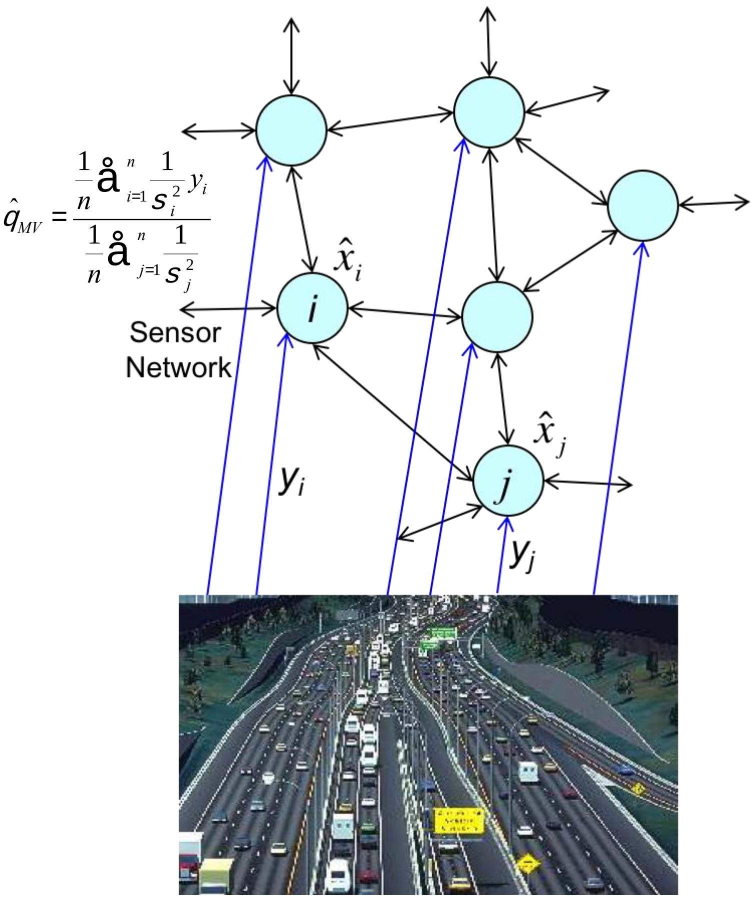
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

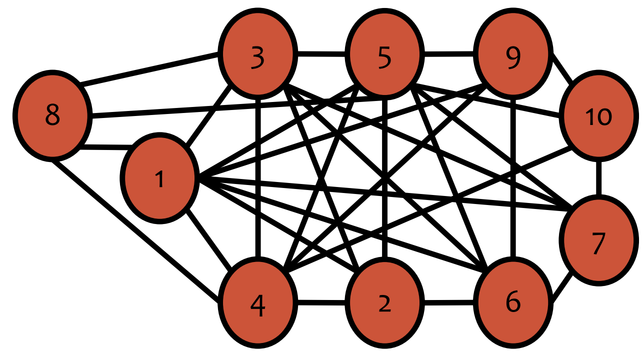
Foundations of CPS Resilience

Xenofon Koutsoukos
Joint work with Aron Laszka, Waseem Abbas, and
Yevgeniy Vorobeychik

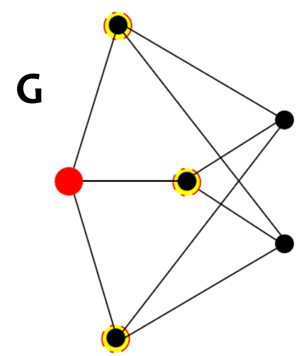
Berkeley UNIVERSITY OF CALIFORNIA · Massachusetts Institute of Technology · NSF · MICHIGAN · VANDERBILT UNIVERSITY

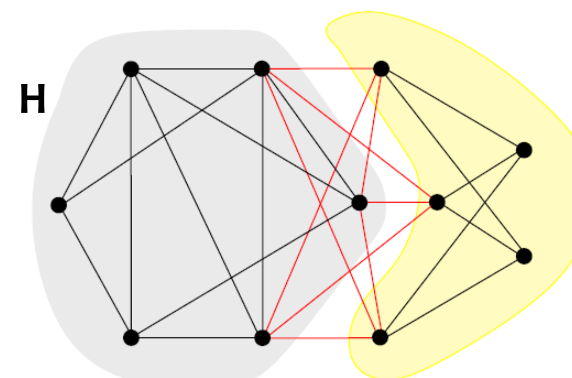
Motivation: Resilient Monitoring and Control of Distributed CPS





- Resilience requires high degree of redundancy (high connectivity)
- We can improve resilience by adding trusted nodes

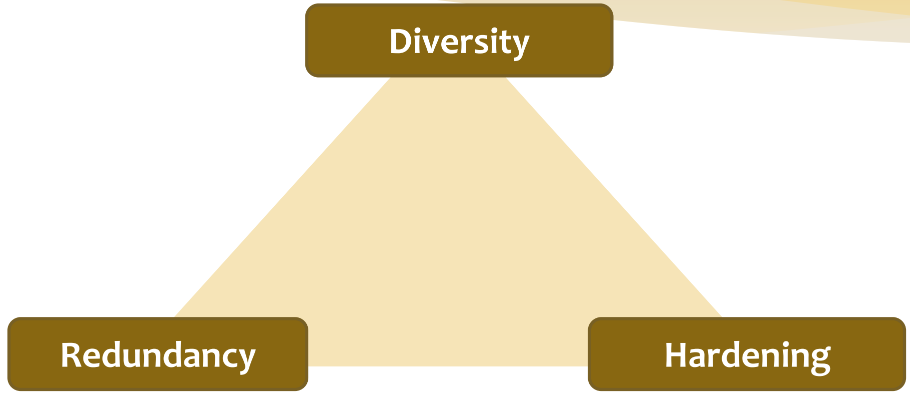




- G is **3-robust** with red trusted node.
- H is also is **3-robust.**

Can we improve resilience by combining redundancy, diversity, and hardening (trust)?

Outline



- Combining hardening and diversity to improve structural robustness of CPS networks
- Integrating redundancy, diversity, and hardening for detection of cyber-physical attacks in water distribution systems
- Integrating diversity and hardening for resilient traffic control systems
- Conclusions and future directions

Structural Robustness in Networks

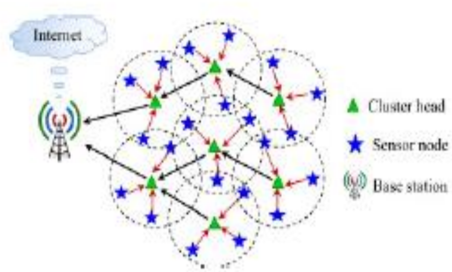
Structural Robustness:

Network's ability to retain and preserve its *structure* as a result of node and edge removals.

Why Structural Robustness?

- Network reliability against faults
- Vulnerability against malicious attacks
- Survivability and resilience

internet topology



sensor network

infrastructure

social network

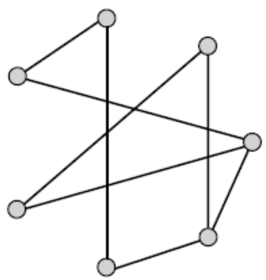
Improving Structural Robustness Using Redundancy

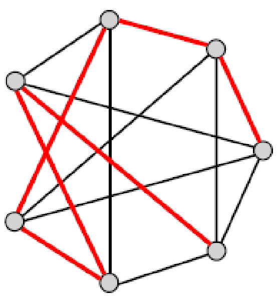
We desire networks to be structurally robust.

How can we improve structural robustness of networks?

(that is, how can we improve network connectivity, r-robustness etc.?)

- A typical way is to add more links and edges (i.e., **<u>redundancy</u>**).

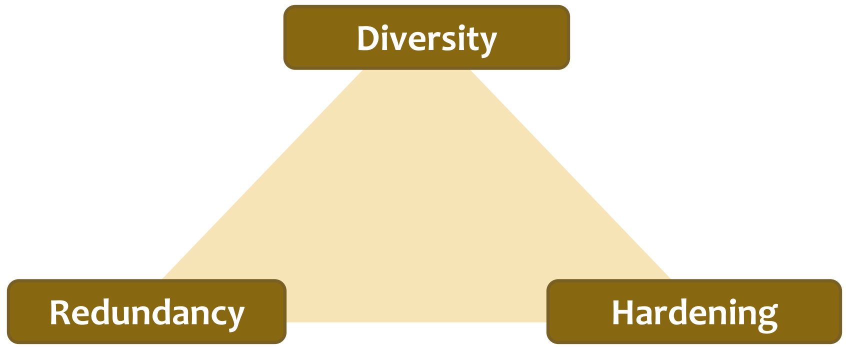




- Cost effectiveness, feasibility issues
- What can be some other ways to improve structural robustness?

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Improving Structural Robustness



Can we utilize the notions of ***diversity*** and ***hardening*** to improve structural robustness in networks?

Hardening:

- Hardening of nodes (edges) against failures and attacks.
- Hardened nodes remain operational at all times.

Diversity:

- Network components with similar functionalities but different implementations.
- Disjoint set of vulnerabilities

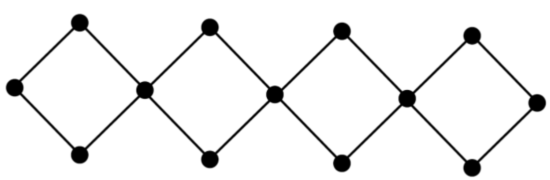
Pairwise Network Connectivity

Pairwise connectivity measures the fraction of **node-pairs** that are connected with each other through a path.

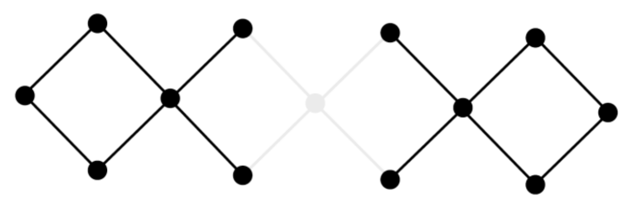
Like connectivity, pairwise connectivity also measures structural robustness of networks.

Applications:

- Determining robustness of communication networks
- Identifying key players in anti-terrorism networks
- Targeted vaccination for pandemic prevention



Pair-wise connectivity = 1

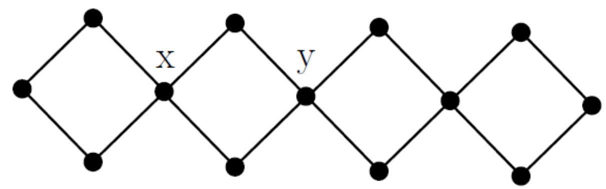


After removing middle node,
Pair-wise connectivity = 0.4545

Pairwise Network Connectivity

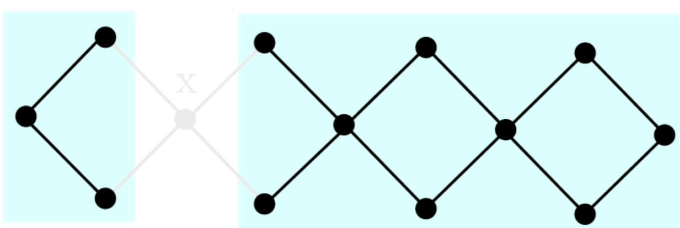
Pairwise connectivity gives more information about the structural robustness of network as compared to vertex-connectivity.

Example: The graph is 1-connected, and becomes disconnected by removing either of the nodes x or y.



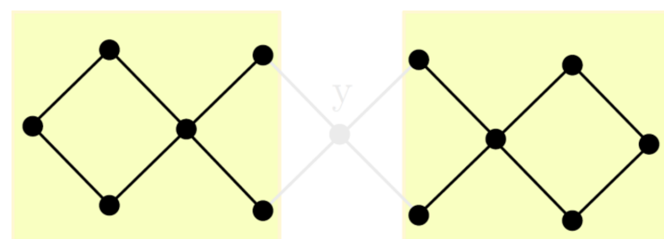
However, pairwise connectivity is different in both cases.

1) Removing x



Pairwise connectivity = 0.59

2) Removing y



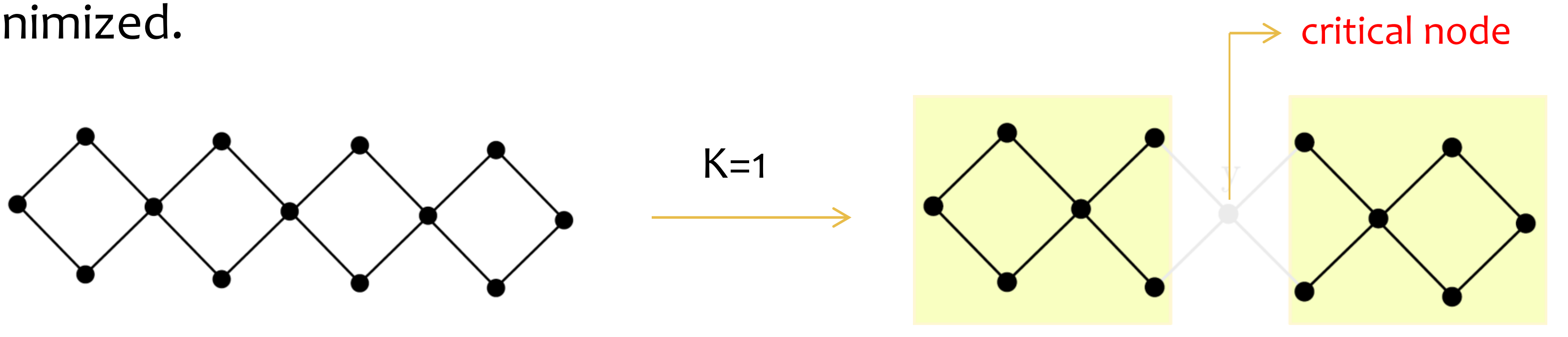
Pairwise connectivity = 0.454

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Attacker's Objective

Critical node detection problem:

Given an undirected graph *G* and an integer *K*, delete a subset of at most *K* nodes such that the pairwise connectivity of the remaining graph is minimized.



Problem Complexity: Critical node detection problem is known to be NP-complete (Arulselvan et al. 2009)

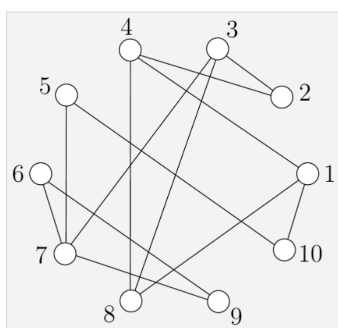
Hardening to Improve Pairwise Network Connectivity

How can we minimize the impact of an attack, that is, maximize the pairwise connectivity of the network remaining after the attack?

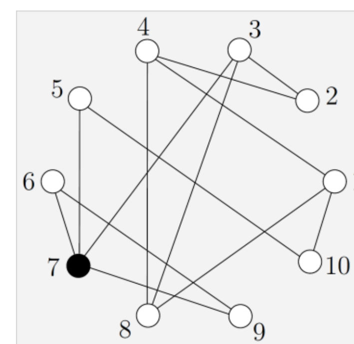
Hardening of nodes:

- A small subset of nodes, say T, is hardened such that these nodes cannot be removed from the network.
- Consequently, attack can be launched only at the nodes that are not hardened.

- Optimal attack of removing two nodes = {1,7}
- Pair-wise connectivity after attack = 0.286



- **Node 7 is hardened**
- Optimal attack = {3,10}
- Pair-wise connectivity after attack = 0.429



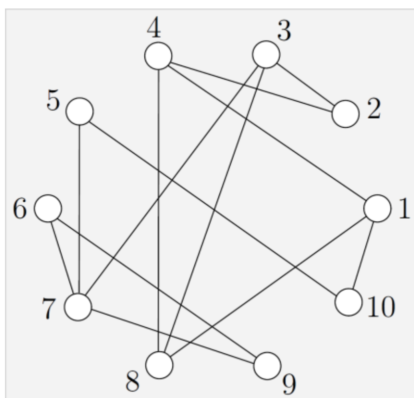
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

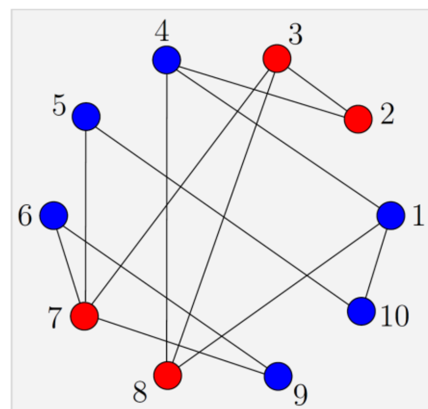
Diversity to Improve Pairwise Network Connectivity

Diversifying nodes:

- Consider that nodes are heterogeneous and are of multiple types.
- Set of node types: $D = \{D_1, D_2, \ldots, D_d\}$.
- Each node belongs to one of the types in D.
- An attacker can only attack nodes that belong to the same type.

- Optimal attack of removing two nodes = {1,7}
- Pairwise connectivity after attack = 0.286





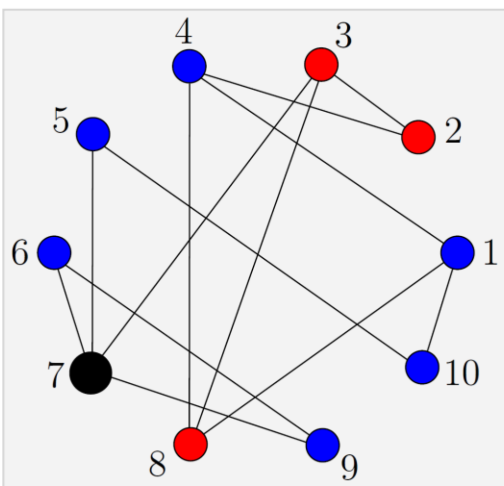
Two types of nodes, red and blue.

- Optimal attack = {2,7}
- Pairwise connectivity after attack = **0.571**

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Combining Hardening and Diversity

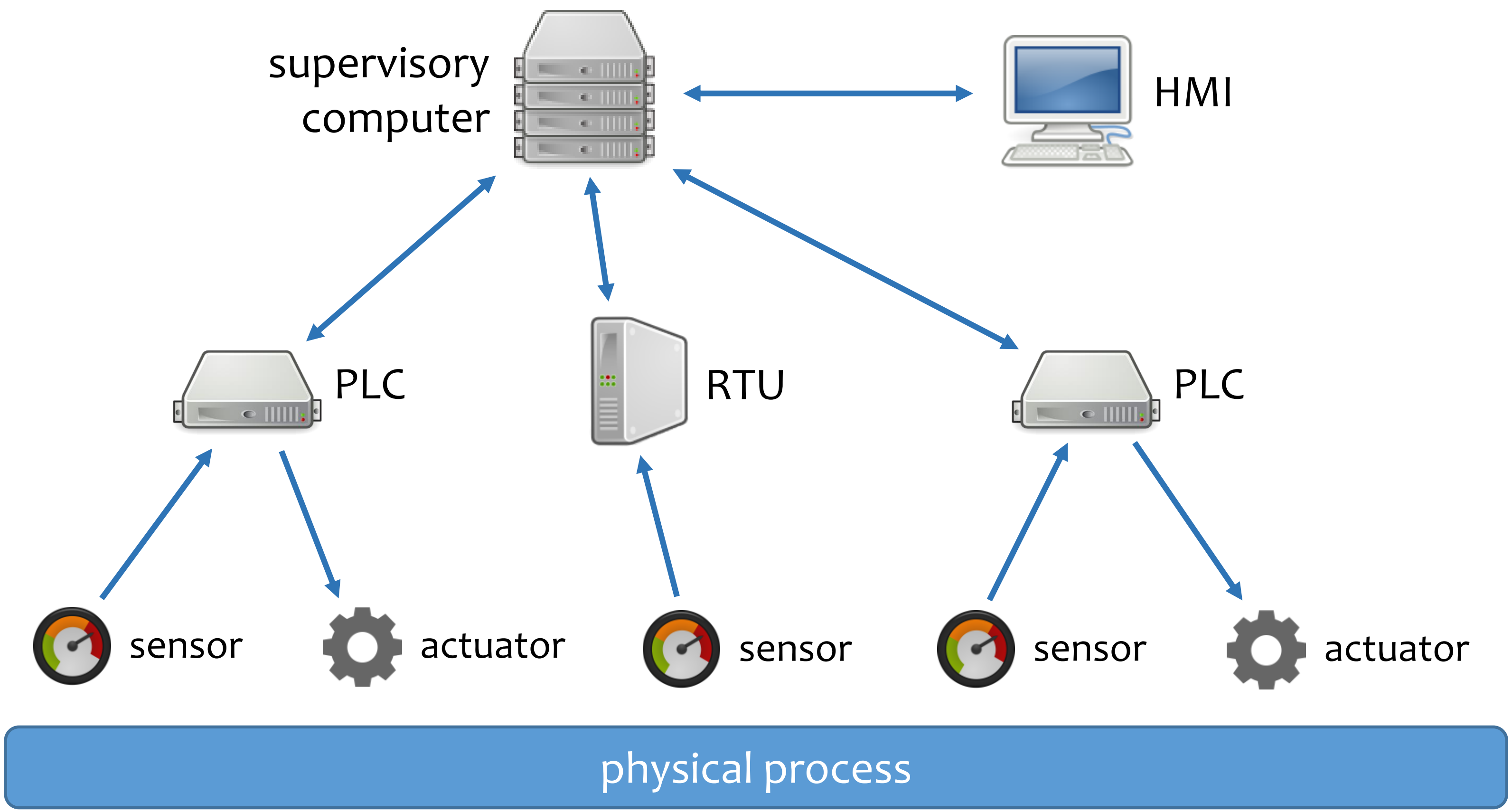
- By combining hardening and diversity, pairwise connectivity resulting after an optimal attack can be further improved.
- Consider **two node types**, **one hardened node**, and an attack consisting of removing two nodes.



- Two types of nodes, red and blue.
- Node 7 is **hardened.**
- Optimal attack consists of removing nodes {1,5}
- Resulting pair-wise connectivity is **0.75**
- Without hardening and diversity, pair-wise connectivity would be **0.286.**

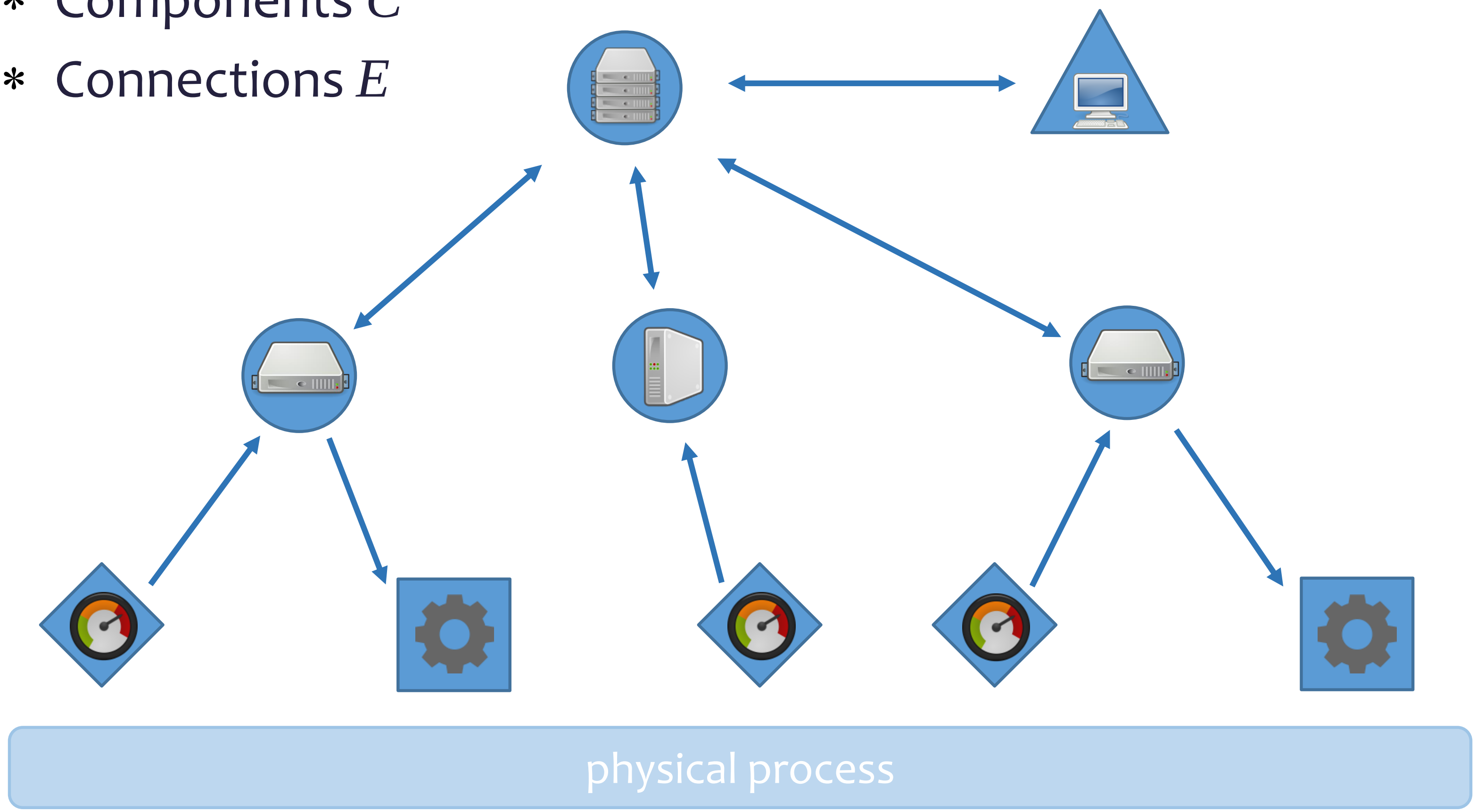
Our goal is to develop a model that allows the principled investment in redundancy, diversity, and hardening for improving resilience in CPS

Example Cyber-Physical System



Graph-Theoretic Model

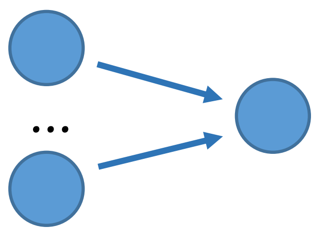
* Graph $G = (C, E)$
  * Components C
  * Connections E



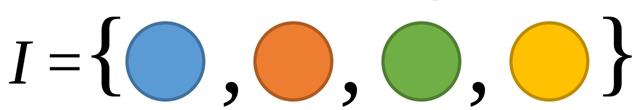
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Components

* Properties of a component $c \in C$
  * Type t_c
    - computational
    - sensor
    - actuator
    - Interface
  * Set of input connections E_c
    * Example:

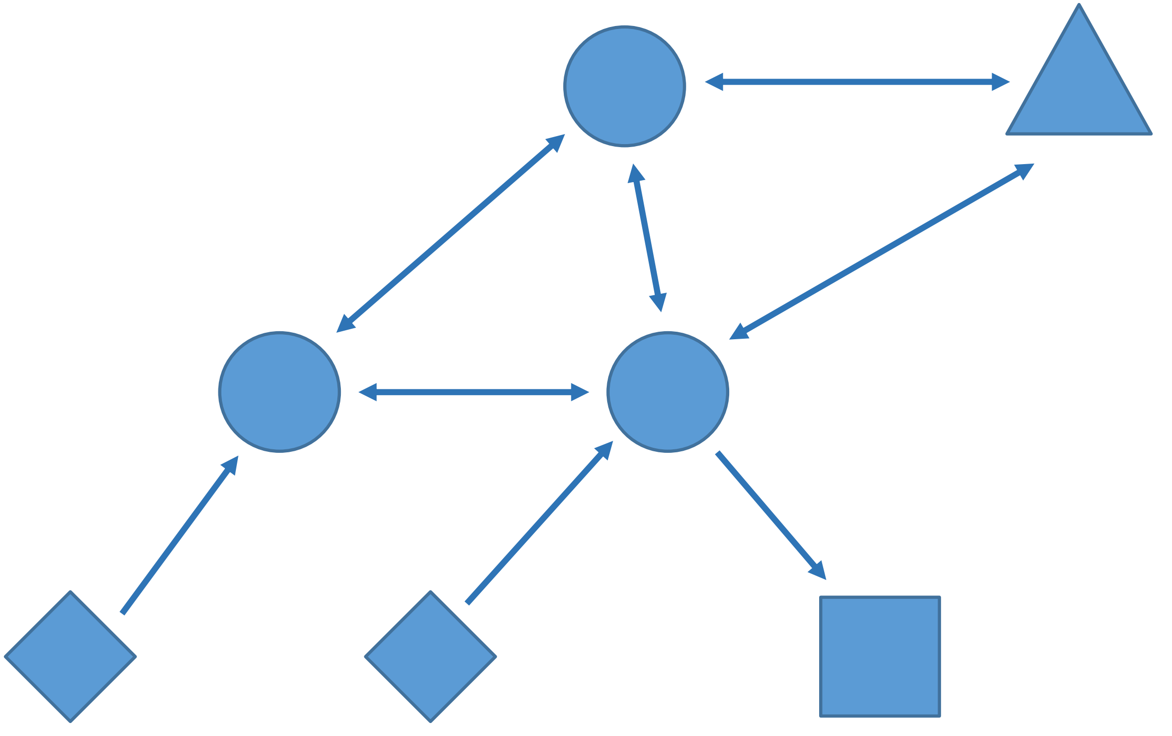


  * Deployed implementation r_c
    * Chosen from a set of available implementations I
    * xample set:



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

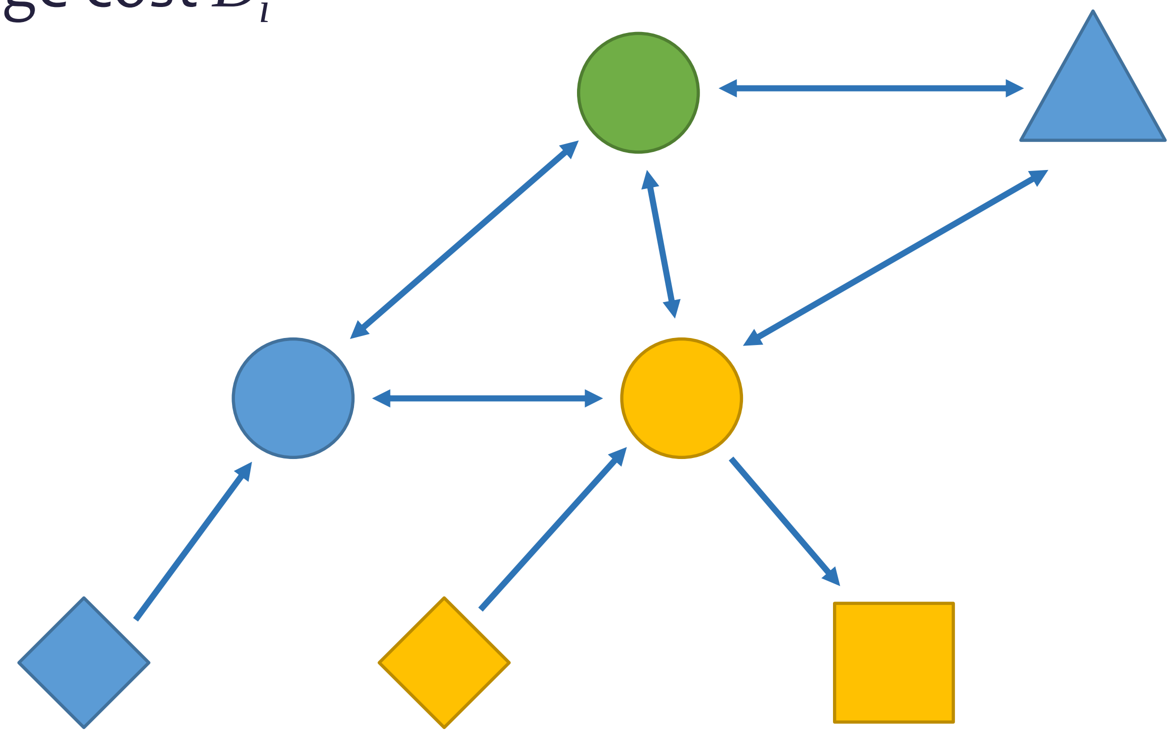
How to improve the resilience of a CPS?



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

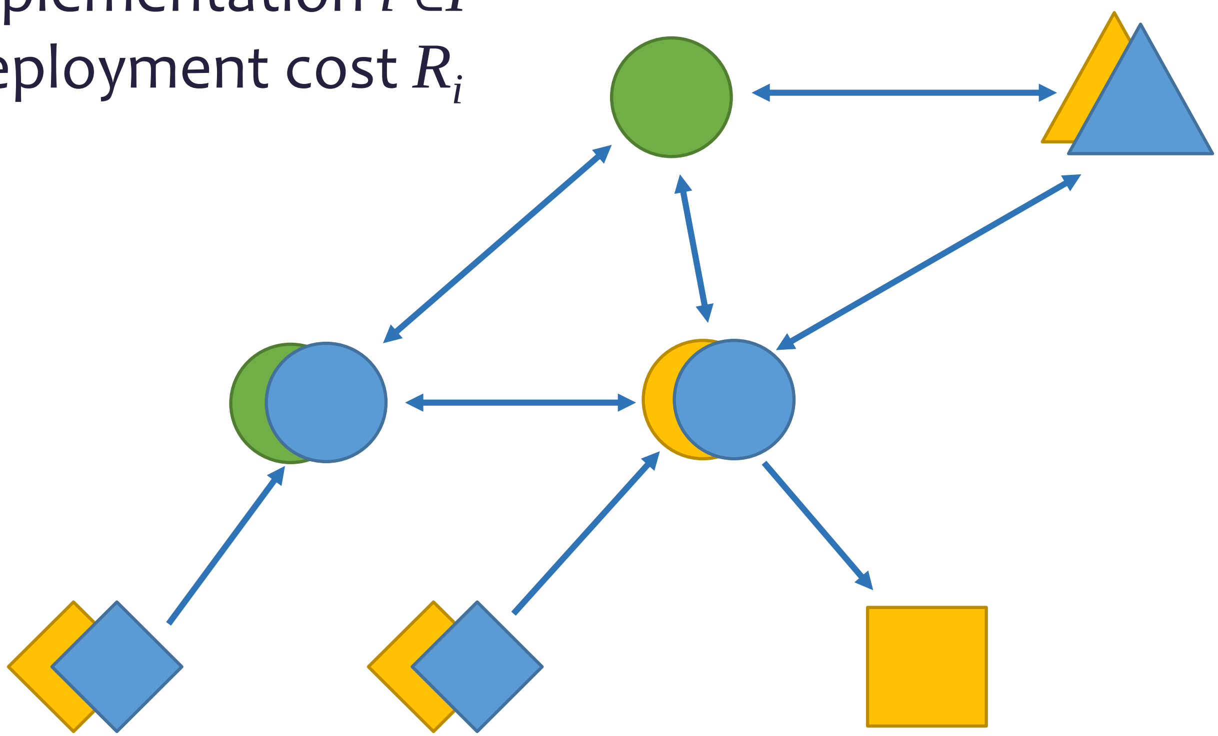
Diversity

* Use a variety of implementations
* Each implementation $i \in I$ has a usage cost D_i



Redundancy

* Deploy additional instances of some components (based on different implementations)
* Each implementation $i \in I$ has a deployment cost R_i



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Hardening

* Harden some implementations (e.g., source code reviews, firewalls, penetration testing)
* Each implementation has a set of available hardening levels L_i
  * Each level $l \in L_i$ has a cost H_l and an estimate of being secure S_l
  * Example levels:
    { (DEFAULT: \$100 000, 0.9),
    (SECURE: \$500 000, 0.95),
    (VERY SECURE: \$1 000 000, 0.99) }
* Example selection:

$\longrightarrow$ SECURE

$\longrightarrow$ DEFAULT

$\longrightarrow$ VERY SECURE

How to quantify security risks?

$$\text{Risk} = \sum_{\text{outcome}} \Pr[\text{outcome}] \cdot \mathit{Impact}(\text{outcome})$$

which components are compromised

what is the probability that they are compromised

what is the impact of their compromise on the system

Probability of Compromise

* Each implementation i is vulnerable with probability $1 - S_{l_i}$ (independently of other implementations)
* Instances of vulnerable implementations are compromised
* A component is compromised if

	Component Type			
	sensor	computational	actuator	interface
stealthy attack	**all** instances are compromised	**all** instances are compromised or **all** input components are compromised		
non-stealthy attack	**majority** of instances are compromised	either **majority** of instances are compromised or **majority** of input components are compromised		

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Impact of Compromise

* Impact depends on the set of compromised components

$$Impact = MaximumDamage(\text{compromised components})$$

  * Exact formulation depends on specific system and context

* We present two example systems
  1. Smart water-distribution monitoring for contaminants
  2. Transportation networks

Resilience Maximization Problem

* Given redundancy, diversity, and hardening expenditures $\boldsymbol{R}$, $\boldsymbol{D}$, $\boldsymbol{H}$, the optimal deployment is

$$\min_{\boldsymbol{r},\, \boldsymbol{l}} \mathrm{Risk}(\boldsymbol{r}, \boldsymbol{l})$$

$$\text{subject to } \sum_{c \in C} \sum_{i \in r_c} R_i \leq \boldsymbol{R},\ \ \sum_{i \in \bigcup_c r_c} D_i \leq \boldsymbol{D},\ \ \sum_{i \in I} H_{l_i} \leq \boldsymbol{H}$$

* Computationally challenging (NP-hard), but typically we can devise efficient heuristics that work well in practice
* General formulation: Given budget $\boldsymbol{B}$, the optimal deployment is

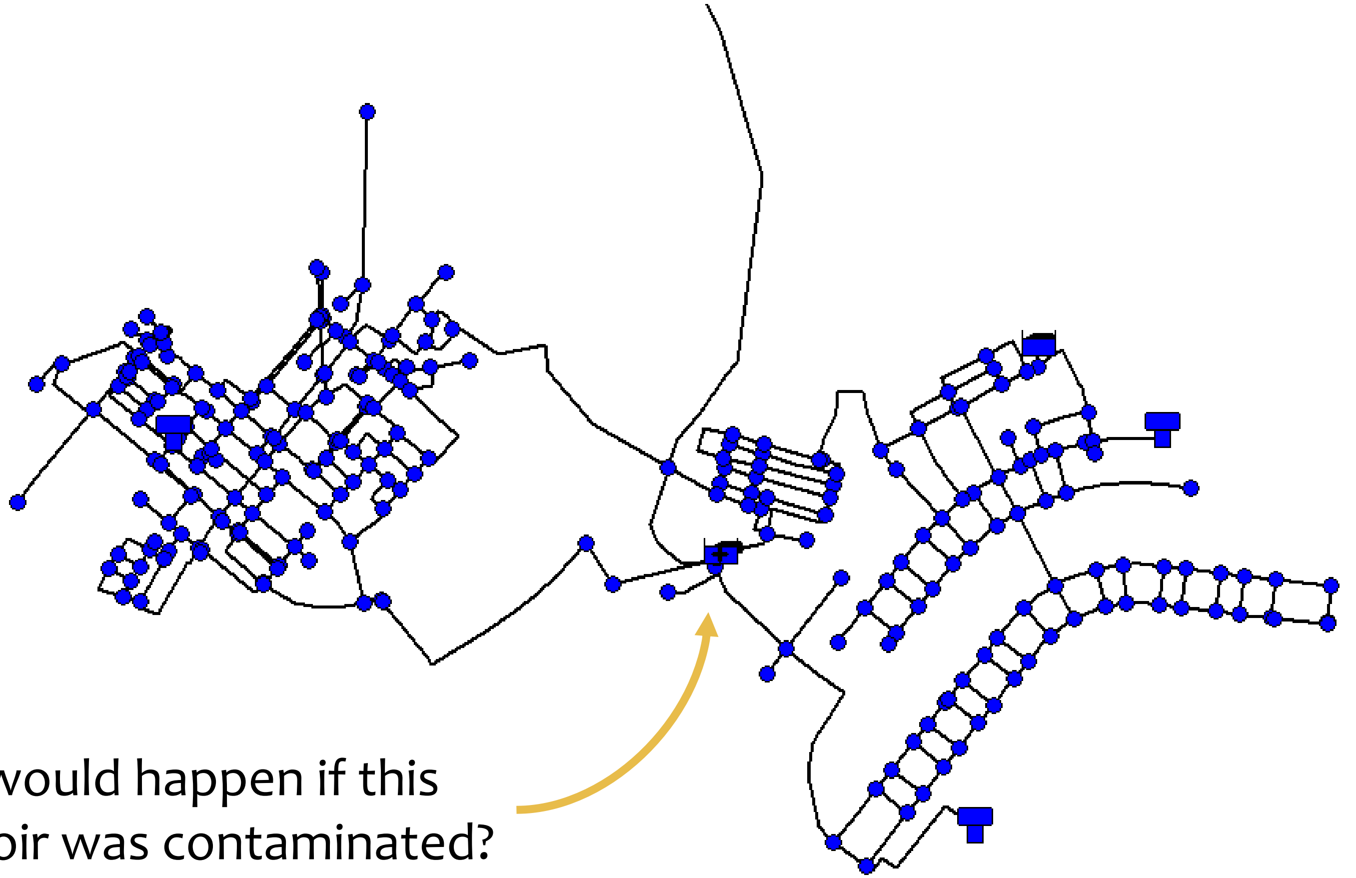
$$\min_{\boldsymbol{r},\, \boldsymbol{l}} \mathrm{Risk}(\boldsymbol{r}, \boldsymbol{l})$$

$$\text{subject to } \sum_{c \in C} \sum_{i \in r_c} R_i + \sum_{i \in \bigcup_c r_c} D_i + \sum_{i \in I} H_{l_i} \leq \boldsymbol{B}$$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Water-Distribution Networks

* Example topology (real residential network from Kentucky)

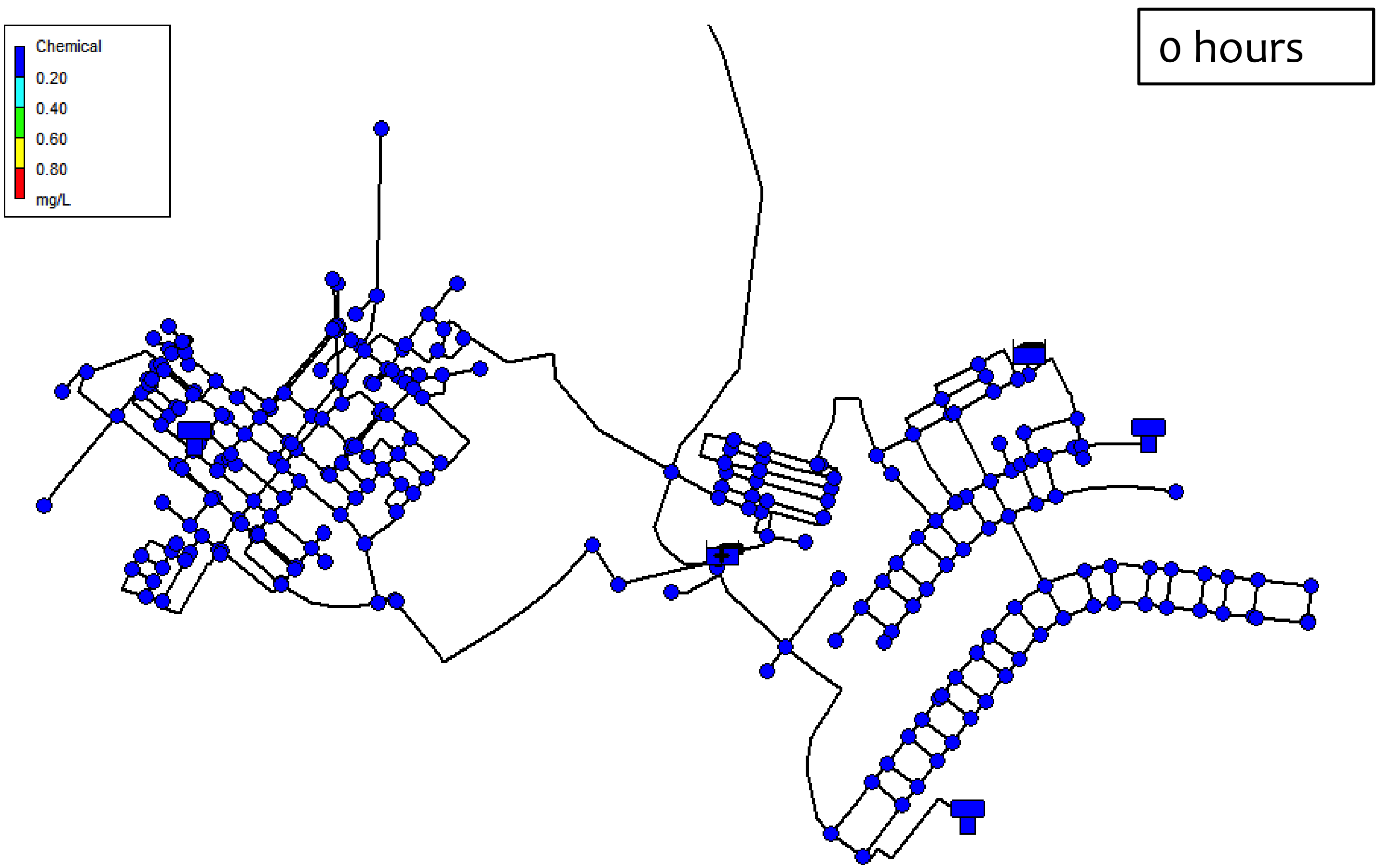


What would happen if this reservoir was contaminated?

FORCES FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

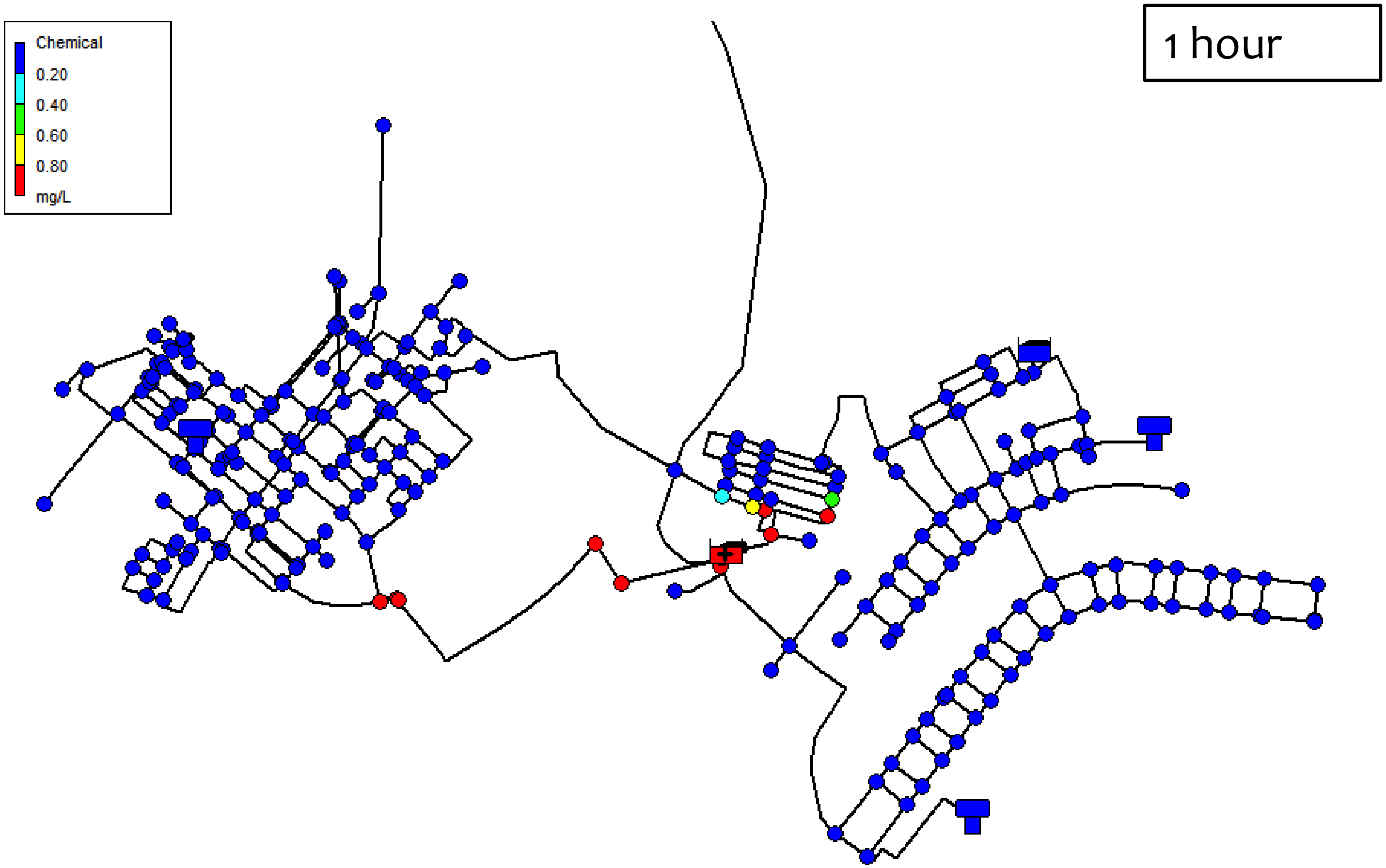
Contamination in Water-Distribution Networks

* Simulation using EPANET



Contamination in Water-Distribution Networks

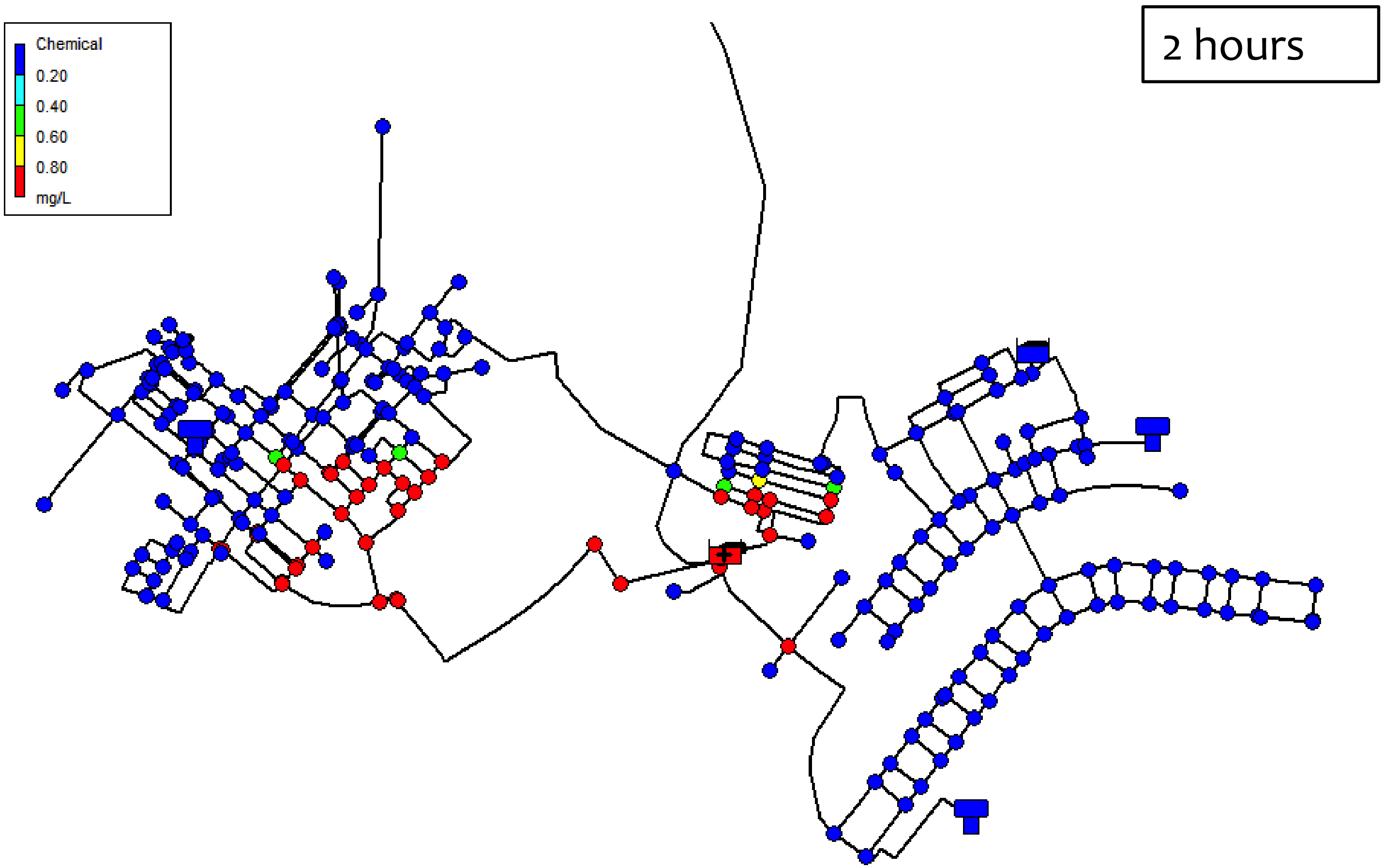
* Simulation using EPANET



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Contamination in Water-Distribution Networks

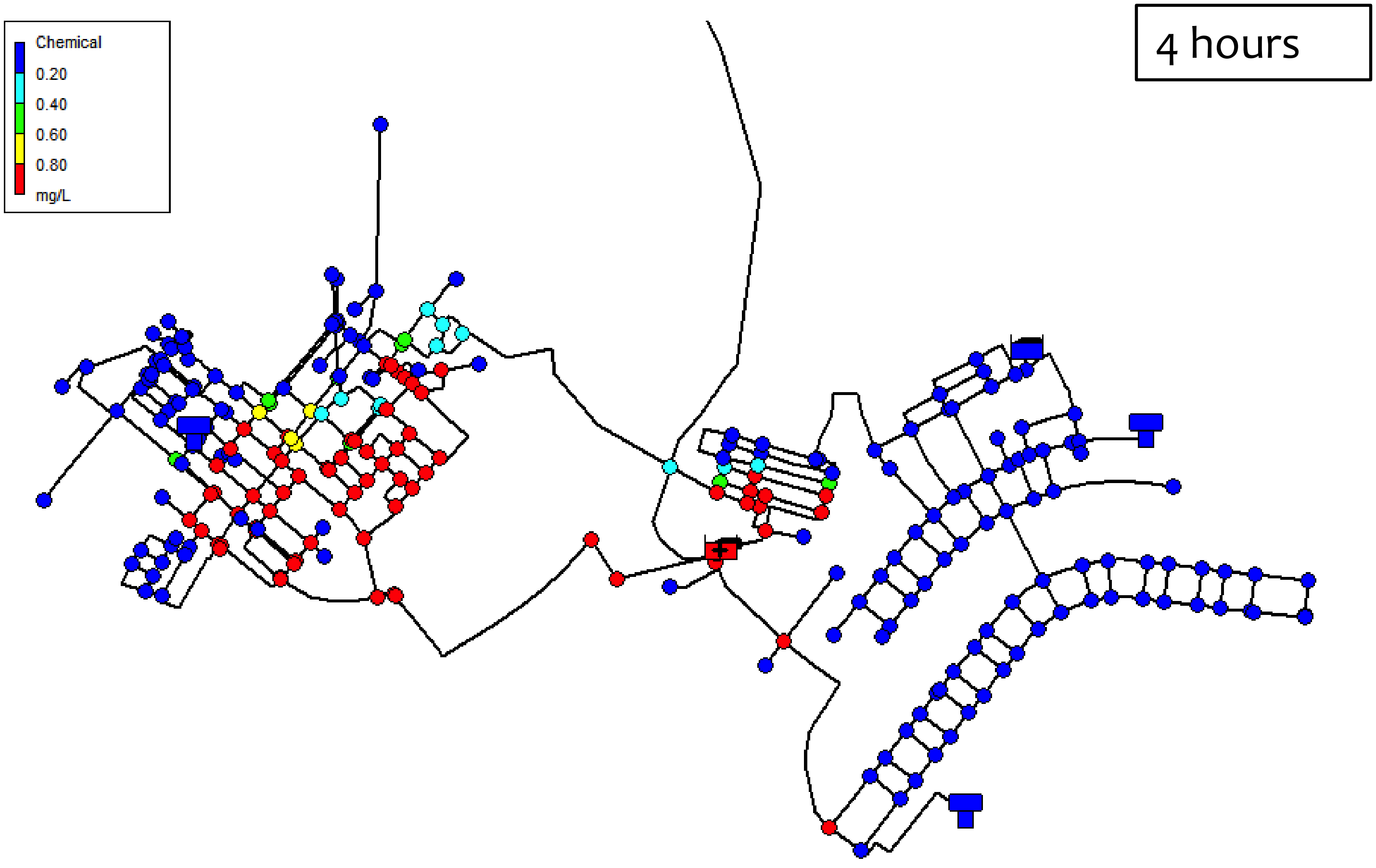
* Simulation using EPANET



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Contamination in Water-Distribution Networks

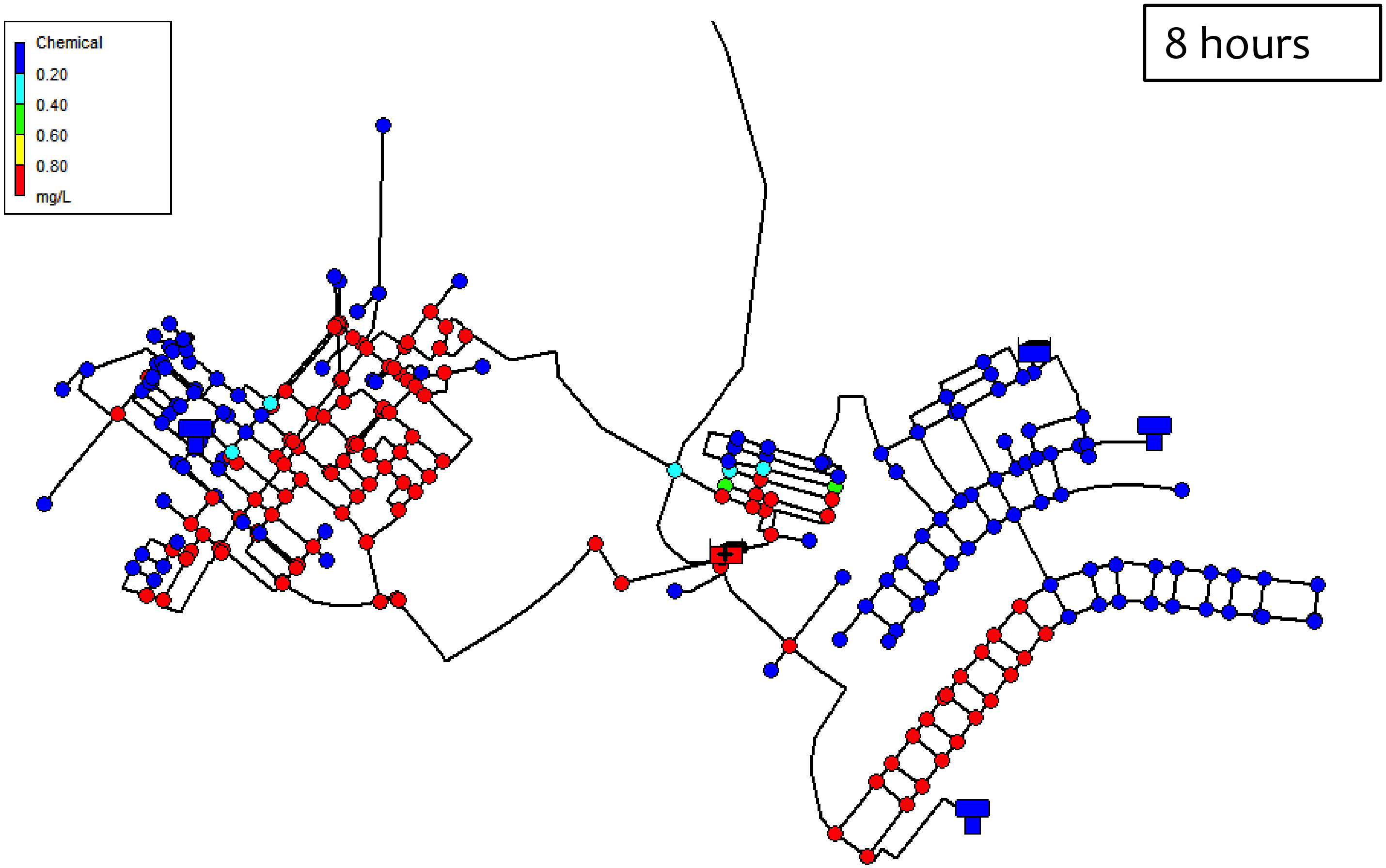
* Simulation using EPANET



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Contamination in Water-Distribution Networks

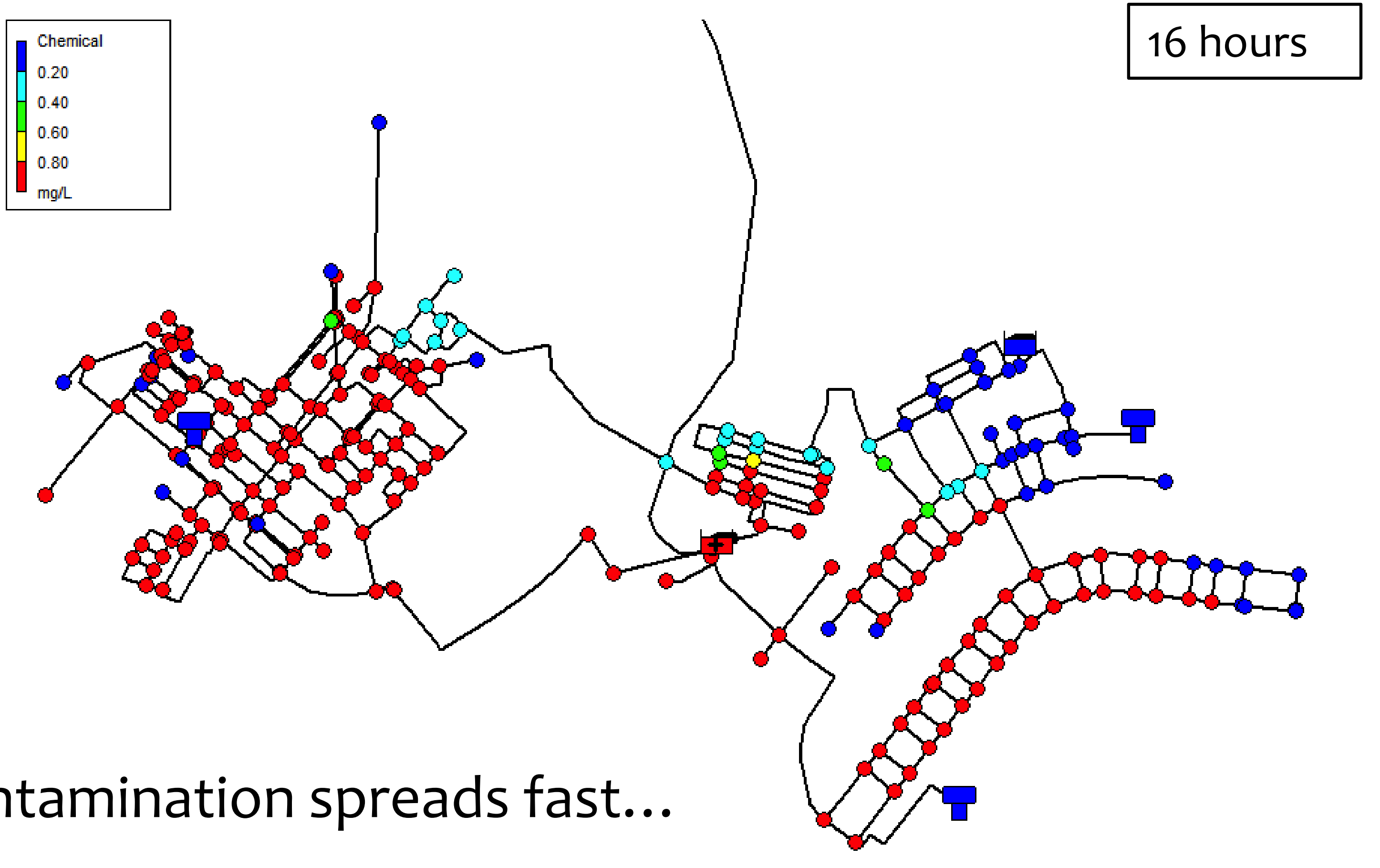
* Simulation using EPANET



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Contamination in Water-Distribution Networks

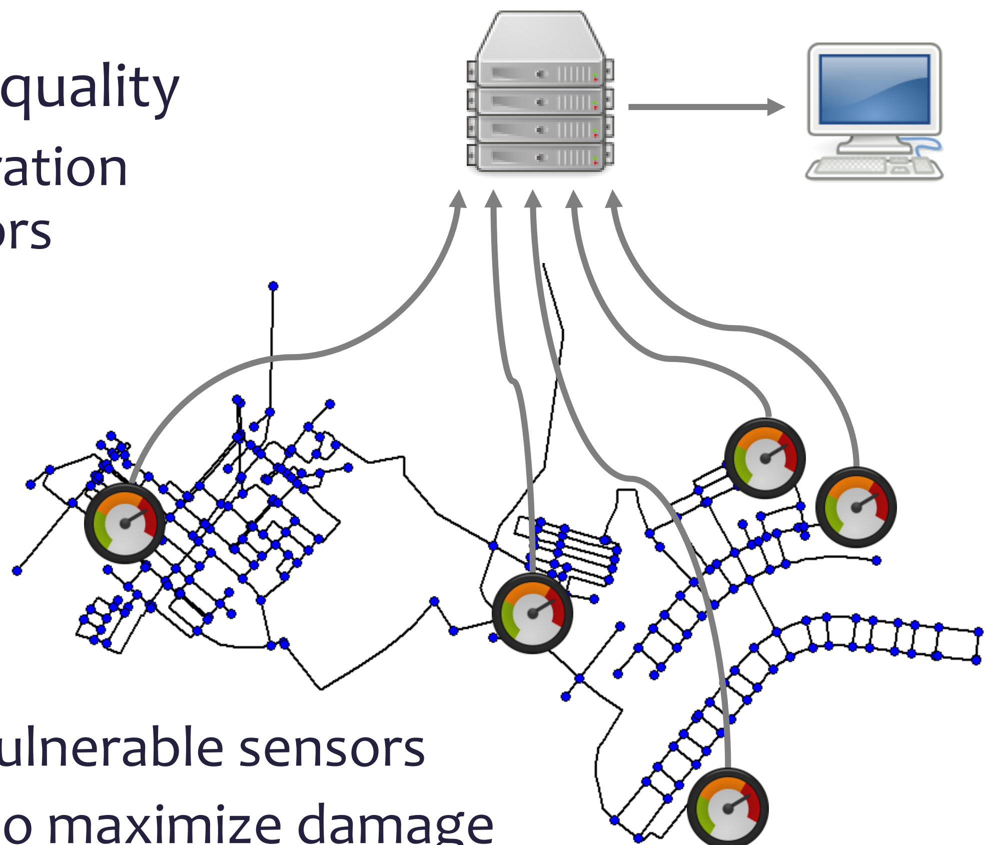
* Simulation using EPANET



Contamination spreads fast…

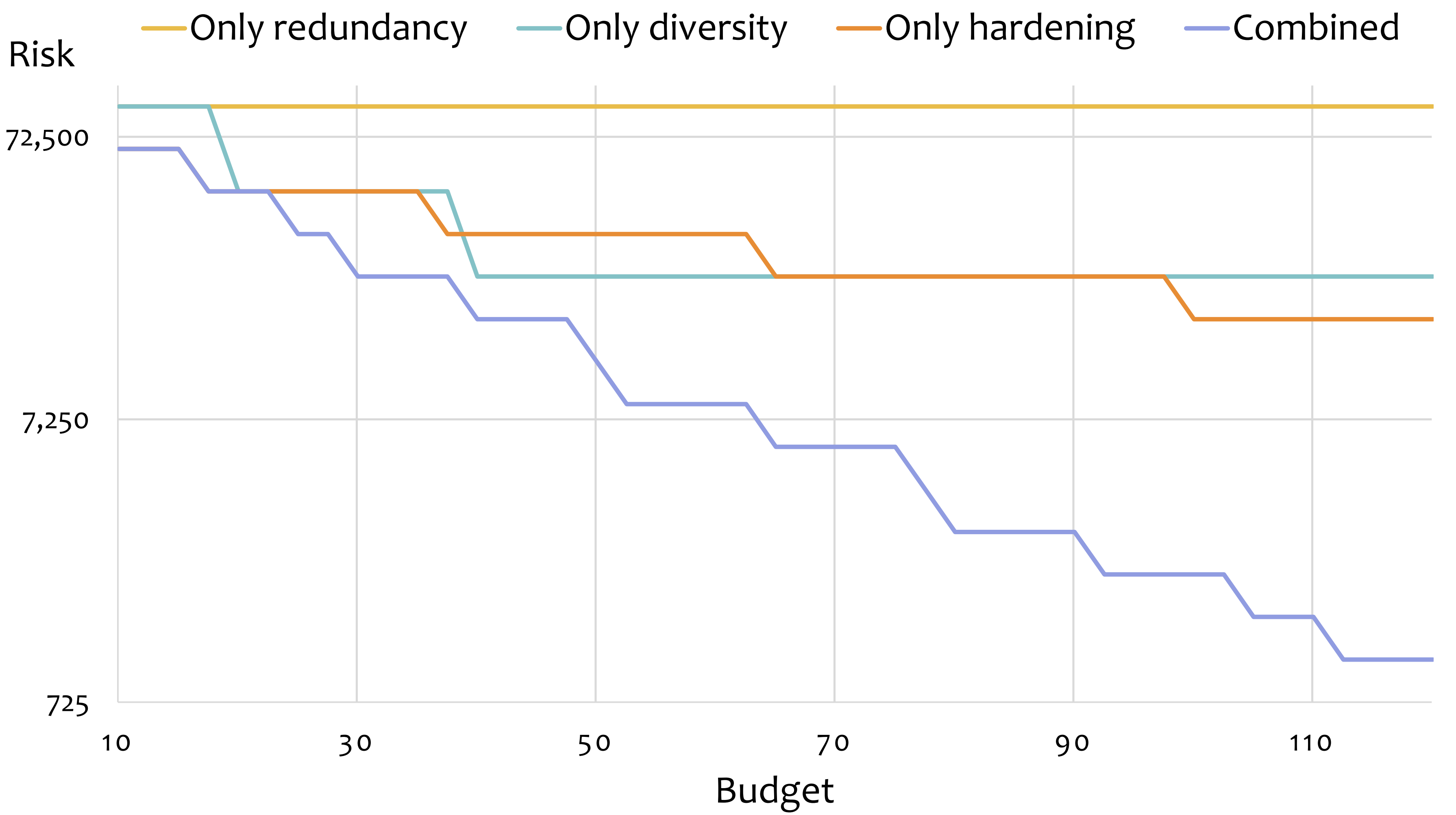
Monitoring Water Quality

- We can deploy sensors that continuously monitor water quality
  - When contaminant concentration reaches a threshold, operators are alerted
- Impact: Amount of contaminants consumed by the residents before detection
- Cyber-physical attack
  - Compromises and disables vulnerable sensors
  - Contaminates the reservoir to maximize damage

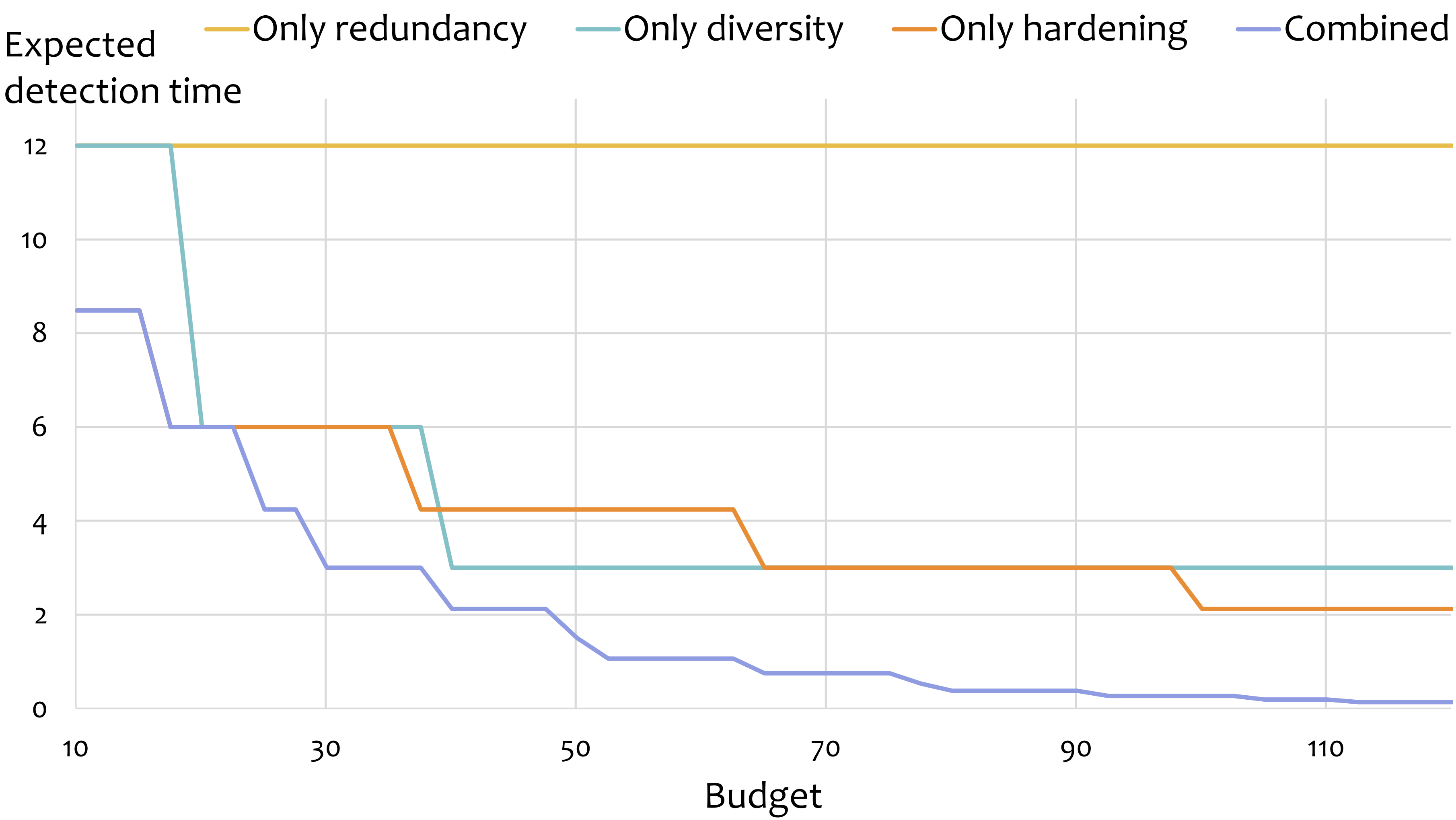


- Defender deploys sensors by combining redundancy, diversity, and hardening to improve resilience

Security Risks

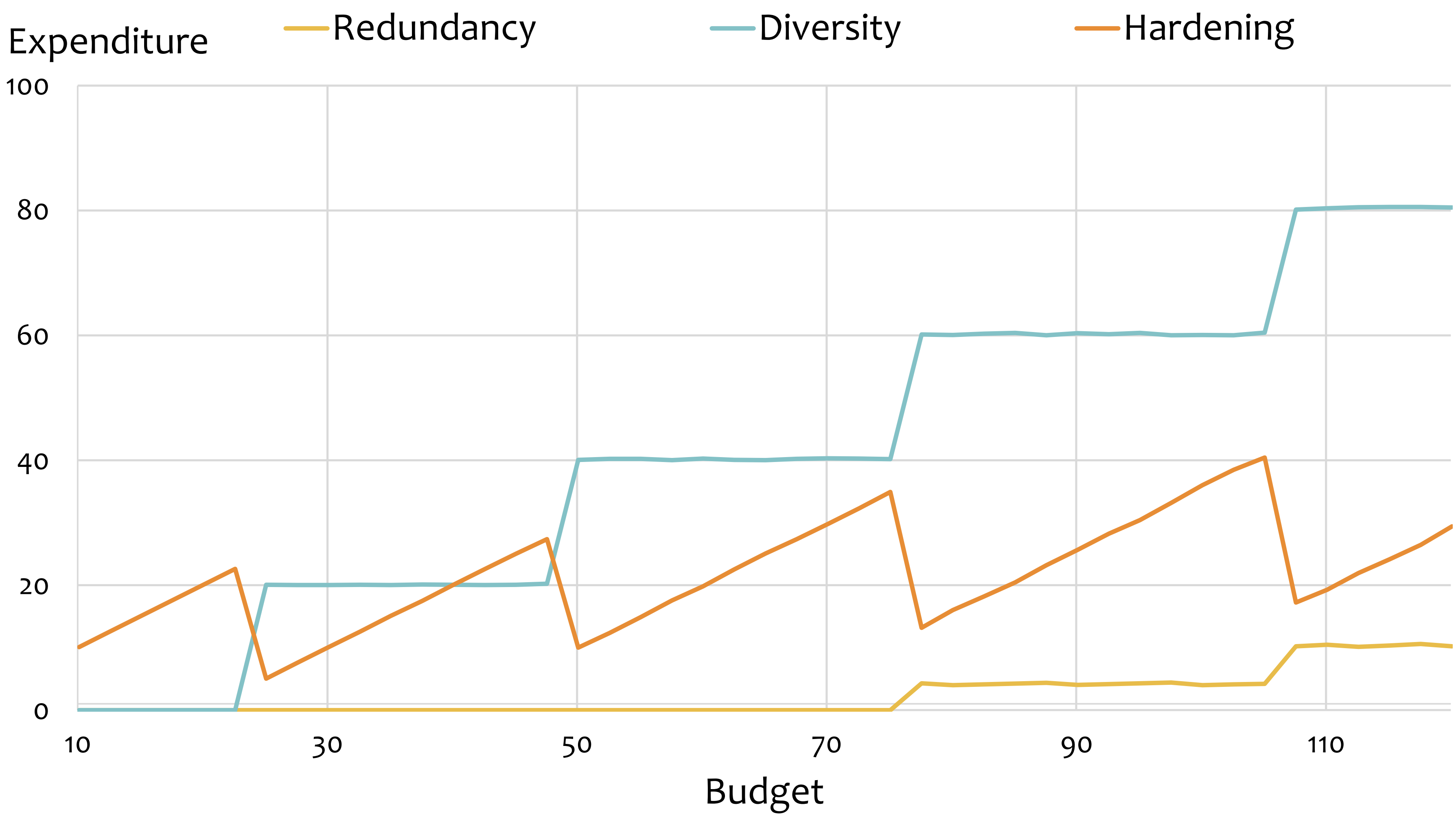


Expected Detection Time



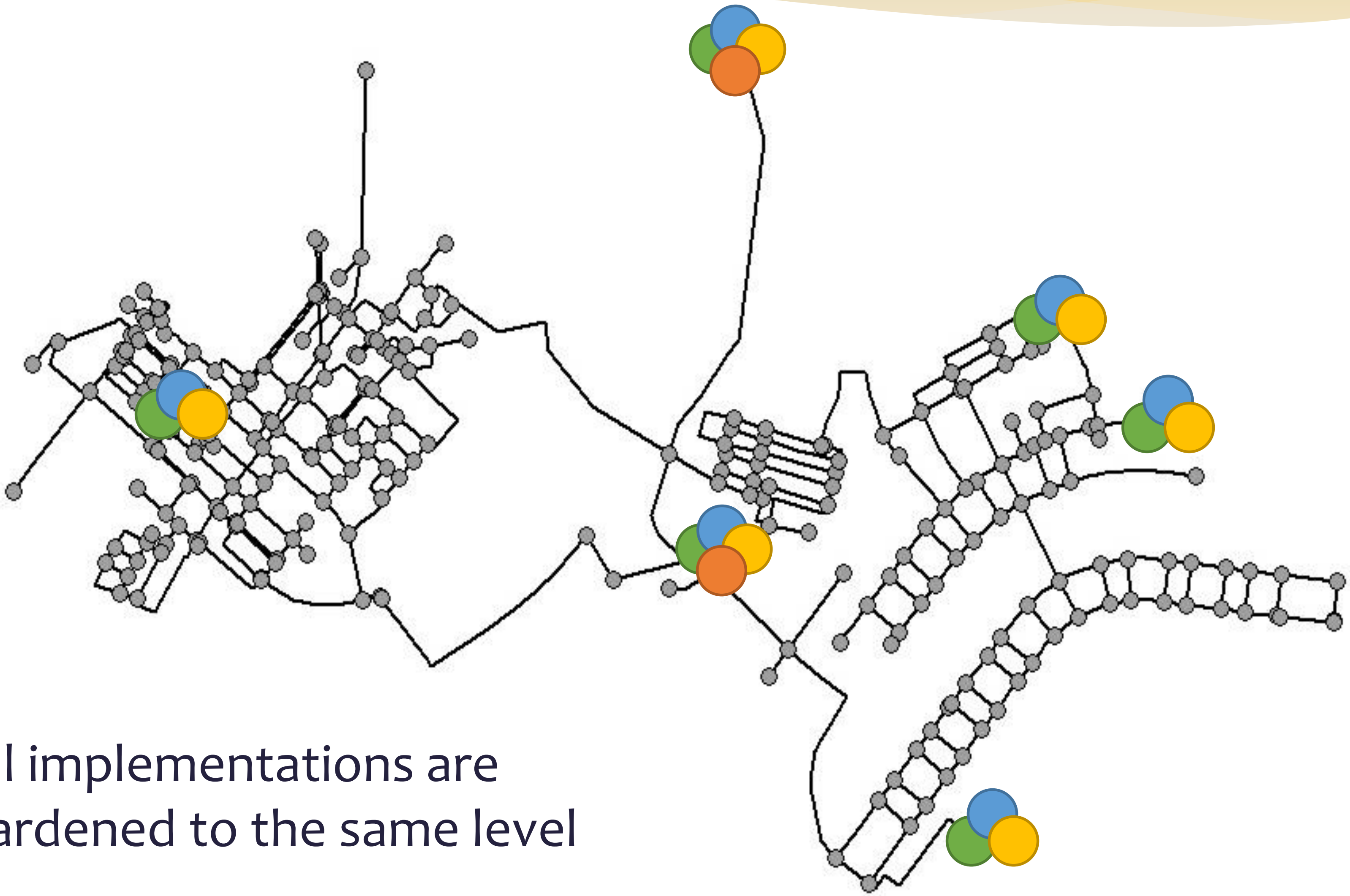
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Optimal Allocation of Investments



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Optimal Deployment ($\boldsymbol{B}$ = 90)

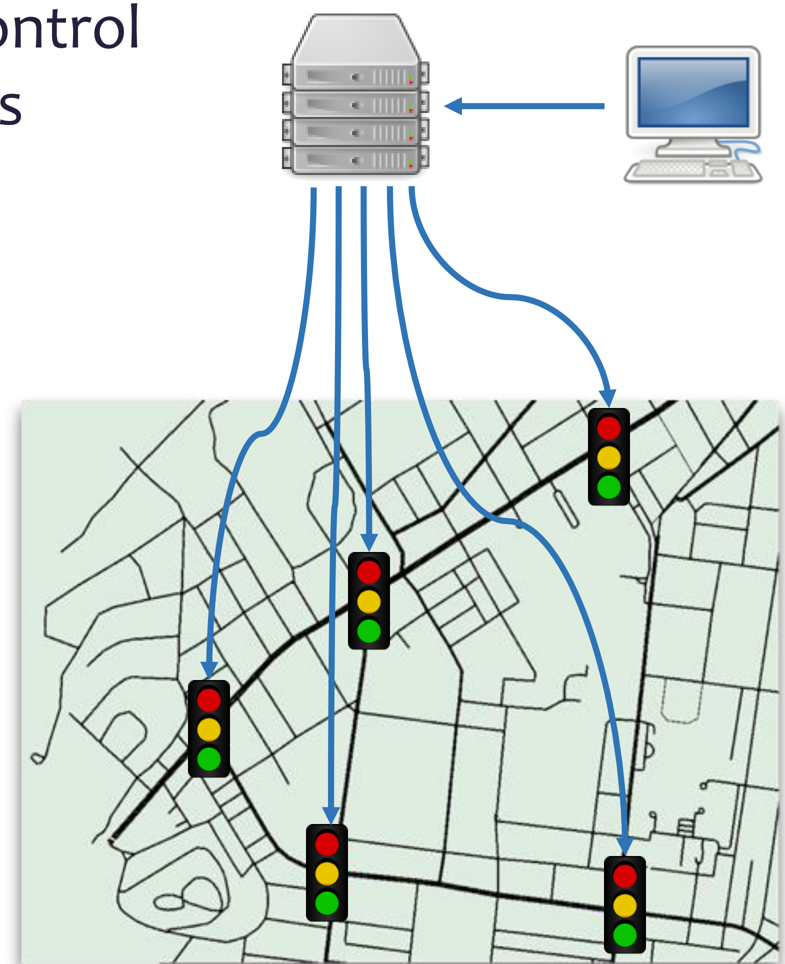


- All implementations are hardened to the same level

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Transportation Network

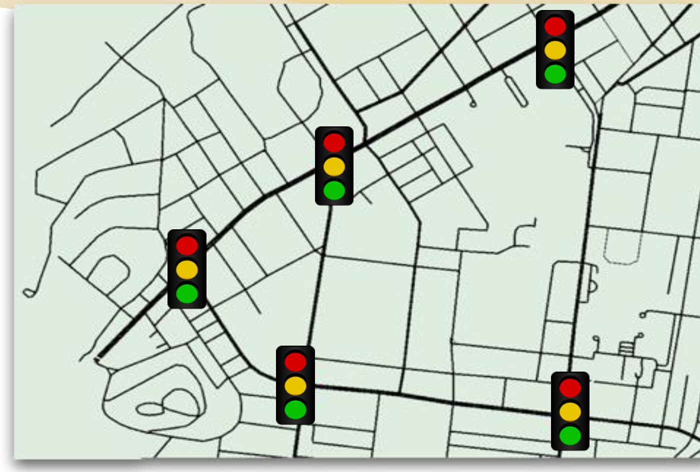
* Attacker may tamper with traffic control systems in order to cause disastrous traffic congestions
* Component
  * Embedded computers deployed at an intersection
  * Control of traffic lights
  * Compromised components may be used by an attacker to disrupt traffic in the intersection



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Transportation Network Risk Model

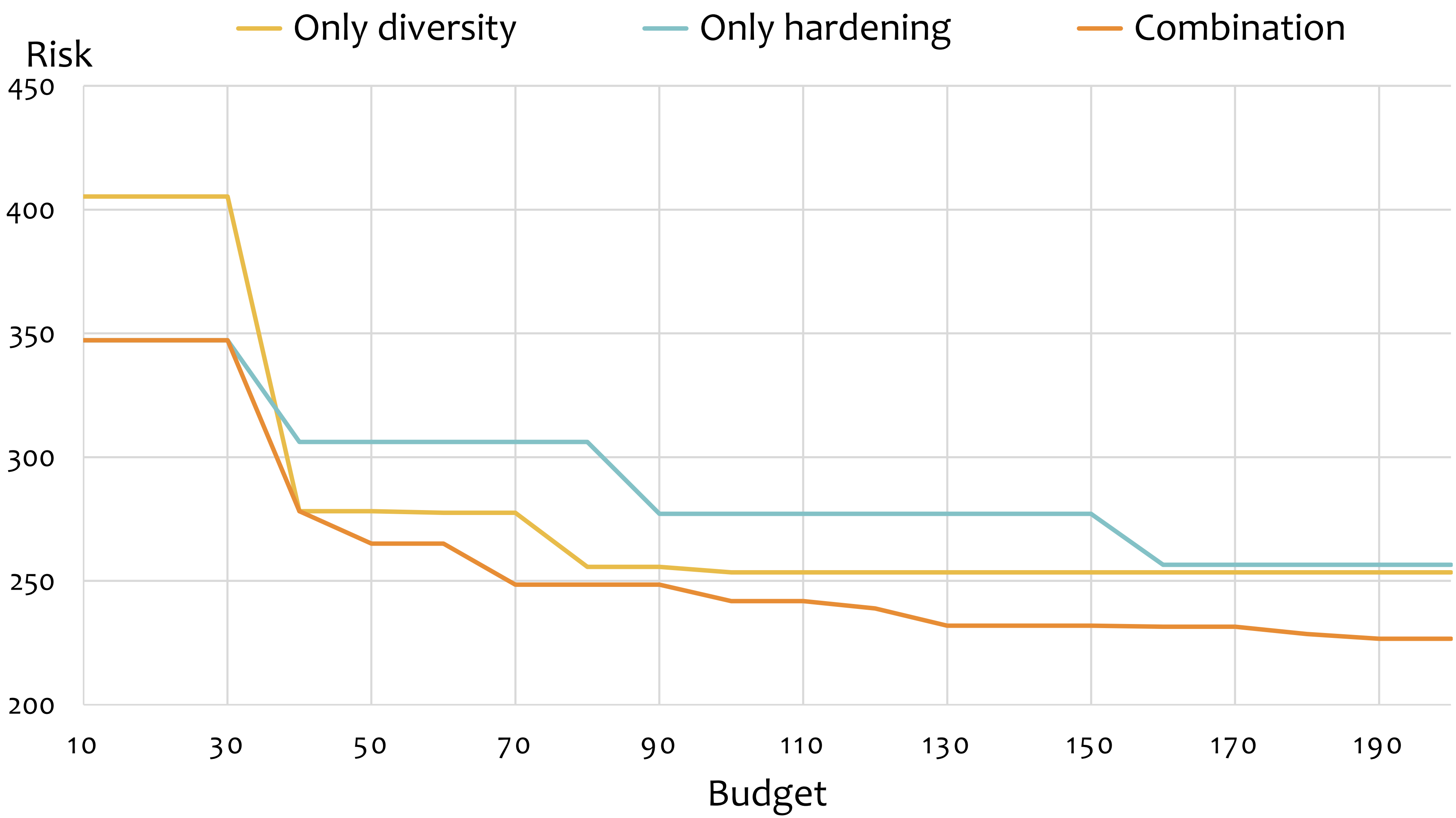
* We do **not consider redundancy** in this case since deploying redundant traffic light controllers requires additional assumptions
* Diversity is based on different software/hardware implementations
* Hardening an implementation decreases the probability that the implementation has an exploitable vulnerability
* The attacker compromises all components whose implementation is vulnerable, and it shuts down the traffic lights corresponding to the compromised components
* Traffic then flows through the transportation network using only uncompromised intersections, and the impact is simply the travel time of the vehicles.



* Damage: Increase in travel time due to adversarial tampering with traffic control
* We can quantify impact either using simulations (inefficient) or using Daganzo's cell transmission model
  * Compromised intersections are "blocked" (no through traffic)
  * Travel time computed by solving the model using a linear program

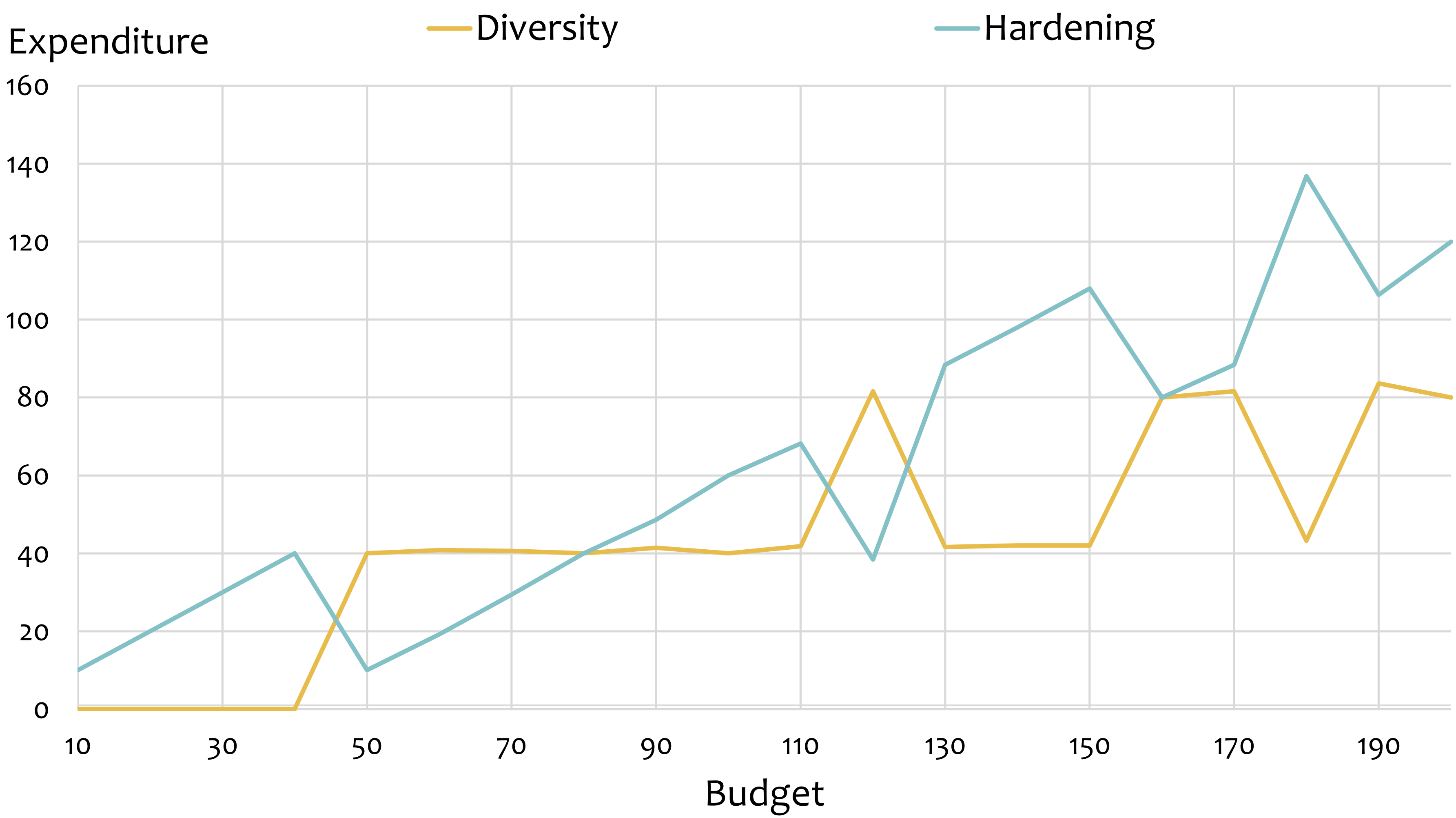
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Security Risks



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Optimal Allocation of Investments



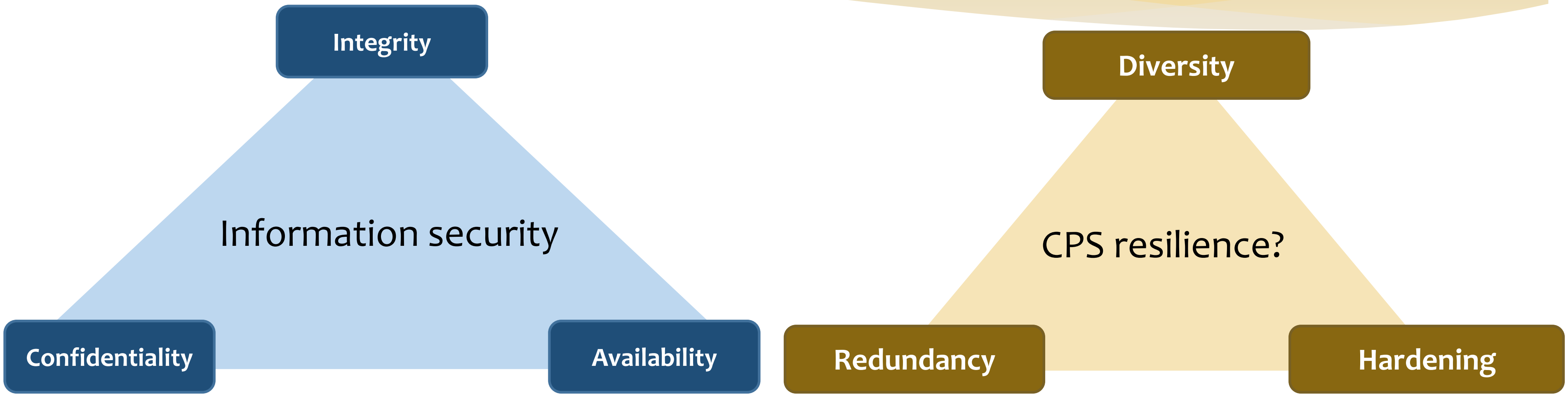
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Conclusions and Future Work

* Develop model for combining redundancy, diversity, and hardening to improve CPS resilience
* Investigate methods for sensors, actuators, computing devices, and networks links
* CPS application domains
  * Water distribution systems
  * Transportation systems
  * Power networks
* Develop analytical methods for improving structural robustness in networks

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Basic Components of CPS Resilience



* The basic components of information security are confidentiality, integrity, and availability and have been used extensively to shape the science and technology of computer security.
* What are the main components of CPS resilience?
* How can we shape research efforts in developing CPS resilient architectures so that we understand and quantify the impact of each proposed solution?
* How do we organize, analyze, integrate, and evaluate the broad range of techniques that are available?