Determination of Alarm Safety Response Time

Ayo Akintoye, Chief Process Control Engineer, Amec Foster Wheeler, Shinfield Park Reading Berkshire

Steve Harrow, Manager Process Engineering, Amec Foster Wheeler, Shinfield Park Reading Berkshire

In the process industries, alarm systems are used to notify operators and other plant personnel of abnormal process conditions or equipment malfunctions. The alarm system helps operators operate the process safely under normal and abnormal conditions and the alarm system needs to be designed correctly to ensure safe and efficient operation. Alarms play a significant role in maintaining plant safety. They are a means of risk reduction which help prevent harm from process hazards. One of the key requirements in safety instrumented system and alarm management design that is too often given little attention is the process safety time and the expected operator response time to an alarm.

As part of the work process for safety design in Amec Foster Wheeler, a methodology has been developed for calculation and specifying the Process Safety Time (PST) of an alarm. The PST is used to determine the alarm operator response time (one of the criteria required during the identification stage of an alarm lifecycle). It is also used in the calculation of the Safety Instrument Function (SIF) response time as required by IEC 61511 in the preparation of Safety Requirement Specification (SRS) during the functional safety lifecycle.

This paper investigates the role of time in the design of alarm and SIF and it also defines the connection between the process and time using PST as well as describes a methodology used in determining the PST. The method is based on using a dynamic simulation tool to simulate the process behaviour to detect unsafe situations and to support the calculation of the process safety time. The paper highlights how the PST is used in the process alarm identification and rationalisation stages of the alarm lifecycle to ensure the number of alarms of a process unit displayed to an operator are manageable and relevant.

Keywords: Process safety time, dynamic simulation, Safety Instrumented Function, Independent Protective Layers

Introduction

Today, process safety is a key aspect of the design and operation of a process plant. The development of alarm management systems, safety integration systems (SIS) and the identification of possible hazards by process hazard analysis (PHA) techniques, require detailed knowledge of the technology (BS EN 6511- 2004). To be considered effective and functionally adequate the system should be capable of responding to the process demands quickly enough to halt the propagation of the hazard scenario it was designed to protect.

The design of Independent Protection Layers (IPL) such as alarms and SIFs identified when conducting process hazard analyses are critical in safeguarding against process upsets that may harm people, the environment and commercial interest.

Alarms and operator responses to them are one of the first layers of protection preventing a plant upset from escalating into a hazardous event. When an alarm fails as a layer of protection, catastrophic accidents such as Milford Haven (UK), Texas City (USA) and Buncefield (UK) can be the result. At the Buncefield oil depot, a failure of a tank level sensor prevented its associated high level alarm from being annunciated to the operator. As the level in the tank reached its final high level, the second protection layer, an independent safety switch (Safety Instrumentation Function (SIF)) failed to initiate a trip which would have automatically shut off the incoming flow. The tank overflowed and resulted in an explosion costing millions of pounds. While this incident was caused by a combination of equipment failure and human error the need for proper design of an alarm or a SIF cannot be overstated (Buncefield Report – 2008). The goal of an effective alarm is to minimize the frequency and impact of abnormal situations. Each individual alarm is designed to provide an alert when the process indication differs from its normal state. During an abnormal condition, the board operator is confronted with making decisions on numerous tasks that must be performed in the appropriate sequence. The timing and order of execution of these tasks determines the outcome of the operator’s effort to mitigate the incident. To assist the operator in executing these tasks effectively, the design of the process safety time (PST) and operator response time is one of many factors that are to be addressed in the design of an alarm management system and Safety Instrumented System.

The process dynamics determine how quickly a process deviation propagates into a hazardous event. The process dynamics are influenced by the process design, operation, mass and heat transfer, reaction kinetics thermodynamics etc. Understanding the dynamic behaviour of a process is crucial in determining the PST which is the first step in identifying the time potential for all protection layers to respond and will be useful in specifying the required response time of each IPL. Fortunately, the importance of models in safety analysis was recognized in the past decade and dynamic models have been increasingly applied to support the solution of any task related to process safety (Ingram – 2004, Labovsky – 2007). The usage of dynamic models allows the designer to generate the deviations from normal operating conditions and also to simulate and analyse the influence of these deviations and the trajectory of the possible safety responses.

As part of the plant design activities carried out on projects at Amec Foster Wheeler, SIL/LOPA reviews helped to identify the IPLs and their required integrity for a given hazard scenario. One key information/data needed by an IPL to meet certain criteria as advised by industrial standard (BS EN-61511 - 2004), is the PST. This paper investigates the role of time in the design of Independent Protection Layers such as alarms and SIFs and defines the connection between the process and time using PST. An approach based on using a dynamic simulation tool to simulate the process behaviour to detect unsafe situations and to determine the process safety time was used to aid the design of Safety Instrument Function and alarm.

Basis of Design

The protective devices or Independent Protection Layers (IPLs) are critical pieces of armour designed to protect process upsets that harm people, the environment and commercial interests. These layers of protection start with safe and effective process control and extend to manual and automatic prevention layers and continue with layers to mitigate the consequences of an event (Figure 1).

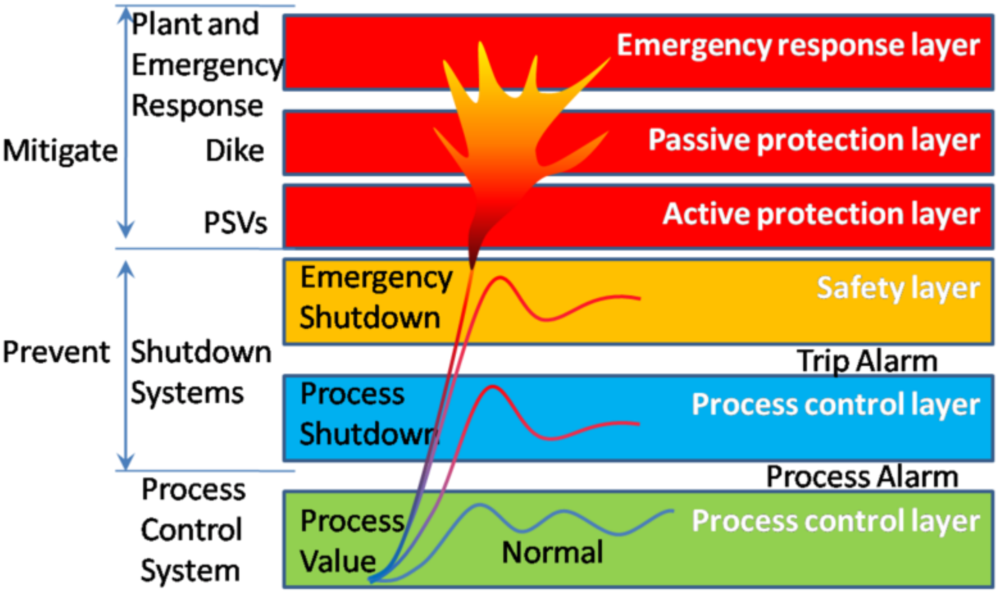


Figure 1: Layers of Protection

The first layer is the basic process control system. This layer provides safety through proper design of control of the process. The second layer is the alarm system which provides the appropriate information to process operators, supporting them in the identification of the cause of the unsafe situation and allows them to take actions to restore the plant to normal operation. The third layer is the SIS. It is a safety system independent of the process control system. It consists of sensors, valves and logic system to make appropriate decisions and take action on the process to bring it back to a safe state. All these three layers are designed to prevent a safety related event. If a safety related event occurs the top three layers (i.e. Active, Passive and Emergency Response) are designed to mitigate the impact of the event. Emphasis is placed on the Shutdown Systems where the alarm and SIF is designed and installed for a specific function of the process, and the design information ensures that the device specified will meet those requirements. Design information includes the following:

- Potential hazard scenarios the device is designed to protect
- Process conditions, including equipment and process limitations

Safety Integrity Level (SIL) Analysis

The quantitative analysis documenting an IPLs capability to protect against a hazard scenario is the SIL calculation analysis. Major inputs to these calculations include process safety time, as well as applicable hazard scenarios for which the IPL is designed and installed to protect against. These inputs are used to generate a specific Probability of Failure on Demand (PFD) for the IPL in question.

Alarm Management

International standards (EEMUA 191 – 2007, ISA-18.2-2008) provide guidance that can help practitioners design, implement and maintain an alarm system that delivers acceptable performance and maximizes operator dependability.

Alarm management activities are structured to follow a lifecycle approach (Figure 2) wherein the key activities are executed in different stages of the lifecycle. The outputs of each stage are inputs for the activities of the next stage. The first stage of the alarm management lifecycle involves the creation of an alarm philosophy document. The document establishes the basic definitions, principles and processes for the design, implementation, maintenance and management of the alarm system. It contains the alarm system performance goals and provides guidance for a consistent approach to alarm management.

One of the most important and relevant activities in the lifecycle approach during the design phase of a plant is the alarm rationalisation. Rationalisation involves reviewing and justifying potential alarms to ensure that they meet the criteria for being an alarm as defined in the alarm philosophy document. It includes defining the attributes of each alarm for example activation time, priority, classification, and type, as well as documenting the cause, consequence, response time and operation action. The rationalisation process is performed by a multi-disciplinary team which typically includes the process engineer, process control engineer, plant operators and safety engineers.

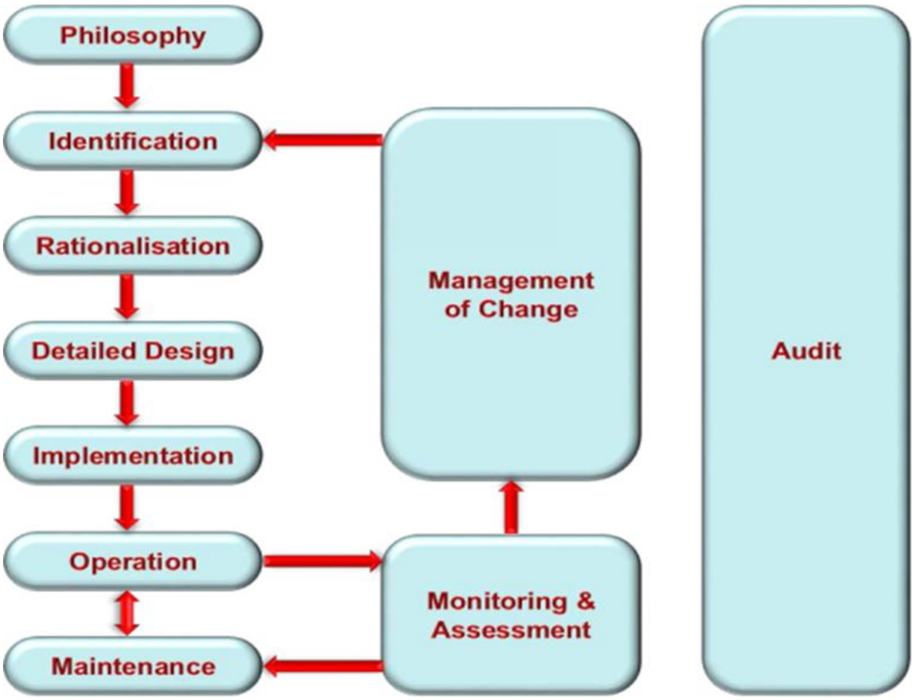


Figure 2: Alarm Management Lifecycle (EEMUA-191)

Determination of Process Safety Time

Methodology

Process safety time (PST) is a function of the behaviour of process and process equipment within the context of a specific unmitigated scenario. International standard (BS EN 61511-2004) defines PST as "the time period between a failure occurring in the process or the basic process control system (with the potential to give rise to hazardous event) and the occurrence of a hazardous event if the safety instrumented function is not performed". This definition can be elaborated further as the amount of time that is available to take action on the process to move it to a safe state after an out-of-control condition has been observed to occur in the process.

The method adopted to calculate the PST is initially based on an analytical approach taking into consideration process theories with known design limits of the equipment. The process variable that is most closely associated with the occurrence of the hazardous event is first identified, and then its value at the point where it is above normal condition and its likely value at the time of the hazardous event or the point at which that hazard can no longer be reliably prevented is worked out. There may be considerable uncertainty finding out the conditions at which the hazardous event occurs, as a result the design limit of the equipment is assumed. For example, loss of containment may be imminent when the vessel pressure rises above the Maximum Allowable Workable Pressure (MAWP). The difference between the MAWP of the vessel and the upper limit of normal operating pressure with the rate of change pressure is used to estimate PST.

The general equation that was developed to estimate the PST is given as:

$$\boldsymbol{PST} = \frac{(\boldsymbol{PVhaz} - \boldsymbol{PVsp})}{\frac{\boldsymbol{dPV}}{\boldsymbol{dt}}} \qquad (1)$$

PST: Process Safety Time. Time between alarm set point and hazardous event

PV_{haz}: Process variable value at the time the hazardous event occurs

PV_{sp}: Process variable value at its alarm set point

$\frac{\boldsymbol{dPV}}{\boldsymbol{dt}}$: Estimated rate of change of process variable over the course of the hazardous event.

The difference in value between the variable design limit value and alarm condition divided by the variable rate of change gives the estimated PST. The variable rate of change is estimated from the mass or energy flow through the system. For liquid level the values is calculated from known operating conditions, vessel geometry and design parameters. The rate of increase or decrease in liquid level is estimated from the volume flow rate from the vessel.

The estimated PST is then reviewed against results from a dynamic simulation model of the plant unit by simulating each hazardous scenario. To model each hazardous scenario identified during the SIL/LOPA reviews, data regarding the process condition, mode of operation and equipment design limit are used in the model. This enables the non-linear behaviour of the process to be factored in. The model is run over time to calculate the PST. Once analysis is complete the PST determined for each scenario is recorded in the project instrumentation database and also on the Cause and Effects matrix for information to be used at further stages of the project. The calculated PST is used to determine the SIF response time.

The calculated PST is also used as part of an alarm classification review to determine operator alarm response time and setting of alarm priority. The operator response time is based on the principle of "Detect-Understand-Decide-Act". The operator needs sufficient time to manage the process upset. Sufficient time is necessary for the operator to detect the problem, understand the nature and extent, decide what to do about the problem and implement the changes. For this to happen, the time to manage the fault must be less than the calculated PST. The recommended minimum allowable operator response time for safety IPL alarm is in the order of 20-30 minutes (EEMUA-191, 2007). This philosophy is applied during the alarm classification review.

Application to Process Unit Design

The above methodology was applied to a para-xylene plant design with particular attention to the safeguarding of the xylene recovery column.

The xylene recovery column fractionates heavy reformate feeds into C8 aromatics, heavy aromatics and benzene. The overhead vapours from the column are partially cooled in the overhead condensers and collected in the column reflux drum. The off-gas from the reflux drum flows through a vent condenser where additional liquid benzene is recovered. The vent condenser is chilled by use of high pressure propylene refrigerant. The non condensed vapour from the vent condenser is sent to fuel gas compressor suction drum to remove liquid hydrocarbon traces before being compressed in a fuel gas compressor then cooled before being sent to a gas header.

The overhead liquid from the reflux drum is partly pumped back to the column as reflux and the rest pumped as distillate feed to the Depentanizer column.

C8 aromatics product is taken off as a side draw, pumped and cooled and sent to a product tank.

A fired heater which operates under balanced draft provides the column re-boiling duty. Part of the column bottom liquid is pumped to the fired heater to provide heating while the remaining liquid is pumped, cooled and fed to Clay treaters for removal of olefins and styrene. Figure 3 below depicts the flow diagram of xylene recovery column unit that was modelled.

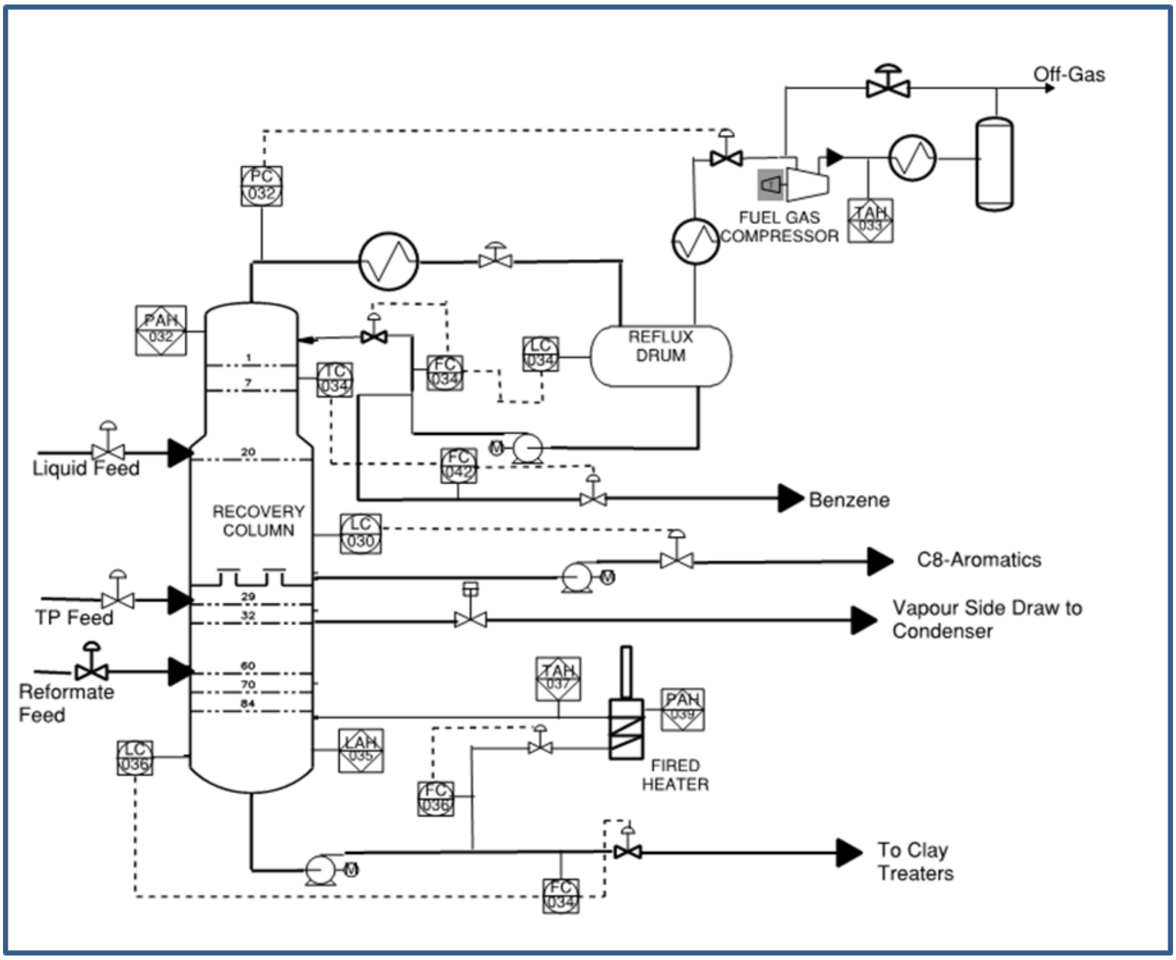
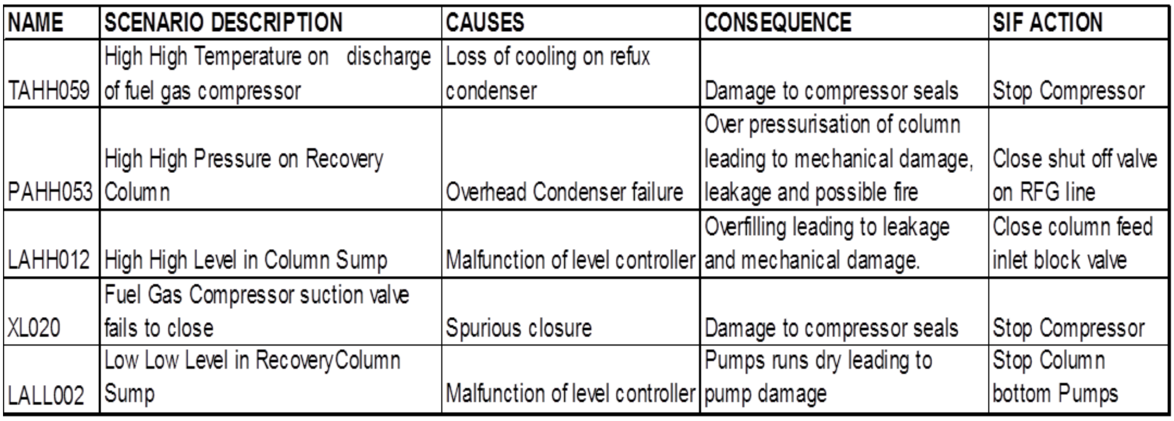


Figure 3: Xylene Recovery Column Unit

From SIL/LOPA reviews many hazard scenarios were identified for which protective elements (e.g. SIFs) are required. Table 1 below lists some of the scenarios identified for the recovery column unit.



NAME	SCENARIO DESCRIPTION	CAUSES	CONSEQUENCE	SIF ACTION
TAHH059	High High Temperature on discharge of fuel gas compressor	Loss of cooling on refux condenser	Damage to compressor seals	Stop Compressor
PAHH053	High High Pressure on Recovery Column	Overhead Condenser failure	Over pressurisation of column leading to mechanical damage, leakage and possible fire	Close shut off valve on RFG line
LAHH012	High High Level in Column Sump	Malfunction of level controller	Overfilling leading to leakage and mechanical damage.	Close column feed inlet block valve
XL020	Fuel Gas Compressor suction valve fails to close	Spurious closure	Damage to compressor seals	Stop Compressor
LALL002	Low Low Level in RecoveryColumn Sump	Malfunction of level controller	Pumps runs dry leading to pump damage	Stop Column bottom Pumps

Table 1: Hazard Scenarios

For each scenario the PST was initially determined using Equation 1 taking into consideration the unit design flow rates. The results were then reaffirmed and adjusted using Aspen HYSYS Dynamics. All the equipment shown in Figure 3 were modelled including the pipelines and shutdown valves. The results below show the dynamic response of some of the process variables identified for each scenario and how the process safety time was derived.

Dynamic Results

High High Temperature on Fuel Gas Compressor Discharge:

The high high temperature scenario was simulated by first running the process model at steady state with the temperature at the Fuel gas compressor discharge at 62^{o}C. Then a disturbance was introduced by closing the refrigerant inlet valve to the vent condenser and observing the rise in temperature. By design the maximum allowed temperature limit for the compressor is 120^{o}C. The high high temperature alarm set point was set at 80^{o}C. Fig 4 shows the dynamic response of the compressor discharge temperature and the PST estimated. The process safety time was estimated as the time difference between the alarm set-point and the maximum allowed working temperature (MAWT) at the compressor discharge.

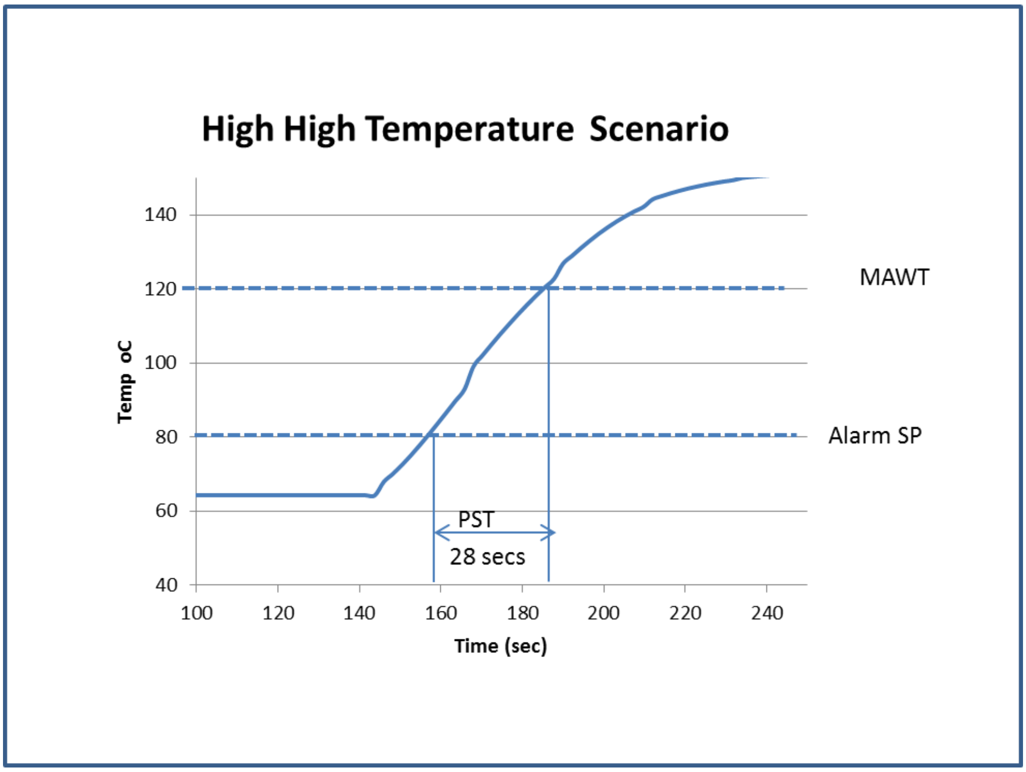


Figure 4: Compressor Discharge Temperature Profile

High High Column Pressure:

For this scenario the dynamic model was run in steady state with the column pressure controlled at its normal value of 0.6 barg. The high pressure excursion on the column was simulated by shutting the overhead block valve and observing the rise in column pressure. By design the maximum allowable pressure limit for the column was 5.3 barg. The high high alarm trip point was set at 0.9 barg. Figure 5 shows the dynamic response of the column pressure with the estimated process safety time. The process safety time was estimated as the time difference between the alarm set-point and the maximum allowed working pressure (MAWP) of the column.

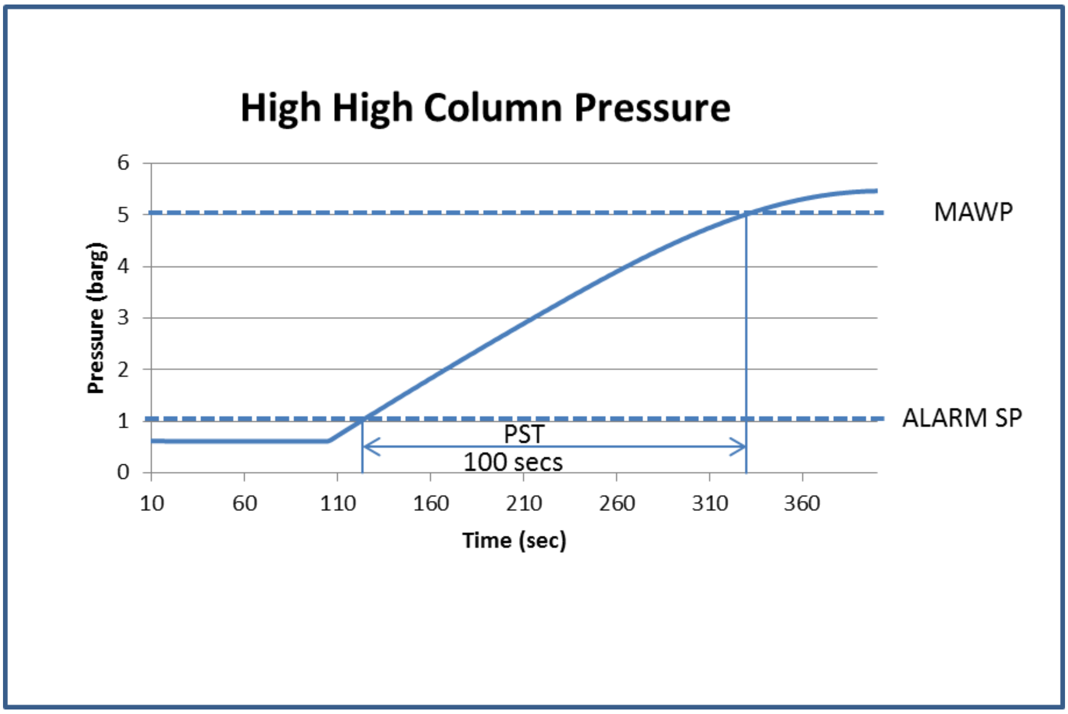


Figure 5: Column Pressure Profile

Low Low Liquid Level in Column Sump:

In simulating this scenario, the dynamic model was first run at steady state with the column sump level controlled at 33% volume. The low liquid level excursion in the column sump was simulated by stopping the inlet feed block valve and the low level transmitter fails to respond causing the level control valve to go fully open. The fall in level in the column sump was observed. Vapour breakthrough in the column sump is assumed to occur when the level in the sump is less than 5% of the column sump volume. The low low level alarm trip point was set at 20% volume. Figure 6 shows the dynamic response of the column sump level with the estimated process safety time. The process safety time was estimated as the time difference between the alarm set-point and the column sump liquid minimum limit.

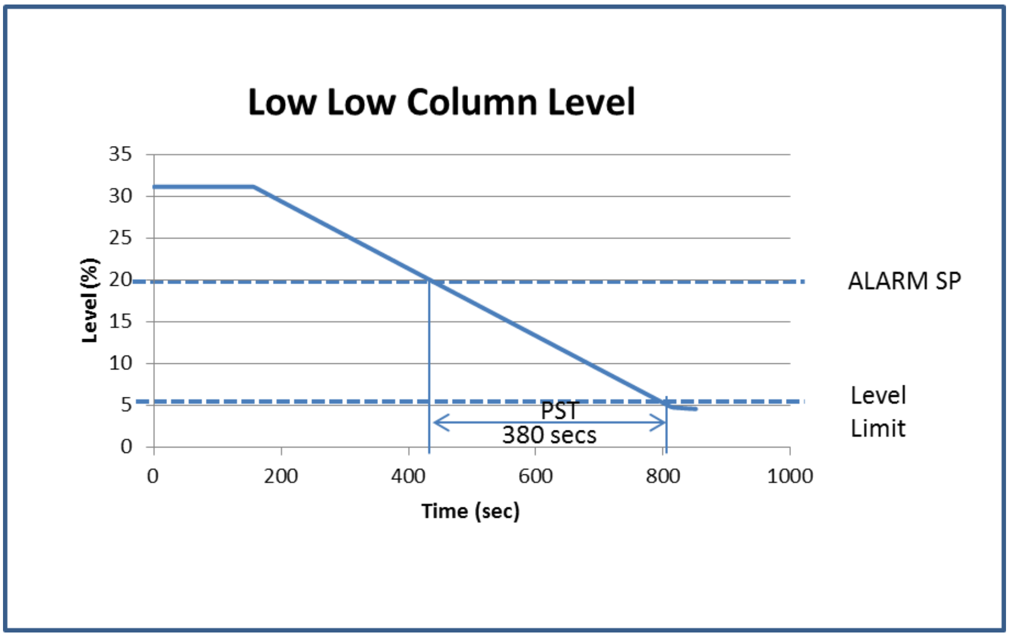
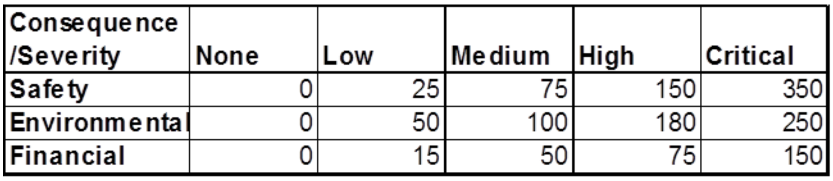


Figure 6: Column Sump Liquid Profile

The estimated PSTs of the above scenarios were well below the recommended minimum allowable operator response time for safety IPL alarm prescribed by EEMUA-191 guideline and as such are demonstrably not effective as a safety alarm independent protective layer.

Alarm Priority

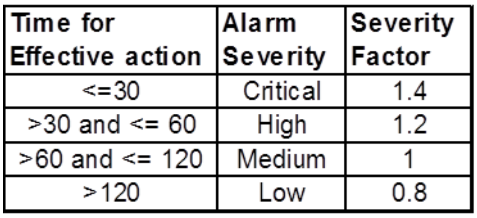
The PST values calculated were used as a guide to determining the alarm priority for each scenario. The assigning of alarm priority was based on a priority definitions table and scoring table (Table 2). The definitions table is used to identify the specific severity of the consequences for each event and the scoring table was used to build up a total combined score for each alarm.



Consequence /Severity	None	Low	Medium	High	Critical
Safety	0	25	75	150	350
Environmental	0	50	100	180	250
Financial	0	15	50	75	150

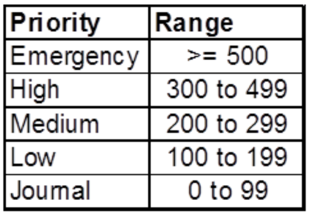
Table 2: Alarm Priority Table

The PST calculated and the severity was applied to the alarm effectiveness table (Table 3) to determine the severity factor. Using the values obtained from Table 2 with the severity factor in Table 3, the priority alarm assigned to each scenario was estimated from the Priority range table given in Table 4.



Time for Effective action	Alarm Severity	Severity Factor
<=30	Critical	1.4
>30 and <= 60	High	1.2
>60 and <= 120	Medium	1
>120	Low	0.8

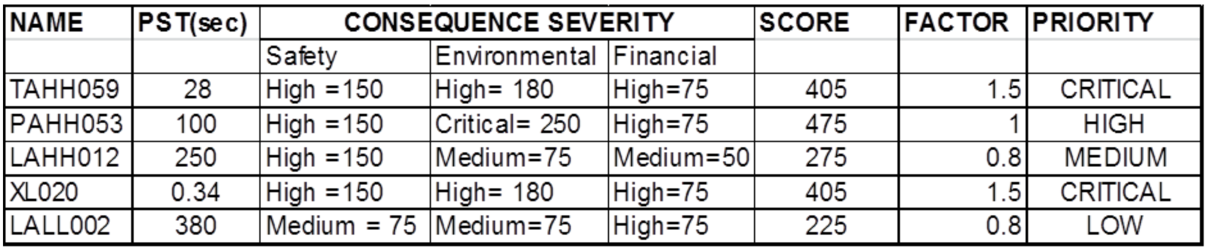
Table 3: Alarm Effectiveness



Priority	Range
Emergency	>= 500
High	300 to 499
Medium	200 to 299
Low	100 to 199
Joumal	0 to 99

Table 4: Alarm Priority Range

Table 5 below shows the alarm priorities for the different scenarios identified.



NAME	PST(sec)	CONSEQUENCE SEVERITY			SCORE	FACTOR	PRIORITY
		Safety	Environmental	Financial			
TAHH059	28	High =150	High= 180	High=75	405	1.5	CRITICAL
PAHH053	100	High =150	Critical= 250	High=75	475	1	HIGH
LAHH012	250	High =150	Medium=75	Medium=50	275	0.8	MEDIUM
XL020	0.34	High =150	High= 180	High=75	405	1.5	CRITICAL
LALL002	380	Medium = 75	Medium=75	High=75	225	0.8	LOW

Table 5: Alarm Priority assigned to scenarios

Conclusion

The development of alarm systems and safety instrumented systems and identification of possible hazards by process hazard analysis techniques require detailed knowledge about the technology. In the application of these techniques the dynamic behaviour of the process is rarely considered.

This article introduces a method based on using a dynamic simulation tool to estimate, verify and confirm PST time that can be used in the design of alarm and protective safety elements (SIFs). The use of dynamic simulation to aid in determining the PST can also be applied to assigning priorities to alarms and resetting alarm set points which all contributes to making the process alarm system more effective in safeguarding the process plant. Furthermore, at the design stage of a process plant, it provides supporting evidence in determining the core attributes that makes alarms and SIFs suitable for their intended purpose.

References

BS EN 61511 -2004, Functional Safety – Safety Instrumented Systems for the Process Industry sector

Buncefield - 2008: The final Report of the Major Incident Investigation Board.

Ingram, G.D., Cameron, I.T.,Hangos, K.M., 2004, Chemical Engineering Science 59

Labovsky, J., Svandova, Z., Markos, J., Jelemensky, L., 2007, Journal of Loss Prevention in the Process Industries 20

EMMUA – 2007, Alarm Systems – A Guide to Design Management and Procurement, Publication No. 191

ISA 18.02, 2008, Management of Alarms System for the Process Industries