



SAFETY NOTICE



Office of Operating Experience Analysis and Feedback • U.S. Department of Energy • Washington, D.C. 20585

DOE/EH-0560

Issue No. 99-01

July 1999

MICROPROCESSOR – BASED FIRE PROTECTION SYSTEM TESTING

Notice Summary

This notice contains information to alert personnel at DOE facilities that limited acceptance testing of microprocessor-based fire protection systems may not be adequate to identify potential system vulnerabilities. Recent industry events have highlighted the potentially serious consequences of unidentified design anomalies in these systems. As a result, personnel responsible for designing, accepting, and testing them should understand which operating characteristics are verified by fire protection system manufacturers and independent laboratories during the listing or approval process and which system aspects are verified by facility personnel during acceptance and subsequent periodic testing. Conservative compensatory measures should be implemented for those cases in which system software cannot be completely verified.

Applicability

This notice applies to all DOE facilities with microprocessor-based fire protection systems. However, the lessons learned may also apply to other microprocessor-based systems. This notice should be processed as an external source of lessons learned information, as described in DOE-STD-7501-95, *Development of DOE Lessons Learned Programs*.¹ EH encourages DOE managers to examine their facilities to determine whether the lessons learned in this notice are applicable.

Fire Protection System Component Descriptions

Microprocessor-based fire protection systems, referred to in this notice as microprocessor systems, may include the following components.

- Fire alarm control unit (panel) – a system component that monitors inputs and controls outputs through various types of circuits.
- Multiplex – a signaling method that simultaneously and/or sequentially transmits and receives multiple signals on a signaling line circuit and that can positively identify each signal.
- Signaling line circuit – a circuit or path between any combination of circuit interfaces, control units, or transmitters over which multiple system input signals or output signals, or both, are carried.
- Power supply – source of electrical operating power, including the circuits and terminations connecting it to the dependent system components. Two independent and reliable power supplies must be provided.
- Initiating device – a system component that originates transmission of a change-of-state. Examples of initiating devices are smoke detectors, manual fire alarm boxes, and supervisory switches.

Multiplex systems consist of master control units connected to circuit interface panels by signaling line circuits. Signaling line circuits are usually self-monitored at a preset time interval to ensure the circuits are being monitored and will activate an alarm if a device in the system is not detected. A simplified schematic of a typical multiplex system is shown in Figure 1.

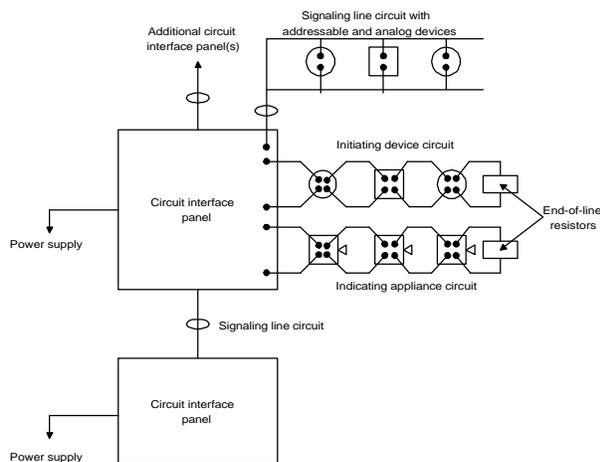


Figure 1. Typical Multiplex System

Microprocessor systems typically include software or “firmware” memory that contains startup and operating programs. This type of software usually includes an electrically erasable programmable read-only memory chip that includes the “firmware.” This code is stored in the chip and can be erased or rewritten using an electronic programming device. It can also be rewritten from the system’s data entry device, and may contain the instructions for the system or the system may interface with a personal computer. The software, “firmware”, or multiplexing scheme can include error checking routines to enhance the reliability of data sent and received by the system to items such as input devices or external monitoring points.

Microprocessor systems may function differently in different operational modes. Many possible scenarios could cause a transient to activate fire panel circuits. For example, recent testing has demonstrated that malfunctions can be induced at elevated operating temperatures. When all possible failure modes cannot be definitively identified, compensatory measures should be taken to ensure worker safety.

Event Summaries

Following are three recent events and three earlier events in which microprocessor system deficiencies were identified.

Rocky Flats Environmental Technology Site Event, 1999

On February 1, 1999, fire department personnel discovered that ten facility fire alarm system monitoring points (referred to as delta points) for fire phones, filter plenum overheat detectors, smoke detectors, and flow alarms were not reporting to the new Unity sitewide fire protection system. Investigators determined that fire protection personnel could select between a user interface or an alarm manager screen to monitor the system. Fire protection personnel had been monitoring the alarm manager screen since January 24, when the Unity system was placed into service. Because that screen did not provide an alarm, no one realized until February 1 (when personnel performing the manual verification discovered it) that ten delta points in the system were not being monitored.

Integrated systems services personnel determined that the data on a local server were corrupted. The local server provides facility delta point monitoring to the Unity system. Investigators have not determined how the server data became corrupted. However, had comprehensive software testing been conducted, this defect might have been identified.²

Idaho National Engineering Environmental Laboratory Event, 1998

On July 28, 1998, a high-pressure carbon dioxide (CO₂) fire suppression system unexpectedly discharged while workers were performing electrical maintenance, resulting in a fatality, several life-threatening injuries, and significant risk to the safety of the initial rescuers.³

Subsequent accident investigations determined that, among other things, the following design

anomalies existed in the Notifier AFP-200 panel.

- The circuit design allowed the power (voltage) to the microprocessor to drop below design minimums after ac power was disconnected and before the standby battery was connected.
- Microprocessors could sometimes generate spurious signals that mimic valid signals, actuating the circuits that released CO₂ when power to the microprocessor was below design minimums.
- The circuit design allowed the driver chips that controlled CO₂ release to react to the above-mentioned spurious signals.
- When the power to the microprocessor dropped below the design minimums, the circuit design maintained sufficient power (voltage) on the solenoid firing circuits to operate them.

Savannah River Site Event, 1998

On April 29, 1998, approximately 1,400 lb of Halon unexpectedly discharged when workers re-energized a Simplex fire system alarm panel electrical circuit after they had relocated several fire detectors. In addition, a second alarm inadvertently activated when workers re-energized the fire alarm control panel to return it to service after the Halon discharge.⁴

Investigators determined that when the system automatically reinitializes after a power loss, it cannot verify if a fire has actually occurred, so it discharges the Halon. They also determined that approximately 30 additional Halon systems are connected to the defective system and that the defect could propagate throughout them and cause all of the systems to discharge their contents.

Earlier Events

In addition to the three recent events, a review of microprocessor system events reported to the Occurrence Reporting and Processing System (ORPS) indicates that such system anomalies have existed at a variety of sites for several years. The review also indicates that corrective actions to prevent recurrence have

not been implemented throughout the complex for anomalies associated with these systems. Following are brief descriptions of three of these events.

- On February 5, 1994, at the Idaho National Engineering Environmental Laboratory, three fire alarms were received at the fire station alarm center because of a failure in a processor miniplex panel board. Investigators determined that (1) the system normally used end-of-line resistors, but the electrical subcontractor failed to install them and (2) the panel microprocessor chip and a dual channel-card main processor chip were defective and required the manufacturer to update and replace them. However, a comprehensive acceptance test would have revealed that the end-of-line resistors were not installed and might have identified the defective processor chip anomaly.⁵
- On April 23, 1993, at the Savannah River Site, a Halon system unexpectedly discharged as a fire chief was attempting to reset an alarm that had been received. Investigators determined that because of faulty system software, the software failed to reset the system after a microprocessor socket contact had been opened. They also determined that the manufacturer's testing program had not detected the software defects. In addition, the DOE program manager noted that corrective actions to replace the defective equipment should have occurred in October 1991, when the manufacturer issued a recall notice.⁶

Testing Practices

The National Fire Protection Association (NFPA) fire alarm code⁷ provides the minimum acceptable maintenance, testing, and inspection requirements for fire alarm systems and associated components. Underwriters Laboratories Inc. (UL)⁸ uses its own internal standard to "list" acceptable system designs. Factory Mutual (FM) uses NFPA 72 and its own internal criteria to "approve" acceptable system designs. Neither verifies that individual systems comply with all NFPA code requirements or are free of software design defects. Post-installation system design verification and validation are important for preventing erroneous system operation.

UL, FM, and other independent testing laboratories do not conduct comprehensive fire system testing to ensure that systems operate as designed. For example, NFPA 72, Section 7-1.6, requires initial and reacceptance testing for fire alarm systems. However, it does not require testing to be performed under abnormal conditions other than a loss of off-site power. Abnormal conditions such as power fluctuations or environmental (e.g., temperature) changes have the potential to initiate unexpected system responses. NFPA, UL, and FM are not explicit about software testing for microprocessor control units and do not require comprehensive testing for all abnormal conditions. Testing should verify that the conditions assumed in the software are consistent with the actual system configuration.

Vendors usually perform system acceptance testing in accordance with contractual stipulations, site maintenance procedures, and operating contractor procedures. However, a review of a number of such procedures found that testing may not always be explicit in regard to (1) what equipment response is acceptable, (2) the effects of harsh environmental conditions, (3) the requirements for acceptance testing of system interfaces with existing equipment, or (4) comprehensive software testing. In addition, a review of site procedures and discussions with fire protection professionals indicated that because personnel involved in designing, procuring, installing, or testing these systems are not always involved in the entire process from design to system acceptance, they view their part of the process in isolation. For example, involving design personnel in system acceptance testing may help to ensure that all necessary system components are installed and tested or annunciated as intended.

Inspection, maintenance, or testing of microprocessor systems can perturb them, causing inadvertent system actuation, false alarms, or the failure to activate when required. Such perturbations can also occur during normal operations as a consequence of electrical malfunctions or system software misapplications. System testing practices that go beyond the minimum requirements and are overseen by personnel who understand the fire protection aspects as well as the electrical, hardware, and software requirements will help to ensure that these systems function as designed.

Conclusions

Microprocessor-based fire protection systems, even if listed or approved by independent laboratories, may not be flawless. Safeguard controls may not exist to prevent corruption of the microprocessor computer systems. System failures can cause death, injuries, and property loss. System vulnerabilities must be identified and precautionary measures implemented where needed to minimize potential failures or to mitigate the consequences of failure.

As a result of this review, it is concluded that

- Microprocessor fire alarm and fire suppression systems are prone to design anomalies that can cause inadvertent actuations.
- NFPA does not mandate comprehensive software testing, and neither UL nor FM requires it.
- Site test procedures are typically not comprehensive enough to ensure that the system software functions as designed.

Recommendations

The following actions should be implemented as an integral part of every site fire protection program.

- The design of new fire alarm and signaling systems and modifications of existing systems should be reviewed, supervised, and accepted by a qualified fire protection engineer and other relevant personnel (such as an electrical engineer). The design review should assure that NFPA codes and DOE standards are met.
- Purchases of microprocessor control units should be reviewed and accepted by the responsible fire protection engineer as part of the site quality assurance/quality control program to assure that they are compatible with the intended use. Software controls should not be relied on if a system discharge would be hazardous to life and health. Only "listed" or "approved" units are

permitted, in accordance with NFPA 72 and DOE-STD-1066-97.⁹

- A comprehensive acceptance test program for fire alarm and signaling systems should be implemented. It should include hardware and software testing under all modes of system operation, including loss of power and other anticipated transient conditions.
- All new fire alarm and signaling systems should be under warranty for an acceptable period until satisfactory system performance is established. Consideration should be given to requiring warranties in the procurement process. DOE system acceptance should not relieve the manufacturer of responsibility for correcting any system anomalies that are related to manufacturing, even if they are not identified until the system is in operation.
- Personnel responsible for fire alarm and signaling system testing and maintenance should be certified by the National Institute for Certification in Engineering Technologies or equivalent and should receive annual refresher training to maintain their proficiency. It may also be desirable to provide responsible personnel with factory-based training on the specific system being installed.
- System malfunctions and other anomalies should be reported in accordance with existing DOE reporting mechanisms (such as CAIRS or ORPS) to facilitate greater awareness of operating experience. System malfunctions and anomalies should also be reported on the fire protection LISTSERV to facilitate sharing lessons learned information.
- Compensatory measures should be implemented in cases where test and evaluation programs do not completely verify system software adequacy. These compensatory measures should be reviewed by a qualified fire protection engineer and ensure that potential software failures do not result in hazards to workers or facility safety system damage. Some typical compensatory measures may include (1) additional worker instructions, (2) procedural changes, (3) additional

mechanical safeguards, or (4) repositioning of supplementary safety equipment

Additional information or questions on microprocessor fire alarm and fire suppression system testing practices may be obtained by contacting the DOE fire protection Authority Having Jurisdiction or a member of the DOE Fire Safety Committee at <http://tis.eh.doe.gov/whs/TechComm/fscindex.html>, or Dennis Kubicki, at (301) 903-4794 or dennis.kubicki@eh.doe.gov.

References

1. DOE-STD-7501-95, Change Notice #1, *Development of DOE Lessons-Learned Programs*.
2. Weekly Summary 99-07 and ORPS Report RFO--KHLL-SITEWIDE-1999-0003.
3. Weekly Summaries 98-30, 98-33, 98-38, and 98-43; Type A Accident Investigation Board Report on the July 28, 1998, Fatality and Multiple Injuries Resulting from the Release of Carbon Dioxide at Building 648, Test Reactor Area, Idaho National Engineering and Environmental Laboratory; Safety & Health Bulletins 98-1 and 99-1; and ORPS Report ID--LITC-TRA-1998-0010.
4. ORPS Report SR--WSRC-HBLINE-1998-0006.
5. ORPS Report ID--EGG-INELSUP-1994-0002.
6. ORPS Reports SR--WSRC-WSALT-1993-0001 and SR--WSRC-WVIT-1992-0029.
7. NFPA 72, *National Fire Alarm Code*, 1996.
8. UL-864, *Control Units for Fire-Protective Signaling Systems*, November, 1996.
9. DOE-STD-1066-97, *Fire Protection Design Criteria*, March, 1997.

This notice is one in a series of publications issued by the Office of Nuclear and Facility Safety to share safety information throughout the Department of Energy complex. For more information, contact Jim Snell, Office of Operating Experience Analysis and Feedback, Office of Nuclear and Facility Safety, U.S. Department of Energy, Washington, D.C. 20585, telephone (301) 903-4094.

Safety notices are distributed to U. S. Department of Energy program offices, field offices, and contractors who have responsibility for the operation and maintenance of nuclear and related facilities and to other organizations involved in nuclear safety. Written requests to be added to or deleted from the distribution of safety notices should be sent to Christine Crow, RPI, 20251 Century Blvd., Germantown, MD 20874, fax (301) 540-2499, or email at ccrow@rpihq.com.

The ES&H Information Center maintains a file of safety notices and supporting information. Copies can be obtained by accessing the safety notice web page at http://tis.eh.doe.gov/web/oeaf/lessons_learned/ons/ons.html or by contacting the ES&H Information Center, (800) 473-4375, U.S. Department of Energy, ES&H Information Center, EH-72, 19901 Germantown Road, Germantown, MD 20874.
