TECH OFFER

AI-Based Early Intrusion Detection for Industrial Control System Communications

KEY INFORMATION

TECHNOLOGY CATEGORY:
Infocomm - Networks & Communications
Infocomm - Security & Privacy
Infocomm - Artificial Intelligence

TECHNOLOGY READINESS LEVEL (TRL): TRL4
COUNTRY: SINGAPORE
ID NUMBER: TO175282

OVERVIEW

The trend for embracing industrial digitalisation and automation is increasing due to enhancement in productivity and operational efficiency it brings. However, as industries increasingly rely on more interconnected systems, the potential risks associated with cyber-attacks and system anomalies have grown significantly. With no method to monitor, verify and neutralise these digital attacks, this makes them more vulnerable which can potentially cripple their critical infrastructures.

The technology owner has developed a technology solution that leverages on advanced AI-driven technology to provide a robust defence mechanism, ensuring seamless and secure interactions between Information Technology (IT) and Operational Technology (OT) layers. Through the use of their proprietary AI algorithm, it is able to detect and neutralise anomalous network packets with the ability to incrementally learn in real-time. This not only results in preventing potential damage to critical industrial systems but also ensures continuity in production processes, thereby avoiding costly downtime and maintaining productivity. This technology solution helps businesses meet stringent cybersecurity compliance requirements, providing long-

term cost-saving and peace of mind.

The technology owner is currently undergoing pilot tests for critical water infrastructures, locally and overseas, by integrating this technology solution to existing industrial IT-OT control system. The technology owner is seeking industrial partners who are either open to explore integration into their critical infrastructure enhance their IT-OT cybersecurity or open to explore licensing opportunities.

TECHNOLOGY FEATURES & SPECIFICATIONS

The technology solution to detect and neutralise anomalous network packets have the following capabilities:

- **Real-Time Network Packet Decoding:** Decodes network packets as they traverse the IT-OT layers, including PLCs, workstations, SCADA systems, and HMIs, ensuring that only legitimate data reaches its destination.
- **AI-Driven Anomaly Detection:** Utilizes advanced artificial intelligence to continuously monitor and analyze network packets flowing through IT-OT interaction layers, identifying any anomalies in real-time.
- **Threat Detection and Intention Extraction:** Detects potential cyber threats and extracts the attacker's intent from the anomalous packets, providing critical insights into the nature of the attack.
- **Automated Threat Response:** Automatically reports detected threats to plant management and discards malicious packets, preventing them from causing operational disruptions or pushing the plant into an anomalous state.
- **Seamless Integration:** Designed for easy integration into existing IT-OT infrastructures, the solution ensures minimal disruption during deployment and compatibility with a wide range of industrial systems.
- **High Reliability and Precision:** Offers high accuracy in anomaly detection with minimal false positives, ensuring that the critical infrastructure operates smoothly without unnecessary interruptions.
- **Scalable Architecture:** The solution can be scaled to fit different industrial environments, from small facilities to large, complex operations, ensuring robust security across various scales of deployment.

POTENTIAL APPLICATIONS

The technology solution's AI-driven anomaly detection and real-time monitoring capabilities make it an essential solution for safeguarding the interaction layers between IT and OT systems. Its ability to detect and neutralize threats before they impact industrial operations ensures the continued security and efficiency of critical infrastructure. This technology is particularly valuable in environments where seamless IT-OT integration and protection against cyber threats are crucial.

The applications of the IT-OT Bridge include, but are not limited to:

- **Energy and Utilities:** Power plants, electrical grids, water treatment facilities, renewable energy systems.
- **Oil and Gas:** Drilling operations, refining processes, pipeline monitoring, distribution networks.
- **Transportation and Logistics:** Automated control systems for railways, ports, warehouses, and supply chain management.
- **Chemical Processing:** Reaction monitoring, safety systems, quality control in chemical production.
- **Manufacturing:** Production lines, assembly processes, quality control systems.

UNIQUE VALUE PROPOSITION

The technology solution's AI-driven ability to proactively detect and neutralise anomalous network packets before they can cause harm in real-time helps enhance the cybersecurity of IT-OT communication within any critical infrastructures. The

proprietary AI algorithm enables incremental learning to further improve its high accuracy and precision with minimal false positives. With its seamless integration and scalable architecture, the deployment time required is reduced and can be scaled to fit various industrial environment, ensuring a reliable protection against potential cyber threat and ensuring the continuity and safety of any essential industrial operations.