INL/CON-24-82232-Revision-0

Architecture Design for Remote Operation of Microreactors: Poster

December 2024

Changing the World's Energy Future

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

INL/CON-24-82232-Revision-0

Architecture Design for Remote Operation of Microreactors: Poster

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

December 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

Architecture Design for Remote Operation of Microreactors

Megan Culler, Dr. Joseph Oncken, Dr. Kaeley Stevens, & Dr. Thomas Ulrich

INTRODUCTION

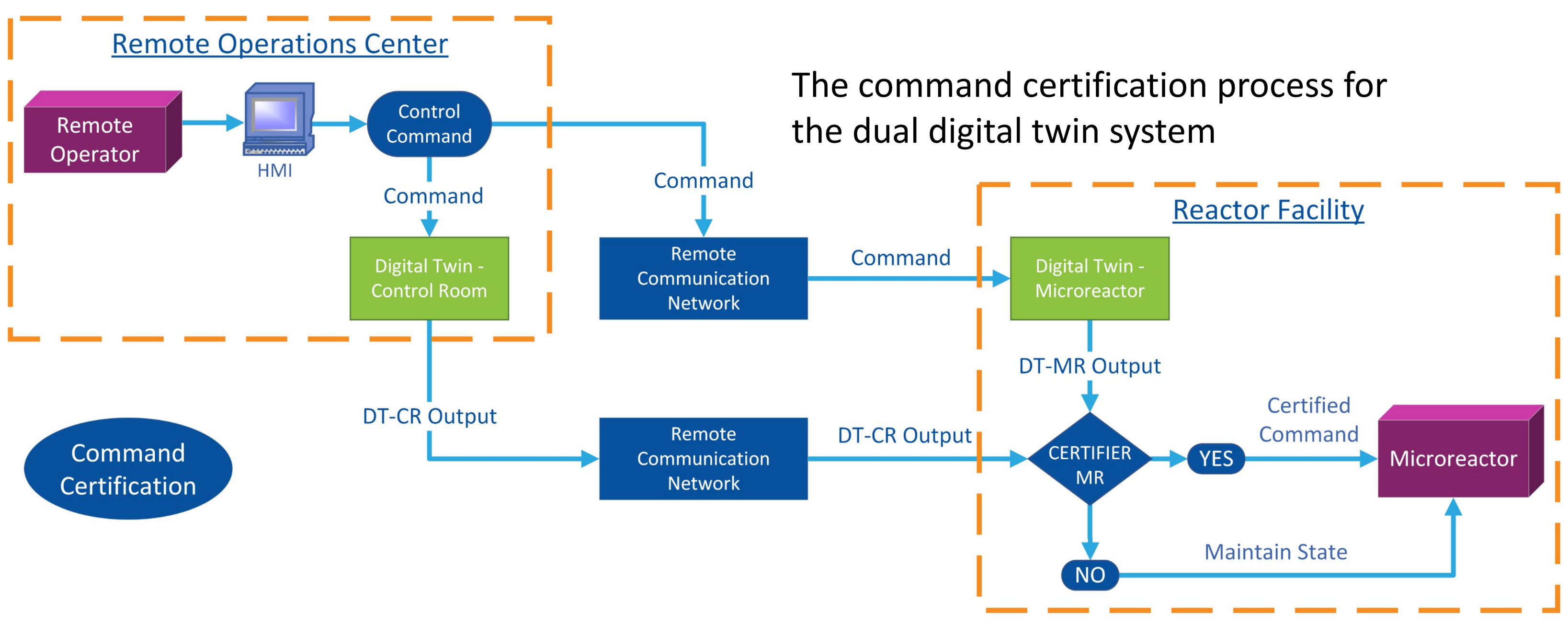
- Microreactors are well suited for remote applications, rural communities, and other islanded loads
- Microreactors will require remote monitoring and operability to be economically feasible.
- Remote operation of critical infrastructure is not a new concept but represents a shift of paradigm in the nuclear industry.
- Potential consequences of nuclear failure to local infrastructure, community, and industry at large create significant perceived risk that requires careful consideration of cyber-resilience for remote operation.

DIGITAL TWIN CERTIFICATION SYSTEM

- Dual digital twin system proposed for cyber-physical resilient implementation of a remote operations paradigm.
- Need a concrete system and functions in place to design supporting architecture.
- Digital twins must agree on expected future state and safety of a command before it is implemented.
- Digital twins must agree on state estimation given current sensor readings before displaying to operator.
- Difficult for adversary to intercept one digital twins' prediction and the raw command/measurements and edit both to look realistic.

NRC Ground Rules for Remote Operation:

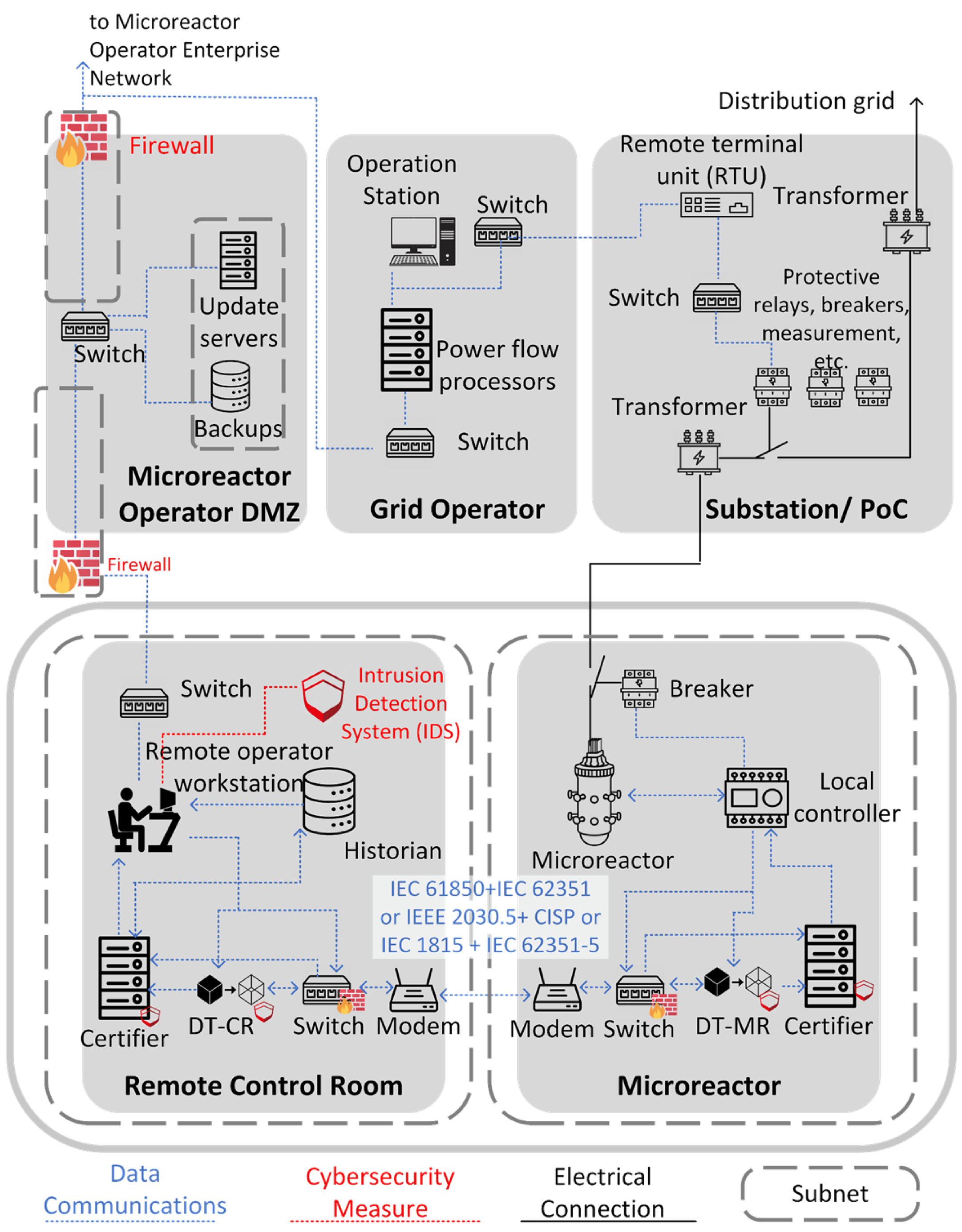
1. Part of design & development from beginning.
2. Engage with pubic to get buy-in and consider societal risk perception.
3. Changes for regulations will be considered based on 1) how well existing regulation accommodates remote ops and 2) how existing regulations address safety and security issues.
4. Guidance should be technology-neutral and performance-based.
5. Concept of "minimal risk conditions" is essential.
6. Data and voice communication infrastructure and security, including cybersecurity, are crucial.
7. Responsibilities of remote operator should be based on level of automation, risk acceptance, and time constraints.
8. Licensing and training of operators in the remote CR will be necessary.
9. On-site or nearby crew unavoidable for planned and emergency operations.
10. Inspections, including cyber and physical security, will be necessary.
11. Physical security of site and remote CR is necessary.



The command certification process for the dual digital twin system

ARCHITECTUAL REFERENCE DESIGN

- Reference architecture is indented to specify devices and network connections required for a remote operations paradigm based on the digital twin certification system.
- Does not address all operational requirements needed to maintain security.
- DMZ will act as a gateway to microreactor operator enterprise network.
- No communications link between microreactor and connected substation (if applicable – could be replaced by DERMS in off-grid application).
- Suitable application protocols are called out, but others work provided they have encryption, authentication, and can support testing and certification.
- Network segmentation is used to provide isolation and limit device integrations to intended pathways.



The proposed reference architecture considers the functional security, and communications requirements and proposes a layout prioritizing cyber-resilience. It proposes a network segmentation and required hardware to meet the functional and security requirements to present proof-of-concept for remote operation of microreactors.

KEY TAKEAWAYS

- Feasible architecture for remote operations of microreactors does not require deviation from state-of-the-art best practices but should be carefully implemented to mitigate risks perceived with this shift-in-paradigm for the nuclear industry.

FUNCTIONAL REQUIREMENTS

INFRASTRUCTURE REQUIREMENTS

Identifying the endpoints in the system.

- Digital twins: high computing power, help create redundancy
- Certifier systems: low computing power, may be a separate process on a shared machine.
- Operator workstation: human-machine interface for remote operator.
- Historian: Can be used to check alignment of current state with previous states of the system
- Local microreactor controller: Implements controls on the microreactor.

COMMUNICATION REQUIREMENTS

- Control center communications: local network at control center, likely wired
- Control center –to- microreactor: two-way communications for controls and measurements over geographic distance, likely wireless.
- Microreactor communications: local network at microreactor, likely wired.
- Latency requirements: Wireless Priority Service to help during congestion.
- Event based vs. state based: state-based recommended for nuclear ops.

SECURITY REQUIREMENTS

SECURING COMMUNICATIONS

- Use standard implementations of encryption for all traffic
- Authentication used to verify sender and limit to intended receiver
- Multifactor authentication (MFA) helps prevent adversary impersonation

ACCESS CONTROL

- Strong passwords, MFA, and role-based access control guided by principle of least privilege helps prevent adversary pivoting if an endpoint is compromised.

LOGGING & MONITORING

- Robust host-based and network logging, stored securely with regular backups

SEGMENTATION

- Private subnets, managed switches and firewalls applying whitelist policies

COMMMUNICATIONS

COMMUNICATION DESIGN

- Physical and Data Link Layers: remote and deployable microreactors will require last-mile wireless connectivity with good range, likely leading to use of satellite or cellular services.
- Network Layer: Can add encryption and authentication at this later. Private networks recommended. Handles dynamic rerouting for comms resilience.
- Transport Layer: TCP likely used for end-to-end communications. Provides network resilience and integrity checks on data. Can handle authentication and encryption.
- Application Layer: many standardized protocols can handle data requirements

www.inl.gov

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy

Idaho National Laboratory