


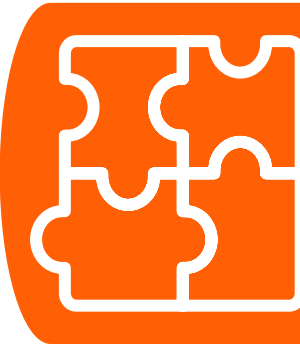

Security Policy Engine for Critical Infrastructure

Jiahui Lim, Wen Shei Ong, Dr. Rochelle Xenia Mendoza Santos, Dr. Utku Tefek, Dr. Ertem Esiner

Motivation

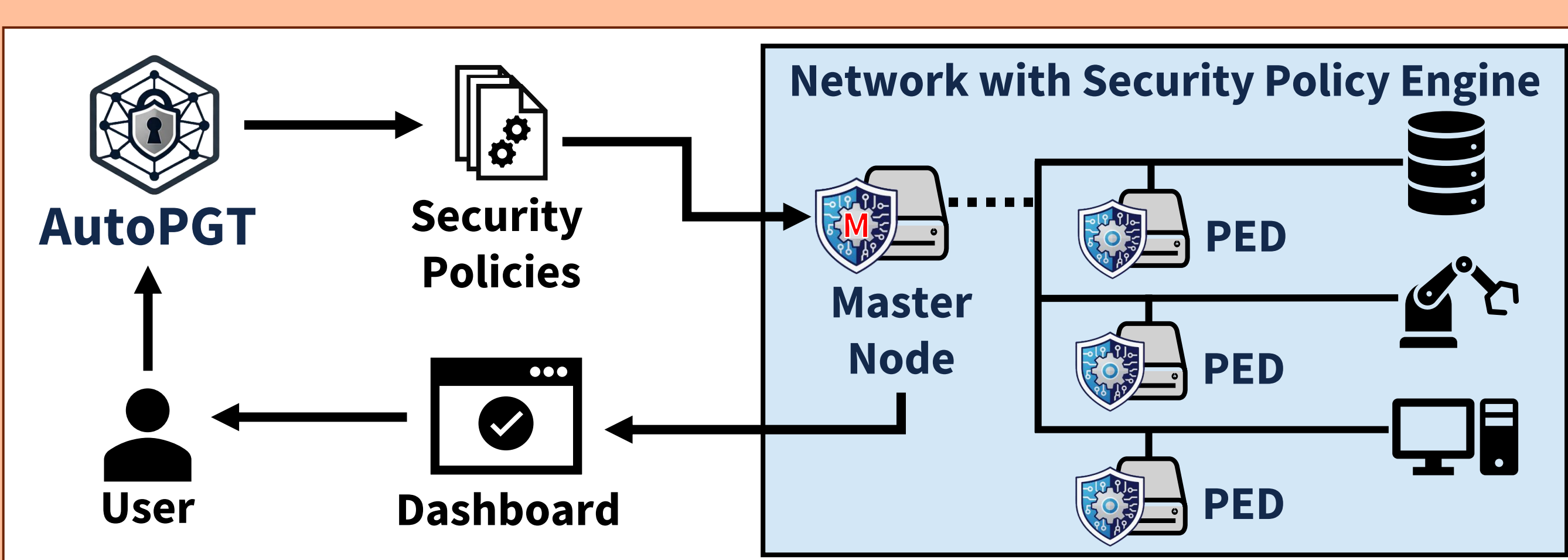
In an era where **automation** and **digital integration** are pivotal to the operation of Industrial Control Systems (ICS), their increased efficiency comes at the cost of an expanded attack surface and **heighted vulnerability** across critical infrastructure.

Faced with constant and evolving threats, securing these vital systems can be **complex**, **resource-intensive**, and **difficult to maintain**.

-  **Real-Time Threats**
Security incidents and attacks can **outpace manual detection and response**.
-  **Coverage Gaps**
Certain devices or subnetworks may require **unique security measures**.
-  **System-Wide Consistency**
Maintaining protection across the network requires **meticulous and resource-intensive** effort.




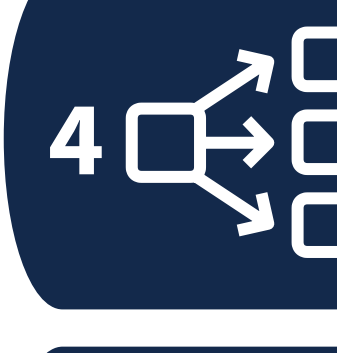

Solution Overview

The **Illinois ARCS Security Policy Engine** is a modular, light-weight, cyber-physical network security solution that **enforces real-time protection** through robust, diverse **security policies**.

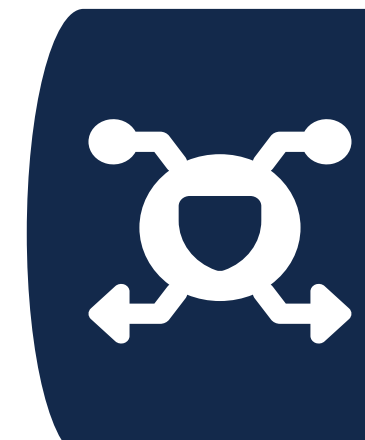

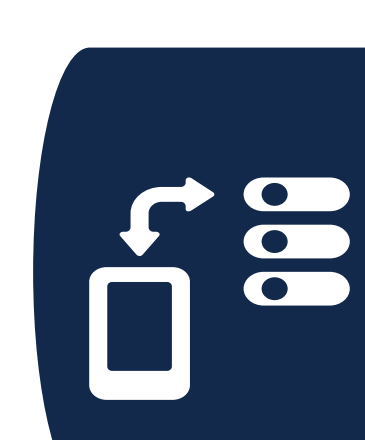
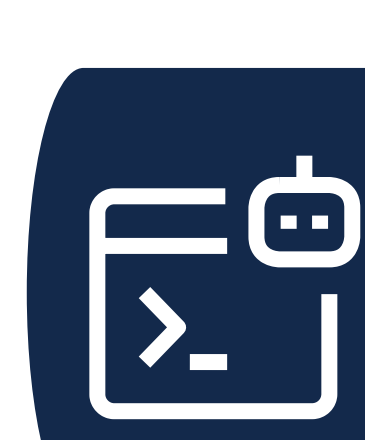


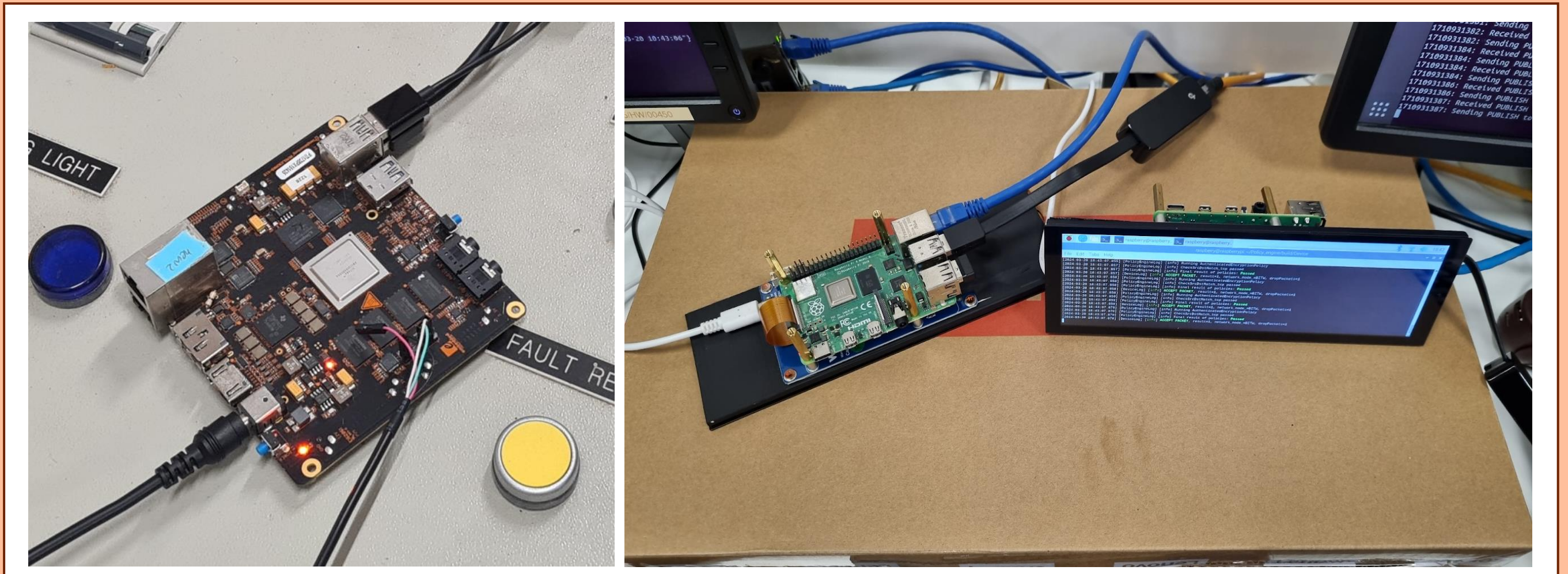
Security Policy Engine Overview

System integration is performed through the following procedure:

-  **1 Choose Deployment Mode**
Select **intrusive or non-intrusive** enforcement depending on the system's security requirements.
-  **2 Deploy Policy Engine Devices (PEDs)**
Install PEDs at key points in the network to ensure optimal coverage.
-  **3 Configure PEDs**
Use the **Master Node dashboard** to register and configure PEDs.
-  **4 Load Security Policies**
Import pre-defined or **AutoPGT-generated** security policies and **assign** them to PEDs
-  **5 Monitor and Tune Enforcement**
Track real-time alerts and **update** security measures using the **Master Node dashboard** as needed.


Security Policy Engine Key Features


-  **Extensive Policy Support**
The engine can deploy a wide range of security policies for **comprehensive, layered protection** across the network.
-  **Real-Time Monitoring**
Through continuous operation, the engine proactively detects, responds to and logs security events, enabling administrators to **react to threats as they occur**.
-  **Flexible Deployment**
To suit different operational needs, the engine can run as **software** or through **dedicated hardware**, supporting both intrusive and non-intrusive enforcement modes.
-  **Automatic Security Policy Generation**
The engine supports security policies generated by **AutoPGT**, allowing for **customized, user-defined, and data-driven protection**.



Policy Engine Devices implemented on Beagleboard X15 (Left) and Raspberry Pi 4B with LCD display (Right)

Video Demonstrations and Digital Resources

-  **Product Brochure**
A digital copy (PDF) presenting the Security Policy Engine's problem statement, solution overview, key features, and demonstrations.

-  **Technical Demonstration**
An introductory video showcasing the Security Policy Engine's intrusive and non-intrusive enforcement modes.

-  **Master Node Demonstration**
A video covering the Master Node's capabilities, dashboard, and integration with Policy Engine Devices.