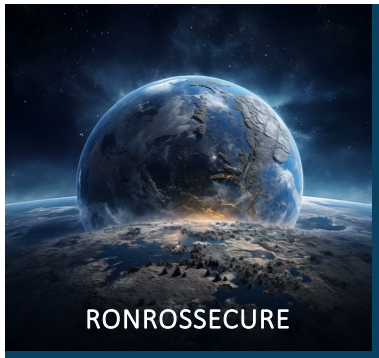
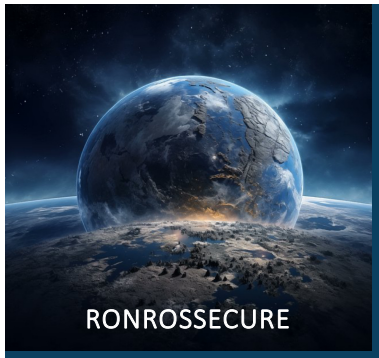
Trustworthy Secure Systems Engineering

An Imperative for National and Economic Security



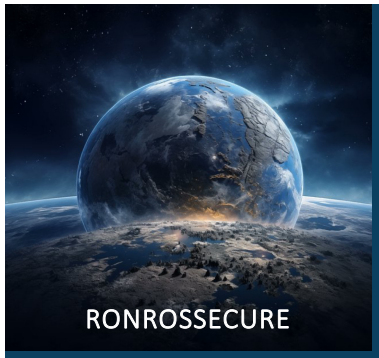
Current Landscape

- 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 has significant shortfalls



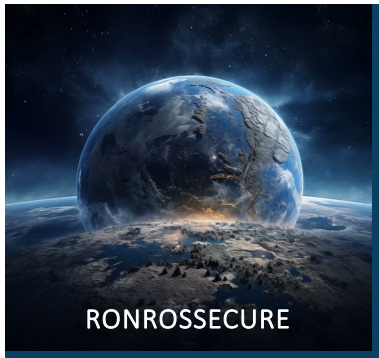
Threats to Modern Systems

- 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)



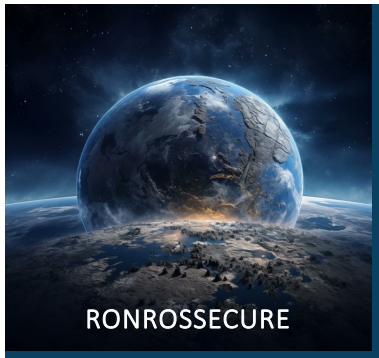
Generational and Institutional Cybersecurity Problems – Part 1

- 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



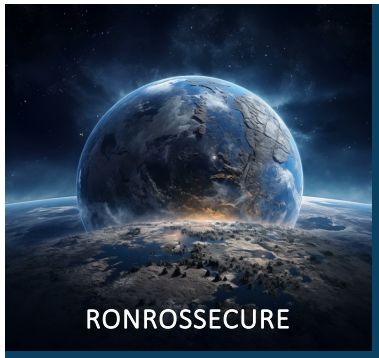
Generational and Institutional Cybersecurity Problems – Part 2

- 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



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.

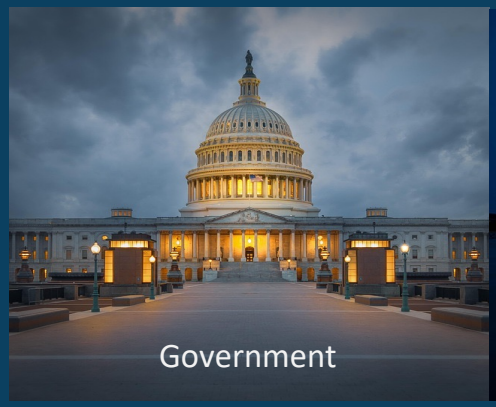


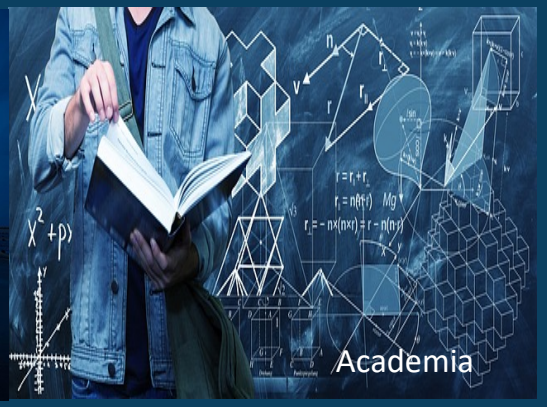
Great national challenges require great national solutions

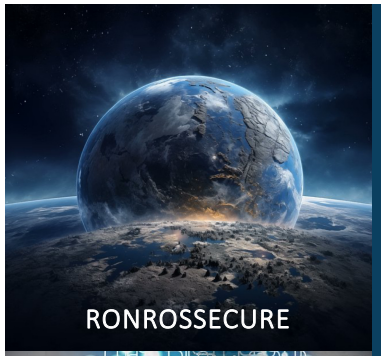
On September 12, 1962, President John F. Kennedy in one of his most memorable speeches, challenged the Nation with his bold moon landing proposal.

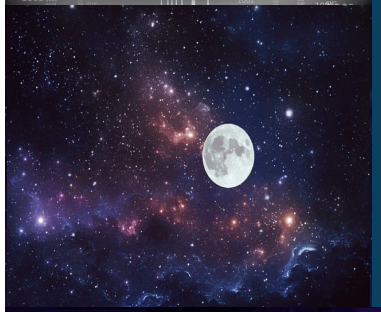
"We choose to go to the Moon in this decade and do the other things, not because they are easy, but because they are hard; because that goal will serve to organize and measure the best of our energies and skills, because that challenge is one that we are willing to accept, one we are unwilling to postpone,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

The Essential Partnership





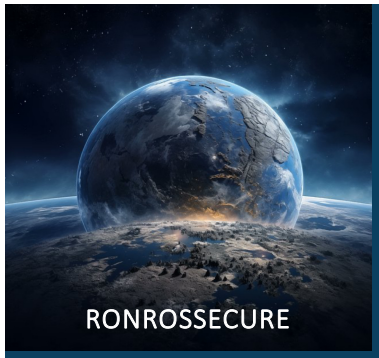




The Solution

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.



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

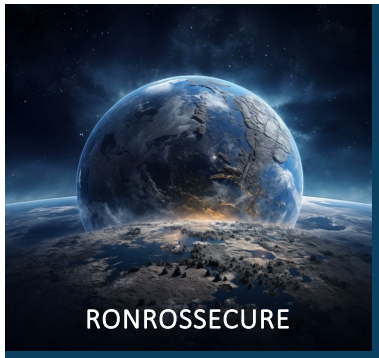
- Trustworthy Secure Systems Security Engineering (TSSE) knowledge, skills, and abilities
- Educational institution support of TSSE curricula programs
- TSSE internship programs in real world pilot projects and test beds

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

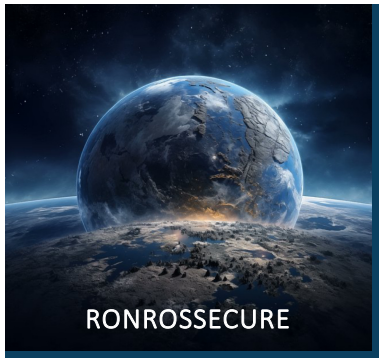
TECHNOLOGIES

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



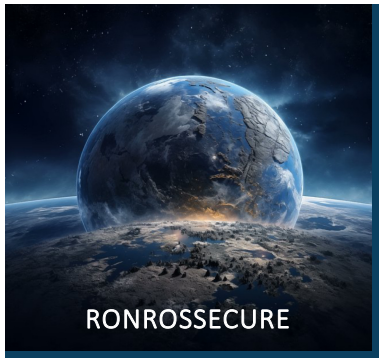
Why *Trustworthy* Secure?

- 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

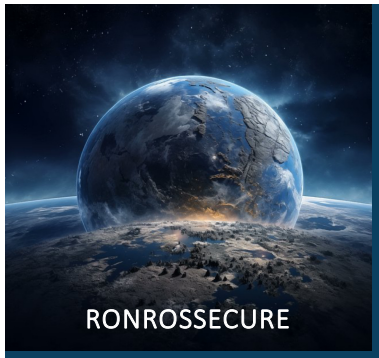
- Security is an emergent property of an engineered system like safety, reliability, and resilience
- Mission protection needs to guide and inform security requirements for functionality and assurance
- Protection needs focus on:
  - ✓ Ensuring predictable system performance under conditions of stress
  - ✓ 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

National Strategy, Laws, Directives, Executive Orders, Regulations, Policies

Government

Industry

Academia

Pillar 1
TSSE
Life Cycle
Processes
Methods

Pillar 2
TSSE
Principles
Concepts
Practices

Pillar 3
TSSE
Test Beds
Experiments
Pilots

Pillar 4
TSSE
Education
Talent
Incubators

Pillar 5
TSSE
Repository
Engineering
Artifacts

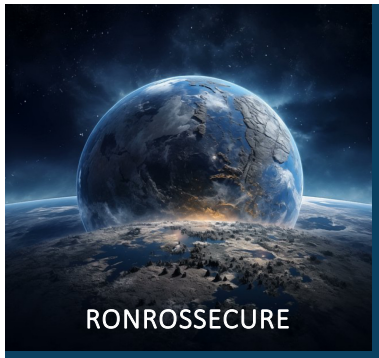
Pillar 6
TSSE
Technology
Transfer to
Partners

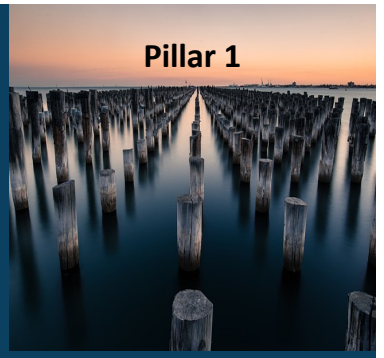
International Partners

Standards Bodies

Consortia

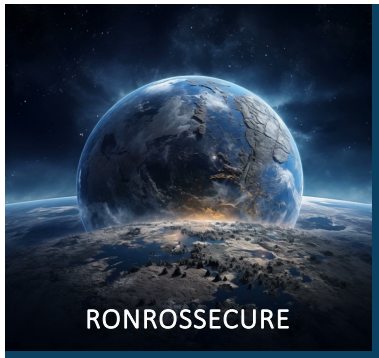
TRUSTWORTHY SECURE SYSTEM ENGINEERING FOUNDATION



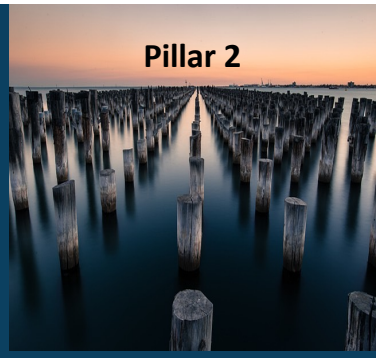


TSSE Life Cycle Processes

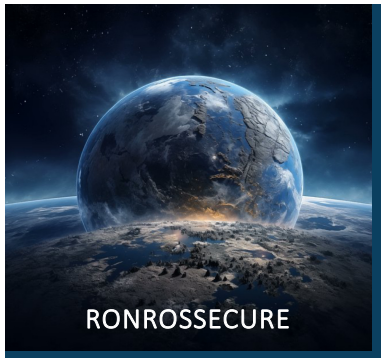
- ISO/IEC/IEEE 15288 Systems and software engineering — System life cycle processes
  https://www.iso.org/standard/81702.html
- NIST Special Publication 800-160, Volume 1 Engineering Trustworthy Secure Systems
  https://doi.org/10.6028/NIST.SP.800-160v1r1
- NIST Special Publication 800-160, Volume 2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



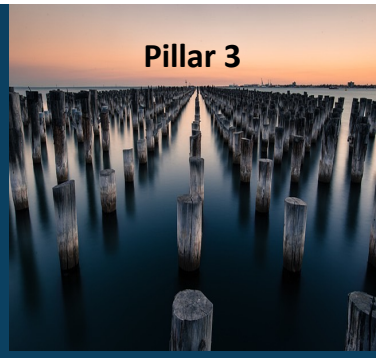
TSSE Principles and Concepts



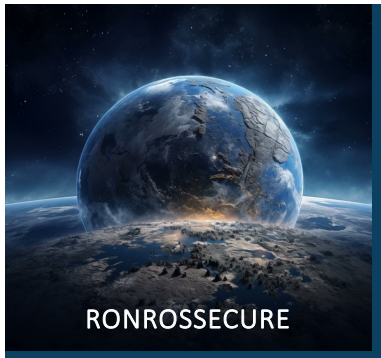
- TSSE Framework
  (Problem, Solution, Trustworthiness Contexts)
- Security Policy and Requirements
- System Security Concepts
  (Protection Needs, Assets, Loss Control, Consequences)
- Trustworthy Secure Design Principles
- Security Functionality and Assurance



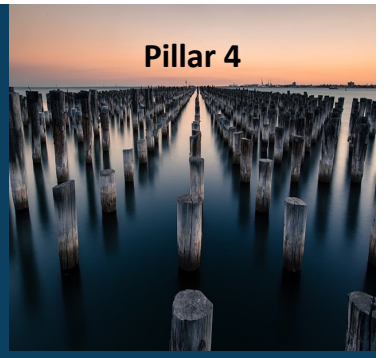
TSSE Test Beds and Pilot Projects



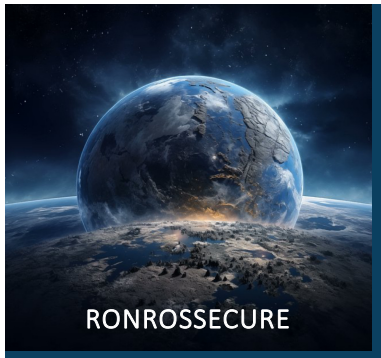
- Apply TSSE design principles, concepts, and practices to real-world systems engineering pilot projects, experiments, and test beds
- Include pilot projects, experiments, and test beds for vertical sectors such as defense, healthcare, space, finance, transportation, and communications
- Share results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



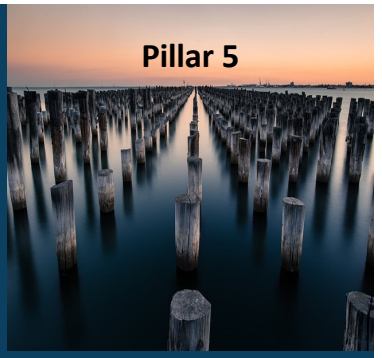
TSSE Talent Incubators



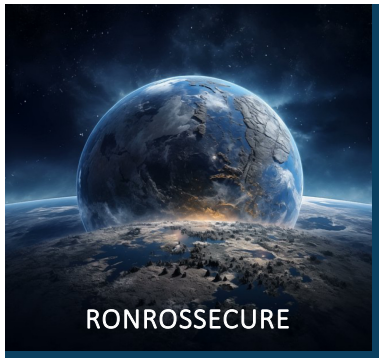
- Define TSSE knowledge, skills, and abilities for students pursuing systems engineering degrees
- Participate in TSSE experiments and pilot projects by providing students for internship programs
- Integrate TSSE principles, concepts, and practices into current engineering curricula
- Develop TSSE courses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



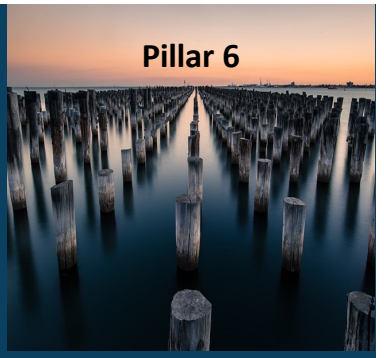
TSSE Repositories



- Collect TSSE experiment and pilot project results including lessons learned and 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

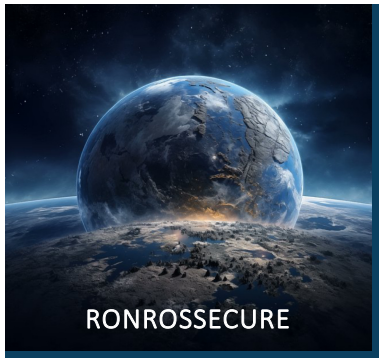


TSSE Technology Transfer



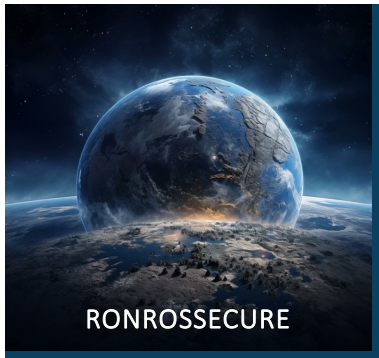
Share best practices with government, industry, academia, consortia, and international partners

- Help industry continuously improve its engineering processes for building trustworthy secure systems
- Help consortia standardize and promote TSSE best practices to improve engineering efficiency and effectiveness
- Help academic institutions improve curricula to ensure students have the requisite TSSE knowledge, skills, and abilities
- Help government create meaningful national strategies and policies that support, incentivize, and promote TSSE activities



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



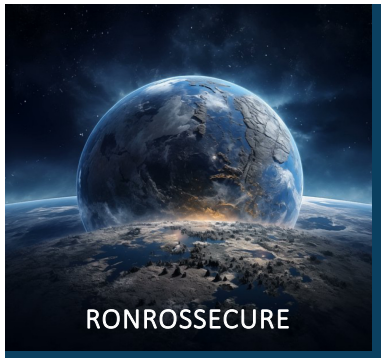
Conclusion

- 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

SunRISE Lessons 1 of 4

Bonus

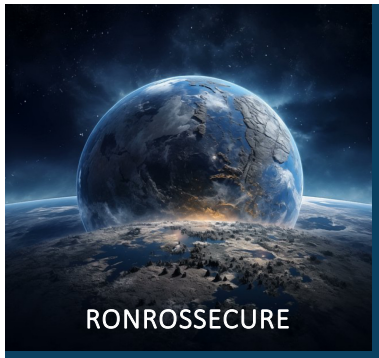
- Compliance-only approach can impede mission success
- Existing fault protection mechanisms also support defense against adversarial activity
- The SSE approach was critical to enable the rapid diagnosis of adversarial impact and consequence to mission objectives



SunRISE Lessons 2 of 4

Bonus

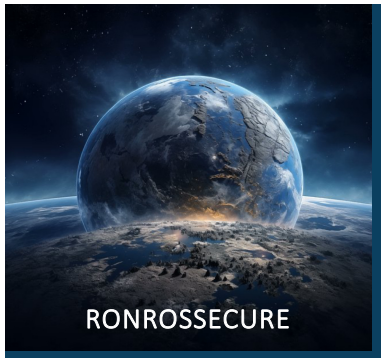
- The SSE approach is not free, but creates reusable artifacts (e.g., requirements, implementation, documents, etc.) that can aid in fulfilling compliance requirements and lowering costs for future projects
- SSE design principles/techniques when developed and implemented with mission engineers reduces the impact of protecting mission operations over a compliance-driven approach



SunRISE Lessons 3 of 4

Bonus

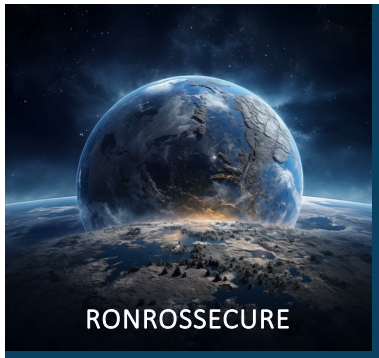
- Cyber-capable mission engineers were critical to engineering effective mission resilient systems
- Small, inexpensive modifications engineered into mission systems can result in significant resilience against cyber adversaries
- Security knowledgeable mission engineers create systems that are more amenable to impactful security improvements



SunRISE Lessons 4 of 4

Bonus

- The digital twin approach allows for a more accurate assessment of threats and their impacts than tabletop scenarios
- Tailored automated alerts of security events reduces the total time from detection to resolution
- The SSE approach results in a system based on security and mission requirements



Ron Ross

CEO, RONROSSECURE, LLC

ron@ronrossecure.com

Cybersecurity Advisory Services

https://ronrossecure.com