SITE 9920
ACCIDENT INVESTIGATION BOARD
REPORT

January 2014

National Nuclear Security Administration

Sandia National Laboratories

RELEASE AUTHORIZATION

February 14, 2014

On December 13, I appointed a joint NNSA/SNL Accident Investigation Board (AIB) to investigate the accident, which occurred at the Sandia National Laboratories/New Mexico, Site 9920 in Albuquerque, New Mexico on December 11, 2013.

The AIB's responsibilities have been completed with respect to this investigation. The analysis and the identification of the contributing and root causes, with the resulting Judgments of Need (JON) were performed in accordance with DOE Order 225.1B, *Accident Investigations*.

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

Edward Bruce Held
Acting Administrator
National Nuclear Security Administration

3/11/14
Date

This report is an independent product of the AIB. The discussion of facts, as determined by the AIB and the views expressed in this 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.

Accident Investigation Board

Don Nichols, AIB Co-Chair
Associate Administrator for Safety and Health
National Nuclear Security Administration

Michael W. Hazen, , AIB Co-Chair
Vice President, Infrastructure Operations
Sandia National Laboratories

Carol Adkins, AIB Team Lead
Director, 1800 Materials Science & Engineering
Sandia National Laboratories

Core Team Members

Marcelino Armendariz, Deputy TAT Lead,
SNL Org. 1751,
micro-electronics, systems knowledge

Noel Duran, SNL Org. 4021,
causal analyst, accident investigator

Ralph Fevig, SNL Org. 4122,
causal analyst, accident investigator

John Franchere, CSP,
Sandia Field Office/NNSA,
accident investigator

Philip Heermann, TAT Lead,
SNL Org. 6530,
accident reconstruction

Mike Lopez, SNL Org. 1679,
high rigor operations SME

Timothy Wallace, SNL Org. 4122,
explosives safety SME

Caren Wenner, SNL Org. 0431,
human factors SME

Michael Zamorski, NNSA NA-00.1,
safety culture

CONTENTS

Executive Summary ..... **iv**
Background ..... *iv*
Summary of Causal Factor Analysis ..... *iv*
Final Thoughts ..... *vi*

Introduction **1**
Background *1*
NNSA/Sandia Field Office 1
Sandia National Laboratories 1
Facility Description *1*
Scope, Conduct, and Methodology *2*

The Accident **4**
Accident Description *4*
Accident Response *4*
Medical Report Summary *4*
Event Chronology *4*

Facts and Analysis **8**
Emergency Response *8*
Post-Event Accident Scene Preservation and Management Response *8*
Assessment of Prior Events and Accident Precursors *8*
Integrated Safety Management (ISM) and WP&C *9*
Corporate Level 9
Defense Systems & Assessments (DSA) Program Management Unit (PMU) Mission Assurance Documents 9
Center 5400 WP&C 10
Center 5900 WP&C 10
Organization and Site Project Level WP&C 10
Conduct of Operations *11*
Supervision and Oversight of Work *12*
NNSA/SFO Oversight *13*
Human Performance Analysis and Interfaces *13*
Design 13
Planning 14
Operations 14
Sandia Explosives Safety Manual (SESM) *15*
Technical Analysis Team (TAT) Analysis *16*

Summary of Causal Factor Analysis **17**
Direct Cause *17*
Core Causes *17*
Failure to effectively implement "safe by design" intent 17
Insufficient WP&C of test operations 17
Insufficient integration and understanding of the project 18
Approach to maturing safety practices and discipline has left some workplaces behind 18

Conclusions and Judgments of Need **19**

Accident Investigation Board **23**

FIGURES

Figure 1: Aerial view of Site 9920 2
Figure 2: Block diagram of the integrated system 5

TABLES

Table 1: Site 9920 Accident Investigation Conclusions 20
Table 2: Site 9920 Accident Investigation Judgments of Need 22

THIS PAGE LEFT INTENTIONALLY BLANK

EXECUTIVE SUMMARY

Background

On December 11, 2013, Site 9920 personnel at Sandia National Laboratories (SNL) were testing an integrated explosive device, supplied by a project team from other Sandia organizations. The test involved communicating to an integrated device (ID) containing a fireset and detonator. During Wednesday's second test, the firing officer (FO) was injured when the ID went off unexpectedly during handling, causing injury to the FO's left hand.

On December 13, NNSA Administrator Bruce Held tasked Don Nichols, NNSA Associate Administrator for Safety and Health, and Michael Hazen, Vice President (VP) of Infrastructure Operations at Sandia National Laboratories (SNL), with convening an Accident Investigation Board (AIB) as a learning opportunity in response to the event.

The AIB visited the accident site, reviewed Sandia's recent past incidents, conducted interviews, and reviewed relevant documentation. A Technical Advisory Team (TAT) was also formed to support the AIB through scientific and engineering analyses, to assist the AIB in understanding the technical aspects that contributed to the accident. Change and barrier analysis were also performed, along with causal tree mapping, to identify the conclusions that drove the Judgments of Need (JON).

This document summarizes lessons learned and knowledge gained from the investigation, and includes recommendations that, when implemented, will reduce the probability of a similar accident.

Summary of Causal Factor Analysis

Direct Cause – integrated device (ID) failure

The direct cause of this accident was a failure in the integrated device, most likely from mechanical disturbance or electrostatic discharge, which caused an unexpected detonation.

Four core causes were identified during the AIB review:

Core cause - Failure to effectively implement "safe by design" intent

The system hazards created by combining individual components were not adequately considered, analyzed or understood by the project team. While the AIB understands that this design was a prototype, the number of hardware and software weaknesses found during the TAT analysis, combined with the lack of a safety theme and system integrator during the design process, indicates that not all opportunities to design out these weaknesses had been adequately addressed during the design process.

Finally, the hazards that could not be designed out of the device were not fully understood and/or explicitly articulated by the project team, and a "what-if" analysis (or similar failure analysis) was not conducted prior to the testing. Thus, the AIB concludes that a high-consequence event with this device was inevitable once it got to the testing phase if, as happened, the device was relied upon to provide safety.

Core cause - Insufficient Work Planning &Control (WP&C) of Test Operations

The Site 9920 team accepted, and then executed, work that their existing hazards analysis and operating procedures did not address, without first analyzing the hazard and then identifying and implementing controls. An expert-based process was used to evaluate whether these tests fell within the approved Site 9920 operating envelope without a detailed review of the existing procedures.

Line management in this organization had not identified and corrected weaknesses in WP&C and conduct of operations. In some cases, assessments were ineffective at identifying issues. In other cases, corrective actions put in place to address previously identified weaknesses were not sustained.

Core cause - Insufficient integration and understanding of the project

Given that the project team did not fully understand the hazards associated with their device, they could not communicate those hazards to Site 9920 personnel. Further, the project team did not communicate that the hazards were actually unknown, which could have driven different controls throughout the testing.

Basic communication between the project team and Site 9920 personnel was too high-level to be effective. For example, at no time did the project team and Site 9920 personnel walk through the Site 9920 test procedures to see if design features were needed to ensure safety during testing, an activity that would have required joint sharing of the expertise of each participant to be effective. Also, the sensitivity around project classification may have (even inadvertently) affected communication between the two groups.

Finally, during the tests, Site 9920 personnel relied on the project team for technical information about the system. The August testing, as well as the tests early in the week of the December series, reinforced Site 9920 personnel's confidence in the system operation. Neither the project team nor Site 9920 personnel knew that the control unit (CU) could communicate incorrect information about the state of the ID. Thus they did not make appropriately conservative decisions.

Core cause - Approach to maturing safety practices and discipline has left some workplaces behind

As is true at all NNSA sites, Sandia's diverse workforce has varying levels of safety practice maturity. Typical approaches to advancing the maturity of safety culture have not been sufficiently tailored to reach all individuals in the workforce, according to their individual needs. For lasting change, organizations need to know that they must change, and their management must both commit to affecting needed change and engage the hearts and minds of individual workers. Those seeking to affect lasting change should pay particular attention to the "outliers" in order to help them reach the desired end state.

Final Thoughts

The AIB reached two overarching thoughts based on the identified core causes.

First, the hardware and software design issues found by the TAT confirm that the device had hazards that had not been previously identified and addressed prior to testing. The AIB acknowledges that it may not be possible for all hazards to be engineered out of a prototype device, and testing is often how prototypes come to be understood. However, in cases where safe by design intent is not feasible in the device being designed, it is crucial for the state of the design to be accurately characterized and communicated to all those who will be working with the device so that mitigating controls can be identified and implemented.

In this case, the project team did not explicitly recognize the hazards that were introduced by combining legacy components and were not aware of the safety issues associated with the device. Thus, they did not accurately communicate those hazards to the Site 9920 team so that appropriate mitigations could be put in place. ***This suggests that a high-consequence event with this device was likely, even if it was tested elsewhere, unless mitigating safety measures were adopted prior to testing.***

Developmental firesets should always be considered armed (and likely to discharge without further stimulus) from the moment they are energized, so that appropriate external engineered controls are applied to ensure personnel safety. Such devices should never be relied on for safety. ***The AIB recommends adopting a policy that developmental designs are "born unsafe" until proven safe through technical understanding and review.***

Second, ***the lack of rigor surrounding WP&C and the lack of formality in conduct of explosive operations at Site 9920 suggests that an accident at the site was likely with another test, even if Site 9920 personnel had not accepted this particular project work.***

The lack of critical thinking during work planning, the expert-based approach to evaluating their operating envelope, and not stopping work when existing site procedures couldn't be performed as written, made an accident inevitable unless conduct of operations were improved. Given that a device being tested may not be, or cannot be, safe by design intent, it is crucial that the operations be conducted within a safe operating envelope (the 'testing system' needs to be safe by design intent).

Site 9920 Accident Investigation Conclusions

Cause No.	Conclusions (Causes)	JON
	Core Cause: Failure to effectively implement "safe by design" intent	
C09	The project team did not recognize that concept design should be considered 'born unsafe.'	1, 6
C15	The project team leads did not recognize the need for a comprehensive design review of the entire system to ensure safety prior to testing with live explosives.	2
C28	The project team did not understand the hazards introduced by the combination of legacy components.	2
C18	Executive management expectations of the implementation of WP&C were not met. Center 5900 believed that WP&C did not directly apply to their role in this project.	1
C19	Because of deficiencies in the design approach, the accident could have happened any time the battery was installed in the unit.	1, 2, 6
C27	There was no "system integrator" responsible for the safety of the integrated device.	2, 3
C40	The project team did not engage safety professionals early in the design process.	1, 5
C03	There is ambiguity in the Sandia Explosives Safety Manual (SESM) requirements and definitions specific to developmental fireset design and control.	12
C07	The Defense Systems & Assessments (DSA) Mission Assurance structure does not integrate safety and security as essential to mission assurance.	3
	Core Cause: Insufficient WP&C of Test Operations	
C02	There is ambiguity in the SESM requirements and definitions specific to anomalous test conditions.	12
C04	Center 5400's implementation of Failure Modes and Effects Analysis (FMEA) is weaker than the robust traditional FMEA approach of rigorous step-by-step activity hazard analysis.	10
C05	Center 5400 does not require a step-by-step job specific activity hazard analysis.	10, 11
C06	The Center 5400 explosive safety implementation using the rigor tool could lead to noncompliance with the SESM.	10, 11
C08	The project team used un-approved procedures to direct explosive operations.	10, 11
C10	The Team 5434-2 procedure for developing a Test Planning, Review and Authorization (TPRA) and accepting work does not require department manager approval as required by Sandia's WP&C manual: MN471021.	10, 11
C11	The Site 9920 FMEA does not adequately analyze the hazards associated with routine activity-level work performed at Site 9920.	10
C12	The Site 9920 FMEA does not address the hazards of developmental firesets.	10, 12
C14	Site 9920 uses an expert-based approach to evaluate work and determine whether a test is within their operating envelope.	10, 11
C16	The TPRA approved in August did not cover the December tests, nor did it accurately describe the scope of the tests performed in either test series.	10, 11
C17	Some explosive procedures in the Facility Standard Operating Procedure (FSOP) are not addressed in the FMEA.	10, 11
C30	The decision that this test fell within the existing operating envelope was performed without a thorough evaluation of existing procedures.	10, 11
C31	The Site 9920 process does not require independent review of the decision to use an existing TPRA to cover additional work.	10, 11
C36	Combining the FO and Safety Officer (SO) roles is not a sound safety structure.	11

C38	Day-to-day management engagement in Team 5434-2 was not sufficient to assure safety.	10, 11, 13
C20	The Site 9920 FSOP (FSOP-EFS-001) does not include procedures for test anomalies, with the exception of misfire and no-fire conditions.	10, 11
C21	The level of operational rigor exhibited by the Site 9920 operations does not meet expectations commensurate with the level of hazardous operations performed at the site.	11
	Core Cause: Lack of integration and understanding of the project	
C34	The project team inadvertently conveyed to Site 9920 personnel more confidence in the safety of the test device than was warranted.	5
C13	Site 9920 personnel did not (and could not technically) recognize the significant hazards in the experimental system. Rather than treating its safety as an unknown, they relied on perceived assurances of safety from the project team.	5, 6, 10, 11
C32	Differences in understanding of the state of the development of the test components, and lack of effective discussion about the hazards introduced by integrating legacy components, contributed to the lack of critical thinking or questions during the planning for this test series.	1, 5,
C29	Classification and sensitivity around the project inhibited effective communication; both among the project design team and with Site 9920 personnel.	4
C33	During the test activities, neither Site 9920 personnel nor the project team took a conservative approach to decision making.	6, 10, 11
C35	Reliance on project personnel contributed to the erosion of the FO's ability to make independent, conservative decisions regarding the test.	5, 6, 11
C37	Site 9920 personnel did not recognize a single point of contact from the project team during the test series.	5
C26	Current Sandia Field Office (SFO) oversight approach does not ensure that every facility is visited. Graded approach for periodicity should not equal zero.	7
	Core Cause: Approach to maturing safety practices and discipline has left some workplaces behind	
C01	The effort to educate and mentor all levels of management in the engineered safety principles and their appropriate application has not yet achieved the desired effect.	10
C41	Sandia has not identified the outliers who are further behind in recognizing the need for safety improvement and discipline.	8
C39	There has been insufficient management engagement to ensure that the intended focus of WP&C improvements on critical thinking and analysis (as opposed to updated processes and paperwork) is understood and implemented in some line organizations.	10, 13
C22	WP&C improvements made in Team 5434-2 as a result of ID-016 (corrective actions that were taken after the Sled Track incident) were not sustained.	8, 9
C23	Management did not ensure identified WP&C weaknesses were effectively addressed at the department level.	8, 10
C24	Center 5400 line management (from team lead through director) self-assessments did not identify the weaknesses in safety performance of explosive operations that contributed to this accident.	9, 10, 13
C25	Center 5400 line management (from team lead through director) processes do not assure that corrective actions are completed and effective.	9, 10, 13

Site 9920 Accident Investigation Judgments of Need

	Judgments of Need	Related Conclusions
1	Sandia needs to develop and implement a plan for applying WP&C and the underlying engineered safety principles, to Sandia's design functions - at all stages of lifecycle (conceptual through test to deployment)	C09, C18, C19, C32, C40
2	Sandia needs to make sure applicable requirements are clearly understood and responsibility for safety of the integrated design and its technical review is well-defined - at all stages of lifecycle (conceptual through test to deployment)	C15, C19, C27, C28
3	Sandia needs to ensure, demonstrate, and communicate an integrated approach to mission assurance (safety, security, WP&C, quality, financials, formality, etc.)	C07, C27
4	Sandia needs to ensure that safety comes before security, and constitutes project need-to-know.	C29
5	Sandia needs to develop and implement a process to ensure all participants have a common understanding of project scope, level of development, requirements (design and test), roles & responsibilities, communication paths, etc. from project inception to completion.	C13, C32, C34, C35, C37, C40
6	Sandia needs to ensure design and activities, including those combining established technologies or commercial off-the-shelf (COTS) parts, are presumed "born unsafe" until they are proven safe through technical understanding.	C09, C13, C19, C33, C35
7	SFO needs to develop and implement a plan for oversight of *all* operations using a graded approach.	C26
8	Sandia needs to use an extent of condition approach, in addition to self-assessment, to find those organizations without mature WP&C implementation (outliers) and focus improvement efforts on them.	C22, C23, C41
9	Sandia needs to assure, through critical and rigorous assessment and continuous learning, that WP&C improvements are sustained within organizations at the management and worker levels.	C22, C24, C25
10	Sandia needs to ensure there is a common understanding of corporate WP&C expectations and engineered safety principles for activity-level work, and implements the tools effectively.	C01, C04, C05, C06, C08, C10, C11, C12, C13, C14, C16, C17, C20, C23, C24, C25, C30, C31, C33, C38, C39
11	Sandia needs to establish a more formal and disciplined conduct of operations approach for all activity-level work, using a graded approach based on the hazard of the work, not the facility.	C05, C06, C08, C10, C13, C14, C16, C17, C20, C21, C30, C31, C33, C35, C36, C38,
12	Sandia needs to update its corporate safety documents to clarify requirements on experimental and developmental work, including response to test anomalies.	C02, C12, C03
13	Sandia needs to require management engage deeply at the operational level with their staff and operations.	C24, C25, C38, C39

INTRODUCTION

On December 11, 2013, during an explosives test series at Sandia National Laboratories' (SNL's) Site 9920, a firing officer (FO) was injured by unintended initiation of the integrated device (ID) while trying to change its battery during an unsuccessful test.

On December 13, NNSA Administrator Bruce Held tasked Don Nichols, NNSA Associate Administrator for Safety and Health, and Michael Hazen, VP of Infrastructure Operations at SNL, with convening an Accident Investigation Board (AIB) as a learning opportunity in response to the event.

The AIB began their formal accident investigation process on December 16. During that time, a Technical Advisory Team (TAT) was also formed to support the AIB through the conduct of scientific and engineering analyses.

This document summarizes lessons learned and knowledge gained from the investigation, and includes recommendations that, when implemented, will reduce the probability of a similar accident.

Background

The organizations related to this accident were the National Nuclear Security Administration/Sandia Field Office (NNSA/SFO) and Sandia Corporation (Sandia).

NNSA/Sandia Field Office

The NNSA/SFO provides oversight of Sandia's activities and implements the Department of Energy (DOE) contract with Sandia.

Sandia National Laboratories

Sandia National Laboratories is a multidisciplinary national laboratory and Federally Funded Research and Development Center (FFRDC). Sandia, a wholly-owned subsidiary of Lockheed Martin Corporation, manages and operates SNL under the DOE contract. Sandia's unique mission responsibilities in the Nuclear Weapons (NW) Program create a foundation from which it leverages capabilities to solve complex national security problems. Sandia develops technologies to sustain, modernize, and protect the United States nuclear arsenal, prevent the spread of weapons of mass destruction, defend against terrorism, protect national infrastructures, ensure stable energy and water supplies, and provide new capabilities to the United States armed forces.

Facility Description

Site 9920, the Explosives Applications and Containment Training Facility (Fig. 1), is located in SNL's Coyote Test Field, east of Tech Area 3. Since 1958, engineers and technicians have used the site to design, assemble, and test explosive experiments in support of Labs-wide programs.

Site 9920 supports experiments involving high explosives for projects related to the Nuclear Emergency Search Team (NEST). The site assists on experiments related to nuclear material dispersion and confinement technology testing for mitigation of blast, fragment, and high consequence material. The site also performs general explosives device testing.

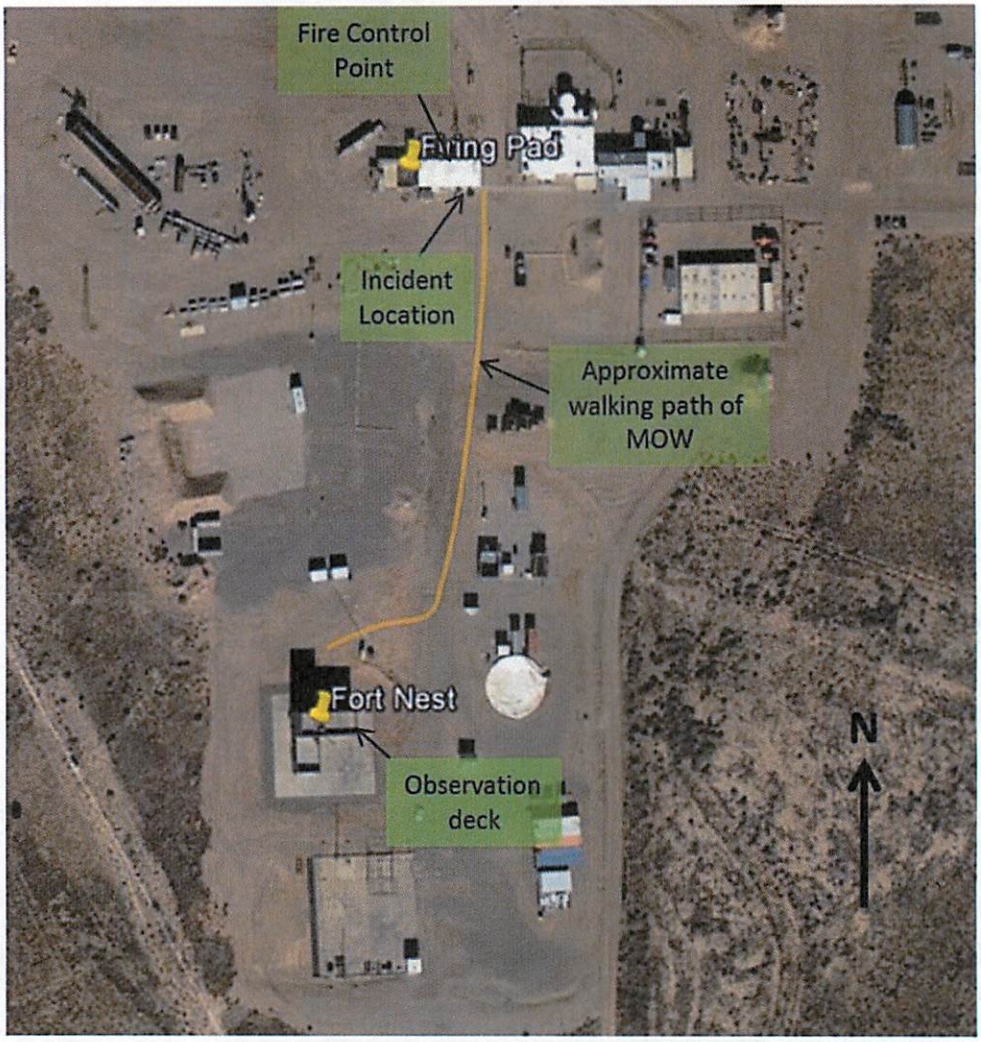

Figure 1: Aerial view of Site 9920

Scope, Conduct, and Methodology

The AIB established a charter (consistent with the NNSA Administrator's direction and DOE Order 225.1B, *Accident Investigations*) with the following principles:

- Maximize the investigation as a learning experience, not only for Sandia, but also for the entire DOE and NNSA Complex,
- Find solutions, rather than blame, while respecting individuals,
- Review the event using the foundational elements of Integrated Safety Management, Safety Culture, Human Performance Improvement and Work Planning and Controls (WP&C) incorporating engineered safety principles,
- Demonstrate a Just Culture by looking at the event as a result of a system of interoperable parts, not a single failure, and find the underlying causes.

The AIB included both NNSA and Sandia participants and was co-led by senior management from both entities. The team included personnel with well-known leadership and expertise in high-rigor operations, human factors, failure analysis, and explosives safety, as well as a strong grounding in safety culture and WP&C. Causal analysts and experienced accident investigators also supported the team. Team participants were dedicated to the team for the duration of the investigation.

A TAT was formed under the supervision of an AIB team member to understand the technical aspects of the test article's failure. TATs have been found to be a useful approach in other evaluations performed by Sandia. The TAT brought in relevant expertise in materials, firesets, communications, explosives, electrostatic discharge (ESD), and electronic circuitry.

The AIB and the TAT collaborated closely and engaged the relevant design and operations communities. The team sought a balance between independent review and partnering with design and test personnel. The AIB and TAT jointly held a system design review and an operations review with relevant personnel. On a daily basis, key management from involved line organizations and Sandia's explosive safety community were invited to participate in daily outbriefs. This allowed them to see the depth and breadth of the investigation and to understand key issues as they were identified.

At the end of the investigation, the AIB Co-Chairs and one of the AIB members held small group meetings with the organizations involved, and discussed the lessons learned and principal observations in a non-threatening environment.

Incorporating both NNSA and Sandia partners in the effort ensured diversity of skills and experiences, which enabled thorough understanding of corporate processes and enhanced the team's knowledge base. The AIB would recommend this approach for future investigations, as a model for maximizing learning.

THE ACCIDENT

Accident Description

At approximately noon on Wednesday, December 11, 2013, Site 9920 personnel were testing an integrated explosive device supplied by the project team. The test involved communicating to a device with an integrated fireset and detonator. The device was placed in a C-4 (~1lb) explosive charge for this particular test.

The December test series had started on Monday, December 9. Several tests were performed on Monday and Tuesday, and three additional tests were planned for Wednesday. During Wednesday's second test, communication was lost between the control unit (CU) and the ID at the firing pad. When communication could not be re-established, the software engineer (SE) asked if the ID could be retrieved from the C-4 and examined. The FO believed that the ID was not armed and safe to handle based on discussion with the SE.

The SE turned off the CU and set it on a cart. The FO went to the firing pad and removed the ID from the C-4, while the SE waited by the cart for FO to return. A repair was made to the ID, and the SE asked to change the battery in the ID as well. The SE then went into Bldg. 9920 to retrieve a battery and a voltage meter.

The FO started to disassemble the ID. The detonator initiated unexpectedly, causing injury to the FO's hand.

Accident Response

Coworkers immediately applied first aid. The SE and two other staff members transported the FO to Sandia Medical, where the individual received initial treatment. The FO was then transported by ambulance to a local hospital, treated, and released.

Site 9920 personnel did not call 911 and therefore there was not a traditional emergency response. Sandia Emergency Management responded to the scene after the event to assure the site was properly cleaned and preserved.

Medical Report Summary

The detonation resulted in limited tissue damage on the outer edge of the FO's hand, just below the fifth digit (pinky), which required five stitches.

No surgery was required; the FO was released after treatment the same day, without being admitted. The FO returned to work quickly and a full recovery is expected.

Event Chronology

In May 2013, Organization 5964 began a project to design and build a "proof of concept" solution for an external customer. The customer specifically desired a remotely-controlled fireset and wanted a demonstration of an integrated unit capable of initiating explosives.

The project team leveraged legacy component designs to develop their integrated solution and matrixed component designers from other Sandia organizations to support the design. Roles and responsibilities for this project included:

- Center 5900 (Systems Research Center) – Customer interface, program/technical lead(s) (PL1, PL2), systems integration (PL1, PL2, SL1), packaging (mechanical engineer [ME]), lead software engineering (SL1), accountable manager for the project
- Center 5300 (RF and Electronic Systems Center) – Communications engineering, circuit fabrication and testing, device assembly and test, software engineering (SE)
- Center 2600 (Engineering Design and Integration Center) – Fireset design, circuit fabrication and testing
- Center 2500 (Energetic Components) – Detonator and booster design, detonator and booster process engineering, fabrication and assembly
- Center 5400 (Integrated Military Systems Center) – Operates Site 9920 (field testing), including firing/safety officer (FO/SO), control officer (CO), explosive operators (SP1, SP2), and team lead (TL)

During the week of Aug. 12-16, 2013, Site 9920 personnel conducted a first series of proof-of-concept tests using a CU and an initial "breadboard" version of the ID. The test device included a wired connection from the capacitor discharge unit (CDU) to the control room of Bldg. 9920, which allowed remote monitoring of the capacitor voltage. Firing was controlled by the CU instead of the Site 9920 fireset.

After these tests, the project team integrated the components into a single device (Fig. 2).

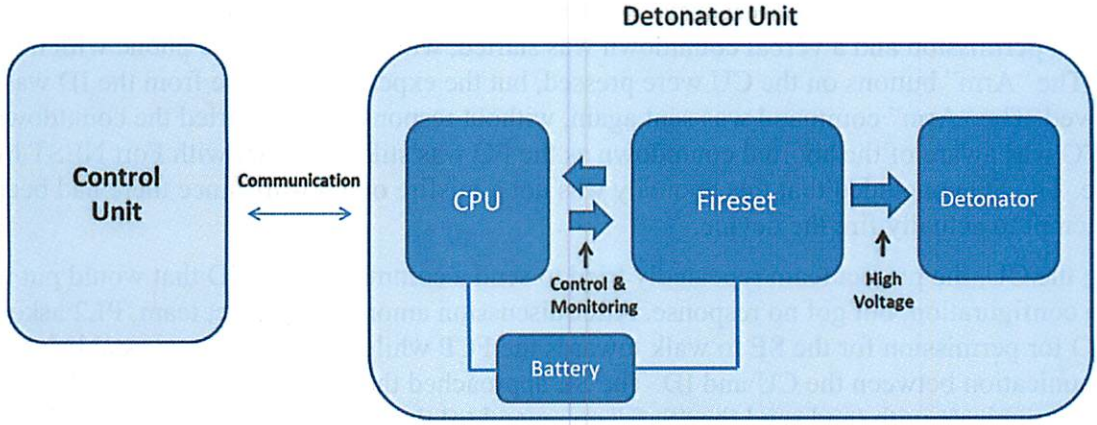

Figure 2: Block diagram of the integrated system

The project team discussed testing the integrated device with Site 9920 personnel in a planning meeting on December 2. Site 9920 personnel concluded that the approved Test Planning, Review and Authorization (TPRA) form from the August 2013 test series would also cover the planned second series of tests. No other TPRA changes were made and a new TPRA for this test series was not developed.

Both the IDs and the CUs used in this test were fabricated at SNL. Assembly was completed on December 4, and they were transported to Site 9920 on December 6.

Testing began on Monday, December 9. Non-explosive tests were performed in the morning, and one explosive test was performed using an ID with a booster and a C-4 charge. During this test the responses received on the CU were not as expected, indicating communication issues

between the CU and ID. The field notes from the ME state that the ID was disassembled and the battery was changed in this unit, though Site 9920 personnel stated that they did not perform this battery change.

Two successful tests were performed on Tuesday, December 10. Three tests were planned for Wednesday, December 11. The first test of the day experienced a problem when the "Arm Enable" light did not illuminate on the CU as expected. Site 9920 personnel recall changing the battery in this unit during the test; the project team does not remember this being done. The test was successfully completed using a replacement ID.

For the second test that day, the FO noted damage on part of the ID. The FO discussed the damage with the project team, who made the decision to continue. This test was to be performed without an optional booster, so the booster was not installed on the ID. After the FO removed the battery tab, energizing the ID, PL2 successfully established communication between the CU and ID. The FO then removed the shorting plug and placed the ID in the C-4. The FO returned to the firing control point (FCP).

Communication between the ID and CU was confirmed, and the "Arm Enable" light on the CU was lit, as expected. PL2, PL1 and the customers took the CU to the selected firing location. As they moved away from the ID, the CU stopped receiving responses from the ID. PL2 requested permission to return to the Fort NEST location so an attempt could be made to communicate from a closer position. PL2 attempted to communicate with the ID when they arrived at Fort NEST and again received normal responses from the ID.

PL2 called the FCP phone to ask permission to continue the test by firing from Fort NEST. The FO gave permission and a verbal countdown was started, with the PL2 on the phone with the FCP. The "Arm" buttons on the CU were pressed, but the expected response from the ID was not observed. The "Arm" command was sent again, without response. PL2 aborted the countdown. The FO was aware of the aborted countdown as the FO was still in contact with Fort NEST by phone. The FO concluded that this anomaly was not a misfire or a no-fire since there had been no attempt to actually fire the device.

Using the CU, the project team repeatedly tried to send a command to the ID that would put it in a safe configuration, but got no response. After discussion among the project team, PL2 asked the FO for permission for the SE to walk towards the FCP while attempting to re-establish communication between the CU and ID. The SE approached the building and continued to try and communicate with (and send the "Safe" command to) the ID. The FO met the SE at the east end of Bldg. 9920; the SE asked if they could attempt to break and then re-establish the communication link. With the FO's agreement, the SE reset and re-established the connection between the CU and ID. However, the Arm Enable light did not come on as it should have. The SE then used the CU to check the status of the ID several times, but the Arm Enable light still did not come on. The SE does not recall sending a command to put the ID in a safe configuration after the connection between CU and ID had been re-established, but did not believe at that point that the ID was armed.

The SE and FO discussed how to proceed, but did not involve others in their discussion. They decided to remove the ID from the C-4 so they could visually inspect the unit. The FO asked the SE if the ID was safe to approach. The SE believed that the ID had not been armed and that it was safe to approach, but there was no visible indicator that could confirm the ID's condition. The SE turned the CU off and placed it on the cart.

The FO approached the ID on the firing pad and removed the ID from the C-4 while the SE remained near the cart. The FO brought the ID back to the cart. The SE repaired the damaged area with a piece of electrical tape. The SE then asked if they could change the battery and the FO agreed. The SE went inside Bldg. 9920 to retrieve a battery and a voltage meter.

The ID circuitry is contained in a compact case that threads into an outer metal tube. The FO began to remove the ID from the outer tube, manually holding the device with the detonator pressed against the heel of the FO's hand, pointed away from the body. The FO tried to unscrew the ID from the outer container, but the device would not rotate. As the FO was attempting to unscrew the ID, the detonator initiated unexpectedly, causing the injury to the FO's hand.

FACTS AND ANALYSIS

Emergency Response

The CO and SE responded immediately after hearing the detonation. They took the FO into Bldg. 9926 to wash the wound. They used gauze from the first aid kit to wrap the injured hand, and electrical tape was used to secure the gauze. No one on site called 911.

The SP1 called to notify the TL about the event. The TL immediately called the Org. 5434 acting manager, who in turn notified the Center 5400 Environment, Safety & Health (ES&H) coordinator. The ES&H coordinator activated a response from Sandia's Incident Command (IC).

Others on site at Fort NEST heard what happened. Some personnel remained at Fort NEST, while others walked back to the FCP. At that point, PL1, PL2, and SE took the FO to Sandia Medical in a government vehicle.

The FO received initial treatment at Sandia Medical, and was then transported to a local hospital, treated and released.

Post-Event Accident Scene Preservation and Management Response

Under direction of the TL, the CO and SP1 secured the site, which included putting away all explosives that were still out into the day magazine.

The ES&H coordinator, safety engineer, explosives safety personnel and others arrived on-site to begin a critique. The IC arrived on site and took action to clean up the biological hazards and secure the site.

The Group 5430 senior manager sent an email to all Group 5430 personnel the morning of December 12, notifying them about the incident and stating "We have also initiated a 'pause' in all Group 5430 explosive operations until further notice."

Assessment of Prior Events and Accident Precursors

The AIB reviewed three events in Sandia's recent past – (1) the unexpected firing of the rocket motor on the Technical Area III Sled Track (October 9, 2008), (2) the lithium fire at Bldg. 6530 in Technical Area III (August 2, 2011), and (3) the improvised explosives and HME training course independent review (November 20, 2012). The joint Sandia-NNSA/SFO Safety Culture Review (February 26, 2013) was also considered as part of this investigation. Issues identified in the causal analyses and incident reports for previous events were similar to what was seen in this event. A key action resulting from the post-Sled Track reviews was the development of the principles of engineered safety. These principles have been integrated into the revised Sandia WP&C manual (MN471021) *Work Planning and Control, Criteria for Safe Design and Operations,* published on April 1, 2013.

In some cases, issues identified for Org. 5434 resulting from assessments performed after those previous incidents had corrective actions that have not been sustained, or corrective actions that were too high-level (e.g., focused on center-level procedures and processes) and not focused on department level actions.

The AIB also reviewed Sandia's processes and management systems for assuring performance and recent assurance and assessments documents for Division 5000, Center 5400, Org. 5434 and

Site 9920. Findings and observations from those assessments were immediately addressed. Recent self-assessments did not identify any issues related to WP&C or conduct of operations. However, FY 2013 quarterly performance summaries from the NNSA/SFO identified activity level performance of WP&C as an area for improvement by Sandia.

Integrated Safety Management (ISM) and WP&C

Corporate Level

As of April 2013, the Sandia corporate procedure ESH100.1.WPC.1, *Plan and Control Work*, requires all new activity-level work accepted after June 1, 2013, to follow MN471021, *WP&C Criteria for Safe Design and Operations*. WP&C under the revised manual supplements the elements of ISM (scoping work, analyzing hazards, controlling hazards, performing work, and feedback and improvement) with additional Sandia-developed engineered safety principles that emphasize the use of critical thinking in how Sandia implements and documents the WP&C for activity-level work (ALW) and design. "Safe by design intent" is a key tenet of this approach.

While new work is required to follow MN471021, legacy work activities are being transitioned to the revised process. The deadline for having all work performed under MN471021 is September 30, 2014. Until that time, both WP&C systems are in use to ensure continued safe operations through the transition. For the work involved in this accident, the project team was conducting its activities under the older WP&C system. Site 9920 had accepted its part of the work after June 1, 2013, and was using their implementation of the revised WP&C approach.

The AIB believes that the engineered safety principles, tenets, and processes of the revised WP&C approach are useful and sound, and should be applied throughout the lifecycle of a project; from paper to production. However, the AIB noted a number of areas in which the current understanding of the intent of the revised approach was lacking, and identified a variety of implementation issues. The following sections discuss implementation of Mission Assurance and WP&C by the organizations involved in the accident.

Defense Systems & Assessments (DSA) Program Management Unit (PMU) Mission Assurance Documents

Work performed as part of the DSA PMU, which includes this project, must follow the DSA principles and the mission assurance process outlined by the PMU. The mission assurance process integrates program/project management, quality management, and system engineering, but does not specifically highlight safety considerations.

For this project, a Statement of Work was developed by the project team that required Sandia to demonstrate, through a test, an integrated capability/device (power source, fireset, and detonator). The project team developed a Project Mission Assurance Category Evaluation (PMACE) and Project Mission Assurance Plan, level D (PMAP-D) for the project in May 2013. A level "D" project is the lowest level of risk.

Center 5900 personnel considered this project too early in the development process to apply their systems engineering process and thus many activities, including design reviews, were not yet required. The AIB believes that such reviews were warranted, given the accepted definitions of Technology Readiness Levels and the fact that the device was to be used to fire explosives. A thorough design review designed to identify hazards present during testing, and to establish

appropriate engineered controls to address them, should have been required before releasing this device for testing with live explosives.

Center 5400 WP&C

Center 5400's WP&C processes are defined in two implementation plans. The older plan is still in use until all Center work is transitioned to the updated WP&C outlined in MN471021, which is codified in an updated plan for Center 5400. Both plans describe the five elements of WP&C and explain how to implement those elements for work within the center.

To analyze hazards, Center 5400 has a procedure and template for conducting Failure Modes and Effects Analysis (FMEAs). The FMEA approach taken by Center 5400 does not implement a step-by-step analysis of what could go wrong in each step of a process, with a subsequent determination of how to prevent and/or mitigate the failure. Instead, Center 5400's FMEA approach analyzes process phases.

Center 5900 WP&C

Center 5900 is in the process of implementing MN471021, but most work is still executed under the old WP&C manual. The focus of WP&C in Center 5900 is on activity-level work being done in the laboratories and facilities that are owned and managed by the center, not design and engineering work. This focus results in a missed opportunity to apply the principles of engineered safety early in the design process to engineer-out hazards that may be present during the development lifecycle, or to ensure that hazards are recognized and alternative protective measures employed.

Organization and Site Project Level WP&C

Project Team (Design)

Center 5900 personnel believed that since no new activity level work was to take place in center-owned space for this project, they were not required to do additional WP&C planning by the old WP&C Manual or MN471021. The AIB believes that the high-consequence nature of the work being conducted should have driven additional WP&C planning.

Development work performed in Centers 2600, 5300, and 2500 for this project was all done under the WP&C requirements for those facilities in which the work was performed. For Centers 2600 and 5300, all work being performed fell within the scope of normal operations for those facilities. For Group 2550 facilities, the work was in scope of normal operations for the first development phase. For the final explosive assembly work done in December, Group 2550 recognized unique aspects of this work that required them to exercise their WP&C processes and to gain additional management approvals before the work could begin.

Site 9920 (Operations)

The previous department manager approved a safety case (required under the revised WP&C Implementation Plan) for Site 9920 operations, which the previous senior manager approved in August 2013. The safety case documents that all required processes and documentation are in place for nominal explosives operations at Site 9920. The safety case credits the Center 5400 ES&H and WP&C processes to identify hazards and implement controls to prevent the defined unacceptable consequences. Consistent with Center 5400 WP&C guidance, the safety case is a summary of other analysis and provides no technical critique of that analysis. Thus, although Site 9920 had implemented the revised WP&C processes, weaknesses in implementation, combined

with basic conduct of operations weaknesses, undermined the effectiveness of their WP&C approach.

Site 9920 personnel developed a TPRA in advance of the August tests that did not fully document the scope of the activities that were ultimately performed; the TPRA was annotated during the test week to address additional test configurations. Site 9920 personnel determined that the August work was within the Site 9920 operating envelope, and therefore, no additional analysis or procedures were required. In December, Site 9920 and project team members agreed that the additional tests could be performed under the existing TPRA, and that no additional analysis or procedures were required.

The FMEA for Site 9920 explosive operations did not address activity level hazards and did not specifically address the hazards associated with this test. The Facility Standard Operating Procedure (FSOP) used to conduct normal operations at Site 9920 also did not address the scope of activities performed in this test. Although both of these documents covered explosive hazards, the controls they contained were not effective for remotely controlled firesets.

When the project team leads and Site 9920 personnel met to discuss the tests, it appears that each side had different expectations of the other. Neither group had sufficient basic knowledge of the other's interests to establish a meaningful and critical discussion about safety. Neither group had a technical basis for concluding that the ID and CU could be tested safely using existing procedures. Neither group asked probing questions of the other to ensure that the ID/CU system could be tested safely using Site 9920 procedures.

Conduct of Operations

While it is recognized that following the specific requirements of DOE O 422.1, *Conduct of Operations,* is not required for this facility per Sandia requirements, the hazardous nature of the work conducted at this site indicates a need to employ a more rigorous or disciplined approach to work than was observed during this investigation.

One focus of a strong conduct of operations program is the development and use of technical procedures. Without effective procedures, the organization must rely on skill-of-the-worker to ensure safety, which may not be appropriate for hazardous operations, especially those that are unique and have not been previously performed. The AIB identified a number of concerns around the procedures used in support of this test.

The FSOP does not include any abort procedures, or procedures for any other anomalous conditions other than misfire or no-fire. There is no evidence that any site or project personnel walked through the FSOP before performing the August or December tests to see how the FSOP applied to the particular nature of the tests or whether design changes were needed to accommodate site procedures. Site 9920 personnel did not recognize that the inability to complete their procedure and checklist as written might suggest the need for a new test-specific procedure to be developed and approved prior to performing the test.

Further, it is not clear whether Site 9920 personnel understood what it means to perform step-by-step procedure adherence. A number of steps from the FSOP could not be followed during both the August and December tests and these were simply marked "N/A" on the checklists used in August. The checklist was not used during the December tests. Management oversight did not reinforce the expectations for effective procedure use at Site 9920.

The Sandia Explosives Safety Manual (SESM) requires procedures for all explosive operations. For the December tests, the project team had informal procedures for the assembly of the IDs, emplacing the device in the C-4, and controlling the use of the CU (which was the equivalent of the control console and key that Site 9920 personnel normally use for positive control of the arming and firing system). These procedures were not Technical Work Documents and would not have met the requirements of the SESM, which requires written procedures for all explosive operations. No procedures were developed for disassembly of the IDs. Site 9920 personnel did not require the project team provide written procedures for these aspects of the operation.

Supervision and Oversight of Work

The Org. 5434 department manager has not historically resided at Site 9920 and has responsibilities for managing staff at a variety of locations across SNL. This, combined with numerous budget, programmatic and personnel responsibilities, makes it difficult to oversee operations on a regular basis. Historically, the department manager has had less of a routine presence at the site than the TL, and has not been routinely engaged in planning or overseeing work at the site. Approvals of TPRAs have typically been done at the team lead level, and it is not clear that the department manager reviewed these documents to provide feedback to the team. Further, department procedures did not reflect that MN471021 requires at least department manager authorization of all work.

The TL holds most day-to-day oversight responsibilities for this site and has the trust of the personnel within the organization. The TL has been a consistent presence for the team. The TL and the current acting manager communicate frequently, but it is the TL who works with the site personnel on a daily basis. It is not clear how much engagement the rest of the site personnel have with the acting manager in the absence of the TL; for example, when the TL was on unscheduled leave prior to the December tests, the acting manager was not called to serve in the test planning role that is usually performed by the TL.

For Team 5434-2, management engagement in operations has been complicated by frequent management changes. Since 2007, there have been 10 department manager changes and four senior manager changes. In many cases, one or both of these roles have been filled in an "acting" capacity and, in some cases, the senior manager was acting in the department manager role in addition to their regular assignment. The frequent manager rotations would make it difficult for any manager to become accepted and trusted by the staff. Even if a manager identified and recognized the need for change within the organization, most were not in place long enough to realize the change, or to ensure that the changes made were sustainable for the long-term. For example, the previous department manager developed a safety case for this site that was approved by the previous senior manager in August 2013. While the safety case is in place, Site 9920 personnel were not familiar with it, and have not adjusted their processes to account for the change. Soon after its implementation, new acting department and senior managers were put in place.

Of the eleven 2012-2013 assessment reports and management walkthroughs reviewed by the AIB, eight of the documented assurance activities found no issues. This raises questions about the rigor of the assessment process being used. Assessments and surveillances that don't identify opportunities for improvement deprive the assessed organization of learning and continuous improvement vital to a learning organization.

Site 9920 personnel promptly corrected issues and observations that were identified. The assessment results may have reinforced the Site 9920 team's perception that their processes and approaches to conducting work met corporate requirements and line management expectations. This perception may have provided a false sense of confidence and reinforced resistance to change designed to improve processes.

Site 9920 was required to undergo a restart activity after the HME incident. The restart required an extent of condition review to address the issues identified by an Independent Review Team (IRT). The IRT identified a number of issues that are very similar to those observed by the AIB during this event. The results indicate that the extent of condition review was narrowly focused and lacked a critical perspective.

NNSA/SFO Oversight

The NNSA/SFO is the onsite federal organization responsible for routine oversight of SNL. SFO conducts its oversight according to an annual Operations Oversight Plan, which follows DOE/NNSA policy and directives for line oversight.

For non-nuclear activities SFO oversight primarily works at the systems level, focusing on how effectively Sandia implements its safety programs and management systems across laboratory operations. Twelve subject matter experts (SMEs) oversee ES&H functions. Rather than attempting to cover the entire set of non-nuclear facilities where potentially hazardous work may occur, focus is placed on functional reviews of facilities identified in a risk ranking process performed by SFO. In addition, SFO has one facility representative for non-nuclear facilities who provides operational oversight of moderate hazard facilities and operations at Technical Areas III and IV.

The SFO Operations Oversight Plan highlighted WP&C as a key operational performance issue identified by SFO in its FY2013 quarterly evaluation reports.

Human Performance Analysis and Interfaces

Design

The role of system integrator was accomplished by a team of individuals from Center 5900. A systems integrator looks at the design as a complete system, rather than a series of independent components.

According to Center 5900 management, a "systems engineer" would have been assigned to the project during the next stage of development. Personnel and management from Centers 2500, 2600, and 5300 indicated that they did not have a clear understanding of how the role of system integrator was being accomplished for the project.

The project team consistently emphasized that they started with legacy component designs, and their completed PMACE documentation referenced the use of commercial off-the-shelf (COTS) parts. Since a safety theme for the device was not established, component safety was analyzed without the benefit of a systems context. A number of component SMEs noted that they may have made different design choices if they had had a better understanding of the entire system. While the project team thought they shared all relevant information, the project team may not have recognized how additional information might have informed the design choices of the

component designers. The project team also did not understand what hazards might be introduced by the combination of legacy components.

Due to classification issues and project sensitivities, much of the work performed by Center 5900 presents unique communication challenges among project team SMEs. Staff working on these projects may be reluctant to give information out of caution related to classification or sensitivity issues (better to say too little than too much), and others may have been "trained" over time to avoid asking too many questions about these projects. The AIB observed these behaviors and believes they resulted in inadequate communication about the project, which limited the amount of information shared and impacted system safety.

Planning

During AIB interviews, the project team used descriptions like "proof-of-concept" and "prototype" to describe the device, and acknowledged that a significant amount of engineering and analysis needed to be done before fielding a final product. However, it is not clear what was communicated to Site 9920 personnel about the state of the device's development. Site 9920 personnel believed that, while some minor changes might be made after this test series, the component designs were essentially final. The ID showed to Site 9920 personnel during the December planning meeting and used during the December test series looked like a finished product, perhaps in an attempt to demonstrate accomplishments to the external customers. Further, Site 9920 personnel understood that any extra devices not used during the test series might be transferred to the external customers. Project team personnel confirmed that this possibility had been discussed, though no formal negotiations had occurred. This would have reinforced to Site 9920 personnel the idea that this was a finished product, rather than a prototype.

The project team personnel are not explosive SMEs and they relied on Site 9920 personnel to tell them what was needed to test their device safely. In discussions with the AIB, the project team indicated that they would have been willing to make design changes to accommodate Site 9920 requirements. It is not known how this was communicated to Site 9920 personnel (e.g., were they waiting for site personnel to make suggestions, or did they ask specifically if any changes were needed). Also, the short time interval between the planning meetings and the test dates (in both August and December these meetings occurred one week before testing) would not have sent the message that many design changes were possible. There was no recognition that Site 9920 personnel may not have the right expertise to ask the right questions, or that the sensitive nature of the project may have made the site personnel unwilling to ask detailed questions about the design and function of the device. The project team personnel did not ask to step through the approved Site 9920 FSOP, nor were they asked to do so by the Site 9920 personnel. Such a review, including procedures covering anomalies, would have helped to identify whether adherence to the FSOP would require a design change, or whether new test protocols were needed to otherwise accommodate the test procedure requirements.

Operations

It was clear that control of site access, permission to fire, and movement within the site was maintained by the FO and CO at Site 9920 during this test series. All members of the project team indicated that they knew that the FO was in charge of the site. The project team specifically discussed asking permission from the FO and CO to take specific actions, and the project team remained in communication with the site personnel during arming and firing operations.

However, because the FO did not have specific technical knowledge about the device being tested, there was a reliance on the project team for detailed input and direction about the operation of the device itself. For example, assembly of the devices was performed using an informal procedure, under supervision and direction of the ME (a member of the project team). The preparation of the devices during the test operation was done under direction of the project personnel who were operating the CU during set-up, and the project team personnel remained in control of the CU during the entire test. The confidence in the project team's (implicit) assertions about their ability to control the device, coupled with an overall lack of understanding of system hazards, led the FO to rely on the input from the project team when making critical operational decisions.

A number of Site 9920 personnel interviewees suggested that the results from the August testing had reinforced their understanding of how the system operated because device voltages and signals were monitored during those tests. Further, events earlier in the December test week, such as successful battery changes and successful troubleshooting of communication issues on previous tests, impacted the decisions made during this anomalous test. These factors may have led the FO and the SE to place too much faith in the status indicators on the CU, which, in this case, actually gave incorrect information about the ID's state. Further, the confidence in the design then contributed to the decision to manually remove the ID from the C-4 and to troubleshoot following the test anomaly.

The FO and SE jointly decided the FO should approach the device and remove it from the C-4; they made no attempt to discuss the planned course of action with the other project team personnel or with other Site 9920 personnel. The project team identified the PL2 as their single point of contact for the tests. However, Site 9920 personnel stated that they saw the project team members as interchangeable; any of the project team could speak for the project, even during the explosive tests.

The dual-hatting at Site 9920 of the FO position with that of the SO position may have also made it more difficult to get input from other Site 9920 personnel, or to get independent checks on safety related actions. However, other Site 9920 personnel stated that, given the information available at the time, they would have not raised concerns about approaching the device or removing it from the C-4.

Sandia Explosives Safety Manual (SESM)

The SESM provides requirements for all explosive operations performed at SNL. The SESM outlines the general process to follow in the event of a misfire. The SESM definition simply states that a misfire is the "failure of a component to function as designed." By this definition alone, CU/ID failures to perform as expected before the accident could be defined as misfires. However, the SESM includes misfire procedures that only make sense if a misfire results from an energy pulse to the firing circuit (SESM 2-13.7). By that practical definition, Site 9920 personnel determined that it was not a misfire when the ID did not respond to the CU commands as expected. However, the SESM does not include requirements for procedures for anomalies such as a failure to arm.

The SESM (SESM 2-1.1S) has a general requirement that all firing of explosives or explosive components must be performed with approved firesets. However, Sandia does not have a process

defined for approving firesets. Further, there is question as to the applicability of this requirement to developmental firesets.

In fact, the manual is silent on developmental firesets. In the absence of clear requirements it is the established position of the Sandia Explosives Safety Office that criteria for firesets are not directly applicable to developmental firesets. This includes the requirement to use approved firesets. Consequently, a general set of explosive safety criteria does not exist to ensure that developmental firesets achieve an acceptable level of maturity and safety prior to being mated to explosives.

Technical Analysis Team (TAT) Analysis

The TAT identified a number of hardware and software weaknesses in the design of the CU/ID system and used the scientific method to analyze the incident. Failure hypotheses considered were triggering events generated by mechanical manipulation, electromagnetic interference (EMI), and ESD.

It was demonstrated that an armed ID can be easily triggered by either mechanical or electrical mechanisms. These include mechanical insults that can momentarily disrupt battery voltage, thereby resetting the electronics due to a software initialization error, or EMI/ESD events, which can trigger the unit or upset the electronics. Both of these conditions were demonstrated in the laboratory. The system also had weaknesses in maintaining state synchronization between the CU and ID. The exchange protocols provided basic synchronization, but were not robust to losses of communication that resulted in misinforming the operators of the ID's current state.

The system's hardware safety features were not fail-safe and provided "forward only" safety. The software is in sole control of arming and firing for the system and therefore either the software must be designated as safety software by Sandia's corporate procedure IM100.3.5, *Provide Quality Software*, or the hazards must be controlled by means other than the software.

The TAT concluded that, since the device is a prototype and the software has not been designated as safety software, the electronics should not be trusted and a proper test setup and procedures are necessary to assure safety. The test setup and procedures used for this test did not properly control the hazards.

SUMMARY OF CAUSAL FACTOR ANALYSIS

The AIB used event charting, barrier analysis and change analysis to conduct the causal analysis. After this analysis, the AIB identified conclusions (contributing causes) that can be grouped into four core causes.

Direct Cause

The direct cause of this accident was a failure in the ID, most likely from mechanical disturbance or ESD, which caused an unexpected detonation.

Core Causes

Failure to effectively implement "safe by design" intent

The system hazards created as a result of combining individual components were not adequately considered, analyzed, or understood by the project team. While it is recognized that this design was a prototype, the number of hardware and software weaknesses found during the TAT analysis, combined with the lack of a safety theme and system integrator during the design process, indicate that not all opportunities to design out these weaknesses had been adequately explored during the design process. It is not clear that the project team considered this design to be "born unsafe," especially considering the reliance on known, legacy components. Further, the project team was not aware of the safety requirements (such as SESM requirements for approved firesets and technical work documents for explosive operations) that applied to, or at least could provide guidance for, this project.

Finally, hazards that could not be designed out of the device were not fully understood or explicitly articulated by the project team, and a "what-if" analysis (or similar failure analysis) was not conducted prior to the testing. Thus, the AIB concludes that a high-consequence event with this device was inevitable once it got to the testing phase if, as happened, the device was relied upon to provide safety. A developmental fireset should be considered armed and likely to discharge without further stimulus from the moment it is energized, and appropriate external engineered controls are required to ensure personnel safety.

Insufficient WP&C of test operations

The Site 9920 team accepted, and then executed, work that their existing hazards analysis and operating procedures did not address without first analyzing the hazard, identifying and implementing controls.

An expert-based process was used to evaluate whether these tests fell within the approved Site 9920 operating envelope without a detailed review of the existing procedures. For example, Site 9920 personnel developed a TPRA for the August tests, but it did not fully describe the scope of the activities. They then used the same TPRA for the December tests without modifications to address the technical changes in the device.

Line management in this organization had not been effective at identifying and correcting weaknesses in WP&C and conduct of operations. In some cases, assessments were ineffective at identifying the issues while, in other cases, corrective actions put in place to address identified weaknesses from previous assessments were not sustained.

Insufficient integration and understanding of the project

The project team and Site 9920 personnel did not interact in a systematic, comprehensive and acceptable manner to develop and deploy adequate layers of defense against unrecognized hazards. There were clear differences between the two groups in their understanding of the development stage of the device; the project team understood the device to be a prototype and Site 9920 personnel understood the device to be much closer to a finished product.

Given that the project team did not fully understand the hazards associated with their device, they could not communicate those hazards to Site 9920 personnel. Further, the project team did not communicate that the hazards were actually unknown, so that the device could be treated appropriately throughout the testing. Project classification and/or sensitivity may have also (even inadvertently) affected communication between the two groups.

Finally, during the tests, Site 9920 personnel had to rely on the project team for technical information about the system. The August testing, as well as the tests earlier in the week of the December tests, reinforced Site 9920 personnel's confidence in the system operation. Neither the project team nor Site 9920 personnel understood that it was possible for the system design to result in incorrect information about the state of the ID being communicated by the CU, and thus did not make conservative decisions with this perspective.

Approach to maturing safety practices and discipline has left some workplaces behind

As is true at all NNSA sites, Sandia's diverse workforce has varying levels of safety practice maturity. Typical approaches to advancing the maturity of safety culture have not been sufficiently tailored to reach all individuals in the workforce, according to their individual needs. For lasting change, organizations need to know that they must change, and their management must both commit to affecting needed change and engage the hearts and minds of individual workers. Those seeking to affect lasting change should pay particular attention to the "outliers" in order to help them reach the desired end state.

The revised approach to WP&C, including engineered safety principles, is in transition across Sandia. Group 5430 has already updated their procedures and guidance documents, and is in the process of updating the documentation for specific operations. In fact, Site 9920 already has an approved safety case and falls under the revised WP&C approach. However, weaknesses were observed in the department-level documents and practices as well as in the guiding center-level procedures that were followed. This suggests that the intent of the WP&C changes may not have been effectively communicated to, and/or fully understood in, this organization.

Center 5900 is still in the process of transitioning to the revised WP&C approach. Interviews suggested that their center implementation is focused on laboratory spaces, neglecting the design and engineering activities that may affect work in those (or other) spaces. This also suggests that the full intent of the revised WP&C approach may not be fully understood in this organization. The AIB believes similar misunderstanding is likely to be common throughout Sandia as the corporation continues to educate its workforce on the revised approach to WP&C and engineered safety principles.

CONCLUSIONS AND JUDGMENTS OF NEED

The conclusions and JONs are listed in the tables below. In addition, the AIB has two final thoughts from this review.

First, the hardware and software design issues found by the TAT confirm that the device had hazards that had not been previously identified and addressed prior to testing. The AIB acknowledges that it may not be possible for all hazards to be engineered out of a prototype device and testing is often how prototypes come to be understood. However, in cases where "safe by design intent" is not feasible directly in a developmental device, it is crucial for the state of the design to be accurately characterized and communicated to all those who will be working with the device so that appropriate compensatory measures can be applied.

In this case, the project team did not explicitly recognize the hazards that were introduced by combining legacy components and were not aware of the safety issues associated with the device. Thus, they did not accurately communicate those hazards to the Site 9920 team so that appropriate mitigations could be put in place. This suggests that a high-consequence event with this device was likely even if it was tested elsewhere, unless mitigating safety measures were adopted prior to testing. Regardless of the specific weaknesses of this device, a developmental fireset should be considered armed (and likely to discharge without further stimulus) from the moment it is energized, so that appropriate external engineered controls can be applied to ensure personnel safety. The AIB recommends adopting a policy that prototype designs are "born unsafe" until proven safe through technical understanding and review.

Second, the lack of rigor surrounding WP&C and the formality of conduct in the explosive operations at Site 9920 suggests that an accident at the site was likely with another test, even if they had not accepted this particular project work. The lack of critical thinking during work planning, the expert-based approach to evaluating their operating envelope, and not stopping work when existing site procedures could not be performed as written, made an accident inevitable unless conduct of operations were improved. Given that a device may not, or cannot, be safe by design intent, it is crucial that the "testing system" be safe by design intent.

The specific conclusions identified by the AIB are below in Table 1 and represent the causal factors (causes). The conclusion numbers reference the AIB technical basis document, which provides additional supporting discussion that should be considered when developing corrective actions. The JONs identified by the AIB are shown in Table 2. The AIB strongly recommends critical thought be applied to corrective action development, especially when adding new or revised processes, to assure they are appropriate, effective, and do not overshadow practical safety and WP&C considerations. A review of current processes to remove inefficient processes should also be considered.

Table 1: Site 9920 Accident Investigation Conclusions

Cause No.	Conclusions (Causes)	JON
	Core Cause: Failure to effectively implement "safe by design" intent	
C09	The project team did not recognize that concept design should be considered 'born unsafe.'	1, 6
C15	The project team leads did not recognize the need for a comprehensive design review of the entire system to ensure safety prior to testing with live explosives.	2
C28	The project team did not understand the hazards introduced by the combination of legacy components.	2
C18	Executive management expectations of the implementation of WP&C were not met. Center 5900 believed that WP&C did not directly apply to their role in this project.	1
C19	Because of deficiencies in the design approach, the accident could have happened any time the battery was installed in the unit.	1, 2, 6
C27	There was no "system integrator" responsible for the safety of the integrated device.	2, 3
C40	The project team did not engage safety professionals early in the design process.	1, 5
C03	There is ambiguity in the Sandia Explosives Safety Manual (SESM) requirements and definitions specific to developmental fireset design and control.	12
C07	The Defense Systems & Assessments (DSA) Mission Assurance structure does not integrate safety and security as essential to mission assurance.	3
	Core Cause: Insufficient WP&C of Test Operations	
C02	There is ambiguity in the SESM requirements and definitions specific to anomalous test conditions.	12
C04	Center 5400's implementation of Failure Modes and Effects Analysis (FMEA) is weaker than the robust traditional FMEA approach of rigorous step-by-step activity hazard analysis.	10
C05	Center 5400 does not require a step-by-step job specific activity hazard analysis.	10, 11
C06	The Center 5400 explosive safety implementation using the rigor tool could lead to noncompliance with the SESM.	10, 11
C08	The project team used un-approved procedures to direct explosive operations.	10, 11
C10	The Team 5434-2 procedure for developing a Test Planning, Review and Authorization (TPRA) and accepting work does not require department manager approval as required by Sandia's WP&C manual: MN471021.	10, 11
C11	The Site 9920 FMEA does not adequately analyze the hazards associated with routine activity-level work performed at Site 9920.	10
C12	The Site 9920 FMEA does not address the hazards of developmental firesets.	10, 12
C14	Site 9920 uses an expert-based approach to evaluate work and determine whether a test is within their operating envelope.	10, 11
C16	The TPRA approved in August did not cover the December tests, nor did it accurately describe the scope of the tests performed in either test series.	10, 11
C17	Some explosive procedures in the Facility Standard Operating Procedure (FSOP) are not addressed in the FMEA.	10, 11
C30	The decision that this test fell within the existing operating envelope was performed without a thorough evaluation of existing procedures.	10, 11
C31	The Site 9920 process does not require independent review of the decision to use an existing TPRA to cover additional work.	10, 11

C36	Combining the FO and Safety Officer (SO) roles is not a sound safety structure.	11
C38	Day-to-day management engagement in Team 5434-2 was not sufficient to assure safety.	10, 11, 13
C20	The Site 9920 FSOP (FSOP-EFS-001) does not include procedures for test anomalies, with the exception of misfire and no-fire conditions.	10, 11
C21	The level of operational rigor exhibited by the Site 9920 operations does not meet expectations commensurate with the level of hazardous operations performed at the site.	11
	Core Cause: Lack of integration and understanding of the project	
C34	The project team inadvertently conveyed to Site 9920 personnel more confidence in the safety of the test device than was warranted.	5
C13	Site 9920 personnel did not (and could not technically) recognize the significant hazards in the experimental system. Rather than treating its safety as an unknown, they relied on perceived assurances of safety from the project team.	5, 6, 10, 11
C32	Differences in understanding of the state of the development of the test components, and lack of effective discussion about the hazards introduced by integrating legacy components, contributed to the lack of critical thinking or questions during the planning for this test series.	1, 5,
C29	Classification and sensitivity around the project inhibited effective communication; both among the project design team and with Site 9920 personnel.	4
C33	During the test activities, neither Site 9920 personnel nor the project team took a conservative approach to decision making.	6, 10, 11
C35	Reliance on project personnel contributed to the erosion of the FO's ability to make independent, conservative decisions regarding the test.	5, 6, 11
C37	Site 9920 personnel did not recognize a single point of contact from the project team during the test series.	5
C26	Current Sandia Field Office (SFO) oversight approach does not ensure that every facility is visited. Graded approach for periodicity should not equal zero.	7
	Core Cause: Approach to maturing safety practices and discipline has left some workplaces behind	
C01	The effort to educate and mentor all levels of management in the engineered safety principles and their appropriate application has not yet achieved the desired effect.	10
C41	Sandia has not identified the outliers who are further behind in recognizing the need for safety improvement and discipline.	8
C39	There has been insufficient management engagement to ensure that the intended focus of WP&C improvements on critical thinking and analysis (as opposed to updated processes and paperwork) is understood and implemented in some line organizations.	10, 13
C22	WP&C improvements made in Team 5434-2 as a result of ID-016 (corrective actions that were taken after the Sled Track incident) were not sustained.	8, 9
C23	Management did not ensure identified WP&C weaknesses were effectively addressed at the department level.	8, 10
C24	Center 5400 line management (from team lead through director) self-assessments did not identify the weaknesses in safety performance of explosive operations that contributed to this accident.	9, 10, 13
C25	Center 5400 line management (from team lead through director) processes do not assure that corrective actions are completed and effective.	9, 10, 13

Table 2: Site 9920 Accident Investigation Judgments of Need

	Judgments of Need	Related Conclusions
1	Sandia needs to develop and implement a plan for applying WP&C and the underlying engineered safety principles, to Sandia's design functions - at all stages of lifecycle (conceptual through test to deployment)	C09, C18, C19, C32, C40
2	Sandia needs to make sure applicable requirements are clearly understood and responsibility for safety of the integrated design and its technical review is well-defined - at all stages of lifecycle (conceptual through test to deployment)	C15, C19, C27, C28
3	Sandia needs to ensure, demonstrate, and communicate an integrated approach to mission assurance (safety, security, WP&C, quality, financials, formality, etc.)	C07, C27
4	Sandia needs to ensure that safety comes before security, and constitutes project need-to-know.	C29
5	Sandia needs to develop and implement a process to ensure all participants have a common understanding of project scope, level of development, requirements (design and test), roles & responsibilities, communication paths, etc. from project inception to completion.	C13, C32, C34, C35, C37, C40
6	Sandia needs to ensure design and activities, including those combining established technologies or commercial off-the-shelf (COTS) parts, are presumed "born unsafe" until they are proven safe through technical understanding.	C09, C13, C19, C33, C35
7	SFO needs to develop and implement a plan for oversight of *all* operations using a graded approach.	C26
8	Sandia needs to use an extent of condition approach, in addition to self-assessment, to find those organizations without mature WP&C implementation (outliers) and focus improvement efforts on them.	C22, C23, C41
9	Sandia needs to assure, through critical and rigorous assessment and continuous learning, that WP&C improvements are sustained within organizations at the management and worker levels.	C22, C24, C25
10	Sandia needs to ensure there is a common understanding of corporate WP&C expectations and engineered safety principles for activity-level work, and implements the tools effectively.	C01, C04, C05, C06, C08, C10, C11, C12, C13, C14, C16, C17, C20, C23, C24, C25, C30, C31, C33, C38, C39
11	Sandia needs to establish a more formal and disciplined conduct of operations approach for all activity-level work, using a graded approach based on the hazard of the work, not the facility.	C05, C06, C08, C10, C13, C14, C16, C17, C20, C21, C30, C31, C33, C35, C36, C38,
12	Sandia needs to update its corporate safety documents to clarify requirements on experimental and developmental work, including response to test anomalies.	C02, C12, C03
13	Sandia needs to require management engage deeply at the operational level with their staff and operations.	C24, C25, C38, C39

ACCIDENT INVESTIGATION BOARD

Don Nichols, Associate Administrator for Safety and Health
National Nuclear Security Administration
AIB Co-Chair

Michael W. Hazen, Vice President
SNL Division 4000, Infrastructure Operations
AIB Co-Chair

Carol Adkins, Director
SNL Center 1800 Materials Science & Engineering
AIB Team Lead

Marcelino Armendariz, Manager
SNL Org. 1751, RF and Optics Microsystem Applications
micro-electronics, systems knowledge
deputy TAT Lead

Noel Duran, Environment, Safety, and Security Professional
SNL Org. 4021, Division ES&H, S&S Quality Ops
causal analyst, accident investigator

Ralph Fevig, Safety Engineer
SNL Org. 4122, Safety Engineering
causal analyst, accident investigator

John Franchere, CSP
Safety Engineer
NNSA/Sandia Field Office
accident investigator

Philip Heermann, Senior Manager
SNL Org. 6530, Intelligent Systems, Robotics, and Cybernetics
TAT Lead, accident reconstruction

Mike Lopez, Manager
SNL Org. 1679, Z HEDP Research Accelerator
high rigor operations SME

Timothy Wallace, Safety Engineering Technologist
SNL Org. 4122, Safety Engineering
explosives safety SME

Caren Wenner, Manager
SNL Org. 0431, Human Factors
human factors SME

Michael Zamorski, Employee Involvement Leader
NA-00.1, National Nuclear Security Administration
safety culture SME