



Foundations Of Resilient CybEr-physical Systems (FORCES) – NSF CNS 1238959

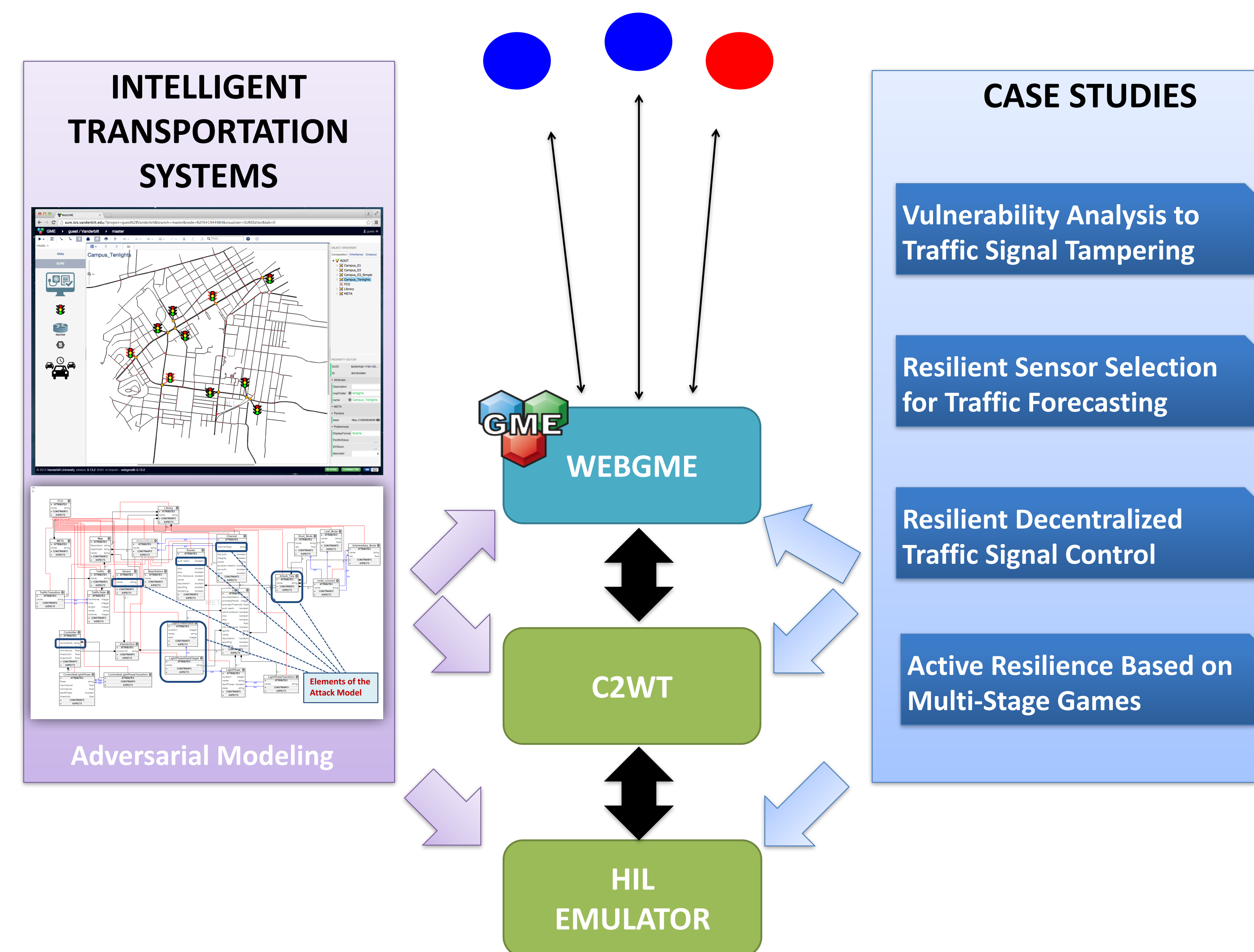
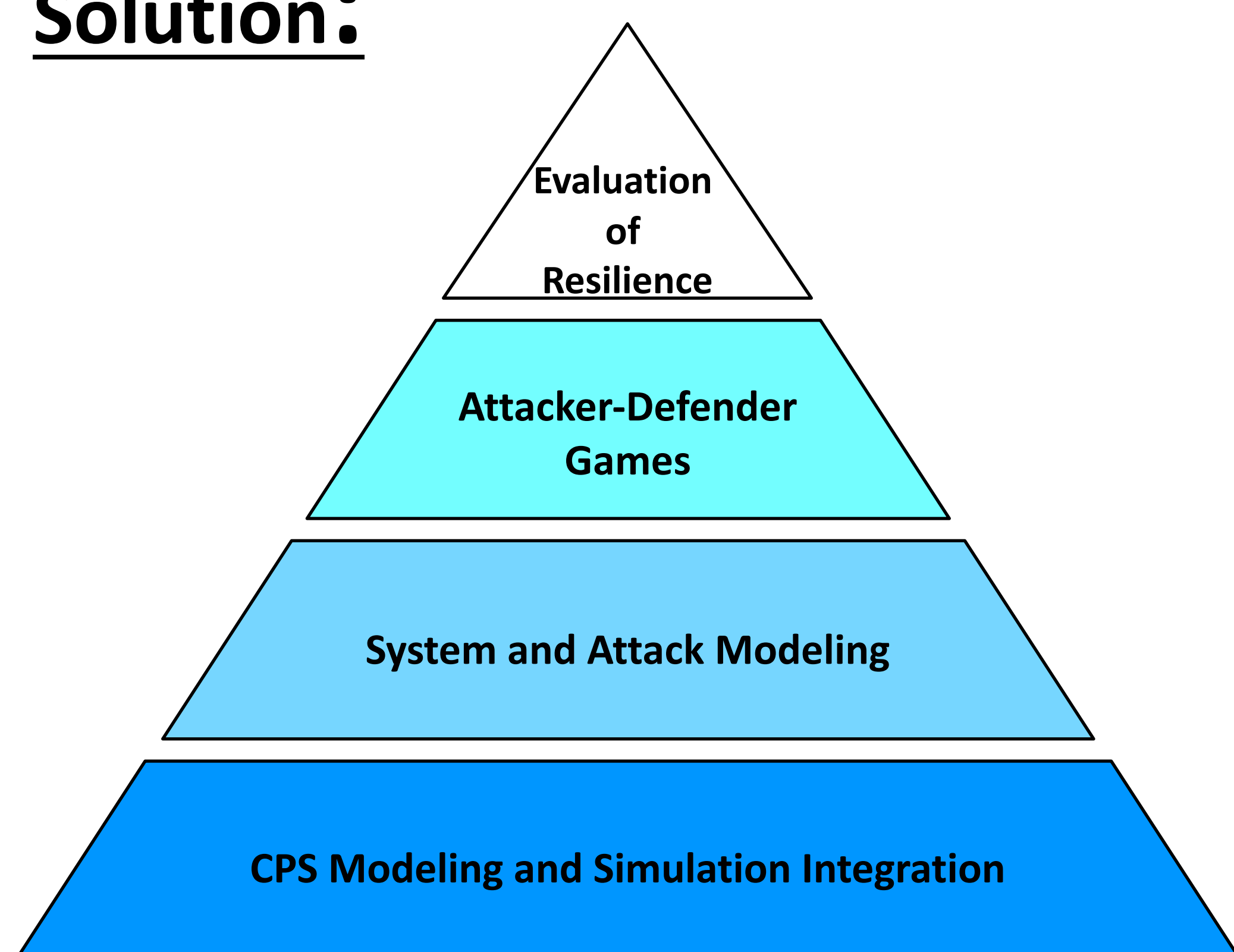
System Science of Secure and Resilient Cyber-Physical Systems

Xenofon Koutsoukos, Gabor Karsai, Aron Laszka, Himanshu Neema, Bradley Potteiger, Peter Volgyesi, Yevgeniy Vorobeychik, and Janos Sztipanovits

Challenge:

- Develop a systematic body of knowledge with strong theoretical and empirical underpinnings to inform the engineering of secure and resilient CPS that can resist not only known but also unanticipated attacks.
- Seek metrics for describing how resilient a CPS is in what kinds of situations under what kinds of threats.
- Perform CPS vulnerability studies based on attacker-defender games using simulations of sufficient fidelity.

Solution:



- Framework for evaluating resilience using attacker-defender games
- Modeling CPS in adversarial environments using WebGME
- Heterogeneous simulation integration using Command and Control Wind Tunnel (C2WT) + Hardware-in-the-Loop (HIL) emulator

Scientific Impact:

- Theoretical analysis must be accompanied by large amounts of experimental work and empirical observations
 - Develop realistic models
 - Integrate heterogeneous simulations/emulations
 - Perform controlled experiments of large-scale CPS
 - Understanding by simulating

Broader Impact:

- Complex CPS abound in modern society and are target of cyber attacks
- Our goal is to equip designers and operators with methods and tools to improve security and resilience
- Education and Outreach
 - Undergraduate/graduate/postdoctoral research and education
 - CPS Summer Camp'17 (high school students)
 - Dissemination:

<http://cps-vo.org/group/forces>
<http://www.cps-forces.org>