

System Safety Applications in Mining

Gerald D. Dransite, Electrical Engineer; U.S. Department of Labor,
Mine Safety and Health Administration, Approval & Certification Center,
Electrical Safety Division; Triadelphia, West Virginia

Presented at the 18th International System Safety Conference, Forth Worth, Texas,
September 15, 2000

System Safety Applications in Mining

Gerald D. Dransite, Electrical Engineer; U.S. Department of Labor,
Mine Safety and Health Administration; Triadelphia, West Virginia

Keywords: mining, system safety, programmable electronics, MSHA, hazards,

Abstract

The mining industry experienced a growth in the use of more advanced programmable electronic systems in the late 1980's. The most complex applications were in the shearer initiated roof support advance systems utilized in longwall mining operations. A number of accidents and incidents occurred after the introduction of these systems which mining personnel perceived as a threat to their safety. The term "ghosting" was used to describe the perceived unpredictable nature of the incidents. In 1991 the Mine Safety and Health Administration (MSHA) investigated and analyzed the nature of the accidents that had occurred. The accidents were found to be due to a complex interaction of different factors: software, hardware failures, the environment, and the human interface. Recommendations were made to avoid future accidents in the specifically identified problem areas, but the same type of incidents continued to occur.

In 1995, MSHA requested assistance from the Pittsburgh Research Laboratory, The National Institute for Occupational Safety and Health (NIOSH), initially to help develop criteria for the evaluation of software for use in longwall mining machinery. NIOSH's initial work established that the evaluation of software in isolation would not lead to successful elimination of the types of accidents experienced. This led to expansion of the effort to include all types of mining machinery using programmable electronics and addressing functional safety from a risk-based system safety process encompassing software, hardware, the environment, and the human interface.

NIOSH researched various world standards addressing system safety in different industries and used this information to draft recommendation documents addressing the functional safety of processor controlled mining equipment applicable to the full life cycle of the equipment. MSHA is currently involved in a cooperative project with NIOSH to achieve voluntary adoption of the system safety recommendations by the mining industry.

MSHA does not intend to pursue a regulatory approach to system safety. A workgroup has been formed, made up of representatives from MSHA, NIOSH, and the mining industry, to develop a best practices guide to help implement the system safety recommendations.

Introduction

This paper chronicles the events and experiences of the Mine Safety and Health Administration in addressing the accidents and incidents resulting from the introduction of programmable electronics to the mining industry and which led to the development of risk-based system safety recommendations

Background

The mining industry has historically been slow in adopting new technology such as computer control and programmable electronics. Initially the application of programmable electronics was to automate simple machine control operations that were still under direct control of an operator such as a continuous mining machine, mine elevator or hoist, or conveyor system. There was also early use of centralized computers for mine-wide monitoring systems that monitored the mine atmosphere and detected fires on conveyor systems. In the late 1980's the mining industry experienced a growth in the use of more advanced programmable electronic systems in longwall mining operations.

The coal industry has experienced major productivity increases as the result of mechanization. According to the U.S. Energy Information Administration, coal industry productivity - the amount of coal produced per worker per hour in underground mines - more than doubled from 1986 to 1997, from 3.01 tons per man-hour to 6.04 tons per man-hour. Longwall mining is primarily responsible for this increase along with the introduction of programmable electronics which allowed automation of more complex mining functions and allowed integrating of mining system functions. Fewer workers were required and

their exposure to the traditional safety health hazards of moving cutter heads, noise, vibration and dust, was reduced. However, the workers were exposed to new potential hazards since the machinery was now under computer control and not under the direct control of an operator. The workers were now exposed to potential unexpected machine movements that were related to the programmable aspect of the machine and how it reacted to component failures. The introduction of computer control produced a heightened sense of anxiety in the workers since they felt a loss of control of the machine when unexpected movements would occur for no apparent reason. It was particularly troubling that these movements had the potential to produce serious injuries or even death.

Longwall Mining

Longwall mining is a highly automated method of mining where massive machines cut and

remove coal while self-advancing shields temporarily brace the mine roof. The roof is allowed to collapse behind the advancing shields, once the coal is removed, and the rock and dirt above drop to fill the void. A shearing machine moves back and forth across the coal face (figure 1) and cuts coal from a panel typically 1,000 feet wide and thousands of feet in length. The cut coal falls on to an automated face conveyor which carries the coal out of the mine. The shields, typically numbering 150-200, individually and sequentially lower, advance, set against the roof, and push the conveyor forward in synchronism with the face shearer as it cuts through the coal and moves forward. Originally these actions were under the direct manual control of operators. By the late 1980's, most longwalls were converted to automated systems under the control of programmable electronics.

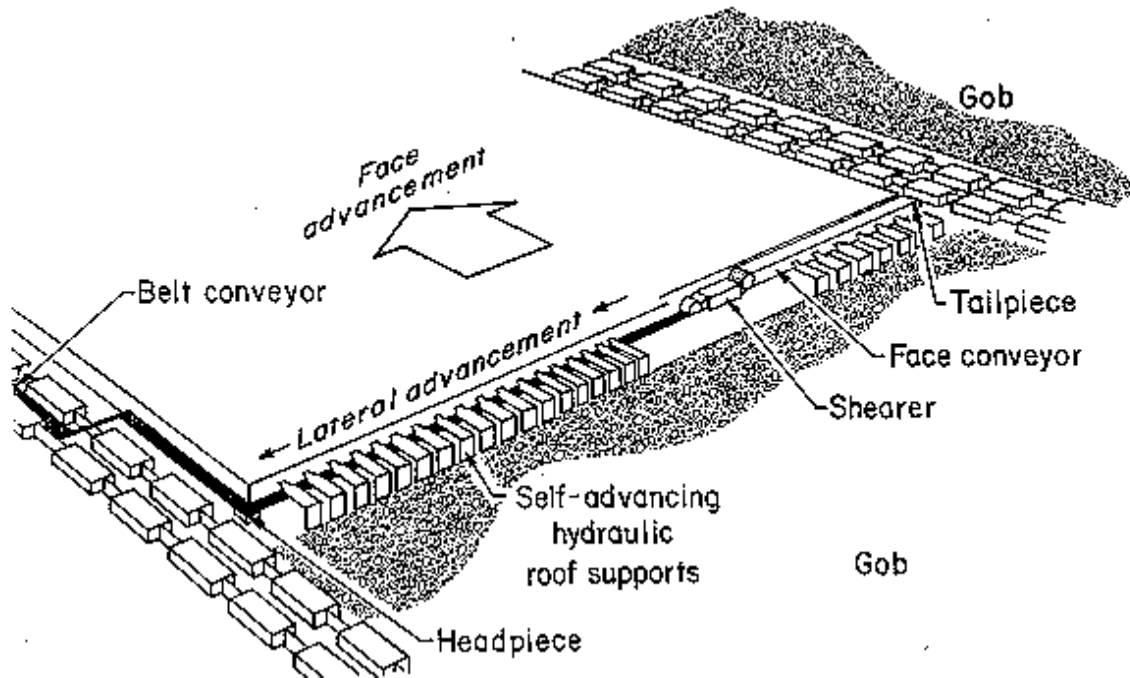


Figure 1-Basic Configuration of a Longwall Mining Face (ref. 1)

The most complex application of programmable electronics is called "Shearer Initiated Roof Support Advance" where the programmable controllers in each shield are electrically coupled to the face-shearing machine, which provides location information to the shields to allow their automatic advance in sequence with the shearing machine. Some systems use a central computer

for control and others use distributed control through a controller in each shield. For this application, the systems typically use custom designed programmable electronics rather than off-the-shelf programmable logic controllers.

Even though the system is semi-automated, workers still need to be present on the face to

operate the shearing machine and supervise the advancement of the shields. In essence they are working inside of a very large machine that is slowly advancing through the coal panel. Worker safety from the collapsing roof is provided by the canopies of the advancing shields, which provide a protected area for them

to move through as the shearer progresses (figure 2).

The primary physical hazards presented by the longwall system are due to the lowering of the shield canopies and the advancement of the shield against the face conveyor. These actions can produce crushing and pinning type injuries if

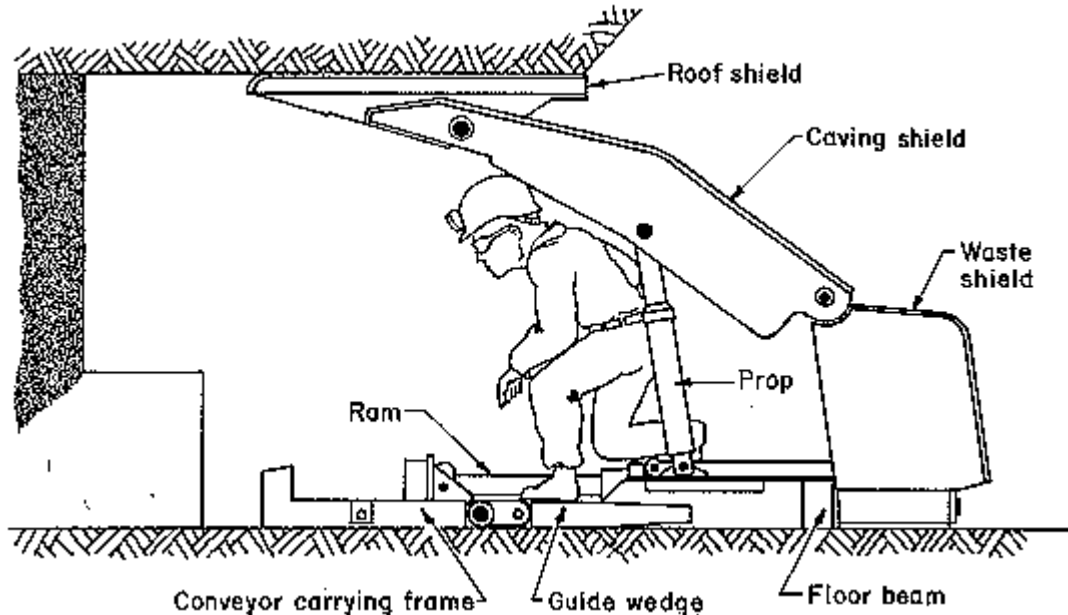


Figure 2-Longwall Roof Support Shield (ref. 1)

a worker is positioned on a shield when this action is occurring, particularly when the movement is not expected.

Concerns With Programmable Electronics

The Mine Safety and Health Administration (MSHA) became concerned with programmable electronics (PE) in 1990 as a result of a pinning accident due to an unplanned longwall shield advance. The cause of this accident was found to be due to moisture collecting on the keypad inside a shield control unit, which produced erratic signals that were interpreted by the PE Controller as valid command signals. The corrective action taken concentrated on maintaining the integrity of the enclosure sealing and changes to the software to improve its error detection capabilities.

There were other reports from equipment operators of unplanned movements and general safety concerns expressed with the use of PE in longwall applications. Because the movements were perceived as mysterious and random, the

term “ghosting” was used by the operators to describe the shield movements. In 1991 MSHA visited all operational longwalls controlled by programmable electronics and collected data on all “ghosting” incidents. The results of the study were as follows:

- 20 longwall installations out of 57 visited had experienced unplanned movement
- 30% of incidents were due to sticking or defective solenoid valves
- 10% of incidents were due to improper operation (operator error or poor training)
- 10% of incidents were due to programming problems
- 10% of incidents were due to moisture entry
- 40% of the incidents were corrected early start-up problems at new installations

Of the incidents due to programming problems, one incident was found due to the software not removing a manually entered program function command after an automatic override function command was initiated. The second incident involved the computer executing commands

entered before a hydraulic system failure that required shutting the system down and then restarting. MSHA published the results of the “ghosting” study in 1992 (ref. 2) and made recommendations focusing on improvements in the following areas:

- *Operator Training*
- *Timely Maintenance*
- *Maintaining Integrity of Enclosure Sealing*
- *Maintaining Alertness for Abnormal Operational Sequences Which Might be Indicative of a Software Programming Problem*

Accident Examples

There was a quiet period for a couple of years and then the “ghosting” incidents returned and intensified in 1994. A shield unexpectedly lowered and injured a face foreman at a longwall mine. There were also complaints from the same mine that shields were “ghosting” and creating a serious personnel safety hazard. The problems were found to be due primarily to failure of the mine operator to conduct timely maintenance. Additionally, operator training was inadequate for following proper operational procedures and sequences, and in providing guidance for recognizing improper system operation.

In the above mine example, 24 shields out of 186 had defective magnetic position transducers. These transducers signaled the controller that a shield had properly advanced. Without a proper advance signal from the transducer, the system was programmed to attempt four advance retries and then go into a “drop and drag” mode where the shield canopy was lowered and the shield dragged into position by the face conveyor advance. This advance attempt would occur even if a shield had properly advanced. With so many shields giving errant advance indications, the PE controller fell minutes behind in attempting the shield advances. Someone on or near a shield undergoing this delayed advance attempt would perceive the movement to be “ghosting.” Additionally, the movement could pose a physical injury threat to someone positioned on the shield. Further compounding the problems, the operators were inputting manual commands to advance the face conveyor when it was still under automatic control. This produced additional unplanned movement when the automatic conveyor advance was later executed.

In this example the system was functioning exactly as it was programmed, but the operators were not properly trained to understand how it was programmed and that manual commands were not to be inputted when the system was under automatic control. The feature in the programming that called for the advance retries served a useful purpose in dealing with adverse geological conditions but was not appropriate with the large number of position transducer failures present on the face. The actions taken to solve these problems concentrated on maintenance of the magnetic position transducers, operator training, and software changes that limited the number of advance retries to two.

A summary of some additional incidents and accidents that occurred through 1999 follows below:

- *Shield advances out of sequence in the automatic mode giving the appearance of “ghosting.” The problem was due to inadequate power supply current capacity.*
- *Foot injury received due to unexpected shield advance. Accident due to lack of maintenance and a lack of understanding of system programming.*
- *Foreman lost all toes of right foot when attempting to pass through the active shield advance area. Accident due to failure to follow proper procedure in pausing the automatic system for safe passage.*
- *Operator pinned by unexpected shield advance. Accident due to sticking hydraulic valve.*
- *System emergency stop function did not always work. The problem was due to a firmware change that pulse width modulated the drive signal to motor valves controlling the shields. The change allowed a 100 microsecond window where an emergency stop command would not be executed if the controller found the motor valve signal in an “off” state.*
- *Unplanned shield movement due to erroneous location information from the shearer controller to the shield advance system controller due to an intermittent hardware fault in the shearer. The movement occurred because of a programming change in the shield advance system controller that inadvertently deleted*

some code that rejected shearer location information outside reasonable parameters.

- *An operator received a serious crushing injury due to an unexpected drop of a shield canopy sprag plate. The accident was caused by a leaking electro-hydraulic valve that controlled the sprag.*
- *A shearer operator received a head and neck injury due to a lowering shield canopy. The cause was due to lack of maintenance on a defective position transducer that caused the shield to go into a programmed "drop and drag" mode under this condition.*

MSHA Forms Partnership with NIOSH

In light of the accident history and the fact that the same types of accidents were reoccurring despite the efforts to prevent them, MSHA concluded a new approach needed to be taken.

Since software was the new element that had been added to the mining systems and seemed to be at the heart of the problems, it was concluded that MSHA needed to develop criteria for the evaluation and acceptance of software and programmed operational sequences used by computerized mining equipment.

MSHA does not presently evaluate software or machine operational sequences for operational safety. MSHA's current regulations and approvals primarily address electrical permissibility in mines. The techniques of explosion-proof construction and intrinsic safety design are used to ensure that hazardous atmospheres containing mixtures of methane gas, coal dust, and air, are not ignited by electrical sparks or thermal sources.

Since MSHA had limited expertise in software evaluation, in 1995, help was requested from the Pittsburgh Research Laboratory, The National Institute for Occupational Safety and Health (NIOSH). The Pittsburgh Research Laboratory was formerly part of the United States Bureau of Mines, and has historically conducted research in mining technology. NIOSH initiated the Control Circuit Safety Analysis Project in late 1995 in response to MSHA's request for help on software evaluation.

NIOSH/MSHA System Safety Project

In early 1996, a safety panel was assembled, including experts representing NIOSH, MSHA,

industry, equipment manufacturers, and academia, to define the scope and objectives of the research project studying the safety of computer controlled mining equipment.

A major goal was to avoid generating controversial guidelines or standards without the input and support of all parties concerned and impacted by the effort. A quality and effective product was wanted that could be reasonably implemented in the real world.

Representatives of academia conducted some early work on the project in surveying and analyzing mining equipment and processes (ref. 3). Problems were identified in software, training, human factors, documentation, hardware, and equipment compatibility. This was supported by MSHA's accident studies, which showed accidents involving software, hardware, the environment, and the human interface. In some of these accidents there was a complex interaction of these factors.

It became clear that the project needed to be widened to consider machine safety from the system point of view; that the software aspects of machine design could not be addressed in isolation as MSHA originally envisioned. It also became clear that the effort needed to go beyond failure analysis since serious accidents had occurred while system components, including software, were functioning exactly as designed.

The project was expanded to include the development of guidelines for system safety applicable to all types of mining machinery utilizing programmable electronics. Previous accident examples have centered on longwall applications, but fatalities have occurred with other types of mining machinery using programmable electronics. Some examples include radio remote control machinery, hoists, and blade mill machinery used at a sand and gravel wash plant.

The Development of System Safety Guidelines

NIOSH researched domestic and foreign standards and guidelines for safety-critical software and systems and found nothing specific to mining (ref. 4). However, approximately 200 computer related safety standards and guidelines were found for other industries addressing the design, analysis, installation, and maintenance of processor-based systems. NIOSH found about

35% of these pertinent for mining applications, and ultimately focused their efforts on 16 documents covering system safety and the system's life cycle.

The goal was not to adopt a specific standard for the mining industry recommendations, but to use the basic principles of the other standards, scaled down in size and complexity for use by the mining industry. Many of the standards were generated by the military and aerospace industries for very large and complex systems containing more than one million lines of software code. Mining systems typically contain less than 70,000 lines of software code.

Although the NIOSH/MSHA System Safety Recommendations have been tailored for the mining industry, they are based on the basic principles of other industry standards and do not conflict with them.

The key standards that shaped the mining safety recommendations were:

IEC 61508 Parts 1-7, Functional Safety: Safety Related systems (ref. 5)

MIL-STD-882C, System Safety Program Requirements (ref. 6)

UL 1998, Software in Programmable Components (ref. 7)

Underwriters Laboratories, Inc. participated in reviewing and providing input on the final recommendation documents.

The System Safety Framework

The recommendations were organized to form a risk-based safety framework for addressing the

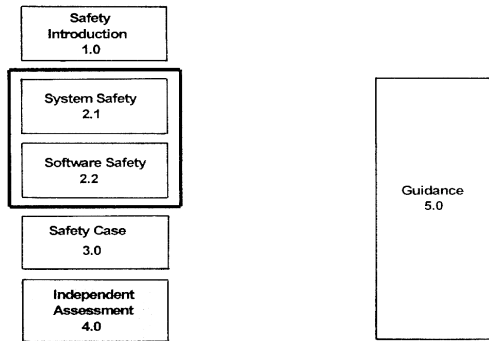


Figure 3-Safety Framework Documents (ref. 8)

functional safety of programmable electronics for mining (figure 3).

The safety framework's set of recommendation documents addresses a system safety process that considers the interfaces and interaction between the hardware, software, humans, and the operating environment for the equipment's life cycle. The tools of risk assessment and hazard analysis are used to increase safety. The system's life cycle (Figure 4) includes the stages of design, certification, commissioning, operation, and maintenance.

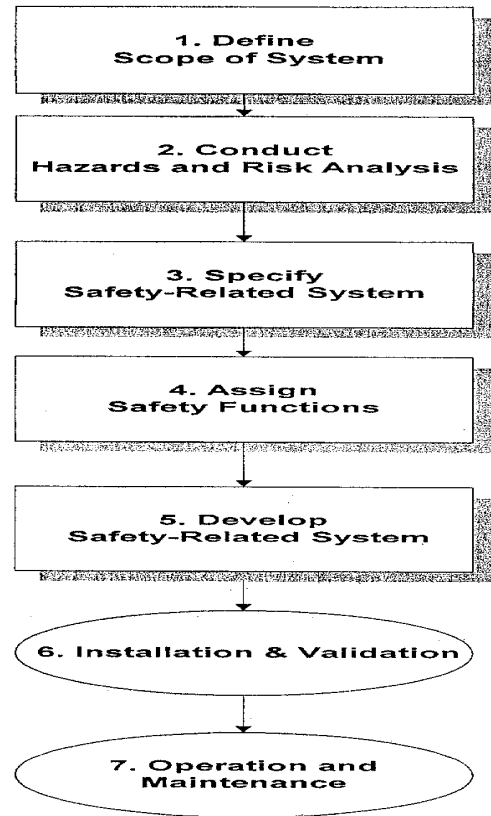


Figure 4-Mining Safety Life Cycle (ref.9)

The first document, *Safety Introduction 1.0*, (ref. 9) was completed and released to the industry at the Joint NIOSH-MSHA Workshop, Programmable Electronic Mining Systems: "An Introduction to Safety", held in August of 1999. This introductory document for the general mining industry provides the basic system and software safety concepts for the functional safety of programmable electronics. The workshop passed on the fundamental system safety concepts to the mining industry and informed

them of the additional pending recommendation documents. The workshop also provided an opportunity to solicit and receive industry feedback regarding the system safety concepts.

Since voluntary industry adoption of the system safety recommendations was sought, it was felt important that industry have input and a role in influencing the final form of the documents. For that reason, an industry workgroup was formed to comment on the recommendation documents. In addition, the workgroup was assigned the task of assisting in the drafting of the *Guidance 5.0* documents (Figure 4). The purpose of these companion documents is to assist users in applying the concepts presented in the Recommendation Documents 2.1, 2.2, 3.0, and 4.0. These guidance documents reinforce the concepts, give description of various methodologies that can be used, and provide examples and references.

The *System Safety 2.1* (ref. 10) and *Software Safety 2.2* (ref. 11) Documents have been drafted and circulated to the industry workgroup for comments. The scope of these documents is "surface and underground safety-related mining systems employing programmable electronics." The goal of these documents is to provide a uniform, systematic approach to identifying hazards, analyzing the risks, and reducing hazards over the entire system lifecycle. The effort starts at the system level and flows down to the subsystems and components. Software is considered a subsystem and is, therefore, a part of the system's safety.

Early year 2000 industry workgroup goals include the finalization of the *System Safety 2.1* and *Software Safety 2.2* Documents, and their companion *Guidance* Documents.

Implementing the System Safety Plan

Forming the industry workgroup was felt to be an important first step on the long road to voluntary industry adoption of the system safety plan recommendations. It was hoped that any initial resistance to the concepts would be reduced and their support gained through understanding of the system safety plan recommendations and potential benefits, and through participation in determining their final form.

The industry workgroup is made up of representatives from mine operators, equipment designers and manufacturers, software writers, state mining enforcement, NIOSH, and MSHA. Although the workgroup, in general, supported the system safety concepts, some concerns were expressed. Some of the larger companies already had some experience with system safety concepts through selling their equipment in foreign countries where a risk assessment and hazard analysis were required. For these companies, adoption of the system safety recommendations was seen as an extension of their efforts to comply with the more comprehensive safety requirements of the world marketplace. However, for the smaller companies designing equipment for the domestic mining industry, the system safety recommendations were seen as a greater burden. The lack of skilled human resources to administer the program and the additional costs were seen as obstacles.

Another hurdle to be overcome is the need for mine operators to make quick changes to equipment and software to accommodate production demands. The system safety plan's Management of Change controls were seen as a potential time delaying obstacle.

Scaling the system safety efforts according to the size and resources of a company will be important for their successful implementation. Phasing in some of the system safety plan recommendations for existing products is seen as a good way for companies to get started in applying the concepts.

First time implementation of the system safety plan recommendations to a new product for the full life cycle of the product will likely add additional cost to the product. However, each succeeding application of the system safety recommendations is expected to see improved benefit/cost ratios. The expected benefits (ref. 1) are in the areas of:

- Improved mine and worker safety
- Fewer equipment and software changes in the field
- Increased equipment reliability and availability
- Reduced design and support costs since safety is designed in from the beginning
- Market advantages, both domestic and international

- Easier and safer integration of multiple mining systems due to a common, systematic approach to safety
- Providing valuable information to assist MSHA in accident investigations

Remaining Work

The two pieces of the system safety framework that need to be completed are the *Safety Case 3.0* and the *Independent Assessment 4.0* Documents.

The *Safety Case 3.0* Document (ref. 9) will define the documentation necessary to demonstrate the degree of safety achieved, provide supporting evidence, and identify limitations for the system and its operation. It is the “proof of safety” that the system and its operation meet the appropriate level of safety for the intended application.

Along with this document, a companion document will demonstrate a case study on an actual mining machine. This will be very helpful in demonstrating the application of the system safety recommendations and provide a teaching tool for the industry. Periodic training seminars are planned to help the mining industry make the transition to the system safety approach.

The final document of the system safety framework to be completed is the *Independent Assessment 4.0* (ref. 9). This document will address the procedures and content for the independent assessment of the Safety Case. It will establish consistent methods for a third party determination of the completeness and suitability of the safety evidence and justifications.

References

1. Joint NIOSH - MSHA Workshop. Programmable Electronic Mining Systems: An Introduction to Safety. Handouts and Background Information, August 17, 1999.
2. Dransite, G. D. Ghosting of Electro-Hydraulic Longwall Shield Advance Systems. Eleventh WVU International Mining Electrotechnology Conference, July 29-30, 1992.
3. Sammarco, J. J., Kohler, J. L., Novak, T., Morley, L. A. Safety Issues and the Use of Software-Controlled Equipment in the Mining Industry. IEEE Industry Applications Society 32nd Annual Meeting, October 5-9, 1997.

4. Sammarco, J. J. Software Safety Guidelines for the Mining Industry. Proceedings 4th International Symposium on Mine Mechanisation and Automation, Brisbane, Australia, July 6-9, 1997.

5. International Electrotechnical Commission. Functional Safety: Safety-Related Systems, Draft IEC61508, Parts 1-7, Version 4, May 12, 1998.

6. United States Military Standard. System Safety Program Requirements, MIL-STD-882C, 1993.

7. Underwriter Laboratories. Software in Programmable Components, UL 1998, ISBN 0-7629-0321-X. May 1998.

8. NIOSH Technology News, No. 477. A Systems Safety Approach for Programmable Electronics. August 1999.

9. Sammarco, J. J., Welsh, J. H., Pazuchanics, M. J., Fisher, T. J. Programmable Electronics in Mining: An Introduction to Safety. NIOSH Special Workshop Publication, 1999.

10. NIOSH/MSHA Draft Document 2.1. System Safety Recommendations for Programmable Electronic Mining Systems. November 15, 1999.

11. NIOSH/MSHA Draft Document 2.2. Software Safety Recommendations for Programmable Electronic Mining Systems.

Biography

Gerald D. Dransite, Electrical Engineer, U.S. Department of Labor, Mine Safety and Health Administration, Approval & Certification Center, Box 251, Triadelphia, WV 26059, USA, telephone – (304) 547-2022, facsimile – (304) 547-2044, e-mail – dransite-gerald@msha.gov.

Mr. Dransite received his B. S. E. E. Degree from Carnegie Mellon University in 1967 and has been employed as an electrical engineer in the Electrical Safety Division at the MSHA Approval and Certification Center since 1983. He has authored the paper “Ghosting of Electro-Hydraulic Longwall Shield Advance Systems” and made various presentations on “The Prevention of Radio Remote Control Mining Accidents.”