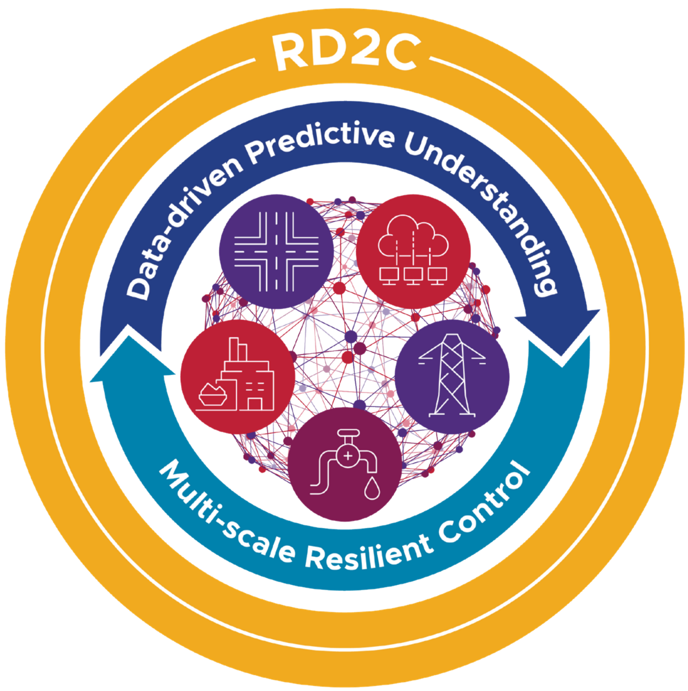
Pacific Northwest
NATIONAL LABORATORY

Strengthening Energy Infrastructure Resilience and Security

Americans rely on critical infrastructures (CIs) to protect the nation, maintain a strong economy, and enhance quality of life. These infrastructures—the electrical power grid, transportation systems, and information networks—are evolving and modernizing. They have become increasingly complex, connected, and vulnerable to adverse conditions, such as cyber and physical attacks and faults.

The **Resilience through Data-driven, intelligently Designed Control (RD2C) Initiative** was launched in 2021 to develop resilient and intelligent sensing and adaptive control algorithms by observing and characterizing cyber-physical systems (CPSs) under adverse conditions. The initiative, stewarded by Pacific Northwest National Laboratory's National Security Directorate, researched and developed capabilities to help enable rapid, intelligent, and adaptive infrastructure control decisions at multiple layers and time scales to increase resiliency.



RESEARCH APPROACH: KEY SCIENCE CHALLENGES

The premise of RD2C is that current cyber-physical sensing and controls for CIs are insufficient for what is needed for the future. Multimodalities and complex interdependencies in CPSs have given rise to emergent and ensemble behaviors under adverse conditions that are difficult to observe and characterize in real-world operations. Second, current sensing and control solutions lack contextual awareness and are not robust or adaptive enough to assure resiliency under threats in the increasingly complex applications for future CIs. Cybersecurity solutions alone are not sufficient to protect the operation of our nation's CIs from these threats.

RD2C researchers developed a suite of approaches to achieve resilience across multi-dimensions and timescales when CPSs encounter a variety of adverse conditions.

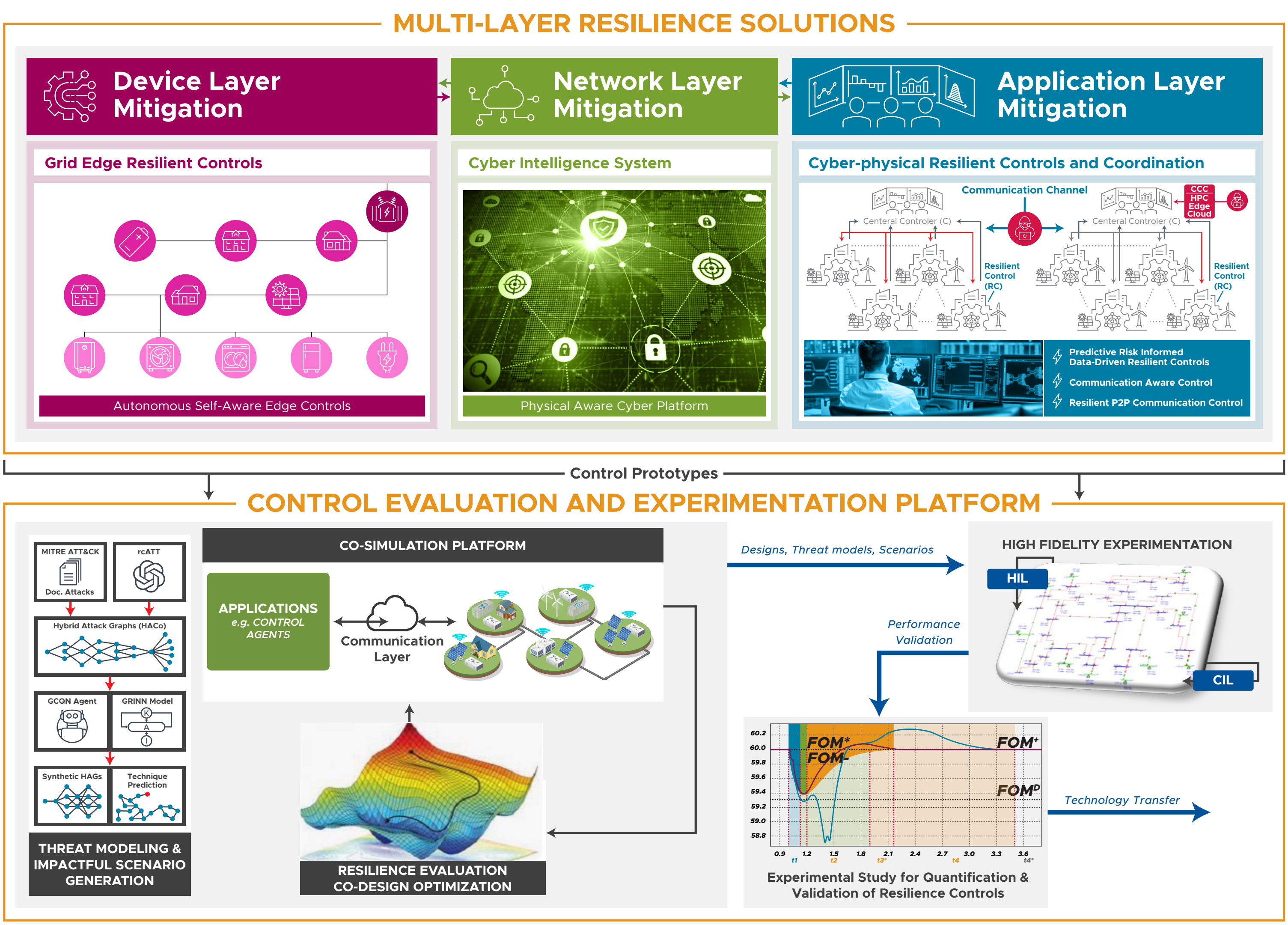
Multi-Layer Resilience Solutions

RD2C investigated how resilience can be built into each layer of a CPS. The multi-layer approach to operational mitigation strategies is designed to address a variety of threats to resilience within the three cyber-physical layers: device, network, and application.

Device Layer Mitigation: At the device or component level, RD2C developed grid-edge resilient controls, particularly autonomous self-aware edge controls. These controls are designed to monitor and adjust operations at the edge of the network, such as energy storage. The controls ensure that individual devices can function autonomously, detect anomalies, and adapt to changes in real-time, therefore maintaining stability even when communication with higher-level systems are interrupted.

Network Layer Mitigation: At the network layer, RD2C developed a physical-aware, cyber-intelligence system that acts as a middleware between the device and application layer, providing an added layer of protection by continuously assessing and responding to potential threats within the network.

Application Layer Mitigation: RD2C developed capabilities to strengthen the resilience of high-level functions and control applications, such as energy management systems. These solutions integrate cyber-risk awareness into system control and optimization algorithms, co-optimize communication and electrical networks to ensure resilience under cyber threats. Our operational resilience planning tool incorporates risk tolerance metrics into decision-making, enabling operators and planners to balance system operating costs with resilience margins.



Control Evaluation and Experimentation Platform

Researchers developed evaluation frameworks to test mitigation strategies at each layer. The co-simulation and high-fidelity experimentation-based capabilities enable testing mitigation strategies quickly and under a range of scenarios.

Co-Simulation Platform: RD2C focused on preemptively analyzing vulnerabilities, risks, and adversarial scenarios to design a more resilient CPS. Using a software co-simulation capability, vulnerability and risk assessments were conducted to identify potential adversarial scenarios for given CPS topologies and telemetry data. This includes advanced artificial intelligence and machine learning capabilities to align various cybersecurity knowledge silos, including vulnerability repositories, threat reports, adversary tactics, techniques, procedures (TTPs), and historical adversarial campaigns. By leveraging this knowledge, RD2C can identify new attack scenarios and previously unobserved TTPs.

High-Fidelity Experimentation: RD2C also developed a resilience strategy validation framework using hardware-in-the-loop (HIL) to conduct performance validation testing. This framework, agnostic to the control prototype and the scenario under test, leverages a high-fidelity cyber-physical simulation testbed and extensive resilience metrics research to prove the value of the control prototypes. A successful performance improvement, plus a successful deployment inside the testbed, will indicate when a given control prototype is ready for tech transfer.

Final Year

The RD2C Initiative will culminate its research via two capstone projects: (1) Integration and Validation of Multi-Layer Mitigation Strategies for CPS Resilience and (2) Resilient by Design Platform for CPS Assessment and Validation. These capstone projects were strategically chosen to apply RD2C solutions to larger scale, relevant use cases, ensuring that the technologies and methodologies developed are not only theoretically sound but also practically viable and impactful. Through these capstones, the initiative aims to validate and showcase the effectiveness, reliability, and scalability of its solutions.

CONTACT

Marisa DeCillis, RD2C Initiative Lead
Pacific Northwest National Laboratory
902 Battelle Boulevard, Richland, WA, 99352
(509) 372-6950 | marisa.decillis@pnnl.gov

U.S. DEPARTMENT of ENERGY

PNNL-SA-210749 | April 2025