SAND2014-1351C

Quality at Sandia National Laboratories

J. Stephen Rottler

Vice President, California Laboratory

Vice President, Energy and Climate Program Management Unit

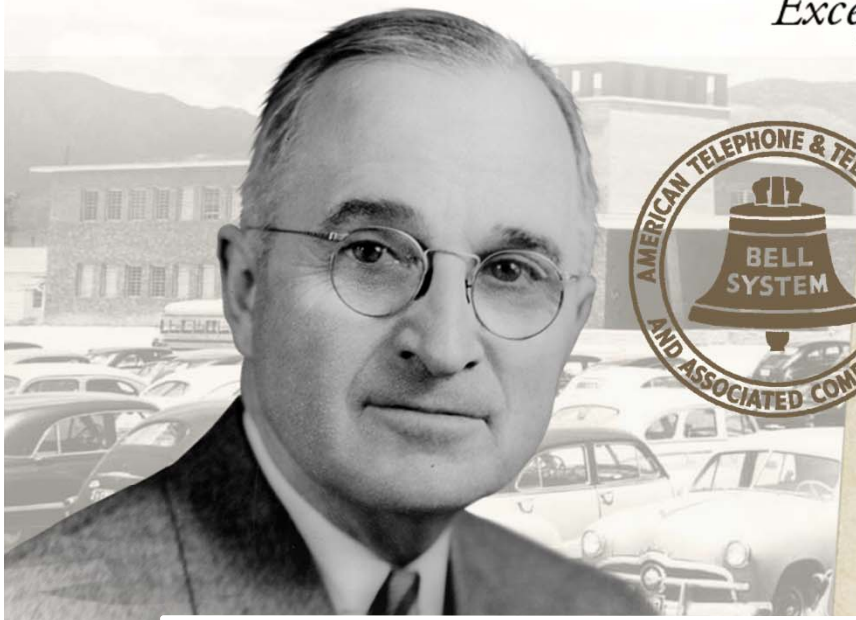
Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

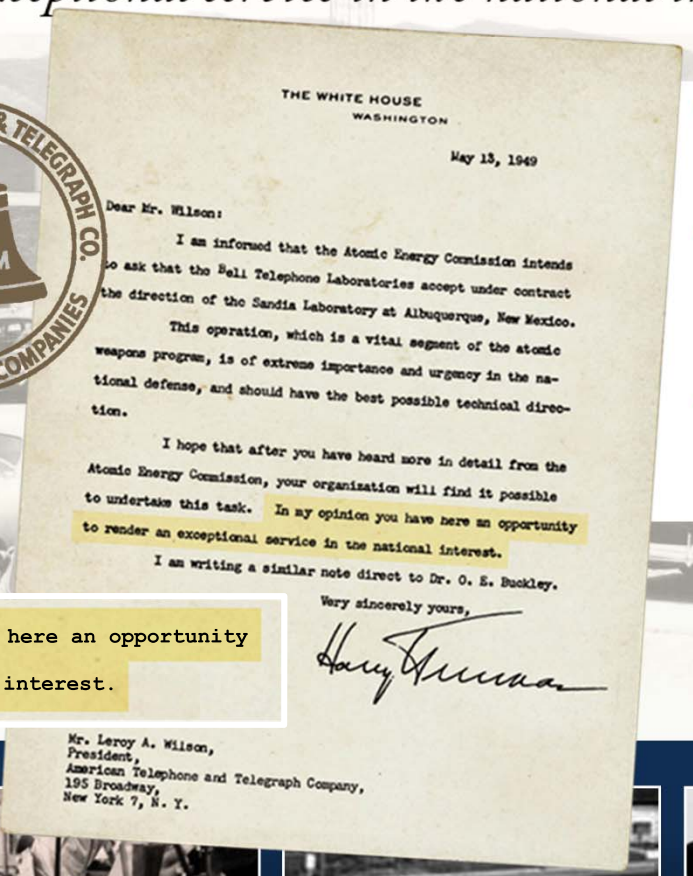
24-26 Feb 2014 International Conference on Software Quality - ICSQ 2014

Sandia's history

Sandia National Laboratories

Exceptional service in the national interest





THE WHITE HOUSE
WASHINGTON

May 13, 1949

Dear Mr. Wilson:

I am informed that the Atomic Energy Commission intends to ask that the Bell Telephone Laboratories accept under contract the direction of the Sandia Laboratory at Albuquerque, New Mexico.

This operation, which is a vital segment of the atomic weapons program, is of extreme importance and urgency in the national defense, and should have the best possible technical direction.

I hope that after you have heard more in detail from the Atomic Energy Commission, your organization will find it possible to undertake this task. In my opinion you have here an opportunity to render an exceptional service in the national interest.

I am writing a similar note direct to Dr. O. E. Buckley.

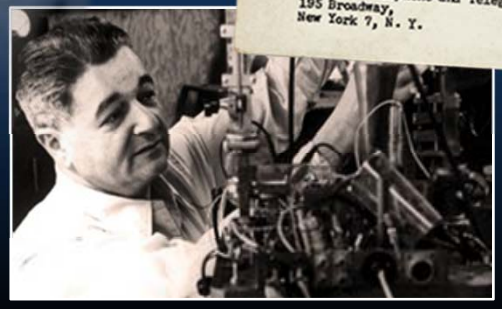
Very sincerely yours,

Harry Truman

Mr. Leroy A. Wilson,
President,
American Telephone and Telegraph Company,
195 Broadway,
New York 7, N. Y.

to undertake this task. In my opinion you have here an opportunity to render an exceptional service in the national interest.

- **July 1945:** Los Alamos creates Z Division
- Nonnuclear component engineering
- **November 1, 1949:** Sandia Laboratory established

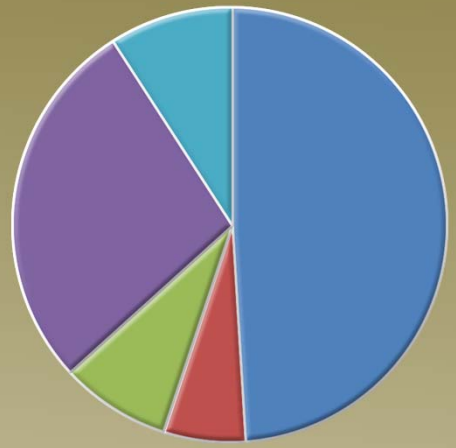


Sandia's mission work reflects national security challenges

Sandia National Laboratories

1950s	1960s	1970s	1980s	1990s	2000s	2010s
NW production engineering & manufacturing engineering	Development engineering	Multiprogram laboratory	Missile defense work	Post–Cold War transition	Expanded national security role post 9/11	LEPs Cyber, Biosecurity Proliferation
	Vietnam conflict	Energy crisis	Cold War	Stockpile stewardship		Evolving national security challenges

Sandia's national security mission areas



FY 2013 Total Budget: $2.5B

- NNSA Weapons
- NNSA Nonproliferation
- Other DOE
- DoD
- Other

Sandia's discipline-based research foundations

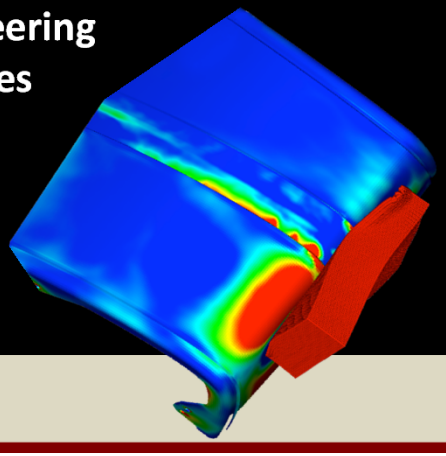
Sandia National Laboratories

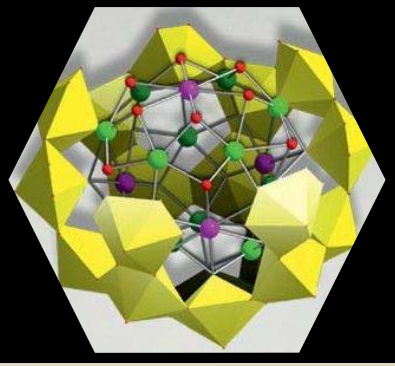
Computing science

High energy density physics

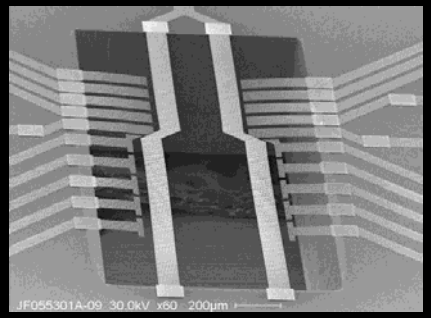
Materials

Engineering sciences





Geoscience



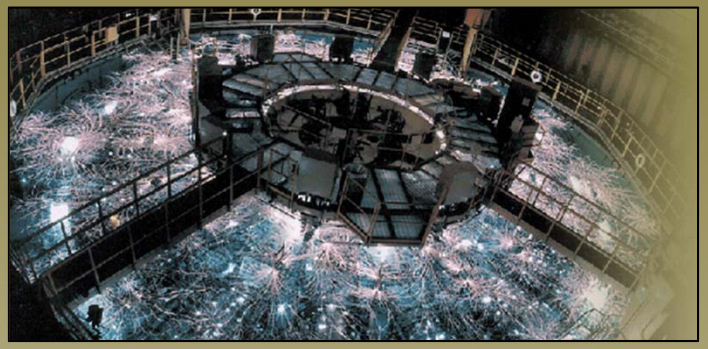
Microelectronics

Bioscience

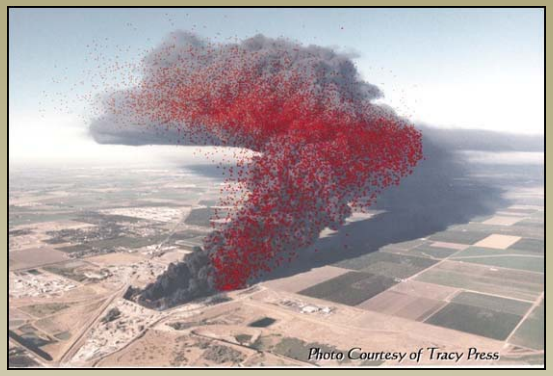
The consequences of failure in our national security mission are unacceptable

Sandia National Laboratories

Nuclear weapon safety and security



Operational safety



Biowatch modeling

Chemical munitions destruction

High consequence personnel recovery systems

Engineering, ethics, and quality

Sandia National Laboratories

- **Engineering** is a profession and **ethics is a defining element** of all professions
- We have an **ethical obligation** to take positive steps to **prevent unwanted outcomes**
- High-consequence engineering organizations, like Sandia, must demonstrate the **utmost commitment to quality** to **achieve mission success**
- **Quality is** …
  - Embedded in our **culture and mindset**, consistent with our personal and organizational values
  - **Enabled** by a minimum set of "rules and tools" that further the sustainment of that culture

Sandia's quality framework

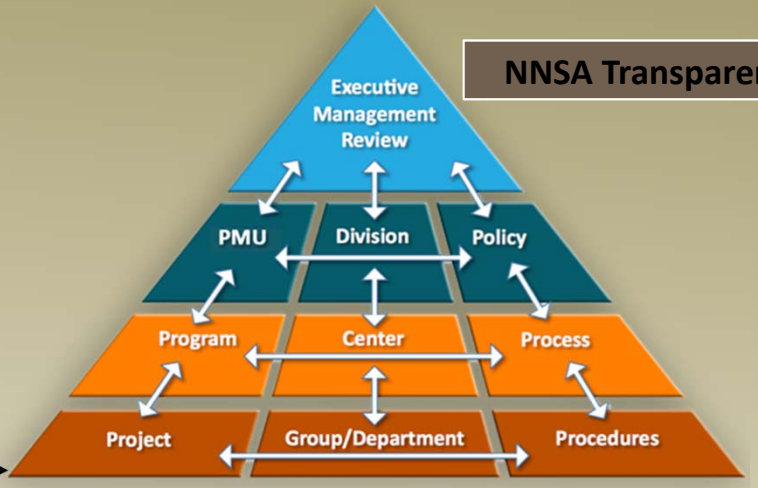
Sandia National Laboratories

Performance Assurance System (PAS)

External and internal audits independently validate performance

Management Reviews

NNSA Transparency



Quality is meeting customer and Sandia expectations consistently and predictably through flawless execution of personal and collective responsibilities

Quality at Sandia: Examples

Sandia National Laboratories

- Sandia's core mission: Nuclear weapon stockpile stewardship
- Software quality for high-consequence applications
- Research quality standards
- Operational safety: Z accelerator

Sandia's core mission:
Nuclear weapon stockpile stewardship

Sandia National Laboratories

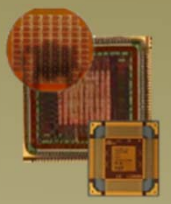
Design agency for nonnuclear components

Production agency

Gas Transfer Systems

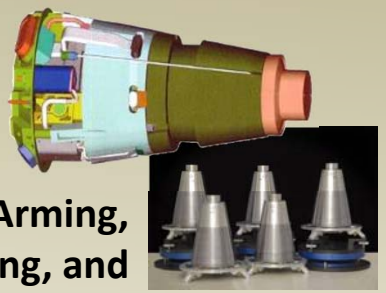
Warhead Systems Engineering and Integration

Microsystems

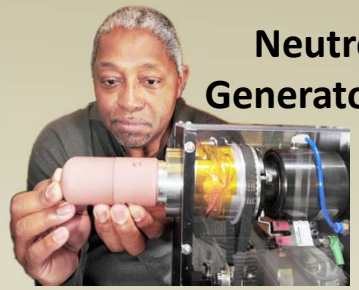


Neutron Generators

Safety Systems



Arming, Fuzing, and Firing Systems



Neutron Generators

Weapon science and technology

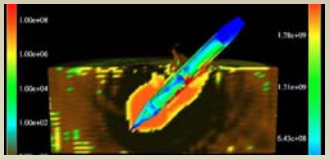
Materials science

Microelectronics

Pulsed power and radiation effects sciences

Engineering sciences

Computing and information sciences



Engineering sciences

Characteristics that drive nuclear weapon quality

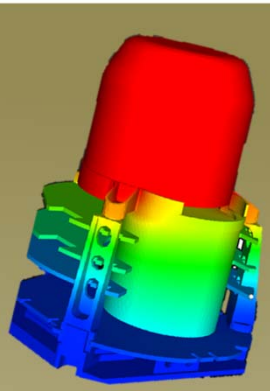
Sandia National Laboratories

- Nuclear weapons must demonstrate **extremely high reliability** in **extreme operating environments** – “Always”
- Consequences of a safety or security failure could be **catastrophic** and are **unacceptable** – “Never”
- Nuclear weapons are produced in **very low volumes** with **detailed craftsmanship**
- Nuclear weapons must endure as part of the nation’s national security deterrent for **long lifetimes** while not being used

Quality and nuclear weapon safety

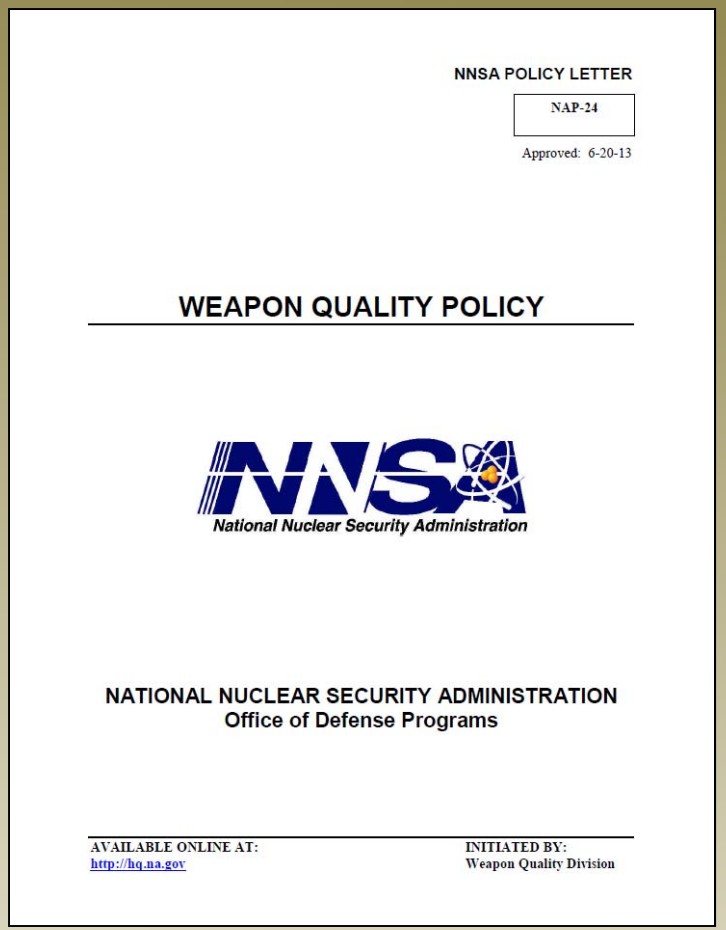
Sandia National Laboratories

- Probability of an accident assumed to be “one”
- Principle-based engineered safety theme
  - Isolation of compatible energy from detonation-critical components until rendered irreversibly inoperable
  - Multiple independent safety subsystems
- Systematic identification and control of critical features
- Nuclear weapon quality management system



Nuclear weapon quality policy

- Quality requirements:
  - Quality improvement (prevention vs. detection)
  - Training
  - Design
  - Instructions, procedures and drawings
  - Document control
  - Procurement
  - Identification, control and status of items
  - Control of processes
  - Inspection, test and acceptance
  - Control of measuring and test equipment
  - Handling, storage, packaging and delivery
  - Nonconformance
  - Corrective action
  - Records
  - Management and independent assessments
  - Software quality assurance



NNSA POLICY LETTER

NAP-24

Approved: 6-20-13

WEAPON QUALITY POLICY

National Nuclear Security Administration

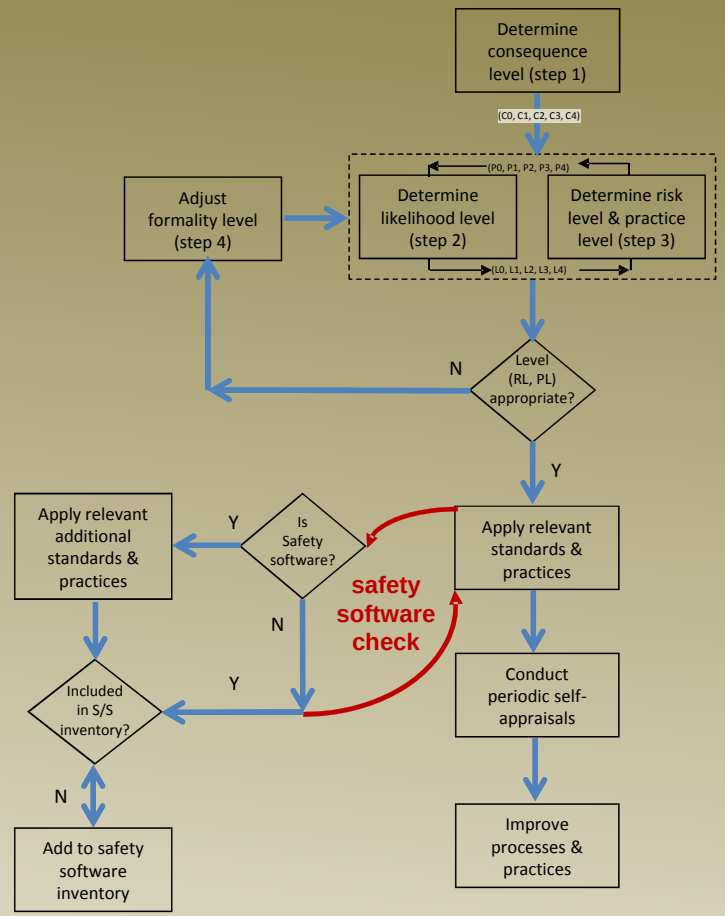
NATIONAL NUCLEAR SECURITY ADMINISTRATION
Office of Defense Programs

AVAILABLE ONLINE AT:
http://hq.na.gov

INITIATED BY:
Weapon Quality Division

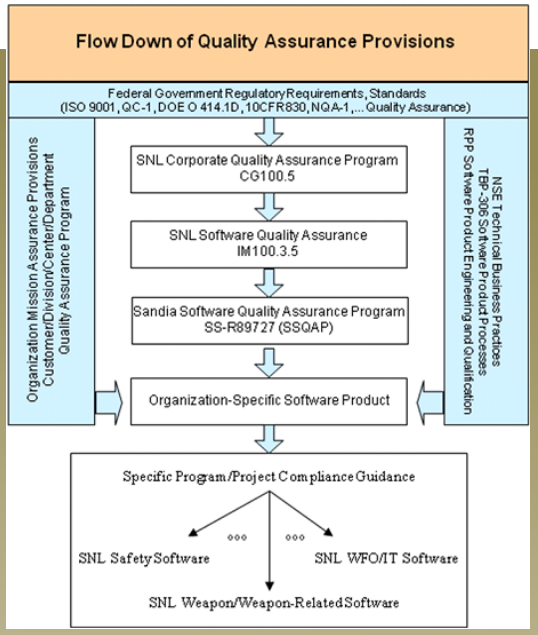
Software quality at Sandia

- Software quality is **imperative** for high-consequence engineering applications
  - **Unacceptable consequences** include loss of life or property, or impact to missions of critical importance
  - Embedded software poses greatest challenges
- Processes rely on **graded level of formality** based on risk assessment



Corporate procedure: Provide quality software

Sandia National Laboratories



- Corporate procedure: Provide quality software
  - Ensure adequate software quality for intended use
  - Sponsor quality software activities
  - Implement quality software requirements
  - Use a documented software process
  - Report quality assurance issues and perform self-assessments
  - Implement software quality processes
  - Document required information
  - Use the specific use specification, SSQAP, for implementation
  - Ensure safety software satisfies requirements of a consensus standard
  - Inventory safety software
  - Assess safety software
  - Provide safety software training
  - Maintain safety software
  - Implement DOE-specified software work activities
  - Conduct a periodic “quality software ” policy adequacy review

Example:
Space shuttle software qualification

Sandia National Laboratories

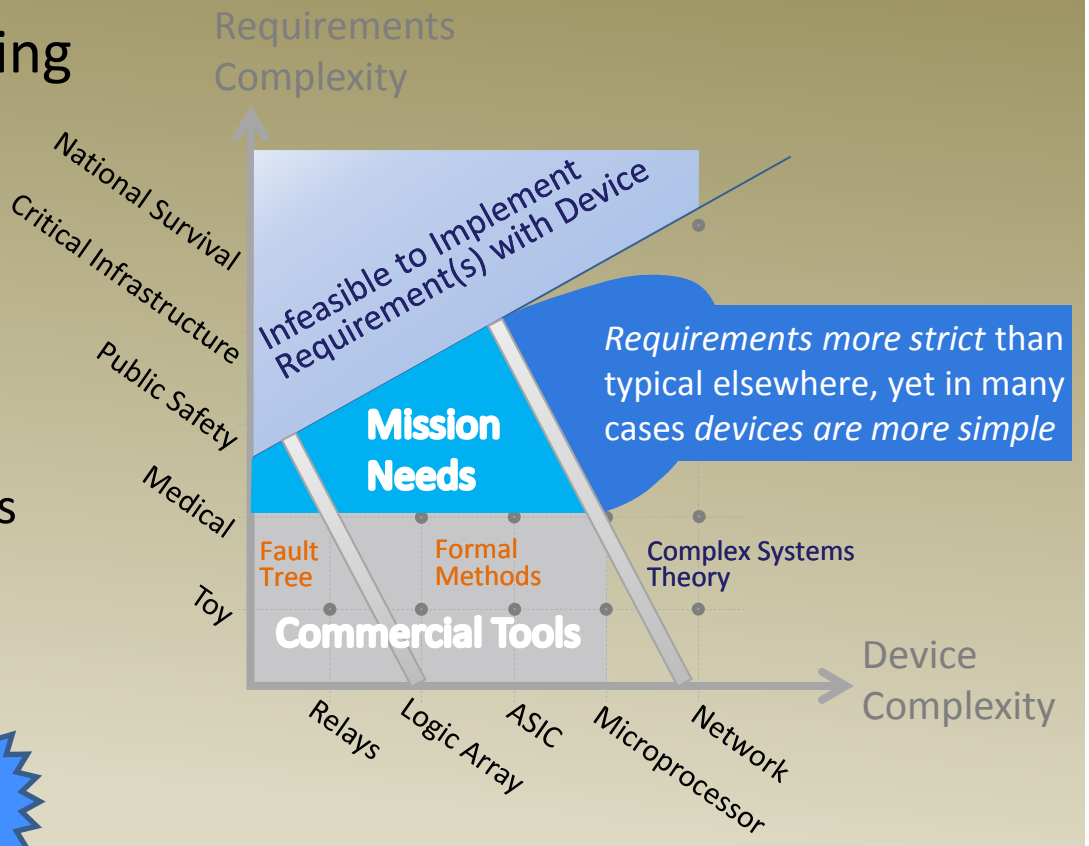
- After the 2003 Columbia accident, NASA requested that Sandia develop a laser-based imaging system to inspect space shuttle thermal protection systems

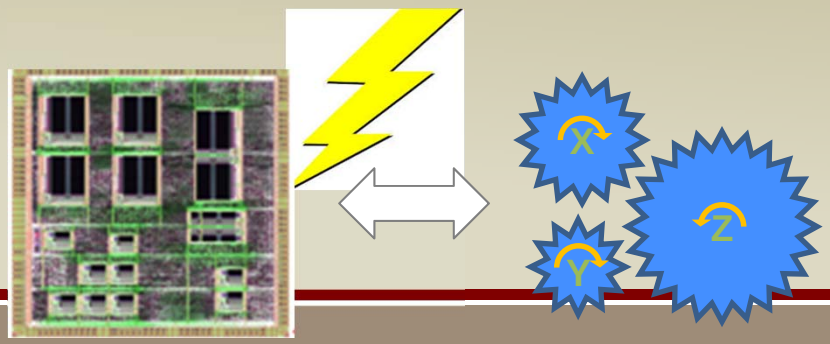
- Imaging system included ground station software
- System used successfully on all post-Columbia missions
  - NASA requested upgraded suite of high-consequence software products
  - Suite re-qualified for use through final mission in July 2011

Formal methods at Sandia

- Mathematical verification to identify **low-probability** violations of **high-consequence** quality, safety, and security properties

- Ongoing research addressing particular mission needs:
  - Large-scale complex systems
  - Abnormal environments
  - Digital-physical systems
  - Security: Adversarial threats

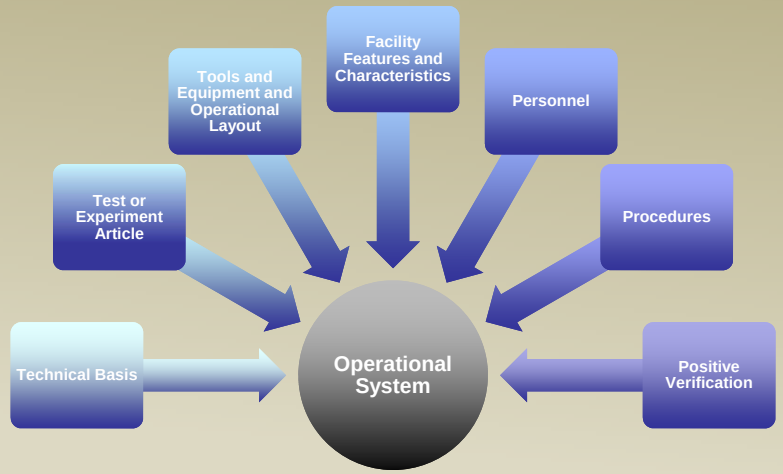




Example:
Operational safety (engineered safety)

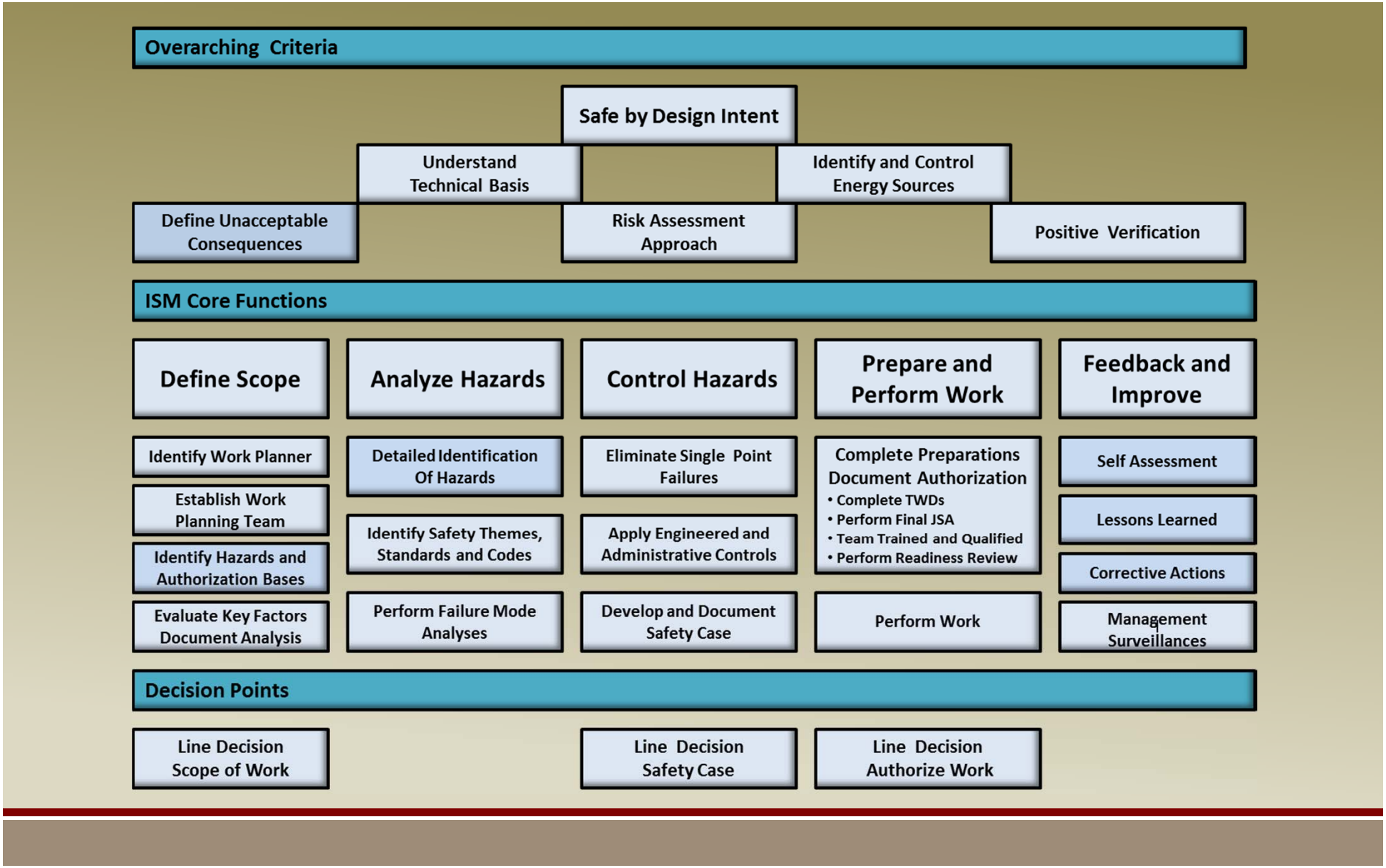
Sandia National Laboratories

- 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



Engineered safety model

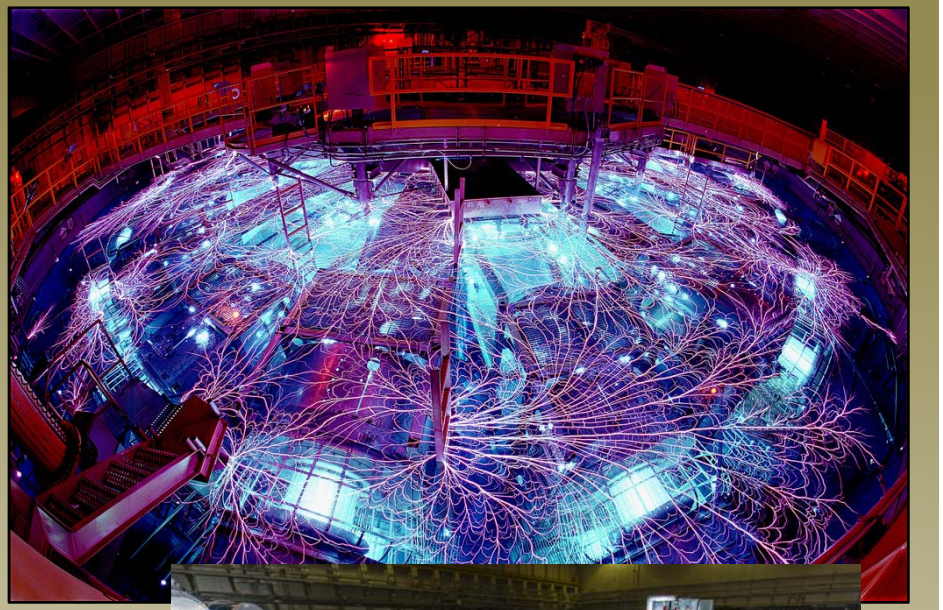
Sandia National Laboratories



Engineered safety model applied to plutonium experiments in the Z facility

Sandia National Laboratories

- Earth's most powerful pulsed-power facility and X-ray generator (26MA)
- Essential to nuclear weapon stockpile stewardship
- Used to measure properties of plutonium at extreme pressures and temperatures



System designed and fielded to assure safe and successful experiments

Sandia National Laboratories

- Identified unacceptable consequences
  - Radiation dose to a worker
  - Environmental contamination
  - > 6 month pause in operation
- Conducted failure mode effects and fault tree analyses
- Identified and implemented solutions
  - Eliminated failure modes
  - Provided positive assurance through 18 formal approvals for critical subsystems prior to key activities in the shot setup timeline
  - Designed a secondary system to manage a containment breach safely

Example:
Research quality standards

Sandia National Laboratories

RESEARCH QUALITY STANDARDS

Table of Contents

1

2

Sandia National Laboratories

Summary

Sandia National Laboratories

- Sandia is driven by the need to **prevent the unacceptable consequences** of a failure in our mission
- We have evolved from an emphasis on control and inspection to an emphasis on **defect prevention** as the **cornerstone** for our approach to quality
- Our culture is built on **values** and **principle-based behaviors and attitudes**
  - We align through our **values, vision and mission** and use **policies, processes and procedures** to enable quality mission results
  - We adopt or develop techniques and practices that enable a **disciplined approach** for the **engineering of products and services** with **assured quality**

Questions?

Sandia National Laboratories

"Excellence is an art won by training and habituation. We do not act rightly because we have virtue or excellence, but we rather have those because we have acted rightly. We are what we repeatedly do. Excellence, then, is not an act but a habit."

Nichomachean Ethics, Aristotle (384-322 BC)