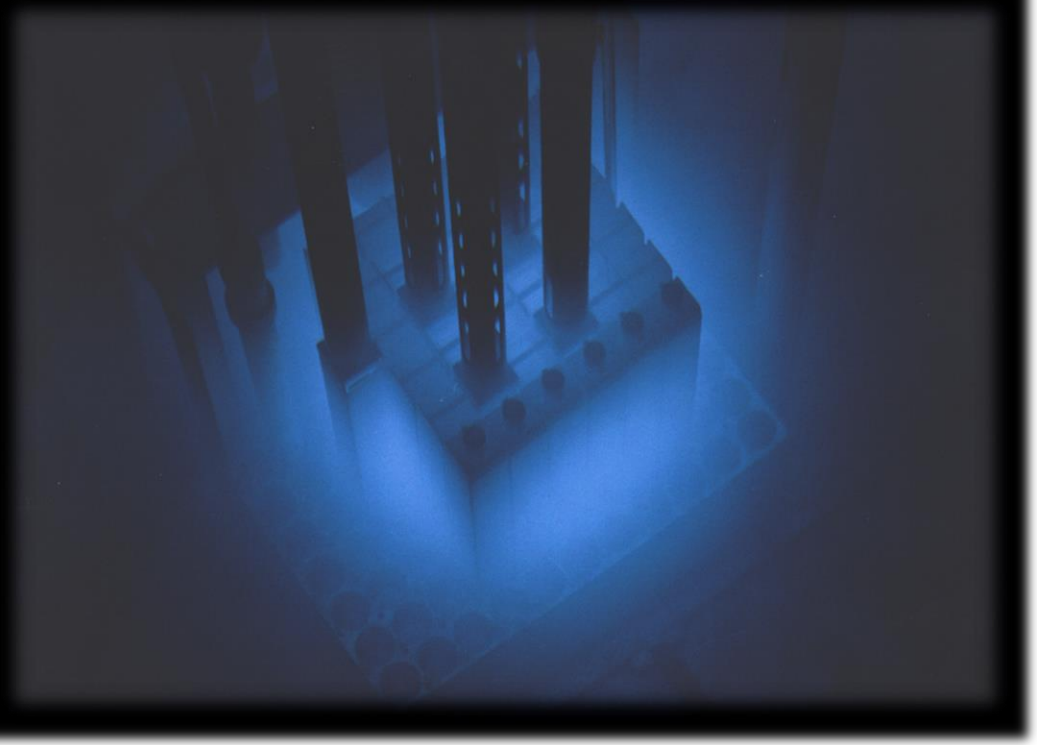
InfoSymbiotics / DDDAS2020
October 2-4, 2020

DATA-BASED DEFENSE-IN-DEPTH OF CRITICAL SYSTEMS



Styliani Pantopoulou, Pola Lydia Lagari, Clive H. Townsend, Lefteri H. Tsoukalas

School of Nuclear Engineering
Purdue University, West Lafayette, IN, US

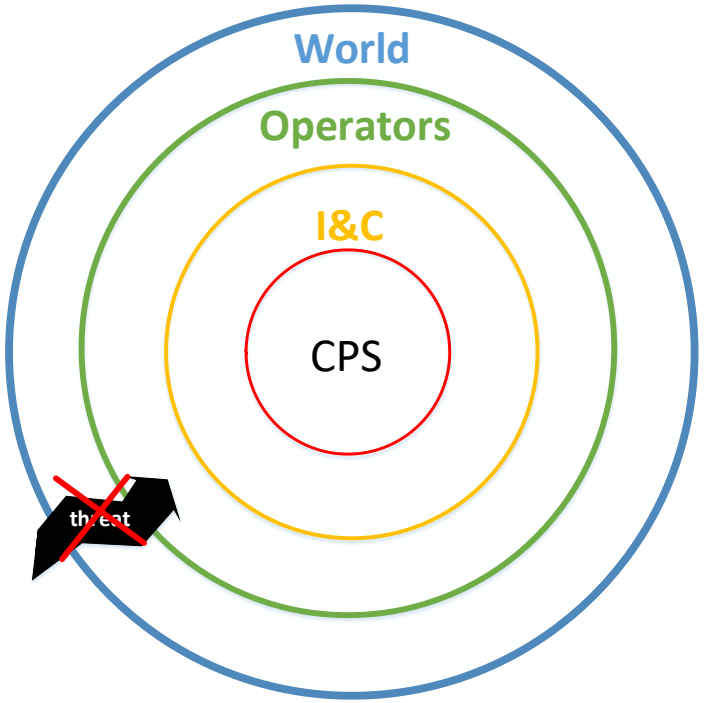
PURDUE UNIVERSITY

Outline

- Motivation
- Methodology
- Results
- Conclusions & Future Work

Motivation

- Cybersecurity in focus because of the multifaceted nature of Cyber Physical Systems (CPS).
- Digitalization and cyber technologies offer advantages; but also pose challenges.
- The DDDAS paradigm can prove helpful towards data assortment and classification.



PURDUE UNIVERSITY

Methodology
System Modeling

- System under review: a Nuclear Power Plant (NPP)

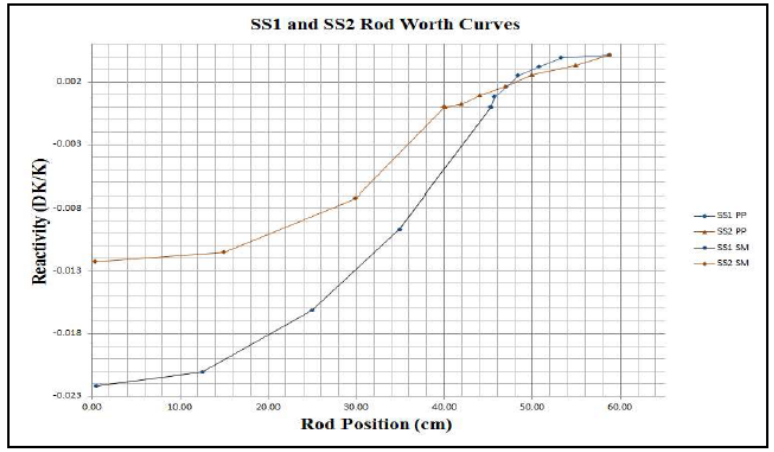
- State-space equations
  - n: neutron density
  - c: neutron precursor density
  - ρ: reactivity
  - z: control rod velocity

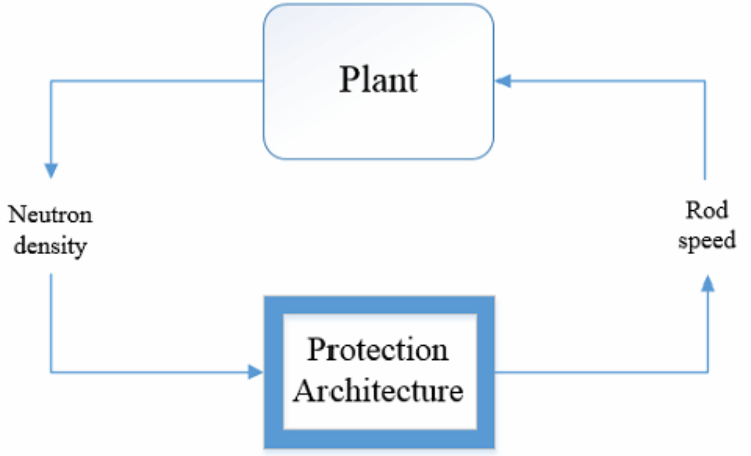
$$\begin{bmatrix}\dot{n}\\ \dot{c}\\ \dot{\rho}\end{bmatrix} = \begin{bmatrix}\frac{-\beta}{\Lambda} & \lambda & \frac{n_0}{\Lambda}\\ \frac{\beta}{\Lambda} & -\lambda & 0\\ 0 & 0 & 0\end{bmatrix}\cdot\begin{bmatrix}n\\ c\\ \rho\end{bmatrix} + \begin{bmatrix}0\\ 0\\ G\end{bmatrix}\cdot z$$

$$n = [1 \quad 0 \quad 0]\cdot\begin{bmatrix}n\\ c\\ \rho\end{bmatrix}$$

- Controlling z gives output regarding n

- ρ is calculated through plant measurements

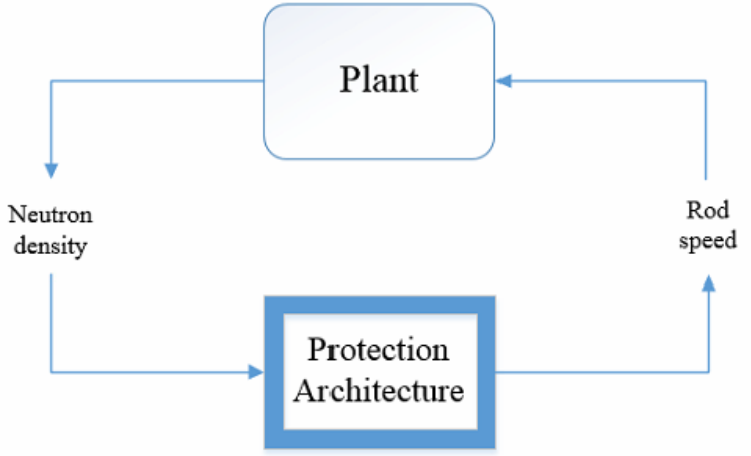


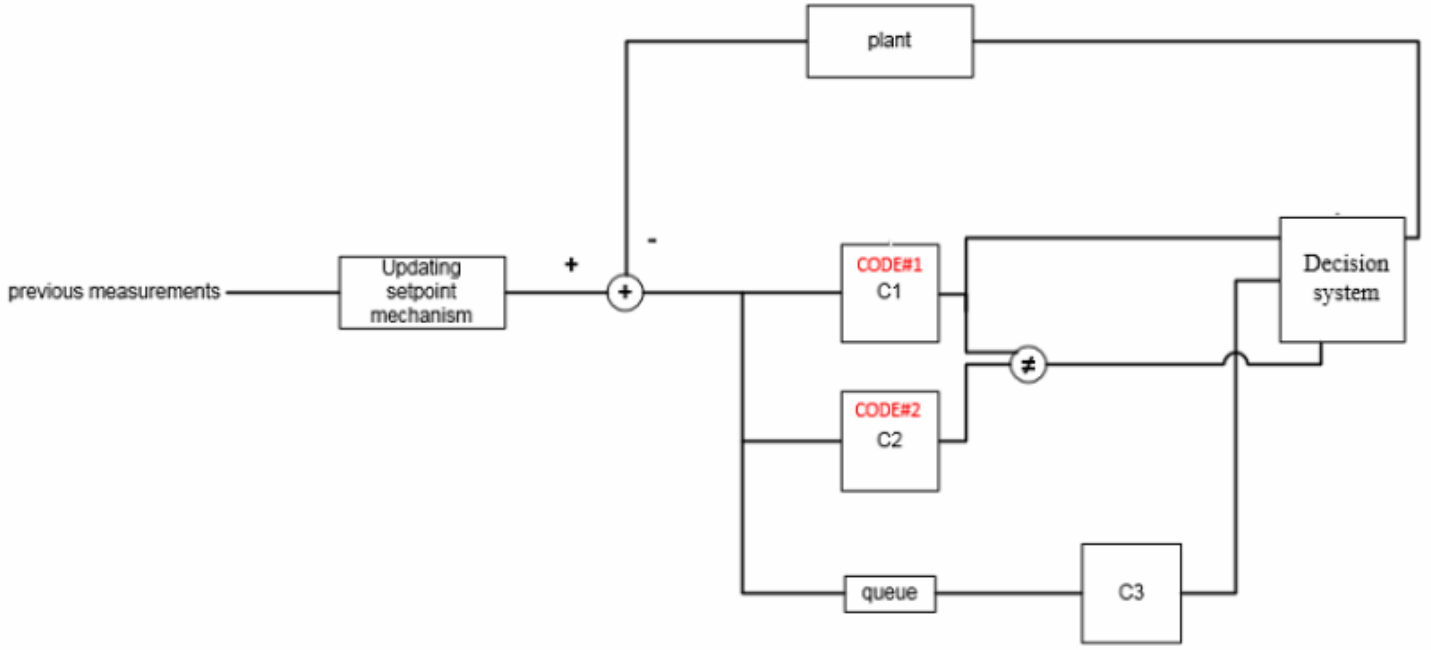


PURDUE UNIVERSITY

Methodology
Mitigation of a Cyber-attack

- Protection architecture
  - PLC controllers
  - Updating setpoint component
  - Delay queue
  - Decision system



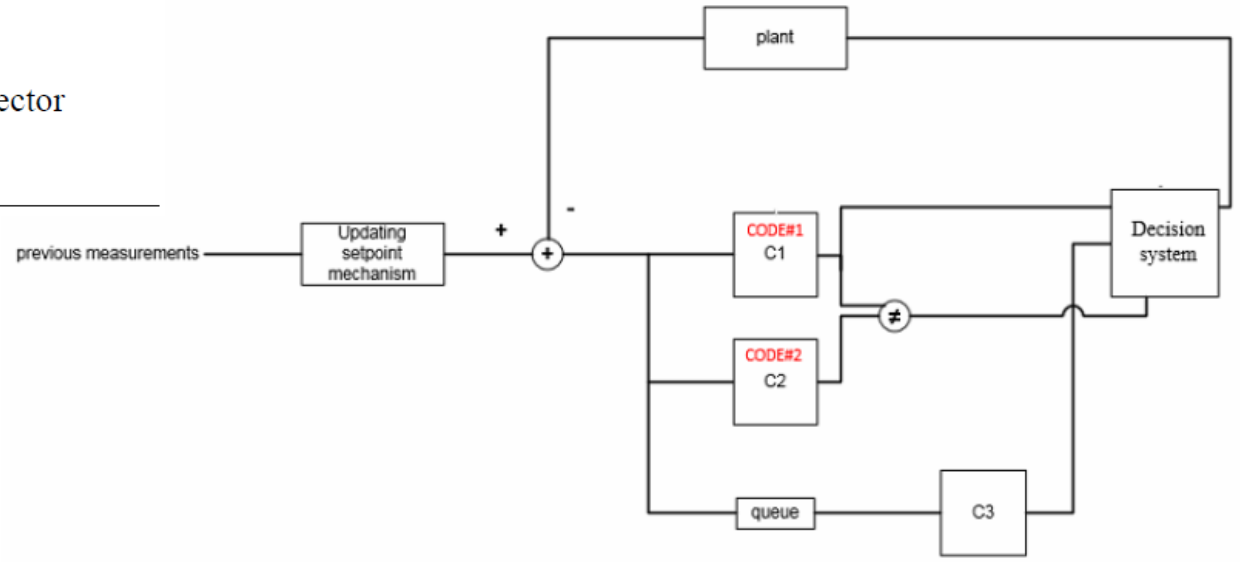


PURDUE UNIVERSITY

Methodology
Mitigation of a Cyber-attack

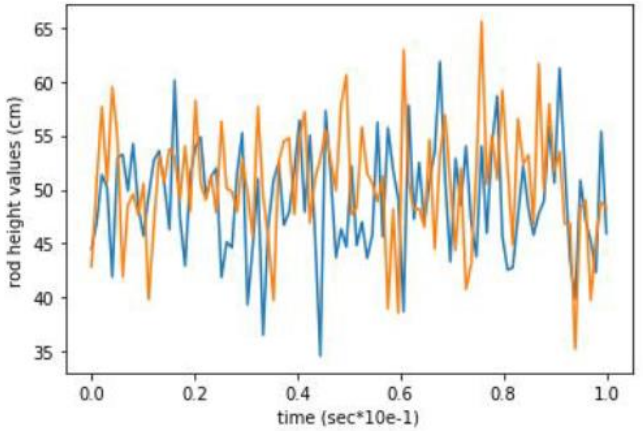
Algorithm

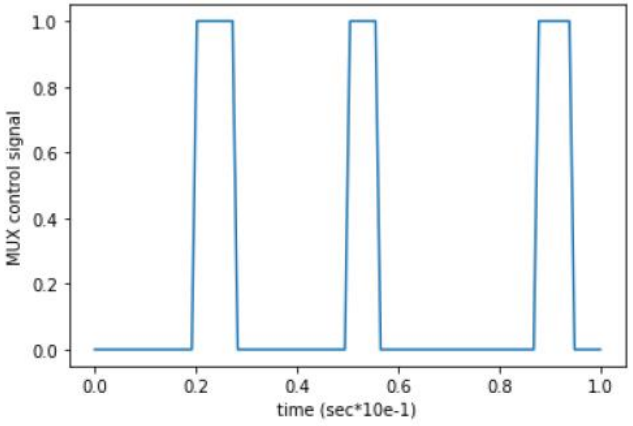
1. Get measurement $x(n)$ from plant
2. $x(n-k)\cdot h(n-k)+x(n-k+1)\cdot h(n-k+1)+\ldots+x(n-1)\cdot h(n-1)=x(n-k+1)$
   ...
   $x(n-1)\cdot h(n-k)+x(n-2)\cdot h(n-k+1)+\ldots+x(n-k)\cdot h(n-1)=x(n)$
3. $\hat{x}(n)=h(1)\cdot x(n-1)+\ldots+h(k)\cdot x(n-k)$
4. Controllers C1 and C2 get error signal $\hat{x}(n)-x(n)$
5. C1 runs PLC_code1, C2 runs PLC_code2
6. Comparator checks $|out1-out2|$
7. If $|out1-out2| \leq$ noise threshold $\rightarrow$ $Mux\_control\_signal = 0$
   Else $Mux\_control\_signal=1$
8. Contents of queue erased and not added to previous_measurements vector
9. C1, C2 get restarted
10. $x(n+1)$ calculated from state space equations



Results

- Response of decision system.
- Plant measurements considered as following the normal distribution, with specific μ and σ.
- When the two controller outputs differ more than a threshold related to noise; C3 forwards its output to the plant.





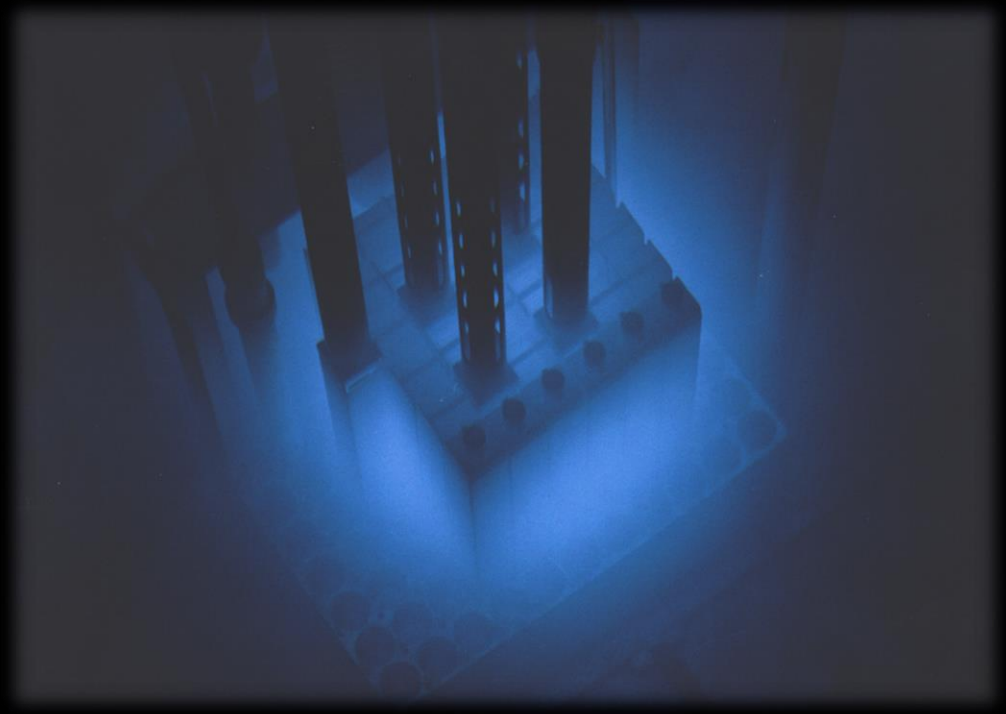
PURDUE UNIVERSITY

Conclusions & Future Work

- Importance and connection of the DDDAS paradigm with critical systems.
- A NPP can be transformed into a trustworthy digital system.
- A second layer of protection or suitable operators' training would aid towards avoiding dangerous situations.
- More complex attack schemes have to be tested in order to ensure the system's integrity and security under a greater variety of circumstances.

PURDUE UNIVERSITY

THANK YOU!
QUESTIONS?



Styliani Pantopoulou, Pola Lydia Lagari, Clive H. Townsend, Lefteri H. Tsoukalas

School of Nuclear Engineering
Purdue University, West Lafayette, IN, US

PURDUE UNIVERSITY