Session 736

Critical Controls - New Imperatives for Industry

Glenn G. Young, C.S.P. - Owner
Glenn Young & Associates, LLC PSM Consulting

Glenn S. Crowe, C.S.P. - Safety Manager
PCS Nitrogen-Phosphates

Introduction

The concept of evaluating control systems on the basis of risk and applying resources to make high-risk controls more reliable is not new. Chemical plant, refinery, and pipeline designers and their insurance carriers have long realized that high-risk controls need to be more reliable than other controls. The document that codified this thinking was ANSI / ISA S.84.00.01 – 2004, Parts 1-3 (IEC 61511 Mod).[1] We will subsequently refer to this document as "S84." The other reference in the field is IEC 61508 "Functional Safety – Safety Related Systems – 1998" and its process-industry specific version, IEC 61511.

S84 is a consensus standard and is not formally binding. S84 has been in common use in the aerospace and nuclear industry since its inception. Chemical plants, refineries, and pipelines, however, are just now coming to the realization that the standard has much to offer them as well.

The regulatory implementation of the S84 became "generally accepted engineering practice" by way of an industrial explosion in 2004 where five workers were killed. The Occupational Safety and Health Administration (OSHA) cited the employer under the general-duty clause for not documenting that the plant's programmable logic controllers and distributed control systems installed prior to 1997 complied with generally accepted engineering practice such as S84. Since this citation was paid without contest, a precedent has been set that these consensus standards are now generally accepted engineering practice in the chemical manufacturing, refining, and pipeline industries.

Both OSHA and the Environmental Protection Agency (EPA) have recognized the potential value of the S84 standard. In fact, multiple companies have been cited over the past decade for not following S84, despite the fact that S84 is a non-binding consensus standard. OSHA and EPA are expected to continue citing companies under the general-duty clause if any shortcoming that might have involved control systems causes a Process Safety Management (PSM) or Risk Management Plan (RMP) incident.

[1] Gruhn, Paul P.E. and Cheddie, Harry P.E. *Safety Instrumented Systems: Design, Analysis and Justification 2nd Edition* - 2006 by The Instrumentation, Systems, and Automation Society

For companies covered under 29-CFR-1910.119 (PSM) or under 40-CFR-68 (RMP), S84 or some variant of the standard should now be considered mandatory.

What does S84 require?

Since this presentation is focused on chemical manufacturers, refineries, and pipelines, the sections of S84 and IEC-61508/61511 that pertain to instrument design will not be discussed.

Instead, the overall requirements of S84 as they apply to the users of control systems are as follows:

1. Perform a risk-based analysis of the hazards caused by failure of the control system to operate on demand
2. Assign a desired reliability to the control system based on the hazard(s) created should the control system fail to operate on demand
3. If the existing control system is adequately reliable: document and maintain existing equipment so that the desired reliability is continued
4. If the existing control system is not adequately reliable: improve reliability until the possible hazard(s) are mitigated by the control system

The previous points are extreme simplifications of both the language and intent of S84. The following sections of this presentation will show methods that are commonly used in the chemical, refinery, and pipeline industries that meet these challenges.

What is a control system?

A control system is any group of one or more sensors connected to one or more logic elements that control one or more actuated elements and the connections between all elements. For example, the following five elements would all be considered a single control system:

1. a flow sensor
2. the connections from the flow sensor to the distributed control system (DCS)
3. the DCS itself
4. the connections from the DCS to a pneumatically-operated flow valve
5. the flow valve itself

A pressure relief valve that opens when a set spring pressure is exceeded would not be a control system because it lacks logic elements.

How is risk assessed for a control system?

Typically, a team identical to the Process Hazard Analysis (PHA) team makes risk assessment for control systems. Normal control functions (pressure, temperature, and flow) are typically covered in the guide-words of the PHA without need for additional assessment. Most often, supplemental layers of protection exist to safeguard against worst-case consequences should the control function fail. For example, if a pressure-control gag-valve on the outlet of a boiler should stick in the closed position, the boiler is also fitted with dual relief valves that prevent the boiler from failing catastrophically.

In the event of trip systems, however, the trip system is typically the “last resort” after hazardous conditions already exist. Usually, there are not enough additional independent layers of protection beyond the trip system to sufficiently mitigate risk. Only the trip system’s proper activation on demand can save the process from catastrophic consequences.

Unfortunately, in the context of a PHA, trip systems are typically thought of as safeguards, not as initiating causes of a scenario. To overcome this limitation, reverse the conventional thinking – *ASSUME* that the necessary conditions are present that would require a trip, and then use the failure of the trip system to operate on demand as the cause of the resulting scenario. Are the remaining independent layers of protection sufficient to mitigate the risk of the worst-case consequence? If so, document that fact and consider the trip system to be of low priority. Otherwise, designate that trip system as a critical control system (CCS) and use the next section of this paper to evaluate the criticality of the trip system.

Because control systems usually have additional layers of protection and trip systems usually don’t, CCS analysis for chemical plants, refineries, and pipelines is typically limited to trip systems. The PHA for the process normally provides sufficient control-system failure analysis. A specific CCS analysis *can* be performed on every control system in the plant, but the time and expense are not usually justified.

How is a desired reliability assigned?

The common method for determining the desired reliability of a CCS is to assume that the conditions requiring the CCS to trip are present and that the CCS fails to function on demand. The PHA team then assesses the severity of the “worst-case” consequences developed. Once the severity is determined, the likelihood of the scenario is given a baseline likelihood of 0.01 (once in 100 years, or “once in the life of the process”).

This likelihood comes from the assumption that once in a 10-year period (0.1) the conditions will exist that require the CCS to trip. The second assumption is that once in a 10-year period (0.1) the CCS will fail to function on demand. Since the conditions must exist AND the CCS must fail the two probabilities multiply (0.1 * 0.1 = 0.01). This starting likelihood can be honed by the use of semi-quantitative analysis such as Layers of Protection Analysis (LOPA) or by fully quantitative analysis methods such as event-tree or fault-tree analyses.

Multiplying the severity times the likelihood provides a risk rating. The risk is then assessed using the corporate risk matrix for the company involved. Use the risk to determine a desired reliability level for the CCS. The desired reliability level is typically expressed in a “Safety Integrity Level” (SIL) for the entire CCS system. The next section will discuss SIL levels in greater depth. Typical risks found in the chemical, refinery, and pipeline injuries generate the following desired SILs:

1. Highest Risk = SIL-3 protection
2. Second-Highest Risk = SIL-2 protection
3. Third-Highest Risk = SIL-1 protection

4. Lower Risks = No SIL needed.

What is a SIL?

In calculating the likelihood of failure for an existing control system, all elements of the control system must be assessed including the sensor(s), the logic element(s), the actuated element(s) or valves, and the connections between these elements. Because a failure of any of these elements or their connections will disable the entire system, the probabilities of failure are additive. Probability of failure on demand (PFOD) of the sensor(s) PLUS the PFOD of the logic element(s) PLUS the PFOD of the actuated element(s) PLUS the PFOD of the connections equals the total control system's PFOD.

The safety integrity level (SIL) is a measure of the reliability of the entire CCS from sensor to actuated element. To meet various SIL levels, the following total PFODs must be met:

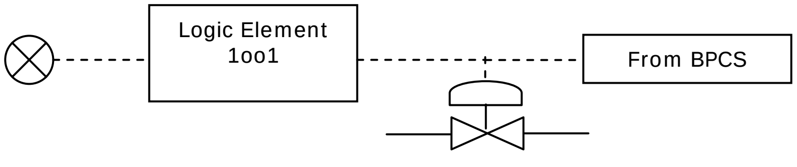
1. SIL 1 – More reliable than one failure in 10 demands, but less than or equal to one failure in 100 demands

2. SIL 2 – More reliable than one failure in 100 demands, but less than or equal to one failure in 1,000 demands.

3. SIL 3 – More reliable than one failure in 1,000 demands, but less than or equal to one failure in 10,000 demands

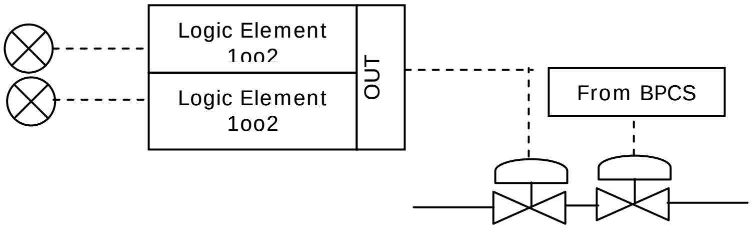
Often, the design of the system can heavily influence the reliability of the function. In the graphics below the logic designations refer to the "voting" of the trip logic. "1oo1" (one-out-of-one) means that there is only one input and when the input shows a failure, the output also sends a failure signal. For 1oo2 (one-out-of-two) systems, if either of the inputs shows a failure, the output also sends a failure signal. For 2oo3 (two-out-of-three) systems, two of the inputs must show a failure for the outputs to send a failure signal. The normal control system is shown below as "BPCS," which stands for "Basic Process Control System." Circles with a cross inside are intended to represent sensors (ALL of which are fully independent from BPCS sensors). Shown below are typical architectures for SIL 1 through SIL 3 systems:

Typical SIL-1 Architecture:

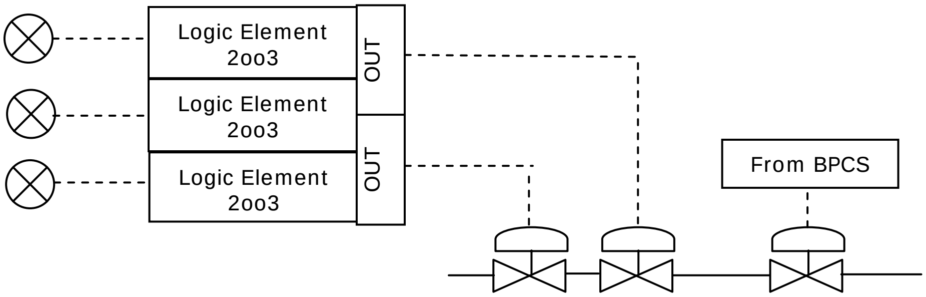


Note that in SIL-1 systems, the actuated element can be the same as used that used by the BPCS if and only if the trip function always overrides the control function AND the actuated element's reliability is maintained at the same reliability as the rest of the CCS.

Typical SIL-2 Architecture:



Typical SIL-3 Architecture:



Note that in most cases, the trip valves are fitted with test bypasses (not shown in the graphics) so that online testing of the actuated element (trip valve or valves) can be performed without shutting down the process. Note also that spurious trips are likely with SIL-1 and SIL-2 systems. Only by adding the redundancy of the SIL-3 system does the probability of spurious trips diminish significantly.

How is an existing control system evaluated?

Evaluate existing control systems by comparing their architecture to the architectures shown above. If the existing control system does not match the desired architecture, the system probably does not meet the desired SIL level. There is often strong internal financial pressure to meet the target SIL reliability with existing equipment. Unfortunately, the amount spent on shortened testing and calibration intervals quickly exceeds the amount of replacing the existing equipment. This is particularly true of CCSs used in services that are dirty or corrosive or for CCSs installed in harsh external environments.

Evaluate field-testing records for the existing control system. Does the “as found” reliability during calibrations and tests meet the reliability requirements for a SIL rating? If not, then the desired SIL level may not have been achieved.

How can the reliability of a CCS be improved?

CCS systems can be made more reliable by one or any combination of the following strategies:

1. Substitute more reliable parts for the originals
2. Add redundancy
3. Test and calibrate more frequently

When installing new systems with SIL ratings, be wary of using manufacturers' data showing instrument, sensor, and actuated-element reliabilities. Manufacturers have a strong financial motive to market their wares in the best possible light. Should a CCS fail to operate on demand, the user of the system, not the manufacturer, will be expected to legally justify why the CCS failed to meet its desired reliability.

Conclusion

Implementation of S84 or comparable standards is now considered standard industry practice for the chemical manufacturing, refinery, and pipeline industries. Resources that may be consulted for additional information include:

1. IEC-61508
2. IEC-61511
3. ANSI/ISA S84.00.01
4. Gruhn, Paul & Cheddie Harry – *Safety Instrumented Systems: Design, Analysis and Justification, 2nd Edition*, Instrument Society of America, 2006