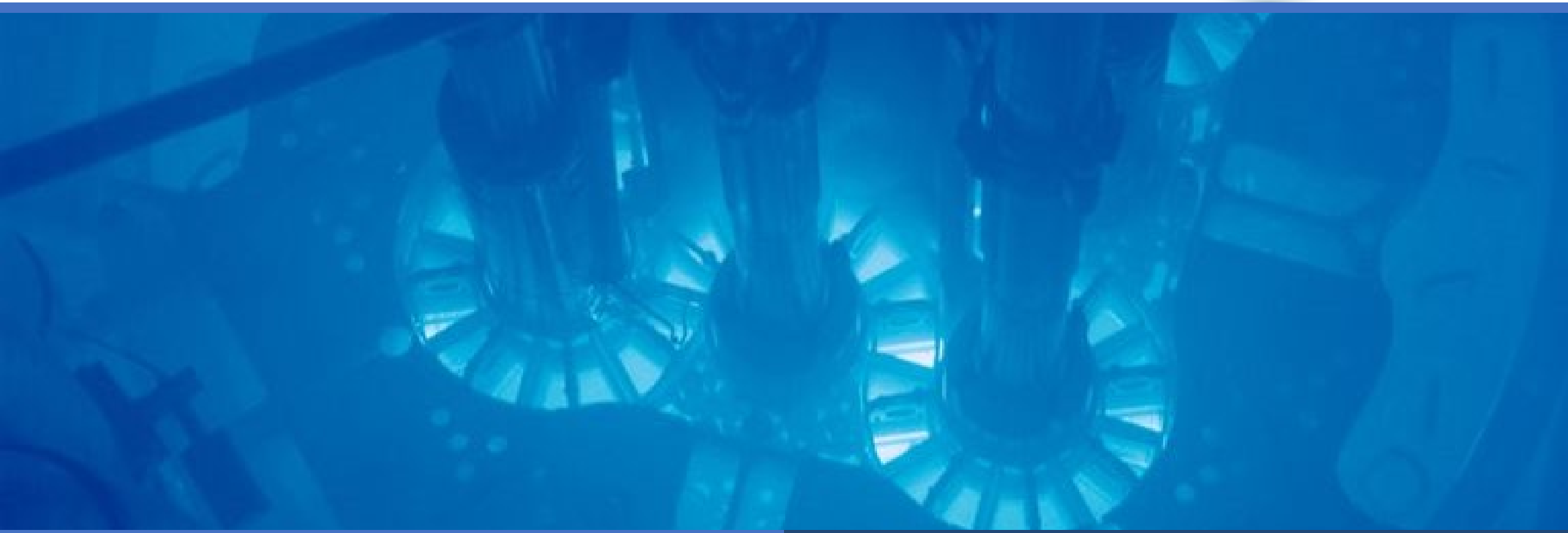
U.S. DEPARTMENT OF ENERGY | Office of NUCLEAR ENERGY

Clean. Reliable. Nuclear.



DOE-NE Cybersecurity R&D

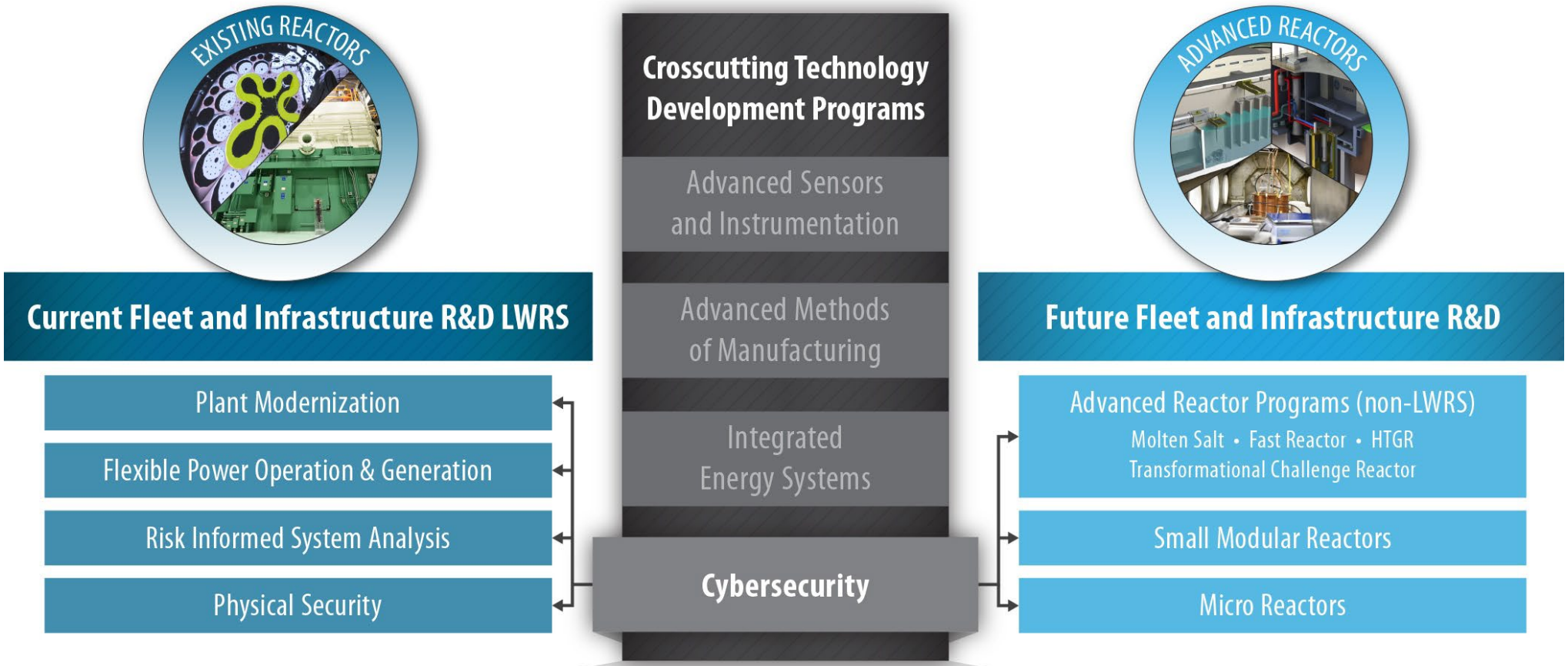
June 2022

Katya Le Blanc, Deputy-NTD
Lon Dawson, NTD

Objectives

- Introduce the program
- Discuss opportunities to coordinate
  - What are the technical and regulatory risks associated with cybersecurity?
  - Are there any concepts, use cases, or applications with cybersecurity concerns?

Connections to other R&D programs, NRC, Industry



Program Goals and Objectives

- The focus of the NE cyber program is to facilitate the future nuclear fleet along with their associated applications and novel use cases by addressing cybersecurity risks. Outcomes include:
  - Techniques to identify and mitigate cybersecurity hazards during design, reducing costs and regulatory challenges
  - Technical basis for documenting cyber risk in a way that can be credited during licensing
  - Support for longer-term, post-deployment use cases that are currently cybersecurity-limited, like autonomous or remote control and wireless applications
  - Technical tools, such as control system design requirements, supply chain protection methods and test beds

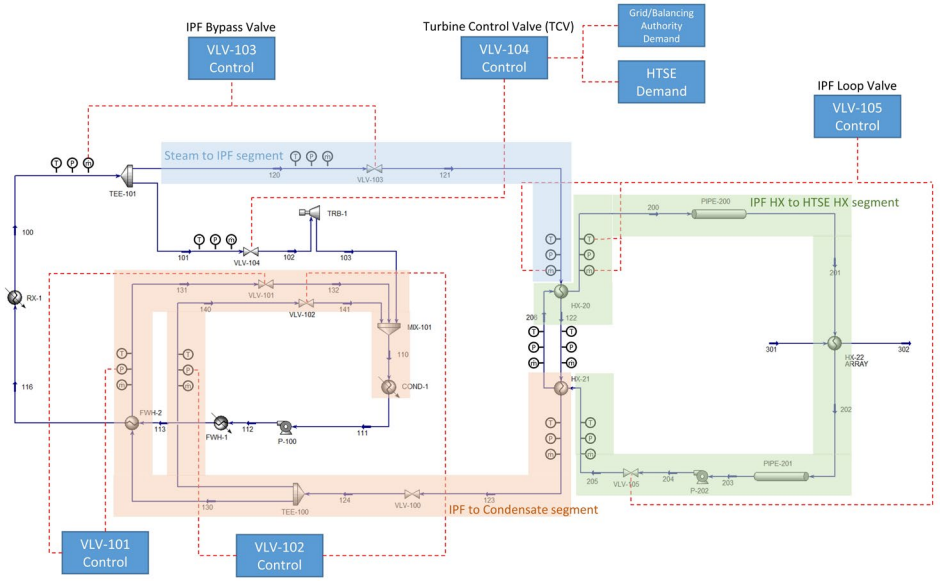
https://www.flickr.com/photos/thirdwaythinktank/37875478862/in/album-72157665372889289/

How can we help?

- Are there cyber security research needs you have already identified?
- Are there *unique* safety or operational considerations for your technologies or applications?
  - Monitoring and control requirements?
  - (Passive) Safety considerations?
  - Plans or needs for wireless communications?
  - Plans or needs for digital twins?
- Any *unique* use cases or applications for technologies (e.g., load following, microgrid, process heat, district heat, distributed energy)?
  - Interfaces from the reactor to external systems?
  - Reactor control signals?
- Important relationships with or plans for control system providers?

Previous Work

- Development and testing of risk analysis tools to support characterization of cyber security risk to nuclear facilities for digital upgrades and new applications
- Cyber security evaluation of the conceptual design for a hydrogen production facility coupled with an existing nuclear power reactor
- Characterization of supply chain attack surface for nuclear facilities
- Development of modeling and simulation test beds to support cyber security research



Current work

- Development of methodology to evaluate the use of wireless communications in safety-related and important-to-safety (SRITS) functions.
- Cyber security review of advanced control system technologies
- Development of subversion tactics against an instantiated Digital Twin and integrated control system loop
- Research into technology and processes that establish roots of trust and leverage these roots of trust to maintain trust throughout the software supply chain
- Development of nuclear-specific cyber informed engineering guidance to address technical and regulatory challenges in all phases of the engineering lifecycle
- Development of ransomware-resistant architectures
- Development of guidance for the existing fleet to develop and maintain a comprehensive software bill of materials to support enhanced vulnerability management

Future Work

- Future research will address the challenges of applications that are likely to be deployed in the future fleet, but may be considered for the existing fleet such as:
  - Digital twins
  - Autonomous operations
  - Remote monitoring
  - Control system design requirements for novel applications

Questions and Discussion

- Thank you!
- Katya Le Blanc, katya.leblanc@inl.gov
- Lon Dawson, ladawso@sandia.gov