Safety Instrumented Systems in Lieu of Pressure Relief Valves

Dustin J. Smith, P.E.

Smith & Burgess
Process Safety Consulting

7600 W. Tidwell Rd., Ste. 600 | Houston, TX 770400
(713) 802-2647 | SmithBurgess.com

Safety Instrumented Systems in Lieu of Pressure Relief Valves

Abstract

There are two aspects to risk assessments: safety issues and regulatory issues. Usually the two are aligned, but not always. This article explains ASME B&PVC Section VIII (Sec VIII)1 requirements along with other industry guidance for using Safety Instrumented Systems (SIS) in lieu of Pressure Relief Devices (PRD, e.g. Pressure Relief Valves or Rupture Disks). For most pressure vessels in petrochemical installations in the United States, the Sec VIII requirements are regulatory requirements. A designer that is implementing facility changes from a corporate risk assessment (e.g. LOPA or HAZOP) would do well to also meet the minimum regulatory requirements for overpressure in Sec VIII. Typical risk assessments allow the designer to consider both the likelihood and consequences of an overpressure scenario in determining if additional mitigation is required. Whereas, Sec VIII does not allow any credible overpressure scenarios (solely based on likelihood) unless there is adequate capacity provided by a relief device. This paper discusses the detailed typical risk analysis compared to the requirements of Sec VIII overpressure protection by system design.

The SIS reliability rating or determination of said rating (e.g. SIL-3 Systems) is outside the scope of this article.

Introduction

In the past ten years, the availability, reliability, and industry acceptance of SIS increased while the cost of these systems decreased. In addition, the continued pressure on organizations to identify and mitigate risk through programs like LOPA (Layer of Protection Analysis) has led to more instances where SISs are the preferred safety devices. Overpressure protection can be provided by system design with SIS, with the introduction of UG-140 into Sec VIII. However, making changes to the facility to meet the corporate risk guidelines may result in a system that does not meet the overpressure protection requirements in Sec VIII, which has specific requirements that are different than typical LOPA implementations. For example, Sec VIII requires systems with water, air or nitrogen to use PRDs if the maximum inlet pressure exceeds 116% of the MAWP.

This article presents a review of the Sec VIII requirements of SIS and safety that can be correlated to speeding. The following is an attempt to illustrate what is meant:

> *Going 35 in a 30 mph* - Are you materially less safe going 35 mph in a 30 mph speed area? Probably not, but it is the wrong argument to make if your goal is to operate the motor vehicle legally and safely. Clearly going 60 mph through a neighborhood is not acceptable. Is following your companies risk assessment (or API's or LOPA's) less safe than following Sec VIII? Possibly not, but where do you draw the line – especially if regulatory agencies have drawn one by Code?

The alternative argument is also valid, just because a vessel is installed to the letter of Sec VIII does not mean that it meets the corporate safety requirements. Again a speeding analogy:

Going 25 in a 30 mph - Are you always safe going 25 mph in a 30 mph zone? Clearly not: an example may be if the local elementary school is cleaning the streets and there are 1,000 eight-year olds doing the work. In this scenario, someone driving their car 25 mph is scary fast, more so if one of the eight-year olds is your child. So following your company's risk assessment (or API's or LOPA's) may require more stringent SIS requirements than following Sec VIII which may be warranted.

There are two aspects to risk assessments: safety issues and regulatory issues. Usually the two are aligned, but not always. A designer that is implementing facility changes from a corporate risk assessment would do well to also meet the minimum regulatory requirements.

ASME Requirement Summary

To meet the requirements of Sec VIII for overpressure protection by system design (e.g. using Safety Instrumented Systems in lieu of Pressure Relief Devices) one of two sections of the code applies based on the maximum expected pressure. If the maximum pressure of the system does not exceed the MAWP, a small amount of documentation is required. If the maximum pressure of the system can exceed 116%, then Sec VIII requires: (1) considerable documentation and (2) that the maximum pressure from any credible scenario not exceed 116% of the MAWP. Sec VIII defers to the Welding Research Council (WRC) Bulletin 498 [2] for the definition of credible. WRC-498 defines credible to be the likelihood at which a risk decision considers the event to "not occur" (the example in the document is 1/10,000 years). Any SIS system would be used to reduce the credibility of the scenario to meet the second requirement listed above.

Other Requirements (API, CCPS/LOPA) Versus Those in Sec VIII

The requirements to replace PRDs with SIS are more stringent in Sec VIII than elsewhere in industry guidance. API (in API STD 521 Annex E)3 states that a relief device can be replaced with a SIS system that has a reliability consistent with the:

1. Likelihood the SIS will be required
2. Consequence of the SIS failing
3. Risk tolerance of the user
4. Requirements of the local jurisdiction

Alternatively, the Center for Chemical Process Safety's (CCPS) LOPA book[4] reviews overpressure protection as one of many possible hazards and requires enough Independent Protection Layers (IPLs) to fill the LOPA gap. The CCPS LOPA guidelines suggest the Probability of Failure on Demand (PFD) of a relief device as between 1/10 and 1/100,000. To base a decision solely on PFD equivalency, one could hypothetically eliminate a relief device with a marginally reliable SIS or potentially even a basic process control valve. LOPA requires that the SIS reliability be specified such that it mitigates the LOPA gap (e.g.

a more reliable system is required to prevent more severe consequences). This is the biggest difference between the LOPA analysis and the requirements in Sec VIII. API/LOPA bases the required reliability of the SIS on consequence severity, whereas Sec VIII does not. In most instances of LOPA that have been reviewed by the author, compliance with external standards or regulatory requirements are not reviewed.

While this may be useful for most other areas of risk assessment, for overpressure protection it may lead to regulatory exposure. Also, the confusion of this nuance for safety requirements is astounding. The worst case the author has seen is a process designer taking credit for a level controller to prevent overfilling on a feed surge drum that had a pressure relief device installed that is undersized for this contingency. This is illustrated in Figure 1, which considered using LCV-1 to protect V-1 from overfilling because PSV-1 was undersized and could not provide protection. The problem with LCV-1 as an IPL is that it could not prevent overpressure in the event the liquid increase was caused by: (1) a high pressure situation downstream of P-1; (2) a closed isolation valve in the line from V-1 downstream; or (3) failure of P-1. In addition, failure of LCV-1 could also be the overpressure scenario initiating event that would require consideration and mitigation. Thus, irrespective of the reliability of LCV-1 compared to PSV-1 (1/10 or 1/100), this SIS cannot perform all the safety instrumented functions and should be discounted as a viable option. Granted, this example does not strictly follow the CCPS LOPA Guidelines.

Regulatory Requirements to Use ASME B&PVC Section VIII

Complying with the overpressure protection requirements of Sec VIII is a regulatory requirement in most instances for pressure vessels in refining or petrochemical installations in the United States. This is because:

- In the United States as a whole, if the fluid is subject to OSHA's Flammable Liquids Code (29 CFR 1910.106) then federal law states that pressure vessels SHALL be built and installed per the 1968 version of Sec VIII if the vessel is used for storage. In refineries and chemical plants, all pressure vessels that contain liquids within the scope of 1910.106 must be built per ASME Section VIII. Interpretations of the OSH Act have allowed industry to comply with current versions of the code (e.g. CPL 03-00-004).
- While states have laws varying from quite prescriptive (e.g. California) to simply relying on federal law (e.g. Wyoming), most states require that pressure vessels comply with Section VIII.[5]

Relief systems designers may find the National Board Synopsis of Boiler and Pressure Vessel Laws, Rules and Regulations (NB-370) useful as it is a summary of local laws and regulations for the United States and Canada.

Overpressure Protection by Design

The following is a summary of the requirements in Sec VIII UG-140 and the referenced WRC-498 for the minimum requirements to eliminate an overpressure scenario using SIS. Appendices 1, 2, and 3

document the requirements in much more detail. These requirements can lead to more stringent SIS reliability requirements than would be specified if based on other industry standards (e.g. API or LOPA).

1. The decision and responsibility to provide overpressure protection by design is up to the user and must be thoroughly thought through, vetted, and documented.
2. There shall be no credible scenario that exceeds 116% of the MAWP. All potential overpressure scenarios that exceed 116% of the MAWP need to be instrumented or designed out of the system (made not credible). *Note that Sec VIII / WRC-498 do not allow for the consequence of overpressure to modify the acceptable scenario frequency.*
3. The analysis is documented and signed by the individual in charge of the unit. This report shall include: drawings, description of the scenarios, and detail the SIS.

The biggest difference between Sec VIII requirements and the CCPS LOPA guidelines is that LOPA allows the user to consider risk and therefore the consequences of overpressure in determining the reliability of the SIS, while Sec VIII explicitly does not.

The following example shows this for two simple systems:

First, a simple risk assessment for the system shown in Figure 2 (using the generic risk matrix found in Table 1) will be performed. This system will be contrasted with another system shown in Figure 3. The analysis for each system will analyze overpressure due to a closed outlet and is predicated on the PSV providing adequate overpressure protection for an external fire scenario but not for the closed outlet scenario.

Overpressure Scenario: Failure closed of FCV-2 resulting in a blocked outlet where the maximum pressure from P-2 (250 psig) exceeds the MAWP (200 psig). Guidance is to assume that a basic process control system will fail 1/10 years.

Scenario Consequence: Failure closed of FCV-2 results in blocked outlet and, if not mitigated, a maximum pressure in the Lube Filter (V-2) of 1.25x the MAWP. Consensus Standard Guidance (API 581 Risk Based Inspection Technology, second edition, Table 7.13)[6] is that it is improbable that a release will occur from this overpressure. However, the potential for gasket leaks was considered and a Consequence of 1 was chosen (based on the risk matrix shown in Table 1).

Current Scenario Frequency: The initiating event frequency is 1/10 years. Thus, the likelihood that the event will occur is 1/10 years, but the complete scenario requires that the event occur and the gasket leaks. The system has been hydrotested to 1.5x the MAWP, which is beyond the maximum potential pressure of 250 psig from the pump. Furthermore, 250 psig at lube oil temperatures is below the limits in ASME B16.5 (260 psig @ 200 °F) for the associated piping. Thus, even if overpressure occurs, it is assumed that a leak is a *rare* event for this system. As such, the frequency gets adjusted to 1/100 to 1/10,000 years based on the maximum pressure and the verbiage in the risk matrix and Table 7.13 in API 581. Therefore, the frequency was set to C, rare, for the system to overpressure and a leak to occur and cause economic damage or hurt someone.

Current Scenario Risk: With a consequence of 1 and a likelihood of C, the risk matrix shows "Low Risk" or 1C. Per LOPA, the system is adequate as is, and modifications are not required for risk reduction.

Sec VIII Analysis - The system has a credible cause of overpressure that exceeds 1.16x the MAWP and does not have adequate relief protection. Therefore, modifications are required to reduce the scenario

frequency to not credible (1/10,000 years Category D from the risk matrix). With the initiating event frequency of 1/10 years, the reduction in frequency needed is 1/1,000 years ,which would need to be mitigated with SIS.

Thus to meet the requirements of Sec VIII, the system requires mitigation irrespective of the LOPA results.

Overpressure Scenario: Failure closed of FCV-3 resulting in a blocked outlet where the maximum pressure from P-3 (500 psig) exceeds the MAWP (200 psig) of the C4 Filter (V-3, Figure 3). Guidance is to assume that a basic process control system will fail 1/10 years.

Scenario Consequence: Failure closed of FCV-3 results in blocked outlet and, if not mitigated, the maximum pressure in the C4 Filter (V-3) could be as high as 2.5x the MAWP. Consensus Standard Guidance (API 581 Risk Based Inspection Technology, second edition, Table 7.13) states that there is a potential that a major release occurs and multiple gasket leaks are probable. For a ground level release of hot Butane, an unmitigated consequence of 4 was selected (based on the risk matrix shown in Table 1 due to the high potential of a Vapor Cloud Explosion).

Current Scenario Likelihood: The initiating event frequency is 1/10 years. , the most frequent likelihoods that the event can occur is 1/10 years, but the complete scenario above requires that the event occur and there is a significant leak or loss of containment which causes harm. Because the system has very little instrumentation and the maximum pressure is 2.5x the MAWP, it is considered probable that an overpressure event will lead to a loss of containment (based on the maximum pressure and the verbiage in the risk matrix and Table 7.13 in API 581). Therefore, the likelihood was set to B, *likely*, for the system to overpressure and for a leak to occur and cause a level 4 Consequence. A "*probable" likelihood* was not chosen since the least frequent A (1/10 years) is the initiating event frequency. Because there is a possibility of the event without a release, the modified likelihood is less than *probable*. Thus, any chance that an overpressure will not result in a loss of containment drives the frequency category to *likely* as the most frequent basis.

Current Scenario Risk: With a consequence of 4 and a likelihood of B, the risk matrix shows "Unacceptable Risk" and modifications are required. Because the consequence will most likely be unable to be mitigated, the likelihood of a release will need to be reduced by 1/100 to 1/1,000 years to move the scenario from an Unacceptable Risk to a Manageable Risk.

Sec VIII Analysis - The system has an overpressure scenario that exceeds 1.16x the MAWP. Therefore, modifications are required to reduce the scenario frequency to 1/10,000 years (Category D from the risk matrix, Table 1). With the initiating event frequency of 1/10, the "gap" is 1/1,000, which needs to be filled.

Table 2 shows that a system can meet the risk requirements using a LOPA analysis but still requires additional mitigation per Sec VIII. As shown in Table 2, the Sec VIII analysis will yield the same SIS requirements for systems irrespective of the consequence of failure of those systems; whereas most risk assessments performed by industry heavily factor in the consequence (by definition).

For some risk matrices, the LOPA for the C4 Filter (Figure 3) could require a more reliable SIS than what would be required by Sec VIII. Furthermore, for the system described in Figure 3, even if PSV-3 was adequately sized for the failure closed of FCV-3, the risk analysis may require additional SIS protection.

The most protection a PSV can provide is 1/100 years (per the example given in the CCPS LOPA guidelines), whereas Sec VIII would consider the system acceptable.

Conclusion

The purpose of this article was to summarize the requirements between Sec VIII and other industry guidance for the use of Safety Instrumented Systems (SIS) in place of Pressure Relief Devices (PRDs). For most pressure vessels that are (or are required to be) designed to ASME B&PVC Section VIII, the code allows the user to specify SIS rather than PRDs (with some service exceptions, see Appendix 2). One of the requirements listed in UG-140 is that there cannot be an overpressure scenario which exceeds the MAWP and is deemed credible. Sec VIII refers the user to WRC-498 to help determine what is meant by "no credible overpressure scenarios". The WRC document allows the user to base the decision on industry guidance, a qualitative analysis, or a quantitative analysis. The examples used in WRC-498 place the frequency of a non-credible scenario at 1/10,000 years. As shown in the examples and summarized in Table 2, the requirement that the scenario be non-credible is generally more stringent than other industry guidance depending on individual company tolerability critera.

References

[1] American Society of Mechanical Engineers, 2013 ASME Boiler & Pressure Vessel Code: Section VIII, Division I. s.l.

[2] J. R. Sims and W. G. Yeich, Welding Research Council, Bulletin 498, January 2005.

[3] API Standard 521, "Pressure-Relieving and Depressuring Systems," American Petroleum Institute, 6th ed., 2014.

[4]Center for Chemical Process Safety, *Layer of Protection Analysis – Simplified Process Risk Assessment*, American Institute of Chemical Engineers, New York, 2001.

[5] National Board Synopsis of Boiler and Pressure Vessel Laws, Rules and Regulations (NB-370).

[6] API Standard 581, "Risk-Based Inspection Technology" American Petroleum Institute, 2nd ed., 2008.

Appendix 1: P_{Max} < MAWP (or < 116% of the MAWP)

This appendix details the requirements in Sec VIII UG-140 for the cases where the maximum unmitigated supply pressure is less than the MAWP/T. MAWP/T is a shortening of the phrase "equal to the MAWP of the vessel at the coincident temperature". The system can be protected by design given the listed criteria is met:

1. It is the user's responsibility to decide and the user shall request that the Manufacturer's data report state that overpressure protection is provided by system design per UG-140(a).
2. Conduct a detailed analysis of the overpressure scenarios:
   - Scenarios in API STD 521 shall be considered
   - A multi-disciplinary team must perform a hazards analysis (e.g. HAZOP, FMECA, What If, or equivalent) to ensure that there are no sources of overpressure.
3. The analysis is documented and signed by the individual in charge of the unit. This report shall include:
   a. P&IDs showing all elements of the system associated with the vessel
   b. Description of all the operating and upset scenarios (including fire) that result from operator error, equipment and/or instrumentation failure

c. Analysis of the maximum pressures / temperatures for all upset scenarios detailing them to be within the limits of the MAWP/T.

Note that most of the requirements collapse to these requirements if the supply pressure is less than 116% of the MAWP/T.

Appendix 2: P_{Max} > MAWP (or > 116% of the MAWP)

This appendix details the requirements in Sec VIII UG-140 for the cases where the maximum unmitigated supply pressure is greater than the MAWP/T. Item 5 below requires that the SIS make the scenario that has the maximum unmitigated pressure non-credible. The system can be protected by design without a relief device or with the combination of a relief device and system design given the listed criteria is met:

1. The vessel does not contain only air, water, or steam (unless the loss of containment of these services/fluids creates a significant safety/environmental concern).
2. It is the user's responsibility to decide and the user shall request that the Manufacturer's data report state that overpressure protection is provided by system design per UG-140(b). If no PRD is installed, jurisdictional acceptance may be required.
3. Conduct a detailed analysis of the overpressure scenarios:
   - Scenarios in API STD 521 shall be considered
   - A multi-disciplinary team must perform a hazards analysis (e.g. HAZOP, FMECA, What If, or equivalent) to ensure that there are no sources of overpressure.
4. The overpressure scenarios shall be readily apparent so that operators or protective instrumentation can take corrective action to prevent the pressure from exceeding the MAWP/T.
5. There shall be no credible scenario that exceeds 116% of the MAWP
   - The overpressure limit shall not exceed the test pressure
   - Credible events or scenario analysis shall be performed per WRC-498.
6. The analysis is documented and signed by the individual in charge of the unit. This report shall include:
   a. P&IDs showing all elements of the system associated with the vessel
   b. Description of all the operating and upset scenarios (including fire) that result from operator error, equipment and/or instrumentation failure
   c. Detailed description of any safety critical instrumentation used to limit the pressure including:
      - Identification of truly independent redundancies
      - Reliability evaluation (quantitative or qualitative) of the system.
7. Analysis of the maximum pressures / temperatures for all upset scenarios detailing them to be within the limits of the MAWP/T.

Appendix 3: WRC Guidance for Not Credible

Sec VIII refers the user to the WRC-498 to determine if an overpressure scenario is credible. This appendix summarizes the requirements in WRC-498 for the user. WRC-498 suggests using one of three methods for determining the credibility of the scenario. Based on this document, these methods only determine scenario credibility, not consequence. It is stated that for Code case 2211 (which was incorporated into Sec VIII as UG-140 in 2007), if credible, then one must mitigate irrespective of the consequence.

1. **Accepted Industry Practice (§3.1.2.1) -** This would be going through the design criteria from non-ASME standards (e.g. API or NFPA) and if any of these standards state that the case does not need to be considered, then it is not credible. Additionally, the user may discount it as well, with proper documentation.
    a. There is no credible means to raise the pressure over the MAWP (e.g. limiting upstream pressures, elevation differences, etc.)
    b. The equipment creating the pressure is installed to industry standards and/or installation deviations are not relevant to code case 2211
    c. There is a five (5) year history that shows the industry standard/practice is successful in avoiding overpressure
    d. There is a written MOC standard that will ensure that change does not affect this overpressure by design analysis/implementation
2. **Qualitative Risk Analysis (§3.1.2.2) -** This would be using a corporate or site risk matrix to determine if a scenario is credible or not and should be consistent with other risk acceptance tools used by the facility acceptable to the relevant jurisdiction(s).
3. **Quantitative Risk Analysis (§3.1.2.3) -** This would use specific or relevant failure data and generate a Fault Tree Analysis or an Event Tree Analysis to determine the probability of a scenario occurring. *This method is required if a safety instrument system is used as an alternative to a pressure relief device.* The probability is then compared against a corporate or site risk matrix to determine if a scenario is credible. Consistency and jurisdictional caveats are the same as for the Qualitative Risk Analysis.

		Consequences			
		1 Minor First Aid No Offsite Effects < $10,000	**2 Major** Onsite Medical Minor Off-site Effects < $100,000	**3 Severe** Employee Hospitalization Public Disruption (e.g. roads) < $1 Million	**4 Catastrophic** Fatalities / Multiple Injuries Shelter in Place / Public Injuries >$1 Million
Likelihood	**A Probable** > 1/10 years	**Manageable Risk**	**Unacceptable Risk**	**Unacceptable Risk**	**Unacceptable Risk**
	B Likely 1/10 to 1/100 years	**Manageable Risk**	**Manageable Risk**	**Unacceptable Risk**	**Unacceptable Risk**
	C Rare 1/100 to 1/1000 years	**Low Risk**	**Manageable Risk**	**Manageable Risk**	**Unacceptable Risk**
	D Almost Impossible <1/10,000 years	**Low Risk**	**Low Risk**	**Manageable Risk**	**Manageable Risk**

Table 1

Table 1: Summary of SIS Analysis

System	Censuses Standard Analysis			Sec VIII Analysis		
	Consequence	Likelihood	SIS Gap	Consequence	Frequency (years)	Δ Freq (years)
Lube Filter (Figure 2)	Low	C Rare	None	N/A	1/10*	1/1,000
C4 Filter (Figure 3)	Catastrophic	B Likely	1/100 to 1/1,000 years	N/A	1/10	1/1,000

**Because Sec VIII only considers the credibility of the overpressure scenario itself and not the consequences, the frequency gap for both scenarios is the same.*

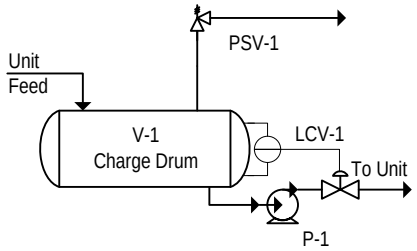

Figure 1: SIS Example

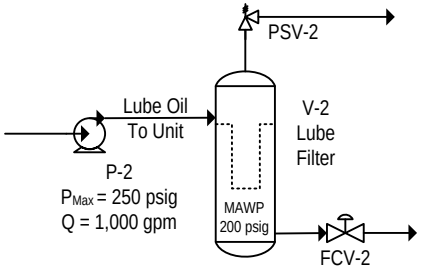

Figure 2: Low Consequence System

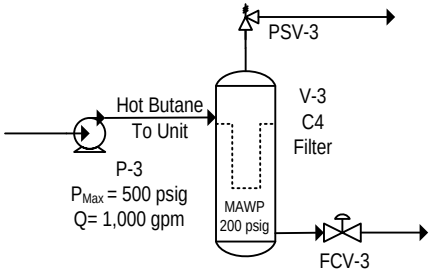

Figure 3: High Consequence System

Safety Instrumented Systems in Lieu of Pressure Relief Valves

Dustin J. Smith, P.E.

Mr. Smith is the co-founder and principal consultant of Smith & Burgess LLC, an engineering consulting firm specializing in Process Safety Management located in Houston, Texas.

7600 W. Tidwell Road, Suite 600
Houston, Texas 77040
Phone: 713.802.2647
info@smithburgess.com
www.smithburgess.com

Keywords: Pressure Relief System Design, Safety Instrumented Systems, Code Case 2211