Mondragon Unibertsitatea

Faculty of Engineering

Null is Not Always Empty:

Monitoring the Null Space for Field-Level Anomaly Detection in Industrial IoT Environments

E. Zugasti[1], M. Iturbe[1], I. Garitano[1], U. Zurutuza[1]

[1] Data Analytics and cybersecurity team, Faculty of Engineering, Mondragon University

Agenda

Mondragon Unibertsitatea
Faculty of Engineering

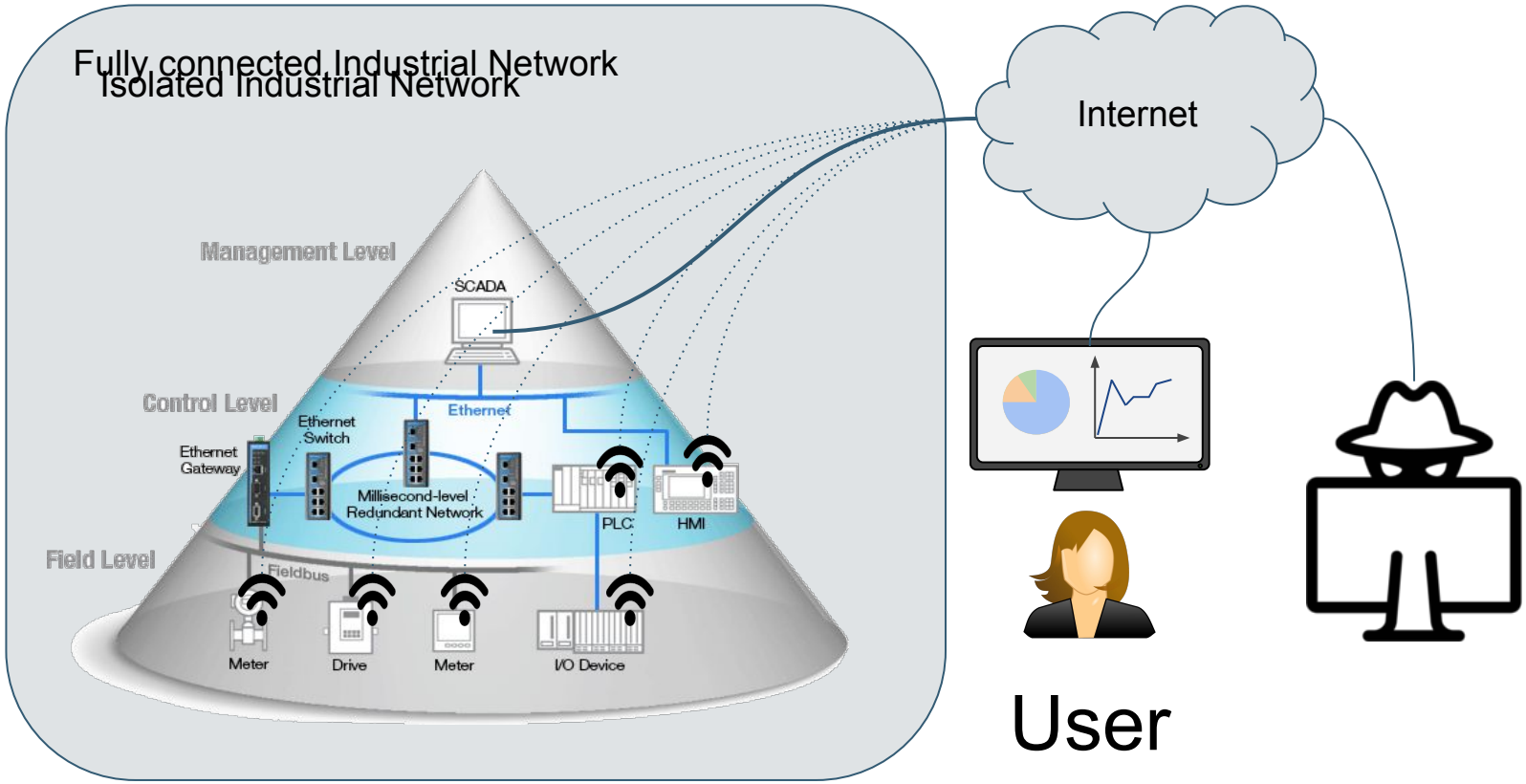
1. Introduction
2. Null Space Anomaly Detection
3. Use Case: Tennesse-Eastman
4. Results
5. Conclusions

1

Introduction

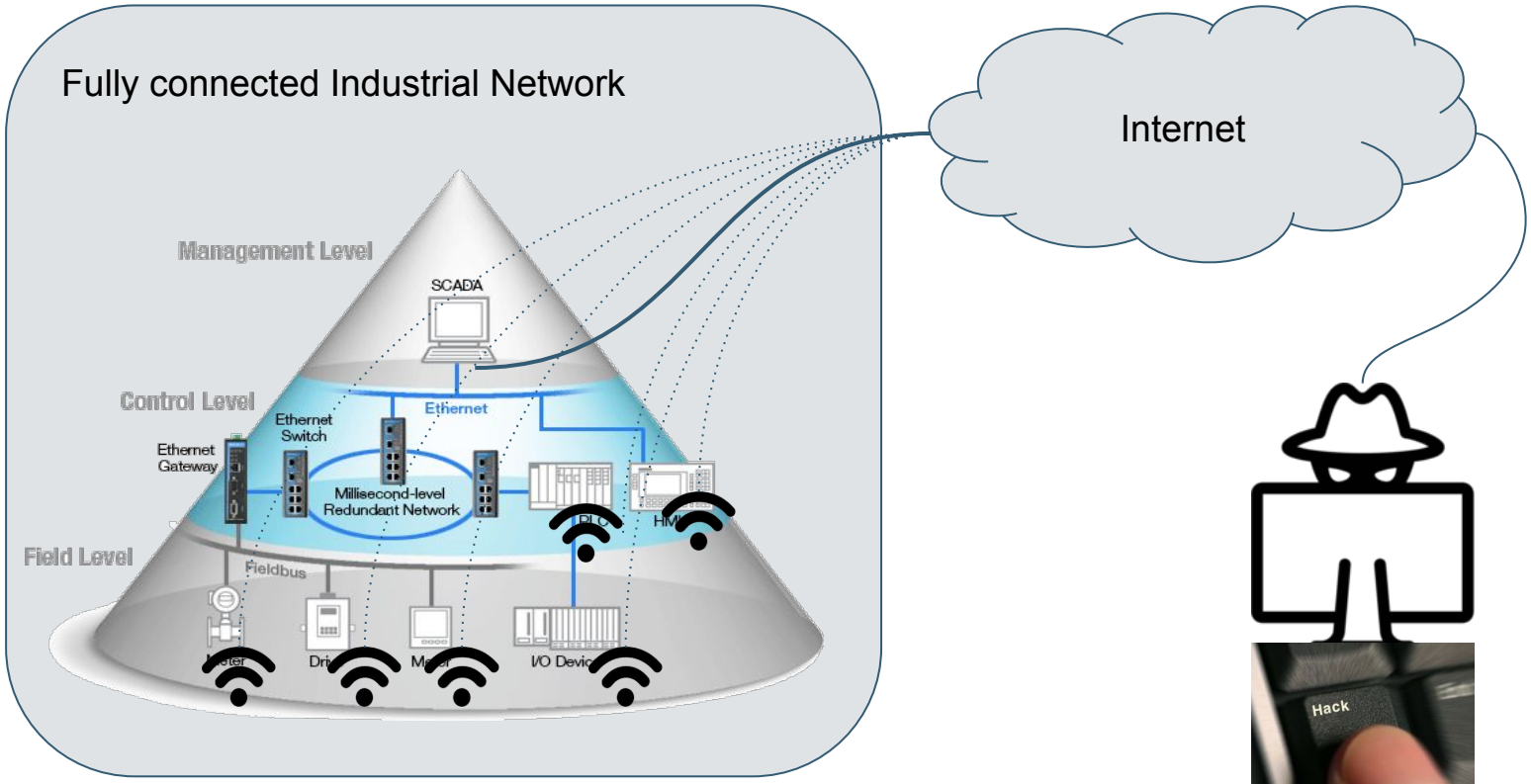
Industrial Networks

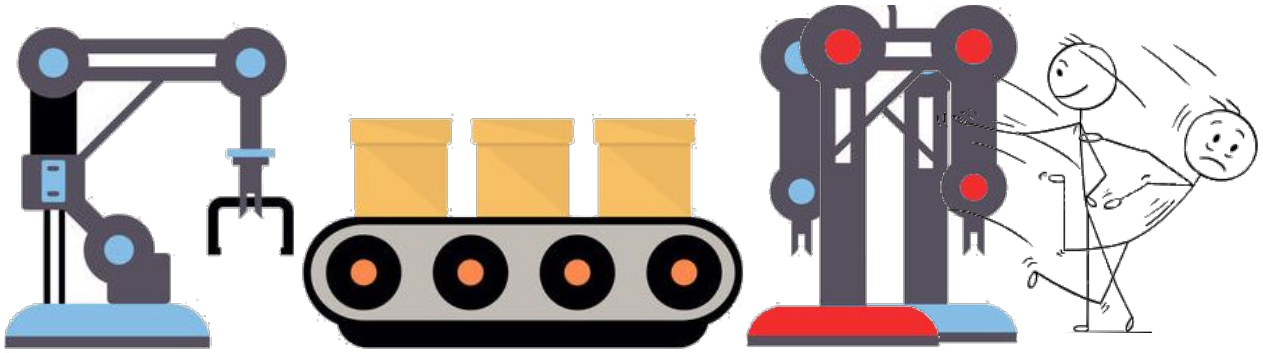
Mondragon Unibertsitatea
Faculty of Engineering



Process Control

Mondragon Unibertsitatea
Faculty of Engineering

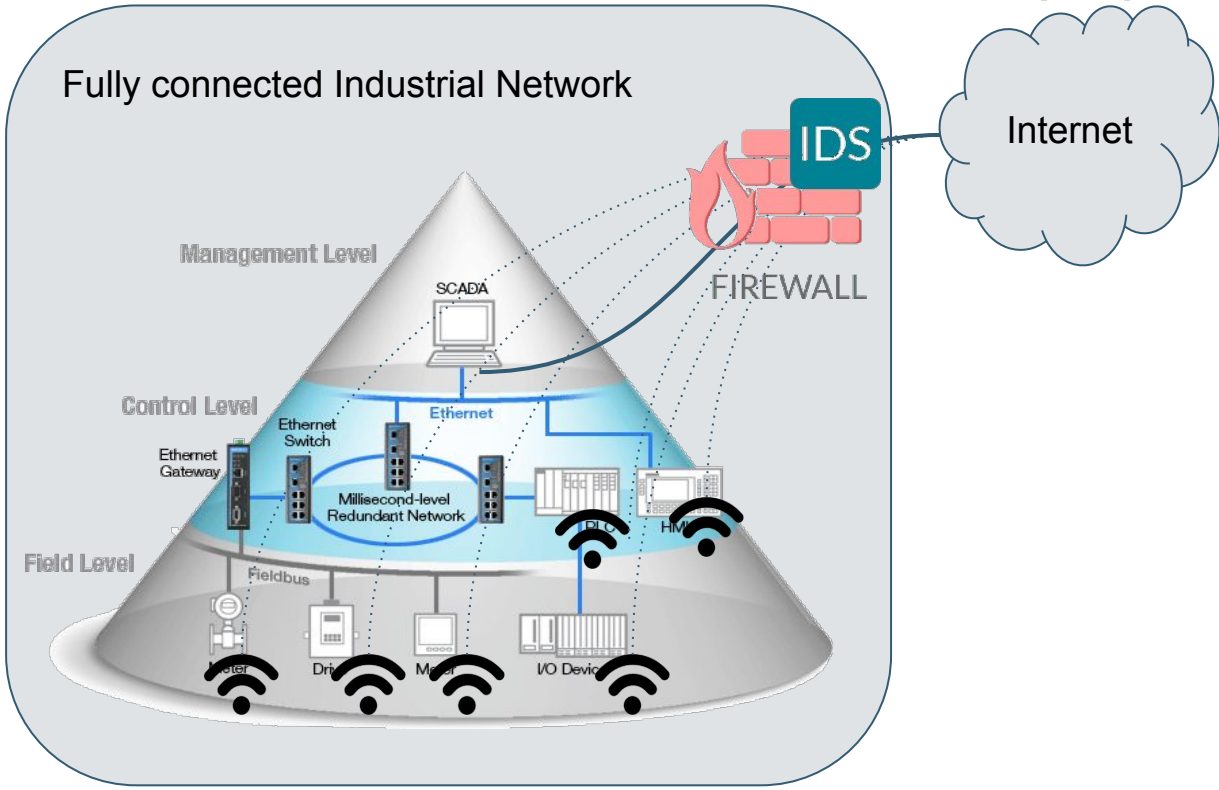




Intrusion Detection System

Mondragon Unibertsitatea
Faculty of Engineering

1. Signature Based IDSs
2. Anomaly Detection Systems (ADS)



This work

Mondragon Unibertsitatea
Faculty of Engineering

We present an **Anomaly Detection System that monitors physical quantities** of the process itself **to detect intrusions at field-level** that can lead to a unwanted activity within the monitored process

2

Null Space Anomaly Detection

Null Space Anomaly Detection

Mondragon Unibertsitatea
Faculty of Engineering

- Multivariate anomaly detection system
- Validated in fields like *Structural Health Monitoring*
- Based in Stochastic Subspace Identification[1]
- Uses time series measured in the process as input

$$\boldsymbol{Y} = [\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_m]$$

- Covariance Driven Hankel Matrix transform

$$\boldsymbol{H}_{p,q} = \begin{bmatrix} \boldsymbol{\Lambda}_1 & \boldsymbol{\Lambda}_2 & \boldsymbol{\Lambda}_2 & \ldots & \boldsymbol{\Lambda}_q \\ \boldsymbol{\Lambda}_2 & \boldsymbol{\Lambda}_3 & \ldots & \ldots & \vdots \\ \boldsymbol{\Lambda}_3 & \ldots & \ldots & \ldots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \boldsymbol{\Lambda}_{p+1} & \ldots & \ldots & \ldots & \boldsymbol{\Lambda}_{p+q} \end{bmatrix}$$

$$\boldsymbol{\Lambda}_i = \left(\frac{1}{N-i-1}\right) \sum_{k=1}^{N-i} \boldsymbol{y}_{k+i} \boldsymbol{y}_k^t$$

[1] P. Van Overschee and B. De Moor, *Subspace identification for linear systems: Theory–Implementation–Applications.* Springer Science & Business Media, 1996.

Null Space Anomaly Detection

Mondragon Unibertsitatea
Faculty of Engineering

- Hankel Matrix → System identification (*Control Theory)*
- For **ADS**, we do not need to identify the system
- We use **Singular Value Decomposition** on Hankel Matrix
- and find the **Null Space (U_{H0})**

SVD decomposition of H

$$H_{p,q} = U_H S_H V_H^t$$

U_{H0} property

$$U_{H0}^t H_{p,q} = 0$$

- Null hypothesis & Residual:

NullSpace Residual

The Residual Matrix is defined:

$$R_{i,j} = U_{H0}^t H_{i,j}$$

- $R_{i,j} = 0$, Healthy State
- $R_{i,j} \neq 0$, Abnormal State

Null Space Anomaly Detection

Mondragon Unibertsitatea
Faculty of Engineering

- Algorithm
  - Learning phase: (NOC datasets)
    - extract Null Space
    - Calculate Residual values for NOC datasets
    - Threshold Calculation
  - Detection phase:
    - Calculate Residuals
    - check whether they are still under the threshold
- Residuals ≈ Anomaly Indicators (AI)[1]

[1] E. Zugasti, A. G. González, J. Anduaga, M. A. Arregui, and F. Martínez, "Nullspace and autoregressive damage detection:a comparative study," Smart Materials and Structures, vol. 21,no. 8, p. 085010, 2012.

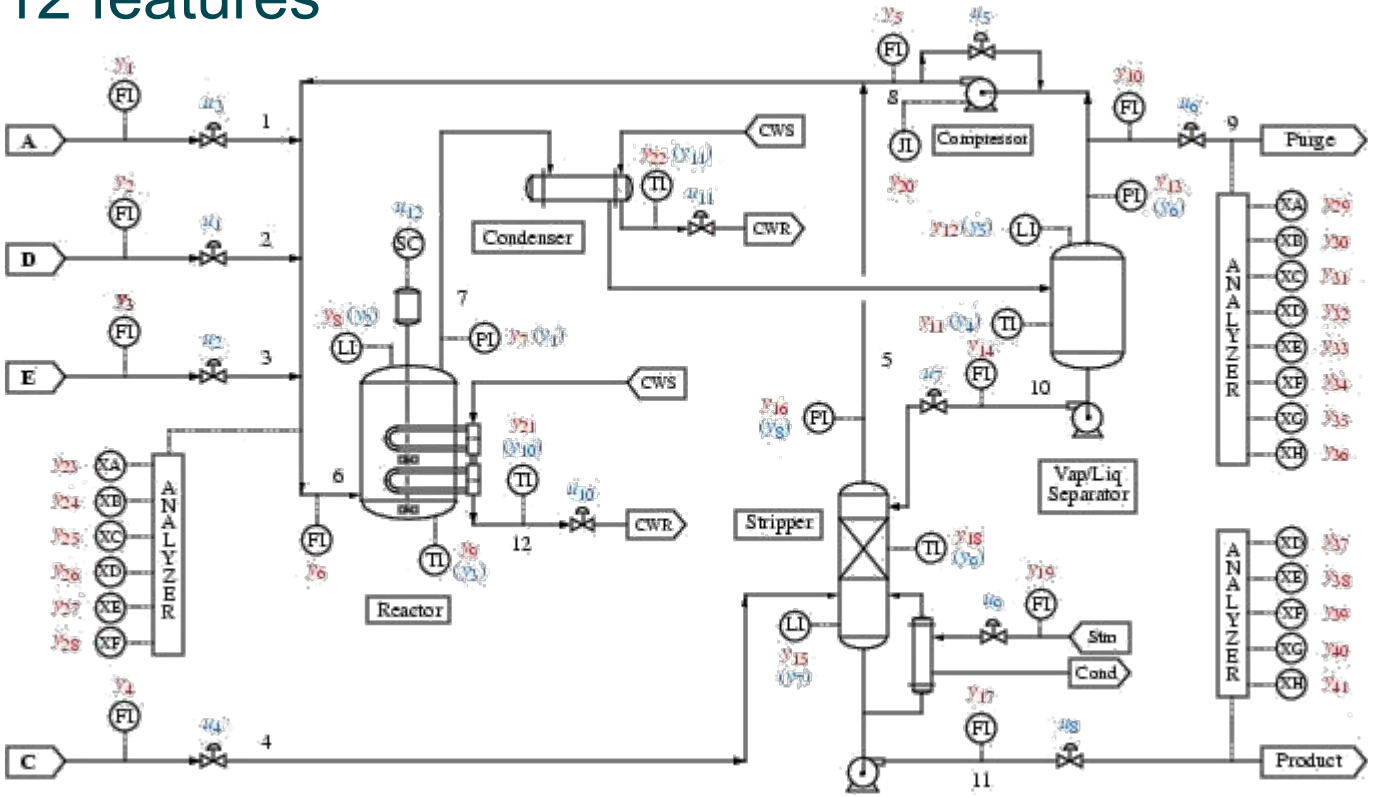
3

Use Case: Tennessee Eastman

Tennessee Eastman Process

Mondragon Unibertsitatea
Faculty of Engineering

- Chemical Process[1]
- From 4 gaseous reactants → 2 liquid products
- 41 + 12 features



[1] J. J. Downs and E. F. Vogel, "A plant-wide industrial process control problem," Computers & Chemical Engineering,vol. 17, no. 3, pp. 245–255, 1993.

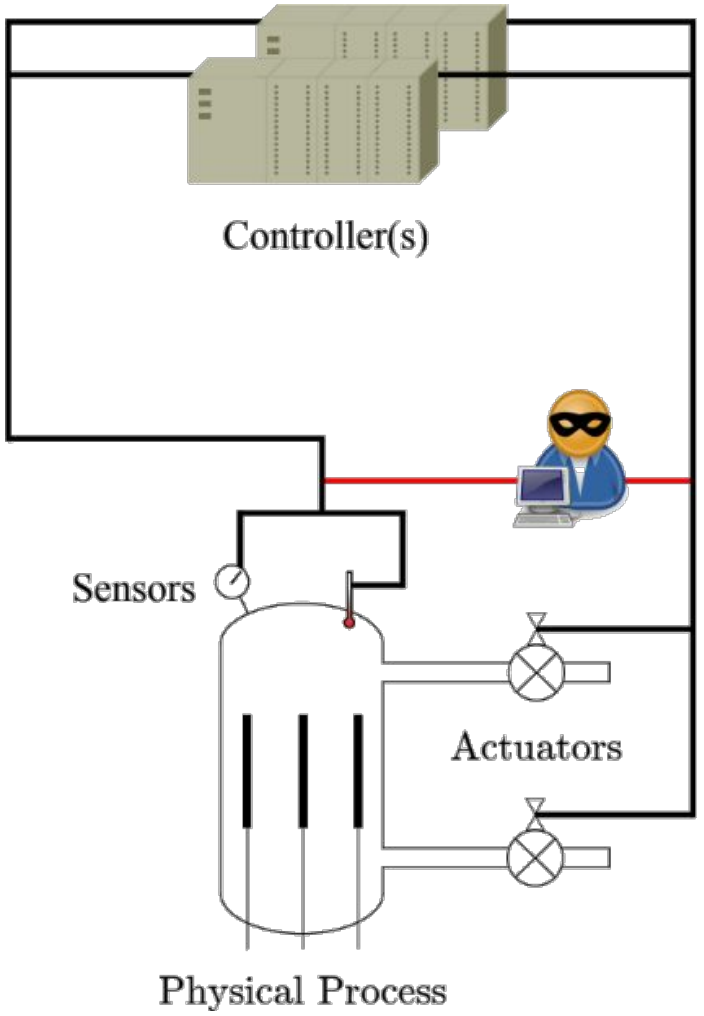
Attack model

Mondragon Unibertsitatea
Faculty of Engineering

- Integrity attack:
  - time series injection
- DoS attack
  - Communication stop
- Performed attacks

Variable number	Variable name	Attack type
XMEAS1	A feed (stream 1)	Integrity
XMEAS8	Reactor level	Integrity
XMEAS9	Reactor temperature	Denial of Service
XMEAS14	Product Separator underflow (stream 10)	Denial of Service
XMEAS17	Stripper underflow (stream 11)	Integrity

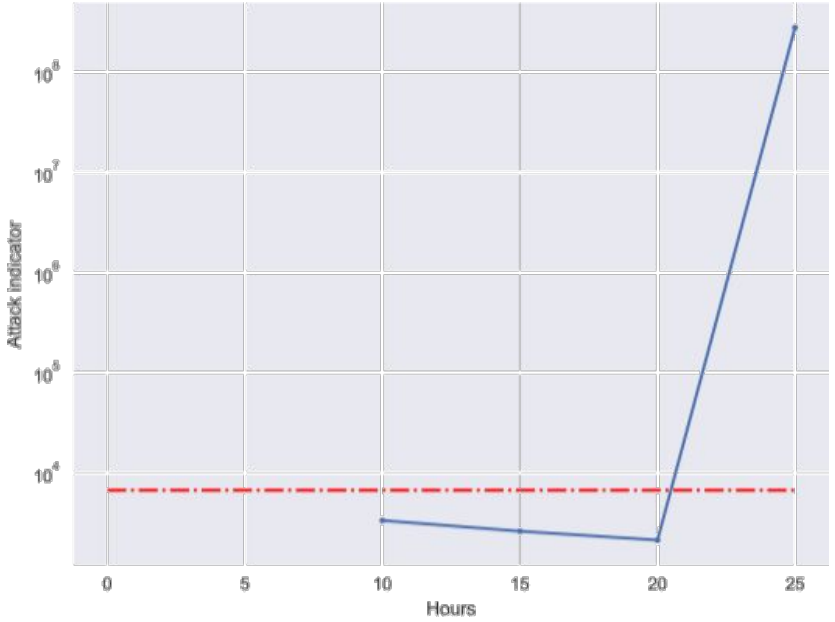
- Simulation time: 72H
  - attack starts after 24H
- Fs=0.027 Hz

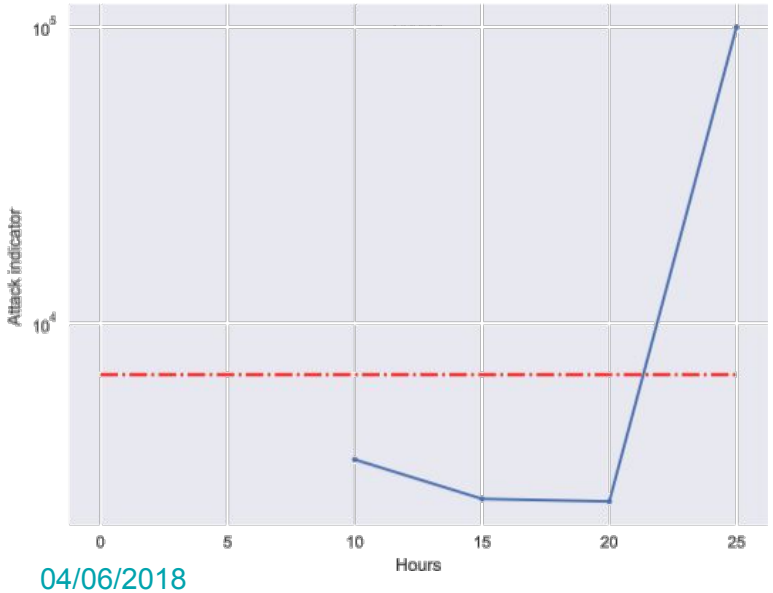


4

Results

Integrity attack results

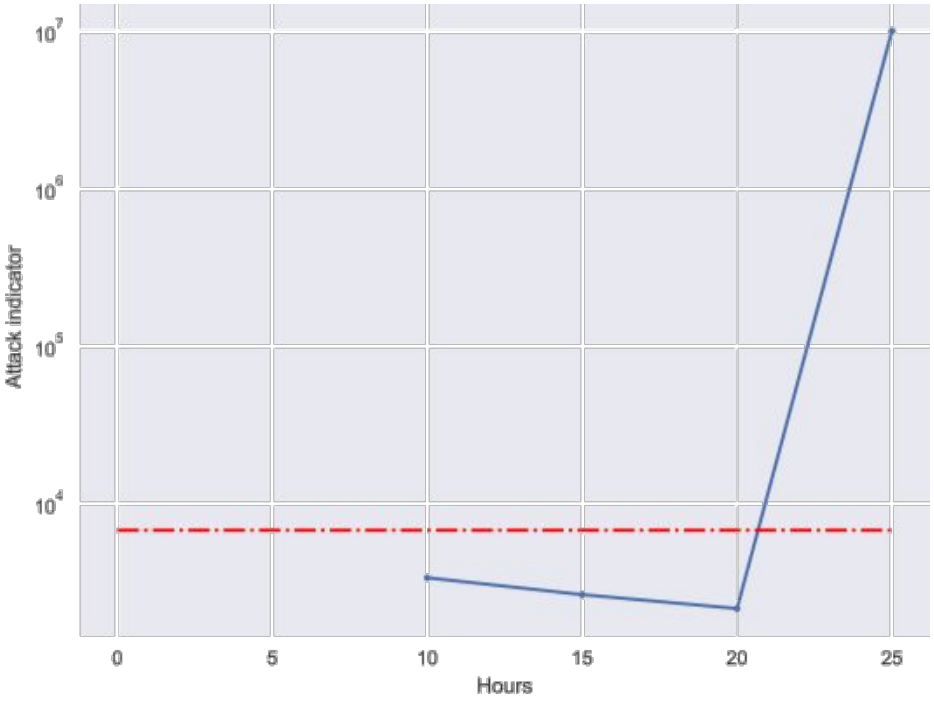


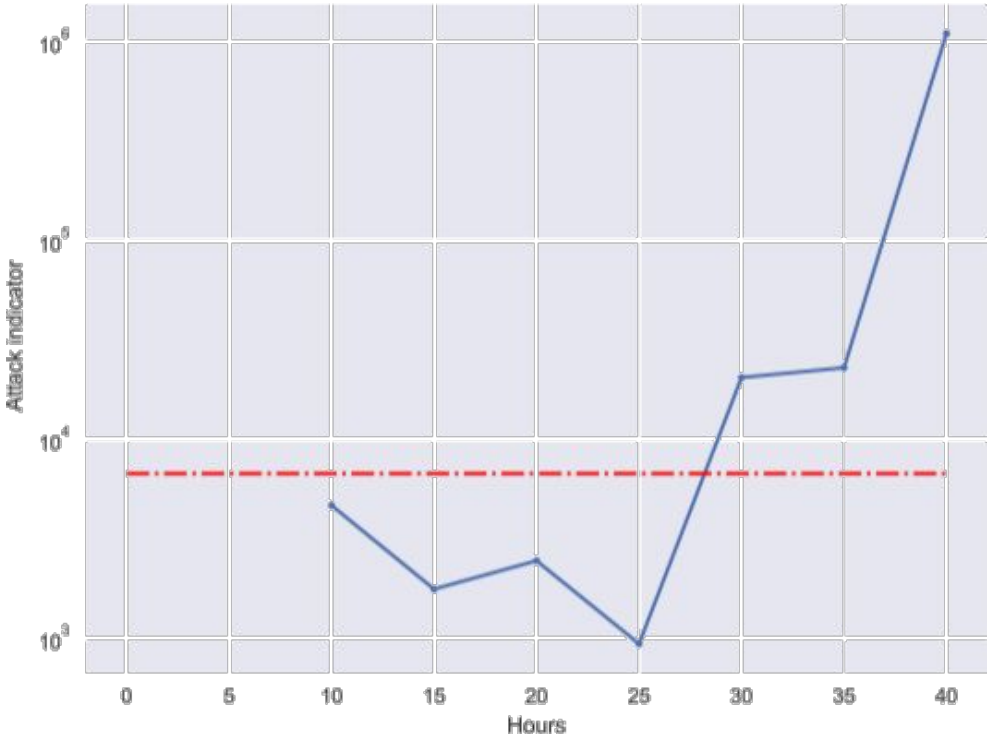


Variable number	Variable name
XMEAS1	A feed (stream 1)
XMEAS8	Reactor level
XMEAS17	Stripper underflow (stream 11)

DoS attack results

Mondragon Unibertsitatea
Faculty of Engineering





Variable number	Variable name
XMEAS9	Reactor temperature
XMEAS14	Product Separator underflow (stream 10)

5

Conclusions

Conclusions

Mondragon Unibertsitatea
Faculty of Engineering

- **Attack detection** in IIoT is still an **open challenge**
- We **present** an **ADS** that **detects field-level anomalies**
- The ADS computes an **Attack Indicator**
- **Approach validated** with Tennesee-Eastman process
  - Integrity attacks
  - DoS attacks

Future Work

Mondragon Unibertsitatea
Faculty of Engineering

- Preprocessing data to have a more sensitive method
  - Normalize the inputs
  - Feature transformation methods
- Sliding-window approach for a faster detection
- Add network-level variables to the ADS
- Use more validation scenarios

Acknowledments

Mondragon Unibertsitatea
Faculty of Engineering

This work has been partially funded by the **PRODUCTIVE 4.0 project**. The project has received funding from the Electronic Component Systems for European Leadership (**ECSEL**) Joint Undertaking under grant agreement No. 737459. This Joint Undertaking receives support from the **European Union's Horizon 2020 Research and Innovation Programme** and the **Spanish Ministry of Economy, Industry and Competitiveness.** It has been developed by the Intelligent Systems for Industrial Systems group, supported by the Department of Education, Language Policy andCulture of the **Basque Government**.

Mondragon Unibertsitatea

Faculty of Engineering

Eskerrik asko

Muchas gracias

Thank you

Ekhi Zugasti
ezugasti@mondragon.edu

Loramendi, 4. Apartado 23
20500 Arrasate – Mondragon
T. 943 71 21 85
info@mondragon.edu