Agent-based Cyber Control Strategy Design for Resilient Control Systems: Concepts, Architecture and Methodologies

Craig Rieger[1], Quanyan Zhu[2] and Tamer Başar[2]

[1]Idaho National Laboratory

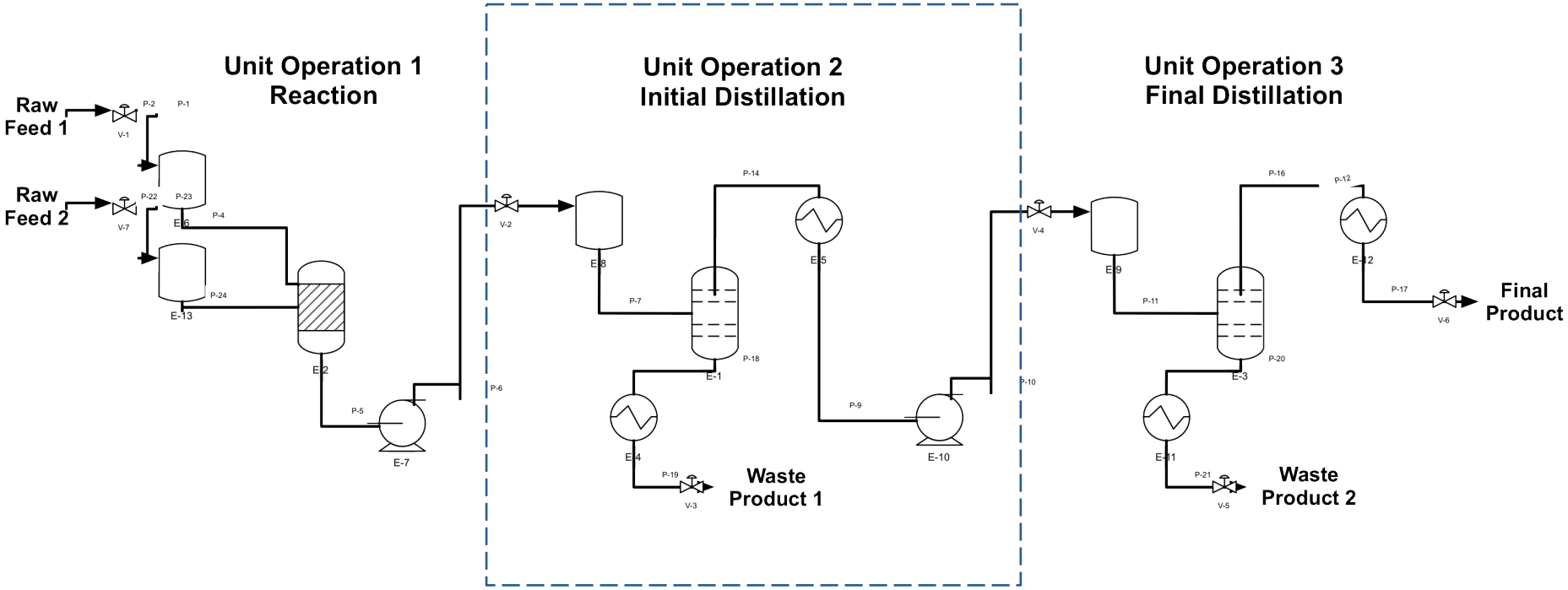
[2]Coordinated Science Laboratory
University of Illinois at Urbana-Champaign

5th International Symposium on Resilient Control Systems
Salt Lake City, Aug. 14-16, 2012

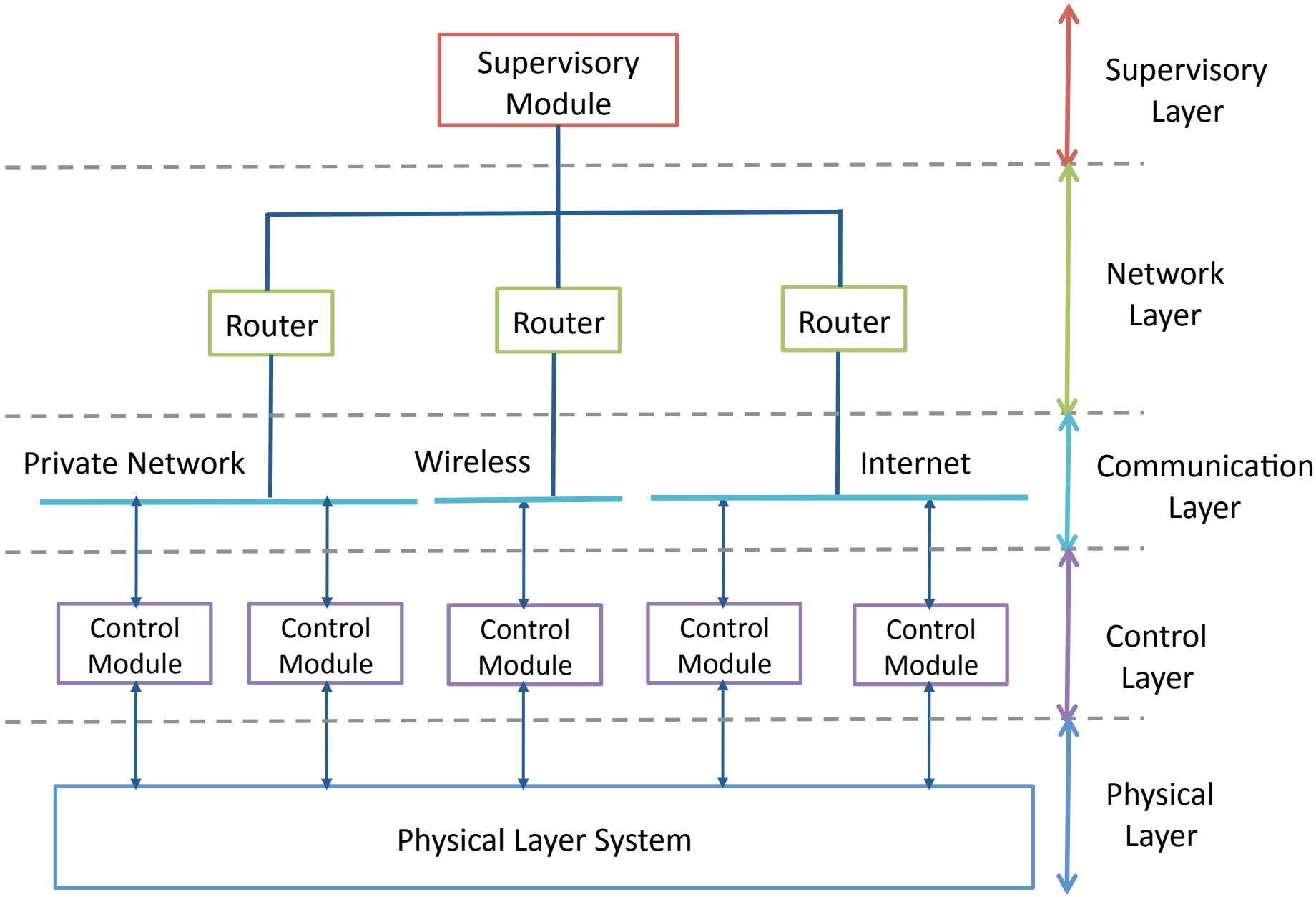
- Introduction and Motivation
- Active and Passive Cyber Defense
  - Feedback Cyber Control
  - Open-loop Cyber Control
- Resilient Cyber Control
- Agent-Based Methodologies
- Hierarchical Layers in Multi-Agent Systems
- Conclusions and Future Work

Resilient Control Systems (RCS) is defined as a control system that maintains *state awareness* and accepted level of *operational normalcy* in *response* to *disturbances*, including *threats* of an *unexpected* and *malicious* nature.

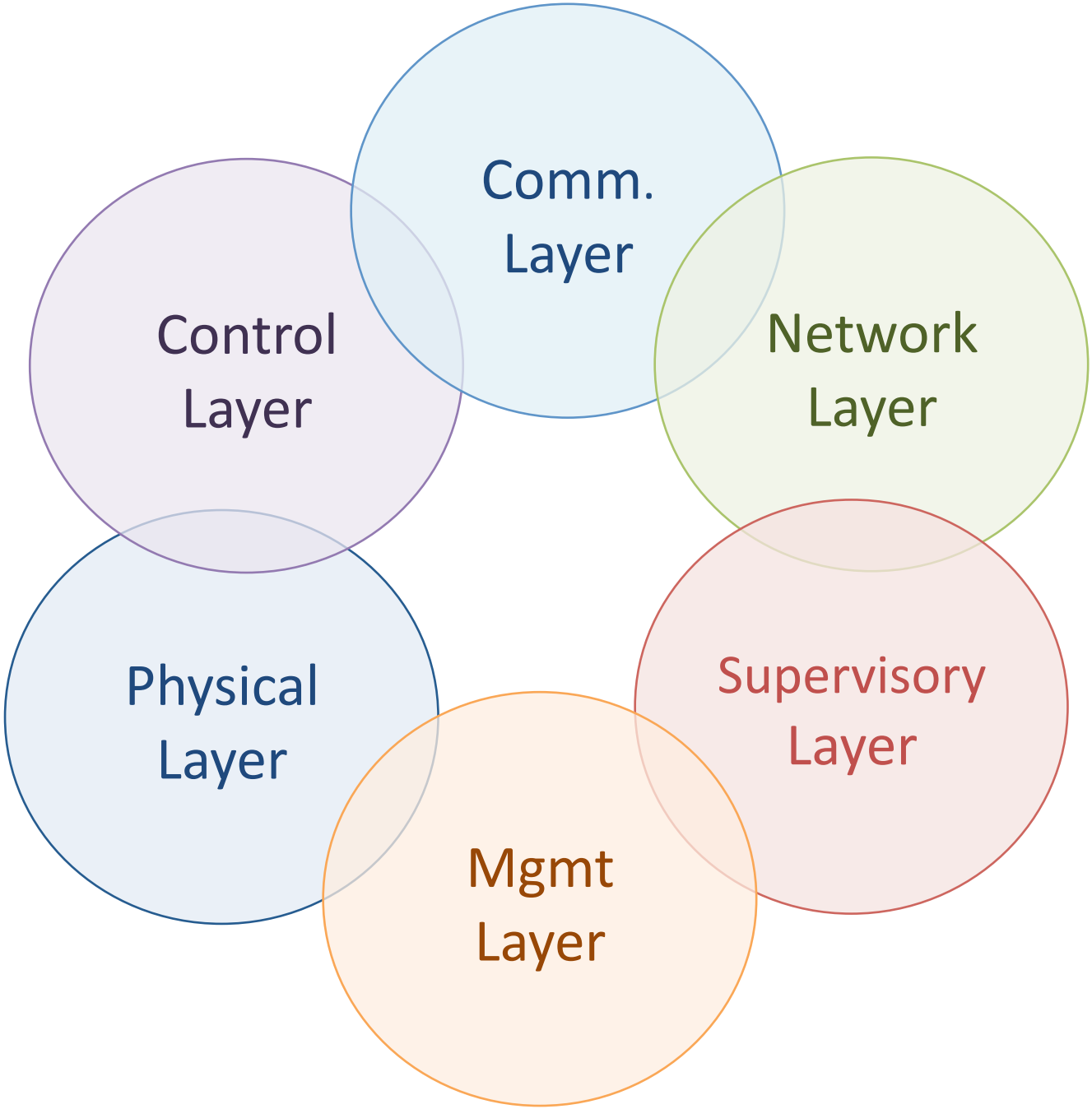
Idaho National Laboratory

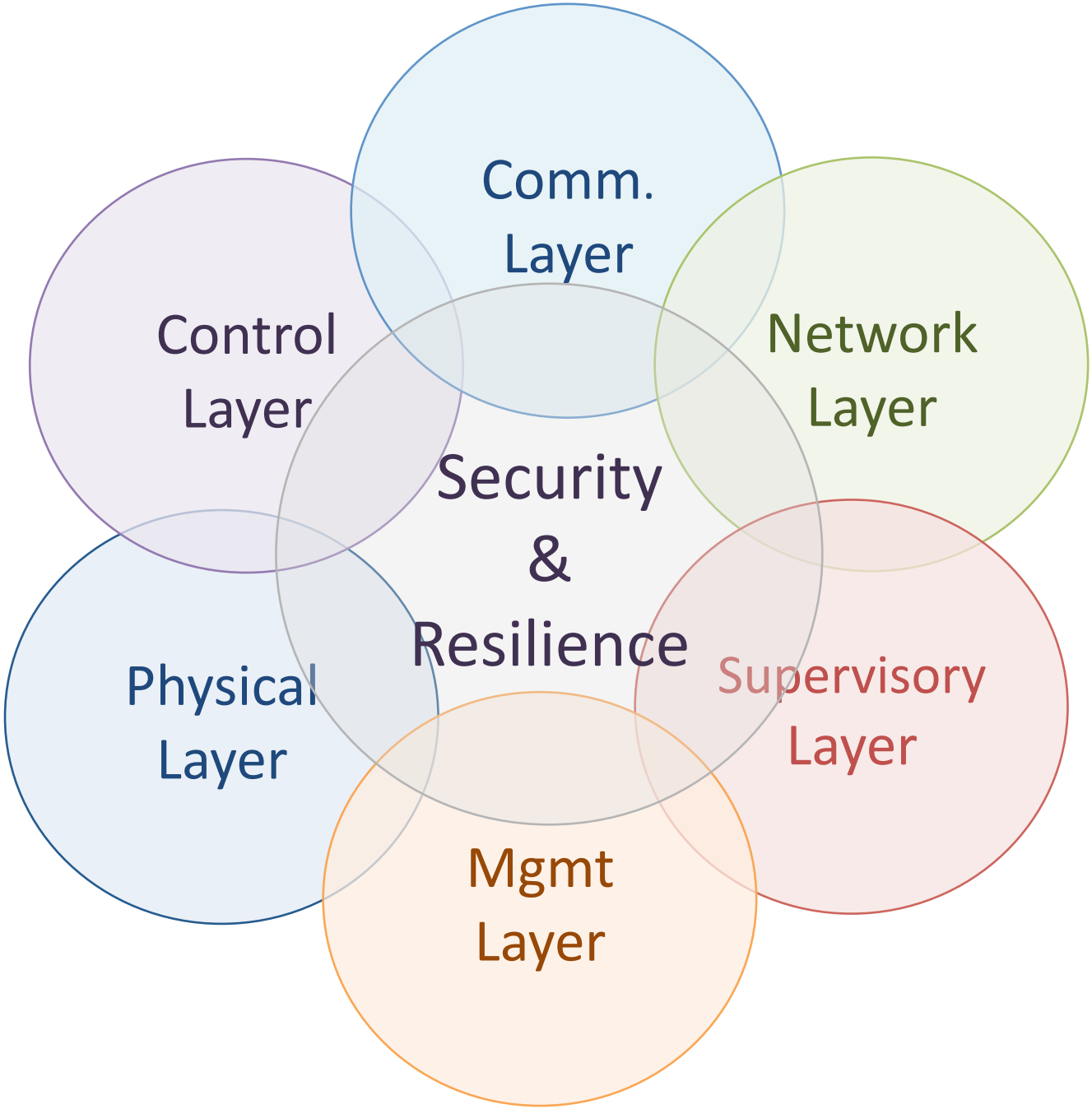


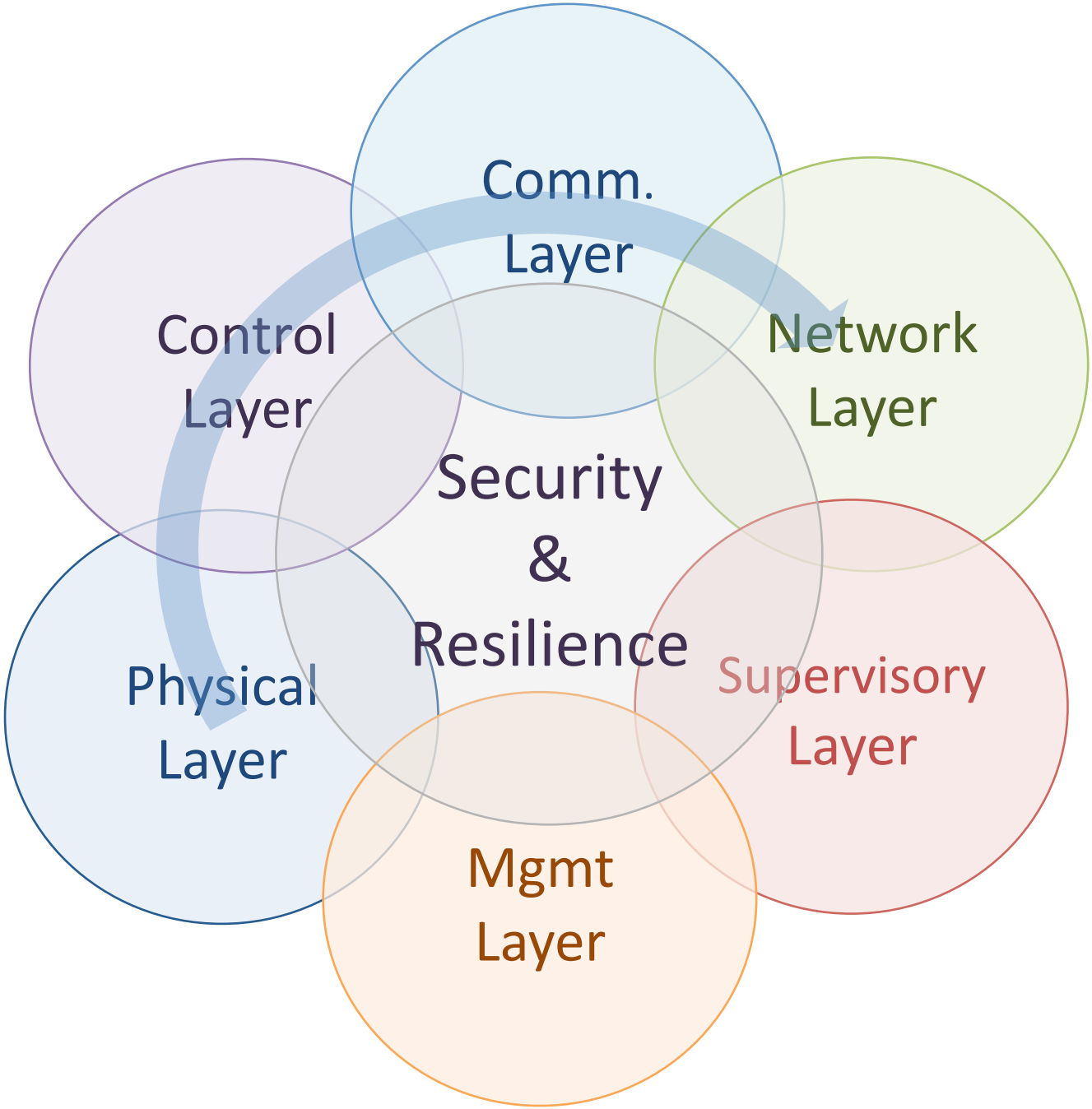
An Example of Industrial Control Systems: Series of Unit Operations of Chemical Plants

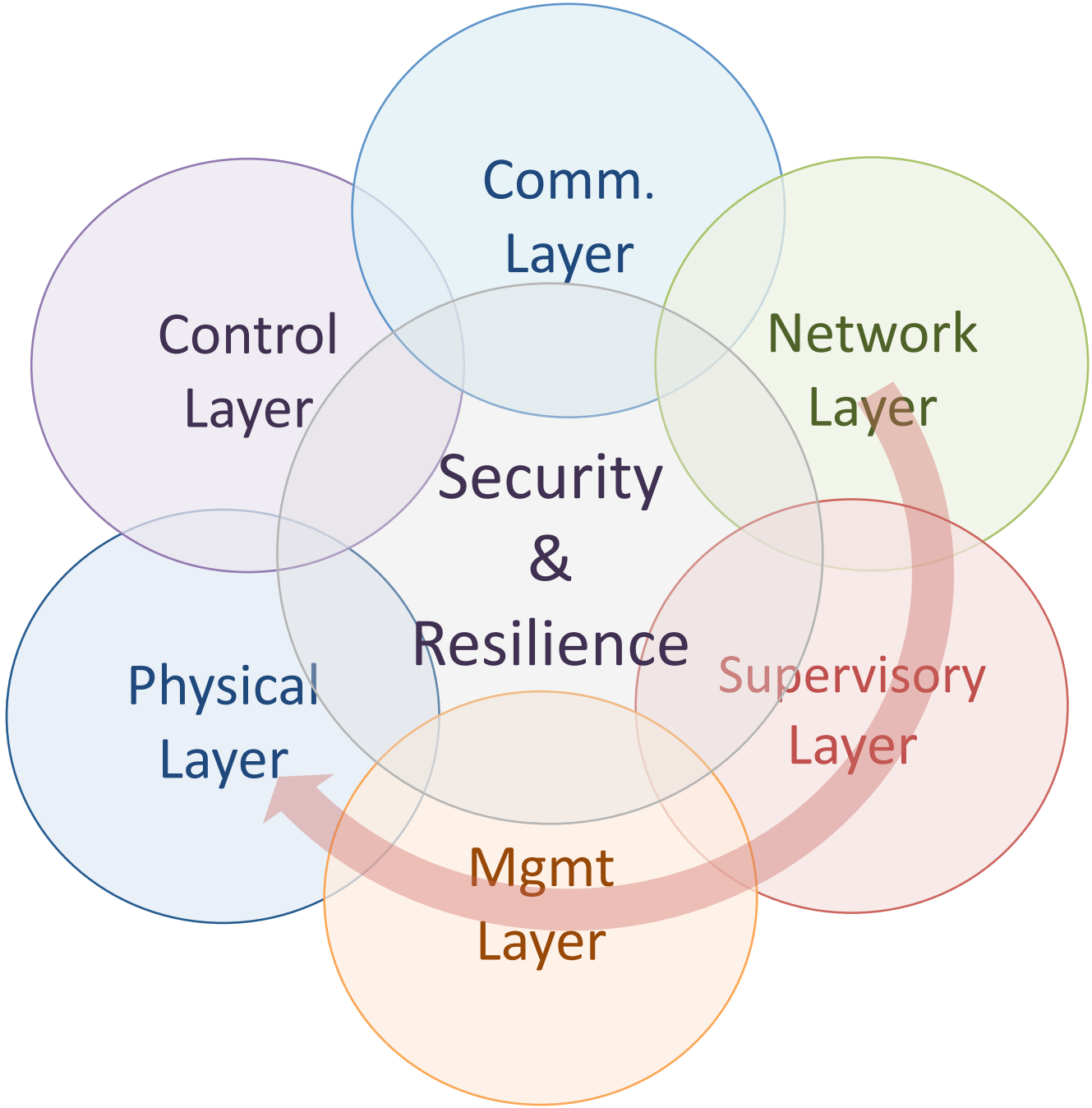


Example: Architecture of CPS Control Systems


Comm.
Layer
Control
Layer
Network
Layer
Physical
Layer
Supervisory
Layer
Mgmt
Layer

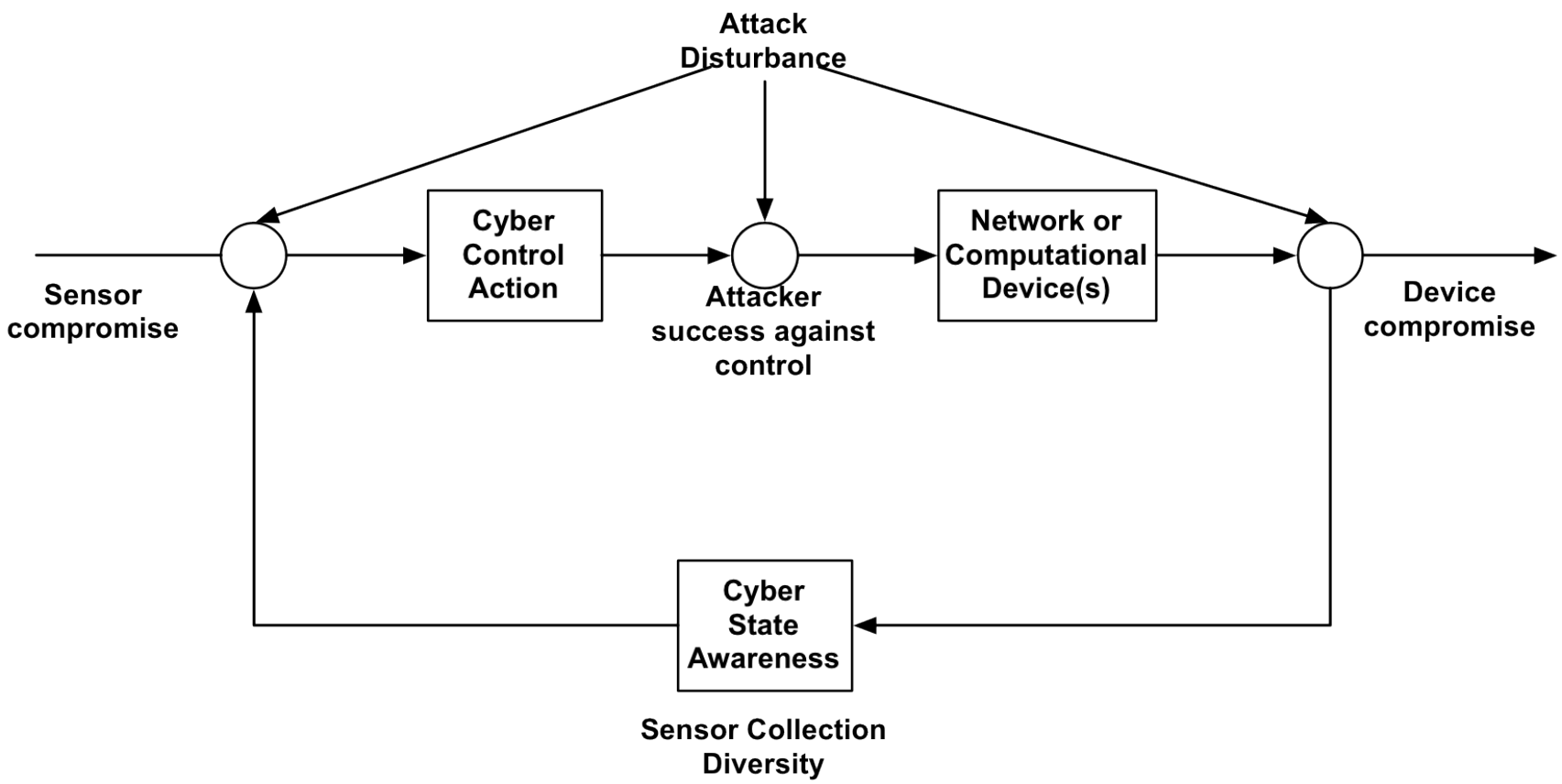

Comm.
Layer
Control
Layer
Network
Layer
Security
&
Resilience
Physical
Layer
Supervisory
Layer
Mgmt
Layer


Comm.
Layer
Control
Layer
Network
Layer
Security
&
Resilience
Physical
Layer
Supervisory
Layer
Mgmt
Layer

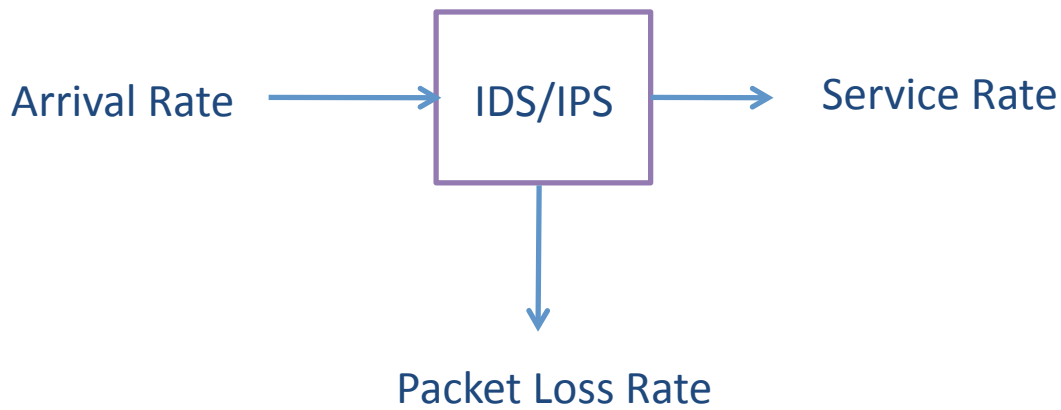

Comm.
Layer
Control
Layer
Network
Layer
Security
&
Resilience
Physical
Layer
Supervisory
Layer
Mgmt
Layer

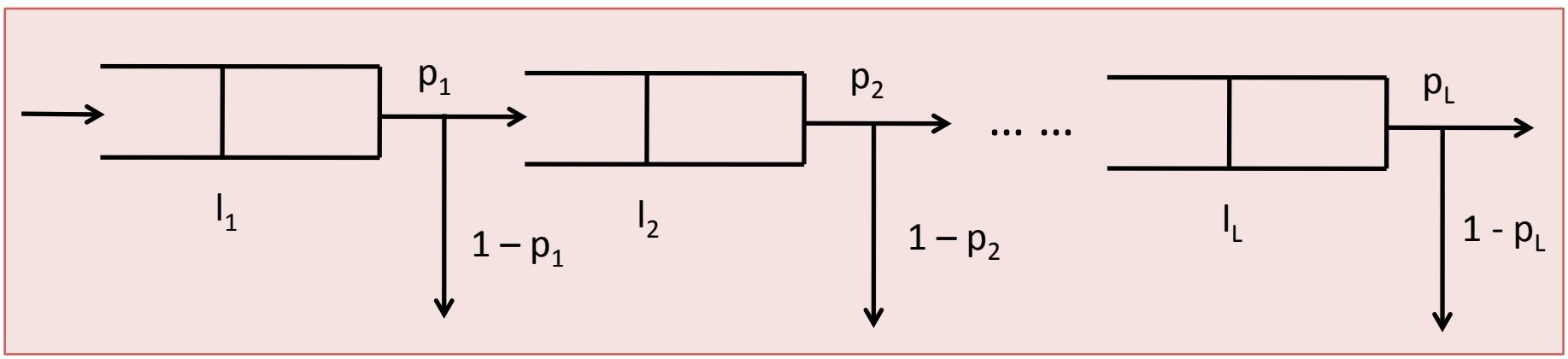
…maintains ***state awareness*** and accepted level of *operational normalcy* **in *response* to** *disturbances*, including *threats* of an *unexpected* and *malicious* nature.

Closed Loop Cyber Control



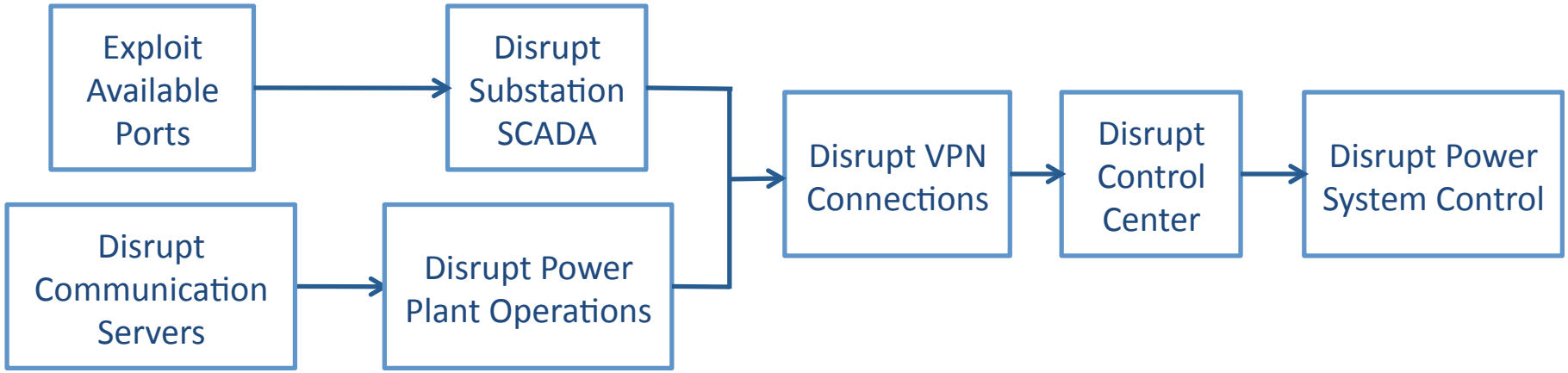
Example 1: Dynamic Configurations of Intrusion Detection Systems





- $1 - p_i$: packet drop rate
- μ_i : service rate
- M/M/1 queue

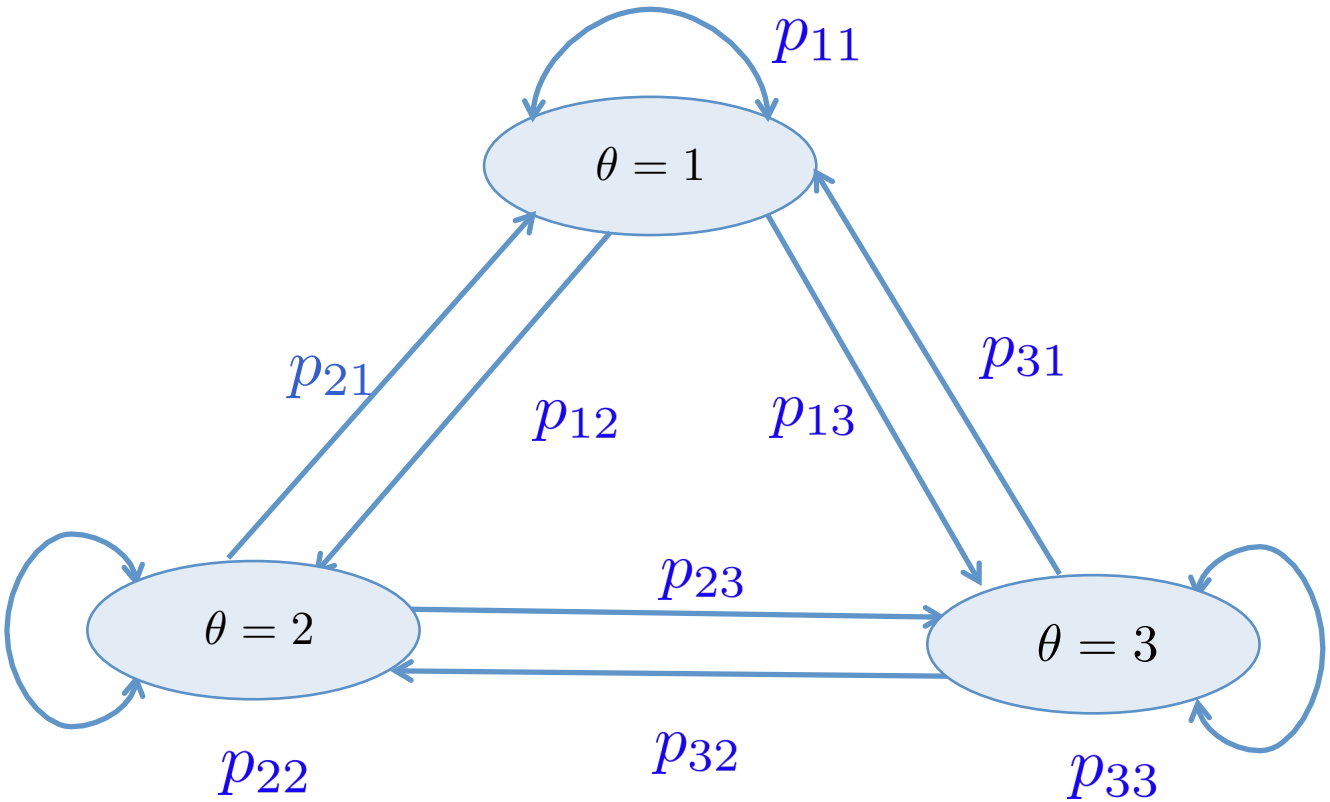
[Zhu and Başar, CPSWeek 2011]




```
alert tcp any any -> any 7580 (msg:"ETPRO SCADA
Siemens Tecnomatix FactoryLink CSService GetFile
path Buffer Overflow"; flow:to_server,established;
content:"LEN|00|"; depth:4; byte_test:4,>,
1028,0,little; content:"|99|"; distance:8; within:1;
content:"|99 00 00 00 08 00 00 00 02 06|"; distance:
0; byte_test:4,>,1024,0,big; classtype:attempted-
user;reference:url,digitalbond.com/tools/quickdraw/
vulnerability-rules; sid:1111675; rev:1;)
```

A SCADA IDS rule to detect CSService CSMSG GetFile buffer overflow in Siemens Tecnomatix FactoryLink

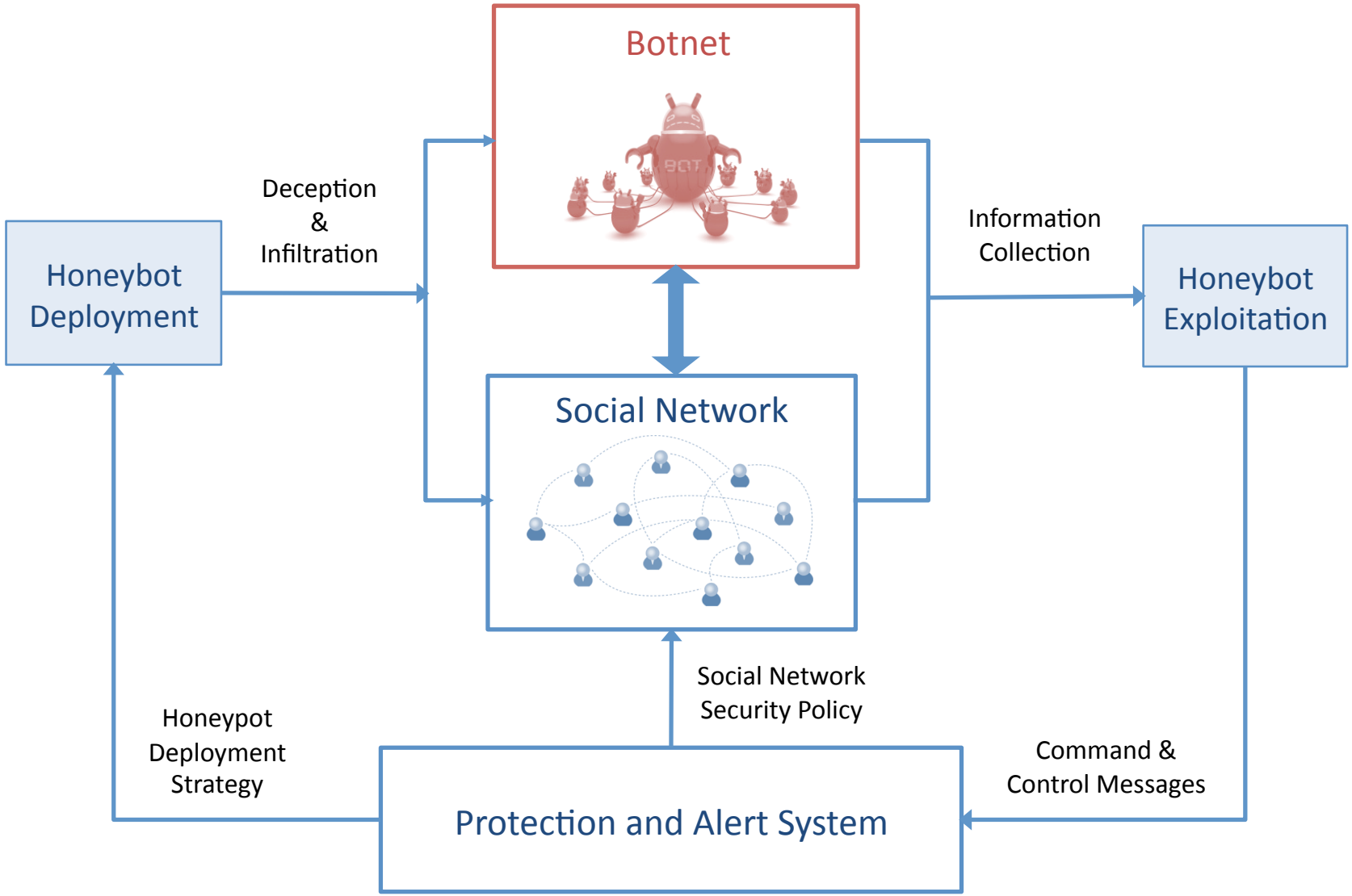
Dynamic Configuration Modeled as a Competitive Markov Decision Process



- The defender chooses a configuration policy that minimizes the long-term cost.
- The attacker chooses a sequence of attacks that maximizes the long-term cost.
- A stationary saddle-point security equilibrium is found for IDS configurations
- Online Q-learning mechanism is used to learn the adversarial environment.

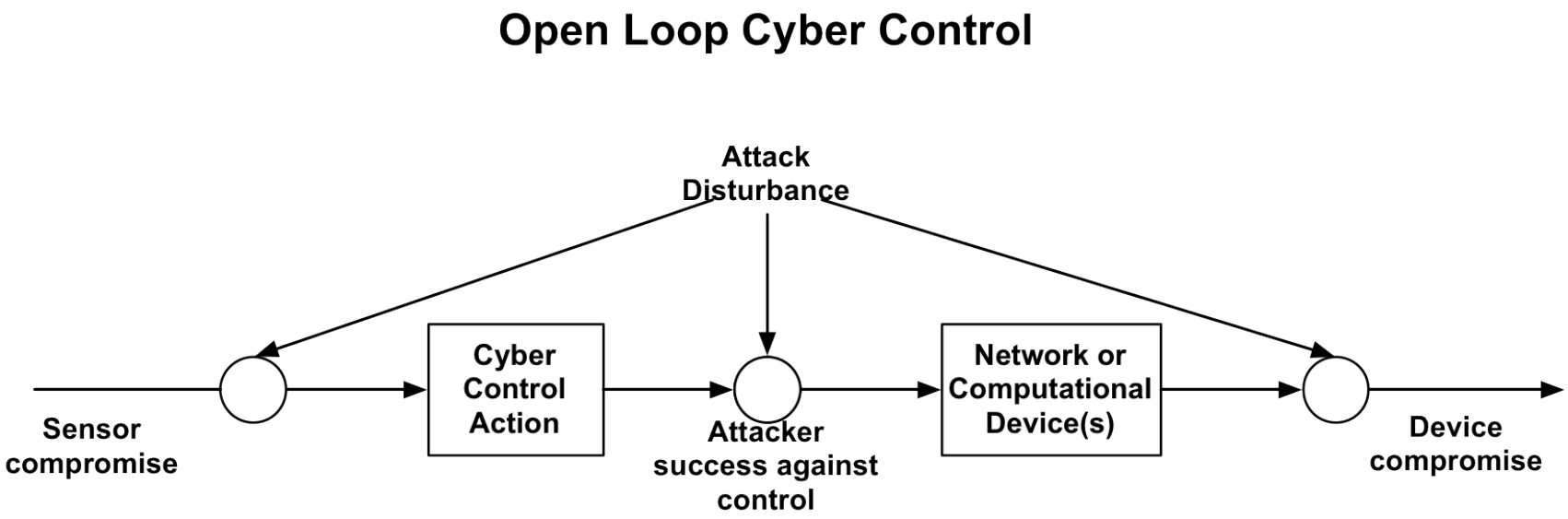
[Zhu and Başar, CDC 2009]

Example 2: Social Networks



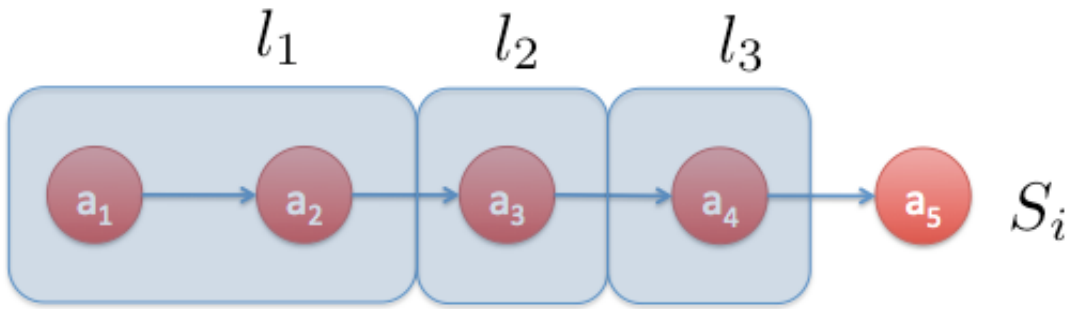
[Zhu et al., Arxiv 2012]

When measurements or observations are not viable?



- Security design with the presence of insecure components or vulnerabilities.
  - Offline default configuration
  - Randomization of system attributes

Example 1: Default Configuration



[Zhu and Başar, GameSec 2009]

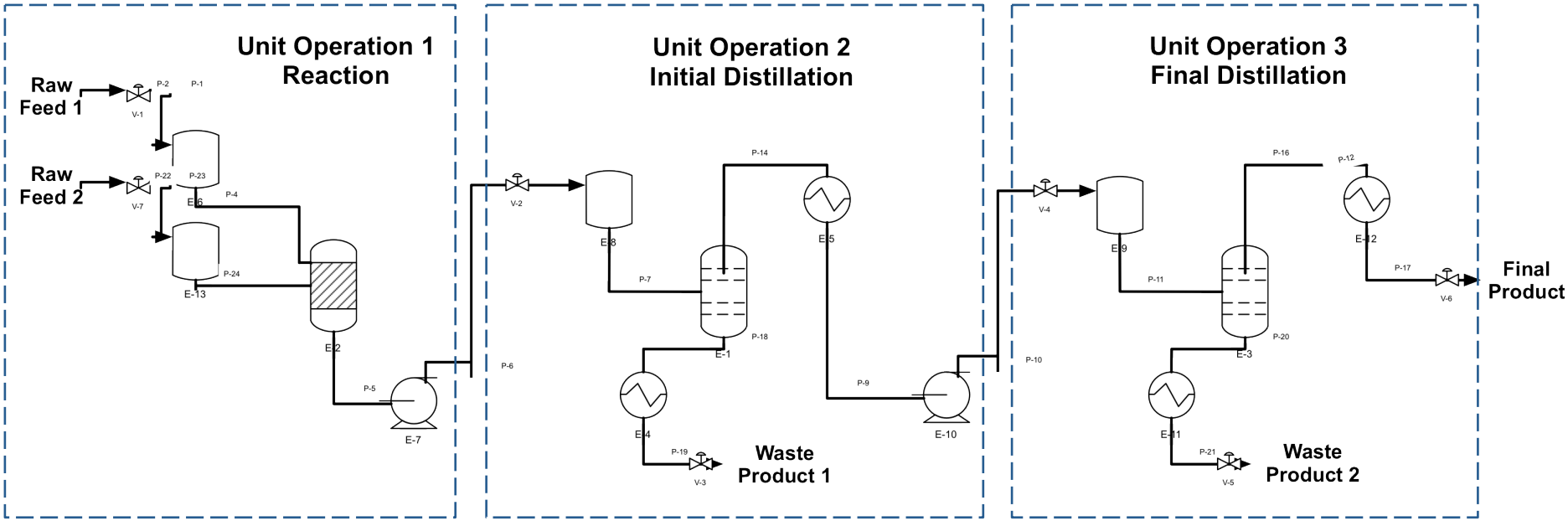
Example 2: Deceptions in Control Systems

- Seven Abstract Dimensions of Security
  - Security Group (SG) Knowledge
  - Attack Group (AG) Knowledge
  - Acccess
  - Vulnerabilities
  - Damage Potential
  - Detection
  - Recovery

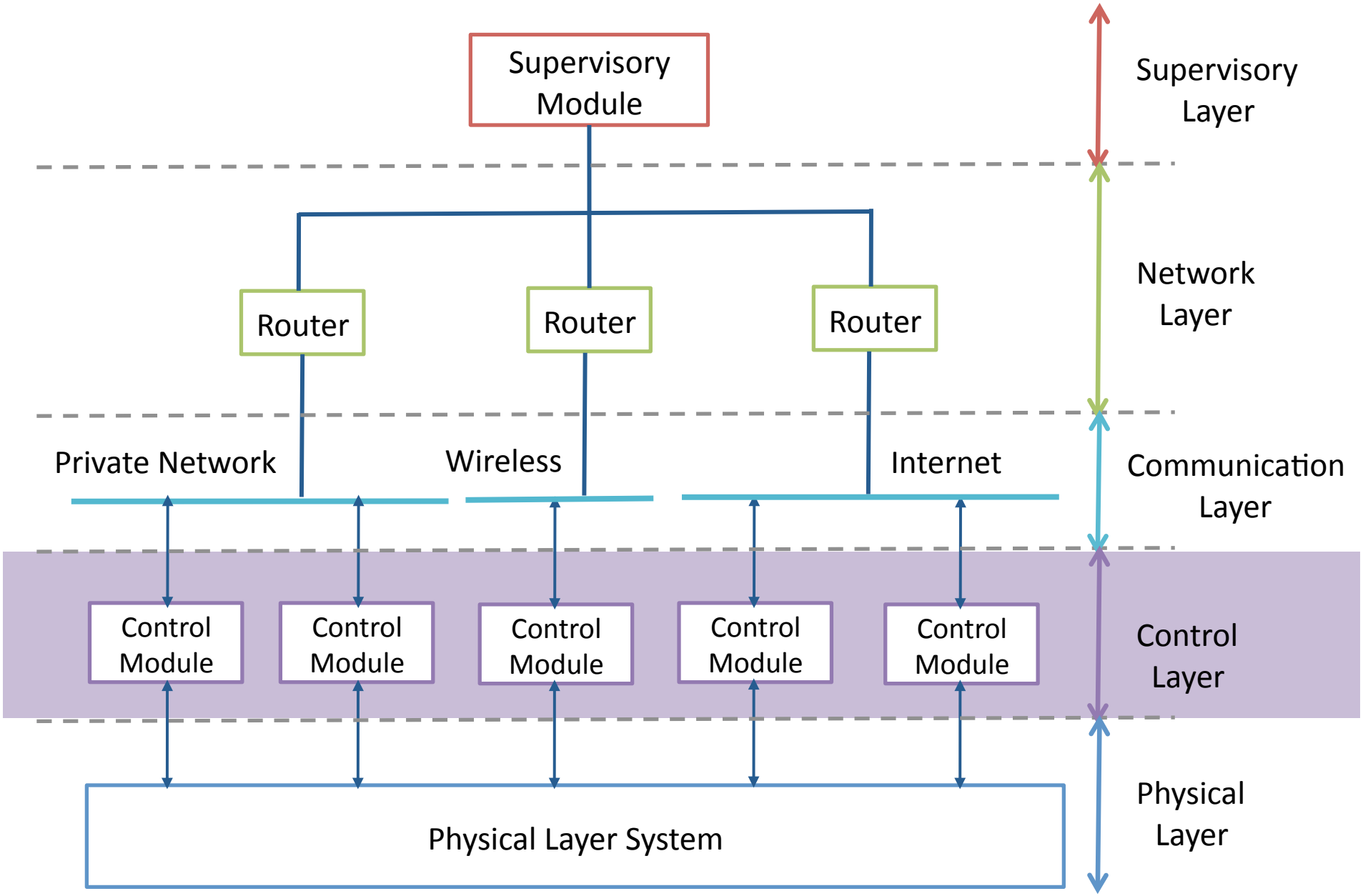
- Dissimulation
  - Masking
  - Repackaging
  - Dazzling
- Simulation
  - Inventing
  - Mimicking
  - Decoying

[McQueen and Boyer, 2009]

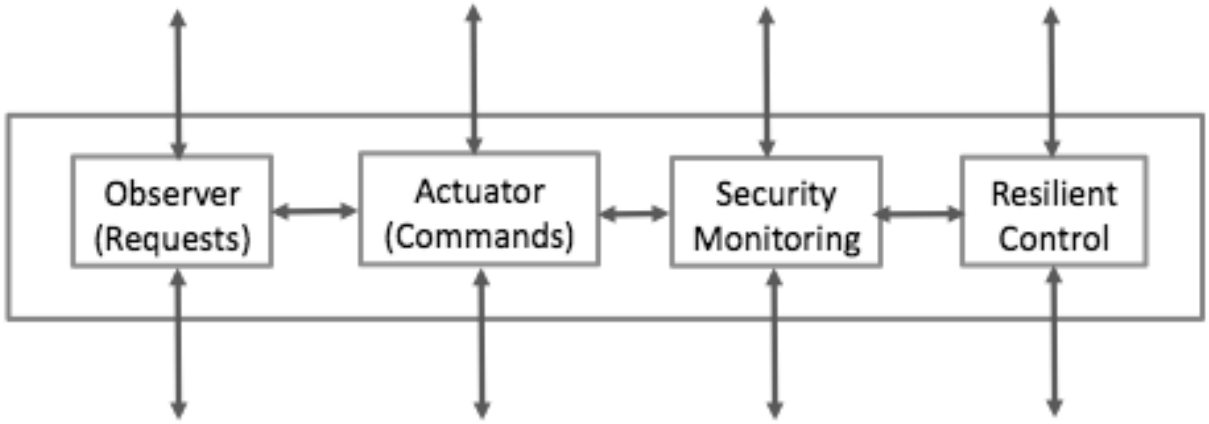
Agent-Based Methodologies



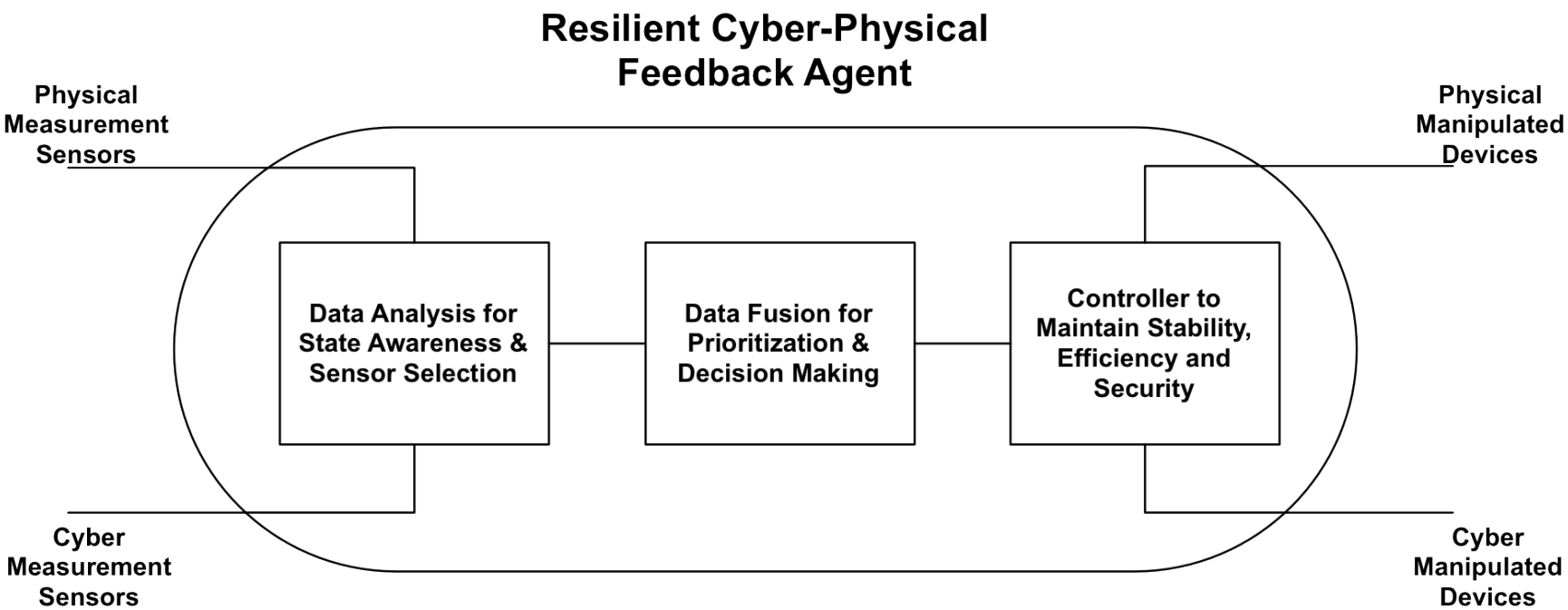
- A collection of separate operations make up an integral unit operation.
- Security and dynamics of one agent are interleaved with the ones of the other agents.
- An agent is equipped with mechanisms of anomaly detection for events, data fusion, fault-tolerant and alert system, etc.



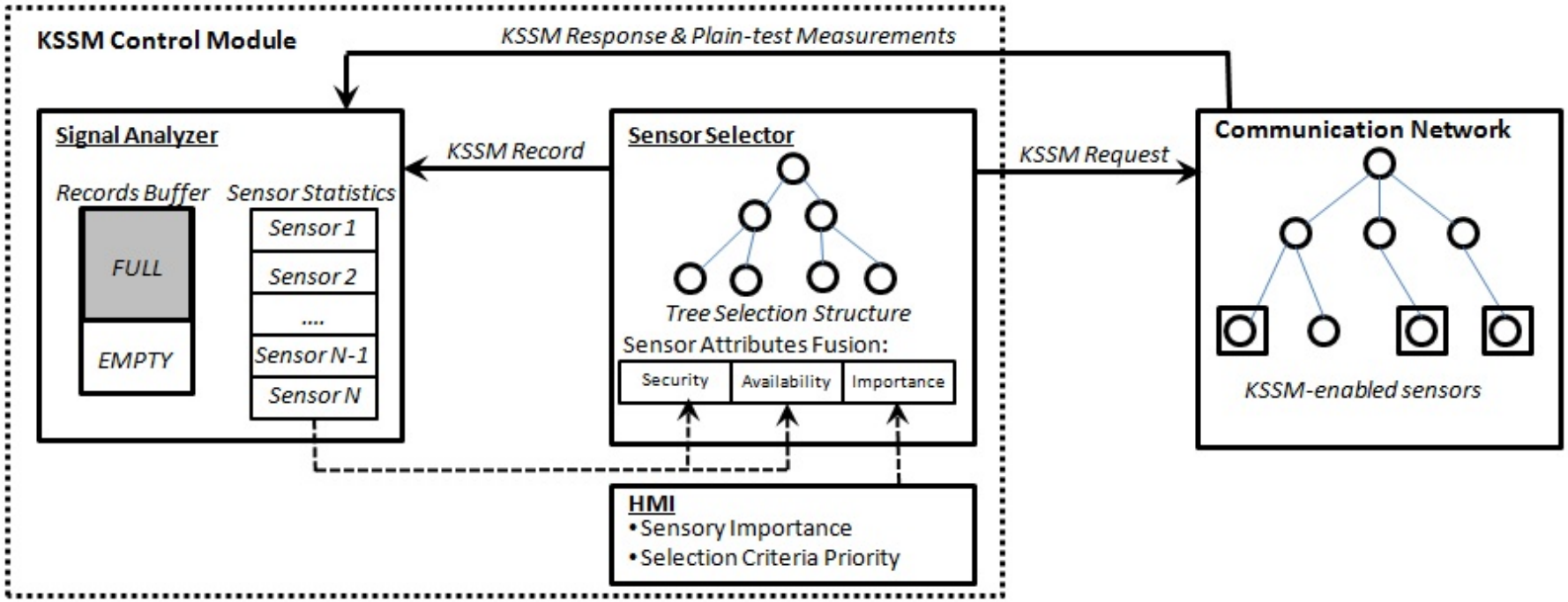
Example: Architecture of CPS Control Systems



Control Module

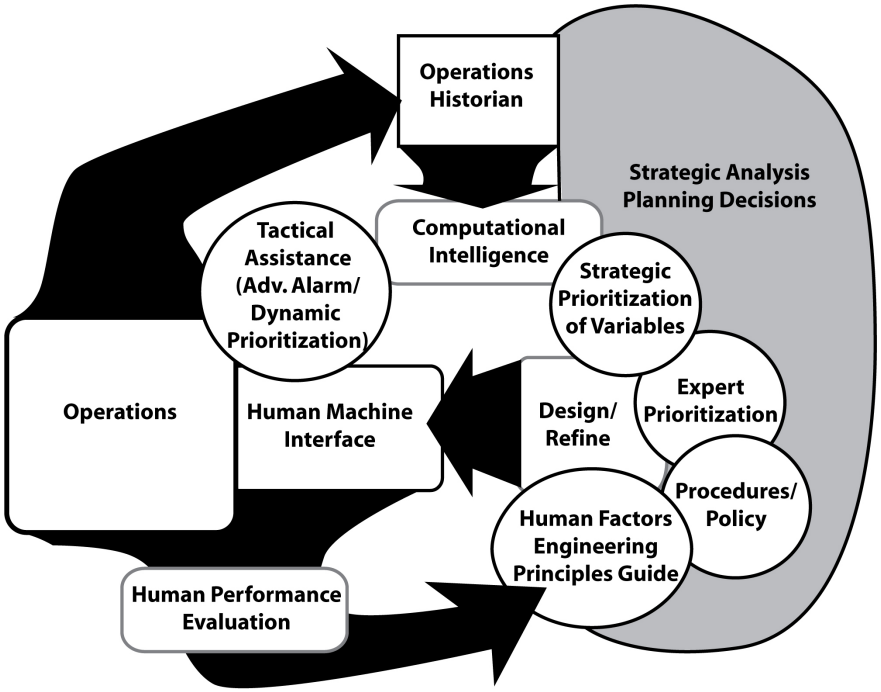


KSSM: Known Secure Sensor Measurement for Data Analysis & Sensor Selection



- KSSM provides a framework for baselining performance and reconfiguring sensors. [Linda et al. 2012]
- KSSM provides information regarding cyber health of the sensor system and can be used to determine the data set used for characterizing state awareness.

Data Fusion for Prioritization and Decision Making



- A necessary attribute of fusion is characterization, prioritization and presentation of information for a mixed human and automated response.
  - Uses raw cyber physical data to provide a prioritization of response based on policy.
  - Integrates the presentation of information for tactical response by human operators and cyber-physical controls in a visualized system.

[Linda et al. 2001]

Decomposing Philosophy of Multi-Agent Systems

Upper Layer: Management

This layer provides the overall philosophical goals and priorities for operations. The sources for this design reign from management, regulators, physical constraints of the systems, etc.

Middle Layer: Coordination

This layer provides the negotiation and potential realignment of resources that best enable meeting the dictated philosophy. Based on renegotiation, the tasking of the execution layer is driven.

Lower Layer: Execution

This layer provides direct monitoring of sensors and control of field devices.

Upper Layer: Management

- Regulatory Requirement: Considering primarily governmental agencies that regulate the operation or its products in some fashion.

- Desired Performance: Whether a production rate or an efficiency objective, this aspect comes from a desire to maximize profit for the organization using the control system.

- Physics-based Limitations: the physics of the design affects the limits of the operation. One must collectively include this when considering the tradeoffs of performance.

Middle Layer: Coordination

- The performance of the system remains within its constraints for operation.
- The ability to share, and ultimately negotiate resources is limited by the uniformity of the system.
- Decisions for shifting of resources can occur at different layers of the multi-agent systems hierarchy, with control action taken at both the middle and lower layers.
- The coordination layer has responsibility for multiple lower level agents, and as such, will better orchestrate shifts in operation to accommodate the performance goals of the management layer.

Lower Layer: Execution

- Decomposition to minimize, and as a result, simplify agent interactions and complex dynamics;
- Development of agent layers in a hierarchical structure;
- Optimization of inter-agent interactions with consensus theory to achieve a common objective;
- Optimization of intra-agent interactions with applicable control engineering, soft and hard computing, defined by most relevant to situation. The ultimate goal is to stabilize the shared manipulated and controlled variables.

Conclusions

- A perspective for cyber security research can be taken from *control theory*, and in doing so, an integrated approach will be taken to *resilience* for industrial process control systems.

- In cyber-physical design, the ability to utilize cyber data for corrective response on the physical system, as well as uncharacterized physical disturbances to correlate cyber exploit, allow for *a holistic approach* never before possible.

- Cyber-physical systems can be codified in the hierarchical multi-agent dynamical system (HMADS) model. Critical infrastructure systems can notionally be *decomposed* into three layers, including management, coordination and execution.