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

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Process Safety Time Analysis for Upstream Facilities

Anupa Beharrysingh, M. Hernandez, C. Ng, C. Maher
Fluor Cooperation,
Sugar Land, TX, 77478.
Emails: anupa.beharrysingh@fluor.com, manuel.hernandez@fluor.com

Keywords: Process Safety Time, Upstream, Safety Instrumented Function

Abstract

Per IEC 61511-1 Process Safety Time is defined as, "the time period between a failure occurring in the process or the basic process control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the safety instrumented function is not performed".

This paper will discuss how Process Safety Times were categorized, evaluated, and verified in order to comply with the standard and on a upstream mega project containing over 580 Safety Instrumented Functions, 350 of which were rated SIL 1 or higher.

In the past, the practice has been to assign general overall values to Process Safety Times, many times for an entire project or possibly for individual units in a process facility. On our recent mega project, our client challenged the engineering team to develop more customized values based on individual processes. Our expectation is that in the future this expectation will grow more stringent and focused. Our control systems and process engineering teams will have to work together to develop the necessary work processes and methods to generate, justify, and report these critical time values.

Definitions

Per IEC 61511 Part 1 Section 3.2.52.1, Process Safety Time is defined as, “the time period between a failure occurring in the process or the basic process control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the safety instrumented function is not performed”.

Per IEC 61508-4, Section 3.6.20, Process Safety Time is the period of time between a failure, that has the potential to give rise to a hazardous event, occurring in the EUC or EUC control system and the time by which action has to be completed in the EUC to prevent the hazardous event occurring.

Therefore, Process Safety Time is essentially; the time from an initiating event to the occurrence of an incident.

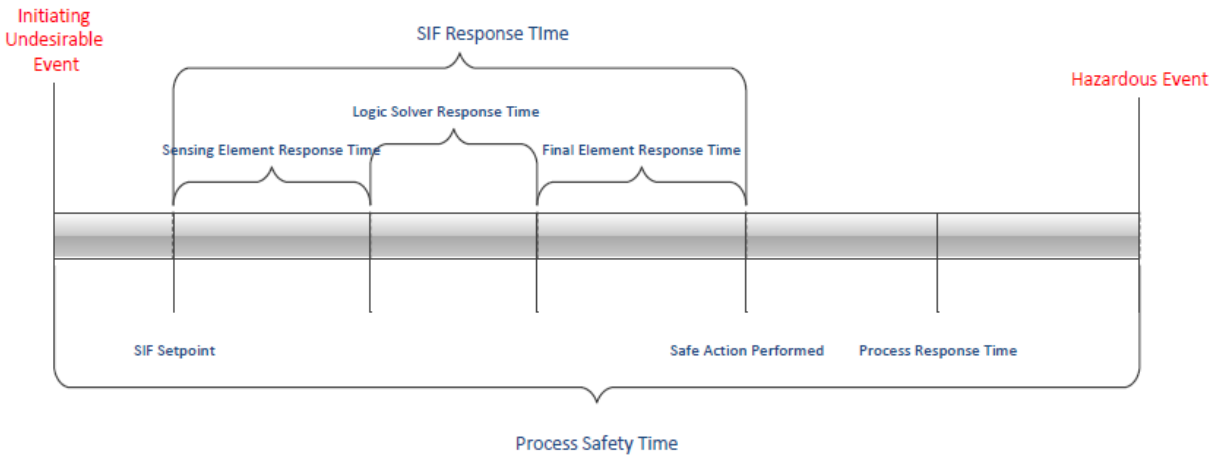

Figure 1.0: Process Safety Time Timeline

IEC 61511-1 Section 3.2.57 defines a protection layer as, “any independent mechanism that reduces risk by control, prevention or mitigation.” The intent of Process Safety Time, PST analysis is to ensure that the SIS protection layer is successful at preventing the imminent hazard.

IEC 61511-1 Section 10.3.2 states the following as a SIS safety requirement: “response time requirements for each SIF to bring the process to a safe state within the Process Safety Time.”

The response time for a SIF will be from detection at the sensor to completion of the final element action. After the final elements have completed their actions, there is a time for the process to respond to the actions before reaching a safe state. This is referred to as the Process Response Time.

The project was committed to demonstrate compliance with IEC 61511-1, Section 10.3.2.

For the assurance of a safe design as well as for compliance with the IEC standard, SIF-RT and PRT as well as safety margins are all considered and summed to ensure that the SIF reacts within the PST.

Process Safety Times are required to be considered for all independent protection layers, not only for safety instrumented functions. When considering the implementation of an alarm, for example, there must be an associated expected time frame in which an operator response or intervention to the alarm is required in order for it to be effective. Similarly with PSVs, these devices are sized and set at a pressure to allow mitigation of system over-pressure / rupture.

The analysis this paper will discuss focuses on Process Safety Times applicable for safety instrumented functions.

PST for a SIF is required to be defined / provided in the project's Safety Requirements Specification, but little direction is provided on how it should be assessed.

Roles and Responsibilities

On a project, PST analysis is a joint effort among a number of responsible parties. These include the client, who will assume ownership and ultimate responsibility for the safe operation of the facility; the General Contractor, who has responsibility for the safe design of systems for the facility; the Main Automation Contractor, who has responsibility for implementation of control and safety related items; and, on occasion, third party vendors who supply packaged systems for the project.

The Client will supply or approve project specifications to be used by the General Contractor, and others, in the development and design of the facility. The Client may have a core group that directs and coordinates project activities on a wide range of projects and may participate in development of and/or approve Process Safety Times developed by an individual project. The client may also supply discipline engineers to oversee specific projects on an ongoing basis. The assigned client engineers may include a control systems engineer and a process/facility engineer. Additionally, client operations personnel from a specific facility may participate in the review and approval of Process Safety Times based on actual facility operating experience.

The General Contractor will bear the overall responsibility for development of a Safety Requirements Specification and for the establishment of Process Safety Times on a project working with an inter-discipline team of process, control systems, and mechanical engineers.

The MAC is tasked with implementation of the Process Safety Times in the MAC supplied hardware, configuration, and programming based on project supplied design documents. Software Acceptance Testing will demonstrate that the required Process Safety Times in the configuration and programming align the provided design documents.

Third party vendor documents will be consulted and evaluated as required to ensure that any Process Safety Time associated with a third party vendor package is capable of meeting the required Process Safety Time.

Project Methodology

After HAZOP, LOPA and SIL assignments for the project were completed, the resulting number of SIFs were 580, 350 of which were rated SIL 1 or higher. Given the number of SIFs which required PST evaluation and the schedule for confirming / finalizing process limits and set-points, the project was tasked with developing a method of PST evaluation to identify and

mitigate any deficiency finding within the project timeframe while still complying with the IEC 61511 standard.

The general practice in the past regarding evaluation or Process Safety Time has been based on generally assigning a maximum operating time for shutdown valves. A project might set a value to cover all shutdown valves regardless of size or process, or there may be varying values established on valve size, with larger valves being assigned a longer operating time than smaller valves. Once these times were established it was up to control systems engineering personnel to specify the correct shutdown valves and auxiliary equipment necessary to meet the established operating times. This might mean having to procure a quick exhaust solenoid valve to allow the valve to move to its safe position in the specified time frame.

As the Process Safety Time practice evolved, process engineers based the times on a system response to process pressure, temperature or level disturbances or upsets.

The project developed a document "Process Safety Time Analysis – Charter" which dictated how the Process Safety Times were to be categorized and evaluated with their associated SIF response time in order to demonstrate compliance.

The document first set the scope boundaries for assessment. All SIFs with a SIL rating of SIL 1 or higher would require PST evaluation. This prioritized the PST assessment and reduced / avoided overloading with non-critical items. Also, no mitigative SIFs would be evaluated (Fire & Gas).

SIFs which were part of a standard vendor supplied package would not be evaluated, as these SIFs would be regarded as 'proven-in-use', provided that the vendor(s) supplied these standard packages for many years and had done their own process safety evaluations.

The document identified the responsible engineering disciplines: Process and Control Systems, where Process engineers were responsible for calculating the Process Safety Times and Control Systems would be responsible for calculating the SIF Response Times.

The document defined the methodology for Process Safety Time evaluation. All SIFs were initially screened and identified as either time critical (PST<60s) or non-time critical (PST>60s). SIFs with a PST>60s underwent a qualitative analysis with a descriptive assessment only. The time critical SIFs (PST<60s) were classified as requiring additional quantitative analysis. This was done based on system configuration and a steady state model.

In each case the hazard cause would be aligned with the cause documented in the HAZOP and SIL assignment reports.

To meet the demands of project schedule and finalize the design, areas of the process were segregated and prioritized for analysis. Process Safety Time analysis would then be performed in order of priority as SIL assignments were completed.

Typical SIF-RTs for each type of sensor, logic solver, and final element were determined and tabulated. These times were then utilized to calculate the overall SIF-RT for each SIF with a SIL assignment greater than or equal to SIL 1.

The end result was a deliverable listing each SIF (with a SIL assignment greater than or equal to SIL 1) along with its associated hazard cause, PST, and SIF-RT.

Process Safety Time Analysis Evaluations

PST calculations took into consideration design tolerances (short term temperature or pressure excursions) allowed by ASME / API codes. Pressure excursions were modeled / analyzed to the PSV set-point. This served to validate the SIS and the physical pressure relief as an independent protection layer.

Of note, low pressure trips are typically used to mitigate against line ruptures or leaks (loss of containment scenarios). In these cases, as the hazardous event has already occurred, no Process Safety Time analysis was done on low pressure safety instrumented functions.

Process Safety Time calculations involving level measurement took into account overflow at full flow rates for HiHi trips and underflow at zero flow rates for LoLo trips.

For pump and compressor trips, rundown times may need to be considered if they allow for hazard escalation.

Project Considerations

What if the PST is less than the SIF-RT? The project considered the following options in order of cost and timing in effort to mitigate the deficiency.

- Review the PST calculation and the assumptions which contributed to the PST calculation.
- Consider altering the trip set-point of the input sensor; for example, raising the LoLo level set-point can give more liquid volume. Lowering a HiHi pressure set-point will provide more of a pressure cushion before reaching overpressure.
- Consider the addition of a quick exhaust solenoid valve to the actuator. In some instances the main contributing factor to the SIF response time is the closure of a safety shutdown valve. In one instance the project was able to reduce the SIF response time by adding a quick exhaust solenoid to an 8” safety shutdown valve. This addition reduced the final element response time from 8s to 2s.
- Consider the possibility of an additional or alternative IPL to the SIF.
- Re-validate / evaluate LOPA scenario.
- Another alternative and last resort was to consider the addition of logic to prevent or mitigate the cause of the scenario. For example, the PST for overpressure on the production header was calculated to be 1.8s. As commitments for a production rate were already made, altering the HiHi pressure trip set-point was not an option. Per the HAZOP report the initiating cause of the potential overpressure scenario was documented to be the failure of a 30” safety shutdown valve.

An advanced warning for the failure of the 30" safety shutdown valve was considered using the safety shutdown valve limit switches which were wired to the SIS. If the limit switches for the valve read that is was travelling un-commanded by the SIS, then the final elements which were required to go to the safe state as part of the overpressure SIF would actuate. By doing this an advanced warning of the failure of the SDV was essentially created and the SIS was programmed to act in the same manner as if the HiHi pressure on the production header was realized.

Summary

There is a general rule of thumb which suggests that the SIF-RT be less than or equal to half of the Process Safety Time; however, as the PST calculations were done to the PSV set-point and not to the time of occurrence of the unwanted event, this rule of thumb was not applied.

At the end of the exercise, despite PST's as low as 1.8s, the project was able to demonstrate compliance with the IEC 61511 requirement for each SIF with a SIL rating of SIL 1 or more.

The development of this integrity critical document required collaboration from multiple groups: Process and Control Systems engineers, Clients, Mechanical package engineers / vendors, Safety engineers, and Subject Matter Experts.

Safety consideration in the process industry must progress continually to ensure safety of people and the environment. The evolution of the evaluation and implementation of Process Safety Time is an indication of how the industry engages in the process of taking standards and guidelines and developing them into the engineering process and final construction. Putting safety first profits everyone involved from the client, the engineering and construction contractors, the public, and the environment. Operating experience will help refine the process of developing the Process Safety Times for future projects.

Abbreviations

Abbreviation	Description
HAZOP	Hazard and Operability Analysis
EUC	Equipment under control
HiHi	High High
IEC	International Electrotechnical Commission
IPL	Independent Protection Layer
LoLo	Low Low
LOPA	Layer of Protection Analysis
MAC	Main Automation Contractor

Abbreviation	Description
PRT	Process Response Time
PST	Process Safety Time
PSV	Pressure Safety Valve
SDV	Safety Shutdown Valve
SIF	Safety Instrumented Function
SIF-RT	Safety Instrumented Function Response Time
SIL	Safety Integrity Level
SIS	Safety Instrumented System