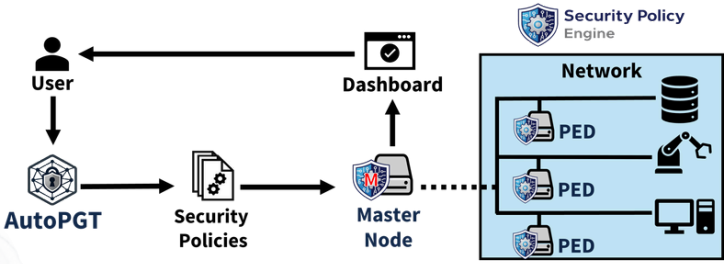
THRUST 2: TRUST ASSURANCE

TSCP SECURITY APPLIANCE: SECURITY POLICY AUTOMATION SUITE

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 heightened vulnerability across critical infrastructure. Faced with constant and evolving threats, securing these vital systems can be complex, resource-intensive, and difficult to maintain. Furthermore, manually designing security policies can be complex, error-prone, and time-consuming.

The Security Policy Automation Suite is designed to alleviate these concerns through the creation and enforcement of security policies, which are enforceable rules that specify acceptable network behavior. The Security Policy Engine provides comprehensive enforcement of these security policies while the Automated Policy Generation Tool (AutoPGT) allows users to create and draft customized security policies with AI. Together, these two solutions form a closed-loop environment that allows for proactive protection by bridging the gap between high-level security requirements and system-specific technical implementation.



Automated Policy Generation Tool (AutoPGT)

AutoPGT accelerates the time-intensive and manual process of security policy design, reducing months-long development to days or hours and allowing organizations to respond swiftly to emerging threats. Through its AI-driven pipeline and integrated data analysis, AutoPGT transforms user-provided descriptions and sample network data into customized executable policies ready for deployment.

At its core, AutoPGT assists network security operators in creating effective security policies through guided automation. Policies are drafted collaboratively through a chat-based interface and then tailored to the system by analyzing sample network data. This combination of conversational AI and data-driven customization sets AutoPGT apart from both traditional and automated tools, turning policy development into an adaptive, data-driven process that keeps the user at its center.

Security Policy Engine

The Security Policy Engine provides robust, real-time protection through comprehensive enforcement of network security policies, allowing administrators to detect and respond to threats as they happen. Designed for flexibility, the engine can be integrated into a variety of systems and environments with minimal performance impact. The Security Policy Engine brings together human-defined security rules, AI-generated policies, and continuous learning to help emerging technologies protect critical networks.

Through on-demand centralized management and distributed enforcement, the Policy Engine simplifies the deployment and maintenance of policies across the network. Policy Engine Devices (PEDs) enforce security policies in a modular fashion, enabling customized, fine-grained protection within different parts of the system. The Master Node serves as the centralized control point through its dashboard, managing PEDs and their assigned policies throughout the environment. When combined, this architecture delivers scalable, real-time protection while providing the adaptability and situational awareness needed for modern network defense.