Technology News

No. 477

NIOSH

July 1999

A Systems Safety Approach for Programmable Electronics

Objective

To address the safety of programmable electronics-based mining systems before this technology proliferates in the mining industry.

Background

According to 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." For mining, programmable electronics (PE) is an emerging technology that enables new capabilities and flexibility. It also can create new hazards and/or worsen existing hazards. PE includes microprocessors, programmable logic controllers (PLCs), and software. Using mine accident data compiled for 1994-97 by the Mine Safety and Health Administration (MSHA), we have identified nine incidents involving PE. We anticipate that fatalities, incidents, and near misses will increase as the quantity and complexity of PE increases with the industry's desire to remain competitive.

PE is found on longwall mining systems; automated haulage vehicles for surface and underground metal/nonmetal mines; remote controllers for underground mining machines; mine elevators and hoists; and mine atmospheric monitoring systems that monitor methane, carbon monoxide, and fresh air flow. During 1992-95, underground coal mine atmospheric monitoring doubled to where nearly 17% of all mines have computer-based systems. From1990 to 1996, programmable longwall systems usage doubled to about 95% of all U.S. longwalls. Microprocessor technology is finding its way into control and monitoring of conveyor systems. Industry is trending toward more utilization and complexity as machinery moves from localized PE control to distributed PE control of machines and processes. This trend is expected to continue because of economic pressures, the need to mine lower grades of coal and ores, and increased difficulties in mining these resources.

Approach

The National Institute for Occupational Safety and Health (NIOSH) is taking a proactive position by generating functional safety recommendations for programmable electronics in mining. The recommendations take the form of a *safety framework* shaped by industry trends, MSHA accident data, and existing national and international standards. We are using a risk-based approach for the *entire system*, rather than just software or hardware. The approach makes safety a part of the early design, where changes are more effective and less disruptive, compared to implementing safety measures after many fatalities and injuries have occurred.

The Safety Framework

The safety framework is a set of recommendations addressing the *functional safety* of PE for mining. It is a systems safety process encompassing hardware, software, humans, and the operating environment for the equipment's life cycle. The safety framework's set of recommendation documents (figure 1) addresses the system's life cycle stages of design, certification, commissioning, operation, and maintenance.

To our knowledge, mining, on a national or international basis, does not have formalized standards addressing the safety of PE; thus, the safety framework is a first step. It is a practical treatment scaled in size and complexity to small mining organizations having just a few people with limited knowledge of functional safety. The framework components are:

- 1.0 *Safety Introduction*.—An introductory document for the general mining industry provides basic system and software safety concepts for the functional safety of PE. The document is supplemented by industry workshops to reinforce these fundamental concepts, create an awareness of the pending NIOSH safety recommendations, and provide a means for valuable industry feedback.

U.S. Department of Health and Human Services

Public Health Service
Centers for Disease Control and Prevention
National Institute for Occupational Safety and Health

CDC
CENTERS FOR DISEASE CONTROL AND PREVENTION

- 2.1 *System Safety Program Plan (SSPP)* and 2.2 *Software Safety Plan (SWSP)*.—These documents draw heavily from national and international standards. The scope is "surface and underground safety-related mining systems employing programmable electronics."
- 3.0 *Safety Case*.—This is a "proof of safety" that the system and its operation meet the appropriate level of safety for the intended application. The recommendations detail the documentation for demonstrating the degree of safety and the supporting evidence.
- 4.0 *Independent Assessment*.—The independent assessment of the Safety Case is addressed. It establishes consistent methods to determine the completeness and suitability of safety evidence and justifications.

Benefits

- Improves worker safety
- Improves mine safety
- Fewer field modifications
- Improves equipment availability
- Lowers design and support costs because safety is designed in early
- Improves national and international market advantages
- Establishes a common, systematic, industry-wide approach to safety

Opportunities

The framework for safety is a starting point for industry guidance documents or voluntary industry standards. Thus, the opportunity exists to form an industry work group to produce these documents. Additionally, a cooperative agreement opportunity exists for a pilot project to implement the safety framework with a mine equipment manufacturer.

Reference

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

For More Information

For additional information, contact John J. Sammarco, NIOSH Pittsburgh Research Laboratory, Cochrans Mill Rd., P.O. Box 18070, Pittsburgh, PA 15236-0070, phone: (412) 386-4507, fax: (412) 386-6764, e-mail: **zia4@cdc.gov**

To receive additional information about occupational safety and health problems, call 1-800-35-NIOSH (1-800-356-4674), or visit the NIOSH Web site at http://www.cdc.gov/

Mention of any company name or product does not constitute endorsement by the National Institute for Occupational Safety and Health.

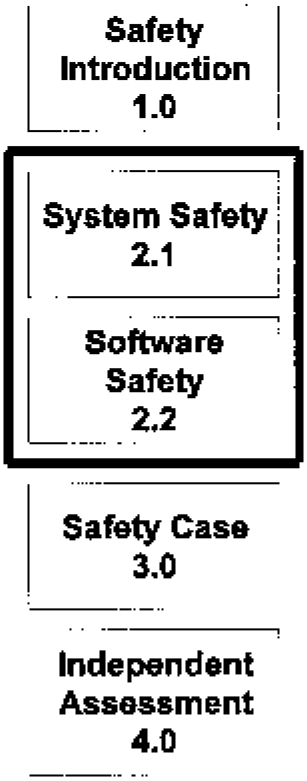

Figure 1.—The safety framework.