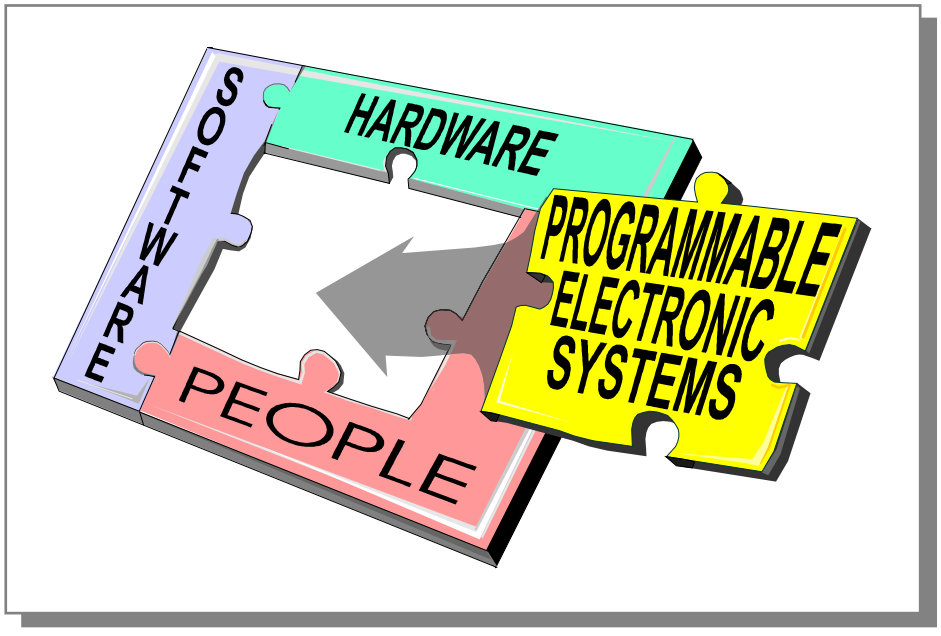
CDC
Workplace Safety and Health

IC 9480

INFORMATION CIRCULAR/2005

Programmable Electronic Mining Systems: Best Practice Recommendations (In Nine Parts)



Part 6: 5.1 System Safety Guidance

Department of Health and Human Services
Centers for Disease Control and Prevention
National Institute for Occupational Safety and Health

NIOSH

Information Circular 9480

Programmable Electronic Mining Systems: Best Practice Recommendations (In Nine Parts)

Part 6: 5.1 System Safety Guidance

By John J. Sammarco, Ph.D., P.E.

DEPARTMENT OF HEALTH AND HUMAN SERVICES
Centers for Disease Control and Prevention
National Institute for Occupational Safety and Health
Pittsburgh Research Laboratory
Pittsburgh, PA

August 2005

ORDERING INFORMATION

Copies of National Institute for Occupational Safety and Health (NIOSH) documents and information about occupational safety and health are available from

NIOSH–Publications Dissemination
4676 Columbia Parkway
Cincinnati, OH 45226–1998

FAX:513–533–8573
Telephone:1–800–35–NIOSH
(1–800–356–4674)
e-mail:pubstaft@cdc.gov
Website:www.cdc.gov/niosh

DISCLAIMER

The information presented in this document is for guidance and illustrative purposes. This document uses simplified examples so that readers can focus on the process and approach. The examples are for illustrative purposes only and do not represent a definitive treatise or recommended design.

This guidance information is not intended to promote a single methodology and is not intended be an exhaustive treatise of the subject material. It provides information and references such that the user can more intelligently choose and implement the appropriate methodologies given the user's application and capabilities.

Mention of any company or product does not constitute endorsement by the National Institute for Occupational Safety and Health (NIOSH). The fictitious names and products mentioned in this document are not meant as inferences to any company or product. In addition, citations to Web sites external to NIOSH do not constitute NIOSH endorsement of the sponsoring organizations or their programs or products. Furthermore, NIOSH is not responsible for the content of these Web sites.

DHHS (NIOSH) Publication No. 2005–150

CONTENTS

Page

CONTENTS–Continued

ILLUSTRATIONS

ILLUSTRATIONS–Continued

TABLES

ABBREVIATIONS USED IN THIS REPORT

AEA	action-error analysis
ANSI	American National Standards Institute
CM	continuous mining
DC	diagnostic coverage
EMI	electromagnetic interference
ETA	event-tree analysis
FAQs	frequently asked questions
FMEA	failure modes and effects analysis
FTA	fault-tree analysis
HAZOP	hazard and operability studies
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IPL	independent protection layer
ISA	The Instrumentation, Systems, and Automation Society
ISO	International Organization for Standardization
LOPA	layers of protection analysis
MCMS	mining control and monitoring system
MOC	management of change
MSHA	Mine Safety and Health Administration
MTBF	mean time between failure
MTTF	mean time to fail
MTTFS	mean time to fail safe (spurious)
MTTR	mean time to repair
NIOSH	National Institute for Occupational Safety and Health
O&SA	operating and support analysis
PE	programmable electronics
PES	programmable electronic system
PFD_{avg}	average probability of failure on demand
PHA	preliminary hazard analysis
PLC	programmable logic controller
RRF	risk reduction factor
SFF	safe failure fraction
SIL	safety integrity level
SIS	safety instrumented system
STEP	sequentially timed events plot
V&V	verification and validation

PROGRAMMABLE ELECTRONIC MINING SYSTEMS: BEST PRACTICE RECOMMENDATIONS (In Nine Parts)

Part 6: 5.1 System Safety Guidance

By John J. Sammarco, Ph.D., P.E.[1]

ABSTRACT

This report (System Safety Guidance 5.1) is the sixth in a nine-part series of recommendations and guidance addressing the functional safety of processor-controlled mining equipment. It is part of a risk-based system safety process encompassing hardware, software, humans, and the operating environment for the equipment's life cycle. Figure 1 shows a safety framework containing these recommendations. The reports in this series address the various life cycle stages of inception, design, approval and certification, commissioning, operation, maintenance, and decommissioning. These recommendations were developed as a joint project between the National Institute for Occupational Safety and Health and the Mine Safety and Health Administration. They are intended for use by mining companies, original equipment manufacturers, and aftermarket suppliers to these mining companies. Users of these reports are expected to consider the set in total during the design cycle.

• 1.0 *Safety Introduction (Part 1).*—This is an introductory report for the general mining industry. It provides basic system/software safety concepts, discusses the need for mining to address the functional safety of programmable electronics (PE), and includes the benefits of implementing a system/software safety program.

• 2.1 *System Safety (Part 2)* and 2.2 *Software Safety (Part 3).*—These reports draw heavily from International Electrotechnical Commission (IEC) standard IEC 61508 [IEC 1998a,b,c,d,e,f,g] and other standards. The scope is "surface and underground safety-related mining systems employing embedded, networked, and nonnetworked programmable electronics." System safety seeks to design safety into all phases of the entire system. Software is a subsystem; thus, software safety is a part of the system's safety.

• 3.0 *Safety File (Part 4).*—This report contains the documentation that demonstrates the level of safety built into the system and identifies limitations for the system's use and operation. In essence, it is a "proof of safety" that the system and its operation meet the appropriate level of safety for the intended application. It starts from the beginning of the design, is maintained during the full life cycle of the system, and provides administrative support for the safety program of the full system.

---

[1]Electrical engineer, Pittsburgh Research Laboratory, National Institute for Occupational Safety and Health, Pittsburgh, PA.

• 4.0 *Safety Assessment (Part 5).*—The independent assessment of the safety file is addressed. It establishes consistent methods to determine the completeness and suitability of safety evidence and justifications. This assessment could be conducted by an independent third party.

• *Safety Framework Guidance.*—It is intended to supplement the safety framework reports with guidance providing users with additional information. The purpose is to assist users in applying the concepts presented. In other words, the safety framework is *what needs to be done* and the guidance is *how it can be done*. The guidance information reinforces the concepts, describes various methodologies that can be used, and gives examples and references. It also gives information on the benefits and drawbacks of various methodologies. The guidance reports are not intended to promote a single methodology or to be an exhaustive treatment of the subject material. They provide information and references so that the user can more intelligently choose and implement the appropriate methodologies given the user's application and capabilities. The guidance reports comprise parts 6 through 9 of the series and are listed below:

- 5.1 *System Safety Guidance (Part 6).*—This guidance supplements 2.1 *System Safety*.
- 5.2 *Software Safety Guidance (Part 7).*—This guidance supplements 2.2 *Software Safety*.
- 6.0 *Safety File Guidance (Part 8).*—This guidance supplements 3.0 *Safety File*.
- 7.0 *Independent Functional Safety Assessment Guidance (Part 9).*—This guidance supplements 4.0 *Independent Functional Safety Assessment*.

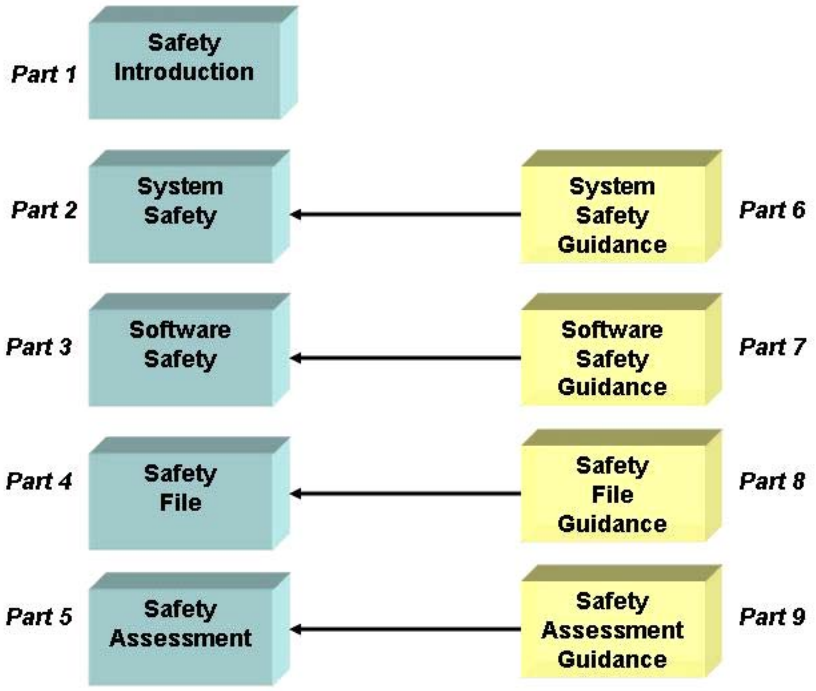


Figure 1.—The safety framework and associated guidance.

ACKNOWLEDGMENTS

The author thanks the System Safety Mining Industry Workgroup for reviewing and providing practical, constructive feedback for this and all previous recommendation documents. Members of the workgroup are listed below.

Name	Company
Anson, Jerry	P&H Mining Co.
Antoon, John[1]	Pennsylvania Bureau of Deep Mine Safety
Ceschini, Bob[1]	Pennsylvania Bureau of Deep Mine Safety
Cooper, David	Forced Potato
Cumbo, Terry	Line Power
Dechant, Fabian	Matric Ltd.
De Kock, Andre	ADK Systems
Erdman, Paul	Joy Mining Machinery
Ferguson, Dan[1]	DBT America, Inc.
Fidel, Mike	Eastern Associated Coal
Fisher, Tom[1]	NIOSH
Flemmer, Mike	NIOSH
Flynn, Chris[1]	Joy Mining Machinery
Flynt, Janet[1]	SSTS, Inc.
Fries, Edward F.[1]	NIOSH
Honaker, Jim[1]	Eastern Associated Coal
Kelly, Gene	MSHA, Coal Mine Safety and Health, District 2
Kenner, Jim	Wisdom Software
Ketler, Al	Rel-Tek Corp.
Koenig, Johannes	Marco
Kohart, Nick[1]	MSHA, Coal Mine Safety and Health, District 2
Lee, Larry	NIOSH
Lewetag, David C.[1]	MSHA, Coal Mine Safety and Health, District 2
Lowdermilk, Scott	Cattron, Inc.
Martin, Jim[1]	Rad Engineering
Murray, Larry	Marco North America, Inc.
Nave, Mike[1]	Consol, Inc.
Oliver, David	Cutler-Hammer Automation
Paddock, Bob[1]	Independent Consultant
Paques, Joseph-Jean[1]	Institut de Recherche Robert-Sauvé en Santé et en Sécurité du Travail (IRSST) (Montreal, Quebec, Canada)
Podobinski, Dave	DBT America
Rhoades, Randy	CSE Corp.
Rudinec, Steve	Oldenburg Group, Inc.
Sammarco, John J.[1]	NIOSH
Schmidt, John[1] (retired)	DBT America
Sturtz, Doug[1]	Matric Ltd.
Van der Broek, Bert	Forced Potato
Watzman, Bruce	National Mining Association
Willis, John	Mitsubishi

[1]Workgroup meeting attendee.

The author also thanks David C. Chirdon, Gerald D. Dransite, and Chad Huntley with the Mine Safety and Health Administration's (MSHA) Approval and Certification Center, Triadelphia, WV, for their assistance in developing this series of reports. In addition, the author acknowledges and thanks E. William Rossi, Industrial Engineering Technician, NIOSH Pittsburgh Research Laboratory, for creating artwork for this publication.

BACKGROUND

The mining industry is using programmable electronics (PE) technology to improve safety, increase productivity, and improve mining's competitive position. It is an emerging technology for mining that is growing in diverse areas, including longwall mining systems, automated haulage, mine monitoring systems, and mine processing equipment. Although PE provides many benefits, it adds a level of complexity that, if not properly considered, may adversely affect worker safety [Sammarco et al. 1997]. This emerging technology can create new hazards or worsen existing ones. PE technology has unique failure modes that are different from mechanical systems or hard-wired electronic systems traditionally used in mining.

The use of a safety life cycle helps to ensure that safety is applied in a systematic manner for all phases of the system, thus reducing the potential for systematic errors. It enables safety to be "designed in" early rather than being addressed after the system's design is completed. Early identification of hazards makes it easier and less costly to address them. The life cycle concept is applied during the entire life of the system since hazards can become evident at later stages or new hazards can be introduced by system modifications. The safety life cycle for mining is an adaptation of the safety life cycle in part 1 of IEC 61508 [IEC 1998a].

System safety activities include identifying hazards, analyzing the risks, designing to eliminate or reduce hazards, and using this approach over the entire system life cycle. These system safety activities start at the system level and flow down to the subsystems and components. More detailed information on the fundamentals of system safety is presented by Sammarco et al. [2001]. Additional resources for PE safety are given in Appendix A.

1.0 Introduction

1.1 The Safety Life Cycle

The safety life cycle is a core concept throughout the System Safety document 2.1 [Sammarco and Fisher 2001]. Section 5.0 of that document gives an overview of the safety life cycle. The various life cycle phases are listed and briefly described in Table 1 below.

Table 1.—Safety life cycle overview
(adapted from IEC [1998a])

Life cycle phase	Objectives
1. Define scope	To determine the boundaries for the PE system and to bound the hazard and risk analysis.
2. Hazards and risk analysis	To identify and analyze hazards, event sequences leading to hazards, and the risk of hazardous events.
3. Overall safety requirements	To specify the safety functions and associated safety integrity for the safety system(s).
4. Designate safety-critical areas	To assign safety functions to various PE-based and non-PE-based safety systems and protection layers. To assign safety integrity levels (SILs).
5. Operation and maintenance plan	To plan how to operate, maintain, and repair the PE-based safety system to ensure functional safety.
6. Safety validation plan	To plan how to validate that the PE-based safety system meets the safety requirements.
7. Installation and commissioning plan	To plan how to install and commission the PE-based safety system in a safe manner and to ensure that functional safety is achieved.
8. Management of change plan	To plan how to ensure that changes will not adversely impact functional safety. To plan how to systematically make and track changes.
9. Design for safety systems	To design and create the PE-based safety system. To follow safety practices for the PE-based safety system and the basic system design.
10. Additional safety technology	As needed; not within the scope of this report.
11. External risk reduction	As needed; not within the scope of this report.
12. Install and commission	To install and commission the safety system properly and safely.
13. Validate	To carry out the safety validation plan.
14. Operate and maintain	To operate, maintain, and repair the PE-based safety system so that functional safety is maintained.
15. Modifications	To make all modifications in accordance with the management of change plan.
16. Decommission	To ensure the appropriate functional safety during and after decommissioning.

1.2 Scope

1.2.1 Surface and underground mining systems using PE for control or monitoring of safety-critical mining systems and functions are within the scope. It is not intended to apply to handheld instruments; however, many of these principles would be useful in designing and assessing this equipment.

1.2.2 Systems, protection layers, and devices using PE that are associated with the system are within the scope. These include—

- Mining control and monitoring systems (MCMSs) using PE
- Safety instrumented systems (SISs)
- Critical alarms

1.3 General

1.3.1 This guidance does not supersede federal or state laws and regulations.

1.3.2 This guidance is not equipment- or application-specific.

1.3.3 This guidance is informative; it does not serve as a compliance document.

1.3.4 This guidance applies to the entire life cycle for the mining system.

1.3.5 This guidance applies mainly to the safety-related parts of the system. However, the guidance can also be applied to the basic system.

2.0 Key Documents

2.1 This guidance document is based on information and concepts from the recommendation documents Introduction 1.0 [Sammarco et al. 2001] and System Safety 2.1 [Sammarco and Fisher 2001].

3.0 Definitions

The definitions are directly from IEC 61508, part 4 [IEC 1998d]. Some definitions are adaptations or newly formed definitions specific to mining.

Channel – Components or subsystems operating together to perform a function. Components and subsystems within a channel include input/output modules, logic systems, sensors, power systems, and final elements.

Common Cause Failure – A failure resulting from one or more events, causing coincident failure of two or more channels of a multichannel system, thus leading to system failure.

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

Dangerous Failure Detected – A failure detected by diagnostic tests such that the system will be placed into a safe state.

Dangerous Failure Undetected – A failure not detected by diagnostic tests such that the system has the potential to result in harm.

NOTE 1: The probability of a dangerous failure is λ_D; the probability of a dangerous failure detected is λ_{DD}; the probability of a dangerous failure undetected is λ_{DU}.

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

NOTE 2: The definition may also be represented in terms of the following equation:

$$DC = \frac{\Sigma \lambda_{DD}}{\Sigma \lambda_{total}} \ , \tag{1}$$

where DC is the diagnostic coverage,
λ_{DD} is the probability of detected dangerous failures,
and λ_{total} is the probability of total dangerous failures.

NOTE 3: Diagnostic coverage may exist for the whole or parts of a safety-related system. For example, diagnostic coverage may exist for sensors and/or logic system and/or final elements.

NOTE 4: The term "safe diagnostic coverage" is used to describe the decrease in the probability of safe hardware failures resulting from the operation of the automatic diagnostic tests.

Dual Channel – Two channels that independently perform the same function.

Error – A discrepancy between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition.

Failure – The termination of the ability of a functional unit to perform a required function.

Fault – An abnormal condition or state that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function.

NOTE 5: A "failure" is an event.

NOTE 6: A "fault" is a state. Faults are random or systematic.

Field Devices – Field devices include sensors, transmitters, operator interface devices (e.g., displays, control panels, pendant controllers), actuators, wiring, and connectors. Field devices are peripheral devices hard-wired or connected by a wireless link to the input/output terminals of a logic system.

Hazard – Environmental or physical condition that can cause injury to people, property, or the environment.

Human-Machine Interface – The physical controls, input devices, information displays, or other media through which a human operator interacts with a machine for the purpose of operating the machine.

Mean Time Between Failure (MTBF) – The expected average time between failures of a repairable system where MTBF = MTTF + MTTR.

Mean Time to Fail (MTTF) – The expected time that a system will operate before the first failure occurs. MTTF includes safe and dangerous failure modes.

Mean Time to Repair (MTTR) – The average value of the time to detect and identify a failure plus the time to repair the failure.

Mining Control and/or Monitoring System (MCMS) – A system using programmable electronics (PE), that responds to input signals from the equipment under control and/or from an operator and generates output signals, causing the equipment under control to operate in the desired manner.

Mishap – An unplanned event or series of events resulting in death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment. In the real world, complete freedom from adverse events is not possible. Therefore, the goal is to attain an acceptable level of safety.

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

Programmable Electronics (PE) – Refers to electronically programmable or configurable devices (e.g., embedded controller, programmable logic controller, single-loop digital controller, distributed control system controller) that are effectively the "brain" of a PE system.

Programmable Electronic System (PES) – Any system used to control, monitor, or protect machinery, equipment, or a facility that has one or more programmable electronics (PE), including all elements of the system such as power supplies, sensors and other input devices, data highways and other communications paths, and actuators and other output devices.

Random Hardware Failure – A failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware.

NOTE 7: There are many degradation mechanisms occurring at different rates in different components. Since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates, but at unpredictable (i.e., random) times.

NOTE 8: A major distinguishing feature between random hardware failures and systematic failures is that system failure rates (or other appropriate measures) arising from random hardware failures can be predicted with reasonable accuracy, but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy, but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot be easily predicted.

Risk – The combination of the probability of occurrence of harm and severity of that harm.

Risk Reduction Factor (RRF) – A measure of lowering the probability of an event from happening. RRF = inherent risk/acceptable risk, or RRF = 1/PFD.

Safe Failure – A failure that does not have the potential to put the safety-related system in a dangerous or fail-to-function state.

NOTE 9: A safe failure is also known as a nuisance failure, false-trip failure, spurious failure, or fail-to-safe failure. The probability of a safe failure is $\lambda_{S.}$

Safe Failure Fraction (SFF) – A measure used for determining minimal redundancy levels where:

$$\text{SFF} = \frac{\Sigma\lambda_S + \Sigma\lambda_{DD}}{\Sigma\lambda_S + \Sigma\lambda_D} \tag{2}$$

or

$$\text{SFF} = 1 - \frac{\Sigma\lambda_{DU}}{\Sigma\lambda_S + \Sigma\lambda_D} \tag{3}$$

Safety – Freedom from unacceptable risk.

Safety Function – A function implemented by single or multiple MCMSs, protection layers, and devices using PE intended to achieve or maintain a safe state for a specific hazardous event.

Safety Instrumented System (SIS) – System composed of sensors, logic solvers, and final control elements for the purpose of taking the mining system to a safe state when predetermined conditions are violated. Other terms commonly used include "emergency shutdown system," "safety shutdown system," and "safety interlock system."

Safety Integrity Level (SIL) – One of three possible discrete integrity levels (SIL 1, SIL 2, SIL 3) of safety instrumented functions. SILs are defined by quantitative or qualitative methods. SIL 3 has the highest level of safety integrity (see Tables 2–3).

Table 2.—Assignment of SIL values for low-demand modes of operation

SIL	Probability of failure on demand average range (PFD_{avg})	Risk reduction factor (RRF)	Qualitative methods
1	10^{-1} to 10^{-2}	10– 100	Method-dependent.
2	10^{-2} to 10^{-3}	100– 1,000	Method-dependent.
3	10^{-3} to 10^{-4}	1,000–10,000	Method-dependent.

Table 3.—Assignment of SIL values for high-demand (continuous) modes of operation

SIL	Probability of failure on demand average range (PFD_{avg})	Risk reduction factor (RRF)	Qualitative methods
1	10^{-5} to 10^{-6}	100,000– 1,000,000	Method-dependent.
2	10^{-6} to 10^{-7}	1,000,000– 10,000,000	Method-dependent.
3	10^{-7} to 10^{-8}	10,000,000–100,000,000	Method-dependent.

NOTE 10: SILs apply to safety functions of systems, protection layers, and devices using PE.

NOTE 11: A low-demand mode of operation is when the safety-related system's frequency of operation is less than once per year or no greater than twice the frequency of tests (proof tests) to detect failures in the safety-related system. A high-demand mode of operation is when the safety-related system's frequency of operation is more than once per year or greater than twice the frequency of tests (proof tests) to detect failures in the safety-related system.

Safety Life Cycle – The necessary activities involved in the implementation of safety-critical systems. The activities begin at the concept stage and cease after the systems' decommissioning.

System – Set of elements that interact according to a design, where an element of a system can be another system, called a subsystem, which may be a controlling system or a controlled system and may include hardware, software, and human interaction. Hardware, software and humans can be system elements.

Systematic Failure – A failure related to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation, or other relevant factors.

NOTE 12: Corrective maintenance without modification will usually not eliminate the failure cause.

NOTE 13: A systematic failure can be induced by simulating the failure cause.

NOTE 14: Example causes of systematic failures include human error in the—
- Safety requirements specification
- Design, manufacture, installation, operation of the hardware
- Design, implementation, etc., of the software

Subsystem – An element of a system.

Total Failures – The combination of all safe and dangerous failures where:

$$\lambda_{total} = (\Sigma\lambda_S + \Sigma\lambda_D) \quad (4)$$

Validation – The activity of demonstrating that the safety system under consideration, before or after installation, meets in all respects the safety requirements specification for that safety system.

Verification – The activity of demonstrating for each phase of the relevant safety life cycle by analysis and/or tests that, for the specific inputs, the deliverables meet in all respects the objectives and requirements set for the specific phase.

4.0 Hazards and Risk Analysis

The objective of hazards and risk analysis is to identify and analyze hazards, the event sequences leading to hazards, and the risk of hazardous events. Many techniques, ranging from simple qualitative methods to advanced quantitative methods, are available to help identify and analyze

hazards. The use of multiple hazard analysis techniques is recommended because each has its own purpose, strengths, and weaknesses.

The *System Safety Analysis Handbook* [Stephans and Talso 1997] provides extensive listings and descriptions of hazard analysis techniques. Some of the more commonly used techniques include preliminary hazard analysis (PHA), failure modes and effects analysis (FMEA), hazard and operability studies (HAZOP), fault-tree analysis (FTA), and event-tree analysis (ETA).

4.1 Preliminary Hazard Analysis (PHA)

Summary: An analysis technique used in the early conceptual stages of design and development. A sample PHA form is shown in Appendix C.

Discussion: The PHA is frequently used early in the conceptual stages prior to design completion. Typically, a team is used to identify potential hazards of the main system and possibly some of the major subsystems. It is used when there is limited information. Therefore, it is a high-level analysis and is not considered final. The PHA output can include ranking of hazards, operational constraints, recommended actions to eliminate or control the hazards, and perhaps additional safety requirements.

A PHA can utilize information including the results of the preliminary hazard list, lessons learned, system and component design data, safety design data, and malfunction data to identify potential hazard areas. PHA does not designate a specific technique; however, checklists and forms are commonly used.

Advantages:
- Useful at conceptual stages
- Relatively quick to implement

Disadvantage:
- Cannot be used to extensively identify and analyze hazards

Mastery: Requires knowledge, experience, and understanding of the application.

4.2 Failure Modes and Effects Analysis (FMEA)

Summary: This analysis identifies failures of components, subsystems, and their effects on the system. In essence, it is a "bottom-up" approach starting with the system's components. The standard, *Procedures for Performing a Failure Mode Effects and Criticality Analysis* [U.S. Department of Defense 1980], provides detailed information on FMEA.

Discussion: This is a systematic technique to identify and analyze safety-critical components and subsystems of a system. FMEA is most effectively conducted during the design phase, thus enabling system design modifications to eliminate critical components or subsystems. Generally, the tabular format or spreadsheet is used. A sample FMEA form is shown in Appendix C. Usually, the analysis is conducted by a few engineers having a detailed understanding of the system and of the various

failure modes for each component and subsystem. Some typical failure modes of mechanical and electronic components are as follows:

- Failure to open or close
- Failure to start or stop
- Short- or open-circuit failure
- Increased or decreased resistance, inductance, capacitance
- Stuck
- Leaking
- Clogged
- Corroded

The following are the basic steps to conduct an FMEA:

(1) Identify the system's components and subsystems
(2) Determine all failure modes for each component and subsystem
(3) Identify the consequences of each failure
(4) Identify elimination or mitigation of failure

Advantages:

- Analysis procedure is simple to understand
- The FMEA tabular results are relatively easy to understand
- Good for situations where a component failure has a major system level safety consequence

Disadvantages:

- Does not identify common-cause failures
- Does not identify multiple failure combinations
- Human errors during operation and maintenance might be missed
- Can be time-consuming for large, complex systems

Mastery: The difficulty to understand the method is relatively low.

4.3 Hazard and Operability Studies (HAZOP)

Summary: A systematic and structured qualitative method of study conducted by a multidisciplinary team. Guide words are applied to various parameters to stimulate thinking concerning possible deviations. As a result of these deviations, potential hazards and causes are identified. Multiple sources provide detailed information about HAZOP [U.K. Ministry of Defence 1998a,b; Redmill et al. 1999]. A sample HAZOP form is shown in Appendix C.

Discussion: HAZOP had its beginnings in the chemical process industry where guide words were designated for process industry parameters such as flow and pressure. HAZOP can be applied to a system, subsystem, process, or procedure and also to hardware and software. HAZOP can be easier to implement at the later stages when designs are firm rather than at conceptual phases. Thus, it is also well suited for hazard identification and analysis of modifications during the management of change (MOC) process.

HAZOP has been extended for the hardware and software of programmable systems [U.K. Ministry of Defence 1998a,b; Redmill et al. 1999]. Hardware and software include:

Hardware:
- Analog hardware
- Digital hardware
- Communications
- Electrohydraulic subsystems
- Electromechanical subsystems
- Miscellaneous hardware (e.g., wires, connectors)

Software:
- Software data flow diagrams
- Software state transition diagrams
- Entity relationship diagrams

Guide words are extended with: *early*, *late*, *before*, *after*. Table 4 lists generic and extended guide words, along with the guide word interpretations. Guide words can be customized for the user's application and system. The guide words are applied to system and subsystem attributes to identify deviations from the design intent that might create a hazard.

Table 4.—HAZOP guide word interpretations

Guide word	Standard interpretation	PES interpretation
No	No part of the intention is achieved	No data or control signal passed.
More	A quantitative increase	More data is passed than intended.
Less	A quantitative decrease	Less data is passed than intended.
As well as	All design intent achieved, but with additional results	Not used here because this is already covered by "more".
Part of	Only some of the intention is achieved	The data or control signals are incomplete.
Reverse	Covers reverse flow in pipes and reverse chemical reactions.	The logical opposite of intention.
Other than	A result other than the original intention is achieved	The data or control signals are complete, but incorrect.
Early	Not used	The signal arrives too early with reference to clock time.
Late	Not used	The signal arrives too late with reference to clock time.
Before	Not used	The signal arrives earlier than intended within a sequence.
After	Not used	The signal arrives later than intended within a sequence.

The HAZOP should be applied throughout the safety life cycle. Early in the life cycle, HAZOP should be applied to block diagrams; as the design progresses, HAZOP should be applied to other system representations, such as electrical schematic diagrams. Many different types of design representations exist. HAZOP can be applied to the following design representations:

- Block diagrams (electrical, mechanical, hydraulic, etc.)
- Schematic diagrams (electrical, mechanical, hydraulic, etc.)
- State transition diagrams
- Data flow diagrams

- Object-oriented diagrams
- Timing diagrams
- Operating instructions
- Operating tasks
- Maintenance tasks

HAZOP should also be applied at the subsystem levels. This includes the electromechanical subsystem, electrical communication subsystem, electronic hardware, and the software. Table 5 lists HAZOP guide words for electrical wiring [Redmill et al. 1999].

Table 5.—Example guide word interpretations for electric wiring

Guide word	Example interpretation for electrical wiring
No	Broken or missing wire or connection.
More	Excessive voltage or current.
Less	Undervoltage or current condition.
As well as	Noise, interference, or EMI in addition to desired signals.
Part of	NA
Reverse	Circuit polarity is connected backwards or the opposite of the intention.
Other than	Wrong wire or signal.
Early	NA
Late	NA
Before	NA
After	NA

NA Not applicable.

HAZOP is a team-based, qualitative technique that uses guide words applied to parameters in order to discover deviations from the intended design. The team should be a multidisciplinary collection of people from technical, organizational, and operational groups. The people are typically highly qualified by extensive knowledge and experience. Typically, five or six persons are on the team. A team might be composed of the following:

- Team leader
- Senior designer
- Safety person
- Operation and maintenance person
- End user
- Project manager

The length of time to conduct a HAZOP study depends on the size and complexity of the system. For a small system, it may take a day of preparation and a few days to conduct the team sessions. A large and complex system may take several days of preparation and a few weeks to conduct the sessions. It is important for the team leader to keep the team focused on the important safety topics and sections and to help ensure that common sense and logic prevails. It is very important that a common pitfall to HAZOP be recognized and dealt with. Often, the study can become quite lengthy, causing the members to lose interest and commitment. This can result if the team tries to go into too much detail or tries to be too comprehensive.

Advantages:

- Very good track record of prior use and success
- Can produce detailed and comprehensive results
- Does not require extensive training or specialized tools

Disadvantages:

- Can be time-consuming for large and complex systems
- Best for short time periods of use because team members can lose effectiveness

Mastery: The difficulty to understand the method is relatively low.

4.4 Fault-tree Analysis (FTA)

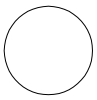
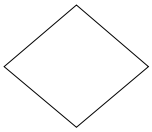
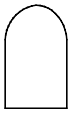
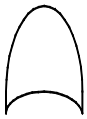
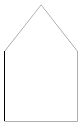
Summary: A logical "top-down" method of structuring events and failures leading to a hazard. The *Fault-tree Handbook* [Vesely et al. 1981] provides detailed information on FTA.

Discussion: FTA is a logical method of deduction utilizing a graphical depiction of events, faults, or logical combinations (Boolean expressions such as AND, OR, etc.) thereof. It begins at the top of the fault tree with an undesirable event. Next, the possible events and logical combinations are developed for the fault tree until the root causes are determined. The root causes can be triggering events or basic faults. It is best to use fault trees on the major events because the trees can grow quite large. FTA can be applied to hardware and to operational modes of the system (i.e., startup, operation, maintenance, and shutdown).

Fault trees are suited to analysis of static situations; thus, dynamic situations involving timing are difficult to implement. Also, fault trees can be qualitative or quantitative. A quantitative fault tree uses probabilities for the events and faults. Finally, the traditional fault tree for the system hardware has been extended to software fault-tree analysis. This is best suited for analysis of the most critical software at the module level of detail.

There is a standard set of graphical symbols to construct the tree. Additional symbols are used for special situations. For example, "transfer in" and "transfer out" symbols are used to enable transition between multiple pages of fault trees. The basic symbols used to construct fault trees are shown in Table 6.

Table 6.—Basic fault-tree symbols

	Event or fault
	Basic event or fault
	Incomplete event or fault
	Inhibit gate
	AND gate
	OR gate
	Trigger event

Advantages:

- Identifies multiple failures
- Identifies multiple events and sequences leading to a hazard
- Identifies common causes
- Provides valuable documentation to aid investigations of mishaps
- Suitable for hardware or software

Disadvantages:

- Can become time-consuming if trees grow very large
- Not suited for timing (dynamic) situations

Mastery: Requires a moderate degree of training and skill to construct qualitative trees; quantitative FTA requires additional training in probability and cut sets.

4.5 Event-tree Analysis (ETA)

Summary: A logical, bottom-up graphical technique to determine outcomes from a single initiating hazardous event.

Discussion: The event tree is useful for determining the probability of each unwanted outcome resulting from a single initiating event. From this, one can determine which outcomes are the most severe or occur with the greatest frequency. Figure 2 depicts a simple event tree. The event tree starts with a single initiating event, a severed hydraulic line, and a frequency of event occurrence of .01 events per year (i.e., once every 100 years). The safety control measures associated with the system are used as headings across the top of the tree. The initiating event is then sequenced through the event tree with the associated control measures. Each control measure has two paths—operate or fail. Probabilities are determined for each of these paths.

Advantages:

- Well suited for single events with multiple outcomes
- Suited for high risks not amenable to simpler analysis methods

Disadvantages:

- Trees can grow large very quickly
- Probabilities may be difficult to estimate
- Can be extremely time-consuming

Mastery: ETA is one of the more demanding analysis methods.

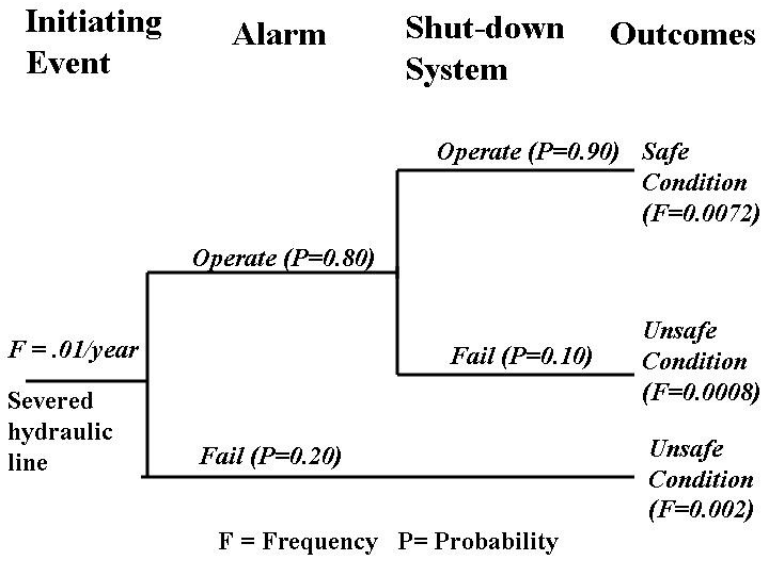


Figure 2.—A basic event tree.

4.6 Potential or Predictive Human Error Analysis

Summary: A team-based method similar in concept to HAZOP; however, this analysis focuses on human tasks and the associated error potential [Center for Chemical Process Safety 1994].

Discussion: Human error causes fall into the following basic categories:

- Complexity – increases the likelihood of error
- Stress – increases the likelihood of error
- Fatigue – increases the likelihood of error
- Environment – adverse environments increase the likelihood of error
- Training – better training reduces the likelihood of error

The members of the team conducting the analysis should consider these error causes as they conduct the analysis. The basic procedure is as follows:

- Identify key human tasks
- Apply the following guide words for each task:
  - Action omitted
  - Incomplete action
  - Incorrect action timing
  - Wrong action
  - Wrong action sequence
  - Wrong selection
  - Action applied to the wrong interface object

A worksheet can be used to document the results. It should include the following information:

- Task
- Error guide word(s)
- Description
- Error consequence
- Strategy to prevent or reduce the error consequence

Advantages:

- The method can identify many potential errors
- Validation studies show that a high portion of errors can be identified by thorough application of the method

Disadvantages:

- Can be time-consuming if many tasks and actions exist
- Effectiveness depends on the team's expertise and effort

Mastery: Requires a high level of team expertise concerning the system.

4.7 Operating and Support Analysis (O&SA)

Summary: Operating and Support Analysis seeks to identify hazards during operation and maintenance, find the root causes, determine the acceptable level of risk, and recommend risk reductions [Harms-Ringdahl 1993].

Discussion: An understanding of the operations, environment, and support (maintenance) philosophy (i.e., training, implementation, etc.) that will be part of the mining process needs to be analyzed. The Operating and Support Analysis (O&SA) is used to identify hazards that may occur. The O&SA is conducted by a team familiar with the system's operation and interaction with humans. Some of the items to be considered include:

- Operating during normal and abnormal conditions
- Making changes to the system
- Maintaining the equipment and software
- Testing of the systems
- Training personnel on the use and maintenance of the systems
- Providing adequate documentation for the systems

Advantages:
- Provides hazard identification in the context of the entire system operation

Disadvantages:
- Requires a high level of expertise concerning the system

Mastery: Requires a high level of expertise concerning the system

4.8 Action-Error Analysis (AEA)

Summary: Action-error analysis (AEA) is used to identify operator errors and the subsequent consequences. AEA specifically focuses on the interactions between humans and the system during operation, maintenance, and testing [Harms-Ringdahl 1993].

Discussion: The basic procedure is outlined as follows for operation and maintenance tasks:

- Identify operator tasks
- Detail the subtasks and actions for each task
- For each action, identify potential operator errors and consequences. As a guide, the following error types are considered for each action:
  - Error of omission (action not taken)
  - Wrong sequence of actions
  - Temporal errors (actions taken late or early)
  - Incorrect actions taken
  - Actions applied to the wrong interface object

Advantages:
- Well suited for automated or semiautomated processes with operator interfaces

Disadvantages:
- Requires a high level of expertise concerning the system

Mastery: Requires a high level of expertise concerning the system

4.9 Interface Analysis

Summary: Interface analysis is used to identify hazards resulting from physical, functional, logical, and temporal interface incompatibilities.

Discussion: Interface analysis is applicable to all systems and interfaces. Numerous interfaces exist such as human-machine, hardware-software, hardware-hardware, and system-environment. The types of interface incompatibilities include:

- Environmental (temperature, moisture, dust, and vibration)
- Electrical (EMI, power sources, supply voltages, and data signals)
- Physical (rate and range of movement)
- Logical (conditional responses based on Boolean expressions)
- Temporal (clock times, response times, and delay times)

Incompatibilities can exist between adjacent, interconnected, interdependent, or interacting system elements.

Advantages:
- Applicable to all systems
- Applicable to all types of interfaces
- Applicable at the subsystem to the component level

Disadvantages:
- Difficult to apply to large or complex systems
- Difficult to find all types of interface incompatibilities for every operation

Mastery: Requires a high level of expertise in diverse areas.

4.10 Sequentially Timed Events Plot (STEP) Investigation System

Summary: STEP is an event-driven approach to define systems, analyze operation, and investigate mishaps.

Discussion: STEP is an analytical approach that graphically depicts sequentially timed events. Events are defined with formatted “building blocks” composed of an “actor and action.” The event blocks are sequentially linked to graphically depict the flow of events that produce an outcome. The

graphical depiction is useful for analyzing and defining events for a given system. STEP analysis can help discover and analyze problems; the analysis is also useful for assessing mitigation options. STEP is also used to analyze the types and sequences of events that lead to an incident.

Advantages:

- Can be applied to define and systematically analyze complex systems or processes
- Facilitates focus group analysis

Disadvantages:

- Perceived as complicated and expensive to implement

Mastery: Requires the ability to translate a system into a sequence of interrelated events. Requires good visualization and deductive logic skills.

5.0 Risk Assessment and Safety Integrity Level Determination

Once a hazard or hazardous event is identified and analyzed, the next step is to determine the associated risk. The level of risk is used to determine which hazards have an unacceptable risk and which have acceptable risks. Once the risks are identified, the safety performance or degree of safety to mitigate risk is determined. The safety performance is quantified by assignment of a level 1, 2, or 3, where 3 is the highest degree of safety performance. These levels are called safety integrity levels (SILs).

It is important to understand that the SIL specifies the safety performance of a safety-related system function to reduce a given risk to an acceptable level.

NOTE 15: For example, a machine has a moving part that is controlled by a PES. There is pinching hazard associated with the part's movement. It is determined that there is a low, but unacceptable level of risk for this hazard and that a safety function is needed to mitigate this risk. The safety function's safety performance is determined to be an SIL 1.

Risk assessment systematically enables the "ranking" of risks such that efforts can be focused to eliminate risks or reduce the risks to an acceptable level. Some risks might be classified as acceptable because they are insignificant or deemed to be at a level that is reasonably practical to assume. For example, not every single risk associated with driving a car is eliminated, yet most of us are willing to accept these risks or we wouldn't be driving cars.

Typically, risk is defined as the product of severity and frequency. Qualitative and quantitative methods are used to systematically assess risk. These methods have advantages and disadvantages. Qualitative risk assessment techniques are relatively simple to understand. They are subjective and the results may vary depending on the person or team of people conducting the risk assessment. These variations result because of variations in experience, knowledge, expertise, and individual perceptions of risk. Quantitative risk assessment is a rigorous technique based on statistical data. It requires highly trained and experienced people as well as large quantities of statistical data. One negative is that the data may not be available. Secondly, the data that are available might not be an

accurate representation for a mining application because it might not have been obtained for similar conditions of dust, moisture, or vibration.

Some of the common qualitative and quantitative techniques are described next. It is the user's responsibility to select the risk assessment technique that is suitable for the application and user's expertise. The risk assessment focus is on safety; however, it is beneficial to consider other types of risk because they may indirectly affect safety. For example, risks to the equipment or mine can indirectly affect the safety of those people that make the repairs.

5.1 Qualitative Techniques

Qualitative techniques are applicable when it is not feasible to quantify risk. Common qualitative techniques include the risk assessment matrix, hazardous event severity matrix, and the risk graph. These techniques vary in terms of the type and detail of available information. The risk assessment matrix [U.S. Department of Defense 1993] is the simplest. Risk is determined by using severity and frequency. The hazardous event severity matrix [IEC 1998f] is similar to the risk matrix, but it also takes independent layers of protection into account (section 5.6.2 gives an example of a layers of protection analysis). The risk graph uses severity and frequency, but it takes two additional parameters into account.

The risk matrix is quite similar to the hazardous event severity matrix. This qualitative method enables the determination of a risk index. The safety integrity level (SIL) can be determined by using the risk index. For each hazard, this basic process is used:

- Determine severity category
- Determine frequency category
- Determine the risk level
- Relate the risk to the SIL

5.2 Severity Categories

Severity categories are defined to provide a qualitative measure of the worst credible accident resulting from human error, environmental conditions, design inadequacies, procedural deficiencies, and system, subsystem, or component failure. Table 7 lists examples of several severity categories.

Table 7.—Broadly defined severity category examples

Category	Broad definitions
Catastrophic	Death, system loss, severe mine or environmental damage.
Critical	Severe injury, severe occupational illness, major system damage, or major mine or environmental damage.
Marginal	Moderate injury, moderate occupational illness, minor system damage, or minor mine or environmental damage.
Negligible	Minor injury, minor occupational illness, less than minor system damage, or less than minor mine or environmental damage.

The severity categories in Table 7 are broad, encompassing severity with respect to personnel safety and health as well as equipment, mine, and environmental damage. The main focus of this document is on personnel safety; therefore, the severity category examples in Table 8 are more definitive for mining.

Table 8.—Severity category examples specific to mine safety

Category	Example definitions for safety
Catastrophic . . .	Death or multiple deaths.
Critical	Severe injury, permanent disability (partial or total).
Marginal	Moderate injury, medical treatment, and lost workdays.
Negligible	Minor injury, first-aid treatment, and no lost workdays.

5.3 Frequency Categories

A quantitative frequency is generally not possible early in the design process or might not be known at all. A qualitative frequency may be derived from experience and evaluation of historical safety data from similar systems. Supporting rationale for assigning a mishap probability should be documented in hazard analysis reports. Table 9 lists examples of general frequency categories.

Table 9.—Frequency category examples

Category	Specific individual item	Frequency[1]
Frequent	Likely to occur frequently	Once per year.
Probable	Occurs several times in the life of an item	Once in 5 years.
Occasional	Likely to occur sometime in the life of an item	Once in 10 years.
Remote	Unlikely, but possible to occur in the life of an item	Once in 20 years.
Improbable	So unlikely, it can be assumed occurrence may not be experienced	Once in 50 years.

[1]For example purposes.

5.4 Risk Assessment Matrix

This matrix maps the risk index to an SIL. The severity and frequency are determined for each hazard and positioned on the risk assessment matrix in Table 10 to determine the risk index [U.S. Department of Defense 1993]. Each cell of the matrix has a risk index and associated SIL.

Table 10.—Risk assessment matrix

	Catastrophic	Critical	Marginal	Negligible
Frequent	A (SIL 3)	A (SIL 3)	A (SIL 3)	B (SIL 2)
Probable	A (SIL 3)	A (SIL 3)	B (SIL 2)	C (SIL 1)
Occasional	A (SIL 3)	B (SIL 2)	B (SIL 2)	C (SIL 1)
Remote	B (SIL 2)	C (SIL 1)	C (SIL 1)	D (no SIL)
Improbable	B (SIL 2)	C (SIL 1)	C (SIL 1)	D (no SIL)

Risk index	Suggested criteria
A	Unacceptable risk
B	Undesirable risk.
C	Acceptable risk with management review and approval.
D	Acceptable risk without review or approval.

For example, one particular hazard of a longwall shield is unexpected movement. Using Table 10, the risk index of this hazard is "A" given a hazard occurrence of occasional and a severity of catastrophic. This risk is unacceptable, and steps must be taken to eliminate or reduce the risk. For purposes of this example, we will assume the risk cannot be eliminated; therefore, a safety function is needed to specifically address the unexpected movement hazard. The safety function performance must meet SIL 3 because SIL 3 is assigned to the "A" risk index in Table 10.

5.5 Risk Assessment Graph

Figure 3 depicts a sample risk assessment graph. The risk parameters C, F, P, and W characterize the risk according to extent of severity, period of exposure, avoiding danger, and frequency of the unwanted occurrence taking place, respectively. The risk graph uses four parameters to characterize risk and then determine the SIL. Variations of the risk graph exist.

The safety standards EN–954–1 [British Standards Institute 1997] and IEC 61508–5 [IEC 1998e] depict variations of risk graphs, yet both use the basic concepts of qualitative estimates for risk in terms of severity, exposure, and avoidance.

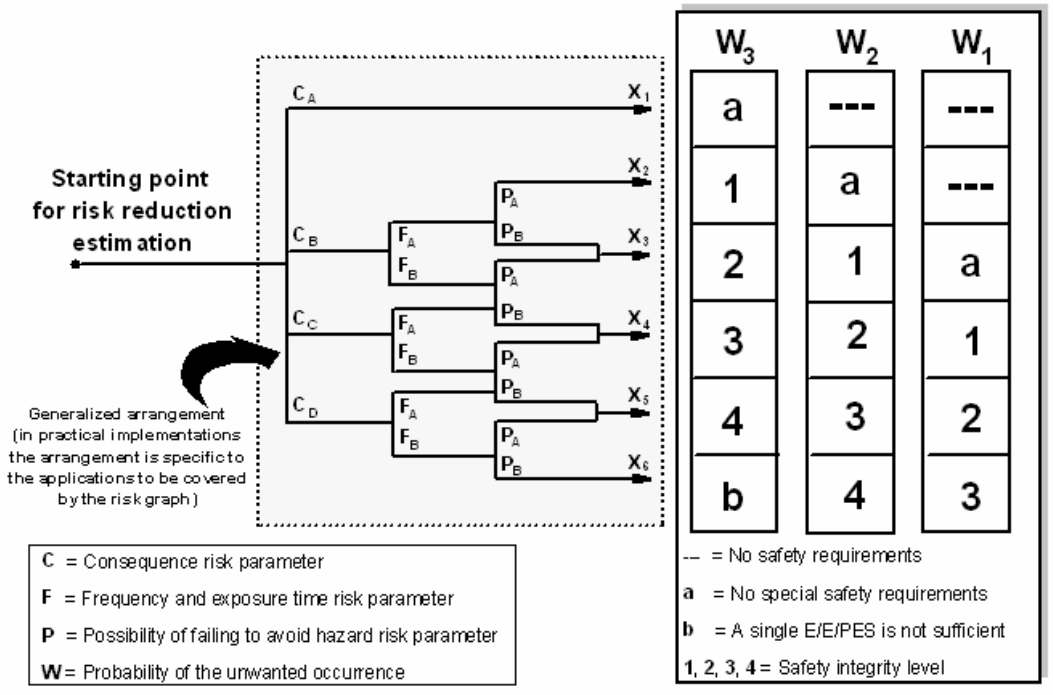


Figure 3.—Risk graph. (Source: IEC [1998e])

5.5.1 Risk Parameters

C – Consequence (severity of injury)

- C_A : Minor injury, first aid treatment, and no lost workdays
- C_B : Moderate injury, medical treatment, and lost workdays
- C_C : Severe injury, permanent disability (partial or total)
- C_D : Death or multiple deaths

F – Frequency and period of exposure

- F_A : Rarely to more often
- F_B : Frequently to continuously

NOTE 16: This does not imply that this is for the same person. It also applies to successive exposure to different people. The exposure period could be an average value based on the total time the system is used on an annual basis.

P – Possibility of avoiding danger

- P_A : Possible under certain conditions
- P_B : Almost impossible

NOTE 17: The possibility of avoidance depends on a few key points: if the hazard can be recognized, if the person can react to avoid the consequence(s), if safe intervention by the person or others can take place. The following factors influence the possibility of avoidance:

- Speed at which consequences occur
- Degree of difficulty to avoid or intervene
- Factors for detection: ambient noise levels, lighting levels, presence/absence of audible/visible alarms
- Degree of awareness (i.e., watch mode, low-concentration mode, high-concentration mode)

W – Frequency of the unwanted occurrence taking place

- W_1 : Very slight
- W_2 : Slight
- W_3 : Relatively high

5.6 Semiquantitative Technique: Layers of Protection Analysis (LOPA)

LOPA is a semiquantitative technique of risk assessment used when multiple protection layers serve to reduce a risk to an acceptable level. Typically, the consequences are determined qualitatively, and the frequency or likelihood is determined quantitatively.

LOPA is helpful to determine if a safety requirement is adequately provided. A safety requirement specifies safety function and safety integrity, as shown in Figure 4. A safety requirement can be implemented by a single protection layer consisting of a single device or safety system. Alternatively, it can be implemented using multiple protection layers. The number and type of protection layers depend on the design to meet the safety requirements.

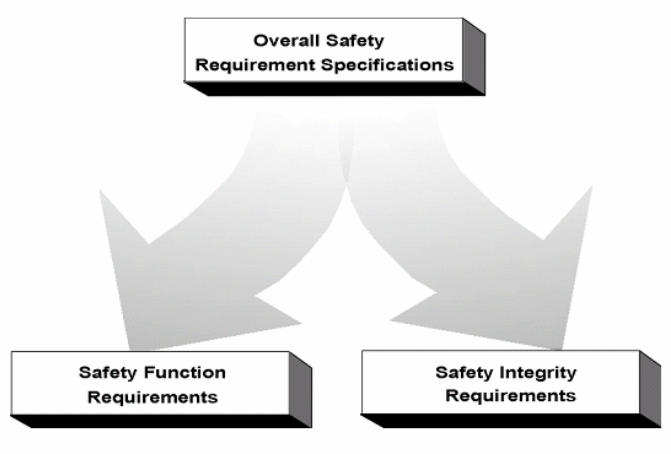


Figure 4.—Overall safety requirements.

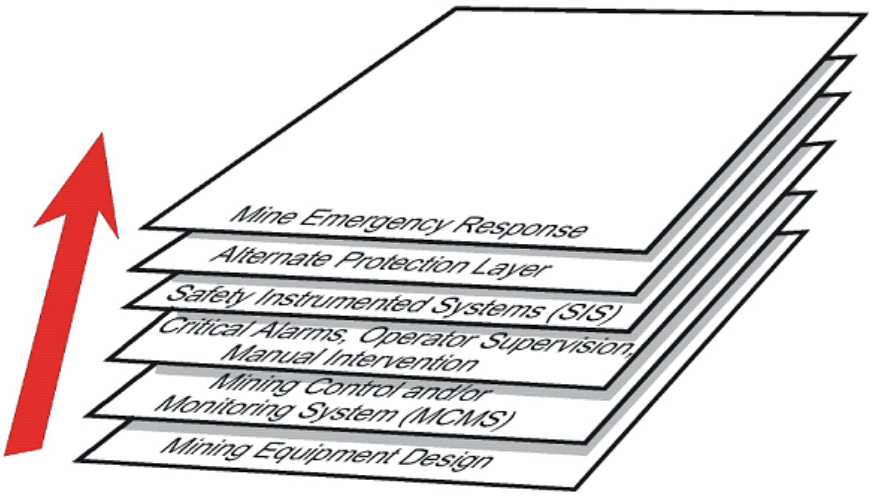


Figure 5.—Example of protection layers for a mining system.

Figure 5 shows an example of protection layers for mining. The protection layers could consist of procedures, alarms, pressure relief devices, electrical protection devices, safety instrumented systems, etc. The layers can be passive or active; however, each protection layer should be independent. An independent protection layer's (IPL) performance should not be affected by another protection layer's failure.

5.6.1 LOPA Benefits

LOPA provides a more objective approach compared to purely qualitative techniques because the frequency or likelihood is determined quantitatively. LOPA enables more diversity and flexibility in the design. This can enable a design to potentially incorporate and account for existing protection layers as long as they are independent. Other potential benefits include:

- Decreased subjectivity
- Increased accuracy
- Increased repeatability
- Reduced cost
- Simplicity as compared to purely quantitative techniques

5.6.2 Example 1: Basic LOPA

LOPA is a graphical technique derived from the event tree. One difference is that LOPA determines only two outcomes: an undesired outcome and outcome with no negative impact. Figure 6 shows a basic LOPA tree with these outcomes.

An LOPA tree consists of three components: a single initiating hazard scenario, multiple protection layers, and two outcomes. A hazard scenario is an unplanned event or series of events that leads to an undesired consequence. In the example shown in Figure 6, the loss of hydraulic pressure is an undesired consequence. The consequence is determined to be once every 2 years (i.e., F = 0.5/year). This hazard propagates through two IPLs and results in two outcomes. The undesired impact event has a frequency of 0.004/year.

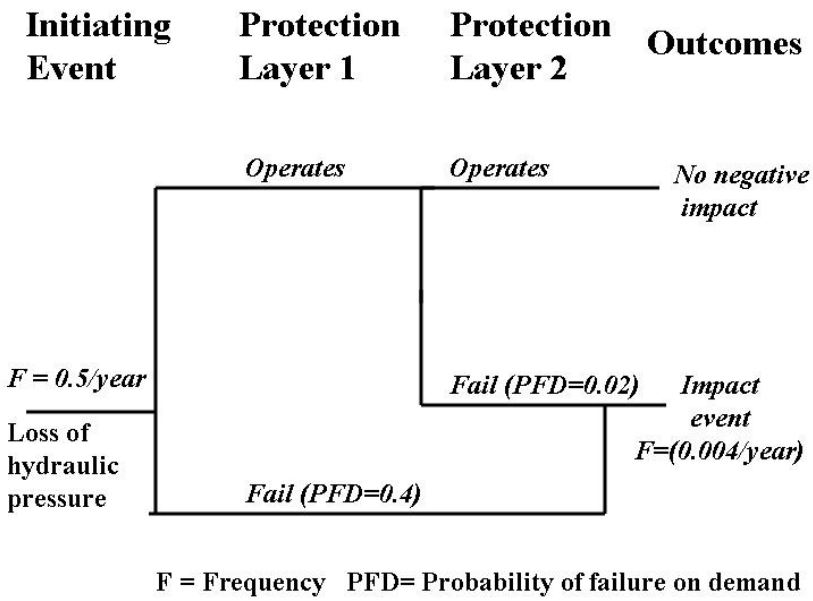


Figure 6.—Layer of protection graphical analysis.

5.7 Quantitative Techniques

The SIL for a single safety function can be determined by calculating the PFD_{avg} as:

$$PFD_{avg} \leq F_t / F_{np} , \quad (5)$$

where PFD_{avg} = the average probability of failure on demand for a low-demand mode of operation,
F_t = tolerable risk frequency,
and F_{np} = frequency of the hazard without the safety function;

NOTE 18: Annex C of part 5 of IEC 61508 defines F_{np} as "the demand rate on the safety-related system" [IEC 1998e].

Once the PFD_{avg} is calculated, it can then be related to an SIL for low demands of operation by using Table 2.

5.7.1 Example 2: SIL Calculation

Fatality data show that one fatality per year occurs because of unexpected machine movements. This is a hazard that the XYZ Mining Machine Company will address. This company has a 40% market share for this particular type of mining machine, so the company estimated that 40% of the yearly fatalities involve its machines. This manufacturer has made a corporate decision to modify the machine by adding a new emergency stop system whose sole function is to prevent these fatalities. Therefore, the demand rate on the emergency stop system is equal to the hazard rate of the machine without the emergency stop system. Therefore, F_{np} = (1 fatality per year) × (0.4 market share (i.e., F_{np} = 0.4)). The company decided it would accept a risk frequency of .0003. The PFD_{avg} is calculated by:

$$PFD_{avg} \leq F_t / F_{np}$$
$$PFD_{avg} \leq .0003 / 0.4$$
$$PFD_{avg} \leq .00075$$

The emergency stop function demand rate is low because the demand rate is equal to the hazard rate F_{np} = 0.4/year. By using Table 2, a PFD_{avg} of .00075 equates to a safety integrity level of SIL 3. Thus, the safety requirements of the emergency stop function will specify an SIL 3. The emergency stop system performance will need to meet the PFD_{avg} requirements to attain SIL 3.

NOTE 19: This hypothetical example uses the quantitative technique of Annex C of part 5 of IEC 61508 [IEC 1998e]. Other quantitative methods are described by ISA–dTR84.0.02 [ISA 1998a,b,c,d,e]. This technical report presents three quantitative methods: (1) simplified equations, (2) fault-tree analysis, and (3) Markov modeling.

6.0 Design Considerations

6.1 General Design Process

The general design process is integrated with the safety life cycle. Figure 7 depicts such a simplified integration. The process begins with a hazard and risk analysis from the safety life cycle. After the SIL is determined, the conceptual design stage begins. The conceptual design stage is where the various design options are identified. The options could include designs realized solely by nonprogrammable hardware or designs combining programmable hardware and software. Once an initial conceptual design is chosen, the design's SIL is determined. If the SIL is not achieved, the design is modified until the desired SIL is achieved.

6.2 Conceptual Design Overview

The conceptual design is part of the safety life cycle realization phase. At this point, the initial hazard and risk analyses are done, and safety requirements are written to define the safety functions and the target SIL values.

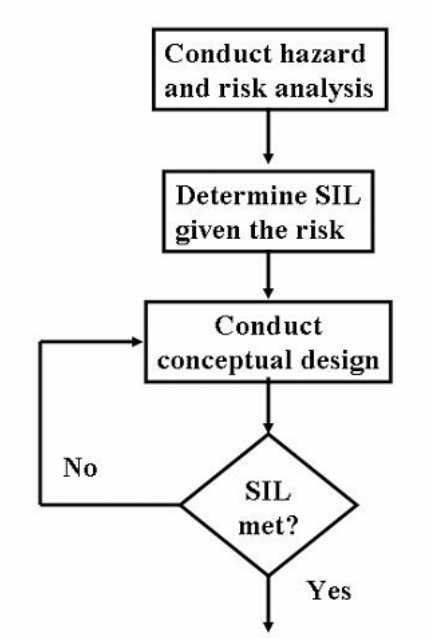


Figure 7.—The general design process to attain the required SIL.

The designer needs to consider many factors and design options. These factors include component failure rates, component technologies, hardware architectures, and testing strategies. The conceptual design process also includes evaluation of the design's safety performance with respect to the target SIL value, and the reliability. If the safety and reliability are not sufficient, then the conceptual design is changed; thus, it is an iterative process, as shown in Figure 8.

6.3 Technologies

The choice of technologies is the first decision the designer should make. Numerous technologies exist. Traditionally, control and safety functions were hard-wired in mining systems. More recently, programmable electronic devices and systems are being used in mining. Devices such as programmable logic controllers (PLCs) have replaced relay-based logic for virtually all applications. In general, the technology choices are:

• *Relays.*—Relays are simple devices, and their failure modes and rates are well known and predictable. They are typically used to implement simple functions requiring just a few inputs and outputs. Typically, relays lack automatic diagnostic, so they are manually tested.

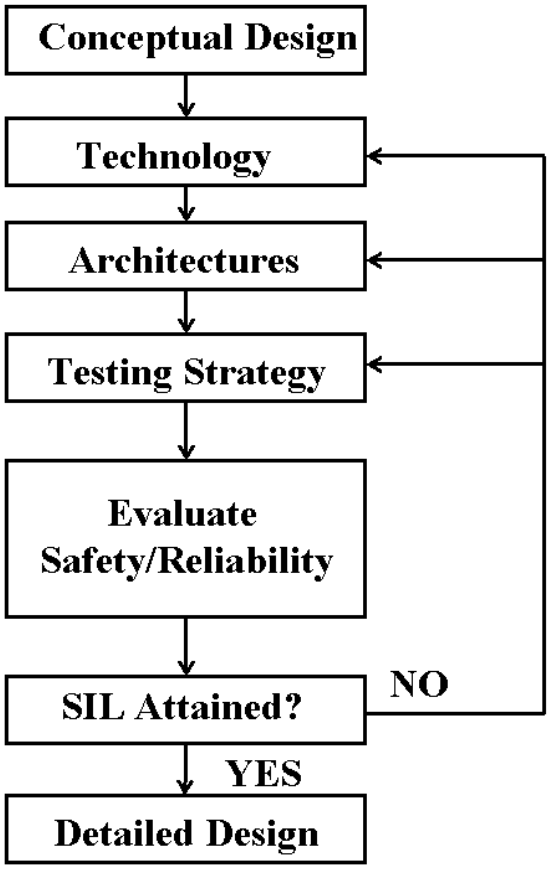


Figure 8.—The conceptual design process is an iterative part of the safety life cycle realization phase.

• *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 and behavior under fault conditions.

• *Programmable electronic devices.*—Microprocessors and PLCs are in wide use. These systems use solid-state devices and software. Programmable electronic systems are more flexible and can offer more functionality than relays. However, the failure modes are not predictable, and failures (hardware or software) can be difficult to detect and diagnose. On-line testing and diagnostics are available.

6.4 Hardware Architectures

The hardware architecture encompasses sensors, logic solvers, and final elements. For example, Figure 9 shows a redundant architecture for a PLC as the logic solver. This architecture is known as a one-out-of-two (1oo2) architecture that provides tolerance for one fault.

Various other architectures are used to add fault tolerance capabilities, as shown in Table 11. The choice of which architecture to use depends on the required SIL and the desired nuisance trip rate (mean time to fail safe (MTTFS)).

Increasing the redundancy does not always increase the safety performance. Therefore, the choice of architecture involves consideration of many factors such as the required SIL and other factors such as MTTFS. The following example stresses these considerations.

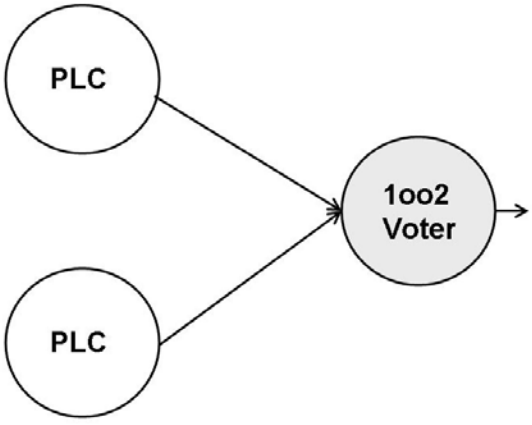
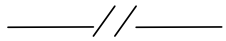
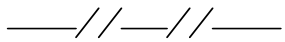
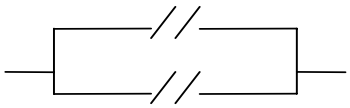
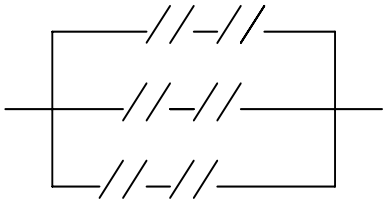


Figure 9.—A redundant PLC architecture.

Table 11.—Various voting architectures and the electrical representation of their voting functions

Architecture	Electrical representation	Comments
1oo1		No-fault tolerance.
1oo2		For deenergized to trip systems. Reduces dangerous failures of energized outputs. Requires two dangerous failures for the system to fail dangerous.
2oo2		For energized to trip systems. Reduces safe failures of deenergized outputs.
2oo3		Tolerates both safe and dangerous failures.

6.4.1 Example 3: Architecture Impacts on Safety Performance

This example involves a simple, normally closed switch used for an emergency stop function. If the switch fails closed, it is a dangerous failure; if it fails open, it is a safe failure. The safe-failure rate (nuisance-trip rate) is .1, or once in 10 years. The dangerous failure rate is the same rate; thus, there is an equal probability of either failure mode. Four architectures are considered for the switch: 1oo1, 1oo2, 2oo2, and 2oo3. The dangerous failure rates for the architectures are shown in Figure 10; the safe failure rates for the architectures are shown in Figure 11.

Increasing the redundancy from 1oo1 to 1oo2 did improve the safety performance as defined by the dangerous fail rate; however, the safe failure rate increased, which increases the MTTFS and results in more nuisance trips. The 2oo2 configuration also increases the redundancy, but the dangerous failure rate doubled. Thus, adding redundancy does not always improve safety.

NOTE 20: A 2oo2 or dual-channel system is generally not suited for an emergency stop function. For instance, if one channel fails such that the output remains energized, then the output will remain energized regardless of the other channel's operation.

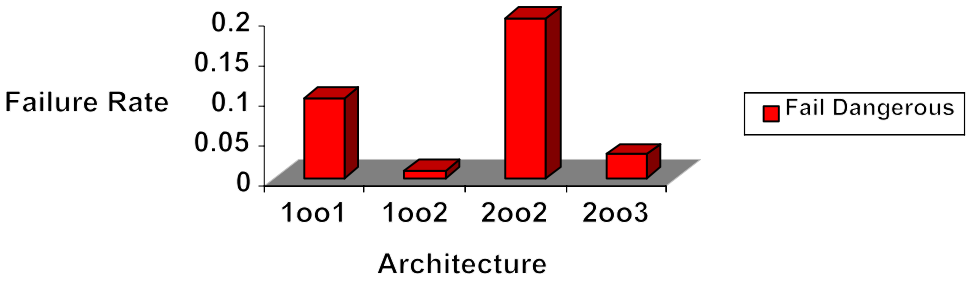


Figure 10.—Dangerous failure rates for various switch architectures.

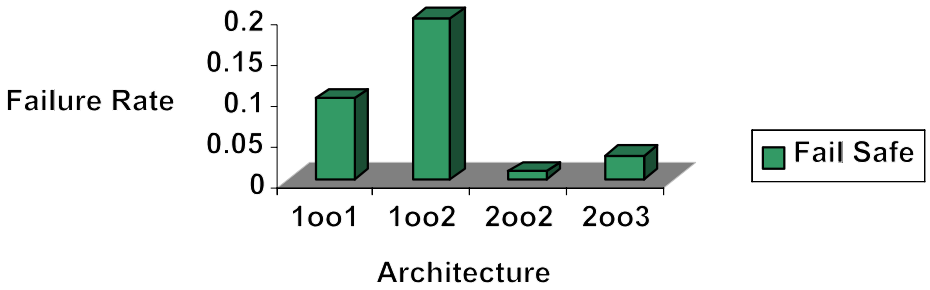


Figure 11.—Safe failure rates for various switch architectures.

6.4.2 SIL Constraints Due to Hardware Architecture

The architecture is a factor in the attainment of an SIL. The highest SIL that can be claimed for a given architecture is restricted. IEC 61508 bases the highest SIL that can be claimed on the following:

- Amount of hardware fault tolerance
- The safe failure fraction (SFF)
- The type of device or subsystem. Simple devices are type A; complex devices are type B.

NOTE 21: All possible failure modes are well known and can be completely determined for type-A devices. The behavior under fault conditions can be completely determined. A relay is considered to be type A. For type-B devices, all failure modes are not completely known or the behavior under fault conditions cannot be completely determined. Also, there is insufficient failure data from field experience to document the dangerous detected and undetected failure rate. A PLC is considered to be type B.

NOTE 22: The safe failure fraction is a ratio of safe and dangerous detected failures to the total failures.

The IEC 61508 architectural constraints for type A and type B are shown in Tables 12 and 13, respectively.

Table 12.—IEC 61508 hardware architectural constraints for type-A safety-related subsystems

Safe failure fraction (SFF)	Hardware fault tolerance		
	0	1	2
<60%	SIL 1	SIL 2	SIL 3
60% to <90%	SIL 2	SIL 3	exceeds SIL 3
90% to <99%	SIL 3	exceeds SIL 3	exceeds SIL 3
≥99%	SIL 3	exceeds SIL 3	exceeds SIL 3

Table 13.—IEC 61508 hardware architectural constraints for type-B safety-related subsystems

Safe failure fraction (SFF)	Hardware fault tolerance		
	0	1	2
<60%	Not allowed	SIL 1	SIL 2
60% to <90%	SIL 1	SIL 2	SIL 3
90% to <99%	SIL 2	SIL 3	exceeds SIL 3
≥99%	SIL 3	exceeds SIL 3	exceeds SIL 3

6.4.3 Example 4: IEC 61508 Hardware Architecture Constraints

This example is based on the 1oo2 PLC shown in Figure 9. The following parameters are known for the 1oo2 PLC:

$PFD_{avg} = .2 \times 10^{-7}$ (SIL 3)
SFF = 91%
Faults tolerated = 1
Component type = B

The 1oo2 PLC meets SIL 2 based solely on the value of PFD_{avg}. Next, Table 13 is used to check the maximum SIL that can be claimed given the hardware fault tolerance and the SFF. For this example, the maximum that can be claimed is SIL 3. Therefore, no SIL constraints are imposed. The system safety recommendations also address SIL constraints. Section 6.6.4.11 of the system safety recommendations [Sammarco and Fisher 2001] lists the minimum fault tolerances, as shown in Table14 below:

Table 14.—Minimum fault tolerances

	SIL 1	SIL 2	SIL 3
Simple subsystem	0	0	1
Complex subsystem	0	1	2

Table 14 is a rough approximation of Tables 12–13; Table 14 does not differentiate between the subsystem type (A or B) and omits the use of SFF as a constraining factor.

6.4.4 Example 5: System Safety Recommendations – Hardware Architecture Constraints

This example is based on the 1oo2 PLC shown in Figure 9 as used in example 4; however, the SFF is neglected. The following parameters are known for the 1oo2 PLC:

$PFD_{avg} = .2 \times 10^{-7}$ (SIL 3)
Faults tolerated = 1
Component type = B

Table 14 is used for this example. The maximum SIL that can be claimed, given a fault tolerance of one, is SIL 2. For this example, Table 14 is more restrictive than Table 13.

6.4.5 Exceptions

There are exceptions to the minimum fault tolerance constraints in Table 14. Any one of these is an exception, provided it is supported by documentation:

(1) The subsystem is inherently safe due to the nature of its design and construction.

NOTE 23: A mechanical actuator linkage is an example.

(2) The subsystem has a documented service history for similar applications and environments.

NOTE 24: An example is a 1oo1 PLC that had a documented service history of safety performance of SIL 2 for longwall mining applications.

(3) The SFF can be determined.

NOTE 25: If the SFF is known, then use the IEC 61508 architectural constraints for hardware safety integrity as listed in Tables 12–13.

6.5 Safe Failure Fraction (SFF)

The SFF was briefly introduced in the previous example. The SFF is a metric used for constraining the maximum SIL that can be claimed regardless of the calculated hardware reliability.

Annex C of IEC 61508–6 [IEC 1998f] presents a sample calculation of the SFF where:

$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD}) /$ total failure rate λ_{total}

$\lambda_{total} = \Sigma\lambda_S + \Sigma\lambda_D$

$\Sigma\lambda_D = \Sigma\lambda_{DD} + \Sigma\lambda_{DU}$

The SFF calculation assumes that a dangerous detected failure will be detected and mitigated to bring the system to a safe state.

NOTE 26: A detailed analysis of λ_S and λ_D might not be practical for complex components. These parameters can be based on engineering judgment. For a complex component, a 50/50 split of safe and dangerous failures is reasonable.

6.6 Failures

Hazards can occur from hardware or software failures. Hardware failures are physical failures and are usually due to random events and wear. They can involve any of the system's physical components, including programmable electronic devices, power supplies, sensors, data communication paths, actuators, etc. Software does not exhibit random wearout failures. Instead, software failures result from systematic (functional) errors. Figure 12 shows the two failure classifications—physical and functional.

Figure 13 shows physical and functional failure distributions for PE-based mining system mishaps. The data cover the period 1995–2001. The population is 100 mishaps and is composed of mishap data from MSHA; New South Wales, Australia; and Queensland, Australia. Random failures exceed systematic failures by about 7%. Note that 15% of the failure sources were unknown. This implies that physical evidence of a failure (random failures) did not occur or was not observed. One could infer that these unknown failures may largely be unspecified systematic errors.

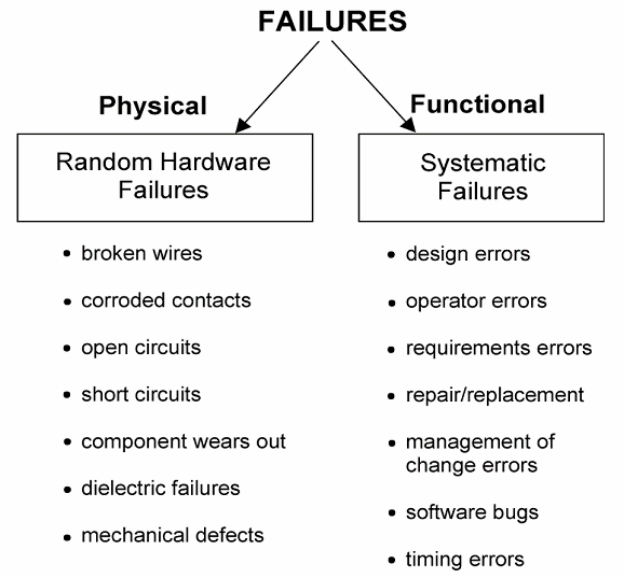


Figure 12.—Failure classifications.

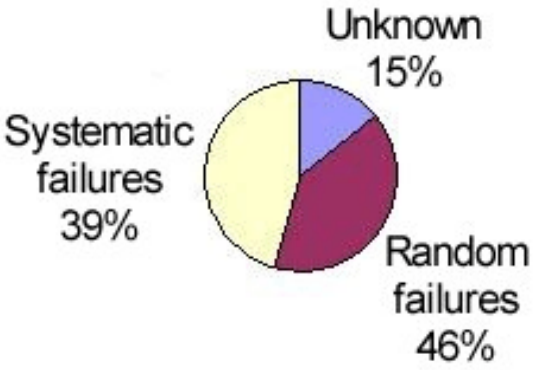


Figure 13.—Random and systematic failure distributions for 100 PE-based mining system mishaps during 1995–2001.

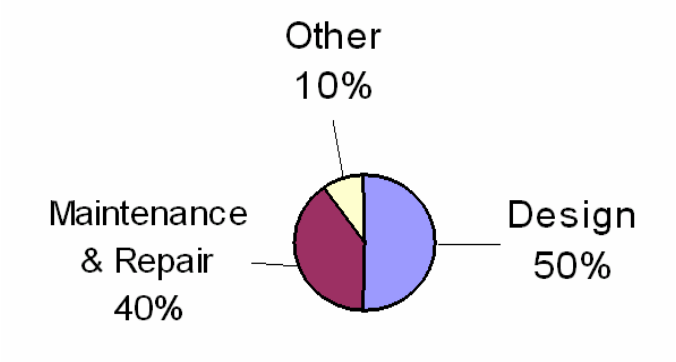


Figure 14.—Systematic failures for 100 PE-based system mishaps during 1995–2001.

6.6.1 Functional (Systematic) Failures

Systematic failures are also known as functional failures. Sources of these failures include hardware and software design errors, errors made during maintenance or repair, operator errors, and errors resulting from software modifications. Figure 14 shows the breakdown of systematic failures as derived from the same data used to generate Figure 13. Design errors comprised 50% of all systematic failures, while failures during maintenance or repair comprised 40%. Together, these two categories comprised 90% of the systematic failures.

6.6.2 Physical (Random) Failures

The harsh environmental factors associated with mining, such as water and dirt intrusion, vibration, shock, and heat, can seriously impact hardware failures. The failures that occur involve electrical connectors, wiring, sensors, power supplies, and solenoids. One example of a random failure is the degradation of rubber seals or boots used to keep out dust and moisture. Figure 15 shows the breakdown of random failures as derived from the same data used to generate Figure 13. Sensor failures comprised the largest category of random failures. Switches are considered a sensor in this analysis.

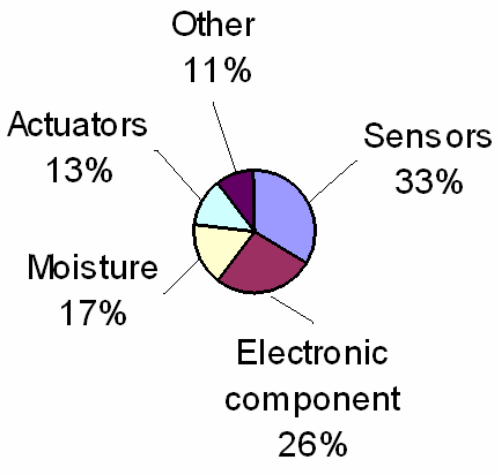


Figure 15.—Random failures for 100 PE-based mining system mishaps during 1995–2001.

6.6.3 Physical (Random) Failure Rates

Multiple types of physical failures exist, and it is important to distinguish these types and their associated rates for evaluating safety integrity levels. The failures are broadly classified as safe failures or dangerous failures. A safe failure is also known as a nuisance failure, false-trip failure, spurious failure, or fail-to-safe failure. Typically, a safe failure results in some type of shutdown. A dangerous failure occurs when the system cannot perform a safety function when it is needed.

Safe or dangerous failures can be detected or undetected; therefore, the failure rate consists of the detected and undetected failures rates as follows:

- Total failure rate $\lambda = \lambda_S + \lambda_D$
- Total failure rate λ = 1/mean time between failure (MTBF)
- Safe failure rate $\lambda_S = \lambda_{SD} + \lambda_{SU}$, where λ_{SD} is safe detected and λ_{SU} is safe undetected
- Dangerous failure rate $\lambda_D = \lambda_{DD} + \lambda_{DU}$, where λ_{DD} is dangerous detected and λ_{DU} is dangerous undetected

If diagnostics are not available to detect failures, then $\lambda_{SD} = 0$ and $\lambda_{DD} = 0$.

6.6.4 Failure Data

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. There are limitations to failure data. Some databases only provide failure rates. In this case, one can set conservative estimates such as 50% of electronic component failures are safe, 75% of relay failures are safe, and 40% of solenoid failures are safe.

Failure rates are typically expressed on a yearly basis. For instance, a single shutoff valve's failure rate could be expressed as .0018/year. In addition to failure rates, the failure modes (safe and dangerous) and the effectiveness of automatic diagnostics are needed.

6.6.5 Failure Data Sources

Numerous data sources exist. Some databases are industry-specific, product-specific, generic, or site-specific. For instance, a site-specific database may contain failure rate and failure mode data for solenoid valves used at a given mine. Some databases are printed in book form; others are available in electronic format.

Some common failure data sources are:

- Offshore Reliability Data (OREDA) [SINTEF 1997]
- Reliability Data for Control and Safety Systems [SINTEF 1989]
- Nonelectronic Parts Reliability Data [Reliability Analysis Center 1995]
- Safety Equipment Reliability Handbook [exida.com 2003]

NOTE 27: This is a partial list of database sources and does not imply endorsement. An extensive listing of failure data sources is available at www.ntnu.no/ross/info/data.php [Norwegian University of Science and Technology 2005].

Databases can be an important source of failure data, but other sources exist. For instance, some PLC vendors can provide model-specific data. Also, some software programs used to calculate safety integrity levels have built-in databases that provide failure rate, failure mode, and diagnostic capabilities for standard electronic and nonelectronic products.

6.7 Diagnostics

Not all failure modes are detectable through the use of diagnostics. In addition, adding diagnostic capabilities could be impractical to implement for some failure modes; therefore, a percentage of failures are typically covered by diagnostics. The term "diagnostic coverage" reflects this situation. A method for calculating diagnostic coverage and a sample calculation is presented in annex C of IEC 61508–6 [IEC 1998f]. Diagnostic coverage (DC) is calculated as follows:

$$DC = \Sigma\lambda_{DD} / \Sigma\lambda_{total}$$

6.8 Common Cause

Common cause factors can exist when using multiple channels or redundancy. Common cause failures occur when a single failure causes other components to fail. For instance, a system has three analog sensors powered from the same electrical source. Although there is redundancy, all three sensors will fail if there is a failure with the electrical source.

Common cause failures could result from a systematic fault such as human error, random hardware failure, or a combination of systematic and random failures.

Annex D of IEC 61508–6 presents a methodology for quantifying common cause. The methodology uses a β-factor to model common cause failures [IEC 1998f].

6.9 SIL Verification

SIL verification depends on the calculation of PFD or dangerous failures per year. The calculations depend on:

- Choice of technology
- Mode of operation (low- or high-demand)
- Architecture
- Diagnostics
- Systematic failures
- Common-cause failures
- Test interval
- Prior service history (proven-in-use)
- Maintenance

For SIL verification, it is useful to reduce the system to an abstraction of three parts: a sensor (S), a logic solver (L), and a final element (FE). Figure 16 depicts this abstraction.

The sensor can be any type sensor such as a switch or pressure transducer. The logic solver could be a relay, solid-state device, or PLC. In some systems, the sensor could be directly hard-wired to the final element; thus, the logic solver is considered the connecting wire. Some examples of final elements include a solenoid valve or a motor starter. The sensor and final element typically have the highest hardware failure rates, so they are the weakest link in a system [Gruhn and Cheddie 1998].

The simple abstraction shown in Figure 16 is useful for verifying the SIL of a safety system with a low-demand mode of operation. For instance, the average probability of failure on demand (PFD_{avg}) of a system's safety function for a low-demand system is calculated by:

$$PFD_{sys} = PFD_S + PFD_L + PFD_{FE} \quad (6)$$

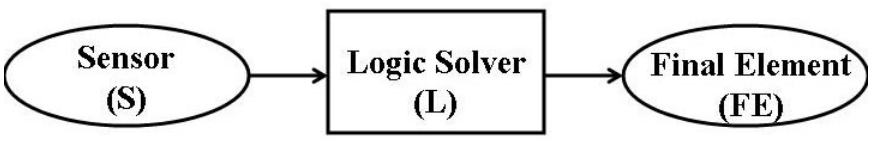


Figure 16.—A system abstracted to three components.

where PFD_S = PFD_{avg} of a safety function for the sensor element,
PFD_L = PFD_{avg} of a safety function for the logic solver,
and PFD_{FE} = PFD_{avg} of a safety function for the final element.

The SIL for a system will not be greater than the lowest SIL of its components.

6.9.1 Example 6: A Simplified PFD_{avg} Verification

A shutdown function is required to have a safety performance of SIL 2. The first conceptual design consists of a single pushbutton switch, PLC, and hydraulic pump contactor connected in series. The pump shuts down when the switch is pressed, thus placing the system to a safe state. The PFD_{avg} of each device is given:

PFD_S = PFD_{avg} of the switch = 1.10×10^{-2} (SIL 2)
PFD_{PLC} = PFD_{avg} of the PLC = 2.50×10^{-2} (SIL 2)
PFD_{FE} = PFD_{avg} of the pump motor contactor = 2.19×10^{-3} (SIL 3)

Using equation 6, the PFD_{sys} is calculated:

$$PFD_{sys} = (1.10 \times 10^{-2}) + (2.50 \times 10^{-2}) + (2.19 \times 10^{-3})$$
$$PFD_{sys} = 3.82 \times 10^{-2} \quad \text{(SIL 2)}$$

The design is verified to meet SIL 2. To increase the system SIL to 3, both SIL 2 components must be changed to meet SIL 3.

6.9.2 Quantitative SIL Verification Techniques

Various techniques can be used to determine PFD_{avg} for a low-demand operation and the probability of dangerous failures for high-demand or continuous mode operation. The following quantitative techniques can be used for verifying that the safety integrity level is achieved:

- *Reliability Block Diagram Technique.*—Annex B of IEC 61508–6 gives examples to determine the probability of hardware failures for low- and high-demand modes of operation [IEC 1998f]. The annex gives examples for 1oo1, 1oo2, 2oo2, 2oo3, and other architectures.

- *Simplified Equations Technique.*—The determination of the SIL via equations is detailed in Parts 1 and 2 of the ISA Technical Report TR84.0.02 [ISA 1998a,b]. This document gives procedures for PFD_{avg} calculations and sample calculations for various architectures. Equations are given with terms for multiple failures during repair, common causes, and systematic errors. Basic equations that drop these terms are also given as follows:

1oo1 $$PFD_{avg} = \lambda_{DU} \times \frac{TI}{2} \quad (7)$$

1oo2 $$PFD_{avg} = ((\lambda_{DU})^2 \times TI^2) / 3 \quad (8)$$

2oo2 $$PFD_{avg} = \lambda_{DU} \times TI \quad (9)$$

2oo3 $$PFD_{avg} = (\lambda_{DU})^2 \times TI^2 \quad (10)$$

where λ_{DU} = failure rate for dangerous undetected failures,
and TI = manual test interval or frequency.

- *Fault-tree Analysis Technique.*—Part 3 of ISA Technical Report TR84.0.02 details the use of fault trees [ISA 1998c]. The graphical nature of this technique affords visualization of failure paths. Fault trees can model diverse technologies and complex failure logic; however, they are not well suited to model time dependencies. Software programs are available for conducting fault-tree analysis.

- *Markov Modeling Technique.*—Part 4 of ISA Technical Report TR84.0.02 details Markov modeling [ISA 1998d]. All possible states can be modeled including fully operational, partially failed (degraded) states, and failed states. Markov models can also include repair and repair rates of failed components. Markov models are well suited for complex devices such as PLCs. These models provide the most accurate analysis. They are also the most mathematically demanding techniques.

6.9.3 Example 7: SIL Verification Using Simplified Equations

A switch is to be used as the sensor for the system shown in Figure 16. This is a simplex system (1oo1 architecture) that does not have diagnostics. The switch needs to meet SIL 2. Calculate the switch SIL using equation 6 and the following parameters:

TI = 8,760 hours or once per year
$\lambda_{DUswitch} = .4 \times 10^{-5}$

$$PFD_{avg} = \lambda_{DU} \times \frac{TI}{2}$$

$PFD_{avg\ switch} = (0.4 \times 10^{-5})\ (8{,}760 / 2) = 1.8 \times 10^{-2}$ (SIL 1)

The switch only meets an SIL 1. The safety performance of the switch can be improved by using a switch with a lower λ_{DU} or by changing the manual test interval to once every 6 months. Increasing the test frequency results in a safety performance that meets SIL 2.

$PFD_{avg\ switch} = (0.4 \times 10^{-5})\ (4{,}380 / 2) = 8.8 \times 10^{-3}$ (SIL 2)

6.9.4 Software Tools for SIL Verification

Calculations by hand can be appropriate for some situations such as initial estimations of PFD for a simple system design where the target is an SIL 1 or SIL 2. For these situations, the simplified equations or reliability block diagram techniques can be used. For other situations, software tools are very useful for performing safety integrity analysis.

Some tools are specifically designed to perform quantitative safety integrity analysis as specified by IEC 61508, IEC 61511, and ANSI/ISA 84.01. In addition to PFD calculations, these tools can calculate mean time to fail spurious (MTTFS). Some tools integrate failure databases and can accommodate various architectures. Sophisticated Markov analysis can be used to quickly produce highly accurate calculations without the end-user knowledge of Markov analysis.

These software tools also help document the analyses and the associated assumptions, failure rates, manual test intervals, common cause factors, and diagnostic coverage. The tools also provide graphics that help users analyze and visualize the safety integrity contributions of sensors, logic solvers, and field devices. Some software tools have demonstration versions available for down-loading. Examples of software tools are:

- CaSSPac www.landmengineering.com/software.html
- FSC SafeCalc hpsweb.honeywell.com/Cultures/en-US
- SilCore www.acm.ab.ca/toolsSilCore.cfm
- SILver www.exida.com/applications/silver.asp

NOTE 28: This list is for example purposes only and does not imply endorsement.

7.0 Management of Change (MOC)

MOC is important to reduce the potential for introducing new hazards or exacerbating existing ones. One way to minimize this potential is to establish a systematic plan or process.

MOC must also apply to software because it is part of the system and modifications can adversely impact safety. Software modifications, as well as hardware modifications, must be analyzed for hazards. Those software modifications impacting safety should be well documented and managed. A management of change process is shown in Figure 17.

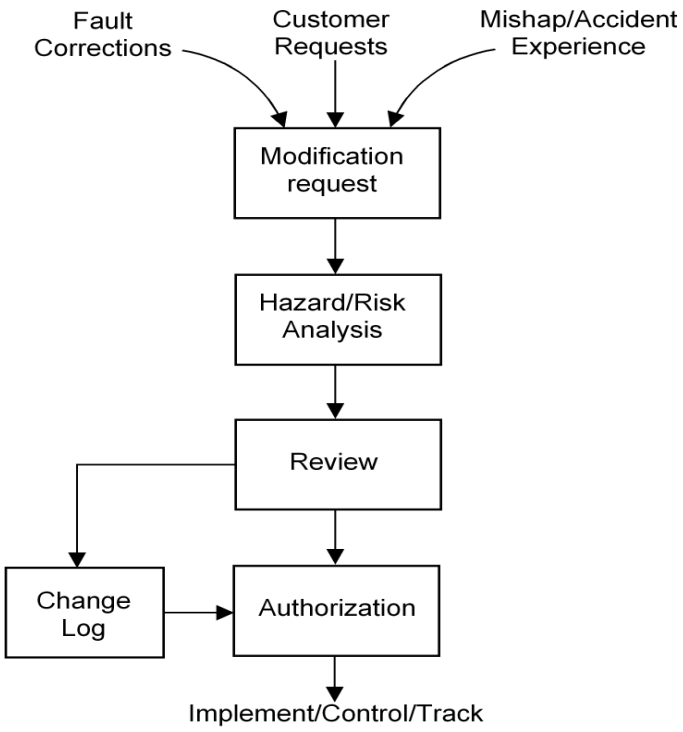


Figure 17.—Management of change (MOC) process.

8.0 Lessons Learned

Past near-mishaps, accidents, and fatalities experienced in mining and other industries have provided an opportunity to generalize some lessons learned.

(1) System and software requirements specifications

Most problems with safety-critical software come from safety requirement specification errors where:

- The requirements specification is incorrect or incomplete.
- The implementation of the requirements specification is incorrect due to mis-understandings and discrepancies.

(2) Mode changes

Mode changes can be a significant source of errors compromising safety. Mode changes include startup and shutdown. Mining systems can have manual, semiautomatic, automatic, and remote operational modes. For example, an accident occurred when changing from automatic to manual then back to automatic operation. The system resumed operation from the last state during automatic mode rather than from the last state from the manual mode. This resulted in an unexpected machine movement, injuring the operator.

(3) Extreme conditions (boundary conditions)

Operation at extreme conditions or boundary points can be an area of potential high risks and should be carefully evaluated; therefore, these points should be identified and tested. Extreme conditions include physical conditions of temperature and moisture, electrical conditions of low or high power, signal inputs and outputs from transducers, and physical conditions of movement such as rate of change and range of movement.

(4) System changeovers

System changes from hardware to software should carefully be analyzed with respect to safety. For example, a simple, hard-wired hardware-based protection system was changed to a PLC-based system. Faults occurred because the new design was more complex, and the design did not take into account new error sources associated with the technology.

9.0 Emergency Stop Function Case Study

A case study is presented in this section. The purpose is to show how the recommendations can be implemented by using a simplified example. This example closely follows the safety life cycle. The example is for learning purposes only. It does not detail every task or process given by the recommendations; however, it does focus on the key concepts and processes.

One safety function, an emergency stop, is presented in this case study. The example shows how a system level safety analysis identifies the need for this safety function and how this safety function is implemented throughout the safety life cycle phases.

9.1 Case Study Description

The case study concerns the design for 30 continuous mining (CM) machines. These machines operate underground to cut coal. Each CM machine can be operated manually by a worker seated in the operator's compartment or by using a remote-control pendant that can be used in a wireless mode or tethered to the CM machine.

The CM's basic operation can be described in three steps, as shown in Figure 18: (1) Coal is cut with a rotating cutter drum that can be raised or lowered by controlling the position of a boom. (2) The cut coal is collected into a gathering pan. (3) The coal is transported from the gathering pan to the end of the machine via a conveyor.

The cutting drum, gathering pan, tail conveyor, and traction motors are powered electrically. The boom position, as well as some other functions, is powered hydraulically. Machine movements are via left- and right-hand crawler tracks; each track is turned with a dedicated electric traction motor. This enables the following machine movements: forward, reverse, forward turn left or right, reverse turn left or right, and pivot left or right. Some of the control functions for the traction motors and the cutting drum are implemented by an onboard industrial PLC.

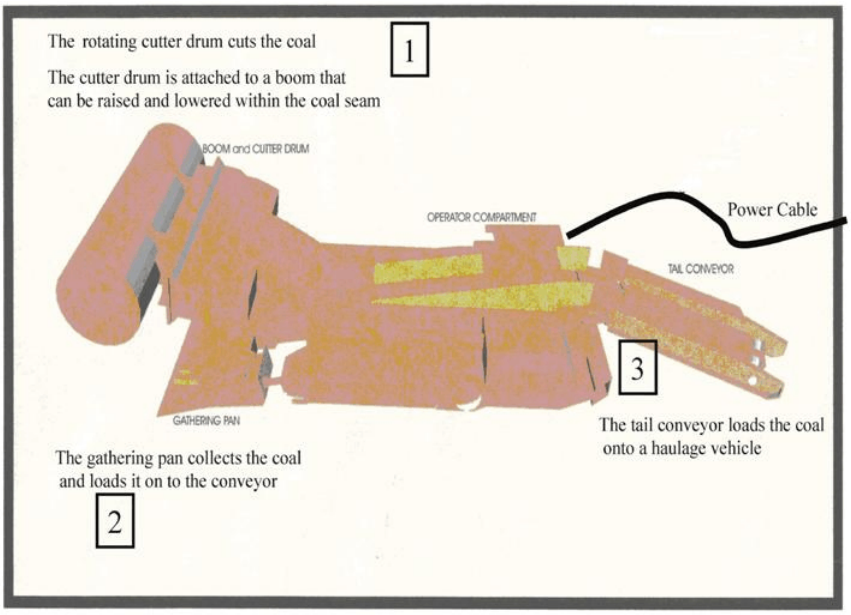


Figure 18.—A continuous mining machine.

9.2 Safety Life Cycle Phases

The case study example follows the safety life cycle shown in Figure 19. Each phase of the life cycle is detailed in the recommendations for system safety [Sammarco and Fisher 2001].

9.3 Scope

The scope is limited to the operator and continuous mining machine. Other support machinery and personnel are excluded in order to simplify this example. This example does not present all hazards associated with operating and maintaining the machine.

9.4 System Hazard and Risk Analysis

The hazard and risk analysis is conducted at the system level for the entire continuous mining machine. Three hazard analysis techniques are used to identify system hazards: checklists, HAZOP, and FTA. Next, the level of risk for each hazard is assigned by use of a risk matrix. The assignment of an SIL for each hazard is based on this risk matrix.

9.5 Hazard Analysis

Multiple hazard analysis techniques are used as detailed in the recommendations for system safety [Sammarco and Fisher 2001]. The techniques used in this example are checklists, HAZOP, and FTA.

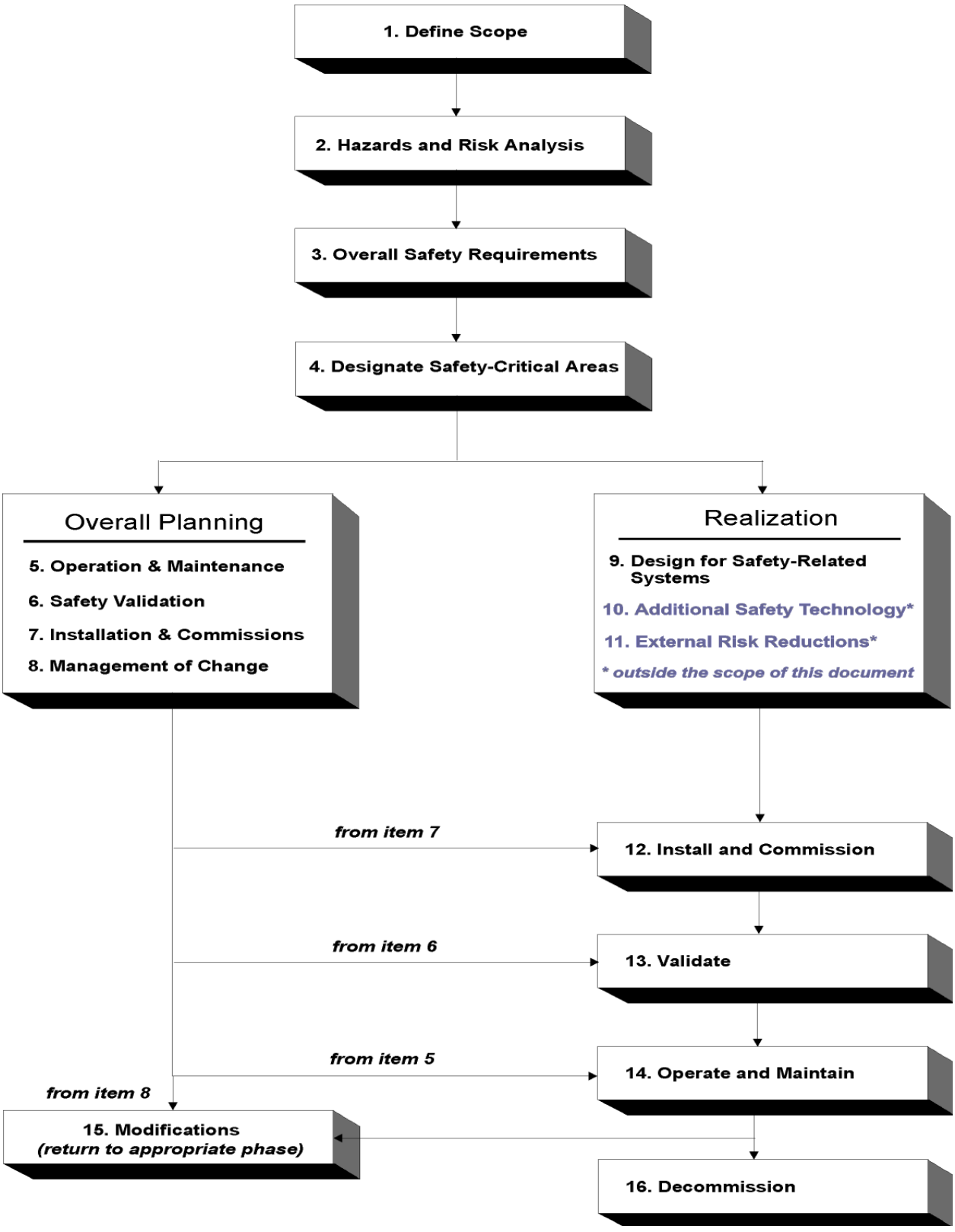


Figure 19.—The safety life cycle.

9.5.1 Checklists

Checklists can be used as a hazard analysis technique to identify hazards, to stimulate thinking, and to pass on lessons learned from mistakes and experience. They can also be used to systematically list design procedures and practices, thus reducing the likelihood of errors of omission during the design phase. The following checklist items have been extracted from Appendix A of the system safety recommendations [Sammarco and Fisher 2001]. The hazard associated with each checklist item is also given. Multiple checklist items can identify the same hazard.

System checklist:

Can a single-point failure cause a hazardous state?

- Response: Yes, loss of machine control could happen if the PLC-based control system failed.

- Hazard: Loss of machine control

Can failure to turn on or turn off solenoids or activators cause an unsafe condition?

- Response: Yes, loss of machine control could happen if the control system failed to safely control solenoids or activators. For example, the tram controls could be stuck in the activated ("on") state.

- Hazard: Loss of machine control

Hardware checklist:

Can the failure of any input or output device cause an unsafe state?

- Response: Yes, if a remote-control pendant tram switch failed in a stuck-on position, then tramming could not be stopped.

- Hazard: Loss of machine control

Will sticking or malfunctioning solenoid valves place the system in an unsafe state?

- Response: Yes, a stuck valve could cause unexpected movement of a hydraulically controlled function.

- Hazard: Unexpected movement

9.5.2 HAZOP

Two HAZOP data sheets are presented for the initial design phases of the machine. The first HAZOP data sheet (Table 15) lists the results of analyzing the pump motor of the hydraulic system. The next HAZOP data sheet (Table 16) lists the results of analyzing the control PLC. Both data sheets are of a high-level HAZOP analysis.

Table 15.—HAZOP data sheet for hydraulic pump

HAZOP

SYSTEM Continuous Miner DATE 2/20/04
SUBSYSTEM Hydraulics
Team Leader: Sammarco
Team Members: Cole, Fries, Jobes

Item No.	Part	Attribute	Guide word	Cause	Consequence	Remediation	Remarks
1	Pump	Hydraulic pressure	No	1. Hydraulic system failure 2. Pump motor failure 3. Electric system failure 4. Broken hydraulic line(s)	No hydraulic functions operational	1. Provide diagnostics to aid repair	1. Safe failure, but undesirable for production
		Hydraulic pressure	More	1. Hydraulic system failure 2. Pump motor failure	Excessive pressure could be a hazard	1. Provide diagnostics to aid repair 2. Use pressure relief valve	1. Hazardous situation
		Hydraulic pressure	Less	1. Hydraulic system failure 2. Pump motor failure	Slow operation	1. Provide diagnostics to aid repair	1. Safe failure, but undesirable for production

Table 16.—HAZOP data sheet for the PLC data line to control the tram functions

HAZOP

SYSTEM Continuous Miner DATE 2/20/04
SUBSYSTEM PLC-based control system
HAZOP Method: X Deviation by deviation ____ Cause by cause
Team Leader: Sammarco
Team Members: Cole, Fries, Jobes

Item No.	Part	Attribute	Guide word	Cause	Consequence	Remediation	Remarks
2	Control data line that controls tram functions	Control data value	No	1. PLC fails 2. Severed wire 3. Connector failure	Loss of tram control because the state of the tram can't be changed. For example, if the machine trams forward, no data is sent to stop it.	Use watchdog timer to check PLC	Dangerous failure
		Control data value	More	Data corrupted	Unexpected machine movement because the machine trams faster than expected	Use data error checking	Dangerous failure
		Control data value	Less	Data corrupted	Unexpected machine movement; machine trams slower than expected	Use data error checking	Safe failure

9.5.3 Fault Trees

Fault-tree analysis is a top-down approach that begins with the undesired outcome at the top of the fault tree and ends with potential causes at the bottom. This example takes the general hazards of loss of machine control (i.e., the state of the mining machine cannot be changed) and unexpected machine movement, and forms a more specific hazard—loss of tram control. Figure 20 shows the fault tree for this undesired outcome. Six events (i.e., PLC fails, tram switch fails) are identified that could lead to the undesired state of loss of tram control. For instance, a low power supply voltage (brown-out condition) for the PLC is a power failure that could cause code execution errors.

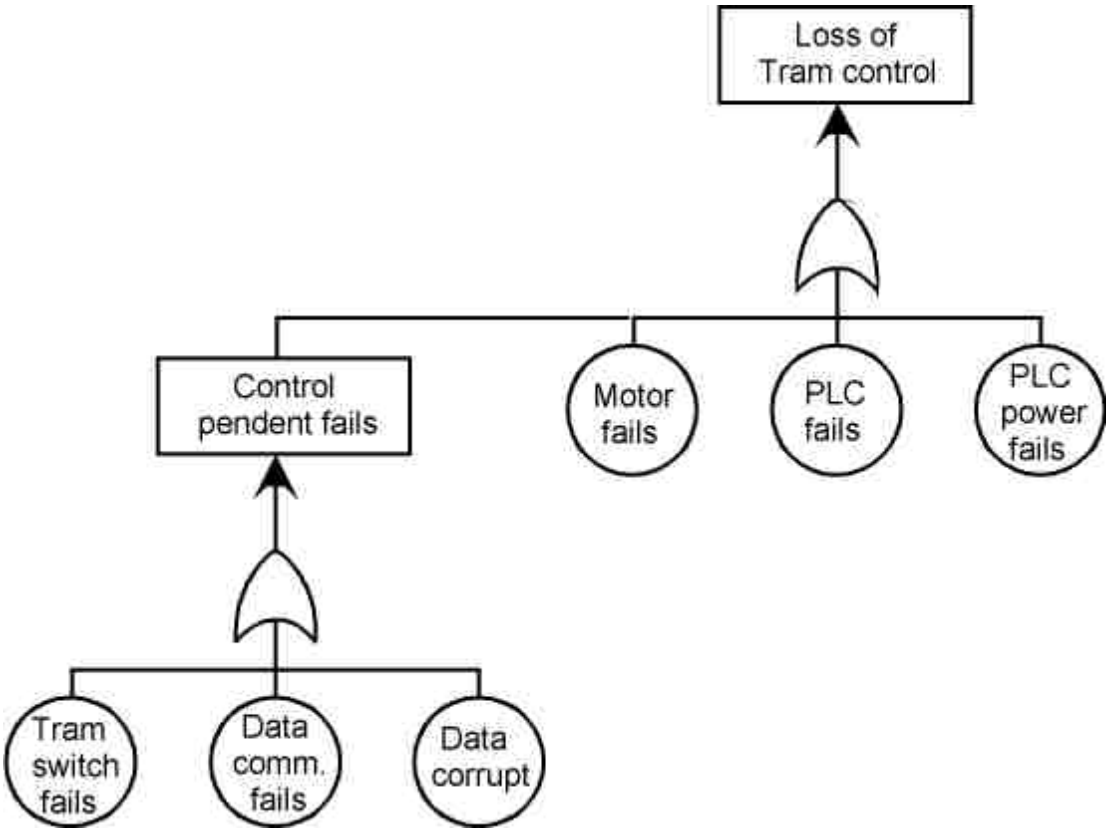


Figure 20.—Fault tree for the loss of tram control hazardous event.

9.6 Risk Determination

The following hazards have been identified:

- Hazard 1: Loss of machine control
- Hazard 2: Unexpected machine movement

The risk assessment matrix (Table 10) is used to determine the level of risk for each hazard and the associated SIL for a safety function to mitigate the hazard. The parameters of severity and frequency are needed to use the risk assessment matrix. The severity is defined by the classifications shown in Table 8; frequency is defined by the classifications in Table 9.

Both hazards could potentially cause a fatality if the machine movement pinned or crushed a miner; therefore, the severity is "catastrophic" based on the severity categories in Table 8. For example purposes, the frequency for each hazard is about once every 2 years based on MSHA accident data for similar machines; therefore, the frequency is classified as "probable" based on the frequency categories in Table 9. The risk for each hazard is unacceptable and assigned an SIL 3 based on the risk assessment matrix in Table 10. The SIL for each hazard is summarized in Table 17.

Table 17.—Hazard summary

Hazard	Description	SIL
H1	Loss of machine control	3
H2	Unexpected machine movement	3

9.7 Safety Requirements

At this point, the hazards H1 and H2 have been identified and assessed as SIL 3. The design strategy is to provide an emergency stop safety function to mitigate these hazards. The safety function requirements are defined in terms of functional requirements and safety integrity (performance) requirements.

9.7.1 Emergency Stop Function Safety Requirements

The safety requirements are specified in terms of functional and safety integrity requirements as shown in Figure 4, “Overall Safety Requirements.”

9.7.1.1 Functional Requirements

Description: The emergency stop function shall shut down the machine such that it stops movement of the machine and all electrical or hydraulic driven devices on the machine.

Associated Hazard(s):
Loss of machine control. Reference hazard H1 of the hazard and risk analyses.
Unplanned movements. Reference hazard H2 of the hazard and risk analyses.

Default State: Tripped (deenergized to the shutdown state).

Safe State(s): Deenergized to trip to a safe state.

Triggering Event(s): Manually pushing in the emergency stop switch shall trigger the emergency stop function.

A single action shall trigger the emergency stop function (see **NOTE 29**).

Reset: Manual reset of devices such as switches and circuit breakers. No automatic resetting of this safety function.

Human/Machine Interface: The interface between the human and machine shall be via a hermetically sealed, pushbutton-type switch.

Human Factors:

The emergency stop function shall be readily accessible and clearly marked for its intended purpose (see **NOTE 29**).

A large red button shall be used for invoking the emergency stop function.

Depressing the button shall trip the emergency stop.

The state of the emergency stop function shall be readily determined by visible inspection of the pushbutton-type switch as follows (see **NOTE 29**):

- The button is down for the duration of the tripped state.
- The button is up during the operational state.

The emergency stop switch shall be clearly visible, yet physically protected from false trips caused by accidental contact (see **NOTE 29**).

The button must be physically reset once the button is depressed.

Response Times:

The emergency stop function shall be completed within 500 milliseconds of its triggering. This includes the response time of the machine's hydraulic and electrical control systems.

NOTE 29: These requirements are derived from the human factors checklist in Appendix A of the system safety recommendations [Sammarco and Fisher 2001].

9.7.1.2 Safety Integrity Requirements:

Target SIL: SIL 3

Diagnostic Requirements: None

Test Requirements:

- Manual test of the emergency stop function at least once per year
- Manual test results should be documented

Constraints: The nuisance trip rate MTTFS shall be less than once per year.

Performance: The safety function demand is once per year (low-demand mode of operation).

9.8 Designate the Safety-critical Areas

The objective of this phase is to assign safety functions to various PE-based and non-PE-based safety systems. The emergency stop function of this example is implemented using two different design approaches.

The first approach assigns the safety function to a non-PE-based safety system. The design uses a dedicated hard-wired circuit; thus, two principles of safe design are followed:

(1) Keep the design simple.
(2) Physically and logically separate the safety and control functions.

The second approach assigns the safety function to an existing PE-based system that implements some of the machine's control functions; therefore, this design does not physically and logically separate the safety function from the machine's control functions.

9.9 Realization Process

The emergency stop function allows a worker to stop the machine in emergency situations. The design uses a pushbutton switch to trip the main line circuit breaker to the machine. All electrical power to the machine is interrupted, thus stopping the machine's traction motors and hydraulic pump.

Two examples are given for the dedicated hard-wired design. The first example uses a generic switch; the second increases the safety performance to SIL 3 by using redundant switches specifically designed for emergency stop functions.

Two examples are given for the PLC-based design. The first example uses an industrial PLC; the second design increases the safety performance to SIL 3 by using a safety PLC.

NOTE 30: Realization requires that random and systematic errors be addressed. Examples 8–11 only address random failures for the system's hardware components. The examples do not address software or the performance of the human operator.

NOTE 31: Examples 8–11 pertain to a safety function performance of SIL 3. This does not imply that all safety functions should be required to meet SIL 3.

NOTE 32: Examples 8–11 are not meant to imply that a human-initiated emergency stop system alone can meet the examples' SIL 3 safety requirement.

9.9.1 Example 8 (see NOTES 30–32): Generic Switch-based Design

The design uses a generic switch directly wired to the main line circuit breaker, as shown in Figure 21. The design can be abstracted as a sensor, logic solver, and field device. The switch is the sensor; the logic solver is the wire; the field device is the circuit breaker. This design is for example purposes. An alternate design would interrupt a pilot circuit instead of tripping a circuit breaker.

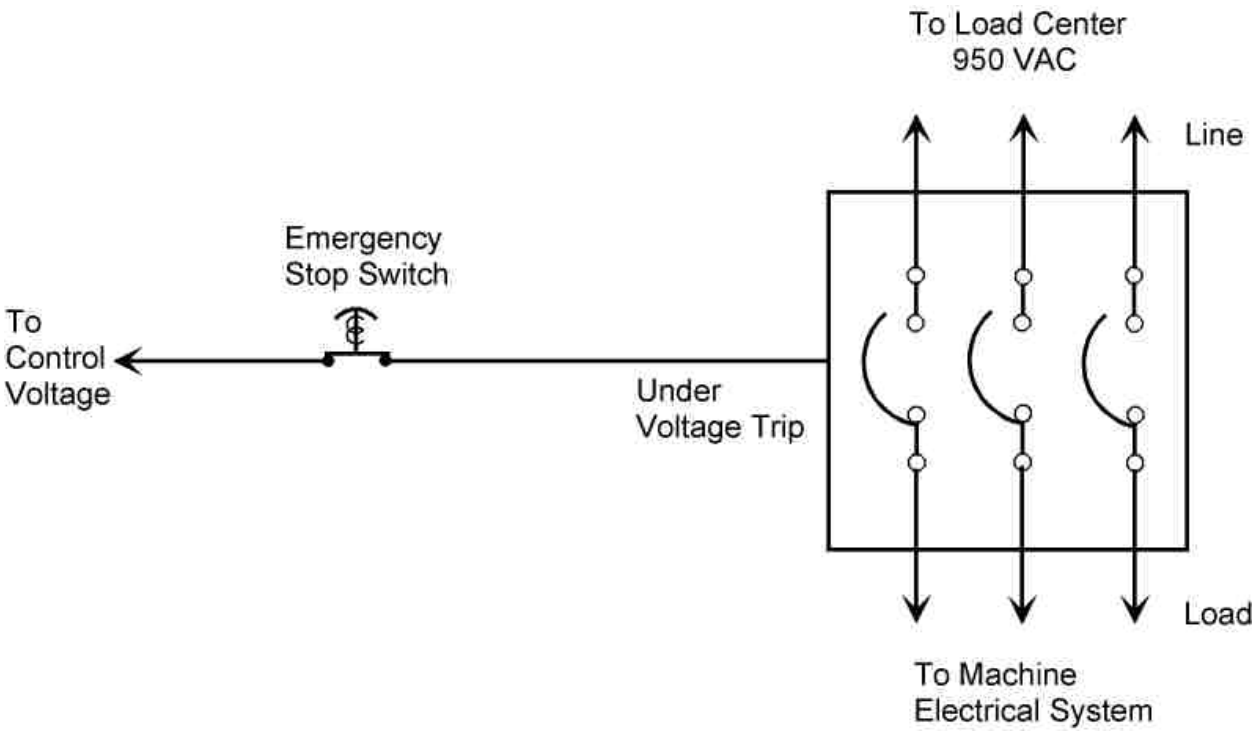


Figure 21.—Emergency stop system using a single, generic switch.

This is a simplex system (1oo1 architecture), so common cause is not considered. None of the components have diagnostics, so safe and dangerous failures are not detected. The following parameters are given:

MTTR = 4 hours

Test interval (TI) = once per year (8,760 hours)

Diagnostic coverage (DC) = 0 (because diagnostics are not used)

Switch parameters:

Failure rate = 1×10^{-6}
20% of failures are safe (switch fails open) = $.20 \times 10^{-6}$
80% of failures are dangerous (switch fails closed) = $.80 \times 10^{-6}$
$\lambda_{DD} = 0$
Normal state = closed

Wire parameters:

Failure rate = 1.1×10^{-8}
90.9% of failures are safe (wire fails open) = 1.0×10^{-8}
9.1% of failures are dangerous (wire fails closed) = $.1 \times 10^{-8}$

Circuit breaker (cb) parameters:

Failure rate = 1.5×10^{-6}
92% of failures are safe (circuit breaker fails open) = 1.38×10^{-6}
8% of failures are dangerous (circuit breaker fails closed) = $.12 \times 10^{-6}$

9.9.1.1 SIL Verification

The SIL is verified by using the simplified equations to find the PFD_{avg} of each component and of the system. The claimed SIL for each component is checked for architectural constraints listed in Table 12.

$PFD_{switch} = \lambda_{DU} \times (TI / 2)$
$PFD_{switch} = (0.80 \times 10^{-6}) \times (8{,}760 / 2)$
$PFD_{switch} = 3.5 \times 10^{-3}$

$PFD_{wire} = \lambda_{DU} \times (TI / 2)$
$PFD_{wire} = 4.38 \times 10^{-6}$

$PFD_{cb} = \lambda_{DU} \times (TI / 2)$
$PFD_{cb} = 5.2 \times 10^{-4}$

$PFD_{system} = PFD_{switch} + PFD_{wire} + PFD_{cb}$
$PFD_{system} = (3.5 \times 10^{-3}) + (4.38 \times 10^{-6}) + (5.2 \times 10^{-4})$
$PFD_{system} = 4.02 \times 10^{-3}$ (SIL 2)

At this point of the verification, the design using a generic pushbutton switch does not meet SIL 3. It is pointless to continue the analysis to determine if any architectural constraints would apply (see Table 12 for constraints). The switch is a limiting component of the design because it only meets SIL 2. The safety performance can be improved by using a switch having a lower failure rate and by adding fault tolerance.

9.9.2 Example 9 (see NOTES 30–32): Redundant Emergency Stop Switch-based Design

The safety performance is increased by changing from a 1oo1 design to a design using a switch with a lower dangerous failure rate and configured in a 1oo2 architecture, as depicted in Figure 22; thus, the system can tolerate one fault.

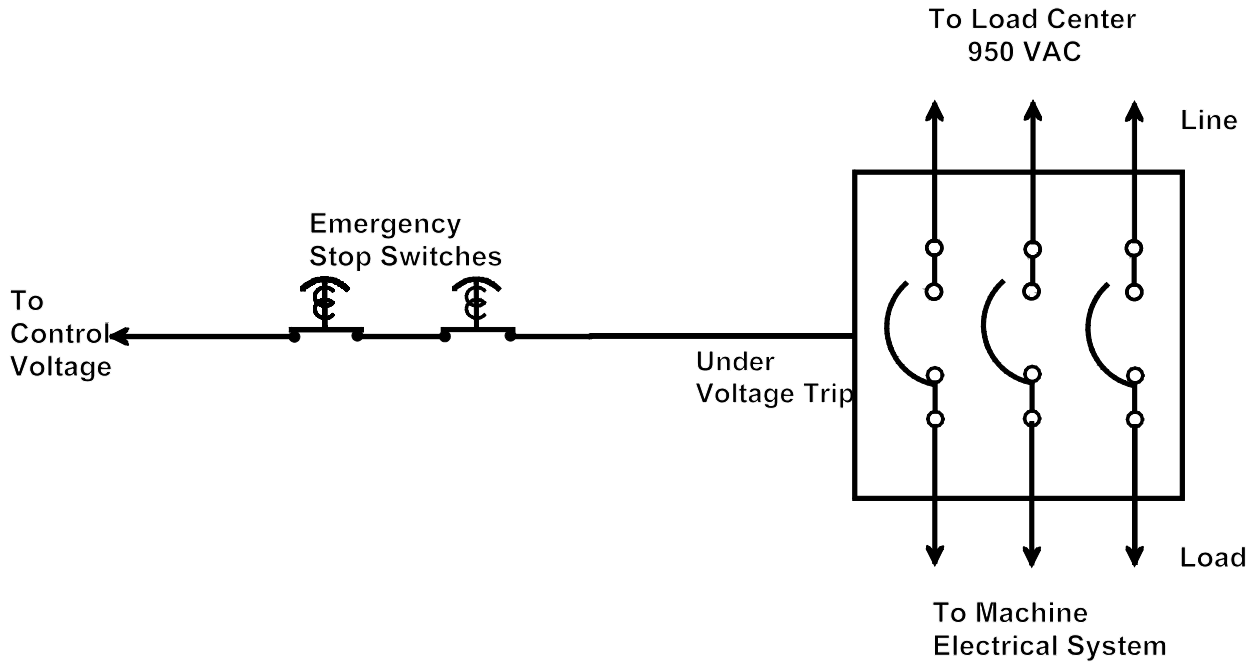


Figure 22.—Emergency stop system using lower failure rate switches.

Low failure rate switch parameters:

Failure rate = 1×10^{-6}
60% of failures are safe (switch fails open) = $.60 \times 10^{-6}$
40% of failures are dangerous (switch fails closed) = $.40 \times 10^{-6}$
$\lambda_{DD} = 0$

9.9.2.1 SIL Verification

$PFD_{1oo2\ switch} = ((\lambda_{DU})^2 \times TI^2) / 3$
$PFD_{1oo2\ switch} = ((.40 \times 10^{-6})^2 \times (8{,}760)^2) / 3$
$PFD_{1oo2\ switch} = 4.1 \times 10^{-6}$

The PFD_{avg} for the wire and circuit breaker are unchanged from the previous example.

$PFD_{wire} = 4.38 \times 10^{-6}$
$PFD_{cb} = 5.2 \times 10^{-4}$

The PFD_{avg} for the system is:

$PFD_{system} = (4.1 \times 10^{-6}) + (4.38 \times 10^{-6}) + (5.2 \times 10^{-4})$
$PFD_{system} = 5.29 \times 10^{-4}$ (SIL 3)

At this point of the verification the improved design meets SIL 3; however, the verification is not completed because the system architecture restriction has not been taken into account. Table 12 is used for this purpose because the system is type A.

The SFF and fault tolerance 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:

$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD}) / (\Sigma\lambda_S + \Sigma\lambda_D)$
$\Sigma\lambda_S = (.60 \times 10^{-6}) + (1.0 \times 10^{-8}) + (1.38 \times 10^{-6}) = 1.99 \times 10^{-6}$
$\Sigma\lambda_D = (.40 \times 10^{-6}) + (.10 \times 10^{-8}) + (.12 \times 10^{-6}) = 5.21 \times 10^{-7}$
$\Sigma\lambda_{DD} = 0$ (because no diagnostics)
$SFF = .793$, or 79.3%

The maximum SIL that can be claimed is SIL 3 using Table 12 with SFF = 79.3% and a hardware fault tolerance of one; therefore, the SIL is not constrained by the architecture. Thus, this design is verified to meet the target of SIL 3.

9.9.3 Example 10 (see NOTES 30–32): An Industrial PLC-based Emergency Stop System

The design uses an existing PLC that provides control functions, as shown in Figure 23. The first conceptual design consists of a pushbutton switch, PLC, and hydraulic pump actuator connected in series, as depicted in Figure 24. In essence, the PLC is "shared" for control and safety functions. This design does not follow the principle of independent safety and control functions.

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

Industrial PLC parameters:

Failure rate = 3.8×10^{-6}
55.6% of failures are safe = 2.11×10^{-6}
44.4% of failures are dangerous = 1.69×10^{-6}
Diagnostics can detect 50% of the safe failures
Diagnostics can detect 35% of the dangerous failures

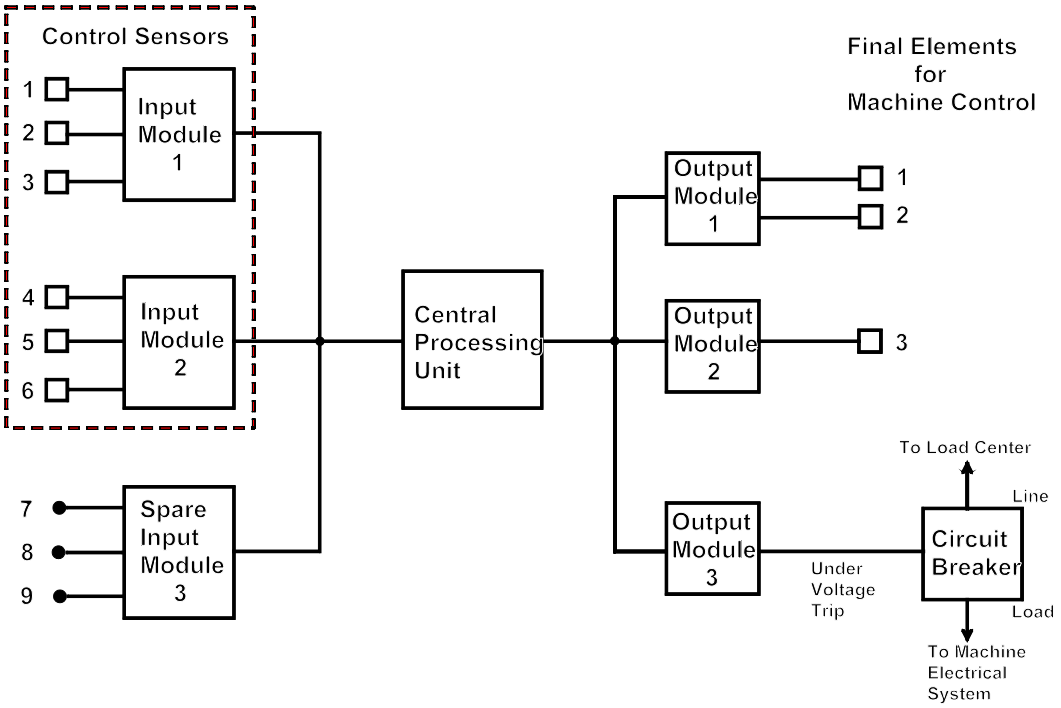


Figure 23.—A 1oo1 industrial PLC used for machine control.

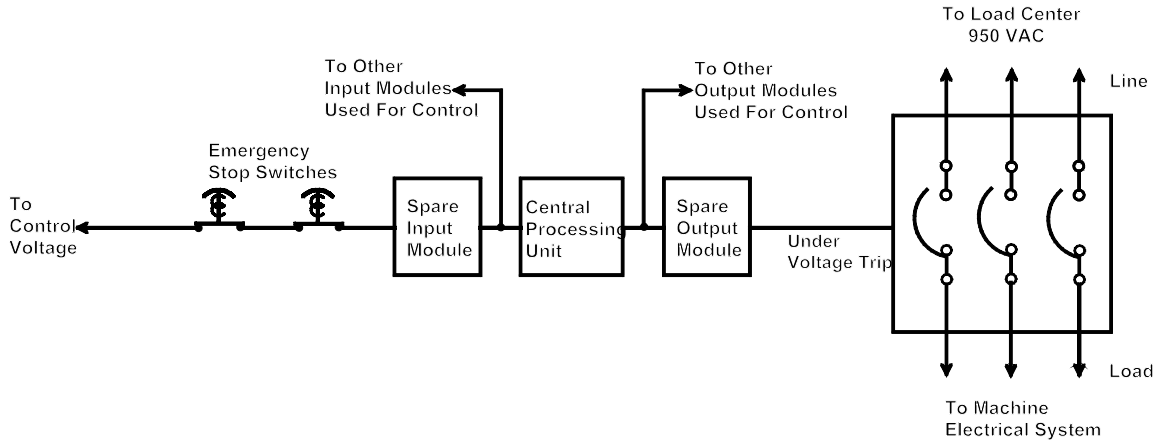


Figure 24.—Conceptual diagram of a PLC-based safety system that shares a 1oo1 industrial PLC used for machine control.

9.9.3.1 SIL Verification

The achieved SIL of this design is verified with the aid of the PC-based software tool FSC SafeCalc (hpsweb.honeywell.com/Cultures/en-US). The software tool performs the calculations of PFD_{avg} given the system architecture and parameters that are supplied by the user. The following parameters are used by the tool:

β [%]	The β-factor or common cause factor. This factor is not applicable to 1oo1 or 1oo1 architectures with diagnostics (1oo1D); therefore, the value "–" is shown.
Type A/B	Component type A or B
λ [1/h]	Failure rate (failures per hour)
MTTF [years]	The mean time to fail (in years)
[%] Safe	The percentage of component failures that result in a safe failure where: [%] Safe = $\lambda_S / (\lambda_S + \lambda_D)$

NOTE 33: This parameter is similar to SFF.

DC Safe	Diagnostic coverage for safe failures
DC Dangerous	Diagnostic coverage for dangerous failures
MTTR [hour]	Mean time to repair (in hours)
TI [months]	Testing interval (in months)

The tool calculates PFD_{avg} for each component and for the system, the SIL, risk and the architectural constraints. Figure 25 shows the results from the SIL tool. The results show that when using this PLC, the 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 industrial PLC. Increasing the redundancy of the switches or circuit breaker will not increase the system SIL.

Group name	Voting	Group type	β [%]	Component name	Type A/B	λ [1/h]	[%]λ Safe	DC Safe	DC Dang.	MTTR [hour]	TI [Months]	PFDavg Part
Switch	1oo2	Redundant	0	ESW-1	A	1.0E-6	60	0	0	4	12	4.08E-06
Industrial PLC	1oo1	Single	-	GA-1	B	3.8E-6	55.6	50	35	4	12	4.79E-03
Circuit Breaker	1oo1	Single	-	LV-CB1	A	1.5E-6	92	0	0	4	12	5.25E-04

Fractional Process Deadtime
Spurious Trip Rate per year

Average Probability of Failure on Demand **5.32E-03**
Safety Integrity Level **1**
Risk Reduction Factor **1.88E+02**
SIL restricted by architectural constraints

Figure 25.—Results from an SIL tool verification of a 1oo2 switch and a 1oo1 industrial PLC. This system meets SIL 1.

The manual calculations of PFD_{avg} for the switch and circuit breaker were done in example 9. The values are similar to those obtained by the SIL tool. For instance, the manual calculation for the circuit breaker was $PFD_{cb} = 5.2 \times 10^{-4}$, and the SIL tool calculation was $PFD_{cb} = 5.25 \times 10^{-4}$. Using the same formulas from example 9, the manual calculation for the PLC results in $PFD_{plc} = 4.77 \times 10^{-3}$. The SIL tool results are more accurate because the equations used by example 9 are approximations.

9.9.4 Example 11: A Safety PLC-based Emergency Stop System

This design example changes the industrial PLC to a safety PLC that is certified to SIL 3. Figure 26 shows the results from the SIL tool. The results show that when using a safety PLC, the SIL = 3. Therefore, by adding one safety function to the industrial PLC used for control, the entire industrial PLC must be replaced with a more costly safety PLC certified to SIL 3 even though the industrial PLC was sufficient for control.

9.9.5 Limitations

The realization phase thus far has addressed the hardware component of the design; however, the realization phase has not been completed because software and human performance have not been addressed.

Human performance is critical for examples 8–11 because the human is a part of the system; the human must initiate the emergency stop. The human element poses significant limitations. For instance, a human might not recognize the need to activate the emergency stop function. Also, there are situations in which the human might not be able to physically reach the emergency stop in time. Human reliability analysis is used to determine human errors such that it can be factored into quantitative SIL verification. Generally, the $PFD_{avg} = 1 \times 10^{-1}$ for human actions; thus, the human operator marginally achieves SIL 1.

It is apparent that the human-activated emergency stop system needs to be combined with additional layers of protection. For example, an independent external watchdog timer circuit that automatically monitors the safety PLC could be used as a second-layer protection.

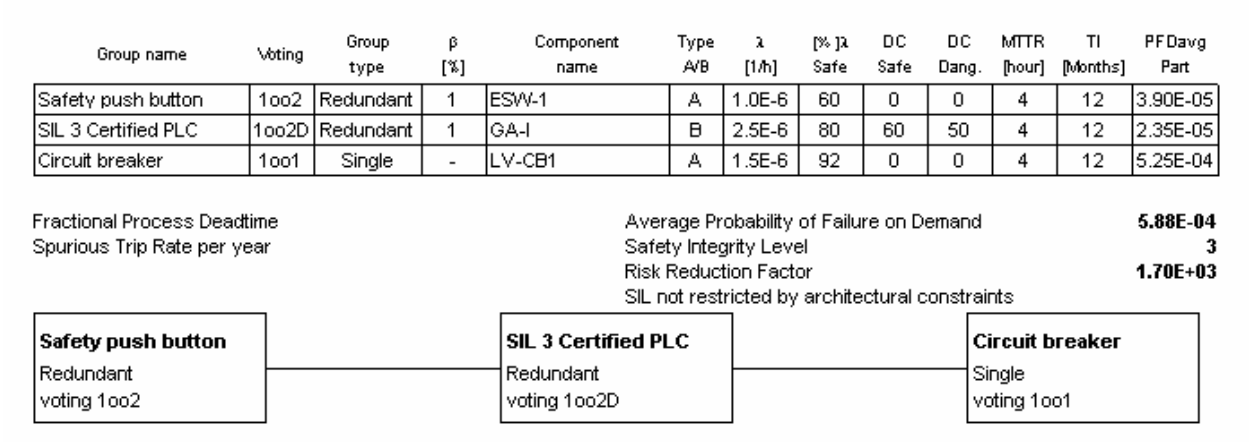


Figure 26.—Results from an SIL tool verification of a 1oo2 system with a safety PLC. This system meets SIL 3.

REFERENCES

Beizer B [1990]. Software testing techniques. 2nd ed. London: International Thomson Computer Press.

British Standards Institute [1997]. Safety of machinery: safety related parts of control systems, part 1: general principles for design. London: British Standards Institute, BS EN–954–1, pp. 6–11.

Center for Chemical Process Safety [1994]. Guidelines for preventing human error in process safety. New York, NY: American Institute of Chemical Engineers, Center for Chemical Process Safety.

exida.com [2003]. Safety equipment reliability handbook. Munich, Germany: exida.com, L.L.C.

Fries EF, Fisher TJ, Jobes CC [2001]. Programmable electronic mining systems: best practice recommendations (in nine parts). Part 3: 2.2 Software safety. Pittsburgh, PA: U.S. Department of Health and Human Services, Public Health Service, Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health, DHHS (NIOSH) Publication No. 2001–164, IC 9460.

Gruhn P, Cheddie HL [1998]. Safety shutdown systems: design, analysis and justification. Research Triangle Park, NC: The Instrumentation, Systems, and Automation Society (ISA), p. 121.

Harms-Ringdahl L [1993]. Safety analysis: principles and practice in occupational safety. London: Elsevier.

Harsh DD, Pederson AE [1997]. Accident investigation report, surface nonmetal mine, fatal machinery accident, Yakima – Pre-Mix #6, Central Pre-Mix Concrete Company, Yakima, Yakima County, Washington, mine ID No. 45–00995. Vacaville, CA: U.S. Department of Labor, Mine Safety and Health Administration, January 8.

Hawkins FH [1993]. Human factors in flight. 2nd ed. Brookfield, VT: Ashgate Publishing Co.

IEC [1998a]. Functional safety of electrical/electronic/programmable electronic safety-related systems. Geneva, Switzerland: International Electrotechnical Commission, Draft IEC 61508–1, Part 1: General requirements, version 4, May 12, 1998.

IEC [1998b]. Functional safety of electrical/electronic/programmable electronic safety-related systems. Geneva, Switzerland: International Electrotechnical Commission, Draft IEC 61508–2, Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems, version 4, May 12, 1998.

IEC [1998c]. Functional safety of electrical/electronic/programmable electronic safety-related systems. Geneva, Switzerland: International Electrotechnical Commission, Draft IEC 61508–3, Part 3: Software requirements, version 4, May 12, 1998.

IEC [1998d]. Functional safety of electrical/electronic/programmable electronic safety-related systems. Geneva, Switzerland: International Electrotechnical Commission, Draft IEC 61508–4, Part 4: Definitions and abbreviations, version 4, May 12, 1998.

IEC [1998e]. Functional safety of electrical/electronic/programmable electronic safety-related systems. Geneva, Switzerland: International Electrotechnical Commission, Draft IEC 61508–5, Part 5: Examples of methods for determination of safety integrity levels, version 4, May 12, 1998.

IEC [1998f]. Functional safety of electrical/electronic/programmable electronic safety-related systems. Geneva, Switzerland: International Electrotechnical Commission, Draft IEC 61508–6, Part 6: Guidelines on the application of parts 2 and 3, version 4, May 12, 1998.

IEC [1998g]. Functional safety of electrical/electronic/programmable electronic safety-related systems. Geneva, Switzerland: International Electrotechnical Commission, Draft IEC 61508–7 Part 7: Overview of techniques and measures, version 4, May 12, 1998.

ISA [1998a]. Safety instrumented systems (SIS): safety integrity level (SIL) evaluation techniques. Part 1: Introduction. ISA dTR84.0.02, draft, version 4. Research Triangle Park, NC: The Instrumentation, Systems, and Automation Society.

ISA [1998b]. Safety instrumented systems (SIS): safety integrity level (SIL) evaluation techniques. Part 2: Determining the SIL of an SIS via simplified equations. ISA dTR84.0.02, draft, version 4. Research Triangle Park, NC: The Instrumentation, Systems, and Automation Society.

ISA [1998c]. Safety instrumented systems (SIS): safety integrity level (SIL) evaluation techniques. Part 3: Determining the SIL of an SIS via fault-tree analysis. ISA dTR84.0.02, draft, version 4. Research Triangle Park, NC: The Instrumentation, Systems, and Automation Society.

ISA [1998d]. Safety instrumented systems (SIS): safety integrity level (SIL) evaluation techniques. Part 4: Determining the SIL of an SIS via Markov analysis. ISA dTR84.0.02, draft, version 4. Research Triangle Park, NC: The Instrumentation, Systems, and Automation Society.

ISA [1998e]. Safety instrumented systems (SIS): safety integrity level (SIL) evaluation techniques. Part 5: Determining the PFD of SIS logic solvers via Markov analysis. ISA dTR84.0.02, draft, version 4. Research Triangle Park, NC: The Instrumentation, Systems, and Automation Society.

Leveson NG [1995]. Safeware: system safety and computers. Boston, MA: Addison-Wesley Professional.

Norwegian University of Science and Technology [2005]. Data sources for risk and reliability studies. [http://www.ntnu.no/ross/info/data.php]. Date accessed: May 2005.

Reliability Analysis Center [1995]. NPRD–95: Nonelectronic parts reliability data, 1995. Rome, NY: Reliability Analysis Center.

Redmill F, Chudleigh M, Catmur J [1999]. System safety: HAZOP and software HAZOP. New York: John Wiley & Sons, Inc.

Sammarco JJ, Fisher TJ [2001]. Programmable electronic mining systems: best practice recommendations (in nine parts). Part 2: 2.1 System safety. Pittsburgh, PA: U.S. Department of Health and Human Services, Public Health Service, Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health, DHHS (NIOSH) Publication No. 2001–137, IC 9458.

Sammarco JJ, Fries EF [2003]. Programmable electronic mining systems: best practice recommendations (in nine parts). Part 5: 4.0 Independent functional safety assessment. Pittsburgh, PA: U.S. Department of Health and Human Services, Public Health Service, Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health, DHHS (NIOSH) Publication No. 2003–138, IC 9464.

Sammarco JJ, Kohler JL, Novak T, Morley LA [1997]. Safety issues and the use of software-controlled equipment in the mining industry. In: Proceedings of the IEEE Industrial Applications Society 32nd Annual Meeting (New Orleans, LA, October 5–9, 1997). New York: Institute of Electrical and Electronics Engineers, Inc.

Sammarco JJ, Fisher TJ, Welsh JH, Pazuchanics MJ [2001]. Programmable electronic mining systems: best practice recommendations (in nine parts). Part 1: 1.0 Introduction. Pittsburgh, PA: U.S. Department of Health and Human Services, Public Health Service, Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health, DHHS (NIOSH) Publication No. 2001–132, IC 9456.

SINTEF [1989]. Reliability data for control and safety systems. Trondheim, Norway: SINTEF.

SINTEF [1997]. Offshore reliability data handbook (OREDA 1997). 3rd ed. Høvik, Norway: Det Norske Veritas.

Stephans RA, Talso WW [1997]. System safety analysis handbook. 2nd ed. Albuquerque, NM: The System Safety Society, section 3.

U.K. Ministry of Defence [1998a]. HAZOP studies on systems containing programmable electronics. Defence Standard 00–58. Part 1. Requirements. Glasgow, U.K.: Ministry of Defence, Directorate of Standardisation.

U.K. Ministry of Defence [1998b]. HAZOP studies on systems containing programmable electronics. Defence Standard 00–58. Part 2. General application guidance. Glasgow, U.K.: Ministry of Defence, Directorate of Standardisation.

U.S. Department of Defense [1980]. Procedures for performing a failure mode effects and criticality analysis. Military Standard MIL–STD–1629A. Washington, DC: U.S. Department of Defense.

U.S. Department of Defense [1993]. System safety program requirements. Military Standard MIL–STD–882C. Washington, DC: U.S. Department of Defense.

Vesely WE, Goldberg FF, Roberts NH, Haasl DF [1981]. Fault-tree handbook (NUREG-0492). Washington, DC: U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Systems and Reliability Research.

APPENDIX A.—INFORMATION RESOURCES

Use of specific names is for identification purposes only and does not imply endorsement by the National Institute for Occupational Health and Safety.

Commercial Sources for Standards

Document Center, Inc.
111 Industrial Rd., Suite 9
Belmont, CA 94002
Phone: 650–591–7600, fax: 650–591–7617
www.document-center.com
e-mail: info@document-center.com

Global Engineering Documents
15 Inverness Way East
Englewood, CO 80112–5704
Phone: 303–792–2181 or 1–800–854–7179
www.ihs.com

Total Information, Inc.
844 Dewey Ave.
Rochester, NY 14613
Phone: 1–800–876–4636

777 East Eisenhower Parkway
Ann Arbor, MI 48108
Phone: 800–699–9277
www.techstreet.com

Internet Sites for Standards Organizations

ANSI Home Page
www.ansi.org

National Standards Systems Network (NSSN) Directory of Standards
www.nssn.org

The IEEE Home Page
www.ieee.org

The Institution of Electrical Engineers (IEE), U.K.
www.iee.org

ISA Standards
www.isa.org

Standards Australia
www.standards.org.au

Standards New Zealand
www.standards.co.nz

U.S. Department of Defense military standards pertaining to software
tecnet0.jcte.jcs.mil/htdocs/dodinfo/index.html

International Organization for Standardization (ISO)
www.iso.ch

Underwriters Laboratories, Inc. (UL)
www.ul.com

International Electrotechnical Commission (IEC)
www.iec.ch

Safety-related Internet Sites

The American Society of Safety Engineers
www.asse.org

Safety-critical Systems Virtual Library
vl.fmnet.info/safety

Safety-related Internet Resources
www.christie.ab.ca/safelist

Software Safety (Massachusetts Institute of Technology, Nancy Leveson, Ph.D.)
sunnyday.mit.edu

Safeware Engineering Corp.
www.safeware-eng.com

The System Safety Society, Inc.
www.system-safety.org

ReadySET template/checklist system for system design requirements
readyset.tigris.org
www.readysetpro.com

The IEC 61508 Functional Safety Zone
www.iec.ch/zone/fsafety

The Motor Industry Software Reliability Association (MISRA)
www.misra.org.uk/index.htm

Organization Acronyms

AIAA	American Institute of Aeronautics and Astronautics Phone: 202–646–7463, fax: 202–646–7508
ANSI	American National Standards Institute Phone: 212–642–4900, fax: 212–302–1286
ASME	American Society of Mechanical Engineers Phone: 212–705–7722, fax: 212–705–7437 or 212–980–4681
ATA	Air Transport Association of America Phone: 202–626–4000
BCS	British Computer Society Contact: Ian Jones, e-mail: ijones@bcs.org.uk
DIN	German Institute for Standardization Phone: (4930) 2601–0
EIA	Electronic Industries Association Phone: 800–854–7179
HSE	Health and Safety Executive, U.K. Phone: (0742) 752539
IEC	International Electrotechnical Commission Phone: 022–734–0150
IEE	Institution of Electrical Engineers, U.K. Phone: +44 (0) 1438 313311, fax: +44 (0) 1438 313465 e-mail: webmaster@iee.org.uk, gopher.iee.org.uk

IEEE	Institute of Electrical and Electronics Engineers, Inc. Phone: 212–705–7900, fax: 212–752–4929
ISA	The Instrumentation, Systems, and Automation Society Phone: 919–549–8411, fax: 919–549–8288
ISO	International Organization for Standardization
MIL–STD	Military Standard, U.S.
MSHA	Mine Safety and Health Administration, U.S.
MOD	Ministry of Defense, U.K.
NASA	National Aeronautics and Space Administration
NEMA	National Electrical Manufacturers Association Phone: 202–457–8400
NIOSH	National Institute for Occupational Safety and Health, U.S.
RAC	Reliability Analysis Center rac.alionscience.com Phone: 888–RAC–USER; fax: 315–337–9932
RIA	Robotics Industry Association Phone: 313–994–6088; fax: 313–994–3338
UL	Underwriters Laboratories, Inc. Phone: 847–272–8800

APPENDIX B.—FREQUENTLY ASKED QUESTIONS (FAQs)

The following questions were asked during NIOSH-MSHA Best Practice Recommendations workshops in the United States and during two similar workshops given in Australia.

- **If a system is reliable, does that mean it is also safe?**

Often, safety and reliability are incorrectly equated in the sense that if a system is reliable, then it is safe. Reliability alone is not sufficient for safety. For example, a reliable system could have unsafe functions and conditions, or it could neglect to provide all the necessary safety functions. The result is a reliably unsafe system! Also, reliability is concerned with random failures; however, failures are not always needed to cause an unsafe condition. Safety is concerned with systematic and random failures and events that impact safety.

Safety is "freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment [U.S. Department of Defense 1993]." Reliability is "the probability that a piece of equipment or component will perform its intended function satisfactorily for a prescribed time and under stipulated environmental conditions" [Leveson 1995]. Thus, a system could be reliable but unsafe, or a system could be safe but unreliable.

- **What is a system?**

One of the first steps of a safety analysis is to define the system. A clear definition of the system is required so that hazards are not omitted from safety analyses. This document defines a system as:

> A set of elements that interact according to a design, where an element of a system can be another system, called a subsystem, which may be a controlling system or a controlled system and may include hardware, software, and human interaction. Hardware, software, and humans can be system elements.

Hawkins [1993] presents the SHEL model of a system. The SHEL model is composed of (S)oftware, (H)ardware, (E)nvironment, and (L)iveware or humans (see Figure B–1). The SHEL model of a system is consistent with our definition of a system.

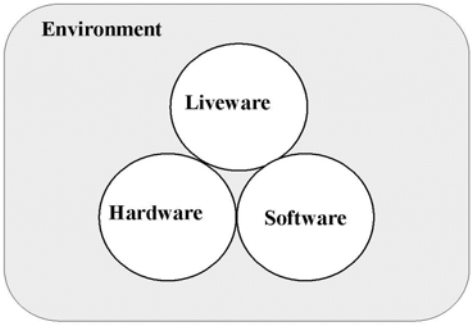


Figure B–1.—The SHEL model of a system.

- **What is the system safety approach?**

System safety, as defined by MIL–STD–882C is "the application of engineering and management principles, criteria, and techniques to achieve acceptable risk, within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle" [U.S. Department of Defense 1993]. System safety received much scientific attention during and after World War II. This was the time when most of our traditional safety techniques were developed to address new challenges posed by systems that were more complex due to the use of new technology [Leveson 1995]. The traditional "fly-fix-fly" approach to safety did not work well with these complex systems. It was too dangerous, costly, and wasteful to continue with this "after-the-fact approach," so the system safety concept was initiated as a "before-the-fact" process. The key system safety concepts are:

(1) Integrating safety into the design
(2) Systematic hazard identification and analysis
(3) Addressing the entire system in addition to the subsystems and components
(4) Using qualitative and quantitative approaches

The system safety process is documented in MIL–STD–882, the most widely known safety standard. Existing safety standards are built upon collections of expertise and experiences (lessons learned) involving fatalities, injuries, and near-misses. In general, standards also provide uniform, systematic approaches. History has shown standards are effective tools for safety.

A common thread among the standards is hazard management; it is core to the system safety approach. The system safety approach includes a combination of managerial and technical tasks to identify and evaluate hazards and to eliminate, reduce, and control hazards through analysis, design, and management procedures.

- **Why use the safety life cycle?**

The use of a safety life cycle is required to ensure that safety is applied in a systematic, comprehensive manner, thus reducing the potential for systematic errors. The safety life cycle concept is applied during the entire life of the system. Hazards can become evident at later stages, or new hazards can be introduced by system modifications. Table 1 of this document lists the safety life cycle phases.

The safety life cycle must be integrated within the overall product development life cycle because safety issues impact overall development issues and vice versa. Secondly, an integrated approach minimizes the likelihood of addressing safety as an afterthought of the system design.

- **Do faults, errors, and failures all refer to the same concept?**

There is much confusion about faults, errors, and failures. Often the terms are used interchangeably. The relationship between a fault, error, and failure is shown in Figure B–2. The following discussion serves to clarify the terminology.

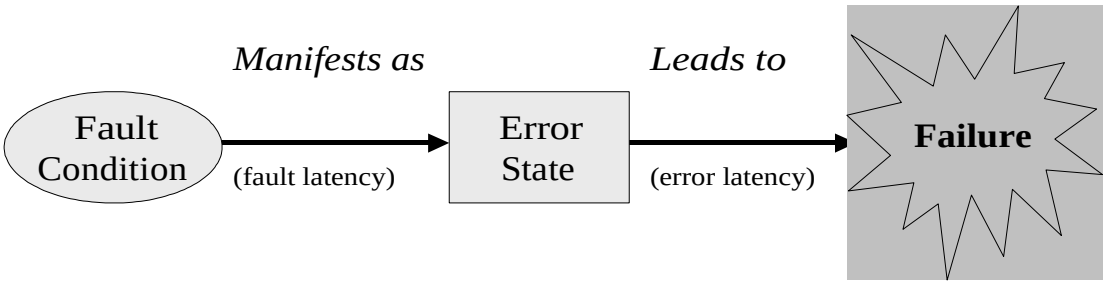


Table B–2.—Fault, error, and failure relationship.

A *failure* is the termination of the ability to perform an intended function. This definition is based on a performance of a function, so failure is a behavior occurring at an instance of time. A *fault* is an abnormal condition. Faults are random (hardware) or systematic (hardware or software). Random faults are due to physical wearout, degradation, or defects; they can be accurately predicted and quantified. Systematic faults pertain to the specification, design, and implementation and are unpredictable. Therefore, software faults are systematic. Faults, both random and systematic, may lead to errors.

An *error* is a system state that has the potential to lead to a failure. When a fault results in an error, the error is then a manifestation of the fault and the fault becomes apparent. Not all faults lead to errors or failures. Some faults are benign or are tolerated such that failure does not occur. Some faults are dormant such that an error state or failure does not occur because the proper conditions do not exist. For example, a fault could reside in a section of software. If that section of software is not used, then neither an error state nor failure will exist.

- **Are complex designs required for safety?**

Simplification is one of the most important design aspects for safety. Complexity makes it more difficult to conceptualize, understand, specify, design, test, document, maintain, modify, and review the system. Complexity also makes it more likely for errors, failure, and unplanned interactions that may cause unsafe conditions. In addition, it increases demands on humans to operate and maintain the system. As a result, humans can unknowingly put the system in an unsafe state during operation or maintenance.

- **How does software contribute to complexity?**

Software is especially prone to complexity because it can be nondeterministic, contain numerous branches and interrupts, contain temporal criticality, and consist of hundreds of thousands of lines of code. Software does not exhibit random wearout failures. Instead, software failures result from systematic (logic or design) errors.

Beizer [1990] gives an example illustrating an aspect of software complexity concerning the number of paths for a section of code. Given that a section of software has 2 loops, 4 branches, and 8 states, Beizer calculates the number of paths through this code to exceed 8,000.

- **Should the entire set of NIOSH recommendations be applied to every programable electronic system?**

The recommendations have limited or no applicability as follows:

No applicability:
- Low-complexity systems

Limited applicability:
- Systems, subsystems, and components with a safe proven-in-use history
- Low-risk systems

First, the recommendations do not apply to low-complexity. The system safety recommendations in section 1.5.1 address low-complexity systems as follows [Sammarco and Fisher 2001]:

> These recommendations *do not* apply to low-complexity systems satisfying these criteria:
>
> (1) The failure modes of the system, all subsystems, and components are well defined and understood.
> (2) The system's behavior under all fault conditions can be completely understood.

Secondly, limited applicability depends on the safe service history and the level of risk. Systems, subsystems, and components having a proven and documented safe history of service, but lacking formal and rigorous verification, can be used without following all of the recommendations. Sections 8.0 to 8.9 of the Independent Functional Safety Assessment recommendations address the proven-in-use concept [Sammarco and Fries 2003]. Limited applicability of the recommendations depends on the risk level. The number of recommendation processes decreases as the risk decreases. For example, Table 2 of the Software Safety recommendations [Fries et al. 2001] lists the software verification and validation (V&V) methods recommended for a low-, medium-, and high-risk software. The recommended V&V methods for low-risk are about 65% fewer than those for high-risk.

Lastly, as an example, the recommendations have limited or no applicability for some systems in the stone industry because these systems have a safe proven-in-use service history or they are low-complexity systems. Our recommendations account for both situations. However, a machinery fatality that occurred in 1997 at Yakima Pre-Mix #6 (a sand and gravel wash plant in Yakima, WA) serves as an example for using the complete set of recommendations. The fatality occurred when the blade mill in which a mechanic/repairman was working started up. The MSHA accident investigation report [Harsh and Pederson 1997] states: "A contributing factor was the mis-programming of the programmable logic controller, which permitted equipment to be inadvertently energized without warning."

APPENDIX C.—SAMPLE FORMS FOR HAZARD ANALYSIS

The forms in this appendix serve as examples. These forms can be adapted to create customized forms. They are also intended to help clarify and reinforce the methods presented in this document.

System/Hardware/Software Change Log

Log No.

1. Submitted by: Date
2. Equipment/device name:
3. Customer name:
4. Proposed change:

5. Reason(s) for change:

6. Identify item(s) to change:

7. Safety/permissibility impact analysis results:

8. Change approved by: _____ Date _____

Hazard Log

Log No.

1. Submitted by: Date
2. Equipment/Device Name:
3. Customer Name:
4. Hazard Description:

5. Initial mishap risk index class: A ___, B ___, C ___, D ___
6. Source of hazard discovery:

7. Hazard cause(s):

8. Action(s) to eliminate or control hazard:

9. Hazard status *(Open, Monitor, or Close)*:

   Date: Status:

   Date: Status:

   Date: Status:

10. Final mishap risk index class: A ___, B ___, C ___, D ___

11. Hazard closure approval by: _____ Date _____

Preliminary Hazard Analysis Form

DATE:

COMPILED BY:

VERIFIED BY:

HAZARD DESCRIPTION	HAZARD CAUSES	HAZARD EFFECTS	INITIAL RISK	CONTROL	STATUS

Failure Modes and Effects Analysis (FMEA)

SYSTEM DATE _____

SUBSYSTEM SHEET _____ of _____

COMPILED BY

VERIFIED BY

Item	Function	Failure mode	Cause	Effect	Failure rate	Comments

HAZOP

SYSTEM _____ DATE _____

SUBSYSTEM _____

Team Leader:

Team Members:

Item	Part	Attribute	Guide word	Cause	Consequence	Remediation	Remarks

Delivering on the Nation's promise:
Safety and health at work for all people through research and prevention

For information about occupational safety and health topics contact NIOSH at:

1–800–35–NIOSH (1–800–356–4674)
Fax: 513–533–8573
E-mail: pubstaft@cdc.gov
www.cdc.gov/niosh

SAFER • HEALTHIER • PEOPLE™

DHHS (NIOSH) Publication No. 2005–150