Accident Investigation Board (AIB)

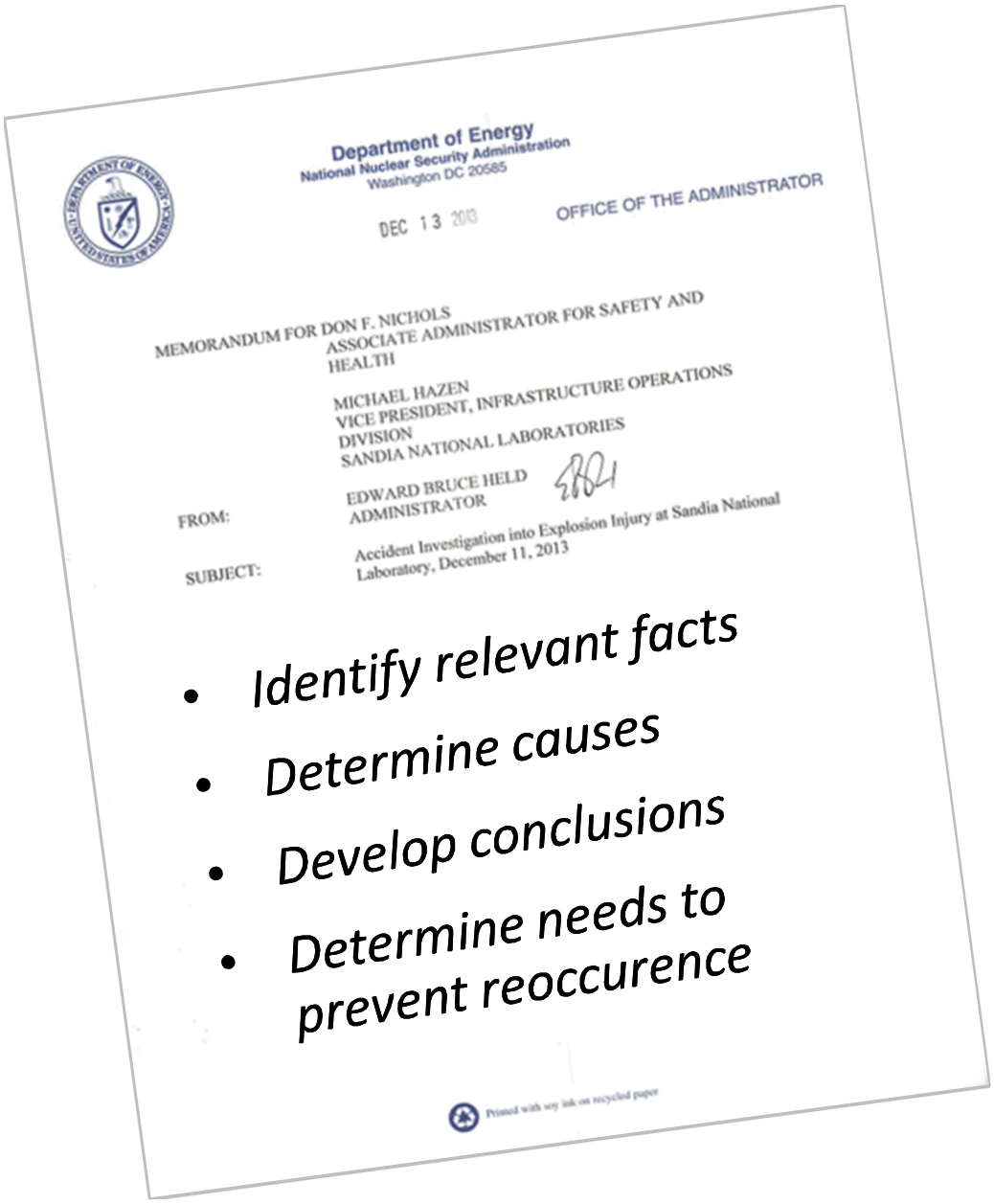
for the Test Site 9920 Event

SAND2014-16600PE

Carol Adkins, 06100

National Nuclear Security Administration

Sandia National Laboratories



Department of Energy
National Nuclear Security Administration
Washington DC 20585

DEC 13 2013 OFFICE OF THE ADMINISTRATOR

MEMORANDUM FOR DON F. NICHOLS
ASSOCIATE ADMINISTRATOR FOR SAFETY AND HEALTH

MICHAEL HAZEN
VICE PRESIDENT, INFRASTRUCTURE OPERATIONS DIVISION
SANDIA NATIONAL LABORATORIES

FROM: EDWARD BRUCE HELD
ADMINISTRATOR

SUBJECT: Accident Investigation into Explosion Injury at Sandia National Laboratory, December 11, 2013

- *Identify relevant facts*
- *Determine causes*
- *Develop conclusions*
- *Determine needs to prevent reoccurence*

Printed with soy ink on recycled paper

TEAM PRINCIPLES

- Maximize the investigation as a **learning experience**, not just for Sandia, but for the entire DOE Complex
- Find **solutions**, rather than blame while respecting individuals
- Review the event using the **principles** of Integrated Safety Management, **Safety Culture**, Human Performance Improvement and **Engineered Safety**
- Demonstrate a **Just Culture** by looking at the event as a result of a system of interoperable parts, not an individual failure, and find the underlying causes, not just 'surface' causes

AIB CORE TEAM

Don Nichols *Co-Chair*	NNSA
Michael Hazen *Co-Chair*	4000
Carol Adkins *AIB Team Lead*	1800
Philip Heermann *TAT Lead*	6512

AIB TEAM

Caren Wenner	0431
Mike Lopez	1679
Marce Armendariz	1751
Ralph Fevig	4122
Noel Duran	4021
Tim Wallace	4122
Mike Zamorski	NNSA
Jef Franchere	NNSA

TAT TEAM

Kim Merewether	0434
Pat Smith	1732
Marce Armendariz	1751
Robert Brocato	1751
Matt Celina	1819
David Damm	2554
Tim Wallace	4122

SUPPORT TEAM

Bess Campbell-Domme	4021
Pam Maestas	4024
Stephanie Holinka	3651
Robin Johnson	TCR

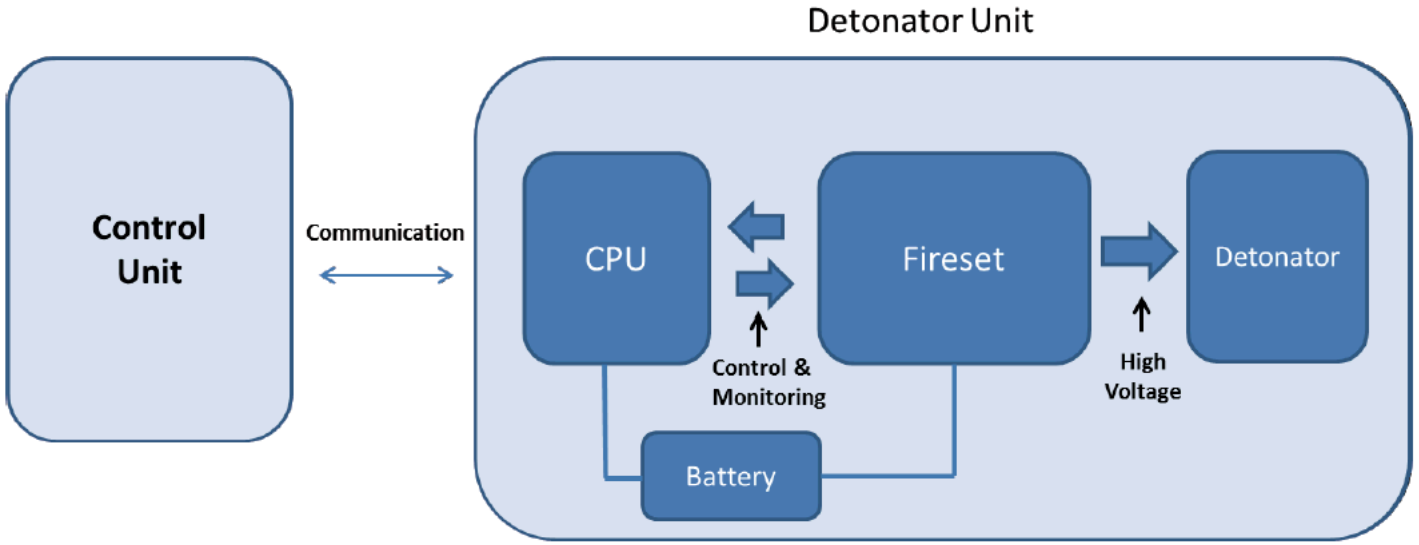
EVENT SUMMARY

During an explosives test at Site 9920, an individual received an injury to their left hand when the detonator in the test unit fired during troubleshooting.

TECHNICAL ADVISORY TEAM (TAT)

Conducted scientific and engineering analysis and provided technical expertise

- Review and understand the design
  - Conduct design reviews (both hardware and software)
- Determine potential failure paths

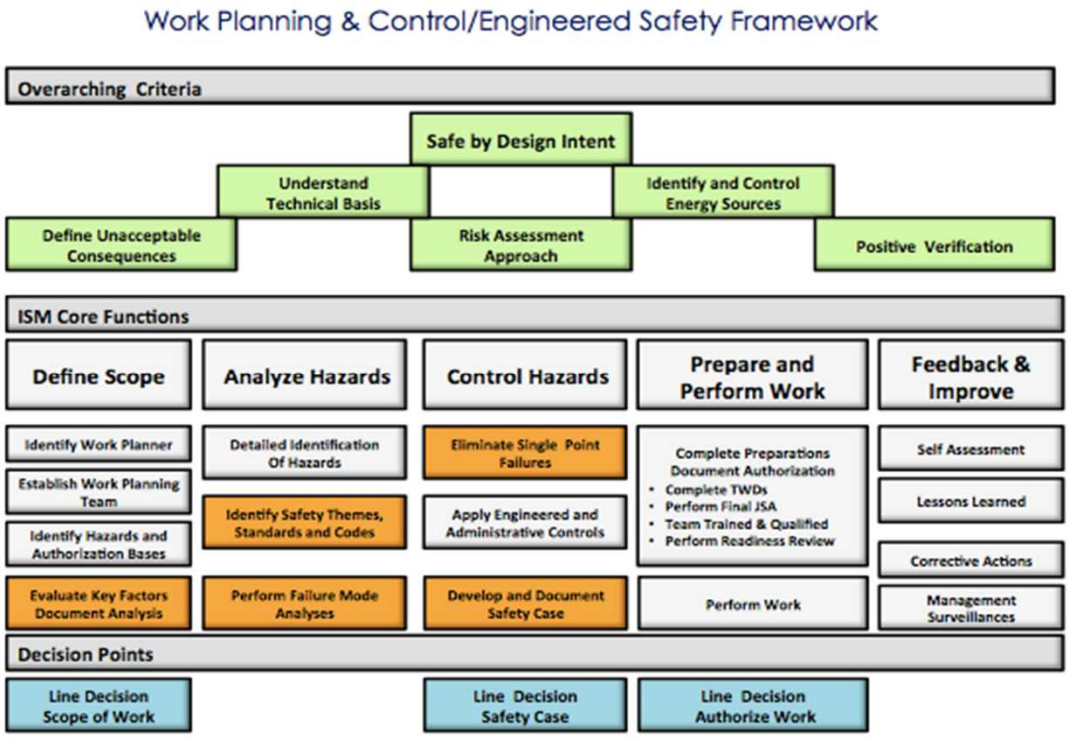


WHY THE CONCERN… ?

From XPL160 Training Video

DIRECT CAUSE

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



CORE CAUSES

① Failure to effectively implement “safe by design” intent

② Insufficient WP&C of Test Operations

③ Lack of integration and understanding of the project

④ Differing safety culture maturity levels

1: FAILURE TO EFFECTIVELY IMPLEMENT "SAFE BY DESIGN" INTENT

Design group did not analyze the development and testing cycle of the device, make the device as safe as they could, and require it to be treated as unsafe while engineered safety protocols were being confirmed.

ENGINEERED SAFETY IN DESIGN

Fireset Design

- Recognized that safety of the system is inherent in the system design, not the design of individual components.
- Made safety recommendations to other component designers, such as the use of the shorting plug.
- Designed in safety features, such as the LED light.

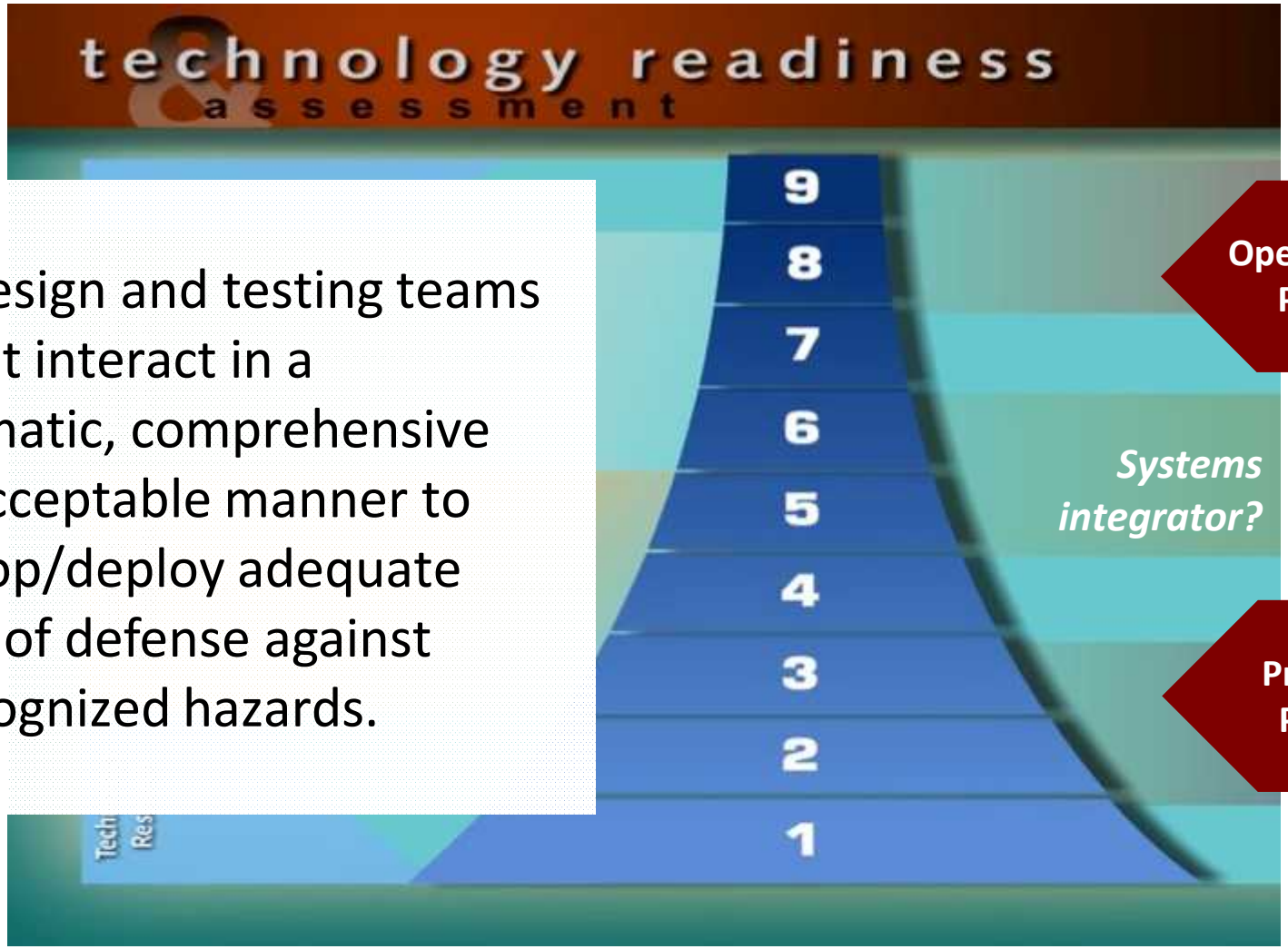
Explosive Assembly

- Applied engineered safety principles when installing the detonator into the test unit.
- Understood the technical basis by learning enough about the test unit to apply three controls to ensure energy would not reach the capacitor.
- Exhibited defense in depth by assuming the detonator would initiate anyway; used a blast shield to protect the worker.

2: INSUFFICIENT WP&C OF TEST OPERATIONS

The operations group accepted and then executed a job that their **existing hazards analysis** and operating procedures did not address, without analyzing the hazard, identifying controls & implementing controls.

3: LACK OF INTEGRATION AND UNDERSTANDING OF THE PROJECT



The design and testing teams did not interact in a systematic, comprehensive and acceptable manner to develop/deploy adequate layers of defense against unrecognized hazards.

4: DIFFERING SAFETY CULTURE MATURITY LEVELS

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.

People who think they "get it," but don't

People who don't realize they need it

IS THIS INCIDENT RELEVANT TO DIVISION 8000?

Do you…

- Have matrixed work?
- Do troubleshooting?
- Do active verification?
- Follow all your processes?
- Communicate well with your partners?
- Modify equipment?
- Have security-driven communication challenges?
- Understand the requirements?
- Understand what is in/out of scope for the safety case?
- Do the critical thinking about how things could go wrong?
- Challenge each other?
- Think about test and use during design?
- Clearly understand and communicate the level of maturity of a design to others?

Accident Investigation Board (AIB)

for the Test Site 9920 Event

Marcelino Armendariz
01751

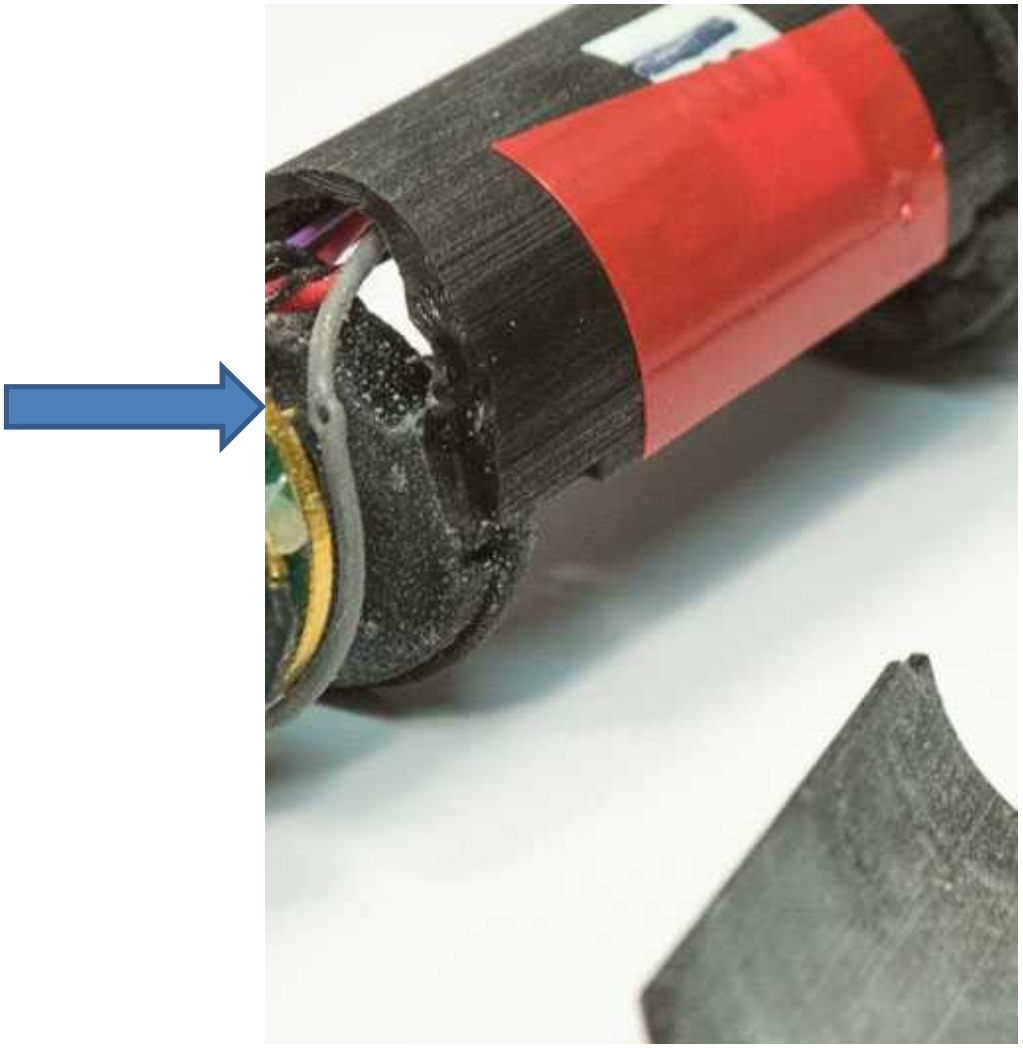
National Nuclear Security Administration

Sandia National Laboratories

Technical **A**dvisory **T**eam

- TAT was formed to provide technical expertise to the AIB.
  - *Understand the technical aspects of detonator initiation (failure modes that contributed to the incident)*
- Composed of experts in firing sets, energetic materials, polymer materials,communications electronics, microprocessors, EM/ESD
- TAT was primarily focused on answering the following question:
  - *Why did the detonator go off when it did?*

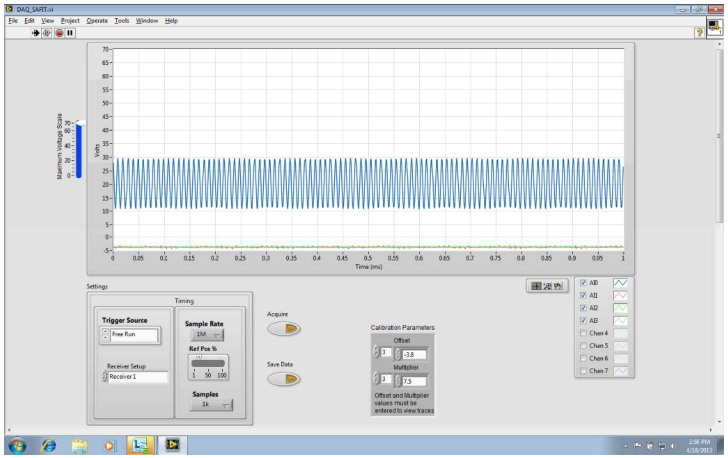
Punctured cable and electronics compartment fragmentation



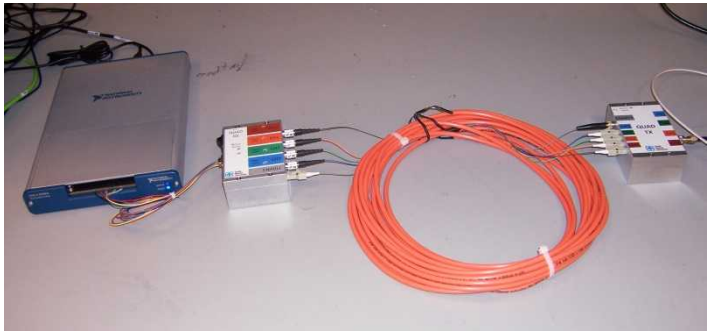
Items that helped expedite analysis

- Evaluation Units available for TAT analysis
- Design reviews with TAT & Design Team
- Device without a detonator immediately available for analysis
- Rapid prototyping of mechanical samples
- Sandia Arming & Firing Integrated Telemetry (SAFIT) available for measurements

SAFIT: Sandia Arming and Firing Integrated Telemetry

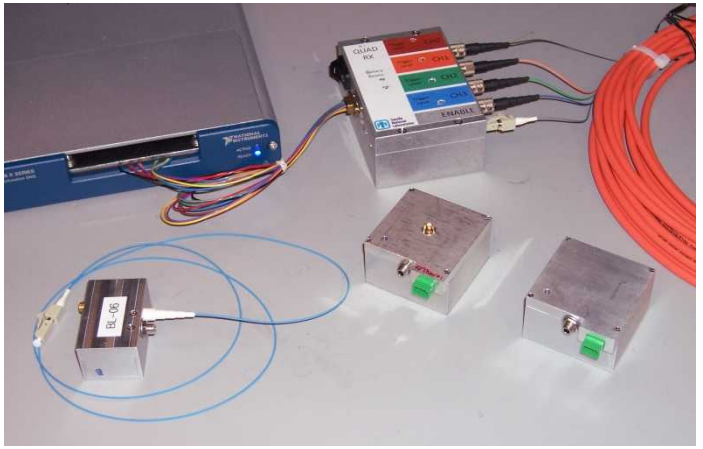


Labview-based display of up to 8 simultaneous signals



Fiber-optic telemetry of low and high voltage signals. Basic setup is shown: ARM, FIRE, low voltage, and high voltage.

Portable data collection using laptop and digitizer



Additional sensors include RF field power, magnetic field, high current discharge (CVT), and small current or voltage sitting at a very high voltage.

Plausible Scenarios

FO attempted to remove the detonator assembly from its housing and found that the threads were seized. On his second attempt, FO applied additional torque to the detonator (based on testimony).

This level of torque caused significant distortion of the interior plastic housing which contained the electronics (verified by lab testing)

- ***Scenario 1***: The distortion led to an intermittent power connection which reset the microprocessor and generated an unintended firing signal

- ***Scenario 2***: Human ESD in the vicinity of the detonator caused the CDU to trigger (demonstrated in the lab)

Scenario 1

- The distortion led to an intermittent power connection which reset the microprocessor and generated an unintended firing signal
  - TAT demonstrated in the lab that a momentary power glitch will reliably cause the microprocessor to reset
  - When the microprocessor resets, it briefly sends a FIRE signal which is sufficient to reliably trigger the CDU
  - The power glitch can be caused by a mechanical shock equivalent to dropping the detonator onto a hard surface from 1/16”.
  - Distortion of the housing is plausible, but was not demonstrated in the lab

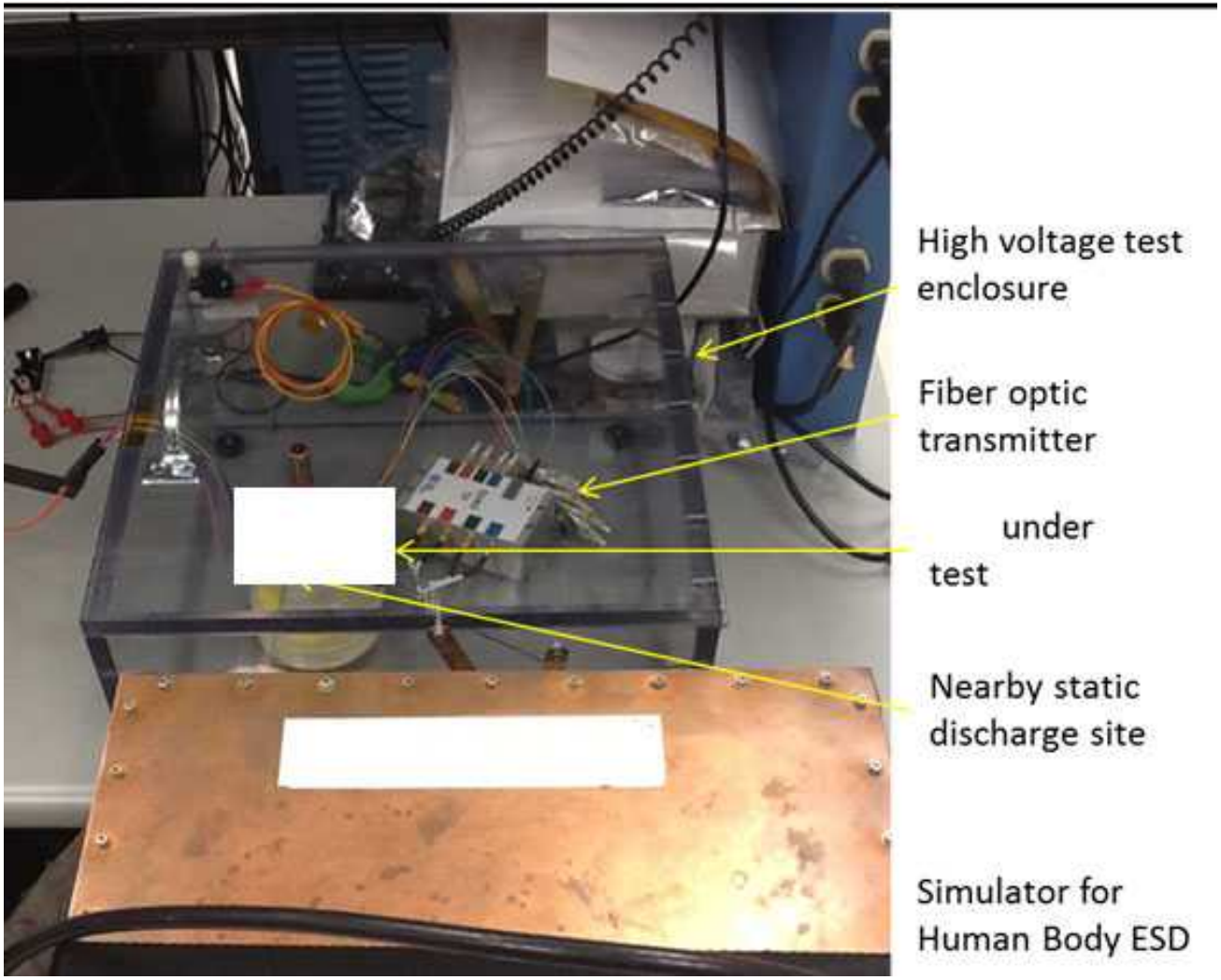
Safety Features to Consider When Designing Electronic Systems

- What happens to the electronics when power is interrupted?
- Characterize the system interconnects (cables, vias, etc.) to make sure they are reliable for the design intended.
- Power glitches need to be considered in the design of electronics.

Scenario 2

- Human ESD in the vicinity of the detonator caused the CDU to trigger (demonstrated in the lab)
  - TAT demonstrated in the lab that indirect human body ESD/EMI couples into the electronics and reliably causes the CDU to trigger
  - The microprocessor was not observed to become “upset” by the EMI

Typical setup for ESD/EMI characterization



Div. 8000 Briefing on the Accident Investigation Board (AIB) for Site 9920

Mike Lopez, 00421

Sandia National Laboratories

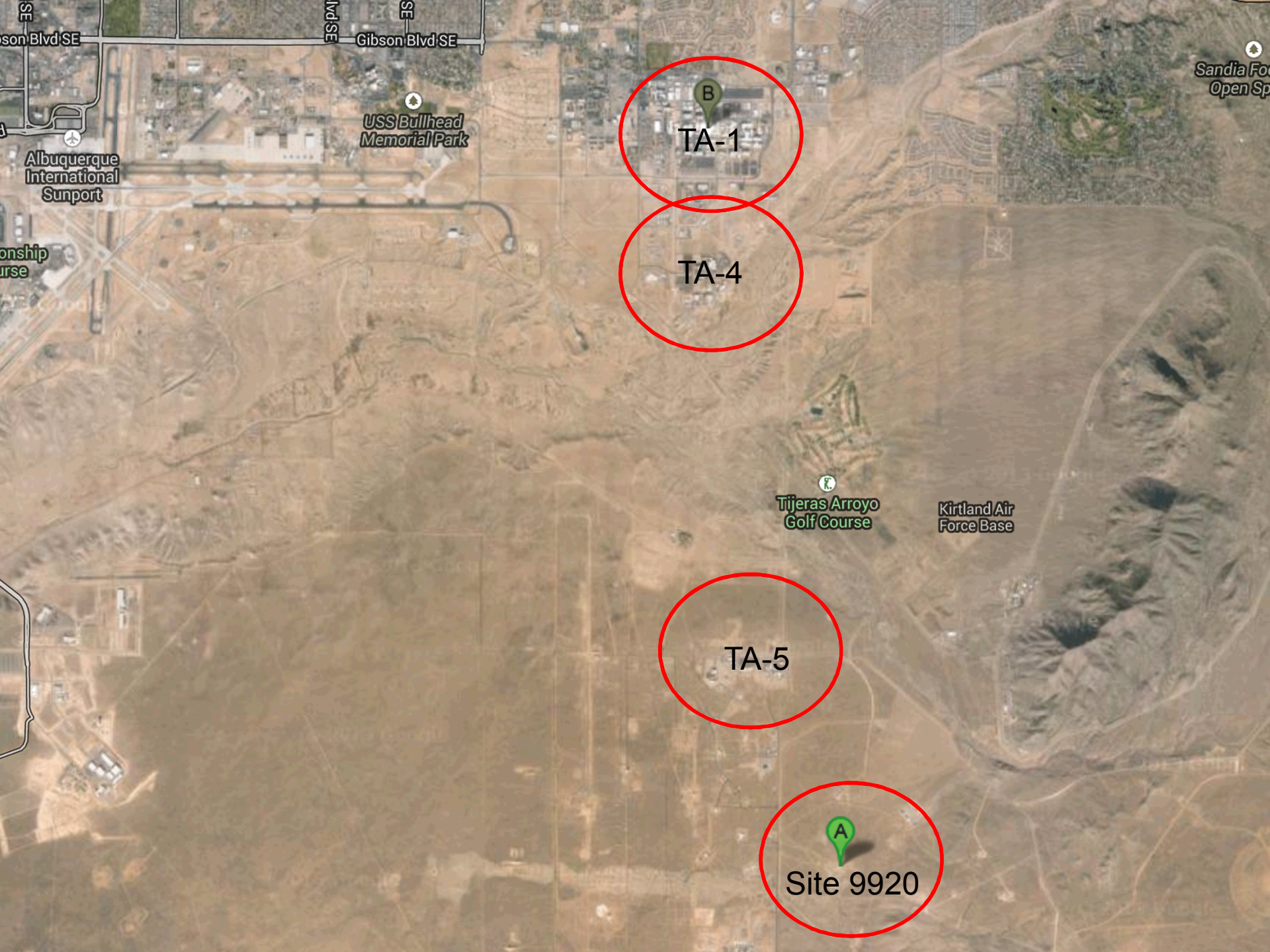
Discussion

1. Let’s go to the site
2. Engineered safety lessons learned
   - Overarching criteria clarifications
   - Safety case insights

c1

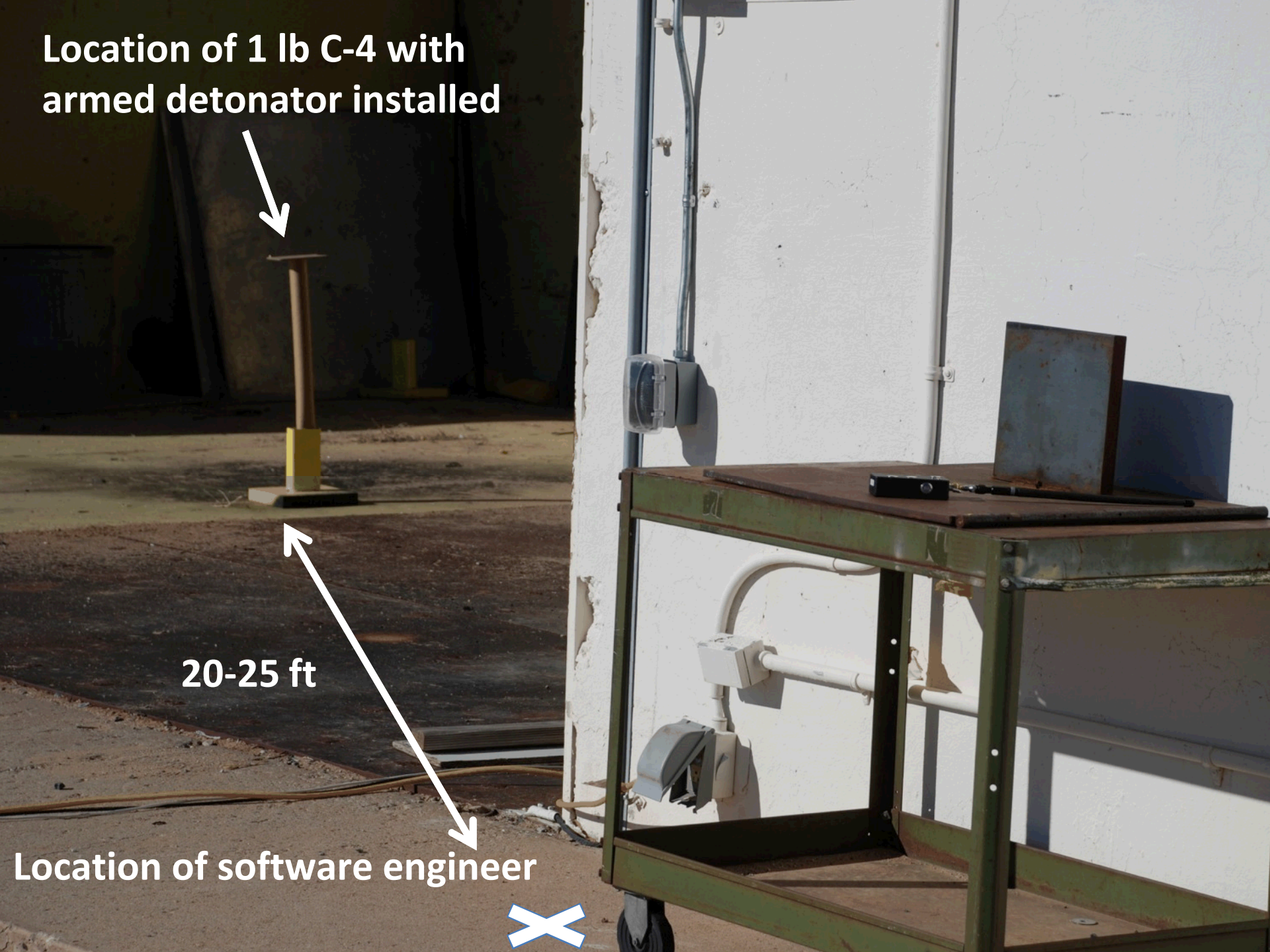
Slide 25

c1 Does this meeting still pertain?
cladkin, 4/1/2014


Gibson Blvd SE
USS Bullhead Memorial Park
Albuquerque International Sunport
TA-1
TA-4
Tijeras Arroyo Golf Course
Kirtland Air Force Base
TA-5
Site 9920


9920
9926
N
W
E
S
0
US Survey Feet


Location of the accident
Location of 1 lb C-4


Location of 1 lb C-4 with armed detonator installed
20-25 ft
Location of software engineer

“It doesn’t apply to us” mindset

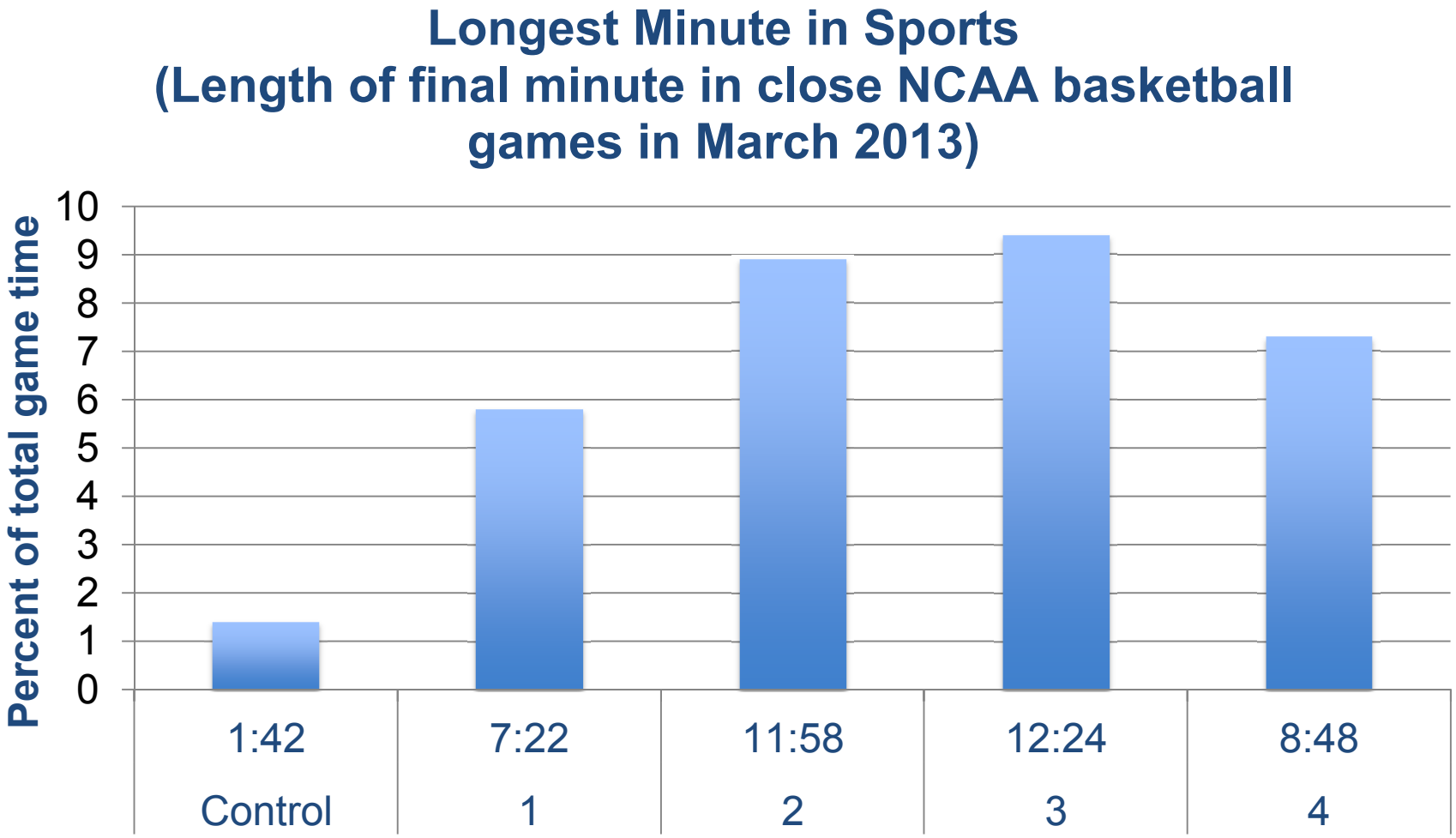
- Seen in the responses to past audits.

We will be tempted

- Fundamental Attribution Error
  - If someone else makes a mistake, they are negligent or incompetent.
  - If you make a mistake, there were all kinds of external factors.

Good safety cultures can only be recognized from the outside. Inside the culture, everyone thinks there is a long way to go.

Things should get slower towards the end



What is engineered safety?

Revised approach to WP&C with engineered safety principles

Engineered safety is not uniformly understood by the workforce

While “engineered safety” is in the vernacular, it is not defined by the corporation.

The new WP&C manual does not define the one term everyone talks about.

The overarching criteria must be interpreted through these principles

- Safety is an attribute of an operational system achieved by intent.
- Use technical expertise to systematically and critically analyze ways in which the system can fail to perform as intended.
- Engineering design of the system prevents identified potential failures or mitigates their consequences.

Safe by design intent

- Designers apply technical expertise to design safety into the system from the beginning of the project.

Understand the technical basis

- It should be demonstrated, through engineering analysis and scientific understanding, how a system is intended to perform and how it can fail to perform.

Identify and control energy sources

- Many of the most serious accidents occur due to the release of hidden or unexpected forms of energy. This criteria specifically asks for extra diligence in controlling energy sources.

Define unacceptable consequences

- Defining the unacceptable consequences is the formal and written addition of specific system safety requirements to the operational system.

Assess risk

- Use of probability of occurrence in determining whether or not to mitigate a failure should be avoided unless the probability of occurrence can be demonstrated through quantifiable evidence.

Require positive verification

- Part of this assurance is that the person in charge assumes “the worst” until the correct configuration is specifically assured by responsible individuals.

The purpose of a safety case is to demonstrate critical thinking

Demonstrated	Not Demonstrated

• Specific to the process
• Technical details
• Involves the workers
• Answers
  – How can it fail?
  – How do you prevent failure?
  – What if it fails anyway?
	• Stops at a general overview
	• Index of other documents
	• Unknown to worker
	• Summary of the PHS hazards
	• Tied more to space than activity level work

Some good indicators

- Describes work scope
- Specifies unacceptable consequences
- Team members' names are recorded
- Team meetings times and discussions summarized
- Describes hazards of activity level work
- Describes mitigations of hazards for the work
- What if scenario analysis
- Describes independent review/assessment (if done)

“Red flag” language

- “Summary” documents
- “Cut & paste” or “Copy this over”
- “We did an umbrella analysis for all work in the lab.” – Red flag for overconfidence.
- “Safety case is useless or meaningless.”

If you find no value in the safety case, don’t sign it.

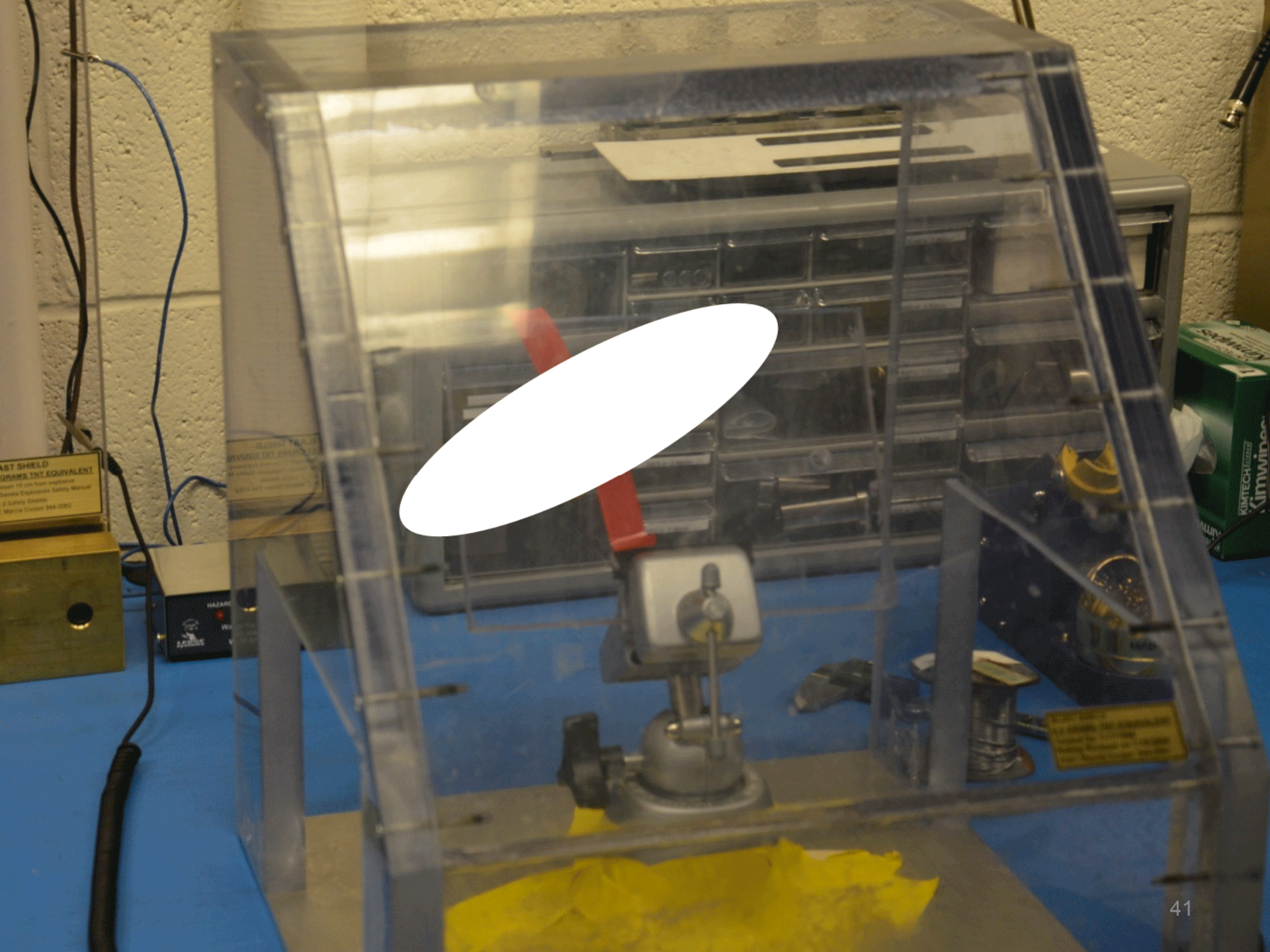
ENGINEERED SAFETY IN DESIGN

Fireset Design

- Recognized that safety of the system is inherent in the system design, not the design of individual components.
- Made safety recommendations to other component designers, such as the use of the shorting plug.
- Designed in safety features, such as the LED light.

Explosive Assembly

- Applied engineered safety principles when installing the detonator into the test unit.
- Understood the technical basis by learning enough about the test unit to apply three controls to ensure energy would not reach the capacitor.
- Exhibited defense in depth by assuming the detonator would initiate anyway; used a blast shield to protect the worker.


AST SHIELD
GRAMS TNT EQUIVALENT
KIMTECH
Kimwipes