Synthesizing Advanced Reactor Control Systems: Achieving Security and Reliability

Daniel G. Cole
Mechanical Engineering
University of Pittsburgh

dgcole@pitt.edu

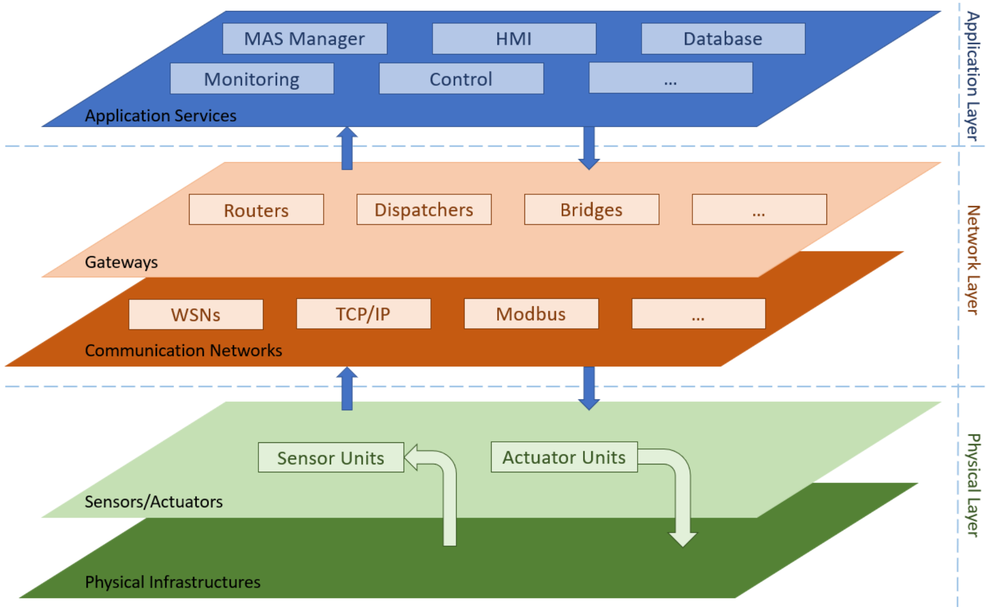
formal methods for cyber-physical systems

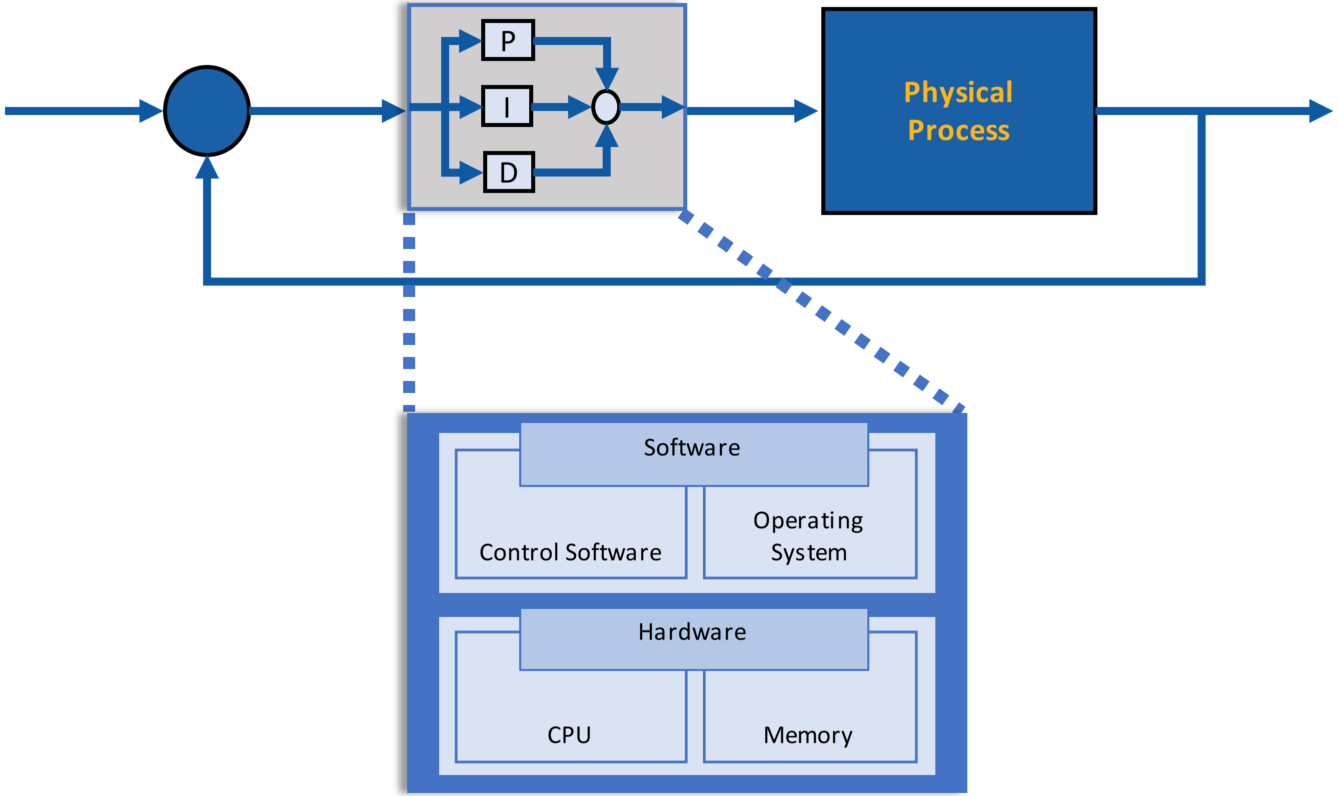
metrics of security and resilience

encrypted control systems

University of Pittsburgh

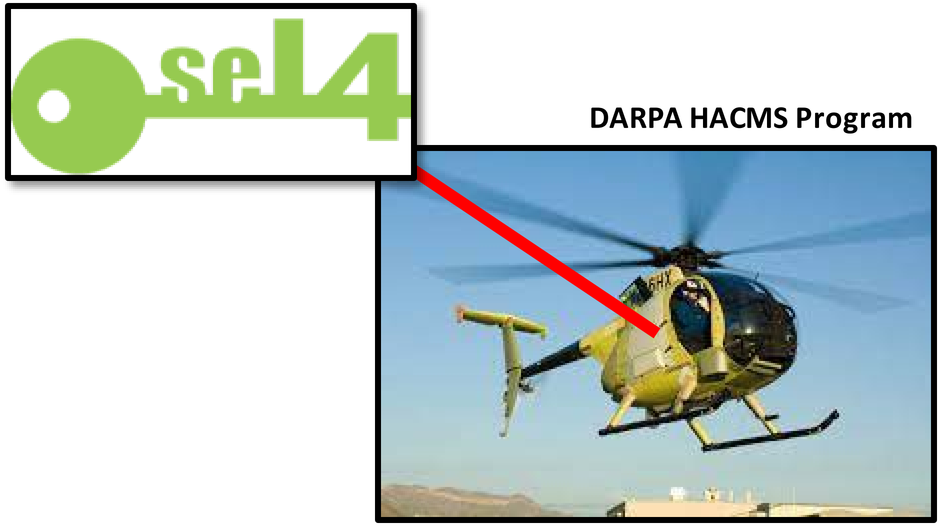
IT cybersecurity alone cannot protect the physical layer
OT security often overlooks cyber as a source of unsafe control actions





University of Pittsburgh

Formal methods approaches enable modeling of complex systems and verifying their properties

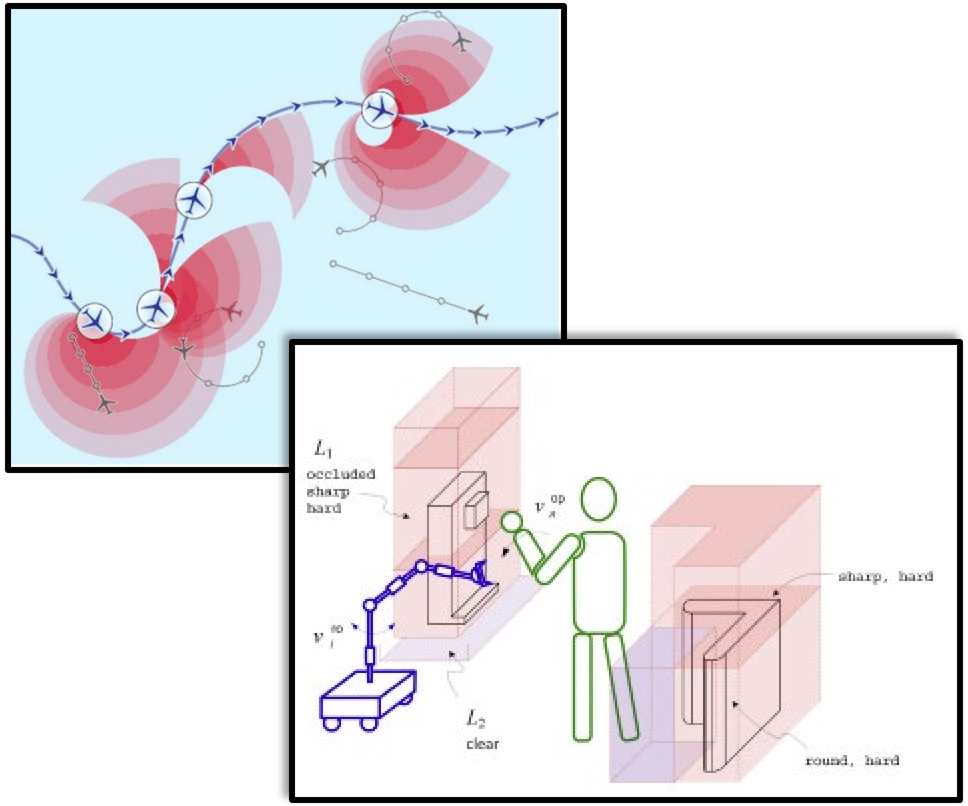


DARPA HACMS Program

Unhackable kernel could keep all computers safe from cyberattack

Hacker-Proof Code Confirmed

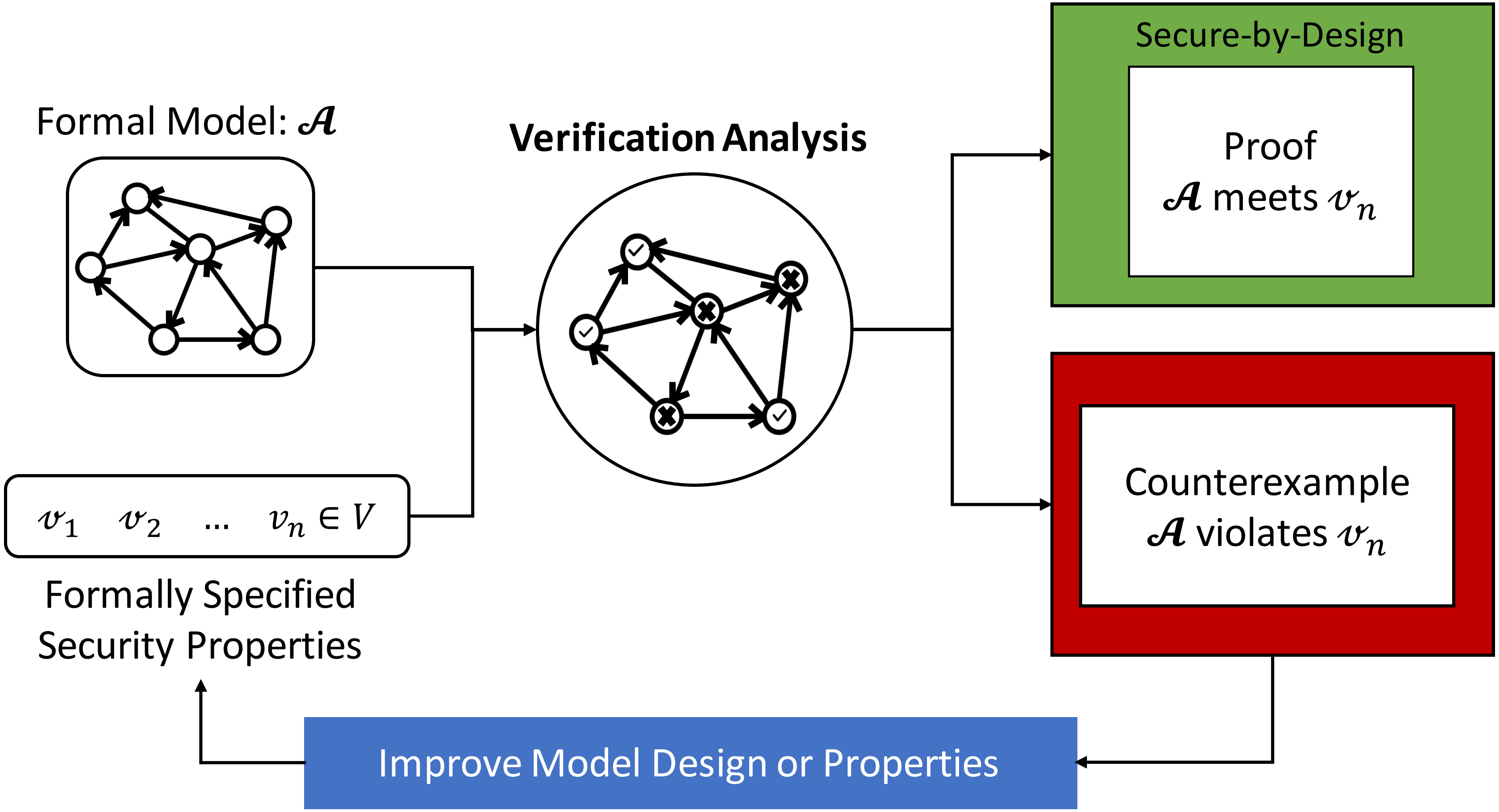
Computer scientists can prove certain programs to be error-free with the same certainty that mathematicians prove theorems. The advances are being used to secure everything from unmanned drones to the internet.



Formally verifying safety properties for control systems.

University of Pittsburgh

Verifying that the model complies with security properties achieves specified secure-by-design goals



Formal Model: $\mathcal{A}$

v_1 v_2 … $v_n \in V$

Formally Specified Security Properties

Verification Analysis

Secure-by-Design

Proof

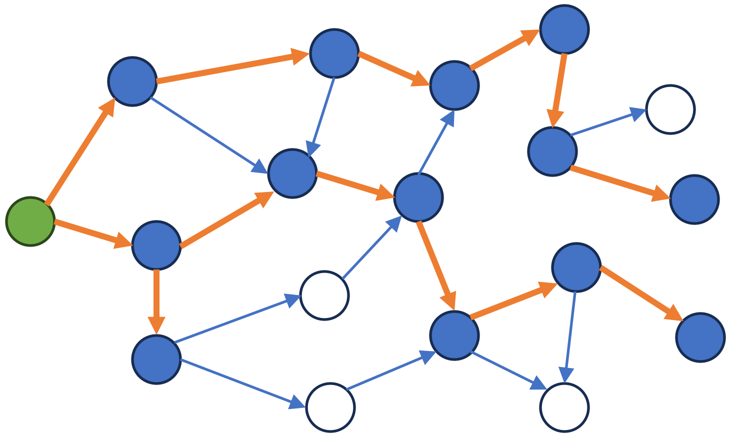
$\mathcal{A}$ meets v_n

Counterexample

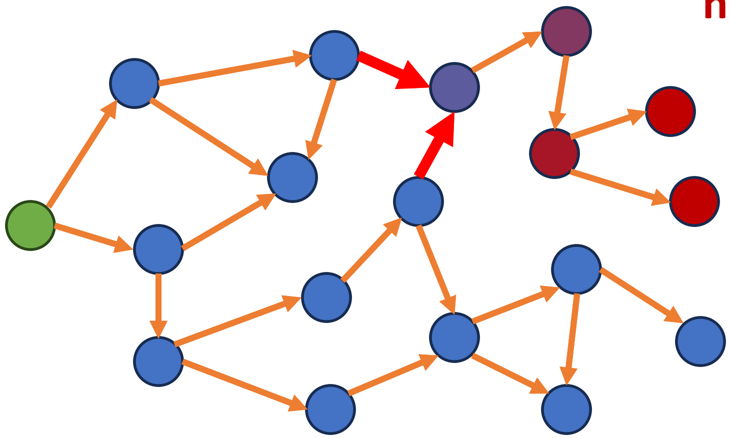
$\mathcal{A}$ violates v_n

Improve Model Design or Properties

Exploring the state space yields unsafe control actions that result in harm. Safer, more secure controllers can then be designed.



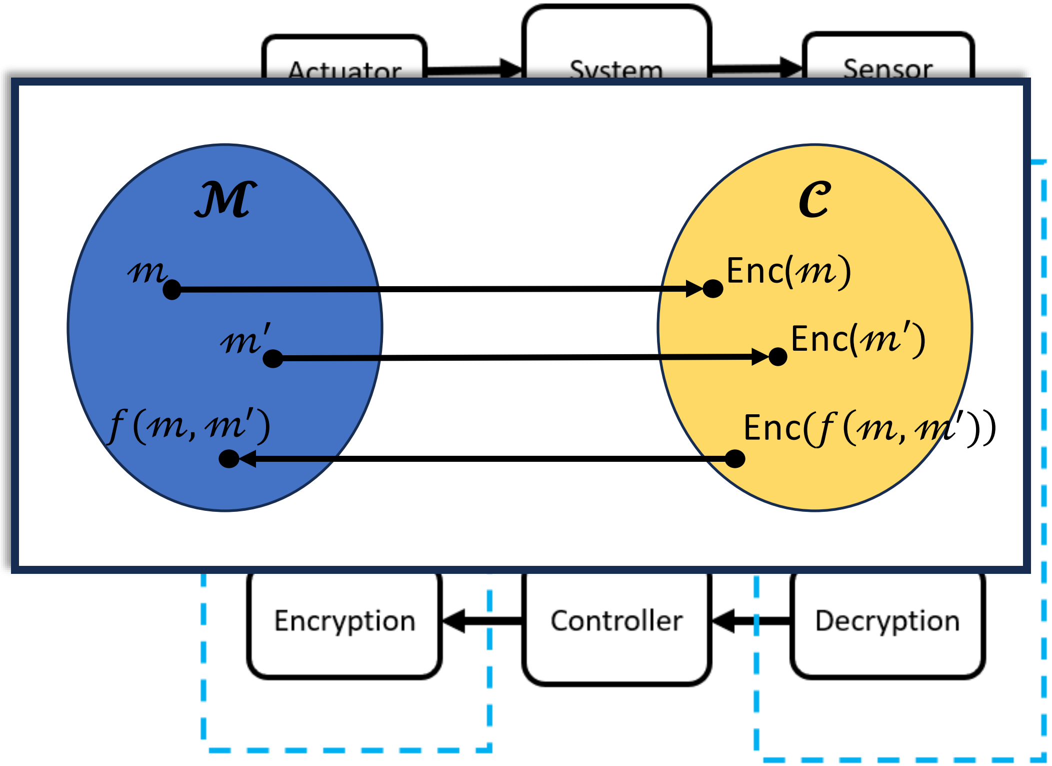
Simulation trace



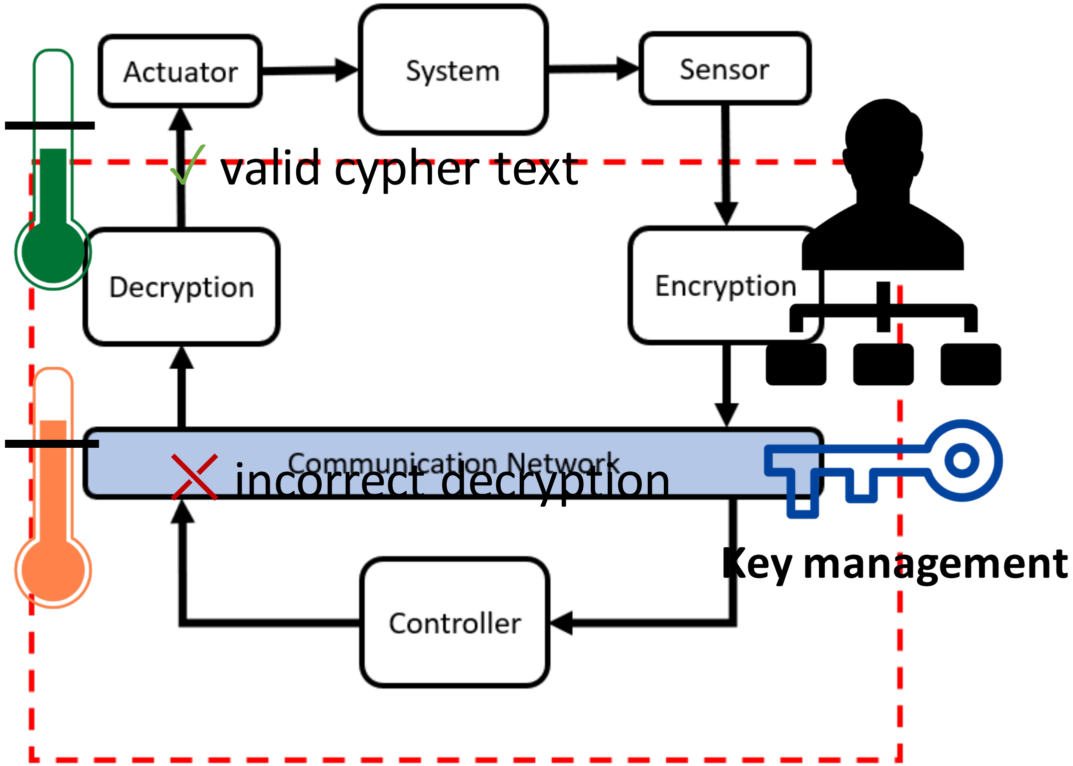
Verification trace

Unsafe control actions lead the system to **harm states**

Homomorphic encryption enables better command control and communications systems

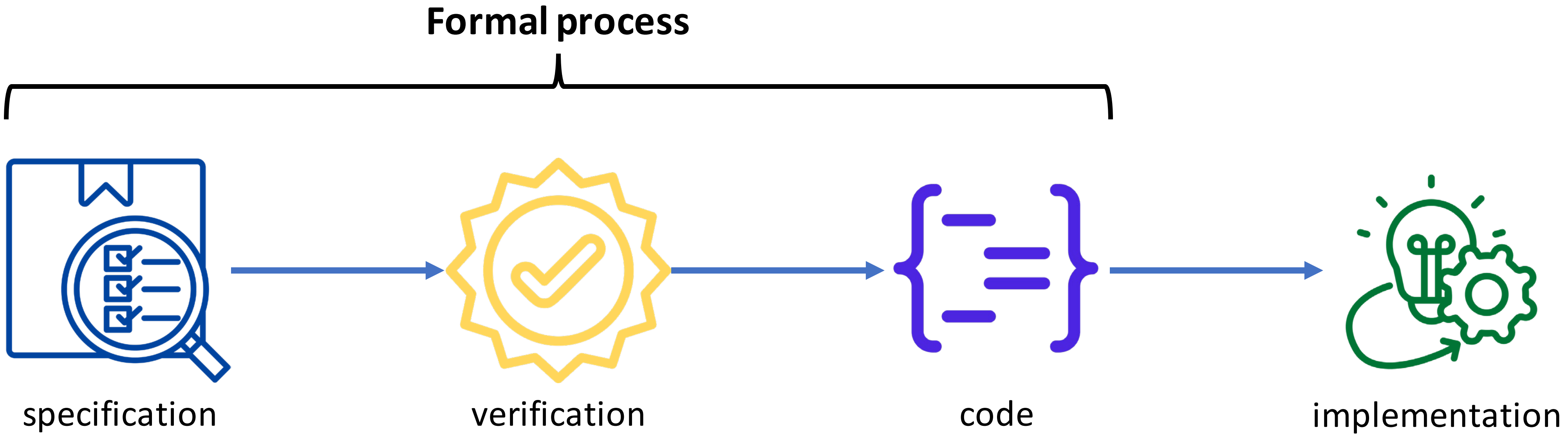


Current Method – Encrypted Transmitted Data



Applied Homomorphic Encryption

If we do these things well, we can improve the security of command, control, and communication systems, AND reduce the cost of development



Better system verification tools yields secure-by-design control systems, improved safety, security, and – done right – a better design process

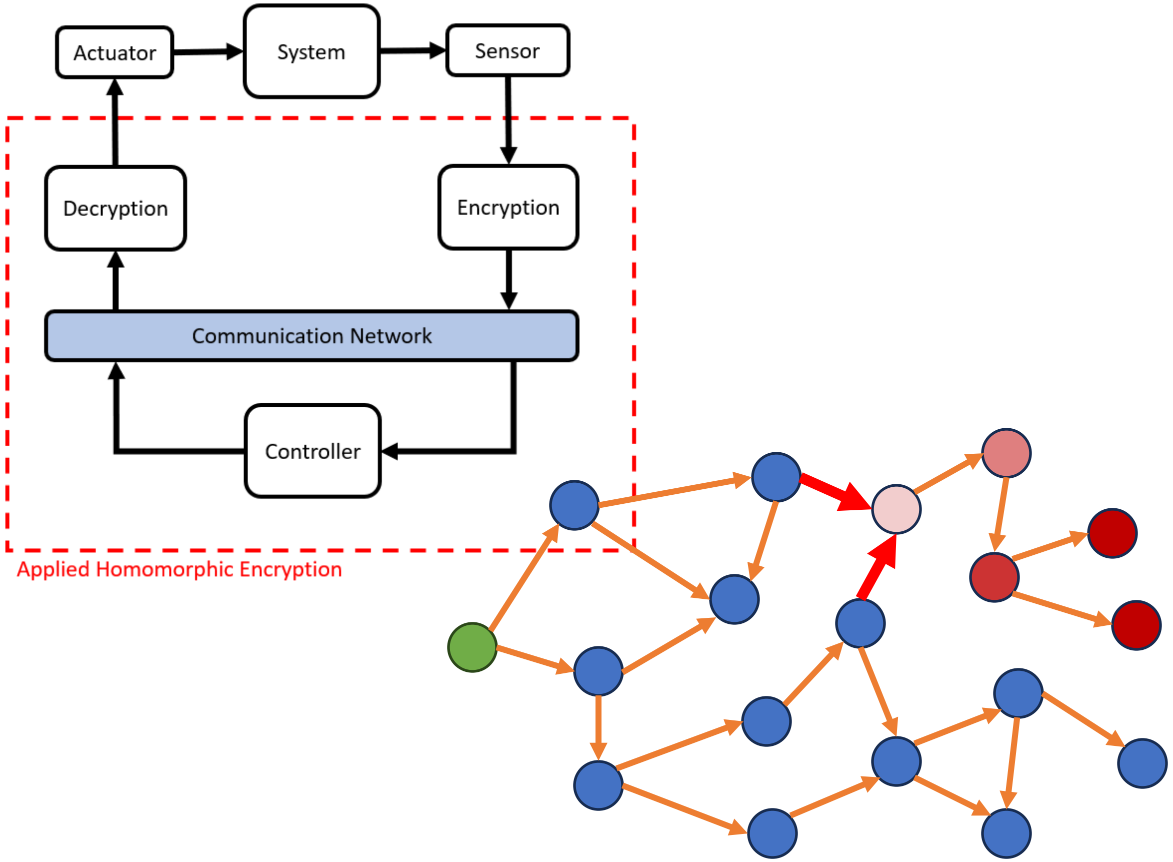
Daniel Cole
University of Pittsburgh

dgcole@pitt.edu

412-624-3069

Robert Lois

Manyu Kapuria



Actuator
System
Sensor
Decryption
Encryption
Communication Network
Controller
Applied Homomorphic Encryption