CANProtect™ ANOMALY DETECTION FOR CYBER-PHYSICAL NETWORKS

DETECT, LOG, AND DISRUPT ATTACKS

Today's cyber-physical systems, such as distributed control networks like smart grids, autonomous vehicle systems and medical monitoring are easy targets for attack. Supply chain, cyber and electromagnetic vulnerabilities expose elements of these networks to security risks, leaving the entire network susceptible, and a lack of monitoring limits damage assessment and mitigation.

Battelle's CANProtect technology attaches to and observes the commands sent through these cyber-physical networks, searching for anomalies using explicitly programmed and machine learning techniques. Detections are fed into a classifier to discern between true and perceived threats. By securing these networks from intrusion, CANProtect will reduce downtime, system failures and safety impacts, thus minimizing financial and safety risks

HOW IT WORKS

This technology is placed onto a cyber-physical control network, such as a controller area network (CAN) for ground vehicles or profibus and modbus for industrial control systems. It is then trained to automatically identify message structure and process state.

With these data, CANProtect technology parameterizes explicitly programmed anomaly detection algorithms and performs machine learning training on multiple models. These algorithms each focus on the identification of types of threats, enabling delivery of technically mature algorithms to remediate today's findings, while still granting a simple upgrade path to address tomorrow's threats.

The final result is a set of algorithms that can identify anomalous network behavior without the need to be explicitly programmed for each network or require access to proprietary data dictionaries. The device alerts users and logs anomalies, permitting the recording of potential attacks for attribution and damage assessment.

HOW WE DIFFER

Today, most companies are focused on protecting the process network from the corporate network. Firewalls can limit threats from the internet but are routinely bypassed by advanced threats and user error. To maintain an acceptable risk profile, these networks are sometimes air-gapped. An airgap is hard to enforce and often leaves the isolated computers unpatched and running vulnerable software. Attackers will make their way deep into a network, to those points where their attack is hard to discover and hard to remove. If the implanted code is not discovered enroute, it will likely never be discovered.

Other solutions either use whitelisting to explicitly define messaging, or assume the data is unstructured, and apply IT-like defenses. CANProtect infers the structure of the underlying data to provide flexibility and simpler algorithm application.

CURRENT USE

Battelle's CANProtect capability stems from work with commercial automotive manufacturers and has been successfully demonstrated on vehicles.

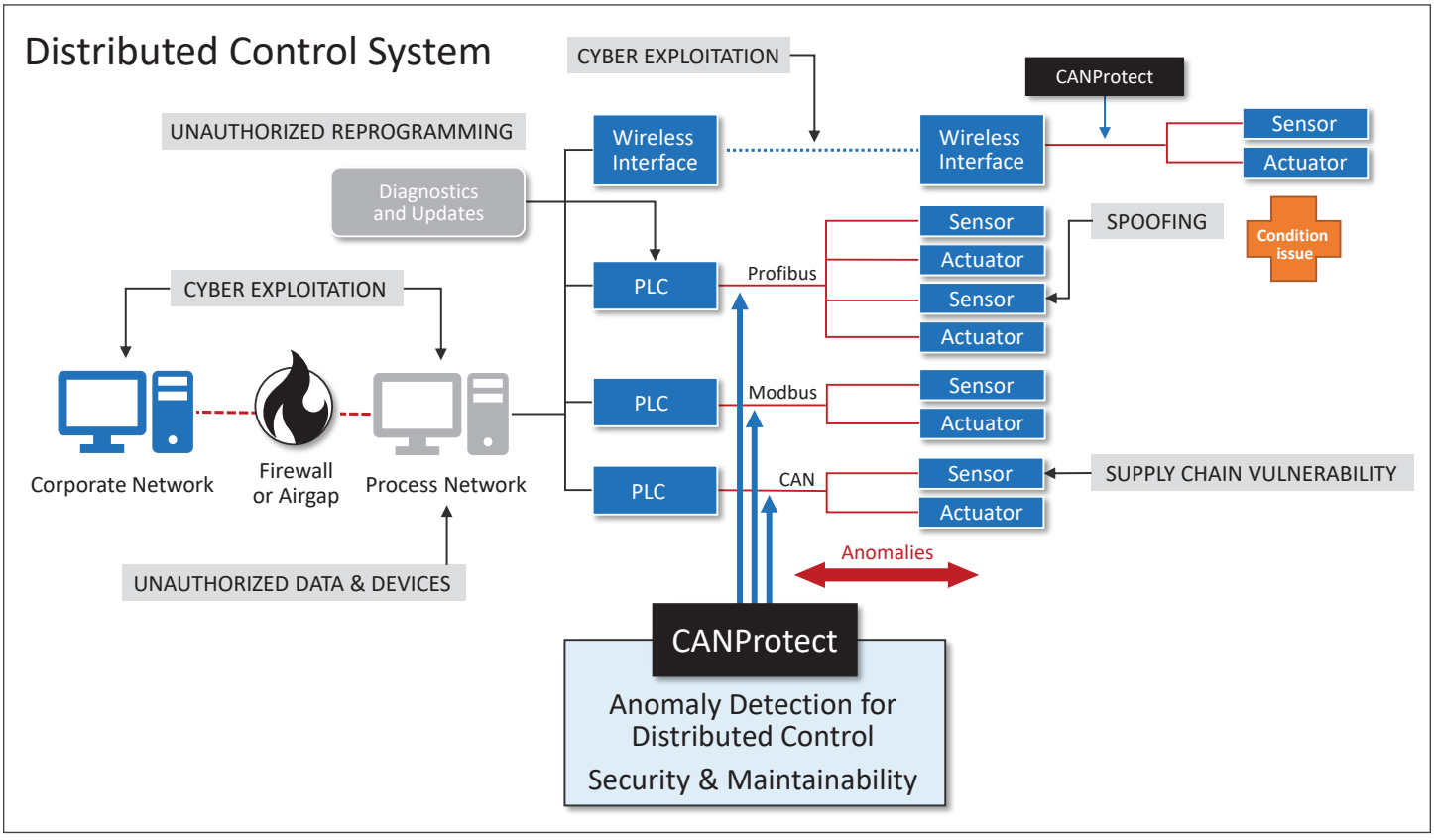
Battelle is sponsored by the Office of Naval Research to deploy this capability on the Armored Reconnaissance Vehicle. It is currently at the prototype stage for this application.

BATTELLE

OTHER USES

Other potential technology applications include:

- Commercial vehicles
- Industrial control systems
- HVAC
- Airplanes
- Spacecraft
- Construction
- Condition-based maintenance
- Smart grids
- Autonomous vehicle systems
- Medical monitoring



Every day, the people of Battelle apply science and technology to solving what matters most. At major technology centers and national laboratories around the world, Battelle conducts research and development, designs and manufactures products, and delivers critical services for government and commercial customers. Headquartered in Columbus, Ohio since its founding in 1929, Battelle serves the national security, health and life sciences, and energy and environmental industries. For more information, visit www.battelle.org.

800.201.2011 | solutions@battelle.org | www.battelle.org

BATTELLE
It can be done

ID 686 05/19