NDIA SED
System Security Engineering Committee

August 25, 2015

Holly Dunlap
NDIA SSE Chair
Raytheon

Beth Wilson
NDIA & INCOSE SSE
Raytheon

Summary of SSE Committee 2015 Achievements, Current Efforts, & Plans

NDIA
NATIONAL DEFENSE INDUSTRIAL ASSOCIATION
STRENGTH THROUGH INDUSTRY & TECHNOLOGY

	Topic	Activity
SSE	**Industry perspective**	Developed industry perspective reports on "Suggested Language to Incorporate System Security Engineering for Trusted Systems and Networks into Department of Defense Requests for Proposals; January 2014" (2) companies provided reports directly to OSD SE, Deputy for System Security and PP in 2014. - ***Request a DASD(SE) response to perspectives submitted*.**
	INCOSE & NDIA SSE Education / Training	Testing framework and competency model using SSE. Provided input to INCOSE / NDIA Education and Training committee. Update provided 4/22.
	SSE Committee Meetings & Metrics Project	1 Day Systems Security Metrics Workshop October 27th, 2014
		Joint DT&E and SSE Committee meeting on Metrics & Measures. 4/22, 6/17, 8/25 • Meeting included PPP relevant updates and activities from OSD SE PPP, briefs from Trusted Suppliers Group, and OSD DT&E.4/22 • Metrics and measures summary and proposed project paper outline with solicitation for authors 4/22, 7/17, 8/25 • SSE & Critical Components Collaboration – NDIA, AF, Mitre, Trusted Suppliers Steering Group 8/25 • Resilient & Trusted Cyber Systems Security Metrics & Measures Framework Whitepaper, collaboration with SSE, DT&E, INCOSE, TSSG • Plan to present at the fall SE Conference
	INCOSE SSE Committee	INCOSE SSE Committee has interest in joining the NDIA SSE Committee Metrics Project. Joining August 25th meeting
SED	**Developmental Test and Evaluation**	2015: Cyber testing guideline connections to Program Protection Planning NDIA DT&E Committee to join the SSE Committee Metrics Project

Completed	Current	Proposed

SSE Committee - 2015 Task Plan
Projects Working Group

Projects in progress 2015:

- **Metrics Project Finalized Outline**
  - Joint effort with NDIA SSE and DT&E
  - Interest from INCOSE SSE & TSSG in collaboration opportunities.
- **NDIA SE SSE Conference Track**
- **AF has expressed interest in increasing collaboration with the NDIA SSE Committee**

Deliverables/Products

- **Resilient & Trusted Cyber Systems Security Metrics & Measures Framework**
  - Plan to present at SE Conference

Schedule / Resources

- **SSE & DT&E Committee Meeting on Metrics & Measures August 25th - Seeking authors**
- **Collaboration opportunity with INCOSE SSE**
  - Virtual meeting opportunities

Holly.Dunlap@Raytheon.com

Issues / Concerns:

- **Request DASD(SE) & Service Update on PPP and SSE.**
- **Meta messages**
  - Expanding security related requirements but want **“no cost” solutions** due to stringent program price points.
  - Requirements are becoming more detailed in SOW & RFP language but **not a real priority as it is not in sections L&M.** This leads to security being traded away.

Joint Systems Security Engineering & Developmental Test & Evaluation Committee in Collaboration with the Air Force, Trusted Suppliers Group, & Mitre

August 25, 2015

Holly Dunlap
NDIA SSE Chair
Raytheon

Joe Manas
NDIA DT&E Chair
Raytheon

Mitre & AF Cyber Integration
Danny Holtzman

Beth Wilson
NDIA & INCOSE SSE
Raytheon

Kaye Ortiz
Trusted Suppliers Steering Group

Don Davidson
DoD Office of the CIO
Sw & SCRM Working Group

Joint SSE & DT&E Committee Meeting August 25th Agenda

Virtual Meeting Time: 1:00 PM –3:30 PM EST (Connection details provided in the slide notes)

Welcome, Introductions, & Agenda (15 min)
Holly Dunlap, SSE Chair, Raytheon

NDIA Systems Engineering Division Update (15 min)
Holly Dunlap

INCOSE SSE (15 min)
Beth Wilson

Resilient & Trusted Cyber Systems Security Metrics & Measures Framework Whitepaper (25 min)
Holly Dunlap

Break (10 Min)

SSE and Critical Components (30 min)
AF / Mitre, Danny Holtzman

Discussion (15 min)

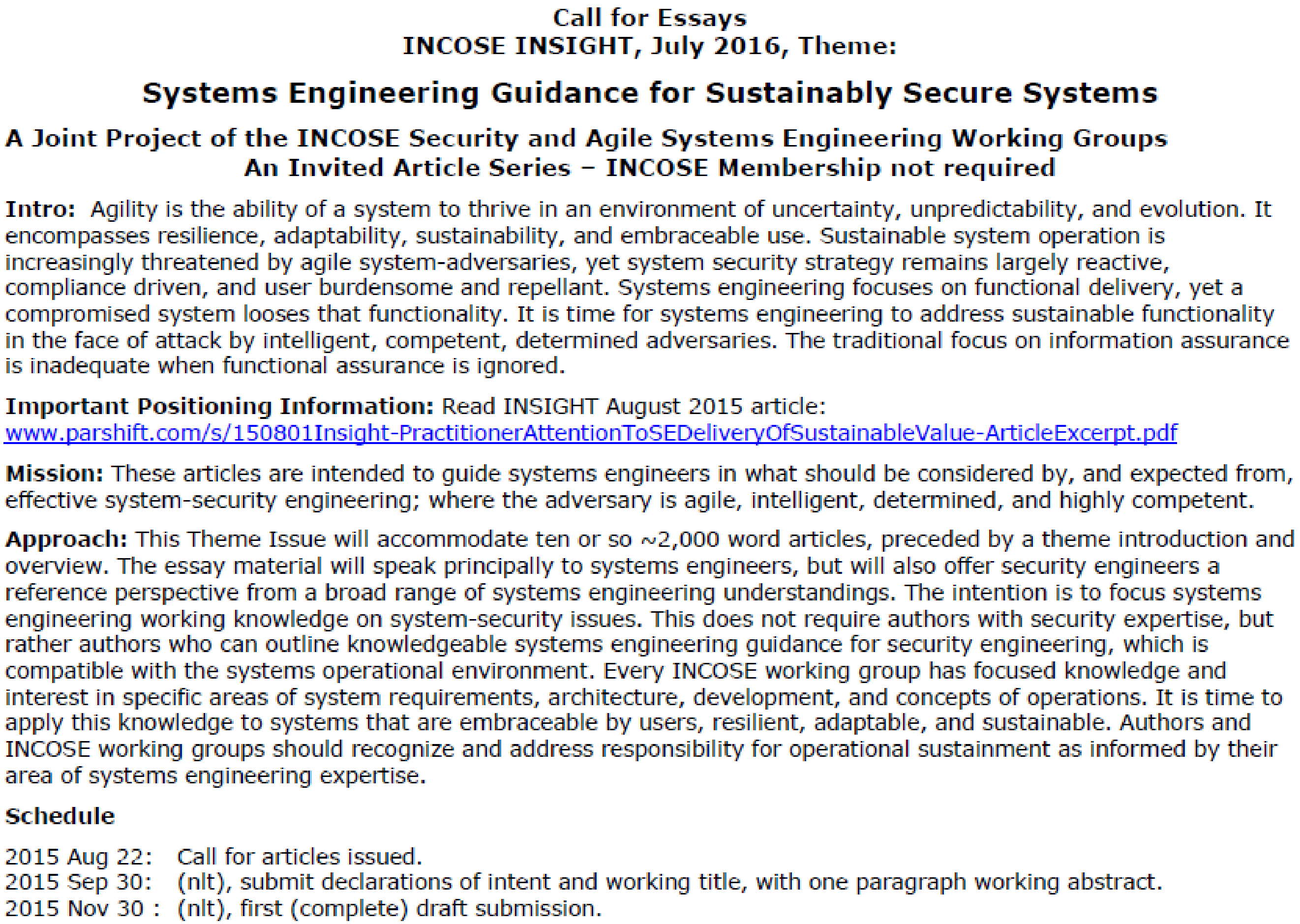
Introduce Plan for AF Collaboration (15 min)
AF / Mitre, Danny Holtzman

Close (10 min)

INCOSE SSE WG Projects

SSE WG Projects
INSIGHT Theme (08Q1, 09Q2, 11Q2, 13Q2, 16Q2)
Self-Organizing Security Pattern Language
Tracks at Non-INCOSE Conferences
SE Handbook: Section 9.6 (New) Systems Security Engineering Section 3.4 (New) Cyber Physical System Case Study
IS Annual Paper Track
SEBoK Systems Security Engineering Primary References
Alliance Opportunities with Security Organizations
NDIA Alliance
Reference Document for SEs on SSE
SE Responsibility Framework for Security
Webinars
Standards Review

INCOSE SSE WG Project INSIGHT July 2016



Call for Essays
INCOSE INSIGHT, July 2016, Theme:

Systems Engineering Guidance for Sustainably Secure Systems

A Joint Project of the INCOSE Security and Agile Systems Engineering Working Groups
An Invited Article Series – INCOSE Membership not required

Intro: Agility is the ability of a system to thrive in an environment of uncertainty, unpredictability, and evolution. It encompasses resilience, adaptability, sustainability, and embraceable use. Sustainable system operation is increasingly threatened by agile system-adversaries, yet system security strategy remains largely reactive, compliance driven, and user burdensome and repellant. Systems engineering focuses on functional delivery, yet a compromised system looses that functionality. It is time for systems engineering to address sustainable functionality in the face of attack by intelligent, competent, determined adversaries. The traditional focus on information assurance is inadequate when functional assurance is ignored.

Important Positioning Information: Read INSIGHT August 2015 article:
www.parshift.com/s/150801Insight-PractitionerAttentionToSEDeliveryOfSustainableValue-ArticleExcerpt.pdf

Mission: These articles are intended to guide systems engineers in what should be considered by, and expected from, effective system-security engineering; where the adversary is agile, intelligent, determined, and highly competent.

Approach: This Theme Issue will accommodate ten or so ~2,000 word articles, preceded by a theme introduction and overview. The essay material will speak principally to systems engineers, but will also offer security engineers a reference perspective from a broad range of systems engineering understandings. The intention is to focus systems engineering working knowledge on system-security issues. This does not require authors with security expertise, but rather authors who can outline knowledgeable systems engineering guidance for security engineering, which is compatible with the systems operational environment. Every INCOSE working group has focused knowledge and interest in specific areas of system requirements, architecture, development, and concepts of operations. It is time to apply this knowledge to systems that are embraceable by users, resilient, adaptable, and sustainable. Authors and INCOSE working groups should recognize and address responsibility for operational sustainment as informed by their area of systems engineering expertise.

Schedule

2015 Aug 22:	Call for articles issued.
2015 Sep 30:	(nlt), submit declarations of intent and working title, with one paragraph working abstract.
2015 Nov 30 :	(nlt), first (complete) draft submission.

INCOSE SSE WG Project NDIA Alliance

	SSE WG Projects # 12 **NDIA Alliance**
2014	**SSE Reference Document** NIST 800-160 review complete
2015	**SSE Competencies** 4/22/2015 meeting: INCOSE/NDIA competency model SSE roles with activities and competencies with proficiency levels Want to fully develop for SSE role
2015	**Metrics and Measures** May 2014 NDIA 3 day PPP Workshop Oct 2014 NDIA 1 day Metrics and Measures Workshop Apr 2015 meeting: kick off joint SSE/DT&E project Jun 2015 meeting: story board report Aug 2015 meeting: joint NDIA/INCOSE

Resilient & Trusted Cyber Systems Security Metrics & Measures Framework

Overall flow:

- What do we have now
- What could we have (with a little effort)
- Recommendations for the future

In the main sections, weave integrating threads:

- Shift left
- Cyber system security assurance case

1. **Introduction** (1/2 Page)
   [Why are we writing this paper?]

2. **Background** (1 1/2 Page)
   [Context and prior work external to the committee]

3. **Prior Work** (3/4 page)
   [Prior work by this committee that provides input to this paper]

4. **Mission Thread Analysis** (2 ½ pages)
   [What is important?]

Resilient & Trusted Cyber Systems Security Metrics & Measures Framework

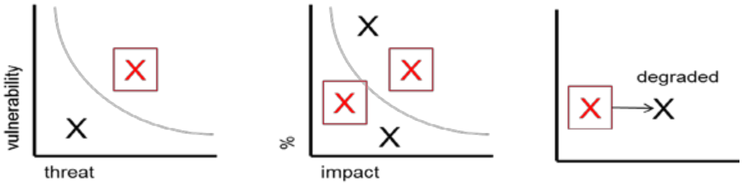
5. **Kpp – System Survivability in the Cyber Contested Environment** (1 ½ pages)
   [What really matters?]

6. **Cyber System Resilience for Mission Assurance** (1 pages)
   [How can we build it in instead of testing it out?]

7. **System Security Risk Metrics & Measures** (1 page)
   [What is the risk? What can we afford to mitigate?]

8. **System Security Assurance Case Model** (1 page)
   [Evidence based evaluation – How am I doing against the plan?]

9. **Bringing it all together. Dunlap Framework** (1 page)
   [What can we afford to mitigate?]



10. **Appendix**
    Taxonomy, Definitions, Ontology Semantics, Mapping of relationships
    Key relevant policies, standards, references, etc.