NDIA System Security Engineering Committee

June 2020

Holly Dunlap
Raytheon
NDIA SSE Committee Chair
Holly.Dunlap@Raytheon.com

Cory Ocker
Raytheon
NDIA SSE Committee Co-Chair
Cory.Ocker@Raytheon.com

SSE Committee Feb – June Summary

Accomplishments:

- IEEE NDIA INCOSE System Security Symposium, 6-9 April 2020
  - Transitioned to Virtual On-Demand Presentations
- AF Weapon System Program Protection / System Security Engineering Guidebook
- INCOSE Fuse System Security Charter & Collaboration
- NIST 800-53 Review & Comment

IEEE NDIA INCOSE
System Security Symposium

~~April 6-9, 2020~~

SYSTEMS SECURITY symposium

Virtual On-Demand Presentations July 1 – August 1st.

The IEEE-INCOSE-NDIA Systems Security Symposium seeks research papers and application studies that focus on the development of secure, safe, and resilient systems. This symposium attempts to address the convergence of cybersecurity, safety, and engineering with interest in the effective application of security principles, methods, and tools to complex systems such as cyber-physical systems, autonomous systems, transportation vehicles, medical devices, large IoT systems, and other systems of interest. Preference will be given to papers and case studies that bridge theory to practice.

Systems Security Symposium 2020

Topics

- Systems Security Work Focused on Advancements in Theory, Practice, and Education
- Engineering of Safe, Secure, and Resilient Systems
- Examples of Mission/Systems Assurance and Assurance Cases
- Model Based Engineering focused on Security, Safety, Trust, Resiliency
- Affordable and Scalable Approaches to Hardware, Software, Firmware Assurance
- Novel Architecture Design and Analysis Examples or Trade-Space Studies
- Trust of Complex Systems with Emphasis on Cyber-Physical Systems
- Security considerations for machine learning / artificial intelligence
- Large-Scale DevSecOps and Agile Approaches for System Development
- System Security Design Considerations for Cloud Environments
- Verification, Validation, and Evidences for Secure System Development
- Extensions of Formal Methods to System-Level Evaluation
- Cybersecurity in Manufacturing and Supply Chains
- Case studies to include automotive, transportation, space, and others
- Cyber-Physical System Event Detection, Investigation, Forensics, and Malware Analysis
- Tailored Risk Management Approaches for Large Complex Systems
- Attack/Defense Modeling, Simulation, and Characterization
- Techniques for Cyber Risk Buy Down in Legacy Systems, Infrastructure, and Enterprises
- Policy, Ethical, Legal, Privacy, Economic, and Social Issues

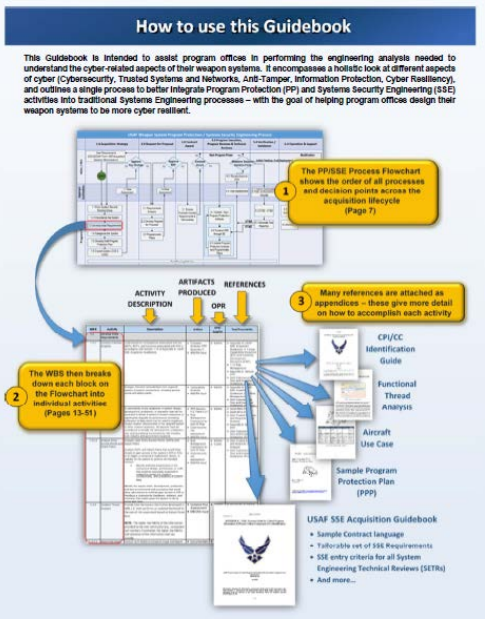
http://www.ieeesystemssecuritysymposium.org

IEEE/NDIA/INCOSE Systems Security Symposium 2020 will now be held as a virtual on-demand conference of recorded paper presentations to be held July 1 – August 1, 2020. Plenary session speakers and panels as well as track session panels will be rescheduled for 2021. We will be offering a virtual presentation option for all of our SSS 2020 authors. The papers of all approved authors will be sent to IEEE with intent to publish in the IEEE XPLORE Library, and the presentations of all who present virtually will be available on the conference website. All authors and attendees will receive a 50% discount on all conference registration fees.

AF Weapon System Program Protection / System Security Engineering Guidebook

- Multi-year collaboration with the AF Cyber Resiliency Office of Weapon Systems
- Currently the most comprehensive SSE / PP Guidebook
- The guide includes:
  - USAF Weapon System PP / SSE Process
  - USAF Process Guide for Critical Program Information and Critical Component Identification
  - USAF SSE Acquisition Guidebook
  - Examples
  - Templates
  - Tools
- Highly recommend using this guide as the preferred reference and encourage the community to continue to improve and mature.
- The AF CROWS continues to be open to feedback.

The USAF SSE Acquisition Guidebook was the primary focus for the SSE Committee



The document is available within the anti-tamper (AT) homepage link: (The documents are located under “resources” tab under “policy” folder. Then click “Air Force” and our documents are located there).
https://at.dod.mil/

Approved for Public Release

Fuse System Security Charter Text

The Future of Systems Engineering (FuSE) is an INCOSE led multi-organization collaborative initiative that has identified a number of specific topics to be investigated (INCOSE nd).

The frontiers of system security threats and opportunities are continuously expanding, which drives a need for systems engineering to enable and facilitate effective systems security at pace. Security reality sets the pace.

Security engineering has responsibility for designing and implementing social and technical preventative measures and counter measures. Systems engineering has responsibility for enabling and facilitating effective system security engineering.

As independent disciplines neither systems engineering, nor security engineering, can address the pace of need. Collaborative and cooperative real-time teaming appears to be necessary for Security in the Future of Systems Engineering.

Our initial focus in the security topic within the FuSE initiative is on foundation development – general concepts for shaping the breadth and depth of future solution strategies. Foundation development projects are akin to TRL-1 and TRL-2 Technology Readiness Levels: basic principles observed and reported, and technology concepts and/or applications formulated. In general this work should deal with concepts that can be carried forward in the near term as opposed to needing hoped-for technology that can not be predicted for useful availability, e.g., quantum computers.

The FuSE security team will conduct active collaborations on foundational work: identifying foundation areas to pursue, establishing project participants in those different areas, beginning those projects, and publishing project results. Three initial papers are offered as inspirational models for identifying additional work at the foundation level (Dove, Willett 2020a, 2020b; Willett 2020).

Approved for Public Release

FuSE System Security Charter v200408

Title: Systems Security in the Future of Systems Engineering
(a FuSE initiative topic project)

Owner: Rick Dove
Initial Team: Rick Dove, Keith Willett (INCOSE), Tom McDermott (SERC), Holly Dunlap, Corey Ocker (NDIA), Delia MacNamara, Shankar Sankaran (ISSS).

What will good look like when we use FuSE to deliver systems?

1. Security Engineers will be active members of the Systems Engineering team.
2. Security will be rapidly reconfigurable, augmentable, and composable.
3. System and component behavior will be monitored for anomalous operation.
4. Modeling will be used to predict variations and prepare contingent courses of action.
5. Security will support rather than impede personal and organizational productivity.
6. System components will be self protective.

What is stopping us from doing this now?

1. SE relates to SecE as an independent specialty practice.
2. Security is viewed as a non-functional cost.
3. Security standards compliance is considered sufficient.
4. Actionable research is in early stages.
5. SE contracts and projects detail features and requirements up front rather than desired capabilities that allow innovative solutions.

What will good look like in 2023-2025?

1. Security Engineering will have full involvement on SE-team.
2. Rapid security reconfiguration and augmentation will have some effective working patterns in practice as an early base line.

What will good look like by end of 2020?

1. Multi-organization collaboration will be active.
2. Initially needed foundation material (TRL-1) for FuSE Security identified.
3. Projects to develop and publish some of the needed foundation material (TRL-1 and -2) active.

Action Plan

1. IS20 initial foundation papers:
   Techno-Social Contracts for Security Orchestration.
   Contextually Aware Agile Security.
   Architecting the Future of System Security.
2. Ongoing: Recruit additional team members.
3. Mid 2020: Periodic web workshops in process identifying additional foundation areas.
4. Late 2020: Addition foundation papers in process

NIST SP 800-53 Revision 5

- Call for comments went out on 22 April
- CRMs submitted and collated
- Committee meeting to review comments and select top concerns held on 19 May

Table 1: Top Industry Concerns – NIST SP 800-53 Revision 5

Topic	Concern	Recommendation
Security and Privacy Engineering Principles	If the current level of detail in the SA-8 controls is placed on contract, the USG will be directing "how" to design verses allowing contractors to use these principles and identify strengths within their system designs. If a checklist / compliance approach is used, this control will be extremely difficult to evaluate.	Provide clarifying statement at the SA-8 control level addressing concern
Integration of other Special Publications	While some references to other SPs are included 800-161, 800-160, etc, there is not clear direction on the interconnection between the policies	Add front matter discussing how the Special Publications are interconnected. When referencing another SP from a control, reference the specific section within that SP that applies. Not the entire document.
Cyber Resilience / System Survivability	Cyber resilience and System Survivability were introduced in the updated front matter, but seem like a hanging chad.	Highlight controls that support resiliency and survivability and add additional details in the supplemental guidance.
SCRM Tracing	Need to understand what controls in other families are related to the SCRM controls	Add trace of SCRM controls to controls in other families that support SCRM
Clarify definition of "domains"	The terms "cross-domain" and "different security domains" are used throughout the document.	Need to clarify the differences between the two terms to prevent confusion.
Anti-Tamper	Need to clarify differences between Tamper and Anti-Tamper, which has additional connotations	Update definitions. Reference other USG publically available policies and offices that specialize in Anti-Tamper

Approved for Public Release

Backup

2020 Plans / Events / Milestones

Primary Focus: IEEE NDIA INCOSE System Security Symposium, 6-9 April 2020

Collaboration/engagement with NNSA, JFAC, Services, OSD

Support OSD Standardization Efforts – Data Item Descriptions, Work Breakdown Structure, etc

Help establish a Software Assurance Committee in conjunction with JFAC

SCRM Community of Interest awareness and participation

Provide recommendations based on recent NDIA Survey on SCRM

Air Force policy review to minimize compliance activities

Advocate for a program perspective on CDI – implementation and impacts

Standards review, comment, and analyze as appropriate:

- NIST 800-53 Rev 5 Security and Privacy Controls for Federal Information Systems and Organizations
- SAE G32 Cyber Physical Systems
- Cybersecurity Maturity Model Certification
- NIST Special Publication 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations
- NISTIR 8276 - Key Practices in Cyber Supply Chain Risk Management
- DoDI & DoDM 8140 Cyberspace Workforce Management

Review and consider SSE related impacts of 5000.02 update

System Security Engineering Committee

Mission / Purpose	Stakeholders / Sponsors / Collaborators
To promote System Security Engineering integration into the Systems Engineering and Mission Assurance processes in the Department of Defense (DoD) acquisition of weapon systems. Chair: Holly Dunlap Co-Chair: Cory Ocker	Stakeholder: OSD (R&E) Government Liaison: Melinda Reed Collaborating organizations: AF CROWS, NAVAIR 4.0, JFAC, NNSA, SAE, INCOSE, IEEE

2019 Accomplishments	2020 Plans / Events / Milestones
Accomplishments (see chart 4): • Projects & Initiatives • Information Exchange • Committee Chair Representation Events: • 20+ SSE Track Briefings at NDIA Systems & Mission Engineering Annual Conference Publications reviewed: • 4 standards/guidebooks/policies reviewed and commented on	Planned Activities • Collaboration with OSD, Services, JFAC, NNSA • SCRM Community of Interest • AF Policy Review to minimize compliance activities Planned Events • IEEE, NDIA, INCOSE System Security Symposium April 2020 Planned Publications • Standardization – DIDs, WBS • 5000.02 Review • OSD Org Chart with SSE Swim Lanes

Mission / Purpose

To promote System Security Engineering integration into the Systems Engineering and Mission Assurance processes in the Department of Defense (DoD) acquisition of weapon systems. To foster the development of System Security Engineering methods, tools, techniques, and processes required for the role of System Security Engineers. To provide a forum for the open exchange of ideas and concepts between government, industry, FFRDC and academia. To develop a new understanding of System Security Engineering and the critical role it plays to ensure system survivability in a cyber contested environment.

Goals

The System Security Engineering (SSE) Committee seeks to:

- ***Advance SSE technical and business practices within the aerospace and defense industry.***
- ***Focuses on improving delivered system security performance including survivability, resiliency, and affordability.***
- ***Promote and emphasize excellence in systems security engineering throughout the program life cycle and across engineering and non-engineering disciplines required for a holistic approach to system security and program protection.***

Objectives

- ***Lead projects in areas that challenge the role and responsibility unique to System Security Engineering.***
  - *Projects may include but are not limited to providing a system security engineering industry perspective on draft or current System Security Engineering relevant government policies, government instructions, industry standards, industry best practices, customer requirements, risk management, etc.*
- ***Support security specialty projects and initiatives by providing a system security engineering perspective that directly effects and interfaces with system security engineering.***
- ***Encourage and promote the advancement, education, and skill development of the role of system security engineering.***

How do we operate?

NDIA Systems Engineering Division (SED) Planning meeting in December.

Attended by OSD & Services Executive Leaders & NDIA SED Committee Chairs

OSD & Services communicate their plans and priority needs for the next year.

Committee Chairs work with their committee to draft a list of priority challenges & candidate projects.

1st meeting of the year, present both the Government SSE challenges and Industry SSE challenges.

The Committee then reviews and proposes projects to address the challenges / needs.

This process establishes the plan for the year. However as opportunities and needs are presented throughout the year, the committee has the opportunity to consider updating the plan.

The SSE Committee typically meets the afternoon of the NDIA Systems Engineering Divisional meetings which are posted on the NDIA Systems Engineering website. We also send out an e-mail to NDIA SSE Committee members so please let us know if you'd like to be added to the committee email list.

We welcome and encourage participation at all skill levels.

Welcome and highly encourage committee members to lead projects and foster collaboration with other security specialty committees and working groups.

***** The number of projects, workshops, collaborations etc. along with the depth, quality, and level of rigor is dependent on the committee members commitment.**

2019 Accomplishments

Activity	Title
Projects & Initiatives	• USAF Weapon System Program Protection and System Security Engineering Process Guidebook • NDIA Critical Program Information (CPI) Assessment and Identification Guide (CAIG) • DoD DRAFT Software Acquisition Pathway Policy Guidance • Cyber Secure & Resilient Approaches for Feature Based Variation Management • IEEE, NDIA, INCOSE System Security Symposium April 2020 • NDIA Systems & Mission Engineering Annual October Conference • NIST SP 800-160 Developing a Cyber Resilient Systems Vol 2: A Systems Security Engineering Approach
Information Exchange	• DASD(R&E) Sponsored SEI SwA Products, PM & Designer Guide • DoD Cyber Workforce Management • SAE G32 Cyber Physical Systems • ASD(R&E) Cybersecurity Challenges – Protecting DoD Unclassified Information • NAVAIR CyberSafe • AF CROWS Program Protection and System Security Engineering Tools • ASD(R&E) CRWS Workshop Series
Committee Chair Rep.	• SecNav Cybersecurity Advisory Panel Meeting • Collaboration on Quality in the Space & Defense Industries Forum, March 2019