# Switched-based Resilient Control of Cyber-Physical Systems

Mariana Segovia Ferreira

Joaquin Garcia-Alfaro, Ana R. Cavalli,
and Jose Rubio-Hernan

June 24, 2021

# Table of contents

# Introduction

## Cyber-Physical Systems

- Control physical process
- Distributed system

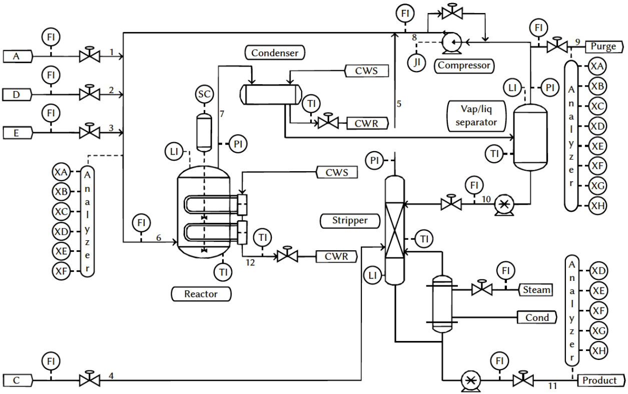
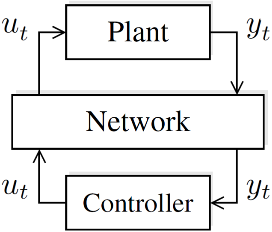



Figure 1: Tennessee Eastman Challenge Process [1].

[1] Ricker, “Decentralized control of the Tennessee Eastman Challenge Process,” 1996.

## System Model

**Feedback Control Loop**: The controller uses the system outputs as inputs to correct the behavior using a mathematical model.




$$x_{k+1} = Ax_k + Bu_k + w_k$$

$$y_k = Cx_k + v_k$$

Figure 2: Normal Behavior.

## Problem

### Cyber-Physical Adversary

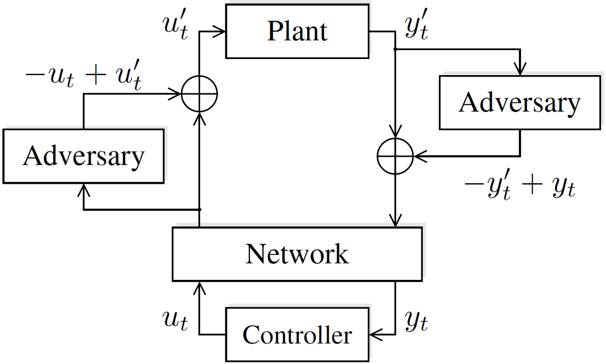



Figure 3: Cyber-Physical Attack.

## Motivation

- Cyber-Physical Adversaries may have a real impact in the physical world
  - Australian water services attack [2]
  - Ukraine attack [3]
  - Stuxnet malware [4]
- Security and safety
- Existing approaches are manual or hardwired with a fixed response that cannot be configured [5]
- Ensuring safety using information security tools is not enough

[4] Falliere et al., "W32. stuxnet dossier," 2011.
[3] Case, "Analysis of the cyber attack on the ukrainian power grid," 2016.
[2] Slay et al., "Lessons learned from the maroochy water breach," 2008.
[5] Piedrahita et al., "Leveraging software-defined networking for incident response in ICS," 2018.

# Switched-based Resilient Control

## Summary

- Switched Linear Control System with decentralized controllers
- Absorb and recover from attacks while guaranteeing the stability
- Validated using the Tennessee Eastman problem [1]

[1] Ricker, "Decentralized control of the Tennessee Eastman Challenge Process," 1996.

## Switched-based Resilient Control

- Differential equations $\rightarrow$ Transfer function $\rightarrow$ State-space model

## Switched-based Resilient Control

- Differential equations $\rightarrow$ Transfer function $\rightarrow$ State-space model

- Linear Time Invariant (LTI) System

$$\begin{aligned} x_{k+1} &= Ax_k + Bu_k + w_k \\ y_k &= Cx_k + v_k \end{aligned} \quad (1)$$

## Switched-based Resilient Control

- Differential equations → Transfer function → State-space model

- Linear Time Invariant (LTI) System

$$\begin{aligned} x_{k+1} &= Ax_k + Bu_k + w_k \\ y_k &= Cx_k + v_k \end{aligned} \tag{1}$$

- Linear Time Variant (LTV) System

$$\begin{aligned} x_{k+1} &= A_{\sigma(k)}x_k + B_{\sigma(k)}u_k + w_k \\ y_k &= C_{\sigma(k)}x_k + v_k \end{aligned} \tag{2}$$

where $\sigma : \mathbb{Z}^+ \to \mathcal{I}$, with $\mathcal{I} = \{1, ..., N\}$ is the subset that contains the indexes of the subsystems and $k \in \mathbb{Z}^+$ in the time interval

# Switched-based Resilient Control

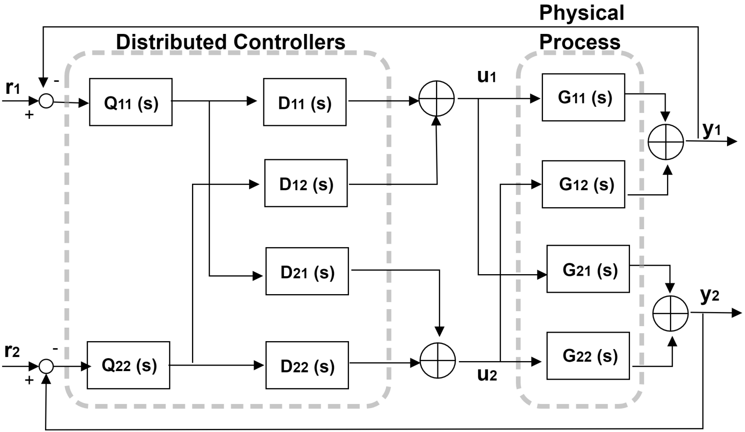



Figure 4: Approach Architecture.

M. Segovia, J. Rubio-Hernan, A.R. Cavalli, J. Garcia-Alfaro, *Switched-Based Resilient Control of Cyber-Physical Systems*, in IEEE Access, vol. 8, pp. 212194-212208, 2020.

# Validation

## Evaluation - Tennessee Eastman Problem

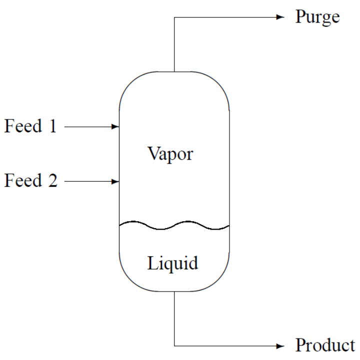
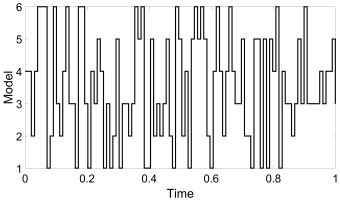



Figure 5: Reduced Tennessee Eastman.

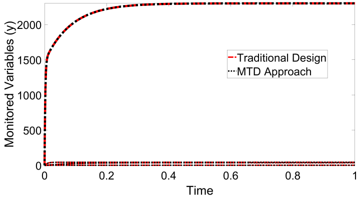
| **Input** | Description |
|---|---|
| u1 | Feed 1 valve position |
| u2 | Feed 2 valve position |
| u3 | Purge valve position |
| u4 | Liquid inventory setpoint |

| **Output** | Description |
|---|---|
| P | Pressure |
| F4 | Product flow |
| VL | Liquid inventory |
| yA3 | Amount of A in purge |

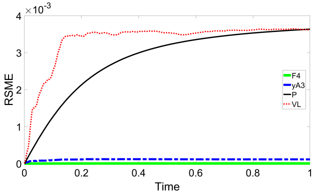
# Switched-based Resilient Control



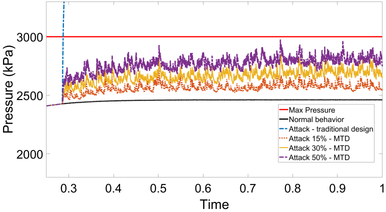

(a) Switching Signal




(b) Normal Behavior




(c) RMSE




(d) Attack Case

## Switched-based Resilient Control

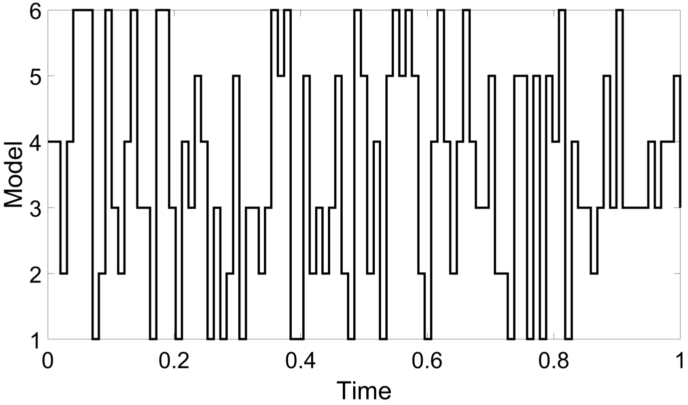



Figure 7: Switching Signal.

## Switched-based Resilient Control

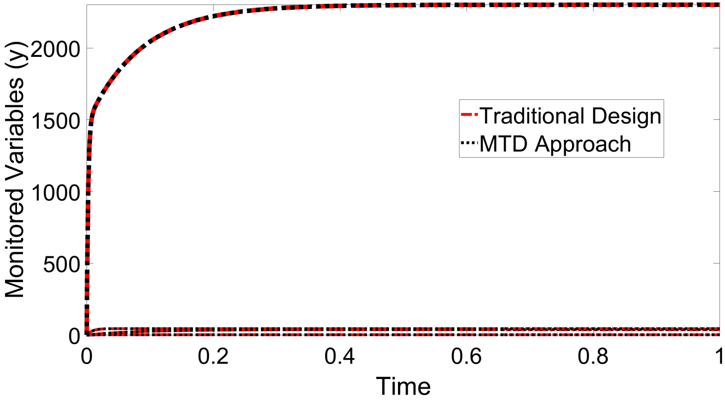



Figure 8: Normal Behavior - Traditional vs. Proposed Design.

## Switched-based Resilient Control

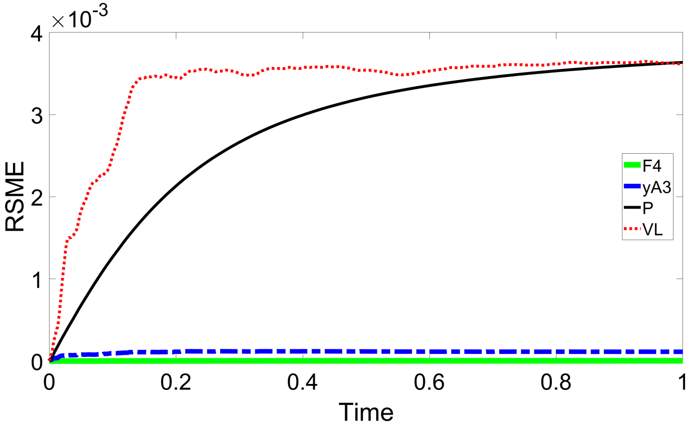



Figure 9: Root Mean Square Error - Traditional vs. Proposed Design.

## Switched-based Resilient Control

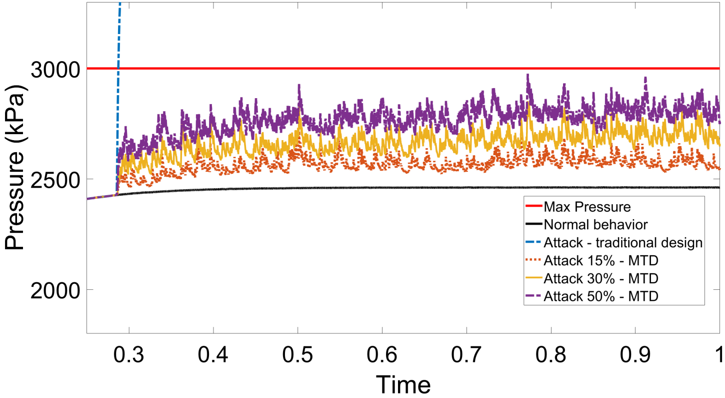



Figure 10: Attack Case - Traditional vs. Proposed Design.

## Attack Effort Evaluation

- Tennesse Eastman problem: $12^{41}$ possible models (approx. $2^{147}$)

| Adversary | Learned Models | Required time effort |
|---|---|---|
| Model 1 | 15% | $2.5 \times 10^{37}$ years |
| Model 2 | 30% | $5 \times 10^{37}$ years |
| Model 3 | 50% | $8.4 \times 10^{37}$ years |

Table 1: Attack Effort.

# Conclusion and Future Work

## Conclusion

- Control theory and cybersecurity provide complementary information
  - Collaboration between network & physical layers
  - Time Invariant System $\rightarrow$ Time Variant System
- Resilient systems can be modeled as Switched Control System
- How to ensure stability when switching unstable models (attacks)

## Future work

### Limitations

- Evaluate the performance impact (cyber components)
- Testing environment

### Open Research Lines

- Performance impact
- Digital twins
- Testing automation

## References

[1] N. L. Ricker, "Decentralized control of the Tennessee Eastman Challenge Process," *Journal of Process Control*, vol. 6, no. 4, pp. 205 – 221, 1996.

[2] J. Slay and M. Miller, "Lessons learned from the maroochy water breach," in *Critical Infrastructure Protection* (E. Goetz and S. Shenoi, eds.), (Boston, MA), pp. 73–82, Springer US, 2008.

[3] D. U. Case, "Analysis of the cyber attack on the ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, 2016.

[4] N. Falliere, L. O. Murchu, and E. Chien, "W32. stuxnet dossier," *White paper, Symantec Corp., Security Response*, vol. 5, p. 6, 2011.

[5] A. F. M. Piedrahita, V. Gaur, J. Giraldo, A. A. Cardenas, and S. J. Rueda, "Leveraging software-defined networking for incident response in industrial control systems," *IEEE Software*, vol. 35, pp. 44–50, January 2018.

## Thank you! Questions?

# Publications

**Journal papers**

- M. Segovia, J. Rubio-Hernan, A.R. Cavalli, J. Garcia-Alfaro, *Cyber-Resilience - A Systematic Survey of Resilience Techniques for Cyber-Physical Systems*, *[Under Evaluation]*.
- M. Segovia, J. Rubio-Hernan, A.R. Cavalli, J. Garcia-Alfaro, *Switched-Based Resilient Control of Cyber-Physical Systems*, in IEEE Access, vol. 8, pp. 212194-212208, 2020.

**Conference papers**

- M. Segovia, J. Rubio-Hernan, A.R. Cavalli, J. Garcia-Alfaro, *Switched-based Control Testbed to Assure Cyber-Physical Resilience by Design*, *[Under Evaluation]*.
- M. Segovia, J. Rubio-Hernan, A.R. Cavalli, J. Garcia-Alfaro, *Cyber-Resilience Evaluation of Cyber-Physical Systems*, in "NCA 2020", pp. 1-8, Boston, USA, November 2020.
- M. Segovia, A.R. Cavalli, N. Cuppens, J. Rubio-Hernan, J. Garcia-Alfaro, *Reflective Mitigation of Cyber-Physical Attacks*, in "CyberICPS 2019/ESORICS 2019", pp.19-34, Springer, Luxembourg, September 2019.
- M. Segovia, A.R. Cavalli, N. Cuppens, J. Garcia-Alfaro, *A Study on Mitigation Techniques for SCADA-driven Cyber-Physical Systems*, in "FPS 2018", pp. 257-264, Springer, Montreal, Canada, November 2018.

## Experimental Testbed

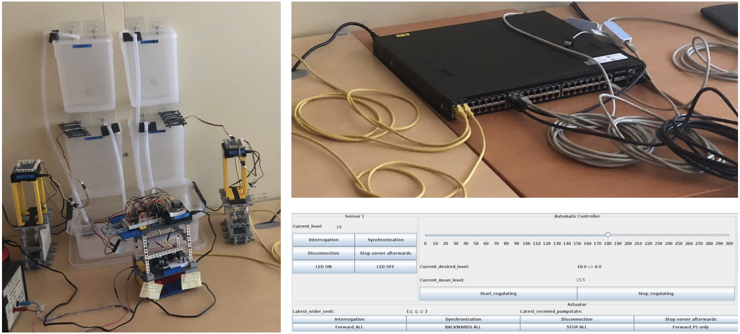



Figure 11: Resilient Water Tank Testbed.

M. Segovia *et al.* , "Switched-based Control Testbed to Assure Cyber-Physical Resilience by Design", *[Under Evaluation]*.

## MTD Model Selection

- **Next model to be executed**

$$hash(K1, j)\ mod\ N$$

K1 - key selected by the orchestrator
j - number of switching interval
N - number of physical models

- **Network configuration transformation**

$$hash(K2, j)\ mod\ P$$

K2 - key selected by the orchestrator
P - Virtual IP address

## SISO vs. MIMO design

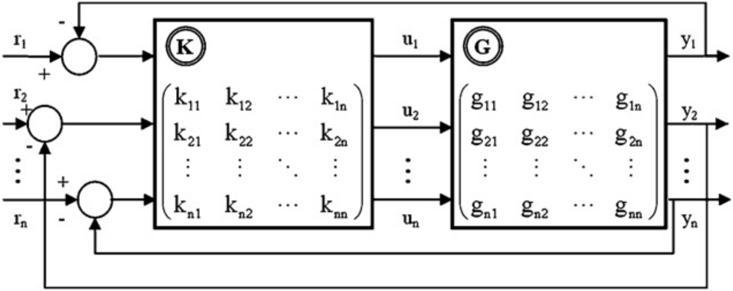



Figure 12: Centrlized Design.

[Picture] Garrido *et al.* , "Centralized multivariable control by simplified decoupling", 2012.

# Distributed Controllers Design

$$Q(s) = \begin{pmatrix} \frac{|G|}{adjG_{11}} & 0 & \cdots & 0 \\ 0 & \frac{|G|}{adjG_{22}} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \frac{|G|}{adjG_{nn}} \end{pmatrix} \qquad D(s) = \begin{pmatrix} 1 & \frac{adjG_{12}}{adjG_{22}} & \cdots & \frac{adjG_{1n}}{adjG_{nn}} \\ \frac{adjG_{21}}{adjG_{11}} & 1 & \cdots & \frac{adjG_{2n}}{adjG_{nn}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{adjG_{n1}}{adjG_{11}} & \frac{adjG_{n2}}{adjG_{22}} & \cdots & 1 \end{pmatrix}$$

Figure 13: Transfer Function Matrix Factorization.

## Stability

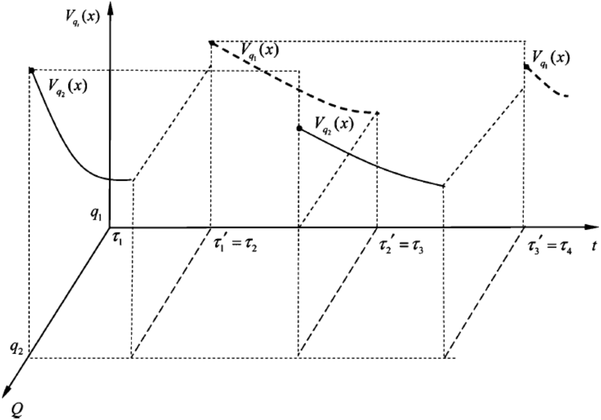



Figure 14: Stable system with Lyapunov decreasing sequence.

[Picture] Lin *et al.* , "Stability and Stabilizability of Switched Linear Systems: A Survey", 2009.

# Stability

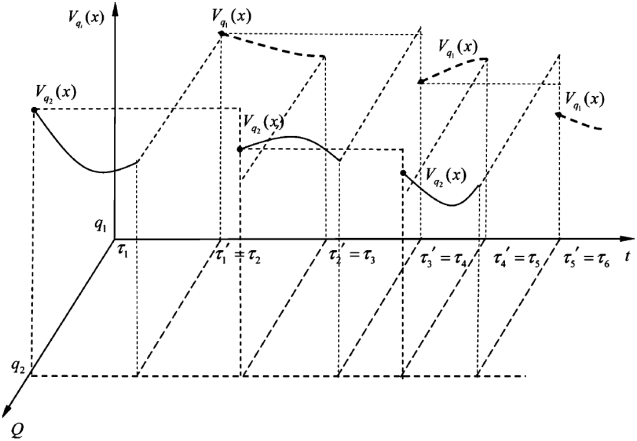



Figure 15: Stable system with unstable periods.

[Picture] Lin *et al.* , "Stability and Stabilizability of Switched Linear Systems: A Survey", 2009.

# Digital Twin

- ✓ Predict behavior
- ✓ Detect attacks (*)
- ? Repair the system state
- ? Regression automated testing

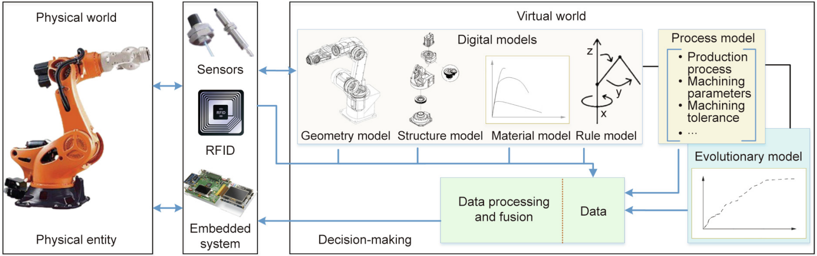



Figure 16: Digital Twin.

(*) Schellenberger *et al.* , "Detection of covert attacks on CPS by extending the system dynamics with an auxiliary system", 2017.
[Picture] Tao *et al.* , "Digital Twins and CPS toward Smart Manufacturing and Industry 4.0: Correlation and Comparison", 2019.