

*Exceptional service in the national interest*



# *Exploring Risks Associated with the Global Expansion of Civilian Nuclear Power*

May 5, 2016

***Susan Y. Pickering***

***Director, Nuclear Energy and Fuel Cycle Programs***

***Presented to GWU Global Nuclear Energy Expansion Workshop***



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. SAND NO. 2011-XXXX

# Drivers



The growing global availability of nuclear technology and materials can increase the risk of state proliferation by reducing the time needed to develop a nuclear weapons program.



A country could potentially use a developing nuclear energy program to mask a nuclear-weapons program



The global expansion of nuclear energy will further strain already taxed IAEA safeguards resources.



The existence of more nuclear technology and materials increases the attractiveness of (and opportunities for) nuclear terrorism and nuclear theft.



The presence of more nuclear materials and technology in countries lacking experience and institutional knowledge raises the potential for accidental release of nuclear or radiological materials into the environment.



The trend towards increasingly digitized and networked nuclear facilities significantly expands operational uncertainty and adds complexity to implementing safeguards and security.

# Nuclear Energy Analysis Framework

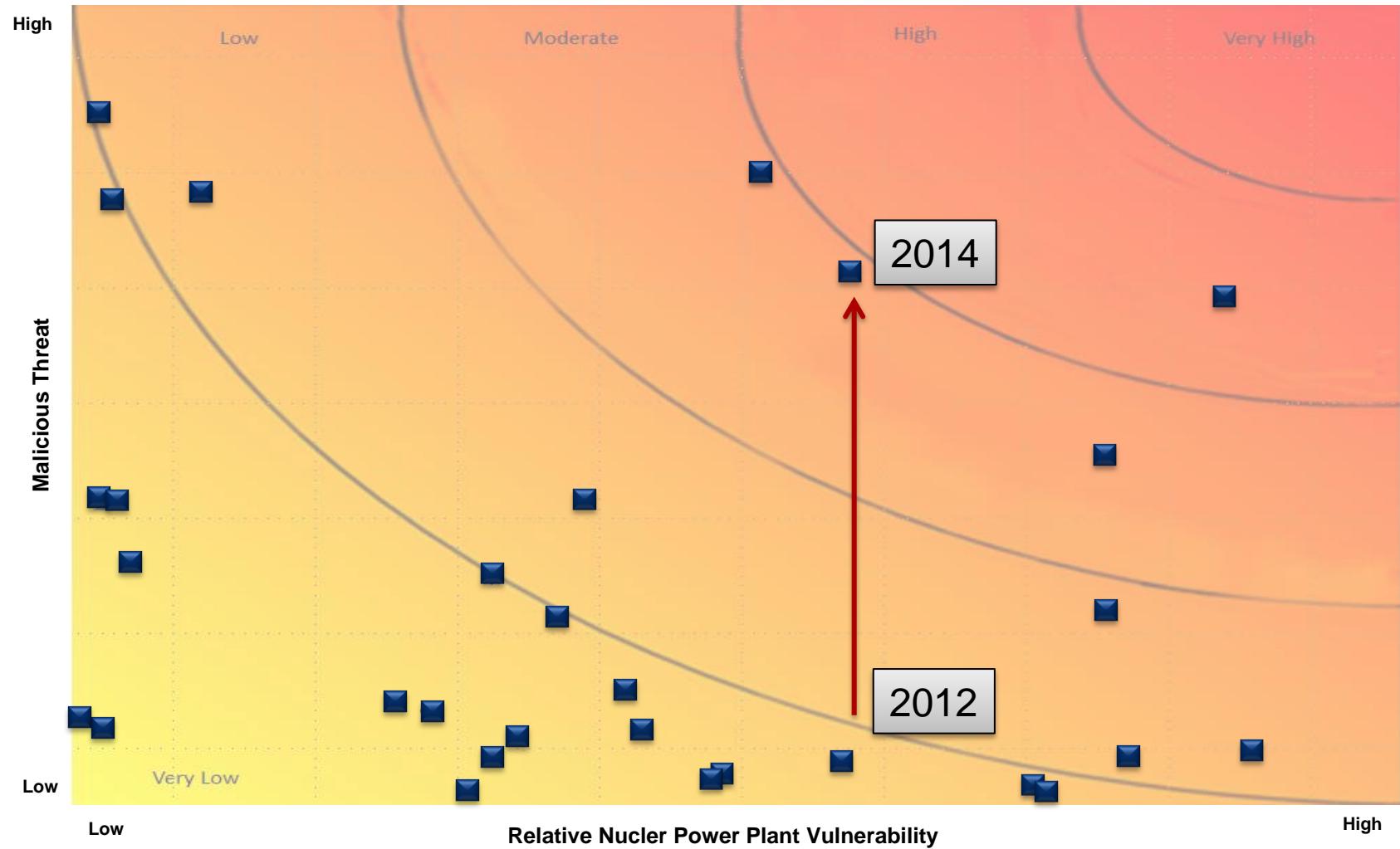
## Three Scenarios

- “Al Qaeda” Scenario – theft of radioactive material for an RDD
- “Nuclear Power Plant as Weapon” Scenario – manipulation or sabotage of a NPP resulting in a major radiological release
- “Dual Use Material Proliferation” Scenario – Nation-state develops indigenous nuclear weapon capability

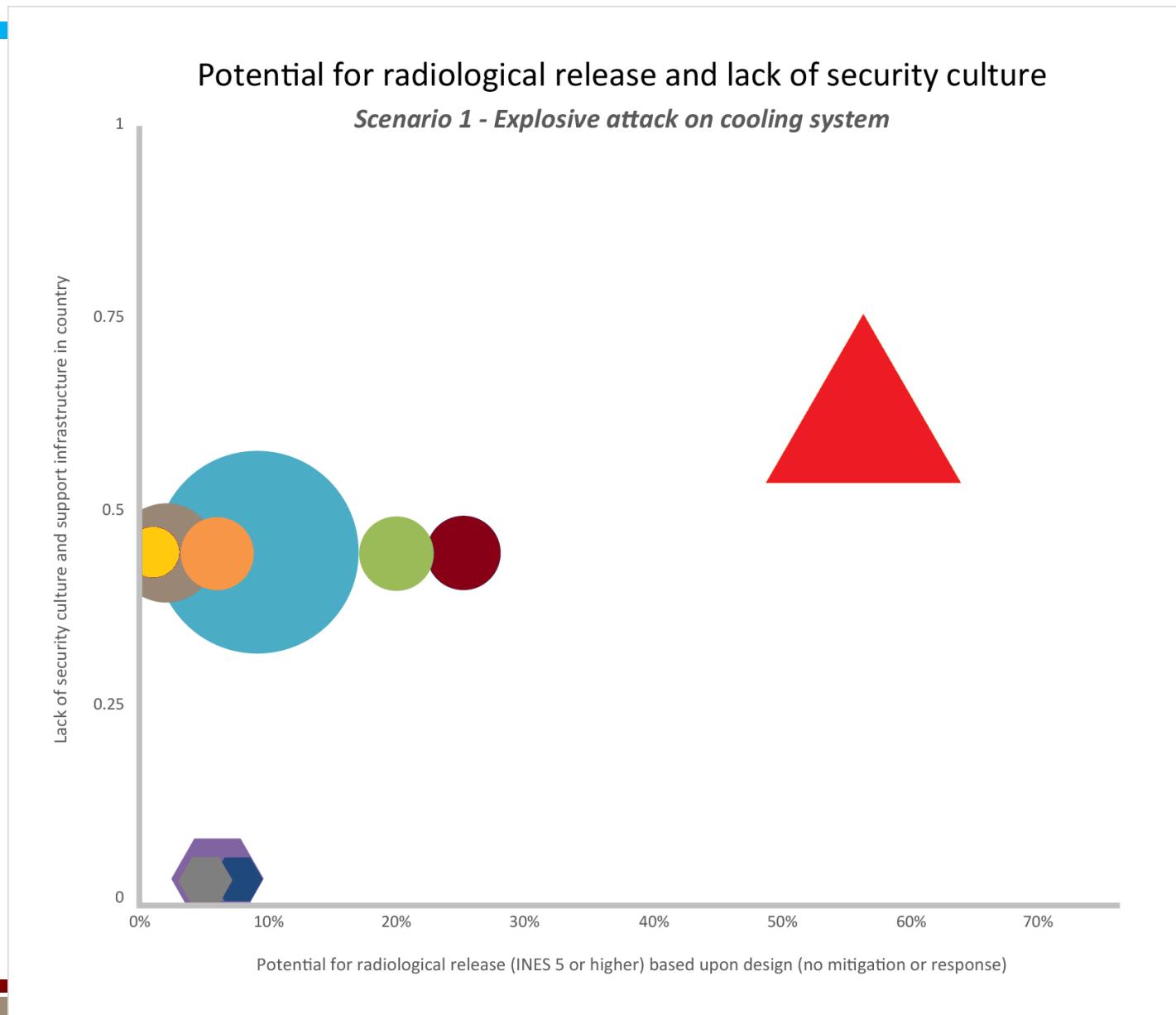
Asset	Threat	Pathway	Triggering Event	Outcome
Expertise	Theft	Accident or Natural Disaster	Major Power Disruption	Casualties
Information	Purchase	Physical Attack	Threat of Proliferation	Economic Damage
Technology	Indigenous Development	Cyber Attack	Major Radiological Release (Dispersion)	Environmental Damage
Materials	Disruption	Black Market Illicit Exchange	Detonation of Device with Nuclear Yield	Coercion of US Interests
Installations		Investment		Public Perception
Transportation				Political Damage

# Relative Country Risk Prioritization

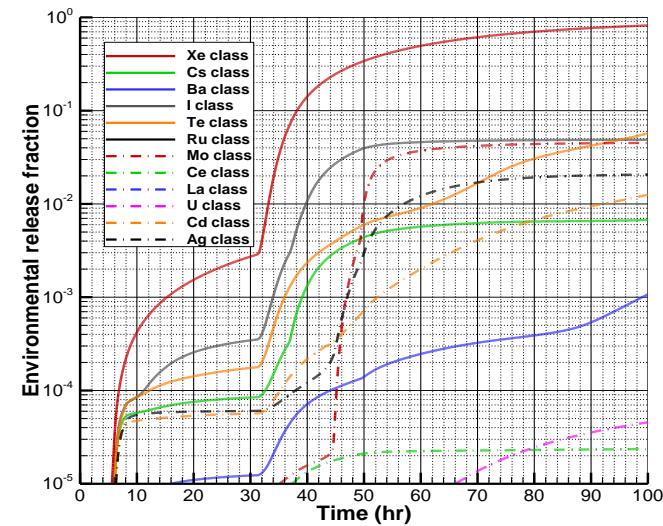
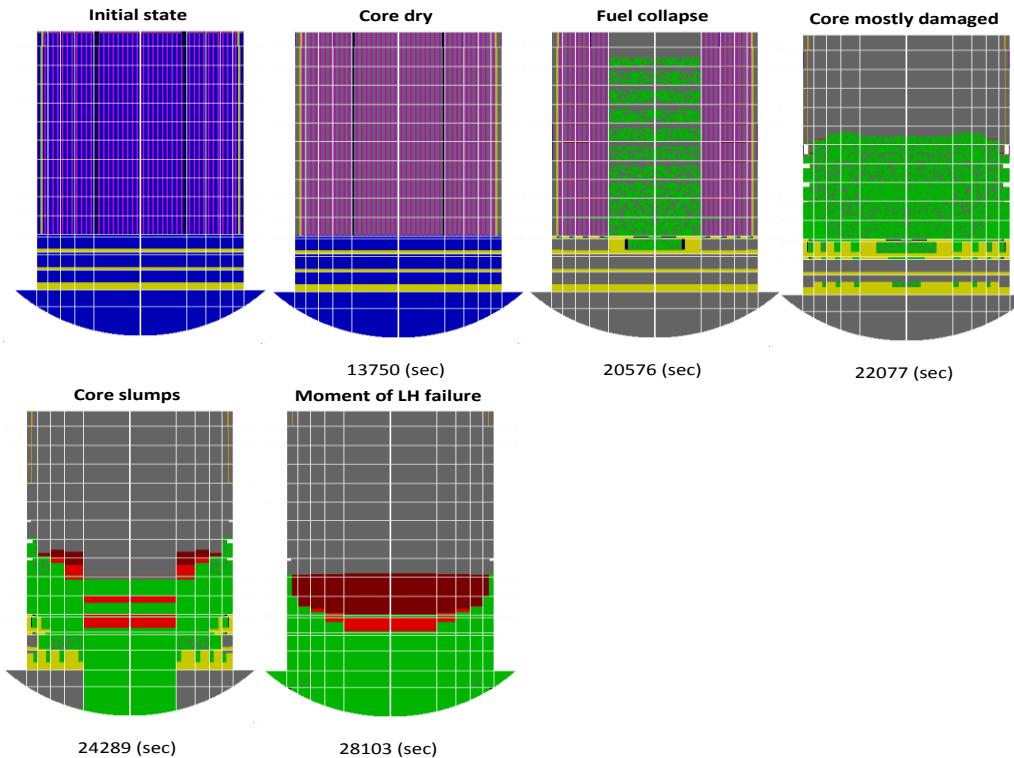
Relative Likelihood for a Malicious Attack on Power Reactors



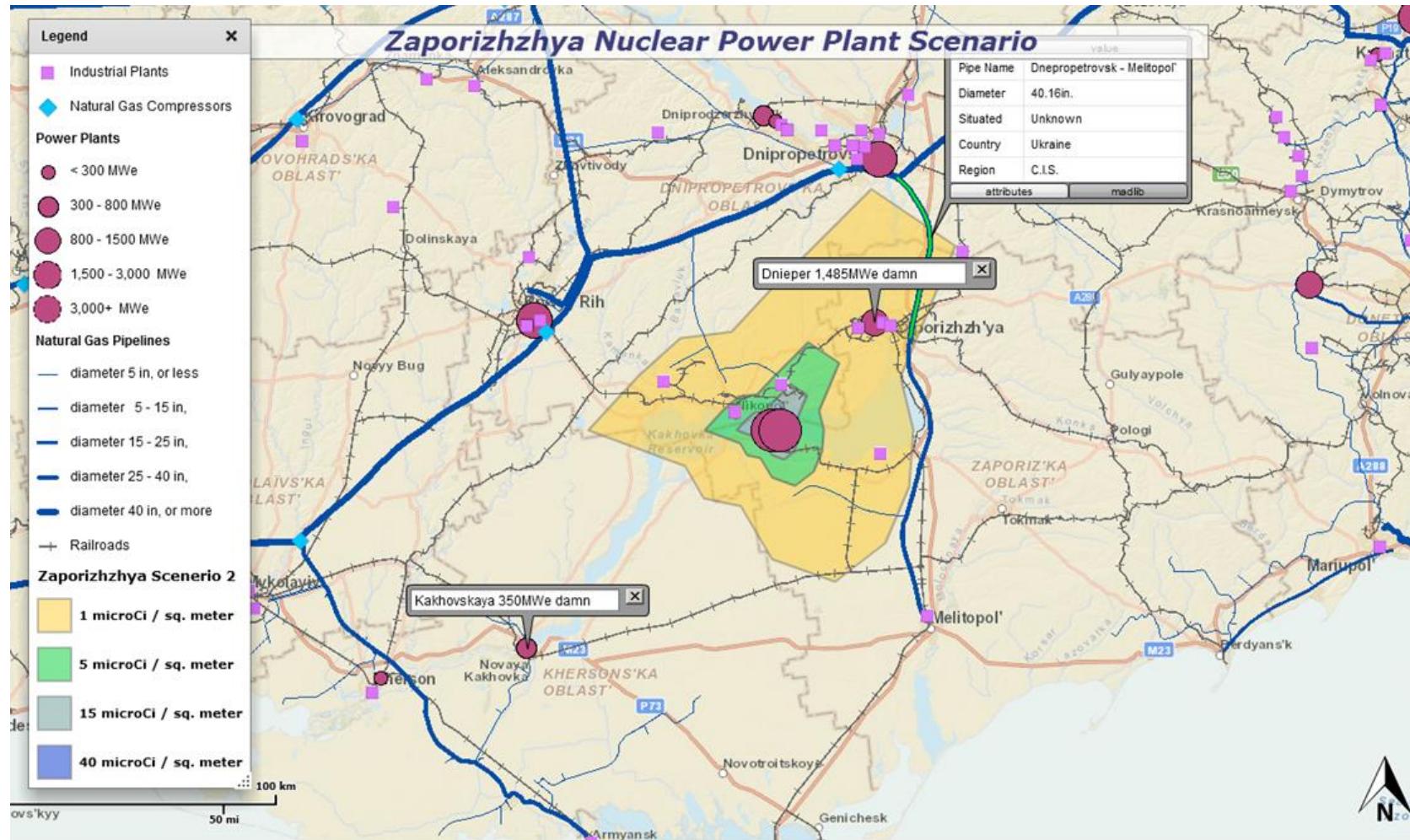
# Relative Reactor Risk Assessment



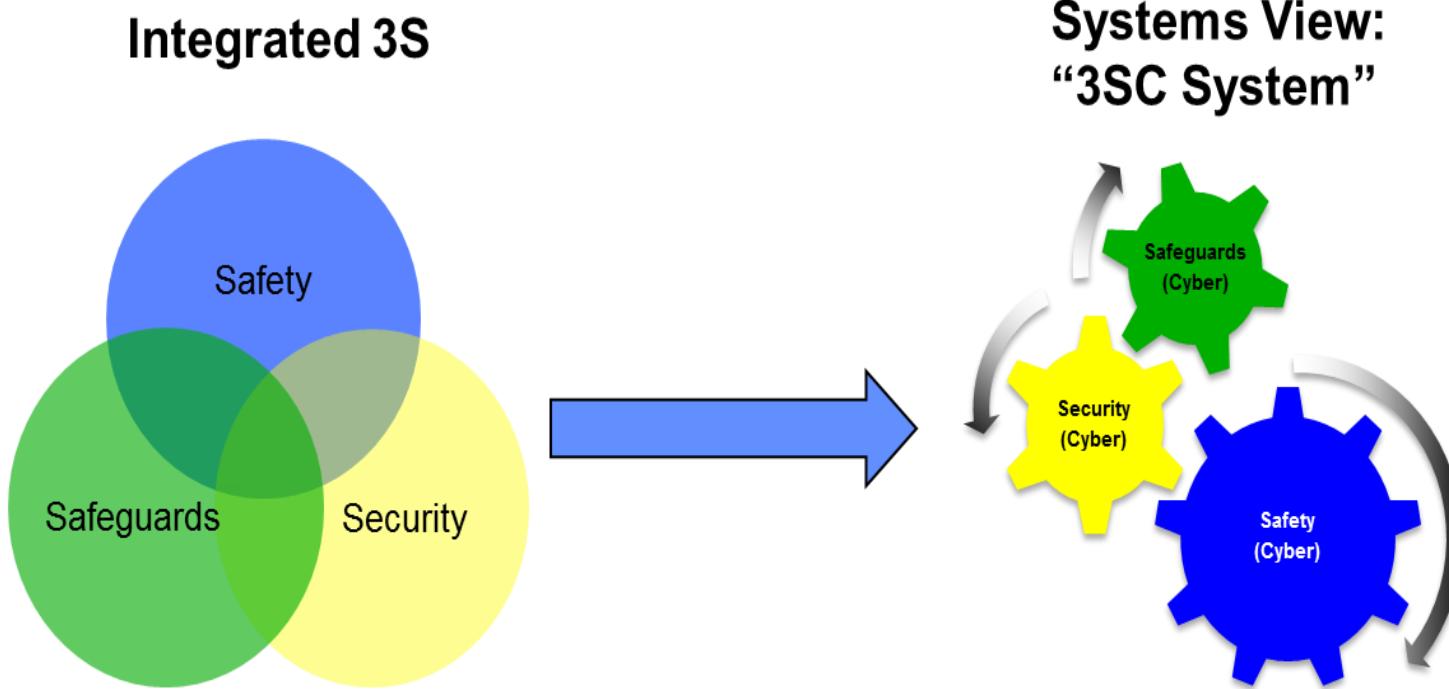
# *State of the Art Severe Accident Technical Analysis Tools*



# Example Offsite Consequences



# Systems View of Nuclear Safety, Security, Safeguards and Cyber Issues



# Conclusions

- Important risks already exist within countries and their reactor designs
- Credible scenarios can lead to core damage and release of fission products
- A systems view highlights the safety, security, safeguards and cyber (3SC) risks that enable
  - Monitoring changes in the risk profiles,
  - Developing strategies and implementing actions, and
  - Making measurable differences in threat space

# ***BACK UP SLIDES***

# Risk Analysis Framework

## Risk Identification

- SME review of civilian nuclear threats
- Nuclear Energy Event Tree Analysis
- Three Scenarios

Development of  
Analytical  
Question

## Risk Prioritization

- Global Nuclear Threat Prioritization plus Nuclear Power Plant (GNTP+NPP) Model
- Non-state actor threat and the vulnerability of NPPs within a country was evaluated

Selection of 3  
countries for in-depth  
analysis

## Risk Assessment

- Identification of potential risks based upon reactor design
- Identification of country factors that can influence the risk

Selection of reactor  
design for mod/sim  
analysis

## Severe Reactor Accident Analysis

- Modeling and simulation of a severe radiological release from a malicious attack on a NPP
- Environmental and human health impacts simulated and evaluated