HIGH INTEGRITY PRESSURE PROTECTION SYSTEMS (HIPPS)

Published in Chemical Engineering Progress, November 2000
Recipient of Bill Doyle Award for Best Paper Loss Prevention Symposium 2000
Accepted for the Instrument Engineers Handbook Volume 3 Chapter 2.6

Features	Instrumented systems that are typically designed to meet safety integrity level 3 per ANSI/ISA S84.01-1996 and IEC 61511.
Purpose	To mitigate identified overpressure scenarios.
HIPPS-Related codes, standards, and recommended practices	American Society of Mechanical Engineers (ASME), Boiler and Pressure Vessel Code, Section VIII – Pressure Vessels, United Engineer Center, New York, NY American Petroleum Institute (API), RP 521, Guide for Pressure Relieving and Depressuring Systems, Washington, DC Instrumentation, Systems, and Automation Society (ISA), ANSI/ISA S84.01-1996, "Application of Safety Instrumented Systems (SIS) for the Process Industry," Research Triangle Park, NC International Electrotechnical Commission (IEC), IEC 61508, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems," Geneva, Switzerland International Electrotechnical Commission (IEC), IEC 61511, "Functional Safety: Safety Instrumented Systems for the Process Sector," Geneva, Switzerland

PMB-295, 2323 Clear Lake City Blvd Houston, Texas 77062-8032
281-922-8324 (phone) ▪ 281-922-4362 (fax) www.SIS-TECH.com

In the process industry, an important safety consideration is the prevention of loss of containment due to vessel or pipeline overpressure situations. Loss of containment can result in impact to human life and the environment, when flammable, explosive, hazardous, or toxic chemicals are released to the atmosphere. Loss of containment can also result in economic impact due to production unit replacement/repair costs and production losses.

Industry standards from the American Petroleum Institute (API) and American Society of Mechanical Engineers (ASME) provide criteria for the design and protection of vessels and pipelines from rupture or damage caused by excess pressure. In conventional designs, pressure relief devices, such as pressure-relief or -safety valves, are used as the primary means of pressure protection. The design of each pressure relief device is based on the assessment of overpressure scenarios, such as typically experienced with the total loss of cooling or power supply.

Conventional pressure relief system design, including relief header and flare sizing, does not examine the reduction in potential loading due to hazard mitigation provided by operator response to alarms or to the initiation of instrumented systems, including basic process control systems (BPCS) or safety instrumented systems (SIS). In fact, until 1996, the American Society of Mechanical Engineers (ASME) codes mandated the use of pressure relief devices for protection of pressure vessels.

However, in some applications, the use of pressure relief devices is impractical. Typical cases include:

- Chemical reactions so fast the pressure propagation rate could result in loss of containment prior to the relief device opening. Examples are “hot spots,” decompositions, and internal detonation/fires;
- Chemical reactions so fast the lowest possible relieving rate yields impractically large vent areas;
- Exothermic reactions occurring at uncontrollable rates, resulting in a very high propagation rate for the process pressure. (The pressure propagation rate for these reactions is often poorly understood.);
- Plugging, polymerization, or deposition formed during normal operation, which have historically partially or completely blocked pressure relief devices;
- Reactive process chemicals relieved into lateral headers with polymerization and thus plugging, rendering the relief device useless;
- Multi-phase venting, where actual vent rate is difficult to predict; and
- Pressure relief device installation creates additional hazards, due to its vent location.

In such applications, the installation of the pressure relief device provides minimum risk reduction. Consequently, other methods of preventing overpressure must be utilized to achieve measurable risk reduction.

Adding to the complexity, in many countries around the world, there is increased pressure from community and regulatory authorities to reduce venting and combustion of gases. In these countries, it is now unacceptable to flare large volumes of gas. The need to balance safety requirements and environmental requirements has resulted in increased focus on using an alternative approach to pressure protection.

Fortunately, API 521 and Code Case 2211 of ASME Section VIII, Division 1 and 2, provide an alternative to pressure relief devices – the use of an instrumented system to protect against overpressure. When used, this instrumented system must meet or exceed the protection provided by the pressure relief device. These instrumented systems are safety instrumented systems (SIS), since their failure can result in the release of hazardous chemicals and/or the creation of unsafe working conditions. As SISs, they must be designed according to the United States standard ANSI/ISA S84.01-1996 or the international standard IEC 61511. The risk typically involved with overpressure protection results in the need for high SIS integrity; therefore, these systems are often called High Integrity Pressure Protection Systems (HIPPS) or High Integrity Protection Shutdowns (HIPS).

Code Requirements

Until August 1996, ASME required the use of pressure relief devices for pressure vessels designed in accordance with Section VIII, Division 1, para UG-125(a) Section VIII, Division 2, para, AR-100. The approval of ASME Code Case 2211 in August 1996 changed this position

by defining the conditions for which overpressure protection may be provided by a SIS instead of a pressure relief device.

The new ruling is designed to enhance the overall safety and environmental performance of a facility by utilizing the most appropriate engineered option for pressure protection. While no specific performance criteria is included in Code Case 2211, the use of HIPPS must result in an installation as safe or safer than the conventional design. The overpressure protection can be provided by a SIS in lieu of a pressure relief device under the following conditions.

a) The vessel is not exclusively in air, water, or steam service.

b) The decision to utilize overpressure protection of a vessel by system design is the responsibility of the user. The manufacturer is responsible only for verifying that the user has specified overpressure protection by system design, and for listing Code Case 2211 on the Data Report.

c) The user must ensure the MAWP of the vessel is higher than the highest pressure that can *reasonably* be achieved by the system.

d) A quantitative or qualitative risk analysis of the proposed system must be made addressing: credible overpressure scenarios, demonstrating the proposed system is independent of the potential causes for overpressure; is as reliable as the pressure relief device it replaces; and is capable of completely mitigating the overpressure event.

e) The analysis conducted for (c) and (d) must be documented.

Recommended Practices

API recommends a number of practices for addressing pressure relieving and depressuring systems in the petroleum production industry. For example, API 521 describes flare system design methods that require assessing the relief load based on a credible overpressure scenarios for relief valve sizing and on the simultaneous venting of all affected vessels for main flare header sizing. The fourth edition of API 521 allows taking credit for a favorable response of the instrumented systems. Despite API 521 permitting design alternatives, API 521 Part 2.2 recommends the use of HIPPS only when the use of pressure relief devices is *impractical*.

Standards

The international standard, IEC 61508, "Functional Safety of Electrical / Electronic / Programmable Electronic Safety Related Systems," establishes a framework for the design of instrumented systems that are used to mitigate safety-related risks. The United States standard, ANSI/ISA S84.01-1996, "Application of Safety Instrumented Systems (SIS) for the Process Industry," and international standard, IEC 51611, "Functional Safety: Safety Instrumented Systems for the Process Sector," are intended to address the application of SISs in the process industries.

The objective of these standards is to define the assessment, design, validation, and documentation requirements for SISs. While these design standards are not prescriptive in nature, the design processes mandated by these standards cover all aspects of design including:

risk assessment, conceptual design, detailed design, operation, maintenance, and testing. Since HIPPS is a type of SIS, the requirements of these standards, as pertaining to each specific HIPPS application, must be investigated and applied thoroughly.

The SIS standards are performance-based with the safety integrity level (SIL) as the primary performance measurement. The SIL must be assigned by the user based on the risk reduction necessary to achieve the user's risk tolerance. It is the user's responsibility to ensure consistent and appropriate SIL assignments by establishing a risk management philosophy and risk tolerance. The risk reduction provided by the HIPPS is equivalent to the probability of failure on demand attributable to all of the HIPPS devices from the sensor through the logic solver and final elements. The relationship between the SIL and probability to fail on demand (PFD) is shown in Table 2.6.A.

The SIL establishes a minimum required performance for the HIPPS. The SIL is affected by the following:

1. Device integrity determined by documented and supportable failure rates;
2. Redundancy and voting using multiple devices to ensure fault tolerance;
3. Functional testing at specific intervals to determine that the device can achieve the fail safe condition;
4. Diagnostic coverage using automatic or on-line methods to detect device failure; and

5. Other common causes including those related to the device, design, systematic faults, installation, and human error.

Because the criteria used to establish the SIL affects the entire HIPPS's lifecycle, the SIL forms the cornerstone of the HIPPS design.

HIPPS Justification

A decision tree can be utilized to facilitate the justification for HIPPS in the process industry. Figure 2.6.A is a simplified decision tree showing the key steps in assessing and designing a HIPPS.

The successful implementation of HIPPS requires examination of applicable regulations and standards, including local and insurer codes that may mandate the use of pressure relief devices. From ASME Code Case 2211, the vessel cannot be exclusively in air, water, or steam service. This exclusion is intended to prevent building utility systems (e.g. residential boilers) from being installed without pressure relief devices. API 521 recommends the use of HIPPS only when the use of a pressure relief device is impractical. It is the user's responsibility to establish the definition of "impractical." Any applicable regulation or standard should be reviewed during early project front-end loading to ensure that the HIPPS approach is acceptable.

ASME Code Case 2211 requires a qualitative or quantitative risk analysis of the potential overpressure scenarios. This hazard or risk analysis is initiated when the process design is sufficiently complete to allow identification of the causes and magnitude of potential overpressure events. Typically, this means the following information is available:

- ✓ Process flow diagrams;
- ✓ Mass and energy balances;
- ✓ Equipment sizing and design requirements; and
- ✓ Piping & Instrumentation Diagrams (P&IDs).

Sometimes, the design team wants to wait until the design is essentially complete before examining the pressure relief requirements and the HIPPS design. Unfortunately, this is the most expensive point to be making instrumentation modifications. For instance, when design is declared as complete, piping and instrumentation diagrams (P&IDs) have been finished, specified equipment MAWP are fixed, long-delivery items have been ordered, and field installation drawings are nearing completion. Then is *not* the time to determine that a HIPPS must be installed, requiring redundancy in field inputs and outputs, a redundant logic solver, and on-line testing facilities, all of which have significant impact on project documentation, schedules, and budget.

The hazard analysis should follow a structured, systematic approach, using a multidisciplinary team consisting of representatives from process engineering, research and development, operations, health and safety, instrumentation and electrical, and maintenance. Typical hazard

analysis approaches include “What-if” Analysis, “What-if”/Checklist Analysis, Hazard and Operability Study (HAZOP), Failure Modes, Effects, and Criticality Analysis (FMECA), Fault Tree Analysis (FTA), or Event Tree Analysis (ETA).

The hazard analysis examines operating (e.g. start-up, shutdown, and normal operation) and upset conditions that result in overpressure. The “Causes of Overpressure” provided in API Recommended Practice 521 should be reviewed to ensure completeness of the hazard analysis. For example, the hazard analysis should examine the following initiating causes for overpressure events:

- loss of utilities, such as electric power, steam, water, etc.,
- runaway reactions,
- fire exposure,
- operating errors,
- maintenance errors,
- block outlet,
- equipment failures, and
- instrumentation malfunctions.

The hazard analysis should document the propagation of each potential overpressure event from the initiating cause to the final consequence (also referred to as the “overpressure scenario”).

ASME Code Case 2211 requires that the User ensure that the MAWP per Section VIII, Division I, Para UG-98 of the vessel is greater than the highest pressure that can reasonably be achieved by the system. "Reasonably be achieved" is not defined in Code Case 2211. However, many users define "reasonably be achieved" utilizing documented risk tolerance criteria. The risk of each overpressure scenario is evaluated in terms of frequency and consequence. During the hazards analysis, the mitigated frequency of each overpressure scenario is determined by assessing the initiating cause frequency and risk reduction provided by any independent protection layers, such as HIPPS. If the risk, as defined by the mitigated frequency and consequence, achieves or is below the risk tolerance criteria, the scenario is considered for removal from the relief device and flare loading calculations.

When it is determined that an overpressure scenario achieves the risk tolerance criteria, the assessment team must ensure that the documentation adequately describes the justification for the team's decision prior to removing the scenario from the sizing calculations for the pressure relief device or the flare system. Careful consideration must be given when removing a scenario, because if the assumptions used to justify the removal are incorrect, the vessel may be left un- or under-protected, resulting in loss of containment and a possible hazardous situation.

Safety Requirement Specification

A safety requirement specification (SRS) must be developed to address each overpressure scenario that will be addressed using HIPPS. The SRS describes how and under what

conditions the SIS will mitigate each overpressure scenario, including a functional logic description with trip set points and device fail-safe state. Only those scenarios that can be successfully mitigated by the SIS can be *considered* for removal from the pressure relief and flare loading calculations. For example, in hydrocarbon applications, the fire case scenario often can not be removed from the sizing calculations due to the inability of HIPPS to mitigate the cause of overpressure.

When specifying the process performance of HIPPS, the process dynamics must be evaluated to ensure that the HIPPS response time is fast enough to prevent overpressure of the vessel. The response time must be evaluated by considering the time it takes to sense that there is an unacceptable process condition; the scan rate and data processing time of the logic solver; and initiation of the final element. For general process industry applications, HIPPS valves are typically specified to have closure times of less than five seconds. However, the actual required closure must be determined for each installation. The valve specification must include acceptable leakage rate, since this affects downstream pressures and relief loading. The valve specification must also ensure that the actuator provides sufficient driving force to close the final element under the worse case, upset pressure condition.

In addition to the safety functional requirements, the SRS also includes documentation of the safety integrity requirements, including the SIL and anticipated testing frequency. At a minimum, the target SIL for the HIPPS should be equivalent to the performance of a pressure relief

device. Reliability information for a single-valve relief system is provided in "Guidelines for Process Equipment Reliability Data" by the Center for Chemical Process Safety. The data in Table 2.6.B indicates that for spring operated pressure relief devices, the minimum target SIL should be SIL 3, which is equivalent to a probability to fail on demand in the range of 1E-03 to 1E-04. When using a pilot operated pressure relief device, the minimum target SIL should be SIL 2, which is equivalent to a probability to fail on demand in the range of 1E-02 to 1E-03. Due to the range of probability to fail on demand, many users choose to design HIPPS at a target SIL 3, regardless of the pressure relief device type.

The SRS must also specify exactly how the HIPPS will be configured to achieve the target SIL. The high availability requirements for HIPPS drive the choices made concerning device integrity, diversity, redundancy, voting, common cause concerns, diagnostic requirements, and testing frequency.

Device Integrity and Architecture

It is important to recognize that the HIPPS includes all devices required to reach the desired fail-safe condition for the process. The HIPPS includes the entire instrument loop from the field sensor through the logic solver to the final elements, along with other devices required for successful SIS functioning, such as SIS user interfaces, communications, and power supplies. For example, if the final elements are air-to-move valves and the safe action requires valve closure, instrument air availability must be considered when determining the overall HIPPS availability. Since all devices used in HIPPS contribute to the potential probability of failure on

demand for the HIPPS, the structure of the instrumented loop must be defined and evaluated as a system so the entire loop meets SIL requirements. A brief discussion of SIS devices follows.

Process Sensors. The process variables (PV) commonly measured in HIPPS are pressure, temperature and flow. Traditionally, these variables were monitored using discrete switches as the input sensor to the safety instrumented systems. Switches worked well for three reasons: 1) Most trip conditions are discrete events, i.e., a high pressure, high temperature, or low flow; 2) Relay systems and early programmable logic controllers (PLCs) processed discrete signal much easier than analog signals; and 3) Switches were usually less expensive than analog transmitters.

The evolution of PES technology has made it easy to use analog PV inputs. The use of transmitters to measure these variables is now preferred over the use of switches. Switches only give a change in output when they are activated and can "stick" or experience some other failure mode that is revealed only when the switch is tested or a demand is placed on it. Transmitters can be continuously monitored and the operability of the transmitters readily observed. A single transmitter providing multiple levels of trip/alarm functions (i.e., low, high and high-high level) can replace multiple switches. With transmitter redundancy employed, out-of-range or deviation alarming can be implemented to ensure a high level of availability.

Most HIPPS applications require 1oo2 or 2oo3 transmitters on all field inputs. Figures 2.6.B and 2.6.C provide illustrations of typical installations. The use of redundant inputs enables the

system designer to incorporate diagnostics into the HIPPS, which significantly reduces the probability to fail on demand for the field inputs. Separate process connections are also recommended to decrease common cause faults, such as plugged process taps. Utilizing diversity in the process variable measurement, where practical, is also recommended in order to reduce common cause failures and consequently the probability to fail on demand.

Logic Solver. The logic solver hardware must be designed to meet the assigned SIL. Since many HIPPS are designated as SIL 3, the logic solver is specified to be compliant with SIL 3 performance requirements, as provided in IEC 61508. The logic solver can be relays, solid state, or programmable electronic systems (PES). If a PES is used, the selected PES should provide a high level of self-diagnostics and fault tolerance. Redundancy of signal paths and logic processing is desirable and the trip output function must be configured as de-energize to trip.

ANSI/ISA S84.01-1996, IEC 61508, and IEC 61511 require that the safety logic be independent from the basic process control system logic. Adequate independence of the safety logic reduces the probability that a loss of the basic process control system hardware will result in the loss of HIPPS functioning. From a software standpoint, independence also reduces the possibility that inadvertent changes to the HIPPS safety functionality could occur during modification of basic process control functions.

Final Elements. The majority of HIPPS utilize dual devices in a 1oo2 configuration. The final elements are typically either 1) relays in the motor control circuit for shutdown of motor operated valves, compressors, or pumps or 2) fail safe valves opened or closed using solenoids in the instrument air supply.

Figures 2.6.D, 2.6.E, and 2.6.F provide illustrations of typical installations when fail-safe valves are used as the final elements. At least one of the valves must be a dedicated shutdown valve. The second valve can be a control valve, but it must be configured fail-safe; have no minimum stops; and its actuation must be controlled by the HIPPS logic solver. The system designer should also examine the initiating cause for the various scenarios to be mitigated using the HIPPS. If the initiating cause for the overpressure scenario is the failure of the control valve, the system designer should strongly consider providing the redundant isolation using two block valves rather than using the control valve and a block valve.

Solenoid operated valves (solenoids) configured as de-energize to trip are used to actuate the fail-safe valves. Solenoids can be configured 1oo1 or 1oo2, but spurious closure of the valves due to solenoid coil burnout can cause process disruptions, loss of production, and downtime. The solenoids can also be configured as 2oo2 to reduce spurious trips, as long as adequate testing is performed to uncover stuck valves or plugged vent ports. The solenoid should be mounted as close to the valve actuator as possible to decrease the required transfer volume for

valve actuation. The exhaust ports should be as large as possible to increase speed of valve response.

Diagnostics

Diagnostic capability should be designed into HIPPS. The ability to detect failures of devices on-line significantly improves the availability of the HIPPS. For example, the use of signal comparison on analog inputs allows annunciation of transmitter failures to the control room. To support the claimed risk reduction associated with diagnostics, operation procedures must require that these alarms be responded to promptly with a work order for repair within the mean time to repair specified in the safety requirements specification. Maintenance procedures must also place high priority on repair of HIPPS devices.

Testing Frequency

If all failures were self-revealing, there would be no need to test safety system devices. Shut down valves that do not close completely, solenoid valves that are stuck in position, and pressure switches with stuck closed contacts are all examples of covert, dangerous failures. If safety system devices are not tested, dangerous failures reveal themselves when a process demand occurs, often resulting in the unsafe event that the safety system was designed to prevent. Testing is performed for one reason, and one reason only, to uncover failures.

The appropriate testing of HIPPS is key to ensure that the availability requirements are satisfied. Architecture, redundancy, and device integrity have a significant effect on the probability to fail on demand and therefore testing frequency requirements. To determine the required testing frequency, quantitative risk assessment is the accepted approach by most Users. In general, all HIPPS components require a testing frequency in the range of 3 to 12 months. On-line and off-line testing provisions should be provided to permit each device to be completely function tested. Any required bypasses must be managed through a change management process with appropriate access security.

Whatever the testing frequency, it is essential that the testing is performed throughout the safety system life. Any changes in the testing frequency must be validated by quantitative methods to ensure that the availability is not lowered to an unacceptable level.

Common Cause Failures

A common cause failure (CCF) occurs when a single failure results in the failure of multiple devices. ASME Code Case 2211 requires that sufficient independence be demonstrated to ensure reliability of the HIPPS performance. To minimize common cause failures, the initiating causes of each scenario identified during the hazard analysis should be examined. Then, the HIPPS hardware and software should be designed to function independently from these initiating causes. For example, if a control transmitter is listed as an initiating cause to the

scenario, the control transmitter cannot be the sole means for detecting the potential incident. At least one additional transmitter will be required for the HIPPS.

Once independence of the HIPPS devices is demonstrated, common cause failures (CCF) related to the design must be examined. The following are often cited as examples of common cause faults:

- Miscalibration of sensors
- Fabrication flaws
- Pluggage of common process taps for redundant sensors
- Incorrect maintenance
- Improper bypassing
- Environmental stress on the field device
- Process fluid or contaminant prevents valve closure

The most critical failure is that the SRS is incorrect at the beginning of the design process and the HIPPS cannot effectively detect or prevent the potential incident. Improper system specification can compromise the entire HIPPS.

Industrial standards and corporate engineering guidelines and standards can be utilized to reduce the potential for CCF. The proposed or installed HIPPS design can be compared to

these standards. Deviation from the standards can be corrected through design revision or documented to justify why this specific application has different requirements.

Checklists can also be used to reduce potential CCFs. A checklist analysis will identify specific hazards, deviations from standards, design deficiencies and potential incidents through comparison of the design to known expectations, which have been expressed as checklist questions.

In some cases, it may be necessary to consider the impact of potential common cause failures when verifying whether the HIPPS can achieve the target SIL. In such cases, the potential common cause failures will need to be considered in the quantitative performance evaluation.

"As Safe or Safer" Verification

The HIPPS must provide an installation that is as safe or safer than the pressure relief device that it replaces. For documentation of the "as safe or safer" and compliance with the target SIL, the design of any HIPPS should be quantitatively verified to ensure it meets the required availability. Quantitative verification of SIL for HIPPS is the generally accepted approach for most users of HIPPS.

A guidance report by ISA (expected final in 2002), ISA TR84.02, recommends use of one of the following methods for SIL Verification:

1. Markov Models
2. Fault Tree Analysis
3. Simplified Methods

Any of these techniques can be utilized to determine whether the design meets the required SIL. If it does not meet the required SIL, the design must be modified until it does.

Implementation and Commissioning

Implementation/commissioning activities must be performed within the bounds of the safety requirements specification and detailed design. Any deviations from these documents must be evaluated for impact on the safety integrity level and on any assumptions made with regard to performance.

Operate and Maintain

The HIPPS must be operated, maintained and tested throughout the life of the plant. The high integrity of HIPPS is often achieved through the use of frequent testing. Once the required testing frequency is determined for a particular HIPPS design, the testing must be performed at

that frequency. If the SIL verification calculation states that the testing is to occur at a 6 month interval, it must be done at 6 months, not one year.

Change Management

Thorough risk assessment and proper design constitute half the battle to successful application of HIPPS. Long-term preservation of the SIL through operation, maintenance, and management of change activities is the other half and, for many Users, is the most difficult part of compliance. Most codes and standards focus solely on design. Once the piece of equipment is "certified" for compliance, the requirements for the code or standard are fulfilled. However, SIL is not just a design parameter. It is also an operational parameter. The choices made during design, including voting, diagnostics, and testing, must be preserved throughout the facility's life. Once the SIS is designed and installed, and a testing frequency is chosen, the SIL is fixed and can only be changed by modification of one of the major design parameters. Consequently, the HIPPS SIL serves as a "management of change" checkpoint.

Advantages and Disadvantages of HIPPS

It is poor safety practice to install and rely on pressure relief devices in services where the sizing of the device is poorly understood or known to be inadequate due to chemical reactions, multi-phase fluids, or plugging. In these applications, alternatives, such as HIPPS, should be examined to ensure mitigation of overpressure events.

Industry is increasingly moving towards utilizing HIPPS to reduce flare loading and prevent the environmental impact of pressure venting. They are becoming the option of choice to help alleviate the need to replace major portions of the flare system in existing facilities when adding new equipment or units. If the header and flare system must be enlarged, significant downtime is incurred for all of the units that discharge to that header. The capital and installation cost associated with HIPPS is attractive when compared to the downtime or equipment cost of flare modification. Another benefit is that the process unit will not flare as much as a process unit designed for full flare loading. In some areas of the world, this is becoming important as regulatory agencies place greater restrictions on flaring of process gases.

The main disadvantage of HIPPS is the careful documentation, design, operation, maintenance, and testing to ensure standard's compliance. Specific regulatory and enforcement jurisdiction requirements must be determined. In some instances, approval of local authorities is required. Regulatory and standards requirements must be understood by all parties, including facility management and instrumentation and electrical, operations, and maintenance personnel.

Any justification for HIPPS must be thoroughly documented through a hazard analysis, which identifies all potential overpressure scenarios and demonstrates that the HIPPS can adequately address each scenario. The ability of the HIPPS to adequately address overpressure is limited by the knowledge and skill applied in the identification and definition of overpressure scenarios.

HIPPS systems are more complex, requiring the successful functioning of multiple devices to achieve the performance of a single pressure relief device. The user must verify that HIPPS will work from a process standpoint and that the HIPPS design results in an installation as safe or safer than a conventional design. The effectiveness of the system is highly dependent on the field design, device testing, and maintenance program. Consequently, the user must understand the importance of application-specific design aspects, as well as the associated costs of the intensive testing and maintenance program whenever a HIPPS is utilized. When a pressure relief device is not installed or is undersized based on conventional design, the HIPPS becomes the "last line of defense," whose failure potentially results in vessel rupture.

Finally, there is no "approved" rubber stamp in any regulation or standard for the use of HIPPS for reduction in the size of relief devices and associated flare system for pressure vessels or pipelines. Substantial cautionary statements are made in the standards and recommended practices, concerning the use of HIPPS. No matter what documentation is created, the user still has the responsibility to provide a safe and environmentally friendly operation.

Bibliography

"Guidelines for Process Equipment Reliability Data," Center for Chemical Process Safety of the American Institute of Chemical Engineers, NY, NY, 1989.

"Safety Instrumented Systems (SIS)—Safety Integrity Level (SIL) Evaluation Techniques," ISA dTR84.0.02, Draft, Version 4, March 1998.

Summers, A.E., K. Ford, and G. Raney, "Estimation and Evaluation of Common Cause Failures," 1999 Loss Prevention Symposium, American Institute of Chemical Engineers Spring Meeting, Houston, Texas, March, 1999.

Summers, A.E., "S84 – The Standard For Safety Instrumented Systems," *Chemical Engineering*, December, 2000.

Summers, A.E., "Techniques for assigning a target safety integrity level," *ISA Transactions*, 37, pp. 95-104, 1998.

Summers, A.E., and G. Raney, "High Integrity Protection Systems and Pressure Relief Systems," IMECE Conference, American Society of Mechanical Engineers, Nashville, Tennessee, November 1999.

Summers, A.E., "Using Instrumented Systems For Overpressure Protection," *Chemical Engineering Progress*, November 1999.

Windhorst, Jan C.A., "Over-pressure Protection By Means of A Design System Rather Than Pressure Relief Devices," CCPS International Conference and Workshop on Risk Analysis in Process Safety, American Institute of Chemical Engineers, Atlanta, GA, October, 1998.

ABBREVIATIONS

ANSI	American National Standards Institute
API	American Petroleum Institute
ASME	American Society of Mechanical Engineers
BPCS	Basic Process Control System
CCF	Common Cause Failure
HIPS	High Integrity Protection Systems
HIPPS	High Integrity Pressure Protection Systems
IEC	International Electrotechnical Commission
ISA	Instrumentation, Systems, Automation Society
MAWP	Maximum Allowable Working Pressure
PES	Programmable Electronic System
PLC	Programmable Logic Controller
PV	Process Variable
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SRS	Safety Requirement Specification

Table 2.6.A: Safety Integrity Levels

SIL **IEC 61508**	**SIL** **ANSI/ISA S84**	**PFD**
1	1	0.1 to 0.01
2	2	0.01 to 0.001
3	3	0.001 to 0.0001
4	Not applicable	0.0001 to 0.00001

Table 2.6.B. Pressure Relief Device Failure to Open on Demand

Pressure Relief Device Type	Failure to Open on Demand		
	Lower	Mean	Upper
Spring Operated	7.9E-05	2.12E-04	7.98E-04
Pilot Operated	9.32E-07	4.15E-03	1.82E-02

Figure 2.6.A: Simplified Design Tree

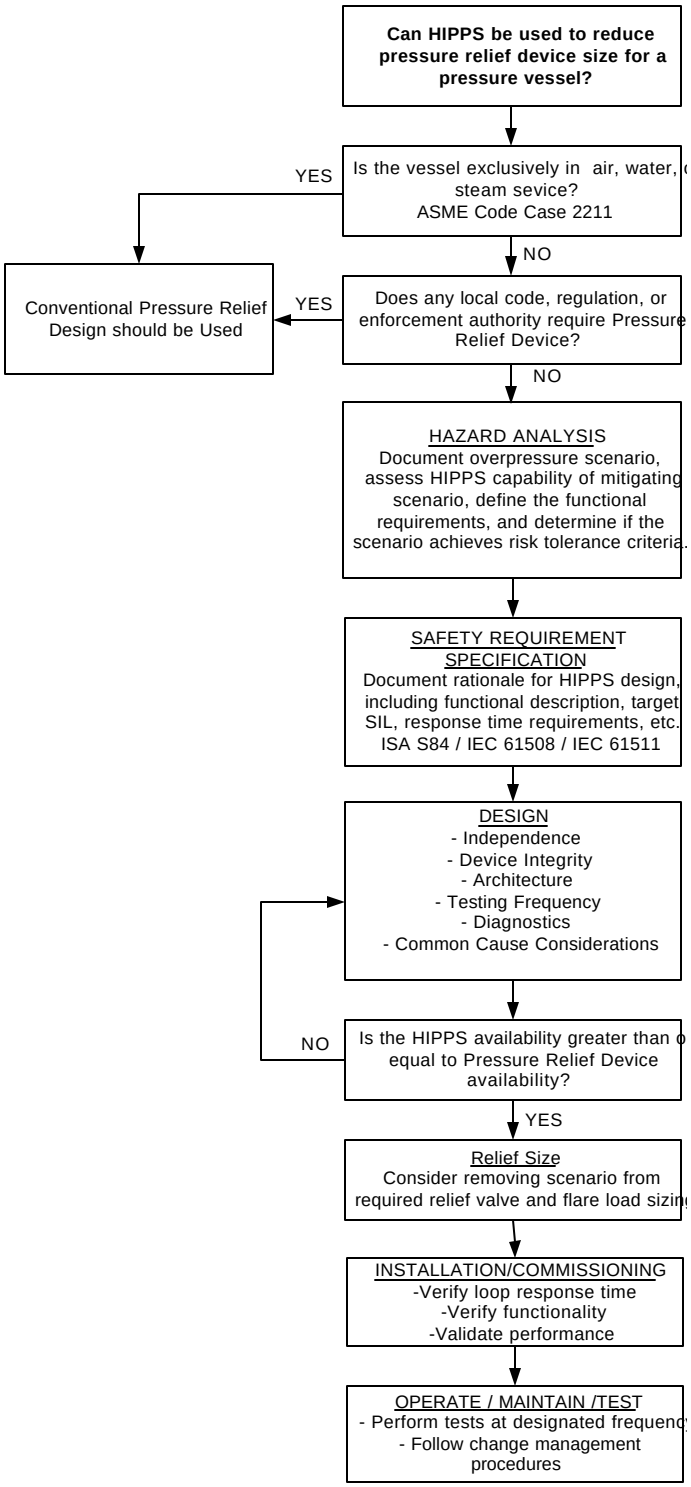

Figure 2.6.B: Installation Illustration of 1oo2 Field Input Devices

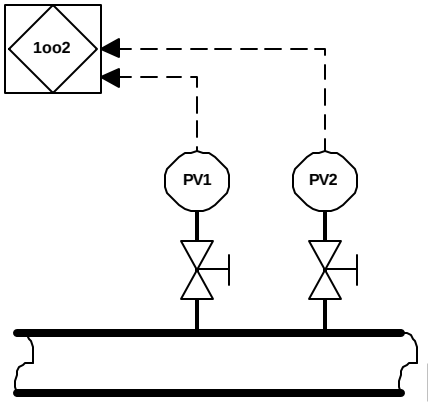

Figure 2.6.C: Installation Illustration of 2oo3 Field Input Devices

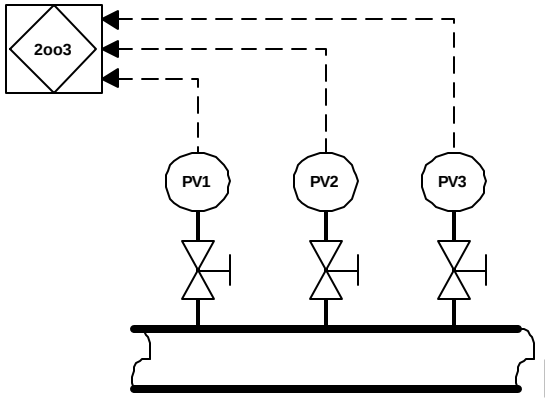

Figure 2.6.D: Installation Illustration for Final elements Showing 1oo2 Valves and 1oo1 Solenoids

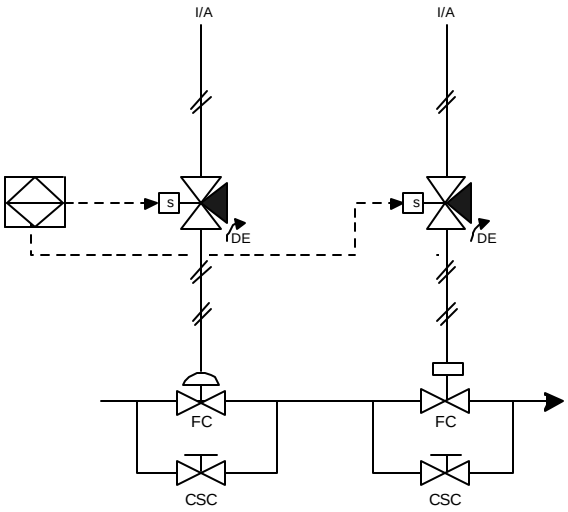

Figure 2.6.E: Installation Illustration for Final elements Showing 1oo2 Valves and 1oo2 Solenoids

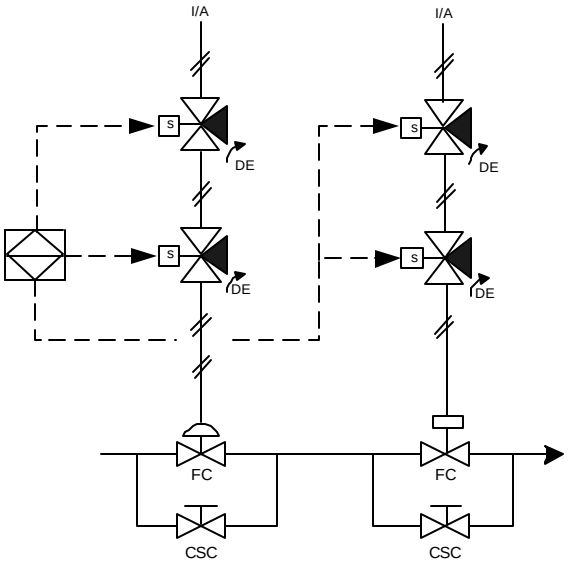

Figure 2.6.F: Installation Illustration for Final elements Showing 1oo2 Valves and 2oo2 Solenoids