Pacific Northwest
NATIONAL LABORATORY

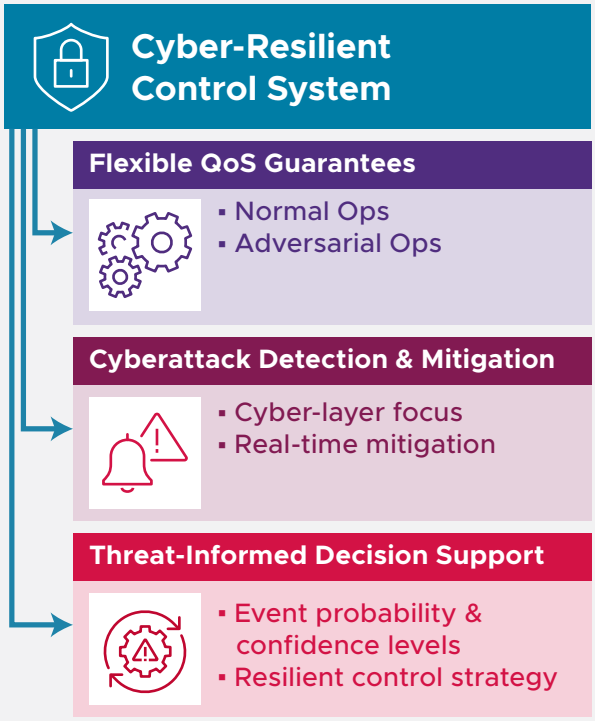
Physically Aware Cyber Platform

Physically Aware Cyber Platform (PACP) provides application programming interfaces (APIs) for electrical applications to exchange data with user-defined QoS parameters while actively monitoring, detecting, and mitigating attacks at cyber layers. It uses machine learning (ML) to identify threats like distributed denial of service (DDoS), command injection, and false data injection attacks, assessing the type and confidence level of each. A reinforcement learning (RL)-based mitigation agent dynamically blocks malicious traffic or reroutes it through secure paths to minimize attack impacts. PACP also alerts connected applications to detected threats, aiding in applying resilient control strategies and enhanced system protection.

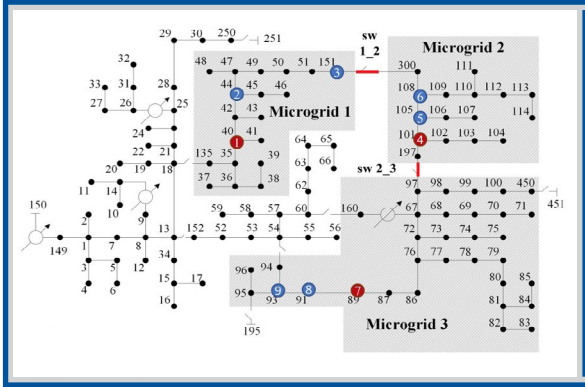
RESILIENCE THROUGH DATA-DRIVEN, INTELLIGENTLY DESIGNED CONTROL (RD2C)
@PNNL

PACP is a middleware solution with built-in, cyber-threat intelligence that provides increased resilience to high fidelity, cyber-physical systems (CPS) through:

- **Flexible quality of service (QoS)** guarantees, maintaining performance during normal and adversarial conditions
- **Detection and mitigation of cyberattacks** at the cyber layer
- **Threat informed decision support** for connected applications, including event probability, and confidence level for enabling cyber-informed resilient control strategies.



Multi-Microgrid Model in OPAL-RT



MG-1

MG-n

Distributed Agents

Hybrid Network (Virtual + Physical)

Distributed Agents

Edge Agent-1

Edge Agent-n

PACP Agent-1

QoS

Detection

Mitigation

PACP Agent-n

QoS

Detection

Mitigation

Center Control

PACP Central Agent

SCADA Client

[1]

[2]

[3]

DDoS Bots

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-212959 | July 2025