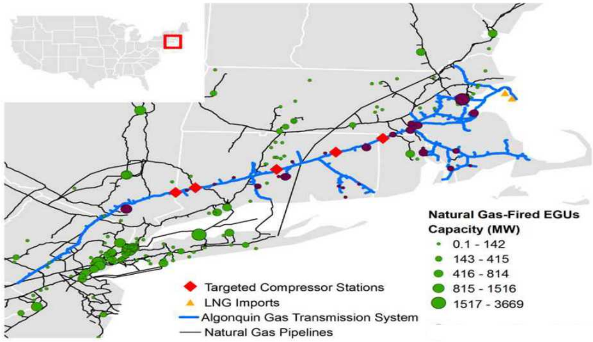
SAND2019-0332C

Sandia National Laboratories
THREAT
EVENT
COMPONENT
SYSTEM
CONSEQUENCES
RECOVERY

Integrated Cyber Physical Impact Analysis (ICPIA)™

Full Spectrum Modeling Framework



2019 Frontiers in Resilience Symposium

Critical Infrastructure Resilience Through Communication, Coordination, and Collaboration

Cyber-Physical Security

Mitch McCrory, Manger, Energy Security Department

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Key takeaways

- Cyber threat is real to our critical infrastructure
- ICPIA is a modeling framework that can help define what needs to be analyzed to answer a cyber and/or physical event
- ICPIA can be entered anywhere in the process dependent on question being asked
- Problem needs to be evaluated through the lifecycle
- There are research opportunities

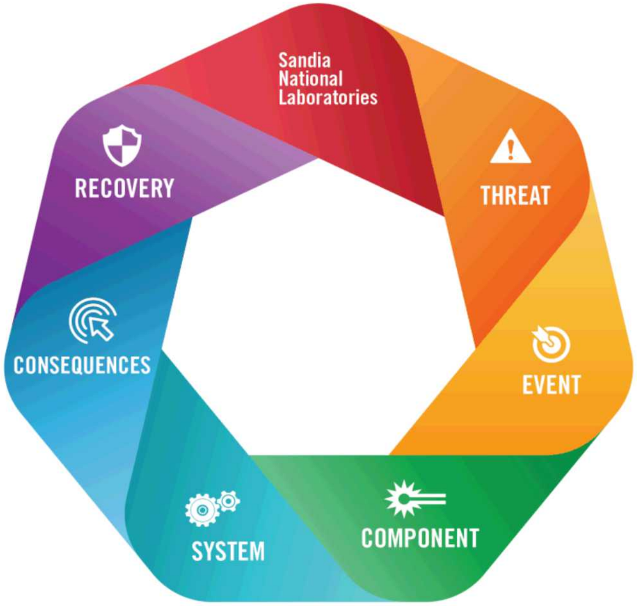
Recent News

- May 9, 2018 - California mandates solar panels on new home construction
- March 15, 2018 – Reuters, "In a first, U.S. blames Russia for cyber attacks on energy grid."
- January 2018 – The Verge, "Hacking Nuclear Systems is the Ultimate Cyber Threat. Are We Prepared?"
- October 2017 – US-CERT, "Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors"
- October 2017 – NTI, "NTI Highlights Growing Cyber Threat to Nuclear Systems in Bulletin of the Atomic Scientists article"
- July 2017 – DHS-FBI, "Hackers Targeted Energy, Manufacturing Facilities"

- December 2015 – Ukraine power grid cyberattack
- November 2015 – Crimea power pylon blown up
- Sept 2015 – Chatham House Report, "Cyber Security at Civil Nuclear Facilities." Identifies multiple issues and recommendations.
- December 2014 – The Guardian, "South Korean nuclear operator hacked amid cyber-attack fears"

Lloyd’s and Cambridge Centre for Risk Studies – Lloyd’s Emerging Risk Report 2015

- Erebos (Greek – deep darkness, shadow) scenario is an attack on the grid serving Washington, DC, and New York City.
- 15 states impacted and 93 million people without power
- Report claims improbable, but technically feasible
- “The scenario predicts a rise in mortality rates as health and safety systems fail; a decline in trade as ports shut down; disruption to water supplies as electric pumps fail and chaos to transport networks as infrastructure collapses. “
- Malware placed and present over several months
- Assumes 50 generators it can control and fail
- Some power recovered in 24 hrs – others over several weeks
- $243 B to US economy and up to $1 T in most extreme case of scenario

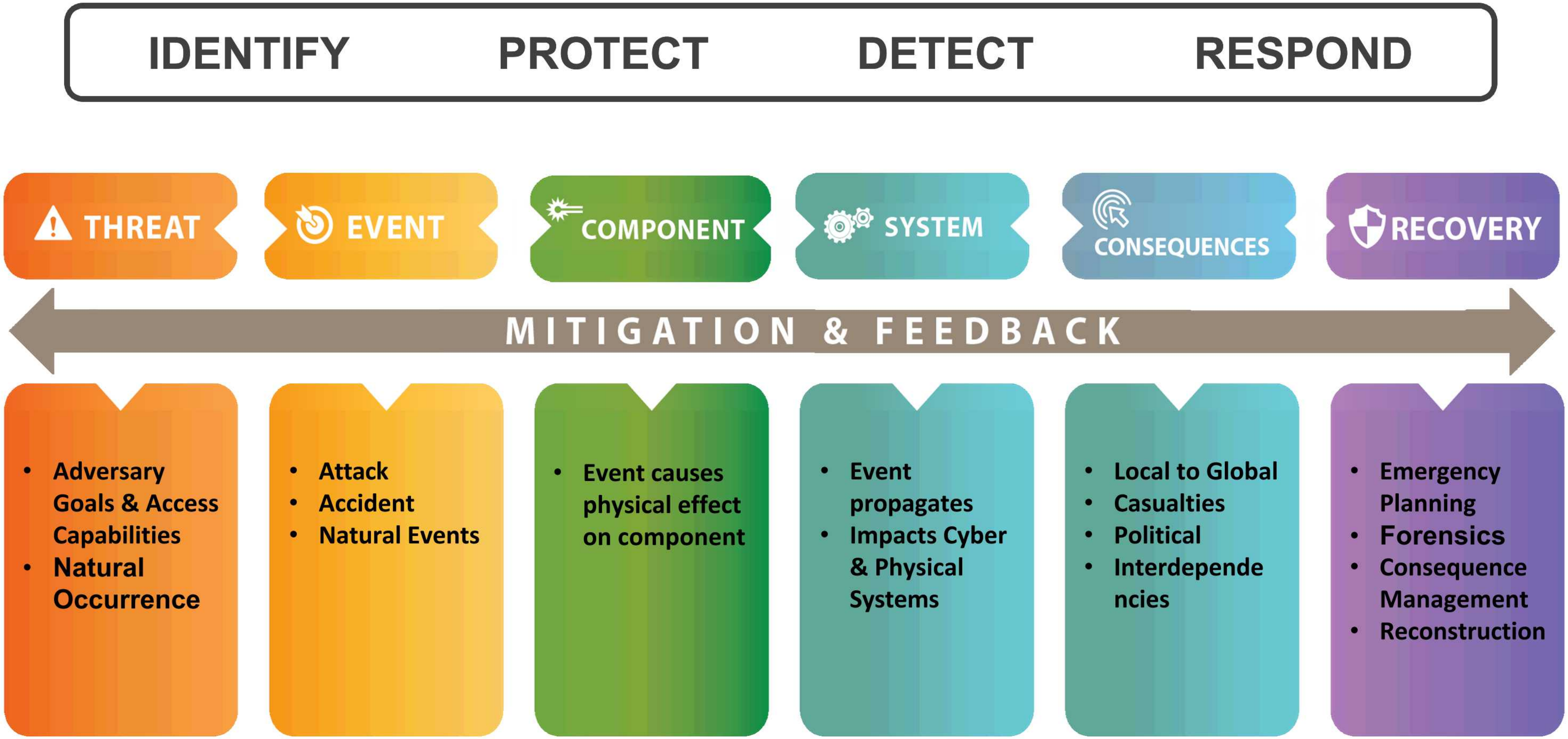


Integrated Cyber Physical Impact Analysis (ICPIA)™

Full Spectrum Modeling Framework

- Sandia integrates an array of modeling and simulation capabilities to manage this risk and secure digital 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



IDENTIFY PROTECT DETECT RESPOND

THREAT

- Adversary Goals & Access Capabilities
- Natural Occurrence

EVENT

- Attack
- Accident
- Natural Events

COMPONENT

- Event causes physical effect on component

SYSTEM

- Event propagates
- Impacts Cyber & Physical Systems

CONSEQUENCES

- Local to Global
- Casualties
- Political
- Interdependencies

RECOVERY

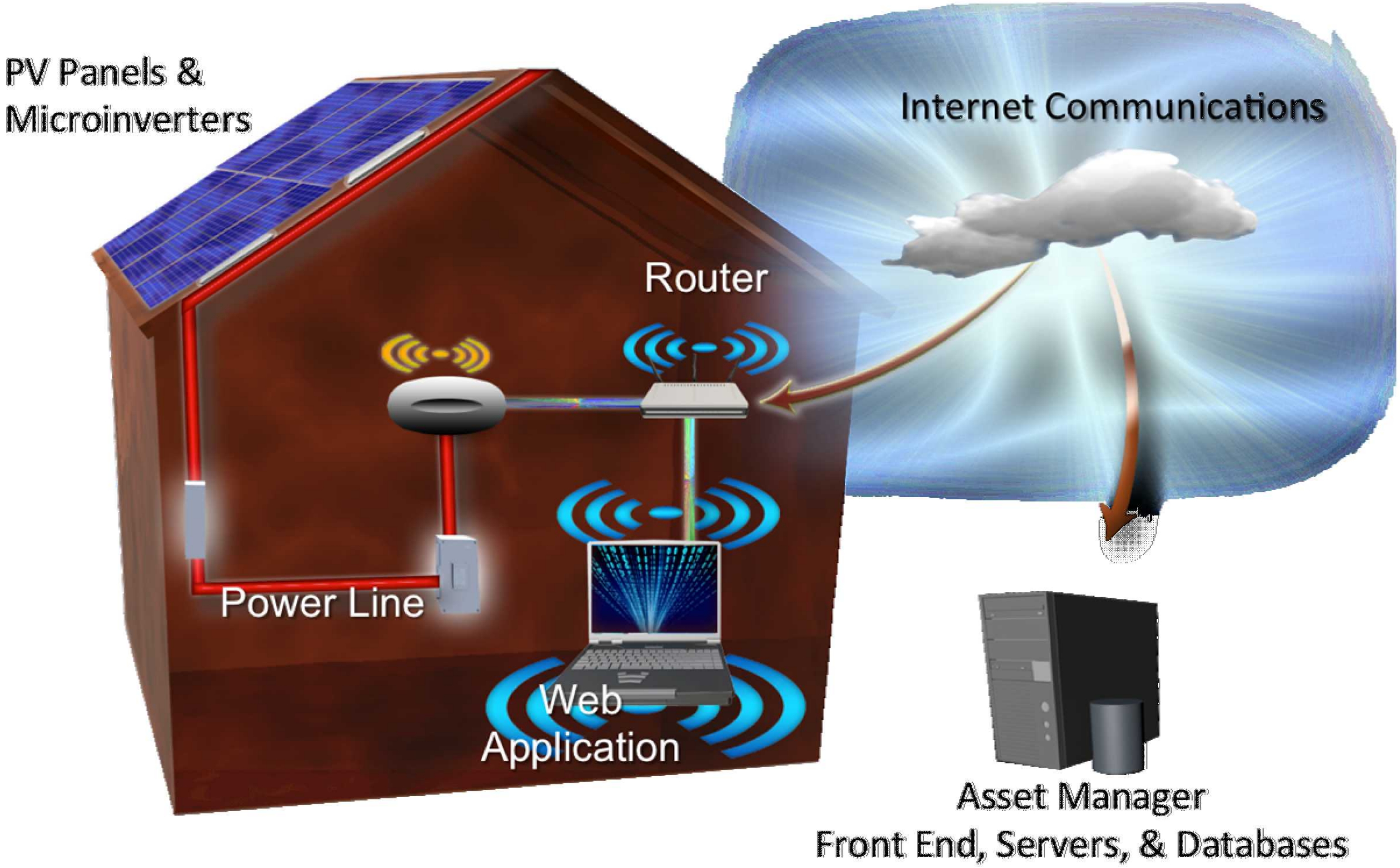
- Emergency Planning
- Forensics
- Consequence Management
- Reconstruction

MITIGATION & FEEDBACK

ICPIA Use Cases

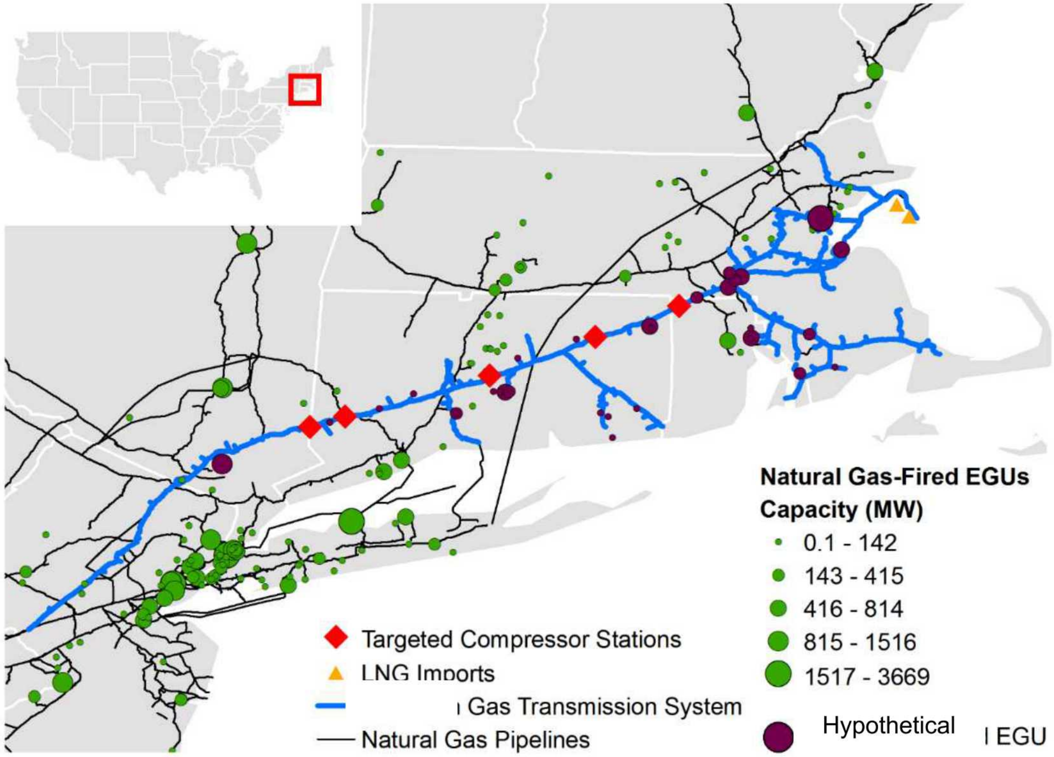
- **Sandia has tools in each modeling domain and the whole is greater than the parts – integrating these tools can:**
  - **Support New Threat Analysis** - Explore the impact of previously unidentified threats and vulnerabilities
  - **Provide test bed for integrating systems** - an Intrusion Detection System (IDS) can be installed and tested in the network emulation
  - **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 cyber attack response procedures
  - **Identify R&D gaps** – for modeling and simulation improvements
  - **Supports integrated risk management** - attack difficulty metrics, impact and consequence analysis, moving to "all hazards" analysis

Hypothetical Attack on PV



Hypothetical Impact to Limited Cyber Attack on Pipeline

A Northeast Gas Transmission pipeline transports ~3 Bcfd of natural gas for delivery to Northeast (of 16 Bcfd total regional inflow capacity)1



Hypothetical Feeds:

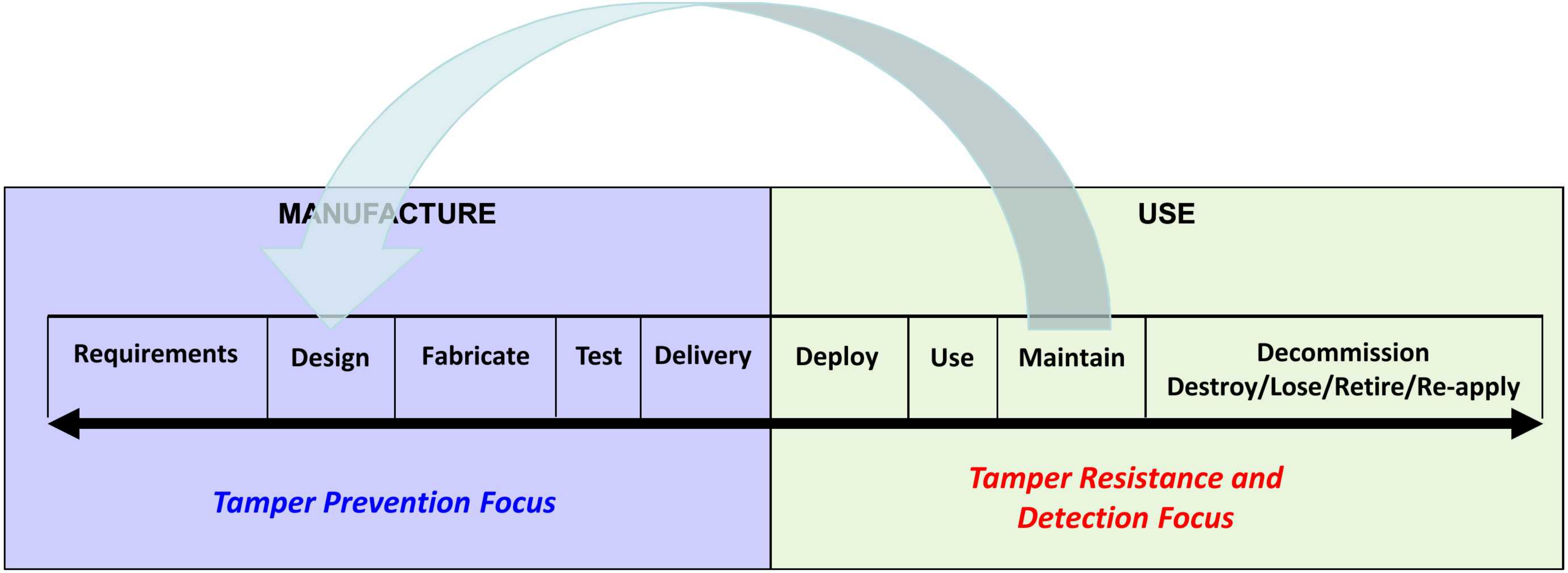
5-9 GW of generation capacity (almost 20 utility-scale facilities). There are 18.6 GW of natural gas-fired power in the Northeast[2]

Scenario

Six compressor stations are targeted due to a hypothetical common vulnerability in the operator’s SCADA system

1. http://www.eia.gov/naturalgas/data.cfm, accessed September 15, 2016
2. Eastern Interconnection Planning Collaborative, Phase 2 Report, July 2, 2015, Table 8-4, http://nebula.wsimg.com/a8424953a8514dd9968b81b16802f900?AccessKeyId=E28DFA42F06A3AC21303&disposition=0&alloworigin=1, accessed September 15, 2016

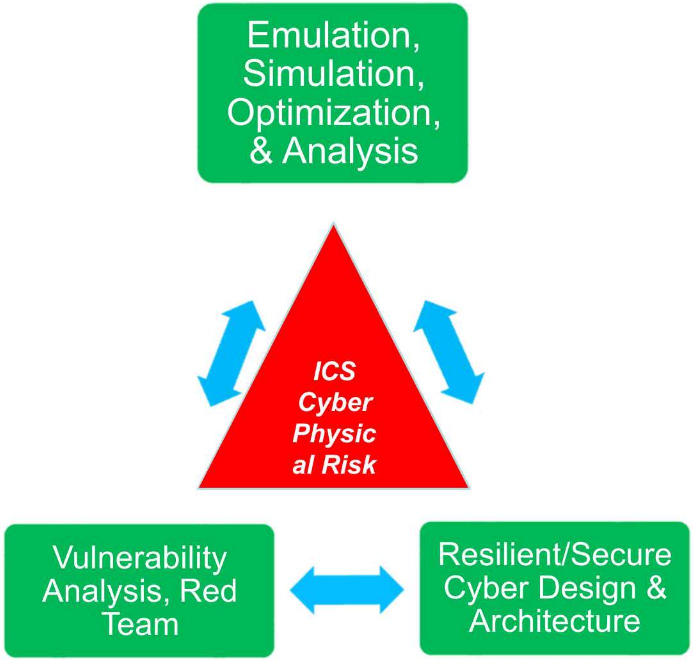
Lifecycle process



Cyber related attack vectors are very different at various stages of a systems lifecycle and should be evaluated for each stage and mitigated per company policy

R&D Opportunities

- Secure Architectures
  - Very broad set of topics
  - Test bed development
- Modeling and Simulation
  - Optimization
  - Threat to consequence an recovery
  - Embedded system modeling
  - Economic
  - Other
- Risk Tools
  - Manage security controls
    - Cyber, physical, environmental, other
  - Tools to help decision makers to make best decisions



Emulation, Simulation, Optimization, & Analysis

ICS Cyber Physic al Risk

Vulnerability Analysis, Red Team

Resilient/Secure Cyber Design & Architecture

Contact Information

- **Mitch McCrory**, Department Manger, Energy Security Department
  - Phone: (505) 845-3031 / Email: fmmccro@sandia.gov