A Demonstration of MBSEsec Applied to Securing Cyber Physical System Communications

Gabe Salinger, Colorado State University

Trae Span, Colorado State University

Jeremy Daily, Colorado State University

Colorado State University

Presentation overview

- Problem Overview & Motivation
- Research Question & Tasks
- Approach
- MBSE Method Overview
- Implementation of MBSEsec
- Recommendations & Conclusions

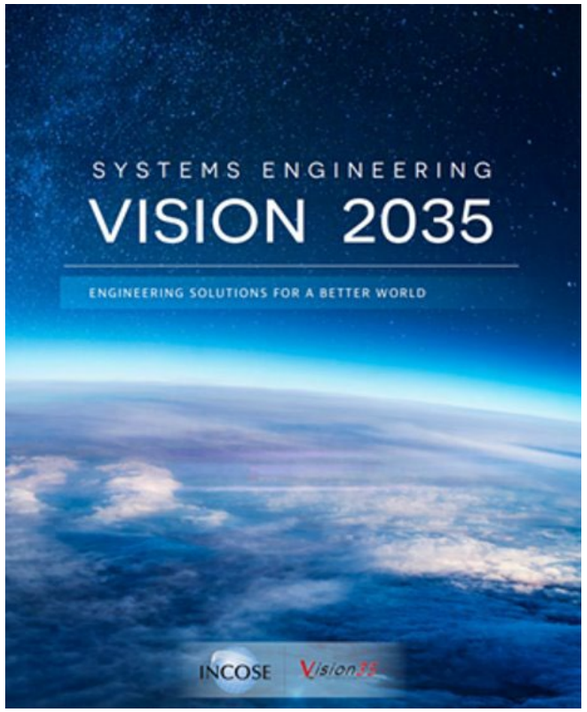
Problem Overview

- Vehicle security has become an underrepresented and important factor in the cybersecurity domain
  - New exploits have been discovered and validated in MHD truck networks [1],[2]
- The Department of Defense has highlighted the need for cyber-physical system design that employs digital engineering tools [3]
- Acknowledged need to improve Cybersecurity by Design
  - Cybersecurity is an emergent property
- The complexity of modern systems requires a well documented process with effective traceability and iteration capabilities

Systems Engineering must play a key role in secure system design

Research Motivation

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



https://www.incose.org/2023_redesign/publications/se-vision-2035

Understanding the System of Interest: **J1939 Protocol**

Transport Protocol

Electronic Control Unit (ECU)

Transport Layer Networking Specifications SAE J1939/21

Controller Area Network (CAN)

Application

J1939 ↔ **ARINC-825-4**

MIL STD 1553

CAN

Physical Network (Wires)

Simulated in SysML

Request Overload → Depletion of traffic from target ECU

Connection Exhaustion → Denial of connections to target ECU

SAE INTERNATIONAL

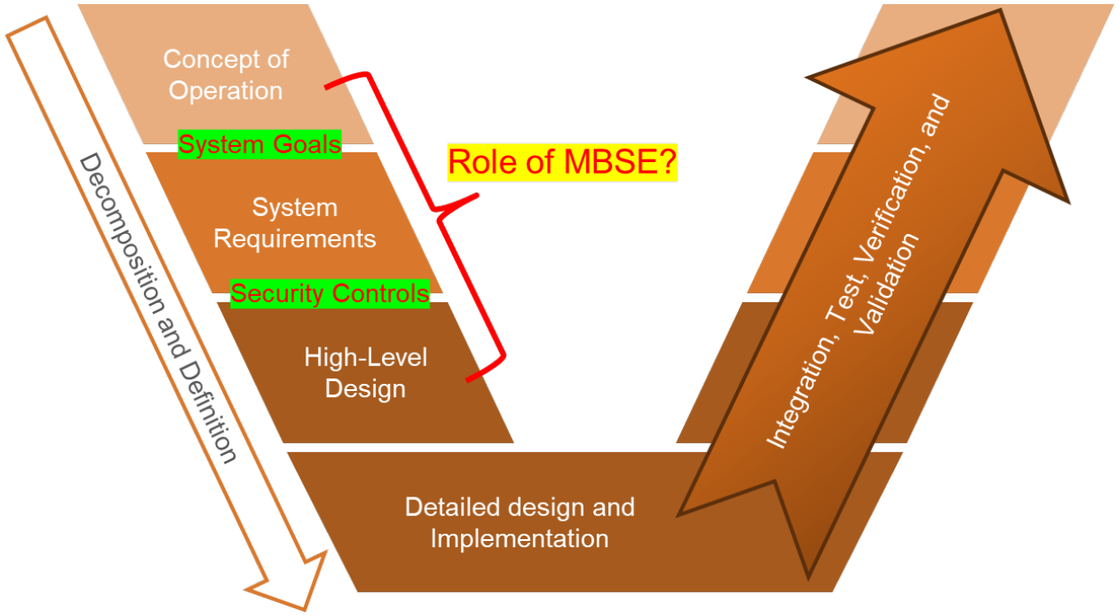
SURFACE VEHICLE RECOMMENDED PRACTICE	J1939™-21	MAY2022
	Issued 1994-07 Revised 2022-05 Superseding J1939-21 SEP2021	
Data Link Layer		

Graphic taken from: R. Chatterjee, S. Mukherjee, and J. Daily, "Exploiting Transport Protocol Vulnerabilities in SAE J1939 Networks," in Proceedings Inaugural International Symposium on Vehicle Security & Privacy. San Diego, CA, USA: Internet Society, 2023.

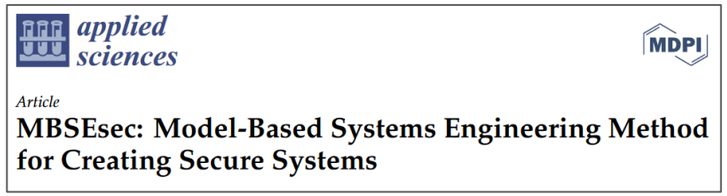
Research Question & Tasks

How can security be addressed in the system development process using MBSE?

- Use an MBSE method to build a model of an SOI that addresses security by:
  - Capture the system's assets
  - Capture security requirements
  - Develop effective security controls.
- Evaluate the effectiveness of the approach to develop a secure architecture
- Provide comments and recommendations

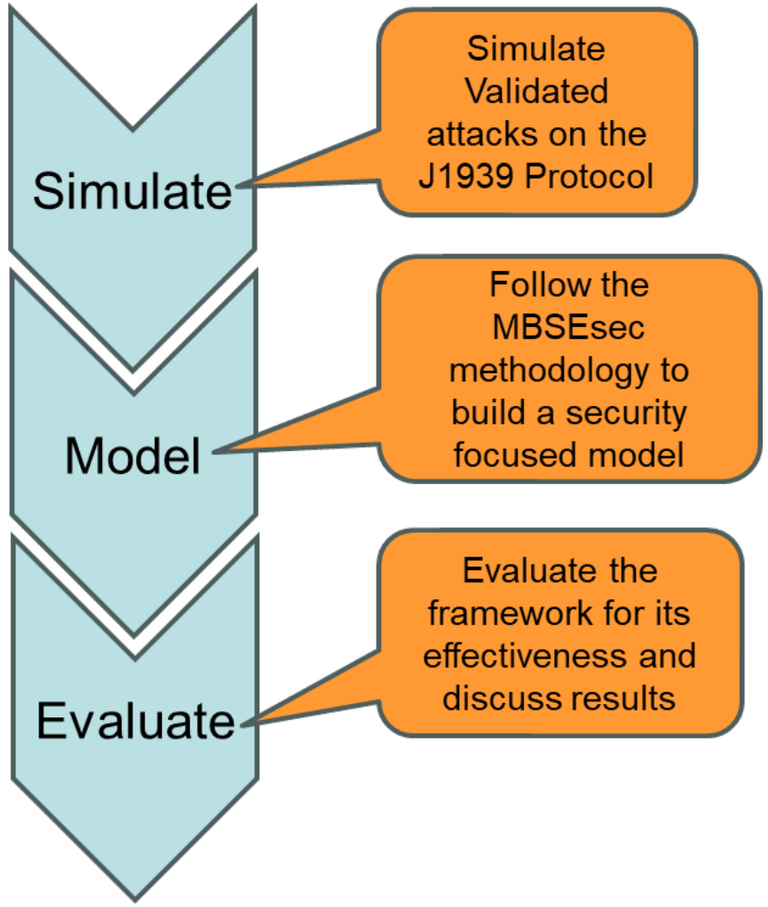


RQ1 Approach:



How can security be incorporated into the system development process using MBSE?

- Explore the effectiveness of *a selected MBSE method* to securing a system with validated exploits
- System of Interest: J1939 Transport Protocol
- This is accomplished by:
  - Developing an understanding of the J1939 transport protocol and its exploits using SysML **simulation**
  - **Develop a model following a prescriptive MBSE method**
  - **Use the method to develop security controls for the system of interest**
  - **Evaluate its effectiveness**
  - **Providing recommendations**



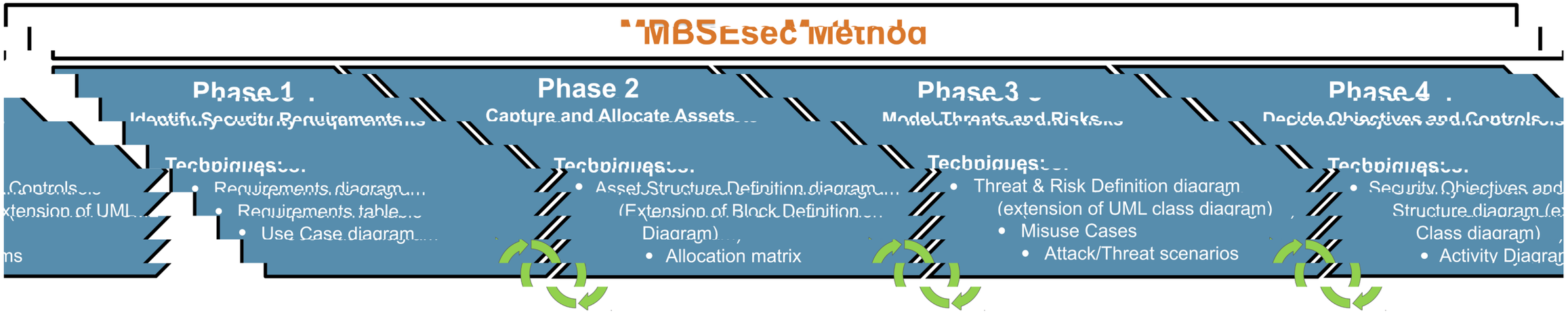
Model Based Systems Engineering Overview

- The role of MBSE is to capture and guide the system design through the development of a system model
- The three core MBSE pillars are [7]:
  - **Modeling language**
    - Defines the elements, relationships, and visual aspects of the diagram
  - **Modeling tool**
    - Authoring software that implements the rules for modeling and visualization based on modeling languages to create and manipulate the model
  - **Modeling method**
    - Provides guidance and a structure that defines what needs to be modeled, at which stages in the process, and how to do it (Techniques).

Must use all three pillars for successful modeling!

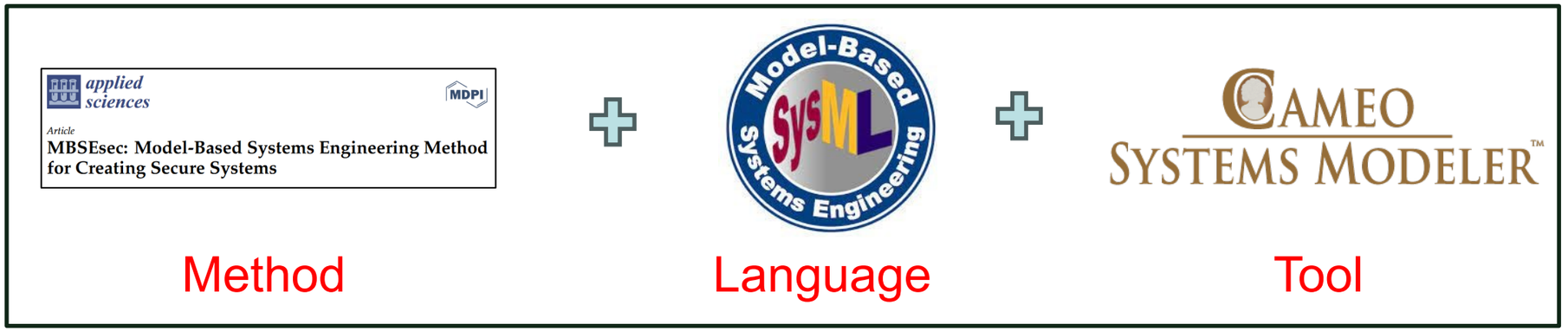
Selected Method: MBSEsec

- Developed by Mazeika et al. in 2020 [26]
  - Follows a simple four step iterative process

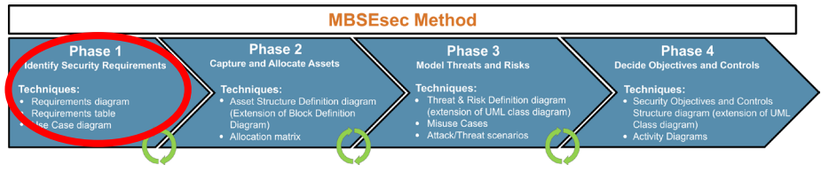


Goal: Apply the MBSEsec methodology (Method) using SysML (Language) in Cameo (Tool) to the J1939 Transport Protocol (SOI).

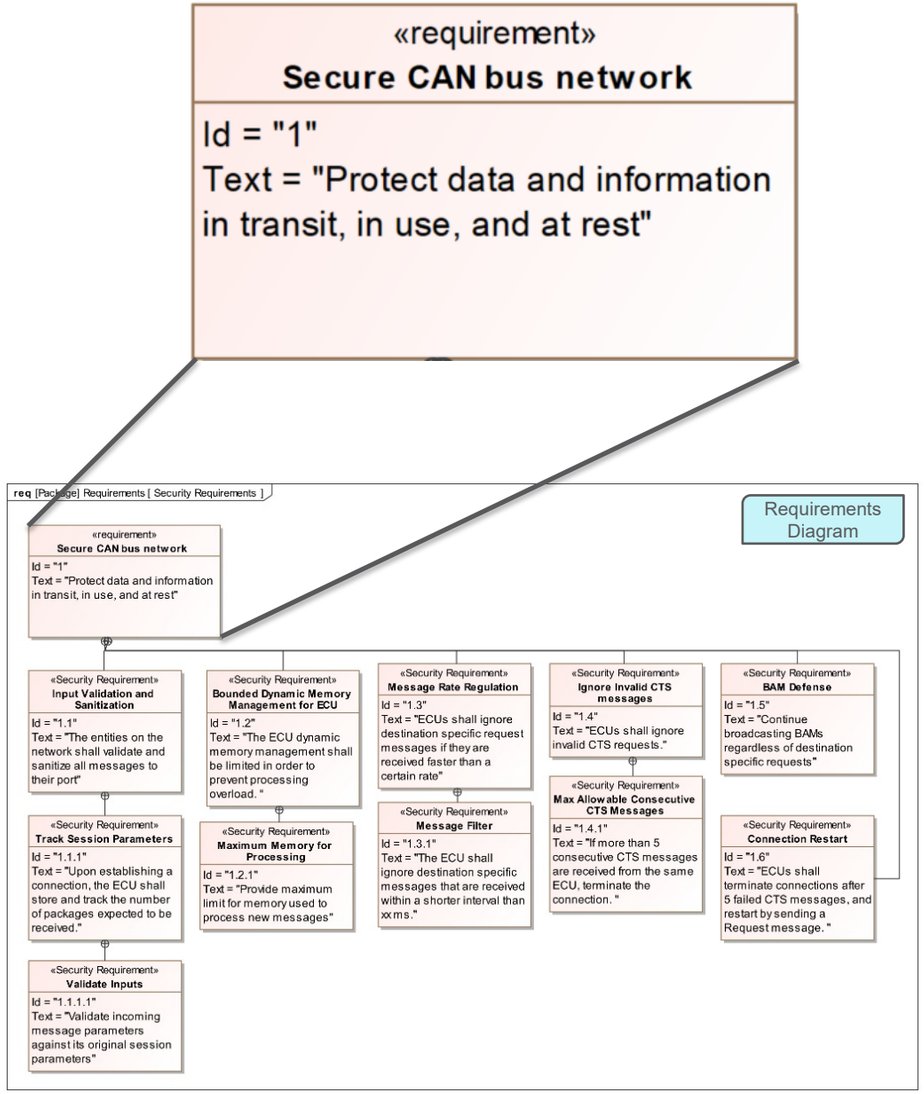
Output: Security requirements, and security controls



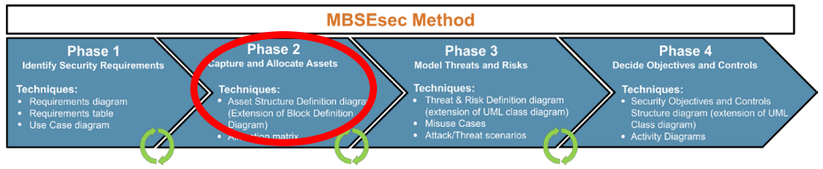
MBSEsec Applied



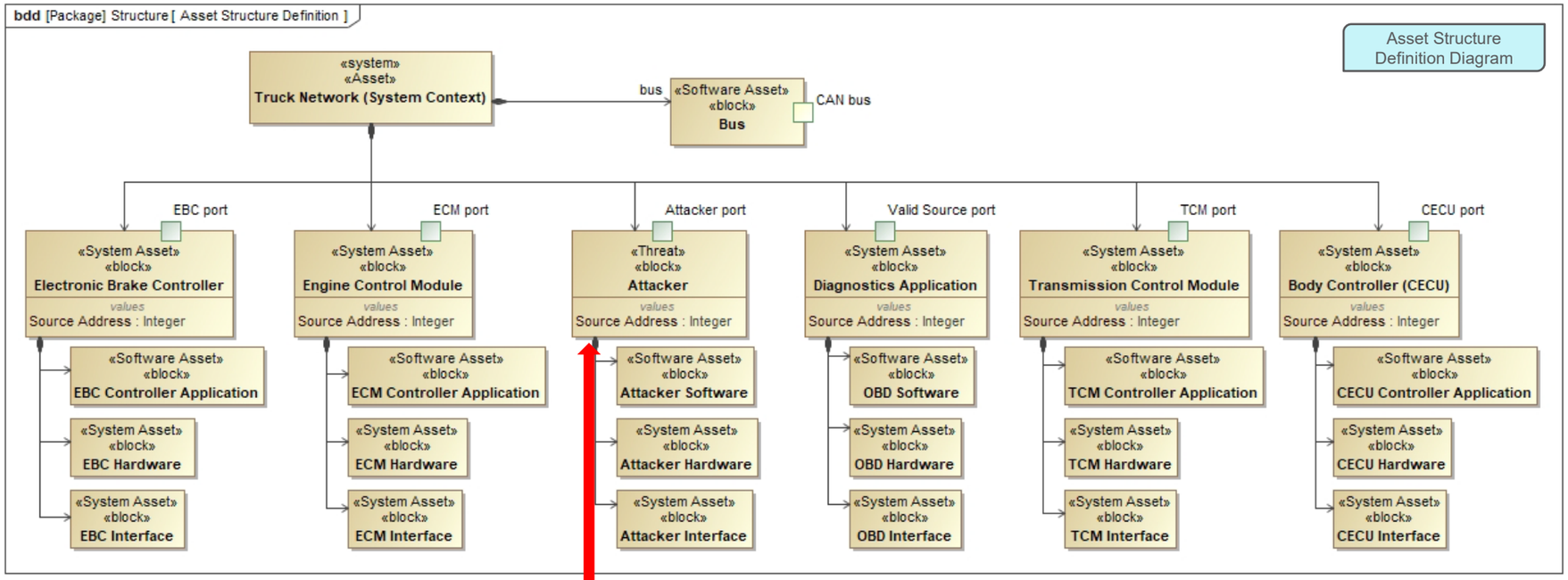
- Identify Security Requirements
  - Targeted security requirements to reduce risk of the proven exploits
  - Requirements tailored to ensure mitigation of Denial-of-Service attacks and prevention of memory overload attacks
  - The discovered vulnerabilities highlight the fact that the ECUs are the system assets that must be secured
    - Incomplete specification leads to undefined behavior
  - Requirements focused on ECU behavior and message handling



MBSEsec Applied Cont.



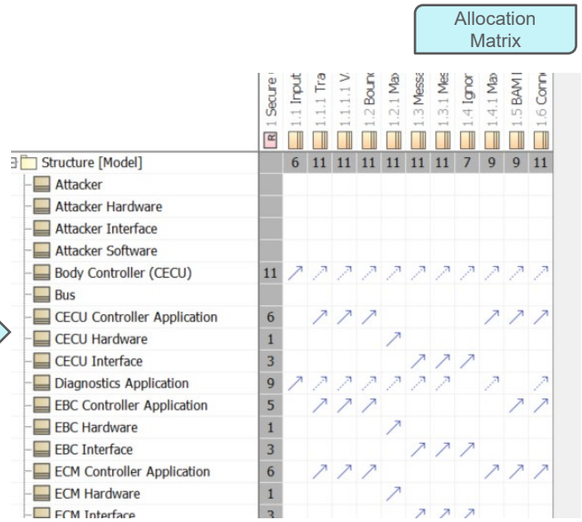
- Capture and Allocate Assets



Added an *Attacker* block to the diagram to:

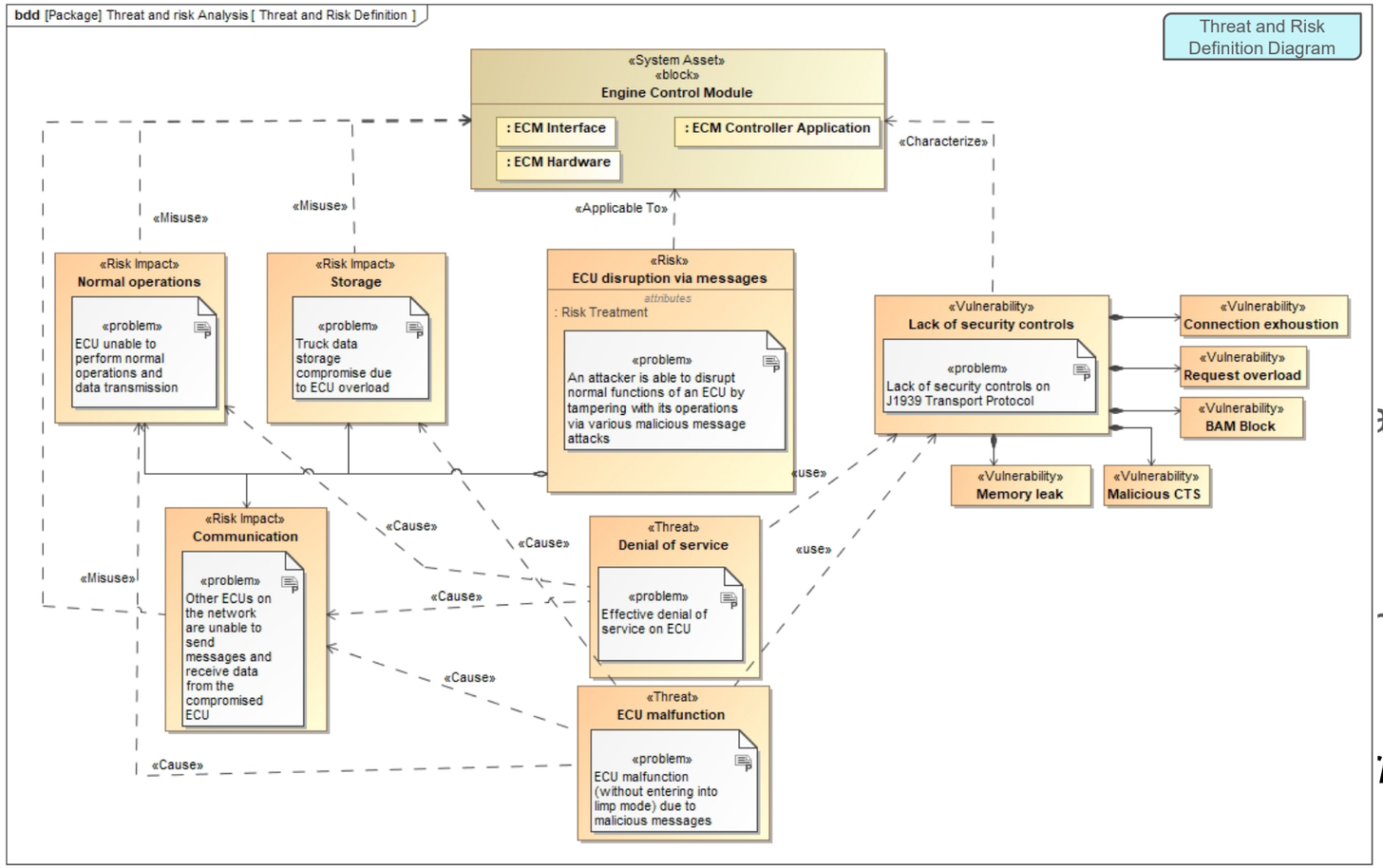
1. Facilitates the principle of zero trust
2. Further elaboration of the behavior diagrams and misuse cases

Allocation



Assets to requirements

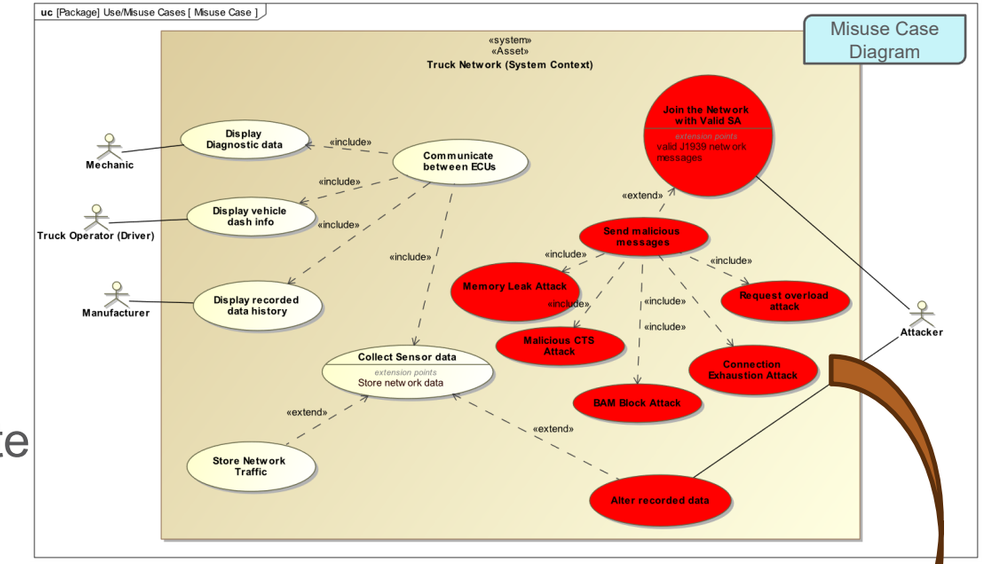
Structural Risk Definition

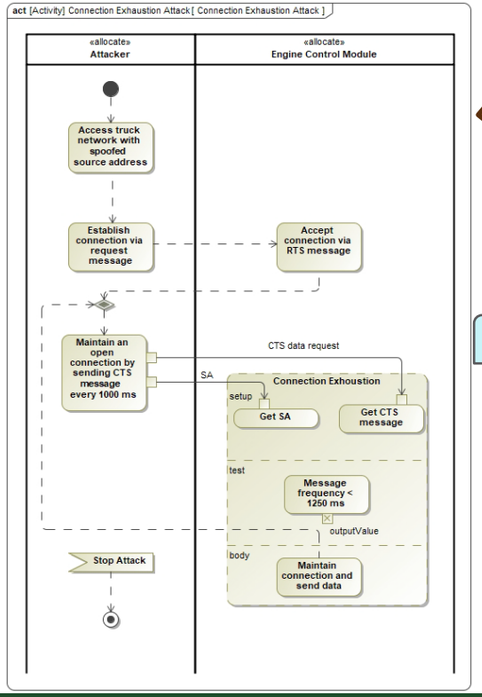


using various malicious message attacks”

Primary vulnerability: *“Lack of security controls on the J1939 Transport Protocol”*

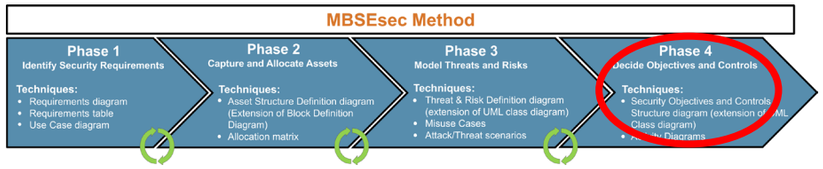
Behavioral Risk Definition





Activity Diagram

MBSEsec Applied Cont.

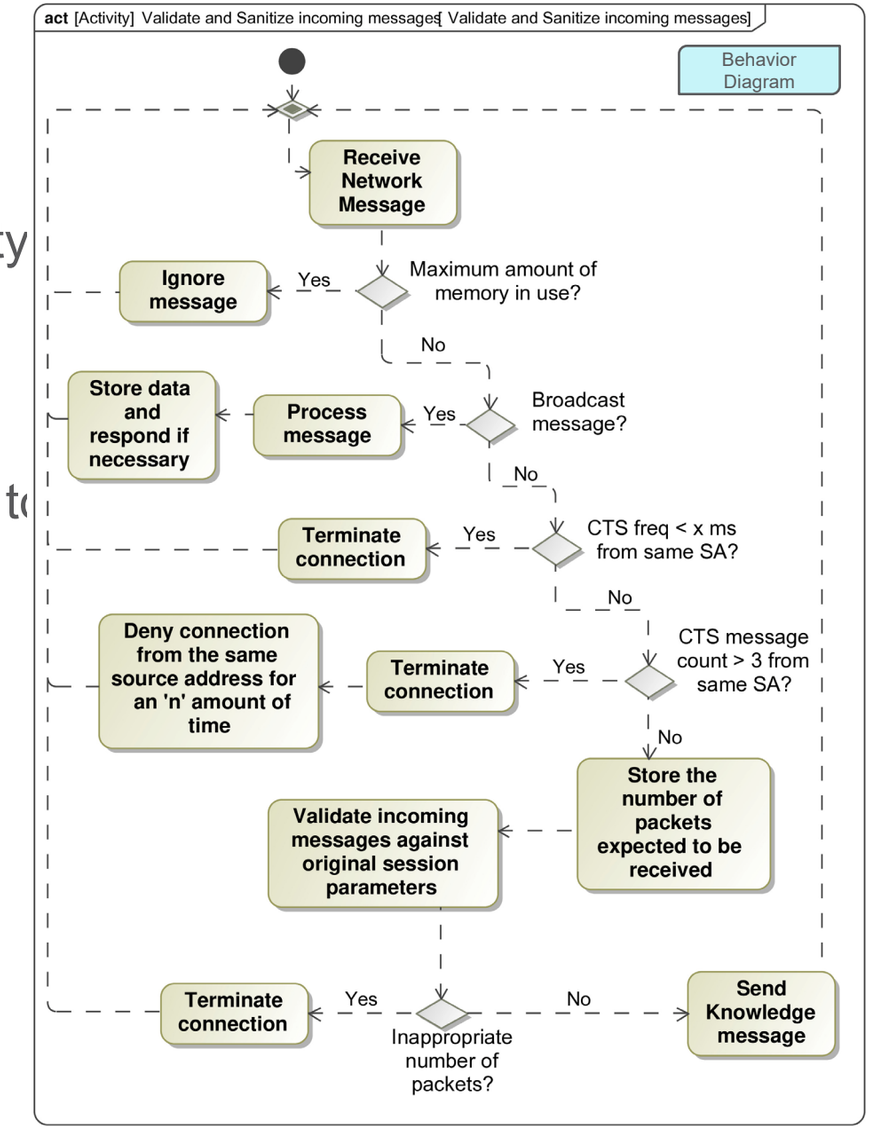


- Decide Objectives and Controls
  - Involves developing a risk mitigation approach by creating security controls

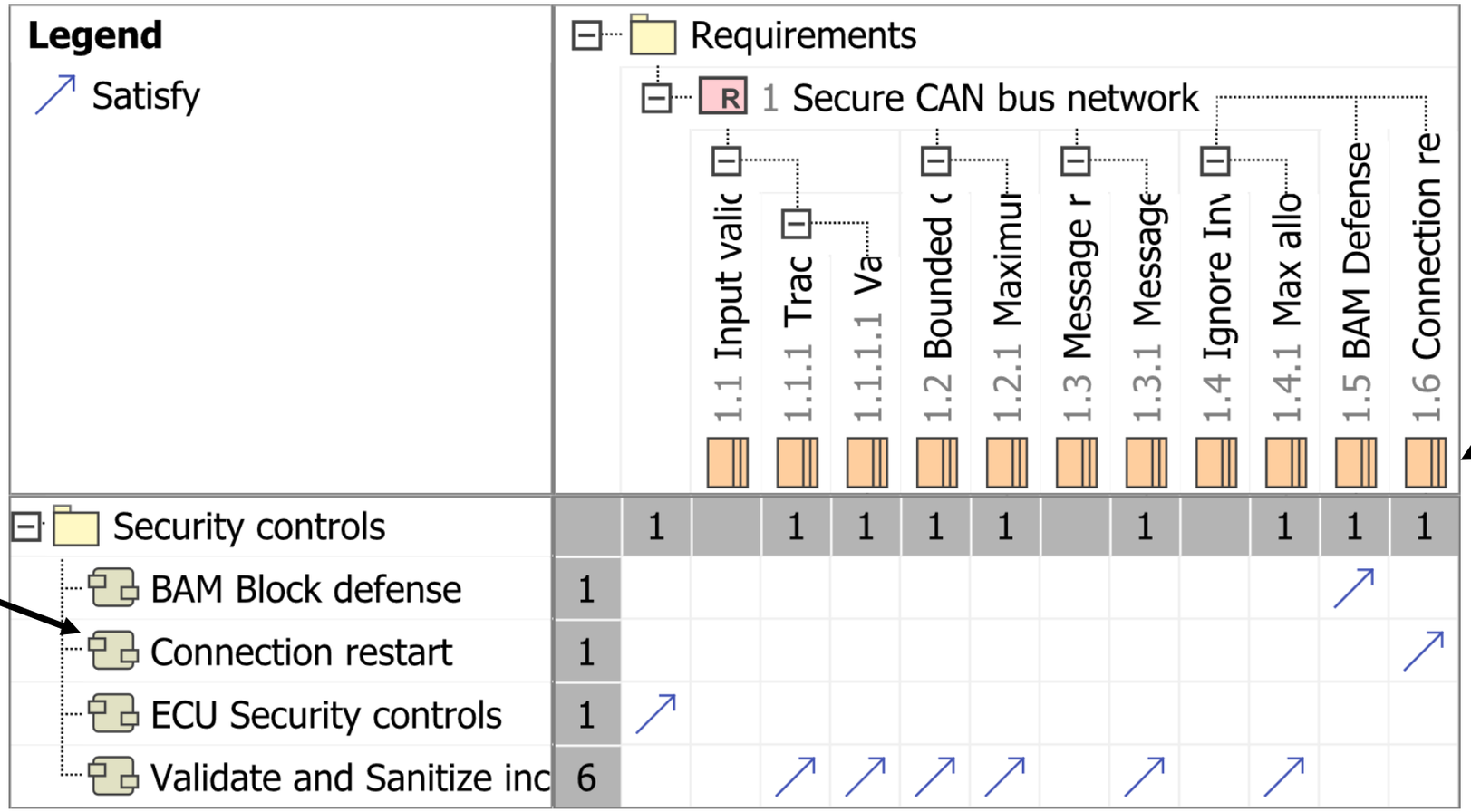
Overall Security Objective: "Defend against transport protocol attacks"

  - Security controls in the form of activity diagrams were developed to meet the security requirements and objectives
    - Validate and Sanitize incoming messages
    - BAM Block Defense
  - Security Objectives and Control diagram was created
    - Relating control behaviors to control objectives

Suggested a method that would make the ECU input parser more robust



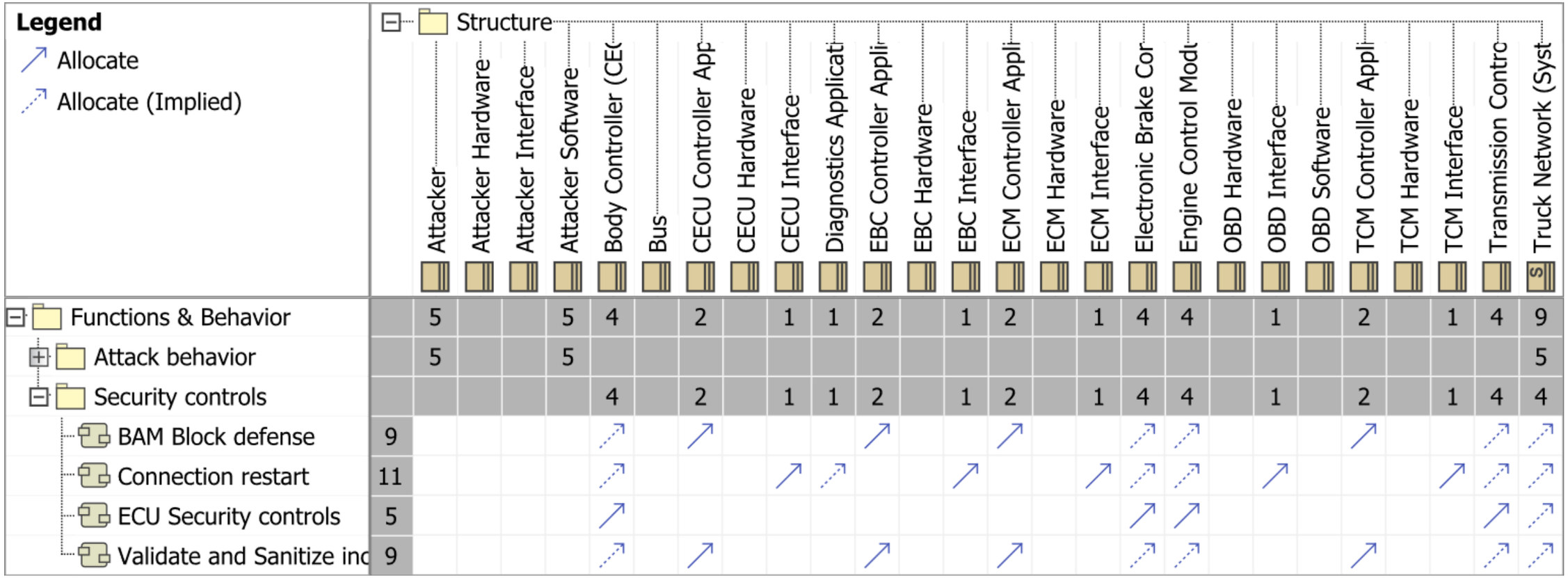
Verification and Satisfaction Checks



Security Controls to Security Requirements

** All requirements are met

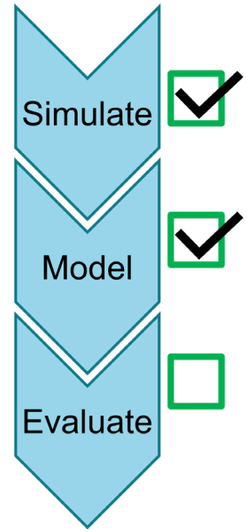
Verification and Satisfaction Checks



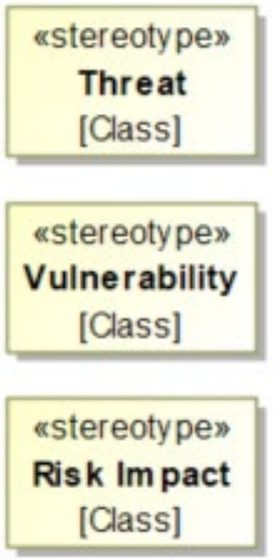
Security Controls to System Assets (components)

** Security controls allocated to appropriate System Assets

Discussion of Results

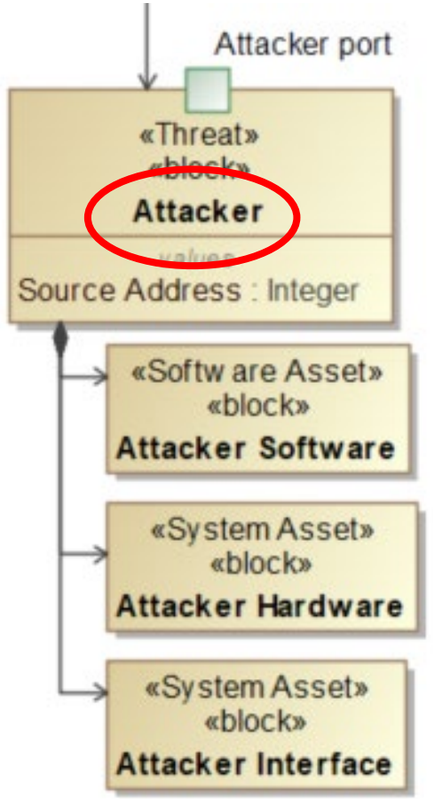


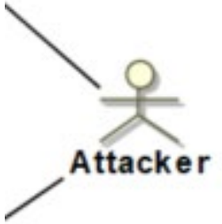
- We applied MBSEsec to a new domain: Heavy vehicle network protocols.
  - Developed security controls in the form of activity diagrams
- Security requirements were iteratively updated when modeling threats and risks: Simple with MBSE
- Easy iteration and model updates due to MBSEsec structure, and the dynamic nature of MBSE
- Applying the MBSEsec profile (Stereotypes) to model elements emphasized the system's security aspects
- The model enhanced traceability
- Brainstorming solutions for the vulnerabilities were effective because of the visual and simplified nature of MBSE



Recommendations

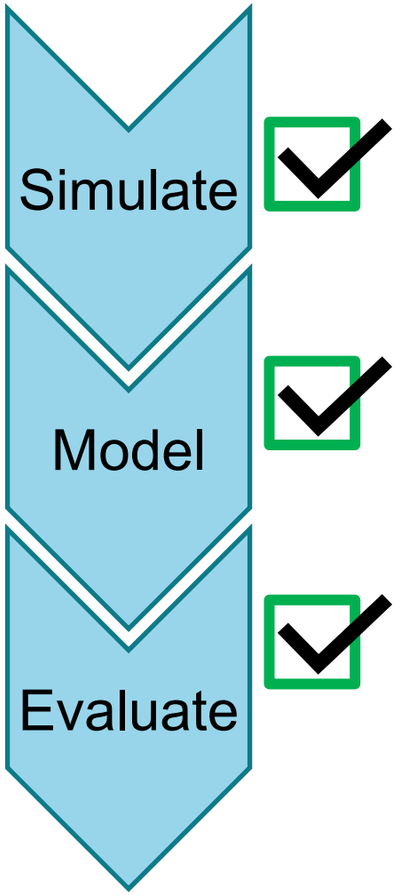
- To enhance the applicability of the MBSEsec method to the compromised system, we added an *attacker* element to the network structure
  - Facilitates the incorporation of zero trust principles as specified by NIST 800-207, and Executive Order 14028 "Improving the Nation's Cybersecurity"
  - Enabled the further elaboration of the behavior diagrams and misuse cases.
  - Improved brainstorming about the attacker's impact on the network
- Effective use of MBSEsec requires a prior threat and risk analysis to identify vulnerabilities
  - Otherwise, MBSEsec is the first iteration of analyzing threats and risks
  - In the case of this work, the threats and risks were already known





Discussion

- MBSEsec offers a valuable method for secure system development
- This method facilitated an effective environment for security control development
- The outputs of MBSEsec phases were continuously reviewed and updated after each phase – made for a more fluid design experience and easy brainstorming
- Using MBSEsec enabled:
  1. Depth of knowledge of the system grew as the model was built
  2. Easy solution driven brainstorming for security controls
  3. Iterative improvement of security requirements and controls
  4. Ease of traceability as the model grew in complexity



MBSEsec provides substantial benefits to security control development

Questions?

Thank you

Colorado State University

References

[1] R. Chatterjee, S. Mukherjee, and J. Daily, “Exploiting Transport Protocol Vulnerabilities in SAE J1939 Networks,” in Proceedings Inaugural International Symposium on Vehicle Security & Privacy. San Diego, CA, USA: Internet Society, 2023. [Online]. Available: https://www.ndss-symposium.org/wpcontent/uploads/2023/02/vehiclesec2023-23053-paper.pdf

[2] M. T. Campo, S. Mukherjee, and J. Daily, “Real-Time Network Defense of SAE J1939 Address Claim Attacks,” SAE International Journal of Commercial Vehicles, vol. 14, no. 3, pp. 02–14–03–0026, Aug. 2021. [Online]. Available: https://www.sae.org/content/02-14-03-0026/4

[3] Department of Defense. Digital Engineering Strategy, 2018.

[4] Systems Engineering Vision 2035: https://www.incose.org/2023_redesign/publications/se-vision-2035

[5] Ron Ross, Mark Winstead, and Michael McEvilley. Engineering Trustworthy Secure Systems. Technical Report NIST Special Publication (SP) 800-160 Vol. 1 Rev. 1, National Institute of Standards and Technology, November 2022

[6] Christopher Delp, Doris Lam, Elyse Fosse, and Cin-Young Lee. Model based document and report generation for systems engineering. In 2013 IEEE Aerospace Conference, pages 1–11, March 2013. ISSN: 1095-323X.

[7] Lenny Delligatti. SysML Distilled: A Brief Guide to the Systems Modeling Language. Addison-Wesley Professional, 2013.

References

[8] Jan Jürjens. UMLsec: Extending UML for Secure Systems Development. In Gerhard Goos, Juris Hartmanis, Jan van Leeuwen, Jean-Marc Jézéquel, Heinrich Hussmann, and Stephen Cook, editors, UML 2002 — The Unified Modeling Language, volume 2460, pages 412–425. Springer Berlin Heidelberg, Berlin, Heidelberg, 2002. Series Title: Lecture Notes in Computer Science.

[9] SO/IEC/IEEE 15288:2015 Systems and software engineering — System life cycle processes, May 2015.

[10] dilson Soares Palma, Elisa Yumi Nakagawa, Débora Maria Barroso Paiva, and Maria Istela Cagnin. Evolving reference architecture description: Guidelines based on iso/iec/ieee 42010, 2022

[11] David D. Walden, Garry J. Roedler, Kevin J. Forsberg, R. Douglas Hamelin, and Thomas M. Shortell. INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities. John Wiley & Sons, Inc, 4 edition, July 2015.

[12] SO/SAE 21434: Road Vehicles - Cybersecurity Engineering - SAE International

[13] Ron Ross, Mark Winstead, and Michael McEvilley. Engineering Trustworthy Secure Systems. Technical Report NIST Special Publication (SP) 800-160 Vol. 1 Rev. 1, National Institute of Standards and Technology, November 2022

References

[14] Joint Task Force Interagency Working Group. Security and Privacy Controls for Information Systems and Organizations. Technical report, National Institute of Standards and Technology, September 2020. Edition: Revision 5

[15] Meenakshi Deshmukh. Security requirements engineering process. In Seminar in Information System, Security Engineering. Citeseer, 2009

[16] Shafiq ur Rehman, Christopher Allgaier, and Volker Gruhn. Security Requirements Engineering: A Framework for Cyber-Physical Systems. In 2018 International Conference on Frontiers of Information Technology (FIT), pages 315–320, December 2018. ISSN: 2334-3141

[17] Adam Shostack. Threat Modeling: Designing for Security. John Wiley & Sons, Hoboken, New Jersey, 2014

[18] Benjamin Fabian, Seda Gürses, Maritta Heisel, Thomas Santen, and Holger Schmidt. A comparison of security requirements engineering methods. Requirements Engineering, 15(1):7–40, March 2010.

[19] Donald Firesmith. Engineering Security Requirements. The Journal of Object Technology,2(1):53, 2003

[20] C.B. Haley, R. Laney, J.D. Moffett, and B. Nuseibeh. Security Requirements Engineering: A Framework for Representation and Analysis. IEEE Transactions on Software Engineering,34(1):133–153, January 2008

References

[21] D. Mažeika and R. Butleris. Integrating Security Requirements Engineering into MBSE: Profile and Guidelines. Security and Communication Networks, 2020:1–12, March 2020.

[22] Michael Brunner, Michael Huber, Clemens Sauerwein, and Ruth Breu. Towards an Integrated Model for Safety and Security Requirements of Cyber-Physical Systems. In 2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), pages 334–340, Prague, Czech Republic, July 2017. IEEE.

[23] Donatas Mazeika and Rimantas Butleris. Identifying Security Issues with MBSE while Re- building Legacy Software Systems. In 2020 IEEE 15th International Conference of System of Systems Engineering (SoSE), pages 83–86, June 2020

[24] Yves Roudier and Ludovic Apvrille. SysML-Sec: A model driven approach for designing safe and secure systems. In 2015 3rd International Conference on Model-Driven Engineering and Software Development (MODELSWARD), pages 655–664, February 2015.

[25] Christian Raspotnig, Vikash Katta, Peter Karpati, and Andreas L. Opdahl. Enhancing CHASSIS: A Method for Combining Safety and Security. In 2013 International Conference on Availability, Reliability and Security, pages 766–773, September 2013.

[26] Donatas Mažeika and Rimantas Butleris. MBSEsec: Model-Based Systems Engineering Method for Creating Secure Systems. Applied Sciences, 10(7):2574, April 2020

References

[27] Jin Seo Park, Daehyun Kim, Seokmin Hong, Hyunjung Lee, and EuiJung Myeong. Case Study for Defining Security Goals and Requirements for Automotive Security Parts Using Threat Modeling. pages 2018–01–0014, April 2018

[28] Ahmad Y. Javaid, Weiqing Sun, Vijay K. Devabhaktuni, and Mansoor Alam. Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In 2012 IEEE Conference on Technologies for Homeland Security (HST), pages 585–590, Waltham, MA, USA, November 2012. IEEE

[29] Dmytro Klets, Igor V. Gritsuk, Andrii Makovetskyi, Nickolay Bulgakov, Mikhail PodrigaloIhor Kyrychenko, Olena Volska, and Nikolai Kyzminec. Information Security Risk Management of Vehicles. pages 2018–01–0015, April 2018.

[30] Rik Chatterjee, Subhojeet Mukherjee, and Jeremy Daily. Exploiting Transport Protocol Vulnerabilities in SAE J1939 Networks. In Proceedings Inaugural International Symposium on Vehicle Security & Privacy, San Diego, CA, USA, 2023. Internet Society.

[31] Bernard Zeigler, Saurabh Mittal, and Mamadou Traore. MBSE with/out Simulation: State of the Art and Way Forward. Systems, 6(4):40, November 2018

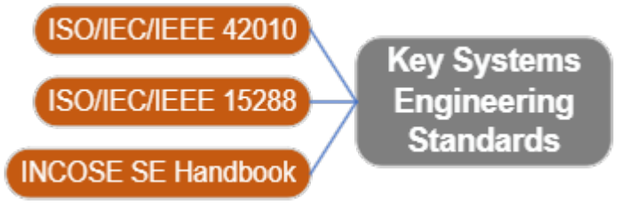
[32] Mason Michael Woodruff. Consequence and likelihood in risk estimation: A matter of balance in UK health and safety risk assessment practice. Safety Science, 43(5-6):345–353, June 2005.

Survey Of Available MBSE Security Methods

- **UMLSec, 2002 [8]**
  - UML Sec uses standard UML diagrams to specify security requirements and attack scenarios. It provides a set of security-related constructs, such as security classes, associations, and constraints.
- **SysMLSec, 2015 [24]**
  - The SysMLprocess involves developing high-level security requirements, analyzing attack trees and ending with hardware and software partitioning.
- **CHASSIS, 2013 [25]**
  - Relies on UML-based diagrams and text-based techniques to develop functional safety/security requirements.
- **MBSEsec, 2020 [26]**
  - MBSEsecis a method for developing secure systems through developing a detailed systems model that outputs security controls.

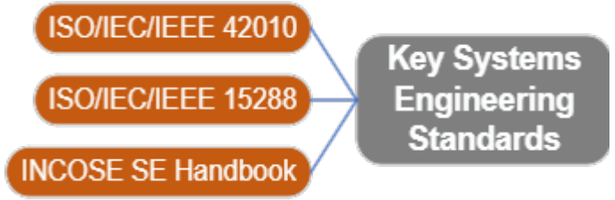
MBSEsec is the most up-to-date and most relevant, because it is a combination of best practices

Key Systems Engineering Standards



- **ISO/IEC/IEEE 42010 [9]**- Software Architecture Description
  - Highlights security architecture by design, need for early stakeholder involvement– traceability!
- **ISO/IEC/IEEE 15288 [10]**- System Life Cycle Processes
  - Emphasizes the systematic and structured nature of systems engineering need for MBSE (traceable model)
- **INCOSE Systems Engineering Handbook [11]**
  - INCOSE Technical Processes
  - Stakeholder security Interest-> Security requirements-> Minimize security risk
  - MBSE improves:
    - Communications, ability to manage complexity, knowledge capture
    - Improves system requirements, architecture, and design quality

Key Systems Engineering Standards



Alignment of ISO/IEC 15288 and SE Handbook

ISO/IEC 15288:2008 System Life Cycle Process	INCOSE SE Handbook v4e Section 4.0
6.4 Technical Processes	***4.0 Technical Processes***
6.4.1 Business or Mission Analysis	4.1 Business or Mission Analysis
6.4.2 Stakeholder Needs and Requirements Definition	4.2 Stakeholder Needs and Requirements Definition
6.4.3 Systems Requirements Definition	4.3 Systems Requirements Definition
6.4.4 Architectural Definition	4.4 Architectural Definition
6.4.5 Design Definition	4.5 Design Definition
6.4.6 System Analysis	4.6 System Analysis
6.4.7 Implementation	4.7 Implementation
6.4.8 Integration	4.8 Integration
6.4.9 Verification	4.9 Verification
6.4.10 Transition	4.10 Transition
6.4.11 Validation	4.11 Validation
6.4.12 Operation	4.12 Operation
6.4.13 Maintenance	4.13 Maintenance
6.4.14 Disposal	4.14 Disposal

How should Security be addressed in these early Processes?

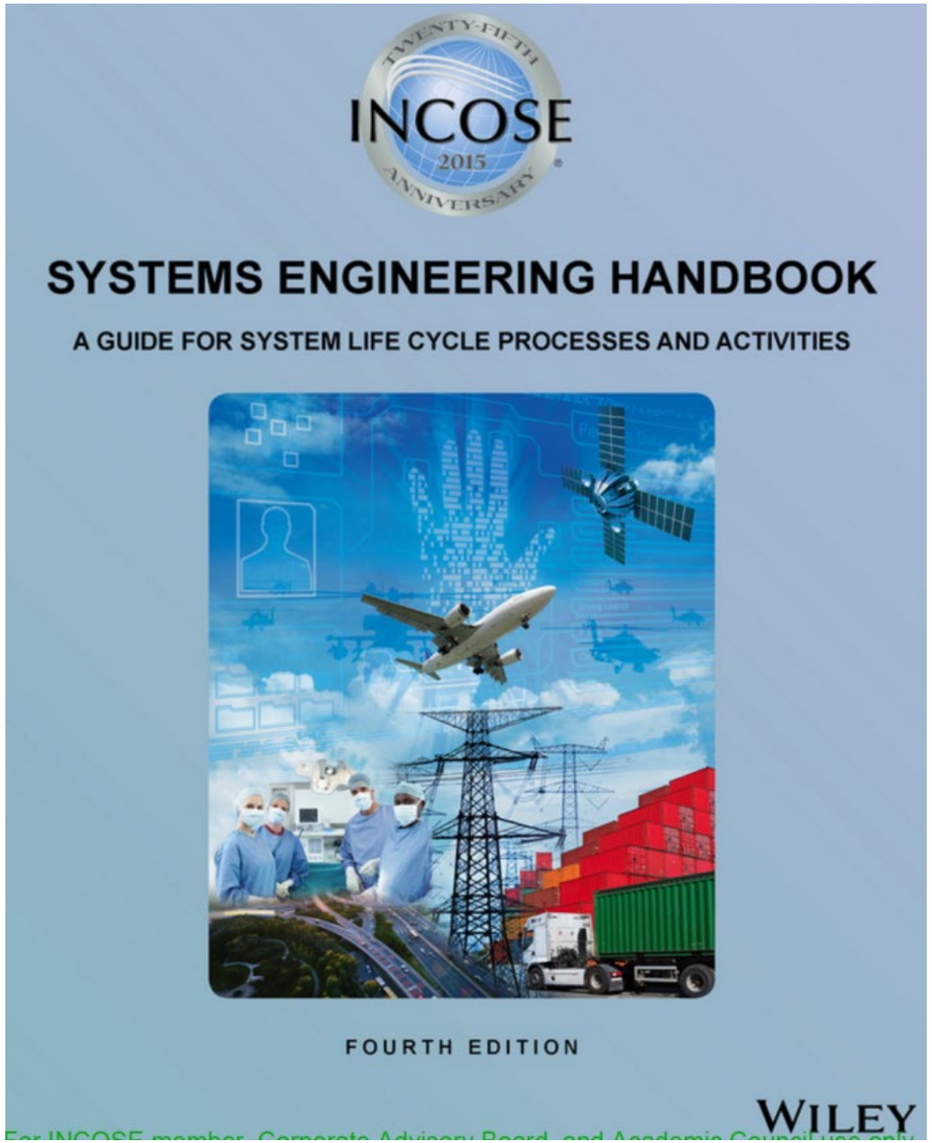
Within the handbook (Chapter 4), security is only lightly addressed, and always grouped with other factors such as “health, safety, security, environment, assurance, adaptability and resilience”

INCOSE MBSE

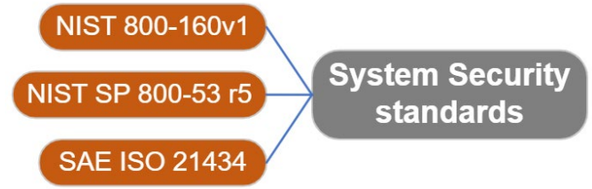
Model Based Systems Engineering (Ch 9.2)

The system model is a primary artifact of the SE process. Used to capture each technical process

MBSE formalizes the application of SE through the use of models.

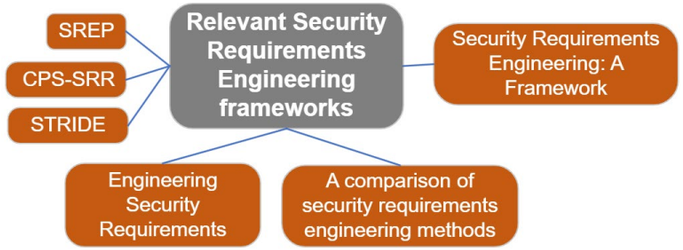


System Security Guiding Standards



- **ISO 21434 [12]**- Cybersecurity Engineering for Road Vehicles (replaced J3061)
  - Introduces TARA (Threat Analysis and Risk Assessment), helps with developing security requirements and controls
- **NIST 800-160v1 [13]**- Engineering Trustworthy Secure Systems
  - Deliver system capabilities at an acceptable level of performance while minimizing (preemptive and reactive measures) the occurrence and extent of loss
- **NIST 800-53 r5 [14]** - Security Controls
  - Encourages the integration of security controls into the system development life cycle
  - Risk based approach: Facilitates early identification and mitigation of security risks during the modeling process

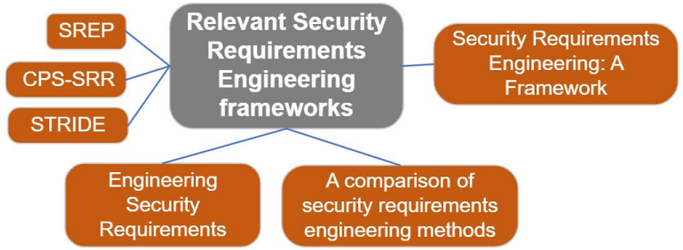
Security Requirement Engineering Frameworks



- **SREP [15]**- Security Requirements Engineering Process
  - Great methodology to incorporate security from genesis of design
  - Design process begins with: Stakeholder agreement, ID critical assets, ID security Objectives
  - Activities Include: security risk assessments, threat modeling, and selection of security controls
- **CPS-SRR [16]**– CPS Security Requirement Repository
  - Extension of SREP focused on Cybe-physical systems– demonstrates its utility
    - Only introduces modeling in step 4 – ID threats and develop artifacts
- **STRIDE [17]**- Threat Modeling Designing for Security
  - Categorizes security threats: Spoofing, Tampering, Repudiation, Info Disclosure, DoS, and Elevation of Privilege

Implement Security at beginning of design and continue throughout, utilize common language (like STRIDE) to ID threats

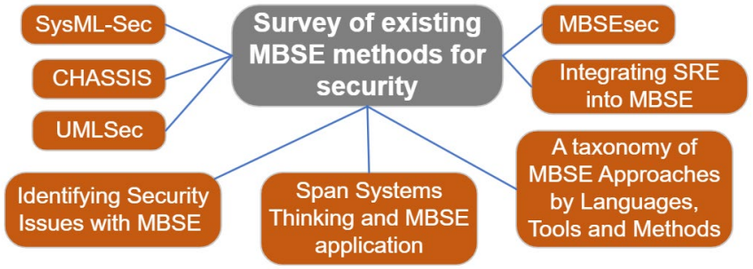
Security Requirement Engineering Frameworks



Other Key takeaways:

- *A Comparison Of Security Requirements Engineering Methods- Fabian 2010 [18]*
  - Security requirements are consequences of the identified threats to the system
  - All security requirements must be done before the design of the system
  - **Security goals** are defined as very general statements about the security of an asset
  - **Security requirements** capture security goals in more detail
- *Engineering Security Requirements- Firesmith 2003 [19]*
  - "Most Requirement Engineers are poorly trained to elicit … requirements"
  - Security requirements can be accidentally replaced with security-specific architectural constraints- constrains optimum design
  - Introduces 12 types of security requirements- useful for guiding the requirements engineering process
- *Security Requirements Engineering: A Framework for Representation and Analysis- Haley 2008 [20]*
  - Security Requirements must satisfy three criteria definition, assumptions and satisfaction

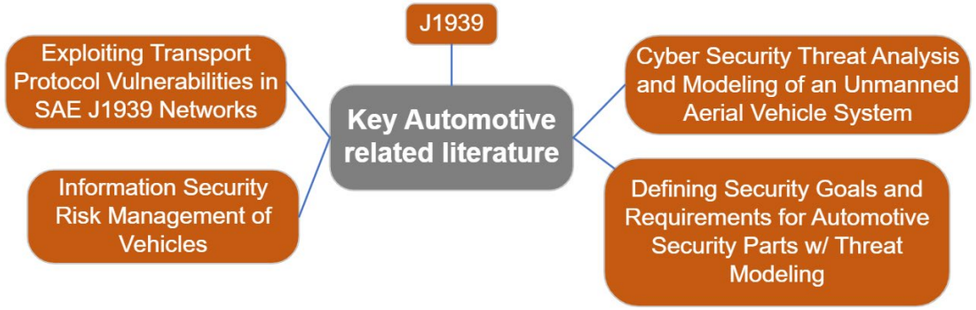
Model Based Systems Engineering Methods for Security



- *Integrating Security Requirements Engineering into MBSE – Mažeika 2020 [21]*
  - MBSE does not directly address the security aspects of a system, rather it is a tool that can be used to generate better requirements. Introduces a Security Profile
- *Towards an Integrated Model for Safety and Security Requirements of Cyber-Physical Systems – Brunner 2017 [22]*
  - Method begins with defining clear security goals, which act as a foundation for the security requirements that follow.
- *Identifying Security Issues with MBSE while Rebuilding Legacy Software Systems – Mažeika 2020 [23]*
  - *Security techniques that can be used in MBSE: Security requirements engineering, Misuse cases, attack scenarios, and security controls*

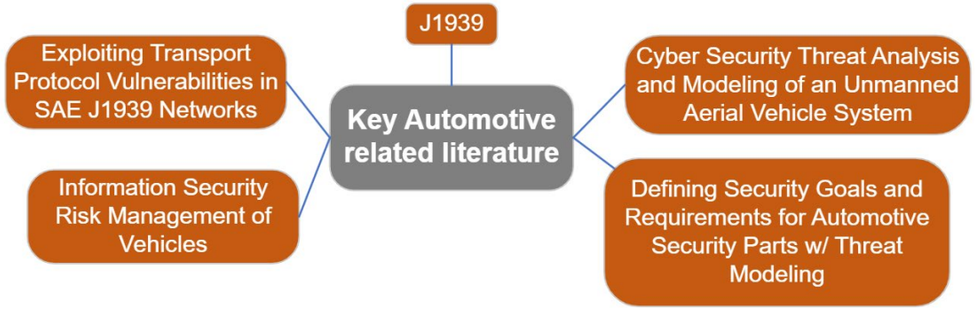
Key Automotive related Literature

The automotive industry significantly influences security engineering because of its high pace of integration and testing of CPS systems



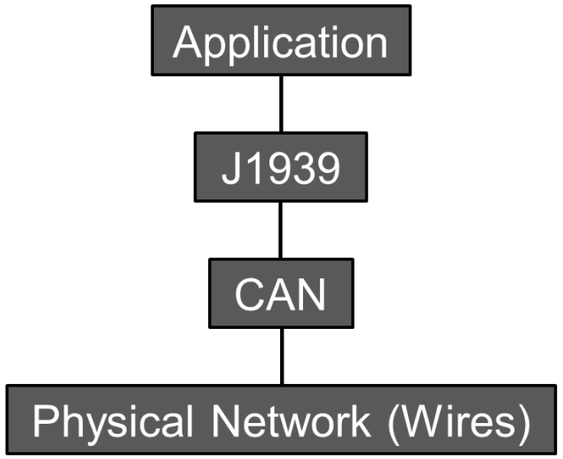
- *Case Study for Defining Security … Automotive Security Parts Using Threat Modeling- Jin Seo Park 2018 [27]*
  - Combine the Microsoft threat modeling process, with STRIDE threat classification, and HEAVENS to classify risk levels.
  - Method used to develop security goals and requirements
- *Cyber Security Threat Analysis and Modeling of an Unmanned Aerial Vehicle System- Ahmad 2012 [28]*
  - Demonstrated the utility of combining architectural definition with risk analysis phase
  - Demonstrated the effectiveness of likelihood and impact as means of risk classification
- *Information Security Risk Management of Vehicles- Dmytro 2018 [29]*
  - Provides key risk management definitions in terms of road vehicles (asset, vulnerability, risk)
  - Demonstrates a methodology for risk classification

Key Automotive related Literature Cont.



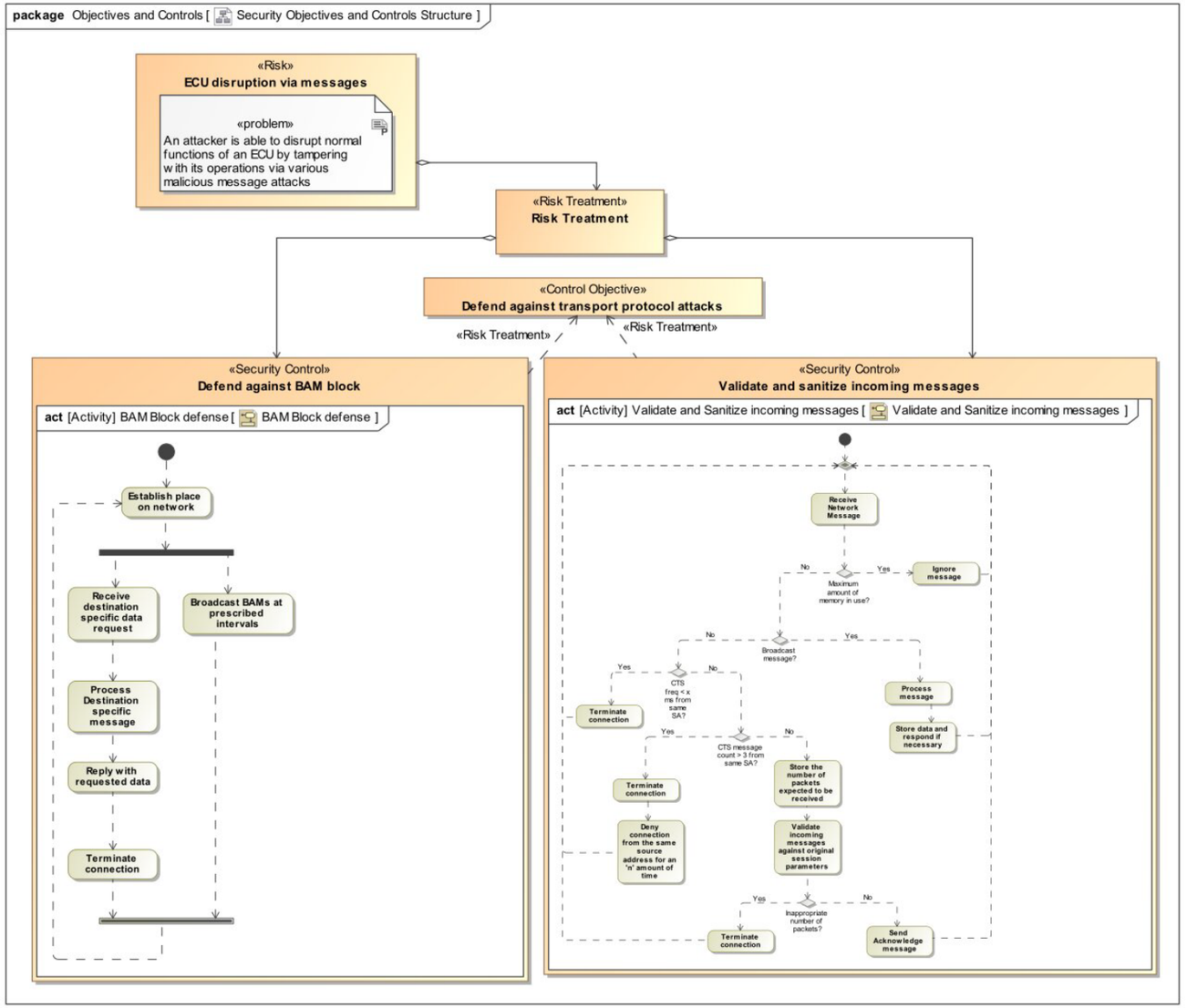
J1939:

- Used as the system of interest for most of the work.
- A standard maintained by the Society of Automotive Engineers (SAE)
- Defines how information is transferred across a network to allow ECUs to communicate information (e.g. vehicle speed)
- J1939 is a 'software specification' that operates on top of a CAN bus.
- CAN (Controller Area Network) is a form of serial communication used on heavy vehicles

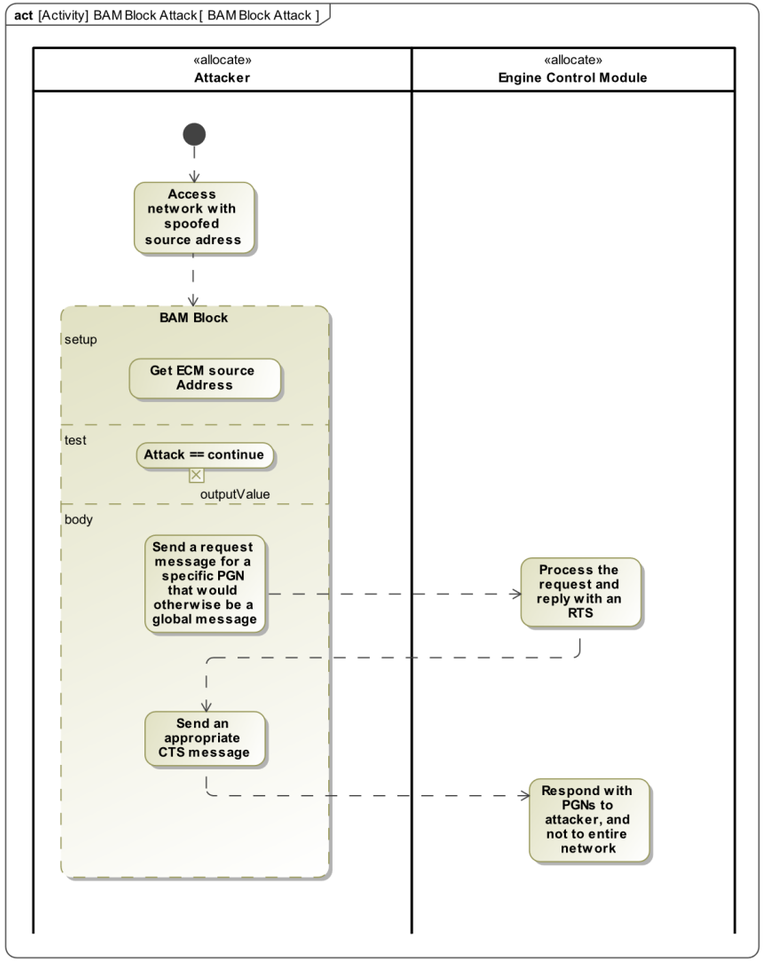


- *Exploiting Transport Protocol Vulnerabilities in SAE J1939 Networks- Chatterjee 2023 [30]*
  - Five different network attacks were conducted and validated on truck networks
    - Request Overload Attack
    - Connection Exhaustion Attack
    - BAM Block Attack
    - Malicious Clear to Send
    - Memory Leak Attack

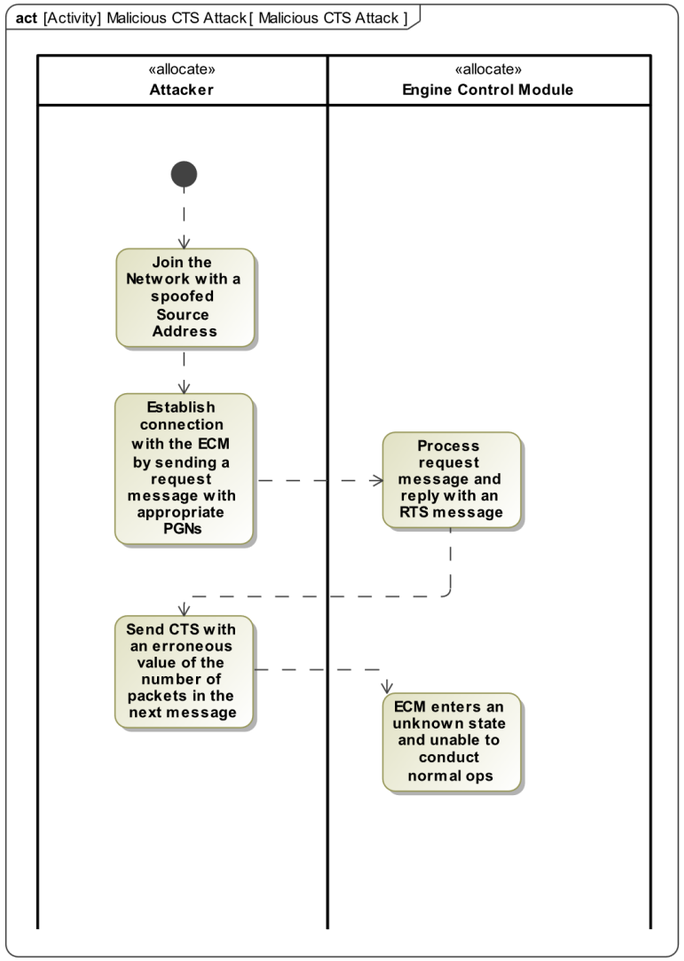
Security Objectives and Control Structure Diagram



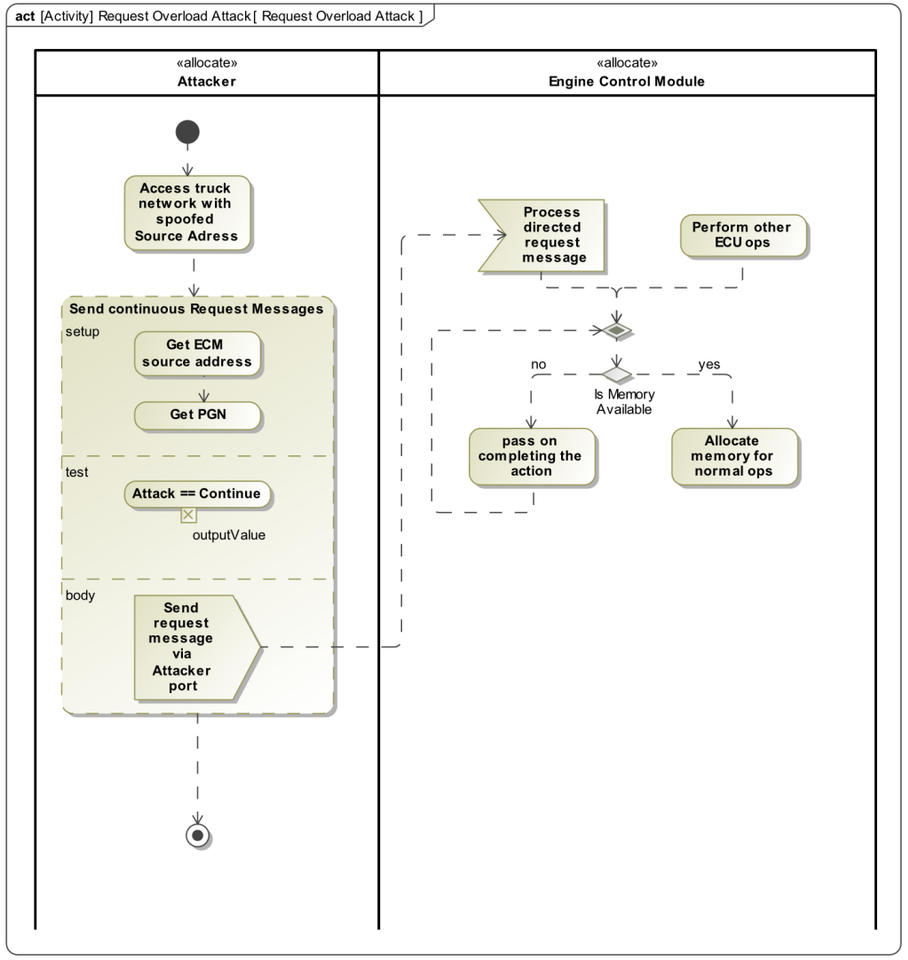
Attack Scenarios



BAM Block Attack



Malicious CTS Attack



Request Overload Attack