Accurate Modeling of Shared Components in High Reliability Applications

White Paper
exida
80 N. Main St.
Sellersville, PA
www.exida.com

exida White Paper Library
http://www.exida.com/Resources/Whitepapers

Abstract

This paper addresses how to model and evaluate the risk reduction factor (RRF) of safety instrumented systems (SIS) when one or more of the components in the SIS can cause the dangerous condition or hazard that the SIS is designed to protect against. Generally a failure that can cause a hazard is referred to as an initiating event (IE). International standards for SIS safety evaluation require that shared components either be prohibited or accurately modeled. Current practice generally falls into one of two extremes, ignoring any degradation of system reliability due to shared components or completely discounting any improvements in reliability as a result of redundancy created by the shared component.

This paper shows how to accurately model shared components in an SIS and proposes a methodology for simplified modeling techniques when certain criteria are met. Ignoring the interaction of shared components can result in estimates of reliability being optimistic by a factor of 2 or more. Conversely, taking no credit for the redundancy created by the shared component results in estimates of reliability that can be overly pessimistic. Several examples modeling shared components with varying degrees of independence illustrate the impact on overall system reliability.

Introduction

The ideas developed in this paper are most easily understood if the reader can refer to a concrete example of a process and the SIS that is protecting it. To that end, we introduce the steam turbine system and its associated SIS depicted in Figure 1. The basic process itself consists of the steam turbine and the basic process control system (BPCS) which includes the shaft speed sensor (BPCS SEN), a logic solver (BCPS L/S) which determines (based on shaft speed) how to adjust the amount of steam flowing into the turbine, a valve positioner (BPCS POS) to provide input to the actuator-control valve combination (BPCS A/CV), and BPCS A/CV itself which directly controls the steam flow into the turbine.

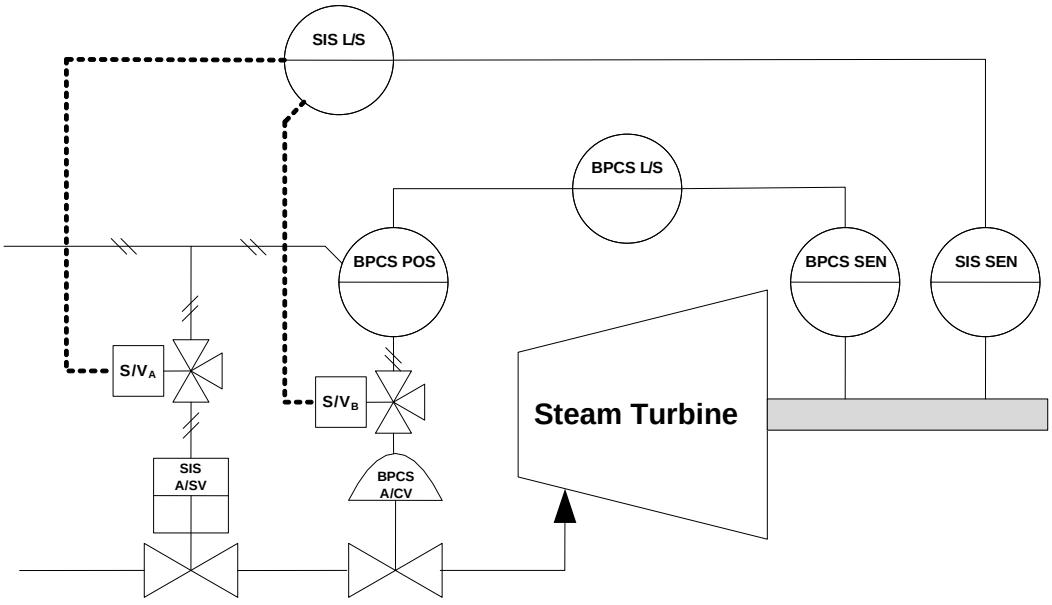

Figure 1 – Steam Turbine Instrumentation

If any component in the BPSC fails in such a way that too much steam is admitted to the turbine this can result in a hazard. In our example the turbine speed can exceed safe mechanical limits leading to serious damage to or destruction of the turbine and possible personnel injury. A failure of the BPCS can be caused by a random failure of the BPCS SEN, BPCS L/S, BPCS POS, or BPCS A/CV. The BPCS could also fail due to a systematic failure such as an operator error or configuration error. The functional safety standards stipulate that the failure frequency for a BPCS be set at a minimum of 0.1 failures per year unless a detailed analysis is performed to justify a lower failure value. If the hazard frequency (HF) is considered unacceptably high, an SIS is added to the system.

In Figure 1, we wish to consider two different versions of the SIS denoted SIS_{IND} and SIS_{SHARED}. SIS_{IND} consists only of a shaft speed sensor (SIS SEN), a logic solver (SIS L/S), a solenoid valve (SIS S/V_A) and the SIS actuator-safety valve combination (SIS A/SV). SIS_{SHARED} consists of all the components of SIS_{IND} plus the solenoid valve, SIS S/V_B, between the BPCS POS and the BPCS A/CV, and the BPCS A/CV. In SIS_{SHARED} the shared component is the BPCS A/CV.

Focus first on SIS_{IND}, i.e., imagine for the moment that in Figure 1 SIS S/V_B does not exist. In this case, if the BPCS fails, it can create the hazard described above which requires SIS_{IND} to act and, if SIS_{IND} is properly functioning, SIS_{IND} can shut down the steam turbine by de-energizing SIS S/V_A which in turn closes SIS A/SV depriving the steam turbine of steam input. In the configuration described, SIS_{IND} is a 1oo1 architecture in that there is no redundancy and all of the components of the SIS must be functioning properly for the SIS to perform its safety function. SIS_{IND} is also clearly completely independent of any failure of the BPCS, i.e., SIS_{IND} is independent of any events that can create the hazard.

Now of all of the components in SIS_{IND}, the one most likely to fail is SIS A/SV. Clearly, the safety performance of the SIS_{IND} could be improved by duplicating the SIS S/V_A *and* the SIS A/SV. However, while the cost of an additional solenoid valve is minimal, the cost of an additional SIS A/SV is significant. Thus a compromise approach is to create SIS_{SHARED} by adding only a solenoid valve, SIS S/V_B, at minimal cost and connecting it to BPCS A/CV as shown in the complete version of Figure 1. Thus, BPCS A/CV is a component shared between the BPCS and SIS_{SHARED}. Now if the BPCS fails and the failure is *not* due to BPCS A/CV, then SIS_{SHARED} acts like a 1oo2 architecture at least with respect to the two actuators and two valves. If however, the BPCS fails due to a failure of BPCS A/CV, then SIS_{SHARED} behaves like the 1oo1 architecture described as SIS_{IND}. This latter case is of special significance because the failure of the shared component is the IE which simultaneously alters the SIS architecture to one of lesser safety performance.

Although we have presented only one specific example of an SIS with a component shared with a BPCS, it is very relevant. The most commonly encountered application where there would be significant benefit to claiming credit for a shared component whose failure could be an IE is when a control valve is used in series with a safety valve.

The most often referenced standard for the design and implementation of SIS is IEC 61508 [1] and when SIS are deployed in the process industries the applicable standard is IEC 61511 (equivalent to ANSI/ISA84.00.01-2004 [2]). Both IEC 61508 and IEC 61511 require that SIS be completely independent from any IE that places a demand on the SIS or from other protective functions *unless the interrelation is properly accounted for*. To date there is no consensus as to the appropriate methodology to account for the interactions. The two extreme approaches, currently used in industry, are to completely ignore any interaction between the SIS and the BPCS, i.e., to analyze the SIS_{SHARED} assuming the BPCS A/CV cannot be an IE resulting in an optimistic reliability model, or to absolutely forbid any sharing leading to more complex and expensive solutions.

In this paper we review the current methods employed to determine the effectiveness of protective functions when one or more of the components in the SIS can be the IE. In order to properly model this type of system it is necessary to understand the failure modes of the component in question as well as its behavior in fault conditions. We decompose complex systems and model their behavior utilizing Markov models to generate accurate failure frequencies for applications with shared components. New methods are discussed and a recommendation is made as to the most appropriate way to model these systems.

Notation

BPCS	Basic Process Control System
BPCS A/CV	BPCS Actuator and Control Valve
BPCS L/S	BPCS Logic Solver
BPCS POS	BPCS Valve Positioner
BPCS SEN	BPCS Sensor
FITS	Failures per 10^9 hours
FMEA	Failure Modes and Effects Analysis
HF	Hazard Frequency
IE	Initiating Event(s)
PFD_{AVG}	Average Probability of Failure on Demand
RRF	Risk Reduction Factor
SIS	Safety Instrumented System(s)
SIS A/SV	SIS Actuator and Safety Valve
SIS L/S	SIS Logic Solver
SIS SEN	SIS Sensor
SIS S/V	SIS Solenoid Valve
λ_i	constant failure rate of component i where i is an abbreviation stipulated above

Assessing Safety Instrumented System Performance

It is usual to assess SIS safety performance by calculating its RRF. In simple systems with only one failure path the RRF is the reciprocal of the average probability of failure on demand (PFD_{AVG}). PFD_{AVG} is a function of equipment selection, redundancy, and testing [3]. RRF can also be expressed as the ratio of unmitigated hazard frequency (HF) to residual HF. In our case the RRF is the frequency that the turbine would overspeed without an SIS divided by the frequency with which the hazard would occur with an SIS.

$$RRF = \frac{HF(\text{without SIS})}{HF(\text{with SIS})} \quad (1)$$

As previously discussed, the functional safety standards set the failure frequency of a BPCS at 0.1 failures per year. If the failure of the BPCS is the only thing that could cause the hazard then the IE would be 0.1/year. There are often other failures that could lead to a hazard such as load rejection from the grid in our example. The frequency of these other IE is added to the IE of the BPCS to determine the aggregate IE frequency for a given hazardous condition. We present examples with total IE ranging from 0.1 to 0.5.

The RRF we compute will depend on how we model the SIS as this will affect the computation of PFD_{AVG}.

Next we consider two different SIS models currently used to calculate PFD_{AVG} and hence RRF.

Current Methodologies for Evaluating RRF

Method 1 – Take no credit for valve redundancy

Some process industries practitioners disallow any sharing of components between general process loops and SIS. This approach is consistent with the standards and results in the most conservation calculation of RRF. Thus, even though many will configure the SIS as shown in Figure 1 (and this is a good practice as it improves safety), they take no credit in the reliability analysis for any improvements in safety. Succinctly put, they configure the SIS as SIS_{SHARED} (a partially redundant SIS as portrayed in Figure 1) but model the SIS as SIS_{IND} (a 1oo1 architecture) for the purposes of computing RRF. Figure 2 shows only the instrumentation associated with the SIS and identifies the boundaries for both SIS_{IND} and SIS_{SHARED}.

This approach has the benefit of being simple, delivering conservative results, and being easy to defend. The main disadvantage is cost. If the SIS valve architecture does not provide sufficient risk reduction there will be a need to add redundancy or additional testing. When a typical safety valve can cost in excess of $50,000 this simplification can significantly impact project and operational costs.

To determine the RRF for SIS_{IND} its PFD_{AVG} was calculated using a Markov Model that accurately accounted for component failure rates, test intervals and effectiveness, and mission time. Based on a 1 year test interval and a 15 year system life the example SIS_{IND} achieved a PFD_{AVG} of 3.53E-2 or a RRF of ≈ 28. This RRF is independent of any failure rates within the BPCS.

Method 2 – Assume full valve redundancy

The second frequently seen approach is to assume that the impact of sharing a component is negligible. Thus, in this method, the SIS is modeled as if the solenoid and actuator-valve combinations are fully redundant and no consideration is given to the scenario where the failure of the BPCS A/CV would be the IE. This is a potentially dangerous over-simplification but it is commonly used in the process industries. As will be shown in the following examples, the impact of this assumption is to overestimate the risk reduction achieved by the SIS.

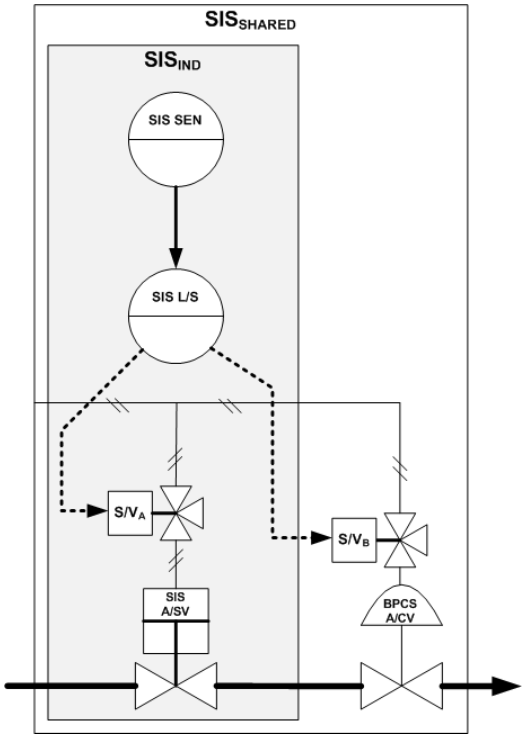

Figure 2 – SIS_{IND} and SIS_{SHARED} Boundaries

To compute an accurate PFD_{AVG} (needed to compute RRF), a system level Markov model was created to represent the actual functioning of the SIS and is shown in Figure 3. In addition to the failure transitions there are also repair transitions that will return the system to the OK state. These have been omitted in the simplified drawing but are accounted for in all computations using this model.

In Figure 3, State 1 represents the situation where all of the components in the SIS including BPCS A/CV are operating correctly. State 2 represents the situation where either the SIS S/V_A or the SIS A/SV or both has failed. State 3 represents the situation where either SIS S/V_B or BPCS A/CV or both has failed. State 4 represents the situation where the SIS is in a state of dangerous failure because there is sufficient component failure to prevent the SIS from taking the process to a safe state in case of an IE.

Now the failure rates, λ_i, for all the SIS components were determined when the Markov Models for Method 1 and Method 2 were completed. Data is available from sources such as the Safety Equipment Reliability Handbook [4]. We have yet to specify the failure rate for BPCS A/CV. To do so, we note that the failure modes of the BPCS need to be determined and documented. Figure 4 shows a fault tree analysis of the BPCS. In the fault tree the control valve assembly is segmented between the valve positioner and the actuator-valve combination. This is due to the fact that if the positioner fails the actuator and valve could still be successful in transitioning to the safe state because of the solenoid, SIS S/V_B, which is installed and controlled by the SIS.

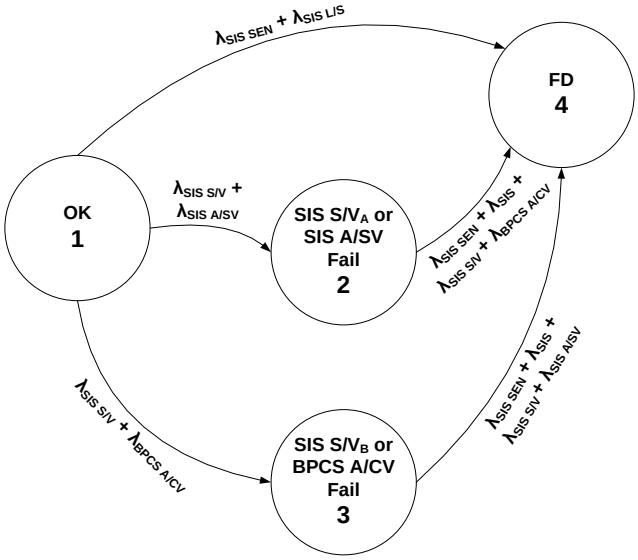

Figure 3 – Simplified Markov Model

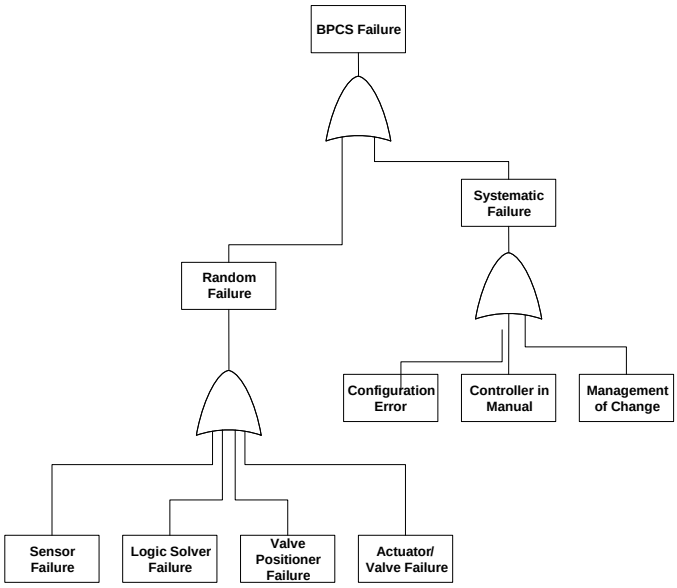

Figure 4 – BPCS Fault Tree

Note that the BPCS failure frequency depends not only on random failures of the BPCS components but also on systematic failures. Based on the review of a large sample of safety interlocks [5], it can be shown that the failure of the BPCS A/CV generally accounts for about 60% of the random failures. We must now determine the breakdown between random and systematic failures.

In research performed by the Health and Safety Executive (HSE) [6], systematic failures were found to be the root cause of 85% of accidents involving automatic protective system. Based on data such as this as well as experience with SIS it is reasonable to allocate some or even the majority of the 0.10 BPCS failure frequency to systematic failures. If the results of the HSE study are used, the allocation would be set at

15% for random failures and 85% for systematic failures.

A 15% budget for random failures would result in a total allotment of 1,710 failures per 10^9 hours (FITS) for the BPCS. (This figure was obtained from a separate analysis not included in this paper.) While some BPCS loops may meet this criteria most probably do not. As the 0.10 failure frequency appears to have been established by more qualitative studies of failures, some latitude can be justified in setting the allocation between random and systematic. Taking as a given that the 0.10 value does a reasonable job of capturing actual failures and looking at typical BPCS random failure rates the argument can be made to set that allocation at a percentage that would accommodate most well designed BPCS loops. Setting the allocation at 25% for random and 75% for systematic results in a total allotment of 2,850 FITS for the BPCS and this meets the criteria laid out above.

Now we can deduce appropriate ranges of values for $\lambda_{BPCSA/CV}$ as follows. The total BPCS IE of 0.1 is divided between random and systematic failures with the random failure percentage between 15% and 25%. So the BPCS IE due to random failures is between 0.015 and 0.025. Attributing 60% of the random failures to BPCS A/CV means $\lambda_{BPCS\ A/CV}$ is between 0.009 and 0.015 failures/year. Even if the random/systematic ratio were set at 50% and 50% respectively, $\lambda_{BPCS\ A/CV}$ would have a maximum value of 0.03 failures/year. Thus, in our calculations we vary $\lambda_{BPCS\ A/CV}$ on the range [0.00, 0.04] failures/year keeping in mind the most probable range is [0.01, 0.03]. Figure 5 shows the risk reduction calculated from both Method 1 and Method 2 over the appropriate range of $\lambda_{BPCS\ A/CV}$. Note the significant, albeit inaccurate, improvement in RRF for Method 2. Figure 5 also includes the calculated RRF for Methods 3 and 4 which are described in the next section.

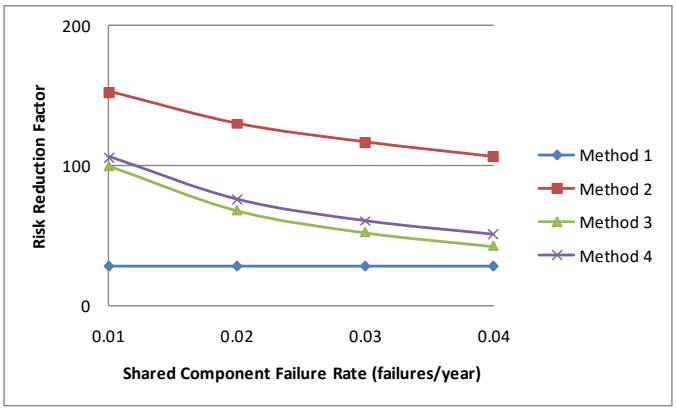

Figure 5 – Risk Reduction Factors, IE = 0.1/year

New Methods for Evaluating RRF in the Presence of Shared Components

Clearly, Methods 1 and 2 represent extremes that are, by their very formulation, either overly pessimistic (Method 1) or overly optimistic (Method 2). But each method does in fact capture one aspect of the total problem. The new methods proposed here, compute RRF (with SIS_{SHARED}) as a weighted average of PFD_{AVG} computed from Methods 1 and 2. The new methods, both of which combine an event tree analysis with detailed Markov models, yield more accurate and realistic results. The two new methods differ only slightly in how they treat the total IE so that one method produces slightly more conservative values for RRF.

Method 3 - Partial valve redundancy, incremental initiating event

The first step is to create an event tree of the scenario in question as shown in Figure 6. Branch 1 (B1) contains the total IE. For failures that are not related to the BPCS A/CV the SIS is modeled with a 1oo2 redundant actuator and valve. The result of B1 is an intermediate event frequency depicting the frequency that the initiating event would propagate past the SIS. Branch 2 (B2) models the failure rate of the BPCS A/CV. The IE for B2 is the BPCS A/CV failure rate. If either or both of those components fail the SIS will not have a redundant actuator and valve and is therefore modeled as a 1oo1 configuration.

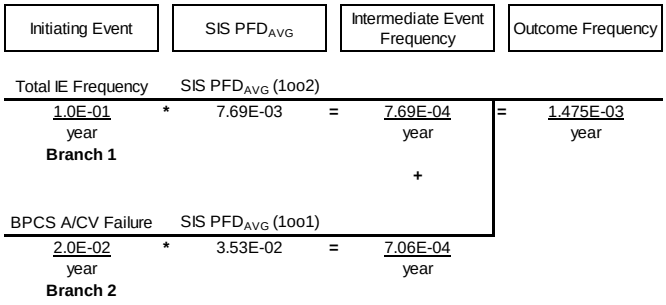

Figure 6 – Shared Component Fault Tree, IE = 0.1/year

The intermediate event frequency of B2 is added to the intermediate event frequency of B1 yielding the total outcome frequency. The RRF is determined by dividing the total outcome frequency by the total IE which is the value used in B1. This model is somewhat conservative in that it treats the failure of the BPCS A/CV as incremental to the total IE.

Method 4 – Partial valve redundancy

An alternative to Method 3 is to subtract the BPCS A/CV failure rate from the IE used in B1. With this approach the sum of B1 and B2 will equal the total IE. Figure 5 shows the results of Method 3 and Method 4 compared to the previous method discussed.

As discussed earlier it is important to set an upper limit to the value that can be claimed for random failures. If the value for random failures is observed to be much more than 0.03 failure per year then the assumption that the IE of 0.1 per year for the entire BPCS should be challenged.

Reviewing the results of the various methods leads us to make the recommendation to utilize Method 3 as the preferred method. Method 3 allows credit to be taken for some degree of redundancy while having the benefit of being slightly conservative in that it increments the total IE by the failure rate of the shared component. Figure 9 shows the deviation from the recommended method (Method 3) when the other methods are utilized.

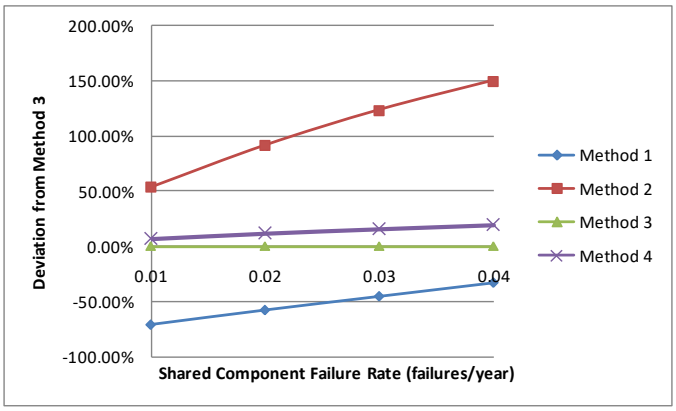

Figure 7 – Deviation from Recommended Method (Method 3), IE = 0.1/year

Sensitivity Analysis

Figures 8, 9, and 10 show the relationship between Deviation from Method 3 and Shared Component Failure Rate for Method 1, 2, and 4 respectively for total IE frequencies from 0.1 to 0.5. The most significant source of error results from the practice of ignoring the interaction of shared components (Method 2). The impact of this assumption diminishes as the failure rate of the shared components decreases as a percentage of the overall IE. Nonetheless in typically encountered applications this error can easily exceed 100% resulting in significant overestimating the effectiveness of the SIS.

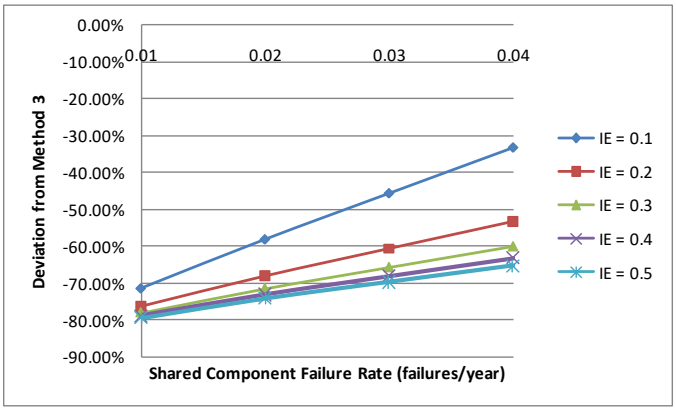

Figure 8 – Method 1 Deviation from Method 3

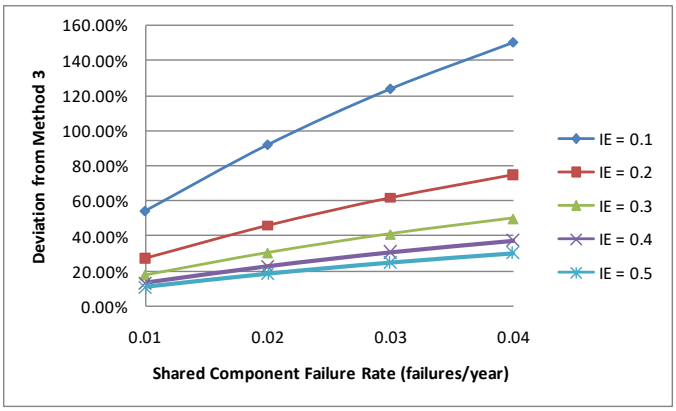

Figure 9 – Method 2 Deviation from Method 3

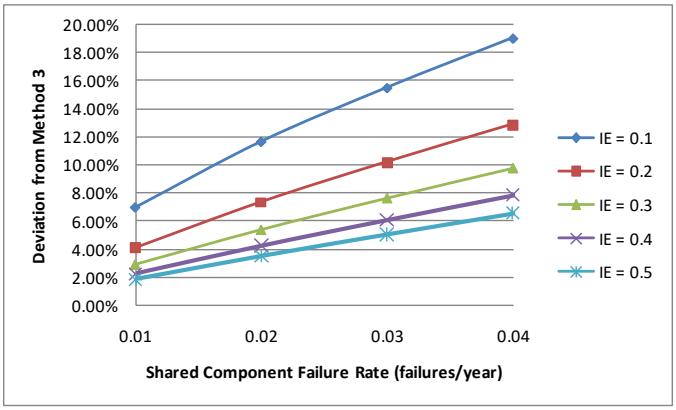

Figure 10 – Method 4 Deviation from Method 3

Recommendations

When dealing with SIS that contain shared components the first step is always to see if there is a practical way to achieve full independence. This may involve adding additional equipment to achieve redundancy or independent paths. While this can be cost prohibitive for valves and actuators it should be considered and is often more reasonable for sensors. If separation is not practical then a quantitative analysis needs to be conducted.

When performing the quantitative analysis it is important to clearly evaluate and document the interdependence between the SIS and the BPCS loop. A fault tree or Failure Modes and Effects Analysis (FMEA) are good techniques for this step. Once the interdependencies are identified the event tree can be constructed.

Utilizing a Markov model tool, solve for the PFD_{AVG} of the SIS with and without taking credit for the shared component. These PFD_{AVG} along with the shared component failure rate are then entered into the event tree and the event tree is solved for outcome frequency. Finally the total RRF is determined by taking the outcome frequency and dividing it by the IE.

References

1. IEC 61508, Functional safety of electrical/electronic/ programmable electronic safety-related systems, Geneva, Switzerland, 2000.
2. ANSI/ISA 84.00.01:2004 (IEC 61511 Mod.), Application of Safety Instrumented Systems for the Process Industries, ISA, Raleigh, NC, USA, 2004.
3. van Beurden, Iwan, “Advanced SIL Verification Techniques,” Proceedings ISA Safety Division Symposium 2008, 24 April 2008, Calgary, AB, Canada.
4. Safety Equipment Reliability Handbook, third edition, 2007, exida.com, LLC, Sellersville, PA, USA
5. O’Brien C., Bredemeyer L., Final Elements and the IEC 61508 and IEC 61511 Functional Safety Standards, 2009, exida.com, LLC, Sellersville, PA, USA
6. Out of Control: Why Control Systems Go Wrong and How to Prevent Failure, U.K: Sheffield, Health and Safety Executive, 1995

Revision History

Authors: Julia V. Bukowski, PhD, Chris O’Brien

exida – Who we are.

exida is one of the world's leading accredited certification and knowledge companies specializing in automation system cybersecurity, safety, and availability. Founded in 2000 by several of the world's top reliability and safety experts, exida is a global company with offices around the world. exida offers training, coaching, project-oriented consulting services, standalone and internet-based safety and cybersecurity engineering tools, detailed product assurance and certification analysis, and a collection of online safety, reliability, and cybersecurity resources. exida maintains a comprehensive failure rate and failure mode database on electrical and mechanical components, as well as automation equipment based on hundreds of field failure data sets representing over 350 billion unit operating hours.

exida Certification is an ANSI (American National Standards Institute) accredited independent certification organization that performs functional safety (IEC 61508 family of standards) and cybersecurity (IEC 62443 family of standards) certification assessments.

exida Engineering provides the users of automation systems with the knowledge to cost-effectively implement automation system cybersecurity, safety, and high availability solutions. The exida team will solve complex issues in the fields of functional safety, cybersecurity, and alarm management, like unique voting arrangement analysis, quantitative consequence analysis, or rare event likelihood analysis, and stands ready to assist when needed.

Training

exida believes that safety, high availability, and cybersecurity are achieved when more people understand the topics. Therefore, exida has developed a successful training suite of online, on-demand, and web-based instructor-led courses and on-site training provided either as part of a project or by standard courses. The course content and subjects range from introductory to advanced. The exida website lists the continuous range of courses offered around the world.

Knowledge Products

exida Innovation has made the process of designing, installing, and maintaining a safety and high availability automation system easier, as well as providing a practical methodology for managing cybersecurity across the entire lifecycle. Years of experience in the industry have allowed a crystallization of the combined knowledge that is converted into useful tools and documents, called knowledge products. Knowledge products include procedures for implementing cybersecurity, the Safety Lifecycle tasks, software tools, and templates for all phases of design.

Tools and Products for End User Support

- exSILentia® – Integrated Safety Lifecycle Tool
    - PHAx™ (Process Hazard Analysis)
    - LOPAx™ (Layer of Protection Analysis)
    - SILAlarm™ (Alarm Management and Rationalization)
    - SILect™ (SIL Selection and Layer of Protection Analysis)

  - Process SRS (PHA based Safety Requirements Specification definition)
  - SILver™ (SIL verification)
  - Design SRS (Conceptual Design based Safety Requirements Specification definition)
  - Cost (Lifecycle Cost Estimator and Cost Benefit Analysis)
  - PTG (Proof Test Generator)
  - SILstat™ (Life Event Recording and Monitoring)
- exSILentia® Cyber- Integrated Cybersecurity Lifecycle Tool
  - CyberPHAx™ (Cybersecurity Vulnerability and Risk Assessment)
  - CyberSL™ (Cyber Security Level Verification)

Tools and Products for Manufacturer Support

- FMEDAx (FMEDA tool including the exida EMCRH database)
- ARCHx (System Analysis tool; Hardware and Software Failure, Dependent Failure, and Cyber Threat Analysis)

For any questions and/or remarks regarding this White Paper or any of the services mentioned, please contact exida:

exida.com LLC

80 N. Main Street

Sellersville, PA, 18960

USA

+1 215 453 1720

+1 215 257 1657 FAX

info@exida.com