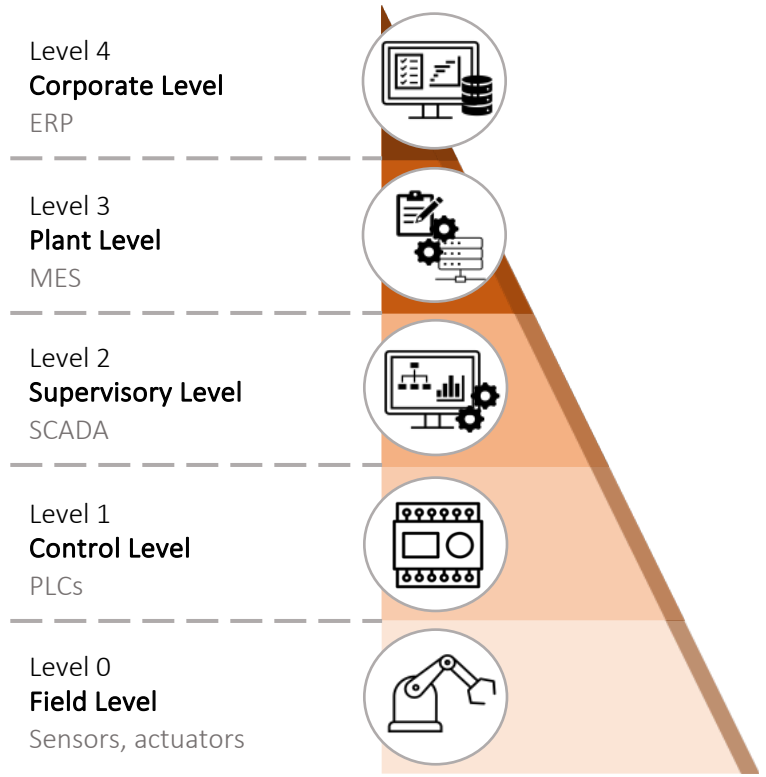
ICS Protocols Anomaly Behavior Analysis: ENIP

Outline

- Overview of Industrial Control Systems
- ICS Protocols
- EtherNet/IP Protocol
- Anomaly Behavior Analysis of ENIP

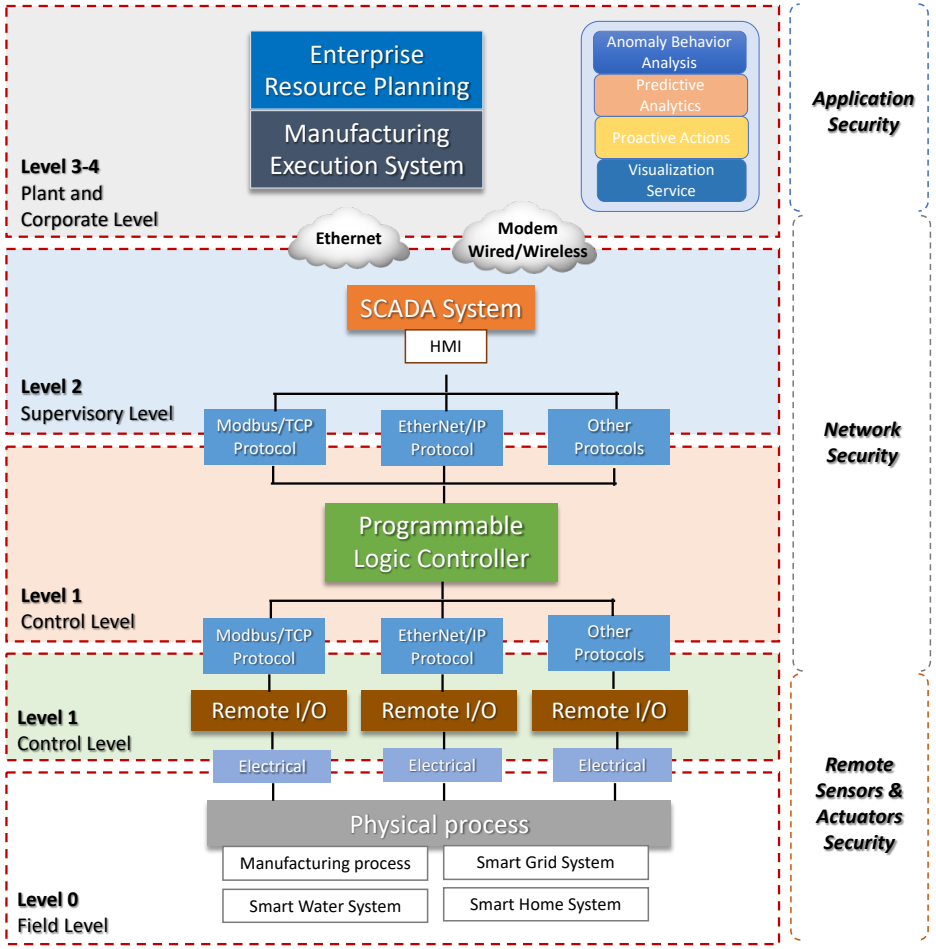
Overview of Industrial Control Systems

- Industrial Control Systems are integrated systems used to control and manage industrial processes, machinery, and critical infrastructure
- ICS primarily performs control, monitoring, and automation tasks to enhance efficiency, reliability, and safety
- Consists of hardware (sensors, PLCs, RTUs) and software (SCADA, HMI) elements



Overview of Industrial Control Systems

- The Purdue Model is a hierarchical network architecture for ICS, originally developed by Purdue University
- It provides a structured approach to secure and manage ICS networks by segmenting them into zones based on their function and security requirements



ICS Protocols

- ICS protocols are communication standards used in industrial automation and control systems
- Designed to be reliable, efficient, and secure in harsh industrial environments
- ICS protocols must be able to operate in real time with minimal latency, and be resistant to noise and interference

Common Industrial Protocols

- **Modbus**
  - Widely used, open-source protocol for communication between PLCs and other devices
  - Master-slave protocol, where a single master device polls multiple slave devices for data
  - Modbus RTU (Serial), Modbus TCP/IP (Ethernet-based)

- **EtherNet/IP** (IP: Industrial Protocol)
  - Uses Ethernet to communicate between PLCs and other devices
  - It is based on the Common Industrial Protocol (CIP)

Common Industrial Protocols

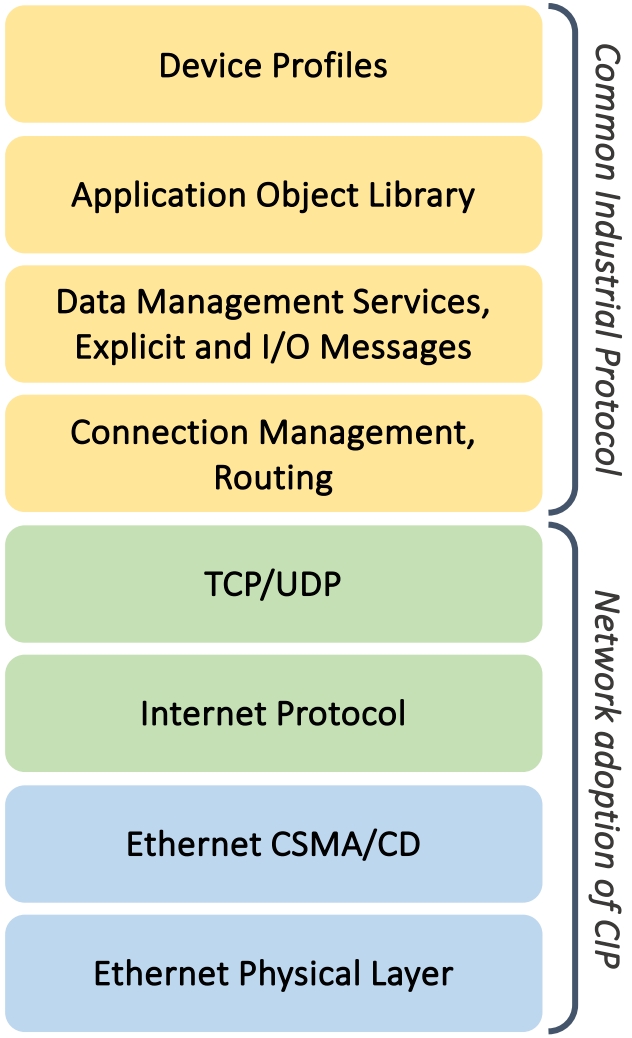
- **PROFINET**
  - Open Industrial Ethernet standard developed by PROFIBUS International
  - Based on Ethernet

- **DNP3** (Distributed Network Protocol 3)
  - Its main use is in utilities such as electric and water companies
  - Developed for communications between various types of data acquisition and control equipment

EtherNet/IP (ENIP)

EtherNet/IP

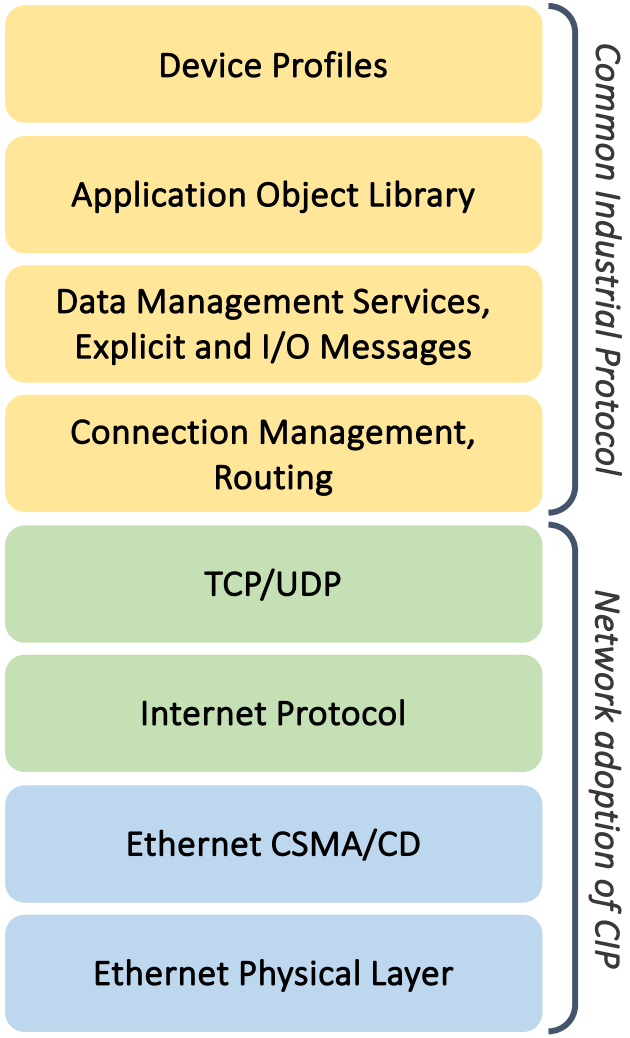
- ENIP adapts the Common Industrial Protocol (CIP) for standard Ethernet (IEEE 802.3) combined with the TCP/IP suite
- Improves connectivity, efficiency, productivity, and flexibility in industrial applications
- ENIP follows the Open Systems Interconnection (OSI) model
- Implements CIP from the session layer to the application layer



EtherNet/IP

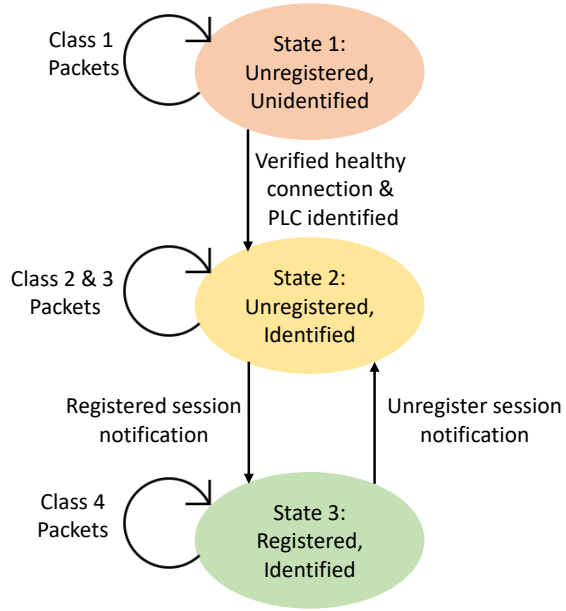
- ENIP defines two forms of messaging:
  - Unconnected: Used for infrequent, low-priority messages, often in the session establishment process
  - Connected: Utilized for frequent explicit messages or real-time I/O data transfers

- Within connected messages, there are two types of connections:
  - Explicit
  - Implicit (I/O Data



EtherNet/IP State Machine

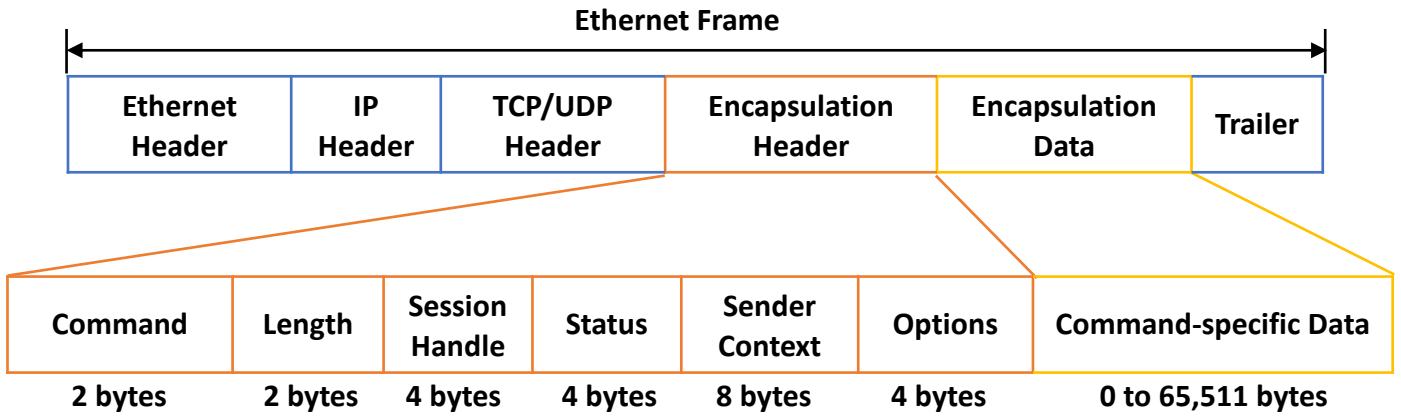
- ENIP is composed of three primary states
  - **Unregistered and Unidentified**: The device has not been identified and has not initiated a session
  - **Unregistered and Identified**: The device has been identified
  - **Registered and Identified**: The device is identified and has successfully created a session, enabling the exchange of more messages



Class 1: • Echo (0x0001): Verify healthy connection
Class 2: • List Services (0x0004): List of available services • List Identity (0x0063): PLC information • List Interfaces (0x0064): List of network interfaces
Class 3: • Register Session (0x0065): Register/Unregister PCCC session • Send RR Data (0x006f): Unconnected data message (e.g. Forward Open/Close CIP commands)
Class 4: • Send Unit Data (0x0070): Connected data message (e.g. Read/Write CIP commands)

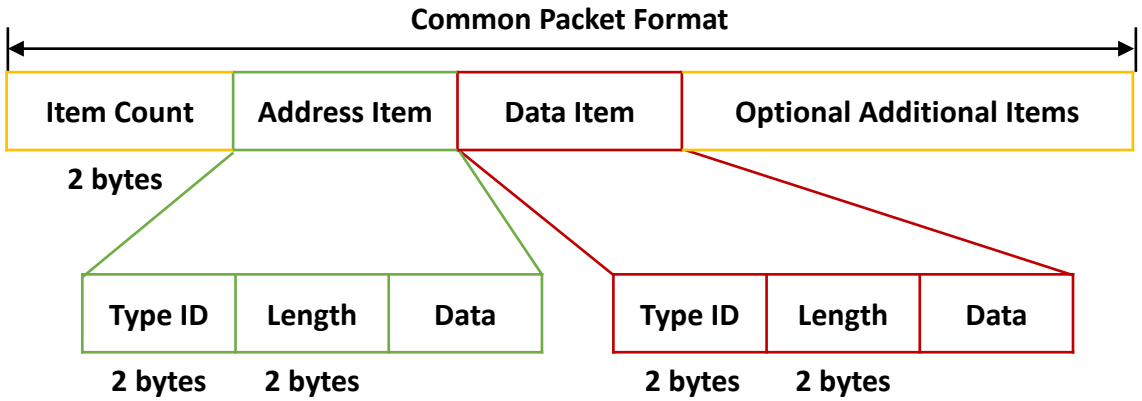
ENIP Frame Structure

- CIP-related data is enclosed within the encapsulation header and encapsulation data
- The following are the most relevant commands
  - List Identity
  - Register/Unregister Session
  - Send RR Data
  - Send Unit Data



ENIP Frame Structure

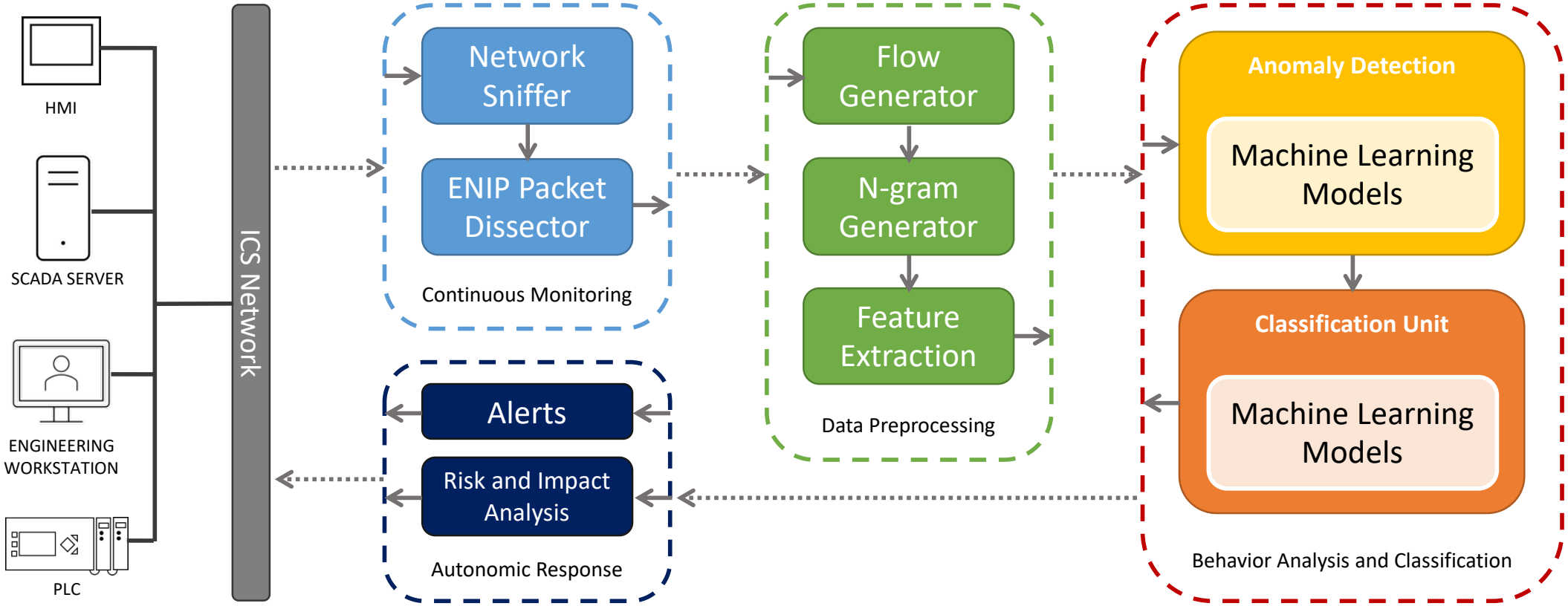
- The Common Packet Format allows for encapsulating multiple items within a single frame
- This efficiency simplifies the transmission of various pieces of information
- The Data Item frame contains essential information, including:
  - CIP Service
  - Command-Specific Data
  - Specification Values



Anomaly Behavior Analysis of the ENIP Protocol

Clarisa Grijalva | University of Arizona

ENIP IDS Architecture

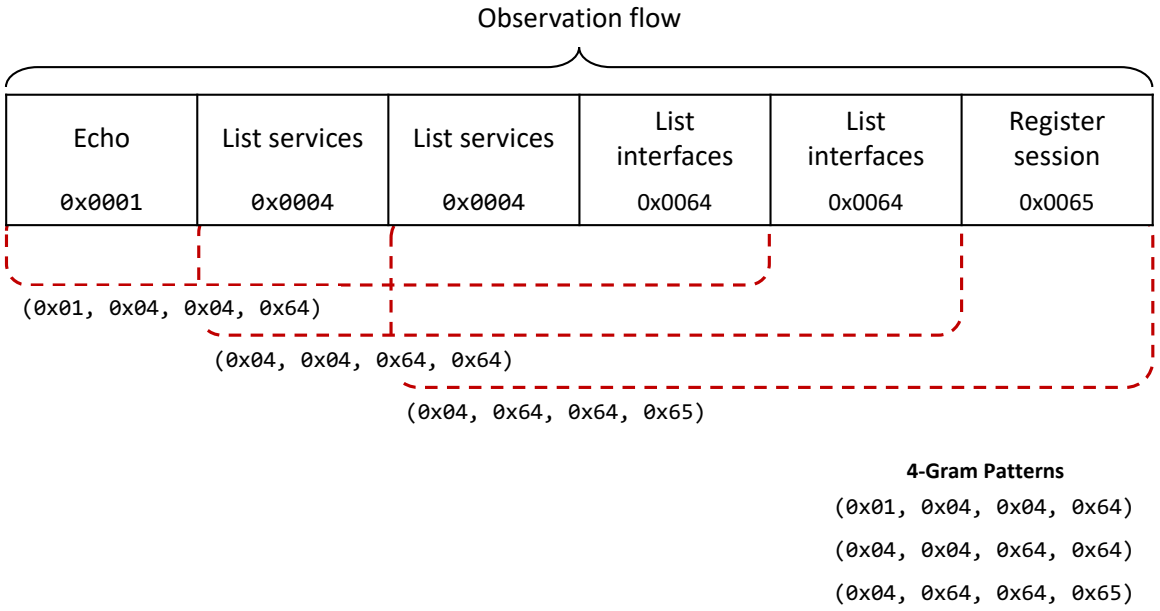


ENIP IDS Modules

- **Continuous monitoring**
  - The IDS will continuously inspect the traffic on the ICS network
  - This module also selects the specific data that will be used in the next modules

ENIP IDS Modules

- **Data preprocessing**
  - The data is split into observation flows, from which the n-grams are obtained, then feature extraction is performed



Flow probability	List interfaces ratio
Total packets in flow	Register session ratio
New n-grams in flow	Send RR data ratio
New n-grams found	Send unit data ratio
Echo ratio	List identity ratio
List services ratio	Others ratio

Features obtained for the ML algorithms

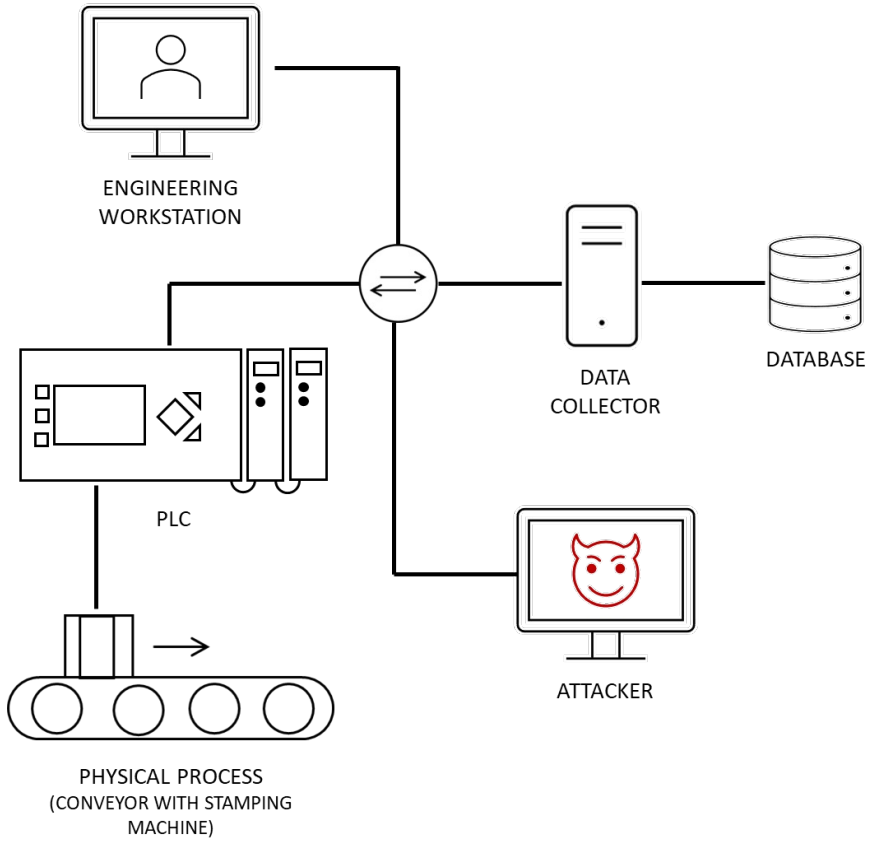
ENIP IDS Modules

- **Behavior analysis and classification**
  - The features obtained are passed to the behavior detection model, if the result is an anomaly, then it's passed to the second model to determine the type of attack
  - The results go to the management engine for analysis

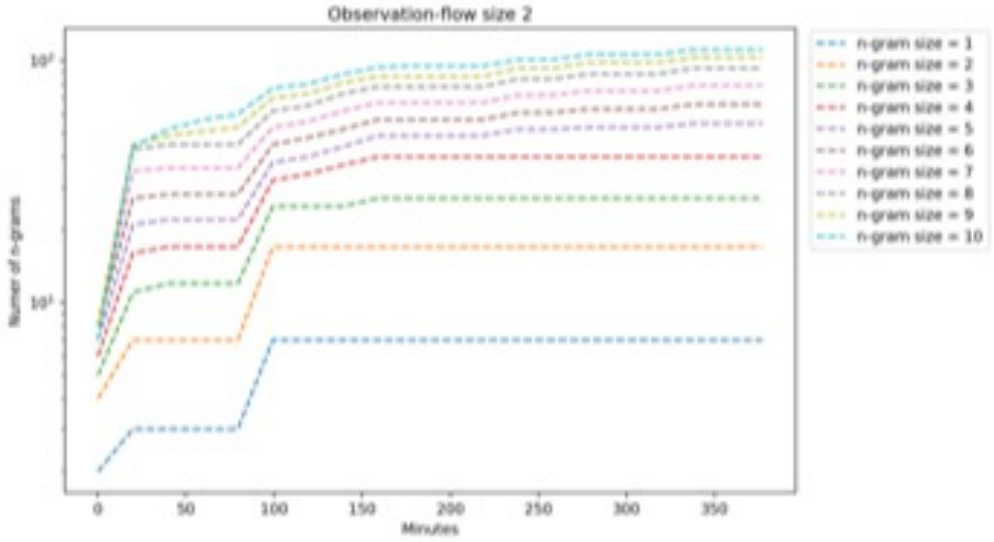
- **Autonomic response**
  - Provides insight into the results of the behavior module, alerts of anomalies, recommends mitigation strategies and provides a risk and impact analysis

Experimental Setup

- Types of attacks
  - Denial of service
  - Data injection
  - I/O Force
  - Program download



Experimental Results



N-grams for normal behavior