SAND2011-5467C

A Robust Approach to Nuclear Weapon Safety

(SAND 2011-XXXXC)

Alton P. Donnell, Jr.

Sandia National Laboratories

Albuquerque, New Mexico, USA

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

Sandia National Laboratories

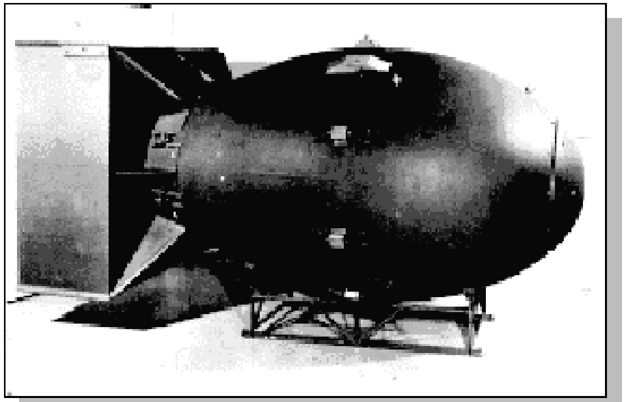
Guidance from the Top

- "Given the profound implications of their potential use, nuclear weapons must be subject to the most precise and stringent command and control, safety, and security possible. …
- We must also prevent accidental, inadvertent, or unauthorized access to or use of U.S. nuclear weapons and protect against their loss, theft, or seizure. …
- …measures shall be consistent with operational requirements and shall be continually assessed against existing and emerging threats as well as technological opportunities for improvement."

President George W. Bush, NSPD-28, 2003

Weapon Design and Safety Changes

Nuclear weapons and their safety designs have changed dramatically over the last 50 years.

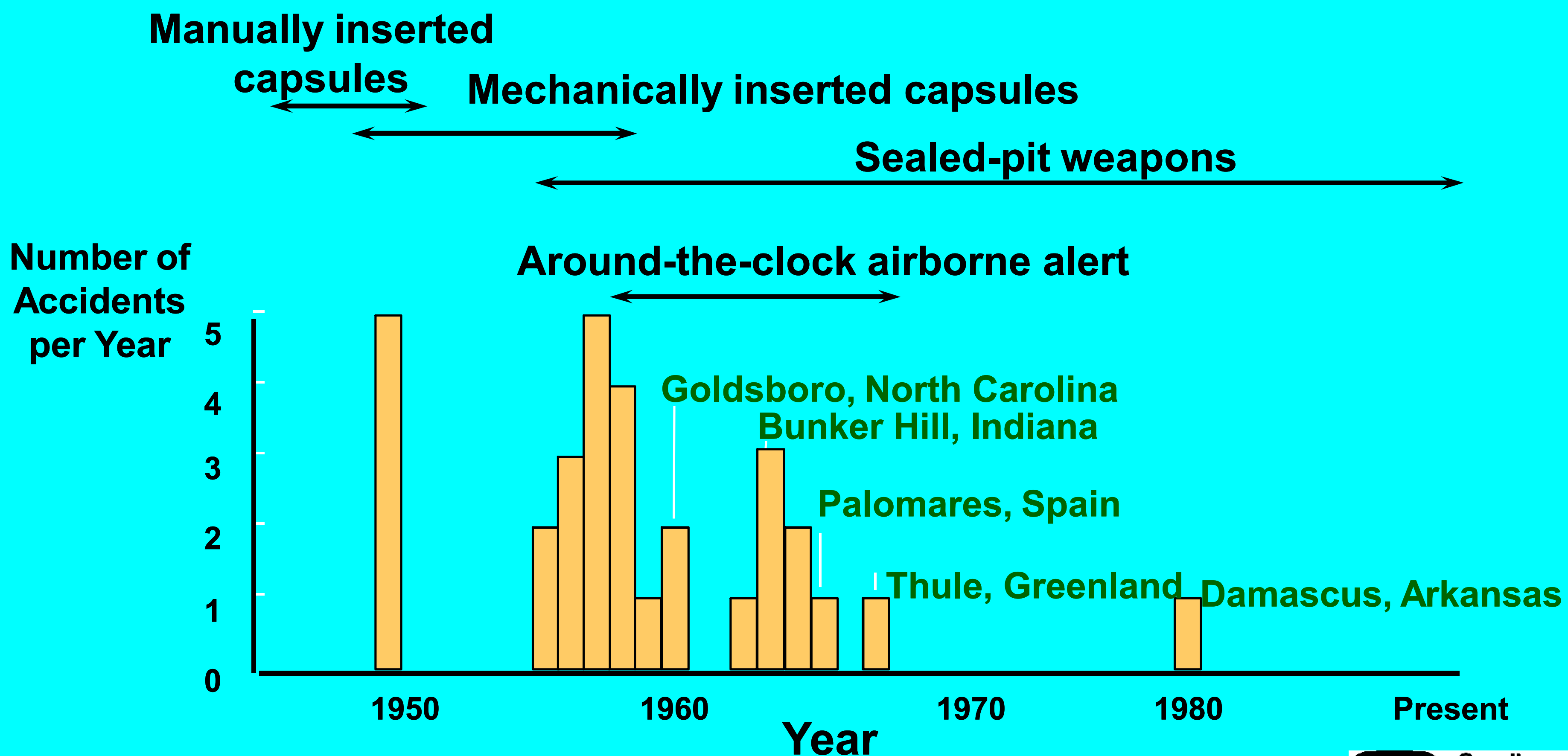


FATMAN

MK 7 Bomb

B61 Bomb

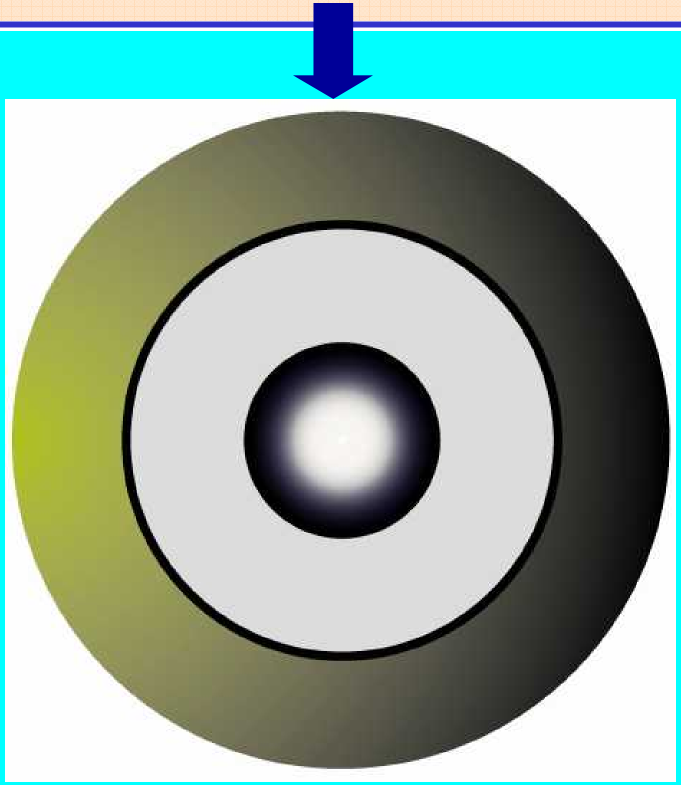
Early Weapon History and Accidents



Sandia National Laboratories

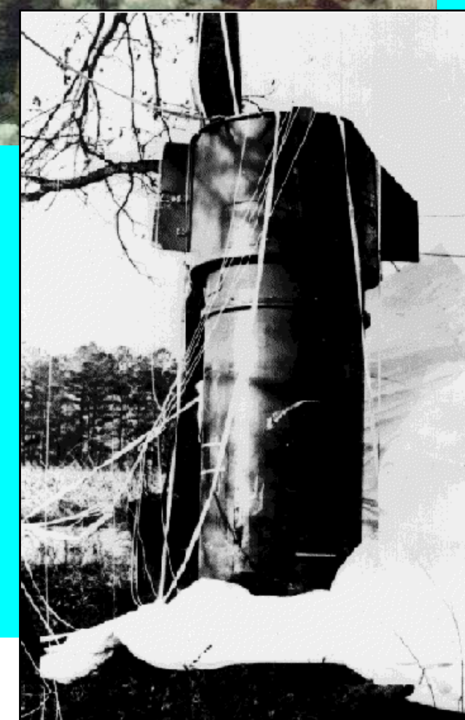
Sealed Pit Weapons
(1957 to present)

- **Pro:**
  - **Efficient**
  - **Requires significantly less fissile material**
- **Con: Must have effective positive measures throughout STS**
  - **Early**
    - **Physics package has no positive measures associated with it**
    - **Some designs not inherently one-point safe**
    - **Significantly increased likelihood of Pu scatter**
  - **Recent**
    - **Designs inherently one-point safe**
    - **Some designs include detonator safing**



GOLDSBORO, NC ACCIDENT
January 24, 1961

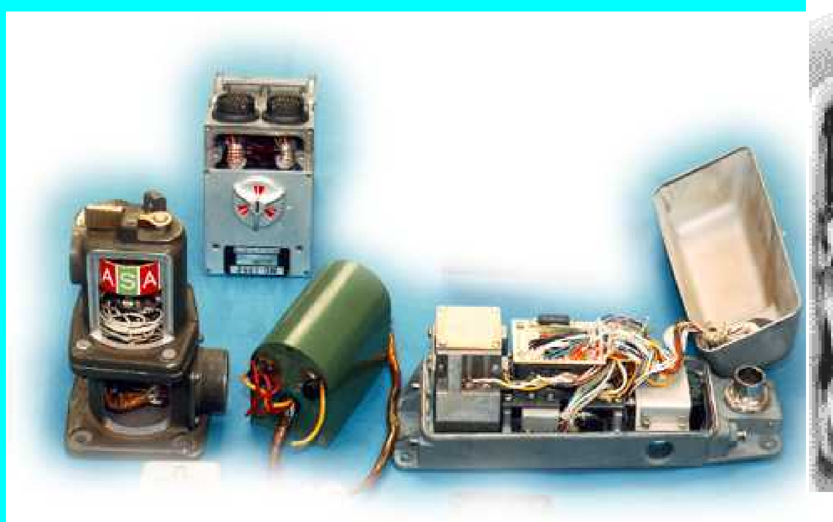
- B-52 airborne alert mission
- Two weapons separated from the aircraft during aircraft breakup
- One bomb parachute deployed and the weapon received little impact damage
- The other bomb fell free and broke apart upon impact -- no explosion
- No detectable radiation and no hazard in the area
- Five of the eight crew members survived
- A portion of one weapon, containing uranium, could not be recovered
- Air Force purchased an easement requiring permission for anyone to dig

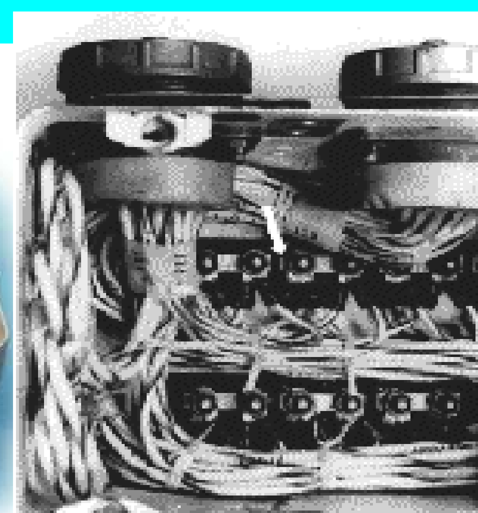


Ready/Safe Switches

- Early safety device
- Mechanical switch
- Manually or mechanically operated
- Interrupted the firing lines
- Many variations

But, between 1961 and 1981, 25 Ready/Safe switches operated inadvertently due to equipment malfunction or human error





Sandia National Laboratories

Bunker Hill, IN Accident

December 8, 1964
Taxing B-58A with 5 nuclear bombs

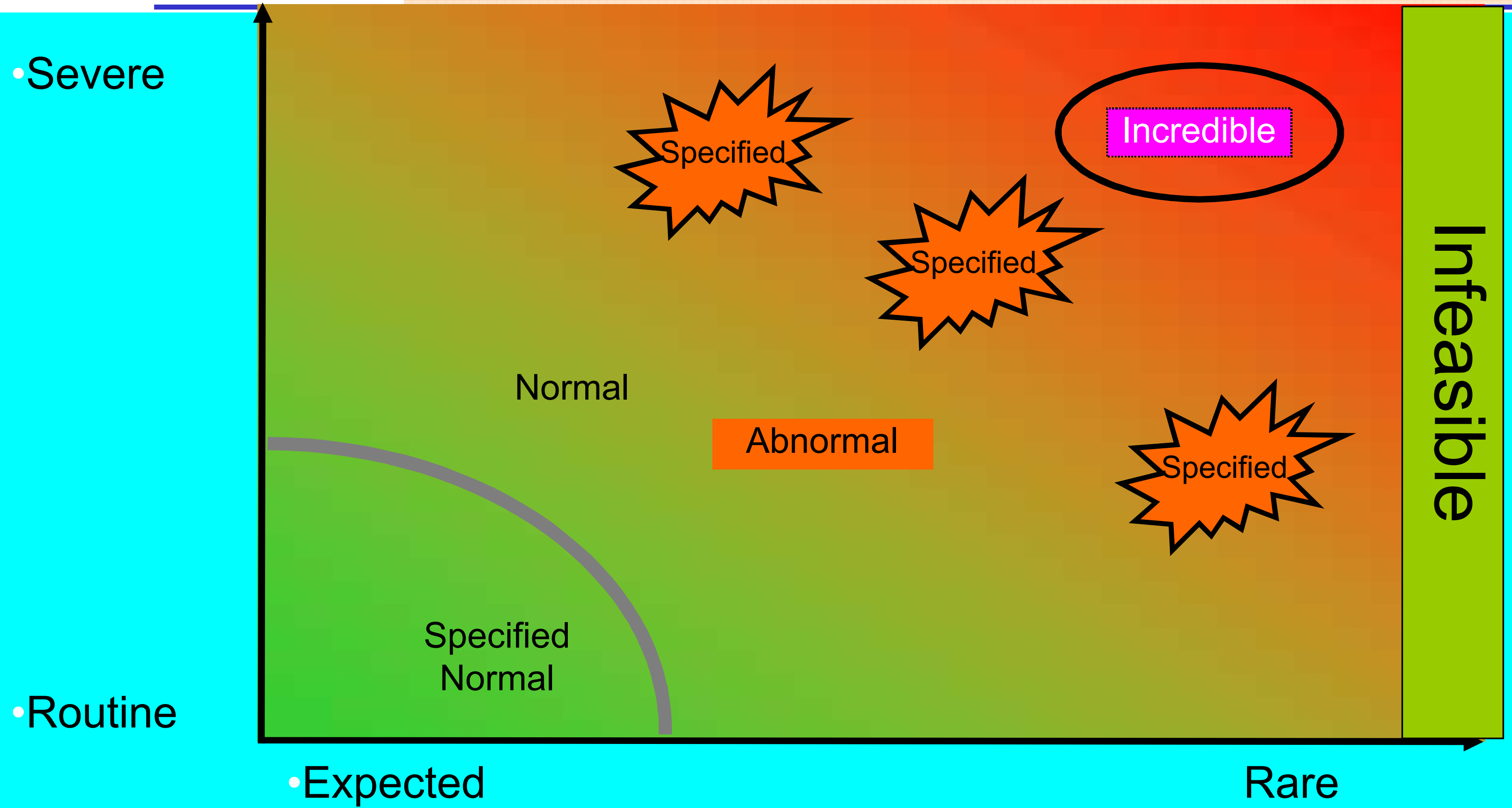
Rethinking Safety after Palomares and Thule

- **Palomares and Thule were major dispersal accidents costing $$$s**
- **Key DoD management decisions**
  - End airborne alert to reduce weapon exposure
  - Examine technology to reduce the potential for dispersal
  - Develop quantitative requirements for premature nuclear detonation

Palomares, Spain 1/66

Sandia National Laboratories

Environments



The very severe environment is ***not*** necessarily ***the most hazardous***

Sandia's Design Philosophy

Nuclear Weapon Safety Throughout All Design Phases

- Fundamental Nuclear Safety Design Requirements
- Supporting Nuclear Safety Design Requirements

- *Nuclear Explosive and Weapon Surety Policy*

Sandia's Nuclear Weapon Surety Policy

By following our philosophy, we will meet both our external and internal requirements

Fundamental Design Requirements

- Provide Assured Safety
- Use the Nuclear Safety Design Principles - **(I^3)**
  - Isolation
  - Incompatibility
  - Inoperability
- Develop a Nuclear Safety Theme
- Identify nuclear safety-critical features (subsystems, components, etc.) necessary for implementation
- Implement the theme by flowing down requirements to the nuclear safety critical subsystems, components, features
- Document in a Nuclear Safety (NS) Specification

What is "Assured Safety"

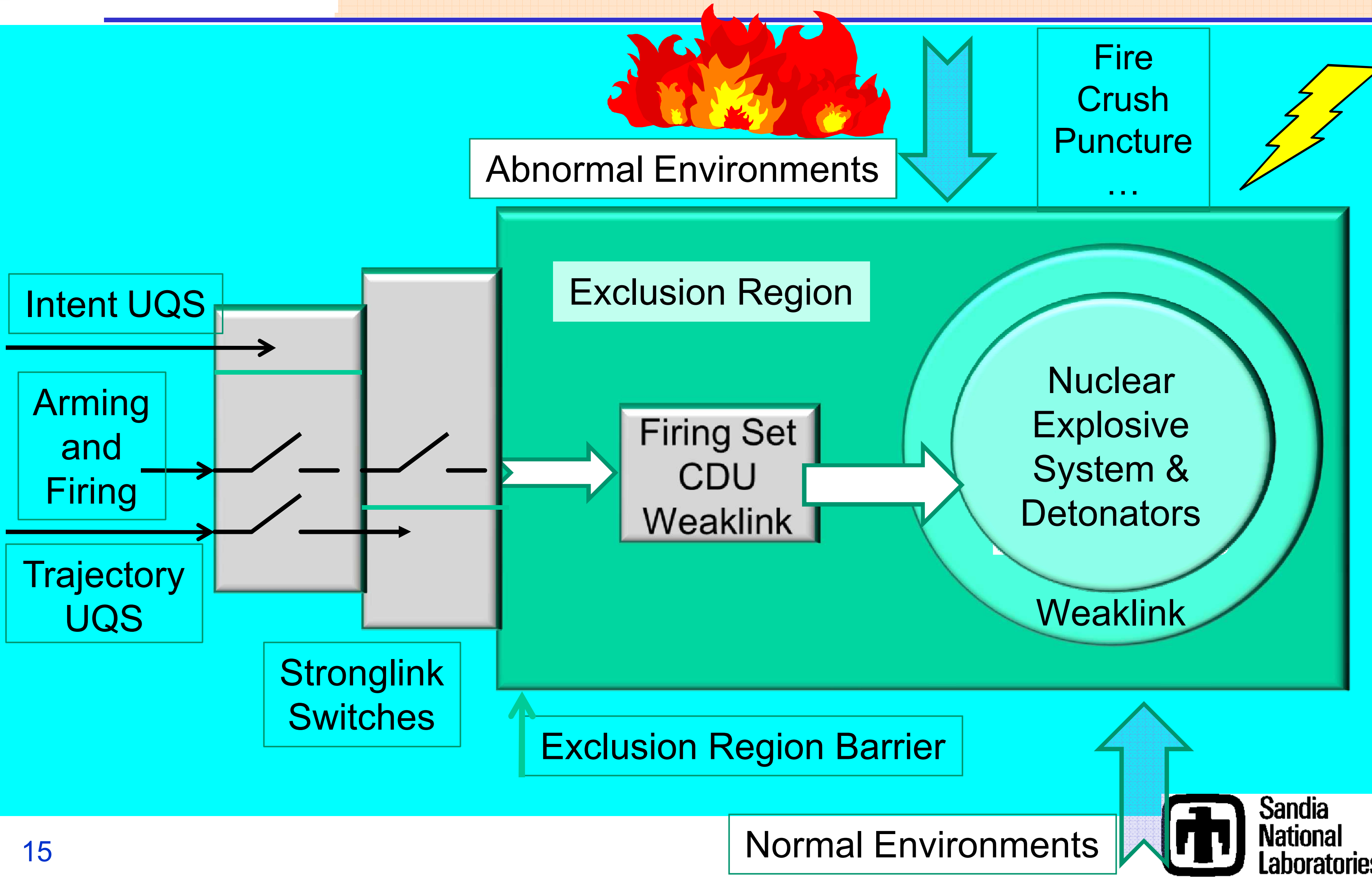
- Assured Safety (Concept)
  - A high-consequence system such as a nuclear weapon, a nuclear reactor, hydroelectric dam, or an electrical grid being designed in such a way that it is safe **regardless of accident scenario and whether or not that accident scenario has been accounted for in the design**.
- Assured Nuclear Weapon System Safety
  - ***Isolation* of compatible energy from nuclear detonation-critical components of an operable nuclear weapon until after the weapon becomes irreversibly *inoperable*.**
- Assured Safety (at other than the system level)
  - Predictably meets nuclear safety requirements

Nuclear Safety Design Principle

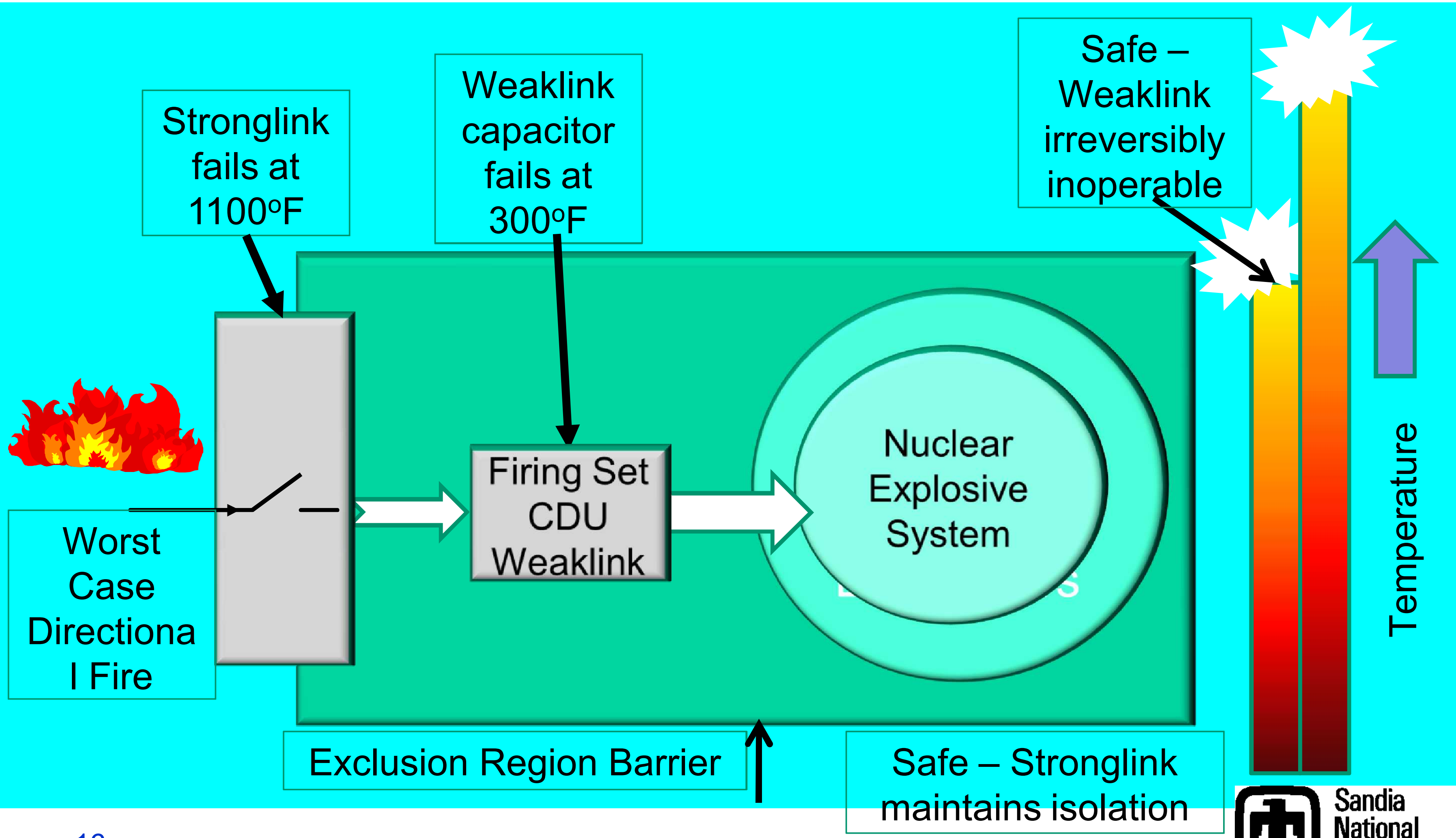
- **Isolation**
  - The predictable separation of detonation-critical elements from compatible energy.
- **Incompatibility**
  - The use of energy or information that will not be duplicated inadvertently.
- **Inoperability**
  - The predictable inability of detonation-critical elements to function.

Sandia National Laboratories

Modern Nuclear Detonation Safety Architecture



Thermal Weaklink Example



Sandia National Laboratories

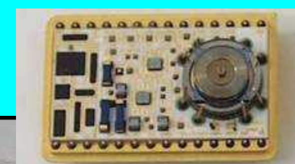
Supporting Nuclear Safety Design Requirements

- Multiple **independent** abnormal and normal environment safety subsystems will be used to ensure the nuclear safety design can meet qualitative and quantitative requirements
- Assured safety will be demonstrated **without precise definition of abnormal environment scenarios**
- Nuclear safety critical features will be designed to
  - be **passive,**
  - to **fail safe**, and,
  - to be **verifiable**
- The number of components that are critical to nuclear safety will be **minimized, but complete**

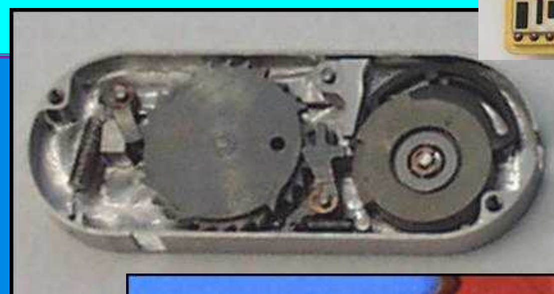
Sandia National Laboratories

Continuing Evolution of Surety Technologies

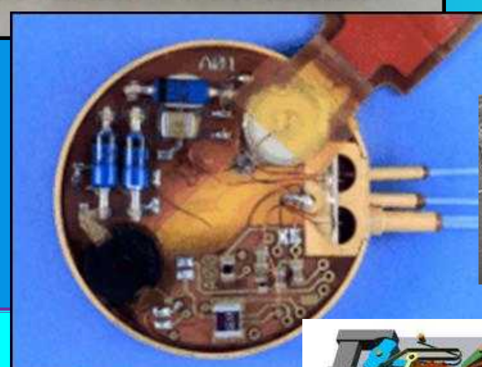
Trajectory Sensor



Detonator Stronglink



Detonator Safety
Multi-Point Safing
Direct Optical Initiation



Micro Firing Set

Optical Stronglink

Slapper Blocking Stronglink

Prevent nuclear yield and SNM dispersal

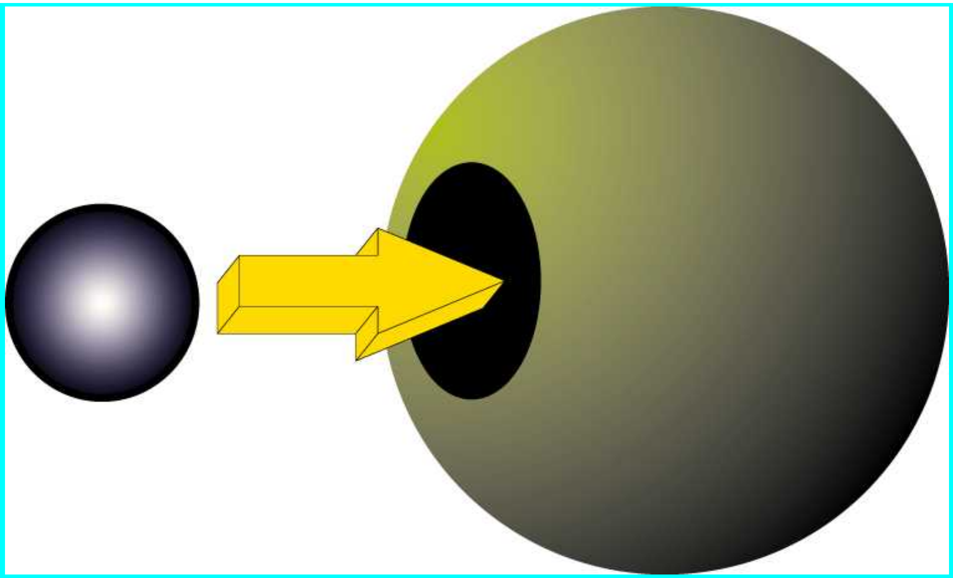
Sandia National Laboratories

Safety Challenges for the Future

- Do we understand the normal and abnormal environments?
  - Are there Black Swans lurking?
  - Potential Fukishimas?
- Have we defined the “requirements space” well enough?
  - Is pre-launch/release well defined?
  - Have we addressed post-launch adequately?
    - Is hitting the right target an element of post-launch safety?
    - Location enablement as a requirement?
    - Or self destruct, if off course?
- Are we serious about integrating “surety”?
  - Is piecemeal good enough? Are stovepipes acceptable?
  - Can a integrated safety, use control, and security system provide a non-linear improvement?
    - Self awareness to include location awareness, surroundings, threats, …
    - Continuous internal communication amongst systems

Questions?

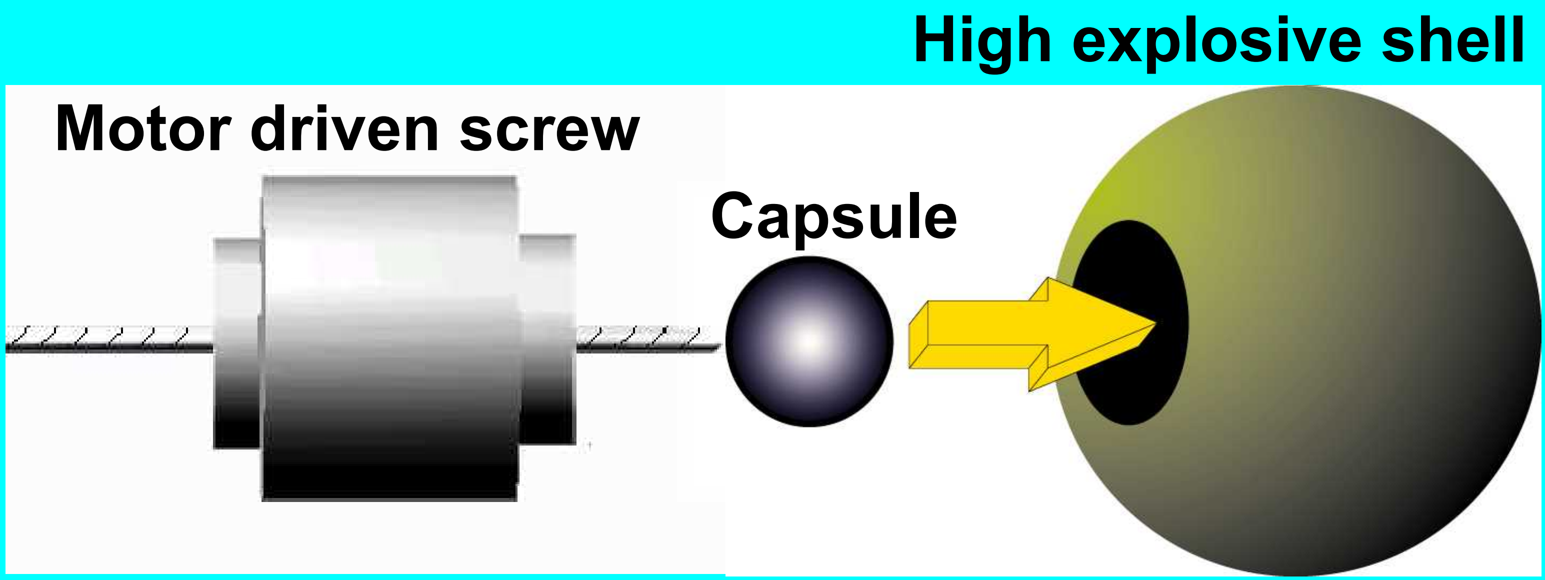
Manually Inserted Capsules
(1945 - 1951)



- **Implementation: Separation of fissile material and high explosive (HE);**
- **Pro: Inherent safety w/o capsule (transportation and storage); assembly only by human intent)**
- **Con: No assured safety with capsule installed**

Sandia National Laboratories

Mechanically Inserted Capsules
(1952 - 1957)



- **Implementation:** **Separation of fissile material and HE and *electrical isolation to motor***
- **Pro:** **Inherent safety w/o capsule**
- **Con:** **with capsule, accident could assemble weapon by operating motor or by mechanical damage**

Sandia National Laboratories