INL/CON-24-81104-Revision-0

Risk Analysis for Remote Operation of Microreactors

October 2024

Megan Jordan Culler, Joe E. Oncken, Thomas A Ulrich, Kaeley Stevens

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/CON-24-81104-Revision-0

Risk Analysis for Remote Operation of Microreactors

Megan Jordan Culler, Joe E. Oncken, Thomas A Ulrich, Kaeley Stevens

October 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Pacific Basin Nuclear Conference

PBNC 2024

Risk Analysis for Remote Operation of Microreactors

Megan Culler

Power Engineer

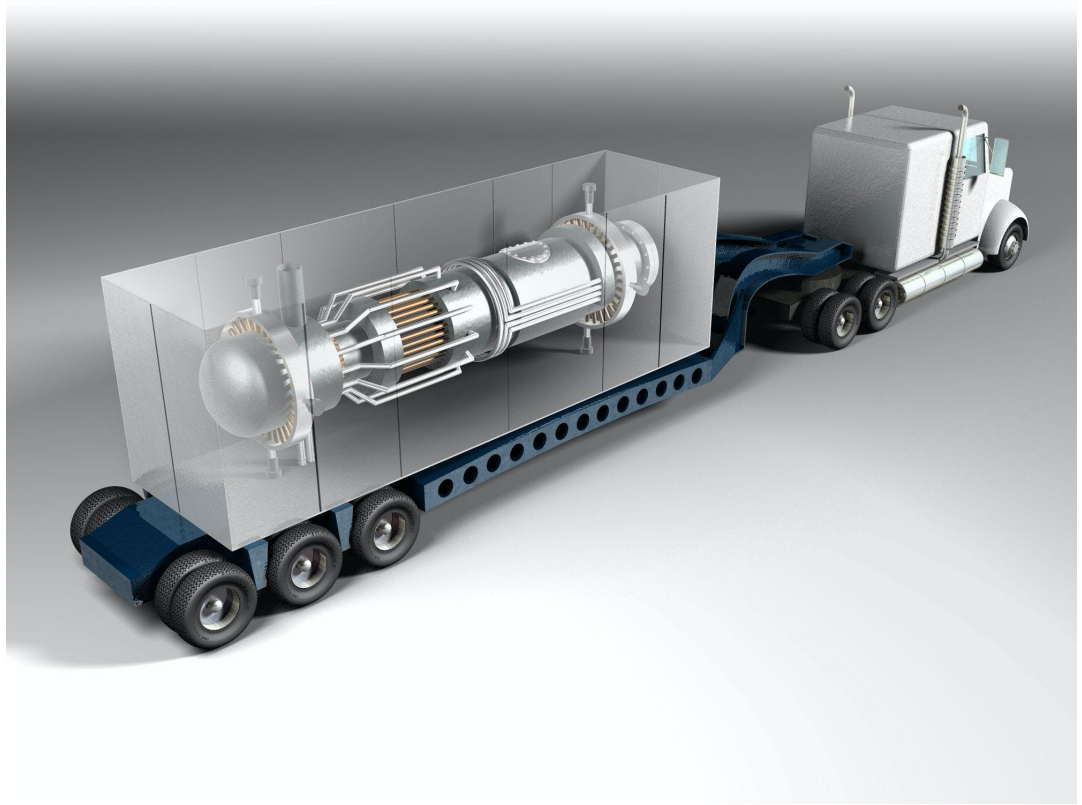
Idaho National Laboratory

ANS American Nuclear Society

INL/CON-24-81104

Microreactor Applications

- Off-grid
- Remote or islanded areas
- Industrial applications (e.g. mining)
- Opportunities to replace diesel fuel
- Stability to add to high-penetration renewable systems



Idaho National Laboratory

ANS

Remote Concept of Operations

Remote Concept of Operations

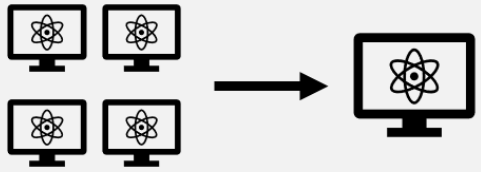
- Remote monitoring and operation is key for the future of nuclear power
- Identify characteristics of a remote concept of operations
- Identify types of technologies, methods, and regulations serve as a precedence for remote operations
- Examine how digital twins can support remote operations to provide operational security and assurance

Idaho National Laboratory

ANS

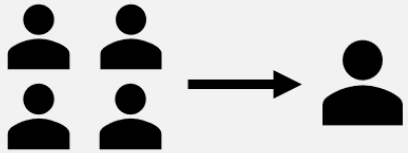
Why is remote operation and monitoring crucial to microreactor technology adoption?

Control Room Centralization



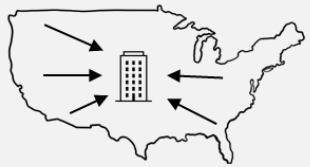
Many individual, small, onsite control rooms can be replaced by a centralized, offsite control and monitoring center.

Reactor Operator Regulations



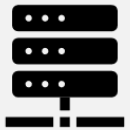
Economies of scale can significantly reduce staffing requirements across a large system of many centrally-operated reactors.

Strategic Siting



The central control room can be sited in an area with low construction costs, a strong labor pipeline, and other amenable qualities: reducing both capital and operational expenditures.

Semi-Autonomous Control



The combination of remote operation and semi-autonomous or autonomous control can allow for significant cost reductions.

Microreactor Adoption

The combined economic benefits of remote operation increases microreactor competitiveness against alternatives – allowing for greater adoption.

As microreactor deployment increases, per unit cost of the operations infrastructure is reduced.

Fleetwide remote operations capability need to be considered early in development in order to take advantage of potential cost savings.

Site where you *need it*

Operate from where its most *economical*

Idaho National Laboratory

ANS

NRC Key Findings

Key findings from Ground Rules for Regulatory Feasibility of Remote Operations of Nuclear Power Plants

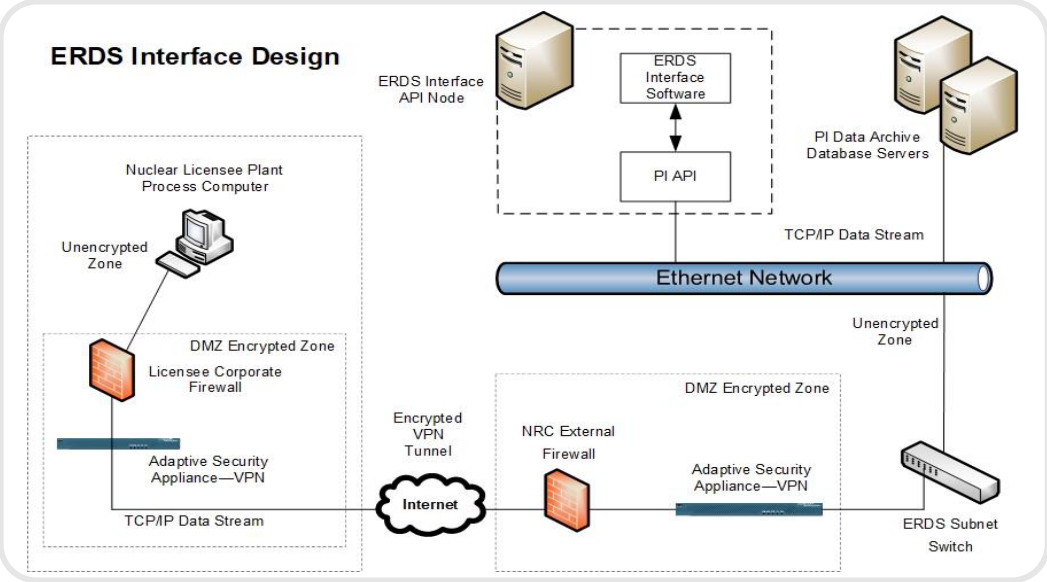
1. Remote operations criteria should be part of the **design and development process from the beginning.**
2. The **public's risk perception** must be addressed by appropriately conveying societal impacts and **accurate safety precautions** that ensure public safety.
3. Changes to regulations are expected and must be addressed as needed (**Part 53** will address some aspects, but others **may require additional or altered regulations**).
4. Guidance on acceptable approaches to meet regulations shall use **technology-neutral** and **performance-based** acceptance criteria.
5. "Minimal risk conditions" representing safe plant conditions following a credible initiating event must be identified with **safe and stable shutdown** being the predominately expected outcome.

NRC Key Findings continued

6. Data and voice **communication infrastructure and security are critical** for remote operations and should be central during the design and development process.
7. Remote operator responsibilities should be based **on automation levels** and “minimal risk conditions” human intervention and time requirements.
8. Operator licensing will be necessary, but due to high levels of automation and inherent safety functions the **level of training and licensing oversight is expected to be reduced**.
9. A **local crew** based onsite or nearby to sever emergency quick response functions has been deemed **unavoidable**.
10. **Physical and cybersecurity inspections are necessary** for both the site and control room facilities, with anticipated possible shifts towards remote inspection capabilities.
11. **Physical security will be required** at both the site and remote control room facilities.

Existing nuclear precedence for remote operation concepts

- Emergency Response Data System (ERDS) is one US nuclear specific precedence for **monitoring**
  - Direct real-time transfer of data from licensee plant computers to the Nuclear Regulatory Commission (NRC) Operations Center
    - **Does not afford control**
    - Intended to support emergency response planning and reporting



NUREG-1394, Revision 2

Idaho National Laboratory

ANS

Non-Nuclear precedence for remote operations and monitoring of nuclear reactors

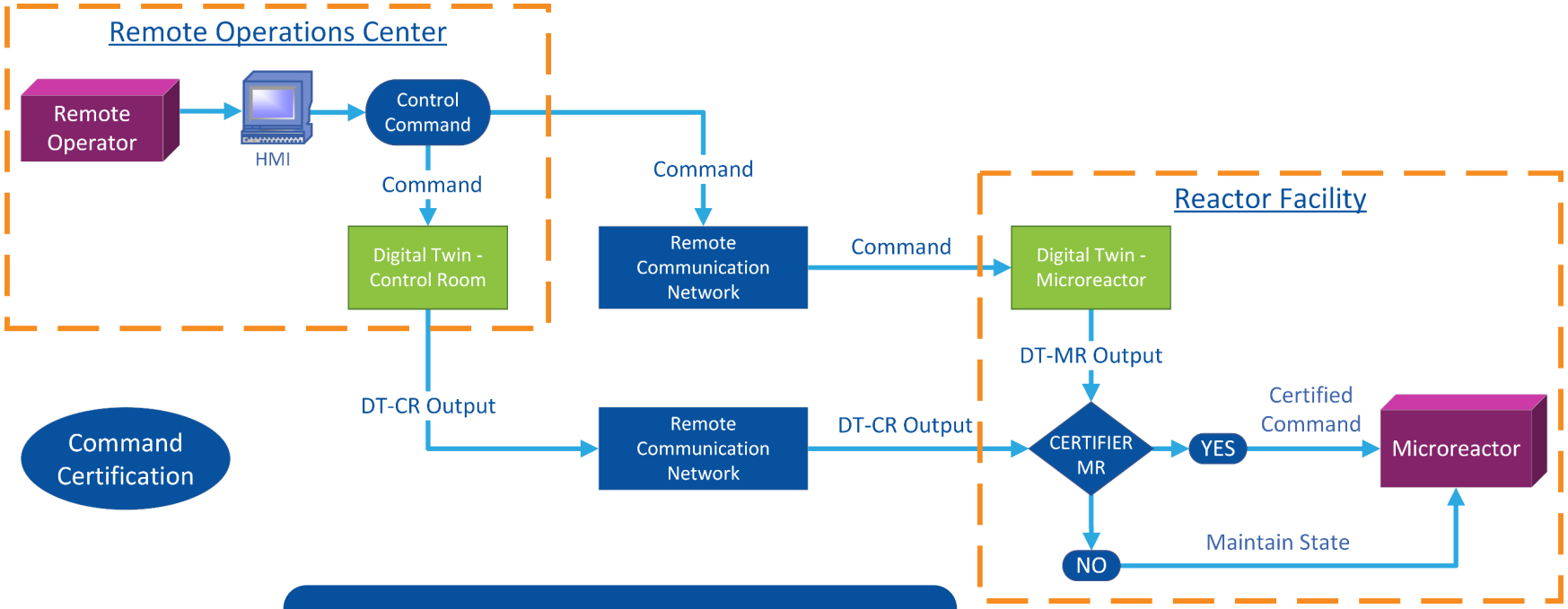
Numerous analogous industries demonstrate geographically distributed control systems methods and technologies

- Electric grid (existing methods, smart grid communication, advanced modelling)
- Distributed Energy Resources (DER)
- Oil and gas
- Aerospace
- Military unmanned vehicles (aerial and land based)

- Nuclear is unique with high stakes
  - Radioactive material release considerations
  - Negative public perception from event a slightly faulty rollout could halt progress indefinitely

Digital Twin Certification System

Operator issues commands that are certified by ***two digital twins*** before the I&C system actuates any controllers on the reactor systems



DT-CR Digital Twin Control Room
DT-MR Digital Twin Microreactor

Idaho National Laboratory

ANS

Cyber-Informed Engineering

	PRINCIPLE	KEY QUESTION
1	**Consequence-Focused Design**	How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?
2	**Engineered Controls**	How do I select and implement controls to reduce avenues for attack or the damage that could result?
3	**Secure Information Architecture**	How do I prevent undesired manipulation of important data?
4	**Design Simplification**	How do I determine what features of my system are not absolutely necessary to achieve the critical functions?
5	**Layered Defenses**	How do I create the best compilation of system defenses?
6	**Active Defense**	How do I proactively prepare to defend my system from any threat?

	PRINCIPLE	KEY QUESTION
7	**Interdependency Evaluation**	How do I understand where my system can impact others or be impacted by others?
8	**Digital Asset Awareness**	How do I understand where digital assets are used, what functions they are capable of, and our assumptions about how they work?
9	**Cyber-Secure Supply Chain Controls**	How do I ensure my providers deliver the security the system needs?
10	**Planned Resilience**	How do I turn "what ifs" into "even ifs"?
11	**Engineering Information Control**	How do I manage knowledge about my system? How do I keep it out of the wrong hands?
12	**Organizational Culture**	How do I ensure that everyone's behavior and decisions align with our security goals?

Idaho National Laboratory

Wright, Virginia L., and Lampe, Benjamin Ruhlig. 2024. "Cyber-Informed Engineering Workbook: CIE Hands-On Training". United States. https://doi.org/10.2172/2371031. https://www.osti.gov/servlets/purl/2371031.

ANS

Risk Assessment

- Subjective scoring intended for use in comparative analysis
- Vetted by independent SMEs
- Large buckets to encompass scores avoid the need for high level of specificity

Score	*Likelihood Interpretation*	*Consequence Interpretation*
1	Unlikely to happen ever, but still a possibility	Needs attention, no immediate impact on process control of safety
2	Likely to happen at least once over 10 years of operation	Needs rapid attention, delayed impact to process control or monitoring
3	Likely to happen at least once over 5 years of operation	Requires immediate attention, impacts to remote monitoring and control
4	Likely to happen at least once over 2 years of operation	Remote immediate attention, potential impacts to process functionality
5	Likely to happen at least once within a year	Requires immediate on-site intervention, potential for physical damage or safety impacts

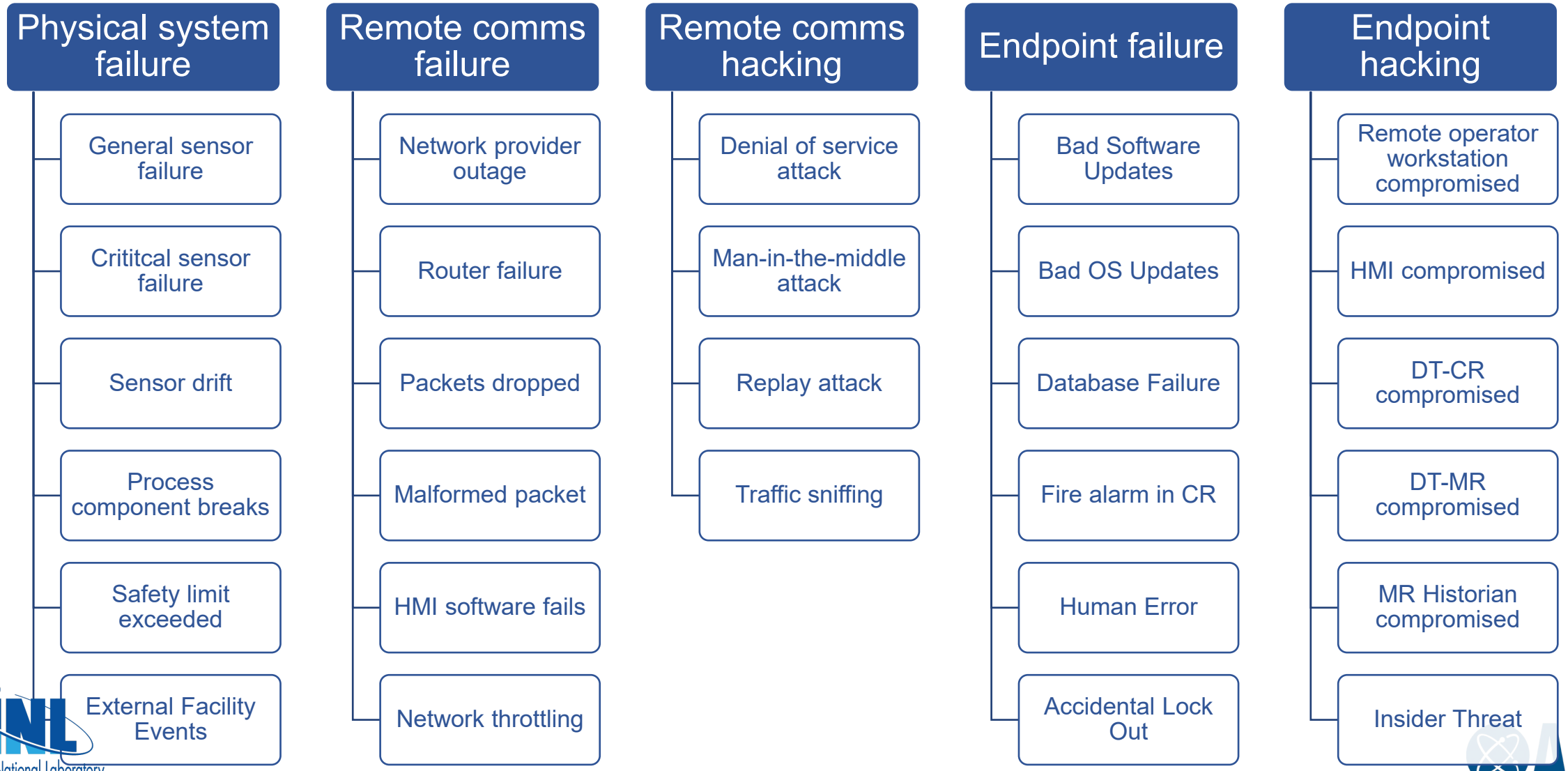
Risk Categories

- Physical system failure (controller and microreactor)
- Remote communications failure
- Remote communications hacking
- Endpoint hacking
- Endpoint failures

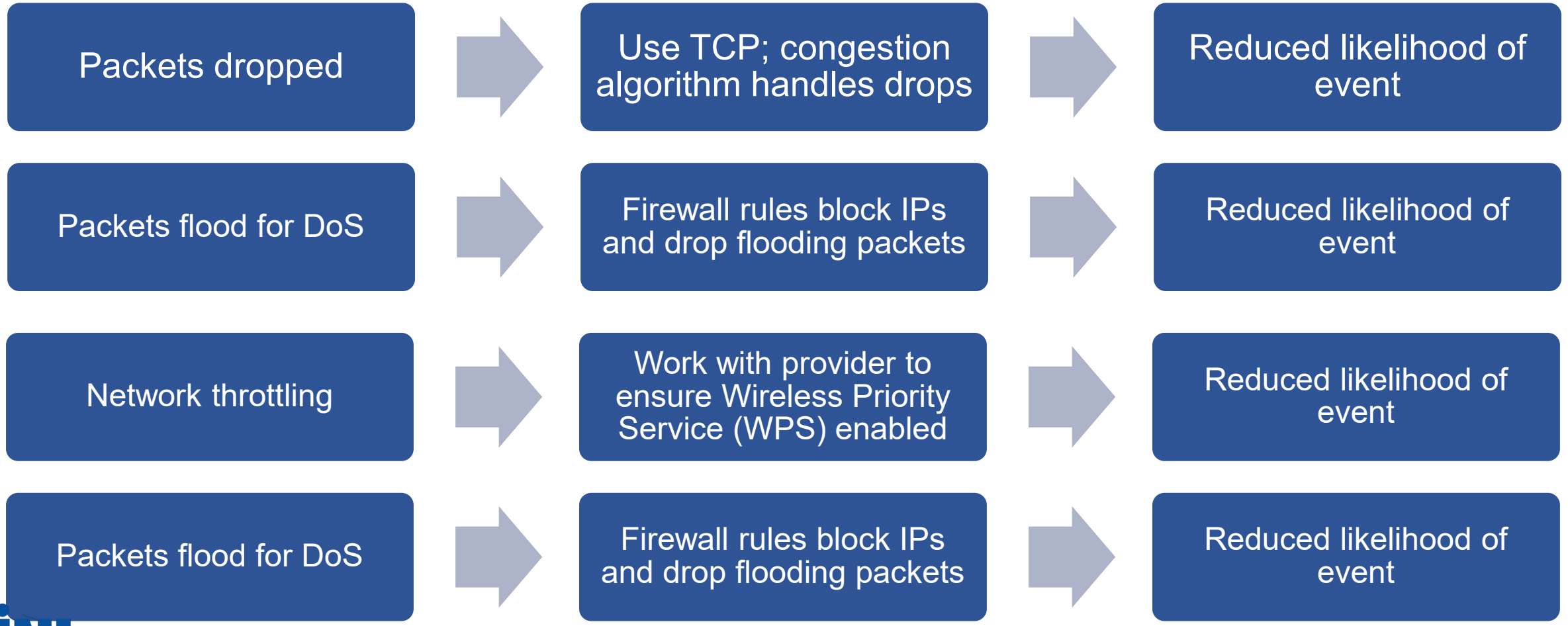




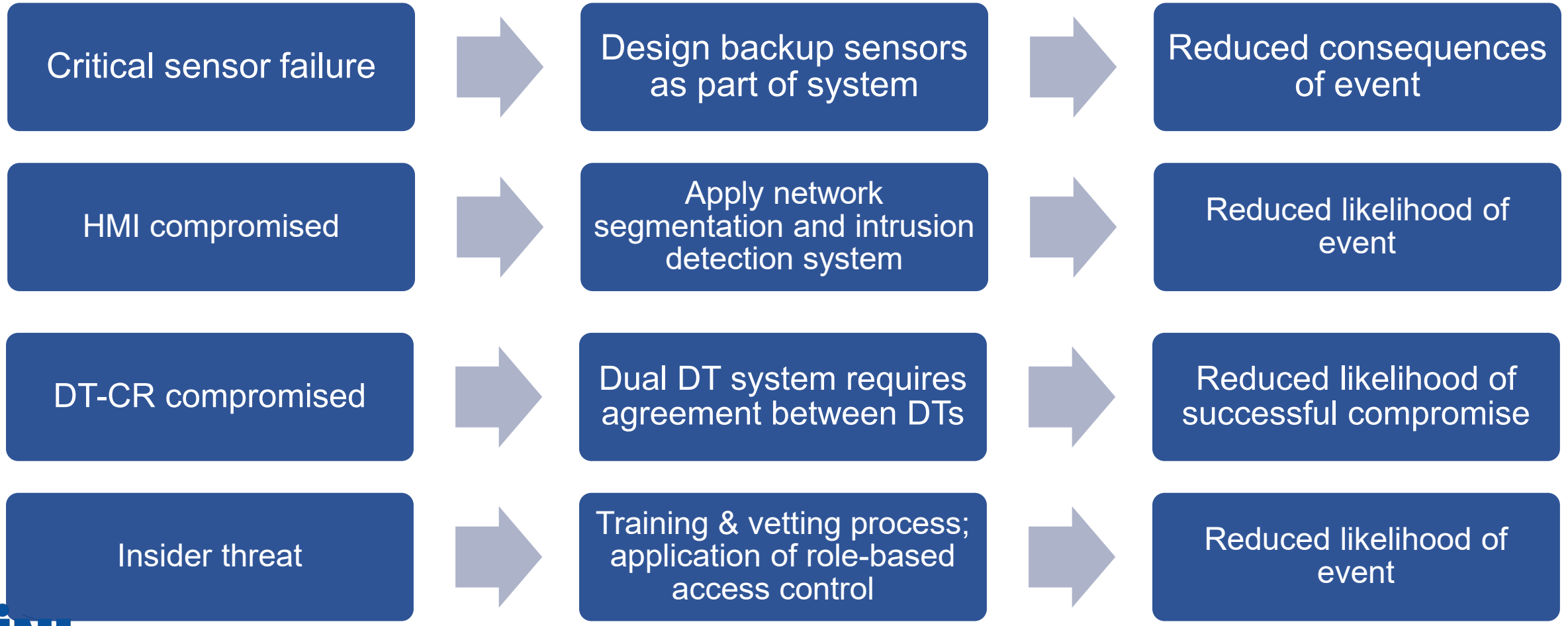
Examples of Risks Considered



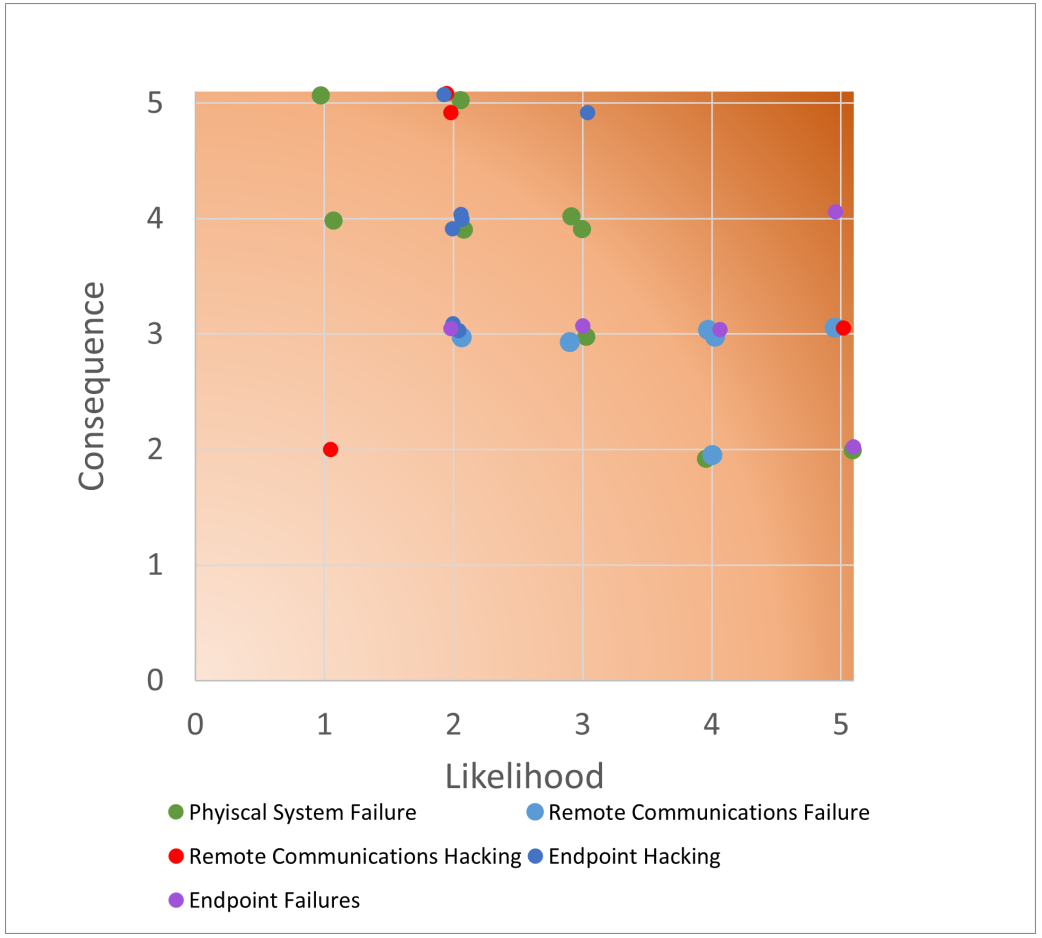
Examples


Packets dropped
Use TCP; congestion algorithm handles drops
Reduced likelihood of event
Packets flood for DoS
Firewall rules block IPs and drop flooding packets
Reduced likelihood of event
Network throttling
Work with provider to ensure Wireless Priority Service (WPS) enabled
Reduced likelihood of event
Packets flood for DoS
Firewall rules block IPs and drop flooding packets
Reduced likelihood of event

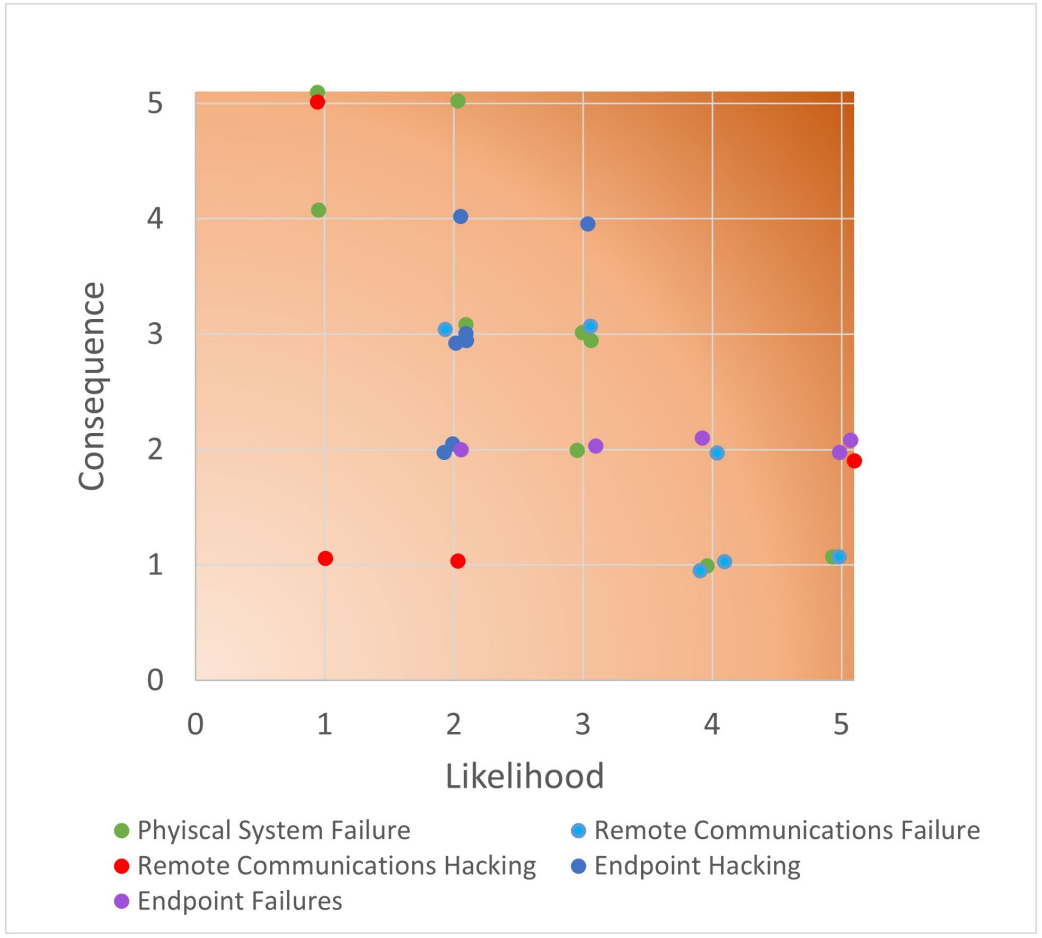
Examples


Critical sensor failure
Design backup sensors as part of system
Reduced consequences of event
HMI compromised
Apply network segmentation and intrusion detection system
Reduced likelihood of event
DT-CR compromised
Dual DT system requires agreement between DTs
Reduced likelihood of successful compromise
Insider threat
Training & vetting process; application of role-based access control
Reduced likelihood of event

Application of Risk Assessment to Risk Categories



Preliminary risk assessment



Mitigated risk assessment

Idaho National Laboratory

ANS

Conclusions

- Cyber-Informed Engineering (CIE) should be applied from the design phase onwards
- Risk classification must precede risk mitigation
- Many mitigations are standard best-practices, which doesn't make them less effective
- All-hazards approach builds in cyber-physical resilience

Questions?

Megan Culler

megan.culler@inl.gov

Idaho National Laboratory