SIL-3, SIL-2, and Unicorns
(There Is a High Probability Your SIL 2 and SIL 3 SIFs Have No Better Performance Than SIL 1)

Presenter
A.M. (Art) Dowell, III, PE
Principal Engineer
Process Improvement Institute, Inc.
16430 Locke Haven Dr.,
Houston, TX 77059 USA
adowell@piii.com

Matias Massello
Engineer
Process Improvement Institute, Inc.
Argentina
mmassello@process-improvement-institute.com

William Bridges
President
Process Improvement Institute, Inc.
1321 Waterside Lane,
Knoxville, TN 37922 USA
wbridges@piii.com

Harold W. (Hal) Thomas, PE, CFSE
Specialist
exida.com LLC
80 North Main Street
Sellersville, PA USA
thomashw@exida.com

Prepared for Presentation at
American Institute of Chemical Engineers
2019 Spring Meeting and 15th Global Congress on Process Safety
New Orleans, LA
March 31 – April 3, 2019

SIL-3, SIL-2, and Unicorns
(There Is a High Probability Your SIL 2 and SIL 3 SIFs Have No Better Performance Than SIL 1)

Presenter
A.M. (Art) Dowell, III, PE
Principal Engineer
Process Improvement Institute, Inc.
16430 Locke Haven Dr.,
Houston, TX 77059 USA
adowell@piii.com

William Bridges
President
Process Improvement Institute, Inc.
1321 Waterside Lane,
Knoxville, TN 37922 USA
wbridges@piii.com

Keywords: SIL, SIF, Human Factors, Systematic Error, Human Error

Abstract

Safety Instrumented System (SIS) standards improved the definition of interlocks and introduced requirements for improved management systems to enforce independence from other Independent Protection Layers (IPLs). SIS standards require verification that the performance of each Safety Instrumented Function (SIF) will be met during its lifetime; where the performance criterion is documented as the target Safety Integrity Level (SIL) or risk reduction factor for the SIF. The SIL is in turn tied to specific values of probability of failure on demand (PFD). The current SIS standards and the TR (Technical Reports, from ISA) that explain how to do SIL Verification calculations do not include accounting for specific human error probabilities -- this is a major deficiency as even the probability of a single human error can be much larger than the target PFD of 0.001 for a SIL 3 and oftentimes a little larger than the PFD of 0.01 for a SIL 2. The SIL Verification methods outlined in the standards and technical reports like ANSI/ISA TR84.00.02 facilitate consistency for the component-only failure rates. As user companies seek to obtain greater risk reduction from their SIS to satisfy their corporate risk criteria, failure to adequately address potential specific human failures can lead to overly optimistic results and a misallocation of resources intended to reduce risk

This paper shows that specific human error during testing, calibration maintenance, and restoration of a SIF is a significant contribution to the true PFD of the SIF for SIL 2 and dominates SIL 3 designs. Unless the human errors are accounted for and then compensated for, it is more likely to find a Unicorn than to actually get two or three orders of risk reduction from SIL 2 and SIL 3 SIFs.

Example methods for human error analysis related to a SIS are provided as well as some proven approaches for controlling human factors. The paper also discusses ways to prevent or else to detect and to recover from errors made in redundant channels (such as used in 1oo2, 1oo3, or 2oo3 voting).

1 Introduction

This paper is an update to a prior paper [1]. In the ensuing seven years, the international and USA global standards organizations have issued new guidance, but the issue raised in 2012 remains the same. Although technology and methods exist to evaluate specific human error probabilities, particularly during maintenance and operation of safety instrumented functions (SIFs), the standards continue to categorize all human error in the systematic failures category and ignore specific human errors in the verification calculation of safety integrity level (SIL).

The failure of SIFs can be due to a number of reasons. Common terminology in the industry characterizes these failures as either random hardware failures or systematic failures. This paper mainly focuses on the systematic aspects (which for convenience include specific human errors); however, all equations presented will also include the hardware failure contribution for completeness.

1.1 Systematic Failures versus Specific Errors

Systematic failures may manifest themselves via a number of failure mechanisms such as:

- Manufacturer design errors
- End user design errors
- Hardware installation errors
- Manufacturer software design errors
- End user programmable configuration errors
- Human error during operation and maintenance
- Management of change errors

As the list above shows, systematic error may be introduced by the manufacturer or the end user. This paper will focus on the end user, as equipment that has been properly reviewed and certified in accordance with IEC-61508 [2] undergoes a formal work process specifically looking to minimize systematic errors from the manufacturer. It is also likely that systematic errors that do occur will manifest themselves during the warranty period, allowing appropriate response to rectify the problem to a suitable level. In addition, the performance of each SIF is expected to be validated versus the safety requirements specification (SRS) during the factory acceptance testing and equipment certified in

accordance with IEC 61508 is also expected to undergo proven in use validation by the manufacturer on a periodic basis to confirm the device SIL capability described in the certification. This validation of specific device SIL capability does not mean the performance of a SIF's safety integrity level is validated as that is an end user's responsibility beyond the control of the manufacturer."

Once under the control of the end user, the variability of application and control greatly increases, making control of specific human errors more difficult. This paper seeks to make the reader more aware of how specific human errors may occur and how they can impact the risk reduction of SIFs.

1.2 Human Error in SIF Failures

Human error during interventions with SIS can have a detrimental effect on the availability of one or more SIFs. There have been numerous cases where SIFs were left in bypass, etc., and an accident occurred. One notable event was at a facility in Institute, West Virginia, USA (in 2008). An SIF was bypassed to allow startup to proceed more smoothly. Reactant was allowed into a vessel without solvent and the temperature of the newly replaced residue treater ran away and it exploded, resulting in two fatalities and multiple injuries. In addition, it was also a near miss with respect to a potential large release of methyl isocyanate from a storage tank located just 80 feet from the explosion [3].

The focus of this paper will be on human interaction errors (usually called specific human errors in this paper). These errors include errors in the operation of the man-machine interface to the SIF (such as leaving an SIF in bypass during unit startup), errors during periodic testing of the SIF, and errors during the repair of failed modules in the SIF. This last type of human error includes the simple case of inadvertently leaving a root valve on an instrument closed.

The SIS standards of the mid-1990s through today recognized that human errors have a deleterious impact on the PFD of an SIF. This effect can be either errors that exist at Time Zero or specific human errors while operating (called systematic errors in some SIS literature and standards). The IEC standards qualitatively covered at length the need to control such errors [4], [5]. For example, Clause 3.2.69, Note 3 [5] says, "…However, safety integrity also depends on many systematic factors, which cannot be accurately quantified and are often considered qualitatively throughout the life-cycle…"

In the Technical Report (TR) from the International Society of Automation (ISA) for how to perform SIL verification calculations, ISA-TR84.00.02-2015 [6], Equation 8.1 (shown here as Equation 1) is given to calculate the SIF probability of failure on demand.

$$\boldsymbol{PFD_{SIF} = PFD_S + PFD_{LS} + PFD_{FE} + PFD_{SS}} \qquad \textbf{Equation 1}$$

where,
PFD_{SIF} is the PFD_{avg} for the SIF **Hardware**, actually $PFD_{hardware}$.
PFD_S represents the various sensors used to detect abnormal process conditions,
PFD_{LS} represents the logic solver used to make decisions based on the process conditions,
PFD_{FE} is the final element used to act on the process,

PFD_{SS} represents any required support systems, such as a power supply in ETT.

ISA-TR84.00.02-2002 [7] did include an additional term (shown here as Equation 2) for contribution of "dangerous system failures" in TR Equation 1a. This term was correctly omitted from the 2015 TR since true systematic failures are not random and base random human errors are not subject to improvement by decreased proof test intervals.

$$\boldsymbol{PFD_{SYS} = \left[\lambda_F^D x \frac{T_i}{2}\right]} \qquad \textbf{Equation 2}$$

where,
PFD_{sys} = dangerous systematic failures
λ_F^D = dangerous failure rate, per year
T_i = test interval, year.

However, Equation 1 did NOT include a term for specific human errors related to interventions by the end user.

Also, the 2002 TR does not give any practical guidance as to which systematic and human errors are most significant. While the 2015 TR has a partial list of safe and dangerous systematic errors in Clause 9.1, it also does not provide guidance to determine which systematic and human errors are most significant.

Likewise, IEC 61511-2017 and ANSI/ISA 6511-1-2018 recommend a qualitative approach to control systematic errors, including human errors, by simply stating that the end user must control all human intervention error (easily said, difficult in practice)..

In practice, most of the systematic error term results from specific human errors. These can include:

- Manufacturer contribution for certified equipment (believed to be negligible relative to end user errors)
- End user errors:
    - Design and installation errors
    - Introduction of undetected failures caused by proof testing
    - Bypass during operation

Of these end user errors, the dominating contribution is generally human errors that leave the protection failed at Time 0. These errors can occur during calibrations, proof tests, and re-commissioning of an SIF following routine maintenance interventions such as:

- Miscalibrations
- Leaving a root valve on an instrument closed
- Leaving an SIF in bypass, i.e.:
    - Bypassing the function due to a spurious trip and failing to remove the bypass.
    - Bypassing the function for startup because the system dynamics require it; however, the designers missed this need during startup mode of the process,

resulting in an operational bypass that requires human intervention to remove the bypass rather than an automated design that removes the bypass.
- Bypassing the final element and failing to remove bypass when the test or repair is complete.

Therefore, a simple equation including the human error terms can replace the equations from ISA-TR84.00.02 (-2002 and -2012). The resulting improved equation is shown in Equation 3:

$$\boldsymbol{PFD_{SIF} = PFD_S + PFD_{LS} + PFD_{FE} + PFD_{SS} + PFD_{SYS}} \quad \textbf{Equation 3}$$

We expand the PFD_{sys} using Equation 4.

$$\boldsymbol{PFD_{SYSi} = PFD_{SYS-PROCi} + P_{HUMi}} \quad \textbf{Equation 4}$$

where,
PFD_{SYSi} = the systematic PFD of the i[th] part of the SIF,
$PFD_{SYS\text{-}PROCi}$ = the systematic errors and failures generated randomly by the process for the i[th] part of the SIF (such as plugging of instrument taps by process materials or contaminants),
P_{HUMi} = the probability of dangerous human error from the i^{th} part of the SIF

(Note that $PFD_{SYS\text{-}PROCi}$ can be modeled as a hardware failure rate and a good inspection and testing program should be able to detect these failures.)

We expand the PFDs to show the sum of the individual device PFDs, (Equation 5).

$$\boldsymbol{PFD_{SIF} \approx \sum PFD_{Si} + \sum PFD_{LSi} + \sum PFD_{FEi} + \sum PFD_{SSi} + \sum PFD_{SYS-PROCi} + \sum P_{HUMi}} \quad \textbf{Equation 5}$$

Further, the overall human error term can be expanded and written as Equation 6.

$$\boldsymbol{P_{HUM} = P_{design\ error} + P_{installation} + P_{proof\ test\ error} + P_{bypassed}} \quad \textbf{Equation 6}$$

Of the four terms in this equation, the first two can be detected and corrected during initial commissioning steps for the SIF. Experience has shown that the last two terms, $P_{proof\ test\ error}$ and $P_{bypassed}$ are likely to dominate the P_{HUM}, though more industry data is needed to support this observation. Assuming that P_{HUM} is dominated by $P_{proof\ test\ error}$ and $P_{bypassed}$, Equation 6 can be further simplified to Equation 7.

$$\boldsymbol{P_{HUM} = P_{proof\ test\ error} + P_{bypassed}} \quad \textbf{Equation 7}$$

Experienced gained from many accident investigations and also from calculations, support the contention that for high SIL designs, the human errors during interventions, $P_{proof\ test\ error}$ and $P_{bypassed}$, dominate the calculated PFD_{SIF}. Unfortunately, most of the SIL verification

calculations today use the truncated Equation 1 (Equation 8.1 in TR84.00.02-2015) instead of the more complete Equation 8 (below).

$$PFD_{SIF} = PFD_S + PFD_{LS} + PFD_{FE} + PFD_{SS} \qquad \textbf{Equation 1}$$

$$PFD_{SIF} = PFD_S + PFD_{LS} + PFD_{FE} + PFD_{SS} + PFD_{HUM} \qquad \textbf{Equation 8}$$

Remember that Equation 1 gives the $PFD_{hardware}$ (only) As a result, most SIL Verification calculations today effectively ignore specific end-user human errors when quantifying their risk reduction capability. This approach is equivalent to saying the system boundary for an SIF only includes the instrumented components (a subsystem). In LOPA (layer of protection analysis) and other quantitative risk assessments, the entire IPL system must be considered [8]. It is critical to include everything that can cause the SIF to fail in the IPL boundary [9].

1.2.1 IPL (SIF) Boundary Example

For example, for a low-level sensor to prevent high pressure gas blow-by (Figure 1), Equation 1 would evaluate only the devices in the narrow boundary:

- the level transmitter,
- the logic solver, and
- the solenoid valve and isolation valve to prevent gas blow-by.

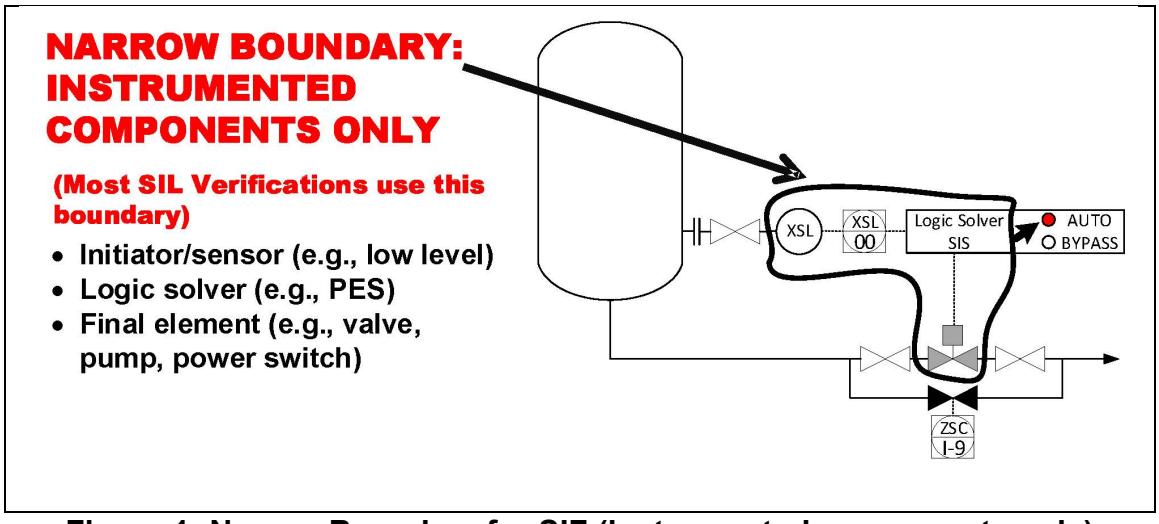

Figure 1: Narrow Boundary for SIF (instrumented components only)

Courtesy Process Improvement Institute, Inc., All Rights Reserved

Equation 8 would include the hardware in Equation 1 but would also include the human errors related to the SIF (Figure 2):

- the root valves and the vessel connection for the sensor(s)
- the auto/manual bypass switch for SIF
- the block valves around the isolation valve, and
- the bypass around the isolation valve.

The additional items in Equation 5 can contribute to the probability that the SIF is bypassed ($P_{bypassed}$) or that the SIF is rendered non-functional after the proof test ($P_{proof\ test\ error}$).

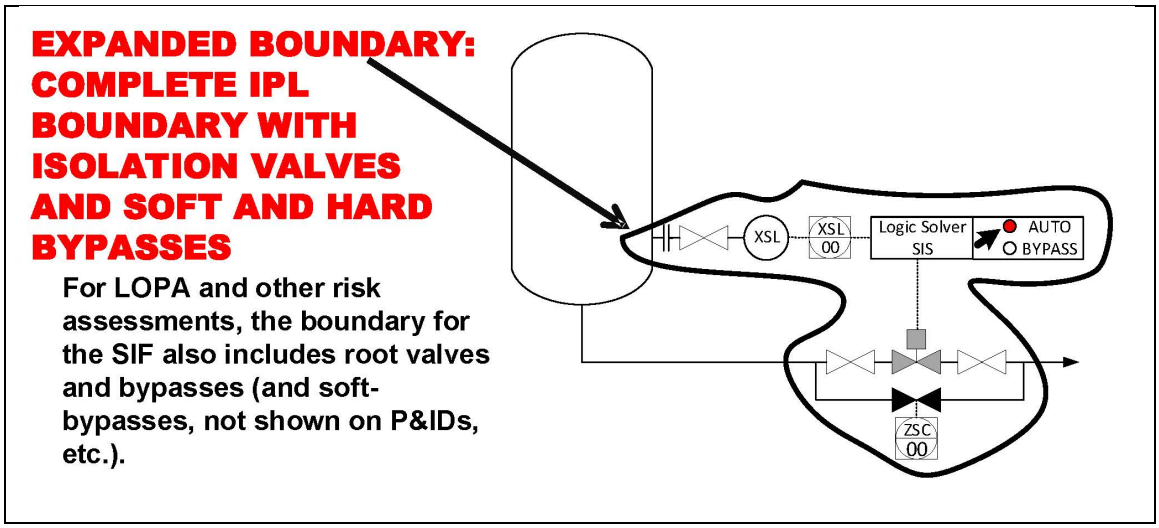

Figure 2: Expanded Boundary for SIF (instrumented components and isolation valves and soft and hard bypasses)

Courtesy Process Improvement Institute, Inc., All Rights Reserved

1.2.2 IPL (PSV) Boundary Example

In another example, if the IPL is a PSV, then the IPL system must include upstream and downstream features, such as isolation valves. Therefore, the probability of leaving an isolation valve closed should be included as a contribution to the overall PFD of the PSV IPL system.

For the remainder of this paper, we will concentrate on the effect of including the probability of human errors for calculation of PFD_{SYS}, and the effect this has on the resulting SIL. For convenience, this paper arbitrarily sets $\sum PFD_{SYS\text{-}PROC}$ = zero. This is being done so the reader can better focus on the human error aspect of systematic errors. $PFD_{SYS\text{-}PROC}$ is worthy of its own paper as its significance is generally dependent on the process fluid properties and/or ambient conditions.

The next two sections of this paper provide a basis for (1) the baseline error rate for human error during interventions and (2) the error rates given coupling of activities, such as occur with redundant systems. Following that, simple examples are provided to help show the relative impact of including human error terms $\sum PFD_{HUM}$ in the calculation of PFD_{SYS}.

2 Human Error Probability for a Single Execution of a Rule-Based Task

To calculate P_{HUMi}, the type of tasks must be defined and the baseline error rate for such a task needs to be established. Note that with excellent control of all of the human factors, a company can begin to approach the lower limits that have been observed for human error, but individual, specific human error probabilities may average about $P_{HUMi} = 0.01$ (which is a relatively large factor in SIL 2 and SIL 3 verification calculations). It is critical to provide detection and correction for specific human errors.

Excellent control of all human factors means a robust design and implementation of management systems for each human factor are achieved with a high level of operational discipline. The first well-researched publication detailing potential lower limits of human error probability was by Alan Swain and H Guttmann (NUREG-1278, 1983) [10] and by others. However, many times, the limits they referenced get used out of context. The lower limits in the NUREG-1278 assume excellent human factors, but such excellent control is rarely, if ever achieved. Additionally, some human errors listed by Swain and others were for a single error under highly controlled conditions, or on a "best day" instead of average error probability or rate over an average year of tasks. In general, Process Improvement Institute (PII) has found it best to use the average error probabilities as discussed in the following section.

2.1 Error Probability for Rule-Based Actions that are Not Time Dependent:

Actions that do not have to be accomplished in a specific time frame to be effective are not time dependent. It should be obvious then that these do not include response to alarms, or similar actions with time limits. Values listed below represent the lower limits for human error rates, assuming excellent control of human factors; these are expressed as the probability of making a mistake on any step:

- 1/100 - process industry; routine tasks performed 1/week to 1/day. This rate assumes excellent control of all human factors. Most places PII visits, the workers and managers and engineers believe this is achievable, but not yet achieved. {Actual data from the Savanah River Site indicated a Miscalibration error probability of 7.0E-3 and a Failure to Restore After Maintenance error probability of 5.1E-3 for an organization with excellent human factors control and data gathering (Table 3, [11]). It is noted that these values could be rounded to 1/100. Organizations are cautioned to determine the actual data for human error rates in their own management systems before using human probabilities lower than 1/100.}
- 1/200 - pilots in the airline industry; routine tasks performed multiple times a day with excellent control of human factors. This average has been measured by a few clients in the airline industry, but for obvious reasons they do not like to report this statistic.
- 1/1000 - for a reflex (hard-wired) action, such as either proactive or minor corrective actions while driving a car, or very selective actions each day where your job depends on getting it right each time and where there are error recovery paths (such as clear visual cues) to correct the mistake. *This is about the rate of running a stop sign or stop light, given no one is in front of you at the intersection; the trouble is measuring this error rate, since you would have to recognize (after the fact) that you made the mistake.*

See Bridges and Collazo (GCPS, 2012) [12] for more details on this topic.

2.2 Adjusting the lower limit rates to estimate a baseline rate at a site

As mentioned earlier, the lower limit rates assume excellent control of human factors in the industry mentioned. Note that airline pilots have a lower error rate than what PII has measured in the process industry. This is due, in part, to the much tighter control by the airlines and regulators on factors such as fitness-for-duty (control of fatigue, control of

substance abuse, etc.). Excellent control of human factors is not achieved in many organizations; therefore, the human error rates will be higher than the lower limit, perhaps much as much as 20 times higher. Table 1 provides adjustment factors for each human factor. These factors can be used to adjust the lower limit of error rate upward or downward as applicable, but the factors should not be applied independently. For instance, even in the worst situations, we have not seen an error rate for an initiating event or initial maintenance error higher than 1/5, although subsequent steps, given an initial error, can have an error rate approaching 1 due to coupling or dependency.

- 1/5 - highest error rates with poor control of human factors; this high rate is typically due to high fatigue or some other physiological or psychological stress (or combination). This is the upper limit of error rates observed with poor human factors and within the process industry. *The error rates in the Isomerization Unit the day of the accident at BP Texas City Refinery [13] were about this rate. The operators, maintenance staff and supervisors had been working about 30 days straight (no day off) on 12-hour shifts.*

For the examples provided later, this paper ***will use a baseline error rate of 0.02 (1/50) errors per step***, which is about average at the sites PII visited in the past 15 years. This value could be justified based on the fact that most chemical process sites do not control overtime during turnarounds and/or do not have a system for controlling verbal communication using radios and phones. In addition, for critical steps such as re-opening and car-sealing the block valves under a relief valve after the relief valve is returned from maintenance, the error probability is about 0.01 (1/100) to 0.04 (1/15) [14]; plus, the average probability of being in a "fail to function" state at time zero for a relief device is between 0.01 (1/100) and 0.02 (1/50) [15, 16, 17] (Bukowski, 2007-2009). Both of these tasks have multiple checks and have procedures (similar to what is done when servicing a SIF and when using bypasses for an SIF) and yet the observed human error probability remains between 0.01 and 0.02.

Table 1. SUMMARY TABLE of 10 HUMAN FACTOR CATEGORIES

Based in part on: Gertman, D.; et. al., *The SPAR-H Human Reliability Analysis Method*, NUREG/CR-6883, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington, DC, August 2005 [18]. PII has modified the list slightly to account for general industry data and terminology and to incorporate PII internal data.

Human Factor Category	Human Factor Issue/Level	Multiplier for Cognitive & Diagnosis Errors
Available Time (includes staffing Issues) – ***for responses only***	Inadequate time Barely adequate time (≈2/3 x nominal) Nominal time (1x what is expected) Extra time (at least 2x nominal and >20 min) Expansive time (> 4 x nominal and > 20 min)	P(failure)=100% 10 1 0.1 0.01
Stress/Stressors	Extreme (threat stress)	5
(includes staffing issues)	High (time pressures such as during a maintenance outage; issues at home, etc.)	2
	Nominal	1
Complexity & Task Design	Highly complex	5
	Moderately complex (requires more than one staff)	2
	Nominal	1
	Obvious diagnosis	0.2
Experience/Training	Low	10
	Nominal	1
	High	0.5
Procedures	Not available in the field as a reference, but should be	20
	Incomplete; missing this task or these steps	8
	Available and >90% accurate, but does not follow format rules (normal value for process industry)	3
	Good, 95% accurate, follows >90% of format rules	1
	Diagnostic/symptom oriented	1
Human-Machine Interface (includes tools)	Missing/Misleading (violates populational stereotype; including round valve handle is facing away from worker)	20
	Poor or hard to find the right device; in the head calc	10
	Some unclear labels or displays	2
	Good	1
Fitness for Duty	Unfit (high fatigue level (>80 hr/wk or >20 hr/day, no day off in 7-day period; or illness, etc.)	20
	Highly degraded fitness (high fatigue such as >15 hr/day, illness, injury, etc.)	10
	Degraded Fitness (>12 hr day and >72 hr/wk)	5
	Slight fatigue (>8 hr per day; ***normal value for process*** industry)	2
	Nominal	1
Work Processes & Supervision	Poor	2
	Nominal	1
	Good	0.8
Work Environment	Extreme	5
	Good	1
	No communication or system interference/damage	10
Communication	No standard for verbal communication rules ***(normal*** value for process industry)	3
	Well implemented and practiced standard	1

3 Human Error Probability for Multiple Executions of a Rule-Based Task

Coupled (dependent) Error Rates: Coupling represents the probability of repeating an error (or repeating success) on a second identical task, given that an error was made on the first task. The increased probability of failure on subsequent tasks given that an error has already been made is known as dependence. The list below provides some starting point guidance on values to use:

- 1/20 to1/90 - if the same tasks are separated in time and if visual cues are not present to re-enforce the mistake path. This error rate assumes a baseline error rate of 1/100 with excellent human factors. If the baseline error is higher, then this rate will increase as well.
- 1/2 - if the same two tasks are performed back-to-back, and if a mistake is made on the first step of two. This error rate assumes a baseline error of 1/100 with excellent human factors. If the baseline error is higher, then this rate will increase as well.
- 8/10 to 10/10 - if the same three tasks are performed back-to-back and a strong visual cue is present (that is, the worker can clearly see the first devices he/she worked on), if a mistake is made on the first steps of the three.
- Two or more people become the same as one person (with respect to counting of errors from the group), if people are working together for more than three days; this effect is due to the trust that can rapidly build.

These factors are based on the relationships provided in NUREG-1278 10] and the related definitions of weak and strong coupling provided in the training course by Swain (1993) [19] on the same topic, as shown here in Table 2. The following relationship is for errors of omission, such as failing to reopen a root valve or failing to return an SIF to operation, after bypassing the SIF. The qualitative values in Table 2 are based jointly on Swain (1993) and Gertman [18] (SPAR-H, 2005 which is NUREG/CR-6883).

One can readily conclude that staggering of maintenance tasks for different channels of the same SIF or for related SIFs will greatly reduce the level of dependent errors. Unfortunately, most sites PII visits do not stagger the inspection, test, or calibration of redundant channels of the same SIF or of similar SIFs; the reason they cite is the cost of staggering the staff. While there is a perceived short-term higher cost, the answer may be different when lifecycle costs are analyzed.

Simple Rule: Staggering of maintenance can prevent a significant number of human errors in redundant channels. In fact, the US Federal Aviation Administration (FAA) requires staggering of maintenance for aircraft with multiple engines or multiple control systems (i.e., hydraulics) (FAA Advisory Circular 120-42B, as part of ETOPS approval [20]. (ETOPS is Extended-range Twin-engine Operational Performance Standards, a rule which permits twin engine aircraft to fly routes which, at some point, are more than 60 minutes flying time away from the nearest airport suitable for emergency landing.)

Table 2: Guideline for Assessing Dependence for a within-SIF Set of Identical Tasks (based partially on SPAR-H, 2005 [18], and partially on field observations by PII)
Courtesy Process Improvement Institute, Inc., All Rights Reserved

Level of Dependence	Same Person	Actions Close in time	Same Visual Frame of Reference (can see end point of prior task)	Worker Required to Write Something for Each Component
Zero (ZD)	No; the similar tasks are performed by different person/group	Either yes or no	Either yes or no	Either yes or no
Zero (ZD)	Yes	No; separated by several days	Either yes or no	Either yes or no
Low (LD)	Yes	Low; the similar tasks are performed on sequential days	No	Yes
Moderate (MD)	Yes	Moderate; the similar tasks are performed more than 4 hours apart	No	No
High (HD)	Yes	Yes; the similar tasks are performed within 2 hours	No	No
Complete (CD)	Yes	Yes; the similar tasks are performed within 2 hours	Yes	Either yes or no

The level of dependency is determined from Table 2 by assessing whether the same person is doing the tasks, the proximity of the actions in time, the proximity of the actions in space (same visual frame of reference), and whether the work is required to make a record for each component:

1. Read down the "Same Person" column and find the applicable row(s), then
2. Read down the "Actions Close in Time" column and find the applicable row,
3. Then check the two columns on the right for that row.
4. The Level of Dependence is shown in the left-most column for the applicable row.

Table 2 has two rows for Zero Dependency (ZD) because ZD can be achieved two different ways:

- Tasks done by different persons or groups (staggered people), or
- Tasks done by same persons or groups, but tasks are done several days apart (staggered times).

Once the level of dependence is known, the probability of either repeat success or repeating errors on identical tasks can be estimated. For these probabilities, we use Table 3, which is a re-typing of Table 20-17 from NUREG-1278 [10] (and the similar table in SPAR-H [18] [Gertman, 2005]).

Table 3. Equations for Conditional Probabilities of Human Success or Failure on Task N, given probability of Success (x) or Failure (X) on Task N-1, for Different Levels of Dependence

Level of Dependence	Repeating Success Equations (but shown as error probability)	Repeating Failure Equations
Zero (ZD)	$P_{Success@N} = x$	$P_{Failures@N} = X$
Low (LD)	$P_{Success@N} = (1+19x)/20$	$P_{Failures@N} = (1+19X)/20$
Moderate (MD)	$P_{Success@N} = (1+6x)/7$	$P_{Failures@N} = (1+6X)/7$
High (HD)	$P_{Success@N} = (1+x)/2$	$P_{Failures@N} = (1+X)/2$
Complete (CD)	$P_{Success@N} = 1.0$	$P_{Failures@N} = 1.0$

4 Illustrative examples

To illustrate the impact (sensitivity) on PFD_{SIF}, we will look at two simple cases and will not provide the details on the calculation of the component aspects of PFD_{SIF}, but instead will provide the results of PFD_{COMP} to be the value obtained by using Equation 1, but without the systematic error terms (the same as using Equation 8.1 in TR84.00.02-2015). Then we will show a simple way to estimate the specific human error term (PFD_{HUM}) and show the resulting impact on PFD_{SIF}. Figures 3 and 4 show a candidate SIL 1 SIF and a candidate SIL 2 SIF, respectively.

4.1 Example 1 - Illustration of Estimate of PFD_{SIF}, for a SIL 1 SIF, with and without consideration of P_{HUM}

For the SIL 1 SIF in Figure 3, the component PFDs were estimated using standard, simplified equations for each, and using generic data available for the components. Based on this calculation, the PFD of the SIF without consideration of discrete systematic error yielded a $PFD_{COMP} = 0.039$. It is noted that the sensor/transmitter PFD contribution is 0.025; this value will be important in the second example included in Section 4.2.

For this example, the term $\sum P_{HUM}$ is next estimated by summing the

- Probability of leaving the root valve for the level switch (sensor/transmitter) closed
- Probability of leaving the entire SIF in BYPASS after maintenance or after some other human intervention (such as an inadvertent error or as a necessity during startup)
- Probability of miscalibration of the level transmitter/switch.

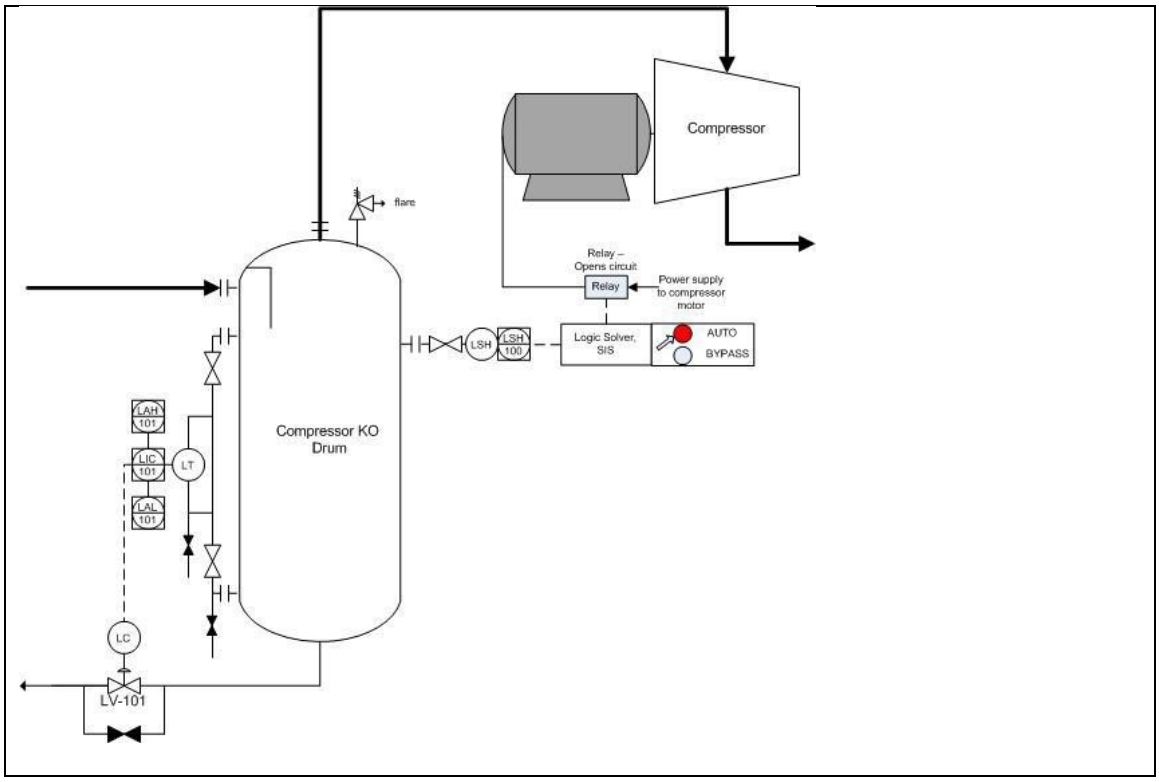

Figure 3. Example of SIL 1 SIF (high level trip of compressor motor)
Courtesy Process Improvement Institute, Inc., All Rights Reserved

Since these are all independent systematic errors, the error rate will simply be 0.02 (the base error rate provided) for each mistake, or:

$$\sum P_{HUM} = 0.02 + \ 0.02 + 0.02 = 0.06$$

This would then give an overall failure probability for the SIF of:

$$PFD_{SIF} = \ PFD_{COMP} + PFD_{HUM} = 0.039 + 0.06 = 0.099$$

Since the PFD_{SIF} is less than 0.1, the instrumented system for high level protection still qualifies as a SIL 1 SIF. But, suppose we wish to improve the reliability and independence of the instrumented system by using a smart sensor/transmitter for the high-level switch (LSH) which will detect null movement of the sensor reading (indicating the valve is closed or the tap is plugged) or suppose we put a limit switch (or captive key system) on the root valve. There is a probability that these safeguards against human error will also fail or be bypassed by the staff, but assuming the probability of that failure is the same as other human errors for this example, 0.02, then the overall system human error is reduced, because the probability of leaving the root valve closed is now ANDed with the probability of smart sensor/transmitter or limit switch failing:

$$\sum P_{HUM} = (0.02 * 0.02) + 0.02 + 0.02 = 0.04$$

Therefore, the revised PFD of the instrumented system becomes:

$$PFD_{SIF} = PFD_{COMP} + PFD_{HUM} = 0.039 + 0.04 = 0.079$$

Sensitivity to Baseline Human Error Rate: If the baseline human error probability increases to 0.04 due to fatigue or extra stress due to schedule constraints, then even with the extra instrumentation to detect valve closure, the PFD of the systematic human error will increase substantially:

$$\sum P_{HUM} = (0.04 * 0.04) \; + \; 0.04 \; + \; 0.04 \; = \; 0.082$$

The revised PFD of the instrument system becomes:

$$PFD_{SIF} = \; PFD_{COMP} + PFD_{HUM} = 0.039 \; + \; 0.082 \; = \; 0.121$$

In this modified case, which is applicable to about a third of the facilities PII has visited in the past 10 years (due primarily to fatigue), the instrumented system no longer qualifies as a SIL 1.

The human error for miscalibration is challenging to reduce, unless there are redundancy and voting of the level sensor/transmitters; then miscalibration errors can be essentially eliminated as an important contribution to human error. This case will be explored in Section 4.2 as part of Example 2. However, the redundancy and voting of transmitters cannot detect an error introduced by using the same calibrator (hardware) that has some error (drift).

The composite error of leaving the entire system in bypass is usually made up of

(1) the inadvertent error to return the system to AUTO after maintenance (a good design would generate a recurring alarm for an SIF in bypass, and a good management system would track and correct such alarms), and
(2) the probability that the staff will make the intentional decision to leave the SIF in bypass, for perhaps a reason not anticipated by the designers. Management of change (MOC) should address the latter case; a strong MOC system should have multiple personnel who would cross-check each other. A bigger issue is failing to recognize that an MOC is needed.

Therefore, this error rate potentially can be reduced by adding repeating alarms to alert the staff that the SIF is still bypassed. A strong management system is essential, else the staff may hear and acknowledge the alarms, but will leave the system in bypass intentionally. Thus, it is critical that the designers anticipate the need for a bypass (such as during startup) and that they provide an appropriate startup bypass that resets the SIF automatically.

4.2 Example 2 - Illustration of Estimate of PFD_{SIF}, for a SIL 2 SIF, with and without consideration of P_{HUM}

For the SIL 2 SIF described in Figure 4, the component PFDs were estimated using standard, simplified equations for each, and using available industry data for the

components. For the case where the sensors are voted 2oo3, the PFD of the SIF without consideration of discrete systematic error yielded PFD_{COMP} = 0.008 (of which the 2oo3 voted sensor portion is 0.0025 and the 2oo3 voted logic solver is 0.003).

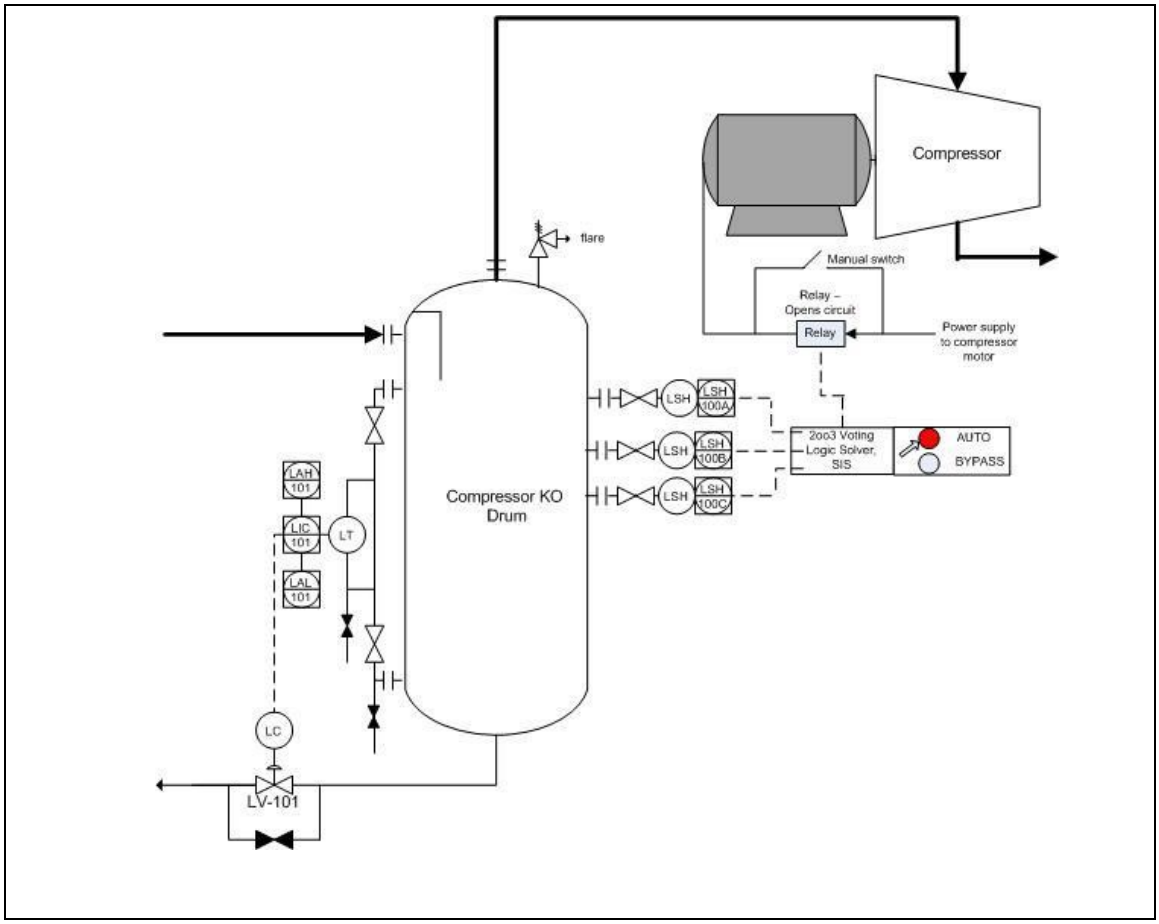

Figure 4. Example of SIL 2 SIF (high level trip of compressor motor)
Courtesy Process Improvement Institute, Inc., All Rights Reserved

For this example, the term $\sum P_{HUM}$ is next estimated by summing the

- Probability of leaving the level sensor/transmitters 2oo3 root valves closed, causing an unsafe failure. (This calculation is shown later).
- Probability of miscalibration of the level transmitter/switch. This calculation is shown later, but for this issue to be a significant probability, two of the three sensors/transmitters must be miscalibrated, unless there is comparison checking, then it would require miscalibration of all three transmitters.
- Probability of leaving the entire SIF in BYPASS after maintenance or after some other human intervention such as an inadvertent error or a necessity during startup; as before, we will use the base error probability of 0.02 as a starting point.
- Probability of leaving the relay bypass closed. As before, we will use the base error probability of 0.02 as a starting point.

$$\sum P_{HUM} = P_{root\ valve} + P_{miscal} + P_{SIF\ bypass} + P_{relay\ bypass}$$

4.2.1 Root valves closed

To aid in the calculation of the probability of leaving 2oo3 root valves closed, we use an event tree to show the conditional probabilities for leaving Valve B closed, given Valve A is open or closed, and similarly, the conditional probability of leaving Valve C closed, given Valve A or B are closed or both Valve A and B are closed. Figure 5 shows the results of this calculation. For the branch probabilities, the equations for high dependency (HD) of the human actions were used (see Table 3); this tree reflects the more prevalent case of redundant channels being maintained on the same day, by the same person, and that level valves are within the visual field of the worker. From Figure 5 the result for the probability of human error of leaving 2oo3 or 3oo3 of the root valves closed is 0.01765. But, the comparison checking between sensors/transmitters will alert the workers that a root valve is closed (assuming 100% detection and correction), so the only valid path is the 3oo3 path; the 3oo3 error case is the bottom row of the event tree in Figure 5. The probability of leaving all three root valves closed is 0.0077.

4.2.2 Sensors Miscalibrated

From the same figure, we can also extract the conditional probability of leaving 3oo3 sensors/transmitters bypassed; assuming comparison checking is in place to note deviations and correct the problem, only the case of 3oo3 errors is applicable. This represents a strong recovery path for the previous errors (100% detection and correction). The 3oo3 error case is the bottom row of the event tree in Figure 5. The probability of miscalibrating all three sensors/transmitters is 0.0077.

$$\sum P_{HUM} = P_{root\ valve} + P_{miscal} + P_{SIF\ bypass} + P_{relay\ bypass}$$
$$= 0.0077 + 0.0077 + 0.02 + 0.02 = 0.055$$

This contribution would then give an overall failure probability for the SIF of:

$$PFD_{SIF} = PFD_{COMP} + PFD_{HUM} = 0.008 + 0.055 = 0.063$$

Since the PFD_{SIF} is greater than 0.01, the instrumented system for high level protection in this example does not qualify as a SIL 2 SIF when accounting for human error probabilities related to interventions with the SIF.

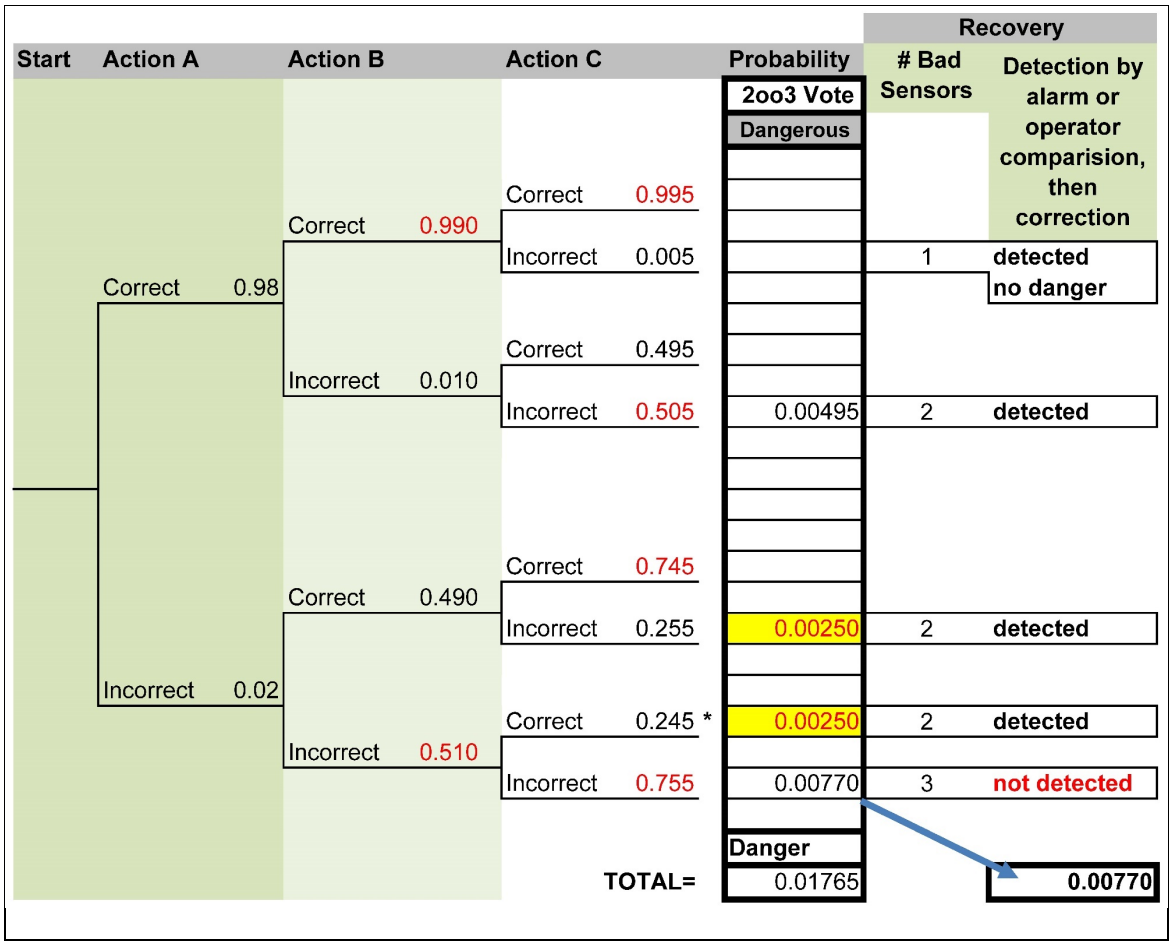

Figure 5. Calculation of Conditional Probability of Not Opening Root Valves; with the Last Column Showing the Probability of Leaving Two or Three Valves Closed (using High Dependence Equations)

Action Examples:

Action A: open Sensor A root valve after maintenance.
Action B: open Sensor B root valve after maintenance.
Action C: open Sensor C root valve after maintenance.

Action A: calibrate Sensor A.
Action B: calibrate Sensor B.
Action C: calibrate Sensor C.

Action A: remove bypass from device A.
Action B: remove bypass from device B.
Action C: remove bypass from device C

4.2.3 Detection and Correction of Sensor Errors

One means to improve the reliability and independence of the instrumented system is to use a smart sensor/transmitter for the LSH which will detect null movement of the sensor

reading, indicating the valve is closed on the tap is plugged. Another possibility is to implement a limit switch (or captive key system) on the root valve. There is a probability that these safeguards against human error will also fail or be bypassed by the staff, but assuming the probability of that failure is the same as other human errors for this example, 0.02, then the systemic human error drops to about zero as the probability of leaving the root valve closed is now ANDed with the probability of smart sensor/transmitter or limit switch failing, as shown in Figure 6.

$$\sum P_{HUM} = P_{root\ valve} + P_{miscal} + P_{SIF\ bypass} + P_{relay\ bypass}$$

$$= 0.0000 + 0.0077 + 0.02 + 0.02 = 0.048$$

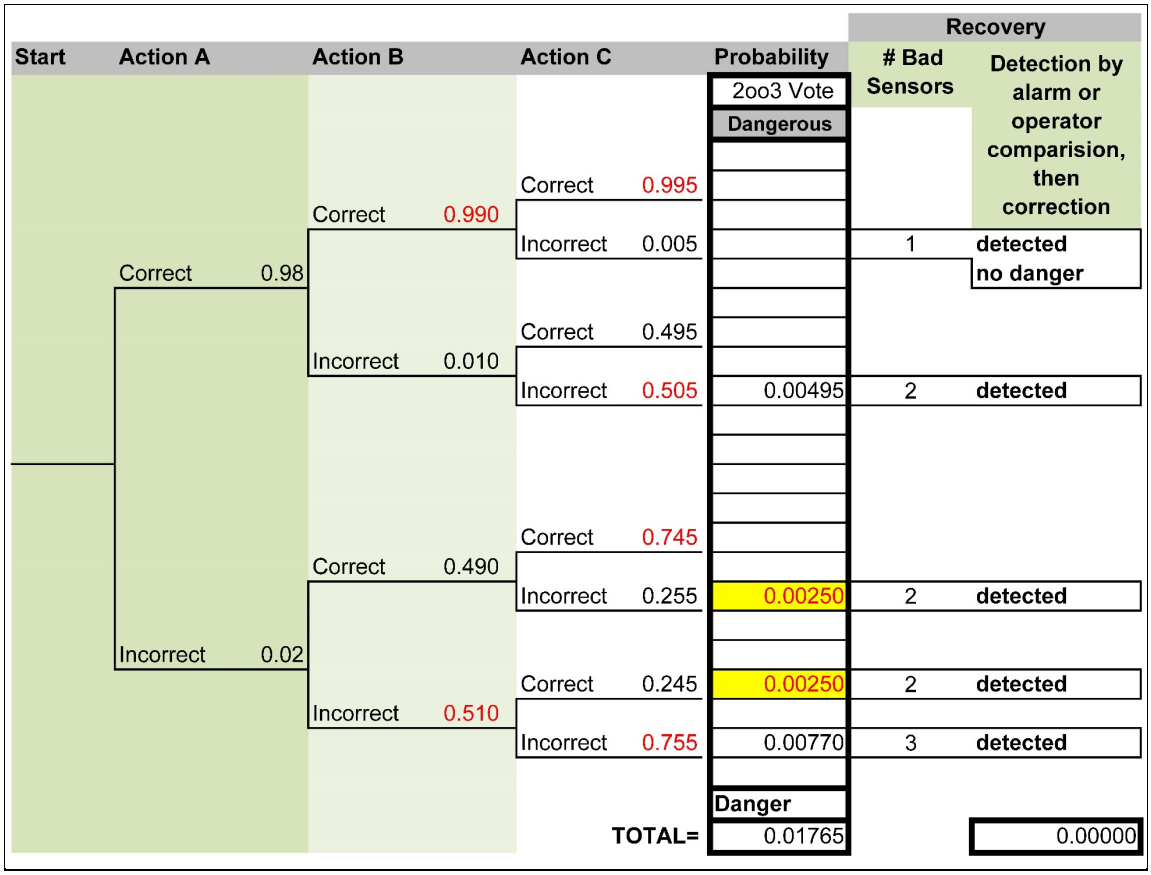

Figure 6. Calculation of Conditional Probability of Not Opening Root Valves; with the Last Column and Last Row Showing the Probability of Leaving Three Valves Closed, and with a Limit Switch or Smart Sensor to Check that Each Root Valve is Open.

Action Examples:

Action A: open Sensor A root valve after maintenance.
Action B: open Sensor B root valve after maintenance.
Action C: open Sensor C root valve after maintenance.

In this case the revised PFD of the instrument system becomes:

$$PFD_{SIF} = PFD_{COMP} + PFD_{HUM} = 0.008 + 0.048 = 0.056$$

Since the PFD_{SIF} is still greater than 0.01, the instrumented system for high level protection still does not qualify as a SIL 2 SIF when accounting for human error probabilities related to interventions with the SIF. But, we have reduced the errors related to dependent failures during checking of the sensors/transmitters as much as possible.

4.2.4 Staggered maintenance

As another alternative (instead of using smart sensors/transmitters or instead of installing limit switches on the root valves) we can reduce potential dependent human error by staggering maintenance activities across different shifts. This would drop the dependence to Low. The dependent error calculations using the Low Dependence equations of Table 3 is shown in Figure 7. From Figure 7, assuming low dependency of human error (LD on Table 3), the result for the probability of human error of leaving 3oo3 of the root valves closed is 0.00016 (assuming that comparison of sensor readings alerts the workers that one root valve is closed -- 100% detection and correction).

From the same figure, we can also extract the conditional probability of leaving 3oo3 sensors/transmitters miscalibrated. As before, only the case of 3oo3 errors is considered applicable, since it was assumed that sensor comparison checking was implemented where any transmitter not miscalibrated will provide the workers an opportunity to note the deviation and take corrective action to fix the problem; this represents a strong recovery path for the previous errors. The 3oo3 error case is the bottom row of the event tree in Figure 7. The probability of miscalibrating all three sensors/transmitters is 0.00016.

Note that sensor comparison checking will not detect miscalibration from using the same calibrator that has an error (drift). If the calibrators are checked frequently enough and corrected, staggering calibration would enable sensor comparison checking to detect a miscalibration.

$$\sum P_{HUM} = P_{root\ valve} + P_{miscal} + P_{SIF\ bypass} + P_{relay\ bypass}$$

$$= 0.00016 + 0.00016 + 0.02 + 0.02 = 0.040$$

This would then give an overall failure probability for the SIF of

$$PFD_{SIF} = PFD_{COMP} + PFD_{HUM} = 0.008 + 0.040 = 0.048$$

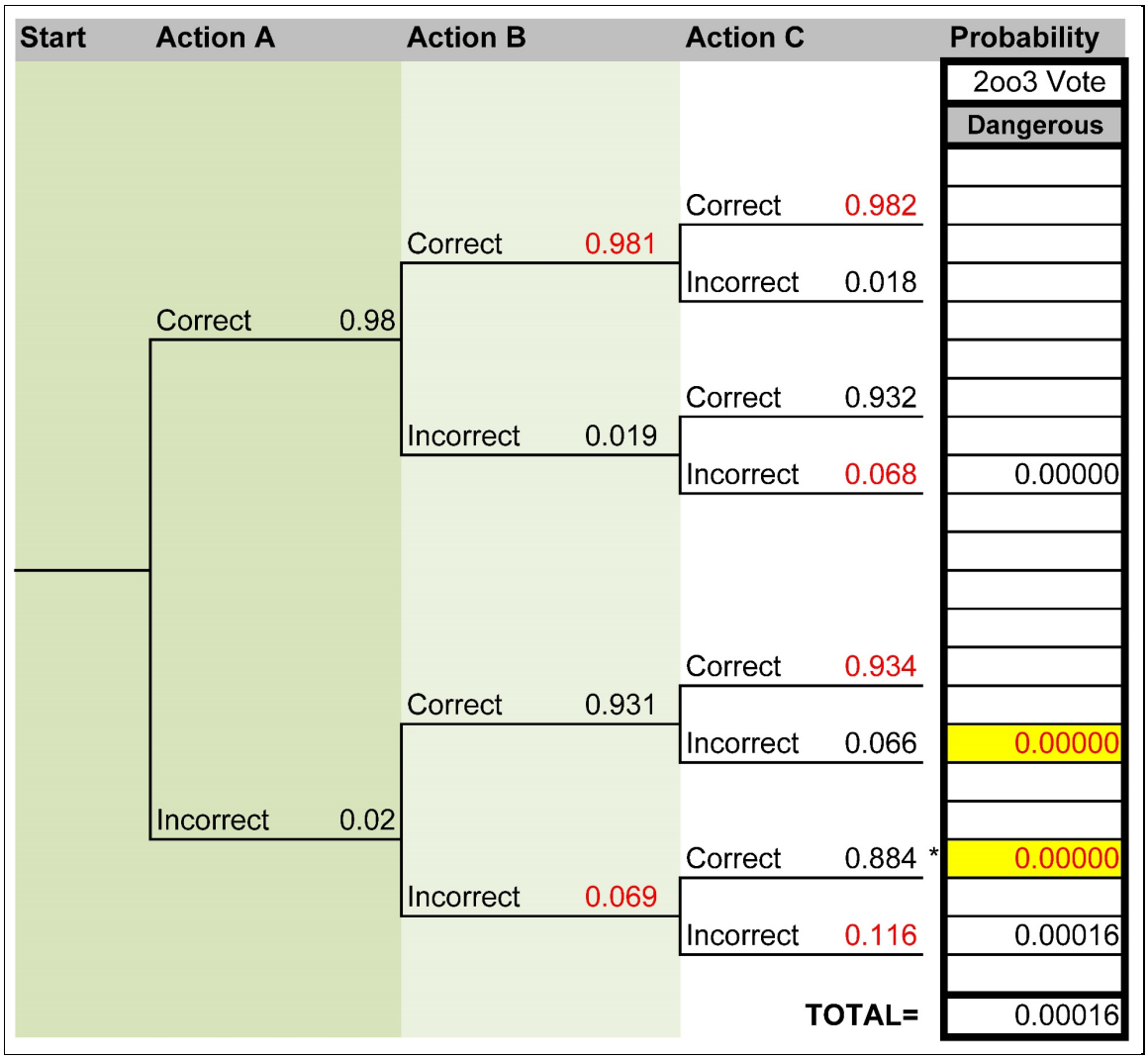

Figure 7. Calculation of Conditional Probability of Not Opening Root Valves; with the Last Column Showing the Probability of Leaving Two or Three Valves Closed (Using Low Dependence Equations)

Action Examples:
Action A: open Sensor A root valve after maintenance.
Action B: open Sensor B root valve after maintenance.
Action C: open Sensor C root valve after maintenance.

Since the PFD_{SIF} is greater than 0.01, the instrumented system for high level protection still does not qualify as a SIL 2 SIF when accounting for human error probabilities related to interventions with the SIF. The weak link in this design is again the human error probability of leaving either the relay bypass closed or the probability of leaving the entire SIF bypassed. This is a common concern on all SIF that have system bypasses. The most effective way to drop these error rates is to eliminate the capability for bypassing the relay and to eliminate the capability for bypassing the entire SIF. Or; we can install a parallel relay with a selector switch so that one relay (and only one) is aligned in the circuit to the

motor of the compressor. This will likely drop the relay systemic human error probability from 0.02 down to 0.0004 or lower. The toughest bypass to eliminate is the one for the entire SIF. It is thought to be only feasible on batch systems or on continuous operations that can be shut down completely for each test interval. However, again, a design with a recurring alarm on bypass and a strong management system to correct the alarm could reduce the bypassed SIF probability to 0.0004 or lower. This change could achieve SIL 2 PFD.

$$\sum P_{HUM} = P_{root\ valve} + P_{miscal} + P_{SIF\ bypass} + P_{relay\ bypass}$$

$$= 0.00016 + 0.00016 + 0.0004 + 0.0004 = 0.001$$

This would then give an overall failure probability for the SIF of

$$PFD_{SIF} = PFD_{COMP} + PFD_{HUM} = 0.008 + 0.001 = 0.009$$

4.2.5 Sensitivity to baseline human error rate:

Obviously, if the baseline human error probability increases to 0.04 due to extra fatigue or extra stress due to schedule constraints, the PFD of the systematic human error will increase substantially and the SIL 2 target becomes even less attainable. Likewise, if suitable operational discipline is adopted to reduce the baseline human error with independent performance measurement to validate the results, the human error rate will be reduced (though it is likely not possible to reduce the baseline human error probability enough to achieve a SIL 2 target, if a SIF bypass is present).

4.3 Example Summary Table

Table 4 shows a summary of key parameters and results from the examples. The examples illustrate the effect of changes in the base human error probability for typical ways that human error can compromise an SIF. The table also shows some examples of error detection and correction that reduce the PFD.

5 Ways to Detect and Manage Human Error for SIFs

Here is a brief summary of techniques that PII has seen employed to detect and manage human error:

- Compare process values for redundant transmitters and alarm on deviation.
- Use logic solver features to detect shorts (bypasses) on de-energize to trip switches (level, pressure, temperature, etc.).
- Avoid blind switches except for tuning fork type level. A level switch at a fixed point can usually detect high level at the same fluid height even if the density changes.
- Provide position switch on bypass valves around final element valves with operator response to alarm to correct, or with shutdown.
- Staggered maintenance as discussed in prior sections.

- Strong maintenance procedures to ensure root valves are open, and all bypasses are removed from the logic solver. Provide alarms for any bypasses in the logic solver.
- Use transmitter diagnostics to alarm on frozen output as it will not only detect hardware failure, but will also detect closed root valves.
- Strong checklist procedures for operations to confirm root valves are open before startup. Requires auditing to determine the human error probabilities. If car seals or locks are used to confirm that root valves and bypass valves are in the correct position, provide a management system that includes auditing to determine the human error probability.
- Strong checklist procedures for operations to confirm sensors are responding correctly during startup. Requires auditing to determine the human error probabilities.
- Design startup bypasses that are automatically removed.
- Use alarm management to improve scenarios of operator response to alarms for extended periods of SIF bypass.

These techniques, if managed well, if documented, and if audited, can be evaluated quantitatively determine the human error probability effects that increase the PFD_{SIF} and the error recovery probability effects that reduce the PFD_{SIF}.

6 Conclusion

As can be seen from the quantitative examples, systematic errors have the potential to significantly impact a SIF in a negative manner. In addition, SIL verifications performed today often do not account for this contribution to probability of failure. In such cases, it becomes increasingly likely that the risk reduction assumed by analysts (who rely upon a SIL 2 to have a PFD of 0.01 or lower) is not sufficient to satisfy corporate risk criteria when the actual risk reduction estimated for the IPL is being counted on, such as an SIF replacing a relief valve, as opposed to analyses that are simply performed on a comparative basis where consistency is more important than the actual numbers.

The paper points to the need for companies to begin:

- Accounting for systematic error (and especially human error probability) in SIL Verifications; otherwise the risk reduction factor from this IPL will be unrealistically optimistic.
- Taking a more in-depth look at the management systems and work processes in place for operations and maintenance and their associated training and revalidation of performance.

Using the mathematics presented, companies can gain insight concerning the relative effectiveness of their practices and find areas where improvements can be made with minimal additional cost. Just as improved human factors improve safety, improved safety performance, if done properly with true operational discipline, should also improve reliability and plant availability.

Table 4: Summary Table for the Examples

Courtesy Process Improvement Institute, Inc., All Rights Reserved

						PFD_{HUM} from Human Errors							Recovery				
Example	**Figure**	**Maint.**	**Baseline Human Error Probability**	**Target SIL**	**PFD COMP**	**PFD ROOT VALVES**	**PFD SIF BYPASS**	**PFD RELAY BYPASS**	**PFD MISCAL**	**Total PFD SYS-HUM**	**Achieved PFD_{SIF}**	**Achieved SIL**	**Detect & Correct the Error**	**PFD change**	**Total PFD SYS-HUM**	**Revised PFD_{SIF}**	**Revised SIL**
4.1	3		0.02	1	0.039	0.02	0.02		0.02	0.06	0.099	1	Root Valves	-0.02	0.04	0.079	1
			0.04	1	0.039	0.04	0.04		0.04	0.12	0.159	0	Root Valves	-0.04	0.08	0.119	0
4.2	4, 5, 6	High Dependency	0.02	2	0.008	0.0077	0.02	0.02	0.0077	0.055	0.063	1	Root Valves	-0.0077	0.048	0.056	1
	4, 7	Low Dependency (Staggered)	0.02	2	0.008	0.00016	0.02	0.02	0.00016	0.040	0.048	1	SIF Bypass	-0.0196	0.001	0.009	2
													Relay Bypass	-0.0196			

7 Acronyms Used

1oo2	One out of two voting architecture
1oo3	One out of three voting architecture
2oo3	Two out of three voting architecture
3oo3	Three out of three voting architecture
λ	Failure Rate, units of time^{-1}
ANSI	American National Standards Institute
CD	Complete Dependence
COMP	Random hardware failure contributions to overall PFD
D	Dangerous
ETT	Energize To Trip
ETOPS	Extended-range Twin-engine Operational Performance Standards
F	Failure/error term
FE	Final Element
FAA	US Federal Aviation Administration
HD	High Dependence
HRA	Human Reliability Analysis
IPL	Independent Protection Layer
ISA	International Society of Automation
LD	Low Dependence
LS	Logic Solver
LOPA	Layer of Protection Analysis
MOC	Management of Change
P	Probability
PES	Programmable Electronic System
PFD	Probability of Failure (dangerous) on Demand
PII	Process Improvement Institute, Inc.
PS	Power supply
PSV	Pressure Safety Valve
S	Sensor
SS	Required Support Systems, such as a power supply in ETT
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SRS	Safety Requirements Specifications
SYS	Systematic failure contributions to overall PFD
HUM	Systematic errors and failures generated by human error
SYS-PROC	Systematic errors and failures generated randomly by the process
TI	Proof Test Interval, units of time
TR	Technical Report (such as for ISA technical reports)
ZD	Zero Dependence

8 References

8.1 References cited

[1] W.G. Bridges and H.W. Thomas, "Accounting for Human Error Probability in SIL Verification Calculations", 8th Global Congress on Process Safety, Houston, TX, April 1-4, 2012, American Institute of Chemical Engineers.

[2] IEC 61508, Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems, International Electrotechnical Commission (IEC), 2010, Geneva, Switzerland.

[3] U.S. Chemical Safety and Hazard Investigation Board, *Investigation Report, Pesticide Chemical Runaway Reaction Pressure Vessel Explosion*, Report No. 2008-08-I-WV, January 2011.

[4] IEC 61511-1:2016+AMD1:2017 CSV, Consolidated version: Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and application programming requirements, International Electrotechnical Commission (IEC), 2010, Geneva, Switzerland.

[5] ANSI/ISA-61511-1-2018 / IEC 61511-1:2016+AMD1:2017 CSV, Functional Safety – Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, definitions, system, hardware and application programming requirements (IEC 61511-1:2016+AMD1:2017 CSV, IDT), International Society of Automation, Research Triangle Park, North Carolina.

[6] ISA-TR84.00.02-2015, *Safety Integrity Level (SIL) Verification of Safety Instrumented Functions*, International Society of Automation, Research Triangle Park, North Carolina.

[7] ISA-TR84.00.02-2002, Safety Instrumented Functions (SIF)-Safety Integrity Level (SIL) Evaluation Techniques Part 2: Determining the SIL of a SIF via Simplified Equations, International Society of Automation, Research Triangle Park, North Carolina.

[8] CCPS, *Layer of Protection Analysis: Simplified Process Risk Assessment*, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY, 2001.

[9] A.M. Dowell, III, "Understanding IPL Boundaries", to be published in Process Saf Prog, March 2018. (Originally prepared for presentation at the American Institute of Chemical Engineers 2018 Spring Meeting, 14th Global Congress on Process Safety, Orlando, Florida, April 23–25, 2018).

[10] A. Swain and H. Guttmann, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Sandia National Laboratories*, 1983 [this document became NUREG/CR-1278– The Human Reliability Handbook, guidelines from the US NRC on Human Reliability Analysis].

[11] STTD. WSRC-TR-93-581, H.C. Benhardt et al, "Savanah River Site, Human Error Data Base Development for Nonreactor Nuclear Facilities (U)", Westinghouse Savannah River Company, Aiken, SC, February 28, 1994.

[12] W.G. Bridges and G.M. Collazo, "Human Factors and Their Optimization", 8th Global Congress on Process Safety, Houston, TX, April 1-4, 2012, American Institute of Chemical Engineers.

[13] U.S. Chemical Safety and Hazard Investigation Board, *Investigation Report, Refinery Explosion and Fire*, Report No. Report No. 2005-04-I-TX, March 2007.

[14] CCPS, *Guidelines for Independent Protection Layers and Initiating Events in Layer of Protection Analysis*, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY, 2012.

[15] J.V. Bukowski, Results of Statistical Analysis of Pressure Relief Valve Proof Test Data Designed to Validate a Mechanical Parts Failure Database, Technical Report, exida, Sellersville, PA, 2007.

[16] J.V. Bukowski and W.M. Goble, Villanova University, *Analysis of Pressure Relief Valve Proof Test Data: Findings and Implications*, 10th Plant Process Safety Symposium, American Institute of Chemical Engineers, 2008.

[17] J.V. Bukowski and W.M. Goble, Villanova University, *Analysis of Pressure Relief Valve Proof Test Data*, Process Saf Prog, American Institute of Chemical Engineers, March 2009.

[18] D. Gertman, H. Blackman, J. Marble, J. Byers, and C. Smith, *The SPAR-H Human Reliability Analysis Method*, NUREG/CR-6883, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington, DC, August 2005.

[19] A. Swain, *Human Reliability Analysis*, Training Course, ABS Consulting (formerly JBF Associates), 1993.

[20] US Federal Aviation Administration, "AC 120-42B - Extended Operations (ETOPS and Polar Operations)", Washington, DC, June 13, 2008

8.2 Additional References

[1] A. Swain, Accident Sequence Evaluation Program (ASEP): Human Reliability Analysis Procedure, NUREG/CR-4772, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington, DC, February 1987.

[2] Human Error Repository and Analysis (HERA) System, NUREG/CR-6903, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington, DC, 2006.