Federal Register Notice: 89 FR 78915, Federal Register :: Networking and Information Technology Research and Development Request for Information on Cyber-Physical Systems Resilience Research, September 26, 2024.

Request for Information on the National Cyber-Physical Systems Resilience Plan

Dr. Peter A. Beling

RFI Response: Cyber-Physical Systems Resilience R&D Plan

Methods in Support of Secure Cyber Resilient Engineering

October 25, 2024

Dr. Peter A. Beling
Virginia Tech National Security Institute

1. **Introduction**

This response presents a **systems-centric approach to cyber-physical system (CPS) resilience**, aligned with the principles of **Secure Cyber Resilient Engineering (SCRE)**. SCRE focuses on integrating cybersecurity and resilience into system engineering activities across the life cycle. Core methodologies and decision support tools for SCRE were developed for the Office of the Undersecretary for Defense, Research and Engineering (OUSD (R&E)) by researchers at Virginia Tech and Stevens Institute of Technology under the auspices of the Systems Engineering Research Center (SERC), a DoD funded University Affiliated Research Center (UARC) [1-8].

Our approach has as its goal the **design of adaptive systems** capable of maintaining operational integrity under adverse conditions. Through selective engineering of **resilience mechanisms**, we aim to preserve CPS mission capability in the face of evolving and unpredictable threats. Our approach relies on a **loss-driven and threat-agnostic** framework for system modeling and risk characterization. The approach also leverages SCRE's focus on **multi-criteria trade-offs and behavior prediction**, providing decision-makers with practical tools to assess and enhance resilience.

2. Secure Cyber Resilient Engineering

The proposed framework combines **system-theoretic modeling, behavior prediction, and dynamic control strategies** to enhance the ability of CPS to preserve essential mission function under adversities created by adversaries, equipment failure, environmental factors, or other causes.

Resilience is treated as a **control problem**, with the focus on maintaining **safe and adaptive control actions** under normal and degraded conditions. Predictive models, based on system behavior, are used to anticipate disruptions and trigger **automated recovery actions**. This predictive capacity aims to provide:

- **Dynamic Adaptation**: The system can **adjust control actions** in real time to maintain operational integrity.
- **Proactive Intervention**: Through real-time monitoring, the framework **identifies early indicators** of failure and preemptively initiates mitigation strategies.

2.1. Systems-Theoretic Process Analysis

At the core of this framework is **Systems-Theoretic Process Analysis (STPA)**, a modeling technique that extends traditional hazard analysis by focusing on how **control structures and unsafe interactions** can contribute to system losses [9]. Unlike conventional reliability models, which concentrate on individual component failures, STPA provides a holistic view of **system control dynamics**, focusing on:

- **Unacceptable Losses and Hazardous States**: The framework identifies critical outcomes to avoid, ensuring that system behavior aligns with mission objectives even under degraded conditions.
- **Control Structures and Interactions**: Control structures within the CPS are modeled to identify how actions (or lack thereof) can trigger hazardous states or lead to cascading failures.
- **Causal Pathways**: STPA traces the interactions between system components, revealing how unsafe control actions can result from human error, software flaws, or unforeseen interactions.

This **top-down, hazard-driven approach** aims to integrate safety, security, and resilience into the design from the outset. The approach also uses Systems Theoretic Process Assessment for Security (STPA-Sec), an extension of STPA with an emphasis on adversarial environments and the modeling of security controls.

The following section describes how SCRE employs STPA to drive the engineering of resilience.

2.2. The SCRE Approach to Threat-Agnostic Resilience by Design

Mission Aware is an approach to cyber resilience-by-design in which the system is engineered to include one or more resilience mechanisms. A basic design pattern for a resilience mechanism would feature processes, called sentinels, that monitor for the symptoms of loss of system functionality or mission capability. In the event of a detection, a sentinel will attempt to reconfigure the system by engaging alternate sets of hardware and software designed to permit continued operation despite the attack. Sentinel-based resilience finds most of its application in cyber-physical systems, such as vehicles and weapons systems, rather than in pure cyber and networking systems such as enterprise information technology systems.

There are many potential technical approaches to the fundamental resilience tasks of detection, mitigation, and recovery. Examples of concepts include:

- **Redundant and Diverse Systems:** Redundant components sourced from multiple suppliers mitigate risks associated with supply chain vulnerabilities and increase system robustness.
- **Configuration Hopping:** Physical and virtual control elements shift dynamically among redundant nodes, disrupting potential attack chains and reducing system predictability.
- **Voting Mechanisms and Graceful Degradation:** Redundant control systems use voting protocols to validate critical actions, while graceful degradation ensures continued functionality during partial failures.

See [11] for a broader discussion of design patterns for resilience mechanisms. All mechanisms share the characteristic that they come with costs in terms of money, complexity, or operational performance. The frameworks described below aim to address the problem of selecting where and how to engineering these mechanism into the system.

The *Framework for Operational Resilience in Engineering and System Test (FOREST)* is a process meta-model that provides a decomposition of operational resilience into the principal mechanisms, options, information flows, and decisions that arise as attacks and resilience responses play out in systems [3, 4]. The framework is composed of eight elements known as Testable Requirements Elicitation Elements (TREEs). The first TREE embodies the notion that there is active sensing to detect loss of function or abnormal behavior in the system. Next, the framework considers the task of isolating a detected incident and the use of diagnostic information as the basis for choosing resilience mode responses. From that point, FOREST expands to include consideration of operator response and supporting technology. For instance, would an operator have confidence in resilience solutions being employed, or does the system provide the operator with the ability to run tests or exercise control to help in gaining confidence in resilience modes of operation. Finally, the framework considers decision support and archiving to allow for post-event analysis and adaptation.

There is significant complexity to the TREEs, and many of them overlap intentionally and deal with issues at the intersections of technology, doctrine, and people. As their name implies, TREEs provide a view of resilience that supports the development of test plans, and associated measures and metrics, for both the technological and operational aspects of the system.

Cyber Resilient Requirements Methodology (CRRM) is a risk-based methodology for addressing cyber security during the design phase of a cyber-physical system [3, 4]. CRRM is intended for use by a multidisciplinary evaluation team reflecting knowledge of the systems operational context, the system design, the cyber threat, and the ability to effectively test:

- Systems Engineering (SE) Team: Responsible for managing the CRRM process and developing system designs and definitions that reflect requirements, objectives, constraints, and stakeholder concerns, and for ensuring the current system design, including resilience modes of operation, can be adequately tested.
- Blue Team: Composed of operationally-oriented members with experience using similar systems. The blue team is responsible for providing consequences and risks to the CRRM process.
- Red Team: Composed of cyber security experts and cyber-attack experts who will provide the likelihood of different attacks given the current system design and resilient solutions.
- Grey Team: Composed of system/operational test experts who will evaluate test and measurement approaches given the current system design and resilient solutions.

CRRM is an integration of the STPA-Sec and FOREST methodologies, based on a Mission Aware model-based systems engineering (MBSE) meta-model. CRRM helps stakeholders identify loss scenarios that are evaluated to determine remediation mechanisms which effectively minimize the loss using sentinel detection patterns and resilience architecture patterns. The architectural tradespace incorporates the set of sentinels and resilience modes which mitigate the most likely cyber-attacks which could lead to the highest priority mission losses that are within the programmatic constraints of development time and budget.

2.3. The Adversity Chain: Contrasting Prevention with Resilience

In the a canonical Cyber Kill Chain (see, e.g., [[12]) , the idea is to show the sequence of categories of activities that an adversary might follow in progressing toward culminating exploit, that we term a *loss scenario*. The loss scenario can be viewed as the point of final action or control on the part of the adversary. Prevention methods in conventional cybersecurity are designed to reduce the likelihood of a loss scenario being realized.

An alternate perspective, and one that is central to resilience, is to reason about how our system might operate given a loss scenario as a starting point. Following the concepts of STPA-sec, the Adversity Chain models a sequence of actions and system state transitions, starting from the state of the loss scenario and possibly ending in a loss state, as defined by the mission and system owners.

These two chain models can be used to frame the problem of achieving cyber survivability. Prevention techniques and practices are used to break Cyber Kill Chains; that is, prevention aims to keep an adversary from progressing to the loss scenario. Often, assurance cases, consisting of formal proofs or structured arguments, are developed to give the program confidence that kill chains are adequately accounted for in the system design. The fundamental perspective of resilience is that not all loss scenarios will be covered by an assurance case. Loss scenarios can and will occur. The CRRM methodology was created to address these cases. CRRM provides a structured approach to identifying key loss scenarios and architecting resilience mechanisms that will prevent the corresponding Adversity Chains from reaching the loss state. We call this “breaking the Adversity Chain”.

2.4. Multi-Criteria Trade-Offs for Resilience Design

A key feature of the SCRE approach is its ability to connect hazard analysis with the engineering trade space. Within the context of the Mission Aware MBSE meta-model, simulation can be used to identify trade-offs between performance, cost, complexity, and resilience. In system acquisition, these trade-offs are critical to setting of technical requirements for resilience mechanisms.

A quantification of mission/system resilience can be derived by indirectly measuring the effectiveness of sentinel scenarios and associated resilience mechanisms in breaking the Adversity Chain. In this context,

the behavior of the mission/system is defined through a set of state and activity specifications for each of the relevant system components, external actors, and environmental interactions. A mission profile is defined using a subjective probability distribution to specify the duration of an activity or state while probabilities are defined for action decision paths in the behavior specifications. The injection of adverse behavior, as defined by identified loss scenarios in CRRM/STPA, is accomplished using a test support system. The sentinel and associated scenarios provide mechanisms to vary the FOREST-based requirement parameters (e.g., sense time, resilience execution time) for associated loss scenarios to understand their effect on mission loss.

4. Current Research: Wind Energy and Critical Infrastructure

In our ongoing research, the Virginia Tech National Security Institute is applying the SCRE methodologies to two classes of use cases:

- **Wind Energy Farms**: Specifically, we are studying cyber resilience for offshore wind energy farms using a pilot site belonging to Dominion Energy. This effort includes collaboration with Stevens Institute of Technology and Old Dominion University in the context of a Center for Offshore Wind Energy, which has a security and resilience focus.
- **Critical Infrastructure Systems**: We are developing a model-based test-bed to represent another a broader class of distributed energy systems.

In the context of the use case, we are studying how SCRE could be enhanced through incorporation of ideas from related methodologies. SCRE provides a foundation for secure system engineering, while **Operational Technology Assurance (OTA)** principles address resilience within **nuclear and energy operations**. OTA, as defined by the DOE's National Nuclear Security Administration (NNSA), focuses on identifying and mitigating **cyber risks specific to OT environments**, such as safety systems, additive manufacturing, and processes that control physical operations.

The OTA framework emphasizes **continuous monitoring and operational assurance** to address risks across the entire system lifecycle, including supply chains and logistics. The integration of **OTA methodologies** with SCRE could enhance the use of **real-time control and physical system adaptation** in resilience engineering.

5. Recommendations for the National Cyber-Physical Systems Resilience R&D Plan

1. **Support the Integration of SCRE and related methodologies such as OTA in the systems engineering process**: Encourage research that aligns **engineering and resilience methodologies**, ensuring secure and adaptable systems.
2. **Develop Tools for Multi-Criteria Resilience Assessment**: Invest in tools that **balance performance, cost, and security** across cyber-physical systems and environments.
3. **Promote Cross-Sector Collaboration**: Engage stakeholders from both public and private sectors to ensure **scalable resilience strategies** aligned with real-world needs.
4. **Expand Early-Phase Threat Modeling and Verification**: Provide automated tools for **threat modeling and vulnerability assessment** during the system design phase to improve cost-efficiency.
5. **Invest in Workforce Development**: Equip engineers and operators with **training in viewing resilience as an engineering topic**, ensuring the next generation is prepared to architect, design, and implement resilient systems.

5. Conclusion

This response outlines a **comprehensive framework for secure cyber-resilient engineering**, combining the strengths of **SCRE and OTA** to address both engineering and operational challenges. By integrating

real-time monitoring, dynamic control strategies, and adaptive recovery mechanisms, the framework ensures that CPSs maintain mission-critical operations in the face of evolving threats.
We look forward to contributing to the **National Cyber-Physical Systems Resilience R&D Strategic Plan** and participating in efforts to advance the resilience of critical infrastructure across the nation.

References

1. Beling, P., Horowitz, B., Fleming, C., Adams, S., Bakirtzis, G., Carter, B., ... & Simon, B. (2019). *Model-Based Engineering for Functional Risk Assessment and Design of Cyber-Resilient Systems*. University of Virginia, Charlottesville, United States.
2. Horowitz, B., Beling, P., Fleming, C., Adams, S., Carter, B., Sherburne, T., ... & Mead, N. R. (2018). *Cybersecurity Requirements Methodology*. Stevens Institute of Technology, Hoboken, United States.
3. McDermott, T., Clifford, M. M., Sherburne, T., Horowitz, B., & Beling, P. A. (2022). Framework for Operational Resilience in Engineering and System Test (FOREST) Part I: Methodology – Responding to "Security as a Functional Requirement." *INSIGHT, 25*(2), 30–37. https://doi.org/10.xxxx/insight.2022.25.2.30
4. McDermott, T., Clifford, M. M., Sherburne, T., Horowitz, B., & Beling, P. A. (2022). Framework for Operational Resilience in Engineering and System Test (FOREST) Part II: Case Study – Responding to "Security as a Functional Requirement." *INSIGHT, 25*(2), 38–43. https://doi.org/10.xxxx/insight.2022.25.2.38
5. Beling, P., Horowitz, B., Fleming, C., Adams, S., Bakirtzis, G., Carter, B., Sherburne, T., Elks, C., Collins, A., & Simon, B. (2021). *Developmental Test and Evaluation (DTE&A) and Cyberattack Resilient Systems*. Stevens Institute of Technology, Hoboken, United States.
6. Carter, B., Adams, S., Bakirtzis, G., Sherburne, T., Beling, P., Horowitz, B., & Fleming, C. (2019). A Preliminary Design-Phase Security Methodology for Cyber–Physical Systems. *Systems, 7*(2), 21. https://doi.org/10.xxxx/systems.2019.7.2.21
7. Fleming, C. H., Elks, C., Bakirtzis, G., Adams, S., Carter, B., Beling, P., & Horowitz, B. (2021). Cyberphysical Security Through Resiliency: A Systems-Centric Approach. *Computer, 54*(6), 36–45. https://doi.org/10.xxxx/computer.2021.54.6.36
8. Horowitz, B., Beling, P., Fleming, C., Adams, S., Carter, B., Vemuru, K., Elks, C., Bakker, T., Cios, K., Bakirtzis, G., & Collins, A. (2017). *Security Engineering FY17 Systems-Aware Cybersecurity*. Stevens Institute of Technology, Hoboken, United States.
9. Leveson, N. G. (2004). A systems-theoretic Approach toSafety in Software-intensive Systems. *IEEE Transactions on Dependable and Secure Computing*, 1(1), 66-86.
10. Fleming, C. (2023). Introduction to STPA-Sec. *Systems Engineering for the Digital Age: Practitioner Perspective*s, 489-505.
11. Beling, P. A., Sherburne, T., & Horowitz, B. (2023). Case Study C: Sentinels for Cyber Resilience. In *Autonomous Intelligent Cyber Defense Agent (AICA) A Comprehensive Guide* (pp. 425-445). Cham: Springer International Publishing.
12. Naik, N., Jenkins, P., Grace, P., & Song, J. (2022, October). Comparing attack models for it systems: Lockheed martin's cyber kill chain, mitre att&ck framework and diamond model. In *2022 IEEE International Symposium on Systems Engineering (ISSE)* (pp. 1-7). IEEE.