SAND2012-10651P

Integrating Engineered Safety and WP&C

Presented to the Safety and Security Oversight Subcommittee of the Mission Committee of the Sandia Corporation Board of Directors

J. Stephen Rottler, PhD

CTO and Vice President, Science and Technology

Sandia National Laboratories

December 19, 2012

LOCKHEED MARTIN

Sandia National Laboratories

Overview

- **Why Engineered Safety at Sandia?**
- **Engineered Safety Concept**
- **Engineered Safety Implementation**

Sandia National Laboratories

Integrated Safety Management is the Basis for Work Planning and Control at SNL

SEVEN GUIDING PRINCIPLES OF INTEGRATED SAFETY MANAGEMENT

1. **Line Management Responsibility for Safety**
   Line management is directly responsible for the protection of the public, the workers and the environment.
2. **Clear Roles and Responsibilities**
   Clear and unambiguous lines of authority and responsibility for ensuring safety shall be established and maintained at all organized levels within the Department and its contractors.
3. **Competence Commensurate with Responsibilities**
   Personnel shall possess the experience, knowledge, skills and abilities that are necessary to discharge their responsibilities.
4. **Balanced Priorities**
   Resources shall be effectively allocated to address safety, programmatic and operational considerations. Protecting the public, the workers and the environment shall be a priority whenever activities are planned and performed.
5. **Identification of Safety Standards and Requirements**
   Before work is performed, the associated hazards shall be evaluated and an agreed-upon set of safety standards and requirements shall be established, which, if properly implemented, will provide adequate assurance that the public, the workers and the environment are protected from adverse consequences.
6. **Hazard Controls Tailored to Work Being Performed**
   Administrative and engineered controls to prevent or mitigate hazards shall be tailored to the work being performed and associated hazards.
7. **Operations Authorization**
   The conditions and requirements to be satisfied for operations to be initiated and conducted shall be clearly established and agreed upon.

Sandia National Laboratories

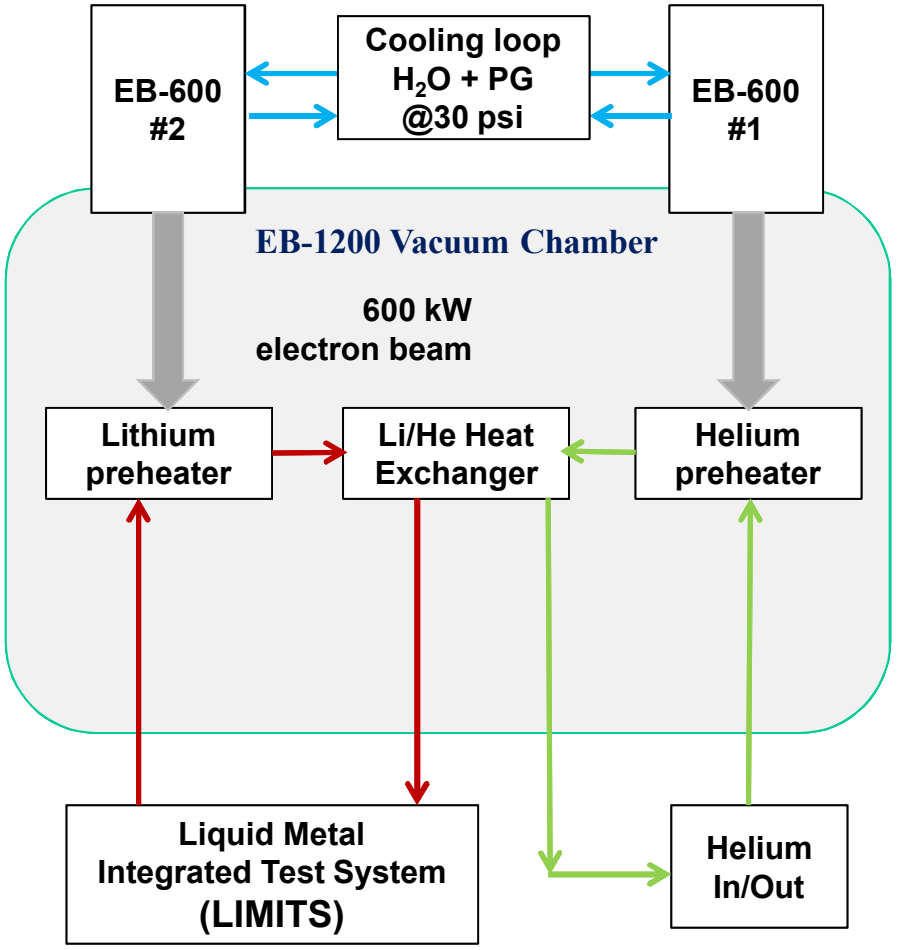
Rocket Sled Track Accident (October 2008)

- **Unexpected ignition of a rocket motor**
- **DOE/NNSA 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"**

Sandia National Laboratories

Plasma Materials Test Facility Accident (August 2011)

- A material failure in the lithium preheater led to…
- A material failure in the e-beam gun ceramic cooling annulus that led to…
- Mixing of molten lithium and coolant that led to…
- An energetic event that severely damaged the EB1200 chamber and caused minor damage to Building 6530



Sandia National Laboratories

Plasma Materials Test Facility Accident Root Causes

- **An incomplete hazard analysis (HA) to identify hazards and controls to prevent the lithium and water from combining and initiating the chemical explosion, and**

- **A design selection process that allowed the specification of incompatible materials for the lithium preheater**

Sandia National Laboratories

Problem Statement

- **Current work planning and control practices are driving a focus on effective conduct of operations**
- **The underlying technical basis for "design safety features" of an activity may be taken for granted or receive inadequate technical review**
- **Work planning and control practices may not detect technical design flaws affecting the safety of an activity**
- **Safety needs to be considered in a "system engineering" context appropriate for an R&D laboratory**

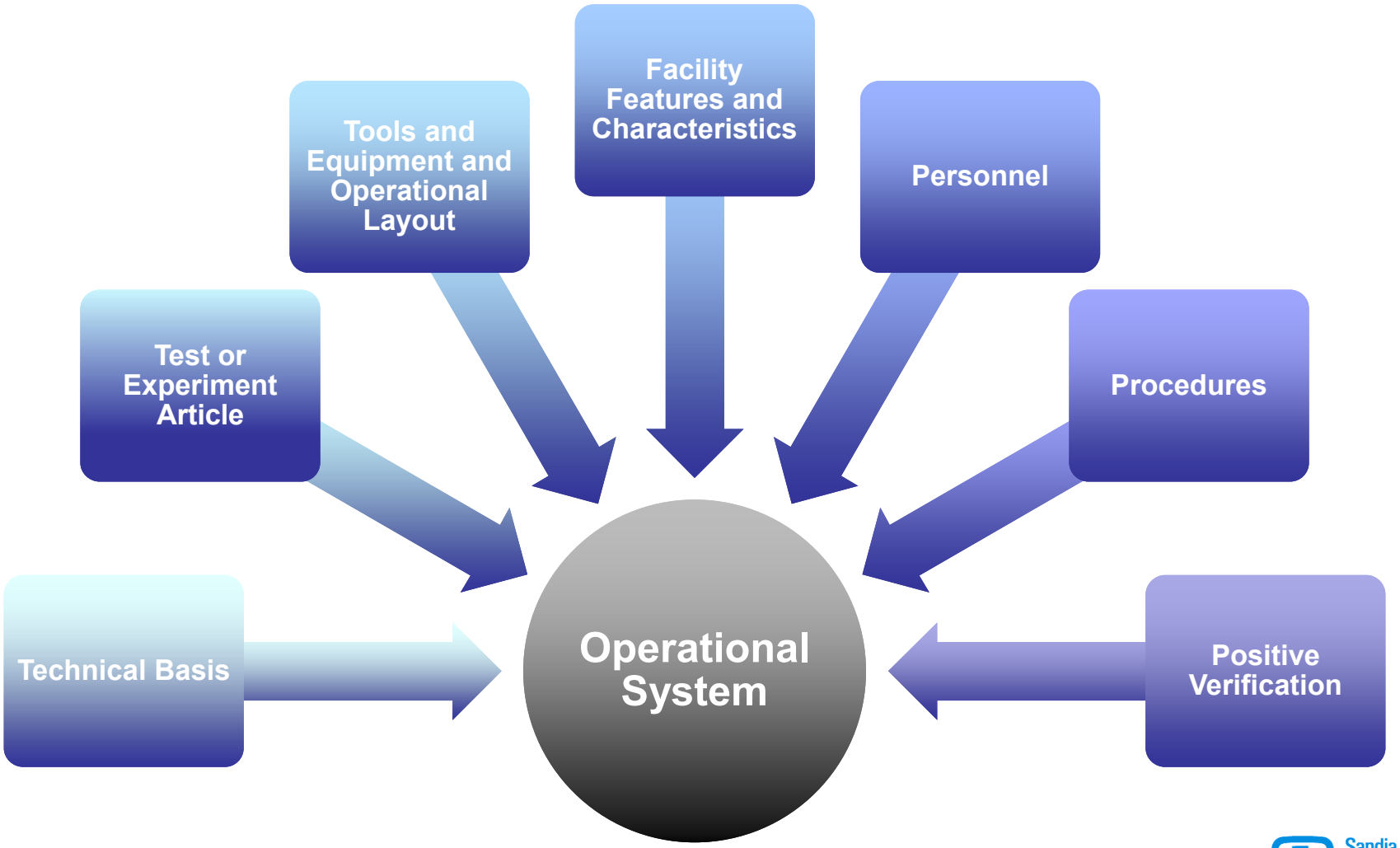
Sandia National Laboratories

What is Engineered Safety?

- **A principle-based approach for designing safe "operational systems"**
- **Safety is an attribute of an operational system achieved by intent**
- **Operational systems are systematically and critically analyzed to identify ways in which they can fail to perform as intended**
- **Operational systems are designed and validated to prevent identified failure modes and to mitigate the consequences of a failure should one occur**

Sandia National Laboratories

The “Operational System”



Sandia National Laboratories

Engineered Safety Objective 1: Design and Conduct Activities as an Operational System

- Design and control activity as a system – verify design intent was achieved
- Establish safety margin criteria and verify they are achieved
- Consider the human factor in all aspects of the system design
- Ensure direct and unambiguous communication, especially at interfaces
- Manage any change in any element as having the potential to affect system performance until verified otherwise
- Positively verify the system is in its intended configuration prior to use

Sandia National Laboratories

Engineered Safety Objective 2: Develop the Technical Basis for Controlling an Activity

- Understand how the system fails to an unsafe condition
- Use credible failure mode and fault tree analyses to clearly identify accident pathways
- Implement a safety theme based on “defense in depth” with multiple independent controls
- Eliminate single point failures leading to the unacceptable consequences
- Mitigate failure modes that cannot be eliminated and lead to unacceptable consequences

Sandia National Laboratories

Engineered Safety Objective 3: Establish Management Expectations

- Identify “Decision Maker”
- Explicitly define the unacceptable outcomes
- Based on accident consequences, specify the “target level” of engineered and administrative controls and their associated requirements
- “Decision Maker” is responsible for three specific decision points

Sandia National Laboratories

Integration of Engineered Safety and Conduct of Operations

Overarching Criteria

- Safe by Design Intent
- Understand Technical Basis
- Identify and Control Energy Sources
- Define Unacceptable Consequences
- Risk Assessment Approach
- Positive Verification

ISM Core Functions

Define Scope	Analyze Hazards	Control Hazards	Prepare and Perform Work	Feedback and Improve
Identify Work Planner	Detailed Identification Of Hazards	Eliminate Single Point Failures	Complete Preparations Document Authorization • Complete TWDs • Perform Final JSA • Team Trained and Qualified • Perform Readiness Review	Self Assessment
Establish Work Planning Team	Identify Safety Themes, Standards and Codes	Apply Engineered and Administrative Controls		Lessons Learned
Identify Hazards and Authorization Bases				Corrective Actions
Evaluate Key Factors Document Analysis	Perform Failure Mode Analyses	Develop and Document Safety Case	Perform Work	Management Surveillances

Decision Points

Line Decision Scope of Work	Line Decision Safety Case	Line Decision Authorize Work

Sandia National Laboratories

Progress in Implementing Engineered Safety

- **Engineered Safety conceptual model developed and socialized - workshops in relevant Divisions completed**
- **More than 50 implementation projects across the laboratory resulting from workshops and voluntary early adopters**
- **Completing internal review of new draft Work Planning & Control (WP&C) Manual: *Criteria for Safe Design and Operations***
- **Integration of engineered safety model with existing Work Planning & Control system is underway**
- **Reviewing new ISM-based work planning and control approach with customers and stakeholders**

Sandia National Laboratories

Path to Full Implementation of Engineered Safety in 2013

- Complete mapping of engineered safety model into existing Work Planning & Control System
- Training and communication campaign
- For ongoing operations, line management will develop a schedule for assessment against new WP&C manual criteria
  - Prioritized by severity of potential accident consequences
  - Assessments will result in line-developed corrective action plans as warranted
- New work as of effective date will be conducted in accordance with new WP&C manual criteria
- Compliance will be assessed independently and judged by the rationale developed to support line decisions on work scope, safety case, and work authorization

Sandia National Laboratories

Integration of the Engineered Safety Model in Work Planning and Control Will…

- Create an ISM-based approach that integrates safe designs with effective conduct of operations
- Establish a credible technical basis for safety in work
- Create an ISM-based safety program that is easier to understand and use by an R&D organization
- Create increased and more effective management engagement
- Further mature and improve the SNL safety culture

Sandia National Laboratories