TYPE A ACCIDENT
INVESTIGATION BOARD REPORT
OF THE JULY 28, 1998
FATALITY AND MULTIPLE INJURIES
RESULTING FROM RELEASE OF
CARBON DIOXIDE
AT
BUILDING 648, TEST REACTOR AREA
IDAHO NATIONAL ENGINEERING AND ENVIRONMENTAL LABORATORY

September 1998

Office of Oversight
Environment, Safety and Health
U.S. Department of Energy

This report is an independent product of the Type A Accident Investigation Board appointed by Peter N. Brush, Acting Assistant Secretary for Environment, Safety and Health (EH-1).

The Board was appointed to perform a Type A Investigation of this accident and to prepare an investigation report in accordance with DOE 225.1A, *Accident Investigations*.

The discussion of facts, as determined by the Board, and the views expressed in the report do not assume and are not intended to establish the existence of any duty at law on the part of the U.S. Government, its employees or agents, contractors, their employees or agents, or subcontractors at any tier, or any other party.

This report neither determines nor implies liability.

On July 29, 1998, I established a Type A Accident Investigation Board to investigate 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. The Board's responsibilities have been completed with respect to this investigation. The analysis, identification of contributing and root causes, and judgments of need reached during the investigation were performed in accordance with DOE Order 225.1A, *Accident Investigations*.

I accept the findings of the Board and authorize the release of this report for general distribution.

Peter N. Brush
Acting Assistant Secretary
Environment, Safety and Health

9/11/98

Date

This page intentionally blank

TABLE OF CONTENTS

Page

EXHIBITS, FIGURES, AND TABLES

Page

List of Figures

List of Tables

ACRONYMS AND INITIALISMS

AC	Alternating Current
CFR	Code of Federal Regulations
CO_2	Carbon Dioxide
CFR	Code of Federal Regulations
CPR	Cardiopulmonary Resuscitation
DC	Direct Current
DOE	U.S. Department of Energy
ES&H	Environment, Safety, and Health
ETR	Engineering Test Reactor
ID	DOE Idaho Operations Office
INEEL	Idaho National Engineering and Environmental Laboratory
kV	Kilovolts
LMITCO	Lockheed Martin Idaho Technologies Company
NFPA	National Fire Protection Association
OSHA	U.S. Occupational Safety and Health Administration
psi	Pounds per Square Inch
SAR	Safety Analysis Report
TRA	Test Reactor Area

This page intentionally left blank.

EXECUTIVE SUMMARY

On July 28, 1998, an unexpected activation of the high pressure carbon dioxide (CO_2) fire suppression system occurred in Building 648 at the Test Reactor Area of Idaho National Engineering and Environmental Laboratory (INEEL). The accident resulted in one fatality, several life-threatening injuries, and significant risk to the safety of initial rescuers. On the following day, the Department of Energy (DOE) Acting Assistant Secretary for Environment, Safety and Health appointed a Type A Accident Investigation Board to conduct an independent investigation of the accident. This report presents the results of that investigation.

At approximately 6:00 p.m., on Tuesday, July 28, 1998, workers were engaged in de-energizing electrical circuit breakers in preparation for preventive maintenance activity on the electrical system in Building 648. Thirteen people were in the building, including foremen, operators, electricians, and fire protection personnel. As the last electrical circuit breaker was opened, the CO_2 fire suppression system unexpectedly discharged without an evacuation warning alarm. Within seconds, the workers found themselves struggling to escape the potentially lethal atmosphere under near zero visibility and the disorienting effects of CO_2.

The Accident Investigation Board determined that this accident was avoidable. Since March 1996, INEEL has experienced several precursor accidents, including two accidents resulting in Type A investigations. These previous accidents indicated a need to significantly improve work planning and controls, perform hazard evaluations, and develop work packages to assure that appropriate safety requirements are integrated into work control documents and performance of work in the field. Initiatives by INEEL to implement enhanced work planning and the Voluntary Protective Program have not been consistently applied to resolve previous Type A accident investigation judgments of need in work and hazard controls and were not effective in preventing or mitigating the accident. The DOE Idaho Operations Office (ID) and Lockheed Martin Idaho Technologies Company (LMITCO), the site operating contractor, have also not been timely in the implementation of the Department's integrated safety management policy to resolve these chronic work control problems and to improve safety performance. These serious accidents and level of safety performance, in fact, indicate continuing acceptance of an informal, expert-based approach to the control of work and the associated hazards.

LMITCO has not been effective in managing the flowdown of requirements and standards applicable to CO_2 fire suppression systems and worker safety, and institutionalizing these requirements. Not institutionalizing requirements into corporate safety manuals, design control processes, procedures, and training programs contributed to less than adequate knowledge and competencies in dealing with the hazard, an inconsistent and deficient application to design, work planning and control and procedures, and inadequate resource prioritization and allocation. The physical lockout of the CO_2 system to protect these workers, for instance, is a requirement and could have prevented this accident. This barrier, however, has been inconsistently applied, and the procedure which requires it has not been updated and was not used for this work. There are clear requirements for training workers on the hazards of emergency response to CO_2 discharges, but the CO_2 hazard had not been incorporated into LMITCO training programs and, on the day of the accident, workers were not sufficiently aware of the hazard, emergency response measures, or the significant limitations of the protection provided. LMITCO placed excessive reliance on the pre-discharge warning alarm, which was never received, and on electronic impairment of the fire panel to protect the workers.

Once the CO_2 system discharged, instantly flooding the room and creating whiteout conditions, the workers were not provided the necessary means to safely escape, including clear exit pathways, breathing apparatus, emergency exit training, exit pathway lighting, or emergency ventilation. The immediate rescue attempts were impeded by the lethal concentration of CO_2, pathway obstacles, low visibility, and absence of self-contained breathing apparatus. Initial rescuers made heroic but life-threatening entries to rescue fellow workers.

The circumstances that would culminate in this tragic accident began to develop years ago. The CO_2 system design, as installed in 1971 and as modified in 1997, did not include required monitoring of system status to ensure at least a 25-second warning alarm regardless of the source of activation.[1] Failure to re-evaluate the need for this system as the risks changed, the absence of a corporate policy and procedures to mitigate risks posed by CO_2, and incremental cost cutting in the site support infrastructure that reduced the availability of self-contained breathing apparatus and search and rescue training also played a role. Most importantly, despite the previous serious accidents at INEEL, LMITCO and ID leadership has not been effective in institutionalizing and implementing requirements, ensuring timely and effective corrective actions to address work planning and control weaknesses, achieving rigor and discipline in the workplace, or implementing the Department's integrated safety management policy in a timely manner.

The Board concludes that ID has not been aggressive or effective in monitoring contractor performance or adherence to requirements, or in ensuring that corrective actions and improvements in hazard and work controls are completed and consistently applied. The Board also finds that LMITCO did not fulfill its contractual obligation to protect workers from a toxic and potentially lethal hazard by establishing requisite design, policies, procedures, hazard analysis, work controls, communications, personal protective equipment, positive system lockout, and training. The contractor failed to prevent actuation of the CO_2 system in occupied space or, alternatively, to ensure adequate warning and escape time and the ability to accomplish immediate search and rescue without risking additional lives. In the words of one of the seriously injured workers, “It's taken one life. We're lucky it didn’t take more.”

[1] If properly designed, two separate and independent signals should have initiated a warning alarm. The first signal was a 30-second pre-discharge warning alarm that did not function. The second signal was a 25-second warning alarm that should have indicated the system was going to discharge. This signal was not functional because it was not installed, although it was specified in the design.

Table ES-1. Causal Factors and Judgments of Need

Root Causes	Judgments of Need
LMITCO did not have a systematic method for identifying, institutionalizing or implementing requirements for the design, installation, and work conducted or affected by the CO_2 fire suppression system	**LMITCO needs to establish and implement a program that complies with and incorporates all applicable worker protection requirements contained in Occupational Safety and Health Administration regulations, National Fire Protection Association 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 that employees are protected from releases of toxic agents from energized systems.** **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.** **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 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 assure that safety basis documentation and procedures for inactive facilities are updated, maintained, and appropriately used.**
ID and LMITCO management has accepted unstructured work controls at INEEL, which contribute to increased industrial safety risks to workers.	**ID and LMITCO management need to expedite the implementation of 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.** **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 application.**

Table ES-1. Causal Factors and Judgments of Need (continued)

Contributing Causes	Judgments of Need
Faulty design and installation of the fire suppression system, due to failure to implement the 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.	**LMITCO needs to verify that all gaseous agent fire extinguishing 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 update fire protection systems drawings and keep them updated to reflect modifications for the as-built plant.** **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.**
Failure to use physical (lockout/tagout) and administrative barriers (current procedures and work planning and control processes) that implemented regulatory requirements.	**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 personnel protection.** **LMITCO needs to ensure that all total flooding gaseous fire suppression systems at INEEL are equipped with an OSHA complaint positive lockout mechanism that is electrically supervised by the releasing system. DOE needs to consider implementing a similar policy across the complex.** **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 provide additional management attention to assure the effectiveness of the work control system. This includes direct involvement of knowledgeable managers in reviewing work and coaching individuals on implementation of the system.** **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.**
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 at the sitewide, facility, and activity levels.	**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.**

Table ES-1. Causal Factors and Judgments of Need (continued)

Contributing Causes	Judgments of Need
Failure of LMITCO to take corrective actions and 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.	**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.** **ID and LMITCO need to strengthen the INEEL issues management process to assure effective prioritization and tracking of issues, identification and resolution of management system weaknesses, and field follow-up, performance-based validation, and closure of corrective actions.**
Failure to identify, institutionalize, and implement requirements for immediate emergency rescue and response to planned and unplanned CO_2 discharges.	**LMITCO needs to assure the ability to accomplish immediate rescue and response to planned and unplanned CO_2 discharges, including the capability to deal with mass casualties having insufficient oxygen.**
Failure on the part of ID and LMITCO to adequately evaluate the impact of incremental cost cutting and infrastructure reductions on worker safety.	**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 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, *CO_2 Extinguishing Systems,* 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 change.**

This page intentionally blank

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

1.0 INTRODUCTION

1.1 BACKGROUND

On July 28, 1998, thirteen workers were engaged in de-energizing electrical circuit breakers while preparing for preventive maintenance activity on the electrical system in Building 648 (Electrical Building) of the Engineering Test Reactor (ETR) Facility in the Test Reactor Area (TRA) of Idaho National Engineering and Environmental Laboratory (INEEL). At approximately 6:11 p.m., as the last 4160 volt circuit breaker was opened, the carbon dioxide (CO_2) fire suppression system discharged unexpectedly and without warning, instantaneously creating a lethal atmosphere with near zero visibility. The accident resulted in fatal injuries to a contractor electrician, injuries to 12 workers, and potential injuries to two others.

On July 28, 1998, one worker died and 14 others were injured or exposed to carbon dioxide when a fire suppression system discharged unexpectedly.

On July 29, 1998, Peter N. Brush, Acting Assistant Secretary for Environment, Safety and Health, U.S. Department of Energy (DOE), appointed a Type A Accident Investigation Board (referred to as "the Board") to investigate the accident in accordance with DOE Order 225.1A, *Accident Investigations* (see Appendix A).

1.2 FACILITY DESCRIPTION

INEEL is located on 890 square miles of desert in a rural, sparsely populated area of southeastern Idaho. INEEL is a multi-program laboratory whose mission is to integrate engineering and applied science to solve problems relating to environmental management, waste disposition, nuclear technology and application, and national security.

The accident occurred in Building 648 of the Engineering Test Reactor Facility in the Test Reactor Area at Idaho National Engineering and Environmental Laboratory.

The TRA (see Exhibit 1-1) contains an operating test reactor, four inactive research reactors, reactor fuel storage areas, laboratories, and area and site support systems. The ETR Facility consists of a

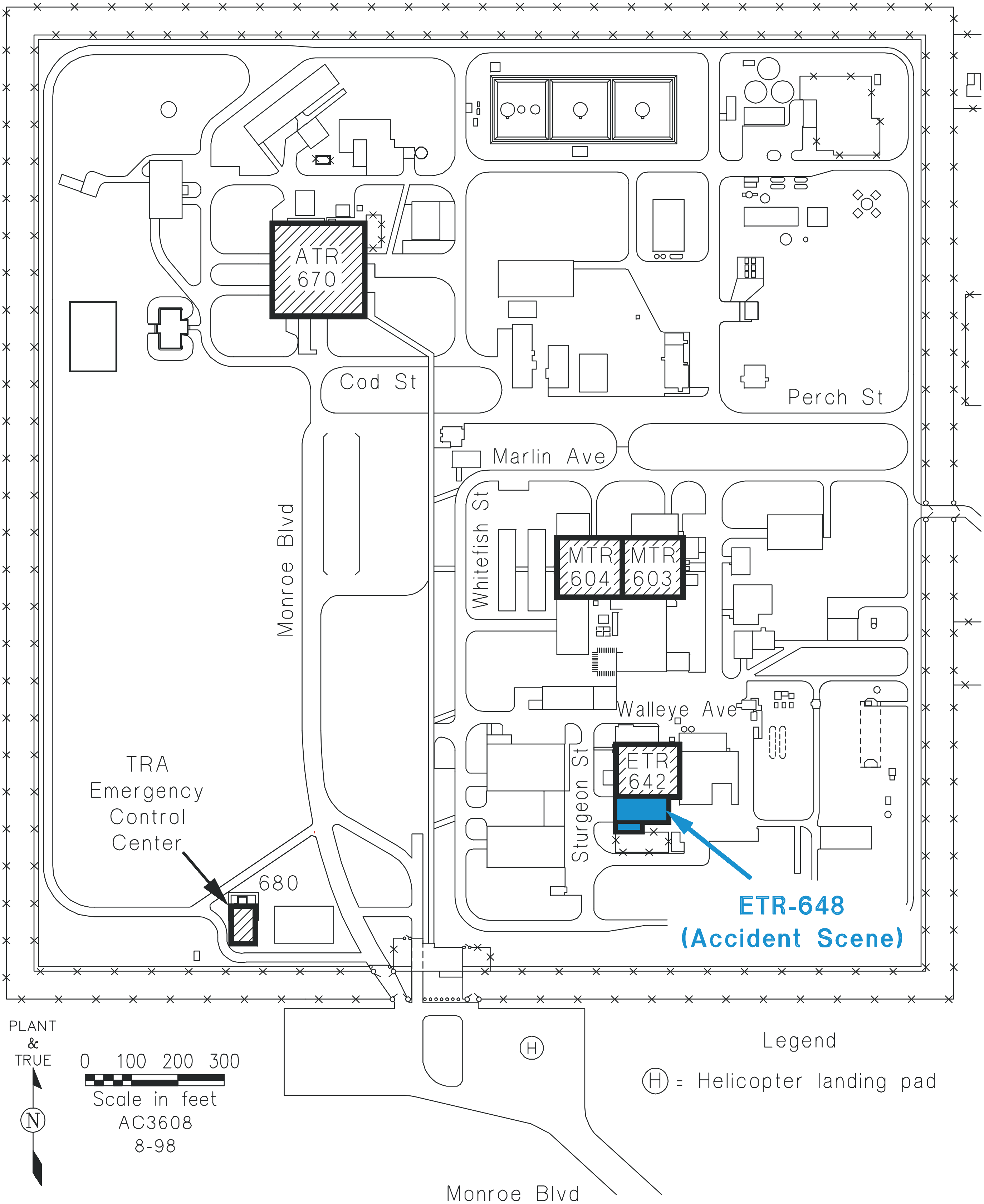


Exhibit 1-1. Site Plan for Test Reactor Area

number of separate buildings that, until it was inactivated in 1982, directly supported the ETR reactor and experimental operations. Building 648 houses electrical equipment for the TRA complex and ETR Facility. It is a two-level structure consisting of the ground-level floor and a basement level that contains electrical cable trays. The accident occurred on the ground level of the building, which contains switchgear, control panels, and power systems.

The electrical components are protected from fire by a CO_2 fire suppression system. When the system is activated, CO_2 is discharged from numerous nozzles in the ceiling of the ground-level floor. The release of CO_2 is controlled by two electronic control heads located in a storage building adjacent to Building 648. Fifty-five 100-pound bottles of CO_2 are also located in the storage building.

The fire suppression system was installed to protect the electrical components housed in Building 648.

Contractor activities at INEEL are managed by the DOE Idaho Operations Office (ID). The facility in which the accident occurred is under the cognizance of the Office of Nuclear Energy, Science and Technology (NE). Lockheed Martin Idaho Technologies Company (LMITCO) is the management and operating contractor for INEEL and for the TRA Facility.

1.3 SCOPE, PURPOSE, AND METHODOLOGY

The Board began its investigation on July 29, 1998, completed the investigation on August 28, 1998, and submitted its report to the Acting Assistant Secretary for Environment, Safety and Health on August 31, 1998.

The Type A accident investigation began on July 29, 1998.

The **scope** of the Board's investigation was to review and analyze the circumstances of the accident to determine its causes. The Board also evaluated the adequacy of safety management systems and work control practices of ID and LMITCO, as they relate to the accident.

The **purposes** of this investigation were to determine the causes of the accident, and to assist DOE in understanding lessons learned to improve safety and reduce the potential for similar accidents at INEEL and across the complex.

The investigation determined the causes of the accident and developed judgments of need to prevent recurrence.

The Board conducted its investigation using the following **methodology:**

Inspecting and photographing the accident scene

- Gathering facts through interviews, document and evidence reviews, and performance testing. The Investigation Board requested and participated in several performance tests:

    - Reenacting the electrical preventive maintenance steps that preceded the CO_2 system discharge, particularly the opening of the eight 4160 volt breakers. The objective was to determine the source of the activation signal to the CO_2 solenoid valves (with the CO_2 system physically disconnected).
    - Examining the manual operation of the chain opener for the Emergency Control Center, where electrical power was not available to open the door and procure the Incident Response Team van and self-contained breathing apparatus.
    - Recommending additional performance testing to further isolate facts regarding CO_2 system activation:

        - The removal of the 25-second mechanical delay from the CO_2 system header and bench testing to verify the length of the time delay. This test is pending.
        - Forensic testing of the CO_2 activation system (equipment and installation). This testing is still in progress.
- Reviewing the emergency and medical response.
- Analyzing facts and identifying causal factors[2] through events and causal factors charting and analysis,[3] barrier analysis,[4] and

---

[2] A causal factor is an event or condition in the accident sequence that contributes to the unwanted result. There are three types of causal factors: **direct cause,** which is the immediate event(s) or condition(s) that caused the accident; **root cause(s),** which is (are) the causal factor(s) that, if corrected, would prevent recurrence of the accident; and **contributing cause(s)**, which are causal factors that collectively with other causes increase the likelihood of an accident, but that individually did not cause the accident.

[3] Events and Causal Factors Analysis includes charting, which depicts the logical sequence of events and conditions (causal factors) that allowed the event to occur and the use of deductive reasoning to determine events or conditions that contributed to the accident.

[4] Barrier analysis reviews hazards, the targets (people or objects) of the hazards, and the controls or barriers that management systems put in place to separate the hazards from the targets. Barriers may be administrative, physical, or supervisory/management.

change analysis[5] to correlate and analyze facts and identify the accident's causes.

- Developing judgments of need for corrective actions to prevent recurrence, based on analysis of the information gathered.

2.0 THE ACCIDENT

2.1 RISKS ASSOCIATED WITH CARBON DIOXIDE

The percentage of CO_2 in the building following the accidental initiation of the fire suppression system was estimated at approximately 50 percent. This is well above the 30 percent minimum concentration necessary for fire protection and is lethal to occupants or individuals, as shown in Figure 2-1. At 50 percent CO_2, the oxygen levels within the building would be approximately 10.5 percent, well below that needed to sustain life. This atmosphere can result in symptoms of nausea; vomiting; near-complete impairment; unconsciousness followed by death and spasmodic breathing; convulsive movements; and death in

The fire suppression system discharged a significant amount of carbon dioxide for fire protection, reducing the amount of oxygen to a life-threatening level.

Facts about Risks Associated with Using Carbon Dioxide as an Extinguishing Agent

- The use of CO_2 is limited primarily by the factors influencing method of application and its intrinsic health hazards.
- At the minimum design concentration (30 percent) for its use as a total flooding fire suppressant, CO_2 is lethal.
- The risk involved with the use of CO_2 systems is based on the fact that the level of CO_2 needed to extinguish fires is many times greater than the lethal concentration.
- Because consequences of exposure happen quickly and without warning, there is little margin for error.
- Although the risk associated with the use of CO_2 for fire protection may be fairly well understood by regulators, standard-setting bodies, and insurers, the risk of CO_2 may not be well understood by maintenance workers who perform maintenance on or around CO_2 systems.
- Since 1975, there have been a total of 63 deaths and 89 injuries resulting from accidents involving the discharge of CO_2 fire extinguishing systems.
- The purpose of a pre-discharge alarm prescribed by the National Fire Protection Association and the Occupational Safety and Health Administration is to allow occupants time to evacuate from an area into which CO_2 will be discharged.
- Evacuation is particularly difficult once discharge begins, because of reduced visibility, the loud noise of discharge, and the disorientation resulting from physiological effects.

Source: *Carbon Dioxide as a Fire Suppressant: Examining the Risks* (Draft)
U.S. Environmental Protection Agency
August 1998

[5] Change analysis is a systematic approach that examines failures in barriers and controls that result from planned or unplanned changes in a system.

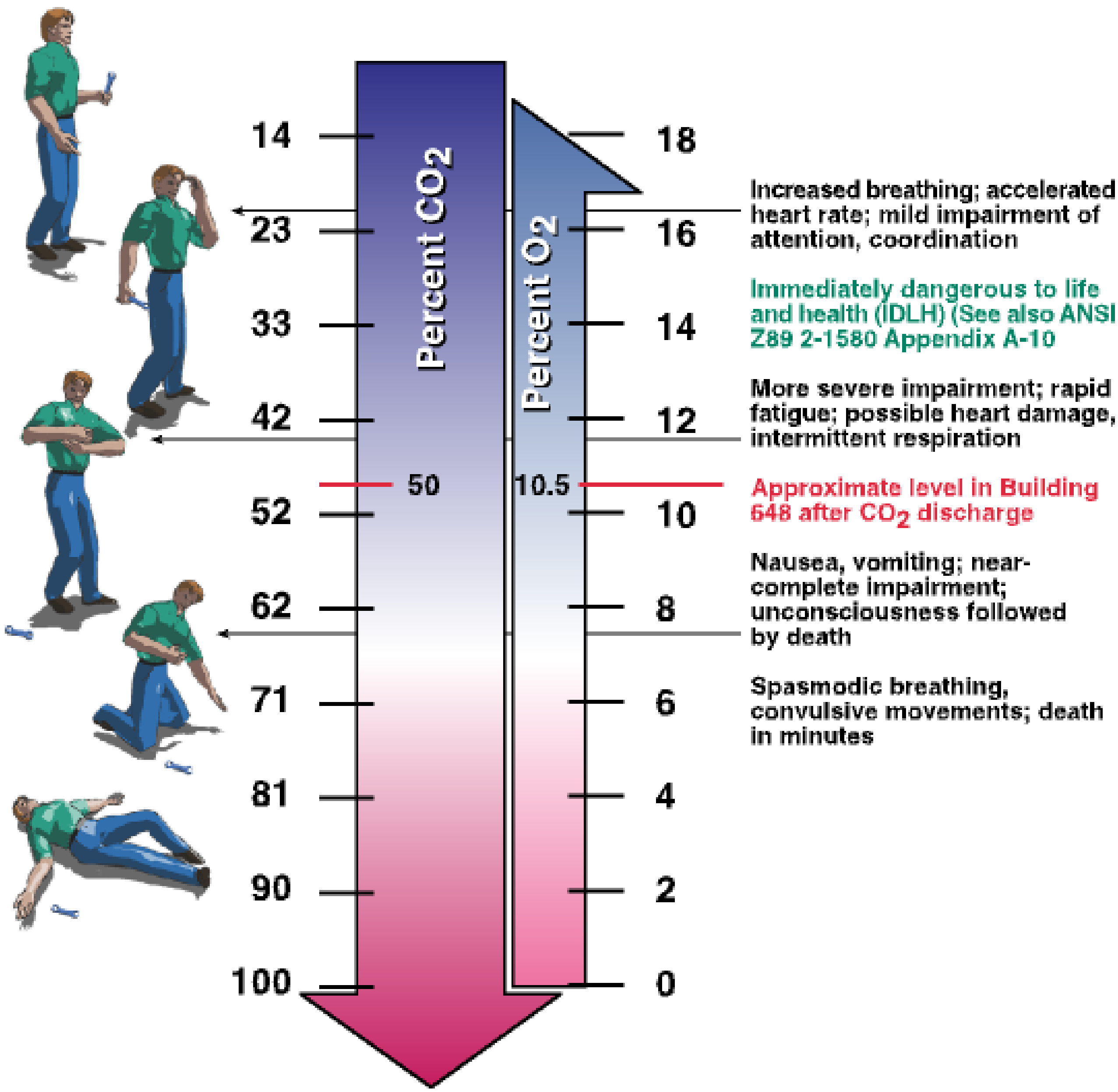


Figure 2-1. Physiological Effects of CO_2 Exposure

minutes. The personnel in the building during the accident experienced vomiting, impairment of actions, spasmodic breathing seizures, and unconsciousness, and their attempts to escape were hindered by the disorienting physiological effects of CO_2.

2.2 ACCIDENT DESCRIPTION AND CHRONOLOGY

Overview. The accident occurred at approximately 6:11 p.m. on Tuesday July 28, 1998, in Building 648 (Electrical Building) of the ETR Facility in the TRA at INEEL. The layout of the building in which the accident occurred, including a schematic of the area depicting the location of injured workers is depicted in Exhibit 2-1. The designations for the workers indicated on the Exhibit (e.g., E-1) correspond to similar citations in the text that follows. At the time of the accident, 13 contractor workers (foremen, operators, electricians, and a fire protection engineer) were in the building.

The accident occurred at 6:11 p.m. on Tuesday, July 28, 1998.

Background. On the afternoon of Tuesday, July 28, 1998, individuals at the TRA were engaged in preparations for a preventive maintenance activity on the Building 648 electrical switchgear. This activity included removal of 4160 volt electrical circuit breakers, vacuuming out breaker cubicles, inspecting ground straps, lubricating racking mechanisms, and basic inspections of the switchgear. This preventive maintenance, which had been changed from a two-year to a four-year frequency, was last conducted in 1994.

Two noteworthy changes had occurred in Building 648 since circuit breaker preventive maintenance was last conducted. A new fire panel was installed as an upgrade to the TRA fire protection system. This new panel controlled the Building 648 high-pressure CO_2 fire suppression system as well as the dry pipe water sprinkler system. In the past, preventive maintenance on these breakers was performed without de-energizing all sections of the 13.8 kV and 4160 volt buses, but rather by de-energizing only sections of the buses as they were being worked on. The decision to de-energize all buses at once for the preventive maintenance in progress at the time of the accident was based on electrical safety considerations.

In support of preventive maintenance being performed on electrical switchgear, the decision was made to de-energize all electrical buses, including the power supply to the fire panel.

Work Planning and Preparation. Building 648 is no longer considered a reactor or process building. In the months prior to the accident, landlord and maintenance responsibility for this facility had been transitioned from Reactor Programs to Site Support Services. On the afternoon of July 28, 1998, the group

The work package and power outage request had been approved the previous day.

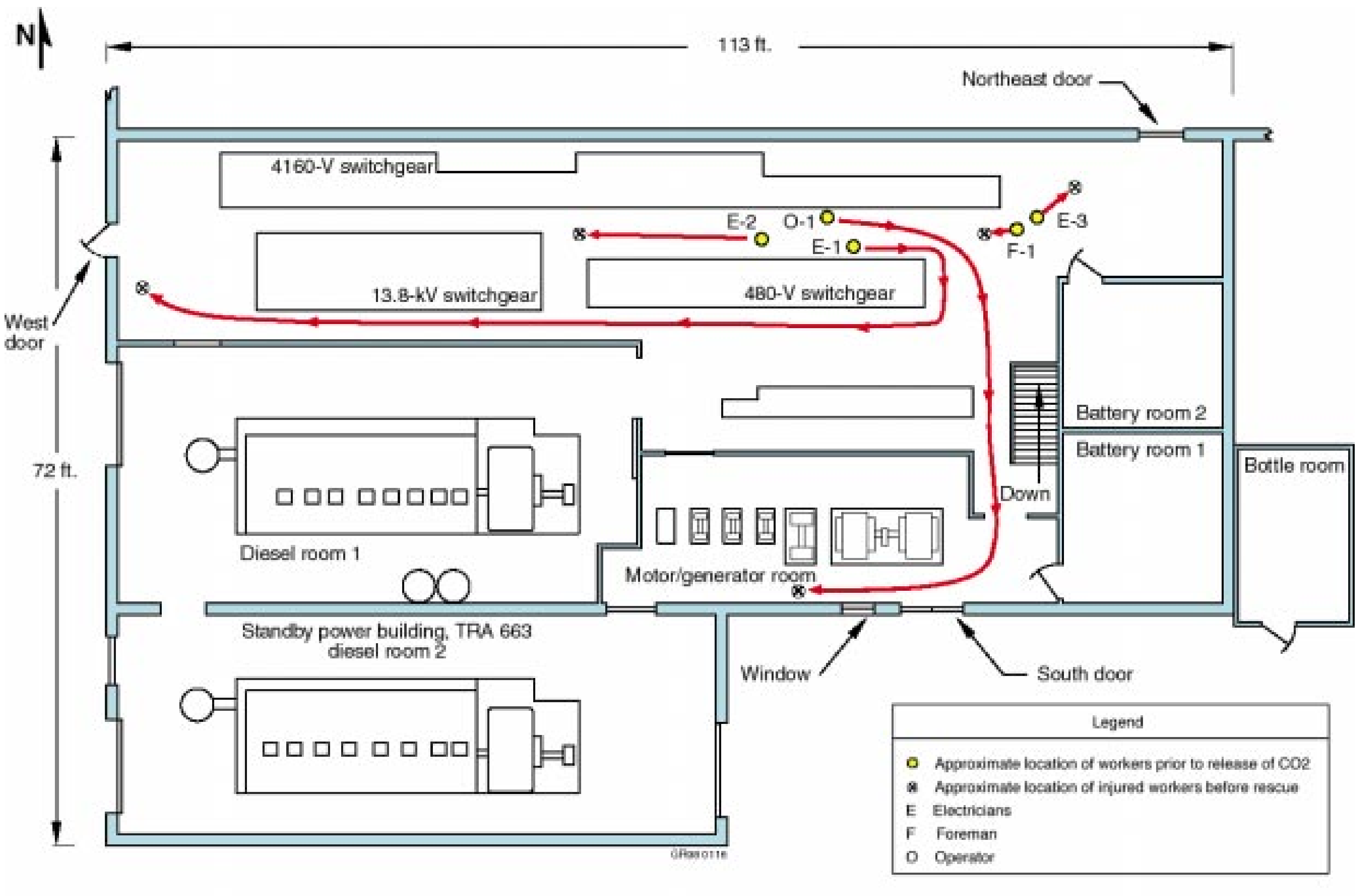


Exhibit 2-1. Building 648 Layout with Escape Routes of Five Injured Workers

designated to be involved in the work activity included a Site Support Services foreman, a TRA foreman, seven electricians from both TRA Operations and Site Support Services, two operators, a utilities operations supervisor, and a fire protection engineer. The work was scheduled after normal working hours to minimize disruptions caused by the loss of power that would occur in conjunction with this work. The power outage impacted several TRA buildings, including the TRA Emergency Control Center. The work package and outage request had been processed and approved on Monday, July 27, 1998.

At the pre-job briefing, a decision was made to disable the fire suppression system electronically, rather than by physical lockout.

At approximately 4:30 p.m., on July 28, 1998, everyone involved in the work met in Building 653 for a pre-job briefing. The scope and approach for the maintenance activity were discussed. The need to complete all work before midnight, due to the need to return the TRA deep well pumps to service, was also discussed. Three teams of two workers each were to be established to accomplish the work within the prescribed schedule. The CO_2 fire suppression system was discussed. It was decided to electronically impair the fire panel signal as a "safety barrier." Impairment, as defined in LMITCO procedures, means any planned or unplanned action that removes automatic protection systems or equipment from service. In this case, it meant disabling the system electronically at the control panel for the system, rather than physically locking out the system. Impairment is a maintenance mechanism for isolating a system; it is not related to personnel protection.

Safety Questions Are Raised. At the pre-job briefing, an operator questioned whether there was a need to remove the electric control heads from the CO_2 bottles to achieve physical isolation and lockout. He was assured that impairment of the alarm panel would preclude the CO_2 system from discharging for any reason during the maintenance activity. The crew broke for lunch at about 4:50 p.m. and agreed to reassemble at about 6:00 p.m. During the intervening period, the remaining requirements of the outage request were completed, and the CO_2 system was impaired.

The Work Begins. At 6:00 p.m. the crew went to Building 648 to begin work preparation. One group of electricians donned high voltage gloves to test the operability of the voltmeter that would be used later for zero voltage checks. This meter had to be tested on an energized position. In the first test attempt, a spare 4160 volt breaker was rolled out into the aisleway, but the meter configuration could not reach energized elements. The group moved to the east end of the 4160 volt bus, where they were able to verify meter operability at the TRA deep well pump breaker position.

About this time, the operators began to open 4160 volt breakers beginning at the west end of the bus and working east. Eight breakers were opened with approximately ten-second pauses between each opening. The total sequence took about one and one-half minutes. The two 13.8 kV breakers were to be opened and locked out next, which would remove all AC electrical power within the building.

The Accident Occurs. At approximately 6:10 p.m., the last breaker in the 4160 volt sequence was opened. The opening of the 4160 volt breakers had gradually eliminated normal building lighting. Lighting was now available from three portable light stands powered by portable generators. At this point, there were a total of 13 workers in Building 648, and a number of them were assembled at the east end of the 4160 volt switchgear.

The last circuit breaker was opened at approximately 6:10 p.m., eliminating normal building power; portable light stands provided lighting.

Within seconds after the opening of the last 4160 volt breaker, the CO_2 fire suppression system unexpectedly discharged and without warning created a lethal atmosphere deprived of oxygen with near zero visibility. Witnesses described hearing a hissing sound and then a “woosh,” followed by “total whiteout” conditions within seconds, in which they could not see anything at all. Most individuals instinctively ran toward the west door by which they entered and which was still open (because cables to the lights were run through it), allowing daylight to shine into the area. Transcribed interviews revealed that escape necessitated groping along switchgear and running into and around obstacles (see Exhibit 2-2). One individual (E-2) describes running into something (perhaps the rolled out 4160 volt breaker), falling down, and then passing out as he took a breath of CO_2.

Within seconds, the fire suppression system discharged, creating a lethal atmosphere and near-zero visibility.

One other individual (O-1) headed in a different direction, through the pump and motor generator room toward an exit door on the south side of the building (Exhibit 2-3). Unable to find the door in the whiteout conditions, he reached a window just past the door. In desperation, he put his hand through the thick glass window embedded with wire, sustaining severe arm lacerations and blood loss before losing consciousness (see Exhibit 2-4). Another individual (E-1) groped along switchgear, only to become entangled in an instrument cart and cable wires en route to the west door (Exhibit 2-5). He tripped, rolled, hit his head, and passed out inside the building.

In the next few minutes, eight workers escaped by groping along the switchgear and dodging obstacles. Five remained in the building.

By this time, eight individuals had escaped the potentially lethal CO_2 fog, and five unconscious individuals were still in the building. One was just south of the west door (E-1), one midway down the 4160 volt aisle (E-2), two at the east end of the 4160 volt bus (F-1 and E-3), and one in the pump and motor generator room on the south side of the building (O-1). (See Exhibit 2-1.)

<u>Consequences of the Accident.</u> A total of 15 personnel received medical treatment or evaluation as a result of the accident. One electrician was fatally injured, and several other workers sustained life-threatening injuries and CO_2 inhalation levels. Sections 2.3.3 and 2.3.4 provide details of the injuries sustained.

One worker died, and several others sustained life-threatening injuries and carbon dioxide inhalation levels.

DIRECT CAUSE

The direct cause of the accident was the inadvertent activation of electric control heads (possibly caused by an electrical transient) that initiated the unexpected release of CO_2 in an occupied space without a pre-discharge warning alarm.

Figure 2-2 summarizes the chronology of significant events leading up to and after the accident.

2.3 EMERGENCY RESPONSE AND MEDICAL EVALUATION

2.3.1 The Initial Emergency Response

Initial emergency response and rescue attempts were conducted by a combination of individuals who had escaped from the building, security police officers, and members of the ATR Incident Response Team. At 6:15 p.m., the Fire Protection Engineer from the work area radioed the alarm center in the INEEL Central Facilities Area approximately 4.6 miles from the TRA, and a fire truck and ambulance were dispatched.

An engineer from the work area called the alarm center at 6:15 p.m., and a fire truck and ambulance were dispatched.

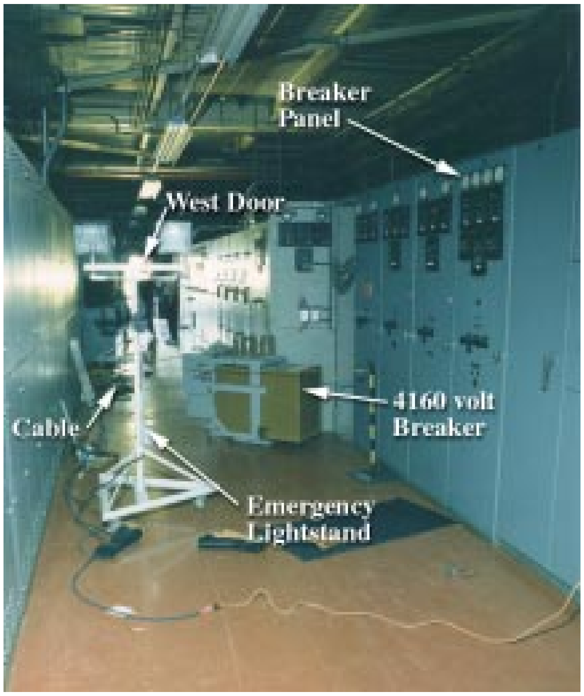


Exhibit 2-2. Switchgear Looking West Toward Exit Door

Exhibit 2-3. Motor Generator Room Near South Door

Exhibit 2-4. Broken Window, South Side

Exhibit 2-5. West Door

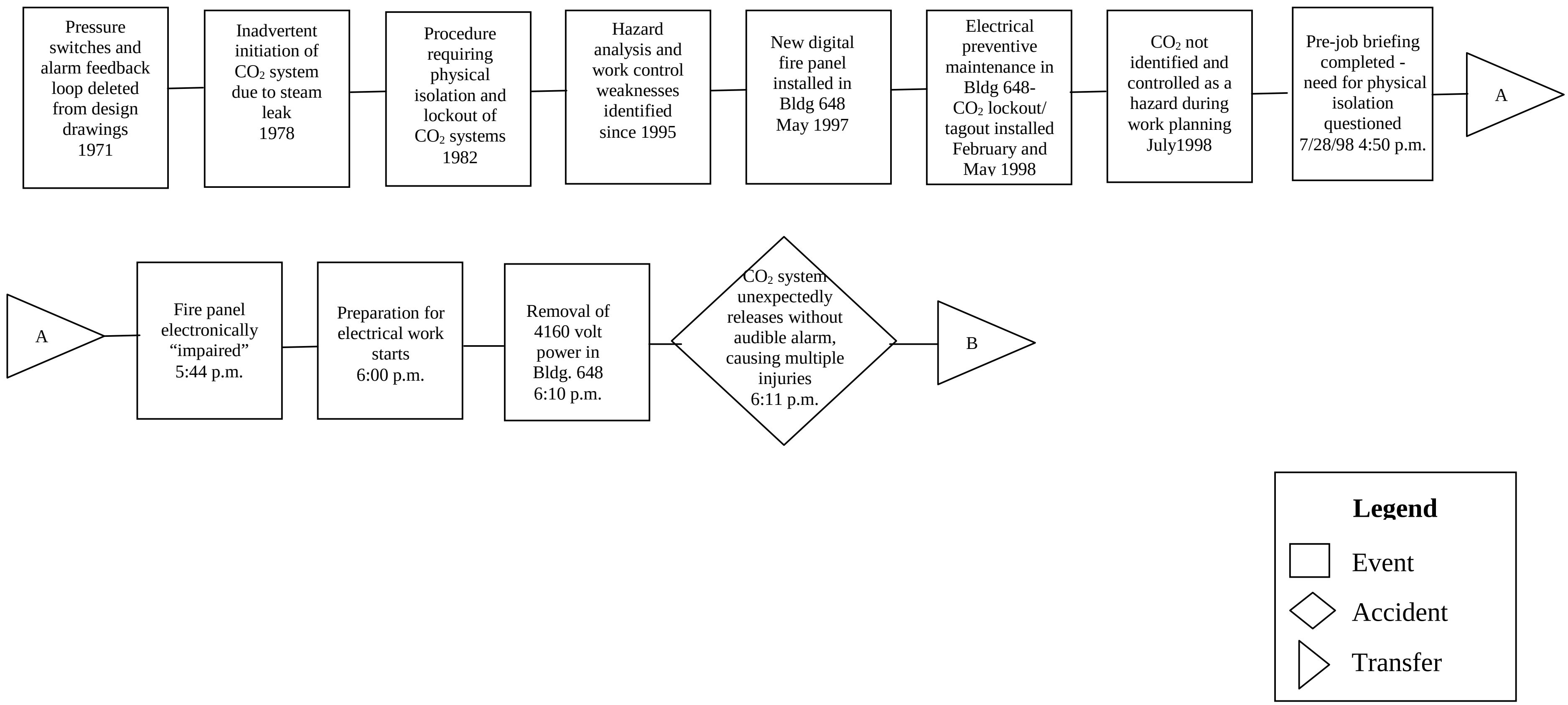
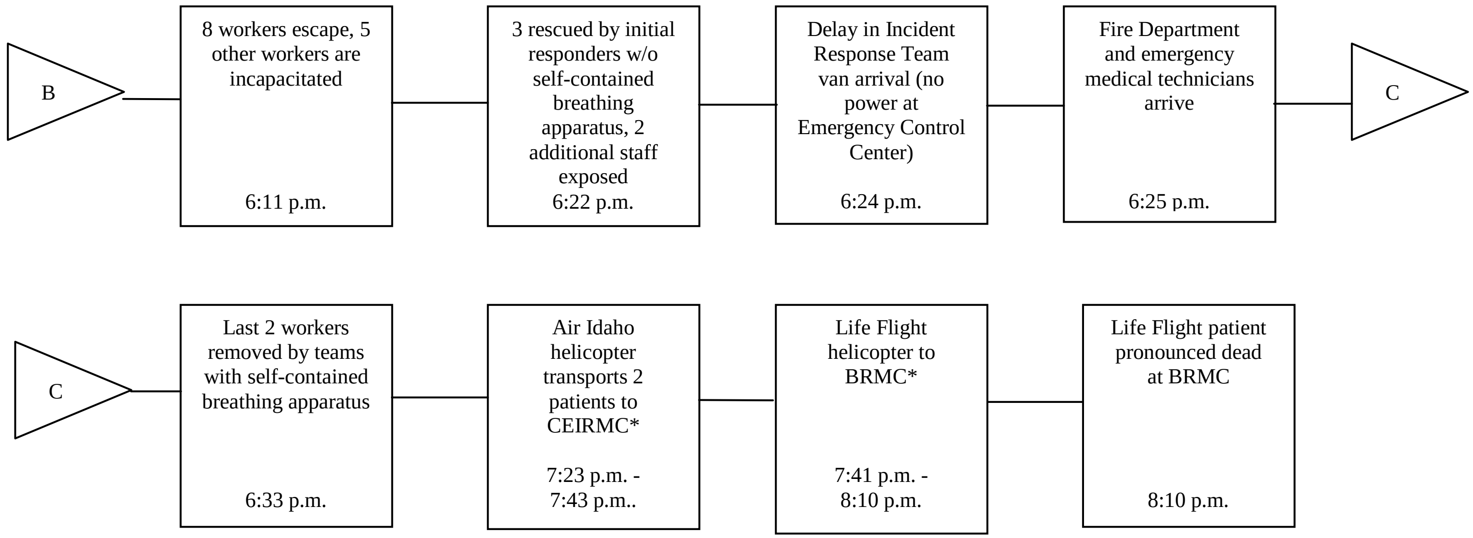


Figure 2-2. Summary Events Chart and Accident Chronology



*CEIRMC - Columbia Eastern Idaho Regional Medical Center (Idaho Falls)
BRMC - Bannock Regional Medical Center (Pocatello)

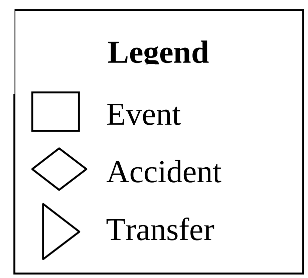


Figure 2-2. Summary Events Chart and Accident Chronology (Continued)

Between the call to Central Facilities Area and arrival of the Fire Department, initial responders proceeded to make repeated attempts to locate and rescue co-workers still trapped in the building. As rescuers gathered at the west door, the hand of an individual appeared out of the fog and rescuers pulled him to safety, as he collapsed in their arms. Rescuers searched for self-contained breathing apparatus[6] to facilitate safe search and rescue, but none were staged or available in the area. An operator was dispatched to the TRA Emergency Control Center to obtain the Incident Response Team van, which contained self-contained breathing apparatus. The power to the Emergency Control Center, however, had been shut off due to the preventive maintenance outage, and the diesel generator was disabled from automatic start. Thus, the garage door could not be opened electrically, and its manual chain opener was inoperable (see Exhibit 2-6). The diesel generator was started after approximately five minutes and the door opened electrically, but this caused a delay in getting self-contained breathing apparatus to the accident scene. Ultimately, the van arrived at Building 648 at 6:24 p.m. Additionally, eleven self-contained breathing apparatus in the Center's break room were not brought to the accident scene. The room used to store the apparatus was dark because of the power outage.

Self-contained breathing apparatus was not readily accessible to the initial responders.

Meanwhile, at the accident scene, two rescuers took a deep breath and went about 15 feet into the building to rescue an injured worker (E-2) who was purple and not breathing, and who went into seizures after rescue. Several attempts were necessary, without the benefit of self-contained breathing apparatus, to rescue another injured party (E-1) tangled up in an instrument cart, cables, and other materials near the west door (see Exhibit 2-5). Rescuers described the effects of the CO_2 as including dizziness, tunnel vision, and disorientation, as they attempted to pull injured parties out while trying to exit for air after short forays into the building.

Rescuers reached several of the unconscious workers, at a risk to their own lives.

[6] Self-contained breathing apparatus is any forced air breathing system that has its own air supply.

Exhibit 2-6. Emergency Control Center Door

Attempting to ventilate the building, two individuals went to the south entrance and were able to jerk open the normally locked doors since the lock was broken. This attempt resulted in rescuing an additional worker lying under the window west of the doors (O-1); during an earlier attempt, he had been obscured by the dense CO_2 fog. Since he was not breathing, cardiopulmonary resuscitation (CPR) was initiated immediately. This was the same worker who had tried to escape by breaking though a glass window, and his severe arm injuries also required immediate medical attention. One individual also went through the ETR Building to reach the exit door in the northeast corner of the switchgear room and chained this door open for ventilation. Two other injured workers in this general area were probably not observed because of the fog and the absence of any temporary or emergency lighting in this corner. One was later rescued and revived (F-1), and the other died en route to the hospital (E-3).

Final rescue attempts reached the last two unconscious workers. One worker died en route to the hospital.

2.3.2 Emergency Response

The text box summarizes the key events involved in emergency response to the accident. Emergency response was activated at 6:15 p.m. on July 28, 1998.

RESPONSE CHRONOLOGY

- **6:25 p.m. - Fire department and ambulance arrive and enter to extricate the last two workers in the building. This occurred within five minutes of arrival.**
- **One of the last two workers rescued (F-1) is successfully triaged with high flow oxygen.**
- **The second of the last two workers (E-3) retrieved is cyanotic (blue) and in full cardiac arrest:**

  - **Difficulty experienced in clearing airway (aspiration)**
  - **Some delay in administering oxygen, due to limited supply**
  - **CPR administered**
  - **Electrical defibrillation at 6:40 p.m. unsuccessful**
  - **Successful intubation is accomplished approximately 28 minutes after the initial CO_2 discharge.**

- **Alert classified at 7:05 p.m.**
- **7:01 p.m and 7:13 p.m. - Air Idaho Rescue and Life Flight helicopters arrive with emergency medical technicians (support also was provided from the INEEL on-call occupational medicine nurse).**
- **7:23 p.m. - 7:43 p.m. - Air Idaho helicopter transfers two patients (O-1 and F-1) to the Columbia Eastern Idaho Regional Medical Center in Idaho Falls.**
- **7:41 p.m. - 8:10 p.m. - Life Flight helicopter transports mortally injured worker (E-3) to the Brannock Regional Medical Center in Pocatello.**

  - **Pacemaker applied and CPR continued in flight**
  - **Pronounced dead at 8:10 p.m.**

- **9:41 p.m.- Eight workers with milder symptoms arrive by van at Columbia Eastern Idaho Regional Medical Center; examined and released.**
- **Two security police officers exposed to CO_2 drive themselves to Columbia Eastern Idaho Regional Medical Center.**
- **Emergency terminated at 12:37 a.m., July 29, 1998.**

2.3.3 Medical Treatment and Prognosis

A total of 15 personnel received medical treatment or evaluation. This includes three employees transported by helicopter, four employees transported by ambulance, six employees transported by van, and two security police officers who drove themselves to Columbia Eastern Idaho Regional Medical Center.

Thirteen workers and two security police officers received medical treatment or evaluation.

Of the 14 surviving employees, 11 were evaluated and treated in the Columbia Eastern Idaho Regional Medical Center Emergency Department and released. The three others were admitted. The operator (O-1) was comatose when admitted, and his respiration had to be supported by a ventilator. He had numerous deep lacerations on his right forearm and hand. A number of muscles and tendons, the radial artery, and the median nerve had been partially severed and were repaired surgically. By July 29, 1998, he was breathing on his own and was removed from the ventilator.

Within the next few days, he came out of the coma and gradually became more alert and oriented. He was able to carry on a conversation, but had a deficit of recent memory. This problem gradually improved. He was able to walk unsteadily, and his speech was somewhat slurred. He was discharged from the hospital on August 5, 1998, and was scheduled for outpatient therapy, including physical therapy, occupational therapy, and speech therapy.

Another injured party (E-2) was not breathing on arrival at the Emergency Department and had to be intubated and his breathing assisted mechanically. He had suffered lacerations his tongue, which he had apparently bitten during a seizure shortly after he was pulled from the building. By the next day, he was breathing on his own and alert. He was discharged on July 31, 1998, and returned to work on August 3, 1998.

The final surviving worker (E-1) who was hospitalized had hit the floor when he fell unconscious, bruising the left side of his head. In the Emergency Department, he was alert and breathing on his own, but was suffering from nausea and vomiting. He was given medication and experienced some sedation and a drop in blood pressure. For this reason, he was transferred to the Intensive Care Unit, but fully recovered by the next day. He was discharged on July 30, 1998, and returned to work on August 3, 1998.

2.3.4 Autopsy Findings and Cause of Death

The injured worker died of asphyxiation.

An autopsy and toxicology screen of the fatally injured worker (E-3) were performed at the Bannock Regional Medical Center and reported by the Bannock County Coroner. The autopsy report was not provided to the Board. However, indications are that the cause of death was asphyxiation complicated by aspiration (inhalation of vomitus).

2.3.5 Analysis

There was no warning alarm before the fire suppression system discharged, and workers' escape paths were impeded by obstacles, carbon dioxide fog, and poor visibility.

No evacuation warning alarm occurred prior to the unexpected CO_2 discharge. Escape from the area was significantly impeded by various pathway obstacles, low visibility, the disorienting effects of CO_2, the failure to designate emergency exit pathways, and inadequate exit path lighting, particularly in the northeast corner and in the pump and motor generator set rooms.

The initial rescue efforts by TRA site personnel—which were crucial, given the concentration and toxicity of the CO_2 atmosphere resulting from the discharge—were impeded by absence of readily available self-contained breathing apparatus. The unavailability of self-contained breathing apparatus resulted in multiple rescue attempts at significant personnel risk, placed the initial responders in the untenable position of having to decide to violate OSHA and LMITCO prohibitions against entry without self-contained breathing apparatus or delay search and rescue until the Fire Department arrived. These individuals elected to risk their own life and safety to rescue fellow workers. Their determination and heroic efforts contributed to three rescues and probably saved the lives of three workers. Had they not been successful, the loss of life might have been much greater and could have included rescuers. These same initial responders also contributed to life-saving activities, including CPR, first aid, and assistance to Fire Department and medical personnel.

The inaccessibility of self-contained breathing apparatus significantly increased the risk of initial rescue attempts.

LMITCO did not establish adequate means for immediate response to lethal levels of CO_2 exposures from an automatic or accidental discharge. and had not adequately considered the need to be prepared for escape from an accidental discharge or to accomplish immediate search and rescue. Prior to the discharge, planning was flawed, preparation inadequate, and equipment was not available to assure safe emergency egress, facilitate immediate search and rescue, or protect workers and initial responders. The decision to not provide electrical power to the TRA Emergency Control Center during the preventive maintenance outage delayed departure of the Incident Response Team van and arrival of the self-contained breathing apparatus at the accident scene. There was also a shortage of oxygen bottles causing delays in administering oxygen to at least one critically injured worker. Although it cannot be concluded that early administration of oxygen could have altered the outcome, its limited availability could have contributed to further fatalities or more serious injuries.

Flawed planning contributed to inadequate immediate search and rescue, workers' difficulty in escaping, and high risk initial rescue efforts.

Barriers designed to and means to facilitate immediate search and rescue were not in place or failed. These included the absence of physical barriers (evacuation warning alarm, personal protective equipment, clear entry/exit pathways, and evacuation lighting) and management barriers (effective immediate rescue and response planning and implementation). Injuries to the workers and immediate response rescuers directly resulted from the unavailability of self-contained breathing apparatus. The barrier failures that created or exacerbated the inability of workers to

Failure of physical and administrative barriers prolonged workers' exposure to the hazard.

escape, or of rescuers to rapidly enter/leave the area, contributed to the severity of the injuries received by the workers, because it prolonged their exposure to the hazard. While proper immediate response and evacuation planning would not have prevented the accidental release of CO_2, it would have mitigated the adverse impacts on workers.

RELATED CAUSAL FACTORS

Failure to identify, institutionalize, and implement requirements for immediate emergency rescue and response to planned and unplanned CO_2 discharges, was a contributing cause to insufficient immediate response and accident mitigation.

There were other contributing causes that impacted accident mitigation (i.e., failure to install a warning alarm and failure to adequately evaluate the impact of infrastructure reductions on worker safety). These causal factors are discussed in Sections 3.2 and 3.5 of the report, where more facts regarding them are presented. Section 4.0 discusses how they relate to the root causes of the accident, and Figure 4-2 depicts this relationship. See these sections for further discussion.

JUDGMENTS OF NEED

LMITCO needs to assure the ability to accomplish immediate rescue and response to planned and unplanned CO_2 discharges, including the capability to deal with mass casualties having insufficient oxygen.

3.0 DISCUSSION AND ANALYSIS

3.1 WORKER SAFETY

General

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.

Safety requirements for worker protection come from many sources.

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.

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

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.

<u>Safe Means of Egress</u>. 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.

<u>Analysis</u>

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.

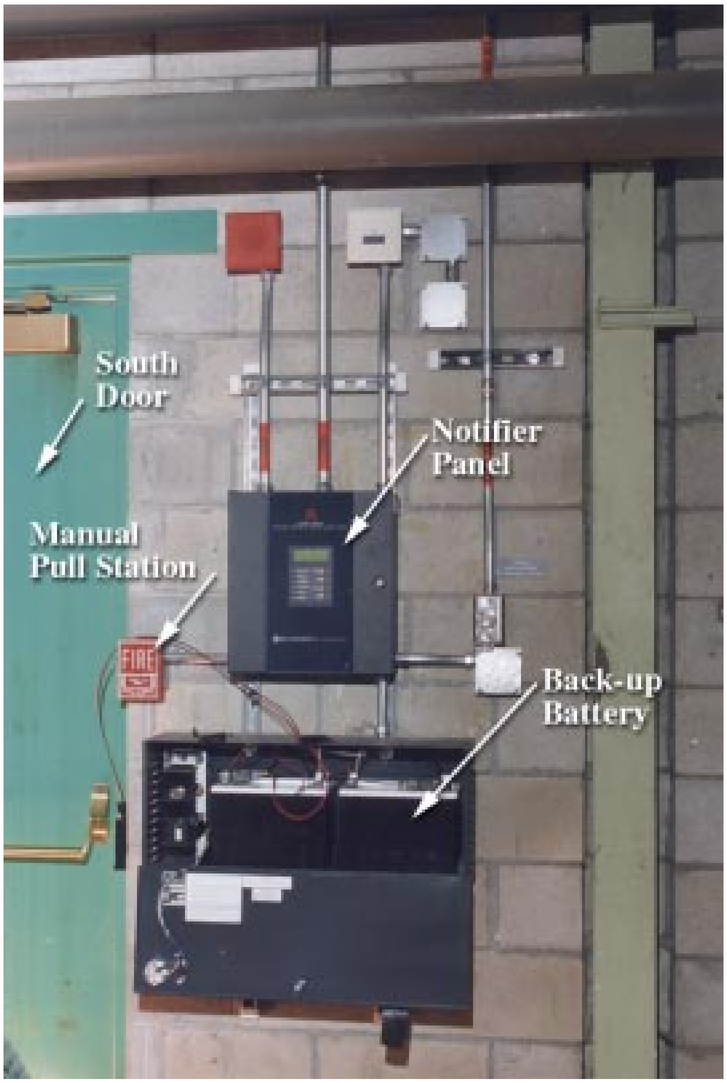


Exhibit 3-1. Notifier Fire Alarm Panel

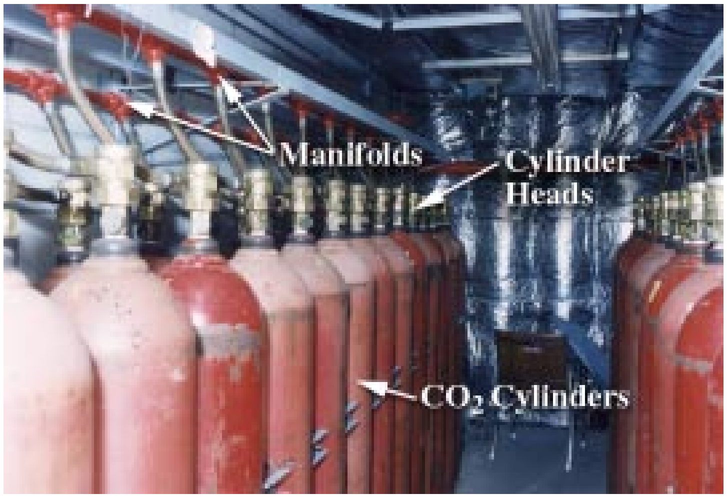


Exhibit 3-2. CO_2 Cylinders and Manifolds

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.

<u>Electrical System Description</u>. 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.

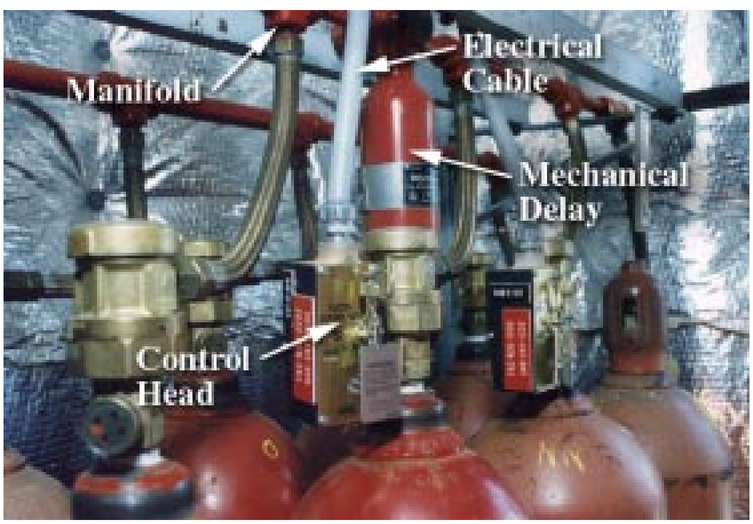


Exhibit 3-3. Control Head and Mechanical Delay Mechanism

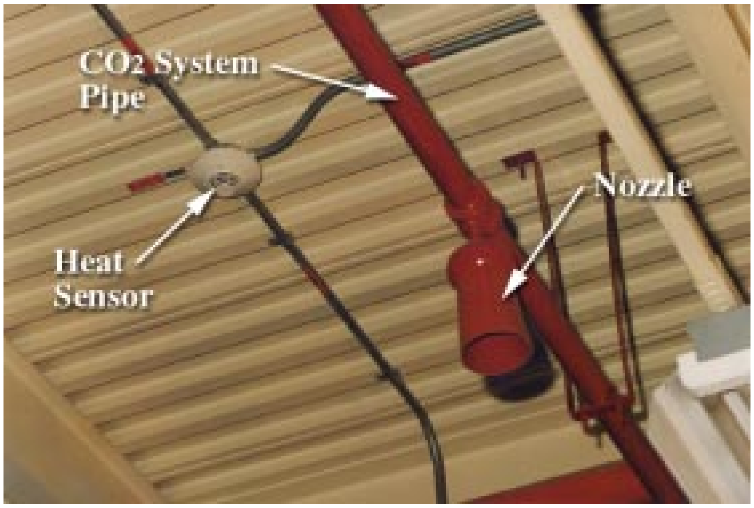


Exhibit 3-4. Overhead CO_2 Discharge Nozzle

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.

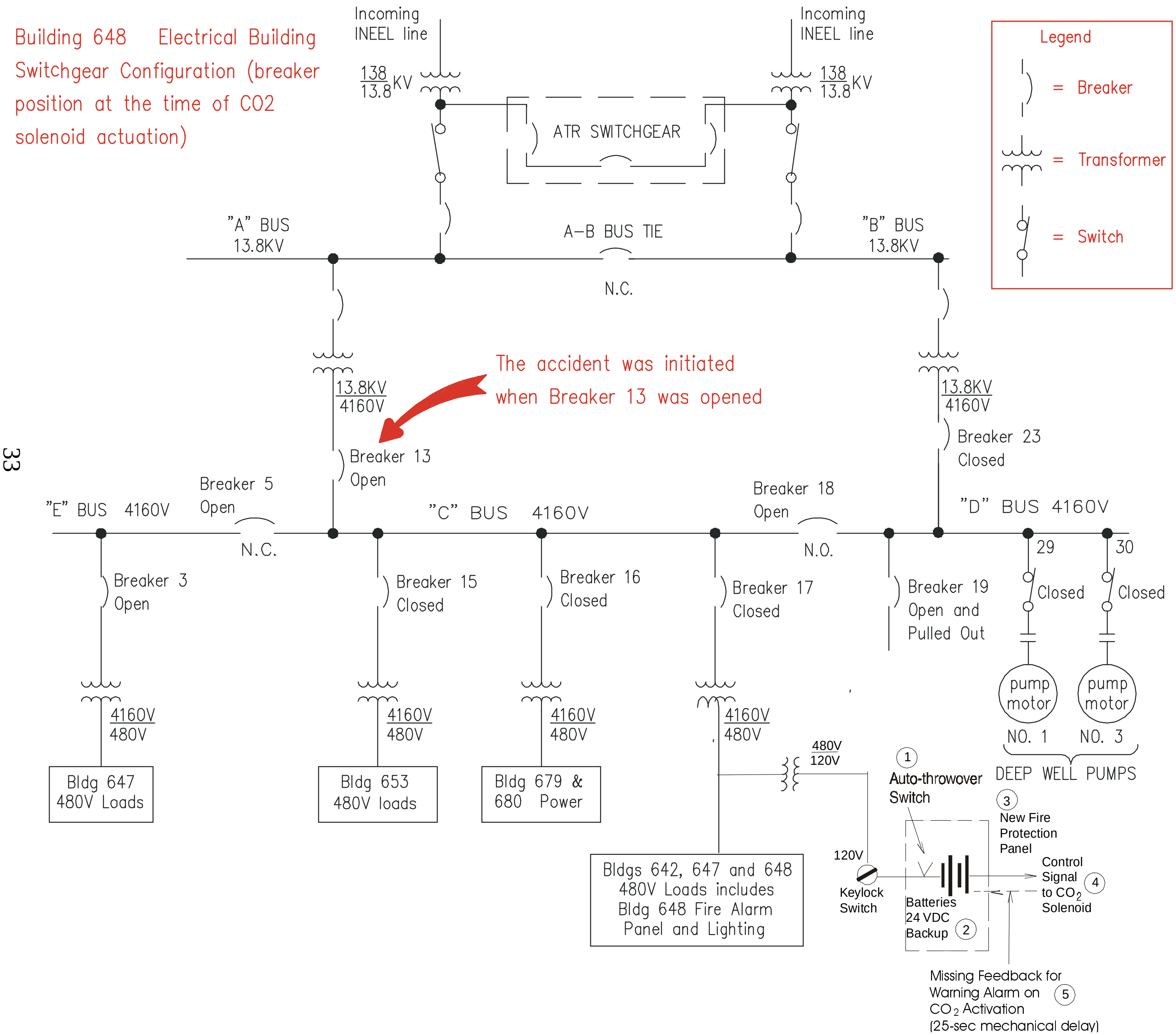


Figure 3-1. Simplified Schematic of Switchgear

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

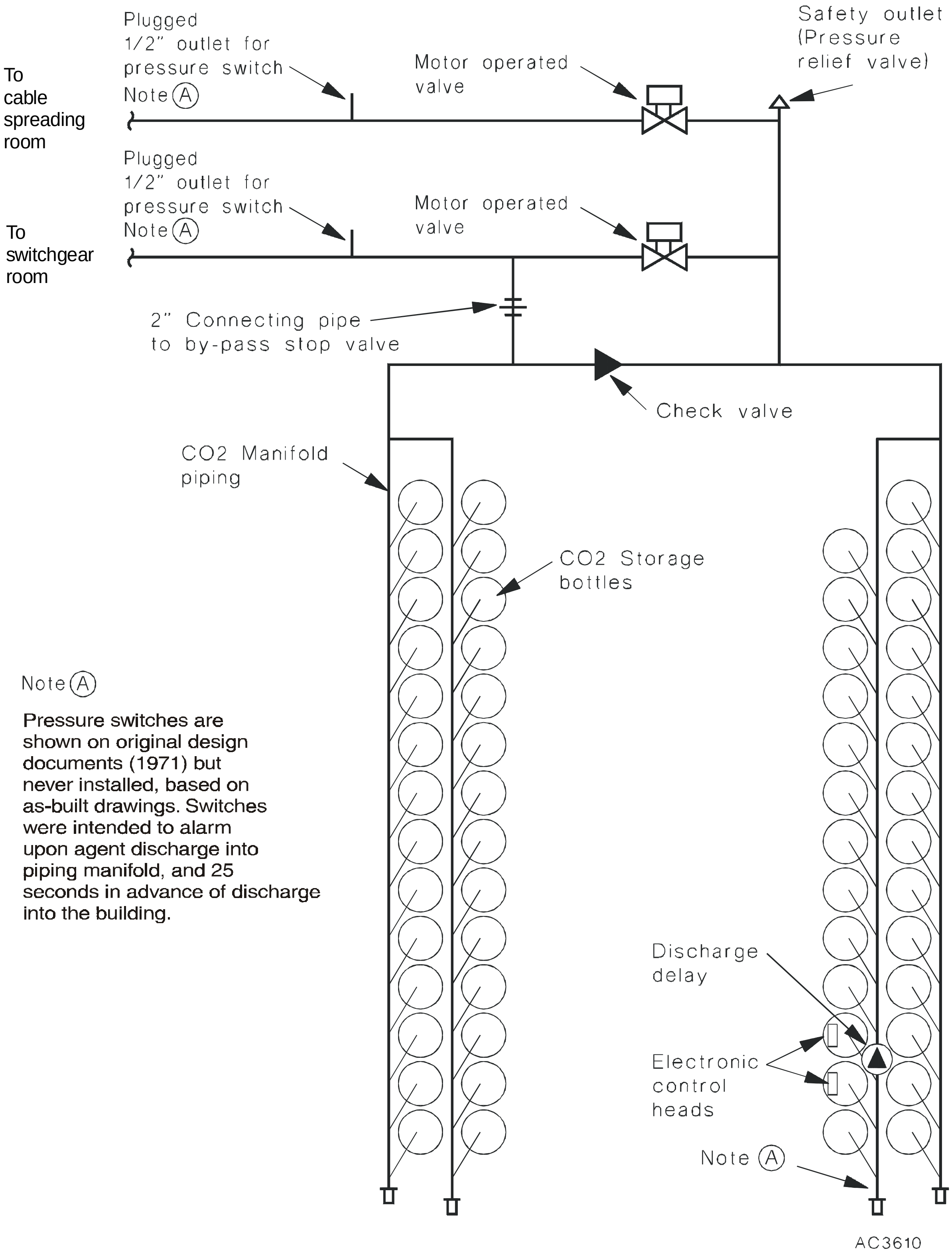


Figure 3-2. Carbon Dioxide System Arrangement Pre Line Item Upgrade

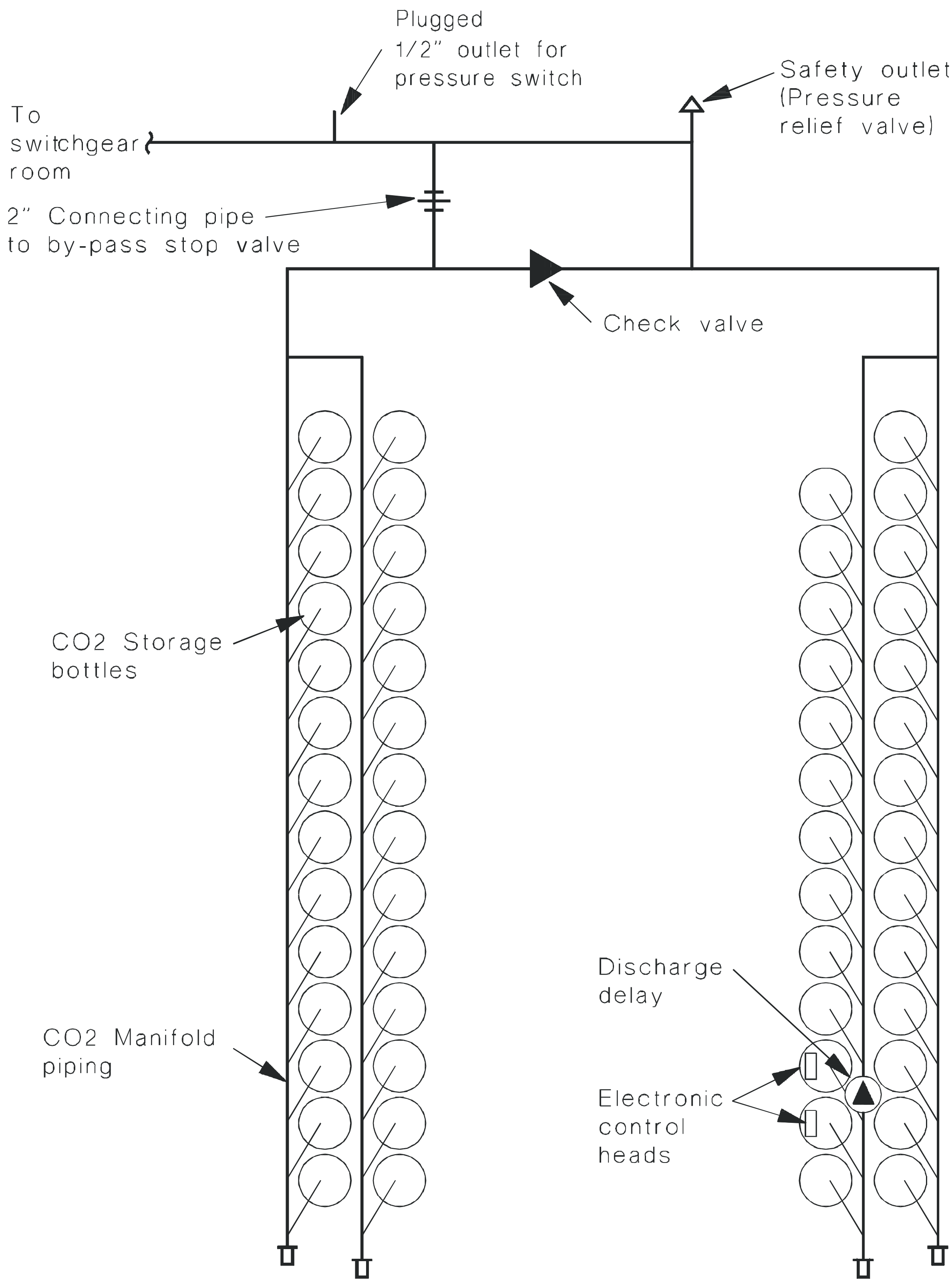


Figure 3-3. Carbon Dioxide System Arrangement Post Line Item Project

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

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

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 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.

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

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 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.

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

> 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.

Training and competency were issues in the accident.

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

- 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.

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

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

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.

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

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 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.

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.

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

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

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.

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

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:

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

- 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.

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

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.

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

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.

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

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

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

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

- 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 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.

4.0 CAUSAL FACTOR ANALYSIS

Causal factors analysis addressed both the causes of the accident and factors affecting accident mitigation.

General. Analysis of the causal factors required two lines of inquiry. The first is the causal chain from the events that preceded the accident, up to the time that the accident occurred. The second causal chain deals with the actions that were necessary to mitigate the effects of the accident after its occurrence. The summary causal factors chart in Figures 4-1 and 4-2 depicts the relationship between the causal factors and the events leading up to and following the accident. The analysis conducted by the Board revealed that the two causal chains were inextricably connected.

Root Cause Determination. The narrative in this section is structured to correspond with the logic used to arrive at all the causal factors for the accident, including the root causes. Since the lower tier contributing causes lead to root causes, they are discussed first. After discussion of the contributing causes, the root causes are identified with a brief analysis. The Board used tier diagramming to arrive at the root causes, which logically flow from the contributing causes. This relationship is depicted on Figures 4-1 and 4-2.

Causal Factors Impacting the Accident's Occurrence. The causal factors that contributed to the accident were:

- Faulty design and installation of the fire suppression system, including failure to install a monitoring or feedback circuit for the discharge header or solenoid valve
- Failure to use physical and administrative barriers that implemented applicable requirements
- Insufficient competency and understanding by staff at all levels of the requirements and procedures for dealing with CO_2 hazards
- Failure to take corrective actions and apply lessons learned from previous accident investigations to ensure that major deficiencies impacting worker safety were addressed.

Physical isolation (mechanical lockout/ tagout) of the alarm system could have prevented the accident

The fire suppression system was impaired electronically, rather than physically isolated by removing the solenoid heads from the system. Thus, **the most direct means that could have prevented the accident would have been mechanical lockout/tagout of the system.** There are several reasons why this positive lockout feature was not used.

FIGURE 4-1.
CAUSAL FACTORS IMPACTING THE ACCIDENT'S OCCURRENCE

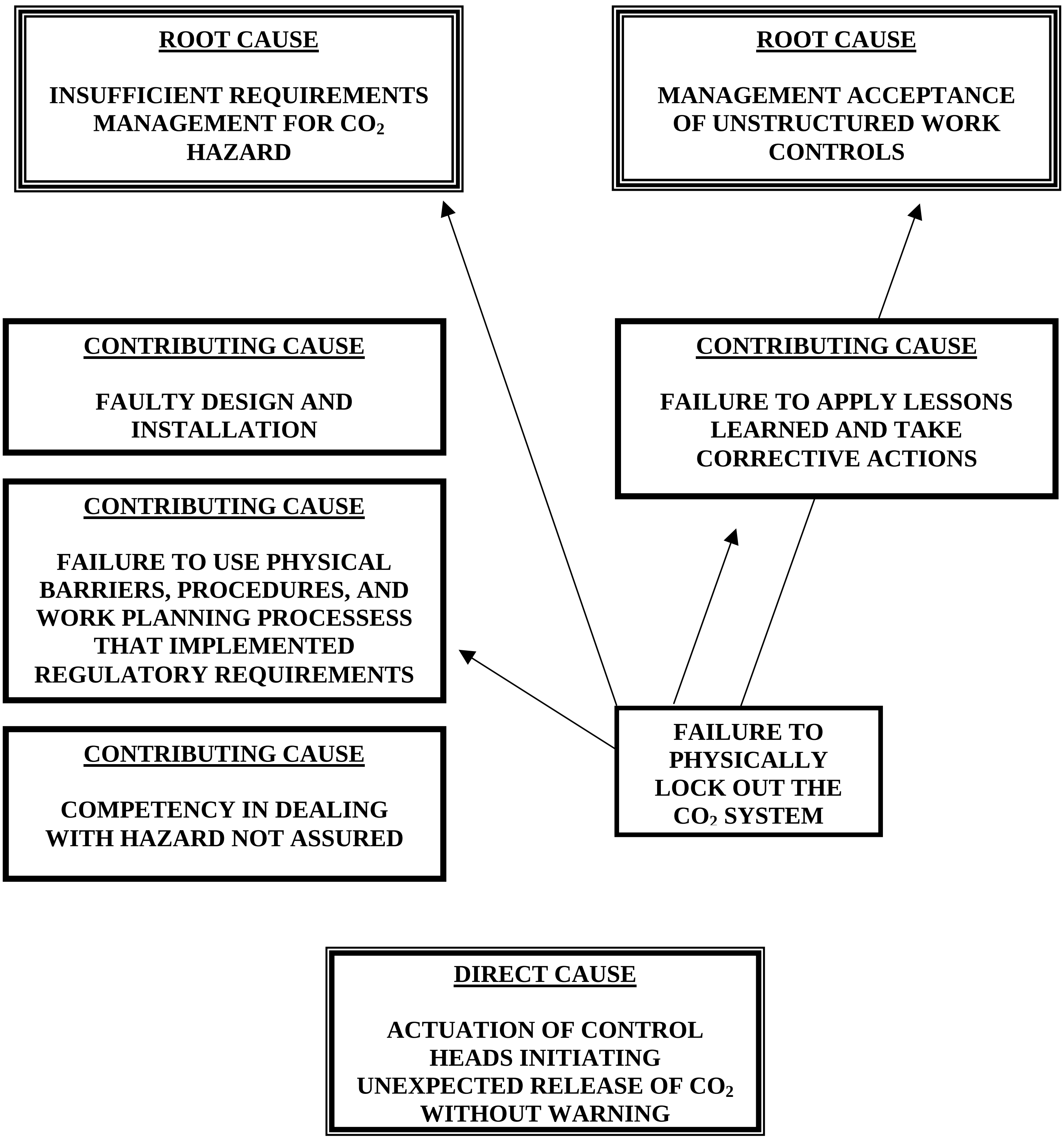


FIGURE 4-2.
CAUSAL FACTORS IMPACTING ACCIDENT MITIGATION

ROOT CAUSE

INSUFFICIENT REQUIREMENTS MANAGEMENT FOR CO_2 HAZARD

CONTRIBUTING CAUSE

FAULTY DESIGN AND INSTALLATION

CONTRIBUTING CAUSE

INSUFFICIENT REQUIREMENTS MANAGEMENT FOR IMMEDIATE EMERGENCY RESPONSE/RESCUE TO CO_2 DISCHARGE

CONTRIBUTING CAUSE

FAILURE OF ID AND LMITCO TO EVALUATE THE IMPACT OF COST AND INFRASTRUCTURE REDUCTIONS ON WORKER SAFETY

DIRECT CAUSE

ACTUATION OF CONTROL HEADS INITIATING UNEXPECTED RELEASE OF CO_2 WITHOUT WARNING

Personnel at all levels of the work planning effort did not understand the hazard, the requirements and proper means for mitigating and isolating the hazard, or the necessary personnel protective measures to take to protect the workers from the hazard. An electronic impairment, which is not a recognized personnel protection mechanism, was employed to provide a safety barrier to workers in the building. Ultimately, the answer as to **why** this physical barrier failed lies in the root causes that are discussed in this section: failure to follow requirements and management acceptance of unstructured work controls. Figure 4-1 highlights this relationship with the accident's root causes.

The hazard, requirements, and protective measures were not well understood.

Failure to use lockout/tagout was a symptom of the identified root causes. However, the importance of the failure to use lockout/tagout to physically lock out the CO_2 system cannot be overemphasized. Had this one action been taken prior to the accident, the accident would have been prevented. Modern accident investigation theory indicates that ultimately the root causes of accidents are found in management system failures, not in the most directly related causal factor in terms of time, location, and place. Thus, although this one action (use of physical lockout/tagout) might have prevented the accident, the ultimate reason it was not used was due to more global management system failures that, if not corrected, will lead to other accidents.

Root causes of the accident are found in management system failures.

Design of the fire suppression system was flawed, and the system was not installed in accordance with the manufacturer's instructions. The normal automatic 30-second system initiation delay and evacuation warning alarm did not function, because it was dependent on a valid and automatic initiation signal which was not received. An installed 25-second mechanical delay of CO_2 initiation could have provided an additional barrier, alarm, and 25-second escape time. A design error resulted in failure to assure a system actuation signal (feedback circuit) from the CO_2 manifold pressure or solenoid operation to the fire alarm panel. This design error was never detected. In the absence of a valid initiation signal and warning alarm, or an alarm associated with an accidental activation and 25-second notification, workers in the building had no pre-warning of the CO_2 discharge. The accidental activation of the CO_2 system is believed to have occurred when the 4160-volt breaker that feeds the 120 volt power supply to the fire alarm panel was de-energized, causing a momentary loss of power to the panel and initiation of the CO_2 discharge as the panel re-energized on 24 volt DC power. The specific causal relationship between the 4160 volt breaker, unexpected loss of power to the panel, and the signal to activate the CO_2 system remains under investigation by LMITCO.

Other deviations in the installation of the system included the application of an auxiliary power supply and shielding of the signaling line circuits. Although the role of this deviation in causing the accident is unclear, it is possible that they provided an unintended pathway for electrical transients that may have caused the CO_2 system to discharge unexpectedly.

Faulty design and installation of the fire suppression system were a contributing cause of the accident.

The design and installation deviations were never discovered by a LMITCO independent engineering review or in the quality assurance review process. This is because of the failure to follow established procedures in the design and installation process for the system, including engineering oversight of installation. Thus, **faulty design and installation of the fire suppression system, due to failure to implement appropriate requirements and procedures and the failure to install a monitoring or feedback circuit for the CO_2 discharged header or solenoid valve position to the discharge alarm, was a contributing cause of the accident.**

Lack of institutionalization and understanding of requirements led to design and installation deviations, as well as work planning process failures.

Further analysis reveals that both the design and installation deficiencies were part of a larger problem and further explains why the lockout/tagout procedure was not followed. This is because there were failures in both of the principal means to effectively implement requirements: through institutionalization and building competency. Throughout the work planning process prior to the accident, there was failure to understand and implement requirements and procedures involving the CO_2 fire suppression systems.

LMITCO does not have an effective institutionalized requirements management system that captured requirements and assured that they flowed down to deal with the CO_2 hazard. Institutionalization methods include policy development, communication, and implementation, manuals and procedures, SARs, and work planning and control processes. These institutionalization mechanisms were either not in place or ineffective, directly impacting the accident. Facts gathered during the investigation support this conclusion:

- Safety manuals did not address the hazard
- The SAR covering Building 648 was out of date
- There was incomplete flowdown of requirements
- Procedures applying to the CO_2 fire suppression system were out of date, under revision, and not used or followed

- Work planning and control processes used were not followed, were expert-based, and were ineffective
- System design was inadequate and not independently verified
- System installation was not subjected to quality control measures
- Lockout/tagout was not used, and impairment was insufficient to prevent the accident.

Accident Contributing Cause: Failure to use physical and administrative barriers.

Thus, a **contributing cause** of the accident was **failure to use physical (physical lockout) and administrative barriers (current procedures and work planning and control processes) that implemented regulatory requirements.**

Reliance on expert judgment, rather than structured work controls, was evident.

Competency is achieved through training, cognitive understanding, validation and testing, on-the-job reinforcement, and re-certification and refresher training. A successful safety management system integrates these components to ensure that managers, staff, and workers carry their knowledge to and use it in the workplace, performing their duties in a safe manner. This is one of the means by which requirements are institutionalized. There is reliance on structured work control processes, rather than expert judgment alone. During the investigation, facts revealed that these elements were either not in place or ineffective:

- Those involved in the design, installation, and approval of these processes did not fully understand the significance of design and installation changes on controlling the hazard and on worker safety.
- Training on the CO_2 hazard and protective measures was not performed
- Managers, safety and engineering staff, supervisors, and workers had insufficient knowledge of the requirements for dealing with CO_2 from the design to the work activity levels.
- Adequate cognitive understanding of the life-threatening potential of the hazard was not demonstrated by building management, the work planner, the fire protection engineer, operators, or the electricians who were not cognizant of the hazard. Individual responsibility of workers to carry out work safely could not have been exercised, because all of those involved believed that they were operating in a safe environment.
- Validation and testing elements of the training program were not in place or not done.
- On-the-job reinforcement and refresher training did not address the hazard.

Thus, a **third 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.**

Accident Contributing Cause: Failure to understand carbon dioxide hazards and requirements for dealing with the hazards.

There were defects in both institutionalization of safety requirements management and competency in dealing with the CO_2 hazard. Both elements contributed to the accident. These two factors ultimately led to the failure to use a positive lockout/tagout of the alarm system prior to work commencing. They also were responsible for the system design and installation failures.

Thus, **the first root cause** in this causal chain 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.**

One of the accident's root causes was lack of a systematic approach to addressing requirements related to the carbon dioxide fire suppression system.

Given the first root cause, a logical question is why ID and LMITCO line management have tolerated the situation that gave rise to the accident. This has been the third serious accident at INEEL in the past two and one-half years. Many of the judgments of need from this investigation are identical to those in the other two accidents. There has been a recurring pattern of ID and LMITCO management that tolerates or is not effective at eradicating informality in work planning and control and in procedure quality, use and adherence, while not implementing effective corrective actions and applying lessons learned. This pattern was identified during the DOE Office of Oversight safety management evaluation conducted in October 1995. If the judgments of need from the two previous serious accidents at INEEL in 1996 had been implemented, it is likely that the CO_2 accident could have been prevented. Therefore, a **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.**

Another contributing cause of the accident was failure to apply corrective actions and lessons learned from previous accidents.

There is ample evidence during this investigation to support these conclusions regarding unstructured work planning and hazard controls at INEEL:

- Procedures were outdated
- There was failure to use or adhere to procedures
- Hazard analyses were informal
- Impairment was an accepted means of personnel protection
- Design modification procedures were inadequate; configuration management lacks rigor, documentation, and competent independent review
- Material Safety Data Sheets for CO_2 , which required the availability of self-contained breathing apparatus, were not used in the work planning and control process
- There was lack of competency in and compliance with applicable DOE, NFPA, and OSHA requirements
- There were inadequate communications to workers on hazards and personnel protective actions.

At INEEL, there is continuing reliance on a non-structured, expert-based approach to work control. However, this system is prone to multiple failures that are putting workers at risk, as they are confronted with safety hazards, now that the emphasis, mission, and risks are shifting away from nuclear research and operations to activities that represent occupational risks to workers. Therefore, the **second root cause** is that **ID and LMITCO management have accepted unstructured work controls at INEEL, which contribute to increased industrial safety risks to workers.**

A second root cause of the accident was management acceptance of unstructured work controls.

Causal Factors Associated with Accident Mitigation. The major causal factors that contributed to flawed immediate emergency response and impacted the consequences of the accident were:

Several causal factors contributed to flawed accident mitigation.

- Failure to identify, institutionalize, and implement requirements for immediate emergency rescue and response to planned and unplanned CO_2 discharges
- Failure to install a pressure switch inputting to the building alarm that would have warned workers that the CO_2 was actuated and about to discharge
- Failure to adequately evaluate the impact of incremental cost cutting and reductions on worker safety requirements.

The flaws in requirements management that impacted accident mitigation are similar to those discussed under system design and installation, procedures, and work planning and control. Prompt discovery and rescue of injured workers were hindered by failure to understand and follow DOE, OSHA and NFPA requirements for a continuously operational evacuation alarm, prompt egress, evacuation lighting, clear exit paths, availability of self-contained breathing apparatus, training on the evacuation plan; and the decision to not provide power to the TRA Emergency Control Center that delayed arrival of the Incident Response Team van.

LMITCO's requirements management system did not assure flowdown of requirements for emergency response planning and implementation. Emergency response plans and procedures did not address response to accidental CO_2 discharges; therefore, immediate search and rescue efforts were not effective and endangered the lives of rescuers, who acted despite the unavailability of proper protective equipment. Furthermore, there was no recognition of the requirements applicable to emergency response to accidental CO_2 discharges.

Therefore, **the failure to identify, institutionalize, and implement requirements for immediate emergency rescue and response to planned and unplanned CO_2 discharges** was a **contributing cause** that impacted the consequences and mitigation of the accident.

A causal factor affecting mitigation was the failure to address requirements for immediate rescue and response to carbon dioxide discharge.

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

Thus, the **second contributing cause** relative to accident mitigation was **failure to install a monitoring or feedback circuit for the CO_2 discharge header or solenoid valve position to the building alarm that would have warned workers that the CO_2 was actuated and about to discharge.** This causal factor is considered inclusive in the faulty design and installation contributing cause discussed under causal factors impacting the accident's occurrence.

Lack of a monitoring or feedback circuit to ensure a pre-discharge warning alarm was another contributing cause affecting accident mitigation.

A **third contributing cause** that impacted accident mitigation was **failure on the part of ID and LMITCO to adequately evaluate the impact of incremental cost cutting and infrastructure reductions on worker safety.**

Failure to evaluate safety impacts of cost cutting and infrastructure changes also contributed to failures in accident mitigation.

Incremental cost cutting at INEEL, due to budget reductions, resulted in reductions in staffing levels, surveillance and maintenance activities, and the movement toward more non-operational or process-oriented activities. Other indications of this impact that were related to the accident were that the ETR SAR was not maintained, operations managers were not involved in activities in Building 648, self-contained breathing apparatus was not readily available at the scene or pre-staged because of consolidation, procedures (including emergency response plans and procedures) relative to the CO_2 system were not updated, and the main and diesel power to the TRA Emergency Control Center was shut off.

All of these impacts had a bearing on the accident. Primarily, they affected emergency response and probably delayed immediate rescue efforts. At worst, delay in immediate rescue contributed to the exposure of the fatally injured electrician to the CO_2 environment.

The effect of incremental cost cutting was not weighed against requirements. The investigation revealed numerous requirements that were either not known, not implemented, or not managed. When costs are reduced, requirements that must be met require resource allocation and, therefore, prioritization. Infrastructure needs, such as maintenance, fire protection, and emergency response, must be addressed. There is a tendency in the Department to overlook these needs and the long-term effects of neglecting them on worker safety. In addition, the mindset that places nuclear operations and hazards at a higher plane than non-nuclear concerns also has an impact. However, as the Department moves to more traditional industrial operations, resulting in the shutdown and disposition of many of its facilities, it is imperative to be more alert for worker safety hazards and requirements.

Causal factors affecting accident mitigation can be traced to the first root cause: lack of a systematic approach to addressing requirements.

Just as there were defects in institutionalization of safety management requirements in the causal chain that led to the accident's occurrence, there were similar failures impacting accident mitigation. The causal factors dealing with a failure to install the feedback circuit for the CO_2 warning alarm and in the immediate response planning and implementation were the direct result of either not identifying, not institutionalizing, or not implementing requirements for immediate response and rescue of workers injured by exposure to the CO_2 hazard. Likewise, analysis of the third contributing cause impacting accident mitigation is also related to failures to recognize and prioritize requirements. Thus, these contributing factors lead to the first root cause identified for the accident's occurrence.

Barrier Analysis. In addition to the causal factor analysis, the Board performed a barrier analysis, which is a systematic assessment of the physical, administrative, and management elements that are intended to protect workers from hazardous materials and conditions. Figure 4-3 presents the results of the barrier analysis. Specifically, it identifies barriers that failed or that did not function as intended.

A number of physical, administrative, and management barriers failed.

Figure 4-4 provides a more detailed assessment of some of the key physical barriers and selected barriers related to immediate emergency response and rescue. It shows how the proper functioning of the barrier could have prevented the accident entirely or reduced its consequences considerably, and the expected consequences if the barrier had functioned as intended. Finally, the figure describes the barrier failure mode, which identifies how action and/or inaction resulted in the barrier not functioning as intended.

As seen on Figure 4-4, the lockout/tagout barrier had the capability to completely prevent the accidental CO_2 discharge and thus to eliminate the possibility of injuries and fatalities. The other physical barriers (e.g., CO_2 header pressure sensors and alarm feedback circuit, in conjunction with the 25-second mechanical discharge) would not have prevented the discharge but would have provided a pre-discharge alarm and time to escape the building if they had functioned properly, thus reducing the likelihood of injuries and fatalities. However, these systems were either not installed or failed.

A variety of barriers related to emergency preparedness could have facilitated emergency escape and immediate search and rescue, thus reducing the risk to rescuers and possibly avoiding serious injuries. However, as discussed previously, weaknesses were evident in many of these barriers, so accident mitigation was not totally effective, and the accident's consequences were not minimized.

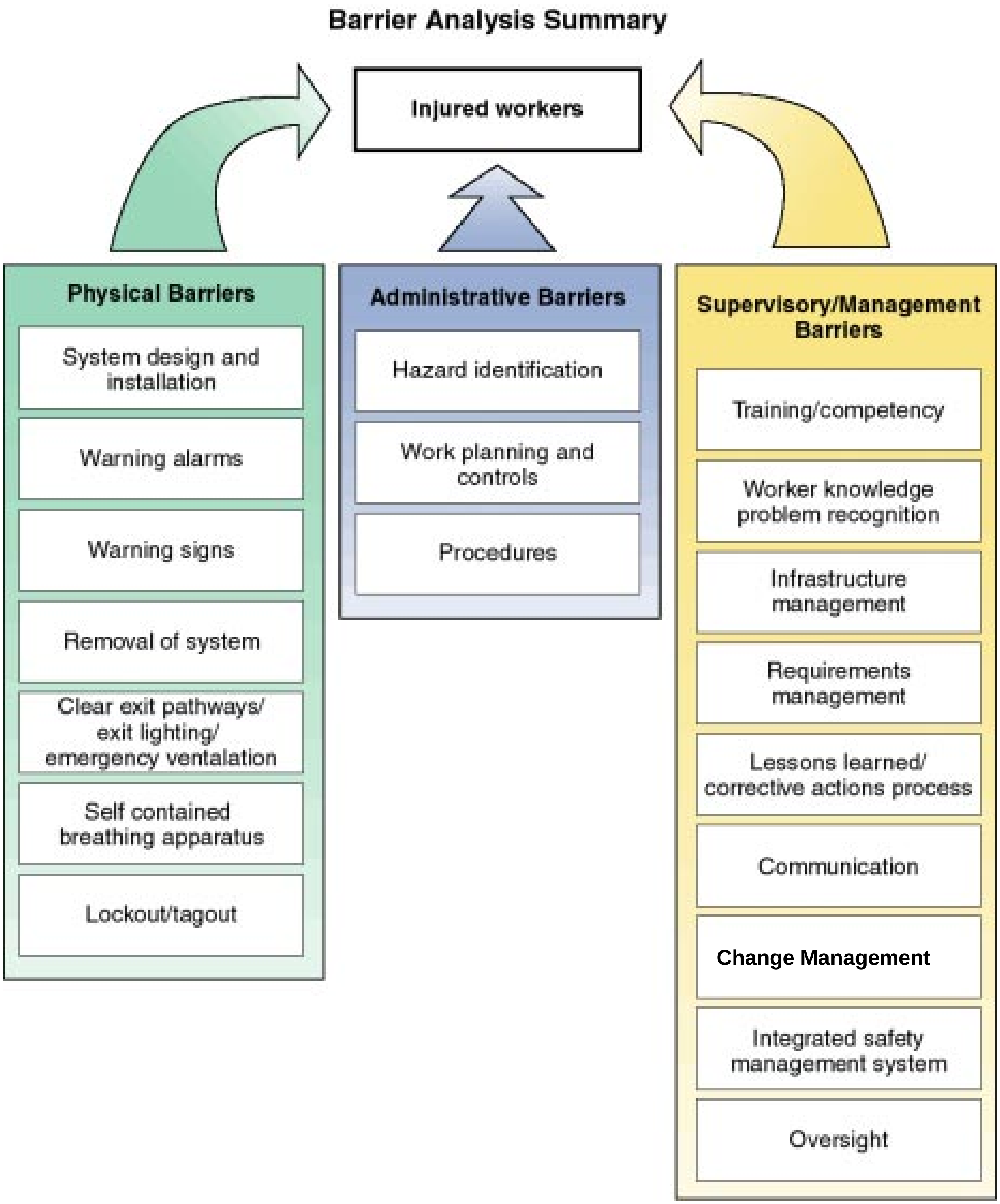


Figure 4-3. Barrier Analysis Summary

Barrier	Methods of Properly Implementing the Barrier	Expected Results with a Barrier that Functions as Intended	Failure Mode
Lockout/tagout	• Positive lockout device or • Remove electric control heads	No CO_2 discharge and thus no accident	• Positive lockout device not installed • No lockout/tagout performed
Manifold, pressure sensors, and feedback loop	• 25-second pre-discharge warning alarm • Mechanical delay	• CO_2 discharge • 25-second escape time • Possibly no injuries or CO_2 exposure	Pressure sensors and feedback loop deleted from design – not installed
• 30-second electronic and pre-discharge warning • 25-second mechanical delay	Total 55-second pre-discharge warning alarm	• CO_2 discharge • Probably no CO_2 exposure or injuries	30-second pre-discharge alarm applicable to valid initiation signal – not received
Immediate emergency response and rescue: – Respirators – Training – Exit lighting – Emergency ventilation – Clear exit pathways – Signs and instructions	• Emergency escape • Immediate search and rescue	• CO_2 discharge • CO_2 exposure • Possibly no serious CO_2 exposure/injury	• Respirators not pre-staged (consolidated) • No training on CO_2 hazard • Search and rescue training discontinued (IRT) • No posted signs/instructions • Pathways not clear or illuminated • No CO_2 evacuation drills

Figure 4-4. Assessment of Selected Barriers and Failure Modes

5.0 CONCLUSIONS

Failure to implement a number of requirements, including integrated safety management, was evident.

LMITCO failed to comply with and implement applicable DOE Orders, OSHA regulations, NFPA standards, and contractual obligations in assuring the protection of INEEL workers against a toxic and potentially lethal hazard. ID was not aggressive in assuring the timely implementation of integrated safety management or effective corrective actions to prevent accidents involving work planning and control. Supporting examples include the failure to:

- Perform a positive lockout and tagout of the CO_2 fire suppression system, a single action that could have prevented this accident
- Include a monitoring and feedback circuit in design of the new fire alarm panel to activate a warning alarm and facilitate safe escape, regardless of the CO_2 initiation signal source
- Prepare for an accidental or manual initiation of the CO_2 fire suppression system, including availability of self-contained breathing apparatus, clear exit pathways, warning signs, and emergency ventilation
- Adequately plan and control work and associated hazards, including hazards assessment, hazard controls, hazards communication, procedure use and adherence, and response to a safety concern
- Provide adequate training to workers on the CO_2 hazard, proper mode of isolation and personnel protection, and recognition and emergency response
- Establish and implement a corporate policy to assure flowdown of applicable safety requirements and institutionalization of these requirements into safety manuals, authorization bases, and procedures in a manner that discusses safety management of a toxic system in occupied spaces
- Effectively implement corrective actions and judgments of need from previous accidents, Type A investigations, and assessments in INEEL work planning and controls, as well as procedural use and adherence
- Provide the necessary level of leadership and followup within ID and LMITCO to expedite the implementation of the Department's integrated safety management policy and to achieve a safety culture conducive to procedure use and adherence, as well as a disciplined and consistent approach to work planning and control.

The Board concludes that LMITCO did not fulfill their required obligation to protect workers from a toxic and potentially lethal hazard, including the requisite design, policies, procedures, hazard analysis, work controls, communication, personal protective equipment, positive system lockout, and training.

Achieving acceptable and sustained safety performance and discipline and consistent work and hazard controls, as well as avoiding serious accidents such as this, will first require ID and LMITCO senior management recognition and acknowledgement that significant change and improvement are necessary at INEEL. Continued focus on a few improving statistics, instead of actual field performance, events, and near-misses, will produce an optimistic assessment and will not achieve the necessary fundamental changes in work planning and control processes, management systems, organizational behavior, and acceptance, understanding, and timely implementation of integrated safety management. Management at all levels must place a higher priority on obtaining realistic performance feedback and on proactive identification and correction of systemic weaknesses, if further accidents are to be avoided.

To avoid further accidents, management must place higher priority on performance feedback and on proactive identification and correction of systemic weaknesses.

6.0 BOARD SIGNATURES

Date: September 11, 1998

S. David Stadler
DOE Accident Investigation Board Chairperson
U.S. Department of Energy
Office of Environment, Safety and Health

Date: September 11, 1998

Thomas R. Staker
DOE Accident Investigation Board Member
U.S. Department of Energy
Office of Environment, Safety and Health

Date: September 11, 1998

William E. Miller
DOE Accident Investigation Board Member
U.S. Department of Energy
Office of Environment, Safety and Health

Date: September 11, 1998

James G. Bisker
DOE Accident Investigation Board Member
U.S. Department of Energy
Office of Environment, Safety and Health

Date: September 11, 1998

Matt A. Hutmaker
DOE Accident Investigation Board Member
U.S. Department of Energy
Office of Nuclear Energy, Science and Technology

Date: September 11, 1998

Walter N. Sato
DOE Accident Investigation Board Member
U.S. Department of Energy
Idaho Operations Office

Date: September 11, 1998

Charles A. Jones
DOE Accident Investigation Board Member
U.S. Department of Energy
Idaho Operations Office

7.0 BOARD MEMBERS, ADVISORS, AND STAFF

Chairperson	S. David Stadler, DOE, Office of Oversight
Member	Matt A. Hutmaker, DOE, Nuclear Energy, Science and Technology, NE-80
Member	Charles A. Jones, DOE Idaho Operations Office
Member	William E. Miller, DOE, Office of Oversight
Member	Walter N. Sato, DOE Idaho Operations Office
Member	Thomas R. Staker, DOE, Office of Oversight
Member	James G. Bisker, DOE, Environment, Safety and Health, EH-51
Advisors	Dennis Vernon, DOE, Office of Oversight Robert Crowley, DOE, Office of Oversight Al Gibson, Paragon Technical Services, Inc. Michael Anderson, DOE Idaho Operations Office Pat Smith, DOE Idaho Operations Office Mark Dumais, Argonne National Laboratory-West
Medical Advisor	Joseph Falco, M.D., Brookhaven National Laboratory
Analytical Support	Gary Swearingen, Pacific Northwest Natioal Laboratory Valerie Barnes, Battelle Columbus
Technical Writer	Dale Moul, Battelle Columbus
Observers	Bob Lange, DOE, Environment, Safety and Health, EH-40 Pat Conlon, U.S. Chemical Safety and Hazards Investigation Board
Union Observers	Brian Morris, Oil, Chemical and Atomic Workers Theresa Mix, Oil, Chemical and Atomic Workers
Attorney	Mary McKnight, DOE Idaho Operations Office
Administrative Support	Barbie Harshman, DOE, Office of Oversight Leisa Weidner, Paragon Technical Services, Inc. Julie Sellars, DOE Idaho Operations Office Shirley Cunningham, Battelle Columbus Kathy Moore, Battelle Columbus

APPENDIX A

BOARD APPOINTMENT MEMORANDUM

This page intentionally blank

Department of Energy
Washington, DC 20585

July 29, 1998

MEMORANDUM FOR JOHN WILCYNSKI, MANAGER
IDAHO OPERATIONS OFFICE

FROM: PETER N. BRUSH
ACTING ASSISTANT SECRETARY
ENVIRONMENT, SAFETY AND HEALTH

SUBJECT: INVESTIGATION OF THE JULY 28, 1998, FATALITY AT TEST REACTOR AREA, IDAHO NATIONAL ENGINEERING AND ENVIRONMENTAL LABORATORY

I hereby establish a Type A Accident Investigation Board to investigate the July 28, 1998, fatality at the Idaho National Engineering and Environmental Laboratory. I have determined that it meets the requirements for a Type A investigation consistent with DOE Order 225.1A, Accident Investigations.

The investigation will be led by my office, with the Board chaired by a member of my management staff. I appoint David Stadler from my office as the Accident Investigation Board Chairperson. The Board will be composed of the following members: Thomas Staker, EH; William Miller, EH, James Bisker, EH, and two members of your office who do not have "direct line management chain responsibility for day-to-day operation or oversight of the facility, area, or activity involved in the accident." A representative from the Office of Nuclear Energy will also be designated to serve on the Accident Investigation Board. The Board will be assisted by advisors and other personnel as deemed necessary by the Board Chairperson.

Given my office responsibilities, I plan to have Dennis Vernon, DOE Accident Investigation Program Manager, of my staff, serve as an Advisor to this Type A Accident Investigation Board.

The scope of the Board's investigation will include, but is not limited to, analyzing causal factors, identifying root causes resulting in the accident, and determining judgments of need to prevent recurrence. The investigation will be conducted in accordance with DOE Order 225.1A. The Board will also focus on safety management systems, including management roles and responsibilities and application of lessons learned from similar type accidents within the Department.

The Board will provide my office with daily reports on the status of the investigation by keeping Glenn Podonsky, Deputy Assistant Secretary for the Office of Oversight, informed of the status and progress of this investigation. These daily reports should not include any findings or arrive at any premature conclusions until an analysis of all the causal factors have been completed. Discussions of the investigation and copies of the draft report will be controlled until I accept and authorize release of the final report. The final report should be provided to my office by August 31, 1998.

cc:
G. Podonsky, EH-2
B.Stone, EH-2
D. Vernon, EH-2
J. Owendoff, EM-1
J. Fiore, EM-42
R. Smyth, EM AI POC
W. McQuiston, ID AI POC
T. Lash, NE-1