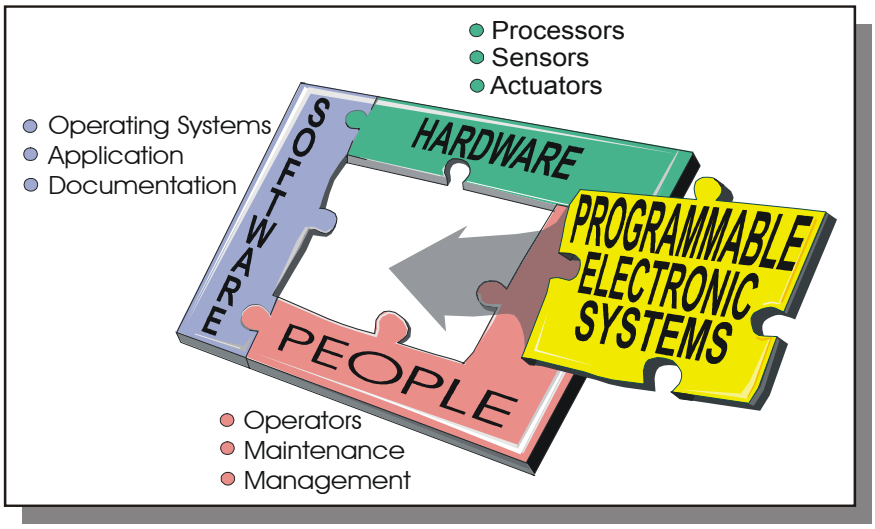
IC 9456

INFORMATION CIRCULAR /2001

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



Part 1: 1.0 Introduction

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 9456

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

Part 1: 1.0 Introduction

By John J. Sammarco, Thomas J. Fisher, Jeffrey H. Welsh, and Michael J. Pazuchanics

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

April 2001

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
Web site:	www.cdc.gov/niosh

DHHS (NIOSH) Publication No. 2001-132

CONTENTS

Page

Abstract 1
Acknowledgments 2
Introduction 2
Need for mining safety life cycle 2
System safety solution overview 4
Mining example 7
Benefits of mining safety life cycle approach 8
Glossary 9
References 10

ILLUSTRATIONS

1. The safety framework and associated guidance 1
2. Primary causes of failure for 34 industrial accidents 3
3. A simplified safety life cycle 4
4. A basic programmable electronic mining system 5
5. Example of protection layers for a mining system 6
6. The impact of change during development and operational phases 9

TABLES

1. Example of a risk assessment matrix 5
2. Safety integrity level performance requirements based on quantitative criteria 6
3. Example of mine mishap scenario 7
4. SIL values 10

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

Part 1: 1.0 Introduction

By John J. Sammarco,[1] Thomas J. Fisher,[2] Jeffrey H. Welsh,[3] and Michael J. Pazuchanics[1]

ABSTRACT

This report (An Introduction to Safety) is the first in a nine-part series of recommendations 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*.—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, and includes the benefits of implementing a system/software safety program.

• 2.1 *System Safety* and 2.2 *Software Safety*.—These reports draw heavily from International Electrotechnical Commission (IEC) standard 61508 and other recognized standards. The scope is "surface and underground safety mining systems employing embedded, networked, and non-networked 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*.—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 meets 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.

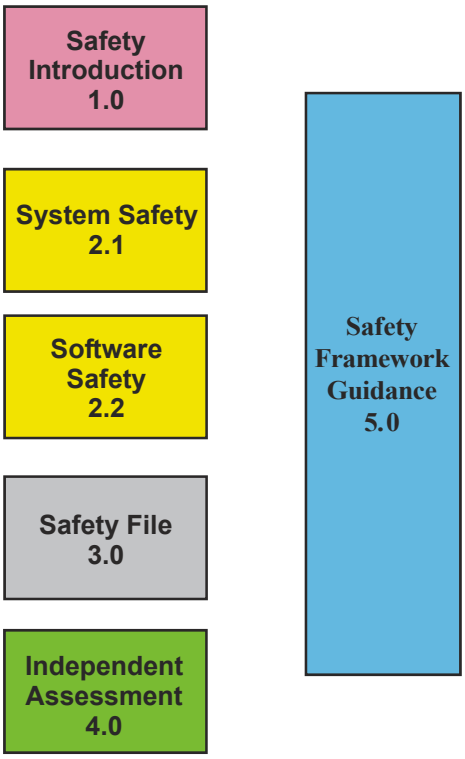


Figure 1.—The safety framework and associated guidance.

[1]Electrical engineer.
[2]Senior research physical scientist.
[3]Supervisory research physical scientist.
Pittsburgh Research Laboratory, National Institute for Occupational Safety and Health, Pittsburgh, PA.

• 4.0 *Safety Assessment*.—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 done by an independent third party.

• 5.0 *Safety Framework Guidance*.—It is intended to supplement the safety framework reports with guidance that provides users with additional information. The purpose is to help 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 treaty 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.

ACKNOWLEDGMENTS

The authors thank 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.

INTRODUCTION

Equipment using programmable electronics (PE) control is increasingly being used in many industrial applications because of the many advantages brought by this technology to the workplace. These include the ability to handle more functions, improved logic solving speed, and networking of communications. This in turn is resulting in added flexibility, reduced cost, and improved product quality. The use of PE control in mining is an emerging technology. The trend in using PE controls for mining equipment is expected to increase because mining's future depends on the use of new technologies. As stated in the *Wall Street Journal* [Phillips 1997]: "Mining, that most basic of industries, is increasingly throwing down its old tools and picking up new technology. It's a matter of survival."

This report is intended to create an awareness of the need for safety planning from conception through decommissioning of PE-based equipment used in mining applications. Because of the rapid increase in computerization of mining processes, issues concerning the functional and operational safety of PE are emphasized. Functional and operational safety start at the system level. Safety cannot be ensured if efforts are focused only on software. The software can be totally free of "bugs" and use numerous safety features, yet the equipment can be unsafe because of how the software and all of the other parts interact in the system. In other words, *the sum can be less safe than the individual parts.*

Thus, a system approach is needed. How does one address the safety of this system? By making the system more reliable, employing redundancy, or conducting extensive testing? All of these are necessary, *but are not sufficient to ensure safety*. Making a system more reliable is not sufficient if the system has unsafe functions. What could result is a system that *reliably* functions to cause unsafe conditions! Employing redundancy is not sufficient if both redundant parts are not safe. Testing alone is not sufficient for safety. Studies show that testing does not find all of the "bugs," and some systems are too complex to test every condition.

The key to safety is to "design in" safety early in the design by looking at the entire system, identifying hazards, designing to eliminate or reduce hazards, and doing this over the system life cycle. More detailed information on system and software safety is presented later in this report and in the references at the end of this report.

NEED FOR MINING SAFETY LIFE CYCLE

The mining industry has been implementing PE technology in mining control and monitoring systems to improve safety and health, increase productivity, and improve mining's competitive position. While providing benefit to the mine operator, PE also adds a level of complexity that, if not properly considered, may adversely affect worker safety. PE technology has unique failure modes different from mechanical systems or hardwired electronic systems traditionally used in mining. Design approaches that incorporate a system safety approach [Bennett 1995] are required to protect workers.

One example of PE in mining is computer-based monitoring of the mine environment. Underground mine environmental monitoring and control began in the late 1970s and grew in the 1990s to where almost 17% [Francart et al. 1997] of all U.S. underground coal mines have computer-based monitoring. These atmospheric monitoring systems (AMS) monitor the mine

environment for numerous items, including smoke, oxygen, temperature, methane, carbon monoxide, and airflow. The central computer station for these systems is typically at a surface location with cabling extended underground to a number of remote sensors. The central computer station collects data from the sensors and presents the information to an attendant, who can take action if monitored sensor data indicate a problem. One of the most frequent applications of AMS in mining involves the placement of carbon monoxide sensors along the belt haulage entry for early warning of the presence of a fire in that entry. By installing such a system, a mine operator in some cases[4] may be able to use the belt haulage entry as an intake air course to ventilate active face areas. Normally, the belt entry must be kept as a neutral air course. The proper functioning of the AMS is relied on to provide workers an early warning before fire products are carried to the "face" where they are working.

Another example of PE in mining is the monitoring and control of longwall mining roof supports. PE-based control of the roof support shield advancement process is found in almost all U.S. longwalls today [Fiscor 1998]. This can exist in bank-control mode where three adjoining shields are controlled together from a single PE controller, or there may be multiple PE controllers controlling all of the shields on the face. Another technology used in longwall mining is shearer-initiated automatic roof support advancement. Sensors are used to detect shearer location, and these data are used by a PE controller to advance the roof supports automatically.

Because PE control is an emerging technology in the mining industry, the number of mishaps involving injury to human life directly caused by a PE fault is very small. However, an increasing number of near misses and unexpected equipment actions are being reported. During 1996-98, eight mishaps involving PE were recorded; four were fatal. Mishaps and near misses involving PE have also occurred before 1996. The most infamous involves longwall faces where PE-controlled longwall roof support shields have been reported to move when the operator did not expect it [Dransite 1992]. Similar situations have been reported for other PE-controlled mining equipment.

The unexpected actions of PE-controlled mining equipment can be attributed to the following:

Poor design caused by—
- Inadequate safety requirement specification
- Lack of software and hardware configuration management
- Design errors

Improper operation caused by—
- Lack of software and hardware configuration management
- Lack of adequate and timely maintenance (e.g., malfunctioning position sensors and solenoid actuator valves)
- Systematic errors (e.g., errors in design)
- Sensor and actuator faults
- Lack of or inadequate training of the operator (the operation of the equipment is not completely understood)
- Poor human-machine interface

Because the mining industry's experience with PE is relatively small, lessons can be learned from other industries that have confronted the issue of PE safety. Therefore, we can focus efforts on the most significant root causes of mishaps and avoid repeating some of the same mistakes. A number of studies concur that most causes are traced to the safety requirement specification for the system. A study by Lutz [1992] on National Aeronautics and Space Administration software found that most problems with safety-related software came from misunderstandings and discrepancies in the requirement specification, i.e., inaccuracies, inadequacies, or confusion in defining the behavior that the PE-controlled equipment is desired to have. A study by the Health and Safety Executive [1995] in the United Kingdom of 34 mishaps involving processor control in industrial applications found that 44.1% of the causes were attributed to the safety requirement specification (figure 2). The second leading cause at 20.6% was attributed to changes after commissioning, i.e., mishaps caused by hazard(s) unknowingly introduced by software modifications after equipment is installed and operating.

PE faults can occur from hardware or software failures. Hardware failures usually result from random events and wear. They can involve any of the system components, programmable electronic devices, power supplies, sensors, data communication paths, actuators, etc. Software does not exhibit random wear-out failures. Instead, software failures result from systematic (logic or design) errors. These failures affect system safety in two ways [Leveson 1995]: (1) output values and/or timing that permits the system to reach a hazardous state or (2) failure to identify or properly handle hazardous events to which it must respond.

A worldwide effort by the International Electrotechnical Commission (IEC) is underway to integrate the safety life cycle into sector-specific safety standards and guidelines. The United States is represented by individuals from various industry sectors, such as the chemical process industry. This effort is

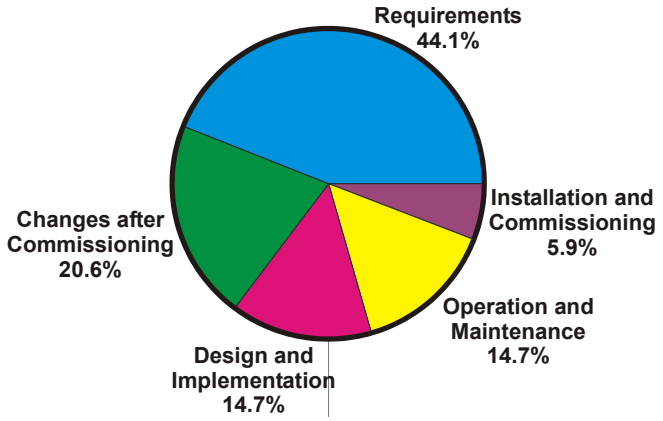


Figure 2.—Primary causes of failure for 34 industrial accidents [Health and Safety Executive 1995].

[4]Granted by MSHA on a case-by-case basis under a petition for modification of the application of a mandatory safety standard under section 101(c) of the Federal Mine Safety and Health Act of 1977.

based on IEC 61508, a standard (in draft form as of this writing) that addresses functional and operational safety [IEC 1998]. It is generic and serves as the "master" from which industry-specific standards are to be formed. One such industry-specific standard for the process industry is ANSI/ISA S84.01 [ANSI/ISA 1996]. At present, the mining industry has not developed a mining sector safety life cycle for its use. This report introduces a safety life cycle approach for the mining industry.

SYSTEM SAFETY SOLUTION OVERVIEW

The system safety concept can be traced back to 1947 where the key concept was to have *safety designed and built into the system*. This concept has since evolved to address the safety of complex, PE-based systems. Leveson [1995] states: "The primary concern of system safety life cycle is the management of hazards: their identification, evaluation, elimination, and control through analysis, design and management procedures." System safety life cycle emphasizes:

- Integrating safety into the design
- Systematic hazard identification and analysis
- Addressing the entire system in addition to the subsystems and components
- Using protection layers for risk reduction
- Qualitative and quantitative approaches

It is important from the very beginning of the mining equipment design to take into account safety considerations (design for safety) for the entire life cycle, including training, installation, operation, maintenance, and upgrades. Safety considerations must not be an afterthought once the design is completed. To achieve this, a safety life cycle is constructed to suit each application. The safety life is explained in detail by IEC 61508 [IEC 1998]. To present an overview of the general concepts, we have generated a simplified version of the safety life cycle (see figure 3) and have described the steps as follows:

(1) The first step in the safety life cycle is concerned with gaining an understanding of the mining application, the conceptual equipment design, and all parts of the system. The boundaries between the equipment under control, the control system, and the people must be determined to establish the system's scope. Figure 4 shows the boundary of a basic programmable electronic mining system.

(2) The second step involves identifying event sequences leading to hazardous events and determining risks associated with these events.

To be effective the hazard analysis process must be applied over the life cycle of the system in a continual and iterative manner. That is, hazard identification and analysis start at the conceptual stage of the project and continue on through the definition, development, production, and deployment stages. Leveson [1995] identifies three basic tasks in the hazard analysis process: (1) identify the hazard, (2) identify and evaluate the hazard causal factors, and (3) evaluate risk.

Many techniques, ranging from simple qualitative to advanced quantitative methods, are available to help identify and analyze hazards. The *System Safety Analysis Handbook* [Stephans and Talso 1997] provides extensive listings and descriptions. Some examples of the more commonly used techniques are the preliminary hazard list (PHL), preliminary hazard analysis (PHA), hazard and operability study (HAZOP), and failure modes and effects analysis (FMEA), which are defined below.

Preliminary hazard list (PHL).—This is the first analysis performed in the system safety process and strives to identify critical system functions and broad system hazards. It uses historical safety data from similar systems and mishap/incident

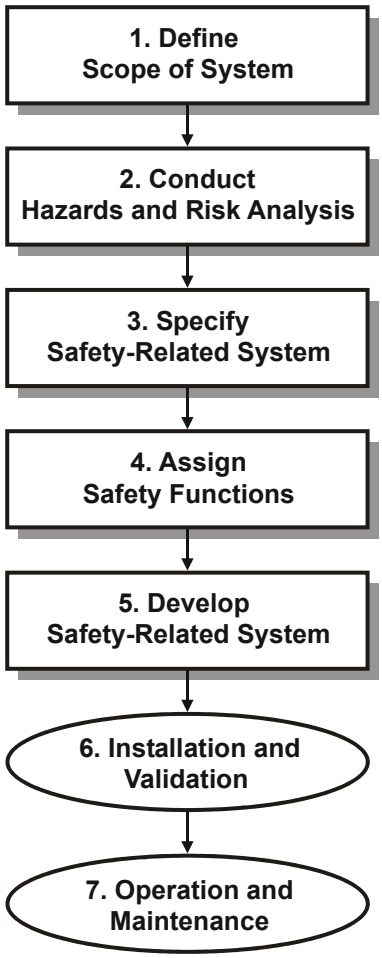


Figure 3.—A simplified safety life cycle.

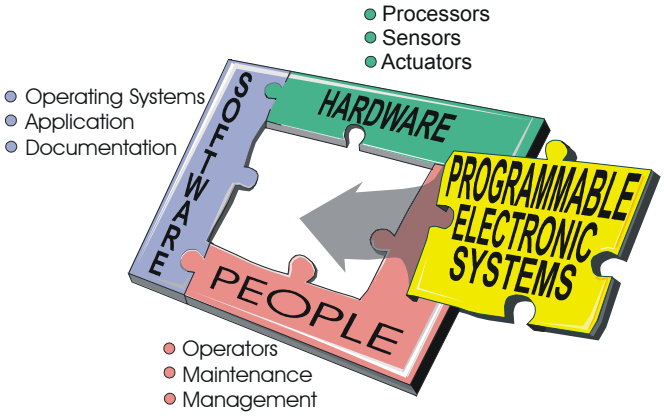


Figure 4.—A basic programmable electronic mining system.

hazard logs to guide the safety effort until more system-specific information is developed.

Preliminary hazard analysis (PHA).—This technique uses the results of PHL, lessons learned, system and component design data, safety design data, and malfunction data to identify potential hazard areas. In addition, its output includes ranking of hazards by severity and probability, operational constraints, recommended actions to eliminate or control the hazards, and perhaps additional safety requirements.

Hazard and operability study (HAZOP).—This is a systematic, detailed method of group examination to identify hazards and their consequences. Specific guide words are used to stimulate and organize the thought process. HAZOP [Ministry of Defence 1998] has been adapted specifically for systems using programmable electronic systems (PES).

Failure modes and effects analysis (FMEA).—This technique uses deductive logic to evaluate a system or process for safety hazards and to assess risk. It identifies the modes in which each element can fail and determines the effect on the system.

Each hazard has associated risks. The hazard identification and analysis outcomes are used to evaluate risks, thus enabling the relative importance and acceptability of each risk to be determined. Not all risks are equal, and some risks can be acceptable. For example, we accept a certain level of risk by driving our cars.

Qualitative and quantative methods are used to assess risk. One qualitative technique, shown by table 1, uses hazard severity and frequency. It aids users to systematically assess risks and then focus efforts on the most significant risks.

(3) The third step involves specifying the safety-related systems and protection layers needed to achieve the required functional and operational safety. The safety-related systems are specified in terms of safety functions and safety integrity. For some systems, a safety instrumented system (SIS) is added to achieve higher levels of safety. Other terms commonly used include "emergency shutdown system," "safety shutdown system," and "safety interlock system." The SIS can be composed of sensors, controllers (commonly called logic solvers), and final control elements for the purpose of preventing a hazardous event from occurring or taking the mining system to a safe state when dangerous conditions exist.

For the safety-related system, both non-SIS and SIS protection layers are considered. The desire is to first provide an appropriate number of non-SIS protection layers. If these do not provide enough protection, then additional SIS protection layers are required. Figure 5 shows an example of protection layers.

(4) The fourth step assigns safety functions. These are intended to achieve and maintain a safe state. Safety functions can be implemented in hardware or software. If these safety functions are implemented by the SIS, then a safety integrity level (SIL) is established for each safety function [ANSI/ISA 1996].

A safety function addressing an infrequent hazard that causes minor safety consequences may not need to be implemented by a SIS; thus, no SIL is assigned. There are qualitative and quantative methods to determine if an SIL is needed, and if so, the associated SIL definition. The SIL defines the level of safety performance needed to achieve the user's mining safety objective. SILs are defined as 1, 2, and 3. The higher the SIL, the better the safety performance and the higher level of rigor

Table 1.— Example of a risk assessment matrix

	Catastrophic	Critical	Marginal	Negligible
Frequent	A	A	A	B
Probable	A	A	A	C
Occasional	A	B	B	C
Remote	B	C	C	D
Improbable	C	C	C	D

Mishap risk index	Suggested criteria
A	Unacceptable
B	Undesirable
C	Acceptable with review
D	Acceptable without review

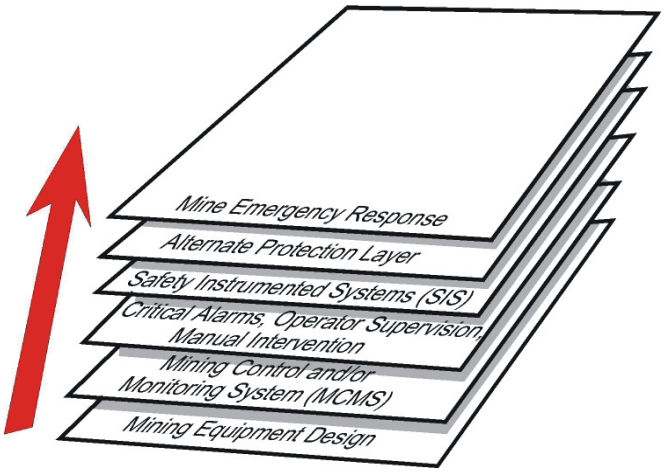


Figure 5.—Example of protection layers for a mining system.

to achieve it. For nuclear power applications, an SIL of 4 is typical. For most industrial applications, a three-level SIL is typical. Safety performance is improved by adding redundancy, more frequent testing, use of diagnostic fault detection, use of different sensors and final control elements, etc. Safety performance is also improved through better control of design, operation, maintenance procedures, and mine safety management.

Associated with the SIL is probability of failure on demand (PFD) average (see table 2). This is a metric to measure safety for the SIS. It is the probability of the SIS failing when a dangerous situation (the safety demand) occurs. Another safety metric is safety availability. This is the percentage of time during system operation that an SIS is able to perform protective functions. Safety availability equals 1 minus PFD. An average PFD for a given time period is used since PFD increases with time. In other words, PFD is very low if the system has operated for 1 hour versus 1 year.

(5) The fifth step involves developing the safety-related designs to meet the safety requirement specifications. All subsystems and components that make up a system must be considered in designing for safety. These include the programmable electronic devices, power supplies, sensors, data communication paths, actuators, the SIS, and the interaction of these components. The total system depends on all subsystems and components to work properly. A failure in one component may cause a catastrophic system failure. This step also includes the generation of safety plans for overall safety validation, operation, maintenance, and management of change.

(6) After installation, the commissioning and pre-startup acceptance test shall be done. Qualitative and quantitative approaches are combined when assessing integrity. Quantitative approaches are fine when implemented by experienced personnel (e.g., person with qualitative understanding). Close evaluation of qualitative versus quantitative shows that almost all applications use both approaches, but in varying degrees.

A pre-startup safety review (PSSR) includes the following:

• Verification that the SIS and non-SIS safety-related system was constructed, installed, and tested in accordance with the safety requirement specifications.

• Safety, operating, maintenance, management of change, and emergency procedures pertaining to the SIS and non-SIS safety-related system are in place and adequate.

• PHA recommendations that apply to the SIS have been resolved or implemented.

• Employee training has been completed and includes appropriate information about the SIS. Depending on the level of interface required between the operator and the machine, the PHA team may recommend that a simulator be available for timely operator training "refreshment."

(7) SIS and non-SIS safety-related system operation and maintenance procedures may be developed at any step of the safety life cycle and shall be completed before startup. If modifications are proposed, their implementation shall follow a management of change procedure. The appropriate steps in the safety life cycle shall be repeated to address the safety impact of the change.

All of these steps require active participation from and interaction with all members of the design team so that components of the system are not designed in isolation. The efficient, safe operation of a system requires that all components be designed with the total system operation in mind. The design team must be familiar with the intended use of the product, taking into account the environment in which it will operate. Participation from the end user is also important up front in the design stage so that the designer understands the needs of the user and how the user plans to use the system and under what conditions.

Table 2.—Safety integrity level (SIL) performance requirements based on quantative criteria

	SIL		
	1	2	3
Safety availability range . . .	0.9 to 0.99	0.99 to 0.999	0.999 to 0.9999
PFD average range	$10^{\&1}$ to $10^{\&2}$	$10^{\&2}$ to $10^{\&3}$	$10^{\&3}$ to $10^{\&4}$

MINING EXAMPLE

Traditionally, mining incidents are viewed in the context of near misses, injuries, and fatalities during operation and maintenance. The example presented here (see table 3) takes a holistic view from beginning to end. The purpose of this example is to create an awareness of dangers posed to all personnel that could have been averted if a system safety approach had been applied during all phases of the life cycle. After a mishap occurs, people are placed in dangerous situations as they inspect, troubleshoot, move equipment, and make repairs. Secondly, this example shows that safe designs are not

Table 3.—Example of mine mishap scenario

Time	Code	People (cumulative)	Narrative
			DAY 1
8:30 a.m.	NM	1	Machine moves unexpectedly, operator moves to escape. No injury.
8:45 a.m.	—	1	Mine personnel contacted: Chief Mine Engineer, Maintenance Engineer, and Safety Engineer.
10:00 a.m.	—	4	All mine personnel contacted arrive and begin troubleshooting.
10:45 a.m.	LTI	4	Maintenance person squats between machine and rib to read diagnostic display. Machine moves suddenly; person breaks arm trying to get out of the way. Medical assistance contacted.
10:50 a.m.	—	4	MSHA District Manager, State Inspector, United Mine Workers of America (UMWA), and Field Service Engineer contacted.
12:30 p.m.	—	6	Medical assistance arrives; person is transported to hospital.
			DAY 2
8:15 a.m.	—	6	MSHA District Manager contacts mine, informing that MSHA will conduct a mishap investigation.
12:00 noon	—	11	MSHA District Accident Investigator, MSHA Technical Support, State Inspector, UMWA, and Field Service Engineer arrive at the mine and begin working.
2:15 p.m.	—	11	The process of duplicating the original problem of unexpected machine movement begins once proper safety precautions are in place and test equipment is connected.
6:00 p.m.	—	11	The problem is duplicated, and the pendant controller is identified as working improperly.
6:15 p.m.	—	13	MSHA takes pendant controller to laboratory for analysis.
			DAY 3
9:30 a.m.	—	13	During analysis, MSHA finds an open electrical connection in the remote-control pendant. MSHA also determines that the software contains an error, since it was supposed to detect this condition. Manufacturer is contacted.
10:30 a.m.	—	15	The manufacturer's hardware and software engineers determine that there is a software bug. The original software is compared with the existing software used when the mishap occurred. A safety-critical portion of software is missing. The software to detect and prevent the machine from going to an unsafe state is missing.
12:00 noon	—	15	It is determined that the safety-critical portion of software was inadvertently omitted due to the rush to meet the customer's demands that the software be modified to add a new function by the next day.
3:15 p.m.	—	16	MSHA Inspectorate issues a citation to the mine operator.
5:00 p.m.	—	16	MSHA Technical Support initiates a Recall/Retrofit Program for these types of pendant controllers.
			DAY 4
5:30 a.m.	—	16	Begin to repair pendant hardware and write a new software patch.
6:00 a.m.	—	16	Fixes are tested and have resolved the problem.
7:00 a.m.	—	17	Meeting with mine management and all those directly involved takes place to explain the problem and the proposed fix.
8:30 a.m.	—	17	All parties satisfied with the proposed fix.
9:00 a.m.	—	17	The manufacturer begins loading pendant memory chips with the new software.
			DAY 5
8:30 a.m.	—	17	Service Engineer arrives with replacement memory chips for the pendant controllers and begins installation.

NM Near miss. LTI Lost-time injury.

limited to only the initial product design stage, but include the need for safety processes when the system is modified. In this example, the software was modified before the mishap. Software is as much a part of the system as the hardware. When software is modified, one must analyze if the modification will create a new hazard or worsen an existing one. Lastly, mishaps typically result from more than one cause. In this case, hardware, software, poor work practices, and poor management practices combine, causing a lost-time injury to a maintenance person.

This fictitious example is for informational purposes only. It is a composite of actual events and is not intended to identify particular people, manufacturers, or mine sites. *Time is compressed for illustrative purposes. In actuality, the scenario could span 2-3 months or more.*

Machine type: Remote-controlled continuous miner
Time line: 8:30 a.m. start, finish, elapsed time ' 5 days
Event code: Near miss (NM), lost-time injury (LTI)

Through a risk-based systems safety approach during all life cycle phases, the injury could have been avoided, as well as the time-consuming and costly activities that follow. Specifically, the causes and related safety life cycle steps to avert them are as follows:

Day 1, 8:30 a.m.: Unexpected machine movement is caused by a combination of an open circuit (hardware fault), an error introduced during the software modification (software error), and the lack of a management of change plan (safety management deficiency) for the software modification.

A management of change plan (see step 5 of the previous section) could have averted the introduction of the software error. This plan manages system changes so that changes are analyzed, reviewed, and well documented systematically and safely. The change analysis consists of a hazard and risk analysis (see step 2 of the previous section) to determine the safety effects on the system. The review process is *not* done by the person making the software change. This independent review increases the likelihood that error will not be overlooked. For example, one person may view a change as insignificant, but another could in fact determine that the change would create a significant risk. Documentation of previous safety-related decisions is also very important to prevent people from inadvertently undoing or omitting things during subsequent modifications.

Day 1, 10:45 a.m.: The maintenance person squats between the machine and rib to read the diagnostic display. For this particular situation, this is a poor work practice because the maintenance person is placing himself/herself in an area of potential danger. However, this person does not have any other options, so he/she is essentially forced to place himself/herself in this dangerous area in order to read the diagnostic display. Therefore, the root cause of this problem is actually an inadequate design of the diagnostic display. Step 2 of the previous section (conduct a hazard and risk analysis) could have identified this hazardous situation since the analysis is done for all phases in the system, including maintenance activities.

BENEFITS OF MINING SAFETY LIFE CYCLE APPROACH

Mining safety life cycle is a good engineering practice that results in improved safety, design, training, operation, and maintenance of a mining process. All participants (i.e., integrator, user, supplier, regulatory authority) benefit from a safety life cycle. We may expect to see for each group the following tangible benefits.

General mining industry:
- Improves worker safety
- Provides a uniform and systematic approach to safety management
- Improves mine safety
- Improves design and reliability to increase quality and throughput
- Facilitates communication among all parties

Mine operator:
- Improves worker safety
- Improves feedback channels to address safety issues and training requirements
- Reduces field modifications (improved safety specification, resulting in a better design)
- Higher uptime
- Reduces exposure of operators and maintenance workers to hazardous situations
- Enhances support from manufacturer

Equipment manufacturer:
- Reduces likelihood that hazardous designs continue in future designs
- Lowers support costs

• Problems identified quickly (provides better diagnosis)
• Product time to field reduced (facilitates approval process)
• Reduced product liability costs (safer design)
• R&D provided with qualitative and quantitative focus for new product development (reduced false starts and reduced development of unnecessary devices)
• New business opportunities presented due to safer designs
• Facilitates design changes early where costs are lower and changes are easier (figure 6)

MSHA:
• Provides invaluable information and documentation for approval and certification
• Provides invaluable information for investigations of fatalities, injuries, and near misses
• Gives essential techniques, methods, and insight required to address the emerging technology of PE

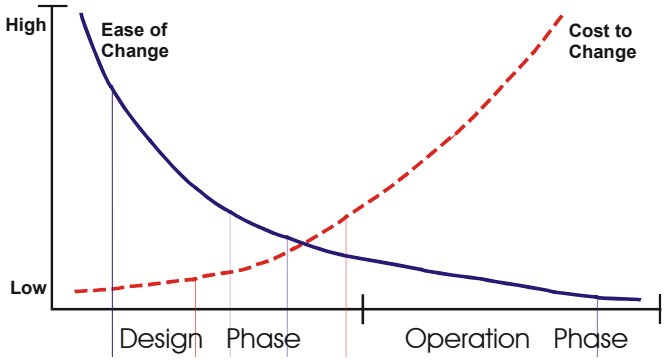


Figure 6.—The impact of change during development and operational phases.

Organized labor:
• Gives security and knowledge that the membership's safety is not compromised by new technologies.

GLOSSARY

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 interacts with a machine in order to operate the machine.

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 [Ministry of Defence 1998]. 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. The average probability of a system failing to respond to a demand in a specified time interval is referred to as "PFD avg."

Process hazard analysis team.—The group of operational, mining, instrument/electrical/control, and safety specialists responsible for the safety and integrity evaluation of the mining process from its inception through its implementation and transfer to mine operations to meet corporate safety guidelines.

Programmable electronics (PE).—Electrically or 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 programmable electronic system.

Programmable electronic system (PES).—Any system used to control, monitor, or protect machinery, equipment, or facility that has one or more programmable electronics (PE). This includes 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.

Programmable electronic mining system (figure 4).—A mining system using PE that responds to input signals from the equipment under control or from an operator and generates output signals, causing the equipment under control to operate in the desired manner.

Protection layer (figure 5).—Engineered safety features or protective systems or layers that typically involve design for safety in the equipment, administrative procedures, alarms, devices, and/or planned responses to protect against an imminent hazard. These responses may be either automated or initiated by human actions. Protection should be independent of other protection layers and should be user- and PHA-team approved.

Safety.—Freedom from unacceptable risks.

Safety availability.—Fraction of time that a safety system is able to perform its designated safety service when the process is operating (PFD ' 1 & safety availability).

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 systems. SILs are defined in terms of probability of failure on demand (PFD), where SIL 3 has the highest level of safety integrity (see table 4).

Safety life cycle.—Sequence of activities involved in the implementation of the safety instrumented systems from conception through decommissioning.

Table 4.—SIL values

SIL	Probability of failure on demand average range (PFD avg.)
1	$10^{\&1}$ to $10^{\&2}$
2	$10^{\&2}$ to $10^{\&3}$
3	$10^{\&3}$ to $10^{\&4}$

REFERENCES

ANSI/ISA [1996]. Application of safety instrumented systems for the process industries. Research Triangle Park, NC: American National Standards Institute, ANSI/ISA S84.01-1996.

Bennett P, ed. [1995]. Safety-related systems: guidance for engineers. London, U.K.: The Hazards Forum.

Dransite GD [1992]. Ghosting of electro-hydraulic longwall shield advance systems. Triadelphia, WV: U.S. Department of Labor, Mine Safety and Health Administration, Approval and Certification Electrical Safety Sentinel, #PC4814-0.

Fiscor S [1998]. U.S. longwall census. Coal Age *3*(2):22-27.

Francart WJ, Schultz MJ, Snyder MP [1997]. Results of 1995 survey: atmospheric monitoring systems in underground coal mines. In: Proceedings of the Sixth International Mine Ventilation Congress, pp. 73-75.

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.

IEC [1998]. Functional and operational safety of electrical/electronic/programmable electronic safety-related systems. Geneva, Switzerland: International Electrotechnical Commission, Draft IEC65108, Part 1 - General Requirements, version 4.

Leveson NG [1995]. Safeware: system safety and computers. Addison Wesley Publishing Co.

Lutz RR [1992]. Analyzing software requirements errors and safety critical, embedded systems. In: Proceedings of the Software Requirements Conference, pp. 99-106.

Ministry of Defence [1998]. HAZOP studies on systems containing programmable electronics. Glasgow, U.K.: Ministry of Defence, Directorate of Standardisation, Defence Standard 00-58, parts 1 and 2.

Phillips MM [1997]. Business of mining gets a lot less basic. Wall Street Journal, Mar 18; sect. B:1 (col. 1).

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

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

DHHS-(NIOSH) Publication No. 2001-132