Call for Articles

INCOSE INSIGHT, June 2022, Theme:

Systems Security in the Future of Systems Engineering (FuSE)

An Invited Article Series – INCOSE Membership not required

Intro: The Future of Systems Engineering (FuSE) is an INCOSE-led multiorganizational collaborative initiative pursuing INCOSE's *Vision 2025* and beyond. To accomplish this the FuSE initiative encompasses a number of topic areas with active projects to shape the future of systems engineering. One such topic area addresses Security in the Future of Systems Engineering. In 2020 a multiorganization workshop team identified eleven strategic foundation concepts appropriate for near-term development. An IS21 paper introduced these concepts with eleven one-page descriptions to instigate and inspire thinking and involvement in the development, exposition, and practice of these foundational concepts. The focus is on strategic intent, leaving ample room for various approaches.

IS21 paper: www.parshift.com/s/210717IS21-FuseSecurityRoadmap.pdf.

Mission: These articles are intended to propose or expose strategies for developing, implementing, and/or practicing the foundation concepts.

Approach: This Theme Issue will accommodate articles specifically addressing one or more foundation concepts identified in the IS21 FuSE Security Roadmap paper linked above. Authors may submit multiple offerings. A brief synopsis of the concepts in table form is on the next page. Appropriate articles include concept strategy development, implemented case study exposure, experimental implementation, and additional community instigation and inspiration. Systems engineering is practiced in one form or another in many domains. These foundation concepts are domain agnostic, and some of them may have an early foothold in some domains worth exposing.

Schedule

2021 Aug 15:	Call for articles issued.
2021 Oct 15:	(nlt preferred) Concept(s) being addressed, working title, and one paragraph working abstract.
2021 Dec 15 :	First (complete) draft submission.
2021 Dec 27:	Feedback comments returned on first draft.
2022 Jan 17:	Second draft submission, if appropriate, for review at IW22.
2022 Jan 29:	Live review: 15 minute presentation with 10 minute feedback at IW22 (in attendance or virtual).
2022 Feb 15:	Detailed comments returned to authors for improvement, as appropriate.
2022 Mar 15:	Final draft submission, formatted for required style, with author-company release.
2022 Apr xx:	INSIGHT editors may contact authors directly with copy-editing suggestions.
2022 Jun xx:	INSIGHT publication.

General guidance

- Articles must speak meaningfully to systems engineers.
- The mission is the objective.
- These are not journal articles, 2000-4000 words is the target.
- Do not use the MS Word reference tool. Citations and references should comply with the Swinburne Harvard reference style. A descriptive guide with examples is available in the Downloads section of the INCOSE IS website. Additional information is available at: http://www.swinburne.edu.au/library/referencing/harvard-style-guide.
- Style guide: MS Word, 12 point Times New Roman, single line spacing, indented paragraphs, with minimal or no (preferred) use of styles. Graphics are highly encouraged and do not take away from word-count.

Evaluation Criteria:

- Fit to the theme, and meaningful to SEs and SE issues.
- Advances the mission.
- Publishability: length (2,000-4,000 words), writing quality, logical, and comprehensible.

Submissions: NO PDF. Send submissions to rick.dove@parshift.com attached as an MS Word document. Be sure to include a title, and author names and email addresses in the by-line underneath the title. Also include an abstract and bio for each author.

Updates to this call-for-articles will be maintained at www.parshift.com/t/2022Call.pdf

The next page has a quick synopsis of the eleven concepts

This table provides a quick synopsis of the eleven concepts and conforms to the material in the IS21 paper, with the exception that the General Barriers column was not in the IS21 paper.

This material is FYI and is not a mandatory prescription for how you may choose to address one or more of the eleven concepts.

Concept Title	General Problem to Address	General Needs to Fill	General Barriers to Overcome
1. Security Proficiency in the SE Team	Insufficient knowledge of system security engineering at the systems engineering level; communication across knowledge and expertise boundaries.	System security and its evolution effectively enabled by systems engineering activity.	Disrespect between SE and Sec people; perception of security as non-functional requirement; finding high level security expertise (architecture/strategy/empathy).
2. Education and Competency Development	Security education is not well integrated with engineering education, creating a skills gap.	Education at all levels focused on security of cyber-physical systems (CPS).	Perception of insufficient scientific/technical rigor for inclusion in engineering programs; engineering faculty security knowledge gap.
3. **Stakeholder Alignment**	Misalignment of security vision among stakeholders. Inconsistent appreciation for security among stakeholders.	Common security vision and knowledge among all stakeholders.	Stakeholder willingness to engage in collaborative convergence.
4. **Loss-Driven Engineering**	Traditional vulnerability assessments and risk/consequence models for security, safety, and related 'ilities occur too late in the SE process.	Standard metrics and abstractions relevant to all system lifecycle phases.	Cross domain vocabulary/taxonomy differences; insufficient respect for potential leverage; solution- rather than problem-dominant security thinking.
5. **Architectural Agility**	Enabling effective response to Innovative threats and attacks.	Readily composable and re-composable security with feature variants.	Comfort with and acceptance of a dynamic security profile.
6. **Operational Agility**	Timeliness of detection, response, and recovery.	Ability for cyber-relevant response to attack and potential threat; resilience in security system.	Comfort with and acceptance of a dynamic response and recovery capability.
7. **Capability-Based Security Engineering**	Security strategies based on available solutions rather than desired results.	Top-down approach to security starting with desired results/value.	Difference between capability and features; solution-dominant thinking; trust that the outcome will be satisfactory.
8. **Security as a Functional Requirement**	As a non-functional requirement, systems security does not get prime SE attention.	Systems engineering responsibility for the security of systems.	Cultural inertia that prioritizes system purpose over viability.
9. **Modeling Trust**	Systems Security has moved away from traditional focus on trust to a more singular focus on risk.	Reinvigorate formal modeling of system trust as a core aspect of system security engineering; address issues of scale with model-based tools and automation.	Entrenched risk-based practices and education; simplicity of communicating and comparing risk metrics; perception of security as a non-functional requirement.
10.Security Orchestration	Disparate security solutions operate independently with little to no coordination.	Tightly coupled coordinated system defense in cyber-relevant time.	Independent stovepipe solution tools; multiple disparate stakeholders; hesitation to explore interdependencies
11.Techno-Social Contracts	Insufficient detection capability for innovative attack methods [with dedicated purpose security components].	Augmented detection & mitigation of known and unknown attacks [with components collaborating for mutual protection].	Trust in the security of the approach; trust in the emergent result.