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
Chapter 3

3.0 DISCUSSION AND ANALYSIS

3.1 WORKER SAFETY

General

Safety requirements for worker protection come from many sources.

DOE Order 440.1A, *Worker Protection Management for DOE Federal and Contractor Employees*, is the current DOE policy for worker protection. However, this Order has not been implemented by LMITCO, nor has it been incorporated into the DOE contract with LMITCO. DOE Orders 5480.4, *Environmental Protection, Safety, and Health Protection Standards*, and 5480.7A, *Fire Protection*, are currently incorporated into LMITCO's contract. These Orders implement National Fire Protection Association (NFPA) Standard 12 and Occupational Safety and Health Administration (OSHA) regulations for worker protection (Title 29, Code of Federal Regulations (CFR), Part 1910, *Occupational Safety and Health Standards*) through the contract. The requirements are summarized in Table 3-1.

OSHA standards require engineering and administrative controls to protect employees from exposure to toxic levels of carbon dioxide.

OSHA regulations recognize worker hazards from CO_2 fire suppression systems and require employers to assure that employees are not exposed to toxic levels of gaseous agents. OSHA has developed standards for control of hazardous energy contained in 29 CFR 1910, Subpart J, *General Environmental Controls*. Standards for fixed extinguishing systems, including fixed extinguishing systems using gaseous agents like CO_2, are contained in 29 CFR 1910, Subpart L, *Fire Protection*. These standards require implementation of engineering and administrative controls to protect employees from exposure to toxic levels resulting from an unplanned release of energy that could cause worker injury. LMITCO implements the requirements contained in 29 CFR 1910, Subpart J, using Management Control Procedure MCP-1059, *Lockout and Tagout*. LMITCO has not defined a procedural mechanism to implement OSHA fire protection regulations in 29 CFR 1910, Subpart L.

NFPA Standard 12, *Carbon Dioxide Extinguishing Systems*, recognizes serious personnel hazards associated with CO_2 and the possibility that personnel could be entrapped in an area protected by a CO_2 flood system. The standard requires posting of warning signs, an operational pre-discharge alarm or warning signal sufficient to allow evacuation, and a lockout when persons not

familiar with the systems and operations of the system are present in the protected space.

Facts and Discussion

Energy Isolation and Provisions for Positive Lockout. An INEEL procedure established in 1982 and the Preventive Maintenance Surveillance and Maintenance Manual requires that CO_2 systems be removed from service, including removal of the electric control heads, prior to maintenance that could cause a release of CO_2. This procedure complies with the requirements of 29 CFR 1910, Subpart J, but was not used as the basis for impairing the CO_2 system to support the preventive maintenance activity that was ongoing at the time of the accident.

The approved procedure for removing the fire suppression system from service was not used.

Servicing, maintenance, and design modification activities were performed on the CO_2 fire suppression system in Building 648 since the revision of the OSHA regulations on January 2, 1990. These regulations require installation of an energy isolation device, or other systems and equipment, capable of accepting a lockout device, whenever major modification of equipment is performed. Modifications to the system piping in 1997 fall into this category and within the purview of the regulations. Design drawings for the Building 648 CO_2 fire suppression system did not include energy isolation devices (such as a manual valve), and no energy isolation device that meets the requirements of 29 CFR 1910.147, Subpart J, was installed in the CO_2 system in Building 648.

Interviews revealed that a draft preventive maintenance procedure for the fire protection system was not used for this activity and CO_2 shutdown, because it was considered too restrictive.

Engineering Controls. CO_2 design concentrations for the fire suppression system in Building 648 exceed the maximum safe level for employee exposure, and a pre-discharge employee alarm was installed for the system in accordance with 29 CFR 1910, Subpart L. However, an alarm was not actuated prior to or during the CO_2 discharge on July 28, 1998, because it was dependent on a valid initiation signal which was not received.

The pre-discharge alarm on the fire suppression system did not activate, so workers had no warning.

Table 3-1. Requirements for Protecting Workers from Hazards Associated with CO_2 Fire Extinguishing Systems

Citation	Requirements
DOE Orders 5480.4 and 5480.7A (through the LMITCO contract)	Establish the framework for worker protection programs requiring compliance with 29 CFR 1910 and NFPA Codes and Standards.
29 CFR 1910, Subpart E	Requires that every exit and way of approach be continuously maintained free of all obstructions to facilitate emergency use. Additionally, Subpart E requires that every automatic alarm system be continuously operational while the building is occupied.
29 CFR 1910, Subpart J	Requires employers to establish a program and to use procedures to control potentially hazardous energy before an employee performs work on equipment that could release energy unexpectedly and cause injury. The regulation also requires that equipment be isolated from the energy source and rendered inoperative by affixing appropriate lockout devices or tagout devices to energy isolating devices. It prohibits the use of push buttons, selector switches and other control circuit type devices as energy isolating devices. After January 2, 1990, energy isolation devices must be designed to accept a lockout device, whenever replacement or major modification of equipment is performed.
29 CFR 1910, Subpart L	Establishes fire protection requirements for fixed extinguishing systems using gas as an extinguishing agent and requires measures to protect workers who may be exposed to possible injury, death or adverse health conditions associated with the extinguishing agent. The regulation requires a distinctive pre-discharge employee alarm or signaling system, when extinguishing agent design concentrations exceed the maximum safe level for employee exposure, and the alarm is required to actuate before discharge to allow employees time to safely exit the discharge area. Subpart L includes requirements for employers to provide effective safeguards that protect employees from potential safety and health hazards associated with CO_2 flood systems, and requires development and use of emergency action plans, posting of hazard warnings signs, and availability and use of protective equipment for rescue.
29 CFR 1910.1200, Appendix E	Requires employers to implement a program to ensure employees are provided information on work place hazards associated with chemicals, and to provide Material Safety Data Sheets and training on workplace hazards to employees.
NFPA 12, Sections 1 through 5	Discusses requirements for personnel safety. This standard requires affixing warning signs inside and outside of spaces where CO_2 can accumulate as well as spaces where CO_2 could migrate. The standard requires a warning signal that provides a time delay sufficient to allow for evacuation under "worse case" conditions, drills or dry runs to determine a safe evacuation time, and evacuation procedures. When personnel unfamiliar with CO_2 systems and their operations are expected to occupy a protected space, "lockout" shall be provided to prevent accidental or deliberate system discharge.

Nevertheless, workers were not trained, as required, to recognize the CO_2 warning alarm, and, during interviews, described it in various ways as a buzzer, bell, and siren.

The CO_2 system discharge header monitoring circuit was not installed as required by the NFPA Code (see Section 3.2 of this report). When combined with the additional mechanical 25-second delay in the CO_2 system, this monitor should have sounded an alarm on solenoid operation and initial CO_2 header

pressurization, and should have provided time for evacuation, even in the absence of valid signal and normal 30-second warning alarm. However, no warning alarm was received prior to the accident.

Administrative Controls. An action plan was not established for responding to Building 648 CO_2 system emergencies, as required by 29 CFR 1910, Subpart L, and as prescribed by the Lockheed Martin Corporate ES&H Policy, which also requires that a plan be established to identify and to abate workplace hazards. Therefore, an action plan was not available during the work planning stages for the job to facilitate communication of escape procedures and escape routes, rescue, and medical duties for employees during emergency evacuation. The ETR Surveillance and Maintenance Manual provides limited guidance, including that the building will not support life 25 seconds after a CO_2 discharge and that re-entry after such discharge must be made using self-contained breathing apparatus. With the normal building communication system shut down due to the electrical outage in Building 648, no provisions were made for emergency communication in the event of a CO_2 discharge. Additionally, CO_2 emergency evacuation drills had not been conducted at TRA, to prepare personnel to exit safety in case of an accidental discharge. Warning or caution signs and instructions were not posted at the entrance to, and inside of, areas protected by fixed extinguishing systems that use CO_2, as required. The LMITCO Health and Safety Manual does not address CO_2 hazards, emergency action plans for facilities with CO_2 systems, or emergency response.

No signage or means of emergency communication was in place to support workers escaping from the building, and no evacuation drills had been conducted.

Personal Protective Equipment. LMITCO's Hazards Communication Program contains a Material Safety Data Sheet that addresses CO_2 health hazards and OSHA required personal protective equipment. The Material Safety Data Sheet stipulates use of self-contained breathing apparatus in case of an emergency and general ventilation and local exhaust to meet Threshold Limit Value requirements for CO_2.

Self-contained breathing apparatus had been removed from the area as a cost-cutting measure.

Self-contained breathing apparatus was removed from Building 648 and other pre-staged areas and consolidated at the TRA Emergency Control Center in 1993, in response to assessments and cost reduction considerations. The need for self-contained breathing apparatus was not discussed or included in the work planning and hazard analysis prior to the work, and it was not staged in Building 648 prior to start of the work.

As noted in Section 2.3.1 of this report, the arrival of self-contained breathing apparatus in the Incident Response Team emergency van from the Emergency Control Center in Building 680 was delayed. Consequently, employees and security personnel made several building entries without air breathing apparatus to rescue injured workers, thus exposing themselves to further risks, in violation of OSHA regulations and LMITCO procedures.

Safe Means of Egress. Obstacles and pathway obstructions hindered both escape from and entry into the area during the accident. Entry doors to Building 648 are normally locked. A broken door latch facilitated locating and rescuing one worker. Unlocking and propping these doors open during the preventive maintenance would have significantly aided in both emergency egress and search and rescue.

Exit pathways were obstructed, and lighting was inadequate. A broken latch on a normally locked door facilitated rescue efforts.

Temporary and emergency lighting in Building 648 was situated to facilitate switching and other maintenance activities, but was not provided at exit pathways and doors to facilitate rescue or emergency egress from the accident scene. The northeast corner and the motor/generator room, where the most serious injuries occurred, were particularly dark.

Analysis

Barriers that either failed or were not in place at the time of the accident included mechanical energy isolation (positive lockout), warning signs, ventilation, exit pathway lighting, clear exit pathways, and self-contained breathing apparatus and emergency action planning to prevent exposure of employees to the toxic effects of CO_2 and to accomplish immediate search and rescue. These barriers all are required by OSHA regulations and/or NFPA standards.

With respect to lockout, NFPA Standard 12, requires that CO_2 systems be locked out when work is being done in the area protected by the system, but does not specify how lockout should be accomplished. This point is effectively moot, because the Building 648 CO_2 system was not equipped in a manner that met OSHA requirements (such as a lockable valve in the CO_2 piping, prior to piping penetration into the building) to assure positive lockout and personnel protection. Lockout of the CO_2 system had been accomplished in the past by lifting the electric control heads. While lifting electric control heads as a means of positive lockout had been used in the past and would have prevented this particular

There was no valve to ensure positive lockout on the fire suppression system.

accident, it does not prevent all modes of CO_2 initiation. A manual isolation valve with remote position indication is easily installed, provides positive isolation, and ensures protection of personnel from all types of CO_2 initiation. According to OSHA regulations, such an isolation device or valve should have been installed during the first significant system design modification, in this case, in 1997. Despite the recognized hazard, physical isolation of the CO_2 system was not employed. This single action could have prevented the accident, injuries, and loss of life, whether it was an actual signal or accidental discharge.

LMITCO also did not adequately consider and implement the necessary hazards analysis and controls to implement these requirements, and make the barriers effective. Had the regulatory requirements been institutionalized through policy, manuals, procedures, work planning activities, and training (see Section 3.3), the accident might have been prevented or the consequences mitigated. The potential for unplanned accidental or manual discharge of CO_2 total flooding systems without a 30-second pre-discharge warning alarm was not anticipated.

An institutionalized approach to requirements management might have identified and mitigated the hazards of the carbon dioxide system.

RELATED CAUSAL FACTORS

Failure to use physical (primarily positive lockout/tagout) and administrative barriers (current procedures and work planning and control processes) that implemented regulatory requirements, was a contributing cause of the accident.

JUDGMENTS OF NEED

DOE needs to actively campaign to improve consensus standards and in the interim should consider strengthening Orders and policies related to fire protection and worker safety to clearly define lockout, to limit occupancy in CO_2 flood areas, and to prevent use of fire system impairments as a means of personal protection.

LMITCO needs to establish and implement a program that complies with and incorporates all applicable worker protection requirements contained in OSHA regulations, NFPA codes and standards, and DOE Orders for CO_2 fire suppression systems and other systems with hazardous gases into applicable manuals, safety analysis reports, procedures, and work planning and control processes to ensure employees are protected from releases of toxic agents from energized systems.

LMITCO needs to ensure that all total flooding gaseous agent fire suppression systems at INEEL are equipped with an OSHA compliant positive lockout mechanism that is electrically supervised by the releasing system. DOE needs to consider implementing a similar policy across the complex.

Note: Other judgments of need also applicable to failure of requirements implementation and work planning are addressed in Section 3.4.

3.2 FIRE PROTECTION AND ELECTRICAL SYSTEMS

Background

Fire protection systems relevant to the accident include a building fire alarm system (installed in 1996/97) and an existing, high-pressure, total flooding CO_2 extinguishing system (installed in 1971). The building fire alarm is configured for releasing service and controls discharge of the CO_2 system. Installation standards applicable to these systems include: NFPA Standard No. 12, *Carbon Dioxide Extinguishing Systems*, NFPA Standard No. 70, *National Electrical Code,* and NFPA Standard No. 72, *National Fire Alarm Code.*

The fire protection systems in Building 648 were upgraded as part of a $25M line item project (FY-92-LICP - INEL Fire and Life Safety Improvement) that started in 1996. This project included replacement of existing fire alarm systems throughout the TRA and modification of the CO_2 system in Building 648 (to eliminate coverage for the basement). The original scope called for controlling several buildings, including Building 648, from a remote panel in Building 647. This was subsequently revised by Contractor Interface Document 199 to require a separate fire alarm control panel in Building 648, specifically configured for releasing service. Test records indicate that the new fire alarm system in Building 648 was put into service in May 1997. Reactor Programs has not yet accepted this system due to concerns with procedures, drawings, and training not being updated.

The new building fire alarm system was put into service in May 1997.

System Description

Fire Protection. The building fire alarm system is controlled by a Notifier Model AFP-200 fire alarm control panel (see Exhibit 3-1). This panel monitors 14 heat detectors, two manual fire alarm stations, two manual (CO_2) releasing stations, and a waterflow detector for the building's dry-pipe sprinkler system. Outputs from the building fire alarm system include one notification appliance circuit (controlling the building evacuation signals), two releasing circuits (controlling automatic discharge of the CO_2 system), and a network interface that allows the Building 648 fire alarm control panel to be monitored by the overall TRA fire alarm reporting system.

The fire alarm system controls the evacuation alarms and the carbon dioxide discharge system.

The CO_2 extinguishing system is a high-pressure, total flooding system. It consists of 55 100-pound CO_2 cylinders connected

together by manifolds, all of which are located in a CO_2 shed attached to the south side of the building (see Exhibit 3-2). The CO_2 manifolds connect to a system of piping and ceiling nozzles inside Building 648.

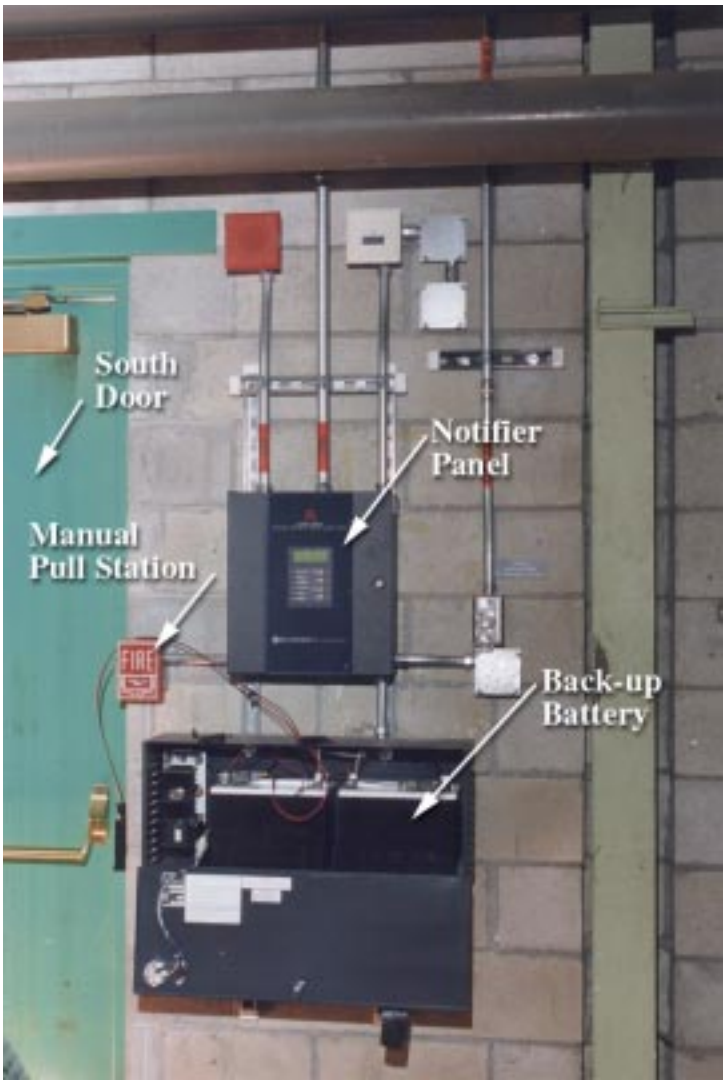

Exhibit 3-1. Notifier Fire Alarm Panel

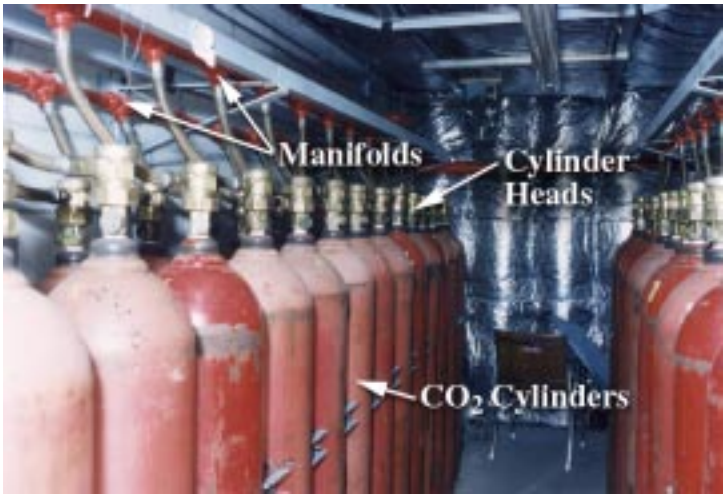

Exhibit 3-2. CO_2 Cylinders and Manifolds

Review of existing drawings indicated that the CO_2 system was originally installed in 1971 as a two-zone system. One zone covered the main floor, and the second zone covered the basement.

Sequence of Operation. As currently configured, discharge of the CO_2 system can be initiated either electronically (via the building fire alarm control panel), or by actuating emergency manual releases in the shed where CO_2 was stored. Electronically operated valves (control heads) (see Exhibit 3-3) on two of the CO_2 cylinders are connected to releasing circuits from the alarm system. When these control heads are energized by the fire alarm system, they open their associated cylinders to the manifold, pressurizing the manifold, and opening pressure-activated valves on the other 53 cylinders. CO_2 then discharges into the building through the distribution piping and nozzles (at pressures of up to 850 psi) (see Exhibit 3-4) until the CO_2 supply is exhausted.

The carbon dioxide system can be activated either electronically or manually.

The CO_2 releasing function was designed to operate automatically upon activation of any single heat detector, upon activation of either of the two CO_2 manual releasing stations, or manually upon activation of the mechanical (emergency) releases on the control heads.

Once activated, the CO_2 discharge sequence cannot be aborted. Each of the two electric control heads is equipped with a lever operated emergency release that allows the system to be manually discharged with no input from the building fire alarm system.

Once activated, the carbon dioxide discharge cannot be aborted.

For safety purposes, the CO_2 system was equipped with two discharge delays: a 30-second electronic delay (prior to activating the control heads), and a 25-second mechanical delay (between operation of the control heads and discharging CO_2 into the building). The electronic delay is a software-controlled function of the fire alarm system; the mechanical delay is a component (similar to a small pressure tank with a restricting orifice) installed in the CO_2 manifold.

A valid activation of the system produces an alarm and allows enough time for workers to evacuate before carbon dioxide is discharged.

In the event of valid operation, the combination of the 30-second electronic delay and 25-second mechanical delay should have provided an alarm and about a 55-second pre-discharge warning. Manual operation using the emergency releases or accidental actuation would bypass the electronic delay, reducing the warning time to about 25 seconds. In any case, the system was not intended to discharge CO_2 into the building without warning.

Electrical System Description. Building 648 houses the major electrical equipment for the ETR and other TRA buildings, such as Building 680. This equipment consists of the 13,800 volt, 4160 volt, and 480 volt switchgear, 480 volt motor control centers, emergency diesel-generators, other motor-generator units, and a lead-acid storage battery bank. The electrical systems in Building 648 were originally designed and installed to provide electrical power at the proper voltages to ETR plant electrical equipment. As the ETR has been shut down and other new buildings have been built, the electrical systems in Building 648 have been modified to accommodate these changes.

Building 648 houses major electrical equipment for the Test Reactor Area.

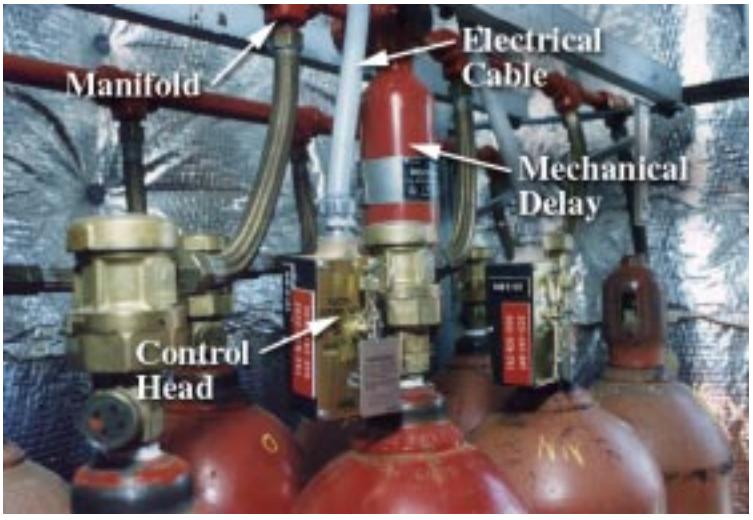

Exhibit 3-3. Control Head and Mechanical Delay Mechanism

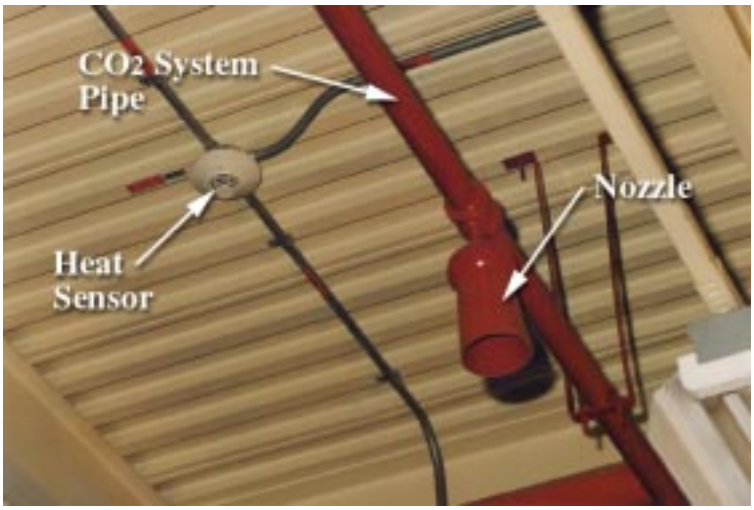

Exhibit 3-4. Overhead CO_2 Discharge Nozzle

Electrical power is provided to Building 648 by three sources: commercial power, diesel power, and batteries. Commercial power is provided from the main INEEL substation by two parallel 138,000 volt lines to the TRA substation, then from the TRA substation to Building 648 on two parallel 13,800 volt lines, and transformed to 4160 volts and fed on two parallel lines to the Building 648 switchgear. These parallel lines feed the 4160 volt bus through Circuit Breakers No. 13 and 23, with Breaker No. 18, which is normally opened, acting to tie together the 4160 bus sections. Breaker No. 13 feeds power to facilities through Breakers No. 15, 16, and 17. Breaker No. 23 feeds power to TRA deep well pumps. The diesel power supply to the Building 648 switchgear is not relevant to the accident. The battery power supply provides direct current (DC) voltage primarily used for switchgear control power at 125 volts DC. A simplified schematic of the relevant switchgear is shown in Figure 3-1.

Fire protection systems in Building 648, as well as building lighting systems, are fed electrical power from 4160 volt switchgear Breaker No. 17, that feeds a 480 volt switchgear Breaker No. 11C, and a 480 volt distribution panel (648-E-25). The fire protection system is fed from this distribution panel, through Lighting Panel K, to a 240 volt transformer, sub-panel KA circuit Breaker No. 5 which supplies 110 volt alternative current (AC) service to the Notifier AFP-200 panel. The fire alarm panel was provided with 60 hours of dedicated emergency battery backup power.

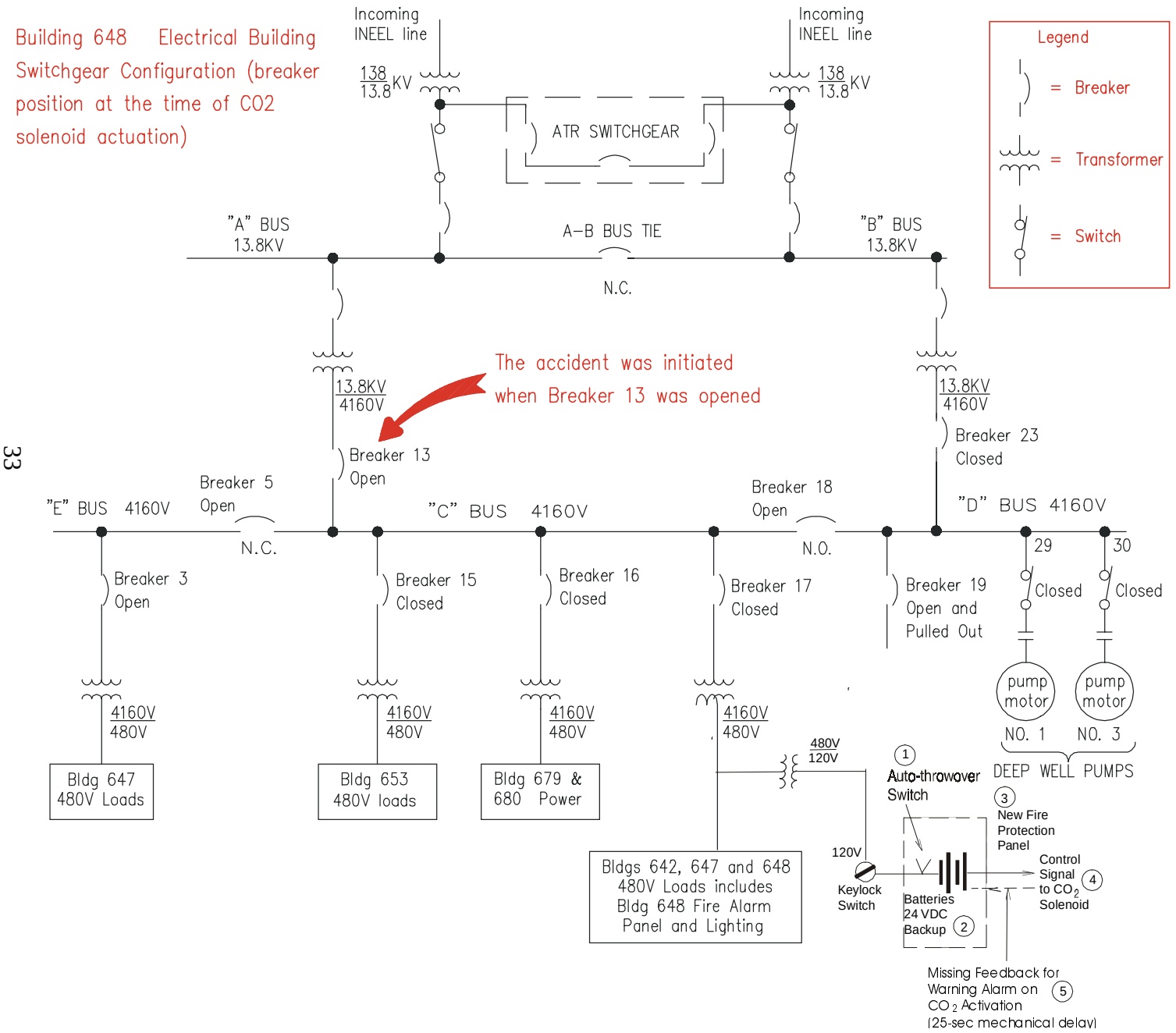

Figure 3-1. Simplified Schematic of Switchgear

Facts and Discussion

The failure to install a carbon dioxide system discharge monitoring circuit prevented a 25-second pre-discharge warning alarm and safe escape.

System Design. The as-installed CO_2 releasing system does not monitor discharge of the suppression system it controls, as required by Sections 3-8.8.1 and 5-7 of NFPA 72, *National Fire Alarm Code*, 1996 edition. This requirement was not identified on the LMITCO approved engineering design documents, nor was its omission subsequently identified. Modifications completed in 1997 changed it to a single-zone system by eliminating selector valves (which controlled where the CO_2 discharged) and the basement level CO_2 piping and nozzles. Figures 3-2 and 3-3 depict the system prior to and after the modifications. Modifications to the CO_2 piping system are not detailed in either design or as-built drawings, with all mechanical design references deferring to original (1971) design documents. These design documents called for installation of pressure switches to the CO_2 manifold with a feedback loop to the fire alarm panel, but the switches and feedback loop were deleted and never installed (see Figure 3-1). LMITCO also failed to install this monitoring circuit during the 1997 modifications and fire alarm panel upgrade. It is not clear that designers understood the significance of having pressure operated backup alarm features in the CO_2 system or the impact of their original removal in 1971. The absence of these pressure switches and monitoring circuit precluded at least a 25-second pre-discharge warning alarm and the opportunity for safe evacuation prior to the CO_2 discharge. During the 1997 modification, LMITCO also failed to install a positive isolation device in the CO_2 system piping as required by OSHA regulations (see Section 3.1 under "Energy Isolation and Provisions for Positive Lockout").

Deviations in the fire alarm system installation could have made it easier for a transient electrical input to trigger the unexpected discharge.

System Installation. The building fire alarm system was not installed in strict accordance with the manufacturer's published installation instructions (as verified by panel and device inspection during this investigation). Deviations include the use of an auxiliary power supply for a releasing application, and shielding errors on the signaling line (addressable) circuits. One of the two releasing circuits is powered by an unregulated, unfiltered auxiliary power supply, which the panel installation manual indicates is only to be used to power notification appliances (i.e., fire alarm bells or horns). Only part of the signaling line circuit is shielded. This circuit branches directly from the control panel terminals; one branch is shielded and the other is not. In addition, the shield drain conductor on the shielded branch is connected to the wrong terminal on the fire alarm panel main board. It is not clear at this time whether these

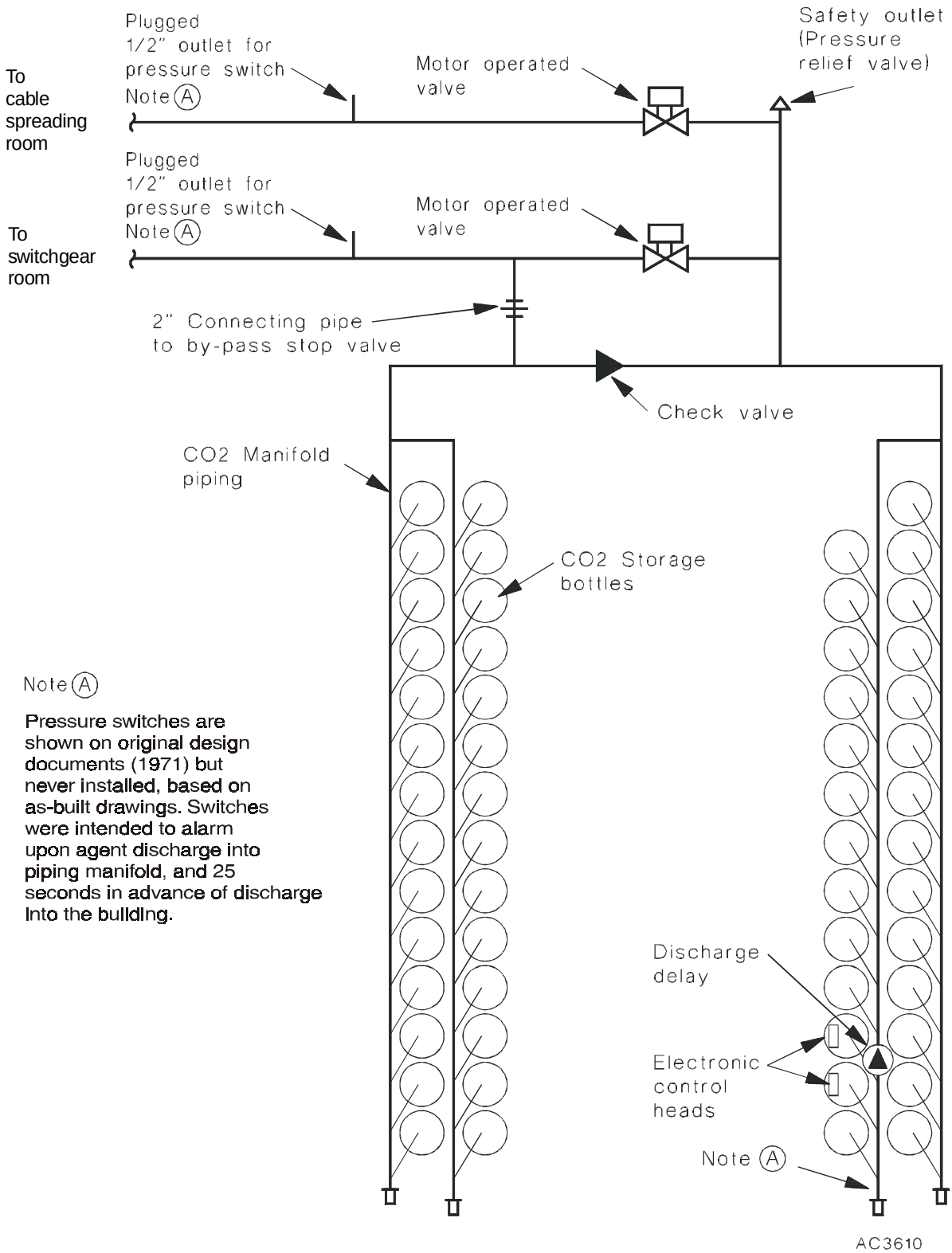

Figure 3-2. Carbon Dioxide System Arrangement Pre Line Item Upgrade

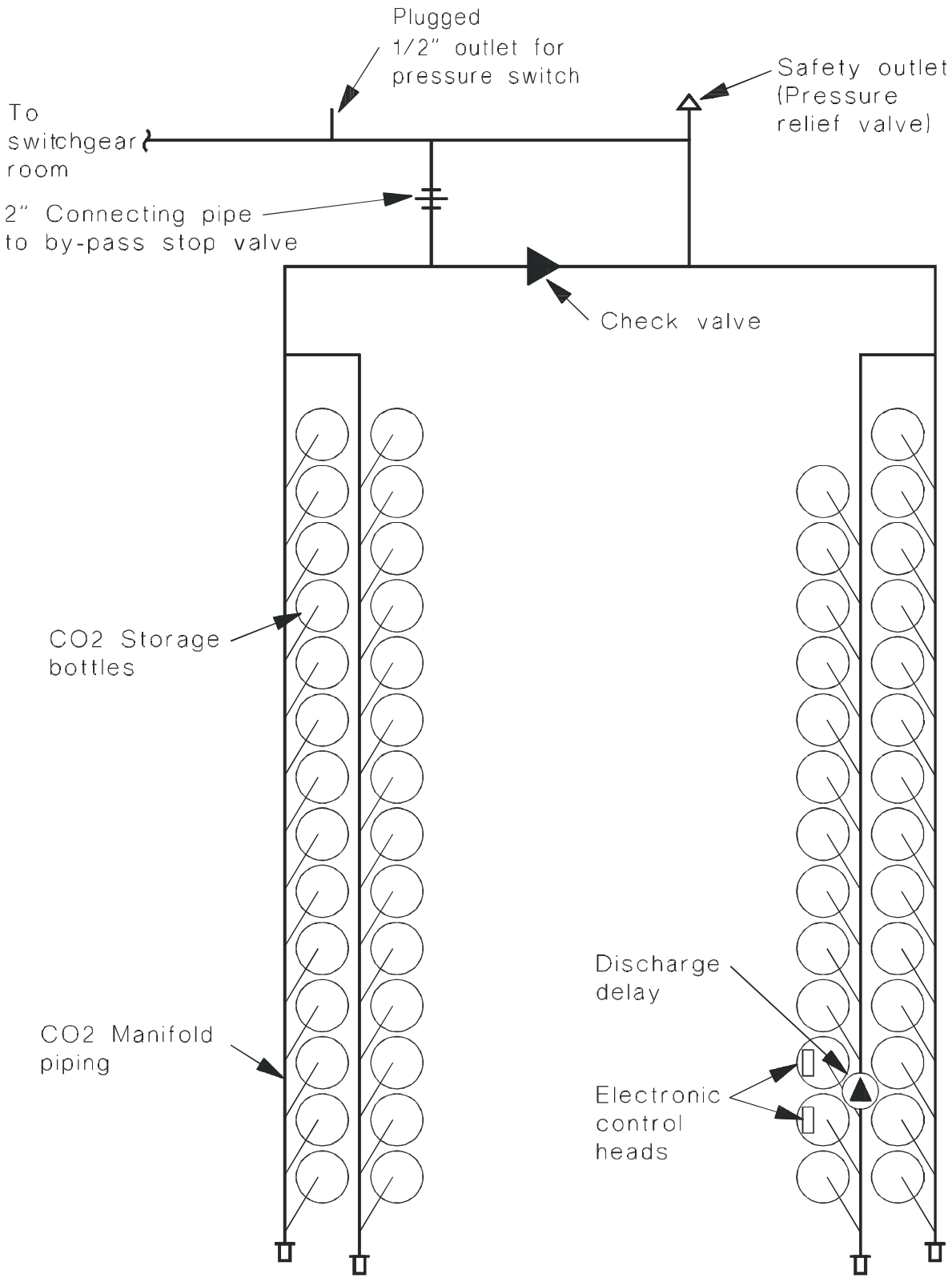

Figure 3-3. Carbon Dioxide System Arrangement Post Line Item Project

installation deviations were significant with respect to the accidental CO_2 discharge. The auxiliary power supply is suspect because opening Breaker No. 13 appears to have been the cause of the CO_2 discharge, presumably as a consequence of a voltage surge or spike. The fact that this power supply is unregulated and unfiltered may make it easier for a transient input to that supply to get through to the panel and trip the releasing circuits. The shielding on the addressable circuits is suspect because it is intended to dissipate transient signals before they can affect system operation.

Initiation of System Discharge. The CO_2 discharge was not mechanically or manually initiated (i.e., there was no valid initiation signal). The mechanical releases on the releasing control heads were both in the normal position with tamper seals in place. The manual releasing stations inside the building were both in the normal (non-activated) position. The light emitting diode indicators on the manual releasing stations both indicated system normal, despite the fact that the system had discharged. Both of the releasing heads appear to have been electronically operated. This suggests that the discharge was initiated by the CO_2-releasing system as a controlled actuation, or as a consequence of an induced or imposed current on the releasing circuits. The building fire alarm panel did not initiate the discharge in the normal manner (i.e., in response to a recognized alarm signal processed in accordance with the system program). The panel history shows no alarms, commanded outputs, or malfunctions. In addition, both fire alarm panel releasing circuits were intentionally disabled via software control at the time of the accident.

There was no valid initiating signal before the carbon dioxide was released, and the fire alarm panel recorded no alarms, commanded outputs, or malfunctions either before or after the release.

Re-acceptance Testing. Review of the system program identified no obvious programming errors. It was noted that the panel history shows that some program changes have been made since the system was installed, apparently without re-acceptance testing as required by NFPA Standard 72. Although re-acceptance testing is primarily intended to verify program changes, the prescribed methods require testing devices in addition to those directly affected by the program change. Consequently, performing re-acceptance testing after each program change would have provided additional opportunities for recognizing design deficiencies.

No errors were apparent in the software, but re-acceptance testing was never performed following program modifications.

System Documentation. System documentation was incomplete. The installing contractor's shop drawings, record of completion, and the LMITCO Operations and Maintenance Manual (dated 1982) have not been revised to reflect the design modifications or the current configuration. Some record drawings have been provided; however, these are incomplete and not entirely accurate.

System documentation is incomplete and inaccurate.

Accident Re-creation. On August 13, 1998, a work package was approved to re-create the accident, including activities leading up to the event, and to copy essential data files stored in the alarm panel's main processor. Included were three circuit breaker disconnection attempts, as well as downloading of the alarm system program, event, and shadow histories prior to returning alarm service to the building. Manufacturer's requirements for downloading stipulate that both normal and emergency power supplies be disconnected, which was included in the work plan. Upon restoration of building alarm service, CO_2-releasing circuits would be disconnected and a thorough system test conducted.

The Accident Investigation Board observed tests designed to re-create the accident.

On August 14, 1998, the circumstances of the CO_2 discharge were successfully re-created by the work package's first attempt at disconnecting the circuit breakers. Opening of 4160 volt Circuit Breaker No. 13 caused the alarm system to shut down momentarily and energized both control heads (CO_2-releasing solenoids). Consistent with the evening of July 28, 1998, audible alarms were silent and the fire alarm system history did not record either an alarm or the actuation of the releasing circuits.

Test personnel decided to curtail the remaining two circuit breaker tests to preserve alarm panel electronics, and proceeded with the downloading portion after resetting both control heads. During the process of removing system power to the alarm panel, a second control head (Solenoid Circuit No. 2) was energized, when power was removed from the main panel but not the auxiliary power supply module (tied to Solenoid Circuit No. 2). Again, no alarms or event histories were recorded at the panel.

Test results suggest that the design of the AFP-200 control panel allows power supply transients (such as those resulting from opening 4160 volt breakers or 110 volt AC contacts) to bypass the system program/logic and energize the releasing circuits. Future testing of this equipment by LMITCO is necessary to determine the exact mechanism by which this occurred.

Test results indicate that the fire alarm control panel allows power supply transients to bypass the control system and energize the releasing circuits.

While the CO_2 system appeared to discharge when Breaker No. 23 was opened on the day of the accident, it actually occurred with the opening of Breaker No. 13, which was earlier in the sequence. This was due to the 25-second mechanical delay to the CO_2 system discharge. The Board has requested that LMITCO test the mechanical delay device to confirm the 25-second delay period associated with this device.

Analysis

Configuration Management. The CO_2 system was not properly designed, because it did not monitor discharge of the suppression system it controlled. This monitoring could have been accomplished by installing a pressure switch on the CO_2 manifold (upstream of the mechanical delay) arranged to activate the evacuation signals upon initial pressurization of the manifold. While this deficiency did not cause the discharge, it was important to the outcome because it allowed the CO_2 system to operate without warning. Had the CO_2 system been monitored as required, the evacuation signals would have provided 25 to 55 seconds warning before CO_2 was discharged into the building. This would presumably have been sufficient time to allow the building occupants to escape without injury.

The failure of the design, design review, and test processes to identify the lack of a discharge monitoring capability represents a systemic weakness.

The reason for this design deficiency has not yet been determined. At this time, it is not clear whether the system designer(s) was qualified, as required by NFPA Standards 12 and 72, and understood the requirements, or whether the applicable standards were in fact used in the design. It is further unclear why the deficiency was not identified in the design review process, during subsequent reviews of contractor submittals (shop drawings, Operations and Maintenance Manual, record of completion, etc.), or during acceptance testing, re-acceptance testing (required after software changes), or preventive maintenance. The failure to install these pressure switches and alarm monitoring circuit occurred both in 1971 (when the switches appeared in the original design drawings and were deleted) and again with the installation of the new fire alarm panel in 1997. Because these reviews cross numerous organizational lines (Engineering, Procurement, Construction Management, Maintenance, etc.), the fact that none of them identified this deficiency reflects a systemic problem.

Poor design modification documentation and the fact that system drawings were not updated made it difficult to pinpoint the causes of these design and design review anomalies. Reactor Programs had not yet signed off on the fire protection modifications, which have been in operation for over a year, because drawings and procedures have not been updated to match the modifications. If requirements for the system and the design and approval process had been known, understood, documented, and implemented, the deficiencies could have been identified and rectified either in 1971 or in 1997. Thus, it is concluded that a failure to understand or implement applicable procedural requirements for system design and installation, including engineering oversight and quality

Outdated system drawings and poor documentation of system modifications make it difficult to pinpoint the causes of anomalies in design and installation.

assurance, contributed to the accident. It is unclear what role ID played in the oversight and acceptance of LMITCO's design process through its delegated capacity as the DOE authority having jurisdiction. No ID signature box is provided on the design modification drawings.

The design and installation flaws in the fire suppression system modification also had an impact on accident mitigation. If the warning that the system was about to discharge had worked, emergency exit could have been accomplished and injuries probably could have been prevented.

RELATED CAUSAL FACTORS

Faulty design and installation of the fire suppression system, due to failure to implement appropriate requirements and procedures, and failure to install a monitoring or feedback circuit for the CO_2 discharge header or solenoid valve position to the discharge alarm that would have warned workers of the CO_2 actuation and imminent discharge were a contributing cause to both the accident and its mitigation.

The discharge of carbon dioxide may have resulted from a transient voltage.

Mechanism of Discharge. The specific mechanism by which the CO_2 discharged remains to be determined. The following hypothesis seems to be consistent with the facts and/or current assumptions:

> The releasing solenoids were not energized by the building fire alarm panel as a logic-controlled output (valid signal). The CO_2 discharge probably was a consequence of external voltage induced or imposed on the releasing circuits or other panel inputs (i.e., via the neutral or ground of the AC power connection, or via improperly shielded signaling line circuits). The maintenance activities in progress at the time of the accident involved disconnecting breakers using 110 volt DC controls. Disconnecting the AC power or a fault in the DC control system could provide a transient voltage. The deviations between the system wiring and the manufacturer's published installation instructions could increase the CO_2 releasing system's susceptibility to induced or imposed transients; and either the interconnections between the switchgear and fire alarm conduit systems or ground could have provided the electrical path.

In response to questions submitted by the Board, the vendor for the panel (Notifier) provided the following information related to panel operation and this accident:

- "There are many possible scenarios that could cause a transient to activate panel circuits without logging the event in history. We believe one prominent possible cause relates to the fact that the AFP-200 is microprocessor-based. Any microprocessor, if sufficiently disturbed by power transients or nearby electromagnetic fields can possible change its program execution. It is possible that the erroneous instructions could include instructions to activate output circuits, including the AFP-200 releasing circuits."

- "Our testing has shown the AFP-200, when used with the separate NR45 charger, can be perturbed momentarily by an AC power loss or an AC voltage transient. When this perturbation occurs, it is possible that the output circuits could momentarily activate."

Testing has shown that a loss of AC power or AC voltage transient can activate the fire panel output circuits (open carbon dioxide solenoid valves).

These responses indicate that the vendor was aware of the potential for an inadvertent output signal from the fire panel on an AC power transient such as the shutdown of the 4160 volt bus, and a resulting activation of the carbon dioxide system solenoids and system discharge. This information, however, was apparently not communicated to INEEL during the panel installation in 1997 or through a vendor notice or bulletin.

This vendor response to the Board also cautioned on the use of the fire panel software circuits to provide protection for personnel:

- "The disable function for Notification Appliance Circuits is via software logic. Disable does not physically open the circuit."

- "NFPA 72 (7-1.5.3) requires that releasing circuits be physically secured from inadvertent activation when performing alarm circuit testing. We believe that software disable to carbon dioxide circuits is not sufficient protection during any type of testing with humans in the hazardous area."

Disabling software at the fire panel is not sufficient protection for humans from the carbon dioxide hazard.

- "NFPA 12 (1-5.1.7) also requires lock-out of carbon dioxide systems when persons are in the area. Software disable is not lock-out."

JUDGMENTS OF NEED

LMITCO needs to verify that all gaseous agent fire suppression systems (i.e., CO_2, Halon, FM200, Inergen, etc.) are monitored for discharge in accordance with NFPA Standard 72, *National Fire Alarm Code*. This monitoring should be configured to assure positive notification to building occupants in sufficient time to allow evacuation of the protected area prior to system discharge. With respect to total flooding CO_2 systems, the combination of a discharge pressure switch and a mechanical discharge delay should be considered.

LMITCO needs to verify the qualifications of its fire protection design personnel, ensure that all fire protection contracts address required contractor submittals, ensure that those submittals receive qualified review prior to acceptance, re-evaluate acceptance testing procedures, and ensure that all required re-acceptance testing is in fact performed.

LMITCO needs to update fire protection system drawings and keep them updated to reflect modifications in the as-built plant.

ID, in its capacity as the "Authority Having Jurisdiction" with respect to fire protection, needs to strengthen its review of fire protection design and design modifications to ensure compliance with applicable requirements, codes, and standards.

LMITCO needs to determine the specific mechanism by which the CO_2 system in Building 648 discharged on July 28, 1998, and take actions as appropriate to avoid a recurrence in the future. Until this is done, the CO_2 system in Building 648 should remain out of service and compensatory fire protective measures implemented, as appropriate.

LMITCO needs to conduct a risk benefit analysis on the continued need for CO_2 fire suppression systems at INEEL and to evaluate the necessity of using total flooding CO_2 for fire suppression in occupied spaces. Where alternatives are not practical for cost or other reasons, facilities should comply with NFPA 101, *Life Safety Code* requirements for high hazard industrial occupancies and all safety-related requirements of NFPA 12 should be strictly enforced. DOE needs to consider implementing a similar policy across the complex, including re-evaluation on a risk-benefit basis as the mission or status of facilities changes.

3.3 TRAINING AND COMPETENCY

LMITCO implements DOE Order 5480.20A, *Personnel Selection, Qualification and Training Requirements for DOE Nuclear Facilities*, requirements through the Advanced Test Reactor Training Implementation Matrix (Issue #005, dated September 18, 1995). This matrix requires trained safety engineers but does not require certification or qualification to any standard, and OSHA and NFPA training requirements are not specified.

Contractor training did not emphasize hazards associated with carbon dioxide systems.

LMITCO requires each employee to attend General Employee Training, which discusses hazards associated with energized systems, radiation sources, chemical use and storage, and hazardous wastes, as a condition of employment. Although both the Hazard Communication Program and General Employee Training address many of the hazards encountered at INEEL, they do not emphasize hazards associated with CO_2 systems. In addition, LMITCO and Lockheed Martin corporate policies and safety manuals do not specifically address the hazard of CO_2 fire suppression systems or define the necessary level of training, hazard mitigation, and emergency preparedness and response as specified in NFPA Standard 12.

The need for training on the hazards associated with the CO_2 suppression system at TRA was noted in 1996 in the LMITCO Multi-Discipline Independent Performance Assessment Report (96-MDA-037) that stated under finding QA-003:

> "Proper indoctrination would inform all personnel as to their personal responsibilities to use and comply with approved LMITCO procedures and identify any additional site specific procedures that may be invoked. As part of this indoctrination (especially site specific portions) new and matrixed personnel could be informed about area hazards like the carbon dioxide fire suppression system still in operation at ETR. (Potential Price Anderson Violation)."

A need for training on carbon dioxide hazards was a finding in a contractor's performance assessment report in 1996, but the training was not implemented.

Management Control Procedure MCP-27, Preparation and Administration of Individual Training Plans, was developed in response to this finding, and the corrective action was closed. However, workers involved in the accident had not received training on the hazards associated with the CO_2 suppression system at ETR. The LMITCO training needs assessments failed to identify the CO_2 hazard, even though that hazard was used as

an example to develop the finding, and the hazard was never incorporated into General Employee Training or indoctrination training for new and matrixed personnel.

Aspects of training and competency that relate to the accident include:

Training and competency were issues in the accident.

- Training provided by LMITCO on fire protection systems was limited in scope:
  - Training on fire protection systems modifications was conducted for operations personnel during Retraining Session 6 in 1996. Utility area operators received a walkthrough on the new fire panel functions in 1997. This training was limited and emphasized electronic features of the panel without discussion of the associated safety requirements.
  - Training had been conducted on Management Control Procedure MPC-585, Managing Fire Protection Impairments, for operations and safety personnel at TRA. The training was conducted as required reading.
- Safety professionals, line managers, and the planner for the work conducted on July 28, 1998, did not analyze the hazards and identify the controls associated with the CO_2 fire suppression system during the work planning process.
- The work planner had not yet received training on the Job Requirements Checklist, a corrective action to a previous Type A accident investigation and a tool intended to assure a thorough hazard identification.
- The design concentration of CO_2 used for fire protection in Building 648 is potentially lethal, but personnel had not been trained on the risk, alarm recognition, or immediate emergency response.
- Workers, planners, and line managers were not cognizant of personnel protection measures contained in 29 CFR 1910, Subpart L and NFPA Standard 12, which would have alerted them to hazards associated with CO_2 fixed fire suppression systems and mitigation measures that could have been employed in the event of an accidental release of CO_2 from the fire suppression system.

Workers in Building 648 had not been trained on the risk, alarm recognition, or immediate response associated with the potentially lethal carbon dioxide hazard.

The TRA Utility Area Operators have a required signoff on the ETR CO_2 fire suppression system as part of initial qualification. The training is conducted as on-the-job training. LMITCO training personnel indicated that training on CO_2 fire suppression systems was not required for other personnel.

Material Safety Data Sheets are used to communicate workplace hazards as part of LMITCO's Hazards Communication Program, contained in Management Control Procedure MCP-2715, Hazard Communication. This program includes a Material Safety Data Sheet for CO_2 that identifies health hazards and personal protection equipment requirements, but it was not used for work planning prior to the accident.

Personnel involved in work planning did not understand the need to physically isolate the fire suppression system or the limitations of electronic impairment for personnel protection.

General Employee Training also emphasizes LMITCO's lockout/tagout policy requiring methods to ensure that employees are protected from unexpected releases of hazardous sources of energy. This policy is implemented by Management Control Procedure MCP-1059, Lockout and Tagout, which is intended to meet the requirements of 29 CFR 1910.147 and DOE Order 5480.19, *Conduct of Operations Requirements for DOE Facilities*. LMITCO determined that energized systems were a sitewide hazard to all employees and performed sitewide lockout/tagout training in 1997 following the 1996 Type A electrical shock accident at TRA. The purpose of the training was to ensure that employees understood the proper isolation methods for energized systems, and affected employees were required to attend. The training plans and materials discuss the hazards associated with energized systems as defined by 29 CFR 1910.147, but do not discuss isolation of the CO_2 system or differences in level of personnel protection provided by impairment, lockout/tagout, or disarming or disabling the energized systems. Personnel involved in the work planning process had LMITCO lockout/tagout training but failed to recognize that the Building 648 CO_2 fire suppression system needed to be physically isolated, not electronically impaired. Further, some individuals involved in the work at the job pre-briefing did not have sufficient understanding of the term "impairment" and its limitations for personnel protection, and believed that the CO_2 system would be unable to activate under any circumstances.

While General Employee Training specifically addresses LMITCO expectations for control of energized systems having potential for accidental discharge, it does not address personnel protection measures associated with CO_2 releases into an occupied

work environment, CO_2 warning signs, alarm familiarization, and safe evacuation in case of an accidental discharge.

Analysis. From the design and installation through the implementation of the work, there was insufficient knowledge or competence at all levels to prevent the accident from occurring. LMITCO engineering staff involved in the design, installation, and approval of the design and installation changes did not understand the significance of these changes on controlling the hazard and on worker safety (see Section 3.2). Line managers, planners, engineers, supervisors, and workers associated with the work did not understand the hazards associated with CO_2, nor did they have sufficient knowledge of the requirements for dealing with the hazards. Knowledge about the CO_2 hazard was not institutionalized through procedures or work planning and control processes. The knowledge base was dependent on an expert-based system, as opposed to a standards-based system that relies on disciplined, documented processes. Thus, the competencies for dealing with the hazard were not integrated across the site. This is the reason that, for example, work planners, the safety engineer, and the fire protection engineer placed an over-reliance on a pre-discharge alarm and electronic impairment of the CO_2 system to protect personnel.

There was insufficient knowledge or competence related to the carbon dioxide hazard at all organizational levels.

The training programs used by LMITCO either did not address the hazard, or failed to identify the requirements for dealing with CO_2 hazards, or both. There is a relationship between these inadequacies and the requirements management program and how the requirements flow down through procedures to the activity level. Because the requirements were not institutionalized through procedures and other mechanisms, and were not incorporated into training programs, individual competencies and application of requirements in conducting hazardous work were not assured.

There was insufficient institutionalization of requirements for dealing with carbon dioxide hazards through procedures and training. Thus, competency was not assured.

The LMITCO training program did not effectively address the potentially lethal CO_2 fire suppression system hazard, and appropriate DOE, OSHA, and NFPA requirements were not incorporated into the training. The program did not meet the Lockheed Martin corporate environment, safety, and health (ES&H) policy requirement to implement a training program that addresses (1) supervisor awareness of safety and hazards and correct methods to prevent injuries/illnesses, and (2) employee training on specific hazards and control measures relevant to job tasks and work processes. Workers (including electricians from Site Support Services) were not provided with sufficient training to understand the hazard, the acceptable means of lockout and

worker protection, or the necessary preparation, recognition, and emergency response to an accidental or valid initiation of the CO_2 system. The workers believed they were using safe work practices, and there was no need to stop work activities for safety reasons.

RELATED CAUSAL FACTORS

A contributing cause of the accident was that competency of staff at all levels to deal with CO_2 hazards was not assured by LMITCO. Those involved with the CO_2 fire suppression system failed to understand the necessary requirements and procedures at the design, work planning and control, and implementation stages of the work at the sitewide, facility and activity levels.

JUDGMENTS OF NEED

LMITCO needs to institutionalize training and incorporate information about CO_2 hazards into INEEL training programs. This should include:

- **CO_2 hazard recognition (including pre-discharge alarm recognition)**
- **Emergency preparedness and immediate response and rescue to CO_2 discharges**
- **Egress requirements and CO_2 evacuation drills for all personnel performing work in buildings protected with CO_2 flood systems**
- **Clarification on the limitations of system impairments for personnel protection, and the use of lockout/tagout**

LMITCO needs to provide training for work planners, fire protection engineers and safety engineers in industry requirements related to CO_2 including personal protection, warning signs, clear exit pathways, and preparations for immediate rescue.

LMITCO needs to conduct sitewide lessons learned training on the root causes and corrective actions associated with this accident, including those related to the level of hazard, protective lockout, emergency preparedness, and immediate response.

3.4 WORK PLANNING AND CONTROL

System Description

The LMITCO process for planning and controlling maintenance work activities has been the subject of much scrutiny over the last few years. Incorporation of corrective actions from two previous Type A accident investigations and several assessments, and

The contractor's work planning and control process has changed as a result of scrutiny over the last few years.

efforts to incorporate Enhanced Work Planning, have all led to recent changes in the work control process. The process, in general, assigns responsibilities; provides criteria to select from two levels of work control (minor maintenance and work order maintenance); provides instructions for preparing and reviewing work, level and types of hazard analysis; and provides a Job Requirements Checklist to be used on a graded approach, approvals and authorization to start work, pre-job briefings, scope changes, post maintenance testing, and closure. The Job Requirements Checklist provides a mechanism to assist in determining the level and type of hazards review and identifying the appropriate expertise to be integrated into the process.

At the institutional level, the LMITCO Integrated Requirements Management Program provides the infrastructure for flowdown of requirements from laws, regulations, and DOE Orders specified in the contract between DOE and LMITCO to the activity level. The program is intended to ensure that a mechanism is in place to implement these requirements. Functional area managers and subject matter experts are assigned to evaluate the site work activities, identify associated hazards and vulnerabilities, and review these against relevant external requirements, non-mandatory consensus standards, Nuclear Regulatory Commission Guides, and industry best management practices. These requirements are then implemented through company-level procedures, facility-specific procedures, training, or other administrative controls. Company-level procedures are generally used if multiple facilities or activities are involved.

A variety of documents guide the conduct of work in Building 648.

The ETR Safety Analysis Report (SAR) analyzes both radiological and industrial hazards for the facility and establishes both design and administrative controls for these hazards. The ETR Surveillance and Maintenance Manual further provides instructions for security, operation, and maintenance of in-service equipment. Table 3-2 is an example comparison of external NFPA personnel safety requirements and guidance for the CO_2 fire suppression systems, and how they were addressed in site documentation from the institutional to the work activity level for the work that was ongoing at the time of the accident.

Building 648 is included in the ETR SAR. Responsibility for Building 648 had recently been transferred from Reactor Programs to the TRA landlord organization. The TRA site landlord organization relied on Reactor Operations for operations and ES&H support. Maintenance, including electricians for the preventive maintenance activity in progress at the time of the

accident, is the responsibility of Site Support Services. This was a recent change.

Facts and Discussion

Integrated safety management includes five core functions.

Integrated safety management activities include five core functions: (1) define the scope of work; (2) identify and analyze the hazards associated with the work; (3) develop and implement hazard controls; (4) perform work safely within the controls; and (5) provide feedback on adequacy of controls and continuous improvement in defining and planning the work.

These five functions provide the necessary structure for any work activity that could potentially affect the public, the workers, and the environment. The discussion that follows analyzes work planning and controls associated with the accident in the context of these five core functions.

Sitewide safety documents do not adequately address the carbon dioxide hazard.

Define the Work. At the institutional level, sitewide safety documents do not reflect that work is performed in areas with CO_2 fire suppression system coverage. Review of facility-level documentation revealed that the ETR SAR generally describes the work activities for the facility. The SAR was outdated and did not address modifications that had been made to the CO_2 system in Building 648. At the activity level, the work to be performed was four-year preventive maintenance on breakers and relays in Building 648. Maintenance Work Order No. 800416, "Perform 4Y PM on High Voltage Switchgear" described the work as four-year preventive maintenance on the TRA-648 4160 volt switchgear breakers, relays, and buses. The Work Order provided adequate instructions to perform these tasks. Outage Request TRA183 identified additional work associated with this activity as follows:

- Secure the TRA-680 diesel generator by placing the selector switch in the off position
- Shut down and restart multiple air conditioner and heat pump units
- Impair the dry pipe sprinkler systems in Buildings 642, 643, and 648 and return these systems to service
- Restart the ETR heat exchanger building, battery room, and cubical exhaust fans.

Identify and Analyze the Hazards. At the institutional level, the INEEL Safety and Health Manual does not discuss CO_2 hazards. The ETR SAR identified CO_2 as a hazard, identified the areas of

Table 3-2. Flowdown of Personnel Safety Requirements for CO_2 Systems

External Requirements - NFPA 12 - Carbon Dioxide Extinguishing Systems*

1. Warning signs at entryways to protected spaces and adjacent areas where the CO_2 could migrate.
2. All persons that can enter the space shall be warned of the hazards, given the alarm signal, and provided with safe evacuation procedures.
3. The pre-discharge warning signal shall provide significant time delay to allow for evacuation under worst case conditions.
4. All personnel shall be informed that discharge directly at a person will cause eye injury, ear injury, or even falls due to loss of balance upon impingement
5. To prevent accidental or deliberate discharge, a "lock-out" shall be provided when persons not familiar with the system are present in a protected space.
6. Consideration shall be given to the possibility that personnel could be trapped or enter into an atmosphere made hazardous by discharge. Suitable safeguards shall be provided to ensure prompt evacuation, to prevent entry into such atmospheres, and to provide means for prompt rescue of any trapped personnel. Personnel training shall be provided. Pre-discharge alarms shall be provided.

Additional information in NFPA 12, Appendix A indicates consideration should be given to :

1. Adequate aisleways and routes of exit kept clear at all times
2. Necessary additional or emergency lighting and directional signals to support quick safe evacuation
3. Only outwardly swinging self closing doors at exits with provisions for panic hardware as necessary
4. Continuous alarms at entrances until the atmosphere has been returned to normal
5. Odor added to the CO_2 so that such atmospheres can be recognized
6. Warning and instruction signs at entrances and within areas
7. Prompt discovery and rescue of persons rendered unconscious in such areas (This can be accomplished by search by trained personnel with appropriate breathing apparatus immediately after discharge stops)
8. Instruction and drills for all personnel within the area including maintenance construction personnel that may work in the area.
9. Means for prompt ventilation of such areas
10. Other steps or safeguards that are necessary to prevent injury or death based on careful study of each particular situation
11. It is recommended that self-contained breathing apparatus be provided for rescue purposes.

* Invoked by DOE Orders 5480.4, *Environmental Protection, Safety, and Health Protection Standards*, and 5480.7A, *Fire Protection*.

Institutional Documentation

At the institutional level, the Safety and Health Manual is intended to provide interpretation and consolidation of requirements found in external regulatory documents. However, the manual does not incorporate external requirements for personnel protection for CO_2 fire suppression systems.

Facility Documentation

The ETR SAR identified the following controls for the CO_2 system:

- Signs at entryways and within the affected areas to warn personnel of the system and associated hazards. These signs were not installed prior to the accident.
- A sign at the entryway to the cable spreading room (basement) warning personnel that the system must be isolated prior to maintenance in the area.
- An alarm with a 30-second delay to warn personnel of an imminent discharge.

Activity

Maintenance Work Order 800416 (Perform 4Y PM on High Voltage Switchgear) did not identify or reference any controls associated with the CO_2 hazard.

coverage, and stated that the benefit of the system outweighed the risk. It is unclear that this conclusion was supported by a formal risk-benefit analysis following shutdown of the reactor or during system design changes in 1997. Not all information in the SAR is accurate, because it did not address previous modifications to the system. In addition, the SAR does not address the potential for an accidental or manual initiation without a 30-second warning alarm.

The hazards evaluation for the work that led to the accident addressed only electrical hazards.

The hazard evaluation for the Work Order addressed electrical hazards only. It did not acknowledge the CO_2 hazard, the exit pathway obstructions, the number of personnel associated with the work, or emergency response for an unplanned or accidental release of CO_2. The planner is an experienced electrician who had previously performed work in Building 648. Although he was aware of the hazard, he did not recognize the need for any further evaluation based on the assumption that 30-second alarm would signal prior to discharge. Thus, no safety analysis of the hazard was performed.

The preventive maintenance activity was exempted from upgraded work and hazard controls.

The planner did not complete a Job Requirements Checklist, because the work was previously approved preventive maintenance and thus exempted from this process. This is despite the fact that this preventive maintenance had not been performed since 1994, and the fire protection panel has been replaced since maintenance was last performed. Completion of the Job Requirements Checklist would have initiated an interactive, walkdown/tabletop group review of the work. This would have provided an opportunity to identify the hazard, discuss the work conditions (number of personnel, exit paths, etc.), and analyze the hazard. Processing the Job Requirements Checklist would have also required involvement of additional personnel in the planning process, including the Fire Protection Engineer.

A safety professional reviewed the work package and did the work site walkdown during a routine building walkthrough. The planner and work foreman were not part of the walkdown. The safety professional was aware of the CO_2 system; however, he did not see the need to include the CO_2 hazard or controls on the work order, and he signed it.

A pre-job walkdown was performed by the work planner, foreman, and two electricians. During the walkdown, the foreman identified several changes to the work package to improve the electrical safety posture, including de-energizing all the

switchgear during the work. This was a change from previous practices in electrical preventive maintenance. Before, individual breakers were de-energized one at a time. A Job Requirements Checklist was not initiated to review the changes, as required by site procedures. Failure to complete the Checklist at this time precluded another opportunity to review the CO_2 hazard against work conditions or to fully evaluate the impact of total de-energization on safety and emergency management.

The work planning and hazards analyses were not performed in an integrated manner.

The Outage Request for the work (TRA183) included impairment of dry pipe sprinkler systems and implementation of fire watches as a compensatory measure in support of the Work Order. However, processing of the Request required only notification, not approval, of the Fire Protection Engineer. Therefore, he was not included in this portion of the work planning process. An adequate review was not conducted or basis established for the shutdown of the Emergency Control Center diesel generator and total loss of power to the emergency control center.

LMITCO personnel had general awareness of the potentially lethal hazard, as demonstrated by the accompanying text box. This knowledge was never translated into a degree of formal hazard control commensurate with the level of hazard.

Develop and Implement Controls. At the institutional level, the Safety and Health Manual is intended to provide interpretation and consolidation of requirements found in external regulatory documents. However, the Manual does not incorporate NFPA and OSHA requirements for personnel protection for CO_2 fire suppression systems.

Despite institutional opportunities to recognize the carbon dioxide hazard, adequate controls were not specified in site documents and were not developed.

Over the last several years, some conduct of operations requirements were not fully implemented and/or maintained for the ETR, as required in LMITCO Conduct of Operations Conformance Matrices for the Facilities/Utilities/Maintenance Directorate. Examples of conduct of operations shortfalls at ETR directly related to this accident involve procedural compliance, procedure maintenance and upkeep, training, and communication of system status.

Investigation of these issues at the facility level revealed that:

- The ETR SAR does not incorporate all NFPA Standard 12 or OSHA personnel safety requirements.

- The CO_2 fire panel was modified in 1996. After this modification, existing procedures for the system in the ETR Surveillance and Maintenance Manual were not revised and a procedure for operation of the system was not established.

- The Reactor Programs ES&H organization was unaware of any responsibilities for updating the ETR Surveillance and Maintenance Manual procedures, including those for the CO_2 system in Building 648. Individuals involved in the planning for Work Order No. 800416 were not aware of the Surveillance and Maintenance Manual procedures.

At the activity level, Work Order No. 800416 for the activity ongoing at the time of the accident did not include any controls associated with the CO_2 hazard.

Procedures associated with the carbon dioxide fire suppression system were not current or used.

LMITCO Staff Were Aware Of The Potential CO_2 Hazard In Building 648

- In 1978, there was a CO_2 discharge from a building steam leak
- A 1982 maintenance procedure required removal of the control heads as a lockout/tagout of CO_2, during work activities that could activate the system
- Lockout/tagout was not consistently used for the CO_2 system in Building 648 - the removal, and lockout and tagout of the control heads was used in February 1998 for fan maintenance. Two weeks before the accident, an "impairment" was chosen for the same work, but an operator decided at the pre-job briefing to remove (lift) the control heads and perform a lockout/tagout.
- There were signs in the basement warning workers to evacuate through ETR Building and not Building 648 on CO_2 initiation
- Engineers did a "walk-out" test to set the 30-second electronic delay and alarm for CO_2 system
- There was a requirement that the CO_2 system be tagged out for work in cable room (basement of Building 648)
- Caution was given during the pre-job briefing on the need to evacuate on receiving the CO_2 30-second warning alarm
- The Fire Protection Engineer identified the need for a safety barrier (electronic impairment) at the pre-job briefing
- The need to remove the heads from the CO_2 bottles was discussed at the pre-job briefing on July 28, 1998, but the operator raising the issue was assured that electronic impairment at the fire protection panel would prevent the CO_2 system from deluging during the work
- When a new CO_2 system was installed at East Butte, an exterior electronic shutoff and a manual isolation valve were installed in response to worker safety concerns.

At the pre-job briefing, the CO_2 hazard was identified and a decision was made to use a fire protection impairment on the system for additional protection. The system was impaired using the keypad control system and a generic sitewide procedure. A procedure for removing the CO_2 system from service by removal of the electric control heads was available but not used. This procedure was part of the ETR Surveillance and Maintenance Manual and was not current, but had not been officially replaced. Site policy required the use of the lockout/tagout process for protection of personnel from unexpected releases of hazardous energy sources. The lockout/tagout procedure requires physical isolation of the energy source. The work order was not revised to reflect this or sent back for further review, after the hazard was identified during the pre-job briefing.

The carbon dioxide hazard was raised during the pre-job briefing, and the decision was made to electronically "impair" the control system rather than physically disconnect it.

There was poor communication regarding the status of the CO_2 system at the pre-job briefing. Precise terminology was not used. The terms "disable and impair" were used interchangeably to describe the status of the system. The electricians believed that "disable or impair" meant that the system would not release under any conditions or that it was physically prevented from working (i.e., the same as removal of the electronic control heads). The operators and the Fire Protection Engineer understood the meaning of "disable/ impair" to be an electronic blocking of the signal to the solenoids without the removal of the control heads.

The significant limitations of an electronic impairment or software disable for personnel protection were not communicated to the workers at risk.

Outage Request TRA183 removed power to the Emergency Control Center. No special instructions were provided to operate the Emergency Control Center diesel generator to ensure the Incident Response Team van could depart the garage.

Perform Work Safely Within Controls. Workers prepared for and commenced the work activity using prescribed procedures and protective equipment. Without the safety umbrella provided by the positive lockout of the CO_2 system, they were unaware of danger. However, there were some activities that unknowingly impeded mitigation response. These included placing temporary lighting stands, instrument carts, chairs, tables, and rolled out breakers into the 4160 volt switchgear aisle; leaving entry doors on the south and northwest sides of the building closed and locked; and increasing the occupancy level in the building without analysis of the impact on emergency escape, accountability, and search and rescue.

Workers were unaware of the danger and left equipment in exit pathways, impeding egress.

Provide Feedback on Adequacy of Controls and Continuous Improvement. A procedure was written after an actuation of the Building 648 CO_2 system in 1978 to require removal of the electric control heads during maintenance activities that could activate the system. This procedure was still in effect at the time of the accident. However, the procedure has not been updated or consistently used. The basis for the procedure was not captured institutionally. In addition, Occurrence Report ID-LITC-TRA-1995-0014, "Engineering Test Reactor Inadequacies With Potential for Unreviewed Safety Questions," dated February 3, 1997, identified safety concerns at the ETR, including:

- The ETR Surveillance and Maintenance Manual was not current. An updated version of the Manual did not address procedures associated with maintaining the CO_2 system.
- Discrepancies between ETR configuration and the SAR. The requirement to post a CO_2 warning sign on the door to the Cable Spreading Room in Building 648 was identified and verified. However, during a LMITCO review of requirements in the SAR for implementation, the need for signs on entryways to Building 648 was not noted. Consequently, the required signs were not installed.

Previous accident and assessment reports have identified deficiencies in the work planning and control process. Recent evaluations indicate persistent performance deficiencies that have not been addressed.

Previous accident and assessment reports had identified deficiencies in work planning and control.

In 1997, during the review for a new East Butte communications facility, employees identified a concern with the potential hazard associated with the CO_2 fire suppression system. In response to the concern, two additional controls were integrated into the design of the system. These controls included a pushbutton control at the entrance doorway to electronically disable the system and a manual valve in the system to provide physical isolation when personnel are working in the facility. These features were institutionalized in a procedure for accessing the facility. While these additional features were included in the design of the East Butte facility, there was no evidence of any analysis of the need or action to incorporate these features into other CO_2 systems at INEEL, including CO_2 systems in Building 648.

Safety features recently incorporated into another INEEL facility to mitigate carbon dioxide system hazards were not analyzed for relevance to the system in Building 648.

Analysis

Several breakdowns in the work planning and control system contributed to the accident. These breakdowns occurred at the institutional, facility, and activity levels. At the institutional level, the significant hazard associated with CO_2 fire suppression systems was not recognized, and external requirements and guidance were not incorporated into institutional processes to provide direction for mitigation of the hazard. Analysis of the breakdowns in work planning and controls indicates that, while some of the mechanisms applied to work planning and control need improvement, systems already in place were not used. Established procedures were not followed in the work planning and hazard assessment processes. Of particular concern was the use of corporate knowledge or experience, in lieu of institutionalizing information related to hazards and controls. One example of this is the lessons learned from an actuation of the system in 1978, which led to development of a procedure for removal of the CO_2 system from service during maintenance activities. The basis for the procedure and its use were not institutionalized. This led to inconsistent utilization of barriers to protect personnel from inadvertent actuation during work in the facility. The examples cited and the circumstances surrounding the accident are indicative of the informality and inconsistency of hazard analysis and work controls associated with the CO_2 system in Building 648. Evidence collected and analyzed during this investigation, as well as documentation dating back to 1995, indicate that implementation of effective work control processes has not been effective, and for the third time in three years was a causal factor in a serious accident. Thus, it is apparent that ID and LMITCO have continued to accept unstructured work controls for some work activities at INEEL, and this situation is contributing to unnecessary occupational risks to workers.

Lack of structure in the work planning and hazard control process increased the occupational risk to workers.

Continued acceptance of unstructured work and hazard controls at INEEL contributed to the accident.

RELATED CAUSAL FACTORS

Causal factors discussed in Sections 3.1 and 3.5 apply to work planning and controls. This includes one related root cause. These causal factors are presented and discussed in a larger context as to how they relate to management systems and requirements management in those sections and Section 4.0.

The Board concludes that the integrated safety management core functions (or the equivalent) were not employed to achieve a disciplined and structured approach to analyzing and mitigating the CO_2 hazard. The LMITCO Integrated Requirements Management Program was not effective in identifying appropriate requirements and providing a mechanism to implement those requirements. Corrective actions for previous incidents were not effective. The disciplined approach prescribed in company procedures for work control were not used to evaluate the CO_2 hazard or to develop and implement controls. Some procedure requirements such as the use of the Job Requirements Checklist were not followed, and others were not understood. An informal, expert-based approach to work planning and controls was being employed before and at the time of the accident. This was not commensurate with either the level of the hazard or DOE, OSHA, and NFPA requirements and guidance on addressing the hazard. Thus, work planning and control deficiencies significantly contributed to the accident.

An expert-based versus standards-based approach was used to analyze and control the carbon dioxide hazard.

JUDGMENTS OF NEED

LMITCO needs to provide additional management attention to assure the effectiveness of the work control system. This includes direct involvement of knowledgeable managers in review of work and coaching individuals on implementation of the system.

LMITCO needs to improve the work control system by providing additional guidance on the performance of hazard evaluations, to include the importance of capturing all potential and credible hazards associated with the work or workspace and the significance of risks created by the hazards; requiring utilization of the Job Requirements Checklist process for applicable preventive maintenance tasks that have not yet been through the process; and expediting the training and qualification program for work planners (in the interim, ensure only qualified personnel are used for this function.)

LMITCO needs to assure that safety basis documentation and procedures for inactive facilities are updated, maintained and appropriately used.

LMITCO needs to provide additional guidance in the outage request procedure to assure documentation of any controls associated with outages that may impact safety and to provide additional guidance to assure that appropriate personnel such as the fire protection engineer are included in the outage planning process when appropriate.

3.5 MANAGEMENT SYSTEMS

Background

ID has contracted with LMITCO to manage and operate INEEL. The current contract integrates five independent contracts into a single contract to achieve cost savings and to consolidate common functions for consistent, sitewide implementation of policies, practices, and procedures. The LMITCO contract includes the following partners with Lockheed Martin: Duke Engineering, Waste Management Federal Services, Parson Environmental, and Babcock and Wilcox. Contractor senior management consists of personnel from all of the partners; in addition, the partners brought in more than 70 managers to assist in the contract transition.

The infrastructure for flowdown of requirements from the contract, laws, and regulations is the Integrated Requirements Management Program. It is intended to assure that requirements are implemented throughout INEEL (see the "System Description" narrative in Section 3.4). The company-level process for flowdown of requirements into implementing documents is described in Management Control Procedure MCP-2447, Requirements Management.

Both Department of Energy and contractor line management perform oversight of safety performance.

ID performs oversight at INEEL by monitoring and evaluating the performance of LMITCO using both line organization staff and independent staff, in accordance with ID Notice 450.A, *Environment, Safety, Health and Quality Assurance Oversight.* The ID line organization at TRA has three dedicated Facility Representatives to provide direct oversight of LMITCO operations. The ID Policy and Assurance Division, independent of the line organization, performs management assessments and independent safety and quality assurance reviews of both ID and LMITCO. The surveillance, appraisal, and management assessment reports are transmitted to the contractor and the ID line organizations for corrective action development, tracking, and closure.

Contractor line management self-assessments and independent assessments, are governed by LMITCO Management Control Procedure MCP-4, Business Assessments. This process employs a series of assessment plans for each aspect of contractor operations, including management and independent assessments, independent audits, worker assessments, surveillance, readiness

reviews, internal audits, performance measures, benchmarking, and continuous improvement processes.

Discussion and Analysis

Processes to address identified deficiencies in work planning and control have not been applied consistently.

Previous serious accidents, Type A Accident investigations, and assessments over the last three years have indicated serious and continuing weaknesses in work planning and control at INEEL. Examples of these precursor indicators are presented in the text box on ID and LMITCO corrective actions. ID and LMITCO have focused on Enhanced Work Planning as a mechanism for addressing work planning and control deficiencies, such as those identified in the text box. The upgraded work and hazard controls have not been consistently applied to all hazardous work activities. Although ID and LMITCO have directed INEEL facilities to implement Enhanced Work Planning and the Voluntary Protection Program, ID and LMITCO management have not ensured effective and consistent implementation across the site.

Full implementation of the Department's integrated safety management policy is scheduled for 1999.

ID and LMITCO have not been timely in implementing the Department's Integrated Safety Management Policy (DOE P 450.4) despite an identified need. The Integrated Safety Management Plan has not yet been submitted to DOE, and full implementation of the policy, in place for over two years, is not scheduled until September 1999. LMITCO has completed a gap analysis to determine the differential between the existing safety management system and integrated safety management. The gap analysis identified many of the same issues as this accident investigation in areas such as requirements management, procedure use and adherence, issues management, prioritization of resources, work planning and control, and training (see text box). However, resolution of these significant gaps is not scheduled in some cases until 1999.

Consistent application of integrated safety management principles would address many deficiencies.

In many respects, this accident was the complete antithesis of integrated safety management. The significant hazard associated with CO_2 was not analyzed in a structured or integrated manner. The hazard controls that were selected were not appropriate to the level of hazard and relied excessively on the expertise of individuals rather than clear standards and approved procedures. The flowdown and institutionalization of requirements into work control documents were inadequate to ensure that workers had

ID AND LMITCO CORRECTIVE ACTION EFFORTS HAVE BEEN INEFFECTIVE	
February 1996	Type A investigation of a fatal fall at the INEEL identified the failure to implement requirements and procedures as a root cause. The investigation found that contractors did not sufficiently identify or analyze hazards or institute protective measures necessary due to changing conditions.
August 1996	Type A investigation of a non-fatal electric shock accident at the INEEL identified, as a root cause, the lack of an effective management control system for developing and implementing adequate work controls. The need for increased management attention and for increased emphasis on correcting identified problems and compiling guidance for work controls, hazard evaluations, and work packages was also identified.
December 1996	A LMITCO internal quality assurance review indicated there was a failure to provide indoctrination training for new or matrixed personnel on "area hazards like the CO_2 fire suppression system still in operation at ETR." This issue is still unresolved.
April 1997	ID assessment of management systems for maintenance work control revealed several concerns: • LMITCO had not ensured continuity and flowdown of requirements. • Hazard identification activities and job safety analyses did not adequately identify or address potential hazards and appropriate control measures prior to performing work. • There were weaknesses and deficiencies pertaining to the lockout/tagout program. • Communication of ID's expectations for contractor maintenance performance needed improvement.
June 1997	EH reviewed corrective actions for the two Type A accident investigations. The review found that several issues, including procedural compliance and hazards analysis, had been closed with inadequate corrective actions.
May 1998	EH reviewed corrective actions taken in response to a 1995 safety management evaluation and performed a second review of corrective actions taken in response to the two Type A accident investigations. These reviews revealed continuing concerns in hazards analyses and the implementation of procedural requirements.
July 1998	ID conducted a followup review of corrective actions taken in response to its April 1997 assessment of management systems for maintenance work control. Draft reports were issued on July 24, 1998, but had not been finalized at the time of this investigation. Findings included: • Corrective actions for the concern on flowdown of requirements were in progress and scheduled for completion on October 30, 1998. • The concern regarding hazards analysis had been closed but was reopened based on a finding that corrective actions were inadequate. • The concern regarding lockout/tagout had been closed but was reopened based on a finding that corrective actions were inadequate. • Corrective actions had not been taken for the concern regarding the communication of DOE expectations to contractors.

INEEL ANALYSIS OF GAPS BETWEEN CURRENT STATUS AND INTEGRATED SAFETY MANAGEMENT REQUIREMENTS (AS APPLICABLE TO THIS ACCIDENT)

Procedures are not followed or enforced.

The company level process does not require ES&H issues to be addressed concurrently with the prioritization of tasks and allocation of resources.

A consistent standard prioritization process does not exist for proper consideration of ES&H needs in indirect-funded activities.

Prioritization, tracking, analysis and closure for issues and commitments at ID and LMITCO are disjointed and lack effectiveness.

There is no readily understood process for integrating ES&H into work planning and execution.

Implementation of the company-wide quality level system is inconsistent with respect to requirements and requirements flowdown to all activity levels.

There is no consistent, integrated process that utilizes a standardized graded approach to identify hazards and risks, and to establish and apply safety controls.

The ID and LMITCO independent ES&H and quality assurance oversight functions do not provide coverage consistent with requirements.

There is no company-level process that verifies qualification and training.

Senior management oversight functions are not fully effective at managing oversight activities or prioritizing corrective actions.

sufficient knowledge to protect themselves against a potentially lethal hazard. Most fundamentally, LMITCO management systems were not effective in assuring that upgraded work and hazard controls were applied to all hazardous work activities.

Because of the significant weaknesses in INEEL safety management indicated by this accident investigation, the Board overlaid these management system weaknesses on the seven principles of integrated safety management:

Integrated safety management encompasses seven principles.

- Principle #1 - Line Management Responsibility for Safety
- Principle #2 - Clear Roles and Responsibilities
- Principle #3 - Competence Commensurate With Responsibilities
- Principle #4 - Balanced Priorities
- Principle #5 - Identification of Standards and Requirements
- Principle #6 - Hazard Controls
- Principle #7 - Operations Authorization

As discussed in Table 3-3, the accident demonstrates that there were significant weaknesses in meeting all of these principles. Supporting details and examples of these weaknesses are contained elsewhere in this report and not repeated here.

ID and LMITCO management have not been effective in implementing the Department's integrated safety management policy at INEEL.

The accident also indicates that ID and LMITCO have not consistently taken a conservative approach to safety. A number of management decisions associated with the management of change and risk did not have had a documented basis and did not reflect a conservative approach to safety:

- The decision to continue use of a toxic or potentially lethal protection system when the ETR was shut down and again when the decision was made to replace the fire alarm panel

- A LMITCO decision to delay implementation of NFPA personnel protection requirements (LMITCO Functional Area Manager and subject matter experts for fire protection and safety determined that the implementation of the personnel protection requirements from the NFPA standards for CO_2 fire suppression systems could be delayed)

- A decision to make incremental reductions in the INEEL safety infrastructure, including consolidating storage of self-contained breathing apparatus, and discontinuing search and rescue training for the Incident Response Team

A number of management decisions reflect the lack of a conservative approach to safety.

- A decision, based on cost and maintenance considerations, not to operate the Emergency Control Center diesel generator during the power outage

- Decisions to use a single electronic impairment to protect personnel against a lethal hazard, and inadequate response to an employee question about the need for positive isolation on the day of the accident

- The decision that training on the CO_2 hazard was not necessary for workers exposed to the risk

- The decision to exempt this work activity from the upgraded work and hazard controls associated with corrective actions to previous serious accidents and enhanced work planning.

Table 3-3. Integrated Safety Management Principles as Applied to the Accident	
Guiding Principle	**Discussion**
Principle #1 – Line management is directly responsible for the protection of the public, the workers, and the environment, including establishing policies, providing leadership, and empowering workers.	ID and LMITCO leadership have not been effective in implementing corrective actions for precursor accidents and assessments, ensuring a consistent and effective approach to controlling work and associated hazards, or implementing integrated safety management in a timely manner.
Principle #2 – Clear and unambiguous lines of authority and responsibility for assuring safety should be established and maintained at all levels within the Department and its contractors.	ID and LMITCO have not established and implemented the necessary level of management control and accountability to ensure the implementation of applicable requirements and standards, consistent work and hazard controls, and adherence to approved procedures.
Principle #3 – Personnel should possess the experience, knowledge, skills, and abilities that are necessary to discharge their responsibilities.	LMITCO has not provided the necessary level of training or procedures to ensure that design engineers, safety personnel, or workers are sufficiently knowledgeable of the requirements, standards, hazards, protective actions, and immediate response associated with CO_2 systems.
Principle #4 – Resources shall be effectively allocated to address safety, programmatic, and operations considerations, including commitment to ES&H programs and resources, integration of safety into all site activities, and the balanced prioritization of services to mission and safety.	LMITCO did not adequately control incremental reductions in the safety infrastructure, analyze risks and benefits of the CO_2 system under changing conditions, or prepare for an emergency response to an accidental CO_2 initiation.
Principle #5 – Hazards and an agreed upon set of standards shall be identified prior to commencing any work in order to protect workers, the public and the environment, including translation of standards and requirements into implementing documents and authorization of work activities.	Applicable requirements and standards associated with CO_2 systems were not adequately identified, incorporated into design controls, procedures and training programs, or communicated to workers at risk.
Principle #6 – Administrative and engineering controls to prevent and mitigate hazards shall be tailored to the work and hazards involved, including application of the five core functions (define the work, analyze the hazards, control the hazards, work within the controls, and provide feedback for continuous improvement).	LMITCO failed to establish adequate corporate policies and procedures or systems design to control the CO_2 hazard or to apply the core functions of integrated safety management (or equivalent controls) to effectively analyze and mitigate the specific worker hazards associated with the work activity.
Principle #7 – The conditions and requirements to be satisfied for safe operations shall be clearly established and agreed upon, including elements associated with operations authorization.	LMITCO and ID failed to assure adequate configuration management over the CO_2 fire suppression system, including ensuring that the design met requirements and standards, as well as updating the safety analysis report and supporting drawings and procedures to reflect modifications and the present system configuration.

The Board concludes that LMITCO and ID management have not provided the necessary level of leadership and control to prevent or mitigate this serious accident. Leadership has not been effective in achieving corrective actions, benefiting from lessons learned, implementing structured and consistent work controls, ensuring procedure use and compliance, or proactively implementing integrated safety management. An appropriate level of management control has not been achieved through the identification, flowdown, and institutionalization of requirements and standards into policies, design control processes, procedures and system drawings, or quality assurance. Performance feedback, another essential element of management control, has also been deficient because of an absence of management field presence, followup, and accountability.

Management has not exercised an adequate level of leadership and control over worker safety.

In the absence of effective management leadership and control, it will be extremely difficult to achieve the necessary change in organizational behavior and discipline and the understanding, acceptance, and implementation of integrated safety management. Most importantly, the informal work and hazard controls, design errors, safety infrastructure reductions, and failure to use and adhere to procedures could result in another serious and avoidable accident.

RELATED CAUSAL FACTORS

Failure to use administrative barriers (current procedures and work planning and control processes) that implemented regulatory requirements was a contributing cause to the accident.

Another contributing cause to the accident is the failure of LMITCO to take corrective actions and to apply lessons learned from previous accident investigations, particularly in work planning and control; and failure of ID and LMITCO to exercise sufficient monitoring and feedback of this process to ensure correction of major safety deficiencies that are impacting worker safety.

A final contributing cause relating to management systems was failure of ID and LMITCO to adequately evaluate the impact of incremental cost cutting and infrastructure reductions on worker safety.

The first root cause of the accident is that LMITCO did not have a systematic method for identifying, institutionalizing, or implementing requirements for the design, installation, and work conducted on or affected by the CO_2 fire suppression system.

A second root cause of this accident is that ID and LMITCO management has accepted unstructured work controls at INEEL, which contribute to increased industrial safety risks to workers.

JUDGMENTS OF NEED

ID and LMITCO line management need to expedite the implementation of the integrated safety management policy including the need for organizational behavior change, increased leadership and management presence, and accelerated application of core functions to all work activities on site.

ID and LMITCO need to strengthen the INEEL issues management process to assure effective prioritization and tracking of issues, identification and resolution of understanding management system weaknesses, and field followup, performance-based validation, and closure of corrective actions.

LMITCO needs to strengthen the contribution of procedures to safety management and the consistent implementation of safety requirements and policies through accelerated updating and quality improvement, field validation, and a deliberate approach to assure consistent use and compliance.

ID and LMITCO need to improve analysis and control of incremental reductions in funding for safety infrastructure, including individual as well as cumulative impacts on safety management and emergency preparedness.

LMITCO needs to conduct a risk benefit analysis on the continued need for CO_2 fire suppression systems at INEEL facilities and to evaluate the necessity of using total flooding CO_2 for fire suppression in occupied spaces. Where alternatives are not practical for cost or other reasons, facilities should comply with NFPA Standard 101, *Life Safety Code*, requirements for high hazard occupancies, and all safety-related requirements of NFPA Standard 12 should be strictly enforced. DOE needs to consider implementing a similar policy across the complex, including re-evaluation on a risk benefit basis as the mission status of facilities changes.

ID and LMITCO need to assure effective quality assurance practices are in place to independently verify that system design modifications are accomplished in accordance with all applicable codes and requirements.