Second Annual Symposium, Mary Kay O'Connor Process Safety Center
"Beyond Regulatory Compliance: Making Safety Second Nature"
Reed Arena, Texas A&M University, College Station, Texas
October 30-31, 2001

Expanding the Applicability of ISA TR84.02 in the Field

Lawrence Beckman
HIMA-Americas, Inc.
10801 Hammerly, Suite 130
Houston TX 77043

Phone: (713) 464-3277
Email: hima.americas@pdq.net

ABSTRACT

ANSI/ISA S84.01 standard was released in 1996. The companion Technical Report TR84.02 is in the process of being completed. The latter document is intended to provide the methodology to implement the safety performance requirements of the standard for the safety system. In this document three (3) techniques are presented; these being Simplified Equations, Fault Tree Analysis and Markov Modeling. Of the three, only the Simplified Equations approach would reasonably be utilized in the field by plant personnel.

The Simplified Equations provided in Part 2 of ISA TR84.02 comprehend common cause failures, systematic failures, and second failure prior to repair scenarios. They do not however comprehend the use of redundant field devices which are dissimilar, and as such have different failure rates. This situation is quite common in practice, and simple to manage using enhanced equations for the computation of PFDavg. A set of these equations for typical redundant architectures in the field, and several examples of their applications in safety loop analysis are derived and presented in this paper

EXPANDING THE APPLICABILITY OF ISA TR84.02 IN THE FIELD

Dr. Lawrence Beckman
HIMA-Americas, Inc.
10801 Hammerly, Suite 130
Houston, TX 77043
(713) 464-3277

Abstract

The ANSI/ISA S84.01 standard was released in 1996. The companion Technical Report TR84.02 is in the process of being completed. The latter document is intended to provide the methodology to implement the safety performance requirements of the standard for the safety system. In this document three (3) techniques are presented; these being Simplified Equations, Fault Tree Analysis and Markov Modeling. Of the three, only the Simplified Equations approach would reasonably be utilized in the field by plant personnel.

The Simplified Equations provided in Part 2 of ISA TR84.02 comprehend common cause failures, systematic failures, and second failure prior to repair scenarios. They do not however comprehend the use of redundant field devices which are dissimilar, and as such have different failure rates. This situation is quite common in practice, and simple to manage using enhanced equations for the computation of PFD_{avg}. A set of these equations for typical redundant architectures in the field, and several examples of their applications in safety loop analysis are derived and presented in this paper.

EXPANDING THE APPLICABILITY OF ISA TR84.02 IN THE FIELD

Dr. Lawrence Beckman
HIMA-Americas, Inc.
Houston, TX

Introduction

In 1996 the ISA S84.01 committee finalized and approved a standard addressing the implementation of process safety system. This standard is performance based and clearly defines safety performance criteria based on Safety Integrity Level (SIL) requirements. The standard was subsequently accepted by ANSI and is now referred to as ANSI/ISA S84.01 - 1996.[1]

To date, ANSI/ISA S84.01-1996 has become the consensus standard for process safety in the USA, and is deemed to meet the "good engineering practice" provisions of the OSHA 1910.119 PSM regulation. However, in the field there is a considerable lack of understanding of how to apply this standard to both determine and achieve the required SIL for the safety instrumented system (SIS). A companion Technical Report, TR84.02[2], is intended to alleviate part of this confusion by providing the methodology to implement the safety performance requirements of the standard for the SIS. This would necessarily include both the PES and the field devices for each safety loop. As such, given an SIL for a process safety loop, one should be able to determine the configuration of the PES, and the redundancy of associated field devices necessary to achieve this required SIL based on specified failure rate data, proof test interval, etc.

Ideally, this is the objective. Practically speaking, it is not easily accomplished in the field. This is for the most part due to the complexity of several techniques presented in the TR84.02 document. The three (3) techniques contained in this document are Simplified Equations, Fault Tree Analysis and Markov Modeling. Of these, only the Simplified Equations technique would reasonably be utilized in the field by plant personnel – it fits most common SIS configurations, and has no SIL restrictions. Given that most of this analysis will be performed in the field (and not by consultants), it is imperative to provide a comprehensive set of Simplified Equations, which include common cause failures, systematic failures, and second failure prior to repair scenarios. The present set of Simplified Equations (obtained from simplified Markov Models) do indeed comprehend all of the above.

Introduction - Contd.

However, they do not comprehend the use of redundant field devices which are dissimilar, and as such have different failure rates; i.e., two different valves in a 1oo2 arrangement. The use of diverse redundant components is quite common in practice, and simple to manage using a set of enhanced equations for the computation of PFD_{avg}. It is the purpose of this paper to derive and provide these enhanced equations, and several examples of their application in process safety loop analysis.

Safety Loop Analysis

A safety loop consists of an independent set of sensors, logic solver resources and final elements necessary to implement a specific safety function. The required performance of a safety loop is defined in terms of its SIL, which is in turn defined by its average Probability of Failure on Demand (PFD_{avg}) over a given time period, typically the Proof Test Interval (TI). The Proof Test Interval is selected because it is the time between function testing of the system. Readers unfamiliar with applying probability theory to determine safety system performance are directed to several references on the subject [3] [4]. The ANSI/ISA S84.01 standard requires that the PFD_{avg} (not an instantaneous PFD value) be used to make this determination. As such, one would calculate PFD_{avg} as follows:

$$PFD_{avg} = \frac{1}{TI} \int_{o}^{TI} P_f(t)\, dt$$

where $P_f(t)$ = Probability of failure (to function). The specific functionality of $P_f(t)$ is an attribute of the architecture selected.

Please note that use of any alternative technique which does not compute the PFD_{avg} over the proof test interval, does not comply with the criterion established in the ANSI/ISA S84.01 standard. Exceptions (i.e., PFD_{inst}, or an approximation of PFD_{avg}) are not allowed. The PFD_{avg} requirement applies to both the PES and associated field devices as well. As such, the testing frequency must be the same for all devices (diverse or identical) used in a

Safety Loop Analysis - Contd.

redundant configuration, given that one is computing the PFD_{avg} value for this configuration as a set. However, testing of individual devices in a redundant configuration can be staggered (not performed at the same time).

Given the above defining equation for PFD_{avg}, I will proceed to derive enhanced Simplified equations for the various redundant architectures having diverse redundant components. For a 1oo2 configuration, given that both failures are independent (common cause failure is not comprehended in this analysis),

$$P_f(t) = P_1(t) \bullet P_2(t)$$

where $P_1(t)$ = Probability of Failure (to function) of Component 1.
$P_2(t)$ = Probability of Failure (to function) of Component 2.

As such,

$$P_f(t) = (1 - R_1(t)) \bullet (1 - R_2(t))$$

$$= (1 - e^{-\lambda_1 t}) \bullet (1 - e^{-\lambda_2 t})$$

$$= 1 - e^{-\lambda_1 t} - e^{-\lambda_2 t} + e^{-(\lambda_1 + \lambda_2) t}$$

where λ_1 & λ_2 are the component (dangerous) failure rates.

$$PFD_{avg}(1oo2) = \frac{1}{TI} \int_0^{TI} P_f(t)\, dt$$

$$= \frac{1}{TI}[t]_0^{TI} - \frac{1}{TI}\left[\frac{e^{-\lambda_1 t}}{-\lambda_1}\right]_0^{TI}$$

$$- \frac{1}{TI}\left[\frac{e^{-\lambda_2 t}}{-\lambda_2}\right]_0^{TI}$$

Safety Loop Analysis - Contd.

$$+ \frac{1}{TI}\left[\frac{e^{-(\lambda_1+\lambda_2)t}}{-(\lambda_1+\lambda_2)}\right]_0^{TI}$$

$$= \frac{1}{TI}[TI] - \frac{1}{TI}\left[\frac{e^{-\lambda_1 TI}}{-\lambda_1} - \frac{1}{-\lambda_1}\right]$$

$$- \frac{1}{TI}\left[\frac{e^{-\lambda_2 TI}}{-\lambda_2} - \frac{1}{-\lambda_2}\right]$$

$$+ \frac{1}{TI}\left[\frac{e^{-(\lambda_1+\lambda_2)TI}}{-(\lambda_1+\lambda_2)} - \frac{1}{-(\lambda_1+\lambda_2)}\right]$$

$$= 1 + \left[\frac{e^{-\lambda_1 TI}-1}{\lambda_1 TI}\right] + \left[\frac{e^{-\lambda_2 TI}-1}{\lambda_2 TI}\right]$$

$$- \left[\frac{e^{-(\lambda_1+\lambda_2)TI}-1}{(\lambda_1+\lambda_2)TI}\right]$$

Approximating $e^{-\lambda T}$ using a Maclaurin series expansion, one obtains

$$e^{-\lambda TI} = 1 - \lambda TI + \frac{\lambda^2 TI^2}{2} - \frac{\lambda^3 TI^3}{6} \quad ; \quad \text{where } \lambda TI < 0.6$$

Substituting into the above equation and simplifying, one obtains

$$PFD_{avg}(1oo2) = 1 + \left(-1 + \frac{\lambda_1 TI}{2} - \frac{\lambda_1^2 TI^2}{6}\right)$$

$$+ \left(-1 + \frac{\lambda_2 TI}{2} - \frac{\lambda_2 TI^2}{6}\right)$$

$$- \left(-1 + \frac{(\lambda_1+\lambda_2)TI}{2} - \frac{(\lambda_1+\lambda_2)^2 TI^2}{6}\right)$$

Safety Loop Analysis - Contd.

$$= \frac{2\,\lambda_1\,\lambda_2\,TI^2}{6} = \frac{\lambda_1\,\lambda_2\,TI^2}{3}$$

For the 2oo2 configuration, given that either component can fail dangerously, one must add the failure probabilities as follows,

$$P_f(t) = P_1(t) + P_2(t)$$

$$= (1 - R_1(t)) + (1 - R_2(t))$$

After integration and simplification, one obtains

$$PFD_{avg}\ (2oo2) = (\lambda_1 + \lambda_2)\ \frac{TI}{2}$$

The equation for the 2oo3 configuration can be derived from the 1oo2 equation as follows:

$$PFD_{avg}\ (2oo3) = \frac{\lambda_1\,\lambda_2\,TI^2}{3} + \frac{\lambda_1\,\lambda_3\,TI^2}{3} + \frac{\lambda_2\,\lambda_3\,TI^2}{3}$$

$$= \frac{TI^2}{3}(\lambda_1\,\lambda_2 + \lambda_1\,\lambda_3 + \lambda_2\,\lambda_3)$$

where λ_3 is the (dangerous) failure rate of the third component.

The equation for the 1oo3 configuration can be derived in a manner similar to the 1oo2 equation given that

$$P_f(t) = P_1(t) \bullet P_2(t) \bullet P_3(t)$$

where $P_3(t)$ = Probability of Failure (to function) of Component 3

Safety Loop Analysis - Contd.

$$= 1 - R_3(t) = 1 - e^{-\lambda_3 t}$$

After integration and simplification, the resulting equation is

$$PFD_{avg}(1oo3) = \frac{\lambda_1 \lambda_2 \lambda_3 TI^3}{4}$$

And the equation for the 2oo4 configuration can be derived from the 1oo3 equation as follows:

$$PFD_{avg}(2oo4) = \frac{\lambda_1 \lambda_2 \lambda_3 TI^3}{4} + \frac{\lambda_1 \lambda_2 \lambda_4 TI^3}{4} + \frac{\lambda_1 \lambda_3 \lambda_4 TI^3}{4} + \frac{\lambda_2 \lambda_3 \lambda_4 TI^3}{4}$$

$$= \frac{TI^3}{4}(\lambda_1 \lambda_2 \lambda_3 + \lambda_1 \lambda_2 \lambda_4 + \lambda_1 \lambda_3 \lambda_4 + \lambda_2 \lambda_3 \lambda_4)$$

Given identical components such that $\lambda_1 = \lambda_2 = \lambda_3 = \lambda_4$, each of the preceding equations can be simplified to the form presented in the ISA TR84.02 Technical Report, Part 2.

Application Examples

A typical situation would be the use of two different shutdown valves (SOVs) in a 1oo2 configuration. Assuming the following data values, compute the PFD_{avg} for a one (1) year proof test interval as follows,

Valve 1	:	MTTFd = 30 yrs.; $\lambda_1^d = 0.0333$
Valve 2	:	MTTFd = 50 yrs.; $\lambda_2^d = 0.020$
Solenoid	:	MTTFd = 40 yrs.; $\lambda_s^d = 0.025$

Application Examples - Contd.

For each pair, the combined failure rate is

$$\lambda_1^{\subset} = \lambda_1^{d} + \lambda_s^{d} = 0.0583$$

$$\lambda_2^{\subset} = \lambda_2^{d} + \lambda_s^{d} = 0.045$$

$$PFD_{avg}\,(1oo2) = \frac{\lambda_1^{\subset}\ \lambda_2^{\subset}\ TI^2}{3}$$

$$= \frac{(0.0583)\,(0.045)\,(1)^2}{3} = 0.0009 = 9 \times 10^{-4}$$

Another example would be the use of diverse sensors in a 2oo3 configuration. Assuming the following data values, compute the PFD_{avg} for a one (1) year proof test interval as follows,

Sensor 1 : MTTFd = 60 yrs.; $\lambda_1^d = 0.0167$
Sensor 2 : MTTFd = 40 yrs.; $\lambda_2^d = 0.025$
Sensor 3 : MTTFd = 50 yrs.; $\lambda_3^d = 0.020$

$$PFD_{avg}\,(2oo3) = \frac{TI^2\ (\lambda_1^d\ \lambda_2^d + \lambda_1^d\ \lambda_3^d + \lambda_2^d\ \lambda_3^d\ )}{3}$$

$$= \frac{(1)^2\ [\ (0.0167)\,(0.025) + (0.0167)\,(0.020)}{3} + (0.025)\,(0.020)]$$

$$= \frac{0.0004 + 0.0003 + 0.0005}{3}$$

$$= \frac{0.0012}{3} = 0.0004 = 4 \times 10^{-4}$$

Application Examples - Contd.

Assuming a PFD_{avg} value for the PES of 0.0005 (SIL 3), the PFD_{avg} for the safety loop would be the sum of the three independent elements (sensors, PES, and final elements),

$$PFD_{avg}\,(\text{Loop}) = \underset{(22\%)}{0.0004} + \underset{(28\%)}{0.0005} + \underset{(50\%)}{0.0009}$$

$$= 0.0018 = 1.8 \times 10^{-3}\ (\text{SIL2})$$

It is interesting to note that field devices (sensors and final elements) contribute about seventy two (72%) percent to the overall PFD_{avg} of the safety loop. Only a small percentage is directly attributable to the PES. This conclusion is consistent with experience in actual field installations.

Summary

The set of enhanced Simplified equations presented above should allow this technique to be applied to more complex safety loop configurations, and expand the utilization of the ISA TR84.02 Technical Report in the field by plant personnel.

No attempt has been made to modify the other terms in the Simplified equations (which reflect common cause failure, systematic failure, and second failure prior to repair scenarios) to comprehend the use of dissimilar (diverse) redundant field devices. This can easily be accomplished by making the appropriate substitutions in the respective equations as follows:

In the 1oo2 equation, compute failure rates as

$$\lambda = \sqrt{\lambda_1 \lambda_2}$$

Summary (Contd.)

In the 2oo2 equation, compute failure rates as

$$\lambda = \frac{(\lambda_1 + \lambda_2)}{2}$$

In the 1oo3 and 2oo3 equations, compute failure rates as

$$\lambda = \sqrt[3]{\lambda_1 \lambda_2 \lambda_3}$$

In the 2oo4 equation, compute failure rates as

$$\lambda = \sqrt[4]{\lambda_1 \lambda_2 \lambda_3 \lambda_4}$$

This would apply to all terms containing dangerous failure rates (i.e., λ^{DD}, λ^{DU}, etc.) in these equations as provided in the ISA TR84.02 Technical Report, Part 2.

References

1. ANSI/ISA-S84.01-1996 "Application of Safety Instrumented Systems for the Process Industries", Instrument Society of America S84.01 Standard, Research Triangle Park, NC 27709, February 1996.

2. ISA-TR84.0.02, Part 1: Introduction; Part 2: Simplified Equations; Part 3: FTA; Part 4: Markov; Part 5: Markov Logic Solver, "Safety Instrumented Systems (SIS) - Safety Integrity Level (SIL) Evaluation Techniques", Instrument Society of America TR84.0.02 Technical Report, Research Triangle Park, NC, 27709.

3. "Control System Safety Evaluation &Reliability", William M. Goble, 2nd. Edition, Instrument Society of America, Research Triangle Park, NC 27709, 1998.

References (Contd.)

4. "Probalistic Risk Assessment", Ernest J. Henley and Kiromitsu Kumamoto, IEEE Press, New York, New York, 1992.

Glossary

MTTFd	Mean Time To Dangerous Failure (Time)
P	Probability of Failure (1-R)
PES	Programmable Electronic System (not a PLC-Programmable Logic Controller)
PFD_{avg}	Average Probability of Failure on Demand over the Proof Test Interval
PFD_{inst}	Instantaneous Probability of Failure (at any given point in time)
R	Reliability (Probability of Successful Operation)
SIL	Safety Integrity Level (1, 2 or 3)
SIS	Safety Instrumented System
t	Time
TI	Proof Test Interval (Time)
λ	Dangerous Failure Rate (Failures per Unit Time)