JUSTIFYING THE USE OF HIGH INTEGRITY PRESSURE PROTECTION SYSTEMS (HIPPS)

Submitted to the
2004 ASME PVP Division Conference
"SIS Application to High Pressure Pipelines and Pressure Vessels"

Edward M. Marszal, P.E., C.F.S.E.

Kevin J. Mitchell, P.E., C.F.S.E.

3366 Riverside Dr, Suite 200
Columbus, OH 43221

KEYWORDS

High Integrity Pressure Protection System (HIPPS), Safety Instrumented Function, SIF, Safety Instrumented System, SIS, Safety Integrity Level, SIL

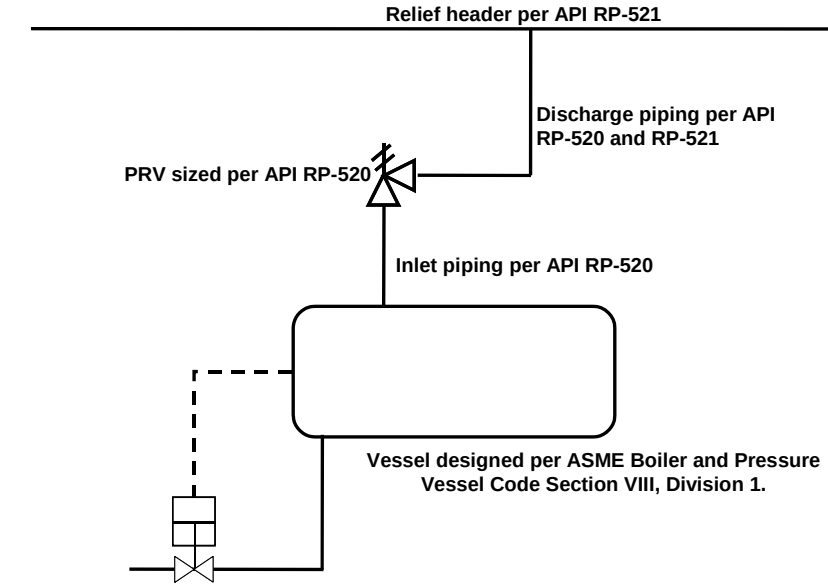
ABSTRACT

As chemical plants and petroleum refineries plan for future expansion, the capability of existing pressure relief systems to safely dispose of higher capacities is often a significant constraint. Current codes and standards now allow for the use of High Integrity Pressure Protection Systems (HIPPS) in lieu of increasing the capacity of emergency relief systems. There is a significant body of knowledge on how to design a HIPPS system once the requirement for one has been established. However, there is gap in knowledge of what situations allow for HIPPS and what practical steps can be taken to determine when a HIPPS is justified. This paper describes the analytical techniques that can be used by engineers to justify a design using instrumented protection in lieu of upgrading the relief system. A review of applicable requirements from codes and standards is included along with risk-based methods to ensure a HIPPS design is as safe as -- or safer than -- conventional relief design.

1.0 Introduction

ASME and the American Petroleum Institute (API) have established standards that govern the design of pressure relieving systems to protect vessels from hazardous overpressure.[1] The applicability of these standards is illustrated in *Figure 1*. Conventional design for petroleum refining involves use of emergency pressure relief devices such as spring-loaded pressure relief valves and disposal using flare systems. Starting in 1996, these codes were amended to allow for examining the reduction in relief system load due to well-designed *Safety Instrumented Systems* (SIS). When the primary purpose of a SIS is to safeguard against equipment overpressure in lieu of conventional relief design, then such a system is referred to as a "High Integrity Pressure Protection System", or HIPPS.

Figure 1 Applicability of Codes and Standards for Pressure Protection



Increasingly, we have noted that there is the potential for upset conditions at chemical plants and refineries that may require equipment to relieve excess pressure at a rate that exceeds the design of flare systems, vent systems, or other disposal systems. Due to this concern, many chemical plants and refineries are now proposing a HIPPS be used to mitigate that potentially hazardous situation. The purpose of the HIPPS is to safeguard against overpressuring equipment and, often, consequently overloading the flare or disposal system.

In general terms, the following overriding considerations apply to analysis and design of a HIPPS system. The overpressure protection system:

1. Must ensure safe equipment operation from overpressure
2. Must comply with applicable laws and ASME Codes
3. Should be consistent with applicable industry recommended practices

The relevant industry consensus codes and standards are:

[1] Overpressure means any pressure in excess of the vessel's Maximum Allowable Working Pressure (MAWP), a safety limit set during the vessel's fabrication.

- American Petroleum Institute (API), Recommended Practice 521, *Guide for Pressure Relieving and Depressuring Systems*, 4th Ed, 1997
- American Society of Mechanical Engineers (ASME), *Boiler and Pressure Vessel Code, Section VIII*, Code Case 2211, August 1996.
- Instrumentation, Systems, and Automation Society (ISA), ANSI/ISA S84.01, *Application of Safety Instrumented Systems for the Process Industry*, 1996.

As per the ASME Boiler and Pressure Vessel code, the key issues to be addressed when using overpressure protection systems in lieu of conventional pressure relief are:

1. Whether the vessel is exclusively in air, water, or steam service
2. User responsibilities in overpressure protection by system design.
3. Ensuring the Maximum Allowable Working Pressure (MAWP) of a pressure vessel is higher than the highest pressure that can *reasonably* be achieved by the system.
4. Risk analysis of the proposed system addressing all credible overpressure scenarios.
5. Proper documentation of the analysis conducted for 3) and 4)

API RP-521 provides the following recommendations for relief system design.

> *Section 2.2: "Fail-safe devices, automatic start-up equipment, and other conventional control instrumentation should not replace pressure relieving devices as protection for individual process equipment.* ***However, in the design of some components of the blowdown header, flare, and flare tip, favorable instrument response of some percentage of the instrumented system can be assumed.*** *The percentage of favorable instrument response is generally calculated based on the amount of redundancy, maintenance schedules, and other factors that affect instrument reliability."*

Both the ASME code and the API Recommended Practice involve making judgments about acceptable risks. API focuses on risk of flare overloading. ASME focuses on risk of individual equipment overpressure.

2.0 Safety Instrumented Systems for Pressure Protection

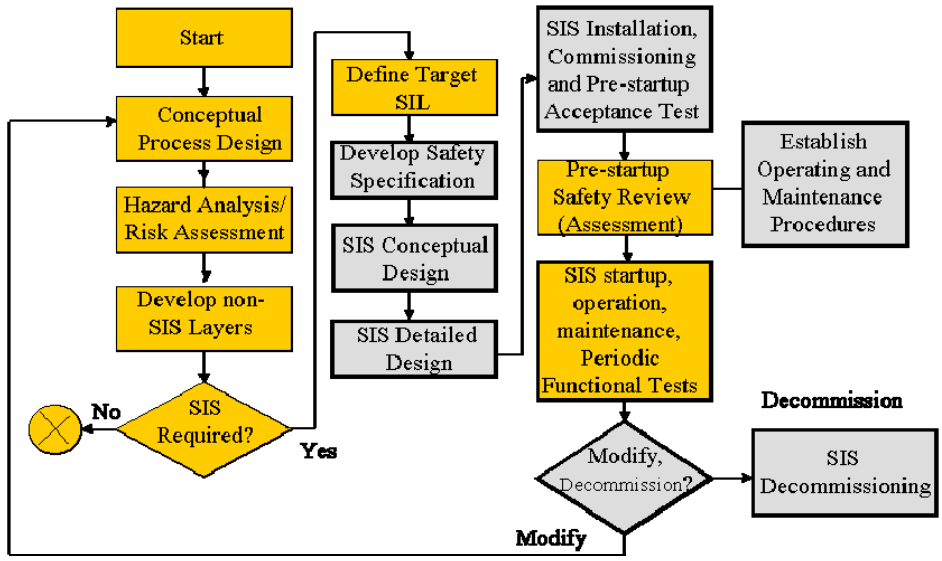
The recent standards describing the implementation of SIS are based on the safety lifecycle. The safety lifecycle is a management system that strives to ensure a functionally safe system if all steps are implemented properly. *Figure 2* illustrates the safety lifecycle provided by ISA. The ISA 84.01 and IEC 61511 standards[2] introduce the concept of Safety Integrity Level (SIL). SIL is a measure of the amount of risk reduction that a Safety Instrumented Function (SIF) is capable of providing, as defined by its average Probability of Failure on Demand (PFD_{avg}).

To use an analogy, even a well-designed, installed, and tested pressure relief valve will have a finite probability that it will fail to open and adequately relieve pressure when a demand is place on the valve (i.e., a hazardous overpressure condition occurs). We expect that a key attribute of a "safe" relief system is that it would have a low probability of failure on demand. Similarly, a "safe" HIPPS system should also have a very low PFD_{avg}. Although the concept is similar, the

[2] Instrumentation, Systems, and Automation Society (ISA), ANSI/ISA S84.01, *Application of Safety Instrumented Systems for the Process Industry*, 1996. International Electrotechnical Commission (IEC), IEC 61508, *Functional Safety of electrical/electronic/programmable electronic safety-related systems*, First Edition, 1998. IEC 61511, *Functional Safety: Safety Instrumented Systems for the Process Sector*, FDIS, 2001.

method we use to achieve safety with an instrumented system is very different that used for conventional relief.

Figure 2 Safety Lifecycle



ISA and IEC require that for each SIF, a SIL target is selected and achievement of that target is confirmed by quantitative analysis of the design. Because the SIL is a measure of the amount of risk reduction, it is a natural question to ask "how much risk reduction is required?" The required amount of risk reduction is a function of the unmitigated risk of the process. You can also think of this as the risk the process poses without considering the benefit of the safety instrumented system. In order to determine the amount of risk reduction that is required, companies will typically compare the process risk against internal guidelines for tolerable risk. The difference between the process risk and the tolerable risk is the required risk reduction capability for the safety system, which is HIPPS in this case. Specifying an appropriate SIL for a HIPPS is discussed in *Section 4* of this paper.

The HIPPS is then designed to meet or exceed this level of performance. The amount of "safety" provided by a HIPPS with a given SIL is categorized based on the average Probability of Failure on Demand (PFDavg) as shown in *Table 1*.

Table 1 Safety Integrity Levels[3]

Safety Integrity Level	Probability of failure on demand (Demand mode of operation)	Risk Reduction Factor
SIL 4	0.001% to 0.01%	100,000 to 10,000
SIL 3	0.01% to 0.1%	10,000 to 1,000
SIL 2	0.1% to 1%	1,000 to 100
SIL 1	1% to 10%	100 to 10

3.0 Overall Risk Analysis Procedure for Justifying HIPPS

The starting point for a HIPPS project is the recognition that there is one or more scenarios where existing conventional relief system cannot adequately handle the load. This usually is indicated by an analysis that shows excessive backpressure on the vessel. The first objective is to determine whether use of HIPPS will allow the plant to justify removing that scenario from the design basis of the relief system. The risk analysis process used to answer this question is shown in *Figure 3*.

Step 1 – Is a vessel exclusively in air, water, or steam service? If yes, then use conventional design –HIPPS is not permissible under the ASME Boiler and Pressure Vessel Code, Code Case 2211.

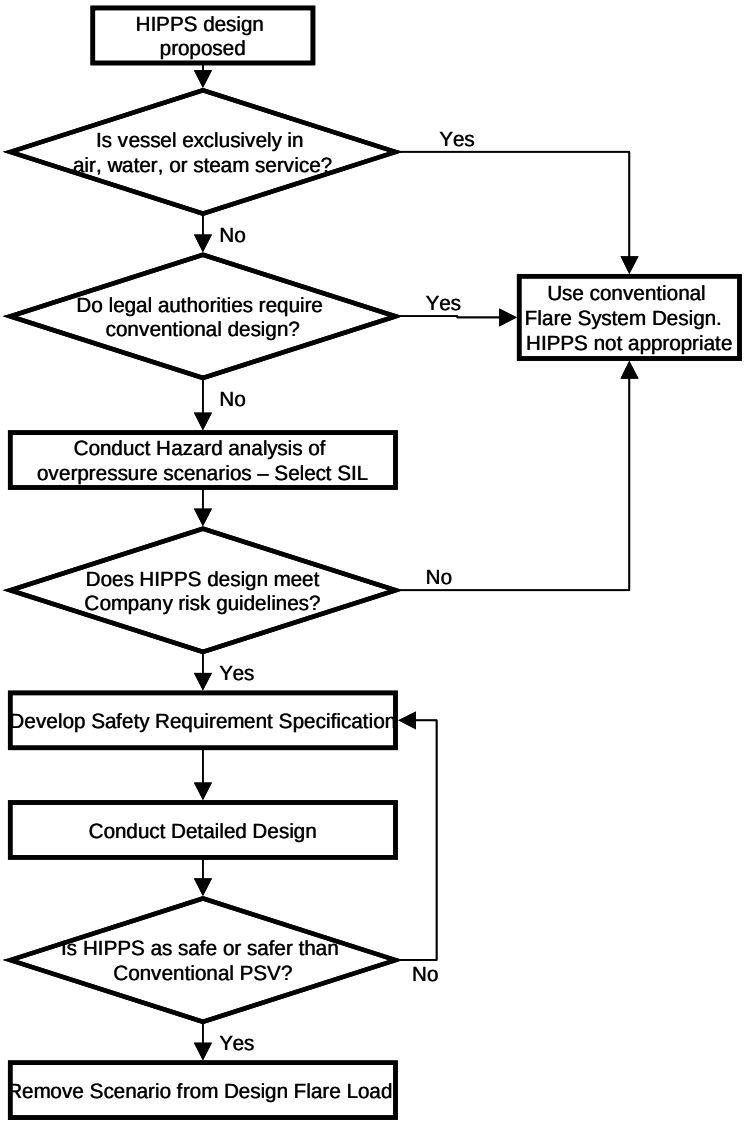
Step 2 – Do legal authorities require conventional design? State and local legal requirements may mandate the use of conventionally designed emergency pressure relief systems.[4] In such situations, HIPPS is not an alternative.

Step 3 – Conduct hazard analysis of overpressure scenarios – Select SIL. This is the subject of *Section 4* of this paper. Each overpressure scenario where conventional relief is inadequate should be evaluated to ensure the MAWP is higher than the highest pressure that can *reasonably* be achieved by the system, when accounting for the benefit of the HIPPS. A SIL will be selected both 1) to achieve this *reasonable certainty* goal and 2) to ensure that company risk criteria have been satisfied.

[3] IEC 61511 uses four categories as shown in the table. ISA 84.01 does not recognize SIL 4, which is almost never required in the process industries.

[4] The authors of this paper disclaim any suggestion that HIPPS can be used in lieu of conventional relief design where such legal requirements exist.

Figure 3 Risk Analysis Process For Justifying use of HIPPS



Step 4 – Does HIPPS design meet company risk guidelines? If the company risk guidelines indicate that the amount of risk reduction required from the HIPPS exceeds the practical limitations of design, then a HIPPS alternative is not appropriate.[5] The project team should use conventional relief if practical or stop the project if risk guidelines cannot be satisfied.

Step 5 and 6 – Develop Safety Requirements Specifications and Detailed Design This is the point where key safety requirements are specified by the design team. These include the type of technology (i.e., programmable, relay based, etc.), the architecture, proof testing intervals, etc. This is also the point that a reliability analysis is conducted to verify that the required SIL can be

[5] For all practical purposes SIL 3 designs are achievable with existing technology. A HIPPS that is capable of delivering SIL 4 performance, is almost never a practical option in the process industries.

achieved by the selected design. The subjects of reliability analysis and SIL Verification calculations are outside the scope of this paper, but these processes are adequately described in *Control Systems Safety Evaluation and Reliability*.[6] Conceptual and detailed design are also outside the scope, but should be conducted per ISA 84.01 and IEC 61511.

Step 7 – Is HIPPS as safe or safer than conventional relief? This is the topic of *Section 5* of this paper. A key step is to verify that HIPPS, as designed, provides a bettered alternative, in terms of safety, than conventional relief design. This should be justified, and, if necessary, the design improved to ensure that HIPPS is as safe, or safer than, conventional pressure relief.

Step 8 – Remove Scenario from Design Flare Load. If the HIPPS can be designed such that: 1) it satisfies the operating company's risk criteria, 2) achieves the specified SIL, and 3) is demonstrated to be as safe or safer than conventional technology, then the relief scenario that is safeguarded by the HIPPS can be removed from conventional relief load calculations.

4.0 Selecting the Right Safety Integrity Level for a HIPPS

Each overpressure scenario where conventional relief is inadequate should be critically evaluated by a team of experts in process engineering, operations, maintenance, control system engineering, and safety. This team will evaluate the risk, determine if a HIPPS is suitable for the application, and specify an appropriate Safety Integrity Level (SIL) for the safety function to mitigate the hazard. There are multifaceted goals when specifying a SIL requirement for HIPPS, especially when considering the number of codes and standards that must be satisfied. Remember, the SIL is a way to measure and specify the amount of risk reduction that is required. At a minimum, the risk must be reduced to achieve all of the following:

1. Ensure company risk management guidelines are satisfied (similar to any other SIF used in within a SIS), and:

2. Ensure the Maximum Allowable Working Pressure (MAWP) of a pressure vessel is higher than the highest pressure that can *reasonably* be achieved by the system. *ASME Boiler and Pressure Vessel Code, Code Case 2211.*

ASME offers no guidance on how to satisfy their *reasonable certainty* criterion. Each user of HIPPS must examine this requirement in light of their own risk management processes. The risk criteria adopted by many companies will generally be sufficient to ensure that the likelihood of a catastrophic event (due to HIPPS failure on demand) is reduced to a low enough level such that it is reasonably certain that it will not occur in the lifetime of the plant. For example, a company that uses a 10^{-4} per year risk criteria as a design basis for a single major hazard will ensure that a HIPPS failure on demand will occur no more frequently than 0.2 percent chance over a 20 year project lifetime.

But how "safe" is "safe enough"? How much safety should be designed into a HIPPS system? This is a key question that must be addressed by each company that intends to operate a HIPPS system. A detailed discussion of risk criteria is beyond the scope of this paper, but it is addressed in Chapter 3 of *Safety Integrity Level Selection.*[7]

---

[6] *Control Systems Safety Evaluation and Reliability*, 2nd Edition, W. M. Goble, 1998, ISA-The Instrumentation, Systems, and Automation Society.

[7] *Safety Integrity Level Selection*, Systematic Methods Including Layer of Protection Analysis, E. Marszal and E. Scharpf, 2002, ISA-The Instrumentation, Systems, and Automation Society.

Most companies make decisions about the acceptability of risk on a hazard-by-hazard basis. In other words, hazards are first identified, and they are individually evaluated, with each being held up against criteria for acceptable risk.[8] In a typical risk assessment process, each hazard is evaluated by measuring the consequence and likelihood (or frequency) of the hazard. Company risk criteria are then used to specify an appropriate Safety Integrity Level (SIL) that will reduce the likelihood of the hazard scenario to an acceptably low level. These criteria may be qualitative or quantitative in nature. Experience of the authors shows that most companies, when using either qualitative guidelines or quantitative criteria, that will ensure each major hazard is reduced to a residual risk of somewhere in the range of 10^{-4} per year (i.e., one chance in 10,000 per year) to 10^{-5} per year (i.e., one chance in 100,000 per year).

Risk analysis of HIPPS is complicated by the issue of how to define a distinct hazard that must be mitigated by the instrumented system. A simple case would involve overpressure of a single vessel from a single cause resulting in a specific consequence, i.e., vessel failure. Unfortunately, in the case of overloading a refinery flare header, the problem may be much more complex. For example, the scenario may involve an overpressure of an entire flare header due to multiple simultaneous relief scenarios. For a petroleum refinery, this is typically caused by loss of power resulting in failure of cooling water to multiple distillation towers. A flare system overload would occur unless HIPPS systems on multiple towers function properly. In this case, the hazard we want to avoid is overloading the flare. But there are potentially multiple causes, and multiple HIPPS systems involved. In this case, a quantitative risk assessment using Fault Tree Analysis (FTA) or Event Tree Analysis (ETA) is recommended. Simple methods such as hazard matrices cannot aggregate risks from multiple causes to ensure a specific hazard is reduced to an acceptable level.

5.0 Justifying "As Safe or Safer"

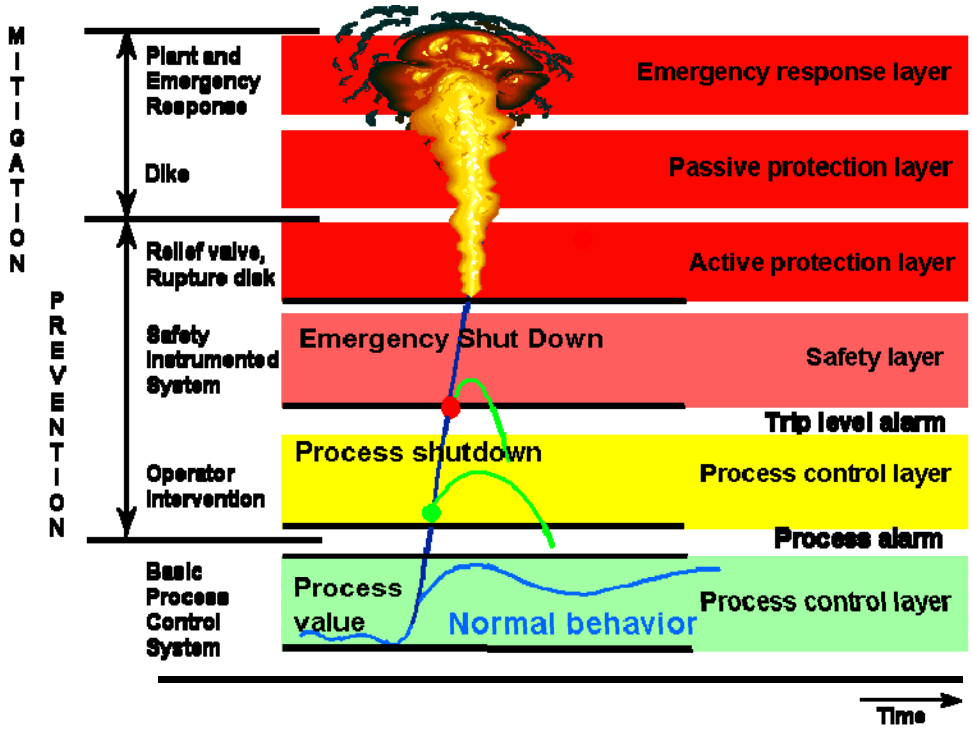
One issue that is must be considered is demonstrating that the proposed HIPPS will enhance overall safety performance at the facility by using the best engineered option. Although this is permitted in ASME Boiler and Pressure Vessel Code, Code Case 2211, there are no specific performance requirements. This begs the question, "if the HIPPS needs to improve safety, how safe is the existing pressure relief device it is intended to replace?" This question ultimately needs to be answered by risk analysis and criteria for ensuring HIPPS is "as safe or safer". This may lead to SIL 1, 2, or 3 designs depending on the required risk reduction capability and the reliability of existing pressure relief devices.

In the case of a process using a HIPPS, the protection provided by the emergency pressure relief valve in the "Active Protection Layer" as shown in *Figure 4* is being replaced, in part or in whole, by the HIPPS as shown in the "Emergency Shutdown Layer". In Code Case 2211 of the *Boiler and Pressure Vessel Code*, ASME specifies that proposed HIPPS should enhance overall safety performance at the facility by using the best engineered option. An interpretation of this requirement is that, at a minimum, the safety integrity level of the HIPPS must ensure the process is "as safe or safer" than the process would be were it to be provided with an adequately-sized conventional emergency pressure relief system. This means the HIPPS must provide as much or more risk reduction than a conventional emergency pressure relief device.

To determine the reliability of conventional pressure relief systems, the authors collected data concerning the frequency of relief valve failures. *Table 2* lists some of the data.

[8] Examples include, over-temperature of fired heater tubes causing tube rupture and fire, or loss of flame in a boiler resulting in fuel gas accumulation and a firebox explosion.

Figure 4 Layers of Protection



The data show an extremely wide range of failure rates. The driving factors are probably the environmental service for the device and the mechanical integrity program that it is subjected to. For relatively clean service and good maintenance – such as would be found in the nuclear industry –,relief valves have been demonstrated to operate at SIL 3 performance (or better). However, there is much data that suggests SIL 1 performance in the chemical industry (in particular, see the 1992 study by HSE of over 12,000 valves).

The following observations are made:[9]

- A properly sized, well-maintained relief valve is probably capable of operating with a probability of failure on demand equivalent to that of a mid-range SIL 2, or better.[10]
- Valves in aggressive service environments such as polymer plants probably are, at best, capable of operating with a probability of failure equivalent to SIL 1.
- Valves with an extensive history in clean service can easily operate at SIL 3.

With these data in mind, many companies have decided that the “as safer or safer” concept generally points in the direction of SIL 3 for a HIPPS system, although that rule of thumb is not universally supported by the pressure relief valve failure data.

[9] The authors do not promote using this data in lieu of site-specific reliability data from a PSV mechanical integrity program.

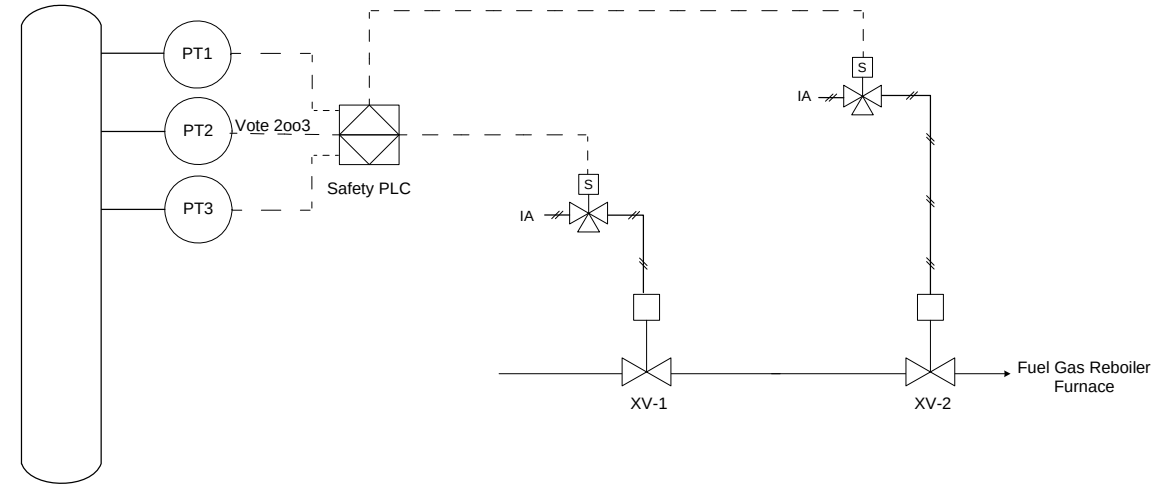
[10] The geometric mean between SIL 1 and SIL 2, which is Risk Reduction Factor of 320.

6.0 Case Study, Refinery HIPPS System

A medium-sized refinery desires to install a new processing unit as part of a clean fuels project. The unit includes a large distillation column. Heat is supplied to this column via a reboiler, which in this case is a large fired heater. The amount of vapor generated in the column is sensitive to the temperature of the vapor/liquid in the column. If a malfunction were to occur that resulted in too much heat input to the column, excessive amounts of vapor would be generated. This could result in a scenario in which the column pressure would exceed MAWP. At this point the emergency pressure relief valve would open and attempt to relieve excess pressure from the column to the refinery's flare system. The amount of vapor that would need to be vented would greatly exceed the capacity of the existing flare system.

The project team proposed a HIPPS be used that would detect hazardous overpressure using three pressure transmitters on the column overhead. A dedicated Programmable Logic Controller (PLC) that is certified for use in Safety Instrumented Systems would monitor the three pressure signals. If any two out of three signals exceeded the pre-defined trip point, the PLC would command the system to shutdown fuel gas firing to the heater. *Figure 5* illustrates the proposed architecture of the system.

Figure 5 Architecture of the Proposed Refinery HIPPS[11]



The refinery assembled a team of personnel with knowledge in process engineering, control system engineering, operations, and maintenance. The team reviewed the potential consequence of flare system overload as well as the likelihood of the causes of overpressure. This scenario represents a serious safety hazard, for which the potential consequences could include:

- High thermal radiation near the flare tip
- Potential loss of flame stability and blowout
- Overpressure and mechanical failure of the flare header

[11] An adequate HIPPS system can only be determined by a process where site-specific hazards are evaluated by a qualified team of experts. This example should not be viewed as typical or representative of a HIPPS in any way.

- Excessive backpressure on vessels resulting in mechanical failure

In general, mechanical systems are designed with safety margins that preclude loss of containment at pressure loads modestly in excess of design. The effectiveness of these safety margins in mitigating the above-listed consequences is hard to quantify because it depends on the extent of flare system overload and the current mechanical integrity of equipment. Further, the ASME code requires an analysis that provides reasonable certainty that pressures will not exceed MAWP (as opposed to risk of mechanical vessel failure at a higher pressure). In light of these factors and to provide a degree of assurance, the potential consequences of pressure in excess of MAWP were considered actual consequences. The team determined that the potential consequence could be catastrophic.

The company has adopted an internal risk guideline that serves to ensure that all major hazards prevented using engineered safeguards such that the likelihood of any single major hazard is no more than 10^{-4} per year. The target maximum event likelihood in this case is therefore, 1 chance in 10,000 per year.

Using Fault Tree Analysis (FTA) the HIPPS analysis team determined the frequency for a demand on the HIPPS would occur due to the malfunction of the Basic Process Control System (BPCS), which is expected to occur, at most, about once every 10 years. Thus the unmitigated frequency ($F_{unmitigated}$) was 0.1 per year. The required risk reduction factor was calculated.

$$PFD_{avg} = \frac{10^{-4}}{F_{unmitigated}} = 0.001$$

The indicated a risk reduction requirement for the HIPPS system equivalent to a SIL 3, i.e., a risk reduction factor of at least 1000.

In addition, the team examined site-specific data concerning the reliability of relief valves at the refinery. The data were not complete, but it indicated that pressure relief valve failures were not common. In fact, the number of specific relief valve failures that could be identified using mechanical integrity program data were so uncommon that it could be argued relief valves could operate with probability of failure in the high SIL 2 or low SIL 3 range.

Considering the data available to the team and the analysis using the refinery's risk guidelines, the HIPPS analysis team specified that the HIPPS should be designed as a SIL 3 safety system.

The final design of the HIPPS system is outside the scope of this example, but it was as per the requirements of ISA 84.01 and IEC 61511. The HIPPS system was designed with a high degree of fault tolerance and high diagnostic capability. The system was tested at a frequency to ensure that that SIL 3 performance could be ensured.

Table 2 Probability of Failure on Demand for Conventional Pressure Relief Valves

Data Source	Probability of Failure to Open on Demand and equivalent SIL Category			Notes
	Low	Mean	High	
CCPS, 1989, Guidelines for Process Equipment Reliability Data	1E-5 (SIL 4)	2E-4 (SIL 3)	8E-4 (SIL 3)	Spring Loaded
CCPS, 1989, Guidelines for Process Equipment Reliability Data	1E-5 (SIL 4)	4E-3 (SIL 2)	2E-2 (SIL 1)	Pilot Operated
Reactor Safety Study, WASH 1400, 1975	3E-6 (SIL 4)	1E-5 (SIL 4)	3E-5 (SIL 4)	Typically steam service See FP Lees, A14/7
French Nuclear Power Stations, 1983	NR	1E-2 (SIL 2)	NR	See FP Lees A14/14 Aupied, LeCoguier Procaccia, 1983 From annual test data
Rijnmond Report, 1977, Risk Analysis of Six Potentially Hazardous Industrial Objects in the Rijnmond Area,	1E-5 (SIL 4)	NR	4E-5 (SIL 4)	Table IX. 1, Probably derived from nuclear data
Risk Analysis for Process Plant, Pipelines, and Transport, JR Taylor, 1994	NR	1E-5 (SIL 4)	NR	P 166. Probably derived from nuclear data
UK Health and Safety Executive, 1992 *Safety Valve Reliability, AB Smith, Loss Prevention and Safety Promotion in the Process Industries, Elsevier*	NR	3E-2 (SIL 1)	NR	“failed to lift”, sample of 12,790 valves from oil & gas, petrochem., chemical, including multi-national companies. In addition, 13% “lift heavy”, i.e., > 110%.
Confidential	NR	2E-2 (SIL 1)	NR	“Seized Closed”, Data from approx. 4000 valves
Confidential	2E-2 (SIL 1)	NR	4E-2 (SIL 1)	“Lifts Heavy” i.e,. above 110% of set pressure. Data 1996 through 1998
Confidential	NR	3E-2 (SIL 1)	NR	1997 publication of Corporate Risk Analysis.
Chemical Engineering, July 2001		6E-2 (SIL 1)		12 failures to open (at 150%) out of 200 valves tested.