The Great Cybersecurity Reset

Trustworthy Secure Systems Engineering

An Imperative for National and Economic Security



Current Landscape

- Significant convergence of cyber and physical systems
- Increasing complexity of systems of all types
- Growing number of systems in U.S. critical infrastructure with unknown or insufficient levels of trust or assurance
- Ubiquitous connectivity results in shared risk of system failures with adverse consequences — some potentially severe or catastrophic
- Rapid emergence of Artificial Intelligence (AI) technologies
- Cybersecurity of systems is significantly failing



Threats to Modern Systems

- Natural disasters (floods, fires, earthquakes, hurricanes)
- Errors of omission or commission in software and firmware (despite efforts to contain them)
- System failures in hardware, software, and firmware
- Cyber attacks from hostile adversaries (increasing in quantity and quality)





Generational and Institutional Cybersecurity Problems – Part 1

- Insufficient alignment with the systems engineering lifecycle, creating a disconnected and increasingly ineffective design and evaluation process
- Insufficient attention to risks involving cyber-physical assets (e.g., ASICs, FPGAs, PLCs, robotic actuators, sensors)
- Inadequate integration of cybersecurity risks into the established framework for overall project risks (e.g., safety, reliability) and engineering tradeoffs



Generational and Institutional Cybersecurity Problems – Part 2

- Inadequate understanding of the full spectrum of attack surface and how to gain effective and efficient coverage
- No defensible basis for cybersecurity ROI due to absence of measurable protection objectives — highlighting need for explicit threat-informed design within the systems engineering process
- Inadequate visibility into the underlying system design (i.e., black box problem) resulting in insufficient assurance in the system capability and resilience



Dartmouth ISTS

The National Challenge

The long-term economic and national security interests of the United States depend on our ability to protect increasingly complex systems in the critical infrastructure that drive innovation, provide basic services, enable global trade, and promote a free society.





On September 12, 1962, President John F. Kennedy in one of his most memorable speeches, challenged the Nation with his bold moon landing proposal.

Great national challenges require great national solutions

"We choose to go to the Moon in this decade and do the other things, not because they are easy, but because they are hard; because that goal will serve to organize and measure the best of our energies and skills, because that challenge is one that we are willing to accept, one we are unwilling to postpone, and one we intend to win."

The Essential Partnership







The Solution

Create an ecosystem that promotes and facilitates the long-term collaboration among government, industry, and academia to develop an enduring and adaptive framework and body of knowledge/practice to institutionalize and operationalize trustworthy secure systems engineering.

The ecosystem concept requires strong national leadership, strategic vision, measurable execution, and effective feedback loops to facilitate continuous improvement.



Dartmouth ISTS

Trustworthy Secure Systems Engineering

Solving difficult and challenging cybersecurity problems for complex systems requires a strategic, holistic systems engineering approach that includes people, processes, and technologies

PEOPLE

- Trustworthy Secure Systems Security Engineering (TSSE) knowledge, skills, and abilities
- Educational institution support of TSSE curricula programs
- TSSE internship programs in real world pilot projects and test beds

PROCESSES

- Life cycle-based systems engineering provides the foundation for system security
- Application of security design principles, concepts, and best practices
- Evidence-based assurance to achieve trustworthy systems

TECHNOLOGIES

- Trustworthy secure system component development
- Assurance cases for increased system component design visibility and transparency
- Promoting trusted system component competition in industry



Why Trustworthy Secure?

- Secure is an absolute term that cannot be achieved absolutely
- Trustworthy is a term that can imply varying degrees of *trustworthiness* according to specified assurance levels
- Taken together, the term *trustworthy secure* allows mission owners to specify system capability and level of protection in the context of cost, schedule, and performance



Foundational TSSE Concepts

- Security is an emergent property of an engineered system like safety, reliability, and resilience
- Mission protection needs to guide and inform security requirements for functionality and assurance
- Protection needs focus on:
 - Ensuring predictable system performance under conditions of stress
 - Minimizing mission or asset impact from intentional disruption or misuse



Six Strategic Pillars in the Ecosystem

- A mission-focused, trustworthy secure systems engineering approach
- Security design principles, concepts, and best practices
- Experimental test beds of real-world systems using a TSSE approach and security design principles, concepts, and best practices
- Incubators of TSSE talent being developed within educational institutions
- Institutions that store and share TSSE experimentation results
- Technology transfer to all communities of interest

These six pillars form a complete and self-sustaining ecosystem for engineering trustworthy systems covering strategy, knowledge, validation, talent, institutional memory, and dissemination.



Trustworthy Secure Systems Engineering Ecosystem





Security Design Principles, Concepts, and Practices



• TSSE Framework

(Problem, Solution, Trustworthiness Contexts)

- Security Policy and Requirements
- System Security Concepts (Protection Needs, Assets, Loss Control, Consequences)
- Trustworthy Secure Design Principles
- Security Functionality and Assurance



TSSE Higher Education Talent Incubators



- Define TSSE knowledge, skills, and abilities for students pursuing systems engineering degrees
- Participate in TSSE experiments and pilot projects by providing students for internship programs
- Integrate TSSE principles, concepts, and practices into current engineering curricula
- Develop TSSE courses that can supplement current engineering courses or support advanced degrees



TSSE Life Cycle Processes, Methods, and Approaches

- ISO/IEC/IEEE 15288 Systems and software engineering — System life cycle processes https://www.iso.org/standard/81702.html
- NIST Special Publication 800-160, Volume 1 Engineering Trustworthy Secure Systems https://doi.org/10.6028/NIST.SP.800-160v1r1
- NIST Special Publication 800-160, Volume 2 Developing Cyber-Resilient Systems https://doi.org/10.6028/NIST.SP.800-160v2r1





System Experimentation Hubs, Test Beds, and Pilot Projects



- Apply TSSE design principles, concepts, and practices to real-world systems engineering pilot projects, experiments, and test beds
- Include pilot projects, experiments, and test beds for vertical sectors such as defense, healthcare, space, finance, transportation, and communications
- Share results to enhance the state-of-the-practice and promote continuous improvement in building trustworthy secure systems



TSSE Repository



- Collect TSSE experiment and pilot project results including engineering artifacts
- Analyze and normalize experiment and pilot project results
- Catalog results and develop online searchable databases for engineering artifacts
- Share experiment and pilot project results with other entities to promote technology transfer



TSSE Technology Transfer

Share best practices with government, industry, academia, consortia, and international partners

 Helps industry continuously improve its engineering processes for building trustworthy secure systems

Pillar 6

- Helps consortia standardize and promote TSSE best practices to improve engineering efficiency and effectiveness
- Helps academic institutions improve curricula to ensure students have the requisite TSSE knowledge, skills, and abilities
- Helps government create meaningful national strategies and policies that support, incentivize, and promote TSSE activities



Dartmouth ISTS

Pillar 4 **TSSE Experiment** and Test Bed

TSSE Experiment and Pilot Project Protecting Cyber-Physical Space Systems



Interagency Partnership NASA, Science Mission Directorate National Institute of Standards and Technology **NASA Jet Propulsion Laboratory**

SunRISE Sun Radio Interferometer Space Experiment

https://csrc.nist.gov/csrc/media/Presentations/2024/protecting-cyber-physical-space-systems/SunRISE-v1.0-Updated9.25.24.pdf





System of Interest



- SunRISE is an array of six toaster-size CubeSats that will work together to study solar activity
- The mission will observe low radio frequency emissions so scientists can understand better how the Sun is able to generate intense space weather storms – known as solar particle storms – that can be hazardous to spacecraft and astronauts
- This research will help scientists forecast space weather, improve our understanding of how our Sun works, and may apply to studies of other stars – particularly those with planets



Dartmouth ISTS

Building Security into the System Life Cycle Replicating the Development Process

NASA Life Cycle Phases	Formulation			Implementation				
	Initiation		Acquisition & Development		Implementation	Operation	Sunset	
Project Life Cycles	Pre-Phase A Concept Studies	Phase A Concept & Technology Completion	Phase Prelimi Desige Techno Comple	e B inary n & blogy etion	Phase C Final Design & Build	Phase D System Assembly Integration & Test	Phase E Deployment Operations Sustainment	Phase F Decommissioning

ACTUAL SunRISE Twin A System Life Cycle: Completed Phase D

SIMULATED

SunRISE Twin B System Life Cycle

Applying NIST SP 800-160 Security Design Principles in Pre-Phase A through Phase C



SunRISE Sun Radio Interferometer Space Experiment



Initial SunRISE Experiment Results

- Increased visibility into the system architecture of Twin B resulted in more effective placement of security safeguards to address threats
- Deflection of common cyber attacks by Twin B that could not be deflected by Twin A
- Faster detection of system incursions in Twin B (i.e., seconds or minutes versus months or never detected in Twin A)
- Reduced system complexity which contributed to achieving a trustworthy secure system that was resilient

The System Authorization to Operate (ATO) issued for SunRISE Twin A was rated "Low Risk." After applying the SP 800-160 security design principles to SunRISE Twin B using the latest threat intelligence, it was determined that SunRISE Twin A, as currently authorized, would be operating at much higher risk rating than expressed by the original ATO.





Summary

- Solving difficult and challenging cybersecurity problems for complex systems requires:
 - An ecosystem that supports, encourages, and promotes cooperation and collaboration among government, industry, academia, and international partners
 - ✓ The elimination of the cybersecurity "stovepipe" and tactical approach to system protection problems
 - ✓ A systems engineering approach that treats security as an emergent property of a system like safety and reliability



Conclusion

• The TSSE Ecosystem:

- Offers a comprehensive model that can be used to solve complex systems security engineering problems and provide a foundation for trustworthy secure systems
- Can be "generalized" and applied to vertical sectors such as healthcare, critical manufacturing, defense industrial base, emergency services, transportation, communications, and nuclear



TSSE Top Priorities and Resource Needs

- **Priority 1:** Recruit additional TSSE Experiments, Test Beds, and Pilot Projects
- Priority 2: Build TSSE Repositories for Best Practices, Engineering Artifacts, Design Patterns, and Lessons Learned











TSSE Top Priorities and Resource Needs

- Priority 4: Define TSSE knowledge, skills, and abilities for students pursuing systems engineering degrees
- **Priority 5:** Review and update current security design principles, concepts, and best practices
- Priority 6: Initiate TSSE technology transfer process with government, industry, academia, and international partners









Trustworthy Secure Systems Engineering Ecosystem

TSSE Priorities by Individual Pillars





Contact Information

Sami Saydjari
Sami.Saydjari@dartmouth.edu
Dr. Ron Ross
Ron.Ross@dartmouth.edu
Dartmouth College
Institute for Security, Technology, and Society
https://ists.dartmouth.edu

Dr. Kymie Tan

Kymie.Tan@jpl.nasa.gov

Principal Investigator SunRISE Pilot Project and Test Bed

NASA Jet Propulsion Laboratory *California Institute of Technology* https://www.jpl.nasa.gov