Programmable electronic and hardwired emergency shutdown systems: A quantified safety analysis

John J. Sammarco, Ph.D., P.E.
National Institute for Occupational Safety and Health
626 Cochran Mill Road, PO Box 18070
Pittsburgh, PA 15236
Jsammarco@cdc.gov

***Abstract*— Emergency shutdown systems (ESDs) for mining machinery provide critical functions to safeguard miners. Traditionally, ESDs were realized with simple hardwired circuits; today, there is a growing trend to use programmable electronic technology such as programmable logic controllers (PLCs). This paper describes an analytical study to quantify the safety integrity of a PLC-based ESD and a hardwired ESD. The safety integrity level of each design approach was determined by quantifying the average probability of failure on demand (PFD_{avg}) as described by the recommendations for programmable electronic mining systems published by NIOSH and the IEC 61508 international standard. The safety analyses addressed system architecture, hardware failure probability, proof test interval, diagnostic coverage, and human error probability. The results indicated that a same level of safety, safety integrity level 3 (SIL 3), could be attained when evaluating random hardware failures. Neither approach could attain SIL 3 if manual activation was used. Human error was the limiting factor where, using human reliability analysis, $PFD_{avg} < 1 \times 10^{-1}$; thus, the ESD does not meet SIL 1. It is apparent that automatic verses human-activation of the ESD is a very important safety consideration. Manually actuated ESDs can only achieve SIL 1 regardless of the technology; therefore, additional independent safety layers of protection are needed to exceed SIL 1. Secondly, it is apparent that the technology choice is very important. The PLC-based ESD was much simpler to design and to validate safety[1].**

Keywords*— *emergency shutdown systems; programmable electronic; mining safety; electronics

I. INTRODUCTION

Emergency shutdown systems, *a.k.a.* safety instrumented systems, safety shutdown systems, protective instrument systems, and safety interlock systems are ubiquitous in mining; they are an integral part of moving machinery such as longwall systems, continuous mining machines, and conveyors. Traditionally, ESDs were realized with electro-mechanical circuits comprised of switches and relays hardwired together. These circuits were relatively simple and easy to understand because they consisted of just a few components and because their behavior under fault conditions could be completely determined. They were also easy to understand in terms of design, operation, maintenance, and repair because the component failure modes were limited, well understood, and generally discernable by visual inspection or by the use of simple instrumentation such as a multi-meter. For instance, one could easily determine that a relay had failed by seeing the contacts welded together or by making a simple resistance measurement of relay coil to determine that the coil had opened.

Today, the mining industry is using modern technologies such as programmable electronics (PE) for mining machine control and for implementing ESD functions. Great care coupled with substantial expertise must be taken to use PE technology (i.e., software, PLCs, and microprocessors). This technology poses unique technical and managerial challenges to assure safety. For instance, all possible failure modes are not completely known or the behavior under fault conditions can not be completely determined for PE-based systems. Also, there are failure modes that are different from electro-mechanical systems. Lastly, anecdotal evidence indicates that there is confusion and uncertainty in the mining industry concerning the safety of PE-based ESDs. For instance, the author has been asked many questions at workshops addressing the safety of PE-based mining systems that he conducted in the U.S. and Australia. Most of the questions were variations of the following: "What must be considered when designing a PE-based ESD?" "Are programmable electronic ESDs as safe as relay-based or hardwired ESD?"

This paper addresses these questions about the safety of PE-based ESDs by conducting an analytical study to quantify the safety integrity of a PLC-based ESD and a hardwired ESD. The safety analyses addresses system architecture, hardware failure probability, proof test interval, diagnostic coverage, and human error probability. The analysis incorporates the latest best practices to address the safety of PE-based mining systems and the IEC 61508 international standard.

II. DEFINITIONS

Diagnostic coverage – The fractional decrease in the probability of dangerous hardware failure resulting from the successful operation of the automatic diagnostic tests.

Dangerous failure – A failure having the potential to put the safety-related system in a dangerous or fail-to-function state.

[1] The findings and conclusions in this report are those of the author(s) and do not represent the views of the National Institute for Occupational Safety and Health.

The probability of a dangerous failure is λ_D and is equal to the sum of λ_{DD} and λ_{DU}.

Dangerous failure detected – A failure detected by on-line diagnostic tests such that the system will be placed into a safe state. The probability of detecting a dangerous failure is λ_{DD}.

Dangerous failure undetected – A failure that is undetected by on-line diagnostic tests such that the system will not be placed into a safe state. The probability of not detecting a dangerous failure is λ_{DU}.

Failure - The termination of the ability of a functional unit to perform a required function. The failure rate λ is equal to the sum of dangerous failures λ_D and safe failures λ_S.

Mean time to fail safe (MTTFS) – The average time until a system fails safely (i.e. a spurious or nuisance trip).

Probability of failure on demand (PFD) – A value that indicates the probability of a system failing to respond on demand for a safety function. PFD pertains to dangerous failure modes. The average probability of a system failing to respond to a demand in a specified time interval is $PFD_{avg.}$.

Safe failure – A failure that does not put the safety-related system in a dangerous or fail-to-function state. The probability of a safe failure is λ_S.

Safe failure fraction (SFF) – A metric (calculated using equation 4) used for constraining the maximum SIL that can be claimed regardless of the calculated hardware reliability.

Safety integrity: The probability of a safety-related system satisfactorily performing the required safety functions under the stated conditions within a stated time period [1].

Safety Integrity Level (SIL) - One of three possible discrete integrity levels (SIL 1, SIL 2, SIL 3) defined by quantitative or qualitative methods. SIL 3 has the highest level of safety integrity for mining [2]. IEC 61508 uses four SILs.

Type A component – All failure modes are known and can be computed. Also, the behavior under fault conditions can be completely determined. A relay is considered to be type A.

Type B component – All failure modes are not completely known or the behavior under fault conditions can not be completely determined. A PLC is considered to be type B.

1oo1 – A one out of one (1oo1) or simplex architecture consisting of a single channel.

1oo2 – A one out of two or dual channel architecture. Diagnostic capabilities are designated as 1oo2D.

III. Best Practices and Standards Ease of Use

NIOSH, working in conjunction with Mine Safety and Health Administration (MSHA), and the System Safety Mining Industry Workgroup, has established a formalized safety framework for PE-based mining systems[3]. It is realized by a five-part set of best practice recommendations and a four-part set guidance documents for use by mining companies, original equipment manufacturers, suppliers, and MSHA. The best practice recommendations are based on IEC 61508. They establish the processes and outcomes for the safety life cycle phases that included system scope, hazard and risk analyses, overall safety requirements, system realization (design), and safety validation of PE-based systems[2]. The best practice recommendations were used to conduct the safety analyses of this paper. These best practice recommendations do not exclude the use of PE-based systems for an ESD. To our knowledge, no standard excludes the use of PE for an ESD.

IV. Conceptual Design Overview

The designer needs to consider many factors and design options for an ESD. These factors include component failure rates, component technologies, architectures, and testing strategies. The design process includes evaluation of the design's safety performance with respect to the target SIL value and MTTFS. If the safety and reliability are not sufficient, then the conceptual design is changed; thus, it is an iterative process (Fig 1.).

A. Technology Choices

ESDs can be implemented using electrical, electronic, pneumatic, mechanical, hydraulic, and programmable electronic elements [4]. The choice of technologies is a decision the designer should make early. In general, the main technology choices are:

- Relays – Relays are simple devices and their failure modes and rates are well known and predictable. They are typically used for simple functions requiring a few inputs and outputs.
- Solid-state devices – These devices do not use software, thus their flexibility is restricted. Solid-state devices can incorporate limited diagnostic and testing features. Some solid-state devices have identifiable and predictable failure modes under fault conditions.

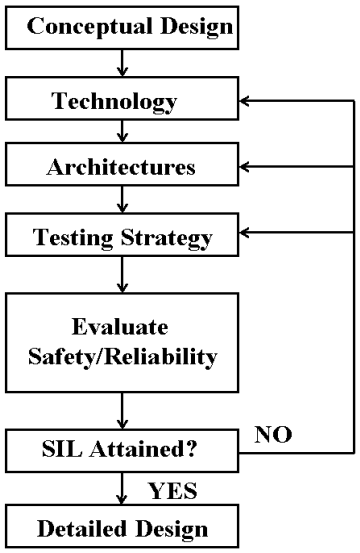


Figure 1. The design process is an iterative part of the safety life cycle.

- PE-based devices – Microprocessors and PLCs are widely used PE-based devices. They are more flexible and can offer more functionality. However, the failure

modes are not predictable and failures (hardware or software) can be difficult to detect and diagnose.

B. *Architectures*

The ESD architecture is important to consider. Various voting architectures (Table I) are used to help realize the required safety performance for a given application. These architectures can also add fault tolerance capabilities; however, merely adding fault tolerance does not always improve safety performance. The architecture choice involves consideration of factors such as the required SIL and the MTTFS. This reliability metric is important for safety because high nuisance trip rates can result in people disabling the ESD.

C. *Architecture impacts on safety performance.*

Frederickson [5] presents several examples of how the architecture impacts safety performance. The examples involve several PLC-based safety systems. We extract the SIL and MTTFS data for the four architectures of Table I, and define a test interval of 12 months. The attained SIL, the approximate PFD_{avg}, and the approximate MTTFS for each architecture is listed by Table II. The results were determined by Markov model analysis of random hardware failure rates.

TABLE I. REPRESENTATIONS OF VARIOUS ARCHITECTURES

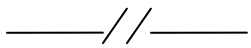
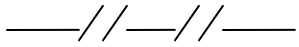
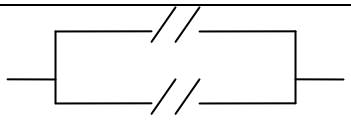
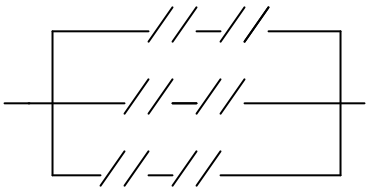
Voting Architecture	Electrical Representation
1oo1	
1oo2	
2oo2	
2oo3	

TABLE II. EXAMPLE SAFETY PERFORMANCES FOR VARIOUS PLC ARCHITECTURES.

Architecture	MTTFS (years)	PFD_{avg}	SIL
1oo1	2.0	1.3×10^{-3}	2
1oo2	0.8	0.003×10^{-3}	Exceeds 3
2oo2	600	2.8×10^{-3}	2
2oo3	210	0.009×10^{-3}	Exceeds 3

Increasing the fault tolerance from 1oo1 to 1oo2 improved the safety performance from SIL2 to SIL3; however, the MTTFS decreased resulting in over double the spurious trips. Increasing the redundancy by using the 2oo2 architecture improved the MTTFS by a factor of 300; however, the SIL didn't improve as compared to the 1oo1 architecture. Thus, adding redundancy does not always improve safety in terms of both the SIL and MTTFS. The 2oo3 architecture has the best safety performance; but, it would be the most costly PLC.

V. SIL CONSTRAINTS DUE TO HARDWARE ARCHITECTURE

The highest SIL that can be claimed for a given architecture is restricted. The IEC 61508 constraints for type A and type B devices are given by the Tables III and IV respectively.

VI. FAILURE DATA SOURCES

Failure data are needed to calculate PFD_{avg} for low demand applications and to calculate the probability of a dangerous failure for high demand applications. In addition to failure rates, the failure modes (safe and dangerous) and the effectiveness of automatic diagnostics are needed.

Numerous data sources exist; some are industry specific, product specific, generic, or site specific. For instance, a site-specific data base could contain failure rate and mode data for solenoid valves used at a given mine. Some common failure data sources are:

- Offshore Reliability Data (OREDA) [6]
- Reliability Data for Control and Safety Systems [7]
- Non-electronic Parts Reliability Data Book [8]
- The Safety Equipment Reliability Handbook [9]

An extensive listing of failure data sources is available at http://www.ntnu.no/ross/info/data.php.

TABLE III. IEC 61508 HARDWARE ARCHITECTURAL CONSTRAINTS ON TYPE-A DEVICES.

Safe failure fraction (SFF)	Hardware fault tolerance		
	0	1	2
< 60%	SIL1	SIL2	SIL3
60% - < 90 %	SIL2	SIL3	exceeds SIL3
90 % - < 99 %	SIL3	exceeds SIL3	exceeds SIL3
≥ 99 %	SIL3	exceeds SIL3	exceeds SIL3

TABLE IV. IEC 61508 HARDWARE ARCHITECTURAL CONSTRAINTS ON TYPE-B DEVICES

Safe failure fraction (SFF)	Hardware fault tolerance		
	0	1	2
< 60%	Not allowed	SIL1	SIL2
60% - < 90 %	SIL1	SIL2	SIL3
90 % - < 99 %	SIL2	SIL3	exceeds SIL3
≥ 99 %	SIL3	exceeds SIL3	exceeds SIL3

VII. ESD COMPARISON

A hypothetical example is presented for two hardwired designs and two PLC-based designs for a ESD to be used on a remote-controlled continuous mining machine. The mining machine does have a PLC that provides some machine control functions.

An ESD is needed to achieve and maintain a safe state for certain hazards identified by a system-level hazard and risk analysis for the mining machine. The hazard for this example is given as unexpected machine movement.

The following ESD designs are examples for illustrative purposes only. The examples do not detail every task or process given by the best practice recommendations for mining; however, they do focus on key design considerations items such as SILs, system architecture, hardware failure probability, proof test interval, diagnostic coverage, and human reliability. Lastly, the parameter values for each design are illustrative; they are assumptions and not actual values.

A. SIL Assignment

The safety performance to mitigate the hazard is defined by one of three SIL values where SIL 1 is the lowest safety performance. The SIL can be determined qualitatively by using a risk matrix or a risk graph (Fig 2.). The unexpected machine movement hazard is assigned SIL 3; therefore, the ESD must attain a SIL 3. The SIL was determined given the parameters C_D, $F_{A,}$ $P_{A,}$ X_5 and W_2 that are defined as follows:

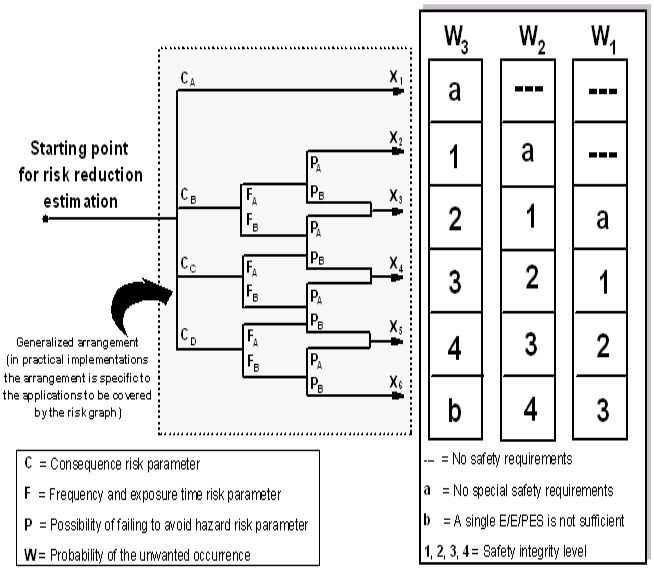


Figure 2. Risk Graph [10]

C - Consequence (severity of injury)

C_A: minor injury, no lost work days

C_B: moderate injury, lost work days

C_C: severe injury, permanent disability

C_D: death or multiple deaths

F - Frequency and exposure time to the hazard

F_A: rarely to more often

F_B: frequently to continuously

P - Possibility of avoiding a hazardous event

P_A: possible under certain conditions

P_B: almost impossible

W - Frequency of the unwanted occurrence taking place

W_1: very slight

W_2: slight

W_3: relatively high

X_n - SIL matrix row identifier

B. Hardwired ESD using a 1oo1 architecture

This design consists of a generic switch directly wired to the main line circuit breaker as depicted by Fig 3. The design can be abstracted as a single sensor, logic solver, and field device configured in a 1oo1 architecture. The switch is the sensor; the logic solver is the wire; the field device is the circuit breaker. None of the components have diagnostics, so safe and dangerous failures are not detected. All components are type A. The following parameters are assumed:

Test interval (TI) = once a year (8760 hours)

$\lambda_{DD} = 0$ (because no diagnostic coverage)

$\lambda_{DU} = \lambda_D$ (because no diagnostic coverage)

Switch: $\lambda = 1.0 \times 10^{-6}$; $\lambda_S = 0.60 \times 10^{-6}$; $\lambda_D = 0.40 \times 10^{-6}$

Wire: $\lambda = 1.1 \times 10^{-8}$; $\lambda_S = 1.0 \times 10^{-8}$; $\lambda_D = .01 \times 10^{-8}$

Circuit breaker: $\lambda = 1.5 \times 10^{-6}$; $\lambda_S = 1.38 \times 10^{-6}$; $\lambda_D = 0.12 \times 10^{-6}$

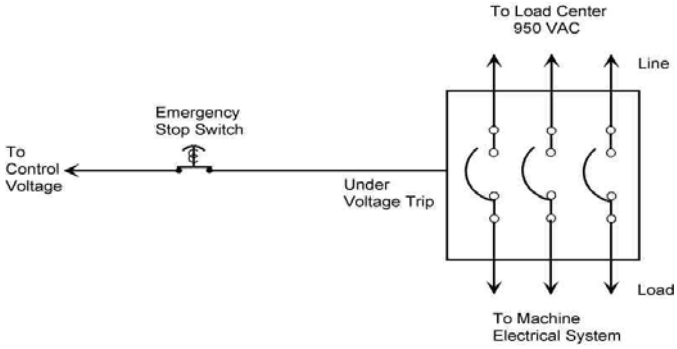


Figure 3. ESD system using a single, generic switch

1) SIL Verification

The SIL is verified by using the simplified equations to find the PFD_{avg} of each component and of the overall ESD. The achieved SIL is determined by using Table V given a low-demand of operation for the ESD. Low demand is when the frequency of operation is less than once a year or no greater than twice the frequency of tests (proof tests) to detect failures in the safety-related system.

$$PFD_{avg} = \lambda_{DU} \times (TI / 2) \quad (1)$$

$PFD_{avg\ switch} = 1.75 \times 10^{-3}$ (SIL 2)

$PFD_{avg\ wire} = 4.38 \times 10^{-6}$ (SIL 3)

$PFD_{avg\ circuit\ breaker} = 5.26 \times 10^{-4}$ (SIL 3)

$$PFD_{avg\ system} = PFD_{avg\ switch} + PFD_{avg\ wire} + PFD_{avg\ circuit\ breaker} \quad (2)$$

$PFD_{avg\ system} = 2.28 \times 10^{-3}$ (SIL2)

TABLE V. SILS FOR A LOW-DEMAND MODE OF OPERATION.

Safety integrity level (SIL)	Low demand mode PFD_{avg}
1	10^{-1} to 10^{-2}
2	10^{-2} to 10^{-3}
3	10^{-3} to 10^{-4}

Next, the MTTFS is calculated for each component and for the overall ESD (Table VI). The equations do not include terms for systematic error rate and common cause terms [11]. The spurious trip rate (STR) = λ_S for this example and MTTFS= 1/ λ_S. The STR for the overall ESD is the summation of the STR for each component. The MTTFS for the ESD is 57.36 years.

C. Hardwired ESD using a 1oo2 switch architecture

The safety performance is increased by using multiple switches in a 1oo2 architecture as depicted by Fig 4. The test interval was unchanged. The switch parameters unchanged and are as follows:

switch: $\lambda = 1.0 \times 10^{-6}$; $\lambda_S = 0.60 \times 10^{-6}$; $\lambda_D = 0.40 \times 10^{-6}$

TABLE VI. MTTFS FOR A HARDWIRED ESD USING A 1OO1 ARCHITECTURE.

Component	STR	MTTFS (hours)	MTTFS (years)
Switch	0.60×10^{-6}	2.5×10^{6}	285.39
Wire	1.00×10^{-8}	1.00×10^{8}	1.14×10^{4}
Circuit breaker	1.38×10^{-6}	7.25×10^{5}	82.72
Overall ESD	1.99×10^{-6}	5.03×10^{5}	57.36

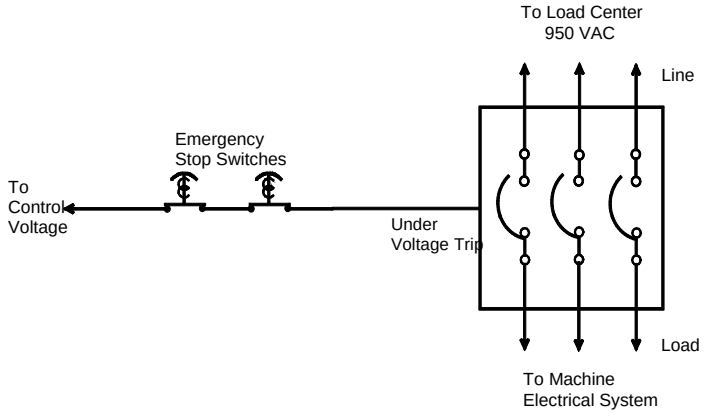


Figure 4. ESD system using switches configured in a 1oo2 architecture

1) SIL Verification

$$PFD_{1oo2\ switch} = (\lambda_{DU}{}^2 \times TI^2) / 3 \quad (3)$$

$$PFD_{1oo2\ switch} = ((.40 \times 10^{-6})^2 \times (8760)^2) / 3 = 4.1 \times 10^{-6}$$

The other components are unchanged where the PFDavg wire = 4.38 x 10-6 and PFDavg circuit breaker = 5.26 x 10-4. Therefore, using equation 2

$$PFD_{avg\ system} = 5.31 \times 10^{-4} \text{ (SIL3).}$$

The new design meets SIL 3 as determined by using Table V; however, the verification is not completed because the system architecture restriction has not been taken into account.

The SFF, fault tolerance, and Table III are needed to determine the maximum SIL that can be claimed. The fault tolerance is one because of the 1oo2 switch architecture. The SFF is calculated as follows using λ_S and λ_D for each component:

$$SFF = (\sum \lambda_S + \sum \lambda_{DD}) / (\sum \lambda_S + \sum \lambda_D) \quad (4)$$

$$\sum \lambda_S = 0.60 \times 10^{-6} + 1.00 \times 10^{-8} + 1.38 \times 10^{-6} = 1.99 \times 10^{-6}$$

$$\sum \lambda_D = 0.40 \times 10^{-6} + 0.01 \times 10^{-8} + 0.12 \times 10^{-6} = 5.20 \times 10^{-7}$$

$$\sum \lambda_{DD} = 0 \text{ (because no diagnostics)}$$

$$SFF = 0.793 \text{ or } 79.3\%$$

The maximum SIL that can be claimed is SIL 3, using Table III with SFF = 79.3% and a hardware fault tolerance of 1; therefore, the SIL is not constrained by the architecture. Hence, the hardware is verified to meet the target of SIL 3.

Next, the MTTFS is calculated for each component and for the overall ESD (Table VII). The STR for switches arranged in a 1oo2 architecture is calculated as follows:

$$STR = 2\lambda_s + 2\lambda_s \quad (5)$$

$$STR = 2(0.60 \times 10^{-6}) + 2(0.60 \times 10^{-6}) = 2.4 \times 10^{-6}$$

The MTTFS for the ESD is 30.12 years.

TABLE VII. MTTFS FOR A HARDWIRED ESD USING A 1OO2 SWITCH ARCHITECTURE.

Component	STR	MTTFS (hours)	MTTFS (years)
1oo2 Switches	2.4×10^{-6}	4.17×10^{5}	47.56
Wire	1.0×10^{-8}	1.00×10^{8}	1.14×10^{4}
Circuit breaker	1.38×10^{-6}	7.25×10^{5}	82.72
Overall ESD	3.79×10^{-6}	26.4×10^{5}	30.12

D. An Industrial PLC-based ESD using a 1oo1 architecture

The design (Fig 5.) is essentially the same as in the prior example except that the logic solver is a generic, industrial PLC. This is an existing PLC that provides machine control functions. The ESD design uses the existing PLC's spare input and output channels. Note that using the system for control and safety purposes is possible, but not recommended [2]. Safety systems should be independent of the control systems. Note that failure of the PLC would impact both the control and safety system.

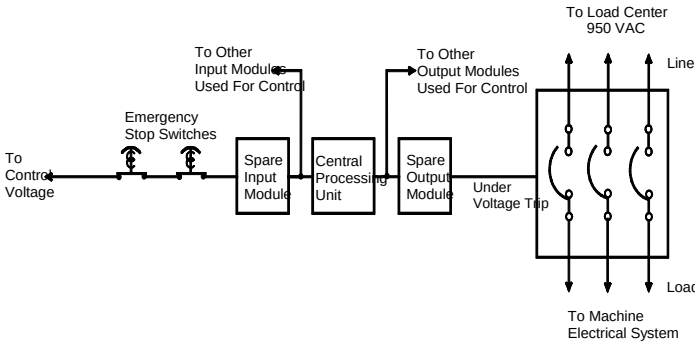


Figure 5. A conceptual diagram of a PLC-based safety system that shares a 1oo1 industrial PLC used for machine control.

The same switches and circuit breaker from the previous examples are used. The following parameters are assumed for a generic, industrial PLC with some built-in diagnostics:

PLC: $\lambda = 3.8 \times 10^{-6}$; $\lambda_S = 2.11 \times 10^{-6}$; $\lambda_D = 1.69 \times 10^{-6}$

The PLC is a type B component.

1) SIL Verification

The achieved SIL of this design is verified with the aid of a PC-based software tool for calculations of PFD_{avg} given the system architecture and other parameters. The following parameters are used by the tool:

β [%] – The β-factor or common cause factor.

Type A/B – Component type A or B

λ [1/h] – Failure rate (failures per hour)

[%] Safe – The safe failure percentage. This is similar to SFF.

DC safe – Diagnostic coverage for safe failures.

DC dangerous – Diagnostic coverage for dangerous failures.

MTTR [hour] – Mean time to repair.

TI [months] – Testing interval.

The tool calculates PFD_{avg} for each component and for the system, the SIL, the MTFFS, and the architectural constraints. Table VIII lists a summary of the results from the tool. The results showed that when using this PLC, the ESD theoretically met SIL 2; however, the PLC is a type B device so the architectural constrains of Table IV were used. As a result, the ESD can only attain SIL 1 even though the design used the same 1oo2 switch redundancy and circuit breaker of previous designs. The limiting component with respect to SIL for the system is the PLC. Increasing the redundancy or the reliability of the switches or circuit breaker will not increase the system SIL. Lastly, the MTTFS for this ESD is 16.17 years.

TABLE VIII. SIL VERIFICATION OF A GENERIC PLC-BASED ESD.

Component	Architecture	Type	MTTFS (years)	PFD_{avg}
Switches	1oo2	A	47.56	3.9×10^{-5}
Generic PLC	1oo1	B	35.14	4.8×10^{-3}
Circuit breaker	1oo1	A	82.72	5.25×10^{-4}

E. A Safety PLC-based ESD system

This design example changes the generic, industrial PLC to a 1oo2D Safety PLC with diagnostics that is certified to SIL 3. Table IX lists the results from the SIL tool. The results show that when using a Safety PLC, the SIL = 3. The SIL was not restricted because of the Safety PLC has redundancy to tolerate one fault. Lastly, the MTTFS for this ESD is 26.17 years.

TABLE IX. SIL VERIFICATION FOR A SAFETY PLC-BASED ESD.

Component	Architecture	Type	MTTFS (years)	PFD_{avg}
Switches	1oo2	A	47.56	3.9×10^{-5}
Safetyl PLC	1oo2D	B	196.5	2.35×10^{-5}
Circuit breaker	1oo1	A	82.72	5.25×10^{-4}
Overall ESD	-	-	26.17	5.88×10^{-4}

VIII. SYSTEMATIC FAILURES

The safety integrity of a system consists of the hardware safety integrity and the systematic safety integrity. Hardware safety integrity is a function of random hardware failures and common cause failures; these are physical failures. Systematic safety integrity is a function of error such as operator error, software design errors, and maintenance errors; these are all functional failures.

Only hardware safety integrity has been considered up to this point. Systematic errors concerning software and the human operator are addressed in the following sections.

A. Software Integrity

Software failures result from systematic (functional) errors. The likelihood of systematic failures is very difficult to estimate; therefore, various processes and techniques are used in an attempt to avoid them. For instance, software safety life cycles have been established that address things such as software requirement specifications, software management of change procedures, and software verification and validation (V&V) methods[12].

The rigor of V&V and the expenditure of resources for systematic failure avoidance increases as the SIL increases. This is evident in software (V&V) techniques listed by Table X [12]. This table applies to the ESD software.

The development and assessment of safety-related software is beyond the scope of this paper. Safety-related software should be developed, verified and validated, documented, and maintained as recommended by the best practices for PE-based mining systems [12] and other standards [1].

TABLE X. SOFTWARE V&V ACTIVITIES FOR VARIOUS SILS [1][12].

V&V Method	SIL 1	SIL 2	SIL 3
Static Analysis:			
Requirements Review	Required	Required	Required
Design Review	Required	Required	Required
Code Review	Required	Required	Required
Structure Analysis	Not required	Required	Required
Boundary Value Analysis	Required	Required	Required
Control Flow Analysis	Not required	Required	Required
Data Flow Analysis	Not required	Not required	Required
Error Anomaly Analysis	Not required	Not required	Required
Functional Testing:			
Equivalence Partitions	Required	Required	Required
Boundary Values	Required	Required	Required
Special Values	Required	Required	Required
Random Testing	Not required	Not required	Required
Structural Testing:			
Statement Coverage	Required	Required	Required
Branch Coverage	Recommended	Required	Required
Multiple Condition Coverage	Not required	Required	Required
Decision-to-Decision Path	Not required	Not required	Required
Data Flow Coverage	Not required	Recommended	Required
Performance Testing	Required	Required	Required
Failure Mode and Stress Testing	Recommended	Required	Required
Modeling and Simulation:			
Structure Diagrams	Not required	Required	Required
Data Flow Diagrams	Not required	Required	Required
Finite State Machines	Not required	Required	Required.
Formal Models	Not required	Not required	Recommended
Performance Models	Not required	Not required	Required
State Models	Not required	Required	Required
Prototypes	Not required	Not required	Required
Symbolic Execution	Not required	Not required	Recommended
Formal Analysis	Not required	Not required	Recommended
Interface Testing	Required	Required	Required

B. Human reliability

Human reliability is critical because the human is a part of the system; the human must initiate the ESD. The human element poses significant limitations. For instance, a person might not recognize the need to activate the ESD or there could be situations in which a person would not be able to activate the ESD in time to prevent a mishap.

Human reliability analysis was used to determine human errors such that it can be factored into quantitative SIL verification. There are a number of practical methods for estimating human reliability such as HEART (human error assessment and reduction technique), THREP (Technique for human error rate prediction), and the method named TESO (empirical technique to estimate operator errors) [13].

Human reliability was calculated for the ESDs using TESO. Basically, TESO estimated the human error probability by the multiplication of five factors; the human task, time stress, operator expertise, anxiety, and ergonomic factors. TESO assigns probabilities for each factor based on a set of conditions specific to each factor. The human task to activate the ESD requires attention; so, the base error rate .01 was assigned for the first factor of human task. The other factors were assigned as time stress = 10 (high), operator expertise = 0.5 (expert), anxiety = 3 (emergency), and ergonomic factors = 1(good). Multiplying each factor results in an error probability of 0.15; thus, the human operator does not even achieve SIL 1. Therefore, the ESD will not meet SIL 3.

IX. SUMMARY AND DISCUSSION

The hardwired ESDs were simple in terms of design and safety verification. They required just a few components, they did not need software, and the safety verifications were straightforward in that simplified equations could be used to calculate PFD_{avg} and MTFFS. However, the hardwired 1oo1 ESD could only achieve SIL 2 with respect to the hardware safety integrity. The SIL could be increased to SIL 3 by increasing the reliability of the switch and adding 1oo2 switch redundancy. Although this met SIL 3, the MTTFS decreased over 50%. Lastly, neither hardwired ESD had any impact on the existing industrial PLC used for control purposes because both ESD designs followed good engineering practices to keep safety systems independent of control systems. Overall, the resources needed to design and verify each design would be anticipated to be relatively low.

Two PLC-based ESDs were presented. The first design used a generic PLC and the same 1oo2 switches from the hardwired ESD design that met SIL 3 with a MTFFS = 30.12 years; however, the generic, industrial PLC-based ESD only met SIL 1 with respect to the hardware safety integrity because the SIL was restricted given that the PLC did not have fault tolerance. Also, the MTFFS decreased about 50% to 16.17 years. The safety performance was increased to SIL 3 by using a safety PLC that was specially designed for safety-related applications. The Safety PLC also improved the MTFFS to 26.17 years. Lastly, both PLC-based ESDs had a significant impact on the rest of the system. The existing generic,

industrial PLC used for control purposes changed from a common PLC to a specialized Safety PLC that offered fault tolerance, better diagnostics, and better hardware failure reliability. Overall, the resources needed to design and verify each PLC-based design would be greater than the hardwired ESDs. First, Safety PLCs have a cost premium depending on the degree of fault tolerance, component reliability, and the diagnostic coverage. Both PLC-based ESDs would also require safety-related software that would require additional resources for design, V&V, documentation, and maintenance. Significant resources are needed for the software. This is especially apparent when inspecting the numerous software V&V activities of Table X.

X. CONCLUSIONS

It is apparent that a safety issue of importance should concern automatic verses human-activation of the ESD. None of the ESDs could attain an overall SIL 3 because manual activation was used. Human error was the limiting factor where the human achieved less than SIL 1; thus, the entire ESD did not meet SIL 1. Additional independent safety layers of protection are needed if any of the ESDs are to exceed SIL 1. The protection layers could consist of procedures, alarms, electrical protection devices, and other safety-related systems that do not require human activation.

Secondly, it is important to consider the architecture because it impacts the SIL and MTTFS as shown by Table II. Increasing the redundancy, regardless of the technology used, does not always improve safety performance.

Thirdly, it is not desirable, in terms of safety and economics, for one system to implement both control and safety functions. Safety systems such as ESDs should be independent of the control systems because a failure of the PLC would impact both the control and safety system. Also, for the examples presented, it does not appear to make economic sense to use the PLC for the ESD because adding the ESD safety function to the generic, industrial PLC used for control caused the entire PLC to be replaced with a more costly Safety PLC certified to SIL 3 even though the generic PLC was sufficient for control purposes.

Lastly, it is apparent that the ESD technology has a significant impact with respect to resources for design and safety verification. Both PLC-based ESDs would require more resources compared to the hardwired ESDs that did not need software. A detailed cost analysis is needed to quantify these differences.

REFERENCES

[1] IEC. “Functional safety of electrical/electronic/ programmable electronic safety-related systems, Part 3: software requirements”. International Electrotechnical Commission; 1998; IEC 61508-3.

[2] J.J. Sammarco, and T.J. Fisher, “Programmable electronic mining systems: best practice recommendations (In Nine Parts); Part 2: 2.0 system safety”. NIOSH; 2001; IC 9458.

[3] J.J. Sammarco, “Safety framework for programmable electronics in mining. Society of Mining Engineers”; 1999 Dec: 30-33.

[4] ISA. “Indentification of emergency shutdown systems and controls that are critical to maintaining safety in process industries”. The Instrument Society of America (ISA); 1995; ISA-S91.01-1995.

[5] A.A. Frederickson, “Comparison of programmable electronic safety-related system architectures”. [Web Page]. Available at: http://www.safetyusersgroup.com/info_service/default.asp?cat_id=1.200 Accessed 2005 Apr 25.

[6] OREDA. Offshore Reliability Handbook. 3rd ed. Norway: Det Norske Veritas; 1997.

[7] SINTEF. Reliability Data for Control and Safety Systems. Norway: SINTEF Industrial Management; 1989.

[8] Reliability Analysis Center. NPRD-95 Nonelectronic Parts Reliability Data. Rome, NY; 1995.

[9] Exida.com, Safety Equipment Reliability Handbook. Exida.com, LLC; 2003.

[10] IEC. “Functional safety of electrical/electronic/programmable electronic safety related systems, Part 5: examples of methods for the determination of safety integrity levels”. International Electrotechnical Commission; 1998; IEC 61508-5.

[11] ISA. Safety Instrumented Systems (SIS) -- Safety Integrity Level (SIL) Evaluation Techniques; Parts 1 to 5. Instrument Society of America; 1998 Apr; TR84.0.02.

[12] E.F. Fries, T.J. Fisher, and C.C. Jobes, “Programmable electronic mining systems: best practice recommendations (In Nine Parts); Part 3: 2.2 software safety”. Pittsburgh, PA: NIOSH; 2001; IC 9460.

[13] D.J. Smith, Reliability, Maintainability, and Risk. London, UK: Butterworth Heinemann; 2000.

BIOGRAPHY

Dr. John J. Sammarco is an Electrical Engineer with the National Institute for Occupational Safety and Health, U.S. Department of Health and Human Services. His Federal service has been devoted to mine safety research in a wide variety of areas including mining machine navigation and guidance, control systems, and sensors. His recent research areas concern system safety, hazard/risk analysis of processor-controlled mining systems, smart wireless sensors, and solid-state lighting systems for mine applications.