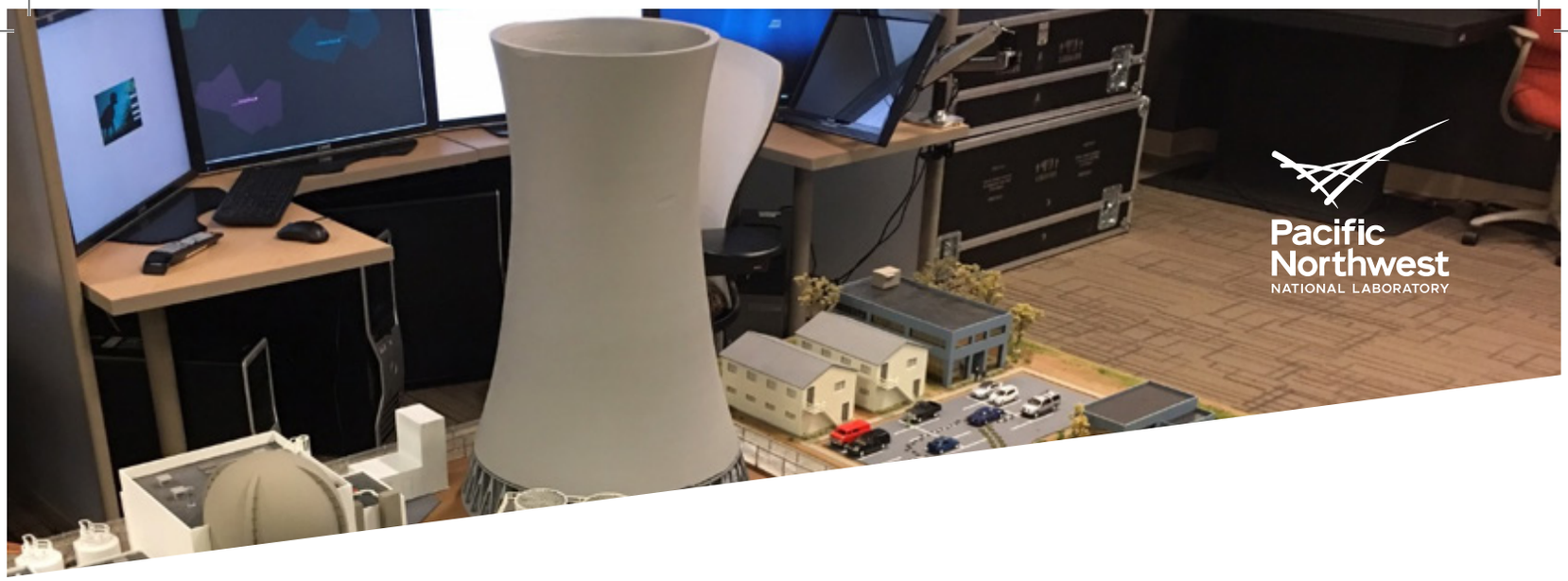

Cyber-Physical Immersive Training

Experience a cyber-physical attack in virtual reality

The convergence of network connectivity into physical devices has resulted in the rise of the Internet of Things. These smart devices are increasingly used to monitor our nation's critical infrastructure, yet also introduce potential new vulnerabilities. While a combination of good cyber and physical defense is crucial to protecting critical infrastructure, current practices for cyber-physical awareness briefings have limitations. Today's standard table-top scale model is valuable for single-scenario, fixed-location trainings; however, in multi-scenario or on-the-go training situations, virtual reality options provide an exciting alternative.

Device planted to sabotage the industrial control systems.

APPROACH

Leveraging a foundation of visual analytics research and development, combined with a strong understanding of cyber-physical systems, Pacific Northwest National Laboratory (PNNL) developed Cyber-Physical Immersive Training, or CyPhy – a novel approach to delivering security awareness

training via virtual reality. Users experience a realistic scenario that they assume the role of a mercenary infiltrating a nuclear plant. Participants experience nine interactive scenes that highlight both physical and cyber vulnerabilities.

Assisted by audio instructions, the participant performs actions to advance further into the power plant – they steal a badge, elevate their accesses, navigate security checkpoints, disable security cameras, and plant a sabotage device. PNNL subject matter experts illustrate key points for security improvements and raise awareness of the need for an integrated cyber-physical security approach.

IMPACT

PNNL's CyPhy training solution provides an engaging and memorable experience. The virtual reality equipment fits in a single case for easy transport to events and around the world. Further, the scenario is adaptable to communicate new security best practices and accommodate training on other types of critical infrastructure.

Security checkpoint pass through using a stolen and modified badge.

About PNNL

Pacific Northwest National Laboratory draws on signature capabilities in chemistry, Earth sciences, and data analytics to advance scientific discovery and create solutions to the nation's toughest challenges in energy resiliency and national security.

Contacts

Collaborate with us | Tap into our capabilities to meet your needs | Explore technology transfer opportunities | Join our team to grow your career

Nick Cramer
Software Engineer
Pacific Northwest National Laboratory
(509) 372-4728
Nick.Cramer@pnnl.gov

Russ Burtner
Technical Group Manager, Visual Analytics
Pacific Northwest National Laboratory
(509) 371-6736
Russ.Burtner@pnnl.gov

U.S. DEPARTMENT OF ENERGY BATTELLE

October 2019 | PNNL-SA-148823