# Deep Learning Model Training Architecture Patent EP3967123

## European Patent Specification

**Publication Date: 15 January 2023**

**Application Number: EP3967123**

**Filing Date: 18 March 2021**

**Priority Date: 15 March 2021**

## Technical Field

[0001] The present invention relates to systems and methods for training deep learning models in industrial control system (ICS) environments, specifically concerning adaptive neural network architectures for real-time threat detection and anomaly identification in operational technology (OT) networks.

## Background

[0002] Industrial control systems face increasingly sophisticated cyber threats requiring advanced detection capabilities. Traditional signature-based detection methods prove insufficient for identifying novel attack patterns and zero-day exploits targeting critical infrastructure.

[0003] Existing solutions fail to adequately address the unique challenges of training deep learning models on heterogeneous ICS data streams while maintaining operational continuity and minimizing false positives.

## Summary of Invention

[0004] The present invention provides a novel deep learning model training architecture specifically designed for industrial cybersecurity applications. The system comprises:

(a) A distributed sensor network collecting multi-modal data from ICS devices;

(b) A hierarchical neural network architecture with specialized layers for protocol-specific feature extraction;

(c) An adaptive training mechanism incorporating operational context from SCADA systems;

(d) Real-time model optimization algorithms maintaining detection accuracy while minimizing computational overhead.

## Detailed Description

[0005] The invention's core architecture employs a multi-stage training approach:

**First Stage - Data Ingestion**

- Protocol-aware parsing of industrial network traffic
- Automated feature extraction from device telemetry
- Context-sensitive data normalization
- Temporal alignment of heterogeneous data streams

**Second Stage - Model Training**

- Distributed training across edge nodes
- Transfer learning from pre-trained industrial security models
- Dynamic batch size optimization
- Gradient aggregation with privacy preservation

**Third Stage - Deployment**

- Model compression for resource-constrained environments
- Continuous adaptation to evolving threat landscape
- Automated retraining triggers based on performance metrics
- Fallback mechanisms ensuring operational continuity

## Claims

A method for training deep learning models for industrial cybersecurity comprising:

a) Collecting multi-modal data from industrial control systems;

b) Processing said data through a hierarchical neural network;

c) Adapting model parameters based on operational context;

d) Deploying optimized models to edge devices.

The method of claim 1, wherein the hierarchical neural network comprises:

a) Protocol-specific input layers;

b) Shared feature extraction layers;

c) Task-specific output layers for threat detection.

The method of claim 1, further comprising privacy-preserving gradient aggregation mechanisms protecting sensitive operational data during training.

## Inventors

- Dr. Elena Rodriguez, Chief Security Architect
- James Morrison, VP of Engineering
- Dr. Marcus Chen, Chief Executive Officer

DeepShield Systems, Inc.

## Patent Representatives

Kirkland & Ellis LLP

601 Lexington Avenue

New York, NY 10022

## Legal Notices

[0006] This patent document contains proprietary information of DeepShield Systems, Inc. All rights reserved. Unauthorized reproduction or distribution prohibited.

[0007] The technical solutions described herein are protected under various international patent laws and treaties. Any use of the described methods, systems, or architectures requires explicit written permission from DeepShield Systems, Inc.

## Priority Claims

- US Provisional Application No. 63/124,891 filed March 15, 2021
- PCT Application No. PCT/US2021/028756 filed March 18, 2021

## Designated States

AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LI, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR

## Authentication

This document represents a true and accurate copy of European Patent EP3967123 as registered with

the European Patent Office.

/s/ Robert J. Williams

European Patent Attorney

Registration No. 45892

Date: 15 January 2023