Addressing the Safety of Programmable Electronic Mining Systems: Lessons Learned

John J. Sammarco, P.E.

National Institute for Occupational Safety and Health
Cochran Mill Road, PO Box 18070
Pittsburgh, PA 15236

Abstract—**The functional safety of programmable electronic (PE) mining systems is an international issue and concern. From 1995 to 2001, 11 PE-related mining incidents in the U.S. were reported by the Mine Safety and Health Administration (MSHA); 71 PE-related mining incidents were reported in Australia. MSHA does not have regulations for formal evaluations of the functional safety of PE mining systems. Hence, the National Institute for Occupational Safety and Health (NIOSH), in partnership with MSHA and the industry, generated the NIOSH safety framework for functional safety of PE mining systems. An overview of the NIOSH framework is given; the key framework elements, the safety life cycle and safety integrity levels are detailed. The safety framework approach has impacted the national and Australian mining industries by enabling the industries to advance from an ad-hoc approach to a formalized and systematic functional safety process. In retrospect, valuable lessons were learned for addressing functional safety and for changing industry perspectives and practices. These lessons continue to benefit mining and are applicable to other industries as well.**

Keywords—Normal Accident Theory; mining safety; system complexity; programmable electronics

I. INTRODUCTION

Many industries are increasingly depending on programmable electronic systems (PES) in safety-critical applications; the mining industry is an active part of this rapidly growing trend. The mining industry is utilizing PE technology to improve safety and health, to increase productivity, and improve competitive positions. When it comes to PE technology, (i.e., software, programmable logic controllers (PLC's) and microprocessors), there are unique technical and managerial challenges for system design, verification, operation, maintenance, and assurance of functional safety. PE technology has unique failure modes different from mechanical or hardwired electronic systems traditionally used in mining. Secondly, PE also adds a level of complexity that, if not properly addressed, can adversely affect worker safety.

This paper presents a process to address the functional safety of PE-based mining systems. The need to address this was driven by MSHA's concerns and the supporting mishap data as described in the following two sections. Next, an overview of the NIOSH safety framework to address PE functional safety is given and followed by a section describing the framework's key concepts and elements. Lessons learned are presented that continue to benefit mining and that could be beneficial to other industries as well. The ensuing section describes the work's impact nationally and internationally. Lastly, future directions are discussed.

II. PURPOSE AND SIGNIFICANCE

The Pittsburgh Research Laboratory of NIOSH has a pro-active project to generate best practice recommendations addressing the functional safety of PE-based mining systems. The objective is to generate a mining industry specific, comprehensive and systematic safety framework incorporating best practices and the latest international thinking for PES functional safety.

Realization of this objective addresses two safety issues for the mining industry. First, the mining industry, on a national or international basis, does not have a formalized, systematic functional safety process for PE-based systems as done by other industries addressing PES functional safety. Therefore, best practices are not uniformly utilized. Secondly, MSHA does have regulations to formally address electrical permissibility in mines; they have a wealth of knowledge, expertise and experience in this area. MSHA does not have formal regulations pertaining to PES functional safety. Even though they have made progress in reducing fatalities and serious injuries involving PE-based mining systems, they realize a mining specific, formalized functional safety process is needed to reach their ambitious safety goals.

III. MISHAP DATA

MSHA's concerns with the functional safety of PE-based mining systems began in 1990 with an unplanned longwall shield pinning mishap [1]. Since then, functional safety has grown to become a major issue and concern internationally [2]. From 1995 to 2001, there were 11 PE-related mining incidents in the United States; four of these were fatalities [3]. Most likely, the total numbers of incidents are under-reported in the U.S. because near misses are not reported and accidents are not required to be reported if they don't involve worker lost-time.

0-7803-7420-7/02/$17.00 © 2002 IEEE

Australia reports all mining incidents; from 1995 to 2001 there were 71 incidents documented for underground coal mines in New South Wales (NSW) [4]. In both countries, the majority of mishaps involved unexpected movements or startups of PE-based mining systems. Next, a historical account of PE functional safety issues and approaches are given.

In 1991, MSHA conducted a study of all longwall installations and found 35% had experienced unexpected movements; they analyzed the data and categorized it as sticking or defective solenoid valves, programming problems (software), water ingress, operator error or poor training, and other miscellaneous problems [1]. Fig. 1 depicts a comparison of factors contributing to PE-based mishaps occurring in the U.S. and in NSW [4]; solenoid valve problems are the leading factor contributing to PE-based mishaps. This does not appear to be unique to mining; process industry data also identifies solenoid valves as a leading cause of failure [5].

MSHA's original response to the longwall mishaps recommended improvements in "operator training, timely maintenance, maintaining integrity of enclosure sealing, maintaining alertness for abnormal operational sequences which might be indicative of a software problem" [1]. These recommendations focused on post-design "fixes." This approach had some success but MSHA realized the approach's limitations for complex PE mining systems and they realized the approach would not enable them to meet their ambitious goals for reducing the mishap rate to as near zero as possible. In 1995, MSHA turned to NIOSH researchers for a new approach. NIOSH proposed a safety framework largely based on the IEC 61508 safety lifecycle. Dransite chronicles these events, and describes some PE mishaps as given in the following excerpt [6].

> "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."

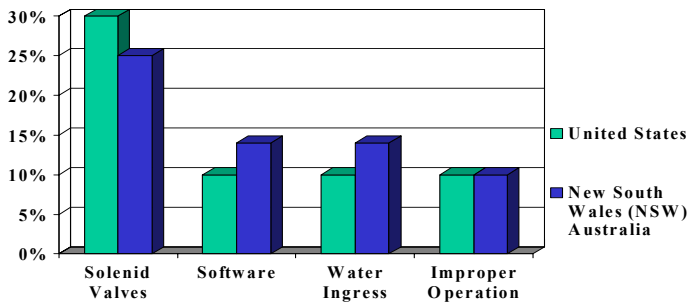

Fig. 1. A comparison of factors contributing to PE-based mishaps in the U.S. and NSW, Australia.

IV. THE NIOSH SAFETY FRAMEWORK

The NIOSH safety framework is a practical treatment scaled in size and complexity to the mining industry [7]. It draws 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.

The safety framework is for use by mining companies, original equipment manufacturers, and aftermarket suppliers. It addresses the various life cycle stages of inception, design, functional safety assessment, commissioning, operation, maintenance, and decommissioning. The framework's nine parts, depicted by Fig. 2, are as follows:

Introduction [8] — This introduces basic system and software safety concepts, discusses the need to address the functional safety of PE, and includes the benefits of a system/software safety program. It also establishes a common knowledge base by defining key terms and concepts.

System Safety [9] — The concepts of safety life cycle and safety integrity level (SIL) are detailed. This is the core document of the safety framework.

Software Safety [10] — This document builds on system safety concepts and provides specific recommendations for the software subsystem.

Safety File [11] — This presents a systematic, complete, and consistent "proof of safety" that the system meets the appropriate levels of safety for the intended application. It starts early and continues throughout the system's life cycle.

Functional Safety Assessment [12] — This document establishes methods to determine the completeness and suitability of safety file evidence and justification. Various levels of independent assessment are established based on the level of safety.

Guidance — Four guidance documents help users apply the safety framework concepts and recommendations. The guidance information reinforces concepts, describes various methodologies, and gives examples and references. The documents provide information and references so that the user can more intelligently choose and implement the appropriate methodologies given the user's application and capabilities.

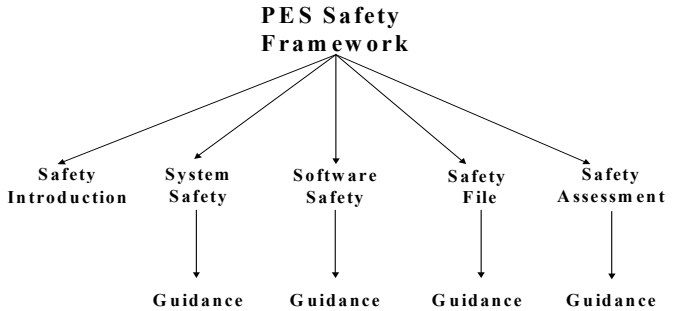

Fig. 2. The NIOSH safety framework

A. Safety Framework Key Elements

The safety framework's key elements and concepts are summarized. The two most fundamental concepts, as with IEC 61508, are the safety life cycle and SIL's. More details are provided for these concepts followed by a brief summary of other key elements.

1) Safety Life Cycle: 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" earlier 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 because hazards can become evident at later stages, or new hazards can be introduced by system modifications. The safety life cycle for mining, Fig. 3, depicts an adaptation of the IEC safety life cycle [13].

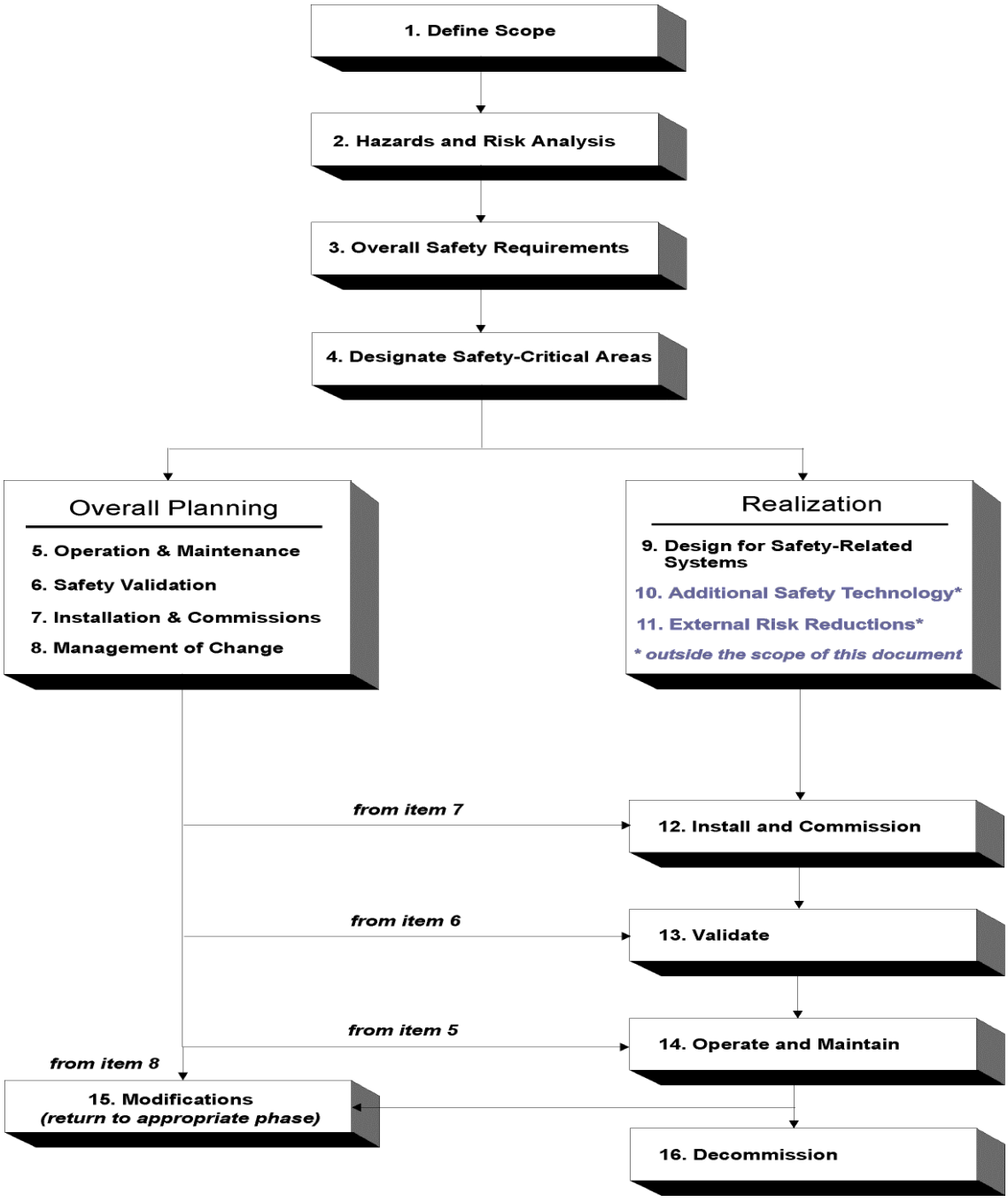

Fig. 3. The safety life cycle. *Adapted from IEC 61508*

Safety life cycle activities include identifying hazards, analyzing the risks, assigning SIL's, designing to eliminate or reduce hazards, verifying SIL's are attained, and documenting the plans, processes and products of the safety 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 [8].

2) Safety Integrity Levels: The concept of determining and verifying SIL's presented the most difficulty for the mining industry as evident from the many questions and discussions during and after our workshops in the United States and Australia. SIL is a term used to specify the probability that a safety function satisfactorily performs given a set of conditions and constraints. Qualitative or quantitative methods are used to determine a SIL for each safety function. Essentially, qualitative methods proportionally assign SIL's to ordinal measures of risk. Table 1 is an example of a calibrated risk matrix for determining a risk rank and associated SIL for each hazard. The matrix is based on hazard severity and frequency. The risk rankings range from one to four with four as the least desirable level of risk.

TABLE I. RISK RANK AND SIL MATRIX

	Catastrophic	**Critical**	**Marginal**	**Negligible**
Frequent	4, (SIL 3)	4, (SIL 3)	4, (SIL 3)	3, (SIL 2)
Probable	4, (SIL 3)	4, (SIL 3)	3, (SIL 2)	2, (SIL 1)
Occasional	4, (SIL 3)	3, (SIL 2)	2, (SIL 2)	2, (SIL 1)
Remote	3, (SIL 2)	2, (SIL 1)	2, (SIL 1)	1, -
Improbable	2, (SIL 2)	2, (SIL 1)	2, (SIL 1)	1, -

For mining, three SIL's are used. The SIL defines the degree or level of safety performance where SIL 3 requires the highest level of safety performance. Table 2 is used to determine the safety performance expressed as the average probability of failure on demand (PFD_{avg}), the risk reduction factor (RRF) and safety availability percentage.

TABLE II. QUANTITATIVE ASSIGNMENTS OF SAFETY PERFORMANCE FOR SIL'S FOR A LOW-DEMAND OPERATION.

SIL	**PFD_{avg}**	**RRF**	**% Availability**
1	10^{-1} to 10^{-2}	10 – 100	90.00 - 99.00
2	10^{-2} to 10^{-3}	100 - 1,000	99.00 - 99.90
3	10^{-3} to 10^{-4}	1,000 - 10,000	99.90 - 99.99

The PFD for a system is determined by abstracting the system to a sensor (S), a logic solver (L), and a final element (FE) and using equation 1 [14].

$$PFD_{sys} = PFD_S + PFD_L + PFD_{FE} \quad \text{where} \qquad (1)$$

PFD_{sys} = Average probability of failure on demand (PFD_{avg}) of a system's safety function;

PFD_S = PFD_{avg} of a safety function for the sensor element(s);

PFD_L = PFD_{avg} of a safety function for the logic solver(s);

PFD_{FE} = PFD_{avg} of a safety function for the final element(s).

The PFD_{avg} calculations depend on the architecture where 1oo1 denotes "1 out of 1" or a simplex system without redundancy and 2oo3 denotes a triple modular redundancy. Equation 2 is the calculation for a simplex system [15].

$$PFD_{avg1oo1} = 0.5 * (\lambda^{DU} * TI) \text{ where} \qquad (2)$$

$PFD_{avg1oo1}$ = Average probability of failure on demand of a safety function for a single channel architecture and assuming mean time to repair is insignificant;

λ^{DU} = Failure rate for dangerous undetected failure;

TI = Manual test interval or frequency.

For example, a simplified safety shutdown circuit consists of a stop switch, PLC, and hydraulic pump actuator connected in series. The pump shuts down when the switch is pressed thus placing the system to a safe state. The shutdown circuit is manually tested once a week or 168 hours.

The switch fails to a dangerous state 5% of all failures and the contactor fails dangerously 10% of the time. Neither component has diagnostics so the dangerous failures are undetected. The PFD_{avg} is calculated as follows:

$PFD_{avg\ plc} = 4.5 \times 10^{-3}$ (supplied by the manufacturer)

$\lambda_{switch} = \lambda_{contactor} = 5 \times 10^{-6}$ failures/hour

$\lambda^{DU}_{switch} = 5 \times 10^{-6} (.05) = 2.5 \times 10^{-8}$ (5% of failures are dangerous)

$\lambda^{DU}_{contactor} = 5 \times 10^{-6} (.10) = 5 \times 10^{-7}$(10% of failures are dangerous)

TI =168 hours

$$PFD_{sys} = PFD_{avg\ plc} + PFD_{avg\ switch} + PFD_{avg\ contactor} \qquad (3)$$
$$= 4.5 \times 10^{-3} + ((2.5 \times 10^{-8} + 5 \times 10^{-7}) / 2) \times 168$$
$$PFD_{sys} = 4.54 \times 10^{-3}$$

Using table 2 and the PFD_{sys}, the safety shutdown circuit meets a SIL of 2.

3) Other Key Elements: The following briefly describes other key elements and concepts:

- Safety is an emergent property of the entire system.
- Safety is not achieved in a discrete phase but in a continuous set of life cycle phases from system concept to decommissioning. Using a safety life-cycle enables safety to be addressed systematically and early.
- Multiple hazard analyses are needed throughout the product's development because each technique has particular strengths, weaknesses, and purpose.
- Management of change (MOC) is needed throughout the development and operation of the system and pertains to both hardware and software. Modifications of safety-critical software can and has introduced new, unforeseen hazards.
- The independent assessment of safety should be carried out incrementally. Conducting preliminary assessments during development and design enables deficiencies and inadequacies to be detected earlier rather than waiting until the entire system is designed.

V. MINING INDUSTRY IMPACTS

The NIOSH safety framework formally and comprehensively addresses the functional safety of PE-based mining systems. This work takes the industry from an ad hoc approach initiated by the latest mishap to a proactive, systematic approach based on best practices tailored specifically for mining. This has, and continues to have, a national and international impact on other government agencies, equipment manufacturers, operators, and academia as evidenced by the following:

- MSHA's acceptance and support: They have adopted the framework documents for use on a voluntary basis and they have provided exemplary support and cooperation. For example, they co-hosted the U.S. workshop, maintained industry participation through an industry workgroup they organized, and were engaged in numerous discussions and reviews of the work.
- Built industry awareness and knowledge: MSHA and the general mining industry is now aware of safety issues driven by data and not perceptions. All parties involved with this work have also gained significant PES functional safety knowledge and expertise.
- International recognition and utilization:
  - Mineral Resources NSW publicly announced they support and will expect all new PE-based mining equipment to conform to the NIOSH safety framework.
  - Mineral Resources NSW and the Minerals Industry Safety and Health Centre in conjunction with the University of Queensland requested and consequently received workshops on the NIOSH safety framework.
  - The course "Mineral Industry Risk Analysis" at the University of Queensland is incorporating material from the NIOSH safety framework.
- Research spin-off: MSHA's Approval and Certification Center formed an internal "Risk Management Development Committee" for non-electronic systems. The NIOSH safety framework was an impetus to the committee's formation.

VI. LESSONS LEARNED

Lessons were learned after considerable expenditures of time and other resources. Many times lessons learned become evident in retrospect; many times the same lessons learned can be employed in future endeavors. Therefore, it's important to identify and document these lessons. Our major lessons learned are as follows:

- Involve the industry early and continuously: The diversity of industry experiences, knowledge, and expertise, proved to be an invaluable asset. This enabled us to address areas we were not cognitive of, and it helped us to realize and maintain a practical approach. Secondly, industry involvement helped improve our working relationships with MSHA and others in the industry.
- Identify and understand issues and perceptions: Early in the project, software safety was identified as the leading area to address. This perception was formed because people felt most uncomfortable with software and because they had limited knowledge and experience in this area [6]. Our data analysis showed that few mishaps were attributed to software errors.
- Establish key concepts, terminology and definitions early: This helped unify industry support and cooperation by establishing common and consistent understandings. It also reduced confusion and related anxieties.
- Decompose the problem: The safety framework was decomposed into nine parts, each associated with a major life cycle stage. This helped to sustain industry involvement and interest by breaking the problem into manageable parts. This also enabled us to work in parallel on multiple parts. Lastly, it enabled us to incrementally introduce new ideas and processes. Therefore, the industry's first steps were manageable and successful. The remaining parts were built upon these early successes.
- Separate the concerns: The safety framework's nine parts were assembled into two groups: 1) recommendation documents describing what needed to be done in terms of plans, processes and best practices; 2) guidance documents containing supplemental information and examples to assist users to determine how to best implement the recommendations. Separation of the "what" from "how" enabled us to maintain clarity and focus.
- Conduct industry workshops: An industry workshop on PE safety concepts and the NIOSH safety framework was held in the United States and Australia. The workshops helped create an awareness of safety issues, transfer fundamental knowledge concerning PE safety, and to obtain stakeholder feedback and input. Secondly, the workshops enabled NIOSH researchers to focus the guidance documents to address the most difficult and important areas identified by workshop participants.
- Use scenarios to convey some types of information: "There are lies, damn lies, and statistics."- Mark Twain. The

mining industry can be a cautious group with a "show me" attitude. We found that by adapting the scenario technique to a mining incident, we could quickly and effectively present a relatively large amount of information to a broad audience, and with a high level of acceptance.

Table 3 lists an abbreviated mine mishap scenario. It is a composite and adaptation of actual events and is not intended to identify particular people, manufacturers, or mine sites. Time is compressed for illustrative purposes. The scenario conveyed key points for PES functional safety. It also accommodated the perspectives of the manufacturer, union, mine operator, and MSHA.

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 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.

First, after a mishap occurs, people are placed in dangerous situations as they inspect, troubleshoot, move equipment, and make repairs. Secondly, the scenario demonstrated the large expenditure of resources to address a mishap. Next, it demonstrates that PES functional safety must be addressed for all life cycle stages, including software modifications. Software is as much a part of the system as the hardware. Before software modifications are made, they must be analyzed to determine they will create a new hazard or worsen an existing one. Lastly, mishaps typically result from more than one cause. In this scenario, hardware, software, poor work practices, and poor management practices combined to cause a lost-time injury to a maintenance person.

VII. FUTURE DIRECTIONS

MSHA studies of PE-based mining system mishaps have concluded that mishaps typically involve multiple factors including complex interactions of software, hardware, humans, and the application environment [6]. The mishaps from complex interactions are explained by Perrow's Normal Accident Theory (NAT) [15]. Perrow theorizes systems with the characteristics of interactive complexity and tight coupling are prone to system accidents. Interactively complex systems have the potential to generate many unexpected, nonlinear branching paths among subsystems. These interactions can be unexpected, incomprehensible, or unperceivable to system operators. Tightly coupled systems respond rapidly to these unplanned interactions such that operators do not have the time or ability to intervene properly.

It is expected that complex interactions will become more problematic as the complexity and sophistication of PE based mining systems escalate. Many functions once hardwired are now being implemented by PE. This creates a level of complexity requiring more resources and more expertise to assure and assess the safety of these complex PE based systems.

NIOSH has begun research to address system complexity. The research objective is to create a complexity assessment methodology to operationalize NAT for PE-based mining systems. The tasks to operationalize NAT include the conversion of theory to practice by establishing concrete, quantifiable system level complexity metrics. The methodology serves to help identify, evaluate, and reduce system complexities. Less complex systems are safer [15], have fewer systematic errors [16] and are easier to verify for safety.

REFERENCES

[1] Dransite GD [1992]. Ghosting of Electro-Hydraulic Longwall Shield Advance Systems. Published in proceedings of the 11th West Virginia University International Electro-technology Conference, Morgantown, WV, July 29-30, pp. 77-78.

[2] Sammarco JJ, Kohler JL, Novak T, and Morley LA [1997]. Safety Issues and the Use of Software-Controlled Equipment in the Mining Industry. Published in the proceedings of the IEEE Industry Applications Society 32nd Annual Meeting, New Orleans, LA.

[3] MSHA [2001]. Fatal Alert Bulletins, Fatalgrams* and Fatal Investigation Reports. Web page, [accessed May 2001]. Available at www.msha.gov/fatals/fab.htm.

[4] Waudby, JF [2001]. Underground Coal Mining Remote Control of Mining Equipment: Known Incidents of Unplanned Operation in New South Wales (NSW) Underground Coal Mines. unpublished

[5] Gruhn, P, and Cheddie HL [1998]. Safety Shutdown Systems: Design, Analysis and Justification. Instrument Society of America (ISA), Research Triangle Park, NC, p. 121.

[6] Dransite, GD [2000]. System Safety Applications in Mining. 18th International System Safety Conference, Sept.

[7] Sammarco, JJ [1999]. Safety Framework for Programmable Electronics in Mining. Mining Engineering, Society of Mining Engineers, 51(12):30-33.

[8] Sammarco JJ, Fisher TJ, Welsh, JH, and Pazuchanics MJ [2000]. Programmable Electronic Mining Systems: Best Practice Recommendations (In Nine Parts); Part 1: 1.0 Introduction, IC9456, NIOSH, Pittsburgh, PA, pp. 1-10.

[9] Sammarco JJ and Fisher TJ [2001]. Programmable Electronic Mining Systems: Best Practice Recommendations (In Nine Parts0; Part 2: 2.1 System Safety, IC9458, NIOSH, Pittsburgh, PA, pp. 1-34.

[10] Fries, EF, Fisher TJ, and Jobes CC [2001]. Programmable Electronic Mining Systems: Best Practice Recommendations (In Nine Parts); Part 3: 2.2 Software Safety, IC9460, NIOSH, Pittsburgh, PA, pp. 1-33.

[11] Mowrey GL, Fries EF, Fisher TJ, and Sammarco JJ [2002]. Programmable Electronic Mining Systems: Best Practice Recommendations (In Nine Parts); Part 4: 4.0 Safety File, IC9461, NIOSH, Pittsburgh, PA.

[12] Sammarco JJ, and Fries EF [2002]. Publication in progress: Programmable Electronic Mining Systems: Best Practice Recommendations (In Nine Parts); Part 5: 5.0 Independent Assessment.

[13] IEC [1997]. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems, Part 1: General Requirements. IEC 61508-1, International Electrotechnical Commission.

[14] IEC [1998]. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems, Part 6: Examples of Methods for the Determination of Safety Integrity Levels. 61508-6, International Electrotechnical Commission.

[15] Perrow C [1999]. Normal Accidents: Living with High-Risk Technologies. Princeton University Press, Princeton, NJ.

[16] Selby, RW and Basili VR [1991]. Analyzing Error-Prone System Structure. IEEE Transactions on Software Engineering 17(2)141-152.