MANGAN
Software Solutions

Safety Requirements Specifications
They don't have to be hard (or expensive)

SLM®
Safety Lifecycle Manager

www.Mangansoftware.com

Table of Contents

The information provided in this document has been developed by Mangan Software Solutions, a subsidiary of Mangan, Inc. This document may contain confidential, proprietary, privileged material and/or trade secrets. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon this information by persons or entities other than the intended recipient is prohibited.

02

1 Abstract

IEC 61511 and ISA 84.00.01-2004, Clause 10, requires that a Safety Requirements Specification (SRS) be prepared for all Safety Instrumented Systems (SISs). The Clause presents a number of items to cover in the SRS, but provides little or no guidance on how a SRS should be developed, organized, or maintained. This lack of guidance results in Operating Companies, SIS Consultants, and Engineering Companies producing a variety of SRSs that vary widely in format, content, and quality. In practice, these SRSs have become extremely expensive to produce and maintain, and really do not meet the intended functionality and value.

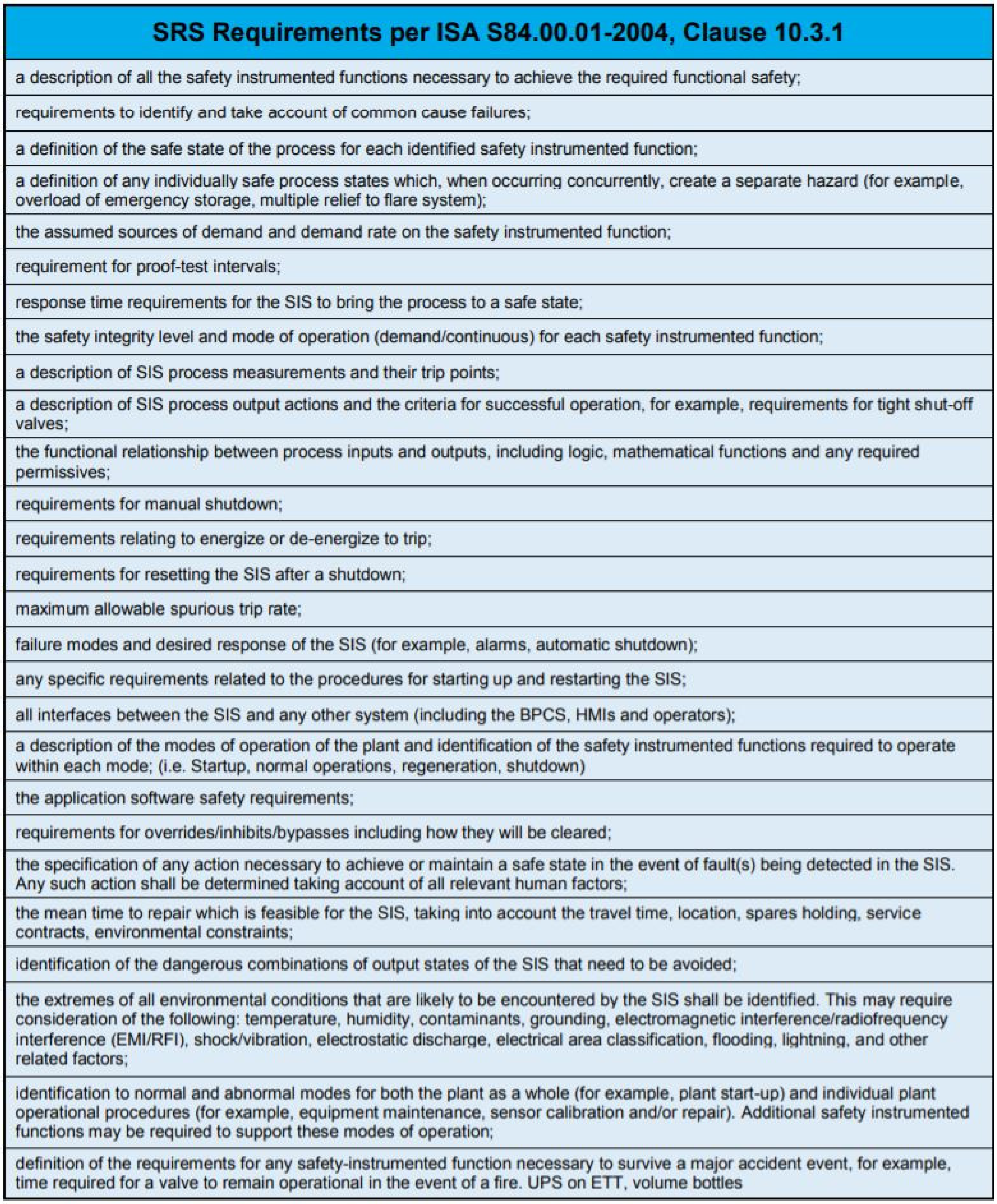
This white paper reviews the purpose and usage of a SRS, identifies some issues observed in SRSs produced by various organizations, provides some practical suggestions for SRS preparation, and discusses the advantages of a Data-Driven SRS.

2 Performance Data Collection

IEC 61511 and ISA 84.00.01-2004, Clause 10, contain the basic requirements for a SRS, summarized in Figure 1. As these Standards are intended to be performance based Standards, there is little direction or guidance provided on how to incorporate these requirements into a SRS. These details are the organizations responsibility. Additionally, the Standards only address requirements to assure that the required Safety Functions operate as required on Demand. The Standards do not address issues that pertain to SIS and Safety Instrumented Function (SIF) reliability, maintainability, or consistency with owner organization practices and standards.

The requirements for a SRS are a result of findings by various studies, including a British Health and Safety Executive (BHE) study (1), 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 are intended to address this fundamental gap by defining the minimum requirements for specification of functional and basic design requirements that are to be included in a SRS that is prepared prior to detailed design, installation, and operation. Figure 8 of IEC 61511 and ISA 84.00.01-2004 shows that the SRS is to be prepared prior to Design and Engineering of the SIS.

IEC 61511 is in the revision process and currently in the ballot stage. While the final Standard is subject to change based upon ballot results, the SRS basic requirements in Clause 10 are generally being 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 expand with the addition of more detailed requirements for proof testing and application programming. Reference (2) provides a description of pending IEC 61511 changes. At the time this white paper went to publication, the Second Edition of IEC 61511 had a late 2015 release date. Current IEC schedules show a projected publication date of March 2016.



SRS Requirements per ISA S84.00.01-2004, Clause 10.3.1
a description of all the safety instrumented functions necessary to achieve the required functional safety;
requirements to identify and take account of common cause failures;
a definition of the safe state of the process for each identified safety instrumented function;
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;
response time requirements for the SIS to bring the process to a safe state;
the safety integrity level and mode of operation (demand/continuous) for each safety instrumented function;
a description of SIS process measurements and their trip points;
a description of SIS process output actions and the criteria for successful operation, for example, requirements for tight shut-off valves;
the functional relationship between process inputs and outputs, including logic, mathematical functions and any required permissives;
requirements for manual shutdown;
requirements relating to energize or de-energize to trip;
requirements for resetting the SIS after a shutdown;
maximum allowable spurious trip rate;
failure modes and desired response of the SIS (for example, alarms, automatic shutdown);
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, HMIs and operators);
a description of the modes of operation of the plant and identification of the safety instrumented functions required to operate within each mode; (i.e. Startup, normal operations, regeneration, shutdown)
the application software safety requirements;
requirements for overrides/inhibits/bypasses including how they will be cleared;
the specification of any action necessary to achieve or maintain a safe state in the event of fault(s) being detected in the SIS. Any such action shall be determined taking account of all relevant human factors;
the mean time to repair 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;
the extremes of all environmental conditions that are likely to be encountered by the SIS shall be identified. This may require consideration of the following: temperature, humidity, contaminants, grounding, electromagnetic interference/radiofrequency interference (EMI/RFI), shock/vibration, electrostatic discharge, electrical area classification, flooding, lightning, and other related factors;
identification to normal and abnormal modes for both the plant as a whole (for example, plant start-up) and individual plant operational procedures (for example, equipment maintenance, sensor calibration and/or repair). Additional safety instrumented functions may be required to support these modes of operation;
definition of the requirements for any safety-instrumented function necessary to survive a major accident event, for example, time required for a valve to remain operational in the event of a fire. UPS on ETT, volume bottles

Figure 1: IEC/ISA 84 SRS Required Items

3 Observations from the Wild

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

One overall conclusion is that all of the organizations observed are clearly struggling with figuring out the content of a SRS and its role in the Safety Lifecycle. It is apparent that a lot of money is being spent on these documents, much of it unnecessarily, and that the SRSs are not really meeting their intended value.

Some of the issues commonly observed are described below:

3.1 SRS Format

Almost all of the SRSs 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 imbedded in them. Often issued documents are in a .pdf format, which makes the imbedded files inaccessible to readers that do not have the source document. Even with a basic Word document format, the final documents vary widely in their details. Often, parallel SRSs produced by the same organization vary in their organization, content, and quality.

3.2 SRS Work Process

It is clear from reviewed SRSs that the organizations producing them are having difficulties in incorporating SRSs into their project execution processes. The Safety Lifecycle defined in the IEC and ISA Standards intends for the SRS to be produced prior to the commencement of detailed design and procurement. It does not appear that this practice is in place when observing the SRSs produced by various organizations.

It’s been observed that in almost all cases, SRSs are being produced either as an afterthought, typically when a Functional Safety Engineer points out to a Project Engineer that a SRS is required, or may have been started but never really completed before detailed design was started. Numerous revisions to the SRS attempt to capture design developments that resulted from not having a complete SRS as the start of design.

The above observations indicate that there has not yet been general adoption of the SRSs position in the Safety Lifecycle. The SRS should be the key document that defines functional and design requirements and prepared, completed, and issued before detailed design activities start. Instead, organizations incorrectly treat the SRS as a post-design document, or the SRS becomes an attempt to document design as design activities progress.

3.2 SRS Content

In many cases, the issues with managing the SRS Work Process described above results in the SRS becoming a bloated document that attempts to capture detailed engineering data rather than addressing only the Functional and Basic Design requirements that a SRS is intended to address.

Most SRSs have been found to be incomplete at the time that the SIS is ready for commissioning, and have had revision numbers in the low 20's. A SRS with this many formal revisions is a strong indicator that the organization producing or managing the SRS does not have a handle on the Work Process or the intent of the SRS. Unfortunately, these observations are more common than not. One has to wonder how many engineering hours have been spent producing documents of this type with no real benefit being realized.

Generally, the SRSs fail to meet the fundamental requirements for clarity and ease of use with the basic requirements of Clause 10.2.1 seldom met. Clause 10.2.1 requires:

> SIS Requirements shall be expressed and structured in such a way that they are:
>
> - clear, precise, verifiable, maintainable, and feasible
> - written to aid comprehension and interpretation by those who will utilize the information at any phase of the Safety Lifecycle

In reality, the SRSs observed are generally not well organized and key requirements lack clarity. Often, the basic requirements aren't stated in the SRS and have been found buried in unrelated text, or in a series of reference documents that may or may not have been included in the SRS. There are instances where data referenced in the main body is not in the referenced material at all.

The fact that fundamental requirements are buried in attached or referenced documents also provides strong evidence that SRSs are being treated more as records of what was designed instead of meeting their intended function of defining design requirements. It becomes extremely difficult to identify if all requirements of Clause 10.3 are in the SRS. The lack of consistency in presentation exacerbates this issue. The developers of these documents often claim to have met a SRS requirement, but often miss the intent entirely.

3.3 Commonly Missed Requirements

The review of numerous SRSs from a variety of organizations has resulted in identification of a number of items required by IEC/ISA Standards are missing. The missing items commonly do not appear in many SRSs and tend to point to a lack of recognition of their importance, or an assumption that "standard practice" covers them. While not all observed SRSs contain the same gaps, they all have some number of the below listed gaps.

A list of the more common SRS gaps is below:

- The SIS installation process description is missing.
- The Operating Modes of the process are missing.
- Often, the SIF operating status in the various Process Operating modes is not described, including startup bypasses or delayed arming, status of the SIFs during shutdown operations,

- or any other operating conditions that might affect the operation of the SIF's.
- Safe States are often not explicitly stated. The expectation is to infer the information 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 lack specificity in the SRS. Often, power systems are either missing or 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 accuracies are not described. Further, definitions for valve failure states, stroke times, and allowable leakage specifications are missing. While device data sheets are referenced, this does not provide definition of requirements. It only results in a description of provided equipment with no assurance that the provided devices meet Safety Requirements.
- Set points for protective functions are often either missing or buried in attachments. While not a direct SRS requirement, the rationale for selecting a set point, such as when based upon an equipment-operating limit, is seldom documented. When considering modifications to a set point value, set point basis data is critical information.
- SIF Reset and Bypass functions are often poorly described or not described at all.
- Required behaviors upon SIS or SIF device faults and failures lack definition.

- Required behaviors upon SIS or SIF device faults and failures lack definition.

- 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, it's assumed that a de-energize to trip interposing relay alone is sufficient.

4 Compliance vs. Completeness

The Safety Performance Standards, IEC 61511 and ISA 84.00.01, do not address robustness and maintainability of SIS Design. These issues are not within the scope of the Standards and the Standards consider such issues as those for which the Owner/Operator should be responsible.

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

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

- Basic installation standards – locations, segregation of SIS and BPCS wiring and installations, labeling, access, etc.
- Power system requirements, such as 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 – electrical codes, building codes
- Requirements for SIF robustness – redundancy, continued operation with partial failures vs. false trips, provisions for testing when on-stream testing
- Site or organization requirements for acceptable suppliers, model lines, 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, initial and periodic testing (format and contents)
- Design and installation requirements, such as wiring specifications, segregation, labeling of Safety Related wiring and devices.

A Site Standard or Technical Practice that defines SIS design usually best addresses these topics and installation practices. This document can be referenced as part of the basic design requirements defined by the SRS.

While the Standards do not address these issues, their scope is directed towards assuring a Safety Function operates. A Safety Functions robustness and reliability are of crucial importance to Operating Organizations.

The basic requirements of Owner/Operators should also appear in the SRS, or should be clearly referenced in the SRS.

5 SRS Development Guidance

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

- Do not treat a 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 the 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 review and SRS approval. Rigorously enforce these as a milestone upon which the start of other engineering is contingent. Do not conduct SRS development in parallel with detailed design.
- Make sure the SRS contains all 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 meet 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, state design and installation requirements in a separate site design requirements and practice document, 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 equipment limits or does not exceed value, make sure this is clearly identified.
- Do not include detailed engineering design data in a SRS.
- Do not revise the SRS multiple times unless there is a real change that affects the required functions and performance of the SIS or its SIFs or related functions. Ideally, a SRS should only go through 3, at most 4 revisions as it is developed.

6 The Value of a Data-Driven SRS

The problems with SRSs based on traditional project engineering practices indicate that there needs to be a better way to develop and maintain SRSs 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, personnel who are knowledgeable and experienced with SRS preparation define the complete requirements for a SRS’s contents. A project that is generating the SRS then uses the database to enter the required data and generate a SRS Report. A SRS is complete with a well-designed database that has all data fields filled out with quality data. It is then 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:

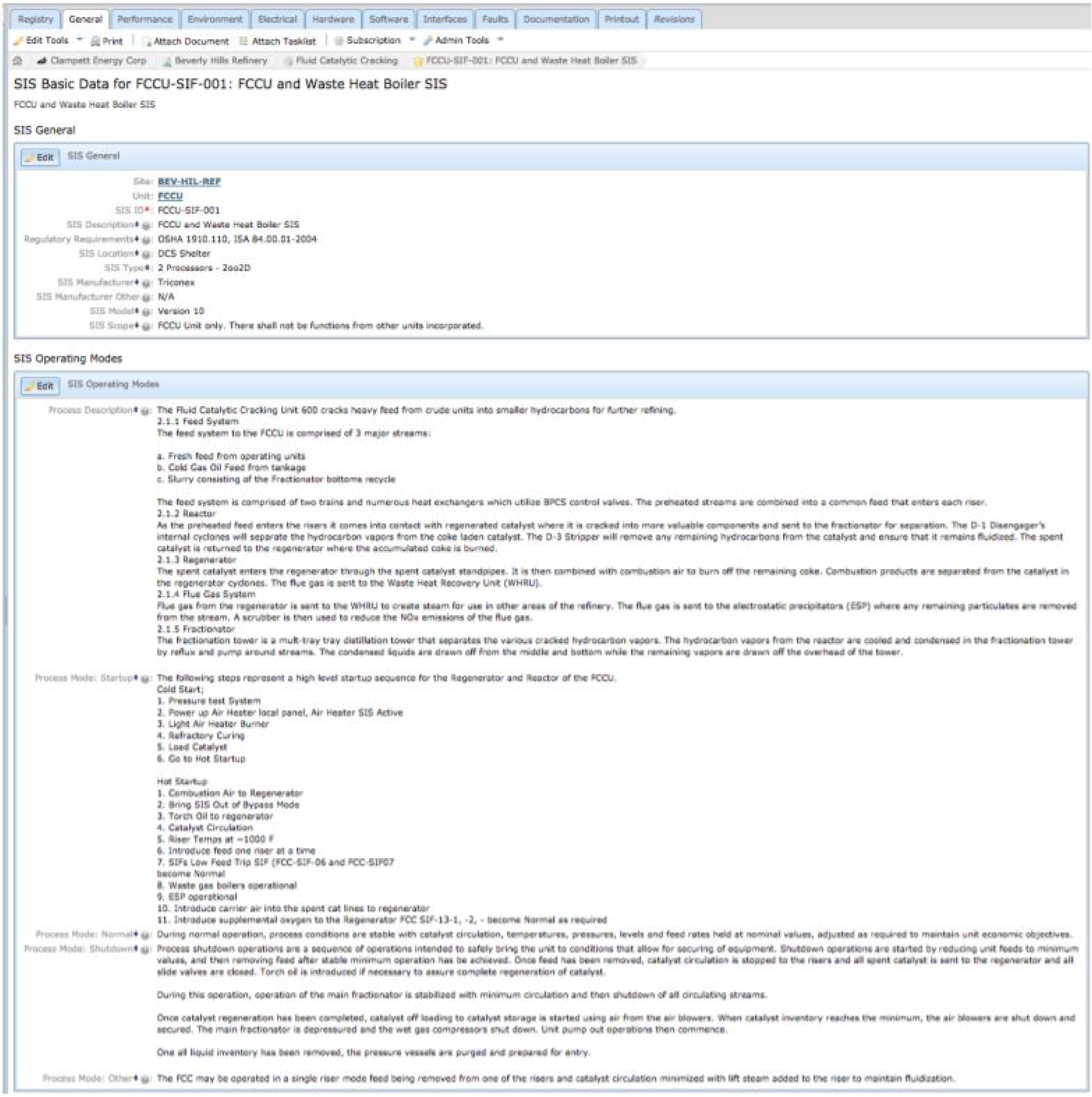
- Drastically reduce costs for SRS development and management. A well-designed SRS data structure with reasonable examples reduces SRS development times to hours rather than weeks or months.
- Personnel knowledgeable in SRS requirements and preparation of SRS contents, layout, and format define a standard that becomes a standard for the organization.
- A less experienced engineer can develop the SRS using previous examples once the data structure is established.
- SRS consistency and completeness can be assured, and missing information can be readily identified.
- SRS data for SISs and SIFs can be copied from other SIS’s and SIFs in the database. Engineers edit for differences, instead of creating from scratch.
- SRS data has a single point of storage and access. The latest versions are always available with changes readily tracked.
- SRS data is available to other steps of the Safety Lifecycle. 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.
- PFDs of common designs can be automatically computed from failure parameters entered for SIF Inputs and Outputs.

Below is an example of a Data-Driven SRS application. There are multiple sections to a complete SRS, including defining the requirements for specification and installation of Logic Solvers and associated support systems, and defining requirements for each SIF or associated function that is implemented within the SIS.

7 SIS Section

Figure 2 shows a SIS Section data entry view. The SIS section contains IEC/ISA required data fields 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.

- General Data – This tab contains data fields to define the SIS ID, Description, Location, Manufacturer, Scope of Application, 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 HMIs 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 procedures and design documentation.
- Printout – This tab presents a complete view of the SRS for viewing printout.



SIS Basic Data for FCCU-SIF-001: FCCU and Waste Heat Boiler SIS

FCCU and Waste Heat Boiler SIS

SIS General

Site: BEV-HIL-REF
Unit: FCCU
SIS ID*: FCCU-SIF-001
SIS Description*: FCCU and Waste Heat Boiler SIS
Regulatory Requirements*: OSHA 1910.110, ISA 84.00.01-2004
SIS Location*: DCS Shelter
SIS Type*: 2 Processors - 2oo2D
SIS Manufacturer*: Triconex
SIS Manufacturer Other: N/A
SIS Model*: Version 10
SIS Scope*: FCCU Unit only. There shall not be functions from other units incorporated.

SIS Operating Modes

Process Description*: The Fluid Catalytic Cracking Unit 600 cracks heavy feed from crude units into smaller hydrocarbons for further refining.
2.1.1 Feed System
The feed system to the FCCU is comprised of 3 major streams:

a. Fresh feed from operating units
b. Cold Gas Oil Feed from tankage
c. Slurry consisting of the Fractionator bottoms recycle

The feed system is comprised of two trains and numerous heat exchangers which utilize BPCS control valves. The preheated streams are combined into a common feed that enters each riser.
2.1.2 Reactor
As the preheated feed enters the risers it comes into contact with regenerated catalyst where it is cracked into more valuable components and sent to the fractionator for separation. The D-1 Disengager's internal cyclones will separate the hydrocarbon vapors from the coke laden catalyst. The D-3 Stripper will remove any remaining hydrocarbons from the catalyst and ensure that it remains fluidized. The spent catalyst is returned to the regenerator where the accumulated coke is burned.
2.1.3 Regenerator
The spent catalyst enters the regenerator through the spent catalyst standpipes. It is then combined with combustion air to burn off the remaining coke. Combustion products are separated from the catalyst in the regenerator cyclones. The flue gas is sent to the Waste Heat Recovery Unit (WHRU).
2.1.4 Flue Gas System
Flue gas from the regenerator is sent to the WHRU to create steam for use in other areas of the refinery. The flue gas is sent to the electrostatic precipitators (ESP) where any remaining particulates are removed from the stream. A scrubber is then used to reduce the NOx emissions of the flue gas.
2.1.5 Fractionator
The fractionation tower is a mult-tray tray distillation tower that separates the various cracked hydrocarbon vapors. The hydrocarbon vapors from the reactor are cooled and condensed in the fractionation tower by reflux and pump around streams. The condensed liquids are drawn off from the middle and bottom while the remaining vapors are drawn off the overhead of the tower.

Process Mode: Startup*: The following steps represent a high level startup sequence for the Regenerator and Reactor of the FCCU.
Cold Start;
1. Pressure test System
2. Power up Air Heater local panel, Air Heater SIS Active
3. Light Air Heater Burner
4. Refractory Curing
5. Load Catalyst
6. Go to Hot Startup

Hot Startup
1. Combustion Air to Regenerator
2. Bring SIS Out of Bypass Mode
3. Torch Oil to regenerator
4. Catalyst Circulation
5. Riser Temps at ~1000 F
6. Introduce feed one riser at a time
7. SIFs Low Feed Trip SIF (FCC-SIF-06 and FCC-SIF07
become Normal
8. Waste gas boilers operational
9. ESP operational
10. Introduce carrier air into the spent cat lines to regenerator
11. Introduce supplemental oxygen to the Regenerator FCC SIF-13-1, -2, - become Normal as required

Process Mode: Normal*: During normal operation, process conditions are stable with catalyst circulation, temperatures, pressures, levels and feed rates held at nominal values, adjusted as required to maintain unit economic objectives.

Process Mode: Shutdown*: Process shutdown operations are a sequence of operations intended to safely bring the unit to conditions that allow for securing of equipment. Shutdown operations are started by reducing unit feeds to minimum values, and then removing feed after stable minimum operation has be achieved. Once feed has been removed, catalyst circulation is stopped to the risers and all spent catalyst is sent to the regenerator and all slide valves are closed. Torch oil is introduced if necessary to assure complete regeneration of catalyst.

During this operation, operation of the main fractionator is stabilized with minimum circulation and then shutdown of all circulating streams.

Once catalyst regeneration has been completed, catalyst off loading to catalyst storage is started using air from the air blowers. When catalyst inventory reaches the minimum, the air blowers are shut down and secured. The main fractionator is depressured and the wet gas compressors shut down. Unit pump out operations then commence.

One all liquid inventory has been removed, the pressure vessels are purged and prepared for entry.

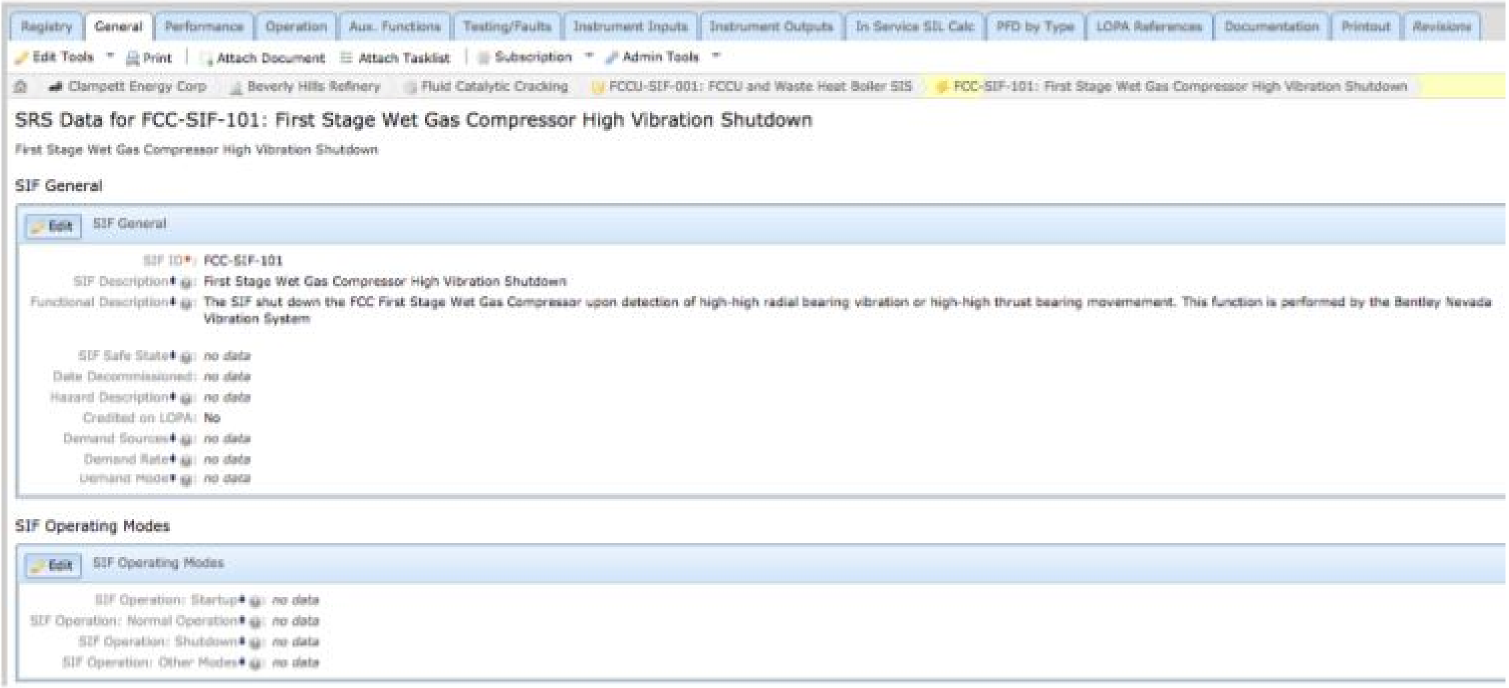
Process Mode: Other*: The FCC may be operated in a single riser mode feed being removed from one of the risers and catalyst circulation minimized with lift steam added to the riser to maintain fluidization.

Figure 2: SIS data for SRS

8 SIF Section

The second and subsequent sections address requirements for each SIF implemented in the SIS. The SIF Section, as shown in Figure 3, contains data fields to define information required by IEC/ISA for the SIS, as well as key robustness and maintainability data for each SIF. This section consists of multiple tabs, each of which covers a required topic.

- 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, including Target and Achieved, Process Safety Time, SIF response times for Inputs, Logic Solver, and Outputs, Trip Points and Basis, Spurious Trip requirements and achieved rates, and 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 SIFs during startup or other operations.
- Testing/Faults – The Testing/Fault tab provides data fields for the description of SIF behavior upon detection of SIS or 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 include 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 – The Documentation tab contains data fields for identification and/or attachment of reference documentation, such as procedures and design documentation. Where the database does not contain links to LOPA or HAZOP scenarios, the applicable sections of these studies may be attached or referenced.
- Printout – The Printout tab presents a complete view of the SRS for printout viewing.



SRS Data for FCC-SIF-101: First Stage Wet Gas Compressor High Vibration Shutdown

First Stage Wet Gas Compressor High Vibration Shutdown

SIF General

SIF General

SIF ID*:	FCC-SIF-101
SIF Description:	First Stage Wet Gas Compressor High Vibration Shutdown
Functional Description:	The SIF shut down the FCC First Stage Wet Gas Compressor upon detection of high-high radial bearing vibration or high-high thrust bearing movemement. This function is performed by the Bentley Nevada Vibration System
SIF Safe State:	no data
Date Decommissioned:	no data
Hazard Description:	no data
Credited on LOPA:	No
Demand Sources:	no data
Demand Rate:	no data
Demand Mode:	no data

SIF Operating Modes

SIF Operating Modes

SIF Operation: Startup:	no data
SIF Operation: Normal Operation:	no data
SIF Operation: Shutdown:	no data
SIF Operation: Other Modes:	no data

Figure 3: SIF data for SRS

9 Non-SIF Functions Implemented in the SIS

A Data-Driven SRS can also be used to document the Non-SIF functions, such as Interlocks that are implemented in the SIS. Basic data for each Interlock or Function, such as ID, Service Description, Functional Requirements, etc., can be defined and automatically included in the SRS. Typically, the number of data fields required to describe an Interlock or other Non-SIF function are substantially less than required for a SIF.

10 Conclusions

The above discussions provide significant evidence that the Processing Industry in general has significant challenges in delivering SRSs that meet the requirements of IEC 61511/ISA 84.00.01-2004. The SRSs produced do not meet the objectives for a SRS, and the gaps observed are common and wide spread.

Furthermore, development of the SRS's has not been efficient or effective, nor have they been completed in a timely manner. This has led to multiple substantial cases of SIS design rework being required with SIS costs and impact upon schedule being far more than is necessary.

One method of addressing these issues is to use a Data-Driven SRS to drastically reduce SRS development time and costs, while assuring consistency, effectiveness, and completeness of the SRS. The result is that the SRS is complete and timely, and detailed SIS design can be performed efficiently with high rework costs avoided.

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

11 References

(1) – Out of Control: Why control systems go wrong and how to prevent failure UK Health and Safety Executive, 1995

(2) – IEC 61511 ed.2. When and What. Heidi Fulgum and Cato Bratt, 11th TÜV Rheinland Symposium, May 13-14, 2014, Cologne, Germany

***Rick Stanley** has over 40 years' experience in Process Control Systems and Process Safety Systems with 32 years spent at ARCO and BP in execution of major projects, corporate standards and plant operation and maintenance. Since retiring from BP in 2010, Rick has consulted with Mangan Software Solutions (MSS) on the development and use of MSS' ProSys SLM Safety Lifecycle Management software and has performed numerous Functional Safety Assessments for both existing and new SISs. Rick has a BS in Chemical Engineering from the University of California, Santa Barbara and is a registered Professional Control Systems Engineer in California and Colorado. Rick has served as a member and chairman of both the API Subcommittee for Pressure Relieving Systems and the API Subcommittee on Instrumentation and Control Systems.*