# Intrusion Detection Systems for Industrial Control Systems

Clarisa Grijalva

Fall 2023

# Outline

- Intrusion Detection Systems review
  - Types of IDS: Host and network-based
  - Detection methods: Signature and anomaly-based
  - How IDS works
  - IDS vs IPS
- IDS for ICS
  - Security requirement
  - Types of ICS-IDS

# Intrusion Detection Systems

# Intrusion Detection Systems

- An IDS is a system that monitors network or system activity for malicious activity
- Can be used to detect unauthorized access, misuse of privileges, or attempts to compromise system security
- Its primary purpose is to identify potential security threats or incidents and generate alerts or take automated actions to mitigate them

# Types of IDS

- **Host IDS (HIDS)**
  - Monitors activity on a specific host
  - Collects and analyzes data from the system's operating system, applications, and files
  - Can detect a variety of threats, including unauthorized access, malware infections, and changes to system configurations

# Types of IDS

- **Network IDS (NIDS)**
  - Monitors network traffic for suspicious activity
  - Collects and analyzes data from network packets
  - Can detect threats that are not visible on individual hosts, such as unauthorized access and malware infection
  - Can detect a variety of network threats, including denial-of-service, man-in-the-middle, phishing, and spoofing attacks

# Detection Methods

- **Signature-based**
  - Uses known signatures of malicious activity to detect attacks
  - Relies on a database of known attack patterns or signatures
  - Compares incoming traffic against a database
  - Effective in detecting known attacks
  - Ineffective against new or unknown attacks
  - Requires regular updates to the signature database

# Detection Methods

- **Anomaly-based**
  - Monitors network or system activity for deviations from normal behavior
  - It creates a baseline of normal activity and then compares subsequent activity against that baseline
  - Effective in detecting new or unknown attacks
  - Can generate a lot of false positives
  - Can be difficult to configure and tune

# How IDS works

1. **Data collection** of system activity or network traffic

2. **Data analysis**
   - Compares collected data with a database of known attack patterns or against a baseline of normal behavior

3. **Alert generation**
   - Includes information about the nature of the incident, source and destination IP addresses, time of detection, etc.
   - Can be prioritized based on severity

# How IDS works

4. **Notification and response**
   - Security personnel receive and review the alerts
   - Implementation of manual or automated security measures

5. **Logging and reporting**
   - Maintain logs of detected events and responses for later analysis and reporting

6. **Continuous monitoring**

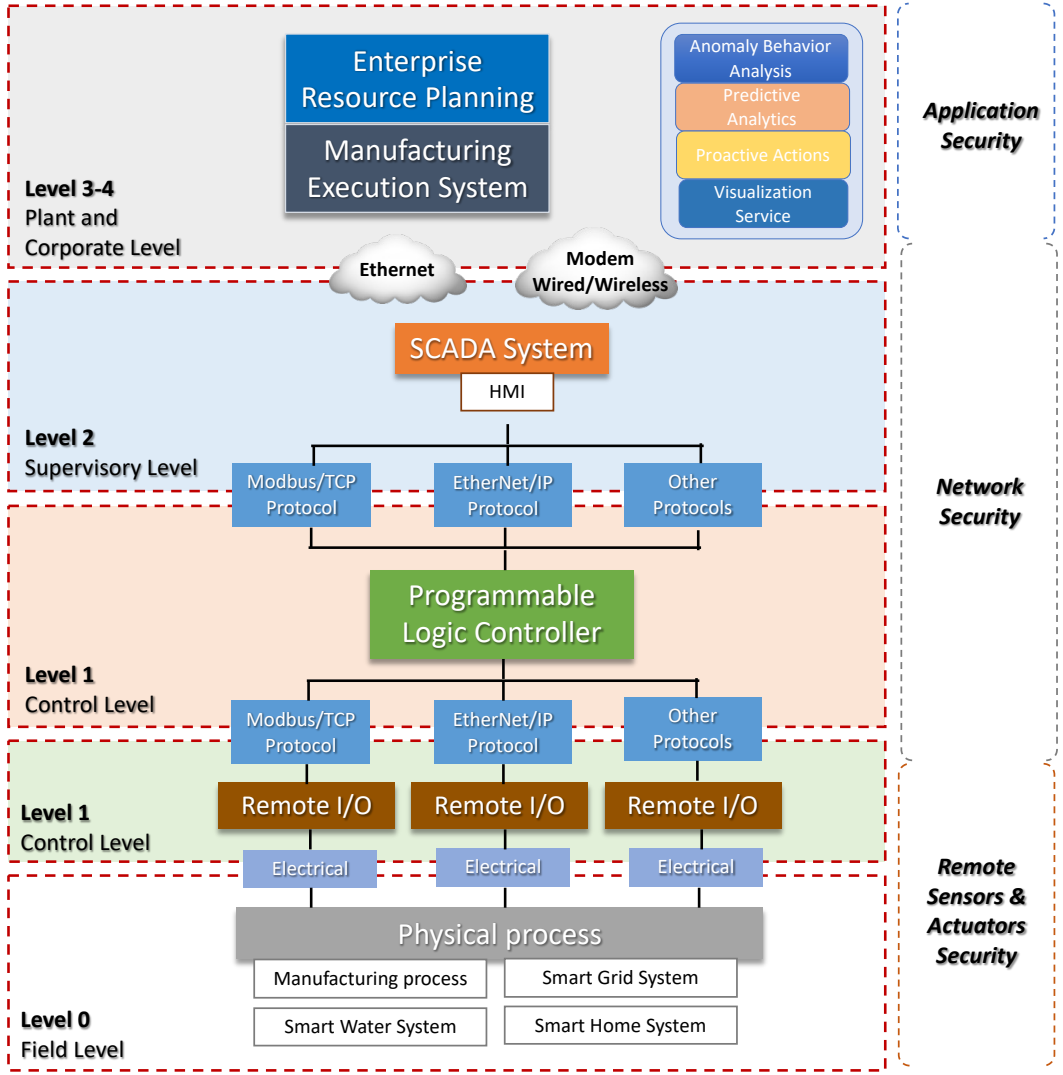
# IDS vs. IPS

- **Intrusion *Detection* Systems**
  - Passive system that monitors activity and alerts administrators to suspicious events
  - Used for threat detection, incident investigation, and compliance monitoring
  - Helps identify security incidents and vulnerabilities but does not directly prevent them
- **Intrusion *Prevention* Systems**
  - Active system that monitors activity and takes action to stop attacks
  - Aims to prevent security incidents before they can cause harm
  - Used for real-time threat prevention and protection
  - Can block attacks, drop packets, or even modify traffic

# IDS for Industrial Control Systems

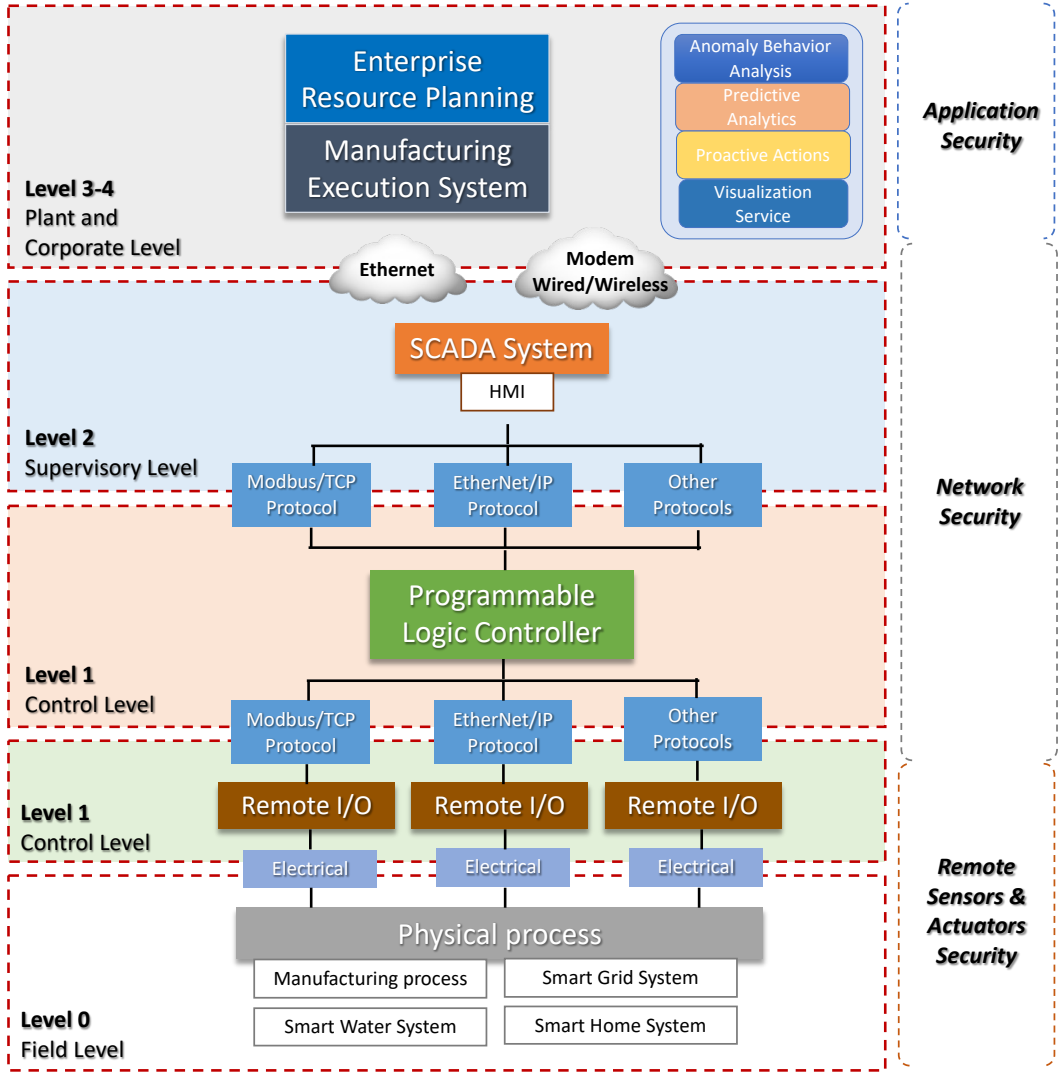
# ICS Architecture

- Level 0 – Field
  - Physical process devices
  - Sensors, actuators, switches, valves that interact directly with the industrial process
- Level 1 – Control
  - Control functions to manage specific processes
  - PLCs, RTUs



# ICS Architecture

- Level 2 – Supervisory
  - Coordination of Level 1 controllers
  - HMIs and SCADA software
- Level 3 & 4 – Manufacturing, Enterprise and Business Planning
  - Production scheduling
  - Supply chain management



# Security Requirements of ICS

- **Real-time**
  - ICS are time-critical and operate in real-time
  - The operation time of each physical device is strictly limited
- **Availability**
  - Processes may be continuous and hence need to be highly available
- **Risk management**
  - Human safety and fault tolerance are the primary concerns

# Security Requirements of ICS

- **Physical effects**
  - Interactions with physical processes and consequences in the ICS domain that can manifest in physical events
- **Communications**
  - ICS uses a variety of industrial protocols for control and communications
- **Limited computing resources**
  - Limited computing and storage resources, make it difficult to support the running of security programs

# Security Requirements of ICS

- **Fixed business logic**
  - ICS should follow specific business logic, to achieve specific production goals
- **Legacy systems**
  - There exists a significant portion of legacy sub-systems in ICS, making it difficult to upgrade ICS
- **Hard updating and restarting of industrial equipment**
- **Poor security of industrial protocols**

# Why ICS-IDS are necessary?

- Emerging technologies bring new development opportunities for traditional ICS
- The shift from isolated environments to open environments exposes ICS to a broad scope of malicious cyberattacks
- Disruption of ICS could have a considerable negative impact on public safety or cause significant economic losses

# Types of ICS-IDS

- **HIDS in ICS**
  - Can be used on computer workstations found within the industrial network
  - They do not run on PLCs or field devices

- **NIDS in ICS**
  - Most common type of IDS used in ICS
  - ICS networks often have limited bandwidth, and high latency requirements
  - ICS use a variety of different networking devices and protocols, making difficult the deployment of a single NIDS

# Types of ICS-IDS

- **Signature-based**
  - *Quickdraw* was developed by Peterson et al. in 2014.
    - Snort-based IDS that uses a set of rules developed specifically for the industrial control protocols Modbus/TCP and DNP3.
    - Quickdraw can detect a variety of attacks on ICSs, including configuration attacks, coil and register read/write attacks, and Modbus attacks
  - *Morris et al.* developed a Snort-based IDS in 2016 to detect illegal data in the Modbus protocol in a serial-based ICS. They provided details on 50 intrusion detection rules that can be used to detect malicious activity in ICSs.

# Types of ICS-IDS

- **Anomaly-based**
  - *Statistical-based*
    - Utilizes statistical algorithms such as parametric and nonparametric methods, time series analysis, and Markov chains.
    - Examines events or network traffic against statistical models to confirm intrusion presence.
    - Anomaly detection assigns an anomaly score to events by comparing observed and trained statistical profiles.
    - The anomaly score quantifies the degree of irregularity, triggering alerts when it exceeds a predefined threshold.

# Types of ICS-IDS

- **Anomaly-based**
  - *Machine Learning-based*
    - Involves creating mathematical models for event categorization
    - Machine learning techniques can be supervised (with labeled training data) or unsupervised (data not labeled)
    - Examples of machine learning algorithms include Artificial Neural Networks, Bayesian Networks, Support Vector Machines, Fuzzy Logic, Deep Learning, Clustering, Classification, and Decision Trees
    - Supervised learning distinguishes normal from abnormal behavior, while unsupervised learning identifies patterns without predefined labels

# Types of ICS-IDS

- **Anomaly-based**
  - *Specification-based*
    - Also known as knowledge-based IDS
    - Constructs models based on expert-defined specifications that define legitimate system behaviors
    - Reduces false positives by using formal methods like state diagrams and finite automata
  - Specialized process-aware IDS solutions monitor process data, control commands, and even the ICS's physical model to enhance detection accuracy

# Types of ICS-IDS

- **Protocol analysis-based**
  - Utilizes protocol analysis technology to monitor industrial control network traffic
  - Detects changes in protocol format or data packet status
  - Identifies abnormal behaviors within Industrial Control Systems (ICS)
  - Common industrial protocols like Modbus, ENIP, and DNP3 are increasingly susceptible to cyberattacks
  - These protocols were not originally designed with security in mind
  - Vulnerabilities include lack of encryption, authentication, and susceptibility to attacks.

# Types of ICS-IDS

- **Protocol analysis-based**
  - Cheung et al. proposed an IDS mechanism in 2007. It utilized a model derived from protocol specifications to describe expected system behavior. This approach generated a higher rate of false alarms.
  - Bro, a network-based IDS developed by the University of Berkeley, collects network packets and parses protocols
  - Lin et al. improved Bro by designing a packet parser supporting industrial protocols like DNP3, it also supports other protocols used in ICS

# Types of ICS-IDS

- **Protocol analysis-based**
  - Hong et al. analyzed smart grid substation systems based on IEC 61850 standards. Detected anomalies or malicious behaviors in multicast messages (e.g., GOOSE and SV) specified by IEC 61850.
  - Protocol analysis-based IDS combined with traffic analysis for more effective intrusion detection
  - Communication patterns defined in ICS protocols and specific business logic are used to extract detection rules

# Types of ICS-IDS

- **Protocol analysis-based**
  - Yusheng et al. introduced the SD-IDS algorithm for real-time deep inspection of Modbus TCP traffic. SD-IDS consists of rule extraction and deep inspection modules.
    - Rule extraction identifies semantic relationships among key fields in the Modbus TCP protocol.
    - Deep inspection detects anomalies or intrusions based on these relationships and real-time traffic data.

# Types of ICS-IDS

- **Traffic mining-based**
  - Protocol analysis-based IDS often struggle with detecting unknown attacks and parsing data packets efficiently
  - Traffic mining-based intrusion detection techniques aim to address these limitations
  - ICS environments exhibit fixed operation objects, static network topology, and limited applications
  - Normal ICS traffic remains relatively stable

# Types of ICS-IDS

- **Traffic mining-based**
  - Traffic mining-based IDS collects data from different regions within an ICS
  - Utilizes data mining (e.g., neural networks, Bayesian classifiers, support vector machines, decision trees) or data analysis (statistical analysis) techniques on collected data
  - Stavroulakis and Stamp's approach extracts five tuples (source IP, destination IP, transport protocol, source port, destination port). Also considers traffic duration and average time intervals between adjacent packets.

# Types of ICS-IDS

- **Traffic mining-based**
  - Hou et al. propose a method based on probabilistic principal component analysis (PCA) to detect abnormal traffic
    - Recognizes the impact of random burst traffic on PCA
    - Uses an Iterative Variational Bayesian algorithm to estimate model parameters
    - Abnormal traffic is detected based on rank changes
    - Effective in suppressing false alarms caused by random burst traffic
  - Artificial neural networks analyzes large volumes of data to identify unknown intrusions. Establish nonlinear mapping relationships between traffic features and system security states (normal/abnormal)

# Types of ICS-IDS

- **Traffic mining-based**
  - Vollmer and Manic extract various network traffic features (e.g., packet size, ICMP details, IP protocol data).
    - Construct input vectors for NN model training
    - Utilize the error backpropagation algorithm for model training
  - Vollmer and Manic propose a sliding window-based feature vector extraction technique
    - Dynamically and accurately extracts 16 network features, including IP addresses, packet counts, time intervals, window duration, data transmission speed, and more
    - Combines BP and LM methods for intrusion detection, achieving high accuracy

# Types of ICS-IDS

- **Control process analysis-based**
  - Control process analysis-based IDS capitalizes on the semantic information and unique characteristics of ICS
  - *Process Data Analysis-based*
    - Monitoring critical process data (e.g., reactor pressure, temperature, pH level) to assess the security status of a physical process.
    - Unexpected changes in process data can indicate intrusion attempts.

# Types of ICS-IDS

- **Control process analysis-based**
  - Krotofil et al. proposed a real-time attack algorithm designed for field devices
    - Uses run analysis to extract noise characteristics from the original value sequence of a process variable
    - Utilizes a triangle approximation technique to determine the dynamic nature of the value sequence
    - Generates a fake but plausible value sequence to replace true values
    - The detection method based on cluster entropy checks the consistency and rationality of the value sequence
    - Detects intrusion behaviors when consistency or rationality is violated

# Types of ICS-IDS

- **Control process analysis-based**
  - Hadž iosmanovic´ et al. designed an IDS method based on semantic analysis of process variables
    - Three-step approach: extracting current values, classifying variables into categories (constants, enums, continuous), and constructing behavioral models
    - Alarms are raised when actual behavior deviates from expected behavior predicted by the model
  - Carcano et al. developed a formal modeling language to describe control system states
    - Supports the Modbus protocol, extendable to other industrial protocols
    - Defines critical states, danger levels, and distance measurement between system states
    - Calculates proximity between the current state and critical states during detection
    - Raises alerts if the proximity exceeds a preset threshold

# Types of ICS-IDS

- **Control process analysis-based**
  - *Analyzing Control Commands*
    - Control commands play a crucial role in ICS, and adversaries may manipulate them to achieve attack objectives
    - Analyzing control commands helps identify intrusion behaviors in ICS
  - Carcano et al. proposed a novel IDS technology for power grids. Introduces a new language to describe control commands in power grids. Provides semantic descriptions for detection features.

# Types of ICS-IDS

- **Control process analysis-based**
  - *Single Packet Signature-based Strategy*
    - Detects illegal packets sent by PLCs or RTUs
    - Utilizes semantic analysis on control commands
  - *State-based Strategy*
    - Detects intrusions by monitoring the states of ICS
    - Invalid control commands often lead to critical system states
  - Lin et al. proposed a semantic analysis technique for control commands in distributed ICS. Forecasts consequences of control commands based on network and physical facilities knowledge. Reveals attackers' intentions by analyzing control commands' outcomes.

# Types of ICS-IDS

- **Control process analysis-based**
  - *Single Packet Signature-based Strategy*
    - Detects illegal packets sent by PLCs or RTUs
    - Utilizes semantic analysis on control commands
  - *State-based Strategy*
    - Detects intrusions by monitoring the states of ICS
    - Invalid control commands often lead to critical system states
  - Lin et al. proposed a semantic analysis technique for control commands in distributed ICS. Forecasts consequences of control commands based on network and physical facilities knowledge. Reveals attackers' intentions by analyzing control commands' outcomes.

# Types of ICS-IDS

- **Control process analysis-based**
  - *Physical Model-Based IDS*
    - Physical models accurately describe the evolution of an industrial control system
    - These models predict expected system outputs, which are compared with observed outputs for intrusion detection
  - Cardeñas et al. constructed a linear state-space model for ICS. The model considers the system's current state, previous states, and control inputs.
  - *Sequence-Based Detection*: Detects anomalies quickly by determining the minimum sequence length for a judgment.

# Types of ICS-IDS

- **Control process analysis-based**
  - *Change-Based Detection*: Detects transitions from normal to abnormal states based on predefined thresholds for residuals or accumulated residuals.
  - Edelmayer et al. created an equivalent linear time-invariant representation of the original time-varying control system. Developed a detection filter based on this representation.
  - Urbina et al. studied methods to limit the impacts of stealthy attacks. Proposed a novel metric to measure the impacts of these attacks

# Types of ICS-IDS

- **Process-oriented**
  - Focus on monitoring the underlying process in the control system rather than monitoring network traffic
  - Intrusion Detection methods
    - Model process variable excursions beyond their appropriate ranges using machine-learning techniques
    - Another method requires plant personnel input to define critical process variable limits

# Types of ICS-IDS

- **Process-oriented**
  - Semantic Security Monitoring (SSM) uses analysis of control-bus traffic messages to construct a 3rd copy of the plant-PLC registers to detect events that suggest that plant operations may be out of specification, out of compliance, or out of a desired safety range

# References


- Kaouk, M., Flaus, J. M., Potet, M. L., & Groz, R. (2019, April). A review of intrusion detection systems for industrial control systems. In *2019 6th International Conference on Control, Decision and Information Technologies (CoDIT)* (pp. 1699-1704). IEEE.

- Colbert, E. J., & Hutchinson, S. (2016). Intrusion detection in industrial control systems. *Cyber-security of SCADA and other industrial control systems*, 209-237.

- Hu, Y., Yang, A., Li, H., Sun, Y., & Sun, L. (2018). A survey of intrusion detection on industrial control systems. *International Journal of Distributed Sensor Networks*, *14*(8), 1550147718794615.