FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

System-Security Co-design

Saurabh Amin and Janos Sztipanovits

Berkeley
UNIVERSITY OF CALIFORNIA

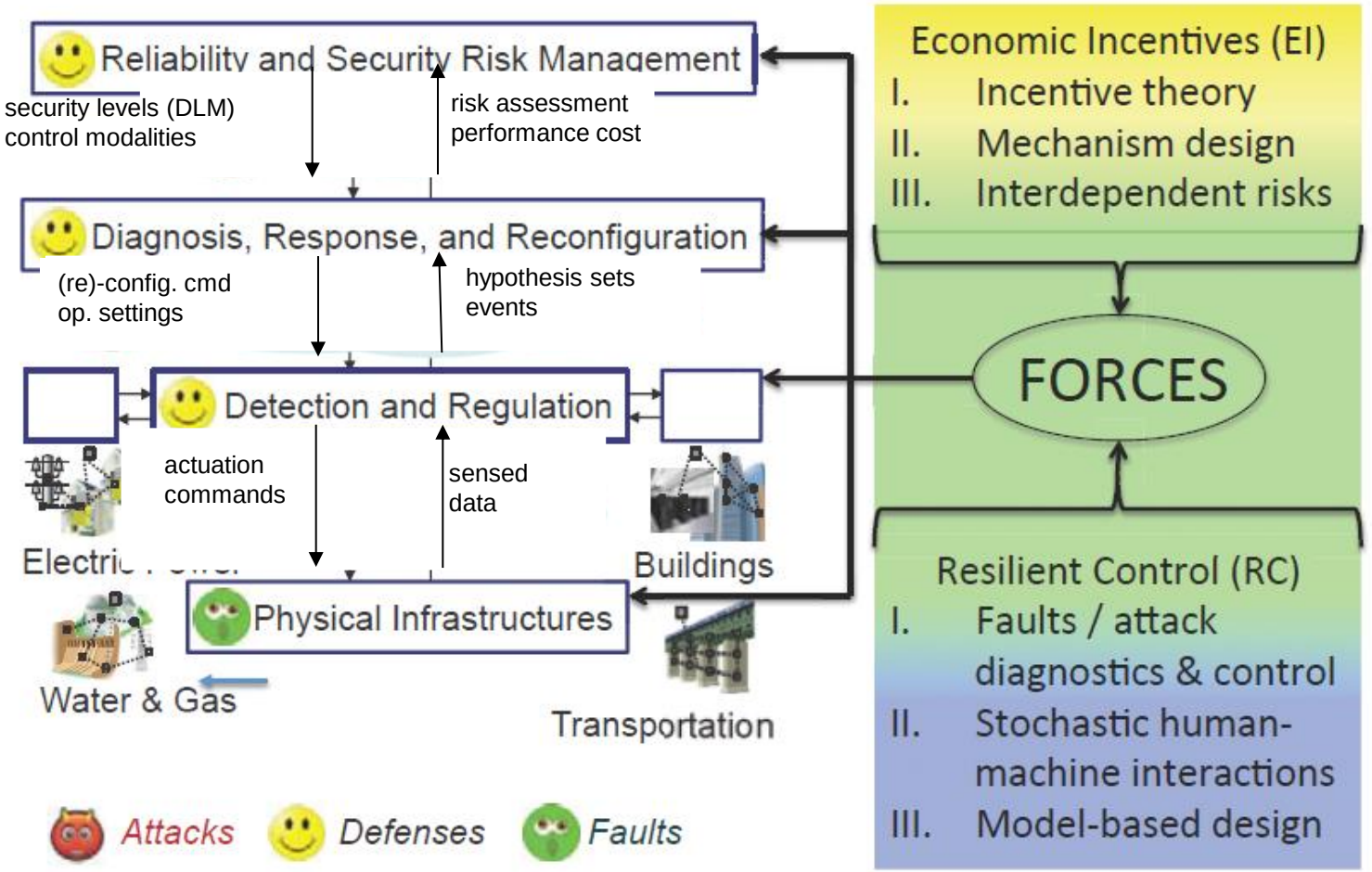
Massachusetts Institute of Technology

NSF

MICHIGAN

VANDERBILT UNIVERSITY

Functional Layers in FORCES

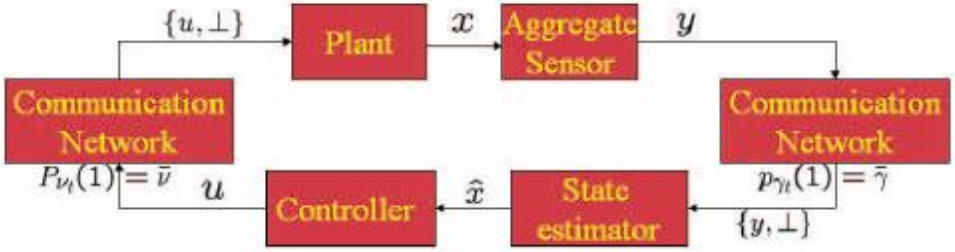


FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

System-Reliability Co-Design

For unreliable communication **(Before FORCES)**

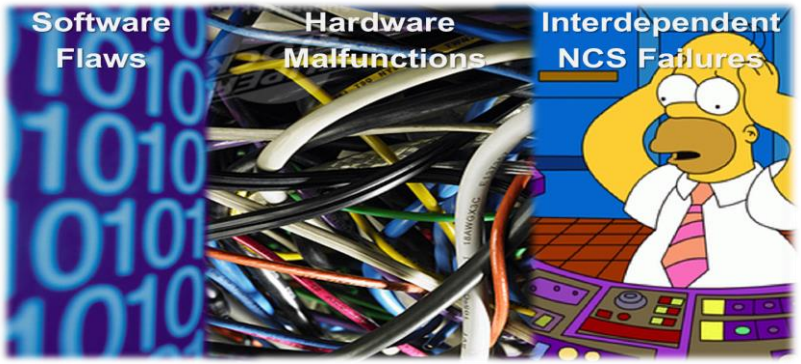
- What is the minimum arrival probability that guarantees *acceptable* performance of estimator and controller?
- How is the arrival rate related to the system dynamics?
- Can we design estimator and controller independently?
- Are the optimal estimator and controllers still linear?
- Can we provide design guidelines?



L. Schenato, B. Sinopoli, K. Poolla, S. Sastry

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

System-Security Co-Design

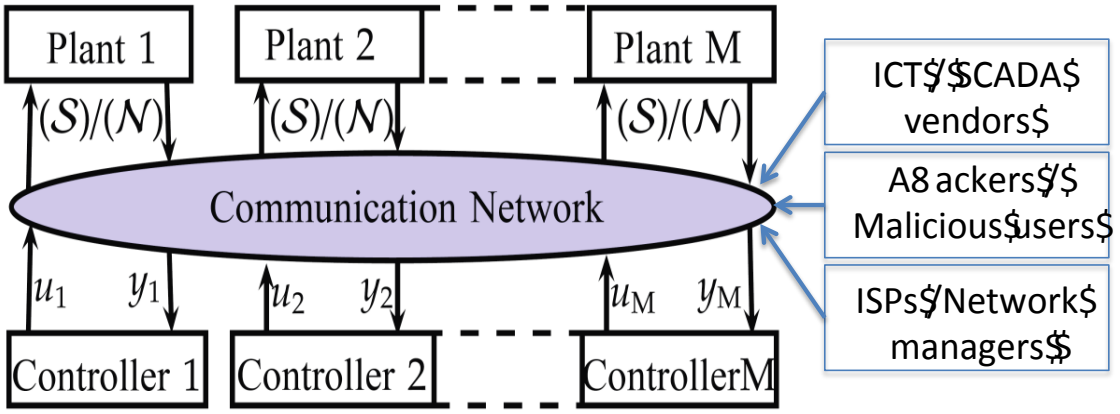


- Interdependencies due to
  - Network induced risks
    - DDOS, deception attacks
  - Wide use of COTS ICT components
    - Correlated bugs & failure points
    - Expect increased interdependencies
  - Observation: Suboptimal incentives to invest in security due to
    - Public good nature (Varian, 2002)
    - Information deficiencies (Teneketzis)
    - Property right deficiencies and high enforcement costs (Schwartz)
  - How to jointly model control and incentives in co-design process:

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Whose Incentives Matter in Co-Design?

* Manufacturers
* Consumers / Users
  * Average / regular users
  * System operators
  * Specialists
* Hackers – users, whose objectives differ from legit users' objectives
* Government(s)



Economic literature focuses on manufacturer and operator incentives, but does not consider constraints imposed by closed-loop control.

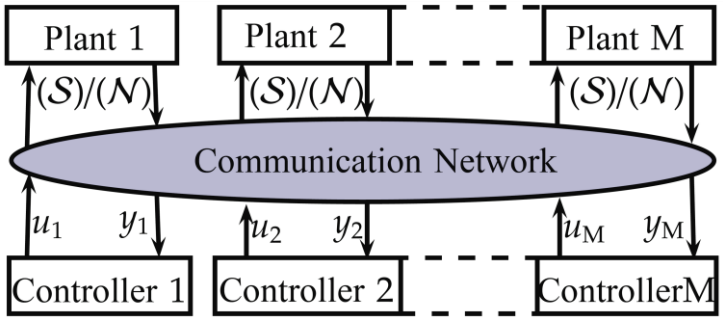
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Interdependence for Network Control Systems (NCS)

- Security failures (attacks S) & reliability failures (faults R) are difficult to distinguish
- Model for communication network failures F:

$$\Pr(S \cup R \mid F) = \Pr(R \mid F) + \Pr(S \mid F) - \Pr(R \mid F)\Pr(S \mid F)$$
$$= \underbrace{\Pr(R \mid F)}_{\text{direct failure (reliability)}} + \underbrace{(1 - \Pr(R \mid F))\Pr(S \mid F)}_{\text{indirect failure (security)}},$$

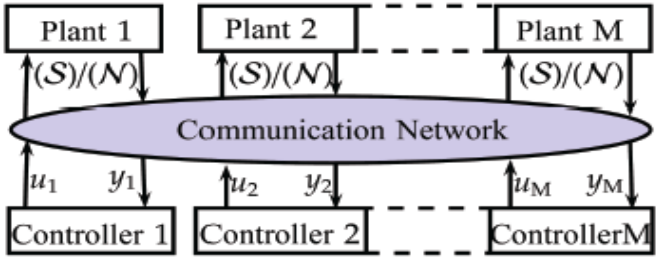
- Interdependence: $\Pr(S \mid F) = \alpha(\eta)$
  - $\alpha(\cdot)$: strictly increasing function
  - η: number of insecure players (NCS)



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Game with Interdependent Security

Two-stage game of 2 (then M) plant-controller systems (players)



For player i

1. (S) or (N) (Stage 1 choice variable)
   If (S) then i incurs per period security cost, $\ell^i \in [0, \infty)$

$$V^i := \begin{cases} S, & \text{player } i \text{ invests in security,} \\ N, & \text{player } i \text{ does not invest in security} \end{cases}$$

2. $u^i \in \mathbb{R}^m$ – control input (Stage 2 choice variable)

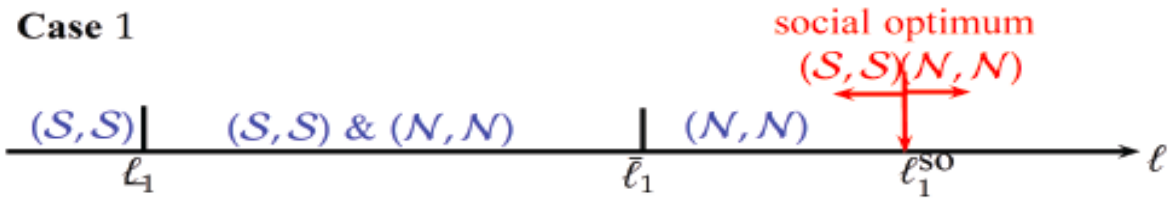
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Individual optima (Nash eq) and Social optima => Implications for reconfiguration and co-design?

Equilibria for Case of Increasing Incentives

Open loop stable NCS

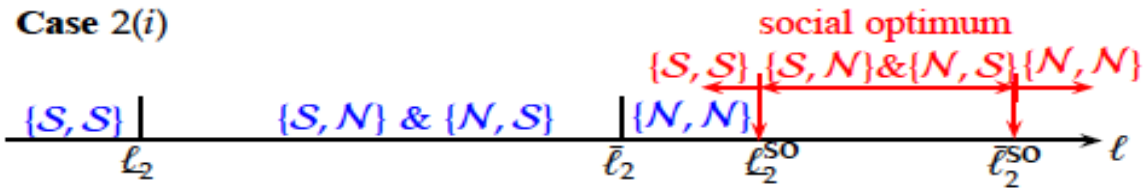
Case 1



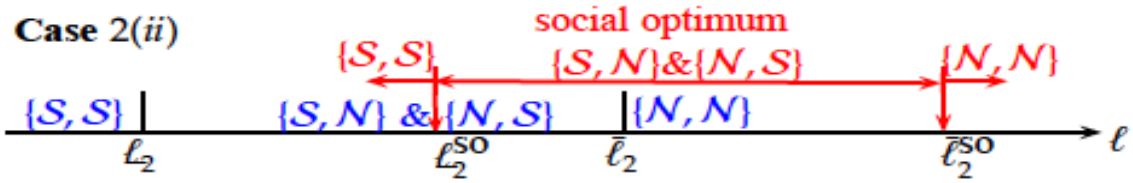
Equilibria for Case of Decreasing Incentives

Open loop unstable NCS

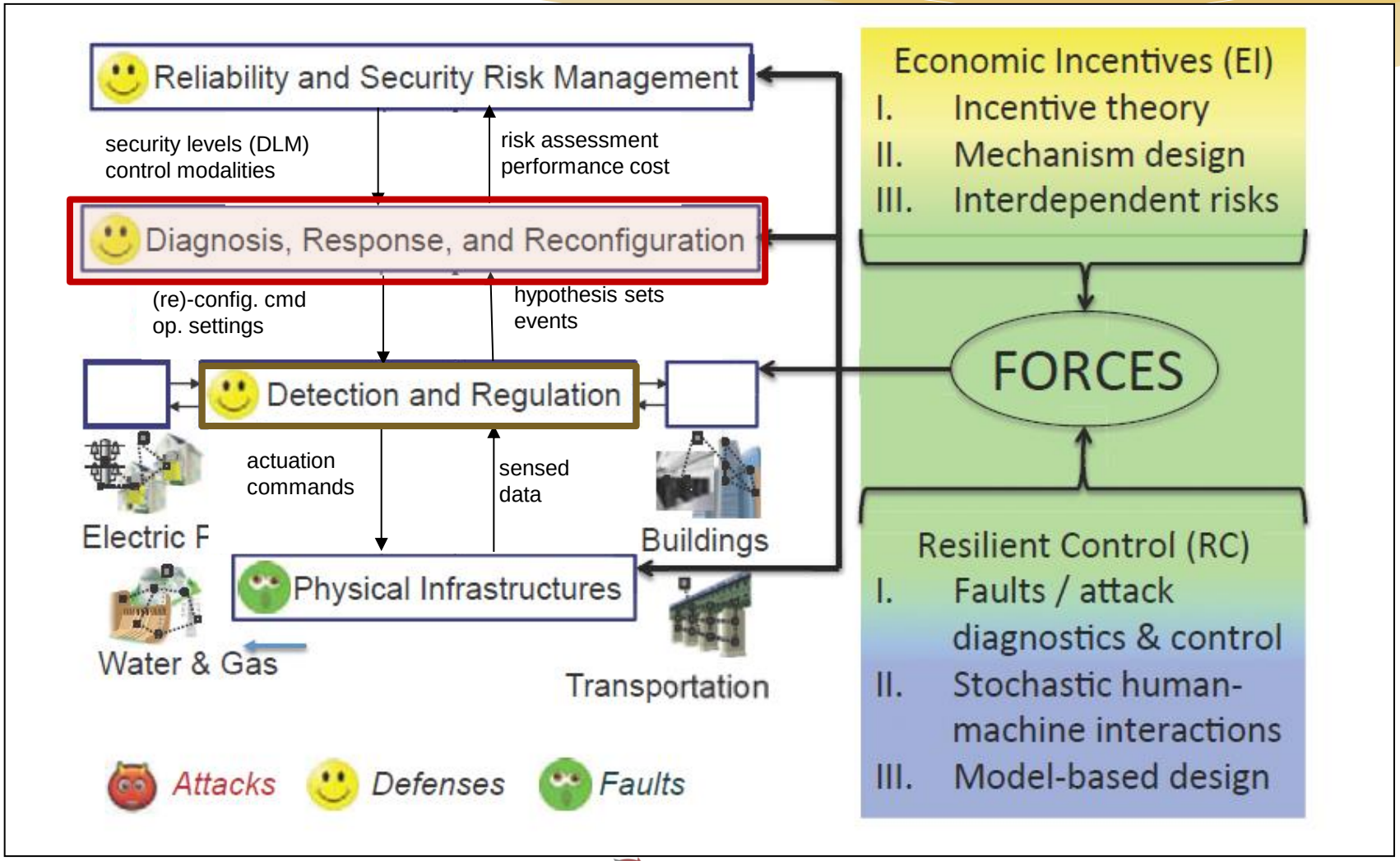
Case 2(*i*)



Case 2(*ii*)



Reconfiguration is Essential for Resilient Control



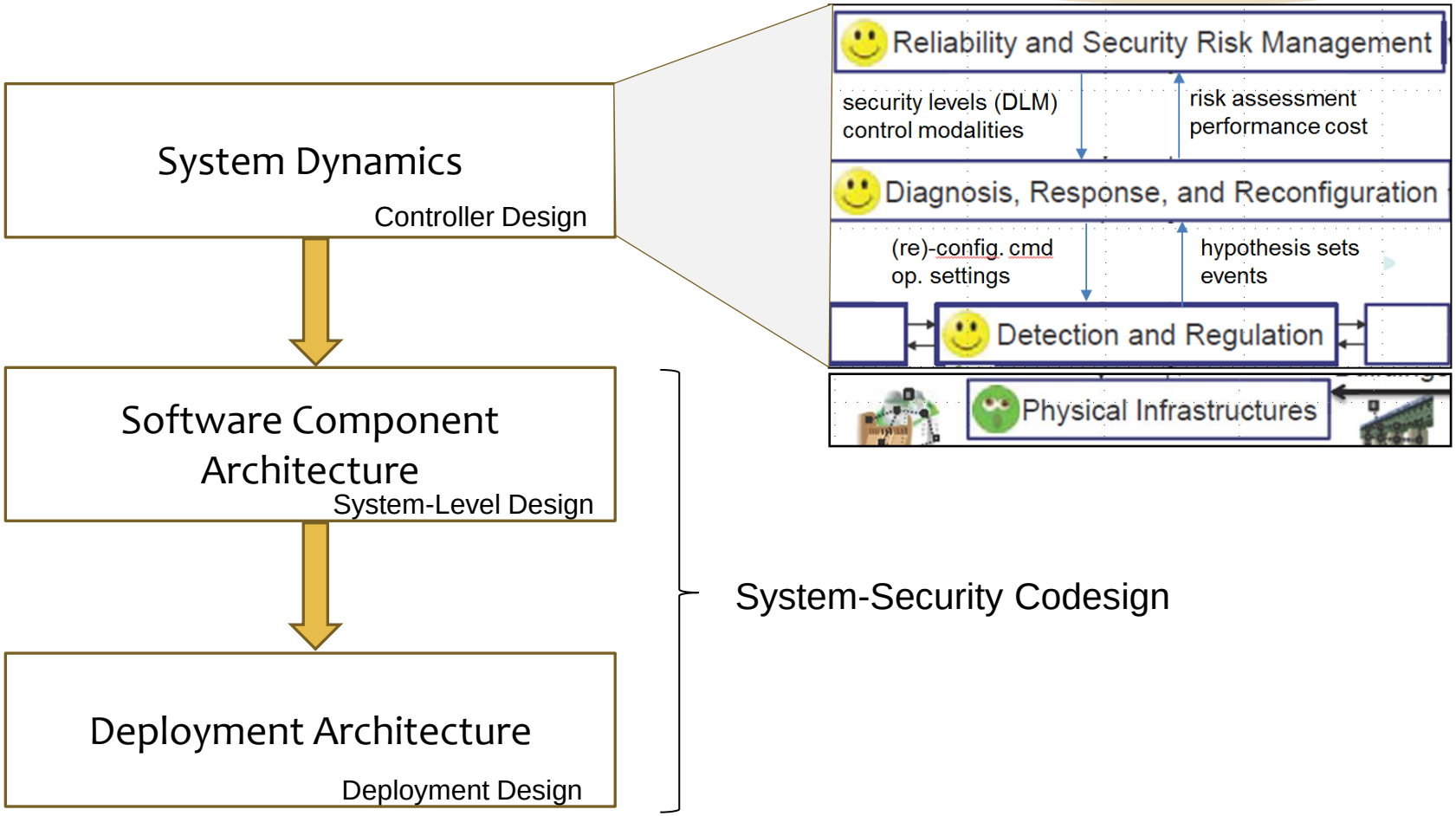
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Objectives of Reconfiguration

* **Change modes of operation of Detection and Regulation**
  - Diagnosis, Response and Reconfiguration forms a supervisory control mechanism – used in hierarchical control approaches (e.g. Pappas, Tabuada)
* **Re-synthesize implementation architecture**
  - Provide interface for changing required security policies
  - Provide models of information flows required to be implemented
  - Provide models for security and performance characteristics of communication links and computing devices
  - Provide precise specification for the reconfiguration space
  - Develop methods for remapping the information architecture to the implementation architecture subject to functional, performance, timing and security constraints

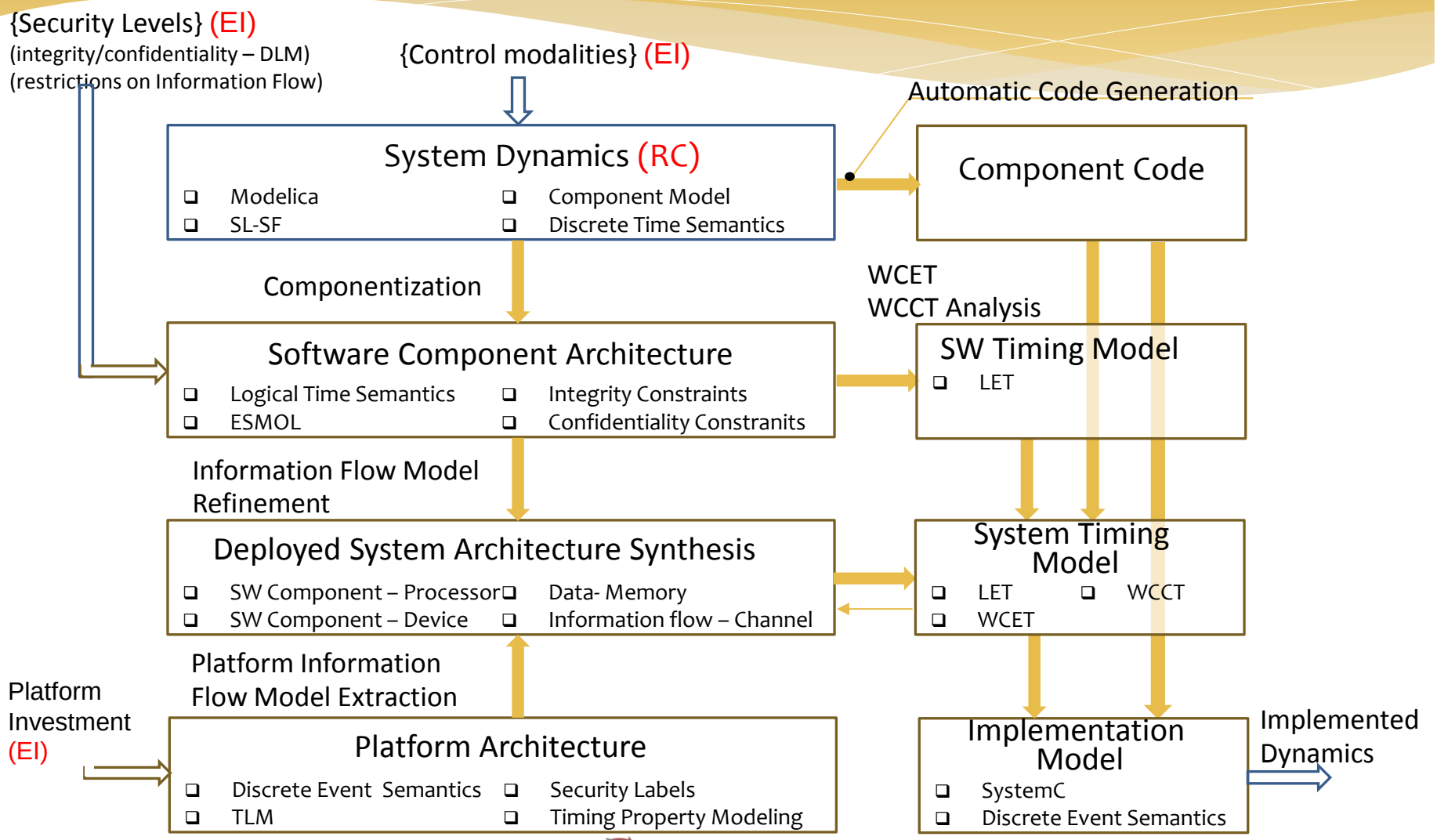
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Co-design Problem



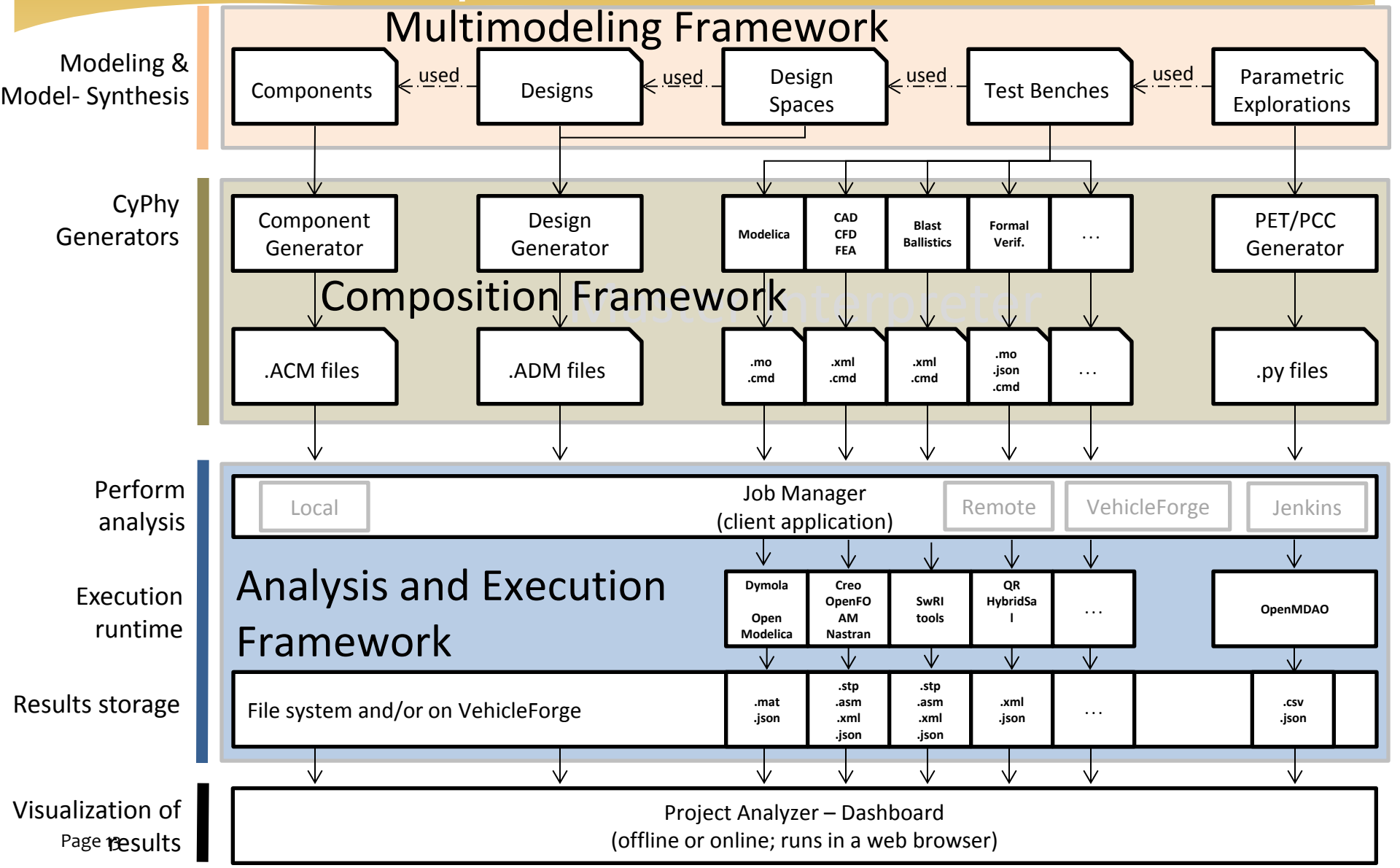
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

System – Security Co-design



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Tool Integration Framework: OpenMETA Tool Suite



Tool Architecture