic requirements are not stated in the SRS and are found buried in unrelated text or in series of reference documents which may or may not have been included in the SRS. There are instances where data referenced in the main body is not to be found at all in the referenced material.

The fact that fundamental requirements are buried in attached or referenced documents also provides strong evidence that SRS’s are being treated more as records of what was designed instead of meeting their intended function of defining design requirements.

It also becomes extremely difficult to identify if all of the requirements of Clause 10.3 have been addressed. This issue is exacerbated by the lack of consistency in presentation. The developers of these documents often claim to have met an SRS requirement, but really have missed the intent entirely.

4.4 Common Missing Requirments

The review of numerous SRS’s from a variety of organizations has resulted in identification of a number of items that are not contained in the SRS but are required by IEC 61511. These missing items commonly don’t appear in many SRS’s and tend to point to a lack of recognition of their importance or an assumption that “standard practice” covers them. While not all observed SRS’s contain the same gaps, they all have some number of the below listed gaps.
A list of the more common SRS gaps is listed below:

- The Process in which the SIS is installed is often not described
- The Operating Modes of the Process are almost never described
- The SIF operating status in the various Process Operating modes are almost never described. This includes such things as startup bypasses or delayed arming, status of the SIF's during shutdown operations or any other operating conditions that might affect the operation of the SIF's.
- Safe States are often not explicitly stated but are expected to be inferred from other data (e.g. device data sheets).
- Requirements that apply to the SIS Logic Solver vs. the requirements for each SIF or non-SIF function implemented in the SIS are often not separated from one another, nor are they clearly organized.
- SIS environmental and installation requirements are often not specified by the SRS.
- Often power systems are not described or are poorly described.
- Key SIF performance requirements such as Process Safety Times, SIF response times, allowable demand rates and allowable spurious trip rates are not defined.
- Functional requirements for Input and Output devices are often incomplete or poorly documented. Input device ranges, response times and accuracy are not described nor are things like valve failure states, stroke times and allowable leakage specifications. Often device data sheets are referenced, but this does not provide definition of requirements. It only results in a description of what was provided with no assurance that the provided devices meet the Safety Requirements.
- Set points for protective functions are often either missing or buried in attachments. While not a direct SRS requirement, often the rationale for selecting a set point, such as when it is based upon an equipment operating limit related, is seldom documented. Set point basis data is critical information when modifications to a set point value are being considered.
- SIF Reset and Bypass functions are often poorly described or not described at all.
- Required behaviors upon SIS or SIF device faults and failures are not defined.
- Failure rates for devices and activating energy sources (air, power) that have energize to trip functionality, such as double acting piston actuators or motor controllers are not always recognized. Often is appears that it's is assumed that a de-energize to trip interposing relay alone is sufficient.

5 Compliance vs Completeness

As a Safety Performance Standards, IEC 61511 intentionally does not address robustness and maintainability of SIS Design. These issues are not within the scope of the Standard and such issues are considered as those for which the owner/operator should be responsible.

While the Standards do not address these issues because their scope is directed towards assuring a Safety Function operates, robustness and reliability are of crucial importance to Operating Organizations, and as such, the basic requirements of owner/operator should also appear in the SRS or should be clearly referenced in the SRS.

An additional aspect of preparation of an SRS is inclusion of Design requirements that are related to SIF robustness and maintainability. While an SRS that addresses all of the Items listed in Clause 10.3 may be considered to be Compliant, the SRS may be far from complete.

Personnel preparing SRS's should be cognizant that the SRS is a set of directions to a Designer, and that without additional direction, the SIS design that results may not meet the owner/operator's expectations. Among the critical items that should be considered for inclusion in the SRS are:

- Basic installation standards including locations, segregation of SIS and BPCS wiring and installations, labeling, access, etc.
- Power system requirements – source power and redundancy, derived power (e.g. power supplies) redundancy and failure behavior. Power reliability requirements for energize to trip functions should also be defined.
- Local regulatory requirements such as electrical codes and building codes.
- Requirements for SIF robustness such as redundancy, continued operation with partial failures vs. false trips and provisions for testing when on-stream testing is required.
- Site or organization requirements for acceptable suppliers and model lines and those devices that the Site or organization has determined as acceptable by prior use.
- Documentation requirements including turnover format
- Expectations for development of procedures for operations, maintenance and initial and periodic testing including format and contents.
- Design and installation requirements such as wiring specifications, segregation and labeling of Safety Related wiring and devices

These topics are usually best addressed by a Site Standard or Technical Practice that defines SIS design and installation practices. This document then can be referenced as part of the basic design requirements defined by the SRS.

6 SRS Development Guidance

Based upon observations of real-world SRS's, individuals and organizations that are responsible for development of SRS's should consider the following guidelines:

- Do not treat an SRS as a new document for every instance. Have a complete document outline, and where practicable, a complete and well-organized SRS for reference.
- Start SRS development early and do not allow engineering and procurement to start until the SRS is completed. Projects should clearly identify deliverable dates for SRS issue for review and SRS approval and rigorously enforce these as a milestone upon which the start of other engineering is contingent. Do not do SRS development in parallel with detailed design.
- Make sure the SRS contains all of the IEC/ISA requirements. Use Table 1 as a checklist and make sure that these requirements are clearly stated in the body of the SRS. Do not make users of the document dig for the information.
- Focus on functional requirements and include engineering details only when they are required to define functional requirements. Do not attempt to make the SRS a repository for the design documents and specifications.
- Do not expect design documents and specifications to substitute for SRS requirements specifications.

- Make sure the SRS identifies critical owner requirements for design and installation standards and provisions required for robustness and maintainability. Where possible, design and installation requirements should be stated in a separate site design requirements and practice document and cited for inclusion as minimum design requirements by the SRS.
- Include the basis for set points, even if the basis is “a comfortable operating margin” above or below a limit. If the set point is based on the equipment limit or do not exceed value, make sure this is clearly identified.
- Do not keep revising the SRS unless there is a real change that affects the required functions and performance of the SIS or its SIF’s or related functions. Ideally an SRS should only go through three, at most four revisions as it is developed.
- Do not allow accounting considerations to divide the responsibility for SRS development and SIS design. Attempting to split SIS responsibilities among several parallel projects that were set up for accounting purposes is not a good idea.

7 The Value of a Data Driven SRS

The problems with SRS’s that are based upon traditional project engineering practices indicate that there needs to be a better way to develop and maintain SRS’s and assure that they are complete and consistent.

One method of doing this is to use a Data-Driven SRS. In a Data-Driven SRS, the complete requirements for an SRS’s contents can be defined by personnel who are knowledgeable and experienced with SRS preparation

A project that is generating the SRS then uses the database to enter the required data and generate an SRS Report. With a well-designed data base, when all of the data fields are filled out with quality data, the SRS is done. It is then fairly easy to maintain or identify where gaps exist.

Use of a Data-Driven SRS has the following benefits to Owner/Operator organizations and Project teams:

- Costs for SRS development and management are drastically reduced. With a well-designed SRS data structure and reasonable examples, SRS development time can be reduced to hours rather than weeks or months.
- SRS contents, layout and format can be defined as a standard by personnel knowledgeable in SRS requirements and preparation, and this becomes a standard for the organization.
- SRS development can be assigned to less experienced and skilled personnel once the data structure and good examples are established.
- SRS consistency and completeness can be assured. Missing information can be readily identified.
- SRS data for SIS’s and SIF’s can be copied from other SIS’s and SIF’s in the database and then edited for differences instead of creating them from scratch.
- SRS data has a single point of storage and access. The latest versions are always available, and changes can be readily tracked.
- SRS data is available to other steps of the Safety Life Cycle – SRS data can be used to generate specification data for physical devices or linked to the LOPA scenarios upon which the Safety Functions are based.

- PFD's of common designs can be automatically computed from failure parameters entered for SIF Inputs and Outputs.

An example of a Ddata-Ddriven SRS application is described below. There are actually multiple sections to a complete SRS: Those that define requirements for specification and installation of Logic Solvers and associated support systems, and those that define requirements for each SIF or associated function that is implemented within the SIS.

8 Developing SRS's with SLM

SLM provides a comprehensive framework for development of Safety Requirements Specifications for an SIS and its SIF and non-SIF functions. Filling in data for the fields provided by SLM will result in a complete SRS that addresses all of the requirements of IEC 61511 and also allows the User to specify requirements for fault tolerance and design robustness that the standards do not address.

SLM also allows Users to clone any existing SIS, SIF, Voting Group or I/O Asset to another SIS or SIF, and to link existing Voting Groups and I/O Assets to multiple SIF's. This functionality minimizes the time required to prepare an SRS and to maximize consistency of functional and design requirements.

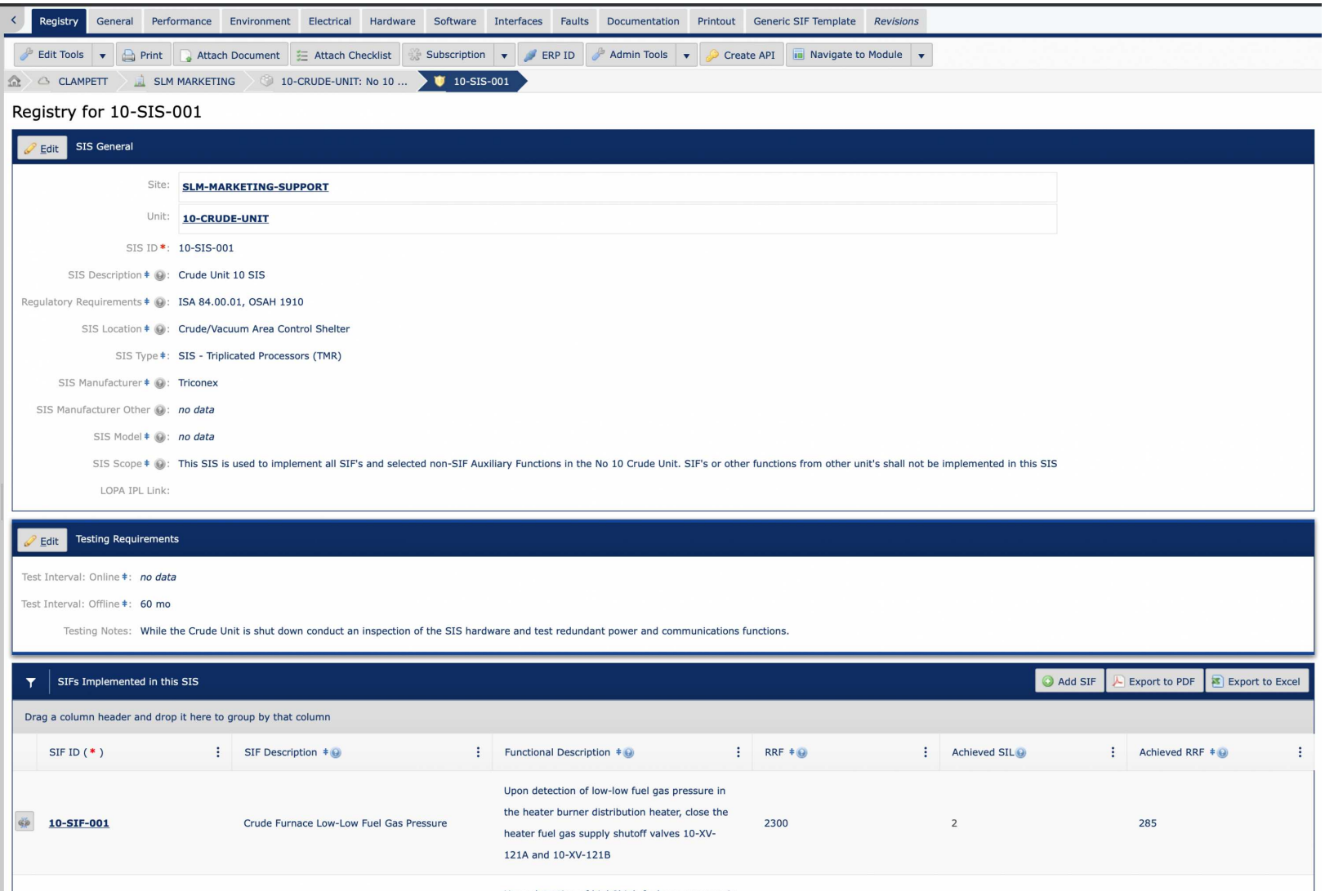
SLM also provides a single point of storage of SRS's, allows for management of change and provides a library of data from which to clone similar SIS's and SIF's. This substantially reduces ongoing costs of SIS and SRS management. In an environment with the SRS data is integrated with HAZOP and LOPA data and Operation and Maintenance Events, a full Safety Life Cycle tool can be realized which further reduces costs of ownership and improves employee access and knowledge of the underlying hazards for which the SIS and SIF's have been installed to prevent.

8.1 SIS Section

An SIS Section data entry view is shown in Figure 2. The SIS section contains data fields required to define data required by IEC 61511 for the SIS as well as key robustness and maintainability data for the SIS. This section consists of multiple tabs, each of which covers a required topic. The data that is contained in the SIS Object and its usage is described in the White Paper "The SLM SIS Object".

- General Data – This tab contains data fields to define the SIS ID, Description, Location, Manufacturer, Scope of Application and Process Descriptions and Operating Modes for Startup, Normal Operations, Shutdown and other Process Modes.
- Performance – This tab contains data fields to define SIS performance requirements such as Mission Time, Response Time, Required Architecture SIL limits, Fault Tolerance, MTTF, MTTR, etc.
- Environment – This tab contains data fields to define SIS environmental conditions such as temperature, humidity, electrical classifications, etc.
- Electrical – This tab contains data fields for power source, SIS and I/O power requirements, redundancy, etc.
- Hardware – This tab contains data fields for general SIS hardware requirements including I/O module requirements.
- Software – This tab contains data fields for SIS software and firmware requirements such as programming software, maintenance software, and firmware and software versions and certifications, etc.
- Interfaces – This tab contains data fields for SIS interfaces to a BPCS, local HMI's or interfaces to I/O equipment or systems.
- Faults – This tab contains data fields for description of SIS failure detection and actions, SIS common cause failures and SIS Fault/Failure Alarms or indications.
- Documentation – This tab contains data fields for identification and/or attachment of reference documentation such as standards, procedures and design documentation
- Printout – This tab presents a complete view of the SRS for viewing printout

Figure 2: SIS data for SRS



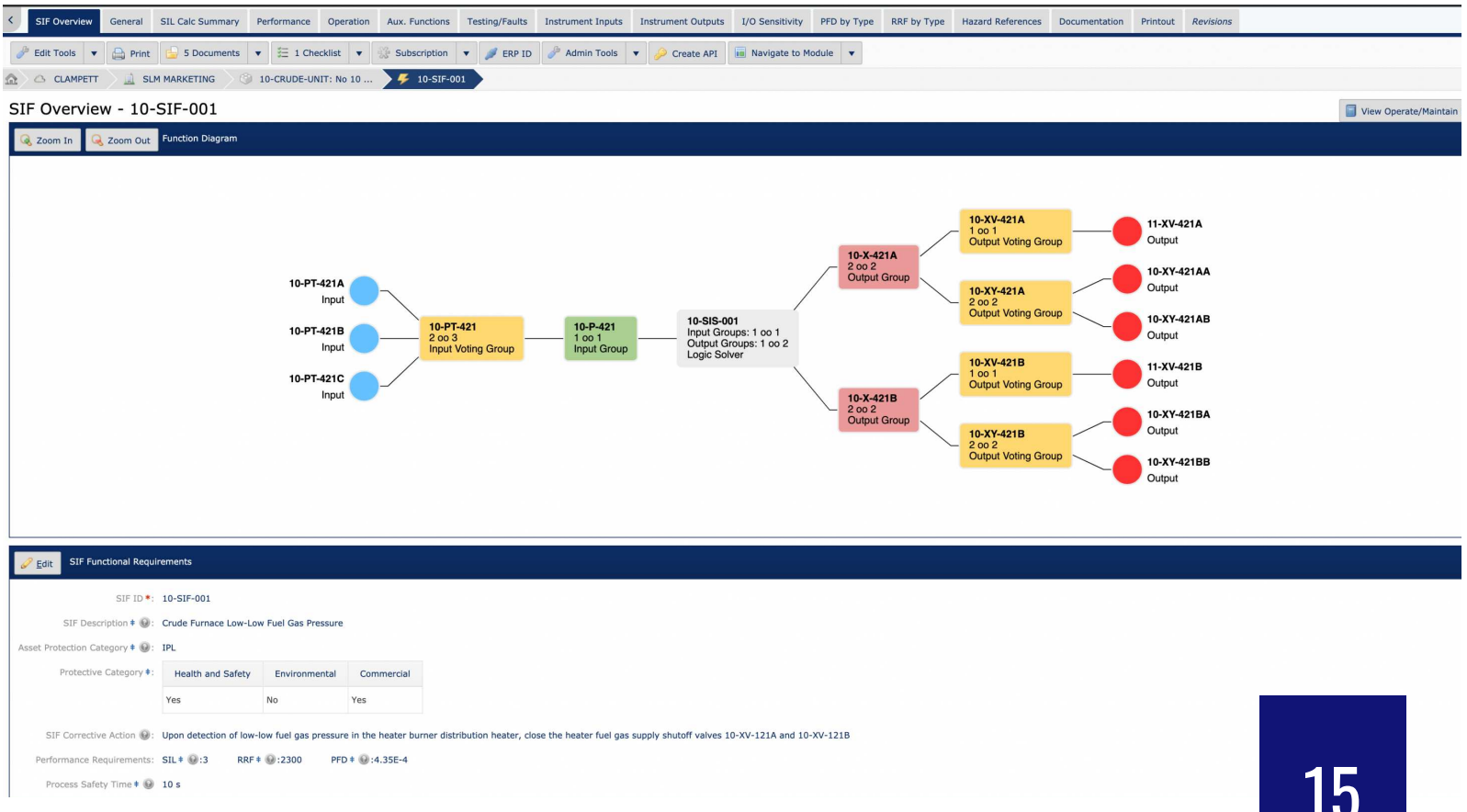
8.2 SIF Section

An SIS Section data entry view is shown in Figure 2. The SIS section contains data fields required to define data required by IEC 61511 for the SIS as well as key robustness and maintainability data for the SIS. This section consists of multiple tabs, each of which covers a required topic. The data that is contained in the SIS Object and its usage is described in the White Paper “The SLM SIS Object”.

- General – The General tab provides data fields for SIF data such as the SIF ID, Description, Safe State, Hazard description for which the SIF is required, Demand Sources and Rates and SIF Operating Modes.
- Performance – The Performance Tab Contains data fields to define the SIF Integrity Levels – Target and Achieved, Process Safety Time and SIF response times for Inputs, Logic Solver and Outputs, Trip Points and Basis, Spurious Trip requirements and achieved rates. Fields are available to define other SIF related data such as Architectural Limits, Hardware Fault Tolerance, Major Accident requirements, Concurrent Safe State Hazards, etc.
- Operation – The Operation Tab contains data fields to define operational requirements such as reset of the SIF, manual shutdown requirements, startup requirements and bypass requirements.

- Aux Functions – The Aux Function tab contains data fields to identify other non-SIF actions that occur when the SIF is activated such as coordination of BPCS controls or tripping other equipment, or interlocks that are used for bypassing or arming SIF's during startup or other operations.
- Testing/Faults – The Testing/Fault tab provided data fields for description of SIF behavior upon detection of SIS, Input or Output Device faults and failures. This section also is used to identify fault or failure alarms, or status indications associated with the SIF that are required to be included in the design. The tab also contains data fields to define the testing methods, testing intervals and the requirements that the design must be included to support testing.
- Instrument Inputs – The Instrument Input tab contains data fields that allow specification of input voting schemes and functional requirements of Input Devices such as certifications requirements, accuracy, response time, trip set points and basis, general service conditions and severity of the services.
- Instrument Outputs - The Instrument Output tab contains data fields that allow specification of output voting schemes and functional requirements of Output Devices such as certification requirements, stroke time, leakage requirements, general service conditions and severity.
- Documentation – This tab contains data fields for identification and/or attachment of reference documentation such as procedures and design documentation. Where the data base does not contain links to LOPA or HAZOP scenarios, the applicable sections of these studies by be attached or referenced.
- Printout – This tab presents a complete view of the SRS for viewing printout

Figure 3: SIF data for SRS



8.3 Inputs, Outputs, and Voting Groups

Each SIF and non-SIF Asset in SLM should have the Input and Output Assets defined. Input and Output Assets may be thought of as a Service Location such as many Maintenance Management Systems use. The Service Location is a place in a process where a physical device is installed. The Service Location has basic functional requirements associated with it but does not include physical specification requirements.

8.3.1 Input and Output Assets

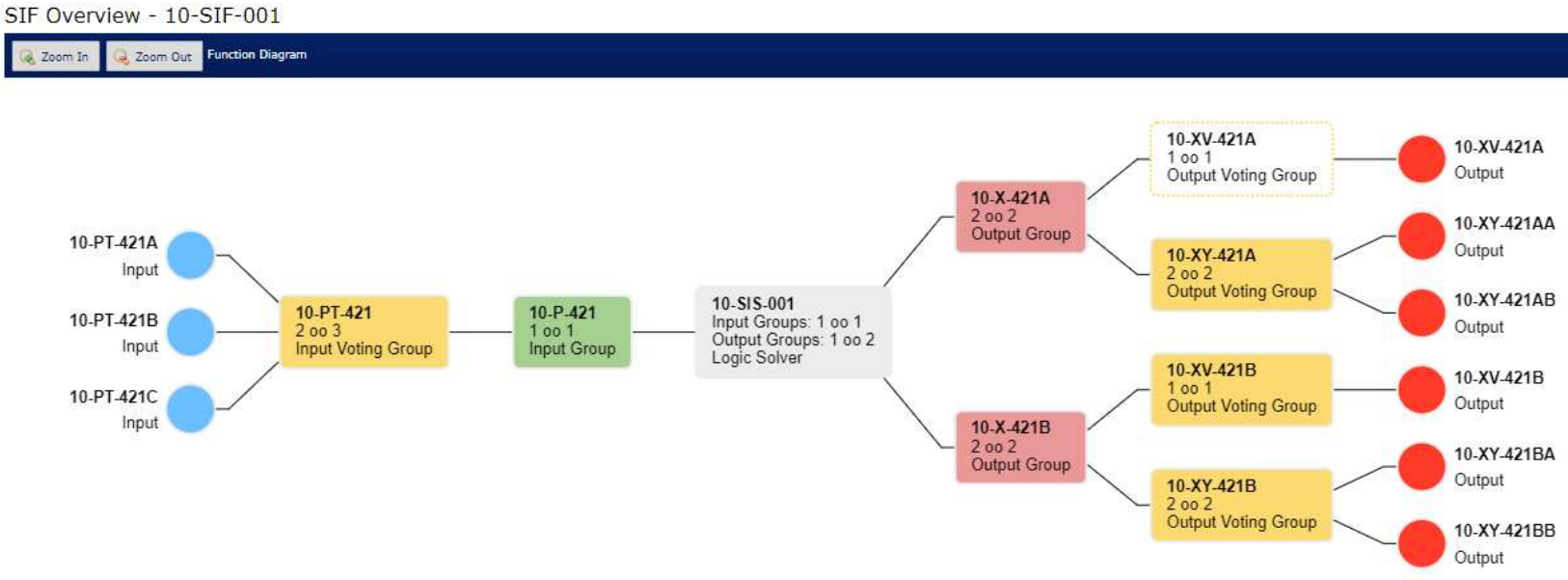
In SLM, Input and Output Assets correspond to locations where an instrument or valve may be installed. In the Instrumented Systems Module, the data for Input and Output Assets is intended to define performance requirements for the locations which must be met by the Devices that are actually installed in the locations.

The details of the Input and Output Assets are described in the White Paper “SLM Input and Outputs – Voting Groups and Assets”.

In the Operate Maintain Module Devices that have specification data such as Manufacturer’s, Model Numbers, Materials, etc. are linked to the Input or Output Asset.

8.3.2 Input and Output Assets

For SIF and HIPS Assets, Input and Output Assets are organized into Voting Groups. These Voting Groups and their associated Input and Output Assets are used by SLM to generate the SIF and HIPS Diagrams as illustrated below. The Voting Group and Input and Output Assets also determine how SLM will perform PFD calculations.



Voting Groups are also used to define other related functional requirements such as the set point for the Group and the basis for that set point and failure response if one or more of the Group's I/O Assets fails

The arrangement of Voting Groups, Assigning ID's and defining other data is a fairly complex subject. There are many ways to present the data depending upon how a User desires to track performance. A complete discussion of the use of Voting Groups discussed in detail in the White Paper "SLM Input and Outputs – Voting Groups and Assets". There are many ways to present the data depending upon how a User desires to track performance.

8.4 Additional Functions

Many times, additional non-SIF functions may be implemented in an SIS. This may be due to a User's choice to implements as many IPL's as possible within the SIS, or a desire to share SIF Inputs with Auxiliary or related functions. A couple of examples of this are:

- An Organization has decided that any alarms used as IPL's be implemented in the SIS in order to enforce management of change requirements
- A SIF has related non-SIF functions such as startup sequences or other non-SIF Interlocks

SLM allows User to include Interlock functions and Alarm functions as children of an SIS object.

9 Cloning and Linking SRS Components

Creating an SRS to fully define and document SIS and SIF requirements involves a lot of data. However, once an Organization has developed an SRS for an SIS and developed the more common SIF's that exist in their processes, the process is generally quite repetitive. SLM provides tools to make the development of subsequent SRS's extremely efficient. These tools also promote consistency in practice and presentation. The process for cloning and linking SRS objects is described in White Paper "Minimizing SRS Development Time with Cloning and Linking".

When an object is cloned, SLM creates a copy of the object and, if selected, all of its child objects. The data fields are all copied to the new object, with the only differences between the source objects and the newly copied objects being that SLM assigns a system ID to the new objects. The User than can edit the ID's and other data as necessary and avoid the labor of having to create everything from scratch. With judicious selection of the source objects, the amount of editing can be kept to a minimum.

Cloning or Linking of SRS Components can be used for the following types of Use Cases.

9.1 Clone an entire SIS

In some cases, a User is going to add an SIS that is very similar to an existing SIF. For example, a parallel Unit or a very similar Unit may require an SIS that is substantially the same as an existing SIS. In this case the User can create a copy of the entire SIS including its SIF's and each SIF's Input and Output Groups, Voting Groups and Assets. Once this copy is completed, the User can edit the new SIS and its components as required to make it specific to the new SIS requirements. Mostly this would consist of editing the object ID's to those require for the new SIS objects and editing some of the text such as Service Descriptions or other Unit specific data.

9.2 Clone an SIS Object Only

In other cases, a new SIS may be using the same SIS design as an existing one, but its SIF's may not be the same. SLM allows a User to create a copy of only the SIS object, which will capture the bulk of the SIS requirements. Some editing of ID's and descriptors will be necessary, but usually most of the other data can stand without modification.

9.3 Clone a SIF

Many SIF's represent common applications that appear in many places within a Site or Enterprise. SLM allows the User to standardize on SIF designs and copy them from one SIS to another or even create a copy in the same SIS. The User has a choice as to whether to copy a complete SIF with all of its I/O or just the SIF object. For example, a User has standardized on a SIF design for fired process heaters. That design can be cloned to other Units and most of the data entry work can be avoided.

9.4 Clone an Existing Input or Output Group

Within an Enterprise, the structure of Input and Output Groups tend to look a lot alike. A single measured value Input Group with 2oo3 voting often has the same structure whether the process measurement is pressure, flow, temperature or level.

SLM allows the User to copy Input and Output Groups that exist in one SIF to another SIF. The structure of the groups (Voting Groups, Assets) is the same as the source Group and the User them many edit ID's and other data as needed.

9.5 Link an Existing Input or Output Group

Often the SIF's or within an SIS will share either Input or Output Assets. For example, a fired heater may have three SIF's – one for high fuel gas pressure, one for low fuel gas pressure and one for low tube side flow. All three SIF's shut off the heater fuel gas. In this case, the Output Groups for the fuel gas valves are the same for all three SIF's. The User should not create 3 sets of Output Groups, but rather should use the same Output Groups and link them to the applicable SIF's

SLM allows a User to Link Objects to different parents, such as linking an Output Group to multiple SIF's. This avoids the work of creating three Output Groups with the same data and improves the accuracy of performance data for the Output Assets involved. The User has a clear view of how many places a particular Asset is used and when Operate-Maintain data is accumulated, the Event data goes against the actual Assets.

9.6 Clone or Link Inout and Output Assets

Input or Output Asset objects may also be cloned or linked to multiple Voting Groups. This is useful in circumstances where data for a specific Input or Output Asset Type is simpler to copy that create.

10 SIL Calculations

The SIF views in SLM contain a SIL PFD Calculation Function. This function uses some data from the SIF and other User entered data and data from the Operate-Maintain Module to calculate the PFD of the SIF. This data is also used to generate the SIF Diagram that is displayed in the SIF Registry View. The Input and Asset failure rate data may be manually entered, or, when available, in-service failure data for the Input or Output Types can be used. The details of the SIL Calculation function are described in the White Paper “SLM SIL PFD Calculations”.

11 Linkages- HAZOP and LOPA to the SRS and SRS to Operate-Maintain Data

As described in the White Paper “Conducting LOPA’s” with SLM” IPL Assets such SIF’s and other IPL Objects such as Alarms, Interlocks, Relief Systems and Non-Instrumented IPL’s may be linked to LOPA IPL’s and through that linkage to the HAZOP and LOPA scenarios that identified the need for the IPL Asset. When Devices in the Operate-Maintain Module are created, they are linked to Input and Output Assets. So, through these relationships, a complete trail from the original HAZOP all the way to the field Device performing a Safety Function exists and can be readily accessed by SLM Users.