HIGH INTEGRITY PROTECTION SYSTEMS FOR NEW AND EXISTING VESSELS

Bryan A. Zachary and Angela E. Summers, Ph.D., P.E.
SIS-TECH Solutions, LP and SIS-TECH Application, LP

"High Integrity Protection Systems for New and Existing Vessels," International Mechanical Engineering Conference, American Society of Mechanical Engineers, La Jolla, California, June 2004.

High Integrity Protection Systems (HIPS) are Safety Instrumented Systems (SIS) implemented to address overpressure scenarios in lieu of a pressure relief valve (PRV). HIPS essentially replaces the PRV for those scenarios that the SIS is designed to prevent. HIPS applications are generally pipeline and pressure vessel overpressure protection.

The fourth edition of API 521 allows credit for a favorable response of the instrumented systems that prevent over-pressure and/or over-temperature. The recommended practice refers to these systems as high integrity protection systems and states that they should be at least as reliable as a pressure relief device.

For new vessels, 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. This requires a detailed analysis to determine the maximum pressure developed due to credible events.

HIPS are SISs and should be designed in accordance with ANSI/ISA 84.00.01-2004. The five major steps for designing HIPS will be discussed for New Vessels and Existing Vessels.

Step 1:

All Vessels

The first step is to develop a list of credible overpressure scenarios under operating and upset conditions involving human error, instrumentation failures, and equipment failures. A multi-disciplined team should perform a systematic study of the hazards. Any commonly used hazard & risk analysis technique can be used for the hazard scenario identification. The CCPS book, "Guidelines for Hazard Evaluation Procedures," provides an overview of several techniques. The CCPS book, "Layers of Protection Analysis: A Simplified Risk Assessment Approach," provides an overview of layers of protection analysis, which is a relatively new analysis technique that is gaining wider acceptance.

The "Causes of Overpressure" described in Section 2 of API 521 should be considered during the 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, such as loss of containment. The consequence evaluation is performed without the consideration of protection layers. For example, a pressure control loop may be used to decrease supply pressure below the Maximum Allowable Working Pressure (MAWP) of a downstream vessel. If this control loop failed, the system pressure would exceed the MAWP of the vessel. The overpressure leads to a potential rupture of the vessel, releasing its flammable contents instantaneously to the atmosphere.

Step 2:

New Vessels

ASME Code Case 2211 recognizes that the previously identified scenarios can be rendered non-credible through the application of inherently safer design and Safety Instrumented Systems (SIS). The CCPS book, "Inherently Safer Chemical Processes: A Life Cycle Approach" discusses methods for designing the process to be more inherently safe. For example, a pump can be specified such that the maximum pump discharge pressure is less than the MAWP of the downstream vessel. For any SIS, ANSI/ISA 84.00.01-2004 should be followed to ensure that the design, operation, maintenance, and testing philosophy provides the integrity necessary to render each scenario non-credible.

ASME Code Case 2211 focuses on the probability of rupture only. The Code Case requires that the event be rendered non-credible. For typical chemical applications, accepted practice at many companies is that the frequency of rupture should be less than 1 in 10,000 years to be considered non-credible. However, for vessels which could potentially release significant quantities of toxic materials, the non-credible criteria is lower (e.g., 1 in 100,000 years), depending on the degree of toxicity, amount of released material, and location of potentially affected people.

As an example, assume an initiating cause frequency on the order of 1 in 10 years (e.g., failure of a process control loop). If an instrumented system is provided to render the scenario non-credible, the SIS would need to achieve Safety Integrity Level (SIL) 3. This is regardless of the specific consequence of the loss of containment.

Existing Vessels

For existing vessels, many users define events that can "reasonably be achieved" by using documented risk tolerance criteria. The risk posed by each overpressure scenario is evaluated in terms of initiating cause frequency and consequence. The mitigated frequency is then determined by identifying the risk reduction provided by any protection layers. During this analysis, no risk reduction credit is taken for the pressure relief valve. If the mitigated risk (without the pressure relief valve) achieves or is below the risk tolerance criteria, the scenario is considered for removal from the relief device and flare loading calculations. For major loss of containment events, this typically results in the requirement for an SIS that achieves SIL 3. For lower consequence events, the SIL requirement may be lower. Thus, the SIL requirement is based on the consequence of the event, as well as the frequency.

Step 3:

Once the SIL requirement is known, the SIS must be designed. The SIS design typically consists of redundant sensors connected to a redundant logic solver with outputs to redundant isolation points, such as pumps and/or valves. The Users' process reliability and testing interval goals often impact the amount of redundancy and diagnostics incorporated in the design. Thus, the user chooses an architecture that achieves the SIL yet also achieves the necessary process reliability and desired testing intervals.

New Vessels

The Code Case requires a "detailed description of any instrumentation and control system, which is used to limit the system pressure." This is fulfilled by the safety requirements specification detailed in ANSI/ISA 84.00.01-2004. The safety requirements specification provides the functional and integrity requirements for the SIS. This document or set of documents becomes a control document that should be maintained throughout the life of the SIS.

Existing Vessels

Over the life of a plant, process optimization projects are implemented, new overpressure scenarios are identified, or pressure relief valves are found to plug. In these cases, the user documents the safety requirements specification for the SIS, as discussed under new vessels, and ensures that the SIS achieves the SIL necessary to meet their risk tolerance criteria.

All Vessels

The Code Case requires "identification of any truly independent redundancies." API 521 also states that the level of credit that can be taken for instrumented response should be calculated based on the redundancy, maintenances schedules, and other factors that affect instrument reliability. Independence between the initiating cause and the protection layer is a fundamental principle of modern loss prevention. In fact, ANSI/ISA 84.00.01-2004 requires the following:

- identification of the initiating cause for hazardous events,
- independence between the protection layer(s) and the initiating cause, and
- evaluation of the impact of any potential common cause failures between initiating causes and protection layers.

Thus, the SIS must exhibit three characteristics: functionality, integrity, and independence. To achieve independence equivalent to the pressure relief valve, the HIPS should be a physically separate system from the basic process control system.

Step 4:

New Vessels

When the design is complete, the Code Case requires a reliability evaluation (qualitative or quantitative) of the overall safety system. The option of qualitative or quantitative agreed with the requirements of ANSI/ISA 84.01-1996. This standard was released prior to the Code Case and required a qualitative or quantitative evaluation of the SIL of each SIS.

The soon-to-be-released ANSI/ISA 84.00.01-2004 has many new requirements, including the requirement that the SIL of the SIS be verified quantitatively. A new guidance document is being prepared by the SP84 committee to assist users in the transition from ANSI/ISA 84.01-1996 to ANSI/ISA 84.00.01-2004. ISA TR84.00.02 is a technical report that provides information on how to perform the SIL verification calculation.

Existing Vessels

For new overpressure scenarios or where the pressure relief system is found to be inadequate, the SIL of the new or retrofitted SIS should be evaluated quantitatively for compliance with ANSI/ISA 84.00.01-2004. The quantitative evaluation ensures that the SIS design, operation, maintenance, and testing philosophy achieves the SIL.

Step 5:

All Vessels

To achieve high integrity, the SIS must be designed using low failure rate, redundant components. The SIS components typically undergo frequent testing, unless substantial diagnostics is provided, in order to achieve the SIL. The SIS must then be operated, maintained and tested throughout the life of the plant.

HIPS Example

Plant personnel were working on a major unit expansion that involved debottlenecking one of the process units. The initial design showed favorable capital cost relative to the increased plant production. A process hazards analysis was performed to identify various overpressure scenarios associated with the expansion. One scenario involved a pipeline supplying gas to the process unit. The pipeline had a pipe specification change from 750-psig to 150-psig. During normal operation, the process pressure was reduced using a pressure control valve. If this pressure control valve failed, the downstream process pressure exceeded the 150-psig pipe specification, resulting in a potential release of a large volume of gas within the process unit. To prevent pipeline rupture, a Pressure Relief Valve (PRV) was located downstream of the pressure control valve. The PRV was designed to safely relieve the pressure to a flare system.

Flare loading was then calculated and a serious problem became immediately apparent. The flare system could not handle the load of the expanded process unit. The largest load was determined to be the pipeline PRV. The cost of expanding the flare system was very high, since the flare header and flare would need to be replaced.

The team began evaluating various options. One option was to relieve the pipeline pressure to the atmosphere rather than to the flare system. Unfortunately, the PRV was located too close to the process unit for safe relief of the large gas volume. The team considered relocating the relief point to reduce the safety risk, but the environmental department vetoed this approach. The release would potentially result in excessive emissions and off-site odors. The proximity of the process unit also made defining a safe vent location difficult and expensive. The team then examined the use of a SIS and determined that the cost impact to the project was considerably less than the flare expansion option. Consequently, the decision was made to install a SIS in order to remove the pipeline relief scenario from the flare load case.

The team looked at the potential cases for overpressure that had been identified. The failure of the pressure control loop was the predominant cause of failure. The team decided to use high pressure to initiate closure of block valves. The team documented the SIS functionality and an integrity requirement of SIL 3.

The I&E department reviewed the target SIL for the other shutdowns in the process unit. No other SIS had a target greater than SIL 1. The team decided to implement the HIPS as a separate relay system, so that a less costly programmable electronic system (PES) could be used for the other SIS. The use of the separate relay system provided two side benefits: it would mimic the independence provided by a pressure relief device and it would minimize potential common cause faults between the main unit SIS and the HIPS.

The first HIPS design assessed by the I&E team incorporated dual (1oo2) pressure transmitters, dual relays, and dual block valves. This design met the minimum fault tolerance requirements in ANSI/ISA 84.00.01-2004. Transmitter diagnostics were provided by sharing the analog signal between the relay system and the Basic Process Control System (BPCS). The BPCS was then used to generate a deviation alarm when the redundant signals begin to deviate unacceptability. Each block valve was actuated using a simplex solenoid. Figure 1 shows a simplified drawing of the initial design.

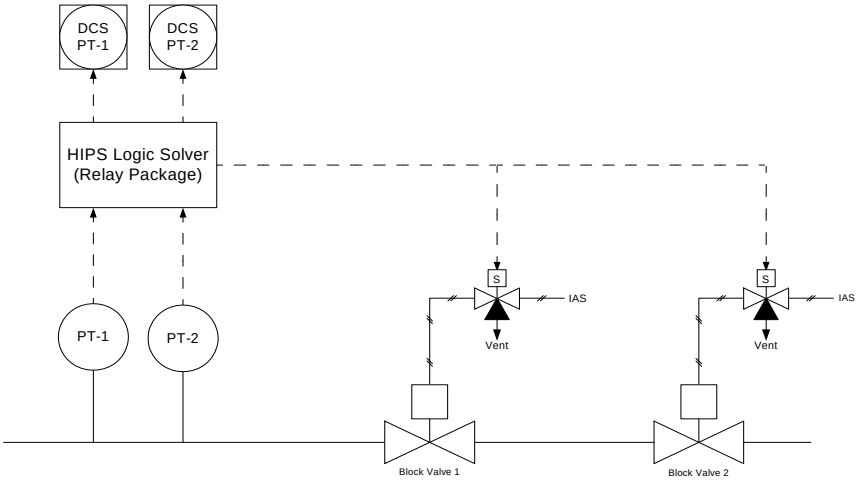

Figure 1. The initial design for the HIPS

This architecture required a one-year testing interval to achieve a PFD_{avg} in the SIL 3 range. Since the refinery unit was on a five-year turnaround schedule, provisions for on-line testing had to be provided. This included the installation of a bypass line and bypass valve (car sealed closed) and a bypass for each transmitter input signal. Further, this architecture had a predicted mean time to failure spurious ($MTTF^{spurious}$) of 7 years. This $MTTF^{spurious}$ was considered unacceptably high by operations management due to the potential production losses.

Consequently, the architecture was changed as follows:

- 2oo3 pressure transmitters with diagnostics
- 2oo3 voting relays (SIS-HIPS)
- ASCO RCS DP, normally closed version, used for valve actuation and partial stroke testing
- Double block valves

The revised architecture is shown in Figure 2.

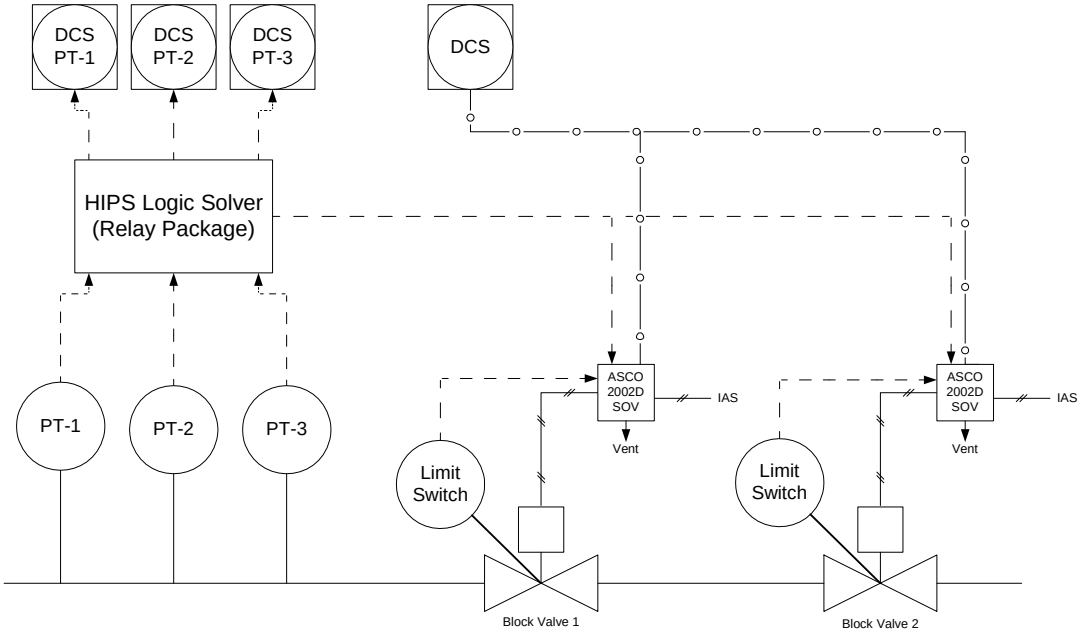

Figure 2. Final design for the pipeline HIPS

Transmitter diagnostics were provided by sharing the analog signal between the relay system and the Basic Process Control System (BPCS). The additional transmitter provided an architecture that could be tested without bypass. The use of the ASCO RCS provided for monthly, automatic testing of the solenoids and partial stroke testing of each block valve without bypass.

The revised architecture achieves a PFD_{AVG} in the SIL 3 range with annual testing of the pressure transmitters, monthly solenoid testing, monthly partial stroke testing of the block valves, and five-year full stroke testing of the block valves. Since full-stroke testing was extended to unit turnaround, full flow bypass

lines and valves were eliminated, yielding substantial reduction in capital cost. The $MTTF^{spurious}$ was also improved to more than 200 years, significantly reducing the potential of a spurious trip.

HIPS Justification

Successful implementation requires examination of applicable regulations and standards, including local codes and insurer requirements that may mandate the use of pressure relief devices. The justification must be based on a hazard & risk analysis following a structured, systematic approach using a multidisciplinary team. This analysis identifies the hazard scenarios in terms of initiating cause and consequence. An independent SIS that meets the functional and integrity requirements is then implemented to address the hazard scenario. As long as the design is as safe or safer than conventional design with a PRV, the design can be optimized to achieve the desired process reliability.

BIBLIOGRAPHY

- Center for Chemical Process Safety (CCPS) (1996). *Inherently Safer Chemical Processes: A Life Cycle Approach*. New York: American Institute of Chemical Engineers.
- Center for Chemical Process Safety (CCPS) (1992). *Guidelines for Hazard Evaluation Procedures*. New York: American Institute of Chemical Engineers.
- Center for Chemical Process Safety (CCPS) (2001). *Layers of Protection Analysis: Simplified Process Risk Assessment.* New York: American Institute of Chemical Engineers.
- Instrumentation, Systems, and Automation Society (ISA) (1996). ISA-84.01-1996. *Application of Safety Instrumented Systems to the Process Industries*. Research Triangle Park, NC: Instrumentation, Systems, and Automation Society.
- Instrumentation, Systems, and Automation Society (ISA) (2004). ANSI/ISA-84.00.01-2004. *Application of Safety Instrumented Systems to the Process Industries*. Research Triangle Park, NC: Instrumentation, Systems, and Automation Society.
- 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
- Summers, A.E., "High Integrity Pressure Protective Systems*," Instrument Engineer's Handbook*, 3rd edition, CRC Press, New York, New York.
- 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.