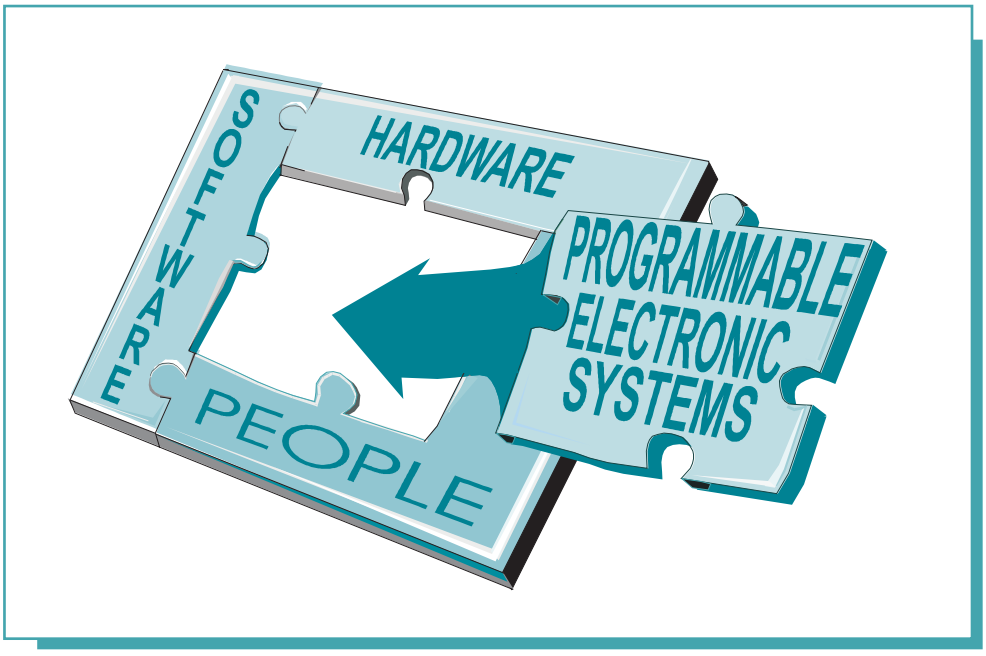
CDC
Workplace Safety and Health

IC 9487
INFORMATION CIRCULAR/2006

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



Part 8: 6.0 Safety File Guidance

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

NIOSH

Information Circular 9487

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

Part 8: 6.0 Safety File Guidance

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

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. 2006–130

CONTENTS

Page

ILLUSTRATIONS

TABLES

ABBREVIATIONS USED IN THIS REPORT

CM	continuous mining
DC	diagnostic coverage
E/E/PES	electrical/electronic/programmable electronic system
FIT	failure in standard time (per 10^9 hours)
HAZOP	hazard and operability studies
I/O	input/output
MCMS	mining control and monitoring system
MISRA	Motor Industry Software Reliability Association
MOC	management of change
MSHA	Mine Safety and Health Administration
MTTF	mean time to fail
MTTR	mean time to repair
NIOSH	National Institute for Occupational Safety and Health
PE	programmable electronics
PFD_{avg}	average probability of failure on demand
PLC	programmable logic controller
SF	safety function
SFF	safe failure fraction
SIL	safety integrity level
SIS	safety instrumented system
TI	test interval

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

Part 8: 6.0 Safety File Guidance

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

ABSTRACT

This report (Safety File Guidance 6.0) is the eighth 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*.

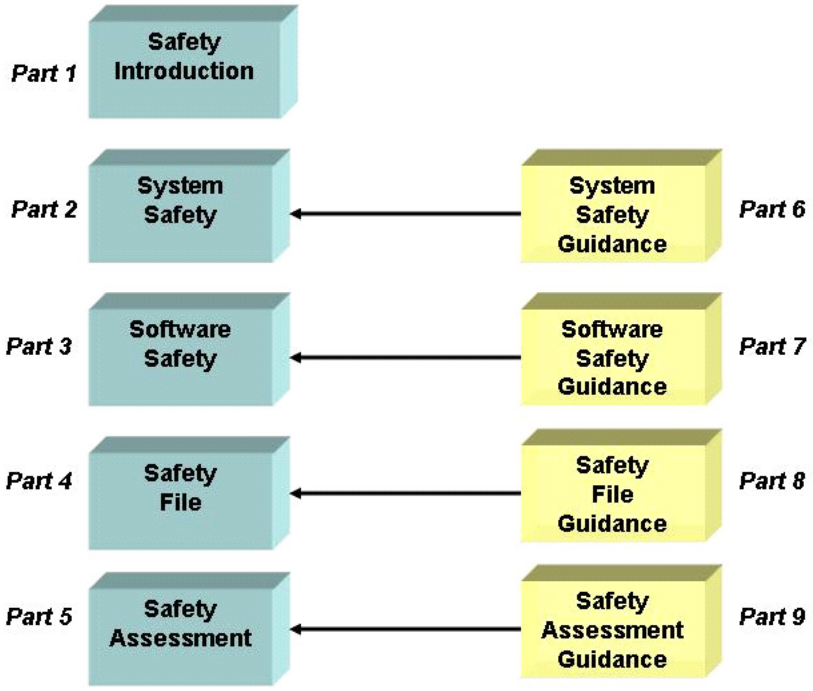


Figure 1.—The safety framework and associated guidance.

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 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 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 following recommendation documents: Part 1: 1.0 Introduction [Sammarco et al. 2001]; Part 2: 2.1 System Safety [Sammarco and Fisher 2001]; Part 3: 2.2 Software Safety [Fries et al. 2001]; and Part 4: 3.0 Safety File [Mowrey et al. 2002].

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 (I/O) 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.

Critical Software – Computer software components and units whose errors can result in a potential hazard or in loss of predictability or control of a system.

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 operation of the automatic diagnostic tests.

Dual Channel – Two channels that independently perform the same 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.

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

Management of Change – Discipline of identifying the components of an evolving system for the purposes of controlling changes to those components and maintaining continuity and traceability throughout the life cycle so as not to introduce additional safety risks.

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.

Noncritical Software – Software whose failure would not have an impact on safety or would not cause large financial or social loss.

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.

Response Time – The total time from the start of an input state change to the corresponding output state change. The response time includes input and output hardware delays, propagation delays, communication delays, and program scan time.

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

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

Software - Computer programs, procedures, and possibly associated documentation and data pertaining to the operation of a computer system.

Software Safety Integrity - Measure that signifies the likelihood of software in a programmable electronic system achieving its safety functions under all stated conditions within a stated period of time.

Software Safety Integrity Level - One of three discrete levels for specifying the safety integrity of software in a safety system.

Supervisory Software - A computer program, usually part of an operating system, that controls the execution of other computer programs and regulates the flow of work in a computer system.

Type-A Device – All possible failure modes are identified and can be computed for A-type devices. The behavior under fault conditions can be completely determined. A relay is considered to be type A.

Type-B Device – All failure modes are not completely known or the behavior under fault conditions cannot be completely determined. Also, there are insufficient failure data from field experience to compute the dangerous detected λ_{DD} and undetected failure λ_{DU} rate. A PLC is considered to be type B.

1oo1D – A single-channel system with diagnostics and without fault tolerance.

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

4.0 Example Safety File

4.1 Introduction

A case study example of a safety file is presented. The safety file concerns an emergency stop safety function for a continuous mining (CM) machine as presented in the System Safety Guidance document's case study [Sammarco 2005]. The purpose is to show how the safety file recommendations can be implemented for a PE-based safety system. The safety file format is based on the format presented in section 4.2.3 of the safety file recommendations [Mowrey et al. 2002].

Section 5.0 below contains the example safety file. The example is for learning purposes only. It does not detail every task or process given by the safety file recommendations; however, it does focus on the key concepts and processes. The example addresses the hardware component of the design, human performance, and the software conceptual design.

NOTE 3: The safety file in section 5.0 below is for example purposes only and addresses one safety function designated as SF5. A complete safety file would address all safety functions.

NOTE 4: The sharing of a PLC for control and safety purposes is possible, but not recommended [Sammarco and Fisher 2001]. Safety functions and control functions should be physically and logically separate.

4.2 An Emergency Stop System

This design approach uses two independent protection layers to achieve the required SIL for an emergency stop function. The first protection layer uses a PLC and is automatically invoked; the second protection layer is a simple hard-wired circuit that is manually invoked by a human. Together, the protection layers enable an SIL 3 safety function.

5.0 Safety File

The safety file in this example is completed to the level needed to have a preliminary independent functional safety assessment. A complete independent functional safety assessment could be conducted once the safety file contains a complete software design description and test results.

PRELIMINARY SAFETY FILE
FOR AN EMERGENCY STOP SYSTEM

Project:
Model X11 Continuous Miner

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

Customer Contract No. 4552004

Prepared by: John Doe, Senior Engineer, March 5, 2004

Approved by: Mary Johnson, Engineer Manager, March 20, 2004

Document No. ACME 1–04
Version 1.0

CONFIDENTIAL INFORMATION

PROPERTY OF ACME MACHINE COMPANY

PRELIMINARY SAFETY FILE
FOR AN EMERGENCY STOP SYSTEM

Revision History

Version	Date	Description of Changes
0	April 2, 2004	Preliminary issue.
1	March 5, 2004	Added hardware architecture description and drawing.

5.1 Executive Summary (Safety Statement)

This safety file is for the design of 20 CM machines, model X11, designed and built by Acme Machine Company. The CM machines are for use in underground coal mining applications in North America and Australia.

This safety file documents and supports the safety claim that the X11 CM machine meets the appropriate level of safety for the intended application.

The X11 CM machine design has five safety functions intended to achieve or maintain a safe state for the hazards and risks identified and defined in the hazard and risk analysis. Table 4 gives a summary of the safety functions and the achieved safety performance, as defined by the safety integrity level (SIL).

Table 4.—Safety functions and associated SILs for the X11 CM machine[1]

Identifier	Safety function	Associated hazards	PFD_{avg}	SIL achieved
SF1	([2])	([2])	2.0×10^{-2}	1
SF2	([2])	([2])	1.19×10^{-2}	1
SF3	([2])	([2])	1.43×10^{-3}	2
SF4	([2])	([2])	4.25×10^{-2}	1
SF5	Emergency stop	Hazard 1 – Loss of tram control Hazard 2 – Unexpected machine movement	5.88×10^{-4}	3

[1]Only one safety function, the emergency stop, is shown for example purposes.
[2]Information not included for this case study example.

5.2 Key Documents

5.2.1 External Documents

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.

5.2.2 Acme Machine Company Documents

The following documentation is supplied by Acme Machine Company:

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.

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.

5.3 Introduction

This safety file documents the functional safety for the design of 20 CM machines.

5.4 Scope

The scope is limited to safety functions 1 through 5 (SF1 to SF5) of the X11 CM machine. Other support machinery and personnel are not included.

5.5 System Overview

A CM machine operates underground to cut coal. Each machine can be operated manually by a worker seated in the operator's compartment or by using a wireless or tethered remote-control pendant.

The CM machine's basic operation can be described in three steps, as shown in Figure 2: (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 is powered hydraulically. Machine movements are via left and right 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 PLC.

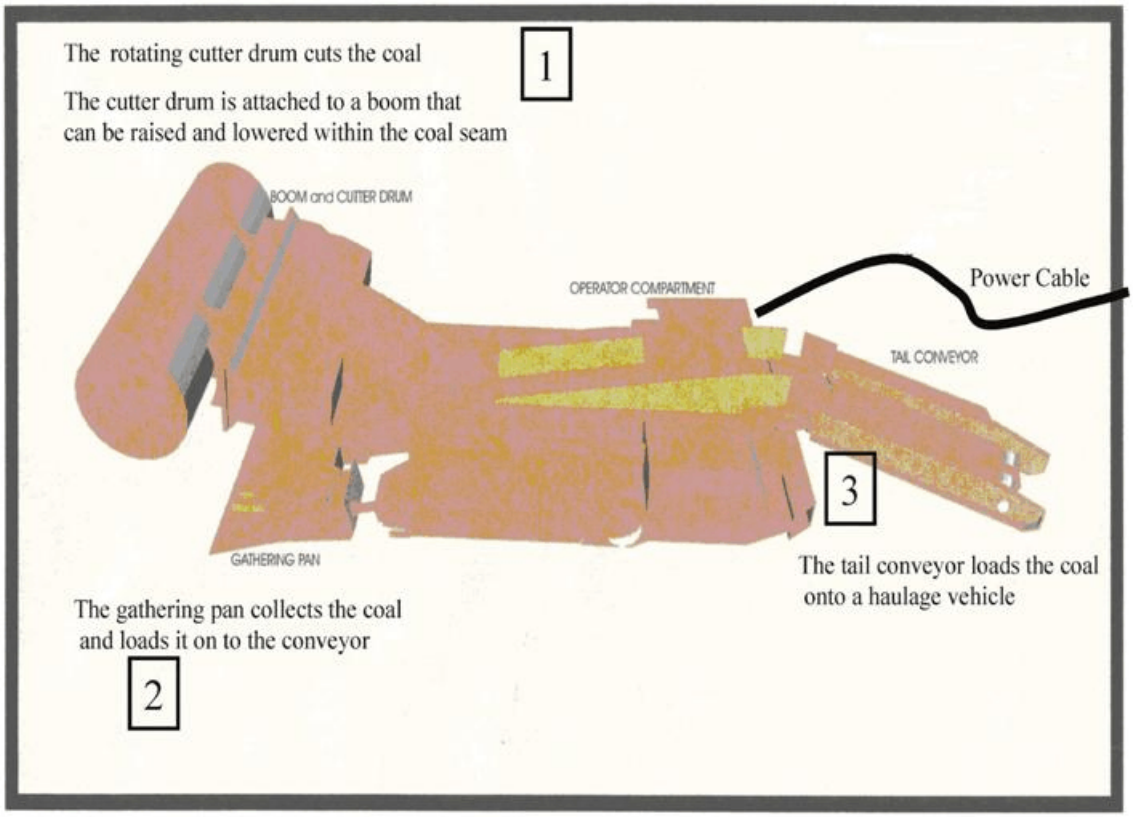


Figure 2.—The X11 continuous mining machine.

5.6 Management of Functional Safety

The management of functional safety is conducted during all stages of the safety and development life cycles. Plans are an important management tool; they are used to systematically establish and document processes, responsibilities, and tasks. Key portions of the following plans are provided:

- System safety plan
- Management of change plan
- Software safety plan
- Software development plan

5.6.1 System Safety Plan

The Acme System Safety Plan, document No. SSP–01–2004, is based on the safety life cycle and recommendations described in the System Safety document 2.1 [Sammarco and Fisher 2001].

The key portions of the Acme System Safety Plan and the associated results from implementing the plan are presented in the following sections.

5.6.1.1 Management of Change (MOC) Plan

The MOC plan pertains to both hardware and software. The plan follows recommendations described in the System Safety document 2.1 [Sammarco and Fisher 2001] and the Software Safety document 2.2 [Fries et al. 2001]. Figure 3 depicts the MOC process.

5.6.1.2 Risk Management

Multiple hazard analyses were conducted as part of the risk management. The hazard and risk analyses were conducted at the system level for the X11 CM machine. Three hazard analysis techniques were used to identify system hazards: checklists, HAZOP, and fault-tree analysis. Next, the level of risk for each hazard was assigned by use of a risk matrix. The assignment of an SIL for each hazard was based on this risk matrix.

5.6.1.3 Hazard Analysis

Multiple hazard analysis techniques were used, as detailed in the System Safety document 2.1 [Sammarco and Fisher 2001]. The techniques used were checklists, HAZOP, and fault-tree analysis.

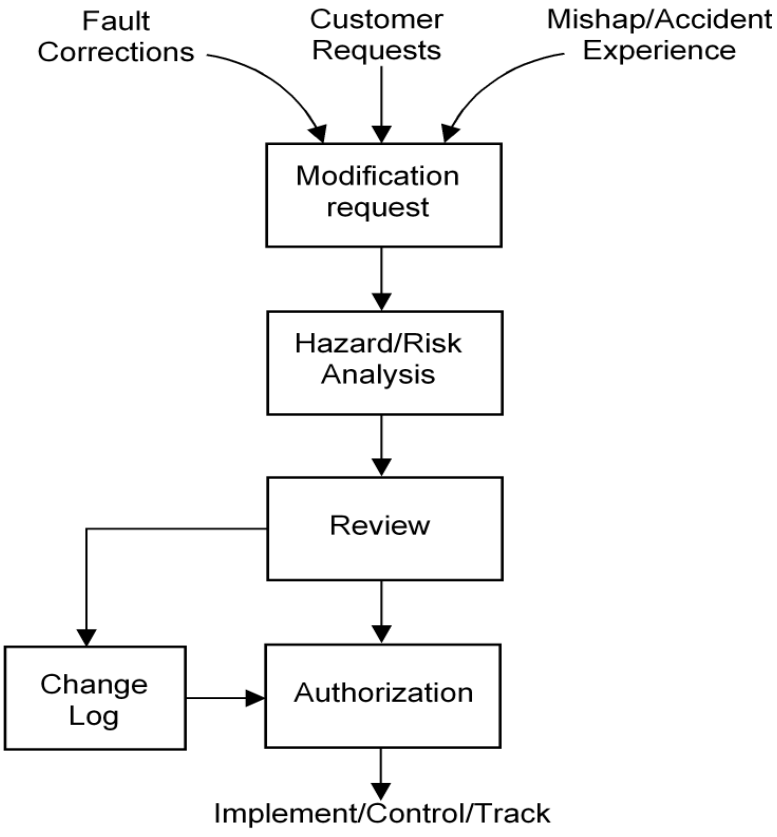


Figure 3.—Management of change (MOC) process.

Checklists

The following checklist items have been extracted from Appendix A of the System Safety document 2.1 [Sammarco and Fisher 2001]. The hazard associated with each checklist item is also given.

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, and 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

HAZOP

A high-level HAZOP data sheet is presented for the initial design phases of the machine. The HAZOP data sheet (Table 5) lists the results of analyzing the PLC data line to control the tram functions.

Table 5.—HAZOP data sheet for the PLC data line to control the tram functions

HAZOP

SYSTEM Continuous Miner DATE 9/20/04
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	PLC data line to control tram functions	Control data	No	1. PLC fails 2. Severed wire 3. Connector failure	Loss of tram control. The state of the tram can't be changed. If the machine is tramming forward, no data are sent to stop it.	Use watchdog timer. Use output monitoring (read back). Use data error checking.	Dangerous failure
			More	1. PLC sends incorrect data values. 2. Pendant sends incorrect data values.	Unexpected machine movement; machine trams faster than expected	Use watchdog time. Use output monitoring (read back). Use data error checking.	Dangerous failure
			Less	1. PLC sends incorrect data values. 2. Pendant sends incorrect data values.	Unexpected machine movement; machine trams slower than expected	Use watchdog timer. Use output monitoring (read back). Use data error checking.	Safe failure
			Reverse	1. PLC sends incorrect data values. 2. Pendant sends incorrect data values.	Unexpected machine movement; machine trams in the wrong direction	Use watchdog timer. Use output monitoring (read back). Use data error checking.	Dangerous failure

Fault-tree Analysis

The general hazards of loss of machine control and unexpected machine movement were combined to make a more specific hazard—loss of tram motor control. Figure 4 shows the fault tree for this undesired outcome. Seven events (e.g., PLC fails, tram switch fails) were 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.

5.6.1.4 Risk Analysis

The following hazards have been identified:

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

A risk assessment matrix was used to determine the level of risk and associated SIL for each hazard. The parameters of severity and frequency are needed to use the risk assessment matrix. The severity was defined by the classifications shown in Table 6; frequency was defined by the classifications in Table 7. The risk matrix is presented in Table 8.

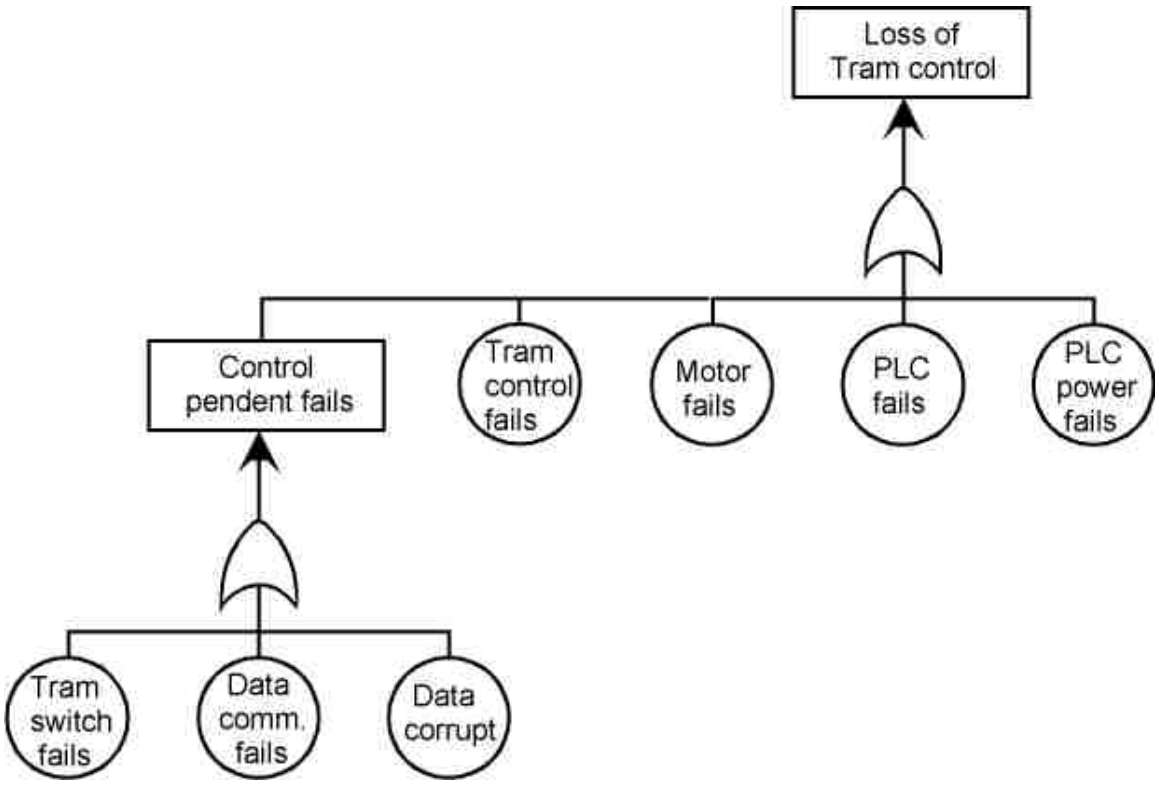


Figure 4.—Fault tree for the loss of tram control hazardous event.

NOTE 5: The risk assessment matrix presented in Table 8 is a tool for conducting subjective risk assessments. The various indices for risk (i.e., A=Unacceptable risk, B=Undesirable risk, C=Acceptable risk with management review and approval, and D=Acceptable risk without review or approval) are largely a management decision based on the amount of risk a company will assume as acceptable.

Table 6.—Severity categories specific to mine safety

Severity 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.

Table 7.—Frequency categories

Frequency 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.

NOTE 6: The frequency categories are a probabilistic component of risk. Therefore, the exposure should be taken into account based on a fixed time. Table 7 uses a yearly exposure as the time basis for the five frequency categories.

NOTE 7: The frequency categories of Table 7 are with respect to the given application concerning a CM machine.

Table 8.—Risk assessment matrix

Frequency category	Severity category			
	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	
A	Unacceptable risk
B	Undesirable risk.
C	Acceptable risk with review and approval of the chief engineer of Acme Machine Company.
D	Acceptable risk without review or approval.

NOTE 8: The risk assessment matrix (Table 8) is with respect to the given application concerning a CM machine. For instance, a fatality (critical) occurring once per year (frequent) corresponds to a risk index of "A, SIL 3." For this example, this is considered an unacceptable risk given the number of people, the number of CM machines, and the corresponding exposure. The risk indices of Table 7 might not be applicable to other applications.

NOTE 9: The risk assessment matrix (Table 8) has four categories of severity and five categories of frequency. Thus, it is a 4×5 matrix containing 20 cells. This is an example risk matrix; it could be simplified to a 4×4 matrix of 16 cells. It is advisable not to create too many cells, which can lead to confusion. Generally, subjective judgment should be limited to six discrete levels, so the largest matrix should be a 6×6 matrix of 36 cells.

Severity

Both hazards could potentially cause a fatality if the machine movement pinned or crushed a miner; therefore, the severity is "catastrophic" based on the categories in Table 6.

Frequency

The frequency for each hazard is about once every 2 years based on MSHA accident data for similar machines; therefore, the frequency is "probable" based on the categories in Table 7.

Risk

The risk for each hazard (Table 8) is classified as "A" given a catastrophic severity and probable frequency. This resulted in an unacceptable risk classification; therefore, the risk must be eliminated or reduced to an acceptable level.

5.6.1.5 SIL Assessment

The SIL for each hazard was determined by using Table 8, where a risk classification of "A" is assigned an SIL 3. The SIL for each hazard is summarized in Table 9.

Table 9.—Hazard and SIL summary

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

5.6.1.6 System-level Safety Requirements

Description: The emergency stop function shall stop movement of the machine and all electrical or hydraulic-driven devices on the machine. This function includes the emergency stop function's default state, safe state, triggering event(s), and the reset.

Associated Hazard(s):

- Loss of machine control. Reference hazard H1 of the hazard and risk analyses.
- Unplanned movements of continuous miner. Reference hazard H2 of the hazard and risk analyses.

Default State: Deenergized.

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.

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.
- Depressing a large red button shall trip the emergency stop function.
- The button must be physically reset to return to the normal state once it is depressed.
- The state of the emergency stop function shall be readily determined by visible inspection of the pushbutton-type switch as follows:
  - The button is depressed and maintained 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.

Response Time: The emergency stop function shall be completed such that no delay is purposely introduced. The total response time includes the response time of the machine's hydraulic and electrical control systems.

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

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

5.6.2 Software Safety Plan

The Acme Software Safety Plan, document No. SWSP–02–2004 follows the software safety life cycle and recommendations of the Software Safety document 2.2 [Fries et al. 2001].

The key portions of the Acme Software Safety Plan and the associated results from implementing the plan are presented in the following sections.

5.6.3 Management of Change (MOC) Plan

All critical software that is generated or modified by Acme must follow the MOC plan described in section 5.6.1.1.

5.6.4 Software Development Plan

All critical software developed by Acme must follow the "V" model of software development, as shown in figure 5. This is a systematic process that begins with the software requirements and concludes with validated software. The "V" model accommodates the iterative nature of software development.

NOTE 10: The "V" model is one of many models for software development. This example does not imply that the "V" model is the only acceptable model of software development.

5.6.4.1 Software Language Restrictions

All critical software that is generated by Acme is limited to the following: a restricted instruction set of ladder logic as supplied by the safety PLC vendor, the Acme coding standard, and MISRA C restricted instruction set for the C programming language.

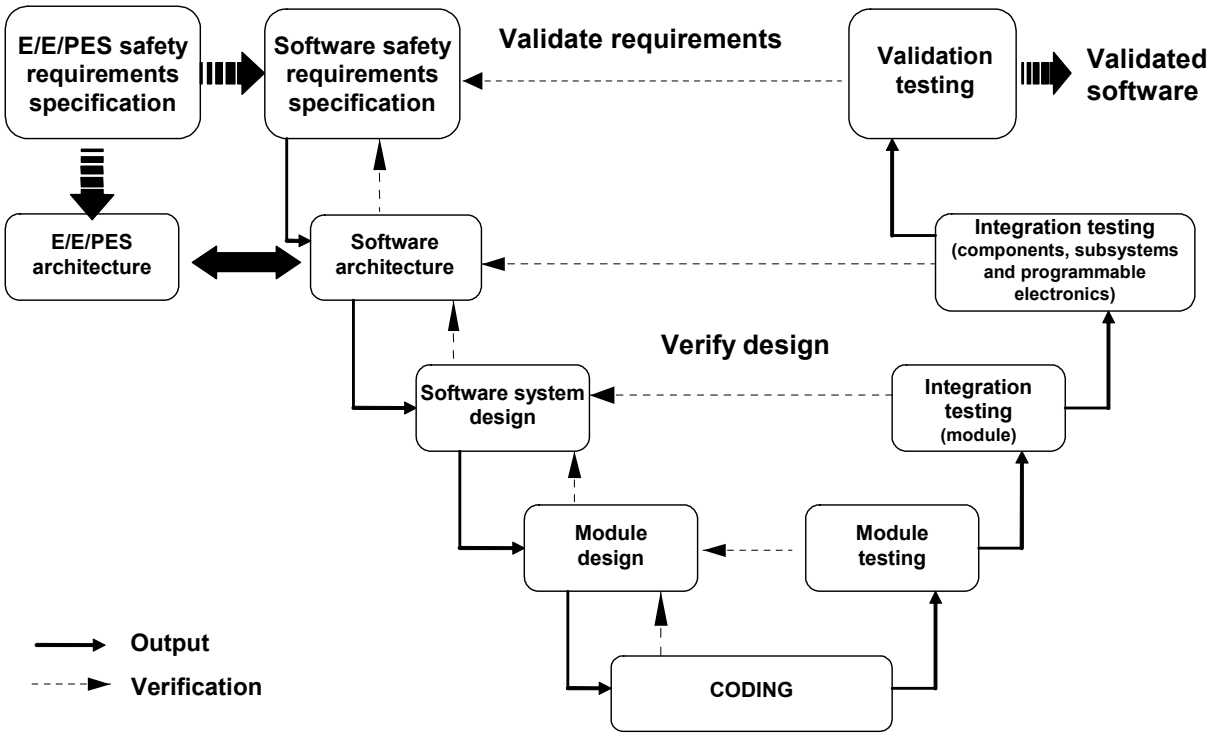


Figure 5.—The "V" model of software development.

NOTE 11: The Motor Industry Software Reliability Association (MISRA) is an industry collaboration that promotes best practices in developing safety-related electronic systems in road vehicles and other embedded systems [MISRA 2005]. MISRA C is a restricted subset of the C programming language for applications requiring SIL 2 and above.

5.6.4.2 Software Safety Requirements

NOTE 12: The software safety requirements should address each software safety function for the system. Only the emergency stop function is shown in this example.

The software safety requirements will comply with the system-level safety requirements (section 5.6.1.6) where appropriate. The safety requirements unique to software are defined below.

General:

- All critical software functions and their associated software modules must be separate from noncritical software functions and modules.
- All program memory for critical software must be hardware write-protected.

Functions:

The software function requirements are modeled by the state/transition diagram shown in Figure 6. The functional requirements are as follows:

1oo2D mode – The PLC is functioning properly and has dual-channel redundancy.

- The emergency stop function must be available in the 1oo2D mode.
- The emergency stop function must be available during fault conditions that result in the PLC changing from a 1oo2D mode to a 1oo1D mode.
- The emergency stop function is invoked if an I/O fault is detected.
- The emergency stop function is invoked if an emergency stop switch is depressed.
- The emergency stop function is invoked if output monitoring detects an unsafe tram condition.

1oo1D mode – The PLC is functioning properly, but it is restricted to 1 hour of operation.

- The emergency stop function must be available in the 1oo1D mode.
- The emergency stop function must be invoked if the PLC fails while in a 1oo1D mode.
- The emergency stop function is invoked when the 1-hour timeout expires.
- The emergency stop function is invoked if an I/O fault is detected.
- The emergency stop function is invoked if an emergency stop switch is depressed.
- The emergency stop function is invoked if output monitoring detects an unsafe tram condition.

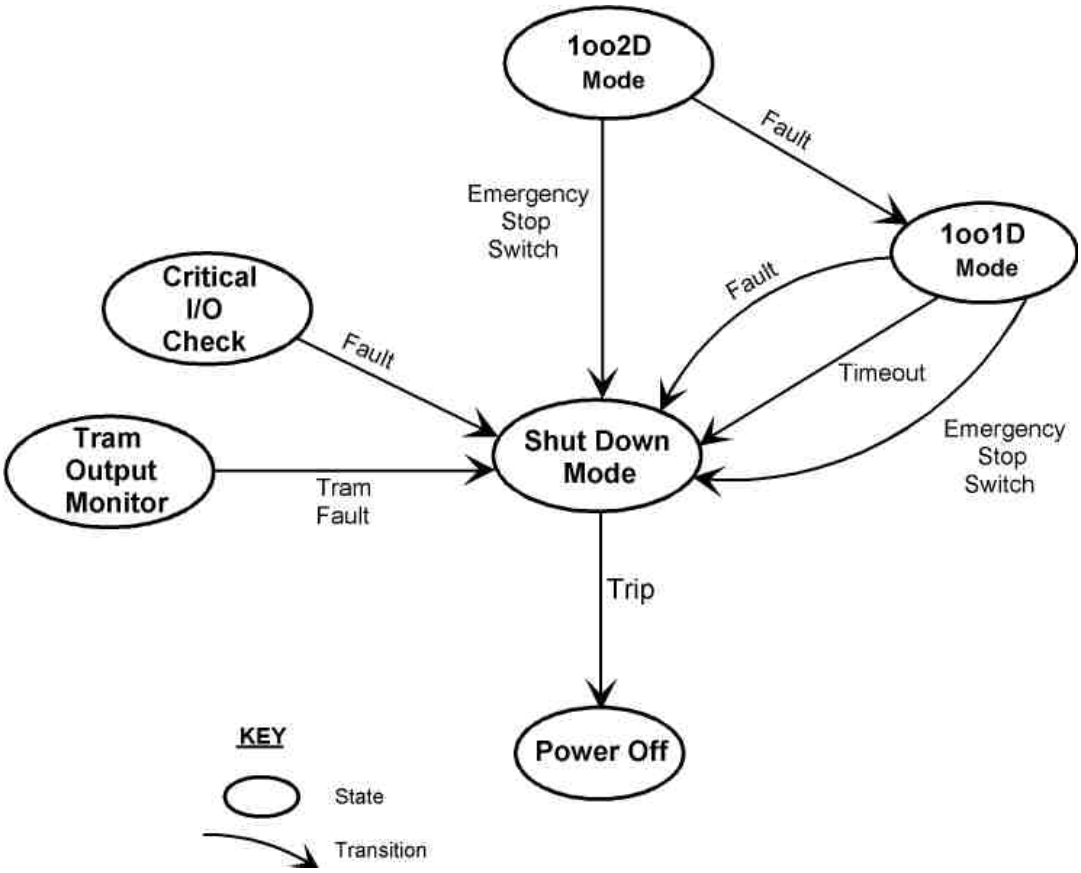


Figure 6.—The software functional requirements for various system states under normal and fault conditions.

Performance: The software scan time must be less than 50 milliseconds. The scan time includes the time to read the inputs, execute the program, run diagnostics, perform communications, and update the outputs.

Safety (Integrity) Level: SIL 3

Failure detection and handling:

- The status of input modules must be monitored and handled as follows (Table 10):

Table 10.—Input status codes

Status code	Status	Result
1	Not used	Not used.
2	Input fault	Trip emergency stop.
3	No faults	Function enabled.
4	Reserved	Function enabled.

- The status of output modules must be monitored and handled as follows (Table 11):

Table 11.—Output status codes

Status code	Status	Result
5	Output fault	Trip emergency stop.
6	No faults	Function enabled.
7	Reserved	Function enabled.

- The PLC mode must be monitored and handled as follows (Table 12):

Table 12.—PLC mode parameters

Mode parameter	Result
Dual (1oo2D mode, no faults)	Function enabled.
Single (1oo1D mode, one fault, no timeout)	Function enabled.
Time (1oo1D mode, 1-hour timeout expired)	Trip emergency stop.
Zero (not operational)	Trip emergency stop.

- The proper sequential execution of critical software must be checked online by using time-stamped program flow sequence monitoring or an equivalent method. An out-of-sequence condition trips the emergency stop.

- Output monitoring of the tram motors is required to verify that the state of the machine's tram motors is consistent with the state of the machine's tram invoked by the machine's operator.

5.6.5 Hardware Design Description

The approach to mitigate the risks of hazards H1 and H2 was to incorporate a safety system for an emergency stop function. The safety system design covers all system hardware components—the emergency stop switches, PLC hardware and software, circuit breakers, current sensors, and the humans interacting with the machine. The emergency stop function was assigned to two independent layers of protection; therefore, each protection layer was designated as safety-critical.

5.6.5.1 Protection Layer 1

The first protection layer is invoked by the PLC. The design 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, e.g., the tram motors are energized when they should be off, the protection layer will shut down power to the tram subsystem.

The protection hardware (Figure 7) consists of a tram motor current sensor, a PLC, and a circuit breaker connected to the tram motor subsystem. The design uses an existing PLC that also provides machine control functions. In essence, the PLC is "shared" for control and safety functions; therefore, this design does not physically and logically separate the safety function from the machine's control functions. Also, the design shares the existing wiring from the PLC to the circuit breaker.

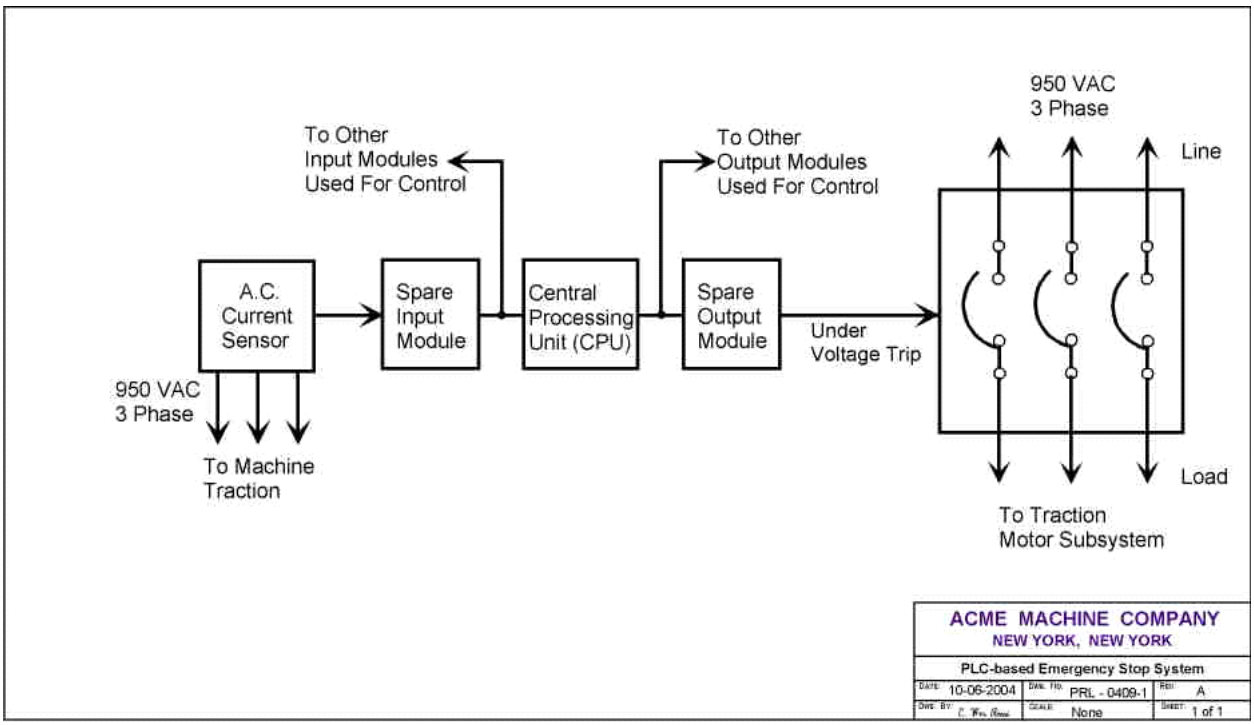


Figure 7.—The layer of protection automatically invoked by the PLC.

NOTE 13: It is generally not recommended to share a PLC for control and safety functions, although it is possible.

5.6.5.2 Protection Layer 2

The second protection layer is manually invoked. The design uses a dedicated, hard-wired circuit. All components and wiring of this design are used only for the emergency stop function; thus, two principles of safe design are followed:

- Keep the design simple.
- Physically and logically separate (isolate) the safety and control functions.

The design uses two switches directly wired to the mainline circuit breaker, as shown in Figure 8. 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.

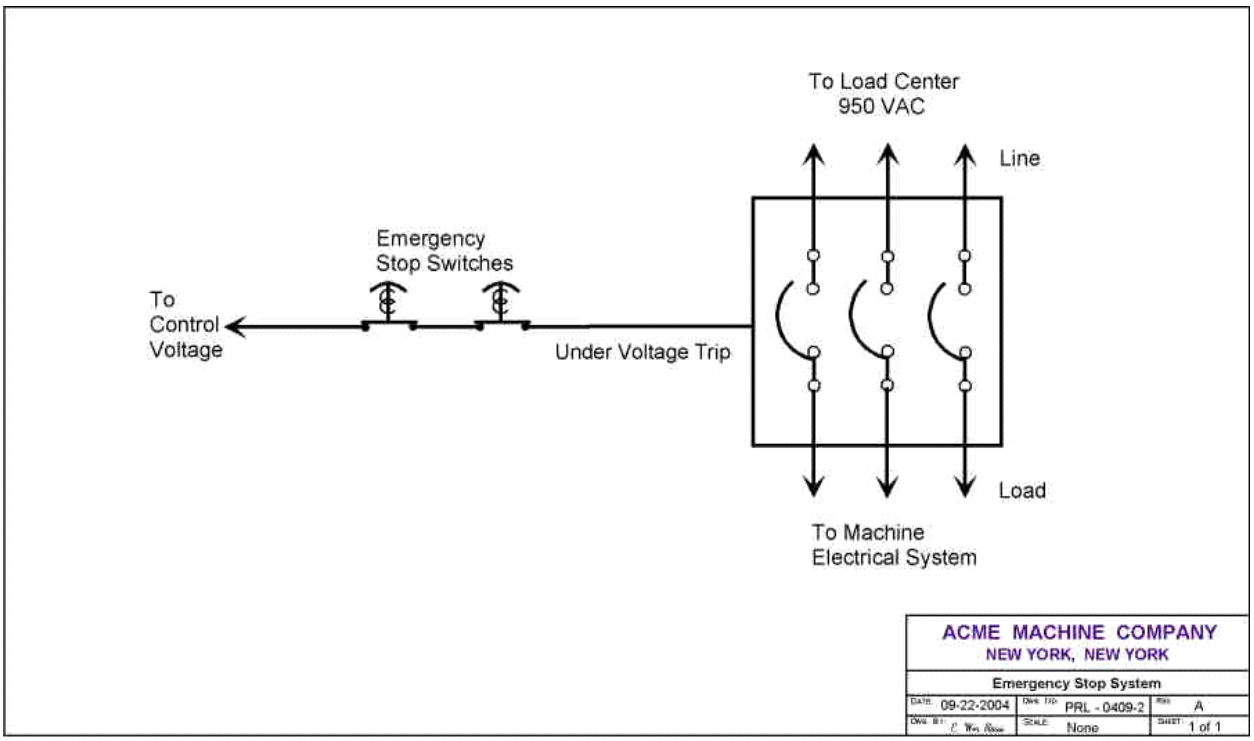


Figure 8.—The human-invoked manual protection layer.

5.6.5.3 PLC Hardware Architecture

The hardware architecture is 1oo2D and is shown in Figure 9. The system uses redundant channels of input and output circuits, and control modules; thus, the system can tolerate one fault. A fault detected by the diagnostics will result in the removal of services for the faulty channel; thus, the system is in a 1oo1D mode and continues to operate—there is not a shutdown. Two concurrent faults will shut down the PLC.

Diagnostics are provided for each channel. The diagnostics for each channel are connected for cross-checking, which improves diagnostic capabilities, safety performance, and availability.

The 1oo2D hardware is physically configured as two 1oo1D PLCs, with each PLC mounted in its own rack and enclosure. One PLC is mounted at the right front side of the CM machine; the other, at the right back side of the machine. This physical configuration improves common cause strength by reducing the exposure to common cause failures caused by physical damage and other environmental stressors.

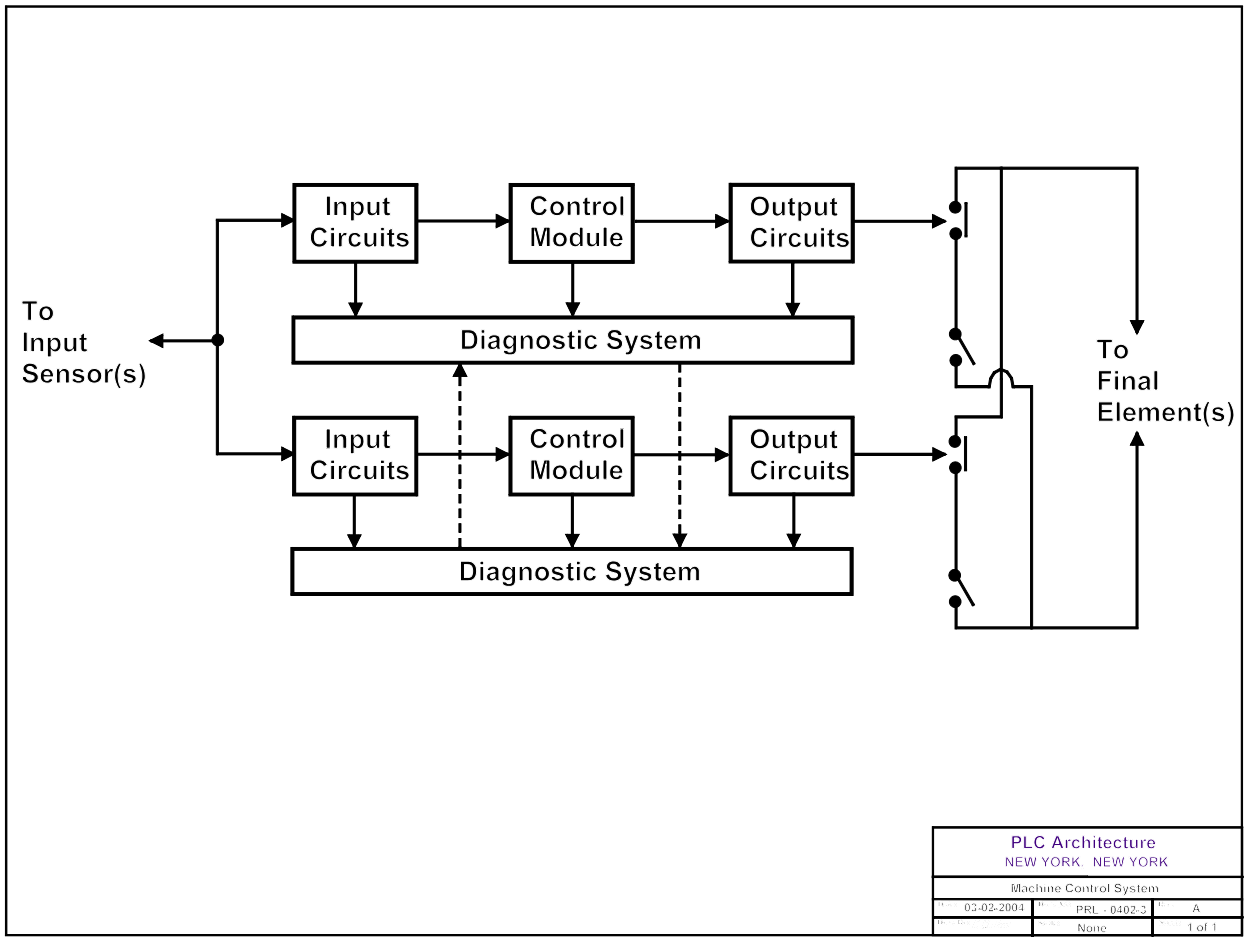


Figure 9.—The hardware architecture for the 1oo2D PLC.

5.6.5.4 Hardware Fault Tolerance

The fault tolerance is shown in Table 13. The operation of the 1oo2D PLC in the presence of one fault is determined by setting one of two options. Option 1 is set if the PLC is used for control purposes only. In this mode, the PLC will continue operation in the presence of one fault and it will operate as a 1oo1D PLC without any time restrictions. The option 2 mode is used when the PLC implements an emergency stop function. If one fault exists, the PLC will operate as a 1oo1D PLC for 1 hour before shutting down. The PLC is configured in the time-restricted option 2 mode because the PLC is used for an emergency shutdown system.

Table 13.—PLC hardware fault tolerance states

Condition	PLC state	Restrictions
No faults	Operates as 1oo2D	None.
One fault	Restricted mode: operates as 1oo1D until 1-hour timeout expires.	Time-restricted operation is used (an optional mode of operation; timeout = 1 hour).
Timeout expired . . .	Shutdown	None.
Two faults	Shutdown	None.

5.6.5.5 Hardware Safety Data

The hardware safety data identify the hardware components and their associated failure data. The safety data are listed in Tables 14–18.

Table 14.—Emergency pushbutton switch data

EQUIPMENT ITEM: Emergency Stop Pushbutton Switch			**Item No.:** SW1, SW2
GENERAL INFORMATION			
Manufacturer	Acme Switch Company		
Model	#SW		
Analog/Digital	Digital		
Architecture Type	A	**Hardware Fault Tolerance**	0
Data Source	XYZ Failure-rate Database		
Comments	Normally closed contacts; no diagnostics		
FAILURE RATE DATA	**PER 10^9 HOURS (FITs)**		
Fail Dangerous Detected	—	λ_{DD}	
Fail Dangerous Undetected	400.0	λ_{DU}	
Fail Safe Detected	—	λ_{SD}	
Fail Safe Undetected	600.0	λ_{SU}	
Safe Failure Fraction (%)	60.0	SFF	

Table 15.—Low-voltage trip circuit breaker CB1 data

EQUIPMENT ITEM: Low-voltage Trip Circuit Breaker			**Item No.:** CB1
GENERAL INFORMATION			
Manufacturer	Industrial Circuit Breaker Company		
Model	LV–CB1		
Analog/Digital	Digital		
Architecture Type	A	**Hardware Fault Tolerance**	0
Data Source	Manufacturer data		
Comments	Deenergizer to trip; no diagnostics		
FAILURE RATE DATA	**PER 10^9 HOURS (FITs)**		
Fail Dangerous Detected	—	λ_{DD}	
Fail Dangerous Undetected	120	λ_{DU}	
Fail Safe Detected	—	λ_{SD}	
Fail Safe Undetected	1,380	λ_{SU}	
Safe Failure Fraction (%)	92	SFF	

Table 16.—Low-voltage trip circuit breaker CB5 data

EQUIPMENT ITEM: Low-voltage Trip Circuit Breaker			**Item No.:** CB5
GENERAL INFORMATION			
Manufacturer	Industrial Circuit Breaker Company		
Model	LV–CB		
Analog/Digital	Digital		
Architecture Type	A	**Hardware Fault Tolerance**	0
Data Source	Manufacturer data		
Comments	Deenergizer to trip; no diagnostics		
FAILURE RATE DATA	**PER 10^9 HOURS (FITs)**		
Fail Dangerous Detected	—	λ_{DD}	
Fail Dangerous Undetected	120	λ_{DU}	
Fail Safe Detected	—	λ_{SD}	
Fail Safe Undetected	1,380	λ_{SU}	
Safe Failure Fraction (%)	92	SFF	

Table 17.—Current sensor data

EQUIPMENT ITEM: AC Current Sensor			**Item No.:** S1, S2
GENERAL INFORMATION			
Manufacturer	Acme Power Company		
Model	#SL		
Analog/Digital	Analog		
Architecture Type	A	**Hardware Fault Tolerance**	0
Data Source	XYZ Failure-rate Database		
Comments	No diagnostics		
FAILURE RATE DATA	**PER 10^9 HOURS (FITs)**		
Fail Dangerous Detected	—	λ_{DD}	
Fail Dangerous Undetected	137	λ_{DU}	
Fail Safe Detected	—	λ_{SD}	
Fail Safe Undetected	853	λ_{SU}	
Safe Failure Fraction (%)	87	SFF	

Table 18.—Data for a safety PLC as supplied by the manufacturer

EQUIPMENT ITEM: SIL 3 Certified PLC			**Item No.:** PLC1
GENERAL INFORMATION			
Manufacturer	XYZ Safety PLC Company		
Model	#SA–3		
Logic Solver Type	PLC	**Certified for Use up to SIL**	3
Configuration	1oo2D	**Beta Factor (%)**	1
Architecture Type	B	**Hardware Fault Tolerance**	1
Data Source	Failure modes, effects and diagnostic analysis (FMEDA) by manufacturer		
Comments	None		

FAILURE RATE DATA	**PER 10^9 HOURS**				
	Model No.	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
Main Processor	SA–3 PLC	7,425.00	75.00	2,375.00	125.00
Power Supply	PS–3	2,250.00	—	250.00	—
Analog in Module	A–3	990.00	10.00	900.00	100.00
Digital Out Low Module	D–3	760.00	40.00	190.00	10.00
Total Safe Failure Fraction (%) = 80.0					

5.6.6 Software Design Description

The software is categorized as follows:

- Application software (e.g., I/O functions)
- Embedded software (e.g., vendor-supplied software, such as the operating system)
- Utility software (e.g., software tools to develop and verify application software; also includes library software such as a C-Compiler library)

The software design pertains to all application software for the emergency stop function. The design begins with a conceptual design and is followed by a high-level preliminary design. The detailed design follows once the conceptual and preliminary designs are accepted.

NOTE 14: The detailed software design is not presented.

5.6.6.1 Software Conceptual Design

The conceptual design is shown in Figure 10. The application software for the emergency stop function is separate from application software used for controlling the mining machine. The embedded software (operating system and software library functions) is the only software used by both control and safety functions.

5.6.6.2 Preliminary Software Design

The preliminary design is depicted by hierarchical decomposition (Figure 11) to the level of software modules. The diagram uses a rectangle to represent a software module.

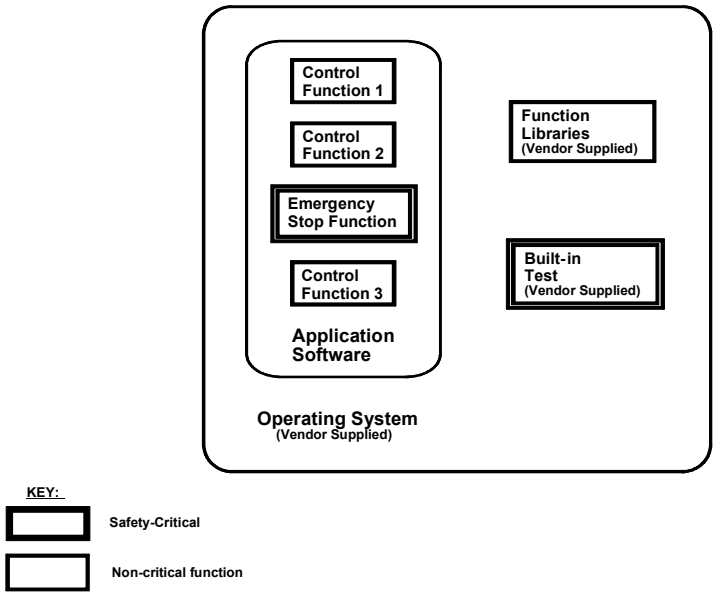


Figure 10.—The conceptual software design.

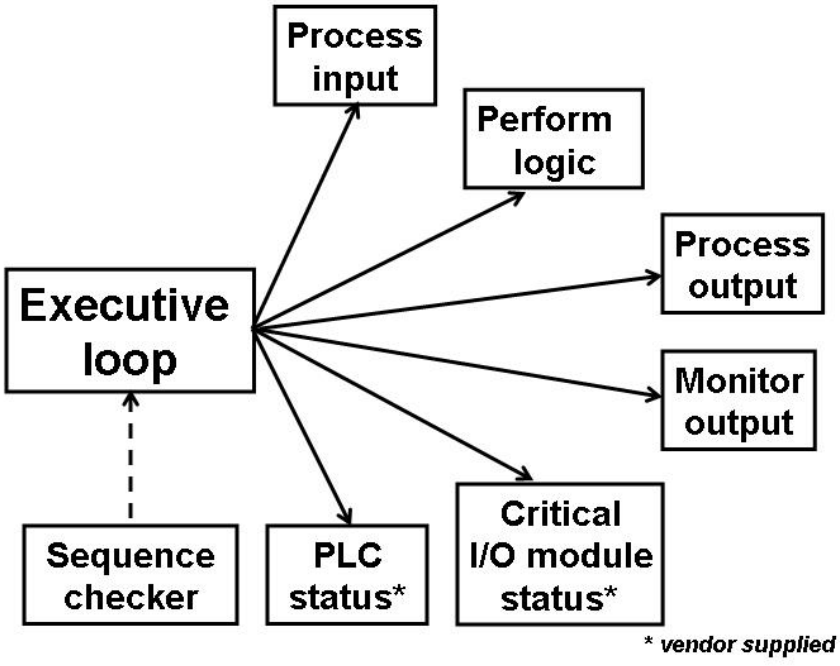


Figure 11.—The preliminary software design.

5.6.6.3 Software Module Descriptions

- Executive loop – Continuous loop of tasks for each scan cycle.
- Process input – Obtain emergency stop switch status and assign input variable value.
- Perform logic – Determine the correct output states given the states of the input, I/O, and the PLC.
- Process output – Control the state of the output to trip the circuit breaker (machine shutdown); send indication of output status where an alarm and indicator light are used to alert people of an output fault.
- Monitor output – The state of the machine's tram motors is checked to see if they are consistent with the state of the machine's tram invoked by the machine's operator. If they are not (e.g., the tram motors are on, but the operator did not request this state), then the tram subsystem is deenergized to a safe state.
- I/O status (vendor-supplied) – Library function that checks the status of safety-critical inputs and outputs.
- PLC status (vendor-supplied) – Library function that checks the PLC status.
- Sequence checker – Verifies that the executive software loop is operating tasks in the proper sequence and within the time limits set for each task to complete.

5.7 Safety Verification of Hardware

The achieved SIL of this design was verified with the SIL calculation tool called SafeCalc [http://www.risknowlogy.com/modules.php?op=modload&name=Downloads&file=index&req=MostPopular&ratenum=50&ratetype=num/]. The tool's calculations are based on Markov models. Version 1.2 of the tool was used.

SIL verification criteria are based on Table 19 below, which lists the SIL assignments for PFD_{avg} ranges. This table is a replication of Table 2 in the System Safety document 2.1 [Sammarco and Fisher 2001].

Table 19.—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.

Architectural constraints are also used as part of the SIL verification criteria. Table 20 lists the architectural constraints for type-A devices; Table 21 lists the architectural constraints for type-B devices.

Table 20.—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 21.—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

The safe failure fraction (SFF) metric was used for constraining the maximum SIL that can be claimed regardless of the calculated hardware reliability.

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

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

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

5.7.1 SIL Verification

SILs were verified by using a software tool that calculates PFD_{avg} given the system architecture, parameters, and assumptions that are supplied by the user. The following component parameters were used by the SIL verification tool:

β [%]	The β-factor or common cause factor. This factor is not applicable to 1oo1 or 1oo1D architectures; therefore, the symbol "–" 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 resulting in a safe failure
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)

5.7.1.1 Assumptions

The results (Figures 12–13) of the SIL verification tool are based on the following assumptions:

- Manual test interval (TI) = once per year
- Mean time to repair (MTTR) = 4 hours
- The pushbutton switches, current sensor, and circuit breaker are type-A devices.
- The wire is the logic solver for the manual protection layer.
- The wire is a type-A device.

5.7.1.2 SIL Verification Tool Results for Hardware

The hardware of protection layer 1 achieves SIL 2, and the hardware of protection layer 2 achieves SIL 3. The detailed results of using the SIL verification tool are shown in Figure 12 for the PLC-based protection layer and Figure 13 for the manual protection layer. Note that no architecture restrictions apply given the SFF of each layer.

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
current sensor	1oo1	Single	-	S1	A	9.9E-7	87	0	0	4	12	5.63E-04
Safety PLC	1oo2D	Redundant	1	PLC	B	2.5E-6	80	60	50	4	12	2.35E-05
Circuit breaker	1oo1	Single	-	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 **1.11E-03**
Safety Integrity Level **2**
Risk Reduction Factor **9.00E+02**
SIL not restricted by architectural constraints

Figure 12.—The SIL verification results for the PLC-based protection layer (layer 1).

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	1	SW1, SW2	A	1.0E-6	60	0	0	4	12	3.90E-05
wire	1oo1	Single	-	wire	A	1.0E-7	90	0	0	1	12	4.38E-05
Circuit breaker	1oo1	Single	-	CB5	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 **6.08E-04**
Safety Integrity Level **3**
Risk Reduction Factor **1.65E+03**
SIL not restricted by architectural constraints

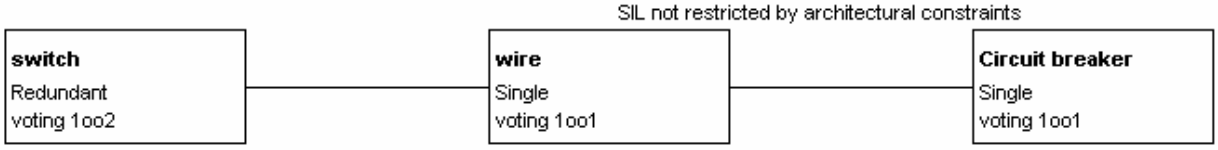


Figure 13.—The SIL verification results for the manual protection layer (layer 2).

5.7.2 The Emergency Stop Function SIL

The total $PFD_{avg} = 11.1 \times 10^{-3}$ (SIL 3) for the emergency stop function given the random hardware failures of both protection layers and the estimated human error rate for activation of the manual protection layer. The total PFD_{avg} was determined by using the fault tree of Figure 14.

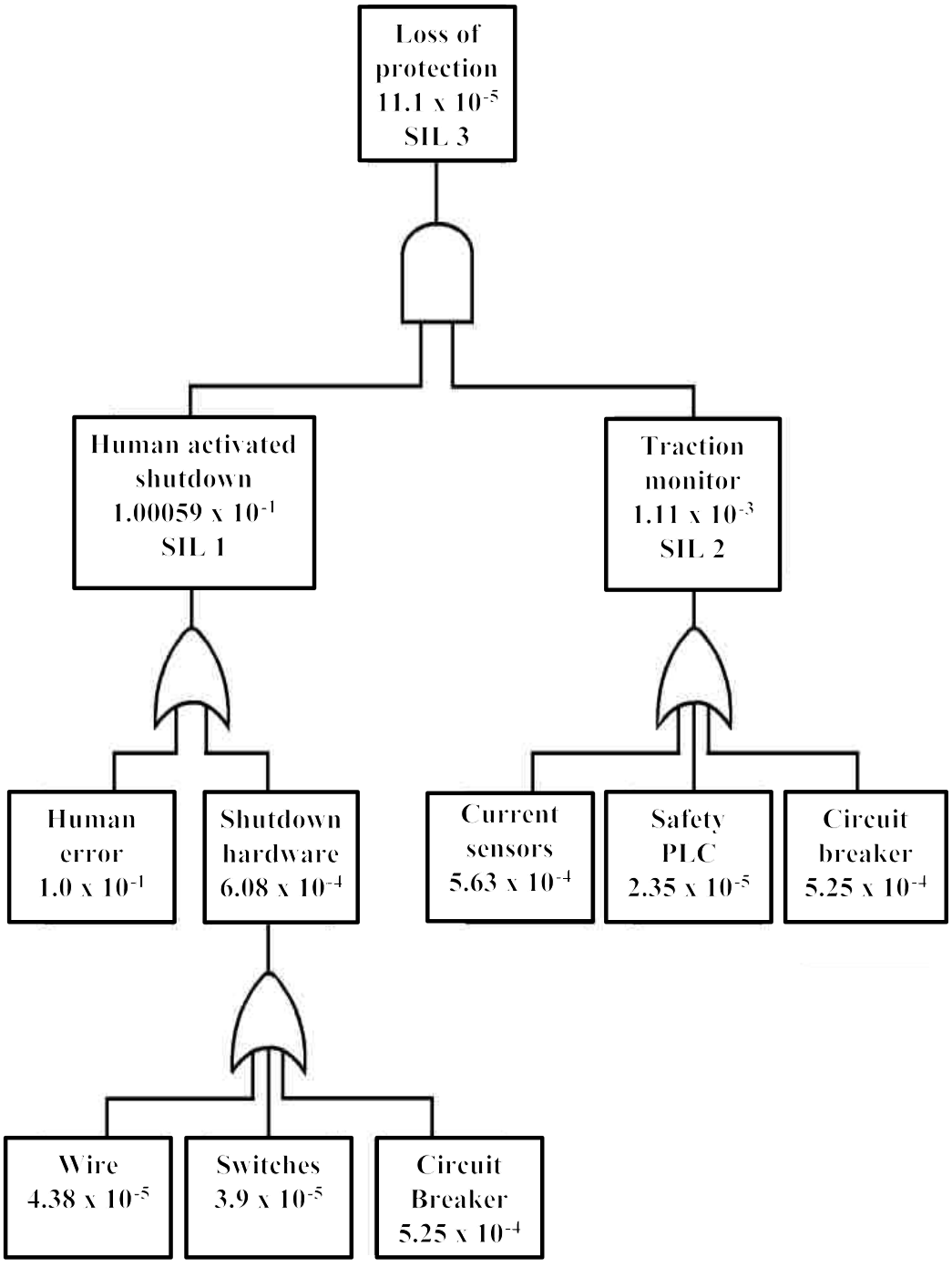


Figure 14.—Fault-tree determination of the total SIL achieved for the emergency stop function.

5.7.3 Conclusion

The emergency stop system hardware design meets the safety requirement of SIL 3 based on the following arguments:

- The two independent protection layers provide an SIL 3 based on the SIL assessment criteria (Table 19) and $PFD_{avg} = 11.1 \times 10^{-5}$.
- There are not any architectural constraints based on the criteria of Table 20 given that SFF >90% and the fault tolerance = 1.
- The SIL verification tool calculations concur that SIL 3 was attained and that there are not any architectural constraints.

NOTE 15: The emergency stop function was realized by using multiple protection layers to overcome the limitations of the human-activated protection.

5.8 Operation and Maintenance Plan

The plan follows the procedures and maintenance schedules as documented by the General Operation and Maintenance Manual document No. O/M–X11–104, which is shipped along with the CM machine to the end user. This document contains a complete description of the emergency stop manual test procedure, the frequency of testing once per year, and a warning that this testing is required for safety.

5.9 Installation and Commissioning Plan

The X11 CM machine can be shipped to the customer site as a completely assembled machine or in sections. The scope of installation and commission includes—

- Unloading or lifting of the machine
- The reassembly of the machine if the machine was shipped in sections
- Preoperation checks
- All initial mechanical adjustments (e.g., traction and conveyor chain adjustments)
- Final inspection checklist
- Startup and shutdown procedures
- Safety function tests

The installation and commissioning shall follow the tasks and procedures identified in the General Operation and Maintenance Manual document No. O/M–X11–104.

5.10 Concluding Safety Statements

5.10.1 The emergency stop system meets the safety performance of SIL 3 when used on an Acme Machine Company continuous miner model X11 and when maintained and tested as defined by the General Operation and Maintenance Manual document No. O/M–X11–104.

5.10.2 The safety performance of SIL 3 was evidenced by the safety validation, the stated assumptions, and the supporting documentation presented in this safety file.

5.10.3 Modifications to the software or hardware could reduce the safety performance; therefore, all modifications must follow the management of change plan, and it must be verified and documented that the safety performance of the system meets SIL 3.

REFERENCES

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.

MISRA [2005]. The Motor Industry Software Reliability Association. [http://www.misra-c.com/]. Date accessed: November 2005.

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 [2005]. Programmable electronic mining systems: best practice recommendations (in nine parts). Part 6: 5.1 System safety 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, DHHS (NIOSH) Publication No. 2003–150, IC 9480.

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, 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.

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 (1–800–56–4674)
Fax: 513–533–8573
E-mail: pubstaft@cdc.gov
www.cdc.gov/niosh

SAFER · HEALTHIER · PEOPLE™

DHHS (NIOSH) Publication No. 2006–130