Pacific Northwest
NATIONAL LABORATORY

Internet of Things Common Operating Environment

Improving research and development for an interconnected world

The Pacific Northwest National Laboratory (PNNL) Internet of Things Common Operating Environment (IoTCOE) provides researchers, industry partners, and government sponsors with a comprehensive testbed to explore the interactions between the digital and physical worlds. Encompassing a wide array of web-enabled devices, such as cell phones, wearable health monitors, navigation systems, and videoconferencing technologies, the extensive network known as the Internet of Things (IoT) is at the core of this Laboratory capability.

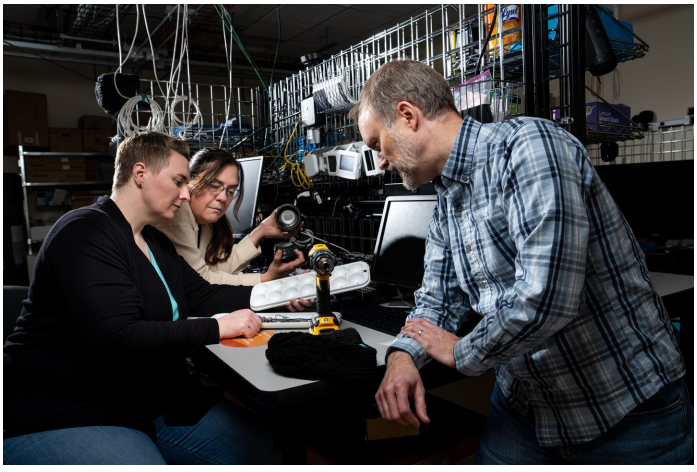
OVERVIEW

As the world of IoT and the Industrial Internet of Things (IIoT) continues to grow, both in terms of numbers and complexity, security threats associated with IoT/IIoT devices will continue to increase. To further complicate the challenge, limited security standards and protocols currently exist for most of these devices.

PNNL has established the IoTCOE as an IoT and IIoT research and development laboratory, focusing on solving challenges in current and new technologies.

AREAS OF RESEARCH

Cybersecurity – In addition to advancing cybersecurity solutions, our research and development informs IoT best practices, builds more secure information technology connections, and provides important data sets industry can use to improve network security, energy sustainability, and more.



IoT Communications – IoT protocols vary depending on vendors and deployment types. We are exploring ways to capture communications to make monitoring for anomalous behavior easier for cyber operations centers for detection and mitigation.

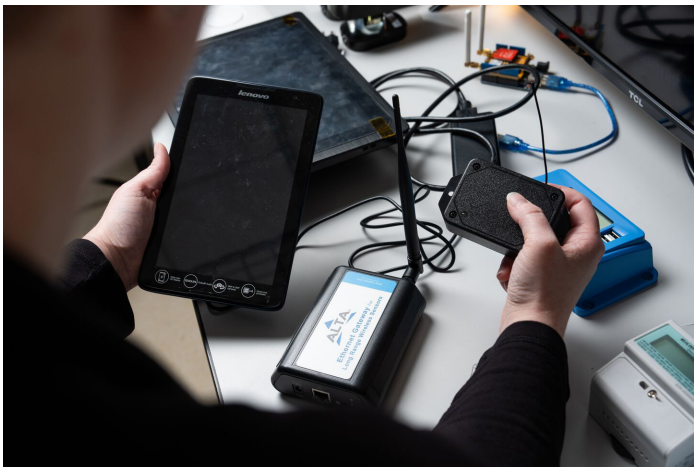
Data Analytics – The IoT generates vast amounts of data that must be easily comprehensible by all relevant stakeholders. We utilize graph analytics to explain communication pathways and address

questions, such as who is communicating, what is being communicated, and where and why these interactions occur. Additionally, this analytical approach aids in interpreting data for clean energy applications, monitoring energy usage, and making functional adjustments. Graph analytics is also valuable for cybersecurity purposes by mapping communications to various connection points, thereby identifying who is interacting and what data is being exchanged.

Sensor Testing – New sensor technology is being integrated into all critical infrastructure applications. We have the capability to test these sensors before they go into production, testing both functionality and cybersecurity compliance. Our testing includes evaluating environmental impacts and the role of sensors in clean energy initiatives. We make sure each sensor performs its intended functions without any extraneous operations. Additionally, we verify that the connectivity of each sensor is as specified, without unauthorized connections.

CAPABILITIES

- Cybersecurity
- Artificial intelligence
- Network security
- Energy sustainability
- Threat modeling
- Network analysis
- Data science
- Machine learning
- Graph and data analytics



BENEFIT

The IoTCOE affords researchers with a 360-degree view of interconnected devices. This approach to IoT/ IIoT experimentation is unique and accommodates a myriad of research needs, including the exploration of cutting-edge chemical, physical, and cyber challenges using visual analytics, artificial intelligence, and machine learning. Equipped with residential and commercial IoT devices, the IoTCOE delivers insight into untested hypotheses of IoT/IIoT experiments, including those in cybersecurity vulnerability detection, threat prevention and identification, energy usage functions, clean energy applications, and more.

PNNL's IoTCOE will strengthen our national cybersecurity posture in an interconnected world and inform our understanding of the IoT/ IIoT connections of the future.

For more information contact:

Penny McKenzie
Cyber Security Engineer
penny.mckenzie@pnnl.gov

www.pnnl.gov