# Information Flow Analysis for Cyber-Physical Security

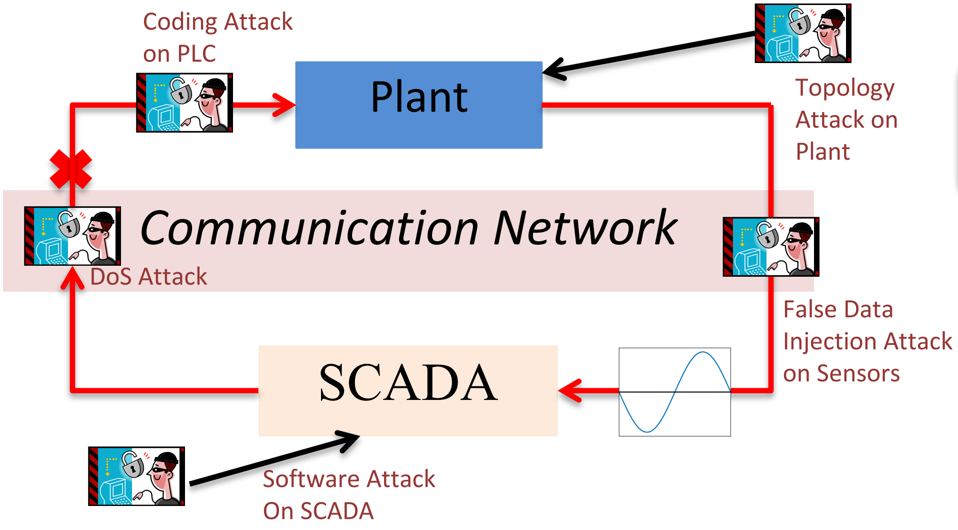
- Bruno Sinopoli, Washington University in St Louis
- Soummya Kar, Anupam Datta, Carnegie Mellon University
- bsinopoli@wustl.edu, soummyak@cmu.edu, danupam@cmu.edu

- Award #: 1646526

# Description

## CPS Researchers Face the Challenge of

*1) Achieving Resilience in the Face of Threats*



*2) Obtaining a Unifying Framework to Solve Problems*

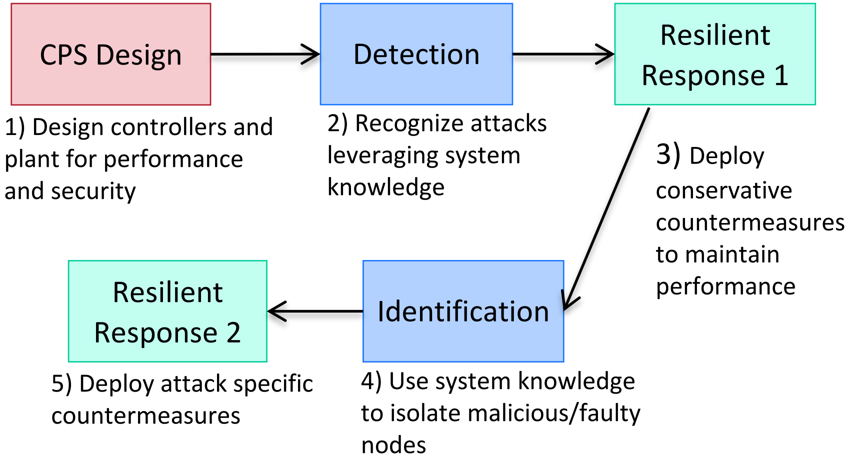
Cyber + Software Security

+

System Theory

## Our Approach

*1) A Process of Accountability involving Detection, Identification, and Correction*



1) Design controllers and plant for performance and security

2) Recognize attacks leveraging system knowledge

3) Deploy conservative countermeasures to maintain performance

4) Use system knowledge to isolate malicious/faulty nodes

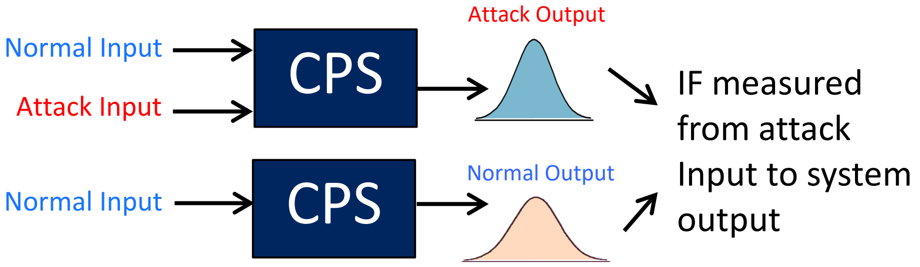
5) Deploy attack specific countermeasures

*2) Information Flow as a Unifying Language/Set of Tools*

**(Today's Focus)**

An Information flow exists from *x* to *y* if information in *x* is transferred to, or used to derive information transferred to *y*

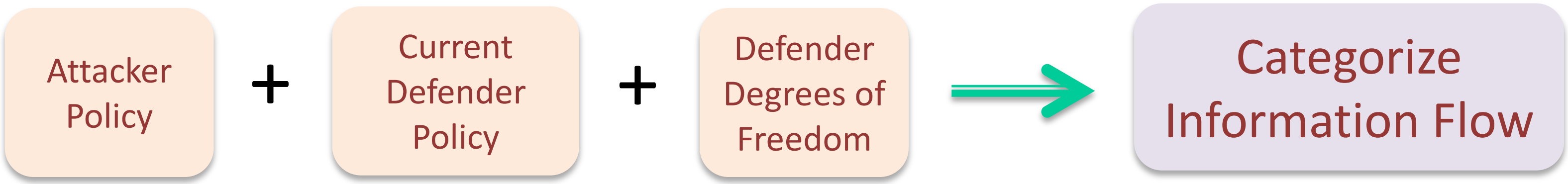
Ex. We propose the **KL divergence** between normal and attack distributions as a measure of information flow to characterize attack detectability



# Findings: A methodology for analysis/design

Goal: Be able to detect new attack vector by designing IF > ε. From prior results, this guarantees the existence of a detector with FA decay rate > ε.

1)



2)

| Type of Information Flow | Detectability of Attack | Illustrated Example | Action Required |
|---|---|---|---|
| Unconditional ε - weak information flow | Attack is stealthy for all admissible defender policies: **IF ≤ ε** | **Zero Dynamics Attacks**<br>**FDI Attacks** | Nothing can be done without increasing the available DOF for the defender |
| Conditional ε - weak information flow | Attack is stealthy for some defender policies (including current): **IF ≤ ε** | **Replay Attacks** | Change Policy: Balance Information Flow and System Performance |
| ε – strong information flow | Attack is detectable for current defender policy: **IF > ε** | **Watermarking Defense against Replay Attacks** | None |

3) If necessary, increase degrees of freedom and/or change the defender policy. Ensure prior attack vectors generate sufficient Information Flow