Is all Safety-Critical Equipment Critical to Safety?

John C. Wincek, Croda, Inc., 8 Croda Way, Mill Hall, PA 17751

Process plants contain myriad pieces of equipment, from tanks, pumps and piping to sensors, actuators and valves. It is obvious to most that chemical-containing equipment must be maintained to prevent a loss of containment incident leading to a catastrophic event. This equipment could be described as safety-critical. But the list extends beyond that point. A valve that fails to open or close when commanded could initiate a chain of events leading to a loss of containment and catastrophic incident. Similarly, a process sensor out of calibration may lead to insufficient cooling and a runaway reaction. Equipment such as this, which could participate in the chain of events leading to a catastrophic event, might also be considered safety-critical. And the list extends even further. A pressure relief valve might be safety-critical. Sensors designed to detect a process upset (perhaps due to the out-of-calibration sensor), and the final elements that bring the process to a safe state might be considered safety-critical. There may be alarms that precede system trips, affording the opportunity to intervene, as well as redundant sensors. There may be displays that allow the operator to monitor and detect upset conditions. The list of potential safety-critical equipment can seem endless. So how does one decide which equipment is truly critical to safety? How does one prioritize the relative importance of safety-critical equipment? Is every alarm, sensor and valve critical to safety? Most importantly, what do employees need to know? This paper will describe a method for identifying the equipment most critical to safety, without which the process should not be operated. By limiting the list of safety-critical equipment to only that which truly is critical to safety, one can easily identify such equipment in the field, on drawings and display screens.

Keywords: Process Safety-Critical Equipment; Safety-Critical Assets

Introduction

Many incidents have resulted from failures of Process Safety-Critical Equipment (PSCE). Examples include:

- In 1984, a light hydrocarbon pipeline between a refinery and a storage terminal ruptured due to corrosion. The resulting explosion killed 500 people[1].
- In 1970, a freight train carrying 12 liquefied propane gas cars derailed. An LPG car ruptured in the incident, releasing its contents and creating a fireball hundreds of feet in diameter. The resulting pool fire caused the BLEVE of several other LPG cars. The derailment was caused by the mechanical failure of a journal bearing on one of the rail cars.[2]
- In 1965 an explosion occurred on a plant manufacturing neoprene. The investigation reveals that the explosion was caused by local overheating in a compressor due to a mechanical failure. This led to the decomposition of monovinyl acetylene, a component used in the manufacture of MVA.[3]
- In the years leading up to the 1984 release of methyl isocyanate in Bhopal India, A Union Carbide Corporation safety team noted deficiencies in safety valve and instrument maintenance programs. Several serious incidents related to mechanical integrity, some with fatal consequences, occurred in the three years prior to the 1984 release, which resulted in thousands of fatalities.[4]

Many companies designate a subset of their assets as Process Safety-Critical Equipment (PSCE). This designation can serve several purposes, including:

- To assist with the prioritization of equipment repairs
- To meet regulatory requirements
- To meet the recommendations of Relevant Good Practice
- To inform the basis for testing, inspection frequency and rigor

Mechanical Integrity is the programmatic implementation of activities necessary to ensure that important equipment will be suitable for its intended application throughout the life of an operation[5]. It replaces the "breakdown maintenance[6]," philosophy with one that strives to keep equipment functioning as intended at all times.

All PSCE should be included in the plant's Mechanical Integrity program. However, it is not uncommon for facilities to over-specify the PSCE and planned MI activities and then fall behind in meeting their schedule or fail to maintain their schedule and have the maintenance repair backlog rise.[7] Being overly aggressive or using an "include-it-all" mentality when specifying PSCE can cause great difficulties later on, including:

- Overloading employees with information
- Placing equipment of lesser importance on the list of highest-priority assets
- Diluting the importance of the PSCE designation by operating without it because it is not "really" critical equipment.
- Causing increased workload for maintenance personnel by increasing the testing and inspection frequency of less-important equipment.

When developing a list of PSCE for inclusion in an MI program, a balance must be achieved between designation of PSCE and other safety-related equipment. One must ask, is all safety equipment actually critical to safety?

Reducing Risk

Process Safety programs are intended to reduce the risk of a catastrophic incident such as a fire, explosion and/or toxic release. Risk is the combination of three attributes[8]: What can go wrong? How bad could it be? and How often might it happen? Many companies strive to reach a risk target, above which the risk is considered to be too high. Risk targets are often based on the likelihood of fatal injuries, as lesser injuries are harder to predict and differentiate. Once the minimum risk criteria are met, one needs to ensure that all regulatory requirements are met, as well as any Relevant Good Practice (RGP). The final test is often to determine if the risk is As Low as Reasonably Practicable (ALARP). ALARP generally requires that the cost of any additional potential safeguards is disproportionate to the potential benefit achieved.[9]

Once any feasible Inherently Safer options have been implemented, there are various categories or types of safeguards employed.

Basic Process Control System (BPCS)[10] – the system that regulates the process within normal production limits. It typically consists of sensors, logic solvers (e.g. Programmable Logic Controllers, Distributed Control Systems), final elements (e.g. valves, alarms) and human interfaces such as display and input screens. It is not uncommon for the BPCS to activate alarms and interlocks based on quality- and/or safety-related limits.

Interlocks – Typically implemented outside of the BPCS using mechanical devices such as relays. For example, a temperature sensor on a pump may be physically wired directly to the motor starter. In the event of high temperature, it would cause the motor starter to disengage, stopping the pump.

Safety Instrumented System (SIS)[11] – An instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensor (s), logic solver (s), and final elements(s). A Safety Instrumented Function is a safety function which is necessary to achieve functional safety

Mitigation Systems – Systems that act after an incident has occurred and function to mitigate the consequences of the incident. These include fire detection and suppression systems, vapor suppression systems, and emergency response teams, among others.

Heinrich's Domino Theory

In 1931, H.W. Heinrich developed what is now known as "Heinrich's Domino Theory[12]." Simply stated, he postulated that any incident is the result of several sequential causal factors. Each causal factor can be thought of as a single domino in a row of dominoes. When the first domino is tipped over, it falls into the next domino (causal factor), which falls into the next, and so on until the final domino falls (the incident occurs).

This same theory can be used to depict a process incident and the various safeguards in place to prevent it. Consider the following incident sequence:

- The operator fails to monitor and adjust the temperature of a chemical reaction, causing both temperature and pressure to rise.
- A high temperature alarm, set near the upper limit of the desired temperature range, activates in the BPCS.
- A second high temperature alarm, based on a redundant temperature sensor and set at the upper limit of the desired temperature range, activates in the BPCS.
- A third BPCS alarm activates near the pressure limit of the process equipment.
- A hardwired interlock activates crash cooling nearer still to the pressure limit of the process equipment, based on a redundant pressure transmitter.
- A SIL 1-rated Safety Instrumented System, using its own dedicated temperature sensor and valves, shuts off all chemical feeds to the vessel near the temperature limit of the process equipment.
- A bursting disk opens at the pressure limit of the vessel, relieving the excess pressure.
- The vessel suffers a catastrophic failure (if all of the above safeguards fail).

Imagine that each of the above items is a domino, aligned in a row (eight dominos) such that toppling the first domino will cause a chain reaction, knocking down the other dominoes in succession. The final domino represents the vessel's failure. If any one of the preceding seven dominoes does not fall (i.e. the safeguard successfully performs its function to prevent the incident), then the vessel failure is averted.

Close examination of the safeguards represented by the dominos reveals some concerning facts:

- The operator's inattention or incapacitation, which served as the initiating event (domino 1), could also result in a failure to respond to the alarms associated with safeguards 2, 3 and 4.
- Although safeguards 2 and 3 use separate temperature sensors, they both depend on the BPCS to sound the alarm at the appropriate time.
- Although safeguard 4 depends on a pressure transmitter instead of a temperature transmitter, it too depends on the BPCS.

- If the operator's failure to maintain temperature control was due to a failure or mis-calibration of the temperature sensor, safeguard 2 may not function for the same reason.
- If the operator's failure to maintain temperature control was due to a failed cooling water valve, safeguard 5 may not function (assuming it operates using the same cooling water valve and/or piping as the failed valve)

Avoiding the concurrent failure of two or more safeguards usually requires that they operate completely independently of each other, as do safeguards 4, 5 and 6. Independent safeguards typically reduce incident frequency by one to two orders of magnitude. Although safeguards that are not independent of each other are common in industry and do provide risk reduction, their contribution typically much less than independent safeguards.

Differentiating between Process Safety-Critical Safeguards and Other Safeguards

Layer of Protection Analysis (LOPA) is a useful tool for differentiating between Process Safety-Critical Safeguards (and equipment) and those that have lesser impact on safety. A LOPA analysis of the above incident sequence may look like that shown in Figure 1. LOPA is typically used to quantitatively show that the process meets a minimum risk target (e.g. government-imposed or company-established limits). Following LOPA a check is made to ensure that all RGP and regulatory requirements are met. As a final step in the Risk Assessment, any additional potential safeguards are evaluated using the ALARP principle.

LOPA imposes a strict set of rules for qualifying a safeguard as an Independent Protection Layer (IPL). These rules are necessary to ensure the necessary conservativeness of the LOPA methodology. In order to be considered an IPL, a device, system or action must be[13]:

1. Effective in preventing the consequences when it functions as designed
2. Independent of the initiating event and the components of any other IPL already claimed for the same scenario
3. Auditable: the assumed effectiveness in terms of consequence prevention must be capable of validation in some manner (documentation, review, testing, etc.)

Only those safeguards that meet these stringent criteria qualify as Independent Protection Layers. IPLs typically reduce risk by orders-of-magnitude, while non-IPL Safeguards reduce risk only incrementally.

Figure 1 – A portion of the LOPA for Operator Fails to Monitor and Control Reaction Temperature

		Probability	Frequency/yr.
Initiating Event	Operator fails to control batch temperature.		1E-1
Enabling Event	Probability that an exothermic reaction is occurring at the time the operator fails to control batch temperature. (Assumes 400 exothermic reactions per year, lasting 2 hours each: (400 batches/yr. * 2 hours/batch) / 8760 hours/year = 0.1	1E-1	
	Frequency of Unmitigated Consequences		**1E-2**
IPL 1	A hardwired interlock activates crash cooling near the pressure limit of the process equipment, based on a redundant pressure transmitter.	1E-1	
IPL 2	A SIL 1-rated Safety Instrumented System, using its own dedicated temperature sensor and valves, shuts off all chemical feeds to the vessel near the temperature limit of the process equipment.	1E-1	
IPL 3	A bursting disk opens at the pressure limit of the vessel, relieving the excess pressure.	1E-2	
	Frequency of Mitigated Consequences		**1E-6**
Non-IPL Safeguard 1	A high temperature alarm, set near the upper limit of the desired temperature range, activates in the BPCS, alerting the employee to take action.. Fails IPL Independence Test due to the operator being a common component with the initiating event.		
Non-IPL Safeguard 2	A second high temperature alarm, based on a redundant temperature sensor and set at the upper limit of the desired temperature range, activates in the BPCS, alerting the employee to take action. Fails IPL Independence Test due to the operator being a common component with the initiating event.		
Non-IPL Safeguard 2	A third BPCS alarm activates near the pressure limit of the process equipment, alerting the employee to take action. Fails IPL Independence Test due to the operator being a common component with the initiating event.		

Limiting PSCE to that which is Truly Critical to Safety

Following the rules of LOPA, one could claim that only those safeguards meeting the requirements of an IPL contribute significantly to risk reduction. Although outside the scope of this paper, it can be shown that elements shared by two or more safeguards provide risk reduction of less than one order of magnitude.[14] This is because the failure of a single component (e.g. temperature sensor) may render multiple safeguards inoperative, and is one reason for the IPL rule of independence.

It follows then that those safeguards that meet the definition of an IPL provide the majority of the risk reduction. Further, LOPA will have shown that the risk reduction provided by the IPLs is sufficient to meet the applicable minimum risk criteria. In other words, the safeguards meeting the IPL criteria are significantly more critical to safety than those that don't.

Following this premise, only the sensors, switches and final elements of the IPLs would be counted as PSCE. Of two temperature elements on a vessel, either of which will trigger a high temperature alarm in the BPCS, only one would be considered PSCE. The risk reduction provided by the second temperature element is not significant enough for it to be considered critical to the safety of the process.

Beyond Safeguards – Other PSCE

The preceding information has shown a method of identifying sensors, valves, interlock, alarms, etc. which are truly critical to safety. These types of equipment, however, make up only a portion of PSCE. For much of the remainder, we must focus on the initiating events of the Layer of Protection Analyses.

Initiating events provide indicators of additional equipment that should be considered PSCE. Equipment such as pumps and tanks, whose failure could initiate a catastrophic incident, should be considered PSCE. For initiating events such as failure of a flange gasket, one must consider more generally what equipment should be included as PSCE – it may indicate that the entire piping system should be considered PSCE. Additional examples of PSCE identified by initiating events are shown in Table 1.

Global PSCE

After the selection of PSCE from the Layer of Protection Analyses, one must consider global categories of physical equipment that may be justified for inclusion. CCPS[15] recommends categories of equipment that should be considered for inclusion (see Figure 2). In keeping with the conservative nature of selecting safeguards for inclusion, one must resist the temptation to globally include all members of an equipment category unless all are truly critical to safety. Consider the following:

- A pressure vessel has been designed according to the principles of Inherent Safety, such that it could contain all foreseeable pressure excursions (e.g. internal ignition, runaway reaction, external fire impingement, steam coil failure, etc.). Is the vessel's Pressure Safety Valve truly critical to safety?
- Consider a chemical reactor that runs only endothermic reactions. While overheating may cause a catastrophic event, the loss of heat will cause no foreseeable hazard. It is conceivable that one would consider only the shutoff valves for the heating system as PSCE, and not the entire heating system (unless of course the heating system itself is pressurized).
- A pump whose casing failure would result in a loss of containment of a hazardous material should be included in the PSCE list. If inadvertent shut-off of the pump causes no foreseeable hazard, then one might question if the pump motor should be considered PSCE.

Table 1 – PSCE Identified by Initiating Events

Initiating Event	Potential PSCE Identified
Failure of chemical unloading hose.	Liquid and vapor-return lines from the transport container to the storage tank.
Pump discharge valve failure causes pump overheating due to deadhead condition.	Pump and the piping systems on both the inlet and discharge sides.
A flange gasket blowout on piping segment.	Piping system
Failure of a nitrogen regulator causes overpressure in storage tank	Nitrogen regulator, storage tank
Failure of tank inerting system leads to internal explosion in a flammable storage tank.	Nitrogen supply system, tank blanketing system
Storage tank failure due to corrosion	Storage tank
Stuck-closed conservation vent fails to provide make-up air during tank pump out, leading to vacuum failure of the tank.	Conservation vent, tank
Failure of cooling water supply leads to runaway reaction.	Cooling water supply system
Overheating of storage tank causing release through pressure safety valve	Heating controls, pressure safety valve.

Benefits of Limiting PSCE List

Many benefits can be realized by limiting the list of PSCE to that which is truly critical to safety. These benefits include reduced resource demands, a clearer understanding of the safety aspects of the process, improved focus on critical testing, inspection and repairs, and establishment of a minimum set of safeguards necessary operate the process.

As discussed earlier, LOPA will identify those safeguards that are necessary to meet the minimum risk requirements. While it is likely no company wants to operate with only the minimum level of safety, it may be acceptable to operate temporarily without some safeguards as long as the minimum risk criteria are still met. In this case, the IPLs from LOPA constitute a list of "must have"

Figure 2 - PSCE Categories

- Pressure vessels
- Atmospheric / low pressure tanks
- Piping and piping components
- Pressure relief devices
- Secondary containment units
- Rotating equipment
- Utility systems
- Mitigation equipment and systems
- Ventilation systems
- Structural components
- Release detection systems

safeguards, without which one is unwilling to operate the process unless a suitable replacement safeguard exists. This list is usually much shorter than the list of all process safeguards.

Because the list of "must have" safeguards is short, it is much easier to train on, and for operators to retain this information. Reacting to the loss of every safeguard as if it were PSCE dilutes the importance of the classification, especially if the process continues to be operated without a suitable replacement safeguard.

Some companies develop (or are required to develop) a Safety Case or Basis of Safety for their process. This is typically designed to show the risk of operating the plant is sufficiently low. The IPLs should be sufficient to show that the process meets the minimum risk standards.

Reducing the list of PSCE to only those items that are truly critical has several benefits. First, the test frequency of equipment not on the list might be reduced, allowing increased focus on the PSCE. This alone has significant resource benefits. Having a smaller set of PSCE will reduce or prevent any backlog of inspections and testing. The number of Mechanical Integrity work orders generated will also be smaller, allowing higher importance and priority to be given to a smaller number of tasks. When managing breakdown work orders, fewer will have the highest priority assigned to them.

Additional Benefits

Because the list of PSCE is now smaller, actions that may have been cost-prohibitive may now be feasible. Actions to better 'immerse' employees in PSCE and its functions, and actions to improve response to process upsets can be taken.

Field Identification

Field identification of PSCE can provide several benefits. PSCE could be identified in several ways, including tagging or painting a special color. Through clear and obvious identification in the field:

- Operators are constantly reminded that PSCE exists and which devices are included.
- Operators finding damaged equipment are immediately alerted to its criticality.
- When the cause of a process issue is identified as a piece of PSCE, the operator immediately knows of its criticality, and can determine that the process may need to be shut down.
- When maintenance arrives to calibrate, troubleshoot or repair a piece of equipment, they immediately know its criticality to process safety.

Identification on Control Room Displays

The control room operator is often the first person to detect process malfunctions such as a sensor failures or valves not operating. By identifying PSCE on his screen, he immediately knows of the criticality of the issue. This can help him to decide who to contact, and how urgent the matter is. It can also provide a common understanding of urgency between operators, maintenance personnel and management. It is likely that all will understand the need to react quickly when told "a piece of PSCE is malfunctioning" instead of "the level transmitter on the condensate receiver tank is malfunctioning."

Identification on Process and Instrumentation Diagrams (P&IDs)

P&IDs are used by many employees in an organization. Project engineers use them to design process upgrades. Process Engineers and production management use them to troubleshoot process issues. Operations and maintenance personnel use them to identify isolation points and understand the process. Hazard Study teams rely on them to correctly depict the process under study. All of these users would benefit from having PSCE easily identified during drawing use. Developing a scheme to mark or otherwise identify PSCE on P&IDs, electrical diagrams, etc. can benefit many different activities for which drawings are used.

Alarm Handling Procedures

Many companies provide procedures to be followed in the event an alarm is activated. Often there are procedures specific to a single or small group of alarms. Development and maintenance of these procedures can be a daunting task given the number of alarms in a typical process plant. By reducing the list of PSCE to only that which is truly critical, one would be better able to maintain procedures for handling Process Safety-Critical alarms.

Management of Change

Change management systems typically require a safety or risk review to ensure that the change does not introduce new risks, and that existing risks remain adequately managed. The list of PSCE, specifically the safeguards and their required sensors and actuators, can be a tool used to ensure that no Process Safety-Critical safeguards are impacted by the change.

Conclusion

Process Safety programs strive to reduce the risk of a catastrophic incident. Often there is a minimum risk criterion that must be met, followed by additional efforts to further reduce the risk. It has been shown that some safeguards do not significantly reduce risk, and therefore are not as critical as those that provide order-of-magnitude risk reduction. Using LOPA as a tool to identify safeguards that provide significant risk reduction and equipment capable of causing a catastrophic incident, only those that provide significant risk reduction will be included in the list of Process Safety-Critical Equipment. While additional categories of equipment must be considered for inclusion, care must be taken to avoid an "include-it-all" mentality, which will lead to a larger-than-necessary list of Process Safety-Critical Equipment. Adding equipment to this list places unnecessary resource demands to inspect, test and maintain critical equipment. By minimizing PSCE, benefits such as improved understanding and focus on critical equipment can be achieved. Additional efforts such as identifying PSCE in the field, on operator screens and P&IDs assist the organization to identify and focus on PSCE. The PSCE list can also be used to focus development of procedures for alarm response, and to ensure that process changes do not impact the safeguards that form the Basis of Safety for the process.

[1] Center for Chemical Process Safety, Guidelines for Risk based Process Safety, Wiley-Interscience, USA, 2007, p. 317
[2] Ibid, pp. 223-224
[3] Mannan S. editor, Lee's Loss Prevention in the Process Industries, 3rd ed., Elsevier Butterworth Heinemann, 2005, Vol. 3, Appendix 1, p. 33
[4] Ibid, Vol. 3, Appendix 5, pp.4-5
[5] CCPS. Guidelines for Mechanical Integrity Systems. (Center for Chemical Process Safety; New York, NY, 2006) p. 6
[6] Guidelines and Recommendations for Process Safety Management (Non-mandatory), 29CFR 1910.119, Appendix C Compliance, Section 9. Mechanical Integrity
[7] Hobbs, Douglas; Taming Mechanical Integrity; Process Safety Progress 27, no. 2; Published online 10 April 2008 in Wiley InterScience (www.interscience.wiley.com). DOI 10.1002/prs.10258
[8]Center for Chemical Process Safety, Guidelines for Risk Based Process Safety. Wiley-Interscience, Hoboken, NJ, p. xliv
[9] Health and Safety Executive, Principles and guidelines to assist HSE in its judgments that duty-holders have reduced risk as low as reasonably practicable, HSE, http://www.hse.gov.uk/risk/theory/alarp1.htm#P32_3493
[10] Center for Chemical Process Safety; Layer of Protection Analysis – Simplified Process Risk Assessment; American Institute of Chemical Engineers, 2001, New York, NY p. 259
[11] IEC-61511-1, Functional safety –Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements, International Electrotechnical Commission, 2003, Geneva, Switzerland, p. 25
[12] Petersen, Dan, Techniques of Safety Management – A Systems Approach, 3rd ed., 1989, Aloray Inc., Goshen, NY, pp. 23-25
[13] Center for Chemical Process Safety; Layer of Protection Analysis – Simplified Process Risk Assessment; American Institute of Chemical Engineers, 2001, New York, NY, pp. 80-88
[14] Center for Chemical Process Safety; Layer of Protection Analysis – Simplified Process Risk Assessment; American Institute of Chemical Engineers, 2001, New York, NY pp. 173-184.
[15] CCPS, Guidelines for Mechanical Integrity Systems. (Center for Chemical Process Safety; New York, NY, pp. 18-21