BURNS McDONNELL

WHITE PAPER / **RISK ANALYSIS AND SYSTEM AUTOMATION**

IMPROVE OPERATIONS AND REDUCE PROCESS RISK BY AUTOMATING THE APPLICATION OF KNOWLEDGE

BY Chad Schaffer

Risk analysis methods such as Layer of Protection Analysis (LOPA) may contribute to an underutilization of the Basic Process Control System (BPCS) to manage process risk. By automating corrective actions in the BPCS, facility owners can experience reduced costs and process risk, and minimize shutdowns.

LAYERS OF PROTECTION

Layer of Protection Analysis (LOPA) is an order-of-magnitude, semiquantitative method to compare the process safety risk presented by the known hazards at a refinery or petrochemical facility against corporate risk tolerance criteria. The goal of a LOPA study is to determine whether the risk presented is acceptable, and if not, identify potential means to make it so.

Figure 1 is a typical representation of how multiple layers of protection guard against the potentially hazardous impacts of a process.

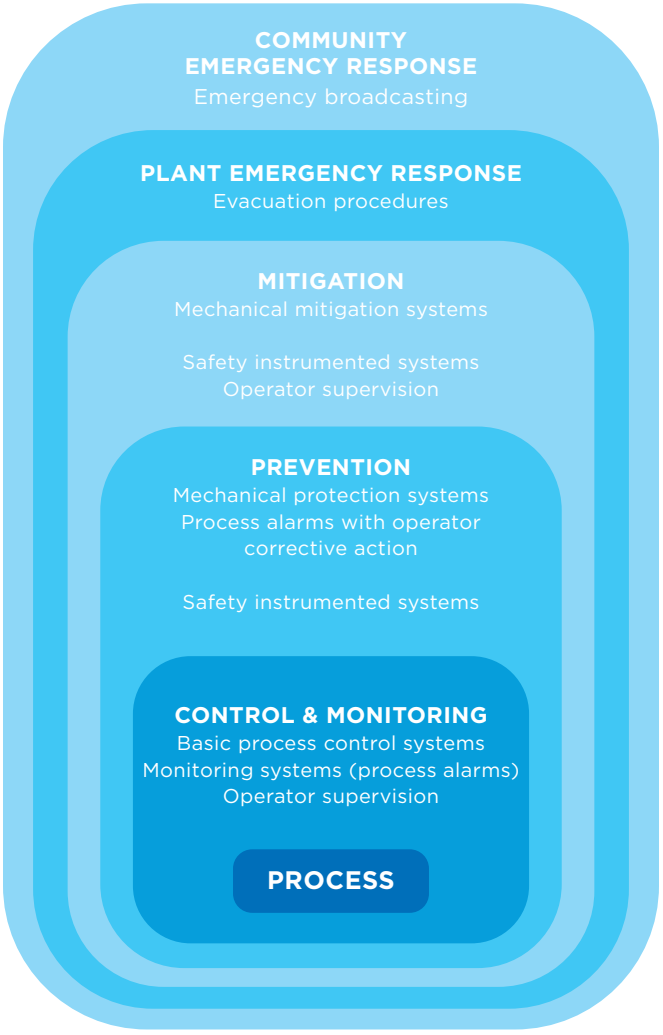

FIGURE 1: *From ISA 61511-2018 "Functional safety – Safety Instrumented Systems for The Process Industry Sector," formerly known as ISA 84.*

THE BPCS LAYER

Most people who have participated in an LOPA study are familiar with the limits on how much credit can be given to the Basic Process Control System (BPCS) when it takes an action to correct an abnormal situation. At most facilities the BPCS is the main distributed control system (DCS) or programmable logic controller (PLC) system that continuously monitors and regulates the process to keep flow rates, liquid levels, pressures, temperatures and other process variables within normal operating ranges.

The Center for Chemical Process Safety (CCPS) book, "Layer of Protection Analysis: Simplified Process Risk Assessment," published in 2001, allows two different approaches for assigning Risk Reduction Factor (RRF) credit to the BPCS. In simple terms:

- Approach A allows for the BPCS to be credited with an RRF of up to 10 if the cause of the scenario is something other than the BPCS. If the cause is the BPCS itself, then no RRF credit can be given to it.
- Approach B allows for the BPCS to be given more credit than is permitted by Approach A. In the case where the cause of the scenario is the BPCS, then it can still potentially be credited with an RRF of up to 10. If the cause of the scenario is something other than the BPCS, then the BPCS can potentially be credited twice, each with an RRF of up to 10, allowing for a total BPCS RRF of up to 100.

There are many caveats around the proper use of Approach B, which the original CCPS LOPA book and a more recent CCPS companion book, "Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis," published in 2015, address in detail.

Approach B has been used by operating companies, both large and small. However, in recent years, there has been recognition that it may give an overly optimistic view of the management of risk by the BPCS. Not every BPCS is installed and operated in a way that achieves an RRF of 100, day and night, year after year, over its entire useful life. Consequently, an unrecognized gap between the real risk and corporate risk tolerance criteria could remain.

For this reason, the use of Approach A is becoming more common, which decreases the amount of risk reduction that can be credited to the BPCS by a factor of 10. Today, the use of Approach B generally requires additional analysis and justification.

ALARM AND SAFETY INSTRUMENTED SYSTEM LAYER CONSIDERATIONS

If the BPCS is not able to keep the process within the normal operating limits, an alarm limit may be reached. The role of the operator to respond to an alarm is typically to take action that either returns operation to within the normal limits or safely stops production.

There are also limits in LOPA about when and how much credit can be given to corrective intervention by an operator. One such limit is that the amount of time required for the operator to receive an alarm, decide what to do about it, then take action to correct the situation (i.e., the response time) must be less than the time required for the hazardous event to develop and pass the point of no return (i.e., the process safety time). If the operator cannot reliably respond in time, then no credit should be given.

The evaluation of how much RRF credit can be assigned to the BPCS is complicated by the fact that operator intervention is often partially dependent on the BPCS. It is usually through the BPCS human-machine interface (HMI) that the operator is made aware of the alarm, and the operator may also rely on use of the BPCS HMI to be able to respond in time.

Consequently, there has been a gray area in how operator response to alarm is addressed within LOPA. Some companies may consider that operator response to alarm is part of the BPCS RRF credits allowed, while others may treat it as separate. Figure 1 reflects this uncertainty, with "process alarms" appearing in both the "Control and Monitoring" and the "Prevention" layers. It appears likely that the new International Society of Automation (ISA) standard currently in development, ISA 84.91.03 "Process Safety Controls, Alarms, and Interlocks as Protection Layers," will make operator response to alarm more formally part of the BPCS credit.

Another complication, according to ISA 61511-2018 "Functional safety - Safety Instrumented Systems for The Process Industry Sector," formerly known as ISA 84, is that a BPCS with an RRF greater than 10 may require it to be designed and maintained as a Safety Instrumented System (SIS). Classifying the BPCS as an SIS is typically not desirable, and in most cases, is not practical.

These factors together have and will generally continue to result in less risk reduction credit being assigned to both the BPCS and the operator during LOPA, and more credit being assigned to the SIS, so that the overall process risk can be managed to the corporate tolerance.

UNINTENDED CONSEQUENCES

A purpose-built SIS is robust — typically suitable for up to Safety Integrity Level (SIL) 3, the equivalent of an RRF of 1,000 — and is generally capable of closing most gaps in the residual risk. The limits placed on the BPCS performance in typical risk analysis methods such as LOPA may serve to discourage some users from maximizing the capabilities of their BPCS because they provide no additional benefit in the risk analysis. This can be a missed opportunity.

The SIS typically behaves similarly to the automatic emergency braking (AEB) features available in newer cars. Like the AEB, normally the SIS is almost invisible because it simply monitors what's happening. Action is only taken when a safe operating limit is exceeded.

In a car, the AEB generally does nothing until it detects that the distance to the vehicle ahead is shrinking and the driver is not applying the brakes strongly enough to stop in time. The AEB intervenes and applies the brakes to prevent a collision. Similarly, the SIS is generally designed to stop the process suddenly and with sufficient force to make it safe.

Just as a car driven by an inattentive driver may have more frequent activations of the AEB system, the reduced emphasis placed on managing risk with the BPCS may result in more frequent activations of the SIS. Unfortunately, restarting a refinery production unit that's been shut down by the SIS is not nearly as simple as getting a car moving forward again.

Unit restart tends to be labor-intensive, expensive and carries greater risk than normal operation. In addition, because many processes operate at elevated temperature and pressure, the equipment and piping must cycle through extremes of mechanical stress, causing wear and tear on them, and reducing their useful life.

While most means used to manage risk are likely to require inspection and maintenance to sustain their integrity, the SIS demands a very high level of testing and documentation. Because of its dormant nature, the SIS requires periodic testing to detect covert failures in the system and demonstrate that it is able to perform as intended. The greater the RRF required, the more frequently testing of the SIS must be performed. Therefore, a shift in risk reduction from the BPCS and operator to the SIS carries with it a need for more frequent testing of a complex system that is intended to cause a process shutdown.

Another unfortunate side effect of the increased emphasis on the SIS for risk reduction is that it has become more difficult to justify projects to improve the real-world performance of the BPCS. This is because the risk analysis will not necessarily allow for additional credit to be claimed.

Why would a company invest in a project to improve the BPCS if it won't demonstrably address the gap in process risk like an investment to improve the SIS would? The good news is that there are a lot of reasons why it makes sense.

BENEFITS OF AUTOMATING THE APPLICATION OF KNOWLEDGE IN THE BPCS

For years many companies in the oil, gas and chemical industries have been dealing with the loss of their most experienced operators to retirement. Recent developments have accelerated the loss of engineers and operators along with the institutional knowledge that they carry. This is an area where additional automation can be beneficial to help make up for knowledge and experience that otherwise would be lost.

ALARM RESPONSE PROCEDURES

When an alarm activates, the operator needs to troubleshoot what is happening in the process and determine an appropriate response. Traditionally, this is done by referencing a written procedure or relying on the operator's knowledge. One automation tool that's available to make this more efficient is the use of alarm response procedures, commonly called "alarm help," within the BPCS, which can be a way to immediately inform the operator of the most likely problems and their solutions. This enables the operator to troubleshoot and respond more promptly and effectively.

AUTOMATED RESPONSE TO AN ABNORMAL SITUATION

Taking this concept a step further, if a certain alarm or process condition is always addressed using the same solution, then the response procedure could potentially be automated. Rather than waiting for the operator to work through the alarm response procedure, the BPCS can immediately take a corrective action to override or constrain the actions taken by its controllers, return the process to its normal limits or move to a safer mode of operation.

For example, if the response to a high-pressure condition is to reduce the flow rate of steam to a heat exchanger, the BPCS can take this action on its own and inform the operator of what it did. The role of the operator then becomes verification that the action taken was sufficient to resolve the upset condition or make further adjustments if needed.

These types of automated responses can be particularly valuable if there is insufficient response time available for the operator to be able to reliably take corrective action. Because the automated response is most likely in the BPCS, it may or may not be able to be credited with any additional RRF. But because it can act more promptly and consistently than a human, it still can be effective at maintaining stable operation and avoiding an SIS shutdown that might otherwise occur.

STATE-BASED ALARMS

Some alarms are only meaningful when the associated equipment is in a certain operating state. For example, if a pump is not intended to be running, then the low flow or low pressure alarm located in the pump discharge is not necessarily useful and could in fact become a nuisance and ignored over time. This is not the case if the pump was intended to be running and the alarm has purpose. A BPCS that keeps track of the intended and actual operating states of equipment can be programmed to shelve alarms that are not relevant at that time.

MULTIVARIABLE ALARMS

Not every alarm has a simple response. Some upset conditions are highly complex and require the operator to review the status of multiple variables to understand what's happening and determine the appropriate response. There is an automation solution for this as well. Multivariable alarms can evaluate the values and trends of several variables simultaneously and present the most likely problem and solution to the operator for implementation.

An example is if there is insufficient oxygen available to completely combust the fuel in a fired heater. The correct response for the operator to take may be dependent on whether it is taken early when the products of incomplete combustion have just started to appear in the flue gas, or later, after a significant volume of combustible material has already accumulated in the firebox.

A multivariable alarm can evaluate variables such as the oxygen and/or combustibles content of the flue gas, process temperatures, and fuel gas flow rate to determine what's happening and suggest the correct response. Equally important, the alarm can suggest responses to avoid, such as not changing air flow in response to a low oxygen alarm.

The correct response generally is to slowly decrease fuel flow until the oxygen in the flue gas recovers. An experienced operator will likely know this. A newer operator may take the incorrect, but instinctive, action to add more air when the oxygen goes low, which could result in an explosion of the accumulated fuel.

CONCLUSION

Identifying opportunities to institutionalize the knowledge of your operators and engineers and maximizing the capabilities of the BPCS can provide many potential benefits, including making it possible for the BPCS to take routine corrective actions more quickly and reliably than even the most experienced operator; providing less experienced operators with the right information to help them respond to alarms in a consistent and predictable manner; and reducing the quantity of SIS activations, as well as the risks and costs that accompany a restart.

BIOGRAPHY

CHAD SCHAFFER is an associate instrumentation and controls engineer at Burns & McDonnell. He leads design teams that are responsible for successful execution of large and/or complex projects, from conceptual design through turnover of the completed facility. Chad is well-versed in industry codes and standards including API, ISA, NFPA, PIP and others with active participation on the API 556 and ISA 84 (ISA 61511) working groups. During his career, he has designed expansions and improvements for facilities such as oil refineries, marine terminals, natural gas liquids (NGL) fractionators, petrochemical and synthetic rubber production plants, batch fine chemicals plants, corn wet and dry mills for ethanol production, food production, and power generation facilities.

ABOUT BURNS & McDONNELL

Burns & McDonnell is a family of companies bringing together an unmatched team of engineers, construction professionals, architects, planners, technologists and scientists to design and build our critical infrastructure. With an integrated construction and design mindset, we offer full-service capabilities with offices, globally. Founded in 1898, Burns & McDonnell is a 100% employee-owned company and proud to be on *Fortune*'s list of 100 Best Companies to Work For. For more information, visit **burnsmcd.com**.

21294-RAS-1220