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

Chapters 4,5,6,7

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

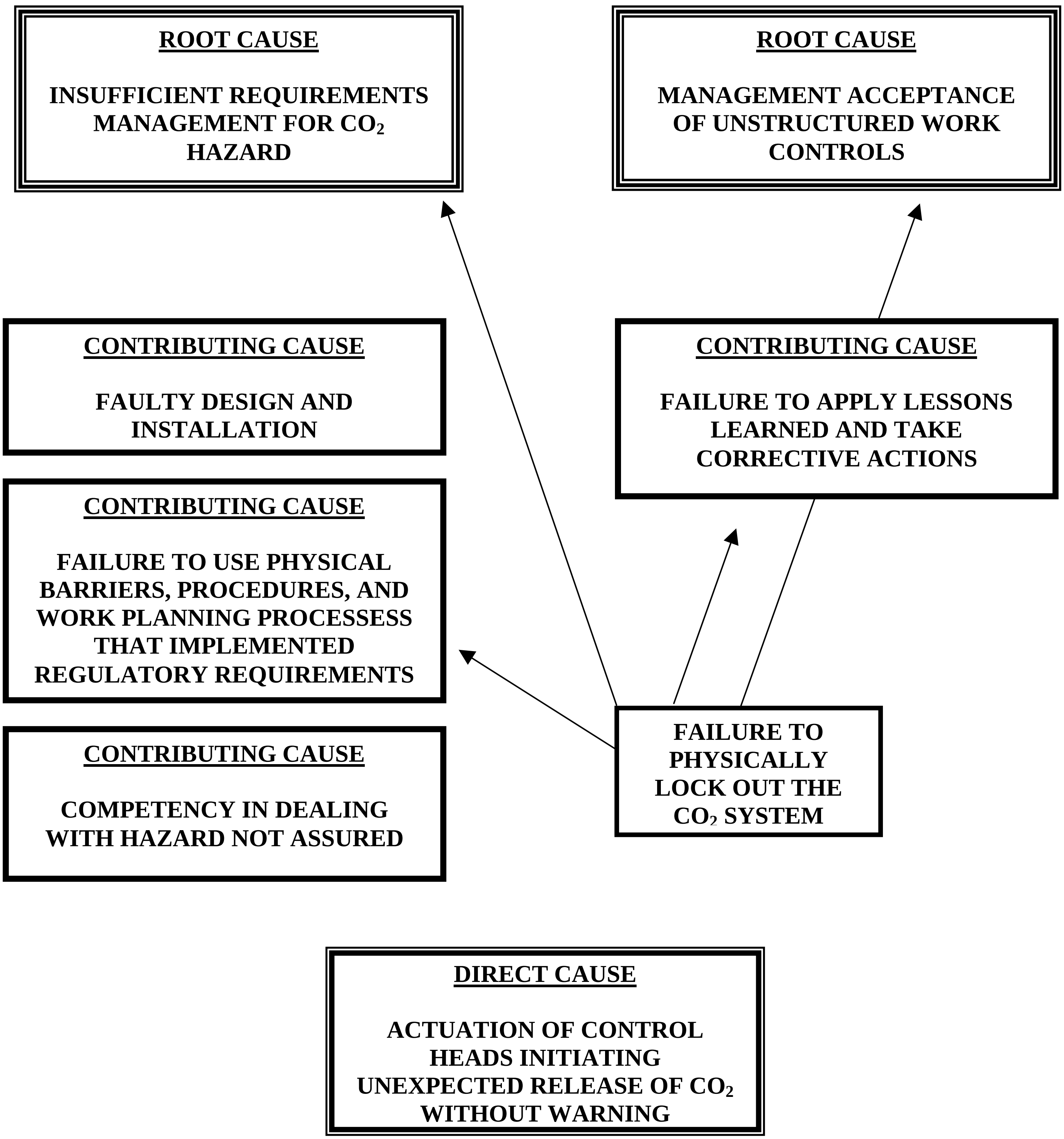

FIGURE 4-2.
CAUSAL FACTORS IMPACTING ACCIDENT MITIGATION

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.

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

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.**

Several causal factors contributed to flawed accident mitigation.

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:

- 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.

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

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.

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.

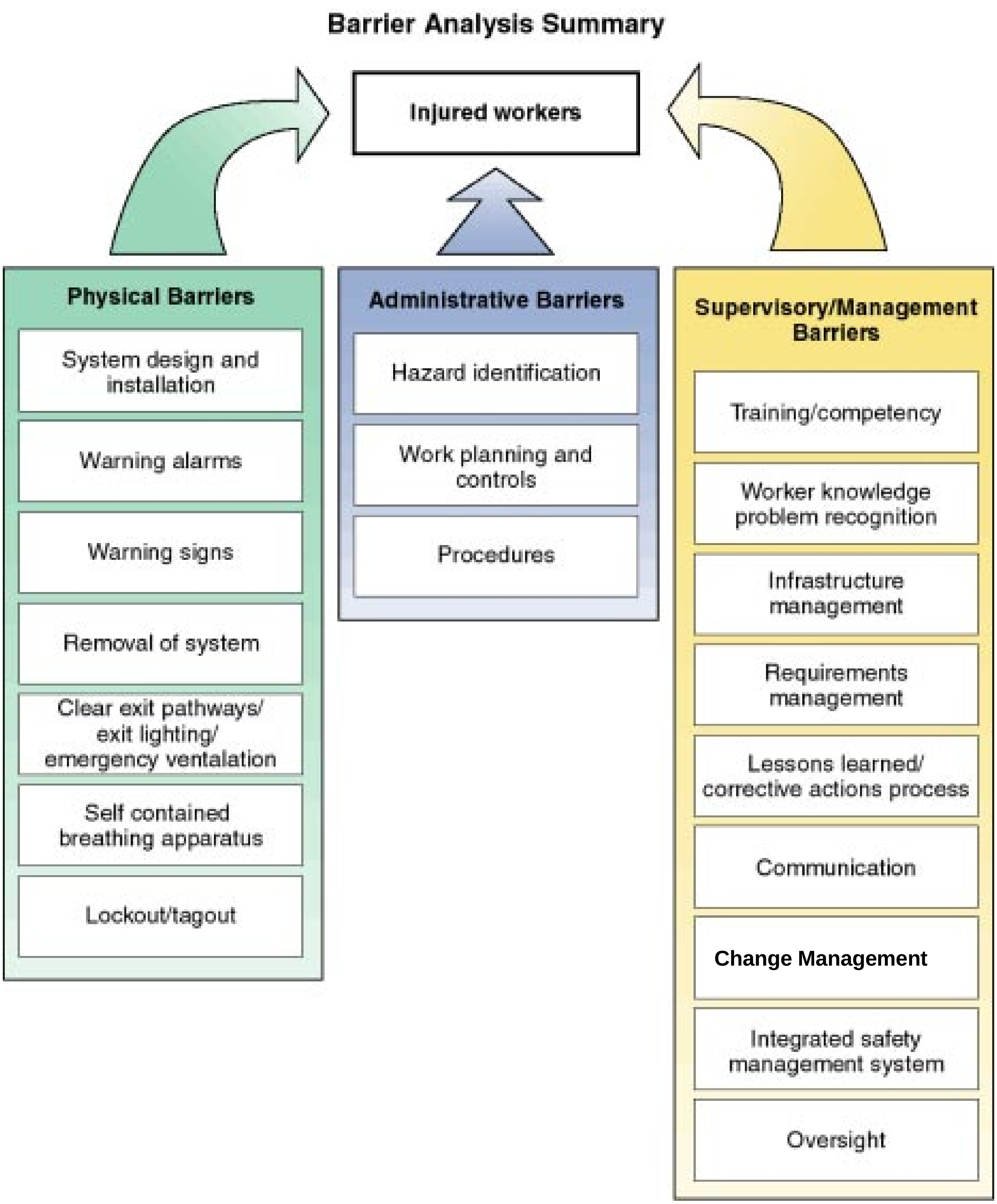

Figure 4-3. Barrier Analysis Summary

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