Date Wed, 16 Feb 2000 085952 -0700
From Meredith Brown racer@lanl.gov
Subject: Blue Alert- Microprocessor-Based Computers and Safety Barriers

Title: Blue Alert- Safety Hazards Associated with the Failure of Safety Barriers under the Control of Microprocessor-Based Computer Systems

Identifier 2000-ID-0001 Date 02/16/00

Summary- Safety hazards associated with the failure of safety barriers under the control of microprocessor-based computer systems need to be identified, analyzed, and mitigated before work is performed.

Discussion- Microprocessor-based control systems have become increasingly popular in the work place because of their versatility and functionality. As a result, microprocessors are being used to monitor and control safety barriers associated with fire protection systems, radiation interlock systems, and manufacturing equipment. These systems tend to be complex and subject to single-point and common-cause failures. Failures occur when the control system can not perform its intended function for any of a number of reasons such as microprocessor malfunction or failure, loss of electrical power, power surge, software logic error, design error, or installation error. Failures of microprocessor-based control systems have the potential to adversely impact the safety of workers, the public and the environment when the microprocessor is exclusively responsible for maintaining a safety barrier or safety system. Five examples of failures of microprocessor-based control systems responsible for safety barriers are listed below

1. Type A Accident Investigation Board Report of the July 28, 1998 Fatality and Multiple Injuries Resulting from Release of Carbon Dioxide at Building 648, Test Reactor Area Idaho National Engineering and Environmental Laboratory, September 1998; (http//www.tis.eh.doe.gov/oversight/acc_inv/acc_investigations.html)

2. Inadequate Interlock Fail Safe Capability of Radiation Source Control System at the RSB/RESL Calibration Facility, CF-638; Occurrence Report No. DOE-ID 90-1 (see Attachment 1);

3. Abnormality Identified in X-Ray Facility Fail Safe System; Occurrence Report No. ALO-AO-MHSM-PANTEX-1994-0003; (see Attachment 2);

4. Milling Incident Involving High Explosive; Occurrence Report No. ALO-AO-MHSM-PANTEX-1993-0064; (see Attachment 3);

5. An investigation of the Therac-25 Accidents by N. Leveson and C S. Turner, UCl Technical Report #92-109, November 1992. (http//www-personal.monash.edu.au/~mecheng/mec3409/softeng/therac25/therac25.html)

In the first example, a design defect in the microprocessor-based fire control system caused the unexpected discharge of a carbon dioxide fire suppression system without annunciation of the

evacuation warning alarm. Eight of the thirteen workers in the building were able to escape. The workers who had escaped and other facility personnel responding to the accident were able to rescue three of the remaining workers from the building. Fire department and ambulance personnel removed the last two workers. The accident resulted in one fatality and injuries to three other workers who required hospitalization. The second example describes the failure of a radiation source control and interlock system. The interlock system was rendered ineffective when the microprocessor-based control system was manually aborted by operating personnel. Additional design features and administrative controls (radiation area monitor, remote video camera, electronic alarming dosimeters, and portable survey meters) provided additional effective safety barriers that prevented any radiation exposure of workers when the interlock system failed. In the third example, a trainee identified an abnormality in a microprocessor-based X-ray facility fail-safe system that allowed the system to be bypassed. The failure was caused by a design defect in the computer software that operated the fail-safe program. In the fourth example, a computer-driven 3-axis mill did not stop at the intended pre-programmed position, and a flat end mill cutter penetrated about 0.75 inch into high explosive. There was no initiation of the high explosive. The possibility of the tool inadvertently moving into the explosive had not been considered in the job safety analysis, and adequate controls had not been incorporated into software programs to ensure that the equipment returned to a proper home start position. The fifth example documents a series of accidents involving a computerized radiation therapy machine that resulted in radiation over-exposure and death of several patients. In this instance, the microprocessor-based computer control system was in exclusive control of critical safety parameters and interlocks. The control system failed to perform its intended safety function because of multiple complex problems associated with the software programs. Fixing each of the individual software "bugs" as they were found did not solve the inherent safety problems associated with failures in the microprocessor-based control system. Additional information on these and other incidents is contained in the references.

In each of these cases, the microprocessor-based control system behaved in an unexpected or undesirable manner under circumstances that were not clearly foreseen at the time of design and installation. As a result, safety barriers under the control of the microprocessors were compromised, potentially placing workers and members of the public at serious risk. The potential safety hazards associated with failure of microprocessor-based control systems need to be recognized by management and safety professionals so that they can be identified, analyzed and mitigated. When warranted, additional design features or administrative controls should be considered to provide redundancy and defense in depth.

Analysis- The lesson for the DOE complex to learn from these incidents and accidents is that potential failure modes of microprocessor-based systems responsible for controlling safety barriers and safety systems need to be identified, analyzed, and mitigated as part of the work control process. When single-point and common cause failures are possible, additional design features or administrative actions may be warranted to control the hazard. These actions are consistent with the core functions of DOE Integrated Safety Management Systems to identify hazards and implement hazard controls (see DOE Policy 450.4). DOE issued a Safety Notice (Issue No. 99-01) in July 1999 to alert personnel at DOE facilities to vulnerabilities associated with microprocessor-based fire protection systems. The notice discusses potential problems and recommended that several actions be implemented as part of site fire protection programs. However, the potential hazards and lessons to be learned were not generalized in their

applicability to other safety disciplines where microprocessors are used to control safety barriers. Design features that may be used in conjunction with microprocessor-based control systems to control or mitigate potential failures include mechanical interlocks and hardware alarms. Redundant and independent microprocessors may be used in some high-consequence situations. Interlocks and alarms need to be designed to operate independently of the microprocessor-based control system, so that they provide redundancy and defense in depth. Interlocks and alarms help ensure that safety barriers remain in place or that immediate notification of barrier failure occurs, regardless of the functional condition of the microprocessor-based control system. Hardware alarms should be based on positive indication of actuation or barrier failure (e.g., switch actuation, solenoid position, gas pressure, detection of radiation, or fluid flow), rather than perceived status based on a software command. Interlocks and alarm functions should be designed in a fail-safe manner. Interlocks and alarms should be under a configuration control program. A comprehensive acceptance test program should be implemented for new installations or modification of existing systems. Additionally, interlocks and alarm functions should be routinely and systematically tested in accordance with detailed procedures as part of a preventive maintenance program.

With respect to the use of microprocessors in safety systems at nuclear facilities, the Nuclear Regulatory Commission has published Regulatory Guide 1.152, Criteria for Digital Computers in Safety Systems of Nuclear Power Plants. The regulatory guide describes a method acceptable to the NRC staff for complying with the Commission's regulations for promoting high functional reliability and design quality for the use of digital computers in safety systems of nuclear power plants. The term "computer" refers to a system that includes computer hardware, software, firmware, and interfaces. Significant emphasis is placed on defense-in-depth against the propagation of common-cause failures within and between functions.

Resolution- Managers and safety professionals should be aware of the potential hazards associated with the failure of microprocessor-based systems responsible for the control of safety barriers. Microprocessor-based systems responsible for the control of safety barriers may be found in numerous applications, including fire protection systems, radiation facility interlocks, x-ray machines, and automated machining and manufacturing equipment. Corporate hazard identification processes and procedures need to be able to identify microprocessor-based systems responsible for the control of safety barriers so that the hazards can be analyzed and mitigated in accordance with core functions of integrated safety management. In cases where the microprocessor-based system represents a single point or common cause failure mode, additional measures should be considered to mitigate, control, or lockout the hazard to protect the safety of workers, the public and environment during routine operations, maintenance, and upset conditions.

Originator DOE Idaho Operations Office
Validator Walter Sato, Assistant Manager for Technology Programs and Operations
Contact Richard Dickson, Performance Assurance Division, (208) 526-0107, dicksorl@id.doe.gov
ADC Joel Trent, DOE-ID Classification Officer
Reviewing Official Joel Trent, DOE-ID Classification Officer
Descriptor Blue / Information
Keywords Microprocessor, computer, interlock, safety barrier, alarm, safety design, safety

system,
References Type A Accident Investigation Board Report of the July 28, 1998 Fatality and Multiple Injury
DOE Functional Category COCM, COLT, COWP, EN, EP, FP, IN, LE, MAIC, MASS, MF, NS, OP, OSGE, QU, RE, RP, SD
Hazard FR, LA, PI, PIRC