MONDRAGON UNIBERTSITATEA

GOI ESKOLA POLITEKNIKOA

FACULTY OF ENGINEERING

On the Feasibility of Distinguishing Between Process Disturbances and Intrusions in Process Control Systems using Multivariate Statistical Process Control

M. Iturbe[1], J. Camacho[2], I. Garitano[1], U. Zurutuza[1], R. Uribeetxeberria[1]

[1]Electronics & Computing Department, Faculty of Engineering, Mondragon University
[2]Department of Signal Theory, Telematics and Communications – CITIC, University of Granada

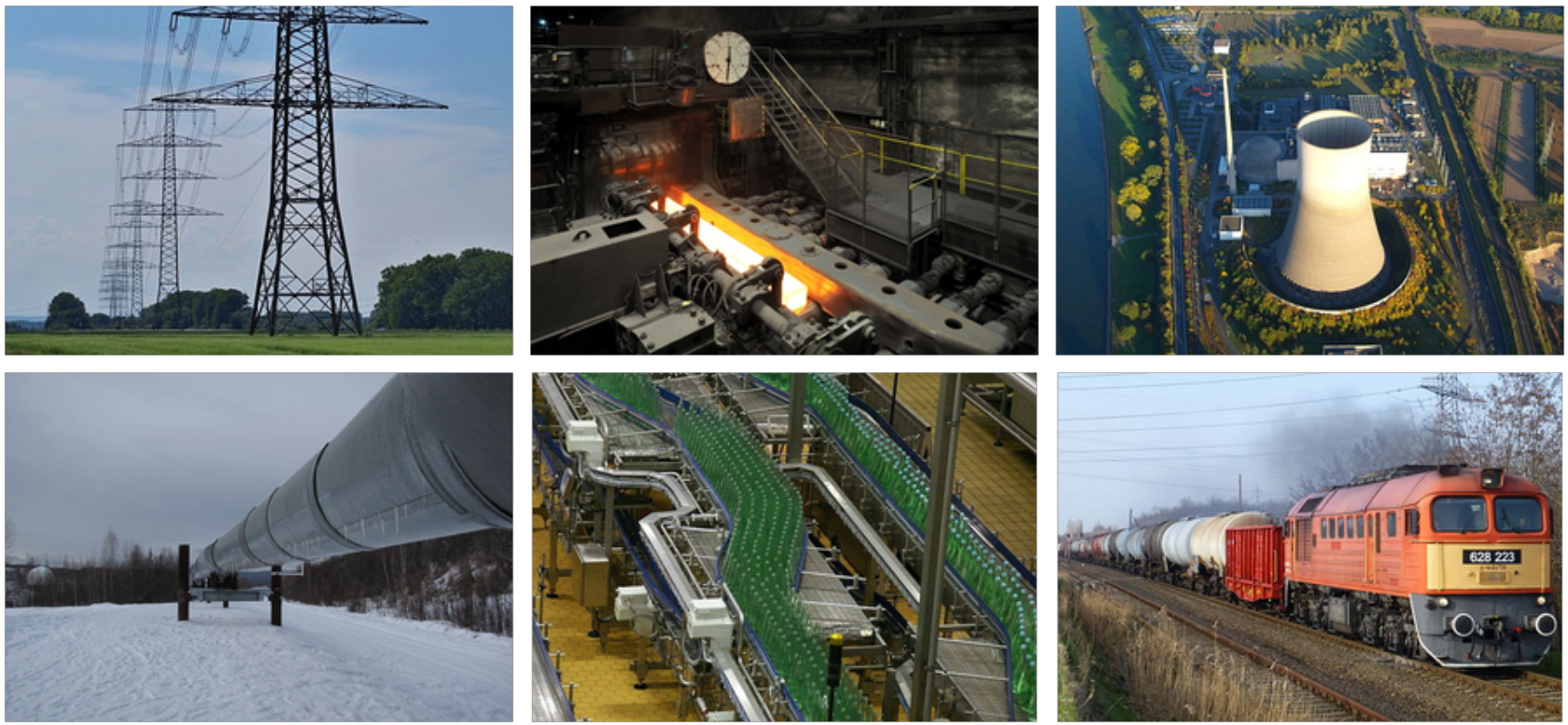
ReSA4CI 2016, Toulouse, France

Agenda

1. Introduction
2. Related Work
3. Multivariate Statistical Process Control
4. Proposed approach
5. Results
6. Conclusions
7. Future work

Introduction

Process Control Systems



PCS vs. IT

	Industrial Networks	IT Networks
Main Purpose	Control of Physical equipment	Data processing and transmission
Failure Severity	High	Low
Reliability Required	High	Moderate
Determinism	High	Low
Data Composition	Small packets of periodic and aperiodic traffic	Large, aperiodic packets
Average Node Complexity	Low (simple devices, sensors, actuators)	High (large servers/file systems/databases)

Related Work

Related Work

ADS research for PCSs is a popular research area.

- Network-level ADSs
- Process-level ADSs

Related Work

Gaps in current process-level ADSs:

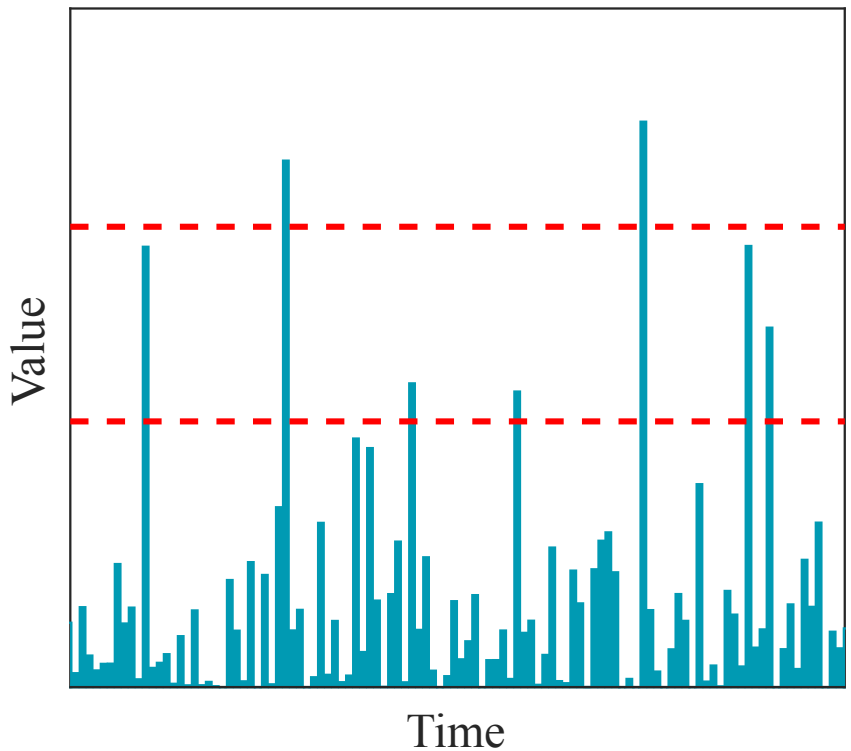
- Require detailed model of the process. [2, 3]
- Ignore process disturbances. [1]

MSPC

Statistical Process Control

- Process Monitoring Methodology for detecting and diagnosing process faults
- Statistical control
- Control Charts

Control Chart



PCA-based MSPC

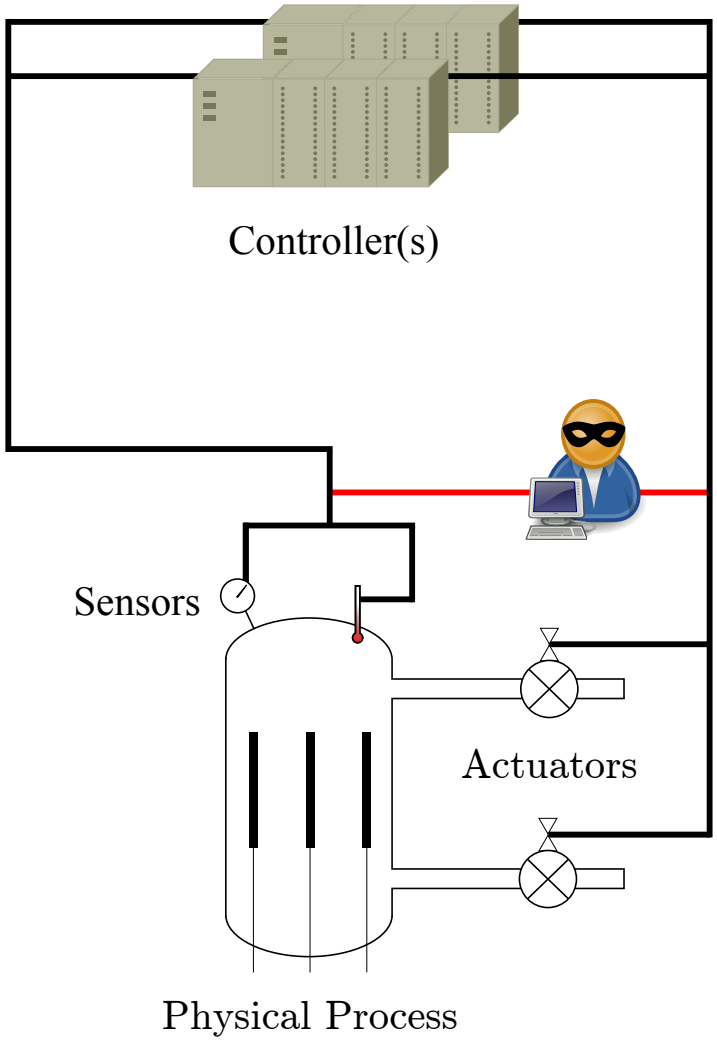
- An extension of SPC
- PCA transforms the original variable space into a new one:

$$X = T_A P_A^t + E_A$$

- Two statistics to be monitored
  - T^2 or *d-statistic*
  - *SPE* or *q-statistic*
- Control charts for these statistics
  - When an anomaly is detected, contribution plots to detect the cause.

Proposed approach

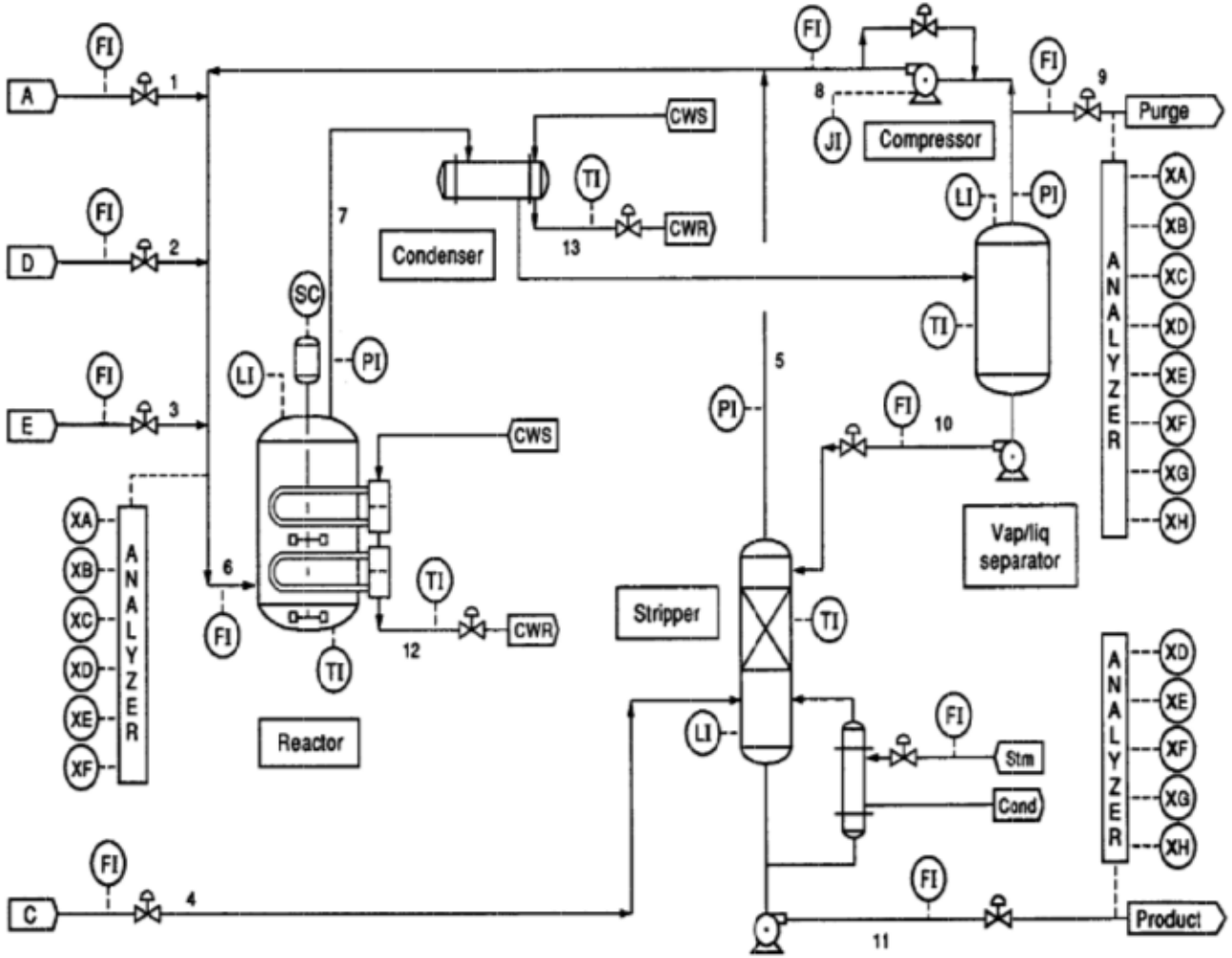
Attack model



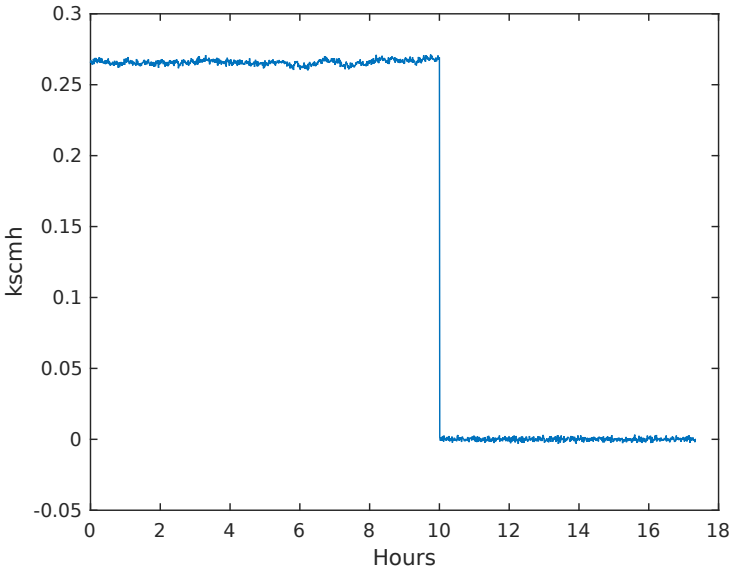
Tennessee-Eastman

- Chemical process
- Presented by Downs and Vogel
- Originally a control algorithm benchmark
- 41 XMEAS, 12 XMV, 20 IDV

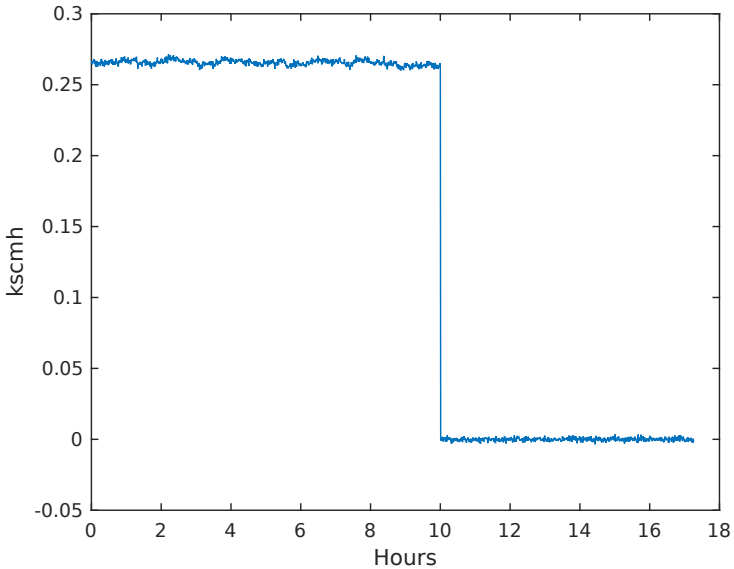
Tennessee-Eastman



Attack and disturbance



(a) IDV(6)



(b) Attack on XMV(3)

Adversary modelling

- Integrity attacks
- DoS attacks

Results

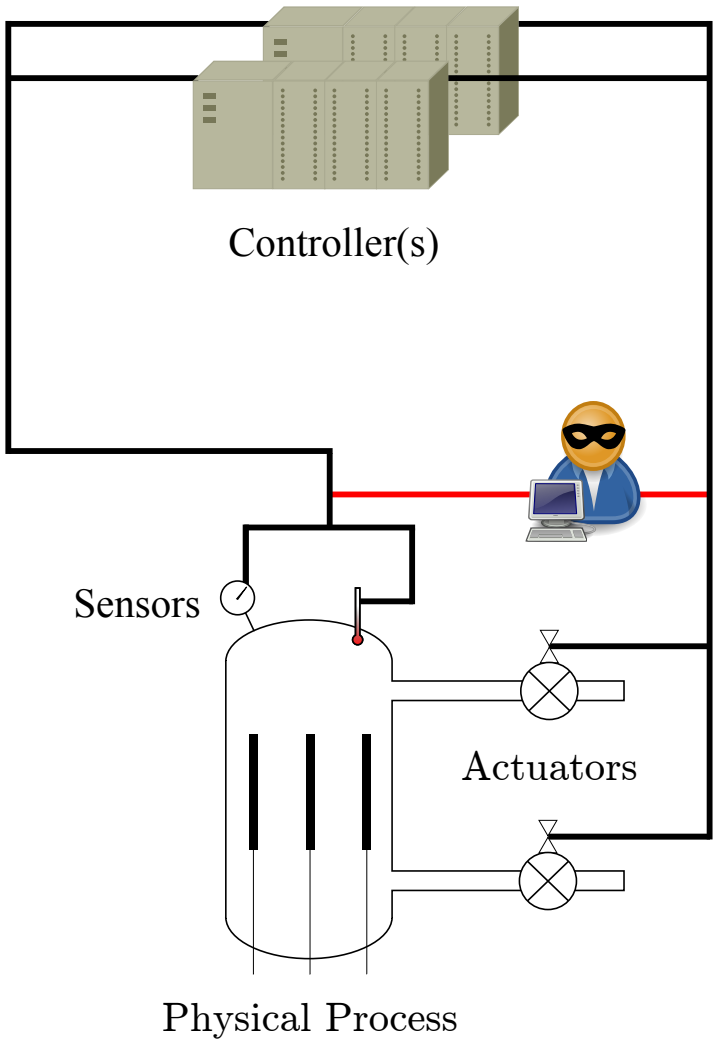
Experimental Results

- Tools
  - DVCP-TE
  - MEDA toolbox
- Runs
  - 72 h. simulations
  - 30 runs for calibration, 10 per anomaly
  - Record values 2000 times per hour

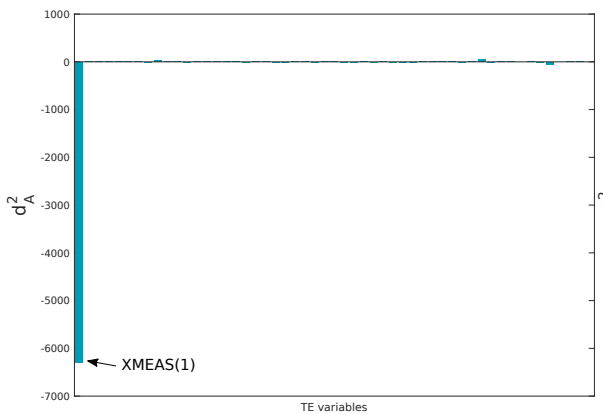
Phases

- Phase I: Model building
  - Calibrate the model, establish control limits for D and Q statistics
- Phase II: On-line monitoring
  - Check if new observations are consistent with the control limits
  - We flag an event as anomalous if three or more consecutive observations surpass the 99% control limit.
  - If an event is anomalous, calculate oMEDA graph for the first out-of-bounds observation.

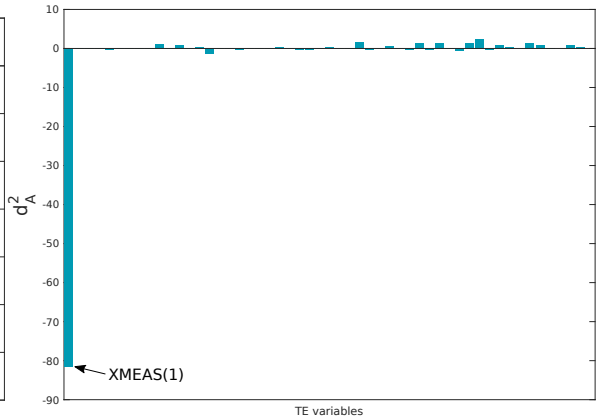
Data viewpoints



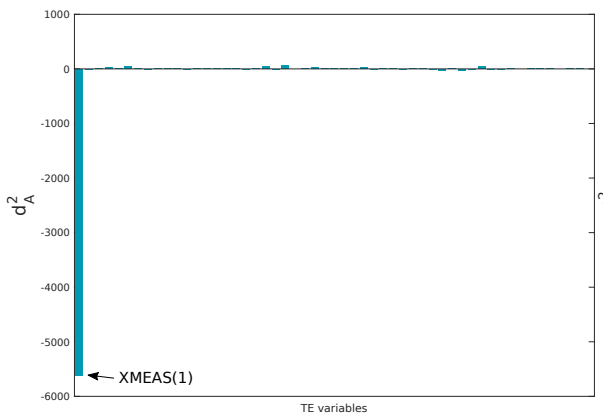
Controller level



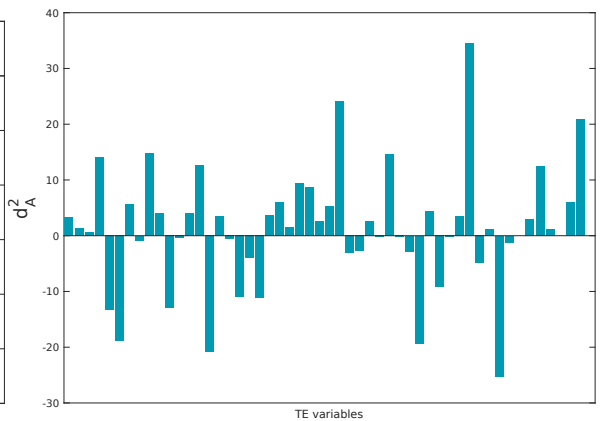
(a) IDV(6)



(b) Int. att. on XMV(3)

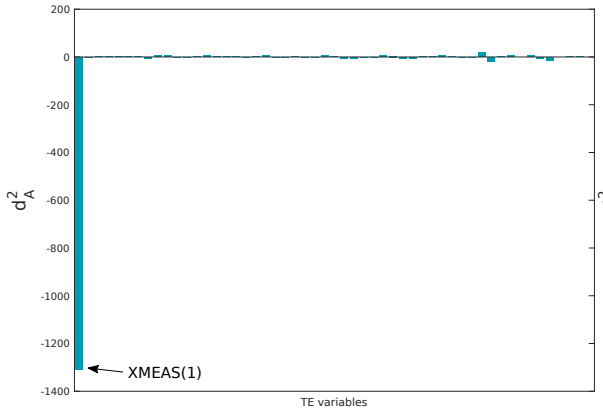


(c) Int. att. on XMEAS(1)

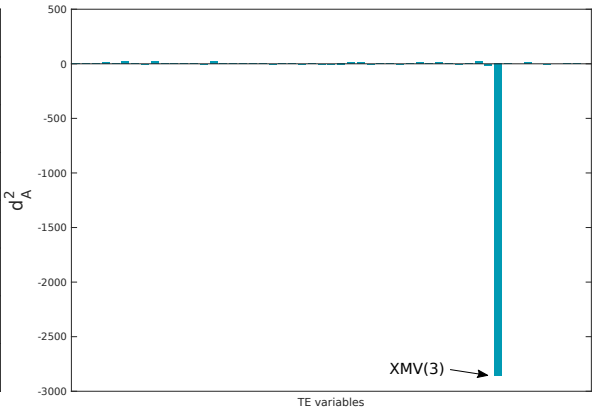


(d) DoS att. on XMV(3)

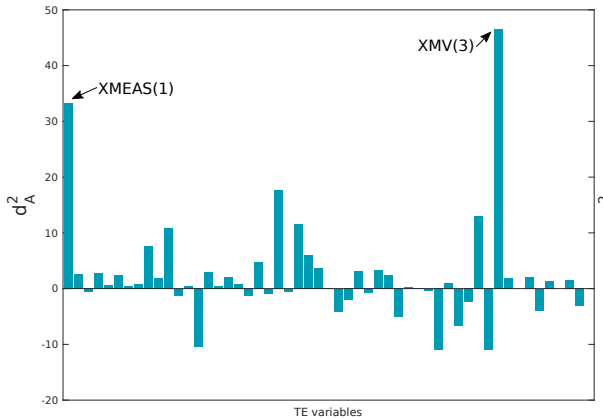
Sensor level



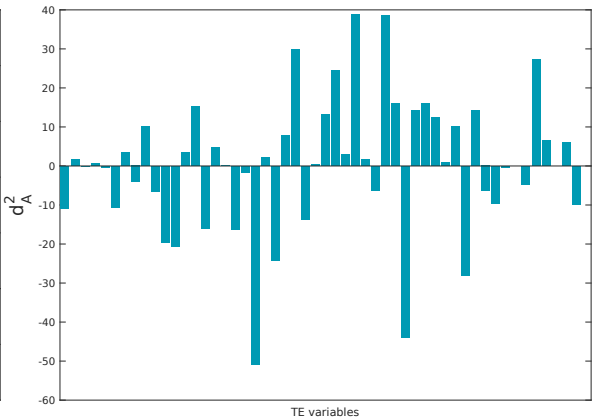
(a) IDV(6)



(b) Int. att. on XMV(3)



(c) Int. att. on XMEAS(1)



(d) DoS att. on XMV(3)

Conclusions

Conclusions

- We have presented a process-independent approach for anomaly detection in PCSs
- Furthermore, it allows the distinction between attacks (integrity and DoS) and disturbances
- Based on MSPC, we extended the model to include sensor and controller level data

Future work

Future work

- Include network-related anomalies to the model
- Faster, more realistic approach for anomaly detection
- Approach showed feasible in IT-only environments

Thank you.

miturbe@mondragon.edu

References I

Istvan Kiss, Bela Genge, and Piroska Haller.
A clustering-based approach to detect cyber attacks in process control systems.
In *Industrial Informatics (INDIN), 2015 IEEE 13th International Conference on*, pages 142–148, July 2015.

Thomas McEvoy and Stephen Wolthusen.
A plant-wide industrial process control security problem.
In *Critical Infrastructure Protection V*, pages 47–56. Springer, 2011.

References II

Nils Svendsen and Stephen Wolthusen.
Using physical models for anomaly detection in control systems.
In *Critical Infrastructure Protection III*, pages 139–149. Springer, 2009.