Improving security and resilience of Cyber Physical Systems

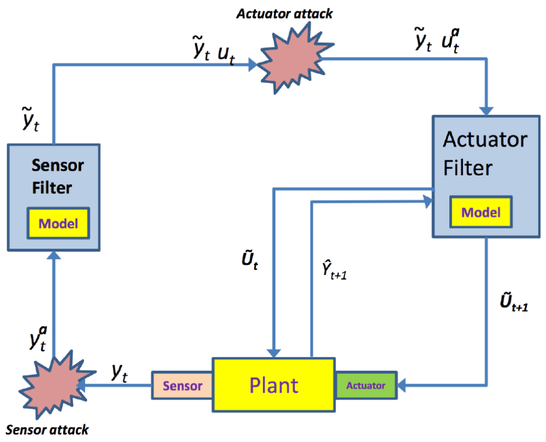
Riccardo Orizio, Prof. Gregory Provan

1

❑ General Problem

– Cyber Physical Systems can represent many real systems, including complex and safety critical ones such as transportation networks, electrical and gas distribution, water treatment plants and SCADA systems.

– These critical systems need to operate reliably in all circumstances, regardless of the number and nature of the anomalies.

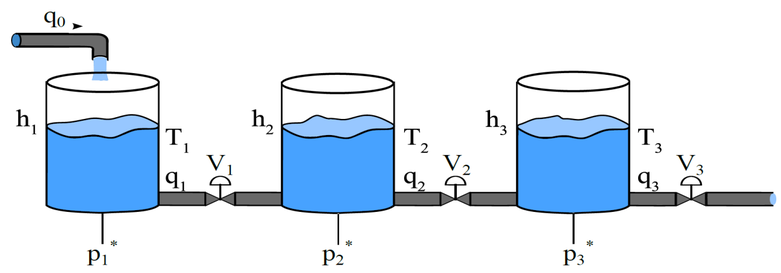


Can we create a tool that can help Cyber Physical Systems in **detecting**, **identifying** and **correcting** an anomaly whenever one would occur?
Can it be used for time critical systems?

2

❑ Methodology

– Experimental research method currently based on simulated data of the three tanks system model.



– Approaches used:
  - Pure model based: modes identification of the system behaviour through reverse inference $x_i = f_j^{-1}(y_j)$;
  - Basic residuals study: studying differences between expected and real sensors data (AvF);
  - Algebraic, basic and personally improved version: extending the residuals study to its data derivatives and studying their patterns (IAA);
  - Data driven: SVM, LSTM, HMM.

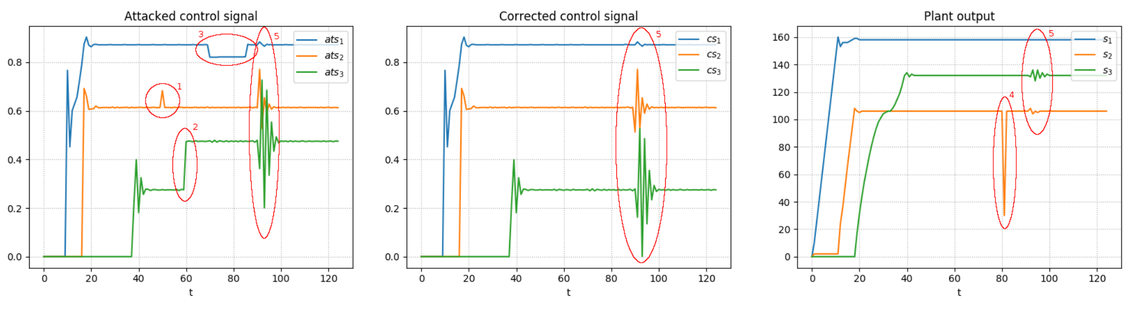
3

❑ Results

– Comparison results of the different approaches shows that the algebraic approach seems better, even when the system is experiencing simultaneous anomalies.

Method	Faults	Detected	False Positive	Missed	FR
Model based	78	53	32	25	0.345
AvF	78	57	15	21	0.607
IAA	78	54	8	24	0.597

– Distinction of the anomaly type: attack or fault.



4

❑ Future

– Currently working on the data driven approach;
– Identifying a small set of approaches that can have good performances having limited computational resources;
– Improving the results effectiveness combining results from different approaches;
– Working with real systems data (e.g. FCU and HVAC systems).

❑ Publications

– Physics-Based Methods for Distinguishing Attacks from Faults, CENICS 2017
– Comparing Physics-Based Methods for Distinguishing Attacks from Faults, DX'18
– Physics-Based Methods for Responding to Attacks and Faults, WIP

Ireland's European Structural and Investment Funds Programmes 2014-2020
Co-funded by the Irish Government and the European Union
European Union
European Regional Development Fund
SOUTHERN Regional Assembly
Promoting our Region