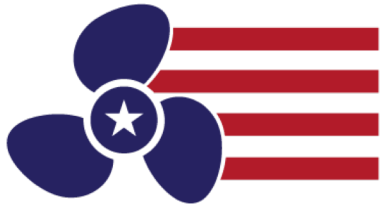


Overview of Cybersecurity

People:

- **John Chandy**, *Professor*, Electrical & Computer Engineering, UConn
- **Sridhar Duggirala**, *Asst. Professor*, Computer Science & Engineering, UConn
- **Benjamin Fuller**, *Asst. Professor*, Computer Science & Engineering, UConn
- **Haibo He**, *Robert Haas Endowed Chair Professor*, Electrical & Computer Engineering, URI
- **Amir Herzberg**, *Comcast Endowed Chair Professor*, Computer Science & Engineering, UConn
- **Omer Khan**, *Assoc. Professor*, Electrical & Computer Engineering, UConn
- **Laurent Michel**, *Professor*, Computer Science & Engineering, UConn
- **Alexander Russell**, *Professor*, Computer Science & Engineering, UConn
- **Sina Shahbazmohamadi**, *Asst. Professor*, Biomedical Engineering, UConn
- **Yan Sun**, *Assoc. Professor*, Electrical & Computer Engineering, URI
- **Marten van Dijk**, *Charles Knapp Assoc. Professor*, Electrical & Computer Engineering, UConn
- **Lei Wang**, *Assoc. Professor*, Electrical & Computer Engineering, UConn



Technology Applications

Access Control

Advanced Biometrics

Communications

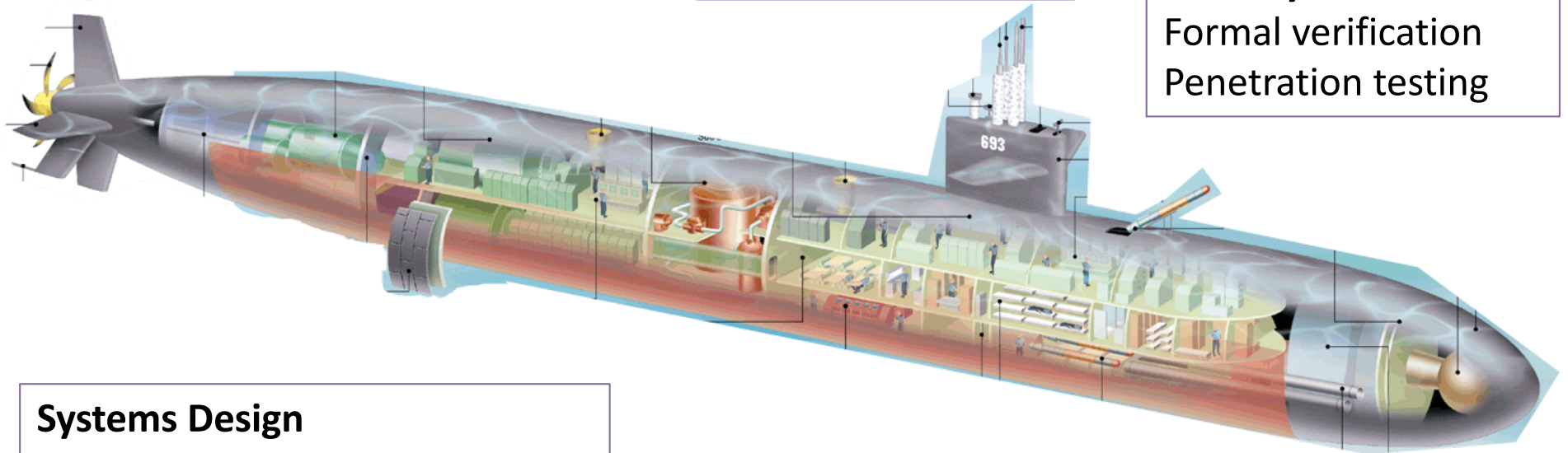
Encryption

Secure protocols

Security Validation

Formal verification

Penetration testing



Systems Design

Secure systems configuration

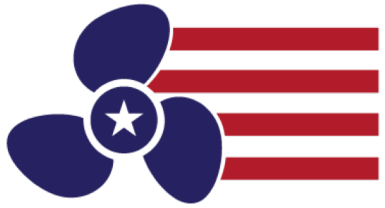
Secure Controls

Resilient Architectures

Electronics

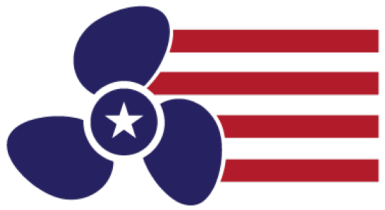
Counterfeit part detection

Anti-reverse engineering



Research Capabilities

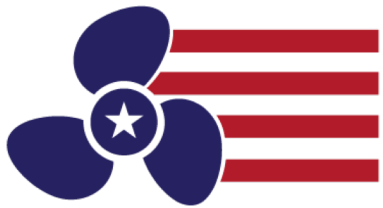
- Systems design
 - Optimal configuration of systems security parameters
 - Secure control algorithms in the presence of malicious inputs
- Counterfeit Detection
 - State of the art imaging for non-destructive testing of counterfeit ICs
 - Nano-tagging of authentic parts
- Penetration testing
 - Comprehensive and holistic embedded systems testing
- Secure protocols
 - Provably secure communication protocols
- Biometrics
 - Error tolerant and refreshable biometrics



Counterfeit Detection and Prevention

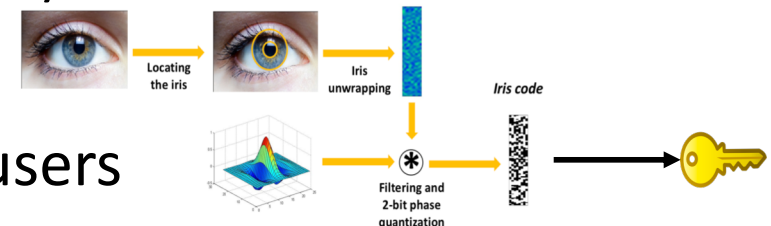
- X-ray and Terahertz modalities to inspect integrated circuits
- Secure supply chain with full tracking of components
- Nano-tagging of parts and components
 - Unique ID that can not be replicated
 - Easily detected for authentication
- Anti-reverse engineering
 - Transient electronics

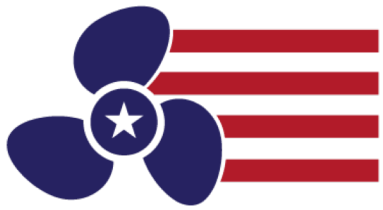




Biometrics

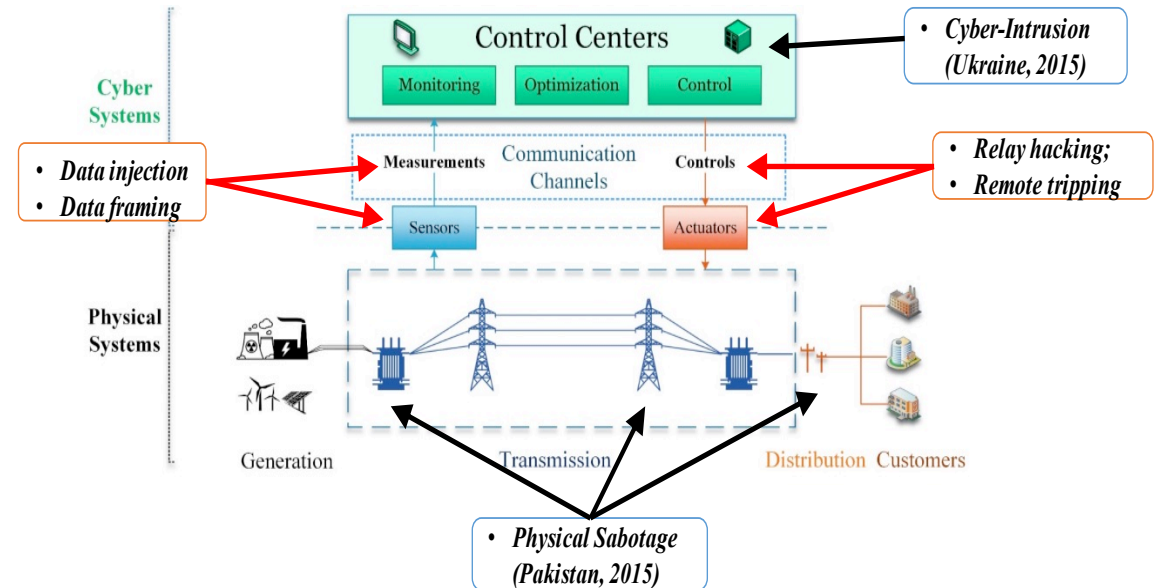
- Strong authentication is important in a closed environment for sensitive operations and to mitigate insider threat
- Current approach uses Common Access Card (CAC) card and PIN
 - Vulnerable to theft, cloning, and left in computer
- Biometrics ensure that stolen CAC card cannot be used
- Primary challenge is performing cryptography with noisy biometrics
- Innovations in key derivation from noisy sources
 - Approach merges biometrics and cryptography
- Secure authentication system from iris
- Improved usability and transparency to users
- Move to continuous authentication, minimize vulnerability window





Resilient Power Grid

Every critical infrastructure from communications to water, every important business functions from banking to farming, and every national defense mission from our borders to our fleet, completely depend on main or micro electrical grids



- **URI Resilient Power Grid Project:**
- Principle Investigators:
- Haibo He, Robert Haas Endowed Chair Professor; Editor-in-Chief, IEEE Trans. On Neural Networks and Learning Systems
- Yan Lindsay Sun, Professor; Editor-in-Chief, SIGPort Associate Editor, IEEE Trans on Signal and Information Processing over Networks

Cascading Failures and Blackouts

- Blackout modeling; GIS-integrated testbed

Vulnerability Analysis

- Concurrent and sequential attacks; Risk graphs

Grid Security and Resilience

- Resilience against False Data Injection (FDI)
- Adaptive Controller for Resilient Microgrid
- Smart Community and Multimedia forensics