Open eXchange Format

of

Security Analysis Models

[openXSAM]

Specification

Version 1.0

Contributors

The following is a list of dedicated contributors whose expertise and efforts have significantly contributed to the development and success of this technical white paper. Their valuable insights and hard work are greatly appreciated.

Automotive Security Research Group (ASRG)

Wilmington, North Carolina, USA

hello@asrg.io

SECURE Team

Itemis

Chicago, USA

info@itemis.com

Abdul Rahman Sattar

Arctic Wolf Networks

abdul.sattar@arcticwolf.com

Shashank Yadav

Asatae Foundation

India

shashank@asatae.foundation

Revision History

Date	Version	Description	Released by
11 Oct 2023	1.0	First Release for Review	John Heldreth

Table of Contents

Contributors **3**

Revision History **4**

Table of Contents **5**

I. Introduction **6**

A. Scope 6

B. Out of Scope 7

C. Keywords 7

D. Glossary 8

E. The State of the Art 10

F. Future Work 13

G. Stakeholders 16

II. Use Cases **16**

A. OPXSAM_UC_001: Risk Information Sharing 16

B. OPXSAM_UC_002: Test Plan Authoring 19

C. OPXSAM_UC_003: Automated Attack Surface Management (ASM) and Detection and Response (D&R) 20

D. OPXSAM_UC_004: Composition of individual TARAs (WIP) 22

III. Methods **23**

IV. Data Fields **24**

A. ID 24

B. UUID 24

C. Name 24

D. References 24

E. Inheritance 26

F. Extensions 27

G. Grouping of Elements 27

H. Contact Information (Referring to UC_001) 27

V. Specification **27**

A. File Description 28

B. Module Overview 28

C. Data Model 29

D. Data Specification 29

VI. Appendix **82**

A. The XML Scheme Definition (XSD) 82

VII. Bibliography / References **118**

I. Introduction

A. Scope

This paper proposes a framework and data model to exchange risk-related information between entities inside and outside of organizations in the automotive industry in a clear, well-defined, unambiguous and machine-readable format.

In this regard, it is important to note that while this framework supports regulatory obligations such as UN ECE R.155 and China Cybersecurity G/BT, it extends beyond the minimum requirements. Regulatory obligations should be the minimum of what companies should be doing to protect themselves and their customers against cyber threats.

The authors have done their best to make reference to regulations and use common terminology throughout this document, but the regulations should not be the driving element of any cybersecurity program. Protecting end-users (drivers, passengers, and pedestrians) through the exchange of risk-related information is the motivation for this document.

As there are many different sources of risk, and each company or risk owner has a different scope of risk, this specification shall not limit the scope of usage. This risk data exchange format can be used for any industry where the user sees fit. It should be noted that this specification was written with the automotive industry in mind and adaptations to fit the use case will always need to be considered.

The following aspects were considered when designing this specification:

- Risk-related data including but not limited to:
    - Assessment Model
    - Item Definition (Asset)
    - Threat Catalog (UN-ECE R.155, Annex)
    - Controls Catalog
    - Assumptions Catalog
    - Damage Scenarios
    - Impact catalog
- Weakness and Vulnerabilities (Clause 8 from ISO/SAE 21434:2021)

- Concept Phase (Clause 9 from ISO/SAE 21434:2921)
- Control Maturity (Verify the attack feasibility levels of control)
- All ISO/SAE 21434 compliant risk methodologies.
- Extended Item definition structure

B. Out of Scope

This specification does not address the following topics:

- Requirements Management: this specification considers only the highest level of security requirements (security goals and claims), but takes no provisions to capture, refine and trace them to more low-level requirements.
- Asset Management: this specification is focused on risk information exchange and limited to the enumeration of assets; it does not concern itself with how those assets are identified or managed over time.
- Data Integrity, Authenticity, Confidentiality: This specification does not prescribe methods to protect the information that is stored in the file against accidental or intentional access and alteration. External means like checksums, encryption, signatures and appropriate access control should be employed by the user of this document.
- Data Quality: The user of this document is responsible for the quality of the data captured within the file.
- Change Management and Traceability of Updates: The user of this document is responsible for configuration management and data traceability with external means like version control systems. The openXSAM specification file itself contains a revision history.

C. Glossary

This section describes all of the used terms, acronyms, and abbreviations used within this document.

Asset

“(An) object that has value, or contributes to value (is an asset). An asset has one or more cybersecurity properties (3.1.20) whose compromise can lead to one or more damage scenarios.”

("ISO/SAE 21434:2021," 2021, p.1)

Example:

"The asset (can be a) personal information (customer personal preferences) stored in an infotainment system and its cybersecurity property is confidentiality."

("ISO/SAE 21434:2021," 2021, p.43)

Attack Feasibility

"(Attack feasibility is an) attribute of an attack path describing the ease of successfully carrying out the corresponding set of actions (in order to realize a threat scenario)."

("ISO/SAE 21434:2021," 2021, p.2)

Attack Path

"(An attack path is a) set of deliberate actions to realize a threat scenario." ("ISO/SAE 21434:2021," 2021, p.2)

Cybersecurity Concept (CS Concept)

"(Cybersecurity concepts are) cybersecurity requirements of the item and requirements on the operational environment, with associated information on cybersecurity controls."

("ISO/SAE 21434:2021," 2021, p.2)

Cybersecurity Control

"(A cybersecurity control is a) measure that is modifying risk."

("ISO/SAE 21434:2021," 2021, p. 2)

Cybersecurity Property

"(A cybersecurity property is an) attribute that can be worth protecting. Attributes include confidentiality, integrity and/or availability."

("ISO/SAE 21434:2021," 2021, p.3)

Cybersecurity Risk

"(Cybersecurity risk is the) effect of uncertainty on road vehicle cybersecurity expressed in terms of attack feasibility and impact." ("ISO/SAE 21434:2021," 2021, p.4)

Damage Scenario

"(A damage scenario is an) adverse consequence involving a vehicle or vehicle function and affecting a road user."

("ISO/SAE 21434:2021," 2021, p.3)

Item

"Component or set of components that implements a function at the vehicle level. A system can be an item if it implements a function at the vehicle level, otherwise it is a component."

("ISO/SAE 21434:2021," 2021, p.3)

Example:

The Body Control Unit and the Headlamp System in a Headlamp System are items.

Impact

"(Impact is the) estimate of magnitude of damage or physical harm from a damage scenario."

("ISO/SAE 21434:2021," 2021, p.3)

Threat analysis and risk assessment (TARA)

"(A TARA) describes methods to determine the extent to which a road user can be impacted by a threat scenario. These methods and their work products are collectively known as a threat analysis and risk assessment (TARA) and are performed from the viewpoint of affected road users."

("ISO/SAE 21434:2021," 2021, p.41)

Threat Scenario

"(A threat scenario is a) potential cause of compromise of cybersecurity properties of one or more assets in order to realize a damage scenario."

("ISO/SAE 21434:2021," 2021, p.4)

Vulnerability

"(Vulnerability is a) weakness that can be exploited as part of an attack path." ("ISO/SAE 21434:2021," 2021, p.5)

D. The State of the Art

This section summarizes some of the existing Risk Specification and Risk Information Sharing standards. The list mentioned here is non-exhaustive and can expand in the future.

Non-Cybersecurity Risk Information Sharing Standards

Among well known risk exchange platforms or formats are **Common Risk Interchange Format (CRIF)**, formerly **International Swaps and Derivatives Association (ISDA)** or **Open Risk Management**, which focus mainly on finance and credit & equity risks, or Risk Data Open Standard, which focuses on the insurance industry. Other risk platforms can be found in Catastrophe Management and in the EU's Food and Feed Data Exchange. Further examples are Common Risk Assessment Framework (CRAF), Open Geospatial Consortium (OGC) standards, Virtual OSOCC Messaging Standard (VOMS), European Feed and Food Ingredients Database (EFSA), European Food Safety Authority (EFSA) OpenFoodTox, and Rapid Alert System for Food and Feed (RASFF). The research was further extended to include threat and control data exchange platforms.

Threat Data Exchange Platforms

Cyber threats are becoming an increasing problem for companies. In order to be able to recognize and react to threats as early as possible, it makes sense to share information and organize the exchange efficiently. The Structured Threat Information eXpression (**STIX**) language was developed for the exchange of cyber threat intelligence (Bacon, n.d.). "With STIX, all aspects of suspicion, compromise, and attribution can be represented clearly with objects and descriptive relationships. STIX information can be visually represented for an analyst or stored as JSON to be quickly machine-readable." (Introduction to STIX, n.d.)

The Trusted Automated eXchange of Indicator Information (**TAXII**) is a protocol for the automatic transport of data (*What Is Trusted Automated eXchange of Indicator Information (TAXII)? | NETSCOUT*, n.d.). The exchange procedure enables information to be exchanged across product and organizational boundaries.

Another format is **OpenIOC**. OpenIOC was developed in 2011 and is written in XML. The aim of the open framework is to share threat intelligence information such as Indicators of

Compromise (IoCs) within organizations and thus ensure a high level of protection (*Indicators of Compromise (IOC)*, n.d.).

In addition to the formats, there are also platforms and communities that have set themselves the goal of simplifying the exchange of threats. One is **MISP Threat Sharing**, an open-source threat intelligence and sharing platform with a JSON core format (*MISP Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing*, n.d.), and the other is **AlienVault Open Threat Exchange (OTX)**, an open threat intelligence community (*AlienVault - Open Threat Exchange*, n.d.). In OTX you can generate so-called pulses, which contain a summary of threats, for example, threat indicators, IP addresses, or file hashes. The pulses can be created from the official Alien vault account but also from anyone in the OTX community. So care must be taken when selecting pulses since the quality of the intelligence is dependent on the submitter. It is possible to subscribe to interesting pulses or authors and also to export the IoC data to OpenIOC, STIX, or CSV.

MISP is designed to help organizations store and share information about threats they have encountered. The platform enables companies to store data such as IP domains, email addresses, and other intelligence about the threats they have encountered (*MISP Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing*, n.d.).

MISP has a unique feature that allows it to identify connections between existing threats and new ones, allowing organizations to respond more quickly to emerging threats. It is a comprehensive repository of information that enables companies to learn from existing threats and respond to new ones. Additionally, MISP provides the ability to share information with the community. This feature allows companies to select what information they want to share and with whom.

To ensure that the shared information is trustworthy, MISP communities are limited to trusted partners and peers. This enables companies to share information with other organizations that they trust, while also receiving information from other sources such as law enforcement or security researchers. MISP's ability to facilitate the sharing of high-quality intelligence among trusted partners is critical in the fight against cyber threats.

Other platforms that support the exchange of threats are **Canadian Cyber Threat Exchange (CCTX)** and **IBM® X-Force Exchange.**

Vulnerability Exploitability eXchange (VEX)

The Vulnerability Exploitability eXchange, or VEX, is a framework designed to facilitate the exchange of data related to vulnerability exploitability. VEX provides a structured and standardized format for sharing information on vulnerabilities, their potential for exploitation, and associated risk factors. This framework is essential for exchanging risk-related data as it

enables organizations and security professionals to comprehensively assess and prioritize vulnerabilities based on their potential impact and ease of exploitation. By offering a common language and data structure for vulnerability information, VEX simplifies the process of sharing and understanding the risk landscape. This allows stakeholders to make more informed decisions about vulnerability management, mitigation strategies, and resource allocation, ultimately enhancing the overall security posture of software systems and networks. VEX plays a pivotal role in ensuring the efficient and effective exchange of risk-related data in the cybersecurity landscape.

CycloneDX

CycloneDX is an open standard in the product development and supply chain security. It serves as a common language for communicating information about software components and their dependencies, encapsulating this data in a structured format known as a Software Bill of Materials (SBOM). This standardized approach to cataloging software components supports exchanging risk-related data by providing a clear and common way to represent the building blocks of software applications. This, in turn, empowers organizations to make informed decisions about their software supply chain by enhancing their ability to identify vulnerabilities, assess licensing compliance, and manage software assets efficiently. CycloneDX simplifies the exchange of risk-related data but also constitutes a standardized asset format which supports other cyber security processes such as vulnerability management and incident response.

VERIS

The Vocabulary for Event Recording and Incident Sharing (VERIS) is a standardized framework that serves as a common language for recording and sharing data about security incidents and events. VERIS encompasses a comprehensive set of data fields and definitions, enabling organizations to describe security incidents in a consistent and structured manner. This standardization is vital for exchanging risk-related data as it ensures a shared understanding of security incidents, their attributes, and the associated impact. By utilizing VERIS, organizations can communicate security incident details accurately and effectively, fostering improved incident response, threat analysis, and risk assessment. This shared framework enhances collaboration among security professionals and organizations, enabling them to exchange critical information with precision, which is essential for making informed decisions in response to security incidents and managing risks effectively in an ever-evolving cybersecurity landscape. VERIS plays a crucial role in promoting standardized and effective data exchange in the realm of cybersecurity.

OSCAL

The OSCAL (Open Security Controls Assessment Language) is an information security assessment language designed to standardize and streamline the process of assessing and

documenting security controls within an organization. OSCAL provides a structured framework for expressing security controls, control baselines, and assessment results in a machine-readable format, ensuring consistency and interoperability across different assessment tools and platforms. By using OSCAL, organizations can effectively communicate security requirements, assess compliance, and share assessment results with stakeholders. OSCAL's modular and extensible nature allows for customization and adaptation to specific organizational needs, while its focus on automation and integration promotes efficiency and accuracy in the assessment process. With its growing adoption and support from industry-leading organizations, OSCAL is becoming a valuable asset in the information security community, simplifying and enhancing the assessment and management of security controls.

However, there exist some standards in this regard, e.g. OSCAL (a machine-readable standard for documenting and assessing IS security controls), NIST OSCAL (OSCAL: The Open Security Controls Assessment Language, n.d.), NISTIR 7693, Asset Identification Specification v1.1 | CSRC, SP 800-150 (NISTIR 7693, Asset Identification Specification V1.1 | CSRC, 2011), Guide to Cyber Threat Information Sharing | CSRC (NIST Special Publication (SP) 800-150, Guide to Cyber Threat Information Sharing, 2016).

E. Future Work

This specification is just in the beginning phases and even though it is published, there are many opportunities to continue the development and extend the use cases even further. We have identified some potential ideas that would be relevant for further development.

Risk Lifecycle Management

By nature, cybersecurity risk is not a static property, but changing over time. It is constantly evolving due to several factors:

First, continuous advancements in technology provide access to powerful computing resources and advanced analytics, enabling sophisticated attack scenarios that cybercriminals can execute for financial gain. Second, increased connectivity in digital systems, as well as changes in business environments such as the widespread shift to remote work during the pandemic increase the attack surface and thus the risk of cyberattacks. Third, cybercriminals adapt their tactics, techniques, and procedures (TTPs), hence security (counter-)measures must co-evolve.

Therefore, organizations need to continually revise and update risk-related data, and adapt their security measures to control risk in this constantly changing cybersecurity landscape. With additional tooling (e.g., model-based risk assessment methods), risk data can be automatically updated in “real time”. Although the completeness of risk models and their accuracy is limited

by human ability to correctly quantify the situational aspects of impact and attack feasibility, risk should still be captured systematically, qualitatively measured, prioritized, and addressed in a meaningful order. As tooling becomes available to calculate risk in “real time”, it will be required to introduce means to capture version information and change history for the risk assessment parameters. This will bring a new dimension of the data exchange format, and will be important for future data transfer scenarios.

Connection to Real-World Data (Intelligence)

Having a connection or relationship to field data and intelligence is crucial for effective cybersecurity. This is because such data can provide valuable insights into the latest trends, tactics, and techniques used by cybercriminals. By staying up-to-date on the latest intelligence, cybersecurity professionals can identify emerging threats and vulnerabilities and take proactive measures to prevent attacks.

Field data can be leveraged in several ways to enhance cybersecurity. For instance, organizations can use threat intelligence feeds to detect and respond to known threats and indicators of compromise (IOCs). SIEM data can also be used to identify unusual behavior and potential security breaches.

Furthermore, analyzing field data can help organizations develop targeted cybersecurity training and awareness programs for their employees. By understanding the most prevalent types of attacks and how they are carried out, organizations can educate their employees on best practices for avoiding common threats like phishing scams and social engineering attacks.

Information might not be specifically relevant for a product at a specific point in time, however it could be used later in the product life cycle. It is important to understand that relevance means only at that specific point in time.

In summary, field intelligence enables organizations to stay informed about emerging threats and vulnerabilities, take proactive measures to prevent attacks, and educate employees on best practices for staying secure online.

File Integrity

File integrity is a vital security property to protect data against accidental changes of data at rest or in transit. There are several techniques that can be used to establish file integrity, including checksums, and cryptographic hashing. Checksums involve computing a fingerprint for a file and then comparing it with the original value to detect any changes to the data. Cryptographic hashes are advanced fingerprinting methods that are sensitive to data manipulation, and robust against side-channel attacks. By maintaining file integrity, organizations can help to protect against simple forms of cyberattacks and accidental changes.

File integrity is usually implemented as part of a comprehensive security strategy that includes other security measures like access controls (reduce attack surface), encryption (ensure privacy), digital signatures (establish authenticity) and access monitoring. Only when implemented together, these security measures help to ensure the authenticity and confidentiality of data and provide protection against a wider range of cyber threats.

Partial Data Sharing

Partial data sharing is a method that allows for restricted sharing of confidential information while maintaining the privacy and security of data. This approach involves utilizing public key technologies to enable either full or partial encryption of data sections, which can be accessed only through authorized read or write permissions.

By utilizing partial data sharing, organizations can provide secure access to sensitive data while preventing unauthorized users from accessing or modifying it. This is particularly beneficial in situations where multiple parties require access to the same data, but each party needs to view or modify only specific sections of the data.

Public key technologies, including digital signatures and encryption, can be employed to ensure that the data is protected and accessible only to authorized users. This helps to mitigate the risk of data breaches, unauthorized access, and other security breaches.

In recent years, partial data sharing has gained popularity among organizations as a way to enhance data privacy and security while still enabling collaboration and sharing of information. By adopting this approach, organizations can maintain a balance between data accessibility and security, ensuring that sensitive data remains secure while being available to authorized parties.

Compatibility with AUTOSAR

It is necessary to consider the existing framework and specifications of AUTOSAR. The proposed framework should be designed in a way that is consistent with the layered architecture, standardized interfaces, and data exchange formats used in AUTOSAR. This will help to ensure that the ecosystem remains standardized, modular, and interoperable, as well as compatible with other components developed by different suppliers.

One approach to making the proposed framework compatible with AUTOSAR is to develop it as an extension to the existing AUTOSAR framework. This extension could include additional specifications and interfaces that enable the exchange of risk-related information between different components of the system.

Another approach is to develop a separate module that can be integrated into the existing AUTOSAR framework. This module would need to be designed in a way that is compatible with

the standard interfaces and data exchange formats used in AUTOSAR, enabling seamless integration with other components of the system.

Extendability

How third parties might be able to extend the existing schema for additional use cases, which are not included in this current version. These are specific entities which might be affected by or gain a value add to the use of OpenXSAM.

Modular

Since there are many existing file and data structures, the complete openXSAM format should be able to be integrated into existing formats that organizations are already using. Basically nesting the complete structure of the openXSAM format inside of an existing data structure. This is of course only possible if the existing standard supports such functionality.

F. Stakeholders

Original Equipment Manufacturers (OEMs)

These companies are the manufacturers and owners of the product risk. For example: General Motors, Ford, Chrysler, BMW, Volkswagen, Mercedes-Benz, etc.

ECU Suppliers

Suppliers that bring hardware and software parts together to perform functions and then are delivered for production at OEMs for end user products.

Managed Service Provider (MSP): Tier 2+

- Testers
- Security Analyst
- Threat Intelligence
- Compliance Team
- Auditors
- Tool Developers

Tier-X Suppliers

- Software Vendors
- Hardware Component (ASIC, IC, Microcontroller, etc.) Manufacturers

II. Use Cases

This section contains primary and secondary uses of the risk sharing information model described in this specification. While this specification does not formalize the interactions, it illustrates what the specified model can be used for.

A. OPXSAM_UC_001: Risk Information Sharing

The primary use case of OpenXSAM is to share risk information in a machine readable format. Using OpenXSAM, Security Analysts will be able to document and share the assets, as well as associated threat and risk information, and relevant cybersecurity controls for threat and risk mitigation. This information can then be shared and made available to various internal teams and services, external organizations and services, and to the wider public through an automated threat intelligence sharing platform. OpenXSAM schema will enable the Security Analysts to specify:

1. The vehicle system make information through the various assets, items, components, and related functions and data flow information that comprise the vehicle;
2. Cyber threat information through threat scenarios, attack steps, damage scenarios, risk, and impact information identified with the associated assets, items, components, and data flows;
3. Cybersecurity Controls needed to mitigate the identified threat and damage scenarios.

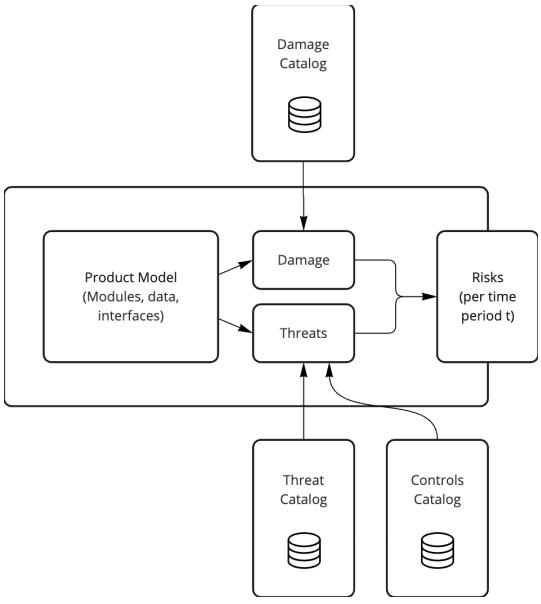

Fig. 1. OpenXSAM Use Case 01

Specifying the cyber threat information using the OpenXSAM schema coupled with the use of a threat intelligence platform to manage, and share this information will enable better risk management within the organization, reduce human error through automated data types, constraints, and integrity checks, enable better version control and traceability, and allow for information transparency and access through proper access control mechanisms and policies.

Properties

Short Name:	Share Product Definition
ID:	OPXSAM_UC_001_1
Description: (User Stories)	As a Security Analyst, I shall describe and share product metadata, that I analyzed and tested for security, in my risk information report that I share with my stakeholders so that they know the specifics of the items that were analyzed during the risk analysis process.
Subject Area:	Risk Information Sharing
Affected Phases:	Development, Operations
Stakeholders:	Security Analysts

Short Name:	Share Product Threat Exposure
ID:	OPXSAM_UC_001_2
Description: (User Stories)	As a Security Analyst, I should be able to share information on the various threat vectors that the product's attack surfaces are exposed to , that I identified during my security assessment of the product, in my risk information report that I share with my stakeholders so that they know the various attacks and threats that can impact the product. As a Security Analyst, I would like to share information regarding threats in risk to all stakeholders.

Subject Area:	Risk Information Sharing
Affected Phases:	Development, Operations
Stakeholders:	Security Analysts, Product, R&D

Short Name:	Share Impact and Damage Information
ID:	OPXSAM_UC_001_3
Description: (User Stories)	As a Security Analyst I should be able to describe and share my impact model, from my security modeling and assessment exercise, with my stakeholders so that they can be aware of the impact and damage on the system in case of a successful attack.
Subject Area:	Risk Information Sharing
Affected Phases:	Development, Operations
Stakeholders:	Security Analysts, Product, R&D, Executives

B. OPXSAM_UC_002: Test Plan Authoring

Security Test Plan Authoring is a secondary use case of OpenXSAM that will be able to be better informed and better managed because of the related information such as Vehicle Make through items, components, and related functions and data flows, and the associated Cyber Threat and Risk Information captured in a well-defined schema. Clause 9 of the ISO/SAE 21434 regulation requires that OEMS, tier 1 and 2 manufacturers, and security analysts provide high-quality documentation during the concept phase of a products lifecycle. Deliverables created during this period include item definitions, cybersecurity goals, and cybersecurity concepts, and mitigations from UNECE R155. During product testing a Test Plan is authored, based on the selected item definitions, cybersecurity controls, and UNECE R155 mitigations, either manually or through automated tools, to verify, validate, and test the cybersecurity of the system under test. The testing outcome is a Test Result Report which can be used to inform changes within a product's cybersecurity feature set.

Properties

Short Name:	Use shared Risk Information for Test Plan Authoring
ID:	OPXSAM_UC_002_1
Description: (User Stories)	As a security tester, I should be able to use the risk information that was shared with me about the product, especially information about product meta information, and attack surfaces, to author relevant security test cases to identify relevant attack vectors that the product is exposed to
Subject Area:	Pentesting, Red Teaming
Affected Phases:	Test Plan Authoring
Stakeholders:	Pentesters, Red Teamers, Security Analysts

Short Name:	Correlate Security Test Report with Risk Information Report
ID:	OPXSAM_UC_002_2
Description: (User Stories)	As a security tester, I should be able to include product reference in my security report that matches with product information in the Product Risk report, so that my audience can correlate the two reports together.
Subject Area:	Pentesting, Red Teaming
Affected Phases:	Reporting Test Findings
Stakeholders:	Security Testers, Security Analysts, Product, R&D, Executives

C. OPXSAM_UC_003: Automated Attack Surface Management (ASM) and Detection and Response (D&R)

ASM and D&R is a secondary use case of OpenXSAM which will leverage the OpenXSAM risk information model for risk-informed detection correlation and attack prediction across attack surfaces, and noise reduction. OpenXSAM will be used here to inform the ASM and D&R pipeline of the risks that have been identified in the vehicle. This information will be coupled with the AI and Machine Learning Models, Information Security Ontologies, and Impact Analytics for zoning in on crown jewels that have critical vulnerabilities, security event correlation, and situation-informed future attack prediction. Information shared through OpenXSAM will also be used to trigger automated workflows in the SOAR (Security Orchestration and Automation Response) platforms for patching critical vulnerabilities.

Properties

Short Name:	Log Ingestion
ID:	OPXSAM_UC_003_1
Description: (User Stories)	As a Security Engineer, I should be able to use the Product Risk Information Report shared with me to identify the relevant logs and telemetry that I should ingest at a bare minimum for continuous security monitoring of the product
Subject Area:	Managed Detection and Response (MDR)
Affected Phases:	Security telemetry and Log Ingestion
Stakeholders:	Security Engineers, Product

Short Name:	Detections Engineering
ID:	OPXSAM_UC_003_2

Description: (User Stories)	As a Security Engineer I should be able to use the Product Risk Information Report shared with me, to identify the security detections I can add to my Managed Detection and Response (MDR) pipeline for continuous security monitoring of the product
Subject Area:	Managed Detection and Response (MDR)
Affected Phases:	Detections Engineering
Stakeholders:	Security Engineers, Product

Short Name:	Behavioral Analytics
ID:	OPXSAM_UC_003_3
Description: (User Stories)	As a Cybersecurity AI Analyst I should be able to use the Product Risk Information Report shared with me, to build behavioral AI models and complex behavioral to detect threats in a timely fashion.
Subject Area:	Managed Detection and Response (MDR)
Affected Phases:	User and Behavior Analytics (UBA)
Stakeholders:	Data Scientists, Security Engineers, Product

D. OPXSAM_UC_004: Composition of individual TARAs (WIP)

Composition of individual TARAs is a secondary use case of openXSAM which will be needed for combining individual TARAs into a full vehicle TARA. The openXSAM scheme will be extended to contain information about the connections to other TARAs. In order to share this information in an easy and unified way, an overview of all possible individual TARAs within a vehicle will be developed. These individual TARAs will be given a standard name so that they can be identified. These names will be used as a standard for the creation of TARAs in the automotive industry. Based on this, the connections can be easily identified.

Properties

Short Name:	Whole vehicle TARA
ID:	OPXSAM_UC_004
Description: (User Stories)	As an OEM, I would like to create a full vehicle (product) TARA by combining already existing TARAs (from the supplier or OEM itself). In order to do so I need a connection between those independent TARAs. The basis for this can be achieved during development of TARAs by using standardized terms and formats to uniquely identify them based on name. Furthermore, already existing connections of individual TARAs can be displayed in XSAM (this is planned as an additional attribute in the header or as an additional element). As a supplier, I would like to create my TARAs in such a format that my customer is able to make full use of them and integrate them smoothly in their full vehicle TARA.
Subject Area:	Naming standard, whole vehicle tara
Affected Phases:	Development
Stakeholders:	OEMs

III. METHODS

There are many different methods regarding risk assessment and analysis. This paper is not focused on the methods, but based on particular methods to test the defined use cases. These methods include:

- TARA (Threat Assessment & Remediation Analysis)
- VARA (Vulnerability Assessment and Risk Analysis)
- MoRA (Modular Risk Assessment)

Threat Assessment and Remediation Analysis (TARA) is a methodology used to identify and assess cyber vulnerabilities and select countermeasures effective at mitigating those vulnerabilities. TARA is part of a MITRE portfolio of systems security engineering (SSE)

practices that focus on improving the cyber security hygiene and resilience of systems early in the acquisition process. TARA uses a catalog of stored attack vector and countermeasure data to inform the process of identifying attack vectors for exploiting system vulnerabilities and potential countermeasures to prevent their exploitation or mitigate its effects. TARA was originally developed in 2010.

VARA, or Vulnerability Assessment and Risk Analysis, is a systematic process for identifying, evaluating, and prioritizing vulnerabilities within an organization's information systems. It involves a comprehensive examination of potential weaknesses, their impact on the organization, and the likelihood of exploitation. VARA is crucial for exchanging risk-related data because it provides a structured approach to assess and communicate the level of risk associated with specific vulnerabilities.

Modular Risk Assessment (MoRA) has emerged as a pivotal approach in the field of risk management, with a history deeply rooted in the quest for more adaptable and precise risk evaluation. The concept of MoRA has evolved as a response to the increasingly complex and dynamic nature of modern risk landscapes. By breaking down the assessment process into modular components, MoRA allows for a more granular analysis of various risk factors, ensuring a comprehensive evaluation of potential threats. This modular approach has become instrumental in various industries, including finance, healthcare, and cybersecurity, as it offers a fine-grained perspective on risk and enables organizations to tailor their risk management strategies to specific vulnerabilities and scenarios. This white paper explores the historical development and paramount importance of MoRA, shedding light on its role in contemporary risk assessment practices and its contributions to more resilient and secure operations.

IV. Data Fields

A. ID

Each element in the data model has an user defined id field. The id is referred to as **localRef:id** in OpenXSAM. The ID is optional. However, when importing an XSAM file, it is advantageous to have IDs specified. This allows imported elements to be clearly assigned to existing elements.

B. UUID

All elements in the document can have additional external ID attribute. The external identifier is referred to as xmlns:ext in OpenXSAM. They will be used for identification if no localRef:id is set. The external IDs may be required, for example, due to data import from several systems.

C. Name

Each element in the data model has a unique name property which uniquely identifies it. The name property is mandatory.

D. References

The relationships between the individual elements/entities are defined by using references. These references enable the referenced elements to be uniquely identifiable. To uniquely identify the elements by references, certain formats must be followed. There are three ways to define a reference. A reference can be identified based on the ID, on a combination of type and name and on the external id. These possibilities will be examined in more detail in the following.

References Based on Name

Assigning

The format for assigning a name to an element is as follows: *name="BodyECU"*

Referencing to it

To identify an element via references based on name, a concept term and an element name need to be declared. It needs to be provided in the following format:

"name/<concept term>/<node name>”

In certain situations, the concept term is not known. Then the reference can be named as the following:

```
Unset
"name/*/<node name>”
```

Example:

```
Unset
target="name/CyberSecurityProperty/I"
target="name/*/I"
concept term = CyberSecurityProperty
element name = I (which stands for integrity)
```

References based on name without specifying the type: Sometimes you might not know the type of the target element. Then you can use name/*/TS.15.

Scope

When ids of elements are not known, it is necessary to be able to create references based on names. Furthermore, these references are more readable. For example, an attack rating of the knowledge factor level “EXPERT” would rather be name-based, because it is easier to build integrations with a readable format, and also because it is resilient over assessment-model changes.

References Based on External UUID

Assigning

The format for assigning an external id to an element is as follows:

ns0:id= "BodyECU” → external ID (see namespace)

Referencing to it

To identify an element via references based on external id, the keyword “ext”, a namespace and the external id need to be declared. It needs to be provided in the following format:

```
Unset
id="ext/<namespace>/<external id>"
```

In certain situations, the namespace does not exist or is not known. Then the reference can be named as the following:

```
Unset
id="ext/*/<id>"µ
```

Example:

```
Unset
target=ext/com.openxsam.io/BodyECU"
target=ext/ns0/BodyECU"
target=ext/*/BodyECU"
xmlns:ns0="com.openxsam.io"
ns0:id="BodyECU"
```

Scope

OpenXSAM allows optional external ids for all elements to build a traceability solution that knows dependencies down to the level of single elements, respecting organization-local flavors. It enables data exchange from external systems as well as repeated import since it holds the external id.

E. Inheritance

The openXSAM document has a tree structure with sub elements. These sub elements can span different modules. They can be identified with references and their individual IDs.

F. Extensions

- OpenXSAM has a standard format which is described in the data specification chapter. In addition, openXSAM offers the possibility to extend the content. This allows full control of attributes and customisation.
- Additional data can easily be added to the existing structure.
- If you want to add additional attributes to the standard format, they have to be marked with a namespace.

G. Grouping of Elements

- With grouping of elements, the organization of data can be improved by enabling a clear separation of concepts as well as a specific classification of content.

- It is possible to create sub-elements to enable the hierarchy of elements.

H. Contact Information (Referring to UC_001)

- OpenXSAM format provides the possibility to contact the relevant stakeholder if a threat is identified.
- A stakeholder is a company which is responsible for the content of the openXSAM file.
- The contact information can be found in the header section of the openXSAM file.

V. SPECIFICATION

This chapter describes the technical details regarding the above defined solution and covered use cases.

A. File Description

Ultimately, the goal of this specification is to generate a structured XSAM file to satisfy the use cases defined earlier. The XSAM file is based on the XML file format and it has the following properties.

File Type: *openXSAM*

File Extension: *.osam /.xsam*

Internet media type/MIME type: *application/xsam+xml*

An XSAM file can represent a complete model containing all modules (see definition in the next section) of the data specification, but it can also represent only individual modules such as item definition or threat catalog. openXSAM also offers the possibility to display only individual elements.

B. Module Overview

This specification is split into the following modules:

- Item definition (technical design description)
- Risk Assessment Module (calculated levels, treatment decisions, possibly including clause 9 things like requirements and cs goals and such, possibly including lifecycle things like validation status)
    - Risks
    - Cybersecurity Controls
    - Cybersecurity (CS) Concepts
    - Cybersecurity (CS) Claims
    - Assumptions
    - Transformations
- Attack Path Identification, Attack Feasibility Rating
- TARA artifacts:
    - Damage Scenarios
    - Threat scenarios
    - Attack steps
    - Attack Feasibility Rating
    - Impact Rating
- Method configuration (assessment model)
- Catalog (threats, controls solutions, technologies, component libraries)
- Vulnerability Management (Clause 8): Theoretical threats Incident Management (Clause 8)

C. Data Model

This section presents a comprehensive diagram showcasing the interrelationships among various data specification modules. The diagram features four distinct modules connected to one another, forming a cohesive network. The connections between the modules illustrate the flow and dependencies of data within the risk model. This visual representation provides a concise overview of the complex relationships that govern the organization and structure of data within the specified model.

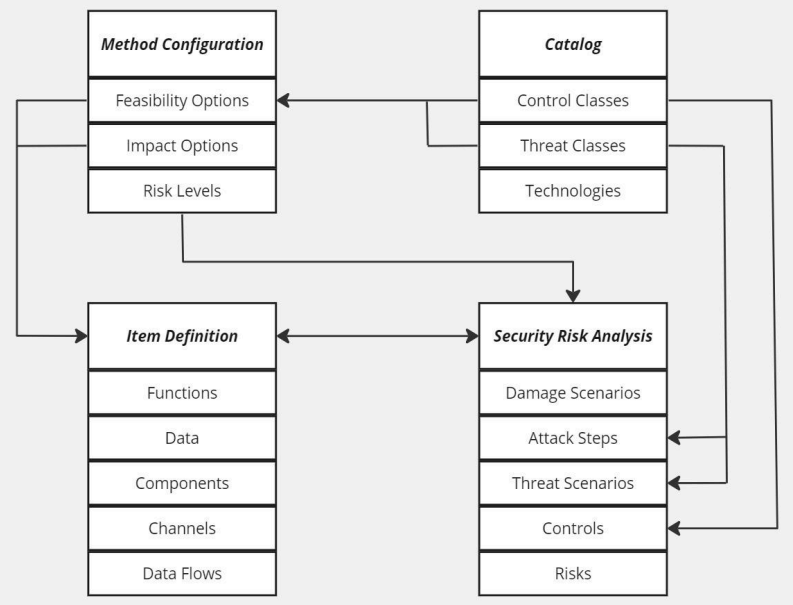

Fig. 2 - Overview of relationships between the Data Specification Modules

D. Data Specification

This section focuses on the fundamental components that define and describe the data within the system. It encompasses three key elements: the item definition module, functions, and data element descriptions. The *item definition* module establishes the structure and characteristics of individual data items, ensuring consistency and accuracy. *Functions* outline the operations and processes performed on the data, providing a clear understanding of its purpose and usage. Additionally, *data element descriptions* provide detailed explanations of the attributes and properties of each data element, facilitating effective data management and interpretation. Together, these components form a robust framework for specifying and understanding the data within the system.

Item Definition Module

The Item Definition is the first step of a TARA process and serves as the foundation to perform a risk assessment. Modeling an item involves identifying the functions, components, data, channels, and data flows. They can be structured into the same system specification chunk but it is preferable to put each entity in its unique chunk.

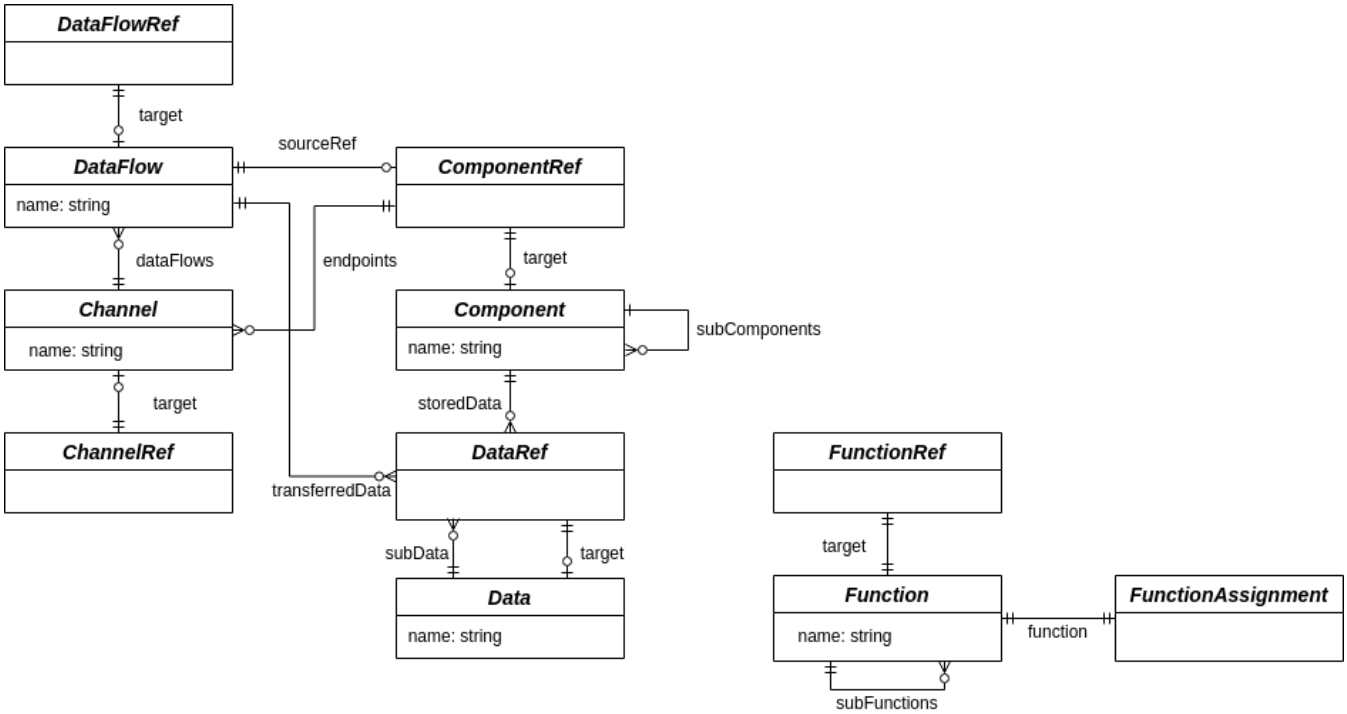

Fig 3: Entity Relationship - Item Definition

Functions

A function contains sub-functions:

```
<SystemChunk name="Functions" virtualPackage="Item Definition">
 <Elements>
  <Function description="Lamp Switch Off Request" id="OffFunc" name="OffFunc" title="Switch Headlamp Off">
   <SubFunctions>
    <Function description="" name="F.1">
     <SubFunctions/>
    </Function>
   </SubFunctions>
```

```
  </Function>
  <Function description="Lamp Switch On Request" name="OnFunc" title="Switch Headlamp On">
   <SubFunctions/>
  </Function>
 </Elements>
</SystemChunk>
```

Properties:

<Function>	Description	Required	Acceptable Values
id	An identifier to define or reference the function based on external sources	No	Free-Text
name	Uniquely identifies the function	Yes	Free-Text
title	A self-explanatory title for the function	No	Free-Text
description	Describes what the function does	No	Free-Text

Sub-Elements:

<SubFunctions>	List of subfunctions	0 up to many <Function>

Data

```
<SystemChunk id="Data" name="Data" virtualPackage="Item Definition">
  <Elements>
    <Data description="" id="OffMsg" name="OffMsg" title="Headlamp Off Message">
      <SubData/>
      <AssignedFunctions>
        <FunctionAssignment isLockedAssigned="false" isLockedDeassigned="false"
target="name/Function/OffFunc"/>
```

```
        </AssignedFunctions>
      </Data>
    </Elements>
</SystemChunk>
```

<Data>	Description	Required	Acceptable Values
id	An identifier to define or reference the data based on external sources	No	Free-Text
name	Uniquely identifies the data	Yes	Free-Text
title	A self-explanatory title for the data	No	Free-Text
description	Describes the data	No	Free-Text

Sub-Elements:

<SubData>	List of subdata	0 up to many <Data…>
<AssignedFunctions>	List of functions assigned to this data	0 up to many <FunctionAssignment…>

<FunctionAssignment>	Description	Required	Acceptable Values
isLockedAssigned		Yes	true OR false

isLockedDeassigned		Yes	true OR false
target		Yes	Reference to the Function defined "name/Function/<FunctionName>" OR “<namespace>/Functionid”

Sub-Elements:

No sub elements.

Components

A component may contain other components. It may store data (modeled by reference)

```
<SystemChunk id="Components" name="Components"
          virtualPackage="Item Definition">
  <Elements>
    <Component description="System component" id="Cmp.Sys" name="Cmp.0" title="System">
      <Technologies/>
      <StoredData/>
      <SubComponents>
        <Component description="" id="ExtECU" name="ExtECU" title="External ECUs">
          <Technologies>
            <TechnologyRef target="name/Technology/CAN" />
          </Technologies>
          <StoredData>
            <DataRef  target="name/Data/OnFunc"/>
          </StoredData>
          <SubComponents/>
          <AssignedFunctions/>
        </Component>
      </SubComponents>
      <AssignedFunctions/>
    </Component>
  </Elements>
</SystemChunk>
```

<Component>	Description	Required	Acceptable Values
id	An identifier to define or reference the component based on external sources	No	Free-Text
name	Uniquely identifies the component	Yes	Free-Text
title	A self-explanatory title for the component	No	Free-Text
description	Describes the component	No	Free-Text

Sub-Elements:

<SubComponents>	Subcomponents to the current component	0 up to many <Component…>
<Technologies>	Technologies used	0 up to many <TechnologyRef…>
<AssignedFunctions>	List of functions assigned to this component	0 up to many <FunctionAssignment…>
<StoredData>	Reference to the data stored.	0 up to many <DataRef…>

<TechnologyRef>	Reference to the technology used	No	

target		Yes	"name/Technology/<TechnologyName>" OR “<namespace>/Technologyid”

<FunctionAssignment>	Description	Required	Acceptable Values
isLockedAssigned		Yes	true OR false
isLockedDeassigned		Yes	true OR false
target		Yes	Reference to the Function defined "name/Functiont/<FunctionName>" OR “<namespace>/Functionid”

<DataRef>	Description	Required	Acceptable Values
id		No	
target		Yes	"name/Data/<DataName>" OR “<namespace>/Dataid”

Sub-Elements:

No sub-elements.

Channels & Data Flows

A Data Flow references the start- and endpoint (defined within a Channel).It may transfer data (modeled by reference). A Channel contains a number of endpoints. Each endpoint references one Component.

```
<SystemChunk id="Channels" name="Channels" virtualPackage="Item Definition">
  <Elements>
    <Channel description="" id="Ch.1" name="Ch.1" title="CAN Bus">
      <Endpoints>
      <ComponentRef id="Ch.1_BodyECU" target="name/Component/BodyECU"/>
    <ComponentRef id="Ch.1_PowSwitAct" target="name/Component/PowSwitAct"/>
        <ComponentRef id="Ch.1_GateECU" target="name/Component/GateECU"/>
      </Endpoints>
      <Technologies>
        <TechnologyRef target="name/Technology/CAN"/>
      </Technologies>
      <DataFlows>
        <DataFlow dataFlowTarget="ext/openxsam/io/Ch.1_PowSwitAct"
dataflowSource="ext/openxsam.io/Ch.1_BodyECU" description="" id="DF.6" name="DF.6" title="OnMsg,
OffMsg: BodyECU - PowSwitAct [CAN]">
          <Technologies/>
          <TransferredData>
            <DataRef target="name/Data/OnMsg"/>
            <DataRef target="name/Data/OffMsg"/>
          </TransferredData>
          <Technologies/>
          <AssignedFunctions>
            <FunctionAssignment isLockedAssigned="false" isLockedDeassigned="false"
target="name/Function/OffFunc"/>
            <FunctionAssignment isLockedAssigned="false" isLockedDeassigned="false"
target="name/Function/OnFunc"/>
          </AssignedFunctions>
        </DataFlow>
      </DataFlows>
      <AssignedFunctions>
        <FunctionAssignment isLockedAssigned="false" isLockedDeassigned="false"
target="name/Function/OffFunc"/>
        <FunctionAssignment isLockedAssigned="false" isLockedDeassigned="false"
target="name/Function/OnFunc"/>
      </AssignedFunctions>
    </Channel>
  </Elements>
</SystemChunk>
```

<Channel>	Description	Required	Acceptable Values
id	An identifier to define or reference the channel based on external sources	No	Free-Text
name	Uniquely identifies the channel	Yes	Free-Text
title	A self-explanatory title for the channel	No	Free-Text
description	Describes the channel	No	Free-Text

Sub-Elements:

<Endpoints>	The possible endpoints of the channel	0 up to many <ComponentRef…>
<DataFlows>	Possible dataflows between the channel endpoints	0 up to many <DataFlow…>
<Technologies>	Technologies used	0 up to many <Technology…>
<AssignedFunctions>	List of functions assigned to this channel	0 up to many <FunctionAssignment…>

<FunctionAssignment>	Description	Required	Acceptable Values
isLockedAssigned		Yes	true OR false

isLockedDeassigned		Yes	true OR false
target		Yes	Reference to the Function defined "name/Functiont/<FunctionName>" OR “<namespace>/Functionid”

Sub-Elements:

No sub-elements.

<DataFlow>	Description	Required	Acceptable Values
dataFlowTarget		Yes	Reference to an endpoint of the ancestor <Channel…> element
dataFlowSource		Yes	Reference to an endpoint of the ancestor <Channel…> element
description		No	
id		No	

Sub-Elements:

<Technologies>		0 up to many <TechnologyRef…>
<AssignedFunctions>	List of functions assigned to this data-flow	0 up to many <FunctionAssignment…>

<ComponentRef>	Description	Required	Acceptable Values
id		No	
target		Yes	"name/Component/<ComponentName>" OR “<namespace>/Componentid”

Sub-Elements:

No sub-elements.

TechnologyRef		No	
target		Yes	"name/Technology/<TechnologyName>" OR “<namespace>/Technologyid”

Method Configuration Module

This module outlines the specification for describing domain-specific sets of attack feasibility and impact options and the categories these options belong to. This information serves as the basis for all risk assessment and related calculations.

Listed below are structures for each of the entities in the method configuration.

Impact Model

Impact Model helps describe the impact on the system in case of a successful attack.

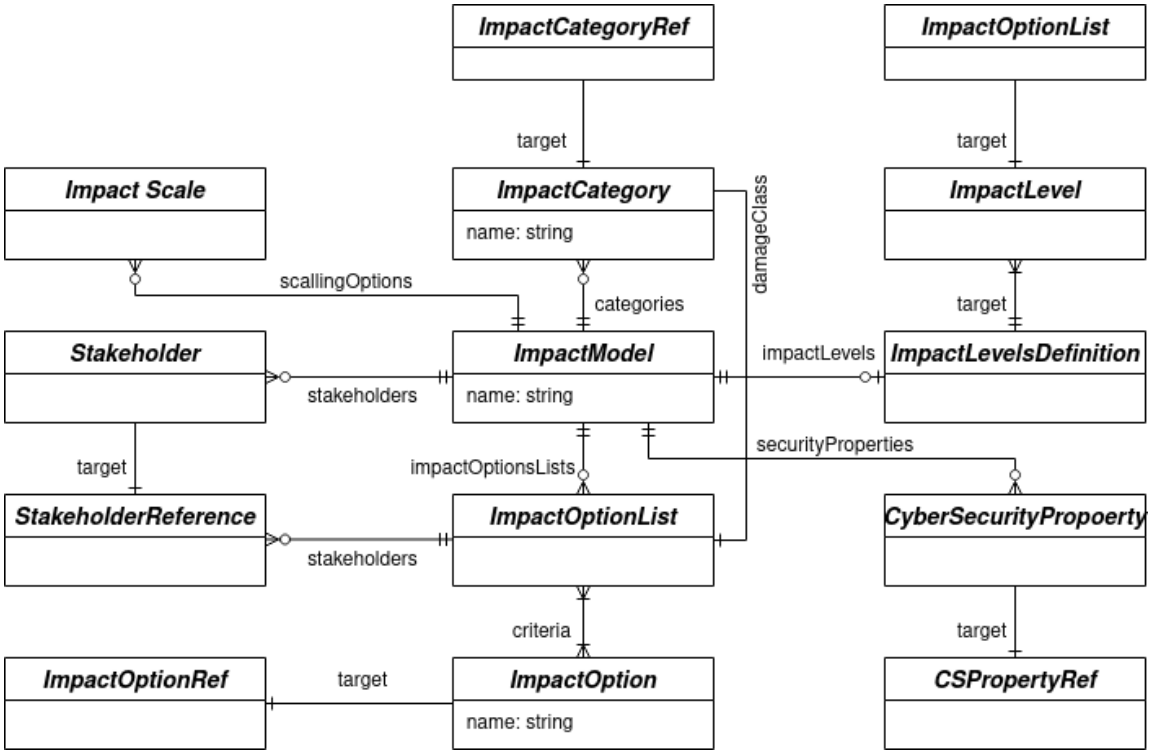

Fig 4: Entity Relationship - Impact Model

```
<ImpactModel id="ImpactModel" name="Impact Model" virtualPackage="Method Configuration">
   <CSProperties>
      <CyberSecurityProperty description="" id="Security_Property_1" name="C"
title="Confidentiality"></CyberSecurityProperty>
      <CyberSecurityProperty description="" id="Security_Property_2" name="I"
title="Integrity"></CyberSecurityProperty>
      <CyberSecurityProperty description="" id="Security_Property_3" name="A"
title="Availability"></CyberSecurityProperty>
   </CSProperties>
   <ImpactLevels>
      <ImpactLevelsDefinition id="LevelsDefinition">
         <Values>
            <ImpactLevel color="C4D79B" description="" id="Impact_Level_1" name="Neg" title="Negligible"
value="0"></ImpactLevel>
            <ImpactLevel color="FFFF99" description="" id="Impact_Level_2" name="Mod" title="Moderate"
value="1"></ImpactLevel>
            <ImpactLevel color="FFEB9C" description="" id="Impact_Level_3" name="Maj" title="Major"
value="2"></ImpactLevel>
            <ImpactLevel color="FFAAAA" description="" id="Impact_Level_4" name="Sev" title="Severe"
```

```
value="3"></ImpactLevel>
            </Values>
        </ImpactLevelsDefinition>
    </ImpactLevels>
    <Stakeholders>
        <Stakeholder description="" id="Stakeholder_1" name="RU" title="Road User"></Stakeholder>
        <Stakeholder description="" id="Stakeholder_2" name="OEM" title="Original Equipment
Manufacturer"></Stakeholder>
    </Stakeholders>
    <ImpactCategories>
        <ImpactCategory description="" hidden="false" id="Impact_Category_1" name="S"
title="Safety"></ImpactCategory>
        <ImpactCategory description="" hidden="false" id="Impact_Category_2" name="F"
title="Financial"></ImpactCategory>
        <ImpactCategory description="" hidden="false" id="Impact_Category_3" name="O"
title="Operational"></ImpactCategory>
        <ImpactCategory description="" hidden="false" id="Impact_Category_4" name="P"
title="Privacy"></ImpactCategory>
    </ImpactCategories>
    <ImpactOptionLists>
        <ImpactOptionList description="RU.S: Safety&amp;#10;Safety impact rating criteria are taken from ISO
26262-3:2018. Controllability and exposure in accordance with ISO 26262-3:2018 can also be considered for
rating impact on safety, if a rationale is provided." id="IO_List_1" name="RU.S"
refinedCategory="ext/com.openxsam.io/Impact_Category_1">
            <Stakeholders>
                <StakeholderReference target="name/Stakeholder/RU"/>
            </Stakeholders>
            <Criteria>
                <ImpactOption description="Rating for S0 can be based on ISO 26262-3:2018, Table B.1."
impactValue="0" id="Impact_Option_1" name="RU.S0" title="No injuries"></ImpactOption>
                <ImpactOption description="Light and moderate injury." impactValue="1" id="Impact_Option_2"
name="RU.S1" title="Light and moderate injuries"></ImpactOption>
                <ImpactOption description="Severe and life-threatening injury (survival probable)." impactValue="2"
id="Impact_Option_3" name="RU.S2" title="Severe injuries"></ImpactOption>
                <ImpactOption description="Life-threatening injuries (i.e., survival uncertain, fatal injuries)"
impactValue="3" id="Impact_Option_4" name="RU.S3" title="Life-threatening injuries"></ImpactOption>
            </Criteria>
        </ImpactOptionList>
        <ImpactOptionList description="RU.F: Financial" id="IO_List_1" name="RU.F"
refinedCategory="ext/com.openxsam.io/Impact_Category_2">
            <Stakeholders>
                <StakeholderReference id="4SjRD0NVDYy" target="name/Stakeholder/RU"/>
            </Stakeholders>
            <Criteria>
                <ImpactOption description="The financial damage leads to no effect, negligible consequences or is
```

```
irrelevant to the road user." impactValue="0" id="Impact_Option_5" name="RU.F0" title="Negligible losses"></ImpactOption>
            <ImpactOption description="The financial damage leads to inconvenient consequences which the affected road user will be able to overcome with limited resources." impactValue="1" id="Impact_Option_6" name="RU.F1" title="Moderate losses"></ImpactOption>
            <ImpactOption description="The financial damage leads to substantial consequences which the affected road user will be able to overcome." impactValue="2" id="Impact_Option_7" name="RU.F2" title="Substantial losses"></ImpactOption>
            <ImpactOption description="The financial damage leads to catastrophic consequences which the affected road user might not overcome." impactValue="3" id="Impact_Option_8" name="RU.F3" title="Personal bankruptcy"></ImpactOption>
         </Criteria>
      </ImpactOptionList>
   </ImpactOptionLists>
   <ScalingOptions>
      <ImpactScale description="" id="Scale_1" name="IS.1" title="Single" value="1"></ImpactScale>
      <ImpactScale description="" id="Scale_1" name="IS.3" title="Many" value="11"></ImpactScale>
   </ScalingOptions>
</ImpactModel>
```

<ImpactModel>	Description	Required	Acceptable Values
id	An identifier to define or reference the impact model based on external sources	No	Free-Text
name	Uniquely identifies the impact model	Yes	Free-Text
title	A self-explanatory title for the impact model	No	Free-Text
description	Describes the impact model	No	Free-Text

Sub-Elements:

<CSProperties…>		0 up to many <CyberSecurityProperty…>
<ImpactLevels…>		0 to many <ImpactLevelsDefinition>
<Stakeholders…>		0 to many <Stakeholder…>
<ImpactCategories>		0 to many <ImpactCategory...>
<ImpactOptionLists>		0 up to many <ImpactOptionList…>
<ScalingOptions…>		0 up to many <ImpactScale…>

<CyberSecurityProperty>	Description	Required	Acceptable Values
id	An identifier to define or reference based on external sources	No	Free-Text
name	Uniquely identifies the CyberSecurityProperty	Yes	Free-Text
title	A self-explanatory title for the CyberSecurityProperty	No	Free-Text

description	Describes the CyberSecurityProperty	No	Free-Text

<ImpactLevelsDefinition>	Description	Required	Acceptable Values
id		No	Free-Text

Sub-Elements:

<Values…>		0 up to many <ImpactLevel…>

<ImpactLevel>	Description	Required	Acceptable Values
color	A color that signifies the impact level	No	Free-Text
id	An identifier to define or reference based on external sources	No	Free-Text
name	Uniquely identifies the impact level	Yes	Free-Text
title	A self-explanatory title for the impact level	No	Free-Text
description	Describes the impact level	No	Free-Text

<Stakeholder>	Description	Required	Acceptable Values
id	An identifier to define or reference based on external sources	No	Free-Text
name	Uniquely identifies the stakeholder	Yes	Free-Text
title	A self-explanatory title for the stakeholder	No	Free-Text
description	Describes the stakeholder	No	Free-Text

<ImpactCategory>	Description	Required	Acceptable Values
hidden	Boolean to indicate if this is a hidden category	No	Free-Text
id	An identifier to define or reference based on external sources	No	Free-Text
name	Uniquely identifies the impact category	Yes	Free-Text
title	A self-explanatory title for the impact category	No	Free-Text

description	Describes the impact category	No	Free-Text

<ImpactOptionList>	Description	Required	Acceptable Values
refinedCategory	Reference to the refined impact category	Yes	"name/ImpactCategory/<ImpactCategoryName>" OR "<namespace>/<ImpactCategoryID>"
id	An identifier to define or reference based on external sources	No	Free-Text
name	Uniquely identifies the impact category	Yes	Free-Text
title	A self-explanatory title for the impact category	No	Free-Text
description	Describes the impact category	No	Free-Text

Sub-Elements:

<Stakeholders…>		0 up to many <StakeholderReference…>
<Criteria…>		0 up to many <ImpactOption…>

<ImpactOption>	Description	Required	Acceptable Values
impactValue	Integer value to quantify the impact option	Yes	Integer
id	An identifier to define or reference based on external sources	No	Free-Text
name	Uniquely identifies the impact option	Yes	Free-Text
title	A self-explanatory title for the impact option	No	Free-Text
description	Describes the impact option	No	Free-Text

<StakeholderReference>	Description	Required	Acceptable Values
id		No	Free-Text
target		Yes	"name/Stakeholder/<StakeholderName>" OR "<namespace>/<StakeholderID>"

Sub-Elements:

No sub-elements.

Attack Feasibility Model

Attack Feasibility Model helps describe the attack feasibility of executing a successful attack on a system.

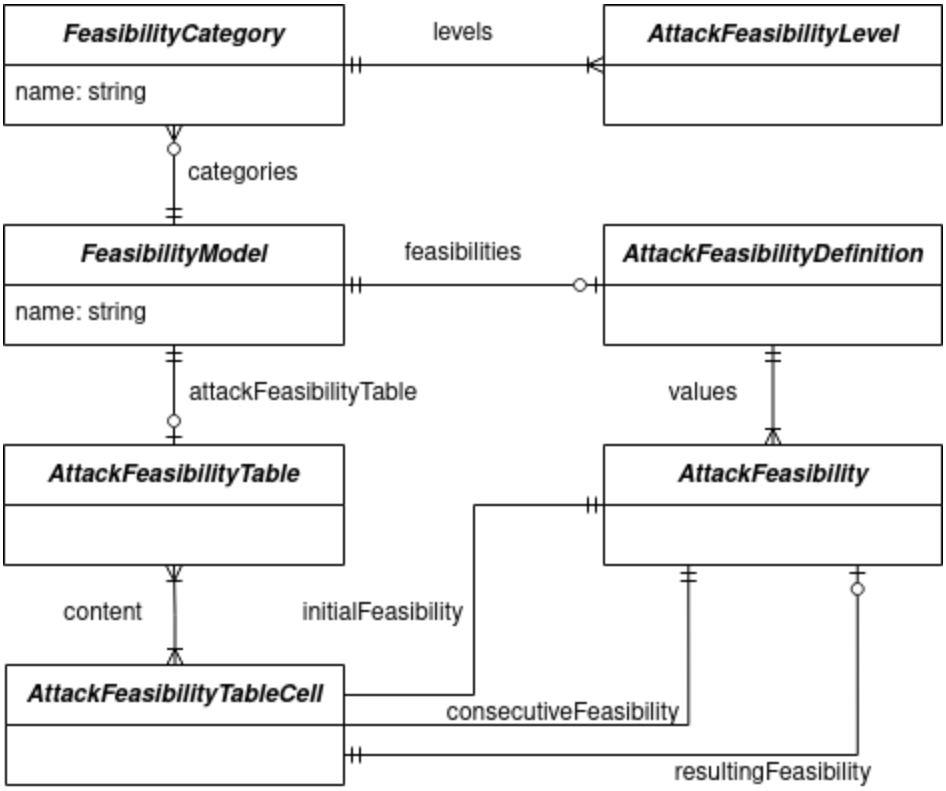

Fig 5: Entity Relationship - Attack Feasibility Model

```
<FeasibilityModel id="FeasibilityModel" name="Feasibility Model" virtualPackage="Method Configuration">
  <Categories>
    <FeasibilityCategory description="The elapsed time parameter includes the time to identify a vulnerability
```

```
and develop and (successfully) apply an exploit. Therefore, this rating is based on the state of expert knowledge at the time of rating." id="FeasibilityCategory_1" name="ET" title="Elapsed time">
        <Options>
          <FeasibilityOption description="" id="FeasibilityOption_1" name="ET0" title="≤ 1 day" value="0"></FeasibilityOption>
          <FeasibilityOption description="" id="FeasibilityOption_1" name="ET1" title="≤ 1 week" value="1"></FeasibilityOption>
        </Options>
      </FeasibilityCategory>
      <FeasibilityCategory description="The expertise parameter is related to the capabilities of the attacker, relative to their skill and experience." id="FeasibilityCategory_2" name="SE" title="Specialist expertise">
        <Options>
          <FeasibilityOption description="Unknowledgeable compared to experts or proficient persons, with no particular expertise.&#10;E.g. Ordinary person using step-by-step descriptions of an attack that is publicly available." id="FeasibilityOption_3" name="SE0" title="Layman" value="0"></FeasibilityOption>
          <FeasibilityOption description="Knowledgeable in that they are familiar with the security behaviour of the product or system type.&#10;E.g. Experienced owner, ordinary technician knowing simple and popular attacks like odometer tuning, installation of counterfeit parts." id="FeasibilityOption_4" name="SE1" title="Proficient" value="3"></FeasibilityOption>
        </Options>
      </FeasibilityCategory>
    </Categories>
    <FeasibilityLevels>
      <AFLsDefinition id="AFLsDefinition">
        <Values>
          <AttackFeasibilityLevel color="C4D79B" description="" minimalValue="25" id="AFL_1" name="Very Low"></AttackFeasibilityLevel>
          <AttackFeasibilityLevel color="FFFF99" description="" minimalValue="20" id="AFL_2" name="Low"></AttackFeasibilityLevel>
          <AttackFeasibilityLevel color="FFEB9C" description="" minimalValue="14" id="AFL_3" name="Medium"></AttackFeasibilityLevel>
          <AttackFeasibilityLevel color="FFAAAA" description="" minimalValue="0" id="AFL_4" name="High"></AttackFeasibilityLevel>
        </Values>
      </AFLsDefinition>
    </FeasibilityLevels>
    <FeasibilitiesTable>
      <AFLTable id="AFLTable">
        <Cells>
          <AFLTableCell consecutiveFeasibility="name/AttackFeasibilityLevel/Very Low" initialFeasibility="name/AttackFeasibilityLevel/Very Low" id="AFLTableCell_1" resultingFeasibility="name/AttackFeasibilityLevel/Very Low"/>
          <AFLTableCell consecutiveFeasibility="name/AttackFeasibilityLevel/Low" initialFeasibility="name/AttackFeasibilityLevel/Very Low" id="AFLTableCell_1" resultingFeasibility="name/AttackFeasibilityLevel/Very Low"/>
```

```
            <AFLTableCell consecutiveFeasibility="name/AttackFeasibilityLevel/Medium"
initialFeasibility="name/AttackFeasibilityLevel/Very Low" id="AFLTableCell_1"
resultingFeasibility="name/AttackFeasibilityLevel/Low"/>
            <AFLTableCell consecutiveFeasibility="name/AttackFeasibilityLevel/High"
initialFeasibility="name/AttackFeasibilityLevel/Very Low" id="AFLTableCell_1"
resultingFeasibility="name/AttackFeasibilityLevel/Medium"/>
          </Cells>
        </AFLTable>
    </FeasibilitiesTable>
</FeasibilityModel>
```

<FeasibilityModel>	Description	Required	Acceptable Values
id	An identifier to define or reference the feasibility model based on external sources	No	Free-Text
name	Uniquely identifies the feasibility model	Yes	Free-Text
title	A self-explanatory title for the feasibility model	No	Free-Text
description	Describes the feasibility model	No	Free-Text

Sub-Elements:

<Categories…>		0 up to many <FeasibilityCategory…>

<FeasibilityLevels …>		0 to many <AFLsDefinition…>
<FeasibilitiesTable …		0 to many <AFLTable…>

<FeasibilityCategory>	Description	Required	Acceptable Values
id	An identifier to define or reference based on external sources	No	Free-Text
name	Uniquely identifies the feasibility category	Yes	Free-Text
title	A self-explanatory title for the feasibility category	No	Free-Text
description	Describes the feasibility category	No	Free-Text

<AFLsDefinition>	Description	Required	Acceptable Values
id		No	Free-Text

Sub-Elements:

<Values…>		0 up to many <AttackFeasibilityLevel…>

<AttackFeasibilityLevel>	Description	Required	Acceptable Values
color	A color that signifies the feasibility level	No	Free-Text
id	An identifier to define or reference based on external sources	No	Free-Text
name	Uniquely identifies the feasibility level	Yes	Free-Text
minimalValue	Integer value that quantifies the feasibility level	Yes	Integer
description	Describes the feasibility level	No	Free-Text

<AFLTable>	Description	Required	Acceptable Values
id		No	Free-Text

Sub-Elements:

<Cells…>		0 up to many <AFLTableCell…>

<AFLTableCell>	Description	Required	Acceptable Values
initialFeasibility		Yes	"name/AttackFeasibilityLevel/<AttackFeasibilityLevelName>" OR "<namespace>/<AttackFeasibilityLevelID>"
id	An identifier to define or reference based on external sources	No	Free-Text
initialFeasibility		Yes	"name/AttackFeasibilityLevel/<AttackFeasibilityLevelName>" OR "<namespace>/<AttackFeasibilityLevelID>"
resultingFeasibility		Yes	"name/AttackFeasibilityLevel/<AttackFeasibilityLevelName>" OR "<namespace>/<AttackFeasibilityLevelID>"

Risk Model

Risk Model helps describe the risk levels based on the combination of information from impact and feasibility models.

```
<RiskModel name="Risk Model" virtualPackage="Method Configuration">
  <RiskLevels>
    <RiskLevelsDefinition>
      <Levels>
        <RiskLevel color="C6EFCE" description="" id="Level_1" name="1"></RiskLevel>
        <RiskLevel color="C4D79B" description="" id="Level_2" name="2"></RiskLevel>
        <RiskLevel color="FFEB9C" description="" id="Level_3" name="3"></RiskLevel>
        <RiskLevel color="FFCC99" description="" id="Level_4" name="4"></RiskLevel>
        <RiskLevel color="FFAAAA" description="" id="Level_5" name="5"></RiskLevel>
      </Levels>
    </RiskLevelsDefinition>
  </RiskLevels>
  <RiskTable>
    <RiskEvaluationTable id="Table_1">
      <Cells>
        <RiskEvaluationTableEntry feasibilityLevel="name/AttackFeasibilityLevel/Very Low"
impactLevel="name/ImpactLevel/Neg" id="Entry_1" resultingRiskLevel="name/RiskLevel/1"/>
        <RiskEvaluationTableEntry feasibilityLevel="name/AttackFeasibilityLevel/Very Low"
impactLevel="name/ImpactLevel/Mod" id="Entry_2" resultingRiskLevel="name/RiskLevel/1"/>
      </Cells>
    </RiskEvaluationTable>
  </RiskTable>
  <RiskTreatments>
    <RiskTreatmentsDefinition id="TreatmentDefinition">
      <Treatments>
        <RiskTreatment description="" id="Def_1" name="Av" title="Avoidance"></RiskTreatment>
        <RiskTreatment description="" id="Def_2" name="R" title="Reduction"></RiskTreatment>
        <RiskTreatment description="" id="Def_3" name="SoT" title="Share or Transfer"></RiskTreatment>
        <RiskTreatment description="" id="Def_4" name="Ac" title="Acceptance"></RiskTreatment>
      </Treatments>
    </RiskTreatmentsDefinition>
  </RiskTreatments>
</RiskModel>
```

<RiskModel>	Description	Required	Acceptable Values

id	An identifier to define or reference the feasibility model based on external sources	No	Free-Text
name	Uniquely identifies the risk model	Yes	Free-Text

Sub-Elements:

<RiskLevels…>		0 to many <RiskLevelsDefinition…>
<RiskTable…>		0 to many <RiskEvaluationTable…>
<RiskTreatments…>		0 up to many RiskTreatmentsDefinition…>

<RiskLevelsDefinition>	Description	Required	Acceptable Values
id		No	Free-Text

Sub-Elements:

<Levels>		0 up to many <RiskLevel…>

<RiskLevel>	Description	Required	Acceptable Values
color	A color that signifies the risk level	No	Free-Text

id	An identifier to define or reference based on external sources	No	Free-Text
name	Uniquely identifies the risk level	Yes	Free-Text
description	Describes the risk level	No	Free-Text

<RiskEvaluationTable>	Description	Required	Acceptable Values
id		No	Free-Text

Sub-Elements:

<Cells…>		0 up to many <RiskEvaluationTableEntry…>

<RiskEvaluationTableEntry>	Description	Required	Acceptable Values
feasibilityLevel		Yes	"name/AttackFeasibilityLevel/<AttackFeasibilityLevelName>" OR "<namespace>/<AttackFeasibilityLevelID>"

id	An identifier to define or reference based on external sources	No	Free-Text
impactLevel		Yes	"name/ImpactLevel/<ImpactLevelLevelName>" OR “<namespace>/<ImpactLevelLevelID>”
resultingRiskLevel		Yes	"name/RiskLevel/<RiskLevelName>" OR “<namespace>/<RiskLevelID>”

<RiskTreatmentsDefinition>	Description	Required	Acceptable Values
id		No	Free-Text

Sub-Elements:

<Treatments…>		0 up to many <RiskTreatment…>

<RiskTreatment>	Description	Required	Acceptable Values
title	A self-explanatory title for the risk treatment	No	Free-Text

id	An identifier to define or reference based on external sources	No	Free-Text
name	Uniquely identifies the risk treatment	Yes	Free-Text
description	Describes the risk treatment	No	Free-Text

Risk Assessment Module

Risk Assessments are important elements of the process of Risk Management. To perform a comprehensive risk assessment, security elements like cybersecurity risks, Assumptions, Cybersecurity Controls, Damage Scenarios, Threat Scenarios need to be described in detail. These entities can be structured into the same security specification chunk but it is preferable to put each entity in its unique chunk.

Listed below are structures for each of the entities in the Risk Assessment.

Assumptions

Assumptions are required properties of a system that are needed to accomplish cybersecurity goals.

```
<SecurityChunk id="Assumptions" name="Assumptions" virtualPackage="Security Analysis">
  <Elements>
    <Assumption description="The item is physically protected by anti-tamper enclosures, which is an
assumption on the operational environment." id="A.1" name="A.1" title="Physical Protection">
      <MaxRL>
        <RiskLevelRef target="name/RiskLevel/1"/>
      </MaxRL>
      <MaxIL>
        <ImpactLevelRef target="name/ImpactLevel/Neg"/>
```

```
        </MaxIL>
        <MaxAFL>
          <AttackFeasibilityLevelRef  target="name/AttackFeasibilityLevel/Very Low"/>
        </MaxAFL>
        <Effects>
          <TransformDamageScenario>
            <Source>
              <DamageScenarioRef damageScenario="ext/com.openxsam.io/DS.1" />
            </Source>
            <Target>
              <DamageScenarioRef damageScenario="ext/com.openxsam.io/DS.2"/>
            </Target>
          </TransformDamageScenario>
        </Effects>
        <InstantiatedClasses>
          <AssumptionClassRef target="ext/com.openxsam.io/AC.1"/>
        </InstantiatedClasses>
      </Assumption>
    </Elements>
</SecurityChunk>
```

<Assumption>	Description	Required	Acceptable Values
id	An identifier to define or reference the assumption based on external sources	No	Free-Text
name	Uniquely identifies the assumption	Yes	Free-Text
title	A self-explanatory title for the assumption	No	Free-Text
description	Describes the assumption	No	Free-Text

Sub-Elements:

<InstantiatedClasses…>		0 up to many <AssumptionClassRef…>
<MaxRL>		0 to 1 <RiskLevelRef…>
<MaxIL>		0 to 1 <ImpactLevelRef…>
<MaxAFL>		0 to 1 <AttackFeasibilityLevelRef..>
<Effects>		0 up to many <TransformImpactOption…> 0 up to many <TransformDamageScenario…> 0 up to 1 <RemoveAllDamage>

<RiskLevelRef>	Description	Required	Acceptable Values
id		No	Free-Text
target		Yes	"name/RiskLevel/RiskLevelName" OR “<namespace>/<RiskLevelid>”

Sub-Elements:

No sub-elements.

<ImpactLevelRef>	Description	Required	Acceptable Values
id		No	Free-Text
target		Yes	"name/ImpactLevel/<ImpactlevelName>" OR “<namespace>/<ImpactLevelid>”

Sub-Elements:

No sub-elements.

<AttackFeasibilityLevelRef>	Description	Required	Acceptable Values
id		No	Free-Text
target		Yes	"name/AttackFeasibilityLevel/<AFName>" OR “<namespace>/<AFid>”

Sub-Elements:

No sub-elements.

<TransformDamageScenario>	Description	Required	Acceptable Values

id		No	Free-Text

Sub-Elements:

<Source>		1 <DamageScenarioRef…>
<Target>		0 to 1 <DamageScenarioRef…>

<DamageScenarioRef>	Description	Required	Acceptable Values
id		No	Free-Text
damageScenario		Yes	"name/DamageScenario/<DSName>" OR “<namespace>/<DSid>”

Sub-Elements:

No sub-elements.

<TransformImpactOption>	Description	Required	Acceptable Values
id		No	Free-Text

Sub-Elements:

<Source>		1 <ImpactOptionRef…>

<Target>		0 to 1 <ImpactOptionRef…>

<ImpactLevelRef>	Description	Required	Acceptable Values
id		No	Free-Text
damageScenario		Yes	"name/ImpactOption/<IOName>" OR "<namespace>/<IOid>"

Sub-Elements:

No sub-elements.

Threat Scenarios

A threat scenario is a potential, rather high level attack. It realizes one or many damage scenarios and consists of a set of attack paths (oftentimes also called attack tree).

```
<SecurityChunk id="ThreatScenarios" name="Threat Scenarios" virtualPackage="Security Analysis">
  <Elements>
    <ThreatScenario description="" id="TS.1" name="TS.1" threatenedBy="AS.1" lessenedBy="A.1"
title="Spoofing on CAN Bus">
      <CauseOfCompromise>
        <ThreatClassRef target="ext/com.openxsam.io/TC.1"/>
      </CauseOfCompromise>
      <ActedOnTOEEs>
        <ChannelRef target="ext/com.openxsam.io/Ch.1"/>
      </ActedOnTOEEs>
      <CustomImpactCombinator/>
      <CustomFeasibilityCombinator/>
      <DamageScenarios>
        <DamageScenarioRef damageScenario="ext/com.openxsam.io/DS.1"/>
        <DamageScenarioRef damageScenario="ext/com.openxsam.io/DS.2"/>
      </DamageScenarios>
```

```
        <Compromises>
          <DeriveCompromisedAssets/>
        </Compromises>
      </ThreatScenario>
    </Elements>
</SecurityChunk>
```

<ThreatScenario>	Description	Required	Acceptable Values
id	An identifier to define or reference the threat scenario based on external sources	No	Free-Text
name	Uniquely identifies the threat scenario	Yes	Free-Text
title	A self-explanatory title for the threat scenario	No	Free-Text
description	Describes the threat scenario	No	Free-Text
lessenedBy	Assumptions that dampen the effect of threat Scenario	No	<AssumptionName>
threatenedBy	Identifying Attack Step	No	<AttackStepName>

Sub-Elements:

<CauseofCompromise …>		0 to 1 <ThreatClassRef…>

<ActedOnTOEEs…>		0 up to many <ComponentRef…>, <ChannelRef…>, <DataRef…>
<CustomImpactCombinator…>		
<CustomFeasibilityCombinator…>		
<DamageScenarios…>		0 up to many <DamageScenarioRef…>

<ThreatClassRef>	Description	Required	Acceptable Values
id		No	Free-Text
target		Yes	"name/Class/<TCName>" OR "<namespace>/<TCid>"

Sub-Elements:

No sub-elements.

<DamageScenarioRef>	Description	Required	Acceptable Values
id		No	Free-Text
damageScenario		Yes	"name/DamageScenario/<DSName>"

			OR “<namespace>/<DSid>”

Sub-Elements:

No sub-elements.

Damage Scenarios

The damage scenario should describe the general damage that can occur to a company when the security goals of that asset (item) can not be met. Damage scenarios describe the adverse consequences (of one or multiple threats) on a vehicle or vehicle function that are affecting the road user.

```
<SecurityChunk id="DamageScenarios" name="Damage Scenarios" virtualPackage="Security Analysis">
  <Elements>
    <DamageScenario description="Unexpected loss of your lamps during adverse conditions during driving may cause a crash, severe safety impact and degradation of functionality, but survival likely." id="DS.1" name="DS.1" normalBehavior="Headlamp stays on" operationalSituation="driving at highway" title="Headlamp turns off unexpectedly">
      <ImpactRatings>
        <ImpactTuple impactCategory="name/ImpactCategory/S">
          <ImpactRating>
            <ImpactRating option="name/ImpactOption/RU.S3"/></ImpactRating>
        </ImpactTuple>
        <ImpactTuple impactCategory="name/ImpactCategory/F">
          <ImpactRating>
            <ImpactRating option="name/ImpactOption/RU.F0"/></ImpactRating>
        </ImpactTuple>
        <ImpactTuple impactCategory="name/ImpactCategory/O">
          <ImpactRating>
            <ImpactRating option="name/ImpactOption/RU.O2"/></ImpactRating>
        </ImpactTuple>
        <ImpactTuple impactCategory="name/ImpactCategory/P">
          <ImpactRating>
            <ImpactRating option="name/ImpactOption/RU.P0"/></ImpactRating>
        </ImpactTuple>
      </ImpactRatings>
      <ConcernedAssets>
        <QualifiedAssetList>
          <QualifiedAssets>
```

```
                <QualifiedAsset>
                  <CsProperty>
                    <CSPropertyRef target="name/CyberSecurityProperty/I"/>
                  </CsProperty>
                  <Toee>
                    <FunctionRef target="ext/com.openxsam.io/F.1"/>
                  </Toee>
                </QualifiedAsset>
              </QualifiedAssets>
            </QualifiedAssetList>
          </ConcernedAssets>
          <Scale/>
          <Todos/>
        </DamageScenario>
    </Elements>
</SecurityChunk>
```

<DamageScenario>	Description	Required	Acceptable Values
id	An identifier to define or reference the damage scenario based on external sources	No	Free-Text
name	Uniquely identifies the damage scenario	Yes	Free-Text
title	A self-explanatory title for the damage scenario	No	Free-Text
description	Describes the damage scenario	No	Free-Text
normalBehavior			
operationalSituation			

Sub-Elements:

<ImpactRatings…>		0 up to many <ImpactTuple…>
<ConcernedAssets…>		0 up to many <QualifiedAsset…>

<ImpactTuple>	Description	Required	Acceptable Values
id		No	Free-Text
impactCategory		Yes	"name/ImpactCategory/<ICName>" OR "<namespace>/<ICid>"

Sub-Elements:

<ImpactRatings…>		0 up to many <ImpactRating…>

<ImpactRating>	Description	Required	Acceptable Values
id		No	Free-Text
option		Yes	"name/ImpactOption/<IOName>" OR "<namespace>/<IOid>"

Rationale		Yes	Free-Text

Sub-Elements:

No sub-element.

<QualifiedAsset>	Description	Required	Acceptable Values
id		No	Free-Text

Sub-Elements:

<CsProperty…>		1 <CSPropertyRef…>
<ActedOnTOEE…>		1 <ComponentRef…> OR <ChannelRef…> OR <DataRef…> OR <FunctionRef…>

<CSPropertyRef>	Description	Required	Acceptable Values
id		No	Free-Text
target		Yes	"name/CyberSecurityProperty/<SPName>" OR "<namespace>/<SPid>"

Sub-Elements:

No sub-elements.

Attack Steps

Attack paths (or steps) are a sequence of deliberate actions to realize one or multiple threat scenarios.

```
<SecurityChunk id="AttackSteps" name="Attack Steps" virtualPackage="Security Analysis">
  <Elements>
    <AttackStep description="" mitigatedBy="C.2" id="AS.1" name="AS.1" refinedBy="AS.2" riskLevel="4"
title="Spoofing - CAN Bus">
      <InstantiatedClass>
        <ThreatClassRef target="ext/com.openxsam.io/TC.1"/>
      </InstantiatedClass>
      <ActedOnTOEEs>
        <ChannelRef target="ext/com.openxsam.io/Ch.1"/>
      </ActedOnTOEEs>
      <InitialFeasibilityOptions/>
      <ConsecutiveFeasibilityOptions/>
      <ExplicitInitialFeasibility/>
      <ExplicitConsecutiveFeasibility/>
      <CustomImpactCombinator/>
      <CustomFeasibilityCombinator/>
      <FeasibilityModel/>
    </AttackStep>
  </Elements>
</SecurityChunk>
```

<AttackStep>	Description	Required	Acceptable Values
id	An identifier to define or reference the attack step based on external sources	No	Free-Text

name	Uniquely identifies the attack step	Yes	Free-Text
title	A self-explanatory title for the attack step	No	Free-Text
description	Describes the attack step	No	Free-Text / Structured data / <any>

Sub-Elements:

<InstantiatedClass…>	The threat class this Attack Step instantiates	0 up to many <ThreatClassRef…>
<ActedOnTOEEs…>		0 up to many <ComponentRef…>, <ChannelRef…>, <DataRef…>
<InitialFeasibilityOptions…>		0 to many <FeasibilityRating…>
<ConsecutiveFeasibilityOptions…>		0 to many <FeasibilityRating…>
<InitialExplicitFeasibility..>		0 to many <FeasibilityRating…>
<ConsecutiveExplicitFeasibility…>		0 to many <FeasibilityRating…>
<CustomImpactCombinator…>		
<CustomFeasibilityCombinator…>		

Cybersecurity Controls

A Cybersecurity Control mitigates a given attack step or threat scenario or modifies the risk, resulting in risk reduction.

```
<SecurityChunk id="Controls" name="Controls" virtualPackage="Security Analysis">
  <Elements>
    <Control dependsOn="may(TS.2, TS.3)" description="" id="C.2" name="C.2" title="Whitelisting CAN
Messages">
      <InstantiatedControlClass>
        <SecurityControlClassRef target="ext/com.openxsam.io/CC.3"/>
      </InstantiatedControlClass>
      <ControlGroups/>
      <InitialFeasibilityOptions/>
      <ConsecutiveFeasibilityOptions/>
      <InitialExplicitFeasibility/>
      <ConsecutiveExplicitFeasibility/>
      <ActedOnTOEEs/>
        <Effects>
          <TransformDamageScenario>
            <Source>
              <DamageScenarioRef damageScenario="ext/com.openxsam.io/DS.1" />
            </Source>
            <Target>
              <DamageScenarioRef damageScenario="ext/com.openxsam.io/DS.2"/>
            </Target>
          </TransformDamageScenario>
          <TransformImpactOption>
            <Source>
              <ImpactOptionRef target="name/ImpactOption/RU.P2"/>
            </Source>
            <Target>
              <ImpactOptionRef target="name/ImpactOption/RU.P3"/>
            </Target>
          </TransformImpactOption>
          <RemoveAllDamage />
          <RemoveImpactOption>
            <Option>
              <ImpactOptionRef target="name/ImpactOption/RU.O0"/>
            </Option>
          </RemoveImpactOption>
          <RemoveDamageScenario>
            <Scenario>
              <DamageScenarioRef damageScenario="ext/com.openxsam.io/DS.3"/>
            </Scenario>
          </RemoveDamageScenario>
        </Effects>
      <CustomImpactCombinator/>
      <CustomFeasibilityCombinator/>
      <FeasibilityModel/>
```

```
        <Todos/>
      </Control>
    </Elements>
</SecurityChunk>
```

<Control>	Description	Required	Acceptable Values
id	An identifier to define or reference the control based on external sources	No	Free-Text
name	Uniquely identifies the control	Yes	Free-Text
title	A self-explanatory title for the control	No	Free-Text
description	Describes the control	No	Free-Text
dependsOn	List of threat Scenarios this control depends on	No	Free-Text
explicitlyNotModeled			true OR false

Sub-Elements:

<InstantiatedControlClass…>		0 up to many <SecurityControlClassRef…>
<ActedOnTOEEs…>		0 up to many <ComponentRef…>, <ChannelRef…>, <DataRef…>
<InitialFeasibilityOptions…>		0 to many <FeasibilityRating…>

<ConsecutiveFeasibilityOptions …>		0 to many <FeasibilityRating…>
<InitialExplicitFeasibility..>		
<ConsecutiveExplicitFeasibility …>		
<CustomImpactCombinator…>		
<CustomFeasibilityCombinator …>		
<Effects>		0 up to many <TransformImpactOption…> 0 up to many <TransformDamageScenario…> 0 up to 1 <RemoveAllDamage>

Control Scenarios

```
<SecurityChunk id="ControlScenarios" name="Control Scenarios" virtualPackage="Security Analysis">
  <Elements>
    <Scenario description="" isDefault="false" id="Sc.1" name="Sc.1" title="One">
      <Controls>
        <SecurityControlSelector target="ext/com.openxsam.io/C.1"/>
      </Controls>
    </Scenario>
    <Scenario description="" isDefault="true" id="Sc.2" name="Sc.2" title="All Controls">
      <Controls>
        <AllControls />
      </Controls>
    </Scenario>
  </Elements>
</SecurityChunk>
```

<ControlScenario>	Description	Required	
id	An identifier to define or reference the control scenario based on external sources	No	Free-Text
name	Uniquely identifies the control scenario	Yes	Free-Text
title	A self-explanatory title for the control scenario	No	Free-Text
description	Describes the control scenario	No	Free-Text

Sub-Elements:

<Controls…>		0 up to many <SecurityControlSelector…>

Threat

A Risk illustrates the risk level present on a threat scenario, attack step, or cybersecurity control.

```
<SecurityChunk id="SecurityChunk_Risks" name="Risks" virtualPackage="Security Analysis">
  <Elements>
    <Risk description="" id="R.1" name="R.1" title="Denial of Service on Gateway ECU, Whitelist of CAN Messages">
      <CausedByElements>
        <ThreatScenarioRef target="ext/com.openxsam.io/TS.3"/>
      </CausedByElements>
    </Risk>
  </Elements>
</SecurityChunk>
```

<Threat>	Description	Required	Acceptable Values
id	An identifier to define or reference the threat based on external sources	No	Free-Text
name	Uniquely identifies the threat	Yes	Free-Text
title	A self-explanatory title for the threat	No	Free-Text
description	Describes the threat	No	Free-Text

Sub-Elements:

<CausedByElements...>		0 up to many <ThreatScenarioRef…> 0 up to many <AttackStepRef…>

<ThreatScenarioRef>	Description	Required	Acceptable Values
id		No	Free-Text

target		Yes	"name/ThreatScenario/<TSName>" OR “<namespace>/<TSid>”

Sub-Elements:

No sub-element.

<AttackStepRef>	Description	Required	Acceptable Values
id		No	Free-Text
target		Yes	"name/AttackStep/<ASName>" OR “<namespace>/<ASid>”

Sub-Elements:

No sub-element.

Threat Catalog Module

```
<ThreatsCatalog id="ThreatsCatalog" name="ThreatClasses" virtualPackage="Catalog">
  <ThreatClasses>
    <ThreatClass description="Identity spoofing refers to the action of assuming (i.e., taking on) the identity of some other entity (human or non-human) and then using that identity to accomplish a goal." id="TC.1" name="TC.1" title="Spoofing">
      <ThreatenedSecurityProperties>
        <CSPropertyRef target="name/CyberSecurityProperty/C"/>
        <CSPropertyRef target="name/CyberSecurityProperty/I"/>
```

```
        </ThreatenedSecurityProperties>
        <Architecture>
          <DataFlowSecurityTarget />
          <ChannelSecurityTarget />
        </Architecture>
        <InitialFeasibilityOptions>
          <FeasibilityRating category="name/FeasibilityCategory/SE" id="Rating.1"
option="name/FeasibilityOption/SE0"/>
          <FeasibilityRating category="name/FeasibilityCategory/WoO" id="Rating.2"
option="name/FeasibilityOption/WoO0"/>
          <FeasibilityRating category="name/FeasibilityCategory/Eq" id="Rating.3"
option="name/FeasibilityOption/Eq0"/>
          <FeasibilityRating category="name/FeasibilityCategory/KoIC" id="Rating.4"
option="name/FeasibilityOption/KoIC1"/>
          <FeasibilityRating category="name/FeasibilityCategory/ET" id="Rating.5"
option="name/FeasibilityOption/ET0"/>
        </InitialFeasibilityOptions>
        <ConsecutiveFeasibilityOptions/>
        <Technologies>
          <TechnologyRef target="ext/com.openxsam.io/CAN"/>
        </Technologies>
      </ThreatClass>
    </ThreatClasses>
</ThreatsCatalog>
```

<ThreatClass>	Description	Required	Acceptable Values
id	An identifier to define or reference the threat class based on external sources	No	Free-Text
name	Uniquely identifies the threat class	Yes	Free-Text
title	A self-explanatory title for the threat class	No	Free-Text

description	Describes the threat class	No	Free-Text

Sub-Elements:

<ThreatenedSecurityProperties...>		0 up to many <CyberSecurityPropertyRef…>
<Architecture>		0 up to many <ComponentSecurityTarget…> 0 up to many <DataFlowSecurityTarget…> 0 up to many <ChannelSecurityTarget…>
<InitialFeasibilityOptions..>		0 up to many <FeasibilityRating…>
<ConsecutiveFeasibilityOptions…>		0 up to many <FeasibilityRating…>

<CyberSecurityPropertyRef>	Description	Required	Acceptable Values
id		No	Free-Text
target		Yes	"name/CyberSecurityProperty/<SPName>" OR “<namespace>/<SPid>”

Sub-Elements:

No sub-elements.

<FeasibilityRating>	Description	Required	Acceptable Values
id		No	Free-Text
option		Yes	"name/FeasibilityOption/<FOName>" OR “<namespace>/<FOid>”
category		Yes	"name/FeasibilityCategory/<FCName>" OR “<namespace>/<FCid>”

Sub-Elements:

No sub-elements.

Cybersecurity Control Catalog Module

```
<SecurityControlsCatalog id="ControlCatalog" name="ControlClasses" virtualPackage="Catalog">
  <ControlClasses>
    <SecurityControlClass description="" id="CC.1" name="CC.1" title="Symmetric encryption">
      <Protects>
        <CSPropertyRef target="name/CyberSecurityProperty/C"/>
      </Protects>
      <ProtectsAgainst>
        <ThreatClassRef target="name/ThreatClass/TC.4"/>
        <ThreatClassRef target="name/ThreatClass/TC.4a"/>
      </ProtectsAgainst>
      <Architecture>
        <ComponentSecurityTarget />
        <DataFlowSecurityTarget />
        <ChannelSecurityTarget />
      </Architecture>
```

```
        <Technologies/>
        <Dependencies/>
        <InitialFeasibilityOptions>
          <FeasibilityRating category="name/FeasibilityCategory/SE" id="Rating.1"
option="name/FeasibilityOption/SE1"/>
          <FeasibilityRating category="name/FeasibilityCategory/WoO" id="Rating.2"
option="name/FeasibilityOption/WoO0"/>
          <FeasibilityRating category="name/FeasibilityCategory/ET" id="Rating.3"
option="name/FeasibilityOption/ET0"/>
          <FeasibilityRating category="name/FeasibilityCategory/Eq"  id="Rating.4"
option="name/FeasibilityOption/Eq0"/>
          <FeasibilityRating category="name/FeasibilityCategory/KoIC" id="Rating.5"
option="name/FeasibilityOption/KoIC0"/>
        </InitialFeasibilityOptions>
        <ConsecutiveFeasibilityOptions/>
        <FeasibilityModel/>
      </SecurityControlClass>
   </ControlClasses>
</SecurityControlsCatalog>
```

<SecurityControlClass>	Description	Required	Acceptable Values
id	An identifier to define or reference the risk based on external sources	No	Free-Text
name	Uniquely identifies the risk	Yes	Free-Text
title	A self-explanatory title for the risk	No	Free-Text
description	Describes the risk	No	Free-Text

Sub-Elements:

<Protects...>		0 up to many <CyberSecurityPropertyRef…>
<ProtectsAgainst...>		0 up to many <ThreatClassRef…>
<Architecture>		0 up to many <ComponentSecurityTarget…> 0 up to many <DataFlowSecurityTarget…> 0 up to many <ChannelSecurityTarget…>
<InitialFeasibilityOptions..>		0 up to many <FeasibilityRating…>
<ConsecutiveFeasibilityOptions …>		0 up to many <FeasibilityRating…>

<CyberSecurityPropertyRef>	Description	Required	Acceptable Values
id		No	Free-Text
target		Yes	"name/CyberSecurityProperty/<SPName>" OR “<namespace>/<SPid>”

Sub-Elements:

No sub-elements.

<FeasibilityRating>	Description	Required	Acceptable Values
id		No	Free-Text
option		Yes	"name/FeasibilityOption/<FOName>" OR “<namespace>/<FOid>”
category		Yes	"name/FeasibilityCategory/<FCName>" OR “<namespace>/<FCid>”

Sub-Elements:

No sub-elements.

VI. Appendix

A. The XML Scheme Definition (XSD)

Functions

```
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
 <xs:element name="SystemChunk">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="Elements">
     <xs:complexType>
      <xs:sequence>
       <xs:element name="Function" minOccurs="1" maxOccurs="1">
        <xs:complexType>
         <xs:sequence>
          <xs:element name="SubFunctions" minOccurs="1" maxOccurs="unbounded">
           <xs:complexType mixed="true">
            <xs:sequence>
             <xs:element name="Function" minOccurs="0" maxOccurs="unbounded">
              <xs:complexType>
```

```
                    <xs:sequence>
                     <xs:element type="xs:string" name="SubFunctions" minOccurs="0"
maxOccurs="unbounded"/>
                    </xs:sequence>
                    <xs:attribute type="xs:string" name="description"/>
                    <xs:attribute type="xs:string" name="id"/>
                    <xs:attribute type="xs:string" name="name" use="required"/>
                    <xs:attribute type="xs:string" name="title"/>
                   </xs:complexType>
                  </xs:element>
                 </xs:sequence>
                </xs:complexType>
               </xs:element>
              </xs:sequence>
              <xs:attribute type="xs:string" name="description"/>
              <xs:attribute type="xs:string" name="id"/>
              <xs:attribute type="xs:string" name="name" use="required"/>
              <xs:attribute type="xs:string" name="title"/>
             </xs:complexType>
            </xs:element>
           </xs:sequence>
          </xs:complexType>
         </xs:element>
        </xs:sequence>
        <xs:attribute type="xs:string" name="id"/>
        <xs:attribute type="xs:string" name="name" use="required"/>
        <xs:attribute type="xs:string" name="virtualPackage"/>
       </xs:complexType>
      </xs:element>
</xs:schema>
```

Data

```
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
 <xs:element name="SystemChunk">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="Elements">
     <xs:complexType>
      <xs:sequence>
       <xs:element name="Function" minOccurs="1" maxOccurs="unbounded">
        <xs:complexType>
         <xs:sequence>
          <xs:element name="SubFunctions" minOccurs="1" maxOccurs="1">
```

```
            <xs:complexType mixed="true">
              <xs:sequence>
                <xs:element name="Function" minOccurs="0" maxOccurs="unbounded">
                  <xs:complexType>
                    <xs:sequence>
                      <xs:element type="xs:string" name="SubFunctions" minOccurs="0"
maxOccurs="unbounded"/>
                    </xs:sequence>
                    <xs:attribute type="xs:string" name="description"/>
                    <xs:attribute type="xs:string" name="id"/>
                    <xs:attribute type="xs:string" name="name" use="required"/>
                    <xs:attribute type="xs:string" name="title"/>
                  </xs:complexType>
                </xs:element>
              </xs:sequence>
            </xs:complexType>
          </xs:element>
        </xs:sequence>
        <xs:attribute type="xs:string" name="description"/>
        <xs:attribute type="xs:string" name="id"/>
        <xs:attribute type="xs:string" name="name" use="required"/>
        <xs:attribute type="xs:string" name="title"/>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
  <xs:attribute type="xs:string" name="id"/>
  <xs:attribute type="xs:string" name="name" use="required"/>
  <xs:attribute type="xs:string" name="virtualPackage"/>
 </xs:complexType>
</xs:element>
</xs:schema>
```

Components

```
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
 <xs:element name="SystemChunk">
  <xs:complexType>
   <xs:sequence>
```

```
<xs:element name="Elements">
 <xs:complexType>
  <xs:sequence>
   <xs:element name="Component" minOccurs="1" maxOccurs="unbounded">
    <xs:complexType>
     <xs:element name="Technologies" minOccurs="1" maxOccurs="1"/>
      <xs:complexType mixed="true">
       <xs:sequence>
        <xs:element name="TechnologyRef" minOccurs="0" maxOccurs="unbounded">
         <xs:complexType>
          <xs:simpleContent>
           <xs:extension base="xs:string">
            <xs:attribute type="xs:string" name="id"/>
            <xs:attribute type="xs:string" name="target" use="required"/>
           </xs:extension>
          </xs:simpleContent>
         </xs:complexType>
        </xs:element>
       </xs:sequence>
      </xs:complexType>
     <xs:element name="StoredData" minOccurs="1" maxOccurs="1"/>
      <xs:complexType mixed="true">
       <xs:sequence>
        <xs:element name="DataRef" minOccurs="0" maxOccurs="unbounded">
         <xs:complexType>
          <xs:simpleContent>
           <xs:extension base="xs:string">
            <xs:attribute type="xs:string" name="id"/>
            <xs:attribute type="xs:string" name="target" use="required"/>
           </xs:extension>
          </xs:simpleContent>
         </xs:complexType>
        </xs:element>
       </xs:sequence>
      </xs:complexType>
     <xs:element name="SubComponents" minOccurs="1" maxOccurs="unbounded">
      <xs:complexType>
       <xs:sequence>
        <xs:element name="Component" minOccurs="0" maxOccurs="unbounded">
         <xs:complexType>
          <xs:sequence>
           <xs:element name="Technologies" minOccurs="0" maxOccurs="1"/>
            <xs:complexType mixed="true"/>
             <xs:sequence>
              <xs:element name="TechnologyRef" minOccurs="0" maxOccurs="unbounded">
```

```
            <xs:complexType>
              <xs:simpleContent>
                <xs:extension base="xs:string">
                  <xs:attribute type="xs:string" name="id"/>
                  <xs:attribute type="xs:string" name="target" use="required"/>
                </xs:extension>
              </xs:simpleContent>
            </xs:complexType>
          </xs:element>
        </xs:sequence>
      <xs:element name="StoredData" minOccurs="0" maxOccurs="1"/>
        <xs:complexType mixed="true">
          <xs:sequence>
            <xs:element name="DataRef" minOccurs="0" maxOccurs="unbounded">
              <xs:complexType>
                <xs:simpleContent>
                  <xs:extension base="xs:string">
                    <xs:attribute type="xs:string" name="id"/>
                    <xs:attribute type="xs:string" name="target" use="required"/>
                  </xs:extension>
                </xs:simpleContent>
              </xs:complexType>
            </xs:element>
          </xs:sequence>
        </xs:complexType>
      <xs:element name="SubComponents" minOccurs="0" maxOccurs="unbounded"/>
        <xs:complexType>
          <xs:sequence>
            <xs:element name="Component" minOccurs="0" maxOccurs="unbounded">
          </xs:sequence>
        </xs:complexType>
      <xs:element name="AssignedFunctions" minOccurs="0" maxOccurs="1"/>
        <xs:complexType>
          <xs:sequence>
            <xs:element name="FunctionAssignment" minOccurs="0" maxOccurs="1">
              <xs:complexType>
                <xs:simpleContent>
                  <xs:extension base="xs:string">
                    <xs:attribute type="xs:string" name="isLockedAssigned"/>
                    <xs:attribute type="xs:string" name="isLockedDeassigned"/>
                    <xs:attribute type="xs:string" name="target" use="required"/>
                  </xs:extension>
                </xs:simpleContent>
              </xs:complexType>
            </xs:element>
```

```
                    </xs:sequence>
                   </xs:complexType>
                  </xs:sequence>
                  <xs:attribute type="xs:string" name="description"/>
                  <xs:attribute type="xs:string" name="id"/>
                  <xs:attribute type="xs:string" name="name" use="required"/>
                  <xs:attribute type="xs:string" name="title"/>
                 </xs:complexType>
                </xs:element>
               </xs:sequence>
              </xs:complexType>
             </xs:element>
             <xs:element name="AssignedFunctions" minOccurs="1" maxOccurs="1">
              <xs:complexType>
               <xs:sequence>
                <xs:element name="FunctionAssignment" minOccurs="0" maxOccurs="1">
                 <xs:complexType>
                  <xs:simpleContent>
                   <xs:extension base="xs:string">
                    <xs:attribute type="xs:string" name="isLockedAssigned"/>
                    <xs:attribute type="xs:string" name="isLockedDeassigned"/>
                    <xs:attribute type="xs:string" name="target" use="required"/>
                   </xs:extension>
                  </xs:simpleContent>
                 </xs:complexType>
                </xs:element>
               </xs:sequence>
              </xs:complexType>
             </xs:element>
            <xs:attribute type="xs:string" name="description"/>
            <xs:attribute type="xs:string" name="id"/>
            <xs:attribute type="xs:string" name="name" use="required"/>
            <xs:attribute type="xs:string" name="title"/>
           </xs:complexType>
          </xs:element>
         </xs:sequence>
        </xs:complexType>
       </xs:element>
    </xs:sequence>
    <xs:attribute type="xs:string" name="id"/>
    <xs:attribute type="xs:string" name="name" use="required"/>
    <xs:attribute type="xs:string" name="virtualPackage"/>
   </xs:complexType>
  </xs:element>
</xs:schema>
```

Channels and Data Flows

```
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
 <xs:element name="SystemChunk">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="Elements">
     <xs:complexType>
      <xs:sequence>
       <xs:element name="Channel" minOccurs="1" maxOccurs="unbounded">
        <xs:complexType>
         <xs:element name="Endpoints" minOccurs="1" maxOccurs="1">
          <xs:complexType>
           <xs:sequence>
            <xs:element name="ComponentRef" minOccurs="0" maxOccurs="unbounded">
             <xs:complexType>
              <xs:simpleContent>
               <xs:extension base="xs:string">
                <xs:attribute type="xs:string" name="id"/>
                <xs:attribute type="xs:string" name="target" use="required"/>
               </xs:extension>
              </xs:simpleContent>
             </xs:complexType>
            </xs:element>
           </xs:sequence>
          </xs:complexType>
         </xs:element>
         <xs:element name="Technologies" minOccurs="1" maxOccurs="1">
          <xs:complexType>
           <xs:sequence>
            <xs:element name="TechnologyRef" minOccurs="0" maxOccurs="unbounded">
             <xs:complexType>
              <xs:simpleContent>
               <xs:extension base="xs:string">
                <xs:attribute type="xs:string" name="id"/>
                <xs:attribute type="xs:string" name="target" use="required"/>
               </xs:extension>
              </xs:simpleContent>
             </xs:complexType>
            </xs:element>
           </xs:sequence>
          </xs:complexType>
         </xs:element>
```

```
<xs:element name="DataFlows" minOccurs="1" maxOccurs="1">
 <xs:complexType>
  <xs:sequence>
   <xs:element name="DataFlow" minOccurs="0" maxOccurs="unbounded">
    <xs:complexType>
     <xs:choice maxOccurs="unbounded" minOccurs="0">
      <xs:element name="Technologies" minOccurs="1" maxOccurs="1"/>
       <xs:complexType mixed="true">
        <xs:sequence>
         <xs:element name="TechnologyRef" minOccurs="0" maxOccurs="1">
          <xs:complexType>
           <xs:simpleContent>
            <xs:extension base="xs:string">
             <xs:attribute type="xs:string" name="id"/>
             <xs:attribute type="xs:string" name="target" use="required"/>
            </xs:extension>
           </xs:simpleContent>
          </xs:complexType>
         </xs:element>
        </xs:sequence>
       </xs:complexType>
       <xs:element name="TransferredData" minOccurs="1" maxOccurs="1">
        <xs:complexType mixed="true">
         <xs:sequence>
          <xs:element name="DataRef" minOccurs="0" maxOccurs="unbounded" >
           <xs:complexType>
            <xs:simpleContent>
             <xs:extension base="xs:string">
              <xs:attribute type="xs:string" name="id"/>
              <xs:attribute type="xs:string" name="target" use="required"/>
             </xs:extension>
            </xs:simpleContent>
           </xs:complexType>
          </xs:element>
         </xs:sequence>
        </xs:complexType>
       </xs:element>
       <xs:element name="AssignedFunctions" minOccurs="1" maxOccurs="1">
        <xs:complexType>
         <xs:sequence>
          <xs:element name="FunctionAssignment" minOccurs="0" maxOccurs="1">
           <xs:complexType>
            <xs:simpleContent>
             <xs:extension base="xs:string">
              <xs:attribute type="xs:string" name="isLockedAssigned"/>
```

```
                        <xs:attribute type="xs:string" name="isLockedDeassigned"/>
                        <xs:attribute type="xs:string" name="target" use="required"/>
                      </xs:extension>
                    </xs:simpleContent>
                  </xs:complexType>
                </xs:element>
              </xs:sequence>
            </xs:complexType>
          </xs:element>
        </xs:choice>
        <xs:attribute type="xs:string" name="dataFlowTarget" use="required"/>
        <xs:attribute type="xs:string" name="dataflowSource" use="required"/>
        <xs:attribute type="xs:string" name="description"/>
        <xs:attribute type="xs:string" name="id"/>
        <xs:attribute type="xs:string" name="name" use="required"/>
        <xs:attribute type="xs:string" name="title"/>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
 </xs:complexType>
</xs:element>
<xs:element name="AssignedFunctions" minOccurs="1" maxOccurs="1">
 <xs:complexType>
  <xs:sequence>
   <xs:element name="FunctionAssignment" minOccurs="0" maxOccurs="1">
    <xs:complexType>
     <xs:simpleContent>
      <xs:extension base="xs:string">
       <xs:attribute type="xs:string" name="isLockedAssigned"/>
       <xs:attribute type="xs:string" name="isLockedDeassigned"/>
       <xs:attribute type="xs:string" name="target" use="required"/>
      </xs:extension>
     </xs:simpleContent>
    </xs:complexType>
   </xs:element>
  </xs:sequence>
 </xs:complexType>
</xs:element>
<xs:attribute type="xs:string" name="description"/>
<xs:attribute type="xs:string" name="id"/>
<xs:attribute type="xs:string" name="name" use="required"/>
<xs:attribute type="xs:string" name="title"/>
</xs:complexType>
</xs:element>
</xs:sequence>
```

```
        </xs:complexType>
       </xs:element>
     </xs:sequence>
     <xs:attribute type="xs:string" name="id"/>
     <xs:attribute type="xs:string" name="name" use="required"/>
     <xs:attribute type="xs:string" name="virtualPackage"/>
   </xs:complexType>
  </xs:element>
</xs:schema>
```

Assumptions

```
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="SecurityChunk">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="Elements">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="Assumption">
                <xs:complexType>
                  <xs:sequence>
                    <xs:element name="MaxRL">
                      <xs:complexType>
                        <xs:sequence>
                          <xs:element name="RiskLevelRef">
                            <xs:complexType>
                              <xs:simpleContent>
                                <xs:extension base="xs:string">
                                  <xs:attribute type="xs:string" name="target"/>
                                </xs:extension>
                              </xs:simpleContent>
                            </xs:complexType>
                          </xs:element>
                        </xs:sequence>
                      </xs:complexType>
                    </xs:element>
                    <xs:element name="MaxIL">
                      <xs:complexType>
                        <xs:sequence>
                          <xs:element name="ImpactLevelRef">
                            <xs:complexType>
                              <xs:simpleContent>
```

```
            <xs:extension base="xs:string">
              <xs:attribute type="xs:string" name="target"/>
            </xs:extension>
          </xs:simpleContent>
        </xs:complexType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="MaxAFL">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="AttackFeasibilityLevelRef">
        <xs:complexType>
          <xs:simpleContent>
            <xs:extension base="xs:string">
              <xs:attribute type="xs:string" name="target"/>
            </xs:extension>
          </xs:simpleContent>
        </xs:complexType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="Effects">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="TransformDamageScenario">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="Source">
              <xs:complexType>
                <xs:sequence>
                  <xs:element name="DamageScenarioRef">
                    <xs:complexType>
                      <xs:simpleContent>
                        <xs:extension base="xs:string">
                          <xs:attribute type="xs:string" name="damageScenario"/>
                        </xs:extension>
                      </xs:simpleContent>
                    </xs:complexType>
                  </xs:element>
                </xs:sequence>
              </xs:complexType>
            </xs:element>
```

```
                <xs:element name="Target">
                  <xs:complexType>
                    <xs:sequence>
                      <xs:element name="DamageScenarioRef">
                        <xs:complexType>
                          <xs:simpleContent>
                            <xs:extension base="xs:string">
                              <xs:attribute type="xs:string" name="damageScenario"/>
                            </xs:extension>
                          </xs:simpleContent>
                        </xs:complexType>
                      </xs:element>
                    </xs:sequence>
                  </xs:complexType>
                </xs:element>
              </xs:sequence>
            </xs:complexType>
          </xs:element>
          <xs:element name="TransformImpactOption">
            <xs:complexType>
              <xs:sequence>
                <xs:element name="Source">
                  <xs:complexType>
                    <xs:sequence>
                      <xs:element name="ImpactOptionRef">
                        <xs:complexType>
                          <xs:simpleContent>
                            <xs:extension base="xs:string">
                              <xs:attribute type="xs:string" name="target"/>
                            </xs:extension>
                          </xs:simpleContent>
                        </xs:complexType>
                      </xs:element>
                    </xs:sequence>
                  </xs:complexType>
                </xs:element>
                <xs:element name="Target">
                  <xs:complexType>
                    <xs:sequence>
                      <xs:element name="ImpactOptionRef">
                        <xs:complexType>
                          <xs:simpleContent>
                            <xs:extension base="xs:string">
                              <xs:attribute type="xs:string" name="target"/>
                            </xs:extension>
```

```
                </xs:simpleContent>
               </xs:complexType>
              </xs:element>
             </xs:sequence>
            </xs:complexType>
           </xs:element>
          </xs:sequence>
         </xs:complexType>
        </xs:element>
        <xs:element type="xs:string" name="RemoveAllDamage"/>
        <xs:element name="RemoveImpactOption">
         <xs:complexType>
          <xs:sequence>
           <xs:element name="Option">
            <xs:complexType>
             <xs:sequence>
              <xs:element name="ImpactOptionRef">
               <xs:complexType>
                <xs:simpleContent>
                 <xs:extension base="xs:string">
                  <xs:attribute type="xs:string" name="target"/>
                 </xs:extension>
                </xs:simpleContent>
               </xs:complexType>
              </xs:element>
             </xs:sequence>
            </xs:complexType>
           </xs:element>
          </xs:sequence>
         </xs:complexType>
        </xs:element>
        <xs:element name="RemoveDamageScenario">
         <xs:complexType>
          <xs:sequence>
           <xs:element name="Scenario">
            <xs:complexType>
             <xs:sequence>
              <xs:element name="DamageScenarioRef">
               <xs:complexType>
                <xs:simpleContent>
                 <xs:extension base="xs:string">
                  <xs:attribute type="xs:string" name="damageScenario"/>
                 </xs:extension>
                </xs:simpleContent>
               </xs:complexType>
```

```
                        </xs:element>
                       </xs:sequence>
                      </xs:complexType>
                     </xs:element>
                    </xs:sequence>
                   </xs:complexType>
                  </xs:element>
                 </xs:sequence>
                </xs:complexType>
               </xs:element>
               <xs:element name="InstantiatedClasses">
                <xs:complexType>
                 <xs:sequence>
                  <xs:element name="AssumptionClassRef">
                   <xs:complexType>
                    <xs:simpleContent>
                     <xs:extension base="xs:string">
                      <xs:attribute type="xs:string" name="target"/>
                     </xs:extension>
                    </xs:simpleContent>
                   </xs:complexType>
                  </xs:element>
                 </xs:sequence>
                </xs:complexType>
               </xs:element>
              </xs:sequence>
              <xs:attribute type="xs:string" name="description"/>
              <xs:attribute type="xs:string" name="id" use="optional"/>
              <xs:attribute type="xs:string" name="name"/>
              <xs:attribute type="xs:string" name="title"/>
             </xs:complexType>
            </xs:element>
           </xs:sequence>
          </xs:complexType>
         </xs:element>
        </xs:sequence>
        <xs:attribute type="xs:string" name="name"/>
        <xs:attribute type="xs:string" name="virtualPackage"/>
       </xs:complexType>
      </xs:element>
</xs:schema>
```

Impact Model

```
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
 <xs:element name="ImpactModel">
  <xs:complexType>
   <xs:element name="CSProperties">
    <xs:complexType>
     <xs:element name="CyberSecurityProperty" maxOccurs="unbounded" minOccurs="0">
      <xs:complexType>
       <xs:simpleContent>
        <xs:extension base="xs:string">
         <xs:attribute type="xs:string" name="description" />
         <xs:attribute type="xs:string" name="id"/>
         <xs:attribute type="xs:string" name="name" use="string"/>
         <xs:attribute type="xs:string" name="title"/>
        </xs:extension>
       </xs:simpleContent>
      </xs:complexType>
     </xs:element>
    </xs:complexType>
   </xs:element>
   <xs:element name="ImpactLevels">
    <xs:complexType>
     <xs:element name="ImpactLevelsDefinition">
      <xs:complexType>
       <xs:element name="Values">
        <xs:complexType>
         <xs:element name="ImpactLevel" maxOccurs="unbounded" minOccurs="0">
          <xs:complexType>
           <xs:simpleContent>
            <xs:extension base="xs:string">
             <xs:attribute type="xs:string" name="color"/>
             <xs:attribute type="xs:string" name="description"/>
             <xs:attribute type="xs:string" name="id"/>
             <xs:attribute type="xs:string" name="name" use="required"/>
             <xs:attribute type="xs:string" name="title"/>
             <xs:attribute type="xs:string" name="value" use="required"/>
            </xs:extension>
           </xs:simpleContent>
          </xs:complexType>
         </xs:element>
        </xs:complexType>
       </xs:element>
       <xs:attribute type="xs:string" name="id"/>
      </xs:complexType>
     </xs:element>
```

```
  </xs:complexType>
 </xs:element>
 <xs:element name="Stakeholders">
  <xs:complexType>
   <xs:element name="Stakeholder" maxOccurs="unbounded" minOccurs="0">
    <xs:complexType>
     <xs:simpleContent>
      <xs:extension base="xs:string">
       <xs:attribute type="xs:string" name="description"/>
       <xs:attribute type="xs:string" name="id"/>
       <xs:attribute type="xs:string" name="name" use="required"/>
       <xs:attribute type="xs:string" name="title"/>
      </xs:extension>
     </xs:simpleContent>
    </xs:complexType>
   </xs:element>
  </xs:complexType>
 </xs:element>
 <xs:element name="ImpactCategories">
  <xs:complexType>
   <xs:element name="ImpactCategory" maxOccurs="unbounded" minOccurs="0">
    <xs:complexType>
     <xs:simpleContent>
      <xs:extension base="xs:string">
       <xs:attribute type="xs:string" name="description"/>
       <xs:attribute type="xs:string" name="hidden" />
       <xs:attribute type="xs:string" name="id" use="optional"/>
       <xs:attribute type="xs:string" name="name" use="required"/>
       <xs:attribute type="xs:string" name="title"/>
      </xs:extension>
     </xs:simpleContent>
    </xs:complexType>
   </xs:element>
  </xs:complexType>
 </xs:element>
 <xs:element name="ImpactOptionLists">
  <xs:complexType>
   <xs:element name="ImpactOptionList" maxOccurs="unbounded" minOccurs="0">
    <xs:complexType>
     <xs:element name="Stakeholders">
      <xs:complexType>
       <xs:element name="StakeholderReference">
        <xs:complexType>
         <xs:simpleContent>
          <xs:extension base="xs:string">
```

```
                    <xs:attribute type="xs:string" name="target" use="required"/>
                    <xs:attribute type="xs:string" name="id"/>
                   </xs:extension>
                  </xs:simpleContent>
                 </xs:complexType>
                </xs:element>
               </xs:complexType>
              </xs:element>
              <xs:element name="Criteria">
               <xs:complexType>
                <xs:element name="ImpactOption" maxOccurs="unbounded" minOccurs="0">
                 <xs:complexType>
                  <xs:simpleContent>
                   <xs:extension base="xs:string">
                    <xs:attribute type="xs:string" name="description" />
                    <xs:attribute type="xs:byte" name="impactValue" use="required"/>
                    <xs:attribute type="xs:string" name="id"/>
                    <xs:attribute type="xs:string" name="name" use="required"/>
                    <xs:attribute type="xs:string" name="title"/>
                   </xs:extension>
                  </xs:simpleContent>
                 </xs:complexType>
                </xs:element>
               </xs:complexType>
              </xs:element>
             <xs:attribute type="xs:string" name="description"/>
             <xs:attribute type="xs:string" name="id" />
             <xs:attribute type="xs:string" name="name" use="required"/>
             <xs:attribute type="xs:string" name="refinedCategory" use="required"/>
            </xs:complexType>
           </xs:element>
          </xs:complexType>
         </xs:element>
         <xs:element name="ScalingOptions">
          <xs:complexType>
           <xs:element name="ImpactScale" maxOccurs="unbounded" minOccurs="0">
            <xs:complexType>
             <xs:simpleContent>
              <xs:extension base="xs:string">
               <xs:attribute type="xs:string" name="description"/>
               <xs:attribute type="xs:string" name="id"/>
               <xs:attribute type="xs:string" name="name" use="required"/>
               <xs:attribute type="xs:string" name="title"/>
               <xs:attribute type="xs:string" name="value" use="required"/>
              </xs:extension>
```

```
            </xs:simpleContent>
           </xs:complexType>
          </xs:element>
        </xs:complexType>
      </xs:element>
     <xs:attribute type="xs:string" name="id"/>
     <xs:attribute type="xs:string" name="name" use="required"/>
     <xs:attribute type="xs:string" name="virtualPackage"/>
   </xs:complexType>
 </xs:element>
</xs:schema>
```

Attack Feasibility Model

```
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
 <xs:element name="FeasibilityModel">
  <xs:complexType>
    <xs:element name="Categories">
     <xs:complexType>
       <xs:element name="FeasibilityCategory" maxOccurs="unbounded" minOccurs="0">
        <xs:complexType>
          <xs:element name="Options">
           <xs:complexType>
             <xs:element name="FeasibilityOption" maxOccurs="unbounded" minOccurs="0">
              <xs:complexType>
               <xs:simpleContent>
                <xs:extension base="xs:string">
                 <xs:attribute type="xs:string" name="description" />
                 <xs:attribute type="xs:string" name="id" />
                 <xs:attribute type="xs:string" name="name" use="required" />
                 <xs:attribute type="xs:string" name="title" />
                 <xs:attribute type="xs:string" name="value" use="required" />
                </xs:extension>
               </xs:simpleContent>
              </xs:complexType>
             </xs:element>
           </xs:complexType>
          </xs:element>
        <xs:attribute type="xs:string" name="description" />
        <xs:attribute type="xs:string" name="id" />
        <xs:attribute type="xs:string" name="name" use="required" />
        <xs:attribute type="xs:string" name="title" />
```

```
        </xs:complexType>
      </xs:element>
    </xs:complexType>
  </xs:element>
  <xs:element name="FeasibilityLevels">
    <xs:complexType>
      <xs:element name="AFLsDefinition">
        <xs:complexType>
          <xs:element name="Values">
            <xs:complexType>
              <xs:element name="AttackFeasibilityLevel" maxOccurs="unbounded" minOccurs="0">
                <xs:complexType>
                  <xs:simpleContent>
                    <xs:extension base="xs:string">
                      <xs:attribute type="xs:string" name="color" />
                      <xs:attribute type="xs:string" name="description" />
                      <xs:attribute type="xs:byte" name="minimalValue" use="required" />
                      <xs:attribute type="xs:string" name="id" />
                      <xs:attribute type="xs:string" name="name" use="required"/>
                    </xs:extension>
                  </xs:simpleContent>
                </xs:complexType>
              </xs:element>
            </xs:complexType>
          </xs:element>
          <xs:attribute type="xs:string" name="id"/>
        </xs:complexType>
      </xs:element>
    </xs:complexType>
  </xs:element>
  <xs:element name="FeasibilitiesTable">
    <xs:complexType>
      <xs:element name="AFLTable">
        <xs:complexType>
          <xs:element name="Cells">
            <xs:complexType>
              <xs:element name="AFLTableCell" maxOccurs="unbounded" minOccurs="0">
                <xs:complexType>
                  <xs:simpleContent>
                    <xs:extension base="xs:string">
                      <xs:attribute type="xs:string" name="consecutiveFeasibility" use="required"/>
                      <xs:attribute type="xs:string" name="initialFeasibility" use="required" />
                      <xs:attribute type="xs:string" name="id" />
                      <xs:attribute type="xs:string" name="resultingFeasibility" use="required"/>
                    </xs:extension>
```

```
                    </xs:simpleContent>
                  </xs:complexType>
                </xs:element>
              </xs:complexType>
            </xs:element>
            <xs:attribute type="xs:string" name="id"/>
          </xs:complexType>
        </xs:element>
      </xs:complexType>
    </xs:element>
    <xs:attribute type="xs:string" name="id"/>
    <xs:attribute type="xs:string" name="name" use="required"/>
    <xs:attribute type="xs:string" name="virtualPackage"/>
  </xs:complexType>
 </xs:element>
</xs:schema>
```

Risk Model

```
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
 <xs:element name="RiskModel">
  <xs:complexType>
   <xs:element name="RiskLevels">
    <xs:complexType>
     <xs:element name="RiskLevelsDefinition">
      <xs:complexType>
       <xs:element name="Levels">
        <xs:complexType>
         <xs:element name="RiskLevel" maxOccurs="unbounded" minOccurs="0">
          <xs:complexType>
           <xs:simpleContent>
            <xs:extension base="xs:string">
             <xs:attribute type="xs:string" name="color"/>
             <xs:attribute type="xs:string" name="description"/>
             <xs:attribute type="xs:string" name="id"/>
             <xs:attribute type="xs:string" name="name" use="required" />
            </xs:extension>
           </xs:simpleContent>
          </xs:complexType>
         </xs:element>
        </xs:complexType>
       </xs:element>
      </xs:complexType>
     </xs:element>
```

```
  </xs:complexType>
 </xs:element>
 <xs:element name="RiskTable">
  <xs:complexType>
   <xs:element name="RiskEvaluationTable">
    <xs:complexType>
     <xs:element name="Cells">
      <xs:complexType>
       <xs:element name="RiskEvaluationTableEntry" maxOccurs="unbounded" minOccurs="0">
        <xs:complexType>
         <xs:simpleContent>
          <xs:extension base="xs:string">
           <xs:attribute type="xs:string" name="feasibilityLevel" use="required"/>
           <xs:attribute type="xs:string" name="impactLevel" use="required"/>
           <xs:attribute type="xs:string" name="id"/>
           <xs:attribute type="xs:string" name="resultingRiskLevel" use="required"/>
          </xs:extension>
         </xs:simpleContent>
        </xs:complexType>
       </xs:element>
      </xs:complexType>
     </xs:element>
     <xs:attribute type="xs:string" name="id"/>
    </xs:complexType>
   </xs:element>
  </xs:complexType>
 </xs:element>
 <xs:element name="RiskTreatments">
  <xs:complexType>
   <xs:element name="RiskTreatmentsDefinition">
    <xs:complexType>
     <xs:element name="Treatments">
      <xs:complexType>
       <xs:element name="RiskTreatment" maxOccurs="unbounded" minOccurs="0">
        <xs:complexType>
         <xs:simpleContent>
          <xs:extension base="xs:string">
           <xs:attribute type="xs:string" name="description" />
           <xs:attribute type="xs:string" name="id" />
           <xs:attribute type="xs:string" name="name" use="required" />
           <xs:attribute type="xs:string" name="title" />
          </xs:extension>
         </xs:simpleContent>
        </xs:complexType>
       </xs:element>
```

```
                </xs:complexType>
               </xs:element>
              <xs:attribute type="xs:string" name="id"/>
             </xs:complexType>
            </xs:element>
          </xs:complexType>
        </xs:element>
      <xs:attribute type="xs:string" name="name" use="required" />
<xs:attribute type="xs:string" name="virtualPackage"/>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

Threat Scenarios

```
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
 <xs:element name="SecurityChunk">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="Elements">
     <xs:complexType>
      <xs:sequence>
       <xs:element name="ThreatScenario" minOccurs="1" maxOccurs="unbounded">
        <xs:complexType>
         <xs:element name="CauseOfCompromise" minOccurs="1" maxOccurs="1">
          <xs:complexType>
           <xs:sequence>
            <xs:element name="ThreatClassRef" minOccurs="0" maxOccurs="1">
             <xs:complexType>
              <xs:simpleContent>
               <xs:extension base="xs:string">
                <xs:attribute type="xs:string" name="id"/>
                <xs:attribute type="xs:string" name="target" use="required"/>
               </xs:extension>
              </xs:simpleContent>
             </xs:complexType>
            </xs:element>
           </xs:sequence>
          </xs:complexType>
         </xs:element>
         <xs:element name="ActedOnTOEEs" minOccurs="1" maxOccurs="1">
```

```
      <xs:complexType>
       <xs:sequence>
        <xs:element name="ChannelRef" minOccurs="0" maxOccurs="unbounded">
         <xs:complexType>
          <xs:simpleContent>
           <xs:extension base="xs:string">
            <xs:attribute type="xs:string" name="id"/>
            <xs:attribute type="xs:string" name="target" use="required"/>
           </xs:extension>
          </xs:simpleContent>
         </xs:complexType>
        </xs:element>
       </xs:sequence>
      </xs:complexType>
     </xs:element>
     <xs:element name="CustomImpactCombinator" minOccurs="1" maxOccurs="1"/>
     <xs:element name="CustomFeasibilityCombinator" minOccurs="1" maxOccurs="1"/>
     <xs:element name="DamageScenarios" minOccurs="1" maxOccurs="1">
      <xs:complexType>
       <xs:sequence>
        <xs:element name="DamageScenarioRef" minOccurs="0" maxOccurs="unbounded" >
         <xs:complexType>
          <xs:simpleContent>
           <xs:extension base="xs:string">
            <xs:attribute type="xs:string" name="id"/>
            <xs:attribute type="xs:string" name="damageScenario" use="required"/>
           </xs:extension>
          </xs:simpleContent>
         </xs:complexType>
        </xs:element>
       </xs:sequence>
      </xs:complexType>
     </xs:element>
     <xs:element name="Compromises" minOccurs="1" maxOccurs="1">
      <xs:complexType>
       <xs:sequence>
        <xs:element name="DeriveCompromisedAssets"/>
       </xs:sequence>
      </xs:complexType>
     </xs:element>
     <xs:attribute type="xs:string" name="description"/>
     <xs:attribute type="xs:string" name="id"/>
     <xs:attribute type="xs:string" name="name" use="required"/>
     <xs:attribute type="xs:string" name="threatenedBy"/>
     <xs:attribute type="xs:string" name="lessenedBy"/>
```

```
            <xs:attribute type="xs:string" name="title"/>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
 </xs:sequence>
 <xs:attribute type="xs:string" name="id"/>
 <xs:attribute type="xs:string" name="name" use="required"/>
 <xs:attribute type="xs:string" name="virtualPackage"/>
 </xs:complexType>
 </xs:element>
</xs:schema>
```

Damage Scenarios

```
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
 <xs:element name="SecurityChunk">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="Elements">
     <xs:complexType>
      <xs:sequence>
       <xs:element name="DamageScenario" minOccurs="1" maxOccurs="unbounded">
        <xs:complexType>
         <xs:sequence>
          <xs:element name="ImpactRatings" minOccurs="1" maxOccurs="1">
           <xs:complexType>
            <xs:sequence>
             <xs:element name="ImpactTuple" minOccurs="0" maxOccurs="unbounded" >
              <xs:complexType>
               <xs:sequence>
                <xs:element name="ImpactRating" minOccurs="1" maxOccurs="1">
                 <xs:complexType>
                  <xs:sequence>
                   <xs:element name="ImpactRating" minOccurs="1" maxOccurs="1">
                    <xs:complexType>
                     <xs:simpleContent>
                      <xs:extension base="xs:string">
                       <xs:attribute type="xs:string" name="id"/>
                       <xs:attribute type="xs:string" name="option" use="required"/>
                      </xs:extension>
                     </xs:simpleContent>
```

```
                    </xs:complexType>
                  </xs:element>
                 </xs:sequence>
                </xs:complexType>
               </xs:element>
              </xs:sequence>
              <xs:attribute type="xs:string" name="impactCategory" use="optional"/>
             </xs:complexType>
            </xs:element>
           </xs:sequence>
          </xs:complexType>
         </xs:element>
         <xs:element name="ConcernedAssets" minOccurs="1" maxOccurs="1">
          <xs:complexType>
           <xs:sequence>
            <xs:element name="QualifiedAssetList" minOccurs="1" maxOccurs="1">
             <xs:complexType>
              <xs:sequence>
               <xs:element name="QualifiedAssets" minOccurs="1" maxOccurs="1">
                <xs:complexType>
                 <xs:sequence>
                  <xs:element name="QualifiedAsset" minOccurs="0">
                   <xs:complexType>
                    <xs:sequence>
                     <xs:element name="CsProperty">
                      <xs:complexType>
                       <xs:sequence>
                        <xs:element name="CSPropertyRef">
                         <xs:complexType>
                          <xs:simpleContent>
                           <xs:extension base="xs:string">
                            <xs:attribute type="xs:string" name="target"/>
                           </xs:extension>
                          </xs:simpleContent>
                         </xs:complexType>
                        </xs:element>
                       </xs:sequence>
                      </xs:complexType>
                     </xs:element>
                     <xs:element name="Toee">
                      <xs:complexType>
                       <xs:sequence>
                        <xs:element name="FunctionRef">
                         <xs:complexType>
                          <xs:simpleContent>
```

```
                                    <xs:extension base="xs:string">
                                      <xs:attribute type="xs:string" name="target"/>
                                    </xs:extension>
                                  </xs:simpleContent>
                                </xs:complexType>
                              </xs:element>
                            </xs:sequence>
                          </xs:complexType>
                        </xs:element>
                      </xs:sequence>
                    </xs:complexType>
                  </xs:element>
                </xs:sequence>
              </xs:complexType>
            </xs:element>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element name="Scale" minOccurs="1" maxOccurs="1"/>
    </xs:sequence>
    <xs:attribute type="xs:string" name="description"/>
    <xs:attribute type="xs:string" name="id"/>
    <xs:attribute type="xs:string" name="name" use="required"/>
    <xs:attribute type="xs:string" name="normalBehavior"/>
    <xs:attribute type="xs:string" name="operationalSituation"/>
    <xs:attribute type="xs:string" name="title"/>
  </xs:complexType>
 </xs:element>
</xs:sequence>
<xs:attribute type="xs:string" name="id"/>
<xs:attribute type="xs:string" name="name" use="required"/>
<xs:attribute type="xs:string" name="virtualPackage"/>
</xs:complexType>
</xs:element>
</xs:schema>
```

Attack Steps

```
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
 <xs:element name="SecurityChunk">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="Elements">
     <xs:complexType>
      <xs:sequence>
       <xs:element name="AttackStep">
        <xs:complexType>
         <xs:sequence>
          <xs:element name="InstantiatedClass">
           <xs:complexType>
            <xs:sequence>
             <xs:element name="ThreatClassRef">
              <xs:complexType>
               <xs:simpleContent>
                <xs:extension base="xs:string">
                 <xs:attribute type="xs:string" name="target"/>
                </xs:extension>
               </xs:simpleContent>
              </xs:complexType>
             </xs:element>
            </xs:sequence>
           </xs:complexType>
          </xs:element>
          <xs:element name="ActedOnTOEEs">
           <xs:complexType>
            <xs:sequence>
             <xs:element name="ChannelRef">
              <xs:complexType>
               <xs:simpleContent>
                <xs:extension base="xs:string">
                 <xs:attribute type="xs:string" name="target"/>
                </xs:extension>
               </xs:simpleContent>
              </xs:complexType>
             </xs:element>
            </xs:sequence>
           </xs:complexType>
          </xs:element>
          <xs:element type="xs:string" name="InitialFeasibilityOptions"/>
```

```
            <xs:element type="xs:string" name="ConsecutiveFeasibilityOptions"/>
            <xs:element type="xs:string" name="ExplicitInitialFeasibility"/>
            <xs:element type="xs:string" name="ExplicitConsecutiveFeasibility"/>
            <xs:element type="xs:string" name="CustomImpactCombinator"/>
            <xs:element type="xs:string" name="CustomFeasibilityCombinator"/>
            <xs:element type="xs:string" name="FeasibilityModel"/>
           </xs:sequence>
           <xs:attribute type="xs:string" name="description"/>
           <xs:attribute type="xs:string" name="mitigatedBy"/>
           <xs:attribute type="xs:string" name="id" use="optional"/>
           <xs:attribute type="xs:string" name="name"/>
           <xs:attribute type="xs:string" name="refinedBy"/>
           <xs:attribute type="xs:byte" name="riskLevel"/>
           <xs:attribute type="xs:string" name="title"/>
          </xs:complexType>
         </xs:element>
        </xs:sequence>
       </xs:complexType>
      </xs:element>
    </xs:sequence>
    <xs:attribute type="xs:string" name="id" use="optional"/>
    <xs:attribute type="xs:string" name="name"/>
    <xs:attribute type="xs:string" name="virtualPackage"/>
   </xs:complexType>
  </xs:element>
</xs:schema>
```

Cybersecurity Controls

```
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
 <xs:element name="SecurityChunk">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="Elements">
     <xs:complexType>
      <xs:sequence>
       <xs:element name="Control" minOccurs="1" maxOccurs="unbounded">
        <xs:complexType>
         <xs:element name="InstantiatedControlClass" minOccurs="1" maxOccurs="1">
          <xs:complexType>
           <xs:sequence>
```

```
        <xs:element name="SecurityControlClassRef" minOccurs="0" maxOccurs="unbounded">
          <xs:complexType>
            <xs:simpleContent>
              <xs:extension base="xs:string">
                <xs:attribute type="xs:string" name="id"/>
                <xs:attribute type="xs:string" name="target" use="required"/>
              </xs:extension>
            </xs:simpleContent>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="ControlGroups" minOccurs="1" maxOccurs="1"/>
  <xs:element name="InitialFeasibilityOptions" minOccurs="1" maxOccurs="1"/>
  <xs:element name="ConsecutiveFeasibilityOptions" minOccurs="1" maxOccurs="1"/>
  <xs:element name="InitialExplicitFeasibility" minOccurs="1" maxOccurs="1"/>
  <xs:element name="ConsecutiveExplicitFeasibility" minOccurs="1" maxOccurs="1"/>
  <xs:element name="ActedOnTOEEs" minOccurs="1" maxOccurs="1"/>
    <xs:complexType>
      <xs:sequence>
        <xs:element name="ChannelRef" minOccurs="0" maxOccurs="unbounded">
          <xs:complexType>
            <xs:simpleContent>
              <xs:extension base="xs:string">
                <xs:attribute type="xs:string" name="id"/>
                <xs:attribute type="xs:string" name="target" use="required"/>
              </xs:extension>
            </xs:simpleContent>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  <xs:element name="Effects" minOccurs="1" maxOccurs="1">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="TransformDamageScenario" minOccurs="0" maxOccurs="1">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="Source" minOccurs="1" maxOccurs="1">
                <xs:complexType>
                  <xs:sequence>
                    <xs:element name="DamageScenarioRef" minOccurs="0" maxOccurs="unbounded">
                      <xs:complexType>
                        <xs:simpleContent>
```

```
                    <xs:extension base="xs:string">
                      <xs:attribute type="xs:string" name="damageScenario" use="required"/>
                    </xs:extension>
                  </xs:simpleContent>
                </xs:complexType>
              </xs:element>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element name="Target" minOccurs="1" maxOccurs="1">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="DamageScenarioRef" minOccurs="0" maxOccurs="unbounded">
                <xs:complexType>
                  <xs:simpleContent>
                    <xs:extension base="xs:string">
                      <xs:attribute type="xs:string" name="damageScenario" use="required"/>
                    </xs:extension>
                  </xs:simpleContent>
                </xs:complexType>
              </xs:element>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="TransformImpactOption" minOccurs="0" maxOccurs="1">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="Source" minOccurs="1" maxOccurs="1">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="ImpactOptionRef" minOccurs="0" maxOccurs="unbounded">
                <xs:complexType>
                  <xs:simpleContent>
                    <xs:extension base="xs:string">
                      <xs:attribute type="xs:string" name="target" use="required"/>
                    </xs:extension>
                  </xs:simpleContent>
                </xs:complexType>
              </xs:element>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
```

```
        <xs:element name="Target" minOccurs="1" maxOccurs="1">
         <xs:complexType>
          <xs:sequence>
           <xs:element name="ImpactOptionRef" minOccurs="0" maxOccurs="unbounded">
            <xs:complexType>
             <xs:simpleContent>
              <xs:extension base="xs:string">
               <xs:attribute type="xs:string" name="target" use="required"/>
              </xs:extension>
             </xs:simpleContent>
            </xs:complexType>
           </xs:element>
          </xs:sequence>
         </xs:complexType>
        </xs:element>
       </xs:sequence>
      </xs:complexType>
     </xs:element>
     <xs:element name="RemoveAllDamage" minOccurs="0" maxOccurs="1"/>
     <xs:element name="RemoveImpactOption" minOccurs="0" maxOccurs="1">
      <xs:complexType>
       <xs:sequence>
        <xs:element name="Option" minOccurs="1" maxOccurs="1">
         <xs:complexType>
          <xs:sequence>
           <xs:element name="ImpactOptionRef" minOccurs="0" maxOccurs="unbounded">
            <xs:complexType>
             <xs:simpleContent>
              <xs:extension base="xs:string">
               <xs:attribute type="xs:string" name="target" use="required"/>
              </xs:extension>
             </xs:simpleContent>
            </xs:complexType>
           </xs:element>
          </xs:sequence>
         </xs:complexType>
        </xs:element>
       </xs:sequence>
      </xs:complexType>
     </xs:element>
     <xs:element name="RemoveDamageScenario" minOccurs="0" maxOccurs="1">
      <xs:complexType>
       <xs:sequence>
        <xs:element name="Scenario" minOccurs="1" maxOccurs="1">
         <xs:complexType>
```

```
                        <xs:sequence>
                          <xs:element name="DamageScenarioRef" minOccurs="0" maxOccurs="unbounded">
                            <xs:complexType>
                              <xs:simpleContent>
                                <xs:extension base="xs:string">
                                  <xs:attribute type="xs:string" name="damageScenario" use="required"/>
                                </xs:extension>
                              </xs:simpleContent>
                            </xs:complexType>
                          </xs:element>
                        </xs:sequence>
                      </xs:complexType>
                    </xs:element>
                  </xs:sequence>
                </xs:complexType>
              </xs:element>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element name="CustomImpactCombinator" minOccurs="1" maxOccurs="1"/>
        <xs:element name="CustomFeasibilityCombinator" minOccurs="1" maxOccurs="1"/>
        <xs:element name="FeasibilityModel" minOccurs="1" maxOccurs="1"/>
      <xs:attribute type="xs:string" name="dependsOn"/>
      <xs:attribute type="xs:string" name="description"/>
      <xs:attribute type="xs:string" name="id"/>
      <xs:attribute type="xs:string" name="name" use="required"/>
      <xs:attribute type="xs:string" name="title"/>
    </xs:complexType>
  </xs:element>
 </xs:sequence>
 </xs:complexType>
</xs:element>
<xs:attribute type="xs:string" name="id"/>
<xs:attribute type="xs:string" name="name" use="required"/>
<xs:attribute type="xs:string" name="virtualPackage"/>
</xs:complexType>
</xs:element>
</xs:schema>
```

Control Scenarios

```
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
 <xs:element name="SecurityChunk">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="Elements">
     <xs:complexType>
      <xs:sequence>
       <xs:element name="Scenario" maxOccurs="unbounded" minOccurs="0">
        <xs:complexType>
         <xs:sequence>
          <xs:element name="Controls">
           <xs:complexType>
            <xs:sequence>
             <xs:element name="SecurityControlSelector" minOccurs="0">
              <xs:complexType>
               <xs:simpleContent>
                <xs:extension base="xs:string">
                 <xs:attribute type="xs:string" name="target" use="required"/>
                </xs:extension>
               </xs:simpleContent>
              </xs:complexType>
             </xs:element>
             <xs:element type="xs:string" name="AllControls" minOccurs="0"/>
            </xs:sequence>
           </xs:complexType>
          </xs:element>
         </xs:sequence>
         <xs:attribute type="xs:string" name="description"/>
         <xs:attribute type="xs:string" name="isDefault"/>
         <xs:attribute type="xs:string" name="id"/>
         <xs:attribute type="xs:string" name="name" use="required"/>
         <xs:attribute type="xs:string" name="title"/>
        </xs:complexType>
       </xs:element>
      </xs:sequence>
     </xs:complexType>
    </xs:element>
   </xs:sequence>
   <xs:attribute type="xs:string" name="id"/>
   <xs:attribute type="xs:string" name="name" use="required"/>
   <xs:attribute type="xs:string" name="virtualPackage"/>
```

```
  </xs:complexType>
 </xs:element>
</xs:schema>
```

Risks

```
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
 <xs:element name="SecurityChunk">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="Elements">
     <xs:complexType>
      <xs:sequence>
       <xs:element name="Risk" minOccurs="1" maxOccurs="unbounded">
        <xs:complexType>
         <xs:sequence>
          <xs:element name="CausedByElements" minOccurs="1" maxOccurs="1">
           <xs:complexType>
            <xs:sequence>
             <xs:element name="ThreatScenarioRef" minOccurs="0" maxOccurs="unbounded">
              <xs:complexType>
               <xs:simpleContent>
                <xs:extension base="xs:string">
                 <xs:attribute type="xs:string" name="id"/>
                 <xs:attribute type="xs:string" name="target"  use="required"/>
                </xs:extension>
               </xs:simpleContent>
              </xs:complexType>
             </xs:element>
            </xs:sequence>
           </xs:complexType>
          </xs:element>
         </xs:sequence>
         <xs:attribute type="xs:string" name="description"/>
         <xs:attribute type="xs:string" name="id"/>
         <xs:attribute type="xs:string" name="name" use="required"/>
         <xs:attribute type="xs:string" name="title"/>
        </xs:complexType>
       </xs:element>
      </xs:sequence>
     </xs:complexType>
    </xs:element>
   </xs:sequence>
   <xs:attribute type="xs:string" name="id"/>
   <xs:attribute type="xs:string" name="name" use="required"/>
```

```
    <xs:attribute type="xs:string" name="virtualPackage"/>
   </xs:complexType>
  </xs:element>
</xs:schema>
```

Threat Classes

```
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
 <xs:element name="ThreatsCatalog">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="ThreatClasses">
     <xs:complexType>
      <xs:sequence>
       <xs:element name="ThreatClass" minOccurs="1" maxOccurs="unbounded">
        <xs:complexType>
         <xs:element name="ThreatenedSecurityProperties" minOccurs="1" maxOccurs="1">
          <xs:complexType>
           <xs:sequence>
            <xs:element name="CSPropertyRef" minOccurs="0" maxOccurs="unbounded">
             <xs:complexType>
              <xs:simpleContent>
               <xs:extension base="xs:string">
                <xs:attribute type="xs:string" name="id"/>
                <xs:attribute type="xs:string" name="target" use="required"/>
               </xs:extension>
              </xs:simpleContent>
             </xs:complexType>
            </xs:element>
           </xs:sequence>
          </xs:complexType>
         </xs:element>
         <xs:element name="Architecture" minOccurs="1" maxOccurs="1">
          <xs:complexType>
           <xs:element name="DataFlowSecurityTarget" minOccurs="0" maxOccurs="unbounded"/>
           <xs:element name="ChannelSecurityTarget" minOccurs="0" maxOccurs="unbounded"/>
          </xs:complexType>
         </xs:element>
         <xs:element name="InitialFeasibilityOptions" minOccurs="1" maxOccurs="1">
          <xs:complexType>
           <xs:sequence>
            <xs:element name="FeasibilityRating" minOccurs="0" maxOccurs="unbounded" >
             <xs:complexType>
              <xs:simpleContent>
               <xs:extension base="xs:string">
```

```
                    <xs:attribute type="xs:string" name="category"/>
                    <xs:attribute type="xs:string" name="id"/>
                    <xs:attribute type="xs:string" name="option"/>
                   </xs:extension>
                  </xs:simpleContent>
                 </xs:complexType>
                </xs:element>
               </xs:sequence>
              </xs:complexType>
             </xs:element>
             <xs:element name="ConsecutiveFeasibilityOptions" minOccurs="1" maxOccurs="1"/>
             <xs:element name="Technologies" minOccurs="1" maxOccurs="1">
              <xs:complexType>
               <xs:sequence>
                <xs:element name="TechnologyRef" minOccurs="0" maxOccurs="unbounded">
                 <xs:complexType>
                  <xs:simpleContent>
                   <xs:extension base="xs:string">
                    <xs:attribute type="xs:string" name="id"/>
                    <xs:attribute type="xs:string" name="target" use="required"/>
                   </xs:extension>
                  </xs:simpleContent>
                 </xs:complexType>
                </xs:element>
               </xs:sequence>
              </xs:complexType>
             </xs:element>
            <xs:attribute type="xs:string" name="description"/>
            <xs:attribute type="xs:string" name="id"/>
            <xs:attribute type="xs:string" name="name" use="required"/>
            <xs:attribute type="xs:string" name="title"/>
           </xs:complexType>
          </xs:element>
         </xs:sequence>
        </xs:complexType>
       </xs:element>
     </xs:sequence>
     <xs:attribute type="xs:string" name="id"/>
     <xs:attribute type="xs:string" name="name" use="required"/>
<xs:attribute type="xs:string" name="virtualPackage"/>
   </xs:complexType>
  </xs:element>
</xs:schema>
```

Cybersecurity Control Classes

```
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
 <xs:element name="SecurityControlsCatalog">
  <xs:complexType>
   <xs:element name="ControlClasses">
    <xs:complexType>
     <xs:element name="SecurityControlClass">
      <xs:complexType>
       <xs:element name="Protects">
        <xs:complexType>
         <xs:element name="CSPropertyRef">
          <xs:complexType>
           <xs:simpleContent>
            <xs:extension base="xs:string">
             <xs:attribute type="xs:string" name="target"/>
            </xs:extension>
           </xs:simpleContent>
          </xs:complexType>
         </xs:element>
        </xs:complexType>
       </xs:element>
       <xs:element name="ProtectsAgainst">
        <xs:complexType>
         <xs:element name="ThreatClassRef" maxOccurs="unbounded" minOccurs="0">
          <xs:complexType>
           <xs:simpleContent>
            <xs:extension base="xs:string">
             <xs:attribute type="xs:string" name="target" use="required"/>
            </xs:extension>
           </xs:simpleContent>
          </xs:complexType>
         </xs:element>

        </xs:complexType>
       </xs:element>
       <xs:element name="Architecture">
        <xs:complexType>
         <xs:element type="xs:string" name="ComponentSecurityTarget"/>
         <xs:element type="xs:string" name="DataFlowSecurityTarget"/>
         <xs:element type="xs:string" name="ChannelSecurityTarget"/>
        </xs:complexType>
       </xs:element>
       <xs:element type="xs:string" name="Technologies"/>
       <xs:element type="xs:string" name="Dependencies"/>
```

```
            <xs:element name="InitialFeasibilityOptions">
              <xs:complexType>
                <xs:element name="FeasibilityRating" maxOccurs="unbounded" minOccurs="0">
                  <xs:complexType>
                    <xs:simpleContent>
                      <xs:extension base="xs:string">
                        <xs:attribute type="xs:string" name="category" use="optional"/>
                        <xs:attribute type="xs:string" name="id" use="optional"/>
                        <xs:attribute type="xs:string" name="option" use="optional"/>
                      </xs:extension>
                    </xs:simpleContent>
                  </xs:complexType>
                </xs:element>
              </xs:complexType>
            </xs:element>
            <xs:element type="xs:string" name="ConsecutiveFeasibilityOptions"/>
            <xs:element type="xs:string" name="FeasibilityModel"/>
          <xs:attribute type="xs:string" name="description"/>
          <xs:attribute type="xs:string" name="id"/>
          <xs:attribute type="xs:string" name="name" use="required"/>
          <xs:attribute type="xs:string" name="title"/>
        </xs:complexType>
      </xs:element>
    </xs:complexType>
  </xs:element>
  <xs:attribute type="xs:string" name="id"/>
  <xs:attribute type="xs:string" name="name" use="required"/>
  <xs:attribute type="xs:string" name="virtualPackage"/>
 </xs:complexType>
</xs:element>
</xs:schema>
```

VII. Bibliography / References

(n.d.). The VERIS Framework. Retrieved April 28, 2023, from http://veriscommunity.net/

(n.d.). Risk Data Open Standard: RDOS. Retrieved May 31, 2023, from https://www.riskdataos.org/

(n.d.). Virtual OSOCC: GDACS. Retrieved May 31, 2023, from https://vosocc.unocha.org/

(n.d.). The VERIS Framework. Retrieved May 31, 2023, from http://veriscommunity.net/

AlienVault - Open Threat Exchange. (n.d.). AlienVault - Open Threat Exchange. Retrieved June 1, 2023, from https://otx.alienvault.com/

Bacon, M. (n.d.). *What is STIX (Structured Threat Information eXpression)? | Definition from TechTarget*. TechTarget. Retrieved May 31, 2023, from https://www.techtarget.com/searchsecurity/definition/STIX-Structured-Threat-Information-eXpression

Bradner, S. (1997, March). *Key words for use in RFCs to Indicate Requirement Levels* [RFC2119]. 10.17487/RFC2119

Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. (2022, May 1). NIST Technical Series Publications. Retrieved May 31, 2023, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

DFV common risk and safety framework. (2023, April 27). Department of Justice and Attorney-General. Retrieved May 31, 2023, from https://www.justice.qld.gov.au/initiatives/end-domestic-family-violence/our-progress/enhancing-service-responses/dfv-common-risk-safety-framework

EFSA's OpenFoodTox: An open source toxicological database on chemicals in food and feed and its future developments. (n.d.). PubMed. Retrieved May 31, 2023, from https://pubmed.ncbi.nlm.nih.gov/33395940/

Food consumption data | EFSA. (2022, December 15). EFSA. Retrieved May 31, 2023, from https://www.efsa.europa.eu/en/data-report/food-consumption-data

Indicators of Compromise (IOC). (n.d.). LIFARS.com. Retrieved June 1, 2023, from https://lifars.com/wp-content/uploads/2017/06/Indicators-of-Compromise-IOC-.pdf

International Organization for Standardization. (2021, 08). In *Road vehicles — Cybersecurity engineering* (ISO/SAE 21434:2021).

Introduction to STIX. (n.d.). oasis-open. Retrieved 11 16, 2022, from https://oasis-open.github.io/cti-documentation/stix/intro

Leiba, B. (2017, May). *Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words* [RFC8174]. 10.17487/RFC8174

The measures: Customs Risk Management Framework. (n.d.). Language selection | Taxation and Customs Union. Retrieved May 31, 2023, from https://taxation-customs.ec.europa.eu/measures-customs-risk-management-framework_en

MISP Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing. (n.d.). MISP Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing. Retrieved June 1, 2023, from https://www.misp-project.org/

NISTIR 7693, Asset Identification Specification v1.1 | CSRC. (2011, June 17). NIST Computer Security Resource Center. Retrieved April 29, 2023, from https://csrc.nist.gov/publications/detail/nistir/7693/final

NIST Special Publication (SP) 800-150, Guide to Cyber Threat Information Sharing. (2016, October 4). NIST Computer Security Resource Center. Retrieved April 29, 2023, from https://csrc.nist.gov/publications/detail/sp/800-150/final

OSCAL: the Open Security Controls Assessment Language. (n.d.). NIST Pages. Retrieved April 29, 2023, from https://pages.nist.gov/OSCAL/

Rapid Alert System for Food and Feed (RASFF). (n.d.). Language selection | Food Safety. Retrieved May 31, 2023, from https://food.ec.europa.eu/safety/rasff_en

SAE 21434:2021 - Road vehicles — Cybersecurity engineering. (n.d.). ISO. Retrieved April 30, 2023, from https://www.iso.org/standard/70918.html

Scott, G. (n.d.). *What Is the International Swaps and Derivatives Association (ISDA)?* Investopedia. Retrieved May 31, 2023, from https://www.investopedia.com/terms/i/isda.asp

Standards. (n.d.). Open Geospatial Consortium. Retrieved May 31, 2023, from https://www.ogc.org/standards/

UN Regulation No. 155 - Cyber security and cyber security management system. (n.d.). United Nations. Retrieved July 19, 2023, from https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security

Vulnerability Disclosure Report (VDR). (n.d.). CycloneDX. Retrieved April 28, 2023, from https://cyclonedx.org/capabilities/vdr/

Vulnerability Exploitability eXchange (VEX). (n.d.). CycloneDX. Retrieved April 28, 2023, from https://cyclonedx.org/capabilities/vex/

Vulnerability Exploitability eXchange (VEX). (n.d.). CycloneDX. Retrieved May 31, 2023, from https://cyclonedx.org/capabilities/vex/

What is Trusted Automated eXchange of Indicator (TAXII)? | NETSCOUT. (n.d.). Netscout. Retrieved June 1, 2023, from https://www.netscout.com/what-is/taxii