MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

20th Annual International Symposium
October 24-26, 2017 • College Station, Texas

I thought I had the right roadmap for implementing a safety system; help!

Simon Lucchini*
Fluor Canada Ltd
Control Systems Department
55 Sunpark Plaza SE
Calgary, Alberta T2X 3R4, Canada
* Presenter E-mail: simon.lucchini@fluor.com

Abstract

International standards IEC 61511 and IEC 61508 provide guidance for the safety system life-cycle phases. Armed with this knowledge, the safety design engineer may feel that he/she can tackle any project. However, the scope of a safety system project can vary considerably. The SIS may be part of a new multibillion dollar process plant, a facility revamp or just involve the addition of a few safety functions to an existing installation. Even though the basic steps may be similar, the execution will vary considerably depending on the overall scope and makeup of the project.

Furthermore, the overall project schedule and resourcing are most often governed by scope other than the safety system. A large project may take four to seven years from conception to startup. Essentially, the safety engineer has to navigate many interfaces in order to formulate a solid SIS design basis (i.e., the safety requirements specification). It is important to understand the complexity that arises from these interfaces since they need careful management.

We need to understand how a project works, what are the critical interfaces for the safety system and when to make timely decisions.

Introduction

IEC 61511 (Figure 7 and Table 2) and IEC 61508 Part 1 (Figure 2 and Table 1) provide guidance for implementing the SIS safety life-cycle phases. However, the execution will vary considerably depending on the overall scope and makeup of the project, even though the basic

steps will be similar in concept. To this point, the standard qualifies the safety life cycle with the following caveat:

“NOTE 1 The overall approach of the IEC 61511 series is shown in Figure 7. It can be stressed that this approach is for illustration and is only meant to indicate the typical SIS safety life-cycle activities from initial conception through decommissioning.”

The overall project schedule and resourcing is most often governed by scope other than the safety system. A large project for a process plant may take four to seven years from conception to startup. The overall control systems content ranges from 8% to 12% of total installed cost (TIC). The safety system may be less than 10% to 20% of the control systems budget (i.e. approximately 1% to 2% of TIC). Engineering content may be less than 6% of TIC (i.e. safety system engineering may be as little as 0.06% of TIC). In other words, the main engineering effort is not focused on the safety system.

There are various project execution elements that can further complicate the design and implementation of a safety system. Some of these include:

- Modularization and distributed the safety systems (e.g., truckable modules to VLM; very large modules)
- Process licensor packages and their specific safety requirements (e.g., polyproplene reactor, Hydrocracker, Coker unit, liquefied natural gas process & many more)
- Mechanical vendor packages with their diverse designs and code requirements (e.g., compressors, fired heaters, water treatment)
- Multiple engineering contractors covering various plant units, depending on the overall plant scope split
- Varying design practices and procedures from the end-user, process licensors and engineering contractors

On large projects, the controls automation scope is often undertaken by a separate company from the main engineering contractors who are responsible for the overall design of the plant units. The automation company may be the DCS & SIS vendor(s) or a 3rd party systems integrator. Hence, there will be a number of groups, including the process licensors, who have an interest in the implementation of the safety system(s).

Thrown into this mix are the end-user standards and specifications. These may not exactly align with the project execution practices of the various engineering companies, process licensors and other automation parties. Essentially, the safety engineers have to navigate many interfaces in order to formulate a coherent safety requirements specification (SRS). It is important to understand the complexity that arises from these interfaces. They need careful management. Complexity can be considered as proportional to two to the power N, where N is the number of interfaces ($C=2^{\wedge N}$). This is not a recognized equation found in the text

books. However, the author has found this a useful model to explain to others how quickly things can get out of hand!

Finally the safety engineer may not yet be on the project when the initial hazard analysis and/or layer of protection analysis (LOPA) are undertaken. It is often the control systems lead who will have to setup systems to take into account the safety life-cycle and establish the safety plan. Hence in many respects this paper is dedicated to those who have to ensure that the work process will support functional safety, well before the safety system specialists are actually assigned to the project.

So what can be done to ensure that the Project adheres to the fundamental tenants espoused in the standards for the safety life cycle?

Aligning the safety plan with the project execution

IEC 61511 Clause 5.2.4 requires that safety planning is carried out in order to follow the safety life cycle. Quite rightly, the standards do not give details on how to accomplish this task. This paper provides suggestions as how safety planning is accomplished and why one would want to do this work. These suggestions are not meant to be the only way this can be done. There are too many project variables to provide a "one answer fits all" solution. Readers will need to adapt the following suggestions to their particular application.

As previously introduced, the scope of control systems generally and safety systems specifically are relatively small compared to other activities on a project. However, the proper design of the controls and safety systems are crucial in the successful and safe commissioning of a facility, way beyond their contribution to TIC. The Project may not fully appreciate this at the beginning, but certainly does at the latter phases. There are final safety sign-offs required to begin the startup of the facility. A thoroughly tested and pre-commissioned safety system is a key element for this sign-off.

What is a project?

A project is simply a scope of work to be accomplished subject to schedule, cost and performance criteria. This is usually covered in a formal contract. The scope includes the physical facilities plus services that range from engineering studies to financial and procurement activities. The important words are scope, priority and schedule (i.e., what are the key things that need to be done first). This paper will be unabashedly using project execution terms and practices. How else are we going to get the job done?

Project terms and definitions

It is important to set out the safety life-cycle in project terms and to understand the key project milestones that affect the implementation of the safety systems. The first step is to understand some key terms used on project, particularly with respect to schedule.

The terms and definitions below are by no means complete and universal. The author has seen a project definitions document that is more than 20 pages long.

Contract (or Prime Contract): The prime contract is a legal document and is sometimes called the main client. It basically defines the agreed scope of work together with specifications and project execution requirements. The contract may be lump sum, lump sum turn-key, cost reimbursable or other hybrid forms. This is an important document for everyone on the project to review for their scope.

Detailed Engineering: The phase of engineering follows FEED (or basic engineering) and starts after financial approval has been given for the project.

Design Basis Memorandum (DBM): This is the conceptual phase where basic process requirements are established in readiness for the FEED stage. Sometimes called FEL 2 or Concept phase .

Front End Engineering & Design: Is the project phase, prior to project approval, which defines project details to minimize uncertainty during execution. FEED includes authorization for expenditure (AFE) quality cost and schedule estimates along with a detailed project scope of work and project execution plan. A risk assessment during this phase identifies HSE, technical, cost and schedule risks that should be mitigated or managed. Sometimes FEED is called front end loading 3 (FEL3) or front end design 3 (FED 3). However, these different execution models are not completely synonymous. There can be overlap between project phases between one execution model and another.

Project Gate: A framework to examine the transition between specific project phases (e.g., from FEL 2 to FEL 3) for compliance to process and company standards and to make comments or approve as required. Most, if not all, projects have rigorous gate requirements for the approval of finances to release the project to the next phase.

Hazard Identification: Process to identify and define the nature of hazards that exist in a process plant (e.g., refinery, boiler, reactor, chemical process, etc). These hazards may be controlled by inherent process design, instrumented systems and/or mechanical devices, operating procedures, etc. IEC61508 & IEC61511 define the use of these independent protection layers (IPL) in relation to Safety Instrumented Systems (SIS)

Hazard Register: Is a central list of HSE-related issues and concerns which require resolution. This will typically include PHA / HAZOP action items plus any recommendations from other reviews (e.g., spacing analysis, consequence models, etc.)

HAZOP: HAZOP is a systematic technique for identifying hazards and operability problems using guide words. The plant is broken down into nodes in order to focus the work. Projects sometimes use the term HAZOP in place of PHA, even if strictly this is not correct.

Management Level Schedule (Level 1): This schedule is at a very high level with major functions and milestones. Even for major projects this would be at most 1 to 2 pages.

Other Schedules: There are other even more detailed schedules (e.g., Level 4 individual discipline & 5 construction, maintenance, turnaround)

Other studies: Studies such as Safety Desktop, "What If?" and other critical examinations are less formally structured but may be more suited to the particular stage of the project. Failure Modes and Effects Analysis (variants with diagnostics & criticality) are more similar to "What If? than to HAZOP.

PFD: Process Flow Diagrams are developed at the conceptual design stage and show the functionality of the process operations. They often contain material flow balances but only show a few key instruments. PFD are useful for understanding the process and interactions in the process.

P&ID: Piping and instrument drawings are the key design documents for any process facility and are under management of change after they have been subjected to HAZOP. These drawings include the complete process piping and vessel design together with the controls, interlock and safety systems. The term process & instrument drawings is sometimes used.

P&ID Review/Study: This activity is a detailed design review of the P&ID prior to the PHA. An important part of this review is to ensure that the controls and safety designs are valid. Other areas of review include verifying the relief and blow down specifications are properly captured on the P&IDs.

Process Hazard Analysis(PHA): A systematic approach to identify, evaluate, and control hazards in processes that could endanger personnel, the environment, the public, or equipment. HAZOP is one type of PHA. The issuance of the PHA implementation specification is a key project milestone.

Project Level Schedule (Level 2): It is a medium detail schedule showing activities and deliverables for engineering, procurement, construction and commissioning. It also shows the critical path and key milestones. This is also known as an area master schedule

Project Level Schedule (Level 3): Fully integrated schedule showing all milestones and critical path and is resource loaded. This can run into several hundred pages. This is also known as a control level schedule.

Project Milestone or Milestone: These are key accomplishments or decision points on the project schedule. Examples include authorization for project expenditure, HAZOP issue P&ID and mechanical completion.

RACI Matrix: Stands for responsibility, accountable, consult and inform. It is a means of defining scope for a task, or series of tasks, together with assigning roles and responsibilities. Many problems can be readily avoided if a RACI matrix is developed and reviewed with key stakeholders early in the project.

There is always just one entity that is accountable for a task/deliverable. Accountable is more like a management/leadership role and does not mean actually performing the task (e.g., engineering manager for automation). There may be several entities who are responsible for performing the task (e.g., HSE professional and functional safety engineer devising the risk tolerance criteria). An entity that is in the consult category needs to have input into how the task is achieved (e.g., 3rd party LOPA facilitator using the risk tolerance criteria). An entity in the inform category just needs the information to perform their subsequent tasks (e.g., SIL verification engineer needing to know what is the client approved SIS) .

Safety integrity level (SIL) allocation/determination: Means of determining the required risk reduction for the safety functions shown on the P&ID. There are a number of available techniques. The methodology used by the Project is typically encompassed in the PHA implementation specification

Key elements of the safety plan for a project

For any project, the most important outcome from the safety plan is to produce the SRS on schedule. This cannot be emphasized enough. Most (if not all) concerns on a project are readily solvable if identified early enough (i.e., in the correct sequence). This means that the safety plan needs to be established fairly early in the FEED phase of the project.

The reader may be surprised by the number of different parties involved in the safety plan, as detailed in the following sections. It is not until the latter stages that the functional safety engineer takes the lead role. This highlights the fundamental problem with designing a SIS. It comes at the tail- end of a complex hazard identification process whose primary role from a project perspective is to issue approved for design P&ID drawings. Safety instrumented functions are there to “clean up” what cannot be done otherwise by the other layers of protection. The development and HAZOP of the P&ID drawings covers an extremely large scope, covering everything from piping and vessel design, machinery configuration, relief and blow-down, isolation design, controls, operational requirements and finally interlock and trip functions.

Waiting passively for the requirements to flow through the project process the information may not be adequate for the task of defining/designing the SIS. The functional safety engineer and/or the lead control engineer should actively ensure that an effective safety plan is in place on the project in time to capture the data required for designing the safety system. It is critical that key elements of the safety plan are included in the project level 3 schedule. There is merit for including the issuance of the safety plan as a milestone in the project level

2 schedule where it would receive project and client management attention. It should be noted that only very high level activities and deliverables are normally accepted for level 2 schedules.

P&ID design review (SIS groups)

The lead process engineer should confirm the methodology for reviewing SIS groups during the P&ID reviews, in preparation for PHA. This activity will support the development of cause & effect drawings, shutdown keys, etc which are commonly used in the development of the SIS application logic.

Key interfaces disciplines include HSE/risk management, process licensor, lead control systems engineer and functional safety engineer.

Establish PHA Procedure

HSE/risk management should issue the PHA process and guidelines. This process will be followed to identify hazards and potential SIFs. The plan should also include preliminary PHA reviews and assessment of mechanical package safety systems.

Key interfaces include the process licensor, end-user, lead process engineer and functional safety engineer.

Define project risk criteria & SIL allocation procedure

HSE/risk management should obtain and review tolerable risk criteria & acceptable spurious trip rate (STR) data and risk ranking methodology applicable to the facility from the end-user.

Under normal circumstances the HSE/risk management group would receive this from the appropriate client organization. This information usually includes the SIL allocation methodology.

Plant operating narrative & safeguarding philosophy

The SIS design needs to include the plant equipment design requirements for operational availability , planned maintenance shutdown/turnaround periods and bypass philosophy. The lead process engineer should confirm this information at an early stage of design. Development of this philosophy would be required for the PHA, SIL allocation and the SRS.

Key interfaces include the process licensor, end-user , lead control systems engineer and functional safety engineer.

Code requirements and specialty systems

The functional safety engineer should review SIS implementation philosophy for high integrity pressure protection systems (HIPPS) and burner management systems (BMS). This work should consider end-user operating standards and requirements of the local authorities having jurisdiction.

Key interfaces include the process licensor, lead process engineer, end-user , lead control systems engineer and fired heater mechanical engineer.

Establish safety requirements specification

This is the fundamental document used to collect information about and hence define the SIS. The function safety engineer should develop an agreed format for the SRS. This ensures that important inputs to the SIS design from the disciplines are received in a timely manner.

Hazop reports, SIL assignments for each SIF, plant operating narratives, safeguarding philosophy, cause & effect drawings and range, alarm & trip Lists together with the SIS narratives are crucial elements to support the SRS.

Key interfaces include HSE/risk management, process licensor, lead process engineer, end-user, lead control systems engineer and lead mechanical engineer.

Device Failure Data

The functional safety engineer should ensure that SIS certification data for procured instruments is obtained (e.g., SIL certificates, relevant end-user “proven in use” device data, safety assessment reports & safety manuals, generic industry data).

Functional safety engineer should also validate device selection against end-user approved vendor list. Furthermore, he/she should confirm that use of diagnostics (e.g., partial stroke testing, external comparison) is in accordance with operations and maintenance procedures.

Key interfaces include process licensor, end-user, lead control systems engineer and mechanical engineer for package equipment (e.g., compressors and fired heaters).

SIL verification

The functional safety engineer should confirm SIL verification methodology including process interface implications for the instrumentation and end-user acceptable calculation software. Constraints in relation to availability of the plant for offline proof testing (i.e., plant turn-around period) should also be identified.

Key interfaces include process licensor, end-user, lead control systems engineer and lead process engineer.

Who is involved in the safety plan?

Since there are so many interface parties the overall accountability for the safety plan would be best placed with project engineering, or equivalent, with strong support by the functional safety engineer. The responsibility for the actual details would be with the specific disciplines as detailed in the RACI matrix.

The parties who have interests in the safety plan include:

- Project engineering/engineering management
- Control systems
- Functional safety engineering(often part of control systems)
- SIS engineering (may be the same as the BPCS engineering)
- BPCS engineering (basic process control systems)
- HSE/risk management
- Process engineering
- Fire & Gas protection engineering
- Mechanical engineering (for mechanical vendor packages; may be skid packages or entire modules)
- End-user management
- End-user operations and maintenance
- End-user HSE/risk management
- End-user project management contractor (PMC)
- Process licensors
- SIS vendor and/or 3rd party system integrator

The assignment of scope and responsibilities can be done in variety of ways and is highly dependent on how the project and contract(s) are set up. The design of large facilities are often split over multiple engineering contractors and would by necessity include a project management contractor and/or end-user engineering contractor. The safety plan, previously mentioned, would need to be adapted in conjunction with the RACI matrix. Some considerations include:

- Split of responsibilities for SIL verification between the engineering contractors and the SIS vendor and/or 3rd party system integrator
- Use of standard designs and safety functions for mechanical packages (e.g., turbo machinery and large compressors)
- Alignment with process licensor required safety function designs that are often required for the performance guarantees

We have a Safety Plan and a RACI Matrix, now what?

As always, for a project it is all about timing and the schedule. Special attention should be given to the following items to ensure a sound safety system basis of design. Special

attention means making decisions at an early enough point in the schedule so as to make a difference!

Mechanical Packages

During the FEED phase of a project most attention is focused on devising a basis for detailed engineering. The level of activity is greatest for process engineering. By the end of FEED the bulk of their work should be done. However, there is also the need for early procurement of mechanical packages due to the extremely long delivery schedules (e.g., large compressors, major vessels and reactors, fired equipment). These packages are invariably on the critical path on the project Level 2 schedule. This means that the mechanical discipline is also engaged early onto the project at a time before the controls and instrumentation group are be fully resourced.

The significance for the controls discipline is the ever increasing number of I/O (BPCS and SIS inputs and outputs) associated with large mechanical packages. This could account for 40% to 60% of all BPCS and SIS I/O, depending on the facility design.

It is worthwhile pausing and considering the implications of this trend for pre-engineered mechanical packages.

Who is going to include the functional safety requirements for the mechanical package purchase orders? Again, this is an item to include in the safety plan right at the beginning of the project.

Details that should be considered when reviewing the design approach for the safety system associated with mechanical packages include:

- Many mechanical package controls and safety functions utilize long established designs. The design comes as part of the “catalogue” and there is a reluctance to change. The package may combine control and safety functions. Does this meet project requirements for SIL allocation?
- Measurement technology may be different to what is selected for the project. Are there issues with acquiring valid reliability data for the chosen instrumentation? Does it meet prior use requirements?
- The mechanical engineering package will often not be available for the HAZOP/PHA undertaken in FEED. How is this accounted for in the schedule for the SRS?
- A mechanical package needs to be connected/interfaced to the main facility. Are the control, interlock and trip design available to complete the SRS in a timely manner?

The above considerations should lead to appropriate functional safety requirements being included in the procurement specification for mechanical packages before the purchase enquiry is issued. Again the pressure will be on the delivery schedule of these large

mechanical packages. Changing requirements mid course after the design has commenced will incur delays. Project directors are not prone to forgiveness when the startup of a multi-billion dollar facility is under threat, particularly when a proper plan would have avoided the problem.

Process Licensors

Process licensors come in a variety of forms. They have a patented process technology that they license to end users (i.e., not licensed to the engineering contractors). Examples can vary from chemical plants (e.g., methanol, sulphuric acid, polypropylene, coke gasification) to refinery processes (e.g., LNG, cokers, hydrocrackers, LC Finers, hydrotreaters). Some process licensors may own and operate facilities as well.

The performance guarantees (i.e. plant throughput, product quality, energy efficiency, risk profile, etc) often places constraints on the engineering design . The licensor will issue design requirements to the engineering design via the end user in order to provide the "guarantee". These requirements may also affect the safety system design:

- Instrument technology and architectures (e.g., 2oo3 orifice flow)
- On/off trip valve technology (e.g., brand and model)
- SIF proof testing requirements
- BPCS to SIS interface configurations
- Risk tolerance criteria

The level of freedom for the design development will depend considerably with the chosen process licensor. Hence, it is crucial that the functional safety engineer reviews the process licensor package and include applicable constraints in the SRS. Any misalignment with the overall project approach to the safety design would need to be identified and resolved in a timely manner. As an example, partial stroke testing may not be compatible with the licensor design but may be required in the SIF design in order to achieve the needed risk reduction factor.

Once again the early identification of potential conflicts between the licensor and project design is key to a successful safety systems design.

Getting setup for SIL verification

So far, the main focus has been about establishing an effective safety plan. This supports a complete and comprehensible SRS which is aligned with the functional requirements of all the interested parties.

The other part of the safety equation relates to the integrity requirements.

We have the risk reductions targets and SIL from the LOPA report, we have the equations from the standards and we have great software. What else do we need to know to finish this project?

Once again, the answer is concerned with getting agreement on key SIL verification parameters at the appropriate time in the schedule and with the same parties as before.

The recommended approach is to formally issue a SIL verification implementation guideline. This ensures that the project provides SIL verification in a consistent and predictable manner. Elements of this guideline would include approved:

- Reliability data sources (e.g., standard industry generic data, vendor safety manual FMEDA data, 3rd party assessment, etc)
- Diagnostic coverage and techniques (e.g., external measurement comparison, partial stroke testing)
- Process safety time design margins
- Proof test intervals and proof test coverage assessments per instrument type
- Repair times and maintenance factors per instrument type
- Useful life per instrument type and per process stream type
- Other miscellaneous factors used in the SIL verification calculation (e.g., offline or online proof testing, tripping on diagnostic failures or not, automatic or manual initiation of partial stroke testing, etc)

Authorities Having Jurisdiction

There are certain types of safety systems that are covered by prescriptive legislation. Examples include:

- HIPPS, high integrity pressure protection systems
- BMS, burner management systems
- Boilers
- Pipeline pressure protection

The requirements for these systems can vary considerably according to region. The main message is that the safety plan needs to take into account the specific requirements of the regulators. It would seem to be a common sense suggestion but the advice is really about identifying requirements early.

As an example, the author is familiar with one region where the authority having jurisdictions require all HIPPS to be designed to SIL 3. This is irrespective of what the SIL allocation study has determined. This “late” requirement may require the installation of additional trip valves at a time when the piping layout design has been completed and issued to the fabricator.

Smaller projects

Smaller projects have their own difficulties. Whilst there may be fewer interfaces the available specialist resources may not be as readily available.

However the concept of getting a safety plan in place early in the schedule is the same. It will not be as complicated as for the large project but it is still needed to ensure a smooth transition from design to commissioning.

Summary

The proper design of the safety system is dependent on the safety plan, SRS and SIL verification guideline being in place early in the project schedule. There are many parties involved in defining these requirements. Getting alignment in a timely manner requires considerable focus. However, this effort will ensure that the detailed engineering work runs smoothly (e.g., SIL verification)

This paper has explored the important elements of the safety plan, who are the key interested parties, where things can go wrong and what can be done to get the complete SRS. In particular, this paper has considered the importance of alignment on requirements with the process licensors and the mechanical package vendors.

References

1. IEC 61511-1 Edition 2.0: 2016, Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements, IEC Central Office 3, rue de Varembé CH-1211 Geneva 20, Switzerland
2. Construction Industry Institute (CII). Home page accessed May 27, 2017. https://www.construction-institute.org/
3. Back to the Future: Why are we doing this HAZOP?, Simon Lucchini, Chief Controls Specialist & Fluor Global Fellow in Safety Systems Design, Fluor Canada, Mary K O'Connor Process Safety Center International Symposium, 2012,College Station, Texas, USA,