Safety Issues and the Use of Software-Controlled Equipment in the Mining Industry

John J. Sammarco
National Institute for Occupational Safety and Health
Pittsburgh Research Center
Pittsburgh, PA 15236-0070 USA
Phone (412) 892-4207 Fax (412) 892-6764 E-Mail: zia4@cdc.gov WWW: http://www.usbm.gov

Dr. Jeffrey L. Kohler
The Pennsylvania State University
University Park, PA 16802 USA
Phone (814) 863-4491 Fax (814) 865-3248 E-Mail: jk9@psu.edu

Dr. Thomas Novak
University of Alabama
Tuscalossa, AL 35486 USA
Phone (205) 348-1680 Fax (205) 348-9455 E-Mail: tnovak@coe.eng.ua.edu

Dr. Lloyd A. Morley
University of Alabama
Tuscalossa, AL 35486 USA
Phone (205) 348-1677 Fax (205) 348-6579 E-Mail: lmorley@coe.eng.ua.edu

Abstract *- Equipment control functions that were once hardwired are being implemented with software and very large scale integrated (VLSI) devices. Often this transition has resulted in increased flexibility, improved quality, and decreased costs. At the same time, it has created new concerns and challenges concerning worker safety. The visible and well-defined ladder diagram for relay-logic has been replaced by programs in which the exact outcome for varied inputs can be more obscure. In the coal mining industry, efforts to automate longwall mining systems have resulted in semiautonomous machines operating within the same space as workers. This paper describes an effort initiated by the National Institute for Occupational Safety and Health (NIOSH) to identify the safety issues related to the use of processor-controlled equipment in mining. Specific findings in the areas of human factors, hardware, and software safety are presented in this paper, and a brief description of a plan to address identified weaknesses is given.*

I. INTRODUCTION

Computer-controlled equipment is increasingly employed in many industrial applications because of the many advantages brought by this technology to the workplace, including increased flexibility, reduced cost, and improved product quality. Computer control employs software and/or the "hard-coded" logic of some VLSI devices. In mining, this technology allows workers to avoid areas where occupational health and safety risks, such as respirable dust and hazardous noise levels, are greatest. It also allows equipment operation to be customized to specific work conditions, thereby improving both safety and productivity. Other applications in mining are more modest and consist simply of replacing certain functions such as overcurrent relaying with computer-based protection. Regardless of the specific application, there are valid concerns for worker safety, and there have been a few accidents and "near misses" to heighten these concerns.

Safety in the mining industry has improved dramatically over the years. Cooperation amongst industry, government, and organized labor has resulted in a training system to improve safety. Nonetheless, mining is an inherently dangerous endeavor that requires constant vigilance to maintain safe conditions. The integration of process-based technology into the industry can lead to many desirable benefits, but at the same time, it could create new and potentially fatal hazards. Overall, the industry's experience with this technology is small,

and as an emerging technology in the industry, no mining industry guidelines or standards, either within the United States or internationally, exist for its safe use. An increase in related accidents may occur if a better understanding of the safety issues is not attained. It is believed that formalized guidelines or standards need to be developed and made available to manufacturers and mine operators.

The Pittsburgh Research Center of the National Institute for Occupational Safety and Health has an active project, as a program element of mining safety research, to address this safety issue. The successful development, acceptance, and use of guidelines for system safety of processor-based mining equipment could have a significant impact on safety when used by mining equipment manufacturers and certification/approval groups.

The most complex application of computer-controlled equipment in mining is semiautomated longwall systems. Furthermore, Organiscak [1] concludes that the longwall industry is evolving toward more automation. Longwall mining in the United States generally consists of driving two to four parallel gate entries (tunnels) on both sides of a large block of coal. One set of gate entries is referred to as the headgate; the other is known as the tailgate. Figure 1 shows the basic layout for a longwall mining system with three entries for the headgate and three for the tailgate. The headgate and tailgate are connected by sets of entries at the extreme ends of the coal block. Coal is usually extracted bidirectionally by a shearing machine along the width of the block between the headgate and tailgate entries. The width of the block typically ranges from 700 to 1,000 ft, and the block's length frequently exceeds 10,000 ft. The equipment for a longwall system basically consists of the shearing machine, the coal haulage system, and the roof supports. The shearer mines coal laterally across the block as it propels itself along an armored face conveyor, which transports the newly cut coal to a belt conveyor at the headgate. The workers, shearer, and armored face conveyor are protected from the caving roof by self-advancing hydraulic roof supports along the entire width of the block. Figure 2 illustrates a shield-type roof support. This type of support consists of roof and floor beams, caving and waste shields, hydraulic props, and a hydraulic ram. Roof support is provided by wedging the shield between the roof and floor by means of the hydraulic props. Each shield is attached to the armored face conveyor via a hydraulic ram. After the shearer passes a given group of shields, the hydraulic rams are extended to push the armored conveyor up to the newly exposed coal face. The shields are subsequently advanced by lowering the roof beams and retracting the hydraulic rams. After the shields advance, the hydraulic props are reset to raise the roof beam and once again provide roof support. Automation of this shield advancement process is found in modern longwall systems [1]. One of the latest technologies developed is shearer-initiated support advancement. Sensors are used to detect shearer location. This data is used by a processor to advance the supports. Also, automatically controlling the cutting height of the shearer (autosteering) is progressing.

II. GENERAL INDUSTRY EXPERIENCE

Other industries have been confronted with the safety issues of new technologies now facing the mining industry. An interesting parallel has been presented by Leveson [2] about the safety of high-pressure steam engines and how this relates to the safety of computer software. Leveson states, "Risk induced by technological innovation existed long before computers; this is not the first time that humans have come up with an extremely useful new technology that is potentially dangerous. We can learn from the past before we repeat the mistakes...in particular, parallels exist between the early development of high-pressure steam engines and software engineering."

Mistakes and related lessons learned in many industries are documented by Newman [3]. He identified problems such as mistakes in the requirements definition, system design flaws, software implementation problems, and willful system misuse.

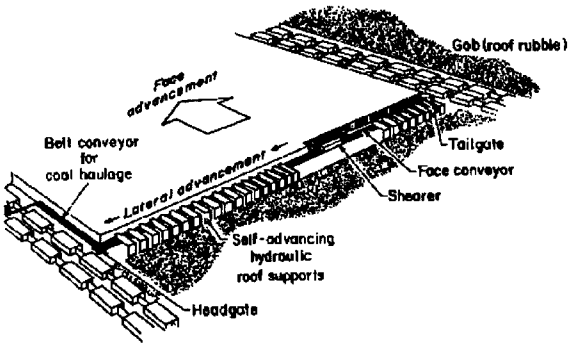

Figure 1. Basic components on a longwall face.

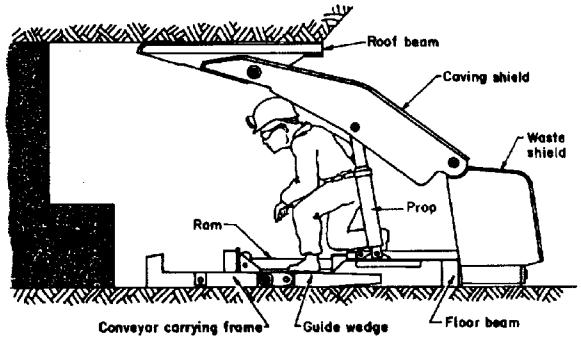

Figure 2. Shield-type roof support.

The industries identified by Newman include defense systems, civil aviation, rail transit, industrial control systems for chemical processes, industrial robots, and the medical field. An example in the medical field is the infamous Therac-25, a computer-based radiation therapy system. Six people accidentally received massive overdoses of radiation, three of which were fatal [4].

A large amount of information documents accidents in many industries involving safety-critical software systems. The mining industry will not be an exception unless preemptive actions are taken. This industry can capitalize on "lessons learned" and existing standards and guidelines. History has shown standards to be an effective tool in preventing accidents [2].

More recent lessons learned for computer control are presented by Lutz [5]. She states that most problems with safety-related software come from misunderstandings and discrepancies in the requirement specification. An IEEE standard exists that addresses software requirement specifications [6]. Many other specifications, guidelines, and handbooks address other aspects of system and software safety. Guidelines and standards have been established to address the development, analysis, installation, and maintenance of processor-based systems. This body of work can be quite helpful to establish guidelines specific to mining since they contain valuable knowledge and experience. They also establish a uniform approach.

An informal survey of approximately 200 computer-related safety standards was conducted by NIOSH. About 35% of these have been identified as useful to mining applications. For instance, some industry-specific standards and guidelines did not parallel the mining in terms of levels of risks, severity of outcomes, and system complexity; hence, they were not selected. Within this group, efforts have focused on the 16 documents shown in Table 1. These are internationally recognized and have gained general acceptance. These documents provide general information to establish processes and guidance relevant to many industries.

The military and aerospace industries are the major generators of standards and guidelines. These industries typically have complex and highly interconnected systems in safety-critical applications involving humans. Systems are so large that system safety involves many people and groups such as reliability engineering, quality assurance, system safety engineering, and software safety engineering.

Mining has much smaller organizations, where only a few people are responsible for processor control systems. These systems typically contain less than 70×10^3 lines of code (loc). A major challenge foreseen is addressing scalability in order to scale down guidelines and standards for the mining industry because many guidelines and standards were created for large, complex systems operating within very large organizations. Few standards address scalability. The U.S. standard MIL-STD-882C [7] is one example. It provides "examples of typically tailored system safety programs based on size or project risk."

III. IDENTIFICATION OF SAFETY ISSUES IN THE MINING INDUSTRY

A. Safety Panel

A safety panel composed of representatives from the mining industry, equipment manufacturers, an industry trade association, the Mine Safety and Health Administration, NIOSH, and academia was formed to discuss safety issues of processor-based mining equipment. The information and ideas that emerged from this panel's meetings were crucial in identifying both the safety hazards and benefits of the technology. Although the members of the panel identified many key issues, they did not have the resources to investigate them in more detail. Toward this end, extramural activity was established with The Pennsylvania State University and The University of Alabama [8].

B. Research Methodology

Initially, the university researchers examined the experience of the agricultural and manufacturing industries with software-controlled equipment, i.e., processor or computer controlled. Next, their work focused on the mining industry, including metal/nonmetal mines and plants, as well as coal mines. Finally, they focused on longwall mining systems, where most of the present concerns with processor-based control exist. Specifically, accidents have occurred and unplanned shield movements were reported.

The first step in their research was an exhaustive literature search to provide background understanding and to uncover other relevant research. This was followed with in-depth interviews of personnel from mining companies, equipment manufacturers, and government agencies. Typically these were conducted on-site. In many cases, more was learned by performing on-site technical analyses of the equipment while observing worker behaviors. Other fact-finding methods such as examination of maintenance records and accident reports provided a comprehensive picture of not only the present and future problems, but also possible solutions. The final step was to analyze the collected information and use it to define the salient present and future problems that must be addressed. Suggested solutions or future courses of action were also identified, although this was not the primary purpose of the project.

TABLE 1
STANDARDS AND GUIDELINES CONCERNING SYSTEM AND SOFTWARE SAFETY

System Safety Programs
* IEC 1508 Parts 1-7 (Draft), Functional Safety: Safety Related Systems.
* MIL-STD-882C, System Safety Program Requirements.

Software Safety Programs
* NASA NSS 1740.13, Software Safety Standard.
* Joint Software System Safety Committee (Draft), The Software System Safety Handbook.
* IEEE Std 1228, Standard for Software Safety Plans.

Software Requirements Specifications
* IEEE Std 830, Guide to Software Requirements and Specifications.

Software Design Practices
* UL 1998, Safety-Related Software.

Software Configuration Management
* IEEE Std 828, Standard for Software Configuration Management Plans.
* IEEE 1042, Guide to Software Configuration Management.

Software Quality Assurance
* IEEE Std 730, Standard for Software Quality Assurance Plans.
* ISO 9000-3, Quality management and quality assurance standards Part 3: Guidelines for the application of ISO 9001 to the development, supply and maintenance of software.
* CAN/CSA Q396.1.1, Quality Assurance Program in Critical Applications.

Software Documentation
* ANSI/ANS 10.3, Documentation of Computer Software

Software Verification and Validation
* IEEE Std 1012, Standard for Software Verification and Validation Plans.
* IEEE Std 1059, Guide for Software Verification and Validation Plans.

Software Maintenance
* IEEE Std 1219, Standard for Software Maintenance.

C. Research Findings

Potential safety problems and some possible solutions to these problems, were identified. They have been grouped into three categories for purposes of this discussion:

- Human factors
- Hardware
- Software

Each category is described in greater detail in the next section of this paper. The application focus of these comments is semiautomated longwall mining systems utilizing shearer-initiated shield movement. Nonetheless, many of the comments have broader application to other types of mining and even other industries.

Human Factors

The semiautomated longwall mining system is only the intermediate step toward the industry's goal of a fully automated system. Numerous technical obstacles have prevented this, and it is likely that the desired goal is years away. In the meantime, however, human workers must interact with semiautomated machines in a confined environment and must do so in a precise manner to avoid injury. In some cases, the movement of a shield can be unexpected by a worker, and if the worker is surprised by the movement, it may be difficult or impossible for the worker to deactivate the shield to prevent possible injury [9].

When a worker is confronted with an unexpected equipment behavior, the worker may be crushed or pinned, or may respond in a manner that will result in bodily injury. Although most shields have an emergency stop, it may be inaccessible to a worker in distress. A more prominently located deactivation mechanism could be helpful. However, such a location is likely to result in unintentional usage from accidental contact, and experience has shown that if safety devices become a "nuisance," they may be deactivated. Another method to alert miners to shield advancement is to use a warning horn or strobe prior to shield movement; this can be ineffective, however, because of the constant background noise that would

result as shields cycle over the length of the face. Perhaps the best solution would be to utilize a proximity detector that would prevent shield movement when the worker is within the shield's range of motion. However, the practical application of such devices is quite difficult in the rugged mining environment.

It is important to note from the foregoing discussion that the problem arises primarily because the automated equipment's movement was unexpected by the worker. This can occur because the worker is unfamiliar with the full range of equipment behaviors, or because a worker manually intervened in the automated cycle and unknowingly caused a change in the point where the automated cycle will restart. Advances in technological features will outstrip worker's ability to understand and utilize these features if a worker's training only consists of on-the-job exposure. Moreover, placing a worker within the operating envelope of semiautonomous equipment increases the potential for an accident. It is widely recognized that special hazards are created when improperly trained workers interact with robotic or automated equipment.

Extensive training has been given to mine workers and undoubtedly has accounted for much of the remarkable improvement in mine safety over the past few decades. Notwithstanding, the benefit of developing special training for workers who interact with semiautomated longwalls should be studied. Furthermore, due consideration should be given to requiring the mine worker to demonstrate basic understanding of the material prior to working with the equipment. The content of this understanding would be equipment specific.

There are virtually unlimited features that can be easily added to computer-controlled systems through simple programming enhancements. Flexibility for situations, both imagined and unimagined, can be incorporated into a product. The price for this flexibility can be complexity of operation. Some mine operators, for example, feel that the operation of the control system is too complex for the average mine worker, even if additional training is provided. Thus, it would seem that equipment manufacturers should seek ways to decrease complexity, and mine operators should scale back their requests for unlimited flexibility. Additionally, the use of *application aids*, such as laminated instruction cards, should be considered to facilitate safe operation of these complex systems.

"User friendly" documentation, whether application aids or complete operation and maintenance manuals, is crucial to the safe operation of such a complex system. However, it was found that some of these systems have been installed and operated before operating and maintenance manuals were even printed. Once provided, the level of documentation may be impressive in its detail, but lacking in its ability to help operators understand the operational nuances of the equipment.

Hardware

The reliability of the modern longwall mining system is remarkable, given the hundreds of thousands of components that need to function correctly and in concert and given the environment in which they function. The harsh environmental factors associated with mining, such as water and dirt intrusion, vibration, shock, and heat, have the potential to seriously impact control system reliability. The failures that occur involve electrical connectors and sensors, although failures of power supplies, solenoids, and electronic control units have also been reported. Improvements specific to this relatively small number of failure modes would have a positive impact on system reliability, and such refinements should be encouraged. However, there is a much more significant problem here. The types of failures that occur directly affect the performance of the control system, and a failed component can result in unexpected movement of the shields. This in turn represents a significant safety concern and points to the need for system-level safety analyses, as discussed later in this paper.

Another hardware issue that was uncovered relates to compatibility among the major subsystems. It is not uncommon for mine operators to purchase the shield control units from one manufacturer, the shields from another, and the longwall power equipment from a third manufacturer. The possibility of problems, including software errors, is increased in these "mix-and-match" systems. Although each manufacturer provides an interface specification to facilitate this process, proprietary concerns could result in the withholding of information. These systems are so complex that safety could be compromised to some extent in these hybrid systems. It would appear that compatibility requirements among equipment manufacturers might need to be improved to reduce the potential failures that adversely affect safety.

Software

A few hundred to a few thousand loc can be required to implement the processor-based functions of a longwall mining system. This is not a particularly large amount compared to many applications. Nonetheless, the routines are complicated with many branching paths. There is evidence that manufacturers are taking extraordinary steps to ensure the integrity of the software. Even so, there are two worrisome aspects to this.

First, it is not clear that the manufacturers are performing system-safety analyses, including fault-tree analysis, which could identify possible adverse actions that are based on foreseeable failures. The efficacy of system-level safety

analyses is well established in a variety of industrial and military applications and is needed for processor-based mining equipment.

The second worrisome practice is that system-level programming is often changed after the equipment is in service. Such changes may be requested and then implemented within less than one or two days; the concern is that this may create hazards or compromise other programmed safety features because there is insufficient time for thoughtful analysis. This change may be necessary to alter the system programming to correct an error or other problem that is detected after the system is in use. Code is sometimes changed to accommodate site-specific conditions that were not initially anticipated. Also, the mine operator may decide to make mining changes that are not readily attainable without altering the program, or in some cases, to operate around failed equipment. Regardless of the reasons, there is tremendous pressure on the manufacturer to perform the changes quickly to minimize lost production costs.

Allowable programming changes should be defined in the system safety analyses. Any changes involving safety-critical areas should precipitate new analyses to ensure that the proposed change will not compromise safety.

IV. RECOMMENDATIONS FOR FUTURE WORK

The previous section listed the major safety concerns that were identified during the course of the university researchers' project. Although each of the concerns could be addressed individually, taken in total, the real need is for an integrated system safety approach.

A. The System-Safety Approach

A classic treatise in this area [10] summarizes the approach as follows:

1. Develop an overall plan for system safety.
2. Conduct an analysis of the product or system in which hazards are identified.
3. Establish safety criteria such as checklists and references to standards and guidelines.
4. Determine the proper hazard control. The order of precedence is to eliminate and control hazards, provide alerts and warnings, and establish procedures.

The benefits of a systems approach are also put forward by Leveson [3], who outlines a system-safety plan and states that such a plan should be the first step in any safety-critical project. Plans for subsystems, such as software, should be included as part of the plan rather than separate entities. MIL-STD-882-C[7] and IEEE Std 830[11] are generally accepted and, respectively, would be beneficial for system safety plans and software safety plans. Next, system safety must be "linked" to software safety [12] such that, systematically the relationships between potential hazards and the associated software are identified.

B. Future Work

The need for this system-level approach has been identified for the mining equipment; furthermore, a need has been identified to complete such an analysis so that it can be used as a model within the industry. During fiscal year 1997, the project focus is to generate a System Safety Plan (SSP) as the first step toward this goal. This SSP will contain adaptations from documents such as IEC 1508 parts 1-7 (Draft) [13] and MIL-STD 882-C [7].

The draft standard IEC 1508 is generic and is intended to form a basis from which other industry-specific standards are to be built, thus enabling a common, international approach to safety. The standard, in seven parts, provides guidance on all aspects of system development, including hardware and software development methods, documentation, and testing methods and tools.

Subsequent tasks, which may extend into fiscal year 1998, include:

1. Generate a general checklist for the hazard analysis stage.
2. Define the methods and tools for a Preliminary Hazard Analysis (PHA).
3. Continue to gather information on accident investigations involving computer-controlled equipment.
4. Define a pilot program for a safety analysis of an existing mining system or subsystem. The intent is to facilitate generation of our guidelines and to provide a case study for implementation.
5. Meet with mining industry software and system engineers to discuss current and proposed methods and tools for system and software safety.
6. Explore cooperative agreements with other government and private organizations to expand our base of knowledge and to gain from their expertise and perspectives.

V. SUMMARY

Mining, as shown in numerous statistics, poses inherent risks and dangers to the health and safety of miners. New technologies, such as computerized control, offer the potential to improve health and safety. However, this technology adds a level of complexity that, if not properly applied, may adversely affect safety. The solution is to develop a systems approach to address the identified safety concerns. The mining

industry can capitalize on lessons learned in other industries using processor-control systems.

The Safety Panel was an effective means of melding the various perspectives of safety concerns, problems, and possible solutions. It became clear that all of the stakeholders in the process were committed to achieving the highest levels of safety possible. Each stakeholder was actively engaged in some effort to accomplish that goal. It also became clear, nevertheless, that an integrated systems approach will be required to ensure that the goal is met.

Establishing guidelines pertaining to system and software safety for mining or any other industry is not a trivial task [14]. However, successful completion, acceptance, and implementation of guidelines will help to ensure worker safety for processor-controlled mining equipment.

VI. REFERENCES

[1] J.J. Organiscak, C. Mark, R.A. Jankowski, and E.D. Thimons. "Health and safety implications of semiautonomous longwall operations," Longwall USA, 1996, pp. 1-13.

[2] N.G. Leveson. "High-pressure steam engines and computer software," International Conference on Software Engineering, Melbourne, Australia, May 1992.

[3] P.G. Newman, Computer related risks. Addison-Wesley Publishing 1995.

[4] N.G. Leveson, Safeware: System safety and computers. Addison-Wesley Publishing 1995.

[5] R.R. Lutz. "Analyzing software requirements errors and safety critical, embedded systems." Software Requirements Conference, 1992, pp. 99-106.

[6] IEEE STD 830. Recommended practice for software requirement specifications, 1993. The Institute of Electrical and Electronic Engineers.

[7] MIL-STD-882C. System safety program requirements, 1993. United States Military Standard.

[8] J.L. Kohler, T.Novak, L.A. Morley. "Identification and analysis of safety issues for processor-based control systems," 1996 Internal Report.

[9] G.D. Dransite. "Ghosting" of Electro-Hydraulic Longwall Shield Advance Systems. U.S. Department of Labor, Mine Safety and Health Administration, PC 4814-0, 1992.

[10] W. Hammer, Handbook of system and product safety. Prentice Hall 1972.

[11] IEEE Std 1228. Standard for Software Safety Plans, 1994. The Institute of Electrical and Electronic Engineers.

[12] J. Flynt, R. Davidson. "Developing the link between product safety standards and software," Annual RELIABILITY and MAINTAINABILITY Symposium, 1996, pp. 1-11.

[13] IEC 1508 parts 1-7 (Draft). Functional safety: safety-related systems. International Electrotechnical Commission.

[14] B.A. Wichmann, "Why is it difficult producing safety critical software?" Ingenuity, pp. 96-104, May 1995.