INCOSE System Security Engineering Working Group Charter

1 PURPOSE

Data breach cases and industrial control system incidents call attention to the inadequacy of current approaches to systems security. Each case presents more compelling evidence of the economic impact of cybersecurity threats. Each case adds to the recognition that security cannot be assumed to be provided by existing standards. Vast sums of money are increasingly directed toward systems security solutions; yet the losses due to security breaches continue to rise.

Holistic system views of verification and validation is the forte of the systems engineer. However, when it comes to cybersecurity, systems engineers typically cede the responsibility to the security profession.

One reason that this situation is prevalent is that systems engineers have not considered it a problem. Systems engineers are taught to divide system requirements into two partitions: functional and non-functional requirements, or capabilities and characteristics. Capabilities always take precedence over characteristics, and security is classified as a characteristic [1]. One otherwise scholarly and astute textbook [2] on systems engineering refers to security as "related to system attributes that enable it to comply with regulations and standards." It is far easier to blame security standards bodies for the outcome of a poor security design than to take responsibility for "building security in [3}." Where security is directly addressed in systems engineering literature, it is circularly defined as a process to ensure security concerns are covered, rather than as a core system requirement [4].

As security practitioners search for workable solutions to the ever-more-complex maze of criminal, nation-state, and terrorist threats they encounter, the trend should be to escape from best practices checklists and return to core systems engineering methods, processes, and tools. However, most security engineers have no experience with these methodologies, and these methodologies have traditionally obscured security requirements. As long as systems engineers do not consider security a functional requirement, it will not be likely to rise to the top of the implementation checklist, because processes for managing system development lifecycles prioritize functional requirements over nonfunctional requirements. The situation is that security practitioners are not being engaged at the design stage, and new approaches to systems engineering will be needed to meet the growing need for secure systems.

This working group (WG) believes that system engineering cannot succeed without accepting core responsibility for enabling and facilitating effective system security – partly in system requirements, partly in system trade space recognition, but mainly in system thinking applied to concepts of operations and systems architecture. Sustaining system functionality in the face of intelligent determined attack requires self-preservation capabilities that adapt and evolve with intelligence, proactive innovation, and strength of community equal to the adversary as a minimum. This requires full system awareness and adaptability, and system-of-system relationships. Security engineering alone cannot accomplish this.

It is both fitting and necessary for INCOSE to assume leadership within the systems engineering community to tackle the evolving needs of systems security, as security engineering is a sub-discipline of SE and the issues are leading edge systems engineering issues: architecture, systems of systems, self-organizing systems, security tradeoffs with human factors, systems thinking – things that are typically high level integrated-system SE issues.

2 GOALS

- Goal: Establish and foster the responsibility for security within Systems Engineering, with effective system security accepted and practiced as a fundamental part of system engineering.
- Goal: Establish and foster self-sustaining cross- community involvement between systems engineers, security engineers, and system security standards.
- Goal: Establish and foster systems engineering guidance for enabling effective systems security in the face of evolving system security needs.
- Goal: Attract an international cadre of engaged participants to broaden the understandings and effectively deal with multi national interests and differences.
- Customer(s)/Stakeholder(s): Systems engineering educators, systems engineering process and standards developers, defense systems engineering acquisition procedure developers, systems engineering leaders and managers, customers of systems that require effective security, systems engineers, and security engineers.

3 SCOPE

This WG will address and foster system engineering design concepts, processes, enabling-support (such as standards and certifications), and community understanding and acceptance of the roles that systems engineering must play in enabling effective systems security in the face of evolving systems complexity and systems security threat.

4 SKILLS AND EXPERTISE REQUIRED

Skills and expertise in cyber security, physical security, control-system security, system engineering processes, systems architecture, complex adaptive systems, systems of systems, self-organizing systems, natural systems, human and organizational behavior, value propositioning, and cross-community collaboration are essential to be successful. Most important, however, is an engaged sense of mission, which is neither a skill nor an expertise, but rather an internal drive that shapes the acquisition and application of skill and expertise. This WG will pursue a phased approach to laying groundwork and developing a participation infrastructure that attracts participants with the breadth of necessary skills and expertise to achieve the goals.

5 MEMBERS, ROLES AND RESPONSIBILITIES

Names of key members and their responsibilities.

- Chair: Rick Dove
  - The Chair shall build consensus among the engaged membership as to appropriate goals and strategies for satisfying the purpose of the WG, and be responsible either directly or through delegation for acquiring and applying necessary resources to execute strategies in pursuit of goals.
  - The Chair shall initiate and lead at least one project at all times that supports the achievement of one or more WG goals.
  - The Chair shall be responsible for status reporting to designated INCOSE Technical Operations personnel.
  - The Chair shall keep the WG membership participation page current for scheduled events, progress, work in process, and relevant supporting documents.
- Co-chairs: Beth Wilson and Ken Kepchar

  - Co-chairs shall assist in the consensus building among the engaged membership as to goals and projects.
  - Co-chairs shall be responsible to act in the absence of the Chair.
  - Co-chair shall initiate and lead at least one project at all times in support of one or more WG goals.
- Chair and Cochair serve at the pleasure of the engaged membership and INCOSE Technical Operations.
- Engaged Membership:
  - Actively engaged in at least one project as lead or participant.
  - Participates in person or remotely in at least one of the two regular workshops each year.
- Membership:
  - Names carried on the membership list at their request, entitling them to activity announcements, access to WG websites, workshop synopses, and documents of work-in-process and finished work.

6 OUTCOMES (PRODUCTS/SERVICES)

- Outcome: Fundamental responsibility accepted within systems engineering for effective security practices established by SE processes and standards.
- Product Category: Systems engineering guidance on needs, roles, and methods that enable effective system security in an evolving threat environment.
- Product Category: Effective security process integration with system engineering processes.
- Product Category: System security standards compatible with systems engineering standards, with both encouraged to keep effective pace with evolving system security and systems engineering realities.

7 APPROACH

The general approach that will guide this WG/Initiative includes:

- The WG shall meet in working sessions during IW and IS sessions each year as a minimum, to advance project work-in-process and consider new projects. Remote attendance and interaction shall be used to allow participation for those unable to attend sessions in person.
- Prime methods for raising awareness and displaying progress toward goals will include papers written for relevant conferences and publication outlets, panel sessions at INCOSE and other appropriate conferences, and essays for INCOSE INSIGHT.
- Decision making will be done by engaged WG members toward achievement of the recognized goals of the WG, with the requirement that leadership for decision achievement is accepted and active. Decisions will be made twice yearly during IW and IS sessions as appropriate.

8 MEASURES OF SUCCESS

Overall measures of success for the WG include:

- The WG goals are mission oriented in a systems and security engineering environment not yet broadly aligned with the goals. The prime measure of initial success will be recognition of security responsibility evidenced in appropriate changes to established system engineering processes.
- Active projects toward recognized WG goals is one indicative measure of success, with quality of active projects taking precedence over quantity.

- Quantity of "project engaged" membership is another indicative measure of success, with continual progress on each project being the measure of an acceptable number of engaged members.

9 RESOURCE REQUIREMENTS

This WG will assess budget requirements yearly and submit budget requests to INCOSE Technical Operations as deemed appropriate to achieve goals. Effective enabling and facilitating Infrastructure support from INCOSE for WG activity is an ongoing requirement. Human resources outside of INCOSE are anticipated as requirements, and methods for identifying and obtaining such resources will be identified as needs arise.

10 DURATION

This Charter will remain in effect until rescinded by the signatory, the signatory's successor as WG Lead, or INCOSE Technical Operations.

11 SIGNATURES

Enter the signature block of the submitter Date: 26-Aug-2016

1st Level of Approval

Technical Director, INCOSE Date: 6 Sep 2016

2nd Level of Approval (Note this will be added by the INCOSE Technical Director when deemed appropriate.)

Chairman, INCOSE Board of Directors Date

References:

1. Buede, D.M., *The Engineering Design of Systems, Models and Methods*. 2009: Wiley.

2. Larson, W., et al., *Applied Space Systems Engineering*. 2009: McGraw Hill.

3. A phrase that, largely due to the community behind the site: https://buildsecurityin.us-cert.gov/bsi/home.html, has become synonomous with software security, but it is used here to refer holistically to any system of interest.

4. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), *Information technology — Systems Security Engineering — Capability Maturity Model (SSE-CMM, ISO/IEC 28127)*. 2002.

Revision History

Date	Revision	Description	Author
22 Nov 2010	1.0	Initial Draft.	Rick Dove and Jennifer Bayuk
28 Sep 2012	2.0	New Co-chairs	Rick Dove
26 Aug 2016	3.0	Revised draft and new co-chair	Rick Dove, Beth Wilson, Ken Kepchar