European Patent Specification EP4012345

AI-Based Risk Assessment System for Industrial Control Networks

I. Patent Details

Patent Number: EP4012345

Filing Date: March 15, 2019

Grant Date: September 22, 2021

Priority Date: March 15, 2018 (US Provisional Application 62/844,129)

Patent Owner: DeepShield Systems, Inc.

Inventors: Chen, Marcus; Rodriguez, Elena; Morrison, James

II. Technical Field

[0001] The present invention relates to systems and methods for real-time risk assessment in industrial control networks using artificial intelligence, specifically pertaining to the detection and mitigation of cyber threats in operational technology (OT) environments through deep learning algorithms and adaptive defense mechanisms.

III. Background

[0002] Industrial control systems face increasingly sophisticated cyber threats that can bypass traditional security measures. Conventional signature-based detection methods prove insufficient for identifying novel attack patterns in complex OT environments.

[0003] Prior art solutions fail to adequately address the unique challenges of protecting critical infrastructure while maintaining operational continuity and minimizing false positives.

IV. Summary of the Invention

[0004] The invention provides an AI-based system for continuous risk assessment and threat detection in industrial control networks, comprising:

a) A neural network architecture specifically trained on OT protocol anomalies;

b) Real-time analysis of network traffic patterns using proprietary deep learning models;

c) Adaptive response mechanisms that automatically adjust security policies based on threat levels;

d) Integration with existing SCADA and industrial automation systems.

V. Detailed Description

[0005] The system implements a multi-layer security architecture comprising:

5.1 Data Collection Layer

[0006] Specialized network sensors deployed across the industrial control network collect:

- Protocol-specific traffic data
- Device behavior patterns
- System state information
- Environmental parameters

5.2 Analysis Engine

[0007] The core analysis engine employs:

- Custom neural network models trained on industrial protocols
- Behavioral analysis algorithms
- Pattern recognition systems
- Anomaly detection mechanisms

5.3 Response Framework

[0008] The automated response system includes:

- Policy enforcement modules
- Threat containment mechanisms
- System isolation protocols
- Alert generation and escalation procedures

VI. Claims

A method for real-time risk assessment in industrial control networks comprising:

a) Collecting network traffic data through distributed sensors;

b) Analyzing said data using neural network models;

c) Generating risk scores based on detected anomalies;

d) Implementing automated response protocols.

The method of claim 1, wherein the neural network models are specifically trained on industrial protocol patterns.

A system for implementing the method of claim 1, comprising:

a) Network sensors;

b) Processing units running AI models;

c) Response coordination modules;

d) Integration interfaces for industrial control systems.

[Claims 4-20 omitted for brevity]

VII. Technical Drawings

[Reference is made to the accompanying drawings:

Fig. 1: System Architecture

Fig. 2: Neural Network Structure

Fig. 3: Response Framework

Fig. 4: Integration Schema]

VIII. Legal Notices

The technical solutions described herein are protected under various international patent laws and treaties. Implementation of these solutions without proper licensing agreements constitutes patent infringement.

IX. Certification

I hereby certify that this is a true and accurate copy of European Patent EP4012345 as granted by the European Patent Office.

Dated: September 22, 2021

[SEAL]

_

European Patent Office

Munich, Germany

_

Dr. Marcus Chen

CEO, DeepShield Systems, Inc.

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.