NDIA Systems Engineering Division

NDIA System Security Engineering Committee

June 2019

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

Cory Ocker
Raytheon
NDIA SSE Committee Co-Chair
Cory.Ocker@Raytheon.com
• Summary of the Committee Status & Accomplishments April – June
• Highlight Key Projects & Engagements
• Review Agenda for Today’s SSE Committee Meeting
• Verbal Sneak Peek - Potential New SSE Committee Project
• IEEE NDIA INCOSE System Security Symposium 2020 Status Update
SSE Committee April – June Summary

• Critical Program Information (CPI) Assessment & Identification Guide Workshop 6/5/2019
  – NDIA SSE Committee & Raytheon Co-sponsored the Draft CPI Assessment and Identification Guide
  – Authorship included government and industry participation with Ninja Donatelli, Raytheon, as the principal author.
  – Approximately 45 attendees.

• AF SSE Acquisition Guidance v 1.4
  – Delivered final review and comments to key AF leadership
    - Mr. Daniel Holtzman, Mr. William Mejias, Mr. Ken Barker, and Mr. Nick Shouse
  – Top 5 List of Concerns and 3 Positive Highlights.
  – Detailed comments using the comment resolution matrix (CRM).
  – NDIA SSE Committee in collaboration with the AF Cybersecurity Industry Technical Advisory Group (CITAG) & NDIA Cyber Division.

• Cyber Secure & Resilient Approaches for Feature Based Variation Management
  - NDIA SSE Committee, INCOSE SSE Committee

• DoD Office of the CIO Cyber Workforce Management - Transition to DoD 8140

• NDIA Architecture Committee
  – Identified an SSE Committee member Paul Work, RTN, to engage with the Architecture Committee to contribute to a whitepaper for Modular Open System Architecture (MOSA)
Project Description: The team will evaluate potential techniques to work systems security into the product line design so that the results of the systems security implementation can be used by all the receiving programs that use the product line assets. The team will explore existing PLE and SSE efforts related to architecture and patterns.

<table>
<thead>
<tr>
<th>Name</th>
<th>Affiliation</th>
<th>Email Address</th>
<th>SSE</th>
<th>PLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beth Wilson</td>
<td>Retired</td>
<td><a href="mailto:beth.wilson@aaai.com">beth.wilson@aaai.com</a></td>
<td>INCOSE</td>
<td>INCOSE</td>
</tr>
<tr>
<td>Bobbi Young</td>
<td>Raytheon</td>
<td><a href="mailto:bobbi.young@raytheon.com">bobbi.young@raytheon.com</a></td>
<td></td>
<td>INCOSE</td>
</tr>
<tr>
<td>Suzanne Hassell</td>
<td>Raytheon</td>
<td><a href="mailto:shassell@raytheon.com">shassell@raytheon.com</a></td>
<td></td>
<td>NDIA</td>
</tr>
<tr>
<td>Nate Simcic</td>
<td>Honeywell</td>
<td><a href="mailto:nathan.simpson@honeywell.com">nathan.simpson@honeywell.com</a></td>
<td></td>
<td>SSE</td>
</tr>
<tr>
<td>Rick Dova</td>
<td>Paradigm Shift International</td>
<td><a href="mailto:dova@paradigmshift.com">dova@paradigmshift.com</a></td>
<td></td>
<td>INCOSE</td>
</tr>
<tr>
<td>Gery Orsada</td>
<td>Lockheed Martin Aero</td>
<td>gery;<a href="mailto:orsada@imce.com">orsada@imce.com</a></td>
<td></td>
<td>NDIA</td>
</tr>
<tr>
<td>Christopher Giudica</td>
<td>Honeywell</td>
<td><a href="mailto:christopher.giudica@honeywell.com">christopher.giudica@honeywell.com</a></td>
<td>INCOSE</td>
<td></td>
</tr>
<tr>
<td>Jim Troff</td>
<td>Raytheon</td>
<td><a href="mailto:James.K.Troff@raytheon.com">James.K.Troff@raytheon.com</a></td>
<td></td>
<td>INCOSE</td>
</tr>
<tr>
<td>Deb Thomas</td>
<td>Raytheon</td>
<td><a href="mailto:Deborah.R.Thomas@raytheon.com">Deborah.R.Thomas@raytheon.com</a></td>
<td></td>
<td>SSE</td>
</tr>
<tr>
<td>Matt Hause</td>
<td>PTC</td>
<td><a href="mailto:mhause@ptc.com">mhause@ptc.com</a></td>
<td>INCOSE</td>
<td>INCOSE</td>
</tr>
<tr>
<td>Ly Vessels</td>
<td>Honeywell</td>
<td><a href="mailto:ly.vessels@honeywell.com">ly.vessels@honeywell.com</a></td>
<td></td>
<td>SSE</td>
</tr>
<tr>
<td>Brian Haan</td>
<td>SAIC</td>
<td><a href="mailto:Brian.haan@saic.com">Brian.haan@saic.com</a></td>
<td></td>
<td>INCOSE</td>
</tr>
</tbody>
</table>

- **Project Objective:** Bring systems security into product line design
  - **Goal:** Identify techniques for implementing systems line design
  - **Goal:** Identify patterns for product line architectures that address systems security
  - **Goal:** Identify variation management approaches for secure and resilient product line assets

- **Progress to Date**
  - Literature search continuing on existing techniques
  - Identified concerns to address in project aligned with goals
  - Identified tasks to apply to notional examples
  - Identified Search and Rescue sample problem and Connected Automobile as notional examples
  - Identify areas in notional examples to characterize with product line variations
  - Identify mission threads in notional examples
  - Developed notional example model to apply techniques

- **Planned Effort**
  - Apply CRAFT and Cyber Resiliency Wheel to Interim SE Products
  - Develop examples showing security application inside product line/variation point
  - Develop examples showing security should be applied outside product line/variation point
  - Relate SSE in PLE to design and testing activities
  - Identify potential SSE in PLE Patterns
  - Develop guidelines for implementing techniques

- **Planned Deliverables**
  - INCOSE INSIGHT Theme Issue Q2 2020
  - Paper(s) at NDIA/INCOSE conference April 2020
  - INCOSE webinar
SSE in PLE
Project Goals and Objectives

Project Vision: Bring systems security into product line design

• **Goal #1**: Identify/develop techniques for implementing systems security as part of product line design
  – Objective 1.1: SSE/PLE techniques aligned with security standards
  – Objective 1.2: SSE/PLE techniques aligned with business sectors
  – Objective 1.3: SSE/PLE techniques to develop secure and resilient product line assets
  – Objective 1.4: SSE/PLE techniques to perform meaningful security assessment of PL assets
  – Objective 1.5: Guidance for implementing SSE/PLE techniques

• **Goal #2**: Identify/develop patterns for product line architectures that addresses systems security
  – Objective 2.1: Security patterns for product line development representing standard solutions
  – Objective 2.2: Notional examples where SSE is best implemented inside PL
  – Objective 2.3: Notional examples where SSE is best implemented in deployed solution
  – Objective 2.4: Guidance for implementing SSE/PLE patterns

• **Goal #3**: Identify/develop variation management approaches for secure and resilient product line assets
  – Objective 3.1: Requirements approaches for SSE flow-down from PL to solutions
  – Objective 3.2: SSE variation management approaches for PL assets
  – Objective 3.3: Test approaches for PL and deployed solution verification (no gaps, no duplicates)
  – Objective 3.4: Systems security techniques for continuous monitoring of deployed solution
  – Objective 3.5: Guidance for implementing SSE/PLE design approaches
  – Objective 3.6: Communication plan (initial and ongoing) to joint SSE/PLE community
Engaged with DoD CIO Team Cyber Workforce Management

Transitioning to 8140
Office of the DoD CIO provided an update.

ON BEHALF OF THE DEPARTMENT, THE DO verschied CIO LED THE DEVELOPMENT OF THE DCWF TO ESTABLISH A STANDARD LEXICON FOR CYBER WORK

- The DCWF is based on the:
  - National Initiative for Cybersecurity Education (NICE) Workforce Framework
  - Joint Cybersecurity Training & Certification Standards (JCTCS)
- The DCWF includes work role descriptions, as well as, baseline tasks, knowledge, skills, and abilities (KSAs) by work role
- The DCWF has been adopted at the national level in NIST Special Publication 800-181, and was used to develop an international workforce framework under the North Atlantic Treaty Organization (NATO) Multinational Cyber Defense Training and Education Project

The DCWF contains 54 work roles divided between 32 specialty areas which are organized within 7 distinct categories

Trends and key challenges impacting cyber workforce:
- **Inconsistent Lexicon**
  - White spaces have been made, the language used to discuss cyber work and skill requirements is inconsistent. This hinders the nation’s ability to assess capabilities, identify skill gaps, and prepare the pipeline of future cyber talent
- **Lack of Cybersecurity Professionals**
  - A recent report by the Partnership for Public Service states, “There is a notable shortage of highly qualified cybersecurity experts, and this government has fallen behind in the race for this talent
- **Disjointed Professional Development**
  - There is a lack of clearly defined roles and career paths for cyber work. Efforts to establish accreditation standards for cyber curricula and certifications have been inconsistent
- **Cybersecurity Viewed as Separate Function**
  - There is often a perception that cybersecurity is a standalone function performed by specific cybersecurity professionals. As a result, cybersecurity is not recognized by many in the broader cyber workforce as being a part of their own daily work.
System Security Engineering Committee Meeting Agenda
6/6/2019 2:00 PM – 5:00 PM EST,
Location: Lockheed Martin Global Vision Center, 22202 Crystal Dr, Arlington, VA
Call in information: (877)336-1275 Access Code: 3019886

Agenda:
• Opening Remarks NDIA SSE Committee Chair, Holly Dunlap
• Update from ASD(R&E) on Engineering Cyber Resilient Weapon Systems activities (Melinda Reed)
• DFARS 7012 Non-attribution Engineering Focused Discussion (please bring your experiences, concerns, lessons learned)
  – Approach
  – Identification of CDI
  – Reducing Risk
  – Return On Investment
• Service Update (Air Force / Navy)
• Out brief from Critical Program Information (CPI) Workshop – Ninja Donatelli
• System Security Symposium 2020
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.

### SUBMISSION DETAILS

#### Theory & Methods
Papers or Extended Abstracts addressing novel ideas, theoretical issues, technology, methodology, or detailed studies. These academic-oriented papers will be peer reviewed and prioritized according to their contribution.

#### Cases & Practical Experiences
Papers presenting practical ideas, lessons learned, and real-world achievements. Papers are reviewed for relevance but not necessarily academic contribution.

Papers and extended abstracts of both categories will be peer reviewed. Papers will be published in the proceedings with an 8-page maximum. Extended abstracts (typically 3–5 pages) will not be published, but will be available to the conference attendees. Student papers are encouraged in both categories.

All submission details are available on the IEEE-INCOSE-NDIA SSS 2020 Submission Portal at [https://2020.ieeesystemssecuritysymposium.org](https://2020.ieeesystemssecuritysymposium.org)
IEEE NDIA INCOSE
System Security Symposium
April 6-9, 2020
http://www.ieeesystemssecuritysymposium.org

Key Dates

- Special Sessions & Tutorial Proposals Deadline: Wed, Jul 31st, 2019
- Initial Deadline: Fri, Aug 30th, 2019
- Acceptance Notification & Feedback to Authors: Thu, Oct 31st, 2019
- Final Draft Paper Deadline: Wed, Jan 15th, 2020

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

General Chair
Bob Rassa
IEEE Systems Council
RCRassa@Raytheon.com

Technical Program Chair
Holly Dunlap
NDIA
Holly.Dunlap@raytheon.com

Technical Program Co-Chair
Beth Wilson
INCOSE
wilsondrbeth@aol.com

Technical Program Committee:
Steve Holt
IEEE Systems Council
smdholt@gmail.com

Kathleen Kramer
IEEE Aerospace & Electronic Systems Society
kramer@sandiego.edu

Tom McDermott
Systems Engineering Research Center
tmcdermo@stevens.edu

Melinda Reed
OUSD (R&E)
melinda.k.reed4.civ@mail.mil

Logan Mailloux
United States Air Force
Logan.mailloux@us.af.mil

For Information Contact:
Shelby Lussier
slussier@conferencecatalysts.com

Location
Marriott Crystal Gateway
Crystal City, VA, USA

SUBMISSION DEADLINES
July 31, 2019
Special Sessions & Tutorial Proposals
August 30, 2019
Initial Manuscript & Abstract Deadline
October 31, 2019
Acceptance Notification