

FAULT MANAGEMENT ANALYSIS

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

Presented at the 35th Annual Loss Prevention Symposium, April 22-26, 2000, Houston, TX.

Published in Process Safety Progress, November 2001

Abstract

In the chemical processing industry, intrinsically safe must be the process engineer's goal, but, in reality, it is often not feasible either technically or economically. In these cases, safety instrumented systems (SIS) are used to detect and respond to process risk. SISs have many components that must work as designed in order to mitigate potential hazardous incidents. Over the years, many of these components have evolved from simple electro-mechanical devices to complex mechanical, electrical, and programmable electronic devices. How these devices fail must be examined in order to understand how each component failure can propagate into fail-safe and fail-dangerous conditions.

This paper proposes the use of fault management analysis (FMA) for the assessment of proposed SIS designs. The FMA leads to the identification of not only the failure modes of each component, but also in the determination of how to appropriately manage the identified failure. This paper will provide examples of how FMA is used to assess SIS components. Then the paper will demonstrate how the proposed design, diagnostics, inspection, maintenance, and testing programs should be modified to improve the SIS performance.

Introduction

Safety in the chemical process industry is maintained using intrinsic and extrinsic safety concepts. Intrinsic safety involves designing the process to be inherently safe (1), thereby eliminating the safety risk. The goal of any project team should be to design the plant for minimum risk. However, at some point, inherent safety reaches an engineering limit where it is no longer feasible to reduce the risk further or an economic limit beyond which it is no longer practical. When the team has reached the end-point of inherent safety, extrinsic safety systems are used to reduce the risk to the tolerable risk level.

Extrinsic safety systems are add-on devices, included in the design for the explicit purpose of preventing or mitigating risk. These safety systems are installed with the intent that they will perform some action at a specific point in an incident scenario and stop the incident propagation. Extrinsic safety often involves the use of active devices, such as safety instrumented systems (SIS), which are comprised of sensors, logic solvers, and final elements. How well each of these devices performs its specific action determines whether the incident is successfully mitigated or a hazardous event occurs.

Mythology

There are many myths associated with SISs, such as the following:

- Myth Example 1: A valve, which is specified as fail to closed position on loss of air, will go to the closed position when the logic solver commands it to do so.
- Myth Example 2: A smart transmitter either fails upscale or downscale depending on it is how it is configured.
- Myth Example 3 Since SIS devices are rarely used, they maintain their integrity without inspection or testing.

These myths can be summarized as follows:

Instruments do exactly what they are supposed to do when they are supposed to do it.

The truth is that everything dies, breaks, or runs out of gas. Everything. This is especially true for SISs. As a SIS designer, it is necessary to embrace this reality. Whether it is called “Murphy’s law” or simply the natural outcome of entropy, all devices have a certain statistical failure rate.

Embrace Reality

Fault Management Program

In order to apply the failure motto to the SIS design, examine each device for its failure modes and create strategies for reducing the impact of reality.

✓ Dies...

The device loses significant functionality so that it can not perform the action.

✓ Breaks...

The device loses functionality so that it performs the action inadequately.

✓ Runs out of gas...

The power source required for the action is lost and the action cannot take place.

More technically, the analysis should begin with a “big picture” failure modes and effects analysis. Why “big picture?” Detailed failure modes and effects analysis (FMEA) is very time consuming. While a great deal of information can be derived from the analysis, the analysis is quite expensive. A macro-level FMEA can provide high quality information at reduced cost, which can be used to develop strategies for mitigating the identified failures.

Therefore, in this analysis, it is not necessary to examine each device down to the chip level. To reduce analysis time, the device should be examined by focusing on replaceable or repairable components. For a logic solver, do not examine the impact of a chip failure on the logic solver. Instead focus on how module failures affect the overall functioning of the SIS.

It is also possible to group components based on how they impact the SIS. For example, the failure of a valve to close can be assessed by examining the valve seat and valve body as one element.

When performing the assessment, list the potential failures that occur in the device, as discussed previously. Next, expand the assessment to list failures in any software or peripheral hardware that are necessary for the operation of the device, such as the following:

- process connections,
- power,
- instrument air,
- hydraulic,
- utilities,
- software,

- communications, and
- human factors.

As an example, consider a transmitter used as an input to the SIS. Table 1 provides a listing of some of the failure modes that might be identified.

Table 1. Typical Failure Modes for a Pressure Transmitter

Failure Modes
Electronic
Isolation Valve Closed
Impulse Line Leak
Impulse Line Crimped
Sensor Deformation
Loss Of Seal Fluid
Build Up Of Fluid In Impulse Line
Left In The Test Mode (smart transmitter)
Power Supply
Out Of Adjustment
Obstructed Or Plugged Tap

When assessing the effect of failure, document how the failure affects the operation of the device from a safety functional viewpoint. If the device is a sensor, how does the failure affect the signal that the logic solver receives? If the device is a final element, how does the failure affect its capability to mitigate the incident? For the pressure transmitter example, Table 2 shows how each failure mode potentially affects the signal. It is important to note that each failure mode may have more than one effect. Each effect should be documented and addressed in the analysis.

Table 2. Failure Modes and Effects for a Pressure Transmitter

Failure Modes	Effects
Electronic	Erroneous reading Fail upscale Fail downscale
Isolation Valve Closed	Erroneous low reading
Impulse Line Leak	Erroneous low reading
Impulse Line Crimped	Slow or no response to process variation
Sensor Deformation	Erroneous low or high reading
Loss Of Seal Fluid	Erroneous low reading
Build Up Of Fluid In Impulse Line	Erroneous high reading
Left In The Test Mode (smart transmitter)	False reading at steady state- no response to process variation
Power Supply	Erroneous reading: Fail downscale
Out Of Adjustment	Erroneous low or high reading
Obstructed Or Plugged Tap	Slow or no response to process variation

At this point, the failure modes and effects are known. Based on the effects on SIS performance, determine how the design could be changed to reduce or eliminate the effect. Typically, the strategies that are employed to reduce the effect of the failure are as follows:

- Specification,
- Device Integrity, i.e. components, materials of construction, etc.
- Installation Details
- Redundancy and Voting
- Testing
- Diagnostics
- Security
- Maintenance and Inspection Procedures

Table 3 shows how these strategies can be employed to mitigate the failure modes previously listed for the pressure transmitter.

Table 3. Fault Management Analysis for a Pressure Transmitter

Failure Modes	Effects	Design Strategy
Electronic	Erroneous reading Fail upscale Fail downscale	Use proven transmitters Consider redundancy to allow signal comparison Test transmitter at frequency appropriate for the safety integrity level assigned to the safety function in which the transmitter is used
Isolation Valve Closed	Erroneous low reading-no response to process variation	Improve procedure and re-check to ensure that transmitter isolation valve is returned to open state after service or testing Consider redundancy with each transmitter on separate isolation valves with signal comparison
Impulse Line Leak	Erroneous low reading	Institute procedures for operation to inspect transmitters during routine rounds Consider redundancy with each transmitter on separate isolation valves with signal comparison
Impulse Line Crimped	Slow or no response to process variation	Institute procedures for operation to inspect transmitters during routine rounds Consider redundancy with each transmitter on separate isolation valves with signal comparison
Sensor Deformation	Erroneous low or high reading	Use transmitter appropriate for service (Pressure, temperature, chemical) Consider redundancy with each transmitter on separate isolation valves with signal comparison
Loss Of Seal Fluid	Erroneous low reading	Use transmitters with remote seals Consider redundancy with each transmitter on separate isolation valves with signal comparison
Build Up Of Fluid In Impulse Line	Erroneous high reading	Use transmitters with remote seals Consider redundancy with each transmitter on separate isolation valves with signal comparison
Left In The Test Mode (smart transmitter)	False reading at steady state-no response to process variation	Improve procedure and re-check to ensure that transmitter is returned to operational state Consider redundancy to allow signal comparison
Power Supply	1. Erroneous reading; 2. Fail downscale	Avoid using components in the transmitter circuit that could limit voltage or current to the transmitter below operating threshold Use redundant power supplies for all safety system field instrumentation
Out Of Adjustment	Erroneous low or high reading	Use proven transmitters Consider redundancy to allow signal comparison Test transmitter at frequency appropriate for the safety integrity level assigned to the safety function in which the transmitter is used
Obstructed Or Plugged Tap	Slow or no response to process variation	Consider redundancy with each transmitter on separate tap to allow signal comparison

For a second example, consider a block valve with a spring return actuator. The results of the fault management analysis are shown in Table 4.

Table 4. Fault Management Analysis for a Block Valve with a Spring Return Actuator

Failure Modes	Effects	Design Strategy
Actuator sizing is insufficient to actuate valve in emergency conditions	Valve fails to close (or open)	Internal guidelines and peer review of actuator sizing calculations
Actuator diaphragm ruptures or leaks	Air is vented from valve and valve goes to fail safe condition (nuisance trip)	Preventive maintenance
Valve packing is seized	Valve fails to close (or open)	Test valve for functioning Consider redundancy
Air line to actuator is blocked or crimped	Valve is slow or fails to move closed or open	Installation and inspection guidelines Use short air line runs
Valve stem sticks	Valve fails to close (or open)	Test valve for functioning Consider redundancy
Valve seat is scarred	Valve fails to seal off	Consider redundancy

Conclusions

Designing SISs involves more than simply selecting the devices from vendor catalogs. It requires an understanding of how SIS devices fail and how to design to prevent these failures from impacting the SIS performance. Fault Management Analysis (FMA) is a method that can be used to better understand the potential failure modes and effects of each device at a macro or total system viewpoint. It begins with a systematic examination of the device, resulting in documentation of an overall strategy for minimizing the impact of each failure mode on the SIS

performance. Implementation of the program ensures that each device is managed successfully throughout its life, resulting in improved safety and installation quality.

References

1. Center for Chemical Process Safety (CCPS) (1996). *Inherently Safer Chemical Processes: A Life Cycle Approach*. New York: American Institute of Chemical Engineers.
2. "Application of Safety Instrumented Systems for the Process Industries," ANSI/ISA-ISA 84.01-1996, ISA, Research Triangle Park, NC, 1996.
3. Summers, Angela E., PhD, "Safety Requirements Specifications in a Capital Project Environment," Control Engineering, website publication, May 2000.
4. Center for Chemical Process Safety (CCPS) (1993). *Guidelines for Safe Automation of Chemical Processes*. New York: American Institute of Chemical Engineers.
5. Summers, Angela E., PhD, "Understanding Safety Integrity Levels," Control Engineering website, February 2000.
6. Summers, Angela E., PhD, "Techniques for Assigning A Target Safety integrity Level," ISA Transactions, 37, pp. 95-104, 1998.