

Engineered Safety Overview

Robert Leland

Director

Climate Change Security

Sandia National Laboratories

August 15-16, 2023

Workplace Safety in Hybrid Federal Laboratories: A Workshop

Hosted by the National Academies of Sciences, Engineering, and Medicine

Engineered Safety – A Risk-Based Approach to Safety for Technical Cultures



- **Old approach:** Identify hazards, apply controls
- **New approach:**
 - Identify risks and manage that risk to prevent *unacceptable consequences*
 - death, serious injury, significant impact to the environment, loss of use of a facility
 - Preference for engineered solutions versus administrative controls
 - Deeper applications of systems thinking
- **Workforce engagement as a critical benefit**
- **Emphasis on principle-based critical thinking**

Principles of Engineered Safety



UNDERSTAND TECHNICAL BASIS

Understanding the technical basis is a deep knowledge of the system and interconnected elements. **If we understand how it works, we can understand how it can fail.**

RISK ASSESSMENT APPROACH

What can go wrong?
How can it happen?
What are the consequences?
What defenses/barriers/controls are in place?
Are the defenses adequate?
What if it still goes horribly wrong?

DEFINE UNACCEPTABLE CONSEQUENCES

Defining unacceptable consequences (vs. undesirable) **provides a framework** to guide us on how much time and effort we want to expend developing various controls and barriers.

IDENTIFY AND CONTROL ENERGY SOURCES

Identification and control of **all energy sources** is a deliberate process. Uncontrolled or unidentified energy sources can result in an accident or system failures.

SAFE BY DESIGN INTENT

Safety is **incorporated into the design** of the system at the very beginning and as a deliberate effort, not as an afterthought.

POSITIVE VERIFICATION

Positive verification is **an ongoing process** to ensure that the work can be performed, is being performed safely, and can be performed as intended.

Other Key Attributes

- Performance of a **formal hazard analysis** at the system level
 - Analyze What-if, Failure Modes and Effects, Hazard Operability, etc.
- Recognition that the **worker** is:
 - part of the system and
 - the primary cause of error
- **Lifecycle analysis** to ensure risks are effectively managed



Systems Approach



System definition includes everything associated with an operation.



*People (workers) are generally the **most common** source of error within a system.*

-James Reason, *Human Error*

Key Benefits



- **Major Events have been significantly reduced.**
 - Previously, Sandia experienced a major event (significant injury or facility damage) about every 18 months.
- **Since implementation in 2014, no unacceptable consequence events have occurred.**
 - Minor events are evaluated and rolled into the Hazard Analysis to update the system controls.
 - Enhanced cultural legitimacy of safety effort

Vignettes

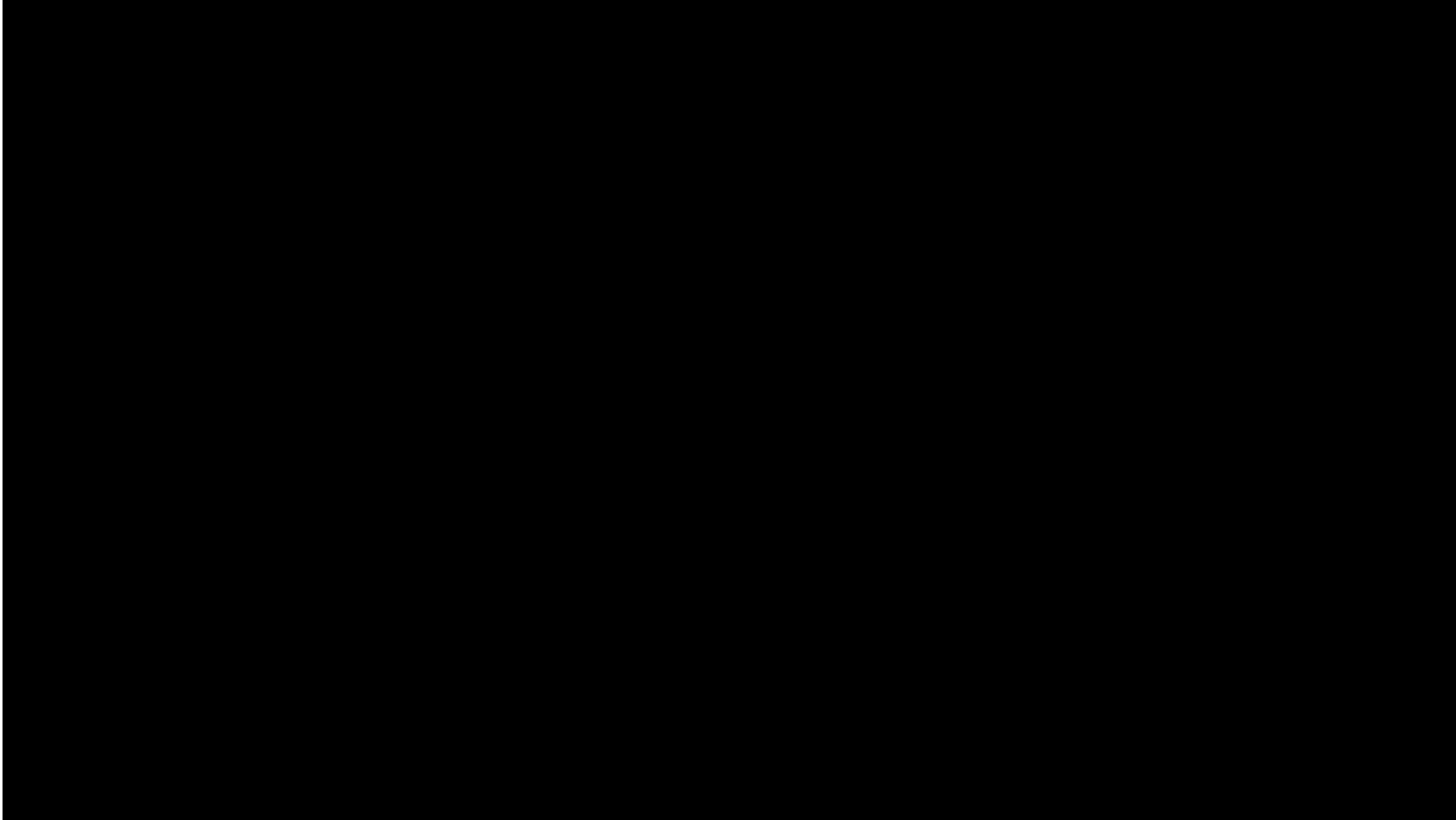


- Arsine gas release at MESA
- Plutonium experiments on Z
- Atomic precision tool phosphine gas control

Engineered Safety at the Z Facility



Atomic Precision Tool





THANK YOU