Session Thirteen

The impact of bypassing and imperfect testing on safety instrumented system performance

Paul Gruhn, P.E., ISA 84 Expert
Global Process Safety Consultant, Rockwell Automation

Abstract

Bypassing and imperfect manual testing have historically been ignored in safety system modeling, yet the impact of both is quite easy to model, and the negative performance impact is much greater than many people realize. In fact, one of many recurring causes of chemical plant accidents has been documented as "inadequate indications of process condition", of which at least one case consisted of operations continuing when a safety instrument was in bypass[1]. The second edition of IEC 61511 about to be released[2] now acknowledges dangerous failures not detected by automatic diagnostics or manual testing. This paper will summarize how these two factors can be modeled and their dramatic impact on system performance.

Safe and dangerous failures

Safety instrumented system hardware is normally dormant (e.g., an isolation valve remains open for long periods of time). Such hardware may fail in two ways: safe and dangerous. Safe failures result in nuisance trips and lost production (e.g., the valve slams shut because the normally energized solenoid coil burns out; there was no process hazard). Dangerous failures result in the system not being able to perform its safety function when required (e.g., the solenoid de-energizes, but the valve is stuck open and does not close on demand). PFD (Probability of Failure on Demand), its reciprocal RRF (Risk Reduction Factor) and SIL (Safety Integrity Level) only relate to the impact of dangerous failures on system performance.

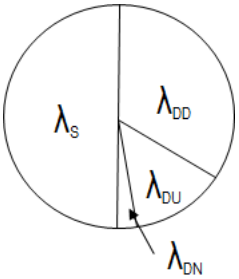
Detected, undetected, and never detected dangerous failures

Some devices ─ for example non-intelligent sensors and valves ─ have no automatic diagnostics at all. A solenoid operated valve cannot tell by itself whether it is stuck open. These failures are referred to as dangerous undetected failures (λ_{DU}). These failures must be tested for manually. The more often devices are tested, the quicker potentially dangerous failures can be detected and repaired, which results in better safety performance.

Some hardware has built-in automatic diagnostic to detect dangerous failures, referred to as dangerous detected failures (λ_{DD}). For example, transmitters and PLCs can detect a variety of internal problems such as being stuck in an endless loop. The greater the level of automatic diagnostics, the lower the quantity of dangerous undetected failures, and the better the overall system performance.

However, automatic diagnostics can never be 100% effective or complete. Some failures may remain in the device for the life (or mission time) of the device. These failures may be referred to as dangerous never detected failures (λ_{DN}). For example, a valve may stroke and close, but not seal completely due to seat damage. Partial stoking will not determine whether the seat is eroded or whether there is a welding rod stuck in the valve. Testing the electronics of a sensor does not determine whether the sensing element itself is responding properly or whether the impulse line is plugged. Removing a sensor and testing it in a laboratory or maintenance shop does not determine whether the sensor will respond properly in the actual process. Testing a level float switch by moving the float with a rod will not ensure that the float will actually float.

All three of these dangerous failure categories, along with safe failures (λ_S), are shown in Figure 1.



C_A = Automatic Diagnostic Coverage factor

C_M = Manual Diagnostic Coverage factor

$\lambda_{DD} = \lambda_D * C_A$

$\lambda_{DU} = \lambda_D * (1 - C_A) * C_M$

$\lambda_{DN} = \lambda_D * (1 - C_A) * (1 - C_M)$

Figure 1: Failure Categories

Modeling system performance

The majority of safety system functions are implemented with non-redundant (simplex) field devices. The following formula can be used to model performance of a non-redundant device. The PFD of the sensor, logic solver and final element are then added to determine performance for the entire function.

$$PFD = (\lambda_{DD} \times (MTTR + (TI_A / 2))) + (\lambda_{DU} \times (TI_M / 2)) + (\lambda_{DN} \times (Life / 2)) + (BD / TI_M)$$

Where: λ_{DD} is the dangerous detected failure rate
MTTR is the Mean Time To Repair
TI_A is the automatic diagnostic test interval
λ_{DU} is the dangerous undetected failure rate
TI_M is the manual test interval
λ_{DN} is the dangerous never-detected failure rate
Life is the proposed life (or mission time) of the hardware
BD is the bypass duration

Base case assumptions and system performance

1. Single smart transmitter with an 80 year $MTTF_D$ ($1/\lambda_D$), 90% diagnostic coverage. (Such a diagnostic coverage factor would be appropriate for either a sensor certified for use in SIL 2, or implementing a standard transmitter using comparison diagnostics with the control system transmitter.)
2. Fault tolerant safety PLC certified for use in SIL 3.
3. Single valve with a 50 year $MTTF_D$ ($1/\lambda_D$), weekly partial stroke testing claiming 80% diagnostic coverage.
4. Yearly manual testing that is 100% effective.
5. No bypassing (i.e., the function is tested when the process is not operating).

The RRF (1/PFD) of this function would be 350, which is in the middle of the SIL 2 range, as shown in Table 1 (the ranges are logarithmic).

Safety Integrity Level (SIL)	Probability of Failure on Demand (PFD)	Risk Reduction Factor (RRF = 1/PFD)
4	≥ .00001 to < .0001	> 10,000 to ≤ 100,000
3	≥ .0001 to < .001	> 1,000 to ≤ 10,000
2	≥ .001 to < .01	> 100 to ≤ 1,000
1	≥ .01 to < .1	> 10 to ≤ 100

Table 1: Performance Requirements

The fault tolerance tables included in safety standards such as ISA 84 (IEC 61511) indicate standard non-redundant designs will usually be limited to SIL 1 performance. However, it is possible to implement simplex field devices that meet SIL 2 performance. There are many devices now certified for such levels of performance, and the standard does allow and acknowledge this (in clauses 11.4.4. and 11.4.5). The previous calculation would be a verification of such a design.

Bypassing is a serious concern

Users need to implement bypasses for a variety of reasons (e.g., start-up conditions, maintenance, testing, etc.). Bypassing can be done a variety of different ways (e.g., jumper wires, keyswitches, 'forcing' of I/O in a PLC, etc.). Bypassing a device means the function will no longer operate on demand. The amount of time that a device is in bypass can have a significant impact on overall performance, especially for non-redundant devices. (Redundant devices can be bypassed one at a time, often with minimal impact on overall safety.)

The standard states "The length of time the SIS is allowed to be in bypass or degraded condition while the operation of the protected process is being sustained shall be defined." While not specifically stated, the basis of the 'length of time' that is acceptable can be determined by simple calculations

The impact of different intervals up to one month using the formula shown above is shown in Table 2.

Time in bypass	Risk Reduction Factor
0	350
1 hour	340
1 day	180
1 week	45
1 month	13

Table 2: Risk Reduction Factor vs. Time in Bypass for a sample non-redundant function

Bypassing this function for one day decreases performance by approximately 50%, with the function now meeting the low end of SIL 2. Bypassing this function for one week decreases performance by approximately 90%, with the function now no longer meeting SIL 2. Bypass intervals longer than one month prevent the function from even meeting SIL 1 performance. The implication is clear; ***do not leave functions in bypass any longer than absolutely necessary, as the impact on performance is much greater that might be intuitively thought***.

The impact of imperfect manual testing

Assuming no bypassing and now just varying the manual test coverage percentage results in the values shown in Table 3.

Manual Test Coverage	Risk Reduction Factor
100%	350
95%	190
90%	130
80%	82
70%	59

Table 3: Risk Reduction Factor vs. Manual Test Coverage for a sample non-redundant function

In the base case modeled above, the risk reduction factor for this function was 350. Assuming a 15 year life (mission time), if the manual test coverage of the field devices drops to 95%, the risk reduction factor is reduced to 190, a reduction of 46%. If the manual test coverage drops to 90%, the risk reduction factor is reduced to 130, a reduction of 63%. Manual test coverage values much below 90% prevent this sample function from even meeting SIL 2. Assumptions that can potentially vary the final answer by more than a factor of two – and potentially prevent the function from meeting the SIL target – are significant enough to warrant paying attention to.

The need for thorough manual testing

Manual testing needs to be as realistic and thorough as possible or else the intended performance level may not be met. The goal is to have the manual test coverage percentage as close to 100% as possible. While most will accept that manual test coverage is rarely 100% (just as automatic diagnostics can never be 100%, and no redundant system can have 0% common cause), determining an accurate assessment of the manual test coverage percentage is problematic. Estimating the manual test coverage factor can be done using either a FMEDA (failure mode, effects, and diagnostic analysis), or a review of detailed maintenance records. Maintenance records offer the most realistic failure rates, yet are often not of sufficient detail to reveal this level of information. Until such detailed data becomes available, estimating the manual test coverage may remain little more than an intuitive engineering judgement.

The combined impact of both factors

Table 4 shows the combined impact of both factors.

Time in Bypass	Manual Test Coverage	Risk Reduction Factor
0	100%	350
1 hour	95%	190
1 day	90%	77
1 week	80%	20
1 month	70%	< 10

Table 4: Risk Reduction Factor vs. Time in Bypass and Manual Test Coverage for a sample non-redundant function

Author Bio

Paul Gruhn is a Global Process Safety Consultant with Rockwell Automation in Houston, Texas. Paul is an ISA Fellow, a member of the ISA 84 standard committee (on safety instrumented systems), the developer and instructor of ISA courses on safety systems, the author of two ISA textbooks, two chapters in other books, and over two dozen published articles, and the developer of the first commercial safety system software modeling program. Paul has a B.S. degree in Mechanical Engineering from Illinois Institute of Technology, is a licensed Professional Engineer (PE) in Texas, and an ISA 84 Expert.

References

1. “Recurring Causes of Recent Chemical Accidents”, James C. Belke, 2004, U.S. Environmental Protection Agency, Chemical Emergency Preparedness and Prevention Office
2. IEC 61511-1 Ed. 2 “Functional safety – Safety instrumented systems for the process industry sector”, 2012 (Committee Draft)