Cyber Situational Awareness in Vehicle Security Operations: Holistic Monitoring and a Data Model

Daniel Grimm, Moritz Zink, Marc Schindewolf, and Eric Sax
Karlsruhe Institute of Technology
Karlsruhe, Germany
{name.surname@kit.edu}

***Abstract*—Vehicles continue to evolve toward automation and connectivity. These software-defined vehicles comprise more potential vulnerabilities and a larger attack surface, including threats to safety. To ensure these cybersecurity risks are properly managed, it is imperative to implement monitoring, analysis and response capabilities to new threats and vulnerabilities. Analysis and response, to be carried out in a Vehicle Security Operations Center, require decision-making, for which awareness of current risks is required. To this end, this paper proposes two elements: First, a holistic monitoring concept that provides data from the vehicle fleet and background information available particularly in the automotive environment. Second, a formalized data model that connects the monitored information to a comprehensive situational understanding of the security posture. To define such a model, we analyzed cyber situation awareness and automotive data models. Being graph-based, our new model shall enable straightforward retrieval of relationships between risks, assets and existing knowledge and provide a flexible backbone for both immediate as well as strategic decisions.**

***Index Terms*—cyber situational awareness, data model, automotive, monitoring, vehicle security operations center**

I. Introduction

Vehicles are evolving from mechanical systems to Software-defined vehicles (SDVs) and IoT devices, increasing the risk of cyber-attacks. Legal UN Regulation 155 [1] and ISO/SAE 21434 [2] emphasize embedding cybersecurity throughout vehicle development. Key to this is Threat analysis and risk assessment (TARA), which prioritizes risks and security measure requirements. Given the inevitability of new threats—e.g., 346 new vulnerabilities in 2022 [3]—ongoing security activities are crucial, including monitoring, triage, vulnerability and incident handling, and software and TARA updates.

Continuous security operations requires technological and procedural support. The introduction of a Vehicle Security Operations Center (VSOC) is therefore recommended [4], [5] to enable a timely response to incidents using suitable processes [6], [7]. But, the required fast response times, diversity of vehicle types and the scales (number of vehicles) and dynamics (situations, e.g. without network connection) are challenges when responding to incidents in vehicle fleets [5].

Security operations tasks require a basis for decision-making, i.e. the security situation must be understood, and the decision makers must ”know what is going on”[8]. For this problem, Cyber Situational Awareness (CSA) is the idea proposed in this work, that was applied to several domains such as military [9], smart cities [10], and enterprises [11].

This paper focuses on adopting CSA in VSOCs by proposing a holistic monitoring strategy and a comprehensive data model to consolidate vehicle security information. Inspired by Knowledge Graph (KG) approaches for cybersecurity [12], we argue that a graph data structure is well-suited for CSA. Unlike rigid relational databases, graph databases (e.g., RDF, Labeled Property Graph (LPG)) handle heterogeneous and evolving data more flexibly. Even NoSQL databases, like Elastic Stack, require schema adjustments for optimal performance [1]. Graph-based approaches balance well between rich query semantics and flexibility.

Problem: Vehicle cybersecurity is gaining relevance, and continuous monitoring is mandatory. For triage, response and other decisions in a VSOC, understanding the security situation is required. Accordingly, improving automotive CSA is desired. However, monitoring concepts for a VSOC, including data models to fuse the available information, are missing.

Method: Automotive-specific requirements and constraints for monitoring were identified, yielding a set of practically available information for CSA. Data models from the automotive domain and IT CSA were analyzed to select the appropriate elements for a (graph-based) automotive security data model. The new data model is formalized as Unified Modeling Language (UML) class diagram.

Contribution: To the best of our knowledge, we present the first data model targeting VSOCs. The model accounts for the special characteristics of vehicles, such as variant-rich software systems, physical context and prior knowledge from the development process. A holistic concept for cybersecurity monitoring of vehicles is presented that yields the data required to populate the data model as a graph database.

II. Background

A. Software-defined vehicles

Vehicles are no longer (only) differentiated through mechanical and electronic properties. In SDVs, sensors and software drive the trends, such as automated driving. While in the past, low-performance Electronic control units (ECUs) were connected with bus systems such as Controller Area Network (CAN), today, in-vehicle networks also contain high-performance computing platforms with Linux-based operating system (OS) and Ethernet. Building on this generic computing

[1] https://www.elastic.co/blog/found-elasticsearch-as-nosql

978-3-903176-66-9 ©2024 IFIP

power and bandwidth, Virtual Machines (VMs), orchestration (e.g. lightweight Kubernetes [13], [14]) and containerization technology [15] are under research. Industrial projects, e.g. Eclipse SDV, aim for virtual testing in the cloud, and decoupling the software and hardware development. In SDVs, services encapsulate the software and connect it with middlewares, e.g. Robot Operating System 2 (ROS 2) or AUTOSAR adaptive, forming Service-oriented architectures (SOA).

B. Security engineering with ISO/SAE 21434

The ISO/SAE 21434 [2] framework addresses every phase of the vehicle life cycle, from concept and product development through production, operations, maintenance, and eventual decommissioning. For collaboration with suppliers, a cybersecurity interface agreement that outlines responsibilities, including vulnerability management actions, is recommended. Although the standard is extensive, it emphasizes the TARA process. The TARA evaluates potential threats to a system, and determines the necessary extent of mitigation measures to these threats. At least, TARA is mandatory for ”items”, i.e. functions on vehicle-level. After identifying the items' assets (such as data and components), threat modelling yields potential threat scenarios. Then, attack paths and damage scenarios are analyzed.

Monitoring, vulnerability analysis and incident response are proposed for the operations and maintenance phase. These project-independent activities also occur in parallel to development cycles. ISO/SAE 21434 suggests several data sources for monitoring, such as cybersecurity specifications, threat scenarios from TARA, previous vulnerability analyses, and external inputs from researchers, supply chain, and governmental bodies. For vulnerability analysis, the TARA methods should be applied. Afterward, incident response can be triggered.

III. Related work

ISO/SAE 21434 mentions data sources for monitoring but lacks on in-vehicle monitoring and their relationships. Research focuses on specific security mechanisms like intrusion detection system (IDS), firewalls, and SDV-based responses [16]–[18]. Recent discussions include automotive security operations [7] and emerging Cyber Threat Intelligence (CTI) collections based on MITRE ATT&CK [19], [20]. Various attack databases, including scientific and commercial sources, are explored, with differing data models [21]–[23]. Graph-based modeling has been applied to automated driving [24], [25], but a comprehensive data model for VSOCs or a holistic cybersecurity monitoring concept is still lacking.

Several works propose KGs and data models for cybersecurity. CyGraph [26] is a model linking mission dependencies, cyber threats, security posture, and network infrastructure, integrating various data sources such as vulnerabilities, network flows, firewall rules, and attack patterns (Common Attack Pattern Enumeration and Classification (CAPEC)). SEPSES [27] maps known vulnerabilities (Common Vulnerabilities and Exposures (CVE)) to weaknesses (Common Weakness Enumeration (CWE)), attack patterns, CVSS scores, and affected components (Common Platform Enumeration (CPE)). Komárková et al. propose CRUSOE [11], a data model designed to enhance an organization's network CSA. It organizes data into layers (e.g., host, network, threat) and details their structure and relationships. The CRUSOE model inspired the ASCOT model, but we extend the existing models to the automotive sector by integrating monitoring data from SDVs with operational context and development data.

IV. Holistic automotive security monitoring

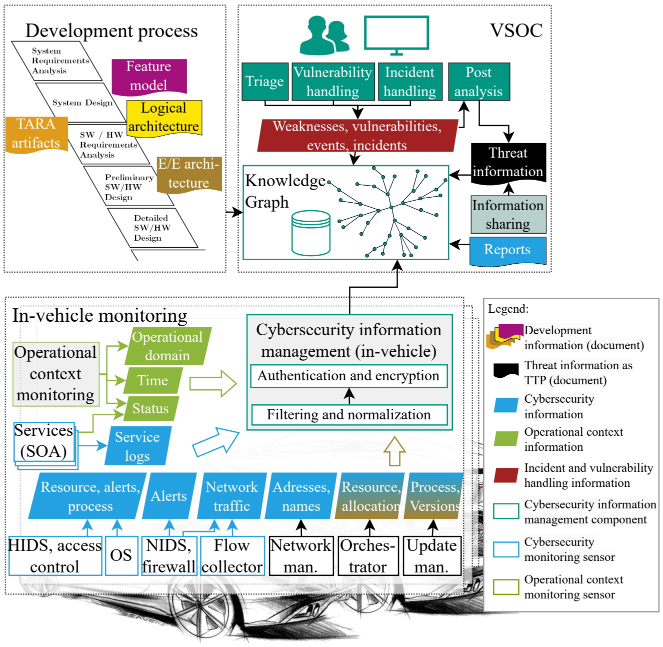
Development process
System Requirements Analysis
System Design
SW / HW Requirements Analysis
Preliminary SW/HW Design
Detailed SW/HW Design
Feature model
Logical architecture
TARA artifacts
E/E architecture
VSOC
Triage
Vulnerability handling
Incident handling
Post analysis
Weaknesses, vulnerabilities, events, incidents
Threat information
Knowledge Graph
Information sharing
Reports
In-vehicle monitoring
Operational context monitoring
Operational domain
Time
Status
Services (SOA)
Service logs
Cybersecurity information management (in-vehicle)
Authentication and encryption
Filtering and normalization
Resource, alerts, process
Alerts
Network traffic
Adresses, names
Resource, allocation
Process, Versions
HIDS, access control
OS
NIDS, firewall
Flow collector
Network man.
Orchestrator
Update man.
Legend:
Development information (document)
Threat information as TTP (document)
Cybersecurity information
Operational context information
Incident and vulnerability handling information
Cybersecurity information management component
Cybersecurity monitoring sensor
Operational context monitoring sensor

Fig. 1. Overview of the holistic monitoring concept, combining in-vehicle monitoring, development process information and external information from information sharing and reports. The vehicle two-way authenticates with the VSOC and sends information via syslog to the Knowledge Graph database.

With the increasing connectivity, and hardware and software becoming similar to IT systems (cf. II-A), IDS and other security monitoring sensors have come to prominence. Although these instruments perceive the network security situation in vehicles solidly, they alone cannot cope with the particularities of vehicles. Namely, monitoring should account for the variable physical context, and the high variability of vehicles, but can profit from the stringent (model-based) development process. Accordingly, our holistic monitoring concept (cf. Figure 1) builds on in-vehicle monitoring, consisting of sensors for the ”cyber” side and operational context monitoring for the ”physical” side of the vehicle. Due to limited remote access and cellular transmission to the VSOC, an in-vehicle management component buffers and filters the information. The filtering is configurable to scale the transmitted information up or down as required. The development process feeds in artifacts to build up relationships between configuration, software, hosts, risks and collected in-vehicle information. From a high-level perspective, the information are atomic components from the eight following areas:

A. Configuration Management

The definition of configurations to engineer different variant is supported by tools. In academia, FeatureIDE has a strong foundation[2]. In industry, the AUTOSAR methodology uses XML-based configuration files, including feature models[3]. Vector Informatik's PREEvision, for instance, supports feature modeling in product lines. During production, hardware is installed based on the configuration selected by the customer, necessitating that the implemented features of each vehicle are digitally available.

B. Logical architecture

Logical system architecture modeling, like configuration management, is supported by tools, e.g. PREEvision and MathWorks System Composer. While the logical architecture may not be fully modeled as SOA, dependencies and capabilities can be derived from existing models, e.g., component interfaces. Interface specification formats like AUTOSAR XML or ROS2 message files enable automated provision. Managing component versions (hardware and software) is challenging. Hardware versions are known at production, but repairs over a vehicle's lifetime complicate tracking. Because delivery of software updates is variable across vehicles due to connectivity issues or customer preferences, the vehicles' update management needs to report its current software versions[4]. In sum, vehicles yield current version information, while the development tools provide components, capabilities and associated data.

C. E/E Architecture

Most of the E/E architecture is statically defined during development, such as network types, sensors, and the software-to-controller mapping for ECUs. Modeling tools export this data, including the version of some basic software (e.g., AUTOSAR classic). OS' version can be queried at runtime. CI/CD tools like Gitlab and Jenkins, which are used in the automotive industry, can produce Software Bill of Materialss (SBOMs), outlining contained third-party components. In SDVs, where software allocation to hosts may be dynamic, the orchestrator provides data on component assignments and network addresses via an API. Additionally, IT tools like Nmap[5] can dynamically identify network services, versions, and OS. Automated approaches for identifying automotive networks and attack surfaces are under research [28], [29].

D. Risk Management

Risk management, mandated by law, relies on TARA in the ISO/SAE 21434 standard [2]. TARA can be unstructured, like brainstorming, which would require manual input to the database. Due to collaboration with suppliers, managing and exchanging TARA artifacts is required, driving the development of formats like openXSAM[6] and tool support for TARA. Accordingly, digital TARA artifacts are expected to be available in the medium term.

E. Cybersecurity Information

Cybersecurity information is generated by sensors within the vehicle, extracted from E/E architecture development artifacts, or comes from external entities such as threat-sharing organizations or researchers. Potential sensors in the vehicle include cybersecurity controls, e.g. IDS (host and network), firewalls, access controls, and other sensors such as flow collection, DNS and DHCP servers / forwarders, the logs of the OS and software services, and the orchestrator. Besides, network addresses, subnets, and domain names within the vehicle are (partly for SDV) set during E/E architecture development. Depending on the sensor, different types of information is generated, including alerts, observed resource usage, such as CPU and RAM, or process execution (non-exhaustive list). Software generates logs, e.g. by built-in mechanisms of Linux, AUTOSAR and ROS 2. CI/CD systems can generate reports by detecting known vulnerabilities in third-party components[7]. External sources provide both structured CTI and (potentially unstructured) reports. In general, requirements on in-vehicle monitoring must be defined and implemented during development. As AUTOSAR standardizes logging, IDS, access control, and firewalls, availability of the required technology is assumed. External sources are strongly required by ISO/SAE 21434. Thus, availability of reports can also be expected.

F. Operational Context

Operational context monitoring focuses on information that describes the safety of the system to observe, in worst-case, the physical impact of attacks. The safety boundaries of a (driving) function are defined by the Operational Design Conditions (ODC) [30], including operational domain (scenery, environment, dynamic objects), users and components' status. For the homologation of automated driving functions, the definition an ODC and its satisfaction are required. Industry suggests a system mode manager to monitor operational domains, which would be the component to provide current operational domain to the VSOC, if privacy restrictions allow.

The status of components can be collected from Diagnostic trouble codes via the diagnostic interface, or, via AUTOSAR mode and network management for software and hardware status. Accordingly, the current operational Context is expected to be available in new vehicles.

G. Incident and Vulnerability Handling

The VSOC personnel is the main user of the database based on the graph-based semantics of the data model. As such, the incident and vulnerability handling processes query and write

[2] https://www.featureide.de/

[3] AUTOSAR Feature Model Exchange Format

[4] Example: Tesla https://www.teslafi.com/firmware.php

[5] https://nmap.org/

[6] https://openxsam.io/wp-content/uploads/2023/06/openXSAM-Towards-a-common-Security-Analysis-Exchange-Format.pdf

[7] https://about.gitlab.com/blog/2023/03/15/getting-started-with-gitlab-application-security

new information to the database for historical tracking and correlation. First, triage creates indicators from cybersecurity information, with relationships to other indicators established through algorithms or manually. These links can be updated during the escalation of security events to incidents, or weaknesses to vulnerabilities. Because remote access is uncommon in vehicles, the execution of responses is expected to be automated, similar to deploying software updates. Therefore, courses of action can be inserted automatically.

H. Threat information

The threat information view relies on CTI and external sources. External automotive CTI sources include threat-sharing organizations like Auto-ISAC [20] (Automotive Information Sharing and Analysis Center), commercial platforms, and databases and catalogs (cf. III). Internal knowledge from observed incidents and vulnerabilities, e.g. attacker techniques and tools, should also be formalized within ”Lessons learned” processes to improve security measures and incident and vulnerability handling [6], [7].

V. The ASCOT data model

In the following, a new graph-based data model is presented in its atomic parts, that links the available information for automotive CSA, resulting from our holistic monitoring concept. ASCOT stands for Automotive Security COntext Toolkit - the data model provides the necessary context awareness for security decisions in a VSOC. Majorly, ASCOT involves aspects of CRUSOE [11], feature-model based configuration management, the ODC taxonomy [30], ISO/SAE 21434 [2], [7] and TTP based CTI modeling similar to MITRE ATT&CK. In total, information from the eight areas of monitoring (cf. IV) is modeled: Threat information, incident and vulnerability handling, risk management, logical system architecture, E/E architecture, cybersecurity information, and operational context. A UML class diagram defines the views and their relationships, without going into detail on attributes. Because we model *data*, not an application, the CLASSES (cf. Table I) contain no methods. The colors of the classes symbolize the respective view (cf. legend in Figure 2). Instances of the classes will be *nodes* in the resulting graph, to be stored in a database. To model relationships, UML associations with unlimited cardinality, and generalizations are used. Associations result in *edges* of the graph, and are directed to support reading the relationship, but shall not limit navigability. Generalization indicates that an information (i.e., node) belongs to two classes. If implemented as LPG, such nodes have several *labels*, which allows to search for information from different viewpoints. Also, it accounts for escalation processes, and unverified information, that are marked as class A first, verified later on to be class B as well.

A. Configuration management

The configuration management view (cf. Figure 2, purple) highlights the differences and similarities in vehicle customer features. A model inspired by product-line engineering is proposed. While configuration management requires 150% models (all possible feature combinations), CSA focuses on 100% models—the configurations actually produced and chosen by customers. This view serves a similar purpose as the “mission” perspective in other CSA models, with the vehicle’s main mission being the provision of customer features.

B. Logical architecture

In the logical architecture view, the vehicle is described by its CAPABILITIES and their dependencies (cf. Figure 2, yellow). This view abstracts the E/E architecture (cf. V-C) and connects customer functions (FEATURE REVISIONS, cf. V-A) with their implementation as services. The view outlines the vehicle’s system perspective, providing insights into the significance of COMPONENTS and their functional impacts.

C. E/E architecture

The E/E architecture represents the ”hosts” and ”network.” This view illustrates physical interconnectivity and software-hardware dependencies (cf. Figure 2, brown), covering hardware and software architecture along with network topology. It maps both traditional E/E architectures with legacy buses and SDVs, showing which software runs on which host. For orchestrated software execution or cloud service connectivity, this view is dynamically updated by the vehicles.

D. Risk management

Risks and potential impacts identified during development are crucial for triage and analysis. This view serves as a key data source and use case, as risk assessments need to be continuously updated. It covers links to configuration, incidents, and vulnerabilities, by connecting ISO/SAE 21434’s TARA taxonomy [2] with other views (cf. Figure 2, orange).

E. Operational context

The ODC taxonomy [30] is the basis for the operational context view (cf. Figure 2, green). This view connects design-time context (assumptions in TARA) with the *Current operational conditions* and *domain* of the vehicle. Although mobility of IT hosts increases (e.g., remote work, smartphones), vehicle mobility is the key operational factor. The CONTEXT view enhances the understanding of other perspectives, especially for assessing the impact and criticality of security events. It helps detect false alarms from IDS due to unusual vehicle behavior, which might not be evident from network data alone.

F. Cybersecurity information

The cybersecurity information view (cf. Figure 2, blue) includes short-lived observables from the vehicle-internal and external communication, reports, and network configuration. CYBERSECURITY INFORMATION is mainly generated by security monitoring tools, which are CYBERSECURITY CONTROLS within the vehicle. The tools gather input from NETWORK ELEMENTS functioning as OBSERVATION POINTS. Additionally, SOFTWARE COMPONENTS and UNITS contribute recorded LOG data or RESOURCE usage. Further derived INFORMATION classes can be added, if required. The triage process creates INDICATORS, marking security-relevant INFORMATION.

TABLE I
OVERVIEW OF CLASSES ACROSS DIFFERENT VIEWS

View	Class	Description
Configuration Management	Vehicle	Configuration of a specific vehicle
	Feature revision	Specific variant and version of a feature
	System revision	All feature revisions of the product line at a certain point in time
	System generation	Unchangeable type and generation of a vehicle
Logical architecture	Component	Hardware and/or software realizing a feature
	Capability	Functionality provided or required by a Component
	Data	Interface type of a Capability or configuration data of a Component
	Version	Semantic tag describing a particular code or hardware configuration of a Component at a given point in time
E/E Architecture	Host	Component, any host that can execute software, either virtualized or physical, including ECUs
	Host cluster	Set of interconnected hosts that share and combine resources for the execution of software
	Host cluster entrypoint	Specific host in a cluster that accepts control commands
	Sensor / Actuator	Hardware Component that is not providing computation resources
	Software component	Provides functionality to the Vehicle or the user, consists of software units
	Software unit	Component, invisible parts of a software component's functionality, including OS, program libraries, and custom code
	Network element	Hardware: Host, Sensor/Actuator, gateways, switches, telematic units
Risk Management	Threat scenario	Compromises cybersecurity property and realizes a damage scenario, has a risk value
	Cybersecurity property	Attribute of a Component or data to protect
	Attack path	Actions to realize a threat scenario, has feasibility rating
	Damage scenario	Adverse consequences, has impact rating
	Cybersecurity control	Component that modifies (reduces) the risk of a threat scenario
Operational Context	Context	Base class for all contexts
	Scenery	Non-movable elements of the operating environment
	Dynamic elements	Movable objects of the operating environment
	Environmental conditions	Includes weather, atmospheric conditions, and connectivity
	Behavior	Behavior of the Vehicle under consideration
	Status	Status of a Component or the Vehicle, including activation status, hardware shutdown, and error conditions
	User status	Status of the driver and passengers
	Time	Local time of the Vehicle, including working hours
Cybersecurity Information	Cybersecurity information	Information for which relevance is not yet determined, including reports, logs, resources, alerts, and network traffic
	Log	Log from a software unit
	Resource	Resource usage measurement or access tracking including CPU, RAM, file system
	Alert	Notification of a cybersecurity control about a detection or blocking (e.g., by an IDS)
	Network traffic	Packets or network flow
	Report	Document with technical findings, especially assessments
	Process	Instance of a program, script or executed command, including updates and diagnostic commands
	Observation point	Network element that provides data for a cybersecurity control
	Network address	Identifier in the network (e.g., IP address, CAN identifier)
	Subnet	VLAN or IP subnet
	Domain name	Name assigned to a server, resolves to an IP address
Incident and Vulnerability Handling	Indicator	Information relevant for an item or Component based on cybersecurity information
	Security event	Indicator of an occurrence relevant for a Component
	Incident	Security event proving active violation of vehicle security, safety, or company security policy
	Weakness	Indicator of a defect or characteristic that can lead to undesirable behavior
	Vulnerability	Weakness that can be exploited
	Course of action	Response to Incidents and Vulnerabilities, aiming at containment, eradication, or recovery
Threat information	Threat source	External or internal provider of strategic information about threats, defined as tactics
	Tactic	High-level behavior of the attacker
	Technique	Technological approach and method used to carry out an attack
	Physical technique	Technique with physical causes, methods, or effects (e.g., access to a vehicle)
	Threat actor	Person, group, or nation-state actor using tools, malware, and techniques
	Tool	Legitimate software or device that can be used by threat actors to perform attacks
	Malware	Malicious code or software inserted into a system, usually covertly
	CVE	Entry in the Common Vulnerabilities and Exposures database

G. Incident and vulnerability handling

The incident and vulnerability handling view (cf. Figure 2, red) connects current and historical incidents. Generalization relations map the taxonomy of incident and vulnerability processes, following a recent update proposal for ISO/SAE 21434 [7], aligning the automotive more closely with IT terminology. Responses (COURSE OF ACTION) are linked to INCIDENTS to create playbooks and track effective actions. Aligning with the ATTACK PATH and DAMAGE SCENARIO connects this view to risk management, enabling the assessment of VULNERABILITIES and INCIDENTS. Additionally, linking to threat information helps infer attackers' intentions. This view supports incident responders and vulnerability assessors and serves as a basis for continuous improvement by identifying patterns (TECHNIQUES) and THREAT ACTORS.

H. Threat information

The final view focuses on the strategic perspective (cf. Figure 2, black) by integrating CTI. It also acts as an incubator for gathering internal threat knowledge. Here, INCIDENTS and VULNERABILITIES are connected to a CTI data model based on Tactics - techniques - procedures (TTP).

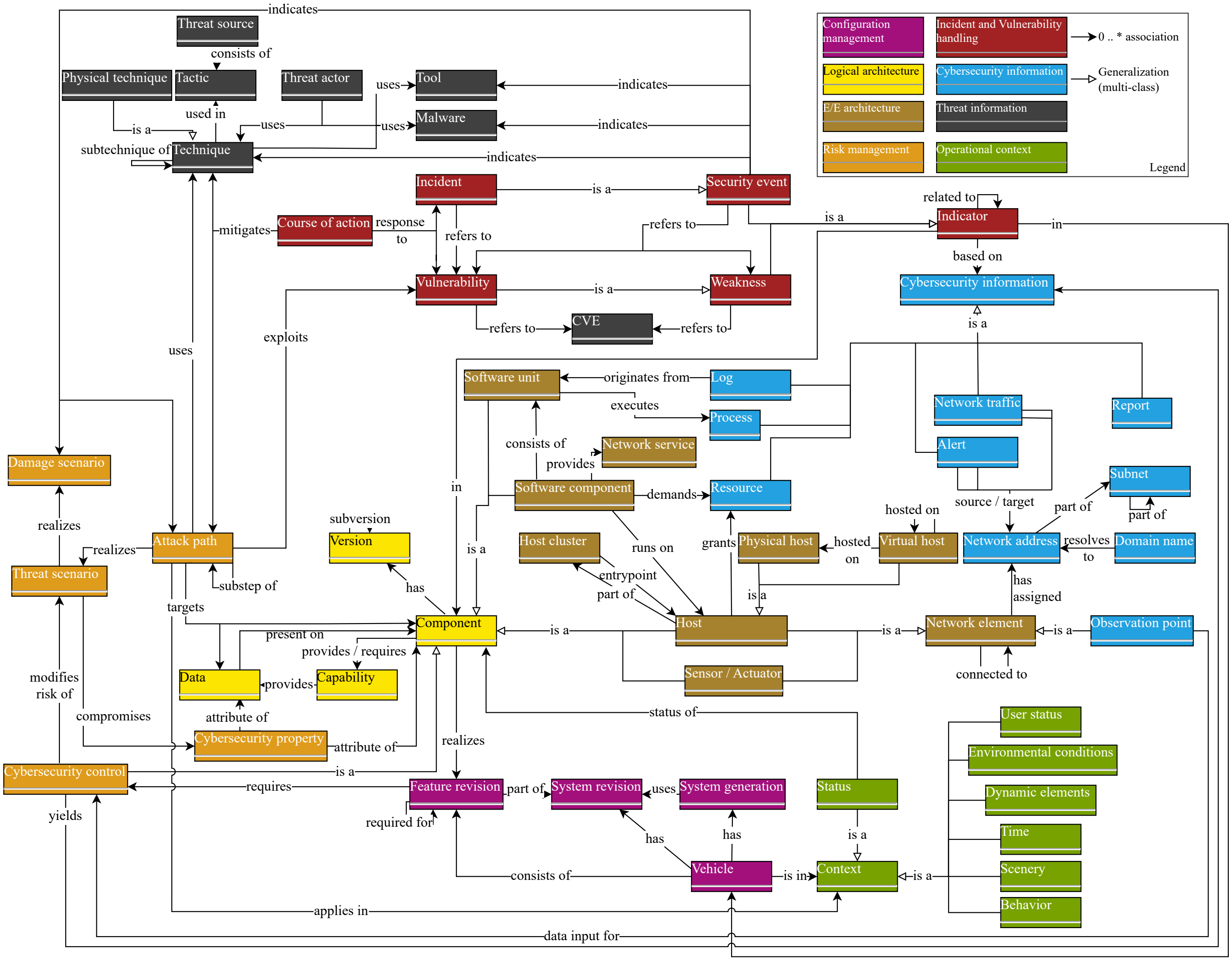

Fig. 2. Full ASCOT data model, combining all views. Legend showing color codes and connectors.

VI. Summary and Future Work

Millions of vehicles must be kept secure over their year-long operations, which includes responding to new threats, incidents and vulnerabilities. VSOCs are the primary approach to timely reaction, despite the challenges of variant diversity, number of vehicles, and physical impacts of attacks. This work is the first to define a comprehensive data model for automotive CSA and correspoding monitoring concept. Network monitoring data and relevant information from within a manufacturer and external sources are fused in a KG to enable perception of the security situation. This model is intended as a unified source of knowledge for VSOCs and as a basis for security decisions.

In the future, responsibilities for filling the database could be defined based on the division into eight views. Besides, access control, the links to employees, the supply chain and insider threats have not yet been fully considered. Use cases of the model will be evaluated using simulated vehicle fleets. In this setting, improvements for the model may be identified.

References

[1] UN Economic Commission for Europe (UNECE), *Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system*, Mar. 2021.

[2] ISO/SAE 21434:2021, “Road Vehicles - Cybersecurity Engineering,” Standard, Aug. 2021.

[3] VicOne, *VicOne Automotive Cyberthreat Landscape Report 2023*, 2023. [Online]. Available: https://documents.vicone.com/reports/automotive-cyberthreat-landscape-report-2023.pdf (visited on 07/03/2024).

[4] F. Langer, F. Schüppel, and L. Stahlbock, “Establishing an Automotive Cyber Defense Center,” in *17th escar Europe*, 2019. DOI: 10.13154/294-6652.

[5] J. Hofbauer, K. K. G. Buquerin, and H.-J. Hof, “From SOC to VSOC: Transferring key requirements for efficient vehicle security operations,” in *21th escar Europe*, 2023. DOI: 10.13154/294-10389.

[6] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, *Computer security incident handling guide*, NIST Special Publication 800-61 Revision 2, Aug. 2012. DOI: https://doi.org/10.6028/NIST.SP.800-61r2.

[7] D. Grimm, A. Lautenbach, M. Almgren, T. Olovsson, and E. Sax, "Gap analysis of ISO/SAE 21434 – Improving the automotive cybersecurity engineering life cycle," in *IEEE 26th International Conference on Intelligent Transportation Systems (ITSC)*, 2023.

[8] U. Franke, A. Andreasson, H. Artman, J. Brynielsson, S. Varga, and N. Vilhelm, "Cyber situational awareness issues and challenges," in *Cybersecurity and Cognitive Science*, A. A. Moustafa, Ed., Academic Press, 2022, ch. 10. DOI: 10.1016/B978-0-323-90570-1.00015-2.

[9] R. Ali, "Cybersituational awareness for the NATO alliance," *The Three Swords Magazine*, vol. 30, pp. 72–75, Jul. 2016.

[10] N. Neshenko, C. Nader, E. Bou-Harb, and B. Furht, "A survey of methods supporting cyber situational awareness in the context of smart cities," *Journal of Big Data*, vol. 7, no. 1, Oct. 2020. DOI: 10.1186/s40537-020-00363-0.

[11] J. Komárková, M. Husák, M. Laštovička, and D. Tovarňák, "CRUSOE: Data Model for Cyber Situational Awareness," in *Proc. of the 13th International Conference on Availability, Reliability and Security*, ACM, 2018. DOI: 10.1145/3230833.3232798.

[12] L. F. Sikos, "Cybersecurity knowledge graphs," *Knowledge and Information Systems*, vol. 65, no. 9, pp. 3511–3531, Sep. 2023. DOI: 10.1007/s10115-023-01860-3.

[13] N. Nayak, D. Grewe, and S. Schildt, "Automotive container orchestration: Requirements, challenges and open directions," in *IEEE Vehicular Networking Conference (VNC)*, 2023. DOI: 10.1109/VNC57357.2023.10136278.

[14] M. Schindewolf, D. Grimm, C. Lingor, and E. Sax, "Toward a resilient automotive service-oriented architecture by using dynamic orchestration," in *IEEE 1st International Conference on Cognitive Mobility (CogMob)*, 2022. DOI: 10.1109/CogMob55547.2022.10118016.

[15] S. Kugele, D. Hettler, and S. Shafaei, "Elastic service provision for intelligent vehicle functions," in *21st International Conference on Intelligent Transportation Systems (ITSC)*, 2018. DOI: 10.1109/ITSC.2018.8569374.

[16] O. Y. Al-Jarrah, C. Maple, M. Dianati, D. Oxtoby, and A. Mouzakitis, "Intrusion detection systems for intra-vehicle networks: A review," *IEEE Access*, 2019. DOI: 10.1109/ACCESS.2019.2894183.

[17] M. Rumez, D. Grimm, R. Kriesten, and E. Sax, "An overview of automotive service-oriented architectures and implications for security countermeasures," *IEEE Access*, 2020. DOI: 10.1109/ACCESS.2020.3043070.

[18] T. Häckel, P. Meyer, L. Stahlbock, *et al.*, *A multilayered security infrastructure for connected vehicles – first lessons from the field*, BROAD workshop at the 2022 IEEE Intelligent Vehicles Symposium (IV) in Aachen, Germany, 2023. arXiv: 2310.10336.

[19] A. R. Yekta, D. Spychalski, E. Yekta, C. Yekta, and S. Katzenbeisser, "VATT&EK: Formalization of Cyber Attacks on Intelligent Transport Systems - a TTP based approach for Automotive and Rail," in *Proc. of the 7th ACM Computer Science in Cars Symposium*, ACM, 2023. DOI: 10.1145/3631204.3631867.

[20] Automotive Information Sharing and Analysis Center. (Mar. 2024), [Online]. Available: https://automotiveisac.com/press-news/the-auto-isac-launches-automotive-threat-matrix-atm-tool-to-enhance-vehicle-cybersecurity-governance (visited on 04/03/2024).

[21] F. Sommer, J. Dürrwang, and R. Kriesten, "Survey and classification of automotive security attacks," *Information*, vol. 10, no. 4, 2019. DOI: 10.3390/info10040148.

[22] Upstream Security, *AutoThreat®Intelligence Cyber Incident Repository*, 2024. [Online]. Available: https://upstream.auto/research/automotive-cybersecurity/.

[23] F. Goldstein, O. Yarkoni, L. Shalmon, H. Glikman, S. Azriel, and G. Molho, "Monitoring automotive cyber risks throughout the deep and dark web," in *19th escar Europe*, 2021.

[24] J. Lüttin, S. Monka, C. Henson, and L. Halilaj, "A survey on knowledge graph-based methods for automated driving," in *Knowledge Graphs and Semantic Web*, Springer International Publishing, 2022. DOI: 10.1007/978-3-031-21422-6_2.

[25] L. Halilaj, I. Dindorkar, J. Lüttin, and S. Rothermel, "A knowledge graph-based approach for situation comprehension in driving scenarios," in *The Semantic Web*, Springer International Publishing, 2021. DOI: 10.1007/978-3-030-77385-4_42.

[26] S. Noel, E. Harley, K. Tam, M. Limiero, and M. Share, "Cygraph: Graph-based analytics and visualization for cybersecurity," in *Cognitive Computing: Theory and Applications*, Elsevier, 2016. DOI: https://doi.org/10.1016/bs.host.2016.07.001.

[27] E. Kiesling, A. Ekelhart, K. Kurniawan, and F. Ekaputra, "The SEPSES Knowledge Graph: An Integrated Resource for Cybersecurity," in *The Semantic Web – ISWC 2019*, Springer International Publishing, 2019. DOI: 10.1007/978-3-030-30796-7_13.

[28] E. F. M. Josephlal and S. Adepu, "Vulnerability analysis of an automotive infotainment system's wifi capability," in *IEEE 19th International Symposium on High Assurance Systems Engineering (HASE)*, 2019. DOI: 10.1109/HASE.2019.00044.

[29] N. Weiss, S. Renner, J. Mottok, and V. Matoušek, "Transport layer scanning for attack surface detection in vehicular networks," in *Proc. of the 4th ACM Computer Science in Cars Symposium*, ACM, 2020. DOI: 10.1145/3385958.3430476.

[30] ISO 34503:2023, "Road Vehicles – Test scenarios for automated driving systems – Specification for operational design domain," Standard, Aug. 2023.