NDIA SE Conference 2016

System Security Engineering Track Session Kickoff

Holly Dunlap

NDIA SSE Committee Chair

Holly. Dunlap@Raytheon.com

"This document does not contain technology or Technical Data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations."

System Security Engineering Track

Agenda

- Welcome
- NDIA Mission
- Introductions
- SSE Committee 2016 Accomplishments
- SSE Committee 2017 Planning
- SSE Track At A Glance

NDIA Mission

Mission:

- To promote the widespread use of systems engineering (SE) in the Department of Defense (DoD) acquisition process in order to achieve affordable and supportable weapon systems that meet the needs of the military users. To provide a forum for the open exchange of ideas and concepts between government, industry and academia. To develop a new understanding of a streamlined SE process.

- The SE Division seeks to effect good technical and business practices within the aerospace and defense industry. It focuses on improving delivered system performance, including supportability, sustainability, and affordability. The division emphasizes excellence in systems engineering throughout the program life cycle and across all engineering disciplines and support functions.

Introductions

Industry
Government
Military
Intelligence
FFRDC
Academia

Policy & Governance
Major Defense Programs
Acquisition
Systems Engineering
System Security Engineering
Resiliency
Cybersecurity
Information Assurance
Software Assurance
Hardware Assurance
Supply Chain
Testing
Standards

Thank you to those that are actively engaged and shaping the future!

2016 Accomplishments Summary

Joint Projects:

- A Path Towards Cyber Resilient and Secure Systems Metrics & Measures
- NIST SP 800-160 Review & Comment
  - INCOSE SSE Committee
- Joint Federated Assurance Center (JFAC) SwA
  - NDIA Software Committee
- NDIA SE Issues Workshop

Provided an SSE Industry Perspective:

- GOMACTech
- Association of Old Crows Cyber Summit
- Optimizing the AF Acquisition Strategy of Secure & Reliable Electronic Components National Academy of Science
- Potomac Institute Tiers of Trust, "Hardware and IP Security: the Buyer's Perspective"

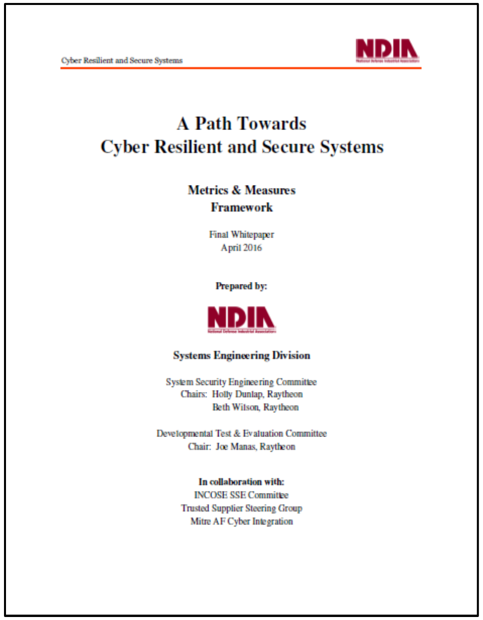
Committee Meeting Guest Speakers:

- Cyber Resiliency Focused SE
  - Suzanne Hassell, Raytheon
- NIST SP 800-160

  Systems Security Engineering: *Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*
  - Michael McEvilley, Mitre
- JFAC SwA
  - Tom Hurt, OSD SE SwA
- System Security Engineering Integrated Technical Processes
  - Danny Holtzman, Mitre - Chief, AF Cyber Integration

A Path Towards Cyber Resilient and Secure Systems Metrics & Measures

Complete!



Cyber Resilient and Secure Systems

A Path Towards
Cyber Resilient and Secure Systems

Metrics & Measures
Framework

Final Whitepaper
April 2016

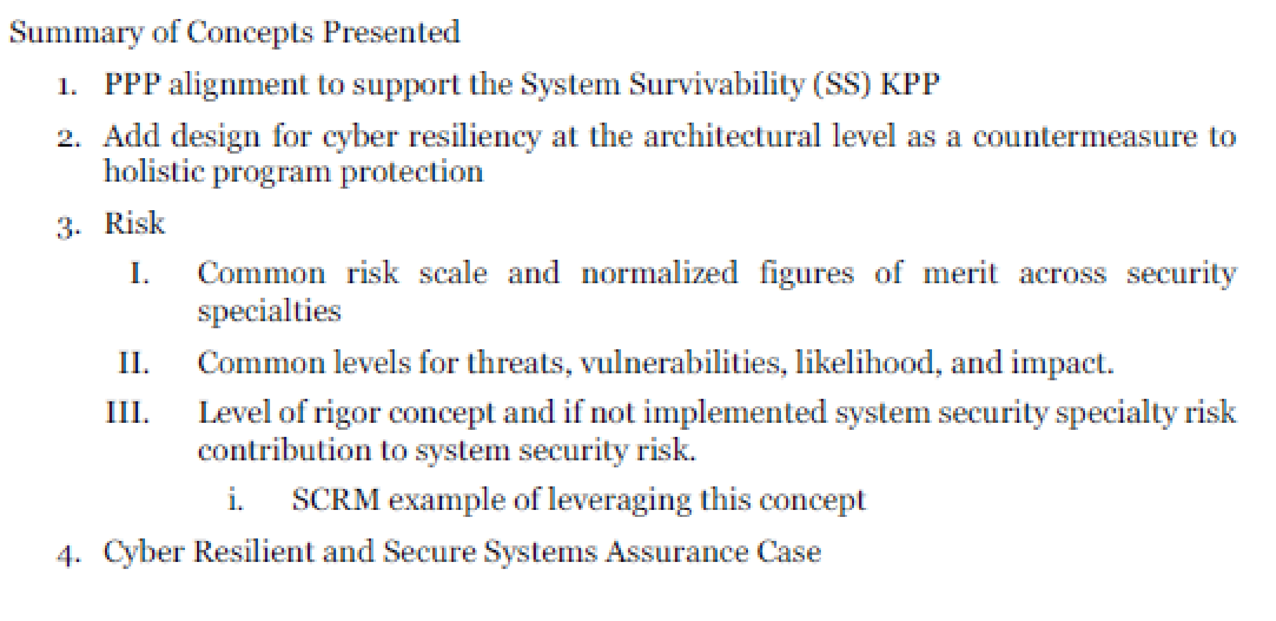
Prepared by:

Systems Engineering Division

System Security Engineering Committee
Chairs: Holly Dunlap, Raytheon
Beth Wilson, Raytheon

Developmental Test & Evaluation Committee
Chair: Joe Manas, Raytheon

In collaboration with:
INCOSE SSE Committee
Trusted Supplier Steering Group
Mitre AF Cyber Integration



Summary of Concepts Presented

1. PPP alignment to support the System Survivability (SS) KPP
2. Add design for cyber resiliency at the architectural level as a countermeasure to holistic program protection
3. Risk
   - I. Common risk scale and normalized figures of merit across security specialties
   - II. Common levels for threats, vulnerabilities, likelihood, and impact.
   - III. Level of rigor concept and if not implemented system security specialty risk contribution to system security risk.
     - i. SCRM example of leveraging this concept
4. Cyber Resilient and Secure Systems Assurance Case

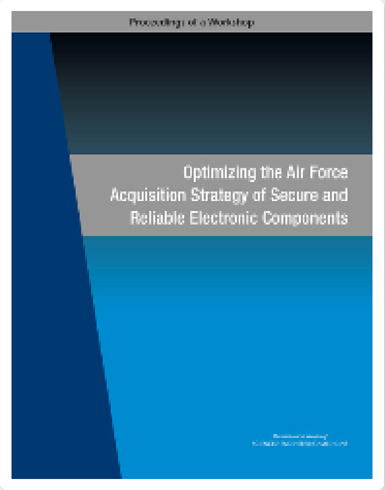
System Security Engineering Chair: Holly Dunlap, Raytheon
Holly.Dunlap@Raytheon.com

Beth Wilson, Raytheon
Beth_J_Wilson@Raytheon.com

The Joint NDIA SSE & DT&E Paper is Posted on the NDIA Systems Engineering Division Studies & Publications Website:

http://www.ndia.org/Divisions/Divisions/SystemsEngineering/Pages/Studies.aspx

Optimizing the Air Force Acquisition Strategy of Secure and Reliable Electronic Components National Academy of Science



Proceedings of a Workshop

Optimizing the Air Force Acquisition Strategy of Secure and Reliable Electronic Components

Description

In 2012, the National Defense Authorization Act (NDAA), section 818, outlined new requirements for industry to serve as the lead in averting counterfeits in the defense supply chain. Subsequently, the House Armed Services Committee, in its report on the Fiscal Year 2016 NDAA, noted that the pending sale of IBM's microprocessor fabrication facilities to Global Foundries created uncertainty about future access of the United States to trusted state-of-the-art microelectronic components and directed the Comptroller General to assess the Department of Defense's (DoD's) actions and measures to address this threat.

Terms of Reference:

1. Define the current technological and policy challenges with maintaining a reliable and secure source of microelectronic components;
2. Review the current state of acquisition processes within the Air Force for acquiring reliable and secure microelectronic components; and
3. Explore options for possible business models within the national security complex that would be relevant for the Air Force acquisition community.

This publication summarizes the results of the workshop.

http://www.nap.edu/catalog/23561/optimizing-the-air-force-acquisition-strategy-of-secure-and-reliable-electronic-components

Partner with Trusted Suppliers Steering Group

Government Microelectronics Applications Critical Technology Conference

GOMACTech Conference

- March 14 – 17 2016 Orlando, FL
- **March 20-23, 2017, Reno, NV**
- https://www.gomactech.net/

Key Note & Industry Panel Session:

“Systems Security Engineering and Cyber Resiliency: The Component Connection”

Major defense systems integrators shared their experience, expertise, and company perspective on integrating security into their program supply chain strategies.

Facilitated by Holly Dunlap

Raytheon, NDIA SSE Committee Chair

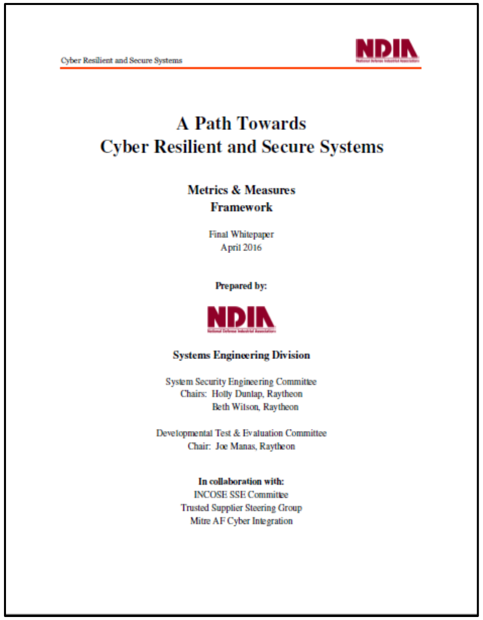
Association of Old Crows Cyber Summit April 2016

Cyber Challenges: Threat, Technologies, and Systems

A classified summit focusing on cyber challenges facing the U.S., Operations Other than War, and its Allies. Speakers and panelists discussed operational needs and technology gaps, strategies and methodologies, resources, systems, and solutions to design and field infrastructure and capabilities resilient to the advanced cyber threats.

NDIA SSE Chair: Holly Dunlap

Cyber Challenge via Systems Security Engineering Prime System Integrator Perspective



Cyber Resilient and Secure Systems

A Path Towards
Cyber Resilient and Secure Systems

**Metrics & Measures
Framework**

Final Whitepaper
April 2016

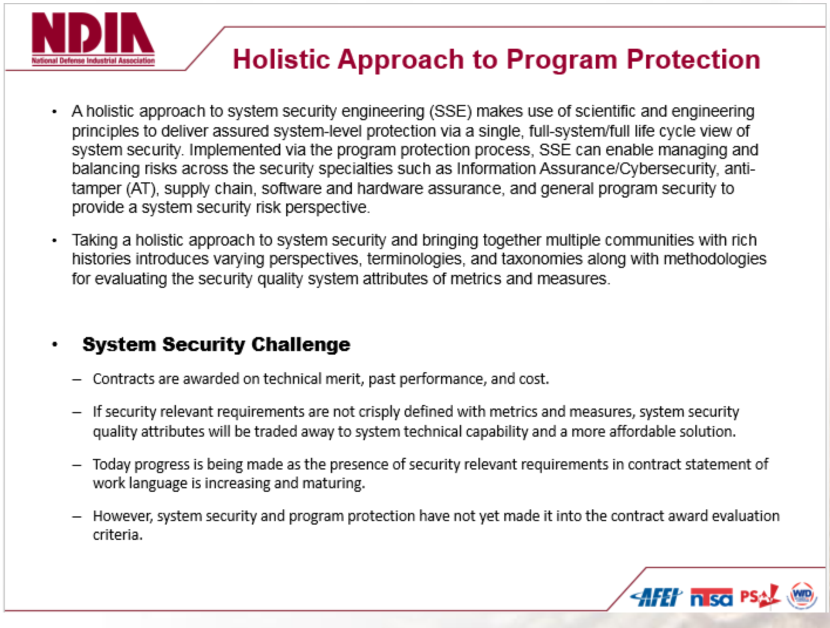
Prepared by:

Systems Engineering Division

System Security Engineering Committee
Chairs: Holly Dunlap, Raytheon
Beth Wilson, Raytheon

Developmental Test & Evaluation Committee
Chair: Joe Manas, Raytheon

In collaboration with:
INCOSE SSE Committee
Trusted Supplier Steering Group
Mitre AF Cyber Integration

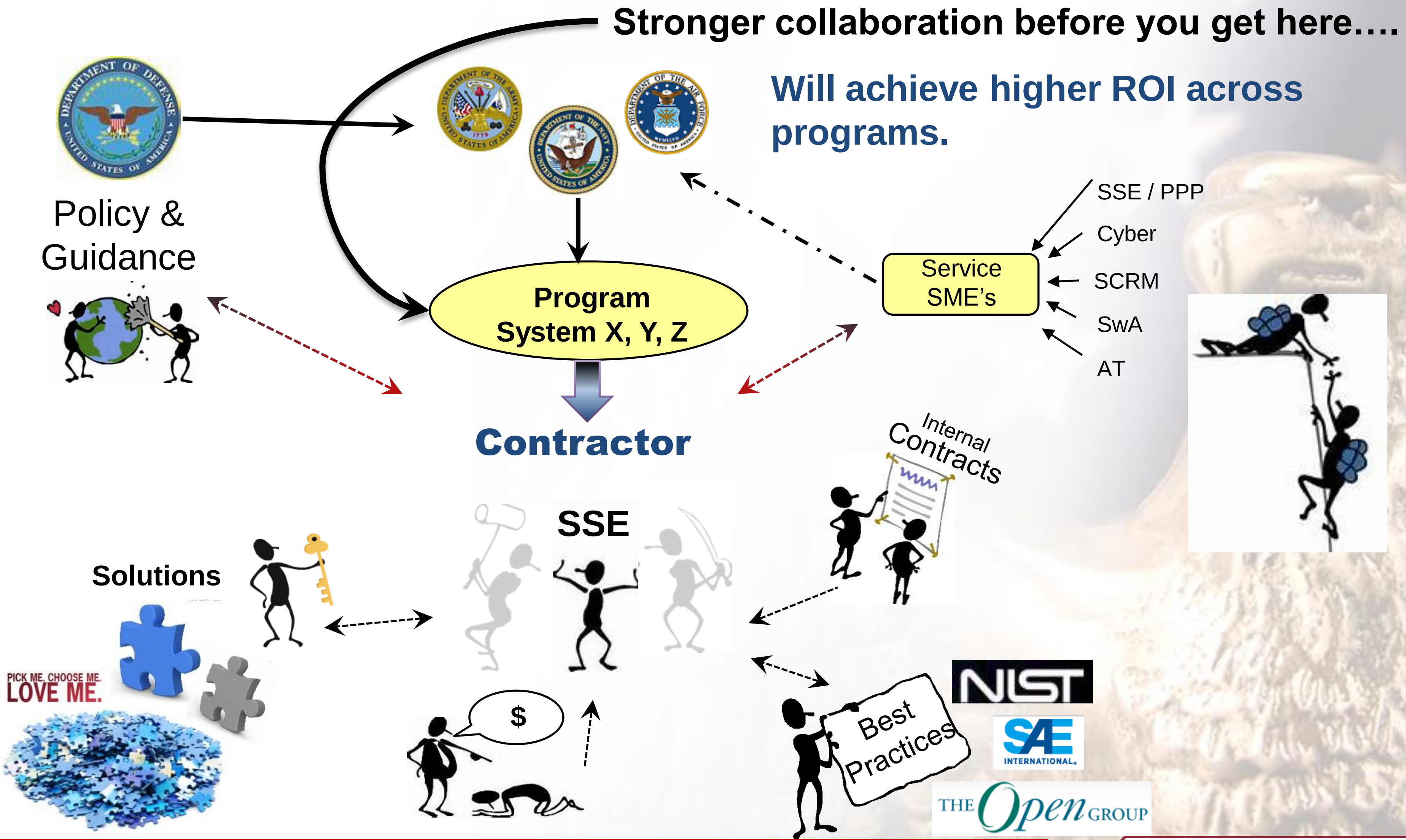


Holistic Approach to Program Protection

- A holistic approach to system security engineering (SSE) makes use of scientific and engineering principles to deliver assured system-level protection via a single, full-system/full life cycle view of system security. Implemented via the program protection process, SSE can enable managing and balancing risks across the security specialties such as Information Assurance/Cybersecurity, anti-tamper (AT), supply chain, software and hardware assurance, and general program security to provide a system security risk perspective.
- Taking a holistic approach to system security and bringing together multiple communities with rich histories introduces varying perspectives, terminologies, and taxonomies along with methodologies for evaluating the security quality system attributes of metrics and measures.

- **System Security Challenge**
  - Contracts are awarded on technical merit, past performance, and cost.
  - If security relevant requirements are not crisply defined with metrics and measures, system security quality attributes will be traded away to system technical capability and a more affordable solution.
  - Today progress is being made as the presence of security relevant requirements in contract statement of work language is increasing and maturing.
  - However, system security and program protection have not yet made it into the contract award evaluation criteria.

This is How We Feel…..



Stronger collaboration before you get here….

Will achieve higher ROI across programs.

Policy & Guidance

Program System X, Y, Z

Service SME's

SSE / PPP

Cyber

SCRM

SwA

AT

Contractor

SSE

Solutions

Internal Contracts

Best Practices

Encourage Stronger Industry & Government Collaboration

SSE Committee Planning 2017

Topics for Consideration:

- System security risk contributions to the program technical performance risk
- System security engineering design principles and practices for embedded systems

Collaboration & Outreach Opportunities:

- Joint Federated Assurance Center (JFAC)
- INCOSE SSE
- NDIA DT&E Committee
- NDIA Trusted Microelectronics
- AF Cyber Secure Task Force
- Navy CyberSafe

Methods:

- Projects
- Guest Speakers

SSE Track At A Glance

- SSE Committee
- Program Protection & Cybersecurity
- SSE, Whose Job Is It Anyway?
- Mission Assurance & Cybersecurity, Academia
- Protecting Unclassified Controlled Technical Information
- Acquisition Strategy, Cyber Resilient Weapon Systems
- NIST SP 800-160 Security Engineering
- Cyber Resiliency in the SE “V”
- SSE for Mission Assurance
- DoD Strategy for Assured Microelectronics
- Critical Component Identification
- Managing the Security Risk for FPGA IP
- Behavior Analysis for Efficient Malware Detection
- System Security Engineering & Cyber Resiliency: Component Connection
- Injecting Security into Decision Analysis
- Whitelisting Products
- Applying RMF for a Successful Program Case Study
- SwA & RMF
- Cyber FMECA, Cyber Effects Criticality Determination
- Joint Federated Assurance Center
- JFAC Industry Outreach
- Systems & SwA Capability Gap Analysis
- Cybersecurity Test Lessons Learned
- Forecasting System Capabilities & Mission Assurance
- System Security Statistical Test Optimization Panel Discussion
- Cyber Modeling & Simulation
- Cybersecurity for Advanced Manufacturing
- Model Based Cyber Enterprise Assessment System
- SE Methods for Incorporating Innovative Technologies in DoD Systems

Export Controlled Marking – See Cover Page

* See Conference Agenda for Detailed Presentation Titles and Presenters

Questions?