High Integrity Protective Systems for Reactive Processes

Angela E. Summers, Ph.D., P.E., President, SIS-TECH Solutions, LP

"High Integrity Protective Systems for Reactive Processes," Center for Chemical Safety Symposium, New York: American Institute of Chemical Engineers, Scottsdale, Arizona, September 23-25, 2003.
"Risk Management for Reactive Processes," Mary Kay O'Connor Process Safety Symposium 2003, Texas A&M University, College Station, Texas, October 28-30, 2003.
"Consider HIPS for Reactive Processes," Chemical Processing, March 2004.

Abstract

Industry standards from the American Petroleum Institute (API) and American Society of Mechanical Engineers (ASME) provide criteria for the design and protection of vessels from rupture or damage caused by excess pressure. In conventional design, pressure relief devices, such as pressure-relief or -safety valves, are used as the primary means of pressure protection.

However, in many reactive applications, the use of a pressure relief valve (PRV) is impractical. Alternative methods of preventing overpressure must be utilized to achieve measurable risk reduction. Fortunately, API 521 and Code Case 2211 of ASME Section VIII, Division 1 and 2, provide an alternative to PRVs – the use of a safety instrumented system. Since these safety instrumented systems must achieve a high safety availability, they are often referred to as high integrity protection systems (HIPS). This paper will discuss how to assess, design, and implement HIPS to effectively manage potential overpressure of equipment used for reactive processes.

Code Requirements

Until August 1996, ASME required the installation of PRVs on all pressure vessels for compliance with Section VIII, Division 1, para UG-125(a) Section VIII, Division 2, para, AR-100. With the approval of ASME Code Case 2211, ASME acknowledged that overpressure protection should be provided by the most appropriate engineered option. The Code Case is intended to enhance the overall safety and environmental performance of a facility. It is not intended as a blanket approval of the operation of pressure vessels without PRVs. While no specific performance criteria are included in Code Case 2211, the use of HIPS must result in an installation as safe or safer than conventional design. HIPS can be used to provide overpressure protection if a quantitative or qualitative risk analysis of the proposed system is conducted, addressing credible overpressure scenarios. It must be demonstrated that the proposed system is independent of the potential causes for overpressure; provides the risk reduction of a PRV; and is capable of completely mitigating the overpressure event.

Recommended Practices

API recommends a number of practices for addressing pressure relieving systems in the petroleum production industry. For example, API 521 provides assessment and design methods for determining relief loads based on credible overpressure scenarios. These relief loads are used for individual vessel relief valve sizing and for main flare header sizing, which includes the simultaneous venting of all affected vessels. The fourth edition of API 521 allows credit for a favorable response of the instrumented systems. Despite API 521 permitting design alternatives, API 521 Part 2.2 recommends the use of HIPS only when the use of a PRV is *impractical*.

Pressure Relief Valves

In conventional design, the primary means of protection against vessel overpressure is a pressure relief valve (PRV). A PRV is a simple, mechanical device that opens in proportion to an increase in pressure over the design set pressure. The pressure is relieved through the PRV either to the atmosphere or to a contained collection system, such as a flare, scrubber, or thermal oxidizer.

PRVs are relatively available devices, as long as they are properly sized, located, inspected, and maintained. Reliability information for a single-valve relief system is provided in “Guidelines for Process Equipment Reliability Data” by the Center for Chemical Process Safety. Table 1 provides a summary of this data, which shows substantial uncertainty in the failure to open on demand.

Table 1. PRV Failure to Open on Demand

PRV Type	Failure to Open on Demand		
	Lower	Mean	Upper
Spring Operated	7.90E-06	2.12E-04	7.98E-04
Pilot Operated	9.32E-06	4.15E-03	1.82E-02

Reactive Processes

Reactive chemicals and their associated processes present complex scenarios for PRV design. Small deviations in reactant concentration or reaction conditions can put the reaction on a path for which the process design, control system, and operating procedures are inadequate to manage. To ensure safe operation, PRVs and safety instrumented systems can be used to mitigate the overpressure caused by the uncontrolled reaction. Unfortunately, many PRVs are improperly sized for reactive processes, because the relief rate calculations are often based on a design and operational envelope that ignores potential reaction paths that are not well understood.

Numerous recent incidents, including those at Georgia Pacific (Columbus, Ohio, 1997), Morton International (Paterson, NJ, 1998), Concept Sciences (Hanover Township, PA, 1999), Chevron Phillips Chemical Company (Pasadena, TX, 1999), and BP Amoco (Augusta, GA, 2001) have proven that there are reactive scenarios under which a PRV is ineffective. These incidents provide evidence of the following scenarios:

- Reaction generates pressure at an uncontrollable rate (e.g., runaway reaction or decomposition) such that an impractically large vent area is required or, in the worse case, an adequately sized PRV is not possible;
- Reaction occurs in a localized area (e.g., hot spots), propagating pressure at a rate so fast that loss of containment occurs before PRV is able to act;
- Reaction occurs in a localized area (e.g., hot spots), raising temperature above thermal decomposition point causing an internal detonation or fire;
- Reaction produces, during normal operation, materials that partially or completely block PRVs; and
- Polymerization reaction continues as material is being relieved through PRV into lateral headers, plugging the relief device and/or lateral header.

Thus, the very nature of the reactive process is often sufficient to justify that the PRV is impractical, as required by API 521. For the cases referenced above, HIPS should be investigated as a means to supplement the PRV for overpressure protection. The PRV will be required to mitigate overpressure due to external fire. The HIPS will mitigate reaction-related overpressure scenarios.

Hazard Analysis

Successful implementation must be based on a hazard analysis of each potential overpressure scenario. The hazard analysis should follow a structured, systematic approach, using a multidisciplinary team. It should document the event propagation from the initiating cause to the final consequence (also referred to as the "overpressure scenario"). The analysis must examine operating and upset conditions that result in overpressure. The examination of operating conditions must include a thorough review of each step involved in start-up and shutdown, in addition to normal operation. For batch and semi-batch processes, each step of operation must be reviewed using typical deviations and batch-oriented deviations, such as skipped steps, steps out of sequence, steps incomplete, steps at wrong time, recipe incorrect, etc.

The analysis should include a detailed examination of reactive scenarios, brainstorming on potential reaction paths that could lead to high pressure. All reaction paths should be examined, including those that may require multiple errors or failures to begin propagating. Once the reaction paths are understood, a HIPS can be designed to address each reaction scenario. In many cases, only one or two HIPS are required for mitigation of all potential reaction scenarios.

Safety Requirement Specification

The safety requirement specification (SRS) includes the functional and integrity requirements for the HIPS. The SRS describes how and under what conditions the HIPS will mitigate each overpressure scenario, including a functional logic description with trip set points and device fail-safe action. For reactive processes, the HIPS design is often complicated by the process dynamics and by complex process variable interactions.

A HIPS design may use a single process variable when the reaction path is relatively easy to detect. For example, on high temperature, the catalyst feed will be stopped or on high pressure, the reaction kill solution will be injected. A single process variable is also used as part of startup permissives to prevent startup under unsafe operational conditions. For example, the catalyst cannot be added until a fixed volume of solvent, which serves as a heat sink, has been added to the reactor.

Multiple process variables are used when the reaction path is more complex. Flow/mass ratios, temperature/pressure relationships, and kinetic calculations are often used. It is best to try to keep the HIPS as simple as possible. However, if the reaction paths are complex, the HIPS complexity will escalate.

When using reactor kill systems, it may be possible to have preemptive interlocks, designed to prevent the reaction from progressing to the point where it must be killed. These preemptive interlocks may close reactor feeds, open a pressure control vent, or close catalyst valves. If the temperature or pressure continues to increase after the preemptive interlock, a reactor kill can be initiated. By using a preemptive interlock, the plant may be able to recover from the process upset much quicker with less production loss and downtime. The combination of the interlocks and the reactor kill system constitute the HIPS for these applications.

The potential rate of pressure escalation must be compared to the HIPS response time to ensure that it is fast enough to prevent vessel overpressure. The HIPS 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 closure speed of the final element. The valve actuator must provide sufficient driving force to close the final element under the worse case, upset pressure condition.

The SRS also documents the safety integrity requirements, including the Safety Integrity Level (SIL) and anticipated testing interval. At a minimum, the target SIL for the HIPS should be equivalent to the performance of a PRV. Reliability information was shown previously in Table 1, illustrating a high degree of uncertainty in the failure to open on demand. The data implies that the HIPS should be designed to meet either an SIL 2 or SIL 3 requirement, depending on the type of PRV. However, it should be recognized that the failure modes of a PRV and the HIPS are different. A PRV that fails to operate at the set pressure may nevertheless operate at a higher pressure, whereas a HIPS is more likely to fail completely. The failure to open on demand uncertainty coupled with the difference in the failure modes results in the vast majority of users setting an SIL 3 target for the HIPS.

Device Integrity and Architecture

It is important to recognize that a HIPS is an entire instrument loop from the field sensor through the logic solver to the final elements, along with other devices required for successful HIPS functioning, such as HIPS user interfaces, communications, and power supplies.

Process Sensors. The most common process variables are pressure, temperature and flow. To achieve the fault tolerance necessary for SIL 3, a minimum of 1oo2 or 2oo3 voting sensors are required. Most HIPS use transmitters for all field inputs to allow input diagnostics to be implemented. This significantly reduces the probability to fail on demand for the field inputs. Separate process connections are also required to minimize common cause faults, such as plugged process taps.

Logic Solver. The logic solver hardware must meet 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 must provide a high level of self-diagnostics and fault tolerance. Redundancy of signal paths and logic processing is necessary and the trip output function must be configured as de-energize to trip.

Final Elements. The final elements are typically 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. To achieve the fault tolerance, dual final elements in a 1oo2 configuration are required. When dual valves are used, both valves are generally dedicated block valves.

Solenoid operated valves (solenoids) configured as de-energize to trip are used to actuate the block valves. The solenoid(s) should be mounted as close to the valve actuator as possible to decrease the required transfer volume for valve actuation. Finally, the exhaust ports should be as large as possible to increase the speed of valve response.

"As Safe or Safer" Verification

The HIPS must provide an installation that is as safe or safer than conventional design, in which a PRV is used to relieve all potential overpressure scenarios. In order to document that this has been achieved, the complete design and operation of the HIPS should be quantitatively verified to ensure it meets the required average probability of failure on demand (PFDavg). HIPS are SIL 3 SIS and are often the only layer of protection against the overpressure event. Consequently, many users require that an independent, third party perform the evaluation of the appropriateness of the design and the determination of the PFDavg.

Conclusion

HIPS can be used to safely mitigate potential reactive overpressure scenarios. As with any instrumented system, good design depends on good specification. For HIPS, the origin of the design is the process hazard analysis, which must identify all overpressure scenarios. Then, the HIPS is designed to mitigate these scenarios. HIPS is often the "last line of defense," so its failure during a reactive scenario will likely result in loss of containment. Consequently, ensuring the integrity of HIPS through proper field design, device testing and maintenance, is the only way to truly ensure safe operation.

Bibliography

✓ 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.
- ✓ "Guidelines for Process Equipment Reliability Data," Center for Chemical Process Safety of the American Institute of Chemical Engineers, NY, NY, 1989.
- ✓ 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
- ✓ "Safety Instrumented Systems (SIS)—Safety Integrity Level (SIL) Evaluation Techniques," ISA TR84.00.02, 2002.
- ✓ Summers, A.E., "High Integrity Pressure Protective Systems," Instrument Engineers' Handbook, Bela G. Liptak, editor-in-chief, 3rd edition, CRC Press, 2002.
- ✓ Summers, A.E., "Consider an Instrumented System For Overpressure Protection," *Chemical Engineering Progress*, American Institute of Chemical Engineers, New York, NY, November 2000.
- ✓ U.S. Chemical Safety and Hazard Investigation Board, "Investigation Report: Chemical Manufacturing Incident," No.1998-06-I-NJ, April 1998.
- ✓ U.S. Chemical Safety and Hazard Investigation Board, "Case Study - The Explosion at Concept Sciences: Hazards of Hydroxylamine," No.1999-13-C-PA, March 2002.
- ✓ Windhorst, Jan C.A., "Over-pressure Protection By Means of A Design System Rather Than Pressure relief valves," CCPS International Conference and Workshop on Risk Analysis in Process Safety, American Institute of Chemical Engineers, Atlanta, GA, October, 1998.

This paper was previously presented at the Center for Chemical Process Safety Symposium, Scottsdale, AZ, September 24, 2003.