Content for October 2011 Newsletter

INCOSE Enchantment Chapter Systems Engineering Challenge Event

September 11, 2019 – Nexus Brewery

Systems engineering "challenges" were submitted by Chapter members to be discussed at the September 11, 2019 Enchantment Chapter meeting held at Nexus Brewery. The goal was to collaboratively explore the nature of the challenge, and brainstorm suggestions to overcome issues while amplifying positive aspects. 3 challenges were submitted, and due to time constraints, 2 were discussed. 14 participants were involved in the event (including 2 remote participants). Ann Hodges facilitated the discussion.

1. **Challenge 1 submitted by Rick Dove**: What are the nascent evolutionary trends in the systems security environment that will shape necessary response capabilities in the Future of Systems Engineering? This is a question about the dawning problem space, not about solution strategies and tactics. Preliminary considerations will be suggested to spur discussion and refinement. (Nascent: just coming into existence and beginning to display signs of future potential.)

Challenge Topic 1 Context

The Future of Systems Engineering (FUSE) is a multi-organization collaborative project with a key concern about the nature of systems security in that future.

The futures of SE and of systems security are determined by the nature of the environments in which they will operate. Those environments are the fitness functions that will naturally select compatible approaches, and select out those which aren't compatible, with prejudice.

No need to guess at what those environments will look like. William Gibson:

"The future is already here, its just not evenly distributed" … yet.

==========

A system interfaces with, and interacts with, its operating environment; and remains viable (capable of working successfully) and relevant (appropriate to current desires) only to the extent to which it is operationally compatible with the *current order*.

Cyber-Physical-Social systems: The social dimension will play a major role in the future of systems engineering, with key implications for system security.

The social dimension deals with symbiotic collaborative relationships among components in an SoI as well as among the SoI and its encompassing SoSs. (components include software, devices, people)

Topic 1. Profiling the Operating Environments

FUSE General SE CURVE	FUSE System Security CURVE
Caprice	
• Survivability (i.e., current order compatibility) • Occurrence and nature of emergent behavior • Game-changing technologies • Availability of symbiotic social relationships	• Innovative attack method • Dependency cascade • AI employment, quantum computing • Collaborative symbiosis (failed and new)
Uncertainty	
• Relevance (i.e., fits current desires) • Cohesion in the greater SoSs (multiple) • Integrity & symbiosis of social relationships.	• Cost vs perceived value (both sides) • Broken physical relationships • Broken/weakened social relationships
Risk	
• Viability (i.e capable of working successfully) • Cohesion among constituent parts	• Inadequate design consideration & execution • Addressing adversity effectively
Variation	
• Operational environments • Social compatibility	• Peer behavior, breech criticality • Social priority conflicts
Evolution	
• Toward more op environment complexity • Toward more SoI complexity • Toward shorter SoI static viability • Toward new technology options • Toward new malevolent threats to viability • Toward greater social involvement.	• IoT in general, external SoS • Component technical scope, internal SoS • Growing attack community (skills and scope) • Increasing technical innovation • Increasing perceived attack value • DevSecOps, increasing connectivity

Need: A short general list that encompass key necessary considerations.
Intent: Irrefutable considerations that can achieve broad consensus.

Major discussion points include:

- Variation aspect – social compatibility with systems and components – SE perspective?
- Health – components/nodes comparing notes of "community", common in ad hoc networks. More common, more necessary
- How critical is a breach? Behavior monitoring – local vs. global perspectives on criticality. Security systems monitor for threats (components or human). Timing – how critical now? Is it a breach or a denial of service? Consequence evaluation – known vs. unknown.
- General strategy development/consideration – consequence varies in environment – breach of criticality.
- General strategy development/consideration – consequence

2. **Challenge 2 submitted by Ann Hodges**: SE in early stage R&D - What are the challenges in applying SE to an early stage R&D? When should SE be applied to early stage R&D? Are there triggers that could identify when SE should be applied? Is there a compelling value proposition for "selling" the idea of applying SE to early stage R&D projects? What SE concepts have the biggest "bang for the buck" in these types of projects? What SE practices, when applied early in an R&D project, support future growth if there is a desire to "productionize" the R&D's focus area?

INCOSE ENCHANTMENT CHAPTER

Topic 2. SE in Early Stage R&D

29th Annual INCOSE international symposium
Orlando, FL, USA
July 20 - 25, 2019

Ann Hodges, Distinguished Member of Technical Staff, CSEP, SAFe SPC4
Sandia National Laboratories

A Federally Funded Research and Development Center Perspective

Systems Engineering in Early Stage R&D Projects

SAND2019-7310 C

www.incose.org/symp2019

What are the challenges in applying SE to an early stage R&D?

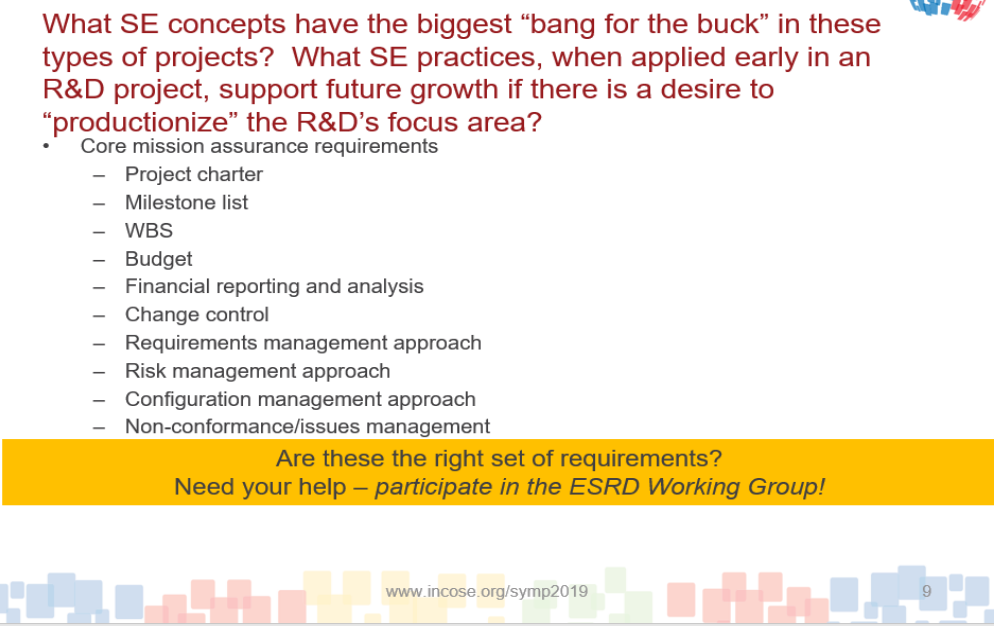
- SE practices may be unfamiliar to researchers
  - Need to reframe
- Determine set of right-sized practices that support future maturation and scalability
  - Right level of rigor
  - Nurture creativity and exploration
  - Preserve research quality, defensible research
- SEs more familiar with high rigor

When should SE be applied to early stage R&D? Are there triggers that could identify when SE should be applied?

- As early as possible
- Should be done for all projects

Is there a compelling value proposition for "selling" the idea of applying SE to early stage R&D projects?

- Right-sized rigor
  - Timing
  - Scope
  - Formality
- Develop "pull" vs. "push"
  - What are researchers' ideas for practices that preserve research quality?
  - Reframe practices to R&D terminology
  - Coach PI, technical team leads in practices
- Templates and examples
  - Don't start with a "blank sheet of paper"



Major discussion points include:

- SE for Early Stage R&D – a design engineering stuy was done by one of the challenge participants. There were multi-dimensional challenges. Enforcement/discipline applied to practices – no mechanism, different priorities/perspectives. Different roles and cultures – IPT tends to be more academic in R&D, government/military sponsors, leads vs. "rank + file" contractors. Inforal networks compromise integrity of SE. Expectations of players.
- Sponsor changing in the middle – charter should be the basis, changes evaluated.
- Charter should define needs, narrowing the scope for R&D project to fill

3. **Challenge 3 submitted by Rick Dove**: Given a general encompassing profile of the problem space, what are the necessary general strategies for compatibility with the operating environments. This is a question about necessary general strategies, not about specific objectives for those strategies, nor about tactical approaches. Strategy objectives and tactics will be context dependent, appropriate for work after reasonable consensus on problem space and necessary strategy is achieved. Preliminary considerations for necessary strategy will be suggested to spur discussion and refinement. ***Didn't discuss due to time constraints.***

Topic 3. Profiling Compatibility Strategies

Strategies for creating and eliminating (…processes/methods associated with):
- Opportunity & risk awareness
- Response actions/options
- Memory assimilation
- Decisions to act

Strategies for improving:
- Awareness/sensing
- Memory in culture, actions/options, ConOps/OpsCon
- Action/option effectiveness

Strategies for accommodating likely migration to (that requires an infrastructure change):
- New fundamentally-different types of opportunities
- New fundamentally-different types of threats

Strategies for modifying:
- Actions appropriate for needs
- Personnel and processes appropriate for actions

Strategies for correcting:
- Insufficient awareness
- Ineffective actions/options
- Wrong decisions

Strategies for dealing with varying:
- Effectiveness of actions and options
- Effectiveness of evaluations

Strategies for expanding and contracting:
- Capacity to handle simultaneous response actions

Strategies for reconfiguring:
- Elements of response actions
- Participants involved in response actions

Need: A short general list that encompass key necessary considerations.
Intent: Irrefutable considerations that can achieve broad consensus.