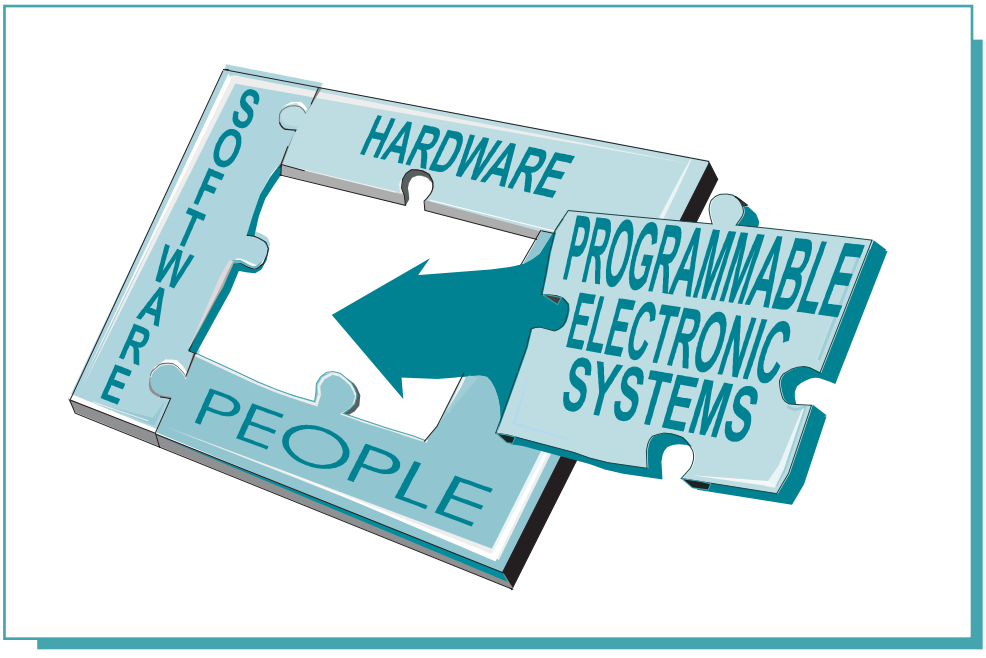
CDC
Workplace Safety and Health

IC 9488

INFORMATION CIRCULAR/2006

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



Part 9: 7.0 Independent Functional Safety Assessment Guidance

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

NIOSH

Information Circular 9488

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

Part 9: 7.0 Independent Functional Safety Assessment Guidance

John J. Sammarco, Ph.D., P.E., and Janet S. Flynt

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

April 2006

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. 2006–131

CONTENTS

Page

ILLUSTRATIONS

TABLES

ABBREVIATIONS USED IN THIS REPORT

CM	continuous mining
DC	diagnostic coverage
E/E/PES	electrical/electronic/programmable electronic system
FSLC	functional safety life cycle
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IFSA	independent functional safety assessment
MCMS	mining control and monitoring system
MSHA	Mine Safety and Health Administration
NIOSH	National Institute for Occupational Safety and Health
PE	programmable electronics
PES	programmable electronic system
PFD_{avg}	average probability of failure on demand
PLC	programmable logic controller
RRF	risk reduction factor
SF	safety function
SFF	safe failure fraction
SIL	safety integrity level
SIS	safety instrumented system
UML	Unified Modeling Language
V&V	verification and validation

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

Part 9: 7.0 Independent Functional Safety Assessment Guidance

By John J. Sammarco, Ph.D., P.E.,[1] and Janet S. Flynt[2]

ABSTRACT

This report (Independent Functional Safety Assessment Guidance 7.0) is the last 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 Administra-tion. They are intended for use by mining companies, original equipment manufacturers, and after-market 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.

[2]President, Safety Requirements, Inc., Cary, NC.

• 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*.

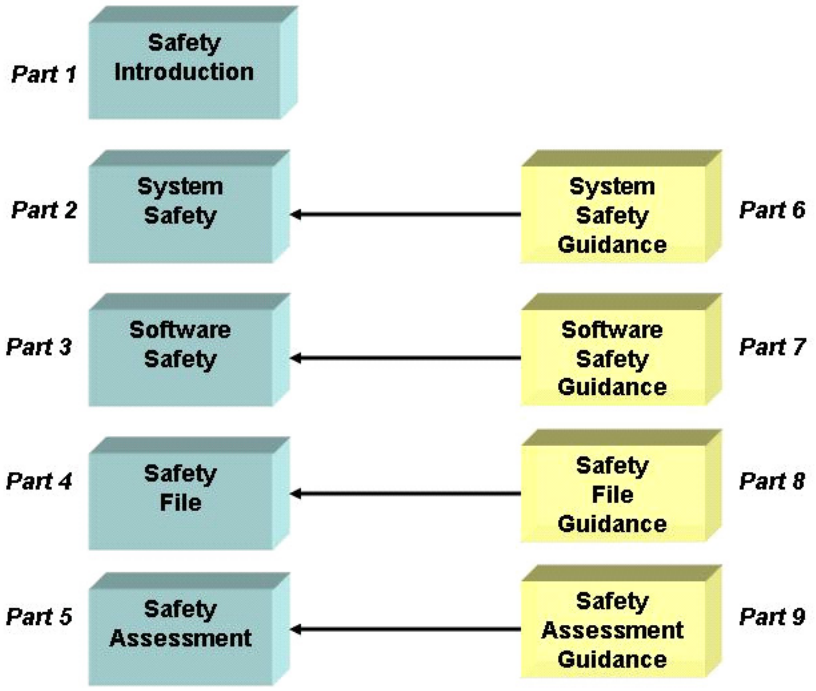


Figure 1.—The safety framework and associated guidance.

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 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. The author also thanks E. William Rossi, Industrial Engineering Technician, NIOSH Pittsburgh Research Laboratory, for creating artwork for this publication; and Robert J. Tuchman, Technical Writer-Editor, NIOSH Pittsburgh Research Laboratory, for his contributions to improve the clarity and quality of this document.

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].

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 this document presents 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

This guidance document provides supplemental guidance information for the Independent Functional Safety Assessment document 4.0 [Sammarco and Fries 2003].

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.

1oo2D – A dual-channel system with diagnostics. This system can tolerate one fault.

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.

NOTE 1: The probability of a dangerous failure is λ_D.

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

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

NOTE 2: The definition may also be represented in terms of Equation 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 systems 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 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.

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.

Safe Failure Fraction (SFF) – The fraction of safe failures and dangerous detected failures in relation to total failures 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 Availability – Fraction of time that a safety system is able to perform its designated safety service when the process is operating (safety availability = 1 – PFD).

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	Dangerous failures per hour	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 Independent Functional Safety Assessment

4.1 Objectives

An independent functional safety assessment (IFSA) is a systematic analysis and study, based on evidence, to judge the functional safety achieved by one or more of the programmable electronics and software components. A typical IFSA involves determining whether—

- The actual procedures and rules adhere to the planned procedures and rules
- The planned procedures and rules are implemented effectively and suitably to achieve the specified safety objectives
- The appropriate methods, techniques, and processes have been used to—
  - Identify and analyze all reasonably foreseeable hazards and risks
  - Mitigate the identified hazards and risks to achieve an appropriate level of safety
  - Assign SILs
  - Verify that the SIL is met
  - Document the system with a safety file document

IFSAs benefit both the manufacturer and the purchaser by providing necessary confidence as to the safety integrity of the PES. Preliminary assessments during the design of the PES electronics and software can result in early detection of problems, including inadequacies in the fail-safe design. Thus, early detection allows corrections to be made more effectively and efficiently. Secondly, the potential for a better safety assessment exists because the assessor(s) can potentially become more familiar with the development process and build the level of understanding at each assessment milestone.

4.2 Scope

As shown in Figure 2, the IFSA is an independent examination of the safety policy/strategy, staffing qualifications, and the functional safety life cycle (FSLC) practices for a PES to determine compliance with specified safety objectives. An IFSA is conducted by an independent assessor who reviews the safety file. The assessor's degree of independence depends on the SIL requirements for the safety functions. The Independent Functional Safety Assessment document 4.0 [Sammarco and Fries 2003] identifies the recommended degree of assessor independence. This information is replicated in Table 4 below.

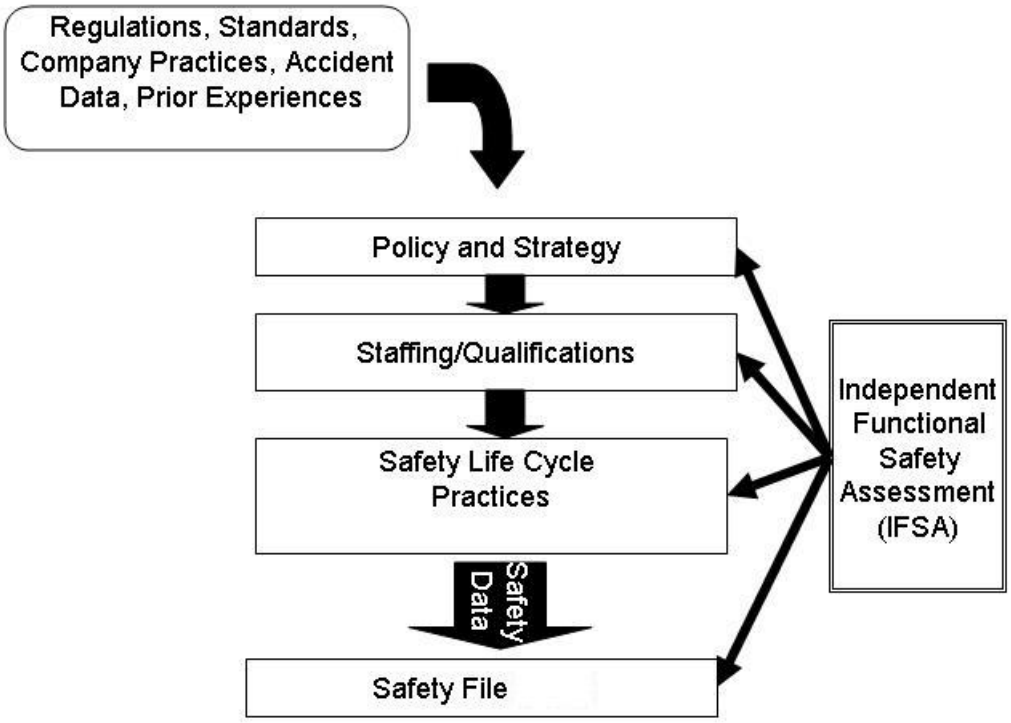


Figure 2.—Scope of independent functional safety assessments.

Table 4.—Recommended degree of independence of assessor

Degree of independence	SIL 1	SIL 2	SIL 3
Independent person	HR	HR	nr
Independent department	—	HR	HR
Third party	—	—	HR

HR = highly recommended. nr = not recommended.
A dash (—) indicates no recommendation.

Source: Adapted from IEC [1998a].

4.3 Types of Independent Functional Safety Assessments (IFSAs)

The number and timing of the IFSAs will depend on the scope, complexity, safety integrity objectives, prior experience of the project staff, and corporate management practices. The greater the SIL requirement, the more comprehensive and frequent the IFSAs. MCMS manufacturers may conduct IFSAs incrementally and in parallel to the daily engineering and use activities.

Three types of IFSAs are recommended [Sammarco and Fries 2003] and are summarized below:

- **Preliminary Independent Functional Safety Assessment** – A review of the MCMS staffing, development plans, and preliminary safety file conducted after the planning and safety requirements specification (phase 8 in the life cycle).

- **Initial Functional Safety Assessment** – An IFSA conducted during the realization phase of the FSLC, typically after design (phase 9 in the life cycle).

- **Followup Functional Safety Assessment** – An assessment conducted periodically after the MCMS has been released and is in use (during operation, maintenance, and decommissioning —phases 14, 15, and 16 in the life cycle).

The *preliminary independent functional safety assessment* is optional, though recommended, for new MCMS projects, project teams, and SILs 2 and 3. The *initial functional safety assessment* addresses the complete system and the full development life cycle once the system is installed and commissioned. The *followup functional safety assessment* addresses changes and modifications to the system during operation, and it verifies the MCMS supplier's continued capability to maintain the appropriate safety integrity level for the MCMS.

Figure 3 shows an example project schedule for the fictitious continuous mining (CM) machine described in the example of a preliminary IFSA for a SIL 3 emergency stop function. The IFSAs are planned at the start of the project. Because the guidance is new, a *preliminary independent functional safety assessment* is planned once all project plans are in place and the safety requirements specification is at a point where design can begin. The *initial functional safety assessment* is planned when the design is complete. Two *followup functional safety assessments* are planned—one for a planned upgrade and one at the end of decommissioning. In addition, periodic followup IFSAs may be added to address risks associated with unplanned modification activity.

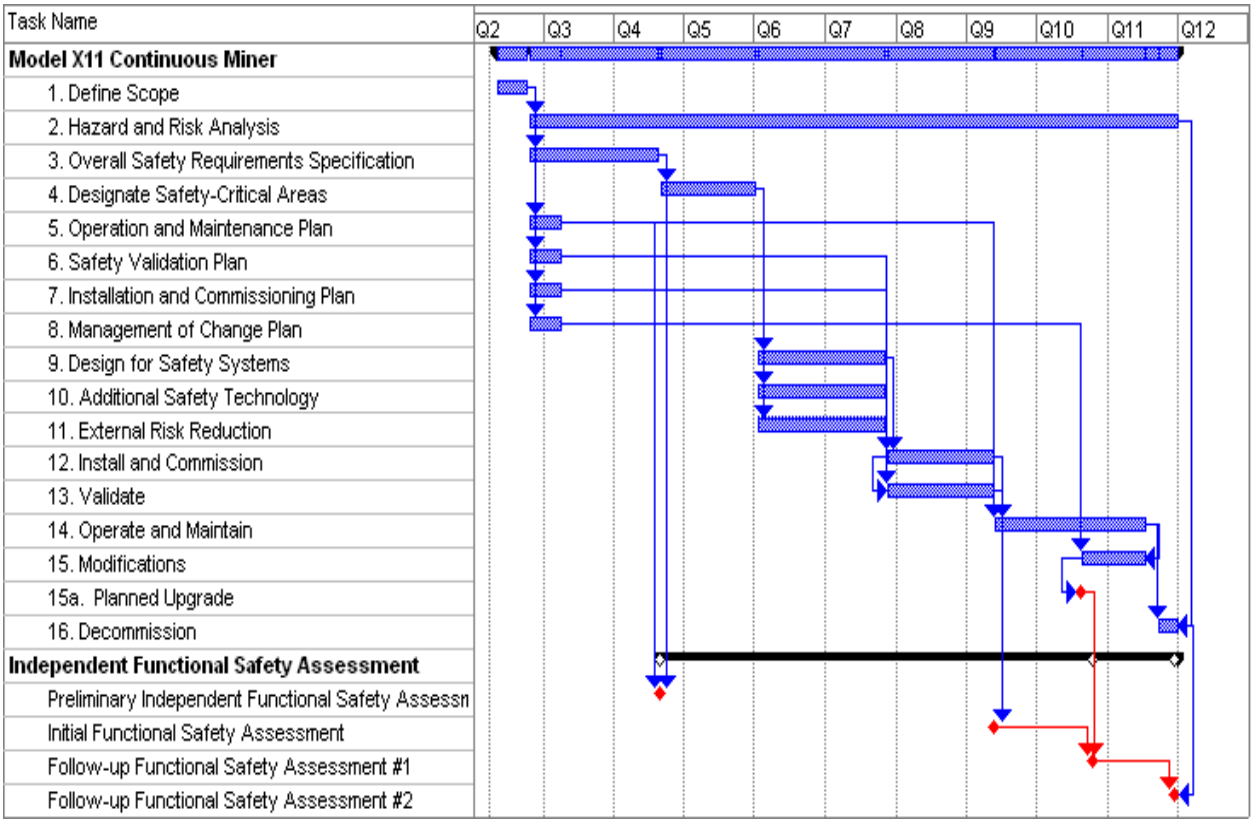


Figure 3.—Example of IFSAs integrated with a project development schedule.

4.4 Independent Functional Safety Assessments (IFSAs) and the Safety File

Traceability is important to reaching closure for the identified hazards. Populating the safety file with deliverables from each phase permits selecting hazards and tracing them from the hazard/risk analyses, through specifications and safety function allocation, to design, and verification. Thus, a thorough review of the safety file provides evidence that the selected hazard was addressed, designed for, and resolved in an acceptable manner.

A manufacturer may also organize the MCMS safety file into subsystem and component safety files. Such an organization may be practical when MCMSs are assembled from components and subsystems acquired from sources outside of the project. The supplier provides safety file documentation when it provides the subsystems and components. As part of the independent functional safety assessment, the subsystem and component safety files may be consulted.

Figure 4 illustrates how a safety file for a particular machine model may reference other safety files for specific subsystems and components. For example, the emergency stop system for a CM machine has separately compiled files for the sensor subsystem, the PE subsystem, and the electrical subsystem. These files may further reference safety files for components.

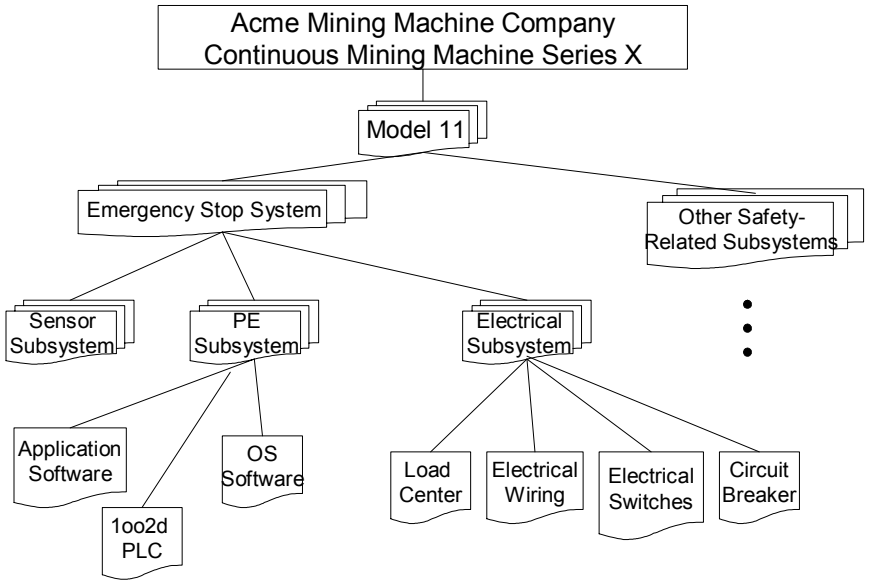


Figure 4.—Organization of the safety file for Acme Model X11 continuous miner.

An advantage to the organization shown is that the subsystem and component safety files may be reused. For example, if Acme decides to build a Model 12 continuous miner that uses the emergency stop system, then the company could potentially reuse the emergency stop system as is or with some updating, depending on the conditions of use and whether parts have been replaced.

4.5 Common Weaknesses of Safety Files

The independent assessment process primarily relies on the safety file documentation. The quality of each safety file will vary because of the following factors:

- Degree of system complexity
- Degree of technical expertise and knowledge
- Degree of safety management expertise and knowledge

Although each safety file is unique, there are weaknesses common among safety files that are important to recognize during the independent assessment process. These include—

- Omission of credible hazards
- Narrow focus on only the obvious or well-known hazards
- Vague hazard descriptions
- Undocumented assumptions
- Incomplete safety requirements
- Insufficient data to support a safety claim
- Overly optimistic estimates for the likelihood of human error
- Unrealistic SIL targets (i.e., SIL targets set too high or low)

4.6 Example of a Preliminary IFSA for an SIL 3 Emergency Stop Function

The example report is completed to the level of a preliminary independent functional safety assessment. The IFSA is based on the safety file example presented in the Safety File Guidance document 6.0 [Sammarco, forthcoming]. A complete independent functional safety assessment could be conducted once the safety file contains a complete software design description and test results.

Appendix A contains an example of a checklist, as completed by the assessor, for the safety data and methods and the conclusion portions of the safety file.

FUNCTIONAL SAFETY INDEPENDENT ASSESSMENT REPORT

Project:
Model X11 Continuous Miner

Company:
Acme Machine Company
427 Main Street
New York, NY

Prepared by:
International Functional Safety Assessors, Inc.

Lead Assessor: Jill Hill
File Number: 987430
Date: February 28, 2005
Document No. ACME 1–04
Version 1.0

CONFIDENTIAL INFORMATION

PROPERTY OF ACME MACHINE COMPANY

PURPOSE/SCOPE

Provide a preliminary independent functional safety assessment of the emergency stop system to be used on the Acme Model X11 continuous miner. The objective is to provide an early independent functional safety assessment of the SIL(s) so as to reduce the potential for costly rework at the final stages of assessment because of an inappropriate assignment of SIL(s).

On February 28, 2005, a preliminary assessment of functional safety practices for an emergency stop system used on the Acme Model X11 continuous miner was conducted. The preliminary assessment focused on the safety requirements activities for the emergency stop safety function. This safety function (SF) is identified as SF 5. The assessment reviewed the assignment of SIL 3 to SF 5 and the allocation of SF 5 to hardware and software components. John Doe and Mary Johnson of Acme Machine Company and Jill Hill of International Functional Safety Assessors, Inc., participated in the preliminary assessment.

PRODUCT DESCRIPTION

The emergency stop system was designed for the Model X11 continuous miner as designed and built by Acme Machine Company. The CM machines are designed for use in underground coal mining applications in North America and Australia.

The safety function SF 5 is to be implemented by the emergency stop system to mitigate the risks of hazards H1, loss of tram control, and H2, unexpected machine movement. The emergency stop function was assigned to two independent layers of protection.

The first protection layer is automatically invoked by the programmable logic controller (PLC) to place the tram subsystem in a safe state of "deenergized." The protection layer uses the output monitoring technique where the tram motor current is monitored and compared to the desired state of the machine. If an unsafe condition exists, i.e., the tram motors are energized when they should be off, the protection layer will shut down power to the tram subsystem. The protection hardware (Figures 5–6) consists of a tram motor current sensor, a dual-channel safety PLC, and a circuit breaker connected to the tram motor subsystem.

The second protection layer is manually invoked by humans. The design uses two switches directly wired to the mainline circuit breaker (Figure 7). Depressing either of the two switches causes a loss of control voltage to the line circuit breaker located on the CM machine, thereby causing the circuit breaker to trip, which shuts down the CM machine. The design can be abstracted as a sensor, logic solver, and field device.

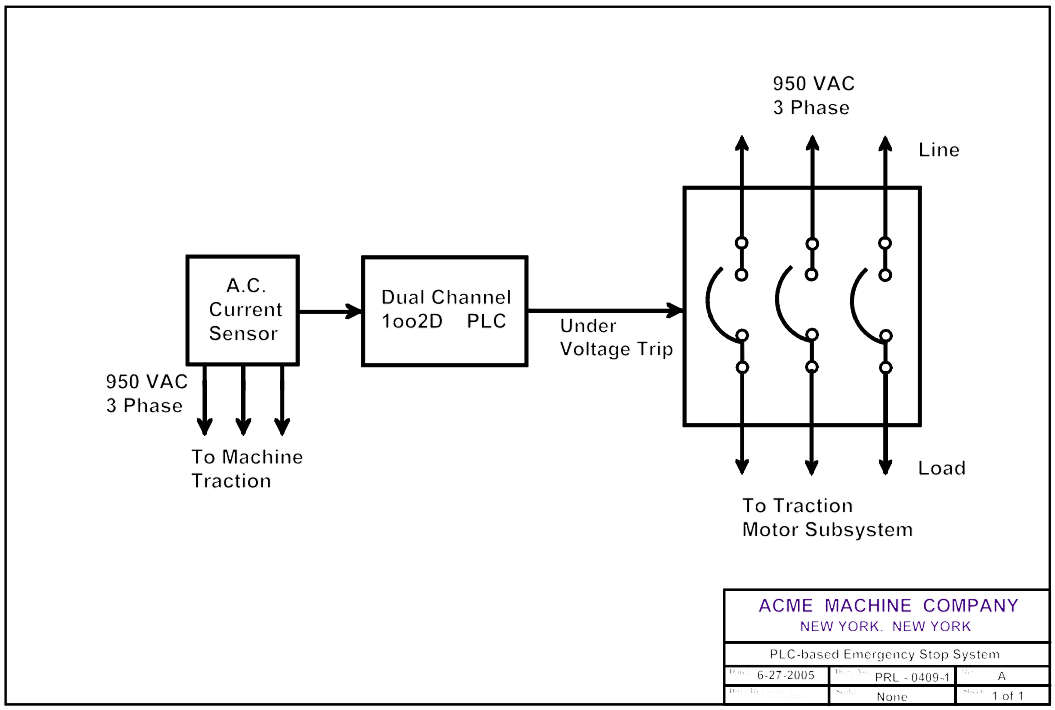


Figure 5.—Conceptual design for the first layer of protection that is automatically invoked by the dual-channel safety PLC.

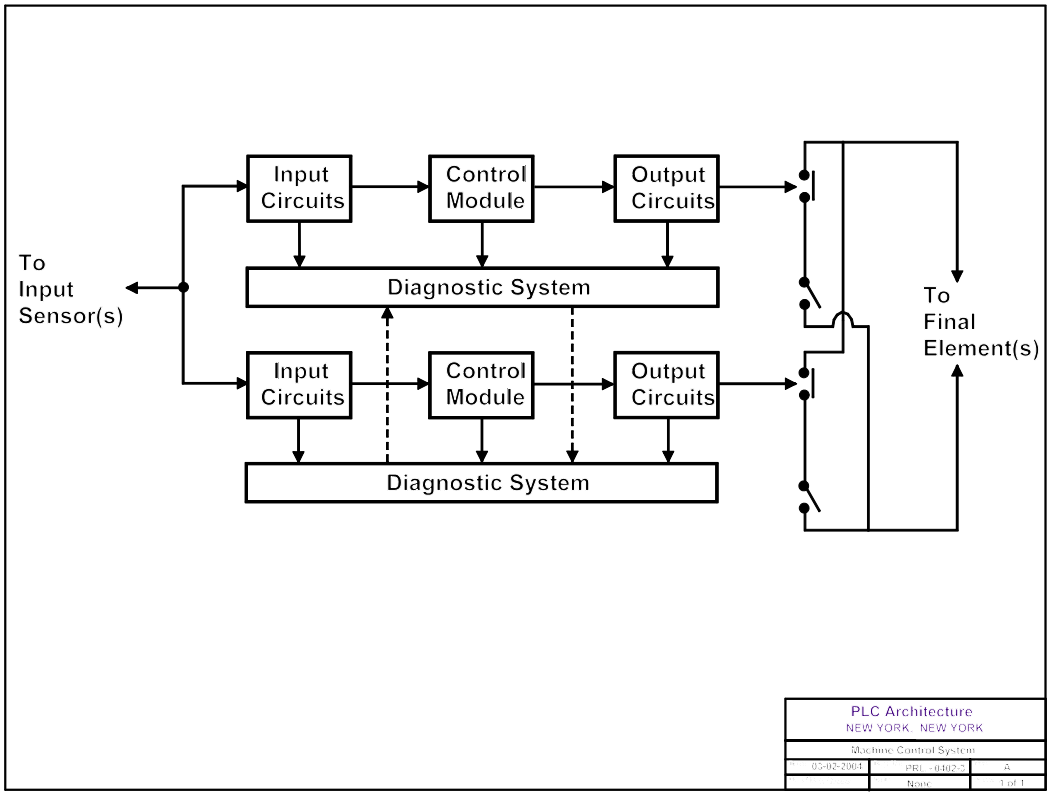


Figure 6.—Redundant dual-channel hardware architecture for the 1oo2D safety PLC.

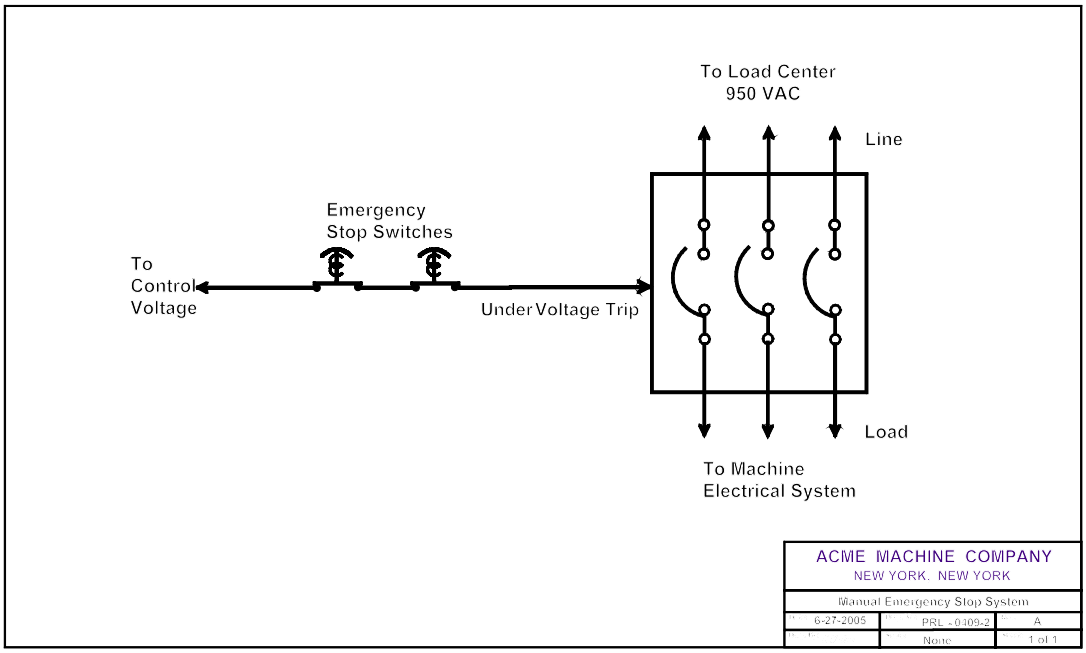


Figure 7.—Conceptual design for the second layer of protection that is manually invoked by depressing the emergency stop switch.

REFERENCED CODES, STANDARDS, AND GUIDANCE

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.

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.

Mowrey GL, Fisher TJ, Sammarco JJ, Fries EF [2002]. Programmable electronic mining systems: best practice recommendations (in nine parts). Part 4: 3.0 Safety file. 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. 2002–134, IC 9461.

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.

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.

USC Title 30–Mineral Lands and Mining; Chapter 22–Mine Safety and Health; Subchapter III–Interim Mandatory Safety Standards for Underground Coal Mines; Section 865–Electrical Equipment; (o) Switches, and (r) Deenergizing of electric face equipment.

DOCUMENTATION REVIEWED

Doe J, Johnson M [2004]. Safety file for an emergency stop system. Document No. ACME 1–04. Version 1.0 model X11 continuous miner. New York: Acme Machine Company, March 2004.

NOTE 15: Acme document No. ACME 1–04 is the example safety file from section 5.0 of the Safety File Guidance document 6.0 [Sammarco, forthcoming].

Acme General Operation and Maintenance Manual document No. O/M–X11–104.

Acme Electrical Components, Circuits, and Systems Manual No. ELEC–X11–104.

Acme System Safety Plan No. SSP–01–2004.

Acme Software Safety Plan No. SWSP–02–2004.

Component Failure Rate Data Sheets.

Acme Emergency Stop System Drawing No. PRL–0409–1.

Acme Emergency Stop System Drawing No. PRL–0409–2.

SIL 3 certification document for the PLC.

FINDINGS

NOTE 16: These findings address only five items of the safety file: (1) the safety requirements, (2) the safety requirements allocation, (3) the emergency stop, (4) software development, and (5) safety file documentation. Typically, the findings would address a more comprehensive list of items.

Table 5.—Assessor checklist of findings

Item	Item Details	Part 2: 2.1 System Safety Recommendations[1]	Preliminary Safety File References[2]	Outcome	Assessor Notes
1. Safety Requirements	Do the safety requirements include operation and maintenance information?	Section 6.3.2	Section 5.6.1.6 System-level Safety Requirements	Accepted	The safety requirements also define testing requirements. Maintenance information seems vague. Perhaps the testing requirements are part of the maintenance; need to clarify this assumption.
1. Safety Requirements	Are safety functions and integrity requirements specified for each hazard?	Section 6.3.4	Section 5.6.1.6 System-level Safety Requirements	Accepted	SIL 3 assigned to hazards H1 and H2. These SIL assignments seem to be appropriate.
1. Safety Requirements	Are the safety requirements complete?	Section 6.3.7	Section 5.6.1.6 System-level Safety Requirements	Accepted	The safety requirements specification contains the information components of Table 6 of the System Safety document 2.1 [Sammarco and Fisher 2001]. All SILs are adequately designated and justified.
2. Safety Requirements Allocation	Have safety functions been identified?	Section 6.4.1	Section 5.1 Executive Summary (Safety Statement)	Accepted	Safety function SF 5 addresses hazard H1 – loss of tram control, and hazard H2 – unexpected machine movement.
2. Safety Requirements Allocation	Have SILs been specified based on the risk assessment?	Section 6.4.3	Sections 5.6.1.4, 5.6.1.5 SIL 3 certification document for the PLC	Accepted	Table 8 of the Safety File Guidance document 6.0 [Sammarco, forthcoming] was followed.
2. Safety Requirements Allocation	Does the SIL determination take into account the allocation of safety functions to multiple systems and protection layers?	Section 6.4.4	Sections 5.6.5.1, 5.6.5.2 Discussion with John Doe and Mary Johnson of Acme as documented in Jill Hill assessor notes dated 2/28/05.	Accepted	There are two layers of protection.

See footnotes at end of table.

Table 5.—Assessor checklist of findings—Continued

Item	Item Details	Part 2: 2.1 System Safety Recommendations[1]	Preliminary Safety File References[2]	Outcome	Assessor Notes
2. Safety Requirements Allocation	If the basic MCMS is also used to implement safety functions, then is the basic MCMS designed to the level of rigor required for the highest SIL of its safety function(s)?	Section 6.4.5	Sections 5.7.1.2, 5.7.2 SIL 3 Certification Document for the PLC	Accepted	Protection layer 1 is integrated into the MCMS controls.
2. Safety Requirements Allocation	If the safety system is implemented separate from the MCMS and assigned multiple safety functions, then is it designed to the level of rigor required for the highest SIL of its safety functions?	Section 6.4.6	Sections 5.7.1.2, 5.7.2	Accepted	Protection layer 2 is independent of the MCMS.
2. Safety Requirements Allocation	Does the allocation of safety functions to multiple safety systems and protection layers take into account common cause failure modes?	Section 6.4.7	Section 5.7.1.2	Accepted	The redundant components take common cause into account by using the β-factor, or common cause factor.
3. Emergency Stop	Is the emergency stop system independent of the hardware and software used for system operation?	Appendix A System Checklist	—	Need more information	More information regarding design rationale and tradeoffs is needed. The PLC is shared for control and safety functions. Also, the design shares existing wiring from the PLC to the circuit breaker. Were other technologies considered for the manually actuated emergency stop, such as a hard-wired design that would be simpler to design, validate, verify, and maintain?

See footnotes at end of table.

Table 5.—Assessor checklist of findings—Continued

Item	Item Details	Part 2: 2.1 System Safety Recommendations[1]	Preliminary Safety File References[2]	Outcome	Assessor Notes
3. Emergency Stop	Can a signal point of failure cause a hazardous state?	Appendix A System Checklist	Section 5.6.5 Hardware Design Description Section 5.6.6.1 Software Conceptual Design	Need more information	PLC mounting and emergency stop switches are physically separated 5 feet to reduce potential for common cause failures. Diagnostics are included, and cross-checking is used. Software development has not progressed to a point where this checklist item can be fully determined. Revisit at initial functional safety assessment.
3. Emergency Stop	Do emergency stops require a single keystroke operator response?	Appendix A Human Factors Checklist	Section 5.6.1.6 System-level Safety Requirements Emergency Stop System Drawing No. PRL–0409–2 Section 5.6.5.2	Accepted	Pushbutton switches are used requiring one stroke. There is no keyboard.
3. Emergency Stop	Are emergency stop switches readily accessible and clearly defined?	Appendix A Human Factors Checklist	Section 5.6.1.6 System-level Safety Requirements Section 5.6.5 Hardware Design Description	Need more information	The requirements specify the switches to be readily accessible and clearly defined. The design is at the preliminary stage, so no hardware has been built to verify if this was implemented.

[1]Sections and appendices cited refer to the System Safety document 2.1 [Sammarco and Fisher 2001].
[2]Sections cited refer to the Safety File Guidance document 6.0 [Sammarco, forthcoming].

CONDITIONS OF ACCEPTABILITY

More information regarding design rationale and tradeoffs is needed. Some of the information will need to be added to the installation, user, and maintenance manuals.

SUMMARY

A preliminary independent functional safety assessment was completed for the emergency stop system for the Model X11 continuous miner. An initial functional safety assessment is recommended after completion of the conceptual design.

All SILs are adequately designated and justified at this preliminary stage.

NOTE 17: The preliminary IFSA typically does not include the software components. Software is usually not available until the initial IFSA. The lack of software does not minimize the importance of the preliminary IFSA because *most safety-related errors occur at the requirements stage*, as described in the Introduction document 1.0 [Sammarco et al. 2001]. Specifically, a study by the U.K. Health and Safety Executive [1995] determined that requirement specification errors were the overwhelming majority mishap causes (44.1%).

NOTE 18: This concludes section 4.6, "Example of a Preliminary IFSA for an SIL 3 Emergency Stop Function." The following information concerns guidance for an initial IFSA and is separate from the emergency stop example.

5.0 Initial IFSA

The initial IFSA is described in section 5.2 of the Independent Functional Safety Assessment document 4.0 [Sammarco and Fries 2003]. This section describes what is provided to the assessor (the inputs), the process for assessment, and the assessment results (the outputs). The degree of assessor independence is shown in Table 2 of the Independent Functional Safety Assessment document 4.0 document, where third-party assessment is recommended for SIL 3.

5.1 Third-party Assessment

Third party is defined as follows [Sammarco and Fries 2003]:

> An organizational division, subsidiary, or other organization that is separate and distinct, by management and other resources, from the organization or department responsible for the activities, subject to functional safety assessment or validation, taking place during the specific phase of the overall E/E/PES or software safety life cycle.

Therefore, the assessment can be conducted by an outside organization. Appendix B lists a sampling of third-party assessment organizations that also offer certification.

5.2 Proven in Use (Service History) as Applied to Software

Proven in use is used to establish safety integrity based on a documented safe history of use. This concept is detailed in section 8.0 of the Independent Functional Safety Assessment document 4.0 [Sammarco and Fries 2003]. Proven in use applies to systems, subsystems, and components. Software is one component of a system; therefore, proven in use can be used to establish the safety of software without the need for formal and rigorous verification.

5.2.1 Software Distinctions

Software exists in many forms. For instance, there are commercially available software tools for developing, testing, and validating software. These tools are important to consider with respect to safety and proven in use; the fact that a tool is commercially available does not justify the tool safety integrity. For example, compiler errors can occur and can go undetected until a mishap occurs.

The safety assessment should take into account the various types of software, such as:

- Compilers
- Operating systems
- Software function libraries
- Application software
- Software configuration management tools
- Software testing tools
- Device drivers

5.2.2 Proven-in-Use Criteria for Software

Software must have documentation to support that the likelihood of a systematic software fault is low enough to achieve the required safety integrity level. If previously used software has not been verified to meet the required safety integrity level, then the assessor(s) should use the following criteria as a guide to establish for proven in use:

- The software specification has not been changed.
- The software has been in use in a different application for at least 1 year.
- The operating experience of the software should be similar (i.e., software designed and used for low-demand modes of operation should not be used for high-demand (continuous) modes of operation).
- The safe service history duration, in terms of failure-free operating hours, should be as shown in Table 6 below [Sammarco and Fries 2003].

Table 6.—Recommended safe service duration for various SILs

SIL	Hazard-free operating hours
1	3×10^2
2	3×10^3
3	3×10^4

NOTE 19: A failure resulting in a fail-safe condition or state is considered hazard-free.

The documentation of software for proven in use should include:

- Identification of the software
- Identification of the system using the software
- Identification of the application and service location
- Software version number

5.3 General Indicators of Software Quality

Software does not exhibit random wearout failures. Instead, software failures result from 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 two loops, four branches, and eight states, the number of paths through this code exceeds 8,000. Therefore, it is usually impractical to test or conduct a safety assessment of 100% of the software.

The assessor(s) should then be observant of "warning" indicators; these indicators can be useful in identifying software for closer scrutiny:

- Software with an excessive history of revisions
- Newly developed software
- Poorly documented software
- Software not subjected to management of change processes
- Development tool changes before the development process is completed (e.g., changing the version or vendor of a compiler)
- Excessively large software modules (e.g., a module exceeding 500 lines of code)
- Software that was not developed systematically (e.g., lack of general coding standards or software development life cycles)

NOTE 20: The indicators are general in nature and are not to be used as definitive signs of a hazardous situation; thus, software could be safe, yet exhibit all of the suggested indicators.

5.4 Assessment of Software Verification and Validation (V&V)

The purpose of software verification and validation (V&V) is to demonstrate that the software is correct and complete with respect to the system and software requirements and design specifications.

Numerous methods of software V&V exist. Typically, multiple methods are needed; this is especially true as the SIL assignment increases. The recommended software V&V methods and the association documentation are presented in the Software Safety document 2.2 [Fries et al. 2001]. Table 2 in the Software Safety document 2.2 lists the recommended software V&V methods for SIL 1, SIL 2, and SIL 3. Section 4.9 details the information requirements for software V&V.

5.4.1 Static and Dynamic Analysis Tools

One of the information requirements for software V&V is found in section 4.9 of the Software Safety document 2.2 [Fries et al. 2001]: description of the facilities, equipment, and software used for testing. This recommendation applies to software tools used for static and dynamic analysis. Many tools are commercially available. Table 7 lists some of the tools that an assessor would likely encounter [Jones et al. 2001].

The use of static and dynamic analysis tools should be documented for the IFSA, as well as the tool itself (i.e., name, supplier, version, etc.). The assessor(s) should then check for this documentation; insufficient documentation should be an issue of concern for the IFSA. One exception to this guidance is software that was proven in use.

Table 7.—Sampling of static and dynamic analysis tools for software

Tool Name	Purpose	Website
PC Lint	C/C++ language checker. Also supports MIRSA C checking. Conducts more extensive checking than a compiler. Checks for syntax errors, initialization and value misuse, redundant code, etc.	www.gimpel.com
Logiscope	C, C++, Ada, and Java code checking; code coverage analysis.	www.telelogic.com/products/tau/logiscope
LDRA Testbed®	C/C++ language checker. Also supports MIRSA C checking. Conducts data flow analysis, loop analysis, structured programming verification, control flow coverage, complexity analysis, etc.	www.ldra.co.uk/testbed.asp
PolySpace	Automatic detection of run-time errors. Available for C, C++, MIRSA C, Ada, UML.	www.polyspace.com
Splint	Static analysis tool geared for coding mistakes and security vulnerabilities.	www.splint.org

REFERENCES

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

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.

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.

Jones C, Bloomfield RE, Froome PKD, Bishop PG [2001]. Methods for assessing the safety integrity of safety-related software of uncertain pedigree (SOUP). London: Adelard LLP. Contract research report 337/2001 for the U.K. Health and Safety Executive.

Sammarco JJ [forthcoming]. Programmable electronic mining systems: best practice recommendations (in nine parts). Part 8: 6.0 Safety file guidance. 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, Information Circular (IC).

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, 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.

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.

U.K. Health and Safety Executive [1995]. Out of control: why control systems go wrong and how to prevent failure. Sheffield, U.K.: Health and Safety Executive.

APPENDIX A.—INDEPENDENT FUNCTIONAL SAFETY ASSESSMENT CHECKLIST AND WORKSHEET

Checklists and worksheets are tools that can help reduce errors of omission for both the assessor and the persons submitting the safety file by providing a systematic structure to the assessment process. The following are examples of completed checklists for the safety data and methods and the conclusion portions of a safety file. Example checklists and worksheets were presented in Appendix D of the Independent Functional Safety Assessment document 4.0 [Sammarco and Fries 2003].

SAFETY DATA AND METHODS DOCUMENTATION

Accept	*Reject*	
X		Product description (vendor's sales literature, general specifications, features)
See comment 1		Implementation document
X		User documents (operator's manual, maintenance manual, training manual)
See comment 1		History files
See comment 1		Hazard log
X		Hazard and risk analysis methods
X		Risk categorization methods
X		SIL categorization methods
X		System safety requirements
X		Software safety requirements
Not applicable		Proven in use documentation, if applicable

Comments:

1. These items were not provided at this preliminary stage of assessment. It is highly recommended that they be created and included for subsequent stages of the independent functional safety assessment.

SAFETY FILE CONCLUSION

Accept	*Reject*	
X		Summary/conclusions
See comment 2		Signed statement affirming that the system is safe to operate

Comments:

2. The signed statement is not applicable at this preliminary stage of assessment.

APPENDIX B.—THIRD-PARTY ASSESSMENT ORGANIZATIONS

Below is a list of third-party organizations offering independent assessments of functional safety. The list is not comprehensive, but it does identify organizations with substantial assessment experience.

This list does not imply endorsement by NIOSH and does not imply that organizations not listed are not qualified to conduct an assessment.

- Factory Mutual Research
  www.fmglobal.com/approvals/approved/categories/safety.asp

- TÜV Rheinland Group Industrial Services
  www.tuv-fs.com/ctpolicy.htm

- Underwriter Laboratories, Inc.
  www.ul.com/software

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. 2006-131