INL/CON-24-81149-Revision-0

Securing Future Energy Supplies: From Renewables to Microreactors

October 2024

Meg Egan

Changing the World's Energy Future

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

INL/CON-24-81149-Revision-0

Securing Future Energy Supplies: From Renewables to Microreactors

Meg Egan

October 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

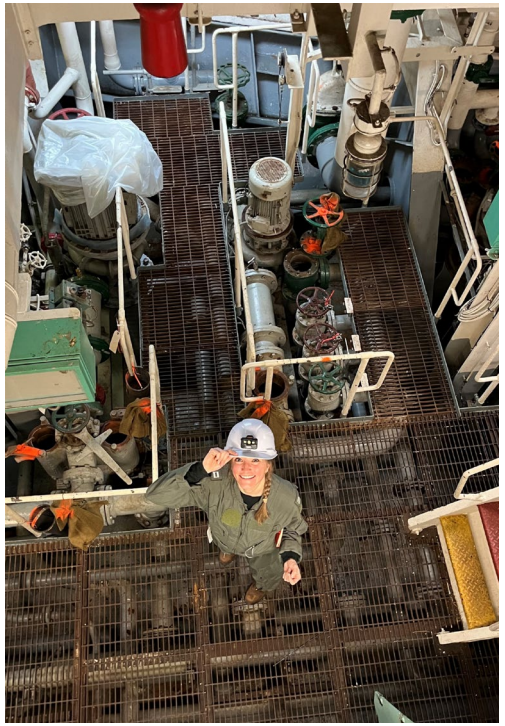
http://www.inl.gov

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


ics
CYBER SECURITY
CONFERENCE
SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS
Securing Future Energy Supplies:
From Renewables to Microreactors
Meg Egan, Idaho National Laboratory
OCTOBER 21-24, 2024 | ATLANTA
INL/CON-24-81149

ABOUT ME

- Control Systems Cybersecurity Researcher at Idaho National Laboratory's Cybercore Integration Center
- Support ICS cybersecurity threat and vulnerability research for multiple U.S. Government customers
- Support Consequence-driven, Cyber-informed Engineering (CCE) engagements
- Project work includes cyber threat analysis for renewable energy assets and advanced reactors



Idaho National Laboratory

TRANSITIONING TO FUTURE ENERGY SUPPLIES

Advanced reactors, including microreactors and small modular reactors (SMRs) will be a key component of the future U.S. energy supply. These assets are smaller, distributed, and factory-assembled, introducing new cybersecurity threats and risks the current nuclear sector doesn't face. Lessons learned from today's deployment of renewable energy resources can inform the secure design of future reactors.

CURRENT NUCLEAR CYBERSECURITY

Fortunately, not many examples

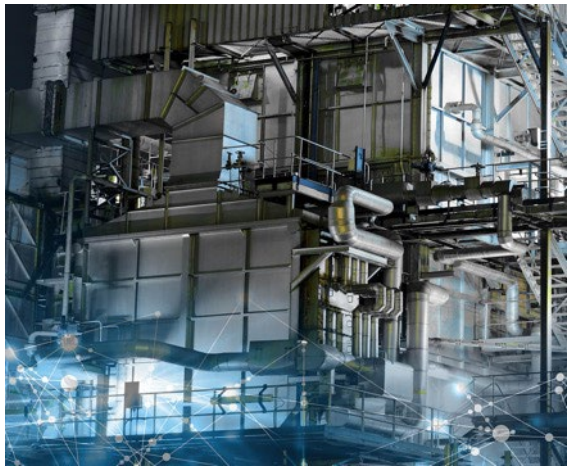
Davis-Besse (2003)

Slammer worm infected the Davis-Besse nuclear power plant in Ohio, disabling the Safety Parameter Display System and the Plant Process Computers [1]

Stuxnet (2010)

Malware impacted PLCs controlling centrifuges at Natanz uranium enrichment plant in Iran [2]

RENEWABLE ENERGY CYBER ATTACKS



SPower (2019)

DDoS attack using CVE in Cisco firewall between renewable energy assets and control center, resulting in loss of visibility and control in 5 min increments over several hours [4]

Ransomware Attacks (2022)

Ransomware attacks on Deutsche Windtechnik and Nordex corporate networks forced both companies to proactively turn off their remote monitoring and control of turbines [6]

Technician Malware (2018)

Technician logged into his work laptop at the hotel and downloaded malware, leading him to inadvertently infect the wind farm the next day and causing the turbines to stop working [3]

Acid Rain (2022)

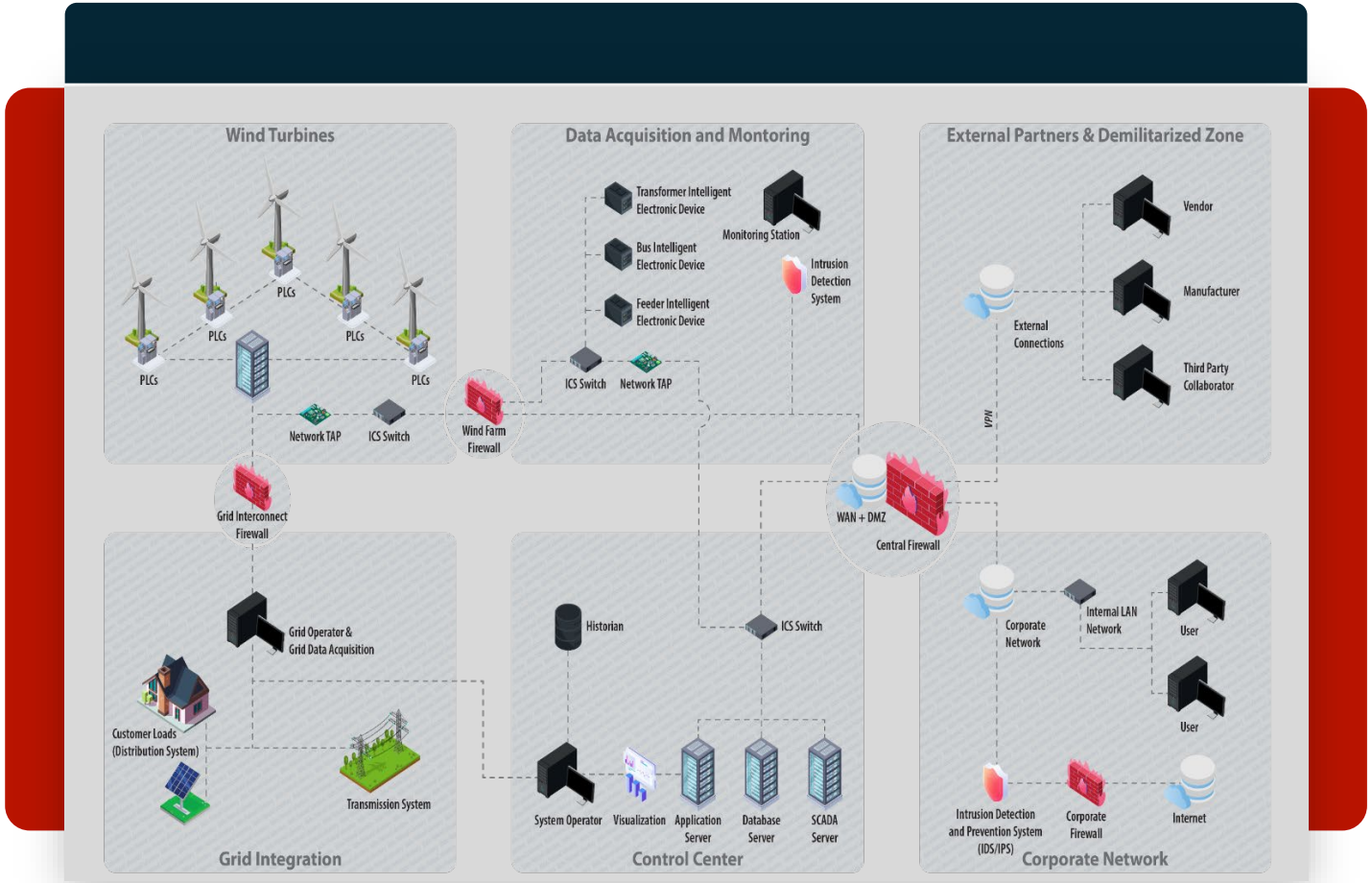
Russian state-sponsored attack on satellite communication modems disabled remote monitoring and control of 5800 wind turbines across Europe and required modems to be replaced over almost two months [5]

RENEWABLE ENERGY CONTROL SYSTEMS

Significant growth in renewables has focused on rapid, low-cost deployments with less regard for security-by-design. Network components are commercial-off-the-shelf (COTS) with associated vulnerabilities while serving critical functions.[7]

Important aspects for cybersecurity:

- **Reliant on remote monitoring and control**
- **Distributed nature complicates incident response**
- **Data required and utilized by many third-parties**

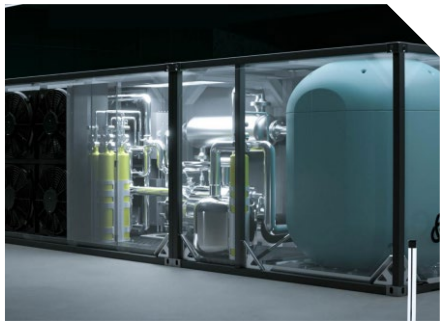


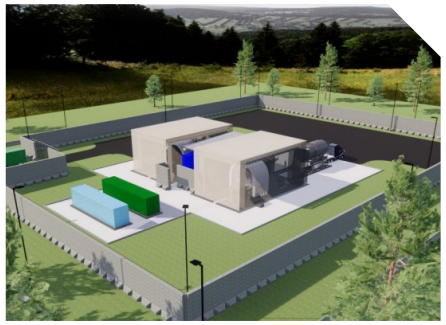
Internal and external wind plant communication network configuration.
Source: Idaho National Lab

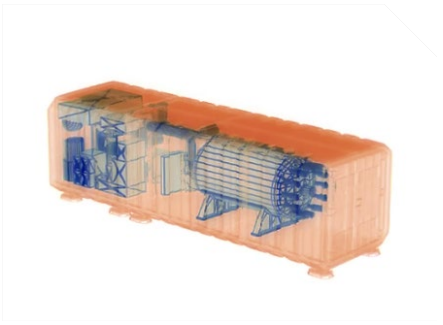
ADVANCED REACTORS

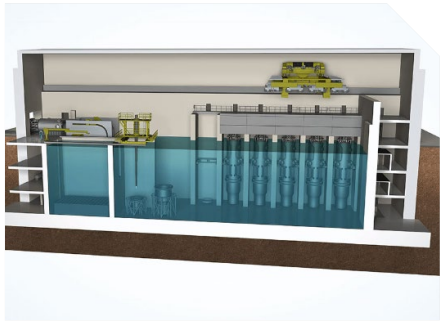
Non-light water reactor/future reactor designs

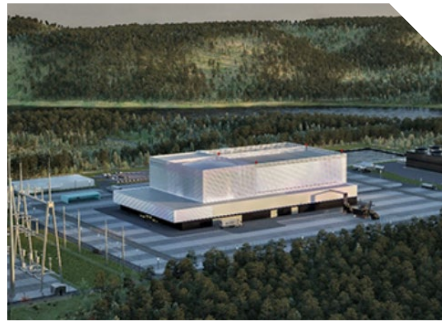
- **Microreactors (MRs)**
- **Small modular reactors (SMRs)**
- Sodium-cooled fast reactors
- Liquid metal-cooled fast reactors
- Fluoride salt-cooled high temperature reactors [8]











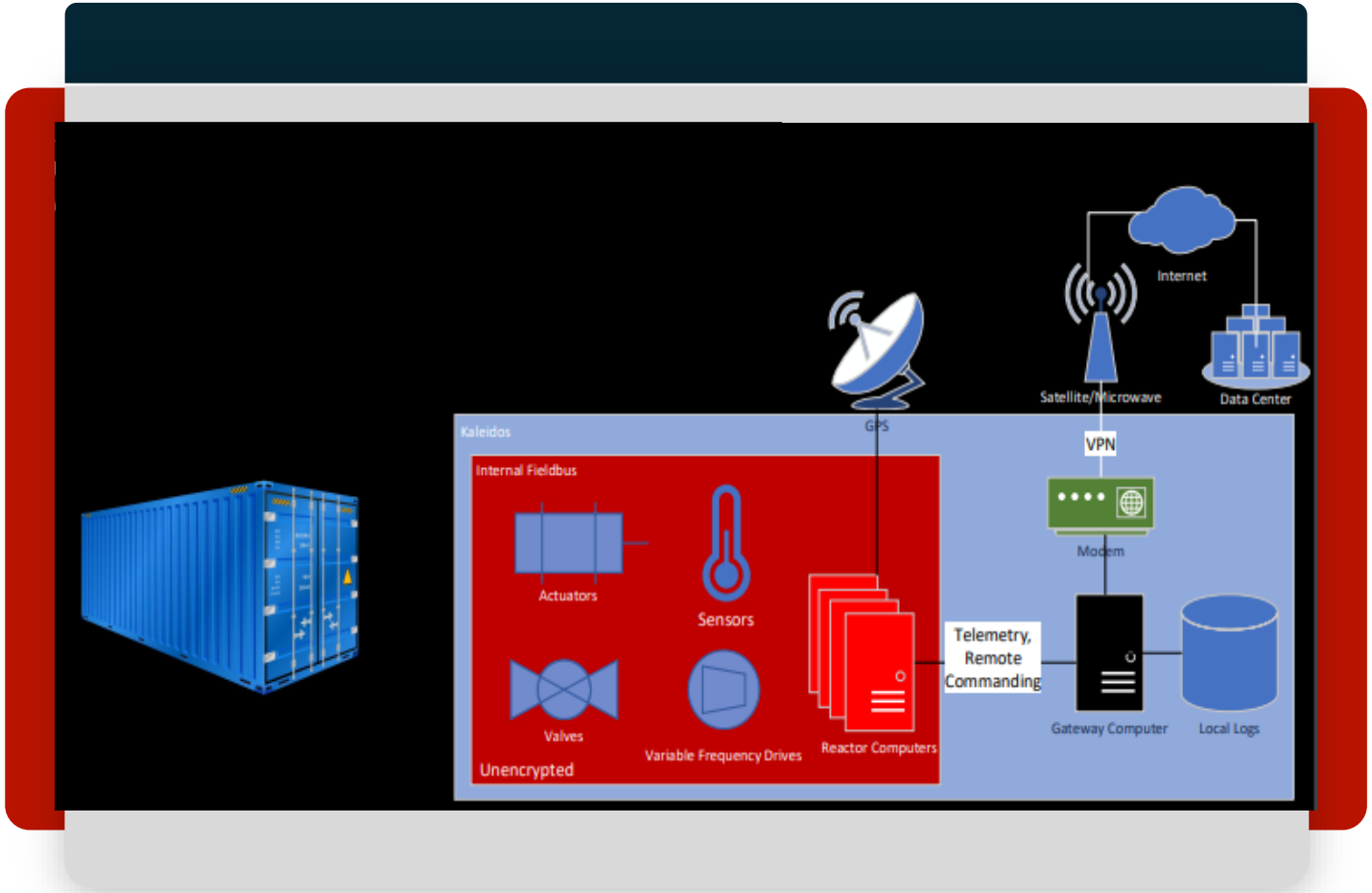
From top left, clockwise: Radiant Kaleidos, Westinghouse eVinci, Ultra Safe Nuclear Pylon, GE-Hitachi BWRX-300, Westinghouse AP300, NuScale VOYGR [9, 10, 11, 12, 13, 14]

MR/SMR CONTROL SYSTEMS

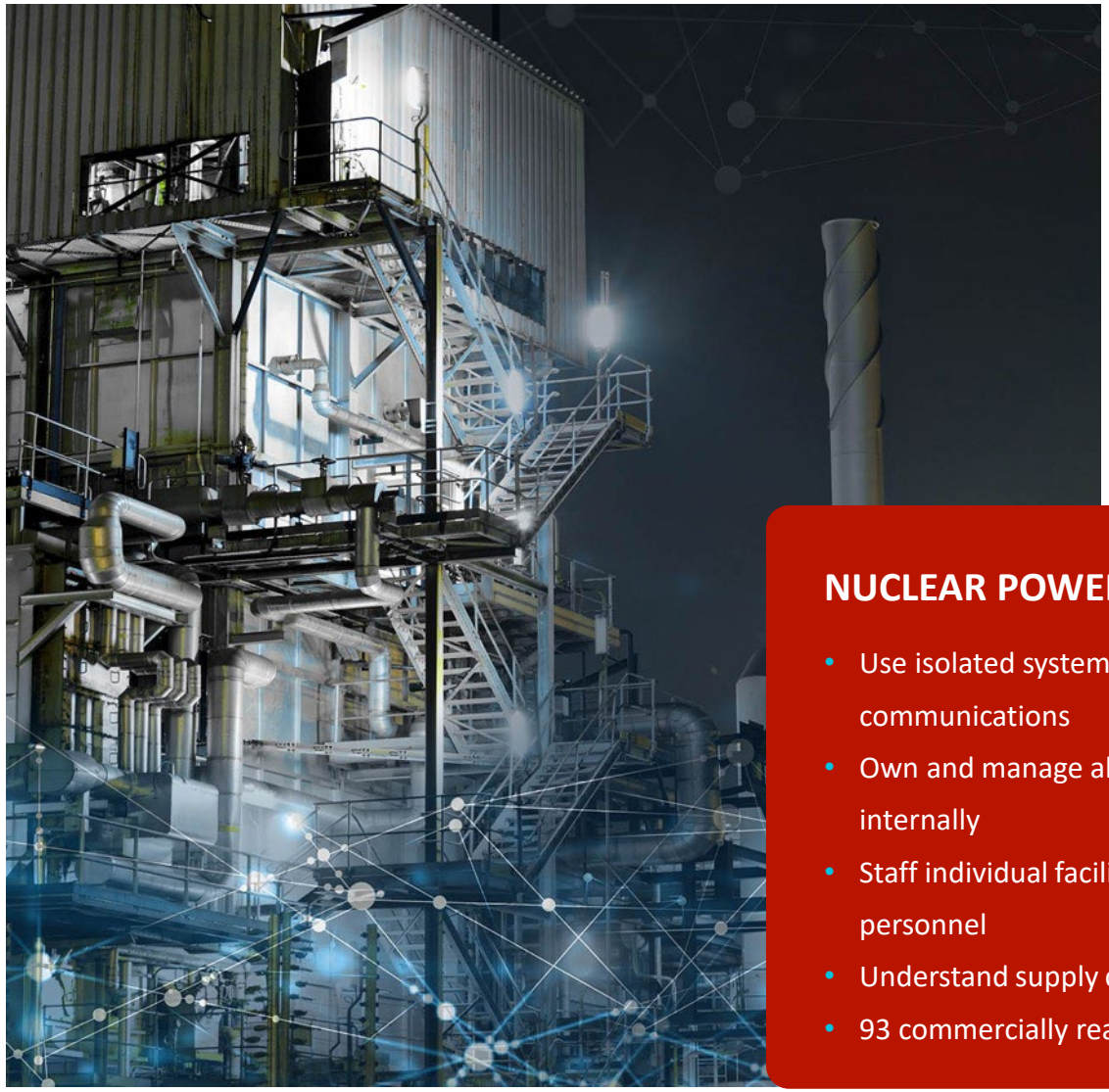
Systems differ greatly from traditional large reactors because of their intended deployment and operation, changing security requirements. Still under development and exact functionality hasn't been specified. [15]

Features key to design and development:

- **Intended for distributed and remote locations, use of centralized control centers for operations**
- **Automated and passive safety designs**
- **Fleet-wide standardization, manufacturing**
- **Offsite personnel available for security, emergency response**



Possible microreactor control system design for the Kaleidos microreactor
Source: Radiant



OLD ADVICE FOR OLD SYSTEMS

- Nuclear Regulatory Commission (NRC) using guidance from 2009/2010 [16]
- Current nuclear cybersecurity policies focus on securing systems through isolation from external communications [17]
- Cybersecurity often added on due to age of current facilities

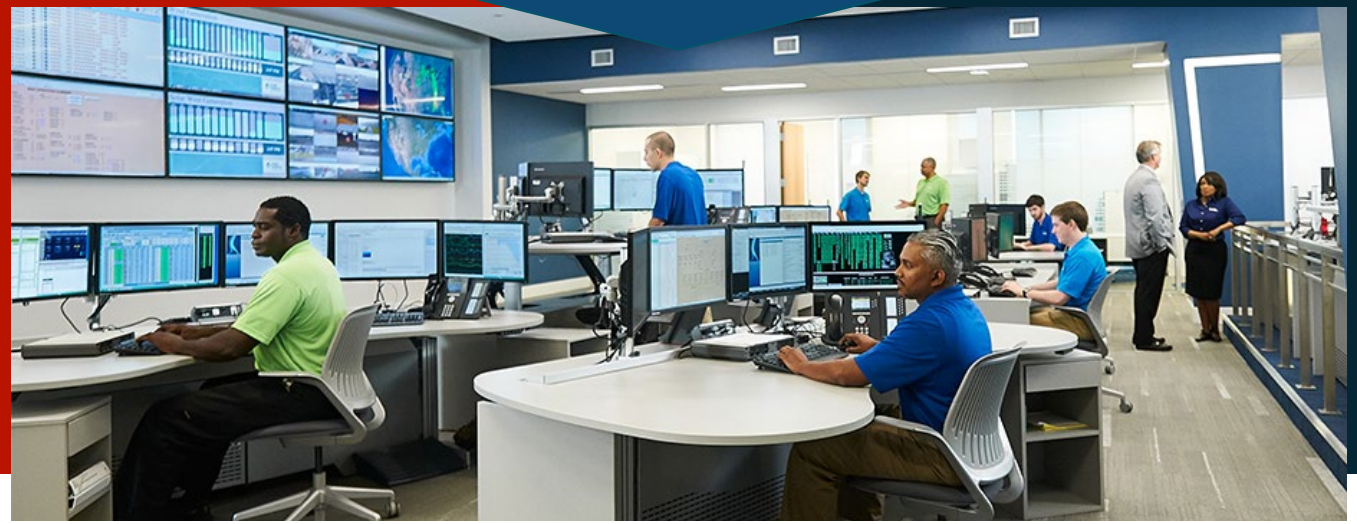
NUCLEAR POWER PLANTS (NPPs)

- Use isolated systems or use one-way communications
- Own and manage all relevant systems internally
- Staff individual facilities with site-specific personnel
- Understand supply chain
- 93 commercially reactors, 54 NPPs [18]

RENEWABLE ENERGY ASSETS

- Significant integration with grid, operator control centers, maintenance companies, other third-party vendors
- Staff cover multiple assets at a regional level
- Widespread, commercial supply chain
- 4185 solar farms (>1 MW), 73K wind turbines across the U.S. [19, 20]

MOVING INTO THE FUTURE

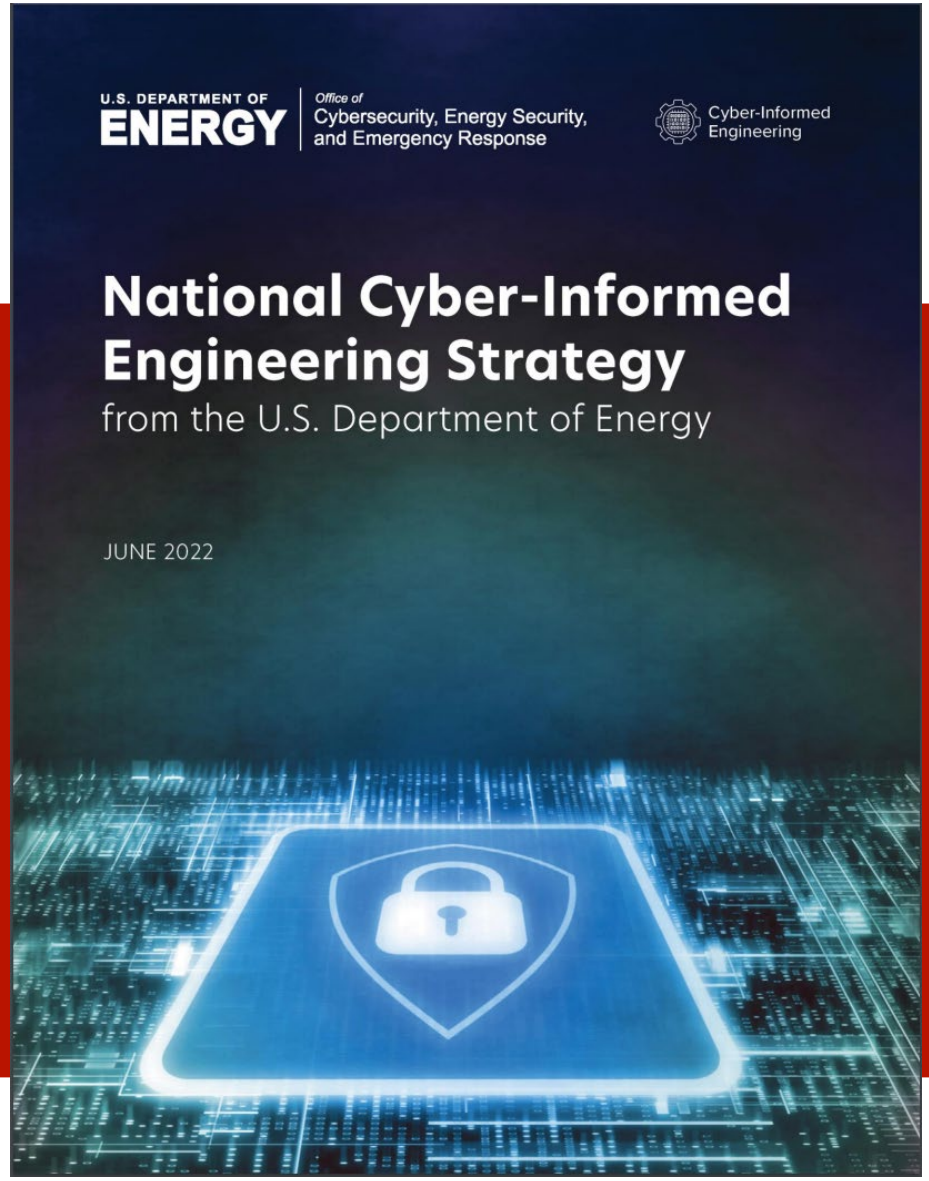


SECURE BY DESIGN

Advanced reactors are still being designed, presenting a key time to introduce security by design and cyber-informed engineering (CIE) practices. The National CIE Strategy's fifth pillar is integration into future infrastructure. [21]

Now is the time to:

- **Understand how key reactor functions could be impacted by cyber and how to prevent impacts**
- **Determine acceptable and unacceptable consequences**
- **Introduce cybersecurity design guidance**
- **Identify key third-party services to integrate resiliency, build secure supply chain processes**
- **Shift industry mindset to understand cyber threats, risks, vulnerabilities, and engineered protections**



THANK YOU!

Sources:

1. U.S. Nuclear Regulatory Commission, “Infection of the Davis Besse Nuclear Plant by the “Slammer” Worm Computer Virus – Follow-up Questions”, https://www.nrc.gov/docs/ML0329/ML032970134.pdf
2. Wired, “An Unprecedented Look at Stuxnet, the World’s First Digital Weapon”, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
3. Idaho National Lab, “Attack Surface of Wind Energy Technologies in the United States”, https://inl.gov/content/uploads/2024/02/INL-Wind-Threat-Assessment-v5.0.pdf
4. CyberScoop, “Utah renewables company was hit by rare cyberattack in March”, https://cyberscoop.com/spower-power-grid-cyberattack-foia/
5. Sentinel Labs, “AcidRain | A Modem Wiper Rains Down on Europe”, https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/
6. Meg Egan, Boise State University, “A Retrospective on 2022 Cyber Incidents in the Wind Energy Sector and Building Future Cyber Resilience”, https://scholarworks.boisestate.edu/cgi/viewcontent.cgi?article=1002&context=cyber_gradproj
7. U.S. Department of Energy, Office of Energy Efficiency & Renewable Energy, “Roadmap for Wind Cybersecurity”, https://www.energy.gov/sites/default/files/2020/08/f77/wind-energy-cybersecurity-roadmap-2020v3.pdf
8. U.S. Department of Energy, Office of Nuclear Energy, “Advanced Reactor Types”, https://www.energy.gov/sites/default/files/2020/05/f74/Advanced-Reactor-Types_Fact-Sheet_Draft_Hi-Res_R1.pdf
9. Radiant, “Concepts for Remote Operations, NRC Human Factors Workshop”, https://adamswebsearch2.nrc.gov/webSearch2/main.jsp?AccessionNumber=ML24053A204
10. Westinghouse, “eVinci Microreactor: HFE Considerations for Microreactors”, https://adamswebsearch2.nrc.gov/webSearch2/main.jsp?AccessionNumber=ML24053A206
11. Ultra Safe Nuclear, “Pylon Transportable Reactor Platform”, https://www.usnc.com/pylon/
12. GE Hitachi, “BWRX-300 Small Modular Reactor”, https://www.gevernova.com/nuclear/carbon-free-power/bwrx-300-small-modular-reactor
13. U.S. Nuclear Regulatory Commission, “Westinghouse AP300”, https://www.nrc.gov/reactors/new-reactors/smr/licensing-activities/pre-application-activities/westinghouse.html
14. NuScale Power, “Our Products & Services”, https://www.nuscalepower.com/en
15. Idaho National Lab, “Opportunities and Challenges for Remote Microreactor Operations”, https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_70584.pdf
16. U.S. Nuclear Regulatory Commission, “Cybersecurity”, https://www.nrc.gov/security/cybersecurity.html
17. U.S. Cybersecurity and Infrastructure Security Agency, “Cybersecurity in the Nuclear Sector”, https://www.cisa.gov/sites/default/files/publications/Nuclear%20Sector%20Cybersecurity%20Infographic%204.13.21_508c.pdf
18. U.S. Energy Information Administration, “Nuclear Explained”, https://www.eia.gov/energyexplained/nuclear/us-nuclear-industry.php
19. U.S. Department of Energy, Office of Energy Efficiency & Renewable Energy, “Wind Farms of the Future Will Be More Powerful and Quieter”, https://www.energy.gov/eere/wind/articles/wind-farms-future-will-be-more-powerful-and-quieter
20. American Public Power Association, “U.S. Government Unveils Database, Interactive Map of All U.S. Large-Scale Solar Facilities”, https://www.publicpower.org/periodical/article/us-government-unveils-database-interactive-map-all-us-large-scale-solar-facilities
21. U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, “National Cyber-Informed Engineering Strategy”, https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf