Something Wicked
This Way Comes …

SE Responsibility for System Security

INCOSE Enchantment Chapter
12 September 2012
Rick Dove
Abstract: Something momentous is happening: INCOSE recognition that system security is the responsibility of Systems Engineering is acknowledged – the next version of the Handbook will make this clear in its mid-2013 publication. That is simply a door opened – now the real work begins. What will the Handbook say? How will the responsibility be socialized, accepted, and deployed? How is effective System Engineering and Security Engineering engagement characterized? How will the SEBoK (Systems Engineering Body of Knowledge) support this responsibility? This presentation will review work in planning and process, including the logic and nature of SE responsibility; text to be distributed throughout the Handbook; a new System Security Engineering section 9.16; a call for INSIGHT 2013Q2 essays themed: The Buck Stops Here; a multi-session security track at IS13 call for papers; the NSA/NIST Systems Security Engineering document-in-process; the DoD Program Protection Plan; the IEEE Smart Grid Vision Project cyber-security work-in-process; and a formative-stage INCOSE Agile Systems Engineering working group with implications for systems security. Invitations for involvement are open.
“A wicked problem is a social or cultural problem that is difficult or impossible to solve for as many as four reasons:

- incomplete or contradictory knowledge,
- the number of people and opinions involved,
- the large economic burden, and
- the interconnected nature of these problems with other problems.

www.ssireview.org/articles/entry/wicked_problems_problems_worth_solving
Fu's software radio was capable of completely reprogramming a patient's ICD in his or her body.

... able to instruct the device not to respond to a cardiac event...

...and tell the defibrillator to initiate its test sequence--delivering 700 volts to the heart ...

...whenever they wanted.
Is Smart Grid security a WG project candidate?

Rick was asked to write up a Future-Technology Topic on Patterns of Self-Organizing Security.

Choi+Shine, www.wired.co.uk/news/archive/2010-08/16/human-pylons
Making semiconductors is a big business—and so is counterfeiting them.

In 2011, over 1300 counterfeit incidents were reported from around the world. That's more than quadruple the number reported in 2009.

The fear is that these counterfeits—including components falsely labeled as military grade—will fail more quickly than the parts they're standing in for.

The National Defense Authorization Act for Fiscal Year 2012 [PDF], aims to fight counterfeiting by requiring government contractors to track and report counterfeits and to be held accountable for replacement costs.
Sustainable System Security – a Critical System Engineering Responsibility

Systems are engineered with expectations: to provide services or carry out missions that justify the development, production, and sustainment investments. This return on investment (ROI) occurs over time. In some cases an ROI might occur with one successful mission; but more often a period of many years is required. Value fails to occur if system life or system ability to carry out its mission during that life is less than required. System lifetime, protection of critical system information, and critical assets that may be protected by a system, are under threat by competitive entities, as well as by unanticipated situational events. System security is the property that guards against and counters these threats – a purposefully engineered property that only emerges successfully from thoughtful system engineering.

Emerging technology is a double-edged sword. Modern technology is both the enabler of remarkable system capability and a source of constantly-evolving adversarial attack. Increasing use, knowledge, and complexity of digital data, control systems, and communication networks compel both new system capability and new vectors for system compromise.

Within the systems engineering taxonomy, security is classified as a specialty engineering activity. To be sure, very special knowledge, experience, and practice are necessary in system security engineering; especially when systems of all kinds are targets for intelligent, resourceful adversaries intent on system compromise. Security engineering is engaged to make a system secure, but when allocated to a separate specialty activity, this engagement is constrained by the nature of an already defined and often implemented system, or limited to ensuring that called-for standards and regulations are met. Constrained evolution of existing systems and characterization as a compliance activity both hamstring the ability of security engineering to accept and dispatch system security responsibility.

Fielding sustainably secure systems today is critical to enterprise needs, yet difficult when system security is less than a paramount thoughtful concern of the system engineering processes. Responsibility lies with both acquirer and supplier.
Responsibility/Accountability

Code of Hammurabi (2200 BC)  
King of Babylonia  
Translated by R.F. Harper

If a builder builds a house for a man and do not make its construction firm and the house which he has built collapse and cause the death of the owner of house – the builder shall be put to death.

If it cause the death of the son of the owner of the house – they shall put to death a son of that builder.

If it destroy property, he shall restore whatever it destroyed, and because he did not make the house which he built firm and it collapsed, he shall rebuild the house which collapsed at his own expense.

Common Law in England (15th Century)

If a carpenter undertakes to build a house and does it ill (not well), an action will lie against him

Napoleonic Code (1804)

If there is a loss in serviceability in a constructed project within 10 years of its completion because of a foundation failure or from poor workmanship, the contractor and architect will be sent to prison

Forensic Engineering, D. Fowler (slide presentation has been removed from the Internet)
SSE-WG Charter: Purpose

PURPOSE

This working group 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 equal intelligence, determination, and strength of community. This requires full system awareness and adaptability, and system-of-system relationships. Security engineering alone cannot accomplish this.

It is fitting for INCOSE to tackle Next Generation Security, as 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.
SSE-WG Charter: Goals and Scope

GOALS

Goal: Establish the responsibility for security within Systems Engineering, with effective system security accepted and practiced as a fundamental goal of system engineering.

Goal: Instigate self-sustaining cross-community involvement between systems engineering, security engineering, and system security standards.

Goal: Establish exemplar profiles of self organizing system-of-system concepts for next generation security.

Customer(s)/Stakeholder(s): Systems engineering educators, systems engineering process and standards developers, DoD systems engineering acquisition requirements developers, systems engineering leaders and managers, customers of systems that require effective security.

SCOPE

This WG will address and foster system design concepts, system engineering processes, enabling support (such as standards), and community understanding and acceptance; all relative specifically to next generation system security characterized principally as self organizing, adaptive, resilient, evolutionary, proactive, and harmonious – in at least equal effectiveness as the system-adversarial communities.
OUTCOMES (PRODUCTS/SERVICES)

Outcome: Fundamental responsibility accepted within systems engineering for effective security established in SE processes and standards.


Product: Next generation security process integrated with system engineering processes. Mid term deliverable.

Security WG Workshop – 23Jan2012 Agenda

08:00 Rick Dove – Introductions and opening general discussions
09:00 Paul Popick – Topic brainstorming

Current Topic Discussions and Concepts
10:00 Beth Wilson, Intro to Topic discussions and general project preparation and work-in-process
11:00 Kristen Baldwin & Paul Popick: Criticality Analysis
12:00 Lunch
13:15 Greg Sweeney: Embedded Systems
13:45 Ken Kepchar: Security Architecture and Security Risk Analysis
14:15 Rick Dove: Thoughts on 2013 INSIGHT essays and IS13 papers for SE/HB compatibility
14:45 Break

Organizational discussion sessions on the nature and structure of the project:
15:00 Kevin Forsberg: INCOSE processes, requirements and guidance for Handbook additions
15:30 Rick Dove: Preliminary planning for Handbook 2012 wiki interaction and consideration for INSIGHT Q2 2013 and IS13 papers
16:30 Standards, Johann Amsenga, Chair South African National Committee on Security Standards and Delegate to SC27
  - Introduction to ISO and the development of International Standards
  - Introduction to SC 27, the ISO committee responsible for Information security standards
17:00 Adjourn

External links to relevant materials
## 35 Attendees 23Jan2012

| 1. Johann Amsenga           | Eclipse RDC                  | amsenga@gmail.com          |
| 2. Kristen Baldwin          | DoD OSD DASD/SE              | dove@parshift.com          |
| 3. Rick Dove                | Paradigm Shift International | cheryl.garrison@ngc.com    |
| 4. Cheryl Garrison          | Northrop Grumman             | evelyn.hirt@pnl.gov        |
| 5. Evelyn Hirt              | Battelle at PNNL             | eagleview2@cox.net        |
| 6. Ken Kepchar              | EagleView Associates, Retired FAA | oskar.j.leon@lmco.com |
| 7. Oscar Leon               | Lockheed Martin              | ron.lyells@honeywell.com   |
| 8. Ron Lyells               | Honeywell                    | smackeen@earthlink.net     |
| 9. Susan MacKeen            | TASC                         | popa.pick ctr@osd.mil      |
| 10. Paul Popick             | DoD OSD DASD/SE & Aerospace Corp | fsalvatore@drc.com       |
| 11. Frank Salvatore         | DRC                          | john.snoderly@dau.mil      |
| 12. John Snoderly           | Defense Acquisition University | rswarz@mitre.org         |
| 13. Bob Swartz              | Mitre                        | sjsutton.243@comcast.net   |
| 14. Stephen Sutton          | U. of Maryland, Retired TASC | tenoriot@gmail.com        |
| 15. Thomas Tenorio          | White Sands Missile Range & NCI/ATA | dr.leon.turner@gmail.com |
| 16. Leon Turner             | Rockwell Collins             | marsha.v.weiskopf@aero.org |
| 17. Marsha Weiskopf         | Aerospace Corp               | kenneth.williams@incose.org |
| 18. Kent Williams           | Booz Allen Hamilton          | beth_j_wilson@raytheon.com |
| 19. Beth Wilson             | Raytheon                     | jwynn@mitre.org           |
| 20. Jackson Wynn            | Mitre                        |                           |

### Live Meeting Attendees

| 21. Paulo Barroso           | Raytheon                     | paulo.barroso@raytheon.com |
| 22. Art Hollows             | Raytheon                     | Art_L_Hollows@raytheon.com |
| 23. Jonathan Goodnight      | DoD OSD DASD/SE              | jonathan.goodnight.ctr@osd.mil |
| 24. Neil Greenfield         | AEP                          | nggreenfield@aep.com       |
| 25. Randy Herbert           | Raytheon                     | randy_herbert@raytheon.com |
| 26. Tom Jones               | Raytheon                     | tom_tj_jones@raytheon.com  |
| 27. Kenneth Lubel           | Raytheon                     | Kenneth_S_Lubel@Raytheon.com |
| 28. Joseph Merkling         | Raytheon                     | joseph.merkling@gmail.com  |
| 29. Jeanette Moody          | Raytheon                     | Jeanette_Moody@Raytheon.com |
| 30. John Molloy             | Raytheon                     | john_molloy@raytheon.com   |
| 31. Chris Sargent           | Sikorsky                     | csargent@sikorsky.com      |
| 32. Phillip Smith           | Raytheon                     | phillip_r_smith@raytheon.com |
| 33. Greg Sweeney            | Sikorsky                     | gsweeney@sikorsky.com      |
| 34. Shirley Tseng           | Tseng                        | shirley_tseng@earthlink.net |
| 35. Ruben Urcuyo            | Raytheon                     | Ruben_Urcuyo@raytheon.com  |
Table of Contents

1 Systems Engineering Handbook Scope
   1.1 Purpose
   1.2 Application
   1.3 Contents
   1.4 Format
   1.5 Definitions of Frequently Used Terms
   1.6 References

2 Systems Engineering Overview
   2.1 Introduction
   2.2 Definition of Systems Engineering
   2.3 Origins of Systems Engineering
   2.4 The Hierarchy Within A System
   2.5 Systems of Systems
   2.6 Use of Systems Engineering
   2.7 Value of Systems Engineering
   2.8 An Allegorical Tale
   2.9 References

3 Generic Life-Cycle Stages
   3.1 Introduction
   3.2 Life Cycle Characteristics
   3.3 Life-Cycle Stages
   3.4 Life Cycle Approaches
   3.5 What is Best for Your Organization
   3.6 Introduction to Three Case Studies
   3.7 References
4 Technical Processes
4.1 Stakeholder Req. Def. Process
4.2 Requirements Analysis Process
4.3 Architectural Design Process
4.4 Implementation Process
4.5 Integration Process
4.6 Verification Process
4.7 Transition Process
4.8 Validation Process
4.9 Operation Process
4.10 Maintenance Process
4.11 Disposal Process
4.12 Cross-Cutting Technical Methods

5 Project Processes
5.1 Project Planning Process
5.2 Project Assessment & Control Process
5.3 Decision Management Process
5.4 Risk Management Process
5.5 Configuration Management Process
5.6 Information Management Process
5.7 Measurement Process

6 Agreement Process
6.1 Acquisition Process
6.2 Supply Process

7 Organizational Project-Enabling Processes
7.1 Life Cycle Model Management Process
7.2 Infrastructure Management Process
7.3 Project Portfolio Management Process
7.4 Human Resource Management Process
7.5 Quality Management Process
8 Tailoring Processes
8.1 Tailoring Process

9 Specialty Engineering Activities
9.1 Design for Acquisition Logistics – Integrated Logistics Support
9.2 Cost-Effectiveness Analysis
9.3 Electromagnetic Compatibility Analysis
9.4 Environmental Impact Analysis
9.5 Interoperability Analysis
9.6 Life-Cycle Cost Analysis
9.7 Manufacturing and Producibility Analysis
9.8 Mass Properties Engineering Analysis
9.9 Safety & Health Hazard Analysis
9.10 Sustainment Engineering Analysis
9.11 Training Needs Analysis
9.12 Usability Analysis/Human Systems Integration
9.13 Value Engineering

Appendix
A: System Life-Cycle Process N2 Chart
B: System Life-Cycle Process Mappings
C: Acronym List
D: Terms and Definitions
E: Acknowledgement
F: Comment Form

Security is missing!
Information security generally refers to the confidentiality, integrity, and availability of the information assets.

Information security management includes the controls used to achieve information security and is accomplished by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures, and software.

Information Security Management System is the life-cycle approach to implementing, maintaining, and improving the interrelated set of policies, controls, and procedures that ensure the security of an organization's information assets in a manner appropriate for its strategic objectives.

9.1.2.6 System Security Analysis
System Security Analysis identifies and evaluates system vulnerabilities to known or postulated security threats and recommends means to eliminate the vulnerabilities or to at least reduce the susceptibility to compromise, damage, or destruction to an acceptable level of risk.
Discussion: Barriers to Effective Systems Security

- Systems Engineers (SEs) don’t know when to ask for system security engineering (SSE)
- SSE focused on checklist
- System security not part of trade space (CONOPS, architecture, strategies)
- Security not considered part of SE by some (SE Journal rejected article as irrelevant to SEs)

Result: Handbook Project

- Focus: “What is the essential knowledge that a SE must have in order to intelligently engage their system security expert?”
- Goal: Make system security an attribute of a well-designed system
Process for Handbook Additions (Kevin Forsberg)
- Handbook effort is part of Knowledge Management working group
- Looking at next generation of the SE Handbook (3.3), current version is 3.2.2
  - Review draft outline end of February/early March
  - Provide annotated outline in June
  - Discuss outline at IS2012 for version 3.3
  - Need authors in fall 2012
  - Draft material to review at IW2013 (June/July)
  - Expect 3 year cycle before 3.4
  - Can provide common content to both SE Handbook and SEBoK, update SEBoK during time between SE Handbook version 3.3 and 3.4.
- Certification exam questions must tie to SE Handbook content
- SEBoK will be a moderated wiki
  - Future may have SEBoK be the SE Handbook (3.3 will be separate)
  - SEBoK governance will be joint INCOSE and IEEE
  - SE Handbook governance related to certification
- Systems Security can be integrated into existing and/or separate section
- Can provide common content to both SE Handbook and SEBoK, update SEBoK during time between SE Handbook version 3.3 and 3.4.

Work Products and Approach
- Immediate Handbook 3.3 Interaction
  - Steering committee: Rick Dove, Paul Popick, Beth Wilson
  - Investigate INCOSE Wiki capability
  - Publish wiki 3.3 outline engagement strategy:
    - Two iterations on 3.3 outline wiki and consolidation by IS12 (July 2012)
    - HB section authoring on approved outline activities completed by year end 2012

Surprise: Handbook Revision 3.3 Kicked Off at IW12
Handbook Project Positioning Info

The Handbook revision is a project of the Knowledge Management WG. Leads on the project are Gary Roedler and Kevin Forrester. Current version is 3.2, new 3.3 version is scheduled for Mid 2013 release – likely planned for availability at IS-2013.

“The [3.3] changes are driven by user feedback, planned changes for ISO/IEC/IEEE 15288, feedback from the SE Body of Knowledge (SEBoK) team, and input from the Knowledge Management Working Group (KMWG) during IW 2012.” [Garry Roedler]


“Version 3 of the INCOSE Systems Engineering Handbook represents a shift in paradigm toward global industry application consistent with the Systems Engineering Vision. Developed for the new systems engineer, the engineer in another discipline who needs to perform systems engineering or the experienced systems engineer who needs a convenient reference, the handbook provides an updated description of the key process activities performed by systems engineers.

“The descriptions in this handbook show what each systems engineering process activity entails, in the context of designing for affordability and performance. On some projects, a given activity may be performed very informally (e.g., on the back of an envelope, or in an engineer’s notebook); on other projects, very formally, with interim products under formal configuration control. This document is not intended to advocate any level of formality as necessary or appropriate in all situations.
Handbook Revision Planning

Kevin Forsberg, 27Jan2012:

We plan on two iterations of the outline before the July IS in Rome. The outline we first develop and release at the end of February will be a starting point to create an annotated outline, with inputs solicited from all Working Groups. What I expect back from the Working Groups in March/April is input to the evolving annotated outline, with a "mature" annotated outline to be distributed in mid-May, so we can have a review by and further input from the WG teams before IS 2012 in July.

I will create a schedule next week covering the February to July time frame...
System Security Engineering WG

Charter:
- to identify effective system security principles consistent with new reality
- to integrate responsibility for system security into the system engineering community

Chair/Co-Chair:
Rick Dove rick.dove@parshift.com
Jennifer Bayuk jennifer@bayuk.com

INCOSE Connect address:
https://connect.incose.org/tb/specialty/systemsecurity
INCOSE Web page:
http://www.incose.org/practice/techactivities/wg/template

Number of Members: ~50 on list

Published Products
- 2008 April INSIGHT Declaration of Responsibility
- 2011Q2 INSIGHT 11 Theme Essays: Systems of Systems and Self-Organizing Security

Work in Process & Planned
- SEBoK Review
- Next Gen Agile-SysSec Patterns
- Security responsibility integrated with Handbook processes/activities
- Security responsibility in CSEP

International Workshop
21 – 24 Jan 2012
Jacksonville, FL USA
2.5 Systems of Systems

“The following challenges all influence the development of systems of systems. (1-7 as is, add number 8): System security is especially complex, as system component interface relationships are rearranged and augmented asynchronously, and often involve COTS-components from a wide variety of sources. Security vulnerabilities may arise as emergent phenomenon from the total system-of-systems configuration even when individual system components are felt to be sufficiently secure in isolation.

2.6 Use of Systems Engineering

Suggestion to follow the paragraph pg 15 that starts “Another factor driving the need for SE is that the time..”:

A recent factor of growing consequence, driving the need for SE, is system security. Systems of all kinds have become targets of opportunity and value for human-directed malicious attacks - running the full range from highly sophisticated nation states to attack-tool enabled psychopaths and malcontents. The ubiquity of digital control systems and value in digital data systems provides a common base of digital-technology vulnerability. Security engineering as an afterthought or as standards compliance has proven to be critically inadequate. From relatively simple systems like medical-device pacemakers, through complex systems like health-care medical records, to systems-of-systems with asynchronous integration and COTS-device multiple-supplier employment - only the systems engineering holistic view can adequately assess and direct the necessary attention to system security.
3.6 Introduction to three case studies

Recommend changing Title to “Introduction to Selected Case Studies.” The SSE-WG would like to develop another case study related to system security.

[NEW 4.1] Mission or Business Analysis

In section 4.2.1.5 p76 in the entry that begins with “design considerations” add supply chain risk management to the e.g. after security requirements.

4.1 Stakeholder needs & requirements

Suggestion section 4.1.1.5 p 60 there is an entry that begins with “establish MOEs” – security should be added to the e.g. list just as safety, reliability, are on the list.

Suggestion section 4.1.1.5 p 60, to include in the list of “Common approaches and tips”: Develop a description of system security threats and the malicious threat community to provide common understanding across the effort and to validate the appropriateness of scenarios. A threat community description may cover the demographic group(s) to which a product will be vulnerable or the specific categories such as insiders and supply chain elements that will be included as purchased items.
4.2 Requirements engineering (definition) process

Suggestion 4.2.14 p 74 to explicitly call out system security as a functional requirement in the “System Functions” bullet item: System Functions – Defines the functions the system must perform, including sustainment of system functional capability and protection of system assets; and defines the functional boundaries for the system to be developed.

Suggestion 4.2.15 p 75: System Functions – Define the functions that the system is to perform. These functions should be kept implementation independent. For more information on approaches for defining and refining system functions see Section 4.12.2.

Suggestion 4.2.1.5 p 76 in the entry that begins with “design considerations” add supply chain risk management to the e.g. after security requirements.

Suggestion 4.2.2.1 p 77: Figure 4.5, External Environment might include a third bullet recognizing the system adversarial/malicious attack community.

Suggestion 4.2.2.4 p 83: 2nd paragraph might recognize security as an ongoing life-cycle requirement in addition to support, with an insertion in the paragraph as “Defining, deriving, and refining functional/performance requirements applies to the total system over its life cycle, including its security and support requirements.”
4.8 Validation Process

Suggestion: describe approaches to testing non functional requirements here including security testing approaches such as penetration testing and misuse or abuse scenarios for validation of security requirements.

Suggestion 4.8.1.2 Description p 135, add the word “security” after safety as shown: […] Validation criteria are selected based on the perceived risks, safety, security, and criticality.

4.10 Maintenance Process

Suggestion 4.10.1.4 Outputs p 144 Maintenance Strategy bullet, add current security effectiveness per: “Accounts for the system’s technical availability, current effectiveness of system security functionality, replacements for system elements and logistical support, maintenance personnel training and staff requirements.

Suggestion 4.10.1.5 p 145 Common approaches and tips, add a fourth bullet: The evolution of the system security attack community and its methods changes rapidly, and must therefore by constantly reevaluated for effectiveness and maintenance.
4.11 Disposal Process

Suggestion 4.11.1.5 Process Activities p 148 Plan Disposal, first bullet add protected assets element, per: “Review the Concept of Disposal, including protected assets that should be removed/destroyed, any hazardous materials and other environmental impacts to be encountered during disposal.

Suggestion 4.11.1.5 Process Activities p 148 Common approaches and tips, add removal/destruction element per: “Disposal analyses include consideration of costs, disposal sites, environmental impacts, health and safety issues, removal/destruction of protected assets, responsible agencies, handling and shipping, supporting items, and applicable federal, state, local, and host-nation regulations.

[NEW 4.16] Design for X

Suggest a reference to Information System Security (9.16) since info security considerations in design are cross-cutting.

5.4 Risk & Opportunity Management Process

Suggest section 5.4.1.5 on page 220 where FMECA is mentioned also include vulnerability analysis to that sentence.

Suggest inserting a reference to Information System Security here since the info security process essentially stems from risk.

6 Agreement Process

Suggest highlighting that security considerations must be extended to the processes used to develop and supply the system to prevent compromise of the system through malicious insertion or counterfeit parts.
9 Specialty Engineering Activities

Suggest reconsidering the word “Activities” in the title Specialty Engineering Activities. Perhaps this would be better left as Specialty Engineering without the word Activities.

[NEW 9.16] System Security Engineering Process

Recommend changing section title to Systems Security Engineering.

Recommended sub-sections (SSE-WG will provide content):

9.16.1 SSE Role in SE
9.16.2 SSE Activities for the Technical Processes
9.16.2.1 Stakeholder Requirements Definition and Analysis SSE Activities
9.16.2.2 Architecture Design SSE Activities
9.16.2.3 Verification / Validation SSE Activities
9.16.2.4 Maintenance and Disposal SSE Activities
9.16.3 SSE Activities for the Project Processes
9.16.3.1 Risk Management Process SSE Activities
9.16.3.2 Configuration Management Process SSE Activities
9.16.4 SSE Activities for the Agreement Processes
9.16.4.1 Acquisition and Supply Processes
9.16.5 References
System Security Engineering WG
IS12 Workshop Agenda
Tuesday July 10, 2012 – 14:00-18:00

14:00  Introductions and WG & workshop positioning, Rick Dove
14:45  Project: Handbook Security Revision – Status and next steps, Beth Wilson
15:00  Handbook Section 9.16 status and discussion, Paul Popick
15:45  Project: INSIGHT 2013Q2 Essays – Status and discussion, Rick Dove
16:15  Project: IS13 Security Track – status and discussion, Beth Wilson
16:45  Project: SEBoK needs Security Document References – discussion, Paul Popick
17:00  International involvement – let’s get some! what does it take? Mike Wilkinson
17:30  Closing wrap-up and other news, Rick Dove
18:00  Adjourn

Mailing Lists: opt in to rick.dove@parshift.com
   (includes non-INCOSE members)
   1) General Announcements (96 people)
   2) Handbook Project Ongoing Status (44 people)
WG Projects

Project 01: WG Mission – Manifesto Style
Project 03: Patterns of Agile Self-Organizing Security (Open)
Project 04: INSIGHT Essays Q2 2011: Sys-of-Sys & Self Organizing Security
Project 05: ITNG Conference Track March 2011: Six SE & Security Authors
Project 06: Handbook inclusion of SE Security Responsibility (Open)
Project 07: INSIGHT Essays Q2 2013: The Buck Stops Here (Open)
Project 08: IS13 Paper Track: SE & Security Engineering (Open)
Project 09: SEBoK Security Engineering Document References (Open)

Future Candidates? (will discuss in final session today – think about it):

- INCOSE Library Product: System Security Engineering for the SE.
- Standards Involvement.
- Smart Grid SE security.
- Collaborative project with new Agile Systems Engineering WG.
- Collaborative project with Autonomous Systems Test & Evaluation WG.
- What else should be considered?
INCOSE Systems Engineering Certification Based on SE Handbook
Open Author Needs and Opportunities: 4 Projects

1. SE Handbook
   - Insert security content (1-2 sentences)
   - New SSE Section 9.16 (2-3? Handbook pages)
   - Expect call for inputs Fall 2012

2. INCOSE Symposium 2013
   - Philadelphia, June 24-27, 2013
   - Security Track
   - 15 page max papers
   - Papers due early Nov 2012

3. SEBoK
   - Need References for Review at IW12

4. INSIGHT Issue 2013
   - 2,000 word essays
   - Sep 2012 Authors selected
   - Nov 2012 Draft essays
   - Jan 2013 Review essays at IW13
   - July 2013 Issue
Section 9.16
Preliminary Outline
Discussion
Systems Security Engineering (SSE) Working Group
SE Handbook update for SSE

Background

◆ Request from SE Handbook WG to add a SSE specialty section to Section 9 of the SE Handbook
◆ Current size of specialty sections range from a paragraph to 3 and a half pages
◆ SE Handbook is aligned with ISO 15288 processes

Approach

◆ Target SSE Section at about 4-6 pages (Ken Kepchar’s guess on allowance)
◆ Align with 15288 Processes
◆ Identify Technical, Project and Agreement Processes that are most significant to SSE implementation
◆ Submitted Draft Outline to SE Handbook Working Group by Mid December
9.16 System Security Engineering (SSE)

◆ 9.16.1 Systems Engineer and Systems Security Engineer Roles and Responsibilities for SSE

◆ 9.16.2 SSE Activities for the Technical Processes
  ➢ 9.16.2.1 Stakeholder Requirements Definition and Requirements Analysis SSE Activities (reference 4.1-4.2)
  ➢ 9.16.2.2 Architecture Design SSE Activities (4.3)
  ➢ 9.16.2.3 Verification / Validation SSE Activities (4.6 & 4.8)
  ➢ 9.16.2.4 Maintenance and Disposal SSE Activities (4.10-4.11)

◆ 9.16.3 SSE Activities for the Project Processes
  ➢ 9.16.3.1 Risk Management Process SSE Activities (5.4)
  ➢ 9.16.3.2 Configuration Management Process SSE Activities (5.5)

◆ 9.16.4 SSE Activities for the Agreement Processes
  ➢ 9.16.4.1 Acquisition and Supply Processes (6.1-6.2)

◆ 9.16.5 References
Systems Security Engineering (SSE) Working Group
SE Handbook update for SSE

SSE Section 9.16 Way Forward

◆ **Word count per section**
  - a 3 page target breaks down to about 1000 words (35 lines per page and 11 words per line)
  - 11 sections (including the intro sections) means approximately 100 words per subsection and 50 words per intro section that has subsection

◆ **Plan**
  - Sections 16.2.1/2.2/2.3 will be drafted in August to establish tone and content scope
  - Remaining Sections need to be drafted by end of September
  - An October-live wiki with limited access will likely be employed after initial drafts
  - Next iteration by first week of November
  - Completion targeted by December 15th

◆ **Authors of Initial Drafts**
  - Section 16.1 – Ken Kepchar (volunteered during workshop)
  - Section 16.2.1 – Paul Popick
  - Section 16.2.2 – Beth Wilson
  - Section 16.2.3 – Rick Dove
  - Need authors for other sections (16.2.4, 16.3.1, 16.3.2, 16.4.1)
SSE Section 9.16 Way Forward

A 100 word budget per section may be difficult to accomplish

- Each section should not go into any practice-detail, but rather stick to general process engagement responsibility
- While recognizing deference between different types of system-projects (large/small; defense/commercial; long-life/short-life; Cyber/physical/human/SoS, etc).

First step into the SE Handbook-Process world for Security –

- each Handbook revision hereafter will have an opportunity to improve the initial V-3.2 door-opener.

Workshop Note: a 4-6 page limit will change these numbers
9.16 System Security Engineering (SSE)

◆ 9.16.1 Systems Engineer and Systems Security Engineer Roles and Responsibilities for SSE
  ▪ The role and responsibilities of the Systems Engineer in SSE
  ▪ Role and responsibilities of the Systems Security Engineer
    • Establishing the top level security requirements and the plan for the use of the SSE
    • Establishing and tailoring the systems engineering technical reviews (SRR, PDR, …) criteria for SSE
  ▪ List of SSE sub-specialties

◆ 9.16.2 SSE Activities for the Technical Processes
  ▪ key activities for selected technical processes overview

Workshop suggestion: add role of SysSecEng in system lifecycle to 9.16.1
9.16.2.1 Stakeholder Requirements Definition and Requirements Analysis SSE Activities (reference 4.1-4.2)

- Identification of stakeholders classes that have a security perspective
- Identification of security mitigation and or/ compliance requirements (Secure design, anti-tamper, FIPS 140-2 compliance, HIPAA, SOX, Supply Chain Risk Management, SOX)
- Abuse and misuse scenarios to describe the operational environment
- Measures of effectiveness for system security
- Mission criticality analysis
- Threat and Vulnerability analysis
- Secure and defensive design requirements
- Abuse and misuse scenarios elaboration
- Risk-cost-benefit trade to determine security requirement
9.16.2.2 Architecture Design SSE Activities (4.3)

- Secure design pattern to analyze security requirements (reference SEI TR)
- Allocate security requirements to system elements
- Updated vulnerability analysis as design is elaborated
- Design for security
  - Isolation and separation of the most critical functions and data from less critical functions and data; separation mechanism include separation kernels, virtualization, and encryption.
  - Detection and monitoring of
    - inputs and outputs to valid values, ranges and formats
    - Faults
    - Intrusions
    - Anomalous behavior
  - Collection of data for forensics
  - Deception (e.g. honey pots)
  - Anti-tamper
  - Fault and attack recovery
  - Real-time adaptation of monitoring, detection and defensive functions
  - Establish programs secure design and coding standards based examination of common vulnerabilities form SEI, CWE.CVE, CAPEC and other sources
9.16.2.3 Verification / Validation SSE Activities (4.6 & 4.8)
- Develop test scenarios and test cases over a range of misuse scenarios and abuse cases (red team, penetration testing, …).
- Ensure that the most prevalent vulnerabilities noted in CVE or SEI websites are prevented.

9.16.2.4 Maintenance and Disposal SSE Activities (4.10-4.11)
- Periodic and event (enhancements, tech refresh, …) driven reassessment of threats and vulnerabilities
- Rapid deployment of security enhancements to address exploited vulnerabilities
- Risk-cost based trade-off deployment of security enhancements
- Protection of intellectual property, security features and environment during disposal to prevent reverse engineering and exploitation
9.16.3 SSE Activities for the Project Processes

9.16.3.1 Risk Management Process SSE Activities (5.4)
- Mission criticality analysis to inform the consequence portion of the risk analysis
- Vulnerability analysis to inform the likelihood portion of risk process
- Describe a cost benefit risk trade-off model to determine the appropriateness of the security features included in the design

9.16.3.2 Configuration Management Process SSE Activities (5.5)
- Limiting access to system and specific modules to minimize risk of malicious insertion
- Keeping records for forensics analysis of configuration changes
- Applying vendor updates and patches to reduce vulnerabilities

9.16.4 SSE Activities for the Agreement Processes

9.16.4.1 Acquisition and Supply Processes (6.1-6.2)
- System security engineering security extends to protecting development environment
- Knowing the origins of the products that make up the
  - System being developed
  - development environment
- Assessing the threats and vulnerabilities to the supply chain
- Protecting the supply chain
- Trade-offs between supply vulnerabilities and design requirements

16.5 References
INSIGHT 2013Q2 Essay Project Status and Discussion
The Interplay of Architecture, Security, and Systems Engineering

There was a time when architects thought about security... and perimeter defense was sufficient. Systems architects must reclaim the practice. Today, all systems are prey.
What’s Inside

President’s Corner 3

Special Feature 7
- Systems of Systems and Self-Organizing Security 7
- Systems of Systems and Security: A Defense Perspective 11
- Securing a System of Systems: Start with the Threats that Put the Mission at Risk 15
- A Model-Based Approach to Support Systems-of-Systems Security Engineering for Data Policies 18
- Systems-of-Systems Issues in Security Engineering 22
- Trading Security and Safety Risks within Systems of Systems 26
- How Do We Measure Security? 30
- Making People the Center of Systems Security 32
- Security in the Age of Social Media: A Systems Engineering Challenge 35
- Understanding Stigmergy as a Pattern in Self-Organizing Adversarial Systems of Systems 37
- Architectural Patterns for Self-Organizing Systems-of-Systems 42

Fellows’ Insight 45
- Key Issues of Systems Engineering 45
- How to Optimize a System 46

Forum 50
- Toward a SoSEK, A Source of Systems Engineering Knowledge 50

Technical Operations 51
- On the Right TRAK 51

INCOSE Operations 52
- Personal Reflections on the Value of Certification 52

INCOSE Events 53
- System Engineering Events from Around the World 53

In Memoriam 57
- In Memoriam A. Wayne Wymore 57

Book Reviews 62
- Ten Steps Ahead: What Separates Successful Business Visionaries from the Rest of Us 62

Final Thoughts 63
- From the Chief Editor 63
What’s Inside

President’s Corner

Special Feature

11 or so ~2,000 word essays written by WG members and associates

Fellows’ Insight

Forum

Technical Operations

INCOSE Operations

INCOSE Events

In Memoriam

Book Reviews

Final Thoughts

From the Chief Editor

The Buck Stops Here:
Systems Engineering’s Responsibility for System Security

July 2013 | Volume 16 Issues 2

A PUBLICATION OF THE INTERNATIONAL COUNCIL ON SYSTEMS ENGINEERING

INCOSE
International Council on Systems Engineering

INSIGHT
Mission: These essays are intended to lower the barriers (toward removal) of effective systems and security engineer mutual engagement. The barriers are those perceived by systems engineers, security engineers, project managers, and program managers.

On-or-Before Schedule
10 Jul 2012: Call for essays issued.
15 Aug 2012: Authors declare intent, topic, and brief abstract to rick.dove@parshift.com.
01 Sep 2012: Authors selected and a coach from the Editorial Committee is assigned.
30 Nov 2012: First (complete) draft essay submission.
29 Jan 2013: Symposium – Presentation/discussion at IW13 (LiveMeeting enabled).
28 Feb 2013: Notification of acceptance – comments for improvement as appropriate.
31 Mar 2013: Final draft submission, with author-company release if necessary.
15 May 2013: Collection sent to INSIGHT editors.
xx Jul 2013: INCOSE INSIGHT publication.

General guidance
INCOSE is a general Systems Engineering association. Essays must speak effectively and meaningfully to systems engineers, and not be directed exclusively to security or software engineers, or defense system interests, with specialty vocabulary and knowledge. Essays should relate real life experience of effective/attempted mutual engagement, with lessons learned as appropriate.
The mission is important, so a coach from the Editorial Committee will be assigned to each author.
12 Essay Author Commitments Currently

Requirements, Requirements Analysis, and Concept of Operations Processes:
  SysE: Paul Popick -- SecE: Mark Snell and Ruth Duggan

Architectural Design Process:
  SysE: Ken Kepchar -- SecE: Kevin Stoffell

Implementation Process:
  SysE: TBD -- SecE: Stephan Thompson

Integration Process:
  SysE: Robert Marchant (also V&V) -- SecE: Carol Woody (SEI)

Verification and Validation and Test and Evaluation:
  SysE: Robert Marchant (also integration) -- SecE: Bruce Hunter

Three large view essays:
– Beth Wilson (SysE): Management’s Processes for Systems and Security Engineering Integration
– Janet Oren (SecE): A General Process-Basis for Integrating Systems and Security Engineering
– Don Gelosh, Worcester PolyTech (Education): Univ. curricula integrating security with systems engineering.

Other Commitments:
- John Miller on Supply Chain

UPDATED CALL
Visit www.parashift.com/s/CallForEssays-INSIGHT2013Q2.pdf for continuing updates to this Call for Essays.
INCOSE Symposium 2013
SSE Track
Food for Thought:

What does the System Engineer need to know about Security Engineering and Systems Security?

What kinds of questions should the Systems Engineer ask of the Security Engineer?

How can Security Engineers engage with Systems Engineers and Systems Engineering Processes effectively?

15 pages maximum
6 papers/track (can do a double track)

July IS2012 finalize theme for call
Systems Engineering Responsibility for System Security

Papers due November 8, 2012
Systems Security Engineering (SSE) Working Group
(Obligated to Develop References for the)

SE Body of Knowledge (SEBoK) Project
Systems Security Engineering (SSE) Working Group
SE Body of Knowledge (SE BoK)

**Background**

- INCOSE has given SSE WG responsibility to “contribute” our Systems-and-Security knowledge to the security section of SEBoK
- SEBoK will eventually be an accessible wiki
- Upcoming monthly Webinar will discuss INCOSE and SEBoK
- Objective of SE BoK
  - Create a SE Body of Knowledge (SEBoK) that defines and organizes the SE Discipline and is globally recognized by the SE community as the authoritative BoK for the SE discipline

**SSE Objectives**

- To have a collection of candidate Primary References for SSE WG circulation prior to, and discussion at, IS13 –
- Select a subset of reference based upon the IW13 discussion to offer to the SEBoK WG
- Identify someone to the lead the SSE contribution to the SEBoK Working Group
  - To lead the SSE effort to collect and discuss the SEBoK references at IS13
First topic under SE and Specialty Engineering is Integration of Specialty Engineering at www.sebokwiki.org/075/index.php/Integration_of_Specialty_Engineering - with a US Air Force “Primary Reference” that displays the figure below.

Security is notably absent – indicating our work of obtaining “primary references” is not limited to the Security Engineering section.
More Than *Primary* References Needed

References

Works Cited


Primary References


Additional References

No additional references have been identified for version 0.75. Please provide any recommendations on additional references in your review.
Primary Reference
Format is explained – but qualifications are not found
www.sebokwiki.org/075/index.php/How_to_Read_the_SEBoK#Primary_Reference_Article
Security Engineering is concerned with building systems that remain secure despite malice or error. Security engineering focuses on the tools, processes, and methods needed to design and implement complete systems that proactively and reactively mitigate vulnerabilities. Security engineering is a primary discipline used to achieve system assurance.

Multidisciplinary Reach
Security engineering incorporates a number of cross-disciplinary skills, including cryptography, computer security, tamper-resistant hardware, applied psychology, supply chain management, and law. Security requirements differ greatly from one system to the next. System security often has many layers built on user authentication, transaction accountability, message secrecy, and fault tolerance. The challenges are protecting the right items rather than the wrong items and protecting the right items but not in the wrong way.

Robust Security Design
Robust security design explicitly rather than implicitly defines the protection goals. The Certified Information Systems Security Professional (CISSP) Common Body of Knowledge (CBK) partitions robust security into ten domains (Tipton 2006):

- Information security governance and risk management addresses the framework, principles, policies, and standards that establish the criteria and then assess the effectiveness of information protection. Security risk management contains governance issues, organizational behavior, ethics, and security awareness training.
- Access control is the procedures and mechanisms that enable system administrators to allow or restrict operation and content of a system. Access control policies determine what processes, resources, and operations users can invoke.
- Cryptography can be defined as the principles and methods of disguising information to ensure its integrity, confidentiality, and authenticity during communications and while in storage. Type I devices are certified by NSA for classified information processing. Type 2 devices are certified by NSA for proprietary information processing. Type 3 devices are certified by NSA for general information processing. Type 4 devices are produced by industry or other nations without any formal certification.
- Physical (environmental) security addresses the actual environment configuration, security procedures, countermeasures, and recovery strategies to protect the equipment and its location. These measures include separate processing facilities, restricted access into those facilities, and sweeps to detect eavesdropping devices.
- Security architecture and design contains the concepts, processes, principles, and standards used to define, design, and implement secure applications, operating systems, networks, and equipment. The security architecture must integrate various levels of confidentiality, integrity, and availability to ensure effective operations and adherence to governance.
- Business continuity and disaster recovery planning are the preparations and practices which ensure business survival given events, natural or man-made, which cause a major disruption in normal business operations. Processes and specific action plans must be selected to prudently protect business processes and to ensure timely restoration.
- Telecommunications and network security are the transmission methods and security measures used to provide integrity, availability, and confidentiality of data during transfer over private and public communication networks.
- Application development security involves the controls applied to application software in a centralized or distributed environment. Application software includes tools, operating systems, data warehouses, and knowledge systems.
- Operations security is focused on providing system availability for end users while protecting data processing resources both in centralized data processing centers and in distributed client / server environments.
- Legal, regulations, investigations, and compliance issues include the investigative measures to determine if an incident has occurred and the processes for responding to such incidents.

Given the variety of security needs and various domains that contribute to system security, a commonly applied architecture and design approach is known as “defense in depth.” This approach implements multiple layers of defense and countermeasures, making maximum use of certified equipment in each layer to facilitate system accreditation.

References
Works Cited

Primary References
- No primary references have been identified for version 0.75. Please provide any recommendations on additional references in your review.

Additional References
SEBoK Security Engineering: Wiki Comments as of 9Jul2012

<table>
<thead>
<tr>
<th>Thread title</th>
<th>Replies</th>
<th>Last modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>References</td>
<td>4</td>
<td>19:44, 8 December 2011</td>
</tr>
<tr>
<td>Integration</td>
<td>2</td>
<td>05:17, 21 November 2011</td>
</tr>
<tr>
<td>Multiple Perspectives</td>
<td>1</td>
<td>20:30, 18 September 2011</td>
</tr>
<tr>
<td>Terminology</td>
<td>1</td>
<td>20:30, 18 September 2011</td>
</tr>
<tr>
<td>General Content</td>
<td>1</td>
<td>20:29, 18 September 2011</td>
</tr>
<tr>
<td>Open Discussion</td>
<td>1</td>
<td>20:29, 18 September 2011</td>
</tr>
</tbody>
</table>

From Bkcase Wiki – The SEBoK is designed to provide pointers to a variety of relevant works within the systems engineering community for a given topic. The author team acknowledges that more diversity of references is still needed. Please provide your feedback on references here, specifically what additional references should be considered for future incorporation.

**References**

**Bkcase, 18 September 2011** – The SEBoK is designed to provide pointers to a variety of relevant works within the systems engineering community for a given topic. For version 0.5, the author team acknowledges that more diversity of references is still needed. Please provide your feedback on references here, specifically what additional references should be considered for future incorporation.

**Stn, 7 November 2011** – The MITRE System Engineering Guide has articles on various aspects of security engineering. These could be included as additional references: Mission Assurance and Certification and Accreditation

**Harold Baker, 21 November 2011** – Good reminder that certification and accreditation (C&A) is a vital companion process to Systems Security Engineering

ABSTRACT: The need for system safety was recognized during the 1940s. Information systems security engineering is now recognized as essential to many contemporary system developments. It has been observed that safety and security requirements often overlap within software-based systems. Both the safety and security disciplines have an objective of operating and failing in a safe and secure manner that is realized through analysis, testing, and/or inspection. Such common objectives and methodologies raise the question of whether cost savings could be realized if the safety and security tasks were executed simultaneously. To study potential cost savings, it is necessary to compare tasks in a similar manner. While safety engineering descriptions are task based and focused on artifacts, information systems security engineering process descriptions are unstructured. The purpose of this research was to establish a comparable process description for systems security engineering. Business process modelling based upon existing process descriptions is, as a starting point, applied to define a framework rendering the process understandable to a broad audience and to allow for focused research and improvement. This research presents the process for creation of an innovative model and completion of the model and supporting documentation. Evidence is provided of early adoption of the model. Reviews from application of the process model have recognized its value in establishing consistency in application of the systems security engineering process and in guiding further research on task execution. The model is also being adopted as the foundation for development of a new government publication addressing systems security engineering.

From page 18 “The National Security Agency is working with the National Institute of Standards and Technology to revise and expand the 2002 [NSA] publication. The model produced by this current research has been provided to the National Security Agency to guide the content of the new publication.” The 2002 NSA publication is titled “Information Assurance Technical Framework” with a focus on “Information Systems Security Engineering Process”.

Page 35 of thesis: “After a July 2010 draft of the described Special Publication was deemed unacceptable by the management of the Agency, the Information Systems Security Engineering process model defined in Appendix B was offered as a framework for the Special Publication. The model was used as the initial outline for the new Special Publication, and many of the defined tasks and output were incorporated into the current draft. While the process model is clearly evident within the new document, it does not reflect all 94 tasks because that level of detail is not the intent for the publication.”
Alignment Considerations

Compatibility with SE governing documents must be considered.

What documents relevant to security issues associated with SE processes should be considered?

What nations have documents that should influence what the handbook addresses and how it addresses?

What domains in addition to military acquisition are relevant.

What standards must be considered?

Are we constrained to strict compatibility, or can we deviate with responsible justification?

-------

Content compatibility, when appropriate, with SE-influential and SE-governing documents should be maintained with cognizance.

Form compatibility with the INCOSE handbook, enabling eventual process integration, should be maintained.
Collaboration with New Agile Systems Engineering WG?

Purpose—The purpose of this working group is to identify and develop a body of knowledge that will inform systems engineering and related processes which require agile system capability. Agile systems of interest to this working group include both systems engineering processes and systems-engineered systems.

This working group views agility as a sustainable system capability, enabled and constrained fundamentally by system architecture. This architecture delivers agile capability as reconfiguration, augmentation, and evolution of system functionality, after deployment; enabling the system to respond to new and immediate situational requirements effectively. Effectiveness of response is measured in response time, response cost, response quality, and response scope sufficient to sustain the system’s functional intent.

Need—The need to understand sustainably agile system design and project management concepts exists on multiple fronts:

· Agile Systems-Engineering development processes have become of interest to the CAB companies, and they are asking that INCOSE develop appropriate guidance.
· Defense organizations have an interest in how agile system concepts might inform agile acquisition processes.
· Quick Reaction Capability (QRC) has been a defense acquisition need for some time and would benefit from an agile response capability by suppliers, yet generally QRC is achieved today by the employment of costly and error-prone overtime work and the increased risk of relaxing formal Systems Engineering processes.
· Both commercial and governmental organizations are finding that the pace of technology and growing user expectations are reducing the effective life time of deployed systems.

Next steps—Under the assumption that the working group will be approved during IS12, organizational activity will occur during the remainder of this year, in preparation for an IW13 kick-off workshop. This will include the creation and population of a SharePoint site, recruitment of WG members from both INCOSE membership and external sources, development of an opt-in announcements mailing list, and an agenda for the IW13 Jacksonville, FL January 26-29 kick-off workshop.

To get on the announcements mailing list indicate that desire to rick.dove@parshift.com, and include any thoughts you may have.
Open Author Needs and Opportunities: 4 Projects

1. **SE Handbook**
   - Insert security content (1-2 sentences)
   - New SSE Section 9.16 (2-3? Handbook pages)
   - Expect call for inputs Fall 2012

2. **INCOSE Symposium 2013**
   - Philadelphia, June 24-27, 2013
   - Security Track
   - 15 page max papers
   - Papers due early Nov 2012

3. **SEBoK**
   - Need References for Review at IW12

4. **INSIGHT Issue 2013**
   - 2,000 word essays
   - Sep 2012 Authors selected
   - Nov 2012 Draft essays
   - Jan 2013 Review essays at IW13
   - July 2013 Issue
“A wicked problem is a social or cultural problem that is difficult or impossible to solve for as many as four reasons:

- incomplete or contradictory knowledge,
- the number of people and opinions involved,
- the large economic burden, and
- the interconnected nature of these problems with other problems.

www.ssireview.org/articles/entry/wicked_problems_problems_worth_solving