Lero THE IRISH SOFTWARE RESEARCH CENTRE
Science Foundation Ireland For what's next
UCC Coláiste na hOllscoile Corcaigh, Éire University College Cork, Ireland

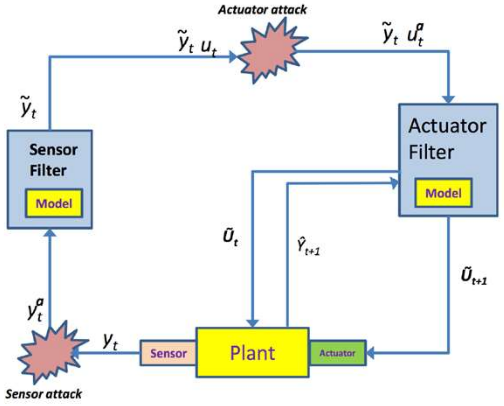
Improving security and resilience of Cyber Physical Systems

Distinction between attacks and faults

Riccardo Orizio, Prof. Gregory Provan

1

❑ General Problem



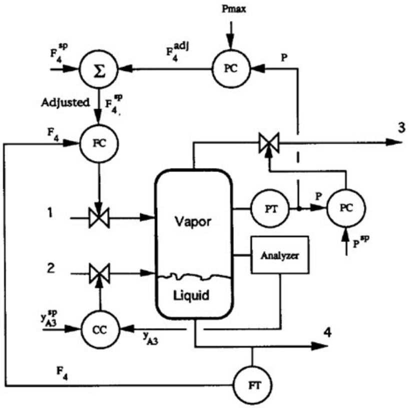
Can we create a tool that can help Cyber Physical Systems in ***detecting***, ***identifying*** and ***correcting*** an anomaly *whenever* one would occur?

Can it be used for critical systems?

2

❑ Impact

- Innovative: combination of model based and data driven techniques;
- Adaptable to different systems;
- Efficient and reactive.



Model of the Tennessee Eastman Process, used for testing. (Ricker, 1993)

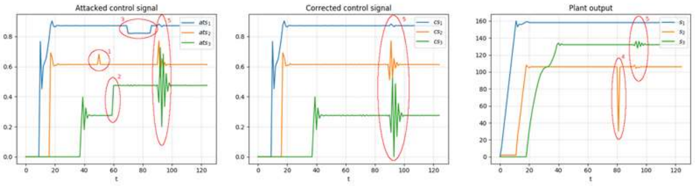
3

❑ Methodologies

- Pure model based: $x_i = f_j^{-1}(y_j)$;
- Residuals study: $r_i = \tilde{y}_k - C\hat{x}_k$;
- Algebraic, residuals and patterns: $r_i,\ \frac{\delta}{\delta t}^{(I,II,III)} y$;
- Data driven: NN, HMM, LSTM.

❑ Results

- Anomaly distinction: attacks vs faults;



- Increased NN detection and identification success rate from 10% to 90%.

4

❑ Future

- Integration of HMM and LSTM methods;
- Improving identification effectiveness;
- Testing on 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

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

Tionól Réigiúnach an Deiscirt
Southern Regional Assembly