Analyze Safety Integrity Levels (SIL) Using Fault Trees

ioMosaic Corporation

An ioMosaic Corporation White Paper
R. P. Stickles, H. Ozog, and F. T. Dyke

Summary

Even before the adoption of ISA-S84.01[3] as a national standard, safety instrumented systems (SIS) were used to mitigate the risks of process hazards. With the establishment of the standard, there is now a framework for defining Safety Integrity Levels (SIL) for such systems and the associated reliability requirements. However, the standard does not address the topic of how to determine what SIL category is needed to fill the independent layers of protection (IPL) gap. It assumes (section 4.2.2) that this analysis is performed prior to applying the principles of the standard.

The IPL gap is usually addressed during a Process Hazard Analysis (PHA) or in a separate exercise such as Layer of Protection Analysis (LOPA) or Fault Tree Analysis (FTA). All of these involve some type of risk assessment (typically risk ranking) against established tolerability criteria. Needless to say, the quality of the IPL gap analysis is very critical to the overall risk mitigation benefit and implementation cost.

As part of the IPL gap analysis for existing plants, it is necessary to determine the SIL credit afforded by the current SIS IPLs. During the PHA, the tendency is to err on the conservative side to avoid overstating the credit. By using FTA, it may be possible to incorporate factors such as functional testing, and to allow the proper credit for existing IPLs.

FTA also has application in establishing the SIL credit for the design of new SISs that are required to address recommendations from PHAs or that are associated with new or modified plant projects. FTA is one of the evaluation techniques for which ISA has developed guidelines[4] to be used for determining the SIL for Safety Instrumented Functions (SIF).

Because ANSI/ISA-S84.01 is a performance based standard, it provides the designer some flexibility as to how the required reliability is achieved. Section 6.2.3 of the standard states that the desired SIL shall be met through a combination of fifteen design considerations that include: separation, redundancy, failure rates and failure modes, and functional testing interval to mention a few. Furthermore, Appendix B.15.2 states, “The functional test interval should be selected to achieve the Safety Integrity Level (SIL).”

The use of functional testing to improve the reliability of interlocks and SISs is a well-established concept. Some examples of how functional test intervals can be adjusted to obtain equivalent SIL reliability are presented below. Fault tree analysis can be used to quantify the effect of adopting a certain functional testing interval on system reliability. Coupling this with cost-benefit analysis allows the designer to compare initial hardware cost against the ongoing maintenance expense of the additional functional testing. Furthermore, with voting SISs, FTA can provide insight on how to set the functional testing interval to obtain the required SIL reliability.

SIL Evaluation using FTA

1. SIS Reliability with Different Voting

One use of Fault Tree Analysis is to assess the probability of failure on demand (PFD) of a SIS with different voting options. An illustrative example is presented below.

Analysis assumptions for Field Sensors with 1oo2 (one out of two) and 2oo3 voting:

Base rate for undetected sensor failure is 0.2/yr.

PFD_{an} = 0.2/yr * (1/2)yr = 0.1 for annual testing

PFD_{san} = 0.2/yr * (0.5/2)yr = 0.05 for semi annual testing

Assume common cause (CC) PFD = 0.01

The fault trees shown in Figures 1 and 2 depict the failure analysis for spurious trip rate (STR) and probability of failure on demand for the 1oo2 configuration. Similar trees can be developed for other XooY arrangements. The STR and PFD results for 1oo2 and 2oo3 voting arrangements are summarized in Table 1.

Table 1: Spurious Trip Rate & Probability of Failure on Demand

Voting Arrangement	STR per year	PFD
1oo2 Annual Testing	0.4	0.02
2oo3 Annual Testing	0.06	0.04
2oo3 Semi Annual Testing	0.03	0.02

The 2oo3 voting configuration is superior to 1oo2 for reducing the STR, but the PFD increases for the same function testing frequency, because there are more components in the system that can fail. Reducing the functional-testing interval to 6 months lowers the PFD of the 2oo3 configuration to the same level as 1oo2 with annual testing. Therefore, with voting systems, it may be necessary to reduce the functional-testing interval to achieve the required SIL reliability.

2. Use of Functional Test Interval to Obtain Equivalent SIL

The application of fault tree analysis has been shown effective in establishing the relative frequency of potential incidents associated with base-case and alternative design concepts. The technique has the versatility to handle equipment and control failures along with human errors. Examples of the application of fault tree and reliability analysis for evaluation of safety interlock systems have been reported. [1][2]

Since ISA is a performance based standard, it sets reliability performance requirements, rather than different integrity levels for an interlock based on configuration such as:

Type 1: Fully redundant
Type 2: Redundant final element
Type 3: No Redundancy

However, it may be possible to achieve a required SIL with lower reliability hardware through reduction of the test interval (i.e., more frequent testing). The following example demonstrates the level of analysis that can be applied. The analysis is done on a level interlock consisting of sensors and final elements. The fault tree logic for the Type 3 level interlock employing a level switch is shown in Figure 3 for the configuration shown in Figure 4.

By including mission time in the system failure analysis [(1)], the expected unreliability of various instrumented system configurations can be estimated. The probability that a device fails to function (unreliability) during a mission is approximately:

$$r_u = \lambda t$$

Where:

λ = component failure rate (failures/unit time)

t = mission time

The unreliability of the system connoted by Figure 3 is therefore:

$$r_{u1} = \lambda_A t + \lambda_B t + \lambda_C t + \lambda_D t$$

The unreliability relationships of more redundant configurations can be obtained in a similar manner. Using appropriate component failure rates, the unavailabilities presented in Table 2 were calculated. As Table 2 illustrates, this provides the decision-maker with a good picture of the reliability trade-offs for a given mission (testing interval) duration.

Table 2: Unreliability of Level Interlock Systems with Consideration of Common Cause Failures [(1)]

Mission Time	Mission Time (Hours)	Unavailability Type 3	Unavailability Type 2	Unavailability Type 1
1 shift	8	0.010%	0.007%	0.005%
1 day	24	0.029%	0.020%	0.016%
1 week	168	0.200%	0.140%	0.110%
1 month	720	0.870%	0.610%	0.490%
1 quarter	2,160	2.610%	1.840%	1.490%
6 months	4,320	5.220%	3.690%	3.030%
1 year	8,760	10.580%	7.540%	6.390%
18 months	12,960	15.660%	11.220%	9.780%
2 years	17,520	21.160%	15.270%	13.720%

This information can also be utilized for determining reliability (availability) for different SIS configurations (e.g., Type 1 - fully redundant). For example, these data were used to determine the interlock reliability (1- unavailability) for the three types of level interlock configurations as a function of functional testing interval (Table 3).

Table 3: Reliability of Different Level Interlock Configurations

Configuration Class	Redundancy	Test Interval	Reliability, %	SIL
Type 1	Fully	Monthly Quarterly Annually	99.5 98.5 93.6	2 1 1
Type 2	Final Element	Monthly Quarterly Annually	99.3 97.8 90.9	2 1 1
Type 3	None	Monthly Quarterly Annually	99.1 97.4 89.4	2 1 0

The reliability values account for common mode failures. As seen, there is a trade-off between testing frequency, and the advantage gained by selecting the next higher SIL.

Combining these results with the ISA 84.01 SIL reliability requirements below

Table 4: Combining Results with the ISA 84.01 SIL

Safety Integrity Level	Availability Range, %
1	90-99
2	99-99.9
3	99.9-99.99

allows the designer to take into account cost-benefit considerations between initial capital cost and ongoing maintenance cost. For example, a SIL 1 might be achieved using a Type 3 configuration with monthly function testing or a Type 2 configuration with annual testing. Using the assumptions presented in Table 5, the net present value (NPV) of the ongoing incremental (beyond annual testing) maintenance cost for monthly function testing is $24,000. In this case, if the incremental cost of a SIL 2 SIS is less than that sum, it would be a no-brainer.

Table 5: Cost-Benefit Assumptions

Cost of Funds	7%
Labor Cost (fully loaded)	$40/hr.
Person hours per test	6 hr.
System Life	15 yrs.

Other considerations, such as equipment availability, potential for spurious trips during testing, and uncertainty about future availability of maintenance labor, could also drive the decision towards installing the SIL 2 SIS over the system requiring more testing. The benefit of FTA is that it allows quantification/justification of the tradeoffs and eliminates gut feel and guessing.

This also points out the need to understand what suppliers of SIS hardware have assumed for period functional testing of the system, to achieve the SIL specified. First, this information is needed to ensure that the facility's Mechanical Integrity program is in agreement with the manufacture's basis.

Second, if the recommended testing interval is annually, it may be possible to "upgrade" the SIL by more frequent functional testing, at least for the lower safety integrity level systems.

Because ANSI/ISA 84.01 is a performance based standard, it allows the designer some latitude for achieving the required availability. Fault tree analysis, with or without adjustments to account for mission time, is a useful tool for evaluating different configurations for meeting the SIL required availability targets or the SIL credit for existing safeguards.

References

1. Freeman, R.A., "Reliability of Interlocking Systems," *Process Safety Progress*, Vol. 13, No. 3, July 1994
2. Stickles, R.P, Melhem, G.A., "How Much Safety is Enough?" *Hydrocarbon Processing*, Vol. 77, No. 10, October 1998
3. ISA-84.01-1996, Application of Safety Instrumented Systems for the Process Industries, Instrument Society of America (1996)
4. ISA-TR84.00.02, Part 3: Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques Part 3: Determining the SIL of SIF via Fault Tree Analysis, Instrument Society of America

Figure 1: 1oo2 Voting - STR

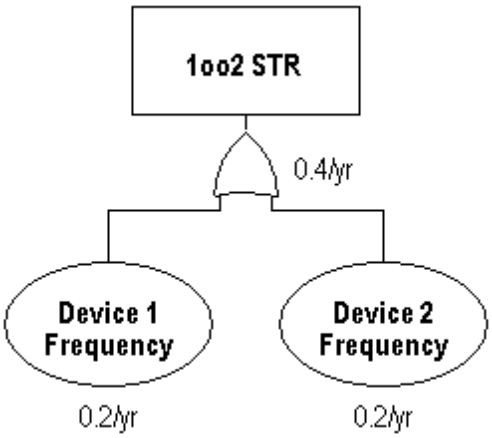


Figure 2: 1oo2 Voting PDF – Annual Testing

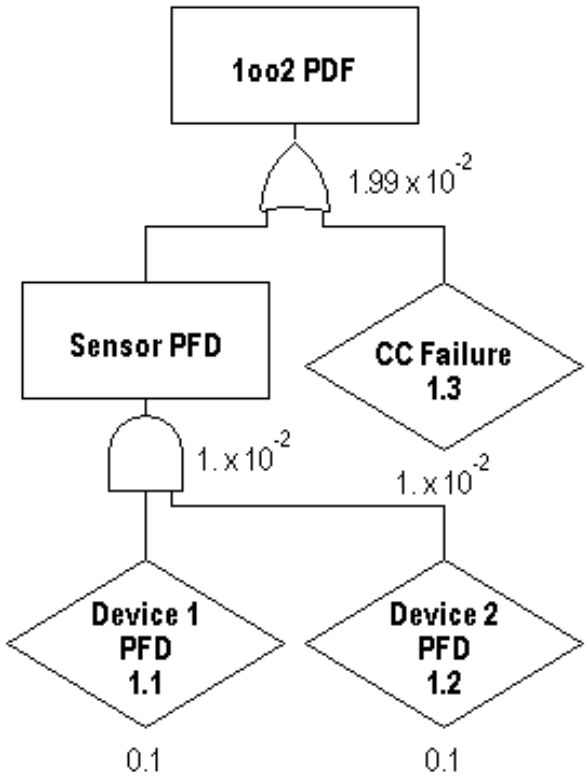


Figure 3: No Redundancy

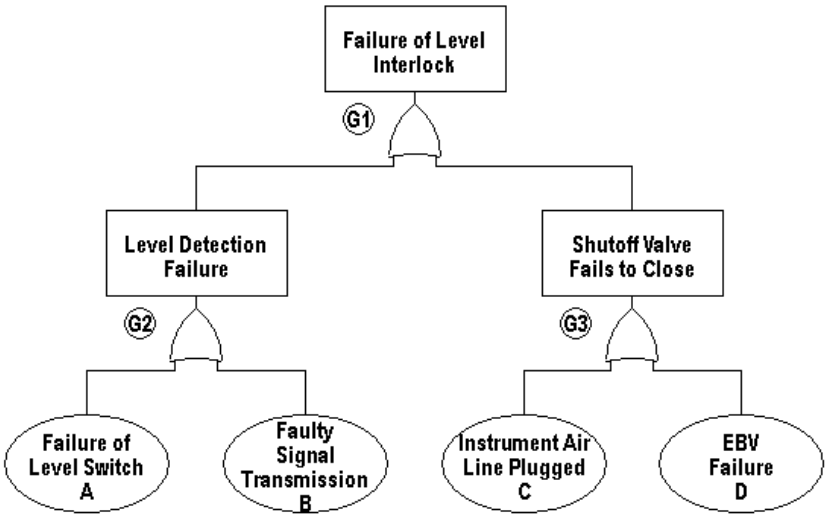
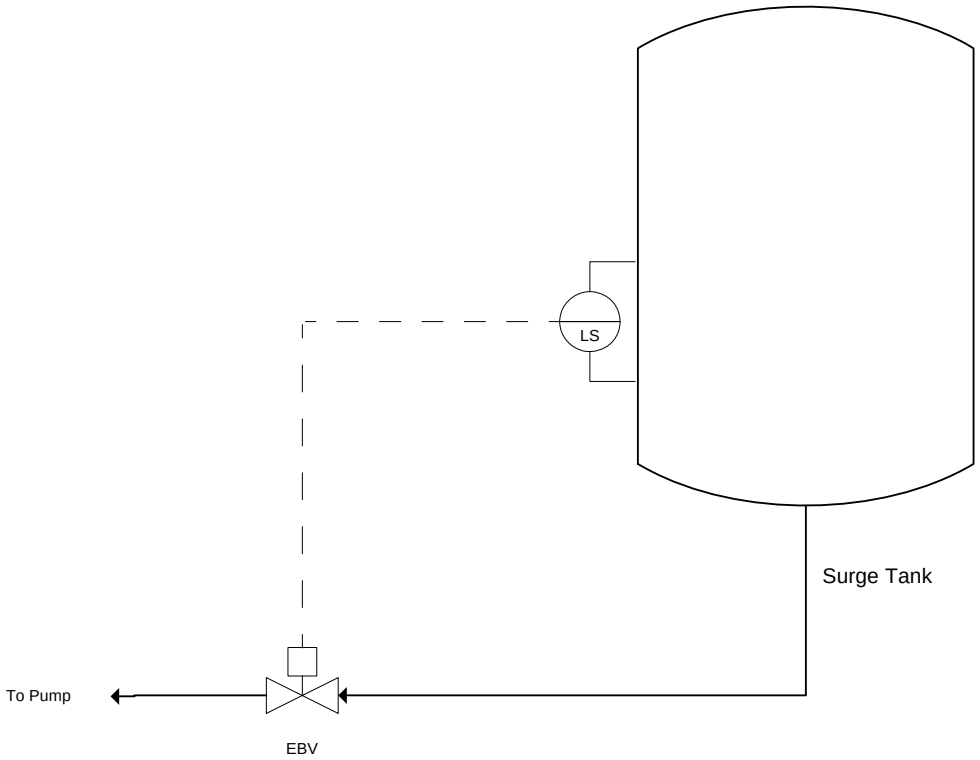


Figure 4: Type 3 Level Interlock



About the Authors

Mr. Stickles is a Partner at ioMosaic Corporation. Prior to joining ioMosaic Corporation, Mr. Stickles worked for Stone and Webster Engineering Corp. for eight years as a process engineer specializing in olefin plant design. He then joined Arthur D. Little, Inc., where he spent 28 years with a variety of responsibilities. He has participated in numerous projects involving hazard and risk assessment of petroleum upstream and downstream operations, petrochemical facilities, pulp and paper mills, primary metals facilities, and energy generation and transmission systems. Earlier in his career at ADL, he conducted many assessments of fuel cell technologies, included a study of fuels and fuel processing options for EPRI.

Mr. Stickles has extensive experience in failure analysis and quantitative risk assessment (QRA) applied to a variety of facilities. He is also a senior Hazard and Operability (HAZOP) study facilitator. He is a training instructor for hazard identification, fault tree analysis, and safeguarding memorandum courses. He has also participated in several major industrial incident investigations, and has provided expert testimony in the area of process safety management.

R. Peter Stickles received his Bachelor of Science in Chemical Engineering and his Master of Science in Engineering from Northeastern University. He is a member of the American Institute of Chemical Engineers, and is a registered Professional Engineer in the Commonwealth of Massachusetts. He was also a member of the National Research Council's Board on Army Science & Technology.

Mr. Ozog is a General Partner at ioMosaic Corporation. Prior to joining ioMosaic, Mr. Ozog was a consultant with Arthur D. Little, Inc. for twenty one years, where he managed the process safety consulting business. He also worked for seven years at the DuPont Company as a process and startup engineer.

Mr. Ozog is an expert in process safety and risk management, process hazard analysis (HAZOP, FMEA, FTA), and process safety auditing. He has helped numerous companies and governmental agencies identify process risks and implement cost effective mitigation measures. He teaches courses in each of these areas and is also an instructor for the American Institute of Chemical Engineers' Educational Services.

Mr. Ozog has a B.S. and M.S. in Chemical Engineering from the Massachusetts Institute of Technology. He is a member of the American Institute of Chemical Engineers and serves on various sub-committees for them.

Mr. Dyke is a Partner at ioMosaic Corporation. Prior to joining ioMosaic Corporation, he was a consultant with Arthur D. Little, Inc. for eleven years. Additionally, Mr. Dyke has twenty-five years of hands-on experience in research and development, pilot plant management engineering design and plant operations. He has worked with both batch and continuous processes manufacturing organic and inorganic chemicals.

Mr. Dyke is an expert in process safety and risk management, process hazards analysis, (HAZOP, FMEA, FTA), relief system design, accident investigation, and litigation support. He has helped numerous clients in the process industries and government agencies solve problems and identify sources of risk and the means to mitigate them. He has taught courses for clients on PHA techniques, and is an instructor for the American Institute of Chemical Engineers' Educational Services Department.

Mr. Dyke has a B.S. and M.S. in Chemical Engineering from Northeastern University. He is a member of the American Institute of Chemical Engineers.

ioMosaic Salem
Corporate Headquarters
93 Stiles Road
Salem, NH 03079

Tel: 603-893-7009
Fax: 603-251-8384

ioMosaic Houston
2401 Fountain View Drive
Suite 850
Houston, TX 77057

Tel: 713-490-5220
Fax: 832-533-7283

ioMosaic Minneapolis
401 North 3rd Street
Suite 410
Minneapolis, MN 55401

Tel: 612-338-1669
Fax: 832-533-7283