Pressure Relief System and Safety Instrumented Systems - Common Weaknesses in Field Implementation

William Bridges
President
Process Improvement Institute, Inc.
1321 Waterside Lane,
Knoxville, TN 37922 USA
wbridges@piii.com

Stephen Bridges
Senior Process Engineer
Process Improvement Institute, Inc.
1321 Waterside Lane,
Knoxville, TN 37922 USA
wbridges@piii.com

Rashed Al-Zahrani
Manager, Process Safety
Jubail United Petrochemical Company (UNITED), a SABIC affiliate
ZahraniRA2@united.sabic.com

Prepared for Presentation at
American Institute of Chemical Engineers
2020 Spring Meeting and 16th Global Congress on Process Safety
Houston, TX
March 29 – April 2, 2019

Pressure Relief System and Safety Instrumented Systems - Common Weaknesses in Field Implementation

Presenters:

William Bridges
Process Improvement Institute, Inc. (PII)

Stephen Bridges
Process Improvement Institute, Inc. (PII)

Keywords: Human Factors, Human Error, Independent Protection Layers, IPLs, Integrity, Asset Integrity, Risk Based Process Safety, RBPS, PSV, Pressure Relief, Pressure safety Valve, Relief Valve, Safety Instrumented System, SIS, SIF, SIL, SIL Verification

Abstract

Pressure relief and safety instrumented systems are often the last line of defense before the occurrence of a catastrophic event. Their design, sizing, and reliability are hence of critical importance for the chemical process industries. Either are touted as capable of achieving a PFD = 0.01 or even 0.001. But, common weaknesses in implementation prevent this from being achieved. These include:

- Failing to take the PFD into account in the design of relief systems that require multiple relief valves to open to achieve the target capacity for the limiting case. Such systems should be designed as MooN instead of NooN.
- Failing to stagger maintenance for multiple channel systems (for multiple PSVs and for multiple sensors or multiple final element SIF). If maintenance or checks or calibrations are performed on the same day by the same person, then redundancy is lost as mistakes will be repeated on the other devices/channels.
- High error rate for control of block valves for relief valves or SIS root valves on taps and impulse lines
- Failure to account for the human error probability in the PFD estimates, resulting in expecting PFDs of 0.001 when only 0.01 is achievable long term.

Data, including from UNITED (a SABIC affiliate), are shared in this paper.

The major deficiencies found in implementation of PSVs an SIS stem from lack of understanding by design engineers of probability of failure on demand (PFD) and stems also from failure to understand and control human error probability in the inspection, test, and preventive maintenance (ITPM) programs and their practices in the field. This paper explains both issues and provides an approach to address these issues.

1 Design Deficiency in Relief Systems – PFD is not expressly considered in the design of relief systems

One major design deficiency seen across about 100 sites around the world is that the PFD of the relief system was not taken into account when designing the relief. Design engineers focus on sizing issues and setting issues such as:

- nature of the material being relieved (phase of the material, but also is it prone to cause plugging or corrosion)
- back-pressure issues in the tail pipes and discharge line/systems
- throughput necessary (and phase of the material, whether gas, vapor, two-phase, or liquid)
- design pressure (including allowable accumulation pressures)

However, very few relief system designers are trained in, or take into consideration, the PFD of the relief system. Because of this, designers specify multiple relief devices that all must open to relieve the throughput for the limiting design case. Instead of specifying a design that requires installed redundancy and instead of accounting for common cause error, they specify barely enough relief devices to me the limiting case throughput demand.

Take the case that a large petrochemical unit is required to relieve a large through of gas on the suction side of a compressor, if the compressor trips off or fails off; and further assume this release will be at relatively low pressure of about 1 atmosphere gauge pressure. For simplicity assume that the designers choosing 10 equally sized PSVs what when summed together will relieve the throughput for the limiting case (10 PSVs will be required to relieve the maximum throughput conceivable). So, if any One PSV does fails to open, then the design case throughput will not be provided; all 10 must open. If the designers do Not take into account the fault tree PFD calculation for the combined failures of the similar PSVs, then the PFD required for process safety of the relief system (all relief devices taken together as a relief system) will be too high, and the system will be under protected. This issue is summarized below:

- Target PFD for the relief system = 0.01
- PFD_1 of each relieve device (PSV) = about 0.01
- 10 PSVs required for the target throughput of the limiting case scenario, meaning if PSV_1 fails to open then we are unprotected from then limiting case, or if PSV_2 fails to open we are unprotected from the limiting case, or etc. for all 10 PSV_N. The overall system PFD is therefore calculated using fault tree as OR gates, which can be approximately reasonably well by summing the discreet PFD of each of the 10 PSVs.

- Therefore, the PFD_{SYS} of the relief system if all 10 PSVs (10oo10) must open for the limiting design case is given approximately as = $\sum$ (PFD_1 of single device) + β* PFD_1 = 10*(0.01) + 0.1*0.01= 0.101 (target PFD Not met)

  Where β is the fraction of failures due to common causes in the design of similar PSVs; this factor for PSVs is approximated here as β = 0.1 (10% fractional failure rate of a single device)

In this case, the set of NooN relief devices will be a factor of 10 less effective than the target PFD of the system (the PFD of the entire relief system is 10 times higher than the target PFD).

If the designers understand the how to estimate the PFD for a multiple device system, then they will instead include extra PSVs in the design, and achieve an MooN design, when M is the number of devices that must open to meet the capacity requirement and N is the total number of PSVs provided in the design. For such designs, then PFD of the system includes OR logic and AND logic, as the extra PSVs (those beyond what is minimally required for the throughput capacity alone) provide standby redundancy against the failure of other PSVs in the relief system. For this case, the PFD_{SYS} of the relief system of the N PSVs given MooN must open to reach the full throughput capacity of the limiting case can be approximated as:

$$PFD_{SYS} = (N!/((N-M+1)!*(M-1)!) * (2PFD_{1oo1})^{N-M+1})/(N-M+2) + \beta* PFD_{1oo1}$$

If MooN is 10oo11 (one additional PSV added to the design, and all 11 PSVs are designed to be online all of the time), then:

PFD_{SYS} (for 10oo11 case) = 0.0083 (target PFD met)

For this case the target PSV was met by adding one extra PSV and the designers simply need to account for the 11th PSV in the overall design of the hydraulics of the relief system.

2 Deficiency in the planning of ITPM activities – dependent human errors are not considered in the planning of tests or checks or PM of similar components in a system consisting of multiple key devices

Another major design deficiency seen across nearly ALL sites (hundreds) around the world is that the PFD of the relief or SIS system failed to account for dependent human errors when multiple similar devices are key to the PFD of the system. This is not a design error, per se, though designs can helped compensate for such errors. Instead this error in inherent in the programming / planning / scheduling of the ITPM activities related to a multiple channel system, as when there is more than one final element, such as multiple PSV or multiple safety block valve (XV), or more than one sensor channel in an SIS.

Probability of repeat errors (Coupled errors) – For many maintenance tasks, making a repeat error or "common cause error" or "dependent error" can lead to failures of all backup systems. Such errors have led to major process safety accidents as well as MANY airplane crashes.

Coupling represents the probability of repeating an error (or repeating success) on a second identical task, given that an error was made on the first task. The increased probability of failure on subsequent tasks given that an error has already been made is known as dependence. The list below provides some starting point guidance on values to use:

- 1/20 to1/90 – if the same tasks are separated in time and if visual cues are not present to re-enforce the mistake path. *This error rate assumes a baseline error rate of 1/100 with excellent human factors. If the baseline error is higher, then this rate will increase as well.*
- 1/2 – if the same two tasks are performed back-to-back but the worker is not in line of sight of the other component/device he/she already worked on, and if a mistake is made on the first step of two. *This error rate assumes a baseline error of 1/100 with excellent human factors. If there the baseline error is higher, then this rate will increase as well.*
- 8/10 to 10/10 – if the same two or three tasks are performed back-to-back and a strong visual cue is present (if you can clearly see the first devices you worked on), and assuming a mistake is made on the first of the two or more activities.
- Two or more people become the same as one person (with respect to counting of errors from the group), if people are working together for more than three days; this is due to the trust that can rapidly build. So, double-checking by someone you regularly work with is not a safeguard.

These factors are based on the relationships provided in NUREG-1278[1] and the related definitions of weak and strong coupling provided in the training course by Swain (1993) on the same topic [2], as shown here in Table 1. The following relationship is for errors of omission, such as failing to reopen a root valve or failing to return a safety instrumented function (SIF) to operation, after bypassing the SIF. The qualitative values in Table 1 are based jointly on Swain[1,2] (1983, 1993) and Gertman (SPAR-H, 2005 which is NUREG/CR-6883) [3].

One can readily conclude that staggering of maintenance tasks for different channels of the same SIF or for related SIFs will greatly reduce the level of dependent errors. Unfortunately, most sites PII visits do not stagger the inspection, test, or calibration of redundant channels of the same SIF or of similar SIFs; the reason they cite is the cost of staggering the staff. While there is a perceived short-term higher cost, the answer may be different when lifecycle costs are analyzed.

Simple Rule: Staggering of maintenance can prevent significant number of human errors in redundant channels. In fact, the US Federal Aviation Administration (FAA) requires staggering of maintenance for aircraft with multiple engines or multiple control systems (i.e., hydraulics) (*FAA Advisory Circular 120-42A*, as part of Extended Operations (ETOPS) approval).[4] (ETOPS is Extended-range Twin-engine Operational Performance Standards, a rule which permits twin engine aircraft to fly routes which, at some point, are more than 60 minutes flying time away from the nearest airport suitable for emergency landing.)

Table 1: Guideline for Assessing Dependence for a within-SIF Set of Identical Tasks (based partially on SPAR-H, 2005 [3] and partially on field observations by PII)

Level of Dependence	Same Person	Actions Close in time	Same Visual Frame of Reference (can see end point of prior task)	Worker Required to Write Something for Each Component
Zero (ZD)	No; the similar tasks are performed by different person/group	Either yes or no	Either yes or no	Either yes or no
Zero (ZD)	Yes	No; separated by several days	Either yes or no	Either yes or no
Low (LD)	Yes	Low; the similar tasks are performed on sequential days	No	Yes
Moderate (MD)	Yes	Moderate; the similar tasks are performed more than 4 hours apart	No	No
High (HD)	Yes	Yes; the similar tasks are performed within 2 hours	No	No
Complete (CD)	Yes	Yes; the similar tasks are performed within 2 hours	Yes	Either yes or no

The level of dependency is determined from Table 1 by assessing whether the same person is doing the tasks, the proximity of the actions in time, the proximity of the actions in space (same visual frame of reference), and whether the work is required to make a record for each component:

1. Read down the "Same Person" column and find the applicable row(s), then
2. Read down the "Actions Close in Time" column and find the applicable row,
3. Then check the two columns on the right for that row.
4. The Level of Dependence is shown in the left-most column for the applicable row.

Table 1 has two rows for Zero Dependency (ZD) because ZD can be achieved two different ways:

- Tasks done by different persons or groups (staggered people), or
- Tasks done by same persons or groups, but tasks are done several days apart (staggered times).

Once the level of dependence is known, the probability of either repeat success or repeating errors on identical tasks can be estimated. For these probabilities, we use Table 2, which is a re- typing of Table 20-17 from NUREG-1278[1] (and the similar table in SPAR-H [Gertman, 2005] [3]).

Table 2. Equations for Conditional Probabilities of Human Success or Failure on Task N, given probability of Success (x) or Failure (X) on Task N-1, for Different Levels of Dependence *Courtesy Process Improvement Institute, Inc., All Rights Reserved*

Level of Dependence	Repeating Success Equations (but shown as error probability)	Repeating Failure Equations
Zero (ZD)	$P_{Success@N} = x$	$P_{Failures@N} = X$
Low (LD)	$P_{Success@N} = (1+19x)/20$	$P_{Failures@N} = (1+19X)/20$
Moderate (MD)	$P_{Success@N} = (1+6x)/7$	$P_{Failures@N} = (1+6X)/7$
High (HD)	$P_{Success@N} = (1+x)/2$	$P_{Failures@N} = (1+X)/2$
Complete (CD)	$P_{Success@N} = 1.0$	$P_{Failures@N} = 1.0$

How to Avoid these Repeat Errors (dependent human error) – The straightforward solution is to follow the rules implemented by the US FAA for aircraft maintenance. This requires staggering the maintenance for each similar device in a set of devices that comprise the IPL.

- So, if there are 11 PSVs for the earlier case where 10oo11 PSVs must open for the design case, then set up the ITPM program such that either (1) there is 3 days between the servicing of each PSV in the set of 11 PSVs (if serviced by the same crew) or (2) have a different crew do the blocking, removing, checking, re-installing of each PSV that is checked on the same day.

- Similarly, if there are 3 instrument channels on a SIL 2 SIF, then either (1) ensure there are 3 days between the servicing of each channel in the SIF if performed by the same technician or (2) have a different technician do the testing, calibration, or checking of each channel that is checked on the same day.

To implement staggering, the site will need to track the ID number of each worker assigned to inspect or test or maintain devices that make up an IPL so that (1) staggering can be ensured up front and (2) staggering can be verified by auditing.

For more details on the major effect dependent errors can have on SIFs, read the earlier papers on the topic [5,6].

One means to improve the reliability and independence of the instrumented system is to use a smart sensor/transmitter for the LSH which will detect null movement of the sensor reading, indicating the valve is closed on the tap is plugged. Another possibility is to implement a limit switch (or captive key system) on the root valve. There is a probability that these safeguards against human error will also fail or be bypassed by the staff, but assuming the probability of that failure is the same as other human errors for this example, 0.02, then the systemic human error drops to about zero as the probability of leaving the root valve closed is now ANDed with the probability of smart sensor/transmitter or limit switch failing, [6].

3 Failing to Account for the Human Error Inherent in the positioning of Root Valves (block valves)

Another major deficiency in high integrity systems is failing to account for the relative probability of human error for such simple tasks like re-opening the block valves on either side of a PSV before the PSV is returned from servicing or similarly failing to re-open the root valve between the process and sensor of SIFs after servicing/checking. One common approach that used by industry is require a lock, or car seal (put in place by a human) on the block valve or root valve, and then administratively ensure the valve is indeed open by an checking the valve position and the placement of the Open Tag using someone other than the person who changed the position of the valve back to open when the maintenance activity was completed. The most common term for such administrative systems is a Car Sealed Open (CSO) or Locked Open (LO) or Chain Locked Open (CLO) system.

The problem observed with such systems, is when the checker is from the same site /local organization, then checking is not truly independent. During the writing of *Guidelines for Initiating Events and Independent Protection Layers*, 2015, CCPS/AICHE [7], the committee members stated that checkers from a site would report that all CSO or LO valves were found in the as-desired position (typically Open) but when an independent checker (from outside of the site) was used to do an unannounced check, they found 4/100 block valves in the wrong position. So, for a PSV, the impact on the system PFD is large:

- Target PFD for the relief system = 0.01
- PFD_1 of each relieve device (PSV) = about 0.01
- Probability of leaving at least one block valve upstream or downstream of a PSV closed is about: P_{HUM_ERR} = about 0.04
- Therefore, the PFD_{SYS} of each relief system with a block valve upstream or downstream is approximately = $PFD_1 + P_{HUM\_ERR} = 0.01 + 0.04 = 0.05$

In this case, the relief system for even a single PSV with block valves will be a factor of 5 less effective than the target PFD of the system (the PFD of the system is 5 times higher than the target PFD).

SIL 2 and SIL 3 SIFs are impacted to the same extent.

How to Avoid these Increases in the Overall PFD of the IPL – The straightforward solution is to not have block valves upstream or downstream of PSVs and not have root valves for SIL 2 or SIL 3 SIFs. But this solution is not always possible due to shutdown schedules for the plant (since if there are no isolation valves, maintenance can only be done when the process line is shutdown).

Another solution is having a truly independent check by an outside auditor about once per year, to find any valves in the incorrect position and to continually encourage accurate internal auditing of CSO, CSC, LO, LC block valves and any SIF root valve. This solution will cost about 1 to 2 staff-days of labor per 100 PSVs or 100 SIFs.

CASE STUDY on Third Party Inspection of CSO Valves for 448 PSV at UNITED (a SABIC Affiliate) in Jubail, Saudi Arabia:

PII was contracted by UNITED to check enough PSVs to determine the actual error rate at the site of PSV block valves being in the wrong position (and also CSO tags missing, though the tag does not affect the functioning of the PSV, obviously, although a missing tag implies that it is more likely in the future for the). There are approximately 2000 PSVs at the site and about 1423 in the 4 units that PII inspected. In these 4 units, 890 of these PSVs were inspected, but only 448 of the PSVs had a block-valve upstream, downstream, or both. (Since the likely error rate was expected to be between 0.005 to 0.05, PII chose to check about 500 PSVs with block valves.) One process safety engineer with 10+ years' experience was assigned to perform this check. Of the 448 PSVs (with block valves) that were checked, zero (0) were found to have a block valve upstream or downstream or both closed instead of open, without there being a valid reason (such as out-of-service for a valid reason); one (1) was found in the wrong position but there was a maintenance work-order for the related vessel. In addition, of the 840 block valves checked (counting both upstream and downstream), 79 were missing car seals, but the valve was in the proper position. The data from the inspection is summarized on the next page.

In this case, the positioning of the block valves were excellent, meaning that the PFD of the relief system is essentially the same as the PFD of the PSV alone, so the human error rate of mispositioning of the block valves are low enough to not effect the estimated PFD of the relief system at this site. But roughly 9% of the car seals were missing (mostly in one unit) which needs to be corrected. The site 50% converted to a more robust car seal mechanism, using uniquely printed metal seals, with plastic encases metal cables. They believe this system will greatly reduce the number of missing seals.

One last caveat on the data reported above: The inspection by a third party (PII) of the car seals was announced in October 2019, but the actual inspection by PII slipped until February 2020. It is possible, therefore, that the staff in the units took extra care in the 4 months to ensure the block valves were in the proper position. But there is no way to know for sure. But if special care was taken, then why were so many car seals missing?

RESULTS of THIRD PARTY INSPECTION of CSO Block Valves for PSVs at UNITED

			Upstream						Downstream					
Unit	PSV Total in Unit	PSV Total Sample	# BVs	# BVs wrong	# CSs on BV	# CS Missing	Fraction (Probability) BVs wrong	Fraction (Probability) Missing CS	# BVs	# BVs wrong	# CSs on BV	# CS Missing	Fraction (Probability) BVs wrong	Fraction (Probability) Missing CS
A	534	363	238	0	237	1	0	0.0042	154	0	153	1	0	0.007
B	65	49	35	0	35	0	0	0.0000	22	0	22	0	0	0.000
C	276	211	43	0	40	3	0	0.0698	154	0	7	0	0	0.000
D	548	267	132	0	89	43	0	0.3258	62	0	31	31	0	0.500
TOTAL	1423	**890**	**448**	**0**	**401**	**47**	**0**	**0.1000**	392	**0**	**213**	**32**	**0**	**0.127**

4 Failing to Account for the Human Error in the Baseline Estimation of the PFD.

The last major deficiency in high integrity systems to be covered in this paper is failing to account for the specific probability of human error in the PFD of the IPL, including for a single PSV installation, a multiple PSV set IPL, and SIL 2 or SIL 3 SIFs. A few of the specific human errors were discussed in sections 1-3 of this paper. For a SIF, below are the typical human errors of interest:

- Probability of leaving the root valve for the level switch (sensor/transmitter) closed
- Probability of leaving the entire SIF in BYPASS after maintenance or after some other human intervention (such as an inadvertent error or as a necessity during startup)
- Probability of miscalibration of the level transmitter/switch.

The new issue here applies to SIL 2 and SIL 3 SIFs more than to PSV or multiple PSV or single or multiple checkvalve IPLs. The reason is that for a SIF the user is required to a complete a SIL Verification calculation that states that the target PFD was achieved by the design. But, as explained in two earlier papers [5,6], the guidelines and standards for SIS from IEC and from ANSI/ISA do not require inclusion of the probability of human error (P_{HUM_ERR} **)** in SIL Verification. If the human error is not required to be in the estimate of the overall PFD of the SIF, then why try to control the human error? Further, leaving such terms out may give false hope that a high integrity IPL was actually achieved, whereas it nearly impossible to actually achieve a PFD of 0.001 for a SIL 3, due to the human error probability that cannot be lowered enough. A SIL 3 with a PFD of 0.001 is as rare as a Unicorn (they very likely do not exist) [6].

In this case, for any IPL with a target PFD of 0.001, the system will typically have a PFD that is 10 times greater than predicted, because the human error contribution was omitted from the PFD estimate. This can lead to the risk of a scenario being too high, and can lead to wasting resources on an IPL that the company believes is much more reliable than it actually is [6].

5 CLOSING

High integrity IPLs, such as PSVs, multiple PSVs with extra capacity, and SIL 2 and SIL 3, are highly vulnerable to human error and to mis-design. These errors have been observed across hundreds of facilities that use or make highly hazardous chemicals. But once these vulnerabilities are known, an organization can take measures to reduce the vulnerability. Not knowing about these vulnerabilities or not addressing them can lead to much higher risk of major accidents, or misallocation of funds and efforts on the wrong IPLs.

6 Acronyms Used

10oo10	ten out of ten voting architecture; all 10 devices must work for the safe state
10oo10	ten out of ten voting architecture; all 10 devices must work for the safe state
ANSI	American National Standards Institute
CD	Complete Dependence
CSC	Car Sealed Closed
CSO	Car Sealed Open
D	Dangerous
ETOPS	Extended-range Twin-engine Operational Performance Standards
FAA	US Federal Aviation Administration
IPL	Independent Protection Layer
ISA	International Society of Automation
LC	Locked Closed
LD	Low Dependence
LO	Locked Open
LOPA	Layer of Protection Analysis
MooN	M devices out of N total devices
NooN	N devices out of N total devices
P	Probability
PFD	Probability of Failure (dangerous) on Demand
PII	Process Improvement Institute, Inc.
PSV	Pressure Safety Valve
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SYS	Systematic failure contributions to overall PFD
HUM_ERR	Specific human errors and failures generated by human error
ZD	Zero Dependence

CSO, CSC, LO, LC

7 References

References Cited

[1] A. Swain and H. Guttmann, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Sandia National Laboratories*, 1983 [this document became NUREG/CR-1278– The Human Reliability Handbook, guidelines from the US NRC on Human Reliability Analysis].

[2] A. Swain, *Human Reliability Analysis*, Training Course, ABS Consulting (formerly JBF Associates), 1993.

[3] D. Gertman, H. Blackman, J. Marble, J. Byers, and C. Smith, *The SPAR-H Human Reliability Analysis Method*, NUREG/CR-6883, U.S. Nuclear Regulatory

Commission, Office of Nuclear Regulatory Research, Washington, DC, August 2005.

[4] US Federal Aviation Administration, "AC 120-42B - Extended Operations (ETOPS and Polar Operations)", Washington, DC, June 13, 2008

[5] W.G. Bridges and H.W. Thomas, "Accounting for Human Error Probability in SIL Verification Calculations", 8th Global Congress on Process Safety, Houston, TX, April 1-4, 2012, American Institute of Chemical Engineers.

[6] A. Dowell III, W.G. Bridges, H.W. Thomas, and M. Massello, "SIL-3, SIL-2, and Unicorns", 15th Global Congress on Process Safety, New Orleans, LA, March 31 - April 3, 2019, American Institute of Chemical Engineers.

[7] CCPS, *Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis*, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY, 2015.