SAND2012-2517C

Exceptional service in the national interest

Sandia National Laboratories

Engineered Safety at Sandia

Kamilla Schwing

2 April 2012

Elements of this presentation are based on the work of
J. Stephen Rottler, PhD, Mike R. Lopez, PhD, and Stephen J. Guidice

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Overview

Sandia National Laboratories

- Why Engineered Safety at Sandia?
- Engineered Safety Concepts
- Engineered Safety implementation at Sandia's Z Accelerator

Rocket Sled Track Accident

- Unexpected ignition of a rocket motor (2008)
- Government Accident Investigation Board
  - Numerous issues related to conduct of operations and work planning and control
- Executive Safety Review Board
  - “evaluate and modify technical processes to ensure they include the safety principles and requirements necessary to achieve safe operations through engineering design”

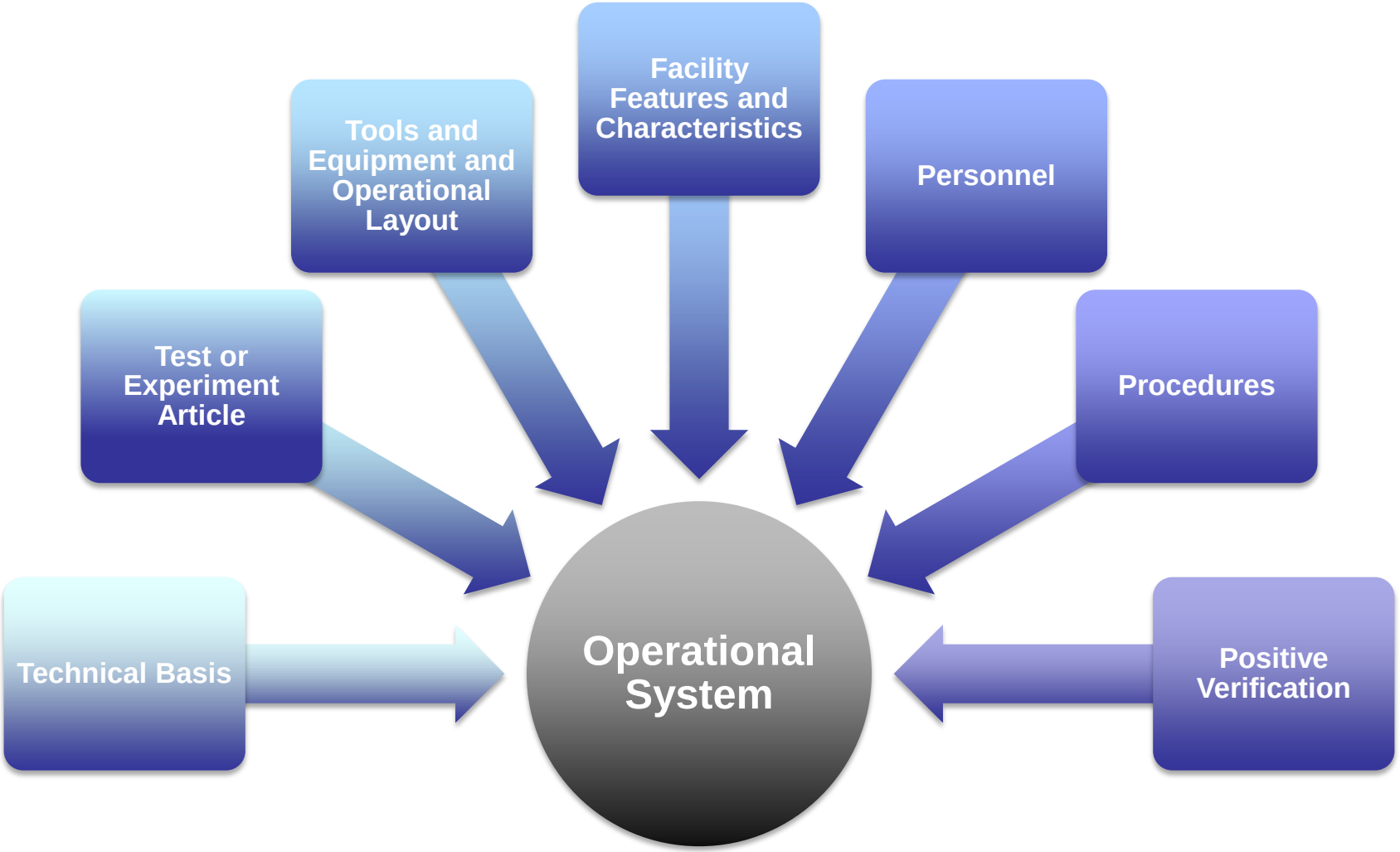
Problem Statement

- The underlying technical basis for the “design safety features” of an activity may be taken for granted or receive inadequate technical review

- Work planning and controls practices cannot be relied upon to detect technical design flaws affecting the safety of an activity

- Safety is not defined in a “systems engineering” context, which is more appropriate for an R&D laboratory

The “Operational System”



What is Engineered Safety?

Sandia National Laboratories

- Employs a principle- and assurance-based approach for designing safe “operational systems”

- Safety is an attribute of an operational system achieved by intent
- The operational system is systematically and critically analyzed to identify ways in which it can fail to perform as intended
- The operational system is designed and validated to prevent identified potential failure modes and mitigate the consequences of a failure should one occur

Engineered Safety Objective 1

Sandia National Laboratories

- Design and conduct activities as an operational system
  - Analyze and control the operational system
  - Establish safety martin criteria and verify they are achieved
  - Ensure direct and unambiguous communication, especially at interfaces
  - Provide positive verification that the system is in its intended configuration

Engineered Safety Objective 2

Sandia National Laboratories

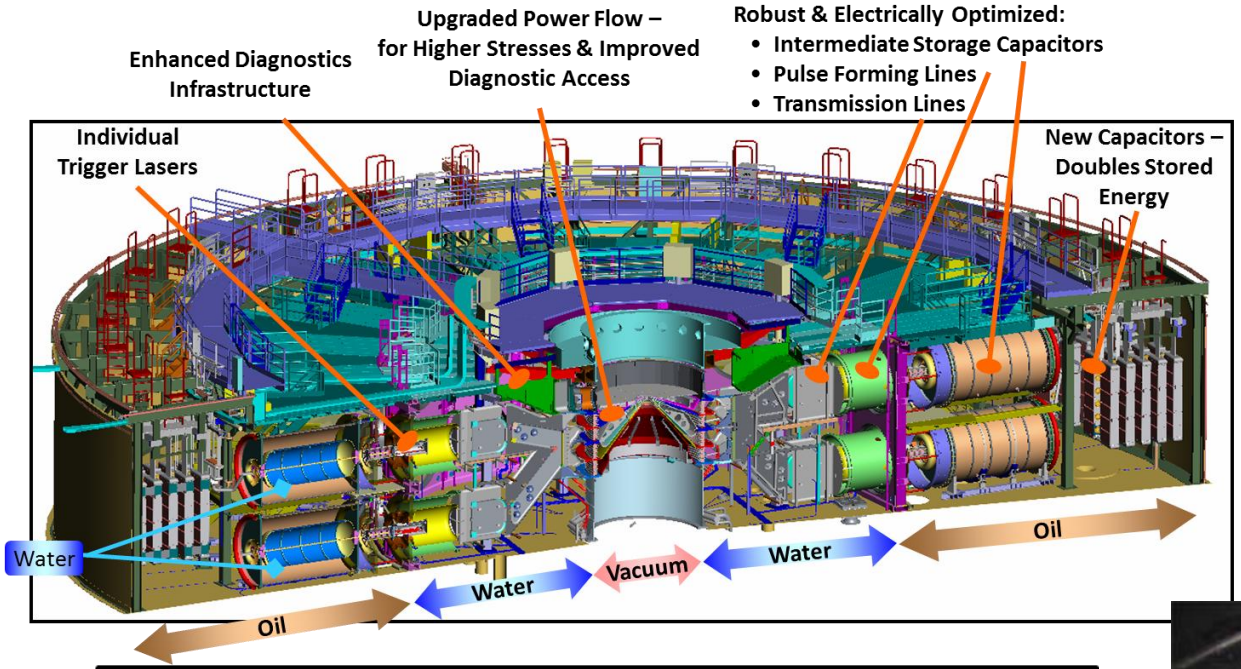
- Develop the technical basis for controlling an activity
  - Understand how the system fails to an unsafe condition
  - Develop a “safety theme”
  - Use credible failure mode and fault tree analyses to clearly identify accident pathways
  - Eliminate single point failures leading to the unacceptable consequences
  - Mitigate failure modes that cannot be eliminated and lead to unacceptable consequences

Engineered Safety Objective 3

Sandia National Laboratories

- Establish clear management expectations
  - Explicitly define the unacceptable outcomes
  - Specify a target level of engineered and administrative controls
  - Designate technical requirements for engineered controls
  - Define process requirements for administrative controls
  - Review and approve the technical basis and controls

Sandia's Z Accelerator



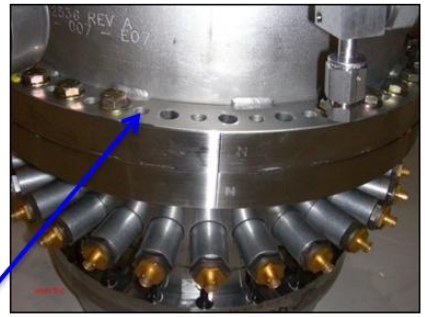
22 MJ stored energy, 26 MA peak current, 100-600 ns rise times

Energy equivalent of 2.5 lbs of high explosive released in few ns

The Z Problem

- The plutonium containment system was designed and fielded to protect workers, equipment, and the environment
  - A hermetic seal on the containment system was breached during a Z shot in March 2009 (26 MA experimental system; no Pu)

vacuum interface seal



6 bolts sheared off

Baffle system

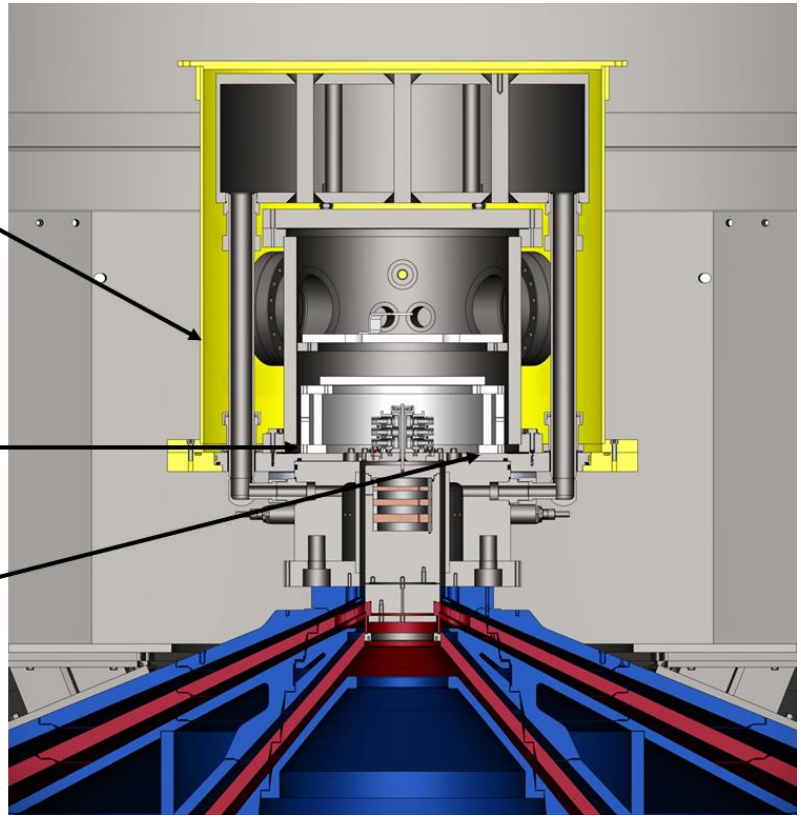
Engineered Safety with Z

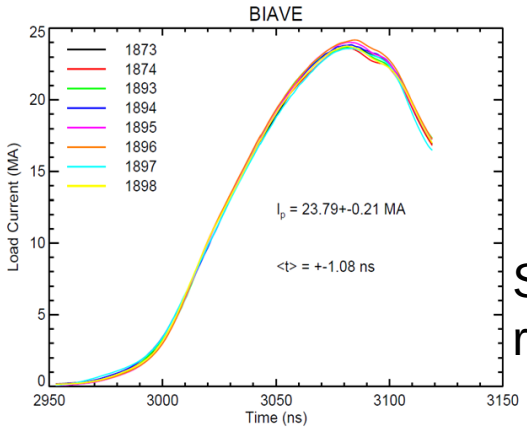
Sandia National Laboratories

- Unacceptable consequences
  - Radiation dose to a worker
  - Contamination of the environment
  - Pause in operation of Z for more than 6 months
- Failure Mode Effects Analysis and Fault Tree Analysis
  - 33 single point failure modes

Eliminate Single Point Failures

- Added a containment chamber that surrounds the Upper Containment Chamber (UCC)
- Changed from a rigid copper gasket to an elastomeric gasket at the UCC interface seal that leaked
- Standardized a welded radial baffle system inside the UCC

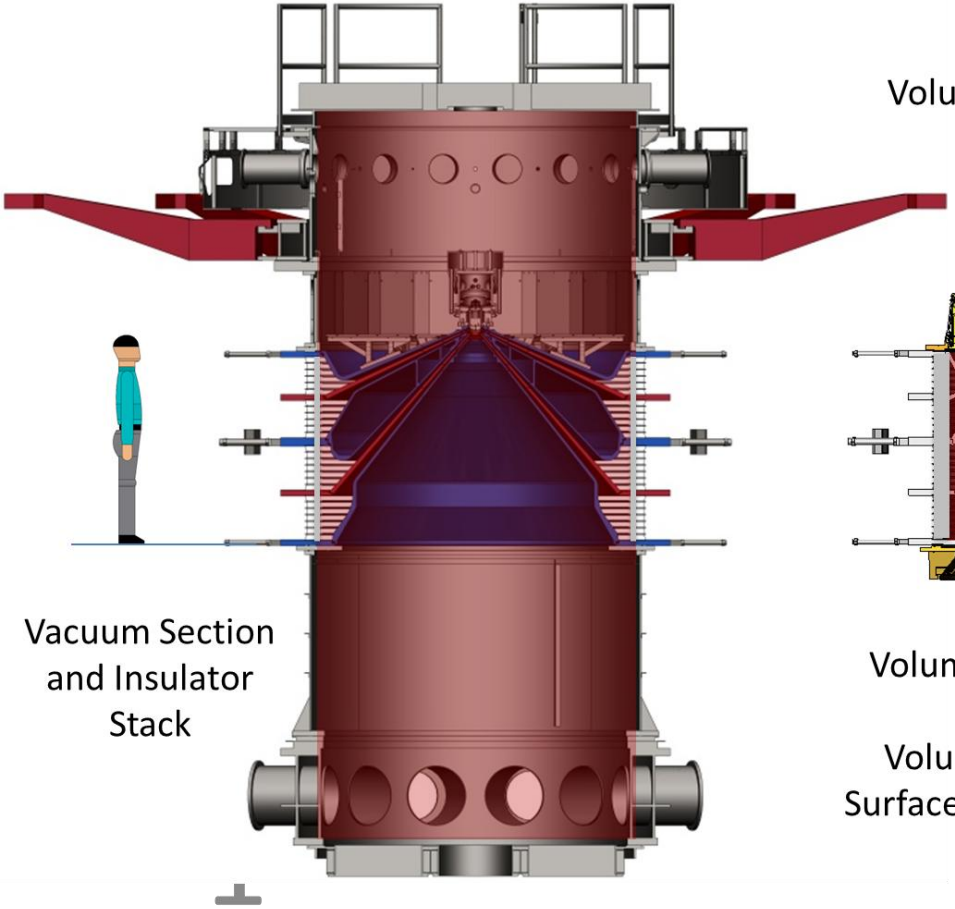




Setting a current limit of 11MA reduces the chance of Pu dispersal

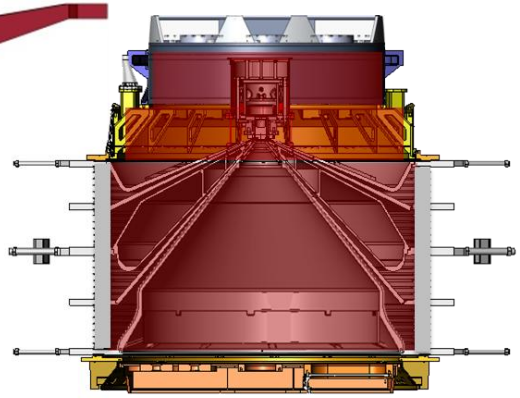
What if the system fails anyway?

Sandia National Laboratories



Vacuum Section and Insulator Stack

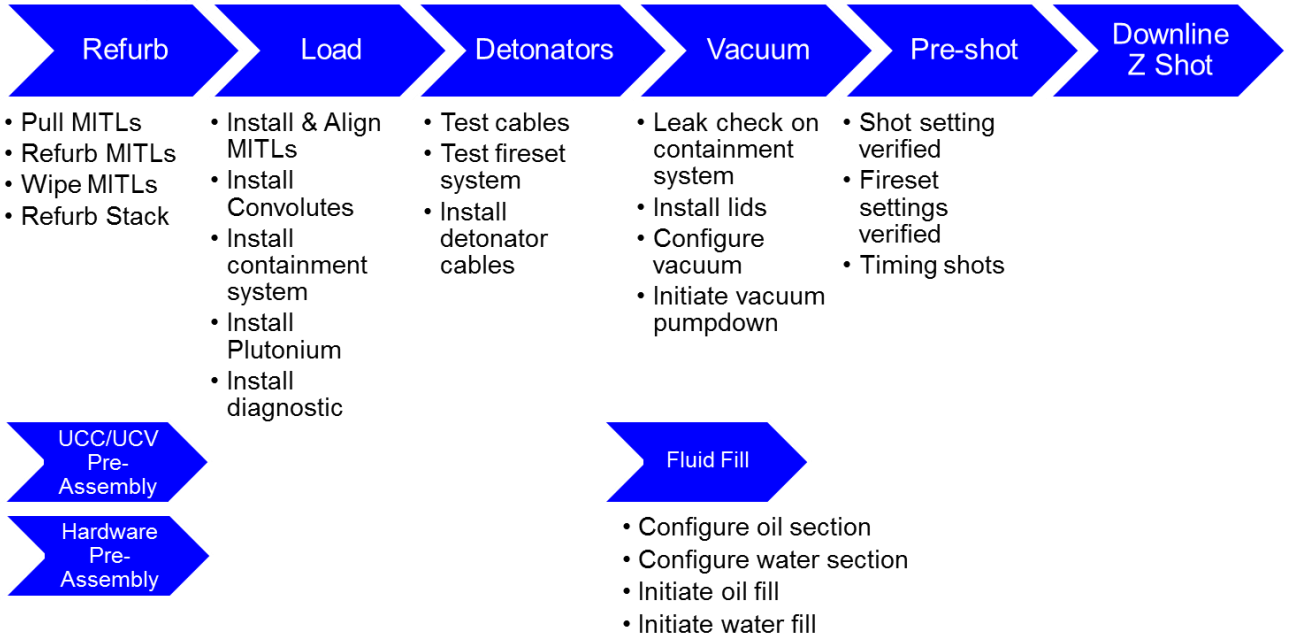
Volume Reduced Secondary Containment



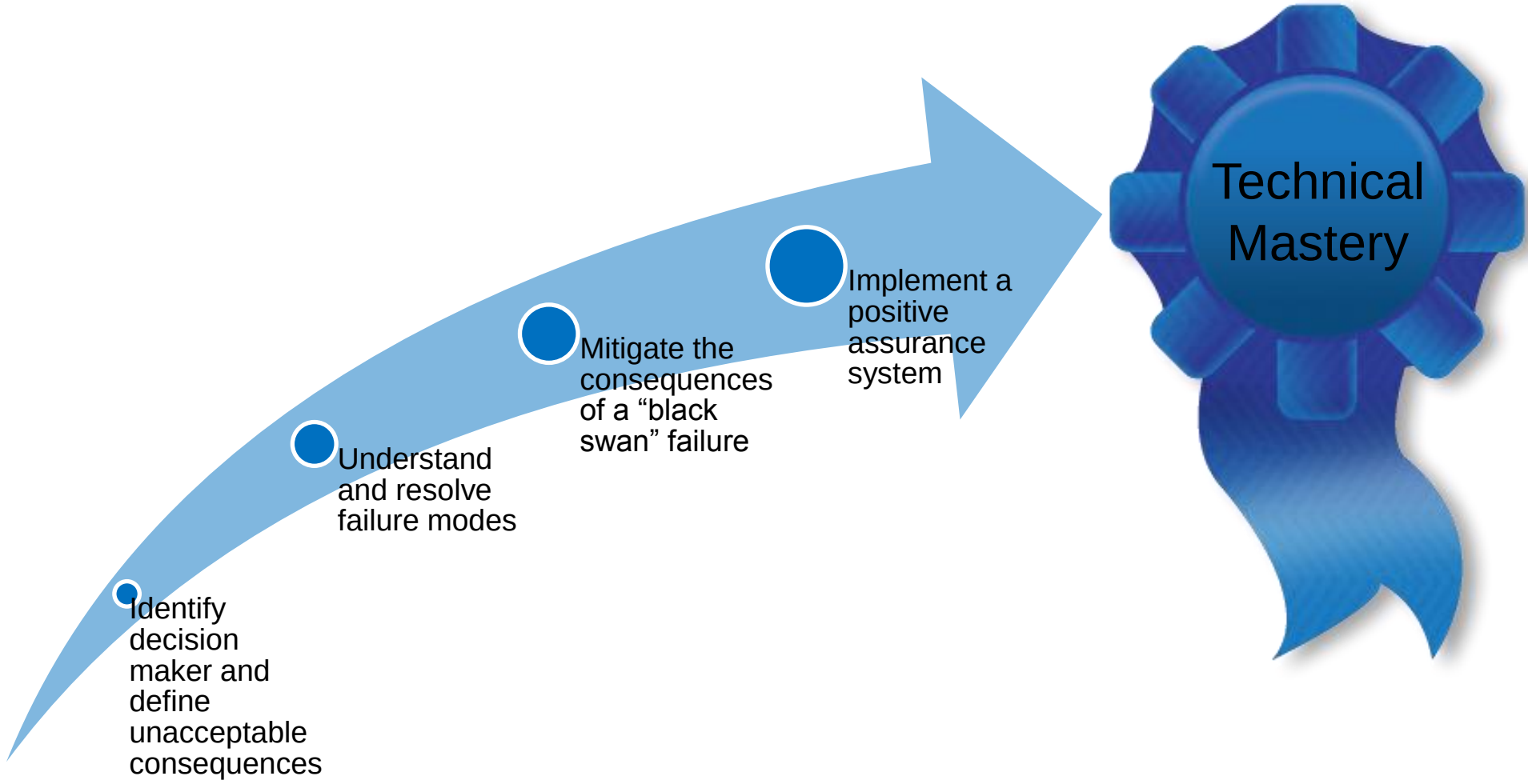
Volume Reduced Secondary Containment
Volume Reduction by 60%
Surface Area Reduction by 50%

Positive Assurance

- Require 18 formal assurances from individuals responsible for critical subsystems to the Z Shot Director prior to five key activities in the shot setup timeline
- Z Shot Director is responsible for granting final authorization immediately prior to the Pu shot



Engineered Safety Workflow



Questions

Sandia National Laboratories