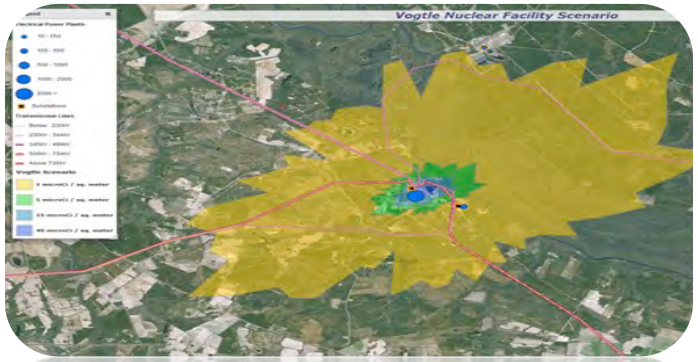
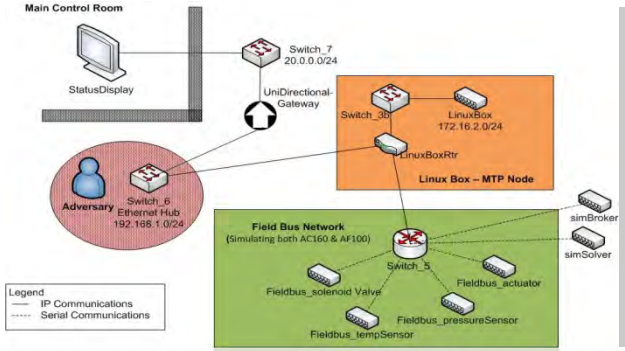
Exceptional service in the national interest

Sandia National Laboratories





Secure and Sustainable Energy Future

Integrated Cyber Physical Impact Analysis

Douglas M. Osborn

Governor's Summit on Energy Security & Infrastructure

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. SAND2016-7845 PE & SAND2016-0090-PE

Sandia Addresses National Security Challenges

1950s	1960s	1970s	1980s	1990s	2000s	2010s
Nuclear weapons	Development engineering	Multiprogram laboratory	Missile defense work	Post–Cold War transition	START Post 9/11	LEPs Cyber, biosecurity proliferation
Production and manufacturing engineering	Vietnam conflict	Energy crisis	Cold War	Stockpile stewardship	National security	Evolving national security challenges

Sandia addresses energy challenges

Sandia National Laboratories

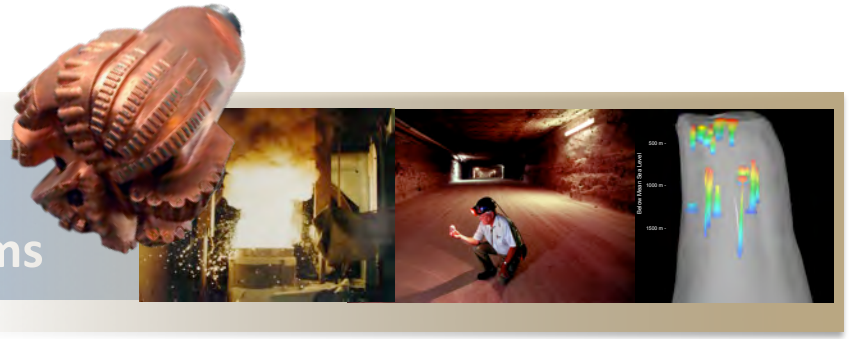
1970s	1980s	1990s	2000s	2010s
Multiprogram laboratory Energy crisis	Missile defense work Cold War	Post–Cold War transition Stockpile stewardship	START Post 9/11 National security	LEPs Cyber, biosecurity proliferation Evolving national security challenges

- Solar
- Nuclear
- Fossil
- Wind
- Geothermal
- Combustion
- Nuclear Waste

- Atmospheric Monitoring
- Water & Energy
- Grid/Energy Storage
- Biomass
- Energy Cyber

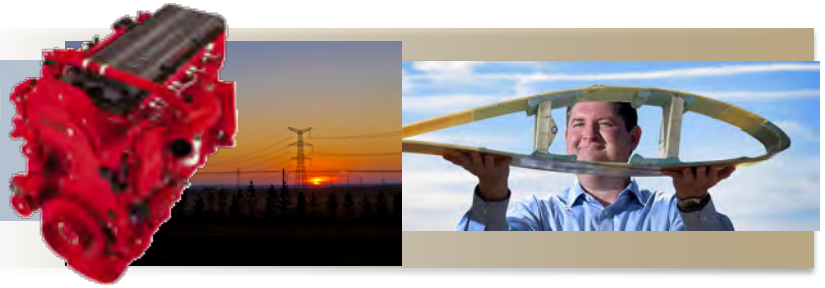
Examples of Sandia's impact

Core, dynamic, and rapid response



Core: Long term research that solves the nation's immense problems

- Drilling technologies, nuclear reactor safety, nuclear waste disposal, and Strategic Petroleum Reserve



Dynamic: Addressing current national Needs on a 5-10 year timeframe

- Efficient engines, renewable energy technologies, and grid modernization

Rapid Response: Quick mobilization of expertise for urgent national needs

- Aliso Canyon, Fukushima, and Deepwater Horizon

Current US Energy Objectives

Secure and Resilient

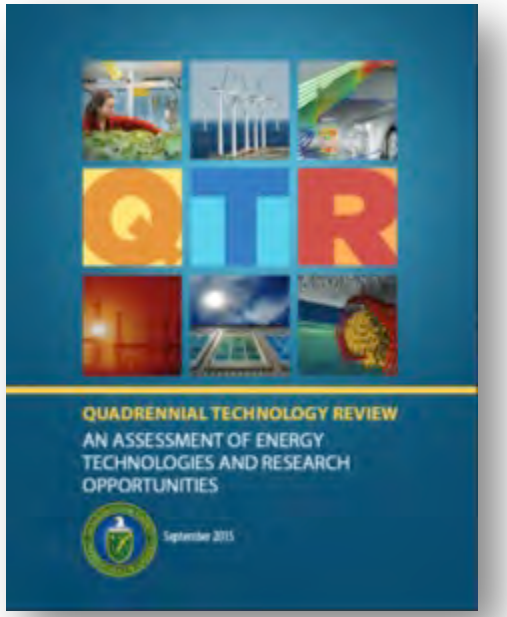
- Energy systems should be secure from and resilient to natural disruptions as well as man-made attacks. Security must be addressed along the entire energy service value chain from supply (energy resources, materials, and technologies) to operations (distribution, storage, and end-use of fuels/ electricity).

Economically Competitive

- Energy systems should provide energy services that are abundant, sustainable, and affordable—taking into account the full market impacts and life-cycle costs of the energy-service value chain.

Environmentally Responsible

- Clean energy systems should minimize air, water, and land pollutant emissions; GHG emissions; biota impacts; and disruption of water and land resources.

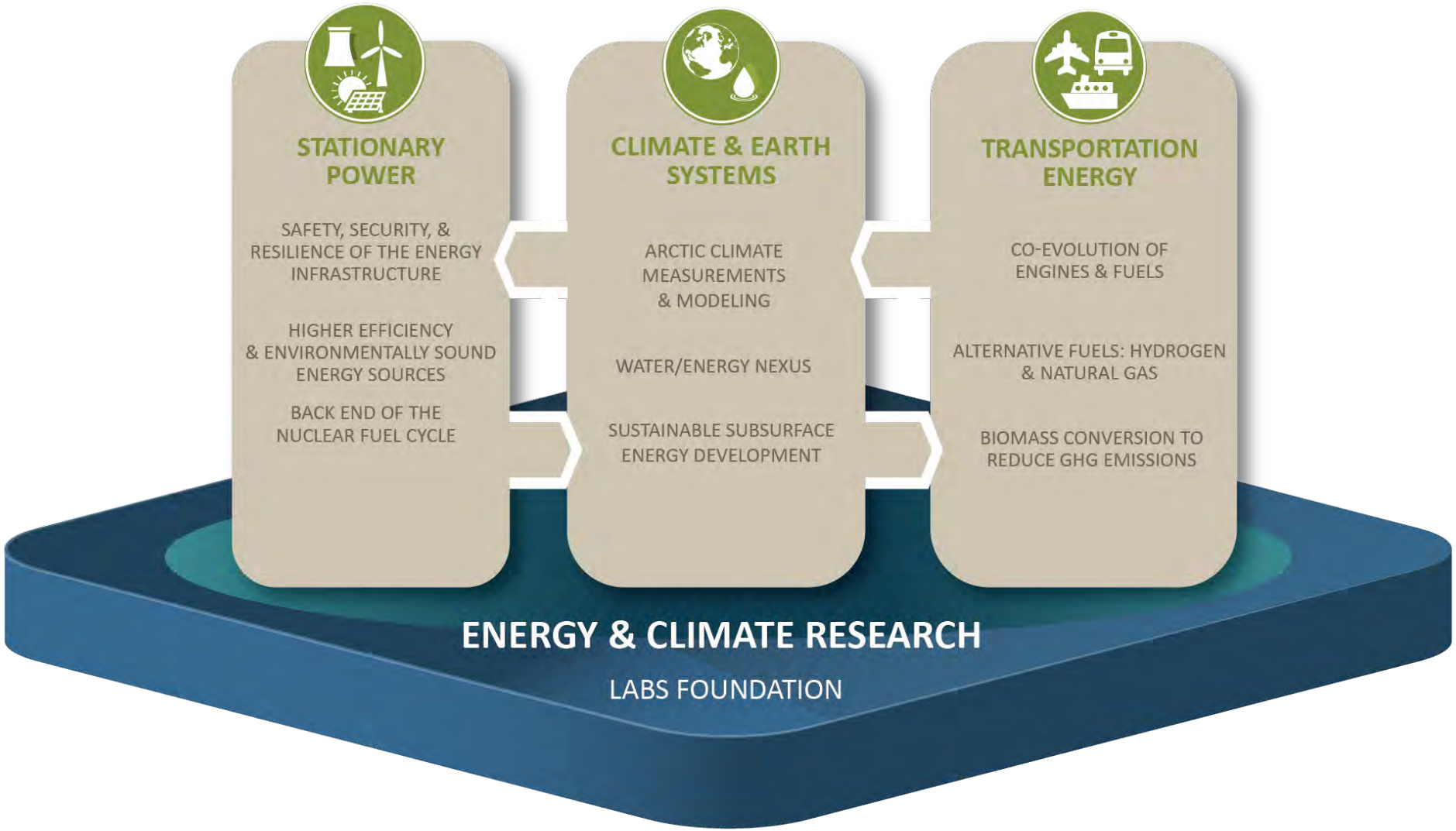


Source: QTR, page 19

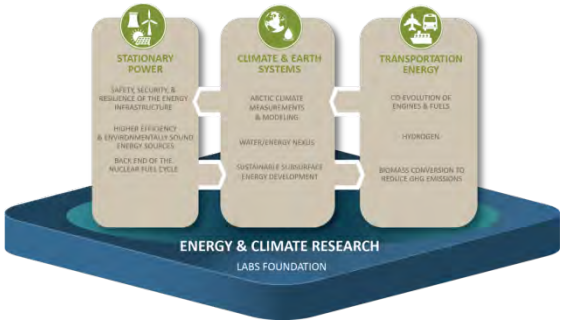
Secure & Sustainable Energy Future
High Level Objective

Drawing upon our differentiating capabilities and as a principal element of the national lab system, Sandia makes major contributions to the nation's energy security and resilience, economic viability, and environmental sustainability.

SSEF Strategy Elements



Stationary Power



Safety, Security & Resilience of the Energy Infrastructure

Protect energy systems through R&D advances in cyber and physical security and resiliency

Higher Efficiency & Environmentally Sound Energy Sources

Advance the next generation of energy technologies

Back End of the Nuclear Fuel Cycle

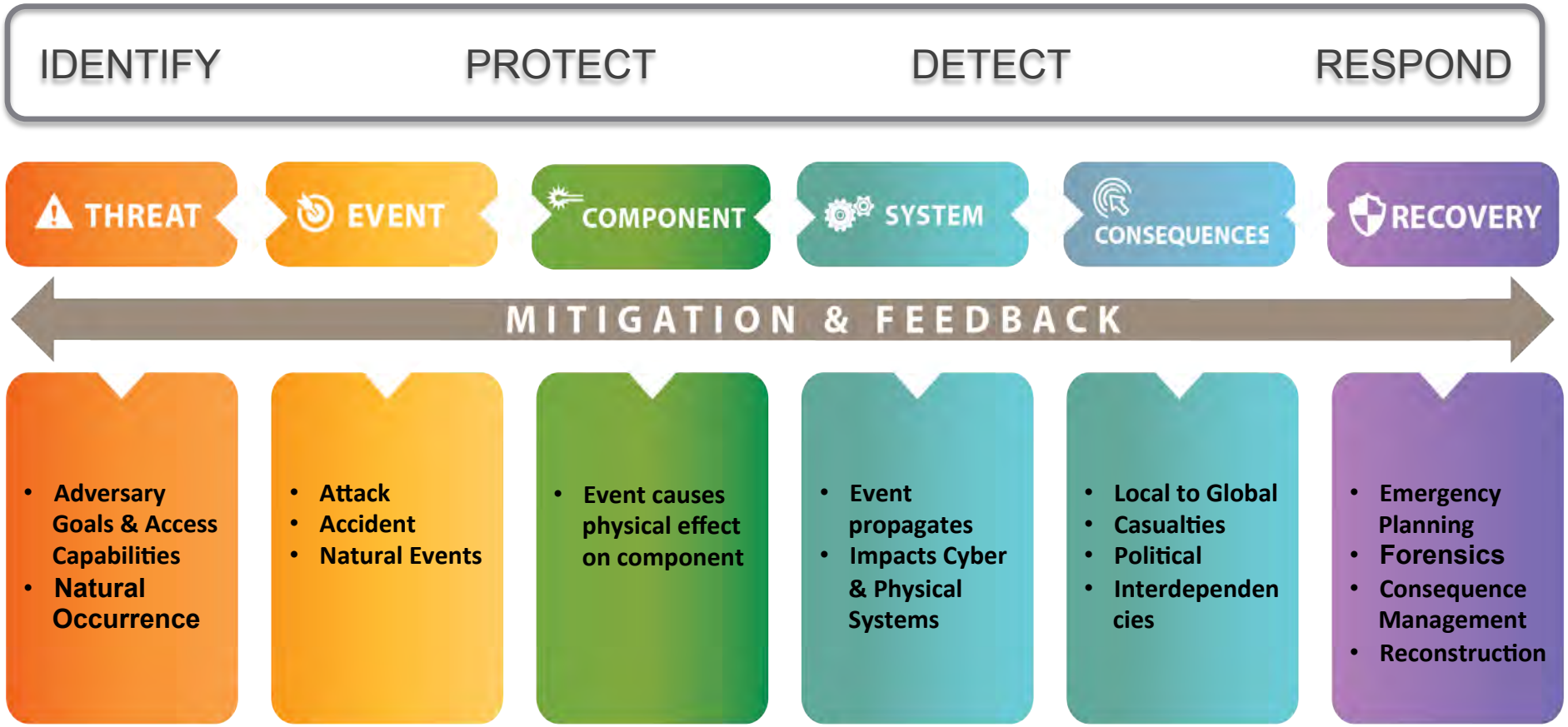
Develop effective radioactive waste solutions across transportation, storage, and disposal

Integrated Cyber Physical Impact Analysis (ICPIA)™

Full Spectrum Modeling Framework

- Sandia integrates an array of modeling and simulation capabilities to manage this risk and secure systems:
  - Threat modeling
  - Adversary-based vulnerability assessment
  - Network and control system emulation, simulation, and analysis
  - Physical system modeling and simulation
  - Critical infrastructure modeling

ICPIA Modeling and Activities



Not linear: Can start anywhere into the framework based on the question asked, or problem to be solved

ICPIA Example Use Cases

- **Support New Threat Analysis** - Explore the impact of previously unidentified threats and vulnerabilities
- **Provide test bed for integrating systems** – upgrading a system and analyze for an improved security posture
- **Help design secure architectures** – evaluating protective measures (detection, deter, respond) such as encryption
- **Act as a training tool** - for Red Team attackers or for Plant Operators to develop event response procedures
- **Identify R&D gaps** – to reduce system risk
- **Supports integrated risk management** - attack difficulty metrics, impact and consequence analysis, moving to "all hazards" analysis

Questions?