Framework for Operational Resilience in Engineering and System Test (FOREST) Part I: Methodology – Responding to "Security as a Functional Requirement"

Tom McDermott, tmcdermo@stevens.edu; **Megan M. Clifford,** mcliffor@stevens.edu; **Tim Sherburne,** sherburne@vt.edu; **Barry Horowitz,** bh8e@virginia.edu; and **Peter A. Beling,** beling@vt.edu

ABSTRACT

An end-to-end methodology for addressing cyber resilience as a development and test philosophy in a system is described. Although focused on cybersecurity, the methodology applies to any resilience concerns and features of a system. Resilience is a functional characteristic of a system, requiring a process to evaluate the function of different aspects of a system under attack or disruption. The result of this process is a set of functional requirements and functional views of cyber resilience processes in a model-based systems engineering tool. The methodology consists of a meta-process model called the Framework for Operational Resilience in Engineering and System Test (FOREST) and a reference architecture metamodel called Mission Aware. In practice these are used to make security and related resilience decisions in capability development using a standard, risk-based approach for cybersecurity requirements development. Part I of this article describes the methodology and Part II presents its use in a case study of a fictional weapon system called Silverfish.

INTRODUCTION

The Department of Defense (DoD) is significantly increasing its efforts to address the rapidly growing operational risks associated with cyber-attacks and adverse actions by insiders. The concepts of system assurance and system resilience describe complementary approaches to managing these cyber risks. System assurance is the justified confidence that a system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle. System resilience is the capacity of a system to maintain or recover from unwanted loss of function. Assurance is a static property of the system as built, whereas resilience is a dynamic property of the system as designed into a set of behaviors.

Unlike system assurance, which by its nature requires a complete system design, the system resilience approach offers the promise that cyber risk can be considered early in the systems engineering process. Because of its definition in terms of system behavior, it should be possible to reason about systems resilience in terms of system functions in advance of a design. Digital engineering and model-based systems engineering (MBSE) are seeing increased applications in the conception, design, integration, verification, and validation (V&V) of mission-critical systems. However, systems engineering for operational and cyber resilience–from concept to system requirements to design–still lacks integrated modeling and dynamic simulation support. Transition to common standards, methods and processes, and tools and techniques are needed. Further development is needed on new metrics, methods, and tools for hazard

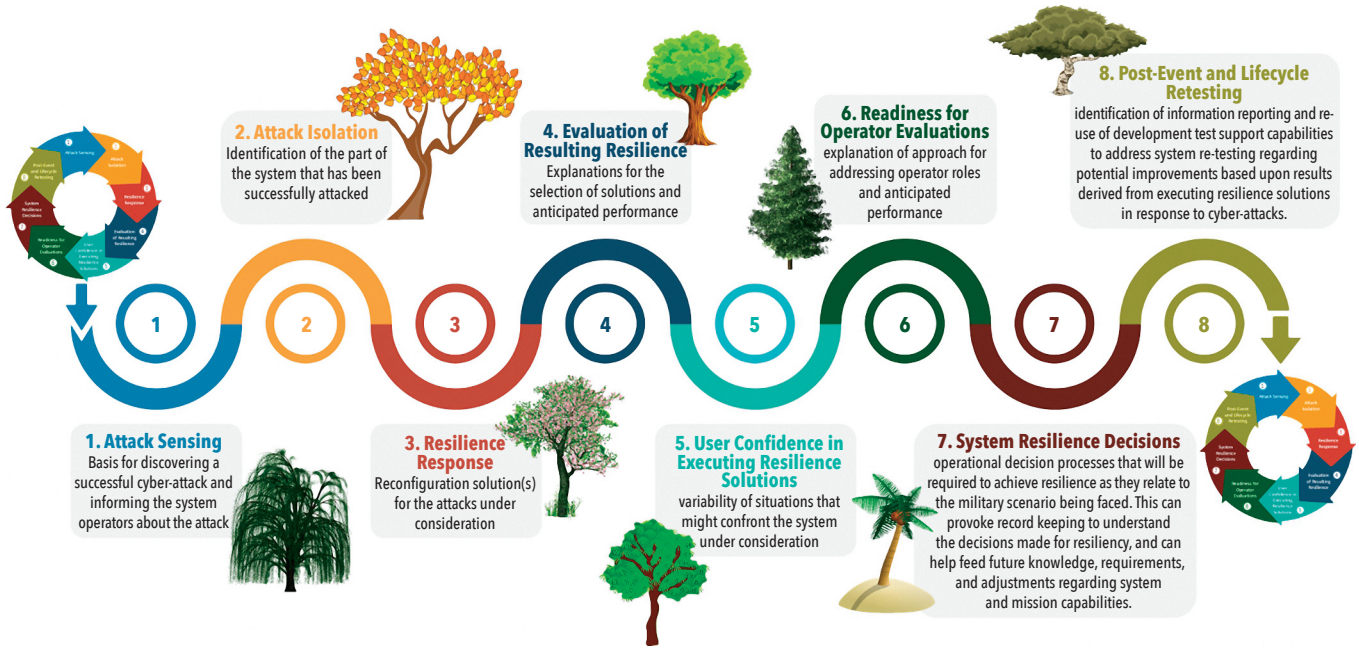

Figure 1. The FOREST metamodel showing the 8 TREEs (Beling et al. 2021)

mitigation. In the context of MBSE, it is essential that new approaches be found to support modeling system functions at the pre-design stages.

Cyber resilience also presents special challenges with regard to test and evaluation. Typically, system requirements can be specified in terms of technology function and can be tested through manipulation of the systems operational environment, controls, or inputs. Cyber resilience is a high-level property and lacks commonly accepted definitions in terms of system requirements and associated test metrics. Moreover, by design, resilience behaviors are exhibited only when the system has lost critical functions. The implication is that the test and evaluation of requirements for operational resilience will involve creating, emulating, or reasoning about the internal systems states that might result from successful attacks. The implication is that the definition, development, and test and evaluation of requirements for operational resilience will involve creating and emulating functional models, then reasoning about the internal systems states that might result from disruptions caused by system failures or successful attacks.

For several years, a principal focus of the Trusted Systems thrust within the Systems Engineering Research Center (SERC) has been the development of methods and tools that support functional system design for cyber resilience in cyber physical systems. The objective of these efforts was to develop and transition an end-to-end systems engineering methodology intended to close the loop between mission level resilience analysis and system development activities using digital engineering and MBSE oriented processes. The completed methodology consists of a meta-process model called the Framework for Operational Resilience in Engineering and Systems Test (FOREST) and a reference architecture meta-model called Mission Aware. In practice these models are used to make security and related resilience decisions in capability development using a standard, risk-based approach. In particular, the methods, practices, and tools assess the quality of different requirements and design solutions based on safety and security risks in the presence of a determined cyberattack. The FOREST and Mission Aware frameworks support the derivation of measures and metrics that could be the basis for test and evaluation in a rigorous systems engineering process. Additionally, they can provide developers with insights that would readily support the development of testable requirements for operational resilience and that would promote the design of systems with some immunity to new as yet unknown vulnerabilities and threat tactics.

FRAMEWORK FOR OPERATIONAL RESILIENCE IN ENGINEERING AND SYSTEM TEST (FOREST)

The Framework for Operational Resilience in Engineering and System Test (FOREST) is a meta-process model for designing and evaluating resilience characteristics in systems. It is primarily focused on cyber resilience but applies generally to any resilience characteristics of a system. FOREST contains eight meta-process elements, called Testable Requirements Elicitation Elements (TREEs) as shown in Figure 1.

FOREST applies at every stage of the systems engineering process and throughout the lifecycle. The framework is meant to be a reusable, repeatable, and practical framework that calls for system designers to describe a system's operational resilience design in a designated, partitioned manner that aligns with resilience requirements and directly relates to the development of associated test concepts and performance metrics. It aims to normalize expectations, enhance quality, and create reuse opportunities associated with the development of requirements and test plans related to achieving operational resilience.

MISSION AWARE CYBER RESILIENCE AND THE CYBER SECURITY REQUIREMENTS METHODOLOGY

While FOREST provides a decomposition of resilience and structure for setting requirements and test activities, it does not include tools or methods to fully support the architecting, design, or engineering aspects of operational resilience. FOREST builds on a meta-model called Mission Aware (MA) which is intended to describe resilience features and decisions in a Model-Based Systems Engineering tool. Figure 2 is a conceptual view of an MA architecture. MA provides a reference architecture for operational resilience of cyber-physical systems in response to security and other potential disruptions. FOREST, the MA meta-model, and the Cyber Security Requirement Methodology (CSRM), a companion methodology for loss-driven resilience design, provide an end-to-end

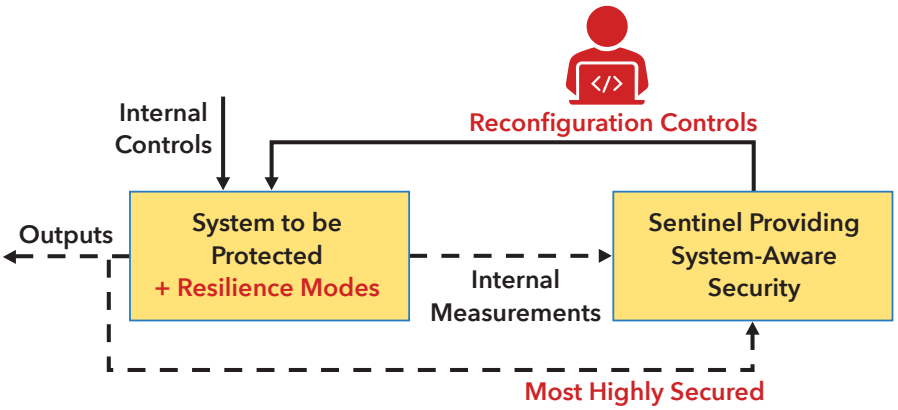

Figure 2. The mission aware resilience pattern (Horowitz et al. 2017)

framework for security as a functional requirement in the systems engineering process.

The primary feature of the MA architecture is a *sentinel* (TREE 1) that monitors the system or mission that is being protected, detects abnormal behavior or other signs of loss of function, alerts system users or mission owners to detected loss of function, and has the capability to switch the system or mission to a resilient mode of operation (TREEs 2 & 3). The resulting behavior is a distinct and separate method of operation for a component, device, or system based upon a diverse redundancy or other design pattern. Resilient modes of operation are designed so that the system can still meet its primary objectives, though with possible loss of operational performance. A *sentinel* should be designed with simplicity in mind so that it is more easily secured.

The FOREST meta-process rests on the use of MA and supporting concepts as the basis for considering the principal options, information flows, and decisions that arise as attacks and resilience responses play out in systems. In our approach, MBSE and the Systems Theoretic Process Assessment for Security (STPA-Sec) are used as a means of standardizing language and concepts across requirements, design, test and evaluation, operational resilience, and systems engineering throughout the lifecycle. These are combined in a standard Cyber Security Requirement Methodology (CSRM) which is used to engage stakeholders in the resilience definition process.

LOSS IDENTIFICATION WITH STPA

Systems Theoretic Accident Model and Processes (STAMP) is a safety analysis method that is based on causation (Young and Leveson, 2014). Causation in STAMP is modeled through hierarchical control, which models each level of a system as a control process, where unsafe control actions can occur. This layered approach to safety has the advantage that unsafe control actions at each level percolate upwards or downwards in the hierarchy that in turn provides a notion of consequence within the safety model. STAMP works in contrast to linear failure modes, where unsafe actions form a chain of events. In STAMP, by contrast, safety violations emerge from the interacting control layers governing the system. Specifically, STAMP is a hazard analysis technique based on an extended model of accident causation. In addition to component failures, STAMP assumes that accidents can also be caused by unsafe interactions of system components, none of which may have individually failed. For this reason, STAMP further asserts that emergent properties, for example safety and security, cannot be assured by examining subsystems in isolation. STPA (System Theoretic Process Analysis) is one flavor of STAMP modeling that is primarily used to proactively identify hazardous conditions and states. STPA-Sec is an extension of STPA with the intention of transitioning the benefits of loss-oriented safety assessment to security (Young and Porada 2017).

The hierarchical control notion within STAMP is a congruent idea with a number of MBSE block diagrams, such as architectural or behavioral diagrams, because they can be augmented to model unsafe control actions in addition to the control system that define the behavior and architecture of the system. Furthermore, MBSE is based on the same hierarchical notion, namely, that systems can be modeled through different views that reside in different levels of abstraction. STAMP

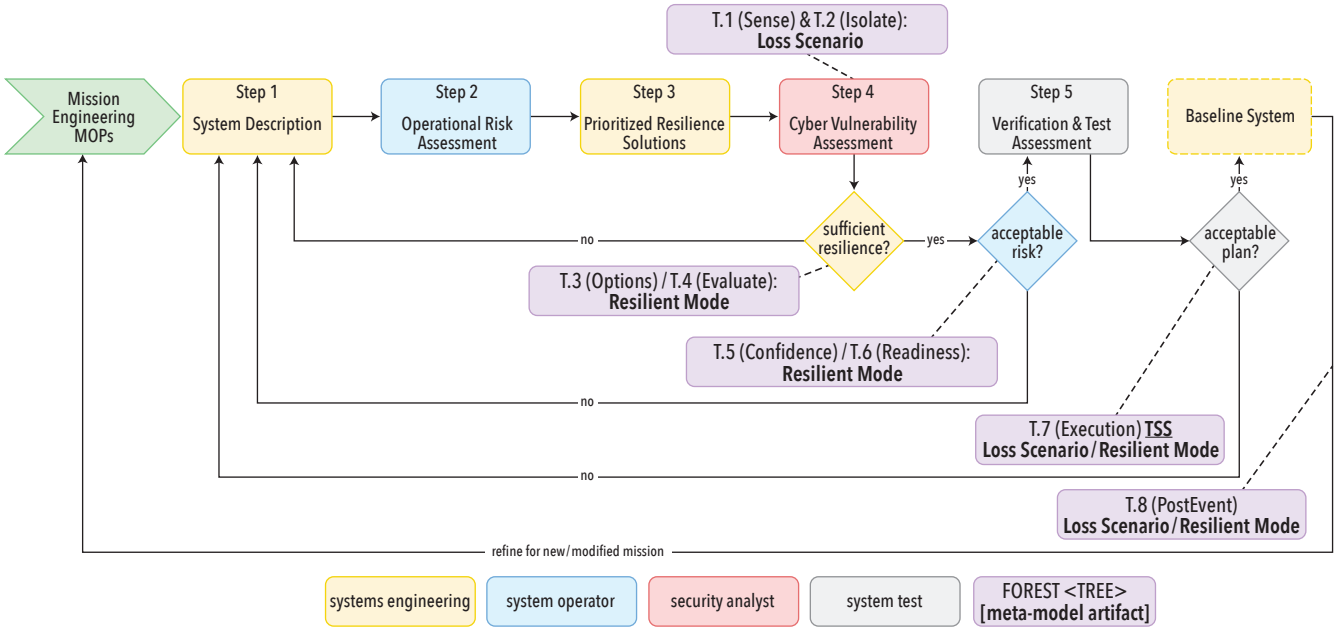

Figure 3. The cyber security requirements methodology (Beling et al. 2021)

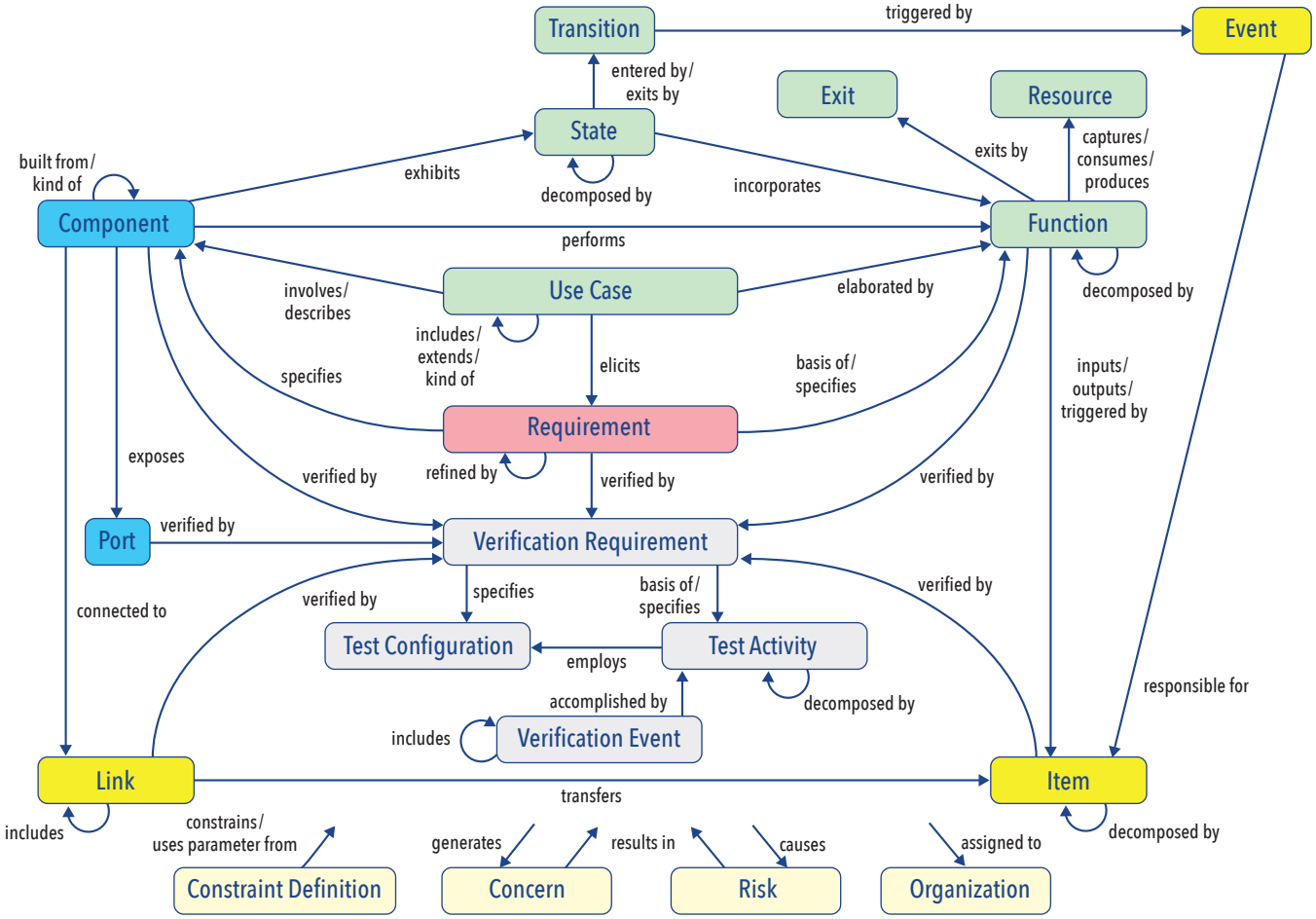

Figure 4. The Vitech systems meta-model (Vitech 2021)

entities are, therefore, an important view of safety and security.

CYBER SECURITY REQUIREMENT METHODOLOGY

CSRM is a risk-based methodology for addressing cyber security during the design phase of a cyber-physical system and utilizes teams of system owners and experts from a wide range of domains. The CSRM process steps are shown in Figure 3.

CSRM is used by a multidisciplinary evaluation team reflecting knowledge of the systems operational context, the system design, and the cyber threat:

1. Systems Engineering (SE) Team – responsible for managing the CSRM 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.
2. Blue Team – composed of operationally-oriented members with experience using similar systems. The blue team is responsible for providing consequences and risks to the CSRM process.
3. 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.

A meta-process and meta-model were developed to support the derivation of measures and metrics that could be the basis for developmental and test of security and resilience properties in the systems engineering process. These provide developers with insights that would readily support the development of testable requirements for operational resilience and that would promote the design of systems with some immunity to new vulnerabilities and threat tactics. Finally, the framework was intended to be tool-agnostic and support use in conjunction with a variety of risk management and design frameworks for operational resilience.

MISSION AWARE MBSE META-MODEL

Mission Aware builds upon a metamodel from the Vitech corporation (Long and Scott 2011). The Vitech metamodel is publicly available and is well-aligned with the SysMLv2 requirement for precise systems engineering semantics. The augmentations to this industry metamodel include a number of enti'=[[ties and interactions to address safety, security, and resilience, which are necessary for the design and deployment of cyber-physical systems. Specifically, the MBSE metamodel represents critical systems engineering concepts and their interrelationships spanning requirements, behavior, architecture, and testing (Figure 4). This integrated model presents a high-level view of not only the ultimate specification of a system, but also the journey to that specification – concerns opened and closed, risks identified and managed. As a mechanism for managing system complexity, the metamodel supports an incremental, layered approach via the consistent relationship across requirements, behavior, architecture, and test domains. There are three primary benefits to using a metamodel: holding the various methods of documentation in alignment, which will reduce workload in maintaining the documents and prevent errors; enforcing a set structure to remain in compliance with systems engineering best practices; and connecting performance metrics like safety, security, and resilience with the system design process.

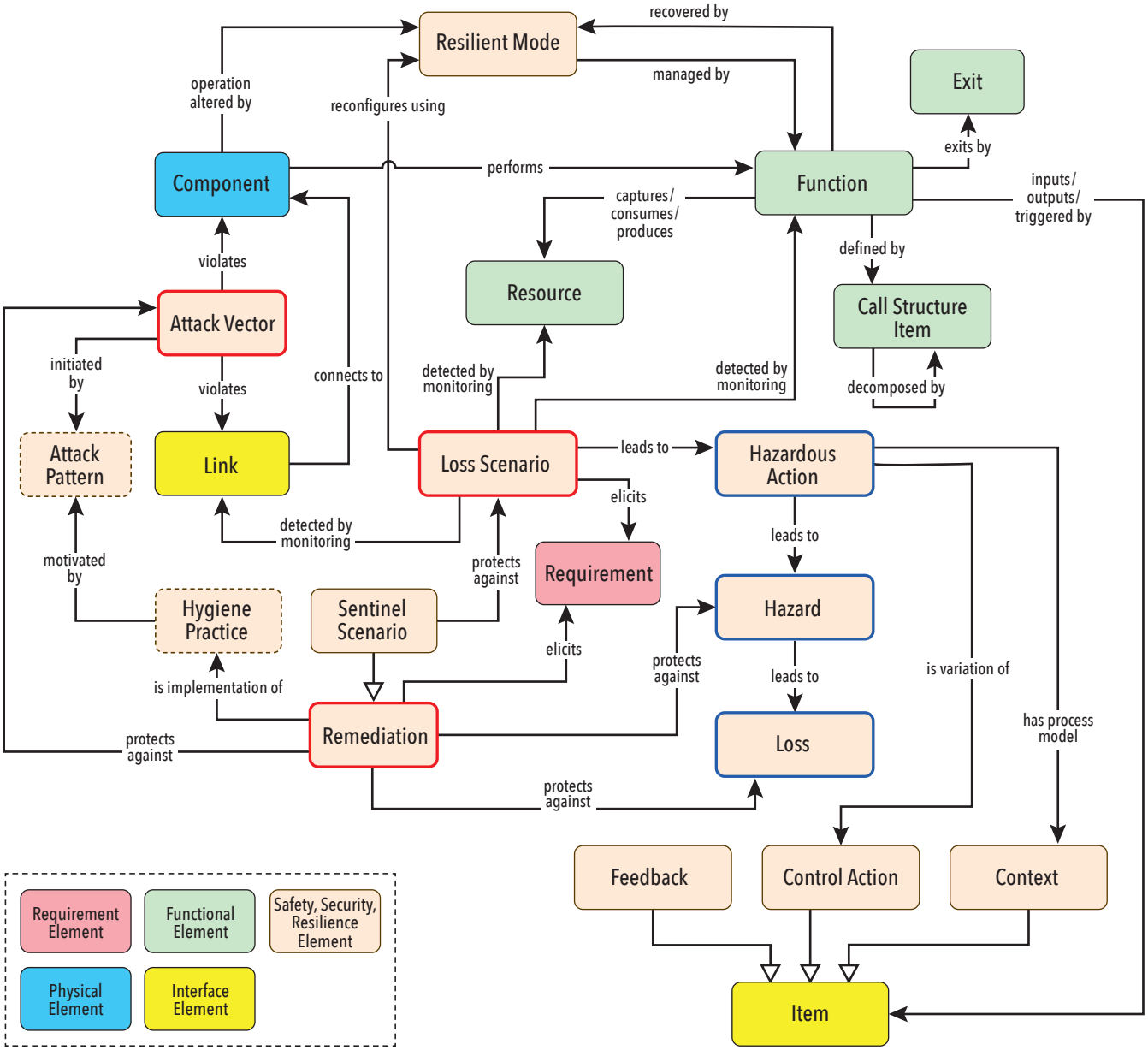

Figure 5. The mission-aware meta-model (Beling et al. 2021)

The MA MBSE metamodel (Figure 5) extends the Vitech model to include concepts from the MA approach to resilient system design. Specifically, the extended meta-model includes resilient modes and extends the behavior with consideration for loss scenarios. Table 1 provides a detailed description of the extensions.

REQUIREMENTS SPECIFICATION USING FOREST

A key concern of any systems engineering model is an understanding of the system's architecture, including its components and physical links which connect them. Components may include hardware elements, software elements, external systems, and/or humans. Of equal concern is an understating of the expected behavior of the system being modeled. Behavior elements include functions, their input and output items as well as any resources provided or consumed. The call structure provides an understanding of behavior control flow including looping, parallel execution, path selection with exit choices, and more. Components perform functions thereby linking the physical architecture with the behavior model. These standard system modeling entities define the engineering process itself and provide structure to the essential design artifact of the system under design.

However, MBSE entities and relationships do not address "-ilities" necessary for the design of cyber-physical systems (CPS). Additional entities for safety, security, and resilience that are specifically related to CPS must be added to provide evidence for the correct behavior of CPS. Such performance metrics are defined in the augmentation of the CPS metamodel and related to already standardized MBSE entities with properly defined relationships. This is an important addition to the standard metamodel provided by Vitech. By adding structure to performance metrics systems engineers are able to design CPS that provide operational assurance in the face of hazards or security violations.

Traditional system performance metrics are captured as parameters of links, components, and/or functions with a constraint definition defining the

Table 1. MBSE metamodel augmentations for mission aware

Element	Entity	Description
Control Structure	Control Action	A controller provides control actions to control some process and to enforce constraints on the behavior of the controlled process.
	Feedback	Process models may be updated in part by feedback used to observe the controlled process.
	Context	The set of process model variables and values.
Risk	Loss	A loss involves something of value to stakeholders. Losses may include a loss of human life or human injury, property damage, environmental pollution, loss of mission, loss of reputation, loss or leak of sensitive information, or any other loss that is unacceptable to the stakeholders.
	Hazard	A hazard is a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss.
	Hazardous Action	A hazardous action is a control action that, in a particular context and worst-case environment, will lead to a hazard.
Vulnerability	Loss Scenario	A loss scenario describes the causal factors that can lead to the unsafe control and to hazards. Two types of loss scenarios must be considered: a) Why would unsafe control actions occur? b) Why would control actions be improperly executed or not executed, leading to hazards?
	Remediation	The hygiene practice or resilience mechanism to protect against a loss, hazard, loss scenario, or attack vector.
Mission Aware	Attack Pattern	An inventory (check list) of potential paths or means by which a hacker can gain access to a computer or network server in order to deliver a payload or malicious outcome. Attack patterns enable hackers to exploit system vulnerabilities, including the human element.
	Attack Vector	3-way associative class between attack pattern, component / link, and remediation which tracks likelihood and severity of the attack pattern after remediation.
	Hygiene Practice	A routine practice (check list) of basic security capabilities to reduce cyber risks due to common or pervasive threats.
	Resilient Mode	A configuration of a target system that remediates one or more loss scenarios.
	Sentinel	A highly secure subsystem responsible for monitoring and reconfiguration of resilient modes for a target system.

equations and relationships between individual entities. Consideration of safety, security and resilience performance metrics require augmentation of the standard MBSE metamodel with additional concepts to capture both an operational risk perspective and an adversarial attacker perspective (Table 1).

Safety and security often require specification of system behavior as a set of feedback control loops. As such, specializations of control action and feedback are provided as subtypes of the standard function input output item. While this phraseology is borrowed from STAMP, it applies to a large number of safety and security methods. STAMP in some sense distills any general framework for "-ilities" at a higher abstraction level – by leveraging notions of uncontrolled actions and control hierarchy – that is suited for use in a metamodel. Specifically, losses, hazards, and hazardous actions are captured and related (by means of leads to) as part of a methodical operational risk assessment process. Additionally, explicit associations are captured to understand an unsafe action as a variation of a specific control action with the process model system state that provides the context for the control action to become unsafe, which is borrowed from the domain of control theory and governs all CPS to some extent.

An important step in assessing any performance metric is to first identify loss scenarios which can lead to unsafe actions. These loss scenarios are the complement of the stakeholder requirements or otherwise define the mission of the system. In the domain of CPS, unsafe behavior and security violations are intertwined, meaning that an attacker could transition the system to a hazardous state. To augment the safety loss scenarios, databases, for example MITRE CAPEC (Barnum, 2008), which contain attack patterns, are consulted. The metamodel relates the notion of loss scenario with the notion of recovery and resilience by identifying how a sentinel, which is a type of remediation, could protect against

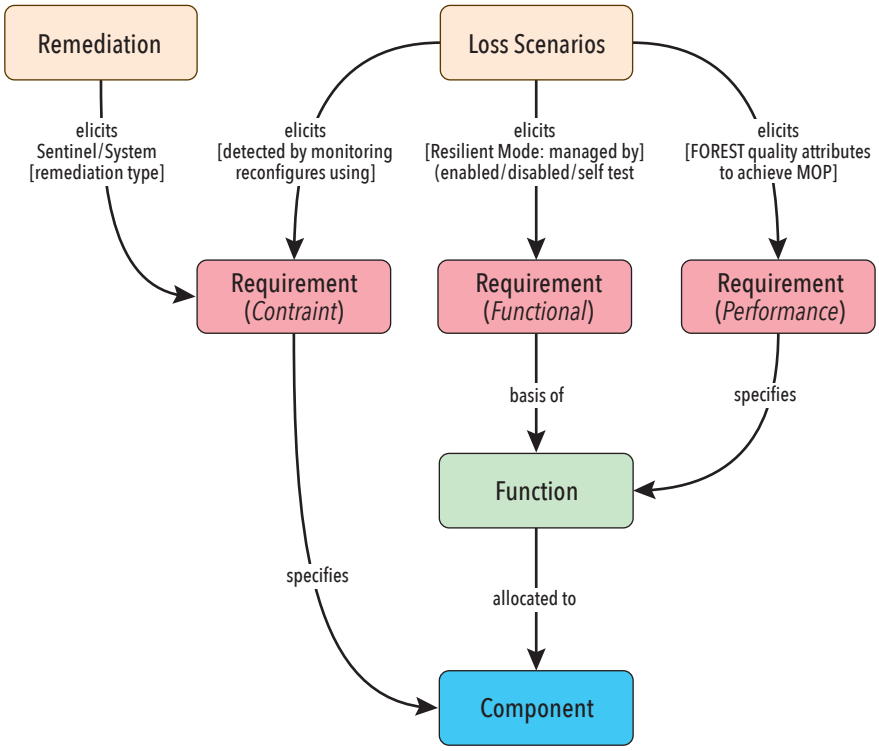

Figure 6. The mission-aware meta-model (Beling et al 2021)

Table 2. Relationships between system quality attributes and FOREST TREEs (Beling et al 2021)

✓ System Measure ✓ Operator Rating ☑ Development Consideration

Quality Attribute	T.1: Sense	T.2: Isolate	T.3: Options	T.4: Evaluate	T.5: Confidence	T.6: Readiness	T.7: Execution	T.8: PostEvent
accuracy	✓	✓						
adaptability						✓		
affordability								☑
availability				✓		✓		
composability			✓					☑
extensibility								☑
failure transparency				✓				
adaptability					✓			
predictability					✓			
recoverability				✓				
repeatability					✓			
safety			✓					
stability							✓	
survivability						✓		
testability	✓						✓	☑
timeliness	✓	✓		✓	✓	✓	✓	☑
usability				✓				

the loss by first indicating how it can be detected by monitoring a link, resource or function and then how the system reconfigures using a specific resilient mode.

The identification of Loss Scenarios and Remediations enables elicitation (Figure 6) of various types of System Requirements:

- *Constraints*
  - that provide Sentinel functions
  - that enable System Monitoring by a Sentinel
  - that provide System Resilient Modes
- *Functions* – that enable System Management (enable/disable/self-test) of Resilient Modes
- *Performanc* – that bound FOREST quality attributes that achieve Mission MOPs

We provide a set of System Quality Attributes (-ilities) for the FOREST TREE steps (Table 2). The quality attributes are used as an instrument to evaluate cyber resilience system design choices and as validation criteria during system test. As noted, some quality attributes are directly *measurable* by the system, some are *rated* by the operators of the system, and others are *considerations* for system development teams by illustrating the system limitations.

CONCLUSIONS

This Part introduced the framework and methods: FOREST as a process model, the MA metamodel as a reusable MBSE pattern, and STPA-Sec and CSRM as activity models in an SE process. The framework provides a decomposition of function and structure focused on resilience and in particular resilience to cybersecurity threats. It is meant to be considered at all stages of systems development and acquisition. The methods can be integrated into a standard systems security engineering (SSE) process beginning with tabletop analysis exercises, progressing to requirements and functional architecture definition, then to design and test, and finally to developmental and operational test and evaluation.

Part II presents the use of FOREST and its companion methodologies in a case study of a fictional weapon system called Silverfish, using a walk through the methods as would be accomplished in full SSE process. ■

REFERENCES

- Barnum, M.S., 2008. Common Attack Pattern Enumeration and Classification (CAPEC) Schema.
- Beling, P., Horowitz, B., Fleming, C., Adams, S., Bakirtzis, G., Carter, B., Sherburne, T., Elks, C., Collins, A. and Simon, B., 2019. *Model-based engineering for functional risk assessment and design of cyber resilient systems*. University of Virginia Charlottesville United States.
- Beling, P., Horowitz, B., Fleming, C., Adams, S., Bakirtzis, G., Carter, B., Sherburne, T., Elks, C., Collins, A. and Simon, B., 2021. Developmental Test and Evaluation (DTE&A) and Cyberattack Resilient Systems, Stevens Institute of Technology Hoboken United States.
- Carter, B., Adams, S., Bakirtzis, G., Sherburne, T., Beling, P., Horowitz, B. and Fleming, C., 2019. A preliminary design-phase security methodology for cyber–physical systems. *Systems*, 7(2), p.21.
- Fleming, C.H., Elks, C., Bakirtzis, G., Adams, S., Carter, B., Beling, P. and Horowitz, B., 2021. Cyberphysical Security Through Resiliency: A Systems-Centric Approach. *Computer, 54*(6), pp.36-45.
- Horowitz, B., Beling, P., Fleming, C., Adams, S., Carter, B., Vemuru, K., Elks, C., Bakker, T., Cios, K., Bakirtzis, G. and Collins, A., 2017. *Security engineering fy17 systems aware cybersecurity*. Stevens Institute of Technology Hoboken United States.
- Horowitz, B., Beling, P., Fleming, C., Adams, S., Carter, B., Sherburne, T., Elks, C., Bakirtzis, G., Shull, F. and Mead, N.R., 2018. Cyber security requirements methodology. Stevens Institute of Technology Hoboken United States.
- Long, D. and Scott, Z., 2011. *A primer for model-based systems engineering*. Lulu. com.
- Young, W. and Leveson, N.G., 2014. An integrated approach to safety and security based on systems theory. *Communications of the ACM*, 57(2), pp.31-35.
- Young, W. and Porada, R., 2017, March. System-theoretic process analysis for security (STPA-SEC): Cyber security and STPA. In *2017 STAMP Conference*.

ABOUT THE AUTHORS

Tom McDermott serves as the Deputy Director and Chief Technology Officer of the Systems Engineering Research Center (SERC) at Stevens Institute of Technology in Hoboken, NJ. The SERC is a University Affiliated Research Center sponsored by the Office of the Secretary of Defense for Research and Engineering. With the SERC he develops new research strategies and is leading research on Digital Engineering transformation, education, security, and artificial intelligence applications. Mr. McDermott also teaches system architecture concepts, systems thinking and decision making, and engineering leadership. He is a lecturer in Georgia Tech's Professional Education college, where he leads a masters level course on systems engineering leadership and offers several continuing education short courses. He consults with several organizations on enterprise modeling for transformational change, and often serves as a systems engineering expert on government major program reviews. He currently serves on the INCOSE Board of Directors as Director of Strategic Integration.

Megan M. Clifford is a Research Associate and Engineer at Stevens Institute of Technology. She works on various research projects with a specific interest in systems assurance, cyber-physical systems, and programs with national and global significance. She previously worked on the leadership team as the Chief of Staff and Program Operations for the Systems Engineering Research Center (SERC), was the Director of Industry and Government Relations to the Center for Complex Systems and Enterprises (CCSE), and held several different positions, including Systems Engineer, at Mosto Technologies while working on the New York City steam distribution system.

Tim Sherburne is a research associate in the Intelligent System Division of the Virginia Tech National Security Institute. Sherburne was previously a member of the systems engineering staff at the University of Virginia supporting Mission Aware research through rapid prototyping of cyber resilient solutions and model-based systems engineering (MBSE) specifications. Prior to joining the University of Virginia, he worked at Motorola Solutions in various Software Development and Systems Engineering roles defining and building mission critical public safety communications systems.

Barry M. Horowitz held the Munster Professorship in Systems Engineering at the University of Virginia, prior to his retirement in May 2021. His research interests include system architecture and design.

Peter A. Beling is a professor in the Grado Department of Industrial and Systems Engineering and associate director of the Intelligent Systems Division in the Virginia Tech National Security Institute. Dr. Beling's research interests lie at the intersections of systems engineering and artificial intelligence (AI) and include AI adoption, reinforcement learning, transfer learning, and digital engineering. He has contributed extensively to the development of methodologies and tools in support of cyber resilience in military systems. He serves on the Research Council of the Systems Engineering Research Center (SERC), a University Affiliated Research Center for the Department of Defense.