Bridging the Gap Between Security and Modularity

Sponsor: DASD(SE)

By

Ms. Giselle M. Bonilla-Ortiz

6th Annual SERC Doctoral Students Forum

November 7, 2018

FHI 360 CONFERENCE CENTER

1825 Connecticut Avenue NW

8th Floor

Washington, DC 20009

www.sercuarc.org

Agenda

- Introduction
- Problem Statement
- A Look at Program Protection
- Generic Modular Open System Example
- Security Concerns
- Research Outcomes and Next Steps
- Conclusion
- References

Introduction

- FY17 NDAA Section 805: Modular Open Systems Approach in Development of Major Weapon Systems
  - Requires design and development with MOSA, to the maximum extent practicable.
- Paradox: How do we design secure and trusted systems that are open and modular?
  - Are security and modularity/openness really at odds?
- Follow Systems Security Engineering (SSE) Principles to start bridging that gap

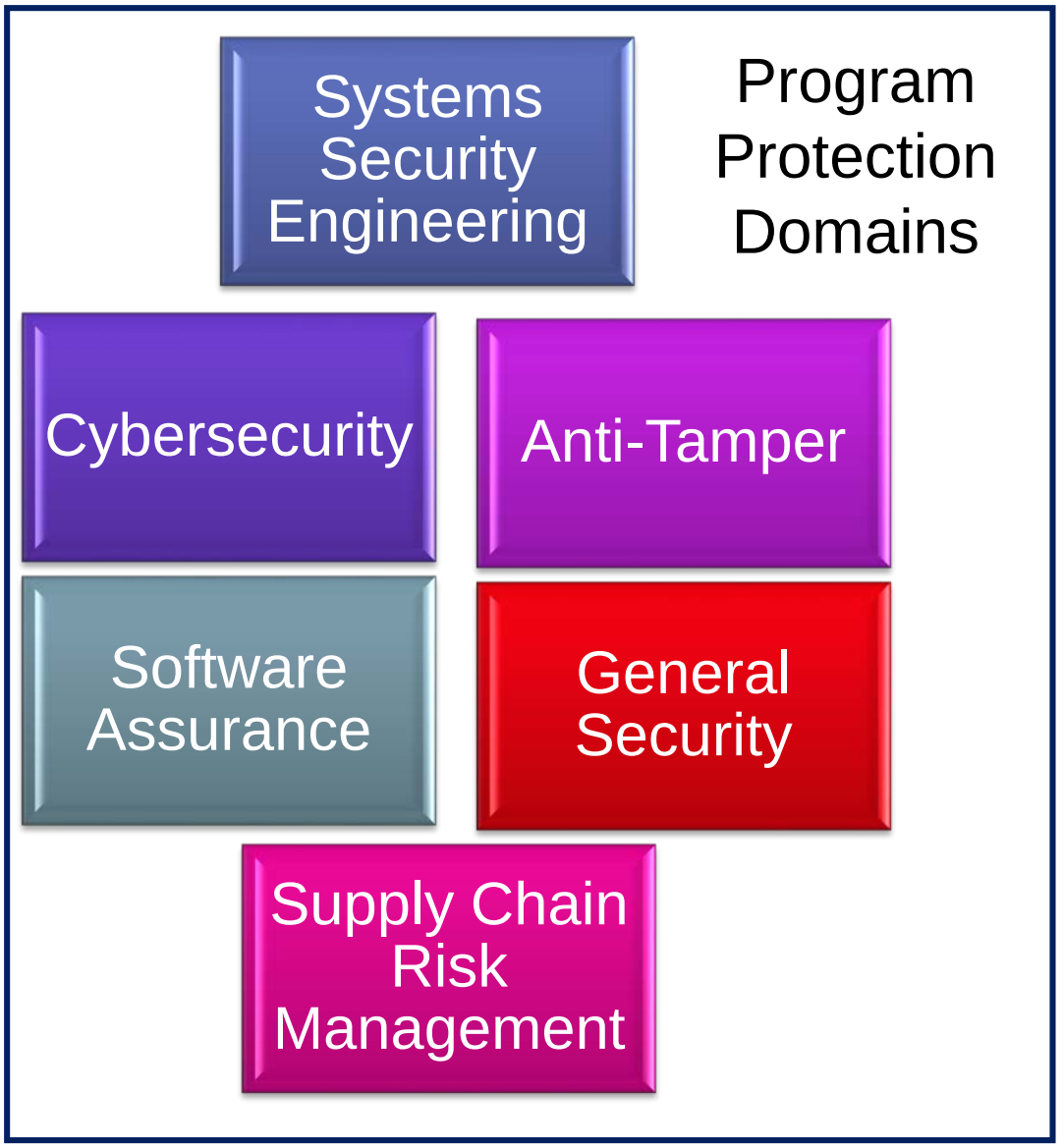
Problem Statement

- Modular Open Systems Approach and security principles seem to be at odds
- How can we reap the benefits of MOSA without compromising, maybe enhancing, security?
- Further research needed on:
  - Applying SSE to securing MOSA compliant systems
  - Establishing metrics to gage security vs modularity
  - Determining when is it better to go for a “closed” security approach

SYSTEMS ENGINEERING RESEARCH CENTER

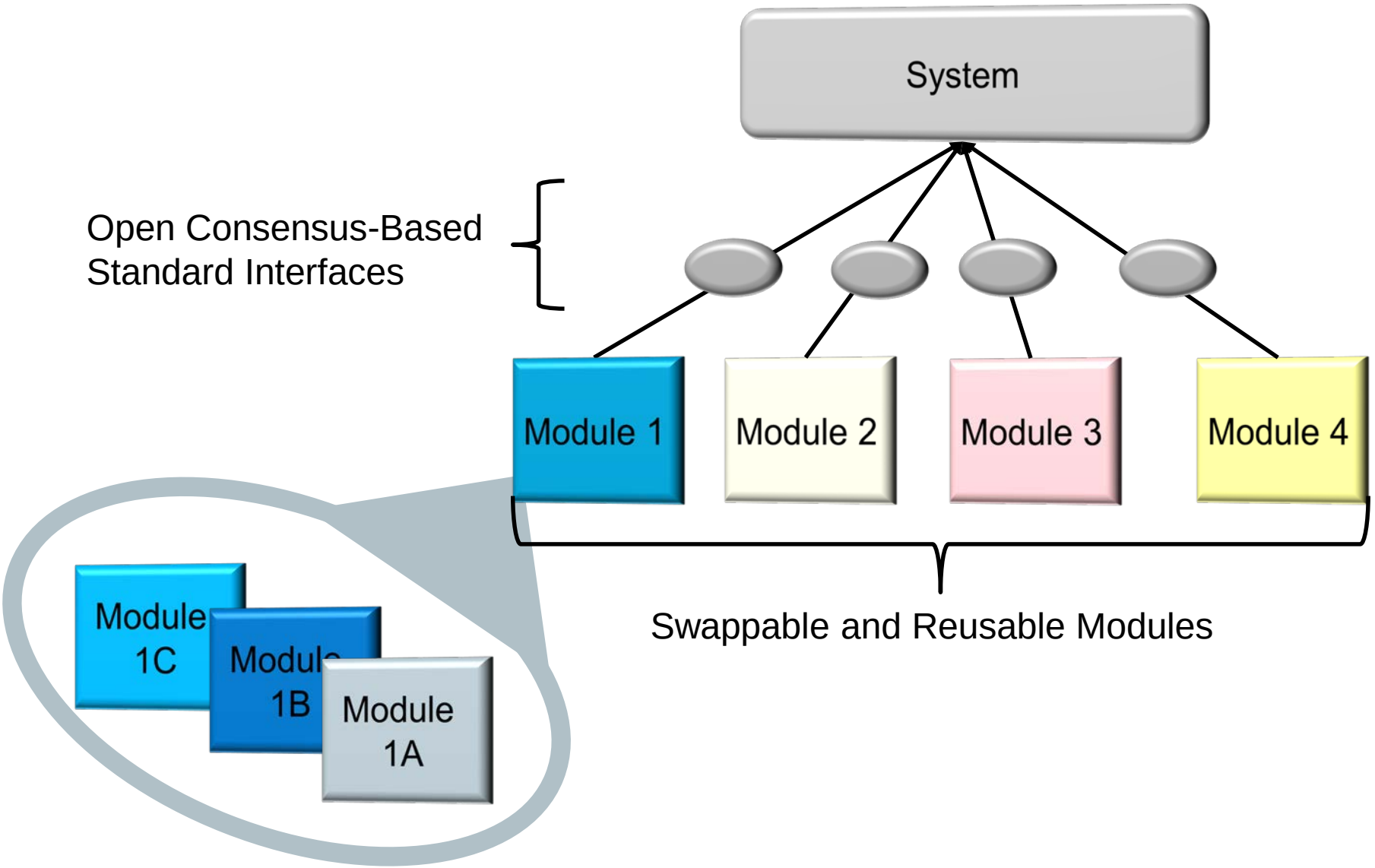
A Look at DoD Program Protection

- Protecting technology, components and denying access to information to unauthorized parties
- Identifying threats, vulnerabilities and mitigating consequence of loss
  - Throughout system lifecycle
- Multiple countermeasures can be employed: Cybersecurity, Supply Chain Risk Management, Anti-Tamper, Software Assurance, etc.
- Brought together by disciplined Systems Security Engineering



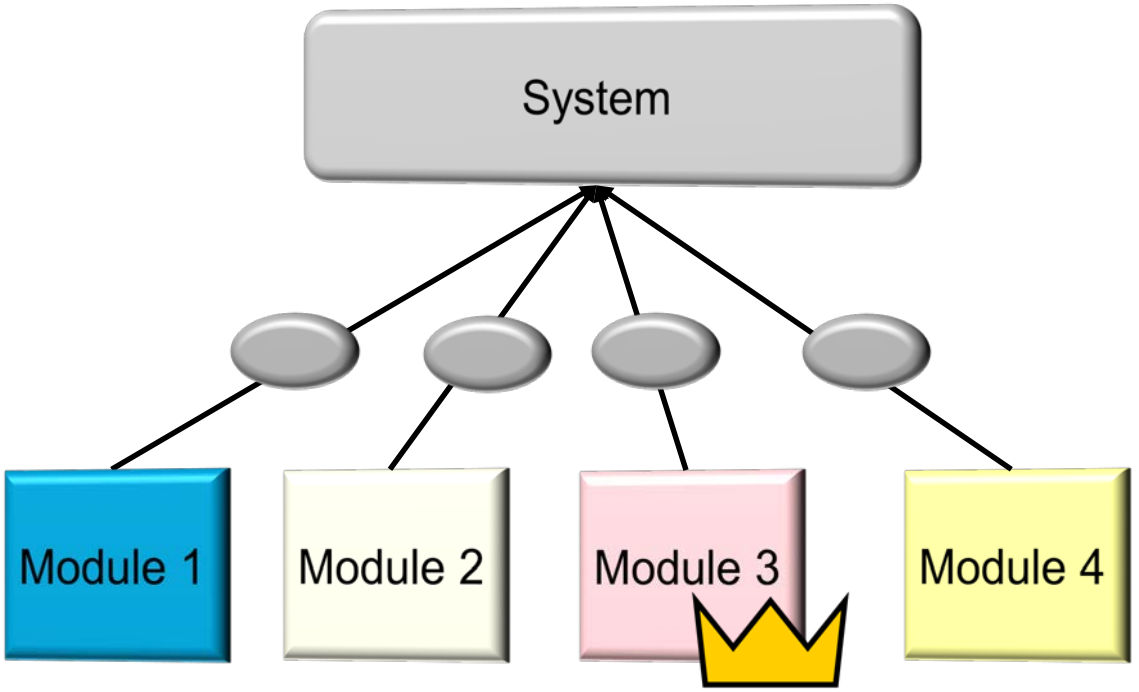
SYSTEMS ENGINEERING RESEARCH CENTER

Generic Modular Open System Example



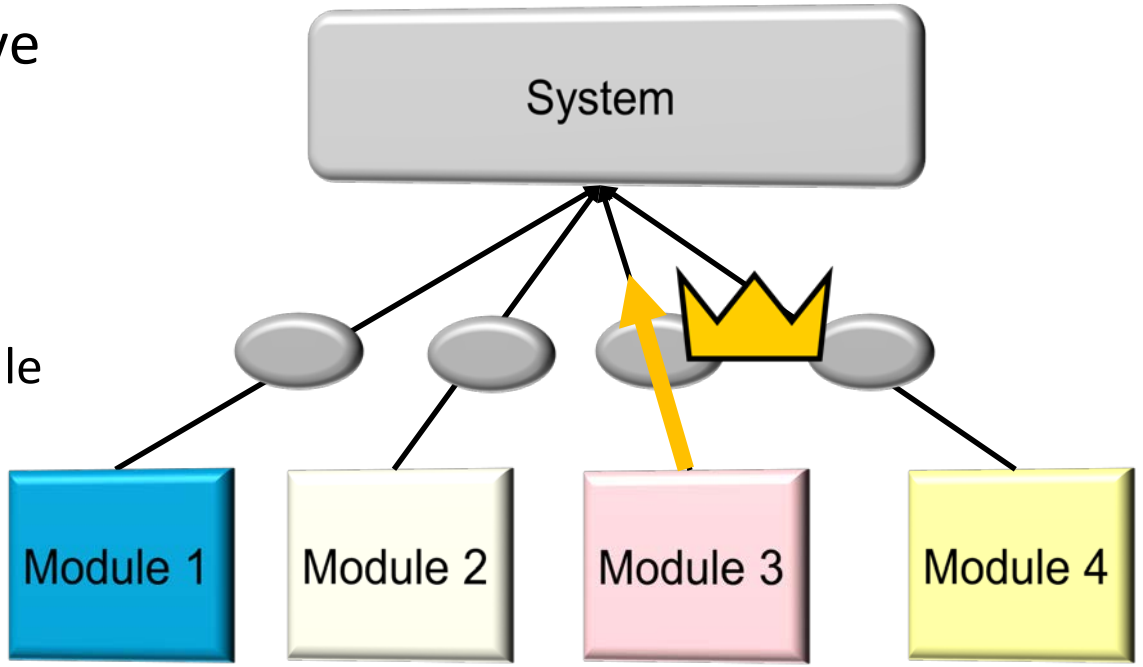
Security Concerns: Loss of Intellectual Property (IP) and Critical Program Information (CPI)

- What if Module 3 contains IP or CPI?
  - Each module should be designed capable of protecting IP and CPI
- Countermeasures:
  - Cybersecurity
  - Anti-Tamper



Security Concerns: Loss of Intellectual Property (IP) and Critical Program Information (CPI)

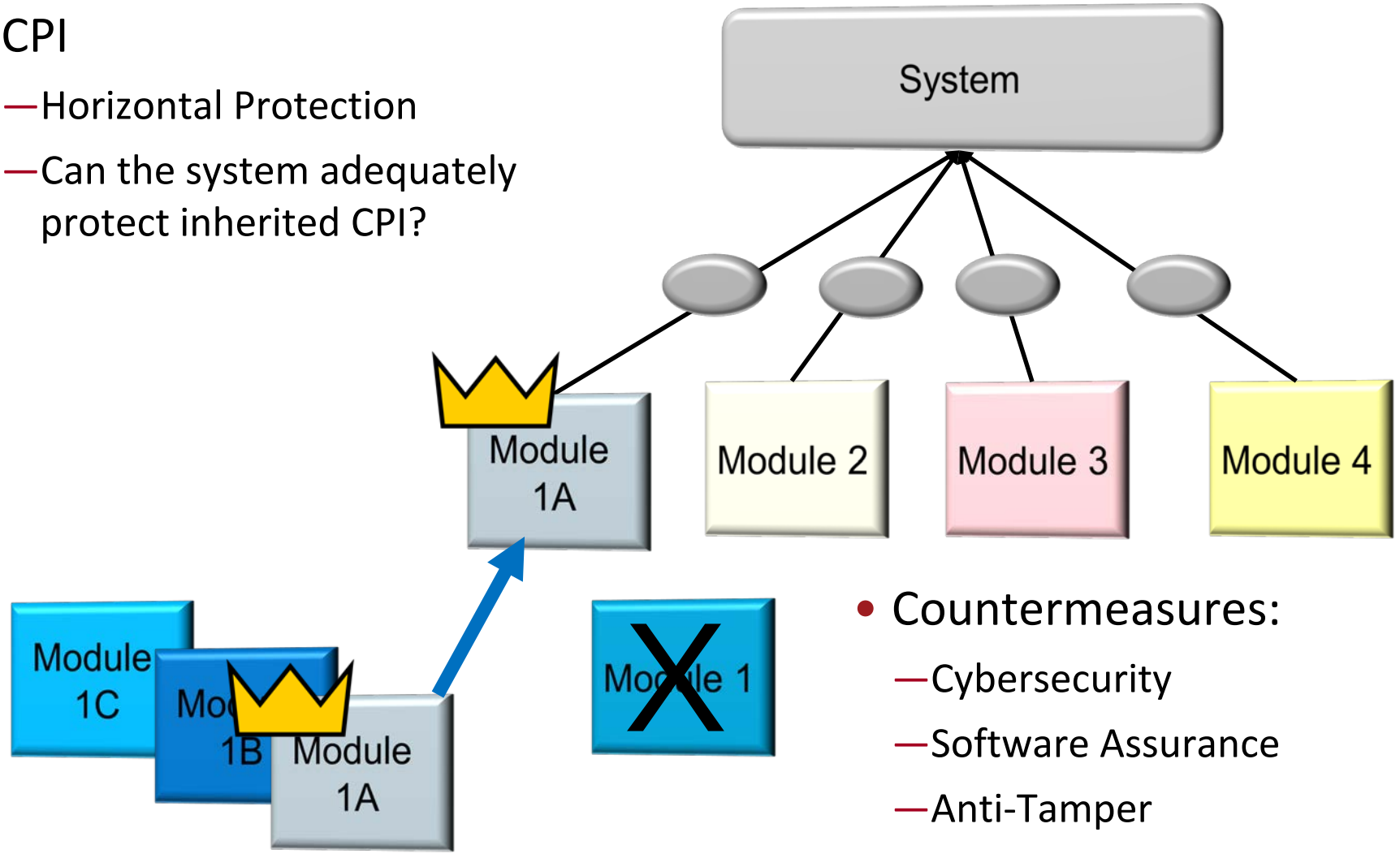
- What if system functionality requires IP or CPI to leave Module 3?
  - —Protection of interfaces
  - —Adequate handling and protection in receiving Module



- Countermeasures:
  - —Cybersecurity
  - —Anti-Tamper

Security Concerns: Loss of Intellectual Property (IP) and Critical Program Information (CPI)

- Swappable modules with IP or CPI
  - —Horizontal Protection
  - —Can the system adequately protect inherited CPI?

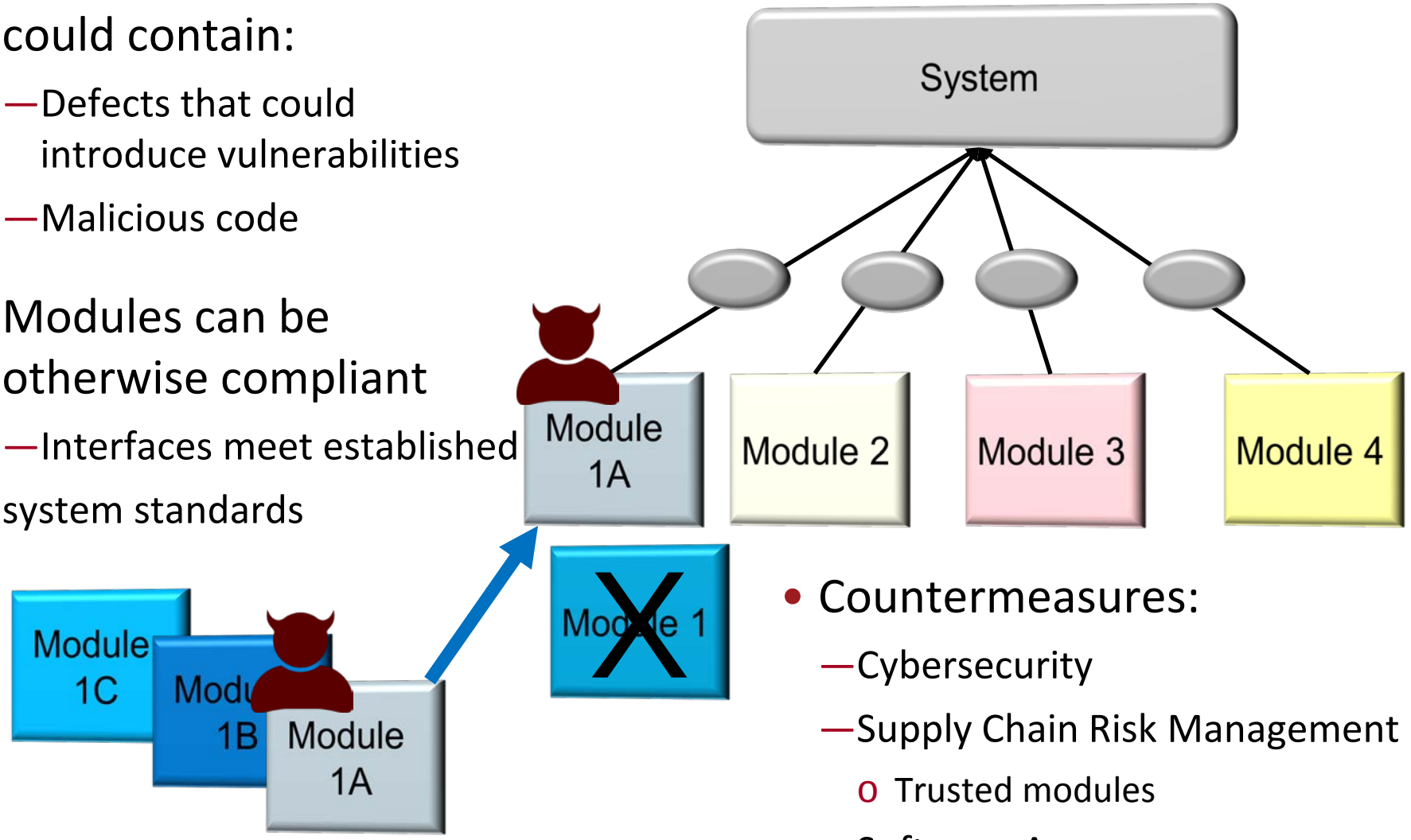


- Countermeasures:
  - —Cybersecurity
  - —Software Assurance
  - —Anti-Tamper

SYSTEMS ENGINEERING RESEARCH CENTER

Security Concerns: Malicious Insertion

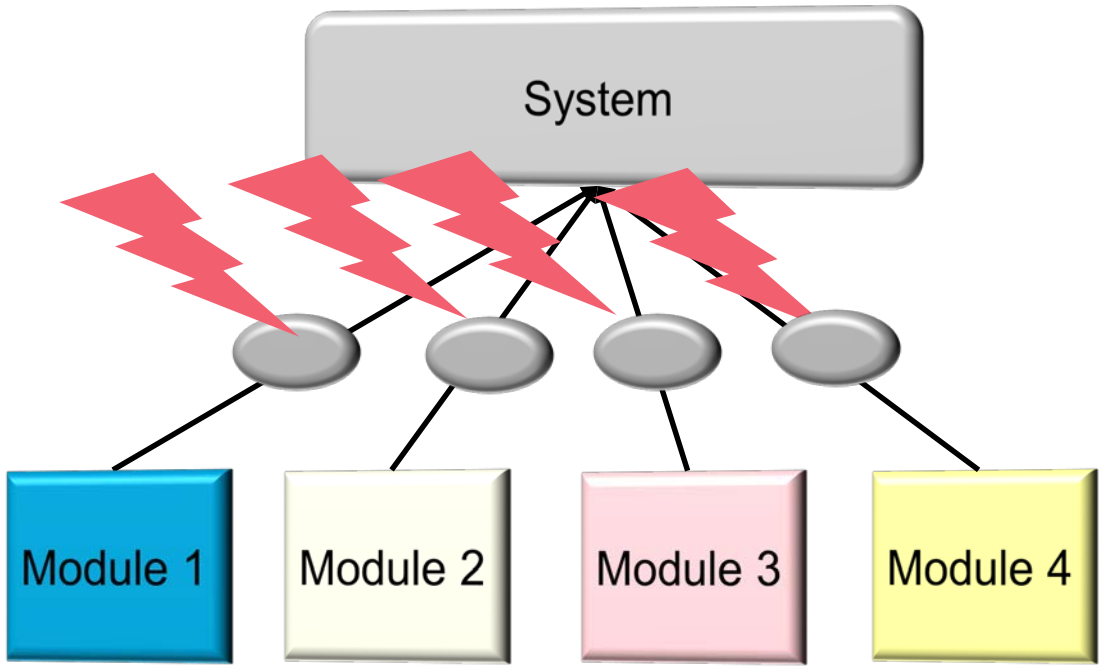
- Swappable modules could contain:
  - —Defects that could introduce vulnerabilities
  - —Malicious code
- Modules can be otherwise compliant
  - —Interfaces meet established system standards



- Countermeasures:
  - —Cybersecurity
  - —Supply Chain Risk Management
    - o Trusted modules
  - —Software Assurance

Security Concerns: Interface Attacks

- Interfaces compliant with Open Standards
  - One successful exploit could potentially affect multiple modules and interfaces
  - Need to understand how to protect critical data traversing through the interfaces
    - While still maintaining openness
  - Public disclosure of open standards or security mechanisms may be a risk to overall security architecture
  - Potential decrease in attacker's needed capability
  - Potential increase of attack vectors



- Countermeasures:
  - Cybersecurity
  - Software Assurance
  - Anti-Tamper

SYSTEMS ENGINEERING RESEARCH CENTER

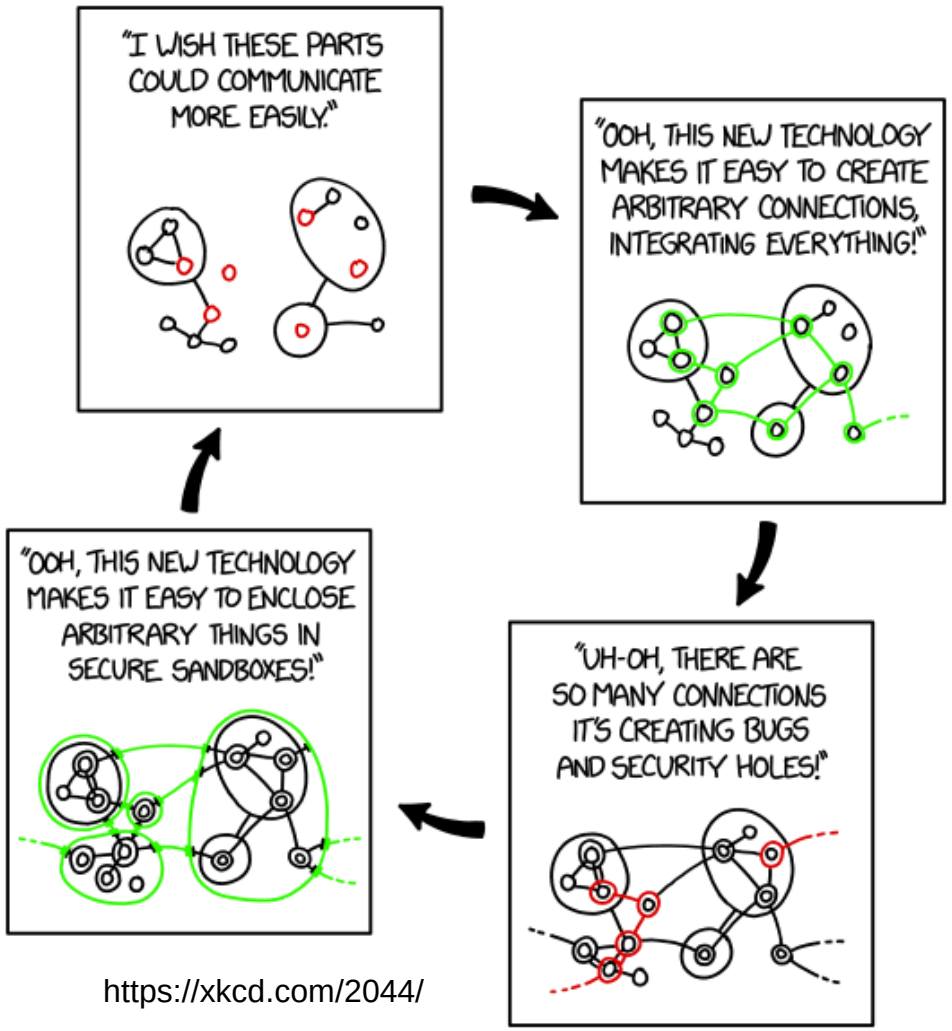
Research Outcomes and Next Steps

- Potential Outcomes of this Research
  - Processes
  - Metrics
  - Best Practices and Recommendations
  - Standards and Certification Processes for secure MOSA

- Next Step: Comprehensive Literature Review

Conclusion

- MOSA security cannot be a “snap-on” solution or an afterthought
- Need a holistic approach to understanding security implications and designing MOSA security architectures
  - —Systems Security Engineering can get us there
- This presentation is just the beginning
  - —Much to research and much to learn!



https://xkcd.com/2044/

SYSTEMS ENGINEERING RESEARCH CENTER

References

- Decker, Bill. “Cybersecurity and Modular Open Systems Approach,” October 26, 2017
- United States Department of Defense “Program Protection Plan Outline and Guidance.Doc,” Version 1.0, July 2011
- Reed, Melinda. “System Security Engineering for Program Protection and Cybersecurity,” October 27, 2017, 18th Annual NDIA Systems Engineering Conference.
- Ross, Ron, Michael McEvilley, and Janet Carrier Oren. “Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.” National Institute of Standards and Technology, November 2016. https://doi.org/10.6028/NIST.SP.800-160.
- Shanahan, Raymond. “Identification and Protection of Critical Program Information (CPI),” October 27, 2017, 18th Annual NDIA Systems Engineering Conference.
- Davendralingam, Navindran, Cesare Guariniello, Shashank Tamaskar, Daniel DeLaurentis, and Mitchell Kerman. “Modularity Research to Guide MOSA Implementation.” *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, January 30, 2018, 154851291774935. https://doi.org/10.1177/1548512917749358.
- Gaska, T. “Optimizing an Icremental Modular Open System Approach (MOSA) in Avionics Systems for Balanced Architecture Decisions.” In *2012 IEEE/AIAA 31st Digital Avionics Systems Conference (DASC)*, 1–23, 2012. https://doi.org/10.1109/DASC.2012.6383101.
- Rose, Leo J., Jonathan Shaver, Quinn Young, and Jacob Christensen. “Open Architecture Applied to Next-Generation Weapons.” edited by Raja Suresh, 90960K. Baltimore, Maryland, USA, 2014. https://doi.org/10.1117/12.2055266.
- Vai, Michael, Kyle Ingols, Josh Kramer, Ford Ennis, Michael Geis, Ted Lyszczarz, and Rob Cunningham. “Anti-Tamper in Open Architecture Systems,” Septecmber 20, 2011; IEEE HPEC 2011.