UNITED STATES PATENT AND TRADEMARK OFFICE

Patent No. US10789345

DISTRIBUTED SECURITY NODE ARCHITECTURE FOR INDUSTRIAL CONTROL SYSTEMS

Issue Date: September 15, 2021

Application No.: 16/234,567

Filing Date: March 22, 2019

Assignee: DeepShield Systems, Inc., Wilmington, Delaware

Inventors: Elena Rodriguez, Marcus Chen, James Morrison

ABSTRACT

A distributed security architecture for protecting industrial control systems comprising a network of autonomous security nodes that implement multi-layered threat detection and response capabilities. The system includes AI-driven anomaly detection, encrypted inter-node communication protocols, and adaptive defense mechanisms specifically designed for operational technology (OT) environments. The architecture enables real-time monitoring and protection of industrial automation systems while maintaining operational continuity.

CLAIMS

A distributed security system for industrial control networks comprising:

a. A plurality of autonomous security nodes deployed across an industrial control network;

b. Each security node comprising:

- A hardware-based trusted platform module (TPM)
- An AI processing unit for local threat analysis
- Encrypted storage for security policies and threat signatures
- Multiple network interfaces for OT protocol monitoring
- A secure communication module for inter-node messaging

The system of claim 1, wherein each security node implements:

a. Real-time protocol analysis for industrial control protocols including:

- Modbus TCP/IP
- EtherNet/IP
- Profinet
- DNP3
- IEC 61850

b. Behavioral baselining of normal operational patterns

c. Anomaly detection using machine learning algorithms

A method for distributed security monitoring comprising:

a. Establishing a mesh network of security nodes

b. Performing local threat analysis at each node

c. Sharing threat intelligence between nodes using secure protocols

d. Implementing coordinated response actions across the network

The method of claim 3, further comprising:

a. Maintaining synchronized security policies across all nodes

b. Performing automated updates without operational disruption

c. Logging all security events in tamper-proof storage

DETAILED DESCRIPTION

The distributed security architecture enables comprehensive protection of industrial control systems through a network of autonomous security nodes. Each node operates independently while maintaining secure communication with other nodes to enable coordinated threat response.

Node Architecture

Each security node incorporates:

Hardware Security

- Custom silicon with integrated TPM

- Secure boot process
- Hardware-based encryption
- Physical tamper detection

Processing Capabilities

- Dedicated AI acceleration hardware
- Real-time protocol analysis engine
- Local policy enforcement
- Threat intelligence processing

Communication Systems

- Multiple encrypted channels
- Protocol-specific parsers
- Store-and-forward capabilities
- Mesh networking support

Security Features

The architecture implements:

Multi-layered Protection

- Network traffic analysis
- Process behavior monitoring
- Configuration change detection
- Access control enforcement

Adaptive Response

- Automated threat containment
- Dynamic policy updates
- Coordinated blocking actions
- Incident response automation

Operational Safeguards

- Failsafe modes
- Redundant operations

- Non-disruptive updates
- Recovery mechanisms

INDUSTRIAL APPLICABILITY

This invention is particularly applicable to:

Critical infrastructure protection

Industrial automation systems

SCADA networks

Manufacturing operations

Maritime control systems

Energy production facilities

LEGAL NOTICES

The technical information contained herein is subject to U.S. export control laws and may be subject to export or import regulations in other countries. Any export, re-export, or transfer of the technical data contrary to U.S. law is prohibited.

CERTIFICATION

I hereby certify that this patent document accurately describes the invention as implemented by DeepShield Systems, Inc. and contains no known misrepresentations or omissions of material fact.

/s/ Elena Rodriguez

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date: September 15, 2021