A Domain-agnostic Framework for Secure Design and Validation of CPS Systems

Rohith Yanambaka Venkata, Nathaniel Brown, Rohan Maheshwari and Krishna Kavi

Dept. of Computer Science and Engineering
University of North Texas
Denton, Texas-76207
Email: {nathanielbrown, rohanmaheshwari}@my.unt.edu {ry0080, krishna.kavi}@unt.edu

***Abstract*—Cyber Physical Systems (CPS) are an integration of computational and physical processes, where the cyber components monitor and control physical processes. Cyber attacks largely target the cyber components with the intention of disrupting the functionality of the components in the physical domain. In this paper, we present SIMON, an Ontological design and verification framework that captures the intricate relationship(s) between cyber and physical components in CPS by leveraging standard Ontologies and extending the NIST CPS framework for the purpose of eliciting trustworthy requirements, assigning responsibilities and roles to CPS functionalities and validating that the trustworthy requirements are met by the designed system. We demonstrate the capabilities of SIMON using a vehicle to infrastructure (V2I) safety application. In addition, we also investigate introducing resiliency measures that will ensure compliance of physical systems to specifications.**

Keywords–CPS Security; Ontology; CPS Privacy; CPS Resiliency; Semantic Web

I. INTRODUCTION

CPS systems consist of electronic or computer systems that control physical systems. These systems use sensors to collect information about the physical system and possibly other situational inputs, process these inputs to determine appropriate decisions and affect these decisions on the physical system via actuators, forming a consistent feedback loop between the physical and computational realms. Additionally, the data collection and transmission of actions may involve the use of communication networks. Well-known applications of CPS systems include smart automobiles, manufacturing including additive (3-D) manufacturing, medical monitoring equipment and smart grids.

The increased reliance on such CPS systems in everyday life has resulted in a corresponding increase in available venues for attack for malicious actors. In contrast with information security, which primarily deals with the protection of valuable information, CPS systems offer attackers the potential to affect the physical world through digital means. Thus, it is essential to understand the inter-relationships between the functions of the physical systems and the cyber (or electronic) systems, and how an attack on one affects the other. In this paper, we present an extension of our prior work on a design validation framework that will enable the design of secure CPS systems [1].

Since CPS systems can contain sensors, actuators, electronic/processing components and communication networks, the number of sources receiving and transmitting information is large when compared to traditional systems that fall under a more strict cyber or physical definition, providing many opportunities to attackers who want to impact the digital or physical realm, or both. Real attacks have been carried out on both power grids and interconnected industrial control systems (ICS); such large-scale attacks are predominantly carried out on the "nation or state actors" [2]. Potential attacks include the purposeful disablement or modification of connected medical equipment vital to patient survival, disablement of smart car brakes leading to collisions, and the sabotage of industrial processes to bring harm to industrial production cycles and/or human workers [2][3]. The increased number of demonstrated and theoretical attacks has prompted a response from the cybersecurity community to attempt to develop frameworks and models to address CPS system security concerns [4].

A primary challenge of conceptualizing CPS system security is determining which threats and corresponding security recommendations apply to CPS systems in general, and which are unique to a specific domain. Another challenge is managing the complexity that arises from CPS systems' dual nature of participating in both the cyber and physical realms, referred to as its heterogeneity. Humayed et al. [2] emphasize how CPS systems should satisfy the three traditional information security requirements—confidentiality, integrity, and availability—as well as safety, a fourth metric specific to the physical nature of CPS sytems. Ashibani and Mahmoud [5] recommend a security analysis at the perception, transmission, and application layers of CPS systems. Such static analyses are helpful for beginning to diagnose vulnerabilities in CPS systems and address them through actionable steps. However, the interconnected nature of CPS systems leaves a desire for a modeling framework that can account for the high complexity of CPS systems and the tendency toward human error.

To address these concerns, we advocate the use of Ontologies to model CPS systems and the relationships between their constituent subsystems. An Ontology is a formal description of knowledge as a set of concepts within a domain and the relationships that hold between them [6]. To enable such a description, we need to formally specify individuals (instances of objects), classes, attributes, and relations as well as restrictions, rules, and axioms. Ontologies not only enable a shareable and reusable knowledge representation but, can also add new knowledge about a domain [6]. Further, we extend the NIST CPS framework [7], which includes 3 phases: conceptualization for capturing requirements of the systems, realization, which describes the design and implementation, and assurance, which enables verification of requirements. In our SIMON framework, we subdivide realization phase by differentiating between an abstract realization and a concrete realization levels. The abstract level translates the conceptual requirements of CPS systems (such as functional, timing, trustworthiness requirements) into responsibilities and roles of system components (such as sensors, actuators, processing elements, communication systems, computational algorithms). The concrete realization level defines specific products used to implement the abstract responsibilities and functionalities (such as selecting a specific IoT system, or a communication

device). Our Ontologies allow for common vocabularies to describe concepts and properties of CPS systems at various levels of the design framework. This permits for adapting best design practices of one domain to the design of systems in another domain.

Our prior work on using Ontologies in vulnerability assessment in cloud systems [8] [9] enables us to extend those Ontologies to address security concerns in CPS systems. Using the NIST CPS framework as a basis for SIMON allows for a broad and integrated view of CPS and positions trustworthiness, among other aspects of CPS design. Furthermore, using standard Ontologies like SOSA [10] will help streamline the process of secure CPS design by considering the properties of a CPS system like sensing and actuation.

The rest of the paper is organized as follows. Section III describes SIMON, our proposed CPS framework. This section also describes the various standard Ontologies, as well as some of our new Ontologies used in the framework. Section IV includes two case studies to show how SIMON can be used for the design and validation of CPS systems. We show some examples of cyber attacks and use reasoners to identify potential compromise of design goals associated with the physical system.

II. Related Work

Extensive research has been conducted in applying Ontologies to either identify or validate the security posture of CPS or IoT systems. Mozzaquatro et al. [11] propose a framework that employs a model-driven approach to designing secure CPS systems. While this may be prudential in some domains, it fails to account for concerns from various stakeholders in a CPS system. This is addressed by the NIST CPS framework [7].

Fenz et al. [12] and Settas et al. [13] propose Ontological frameworks that are complemented by Bayesian analysis to predict threat probabilities in cloud systems. The key competencies of these contributions is vulnerability assessment and threat modeling for cyber systems in the cloud. These frameworks are not directly applicable to CPS systems because they do not account for the physical components of these systems. Moreover, additional vulnerabilities exist in the intersection between cyber and physical components in a CPS system. Modeling this interaction is essential in understanding the impact of a potential compromise.

Gonzalez-Gil et al. [14] describe an Ontology for Machine to Machine (M2M) data security in Internet of Things (IoT) systems. The focus of this work is to define a semantic framework to facilitate knowledge sharing and improve security of IoT systems. The Ontology describes various data security traits involved in data access and exchange in IoT systems. Its purpose is to serve as a common vocabulary supporting the description of the security mechanisms associated with data and data exchange, which are strategic and crucial in varied domains, such as data provisioning, service aggregation and data processing [14]. While the knowledge sharing property of an Ontology is leveraged in this work, the logical reasoning property is not. Hence, the true capability of Ontologies is not fully harnessed.

Bhandari and Gujral [15] present a semantic approach to modeling the security posture of a network. A computer network is a dynamic entity with a constantly changing topology. The addition and removal of new services, hardware components and sub networks, and modification of new user roles contribute to the dynamic status of a network. This work can be considered a precursor to the Structured Threat Information Expression (STIX) Ontology that is discussed in Section III.

Lannacone et al. [16] describe an Ontology developed from a database of cyber security knowledge graphs. It is intended to provide an organized framework that incorporates information from a variety of structured and unstructured data sources.

Current research investigating the feasibility of semantic technology for security in CPS appears to the limited to knowledge reuse. Several semantic frameworks have been developed to understand the security posture of cyber systems. While these frameworks may provide an insight into the security issues that plague various CPS systems, this information may be unreliable because the frameworks do not account for the tight coupling between cyber and physical components. Furthermore, identifying security concerns at the design stage of CPS systems using Ontologies has not been explored.

SIMON aims to bridge the gap between system design and validation using cyber threat data from multiple sources. We believe that this approach will help in the design of secure CPS systems.

III. SIMON Framework

The proposed framework combines (and extends) existing standard specification Ontologies such as Semantic Sensor Networks (SSN), and develop new ones as required by the domain of interest. Let us take a closer look at some of the Ontologies and frameworks used in our research.

A. NIST CPS Framework

National Institute of Standards and Technology (NIST) has developed a framework that provides guidance in designing, building and verifying complex CPS systems [7]. The framework captures generic functionalities that CPS provide, the activities and artifacts needed to support conceptualization, and realization and assurance of CPS design [7]. Designing a CPS system involves:

- **Conceptualization -** This involves capturing all activities related to high-level goals, functional requirements and organization of CPS as they pertain to what the CPS is supposed to do. It provides a conceptual model of the CPS system under consideration and can be used to capture requirements from different perspectives (such as functional, timing, trustworthiness, business).
- **Realization -** This involves capturing all activities surrounding the detailed engineering, design, production, implementation and operation of the desired systems. However, to facilitate comparing Ontological models of CPS systems, we propose bifurcating the overarching realization phase described in the NIST CPS framework into the following sub-phases.
  - **Abstract Realization -** In this phase, design goals are broken down into roles and responsibilities and delegated to subsystems and interfaces. For example, we may identify that the network communications needed in the system will be handled by a wireless data

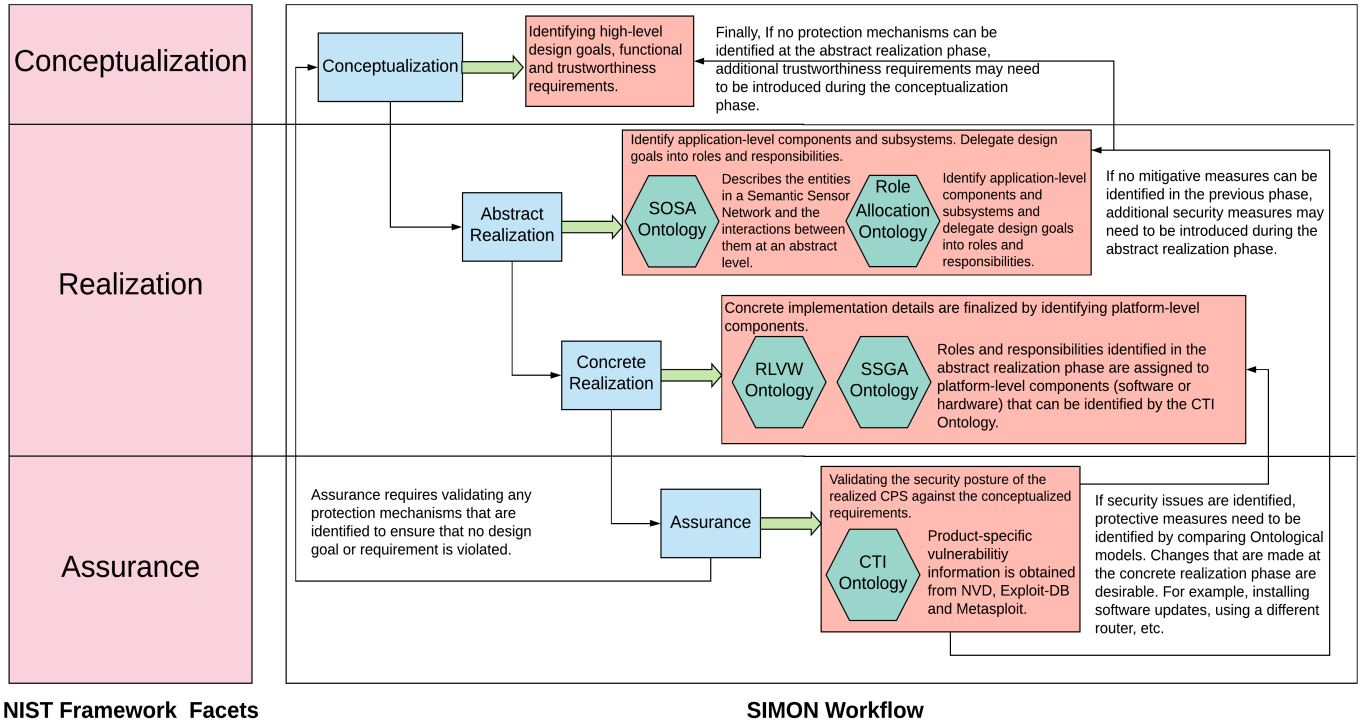

Figure 1. The SIMON Ontological Framework.

communication application but not provide details on either the specific hardware device or communication protocols. We use Ontologies to capture the Abstract Realization.

- **Concrete Realization -** The roles and responsibilities identified during the abstract realization phase need to be implemented by specific products. For example, a Cisco ASR1002-10G-HA/K9 may be selected as the wireless data communication role identified in the Abstract Realization phase. We use Ontologies to relate the products used for various functions and roles identified in the Abstract Realization.

- **Assurance -** The assurance phase deals with obtaining confidence that the system built in the realization phase satisfies the model developed in the conceptualization phase [7]. In our case, we use reasoners to infer and derive assurances (or violations) that the security goals are met. We use additional Ontologies to capture cyber threat data so that vulnerabilities, cyber attacks and possible mitigations can be related to the products identified in Concrete Realization; we rely on NIST Common Platform Enumeration (CPE) identities with specific products for this purpose.

SIMON can be used to modify the CPS design at any of the various phases to address any design violations discovered by our reasoners. Figure 1 describes an abstract view of our framework for the design and verification of CPS systems, focusing on security and trustworthiness.

B. Role Allocation

Requirements traceability is an essential property in identifying changes/modifications to components that will improve the security posture of a CPS system. Delegating design goals from the conceptualization phase into roles and responsibilities for entities identified in the two realization phases will help achieve traceability.

The abstract realization phase involves identifying application-level components, sans the implementation details. Each system identified in this phase can be used to define a role that associates a set of conceptualized functional requirements for the underlying sub-systems to realize. In addition, each role be assigned security responsibilities to be fulfilled. The responsibilities from abstract realization are mapped to the specific concrete realizations: several abstract roles may be assigned to a single concrete component. A detailed example is presented in Section IV.

The trustworthiness requirements as described by the NIST CPS Framework include:

- **Privacy:** Addresses concerns pertaining to the prevention of unauthorized agents gaining access to data stored in, created by or transiting through a CPS system or its components [7].
- **Reliability:** Addresses concerns related to the ability of a CPS to deliver stable and predictable performance in the expected conditions [7].
- **Resilience:** Addresses concerns related to the ability of a CPS to withstand instability, unexpected conditions, and gracefully return to predictable, but possibly degraded performance [7].
- **Security:** Addresses concerns related to the ability of the CPS to ensure that all of its processes, mechanism (both cyber and physical), and services are afforded internal or external protection from unintended and unauthorized access, change, damage, destruction, or use [7]. Security

can best be described through three lenses:

- **Confidentiality:** Preserving authorized restrictions on access and disclosure.
- **Integrity:** Guarding against improper modification or destruction of system, and includes ensuring non-repudiation and authenticity
- **Availability:** Ensuring timely and reliable authorized access to and use of a system.

We use several different Ontologies in our framework to describe the concepts, properties and restrictions associated with CPS systems at each of the design phases described in this section.

C. Sensor-Observation-Sampling-Actuator Ontology (SOSA)

The Sensor-Observation-Sampling-Actuation Ontology (SOSA) [10], a subset of the Semantic Sensor Network (SSN) Ontology, presents a conceptualization of all entities, activities and properties that typically constitute a CPS. SOSA is a World Wide Web Consortium (W3C) standard specification.

The *core structure* of SOSA Ontology encompasses all of the three modeling perspectives of sensors and actuators; the activities of observing, sampling, and actuating [10]. Each activity targets a feature of interest by either changing its state or revealing its properties by following a designated procedure. All activities are carried out by an object, also called an *agent*.

SOSA aims to strike a balance between the expressivity of the underlying description logic, the ease of use of language features and the expectations of the target audience, while accommodating a broad range of domains and applications [10].

D. Cyber Threat Information Ontology

The activities of observing and sampling must be followed by communicating and processing the data to interpret the observations and making decisions on the actions. These actions are then used to control physical systems through actuation. The communication and processing subsystem, which is not directly included in the SOSA Ontology, can expose the cyber and physical components of the CPS to security attacks. Thus, SOSA must be extended to describe the processing and communication subsystems. This allows us to relate cyber threat data from multiple sources to obtain insights into the security posture of a CPS system under consideration. We have defined an Ontology that captures Cyber Threat Information (CTI) from three sources:

- **The National Vulnerability Database (NVD) -** A U.S. government repository of standards-based vulnerability management data [17].
- **Exploit Database -** An archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers [18].
- **Metasploit -** A framework for developing, testing and executing software exploits [19].

Our Ontology can easily be extended to capture CTI from other sources. The cyber threat Ontology is underpinned by the STIX structured language [20], that enables organizations to share, store and analyze CTI in a consistent manner, allowing security communities to better understand what computer-based attacks they are most likely to see and to anticipate and/or respond to those attacks more effectively. The STIX Ontology utilizes twelve core concepts: Attack pattern, Campaign, Course of Action, Identity, Indicator, Intrusion Set, Malware, Observed Data, Report, Threat Actor, Tool and Vulnerability.

Attack Pattern describes ways that threat actors attempt to compromise targets, and *Campaign* categorizes malicious activities that occur over a period of time by identifying their intended targets. *Vulnerability* describes a flaw in software (or hardware) that can be exploited by a *Threat Actor* to breach a target.

Our objective in defining the CTI Ontology is to unify information from three sources (described earlier in this section) and facilitate logical reasoning about the security of CPS using *Axioms*. Axioms are rules used by a reasoner to infer additional information that may be hard to define in a knowledge representation language. To provide a perspective of the complexity of CTI Ontology, it includes 6657 axioms that describe CTI data. In addition to STIX, the our CTI Ontology also inherits characteristics from two additional Ontologies:

- **Cyber Observable Expression (CybOX)** - A standardized language for encoding and communicating information about cyber observables [20]. Using CybOX language [21], relevant observable events or properties pertaining to an attack pattern can be captured.
- **Common Attack Pattern and Enumeration (CAPEC)** - Provides a dictionary of known patterns of attack employed by adversaries to exploit known weaknesses in cyber-enabled capabilities [22].

E. MITRE ATT&CK Framework

The CTI Ontology obtains a perspective on the common techniques and tactics used by adversaries through the MITRE ATT&CK framework [23]. This information is useful while assessing an organization's cyber risk and to prioritize threat response. The framework, which stands for Adversarial Tactics, Techniques, and Common Knowledge, was officially released in May 2015 but has undergone several updates since then. Successful and comprehensive threat detection requires understanding common adversarial techniques and prioritize threats that may especially pose a severe risk to an organization, in addition to detecting and mitigating these attacks.

The ATT&CK framework is a comprehensive matrix of tactics and techniques. The aim of the framework is to improve post-compromise detection of adversaries by illustrating the actions an attacker may have taken. It is vital to understand how the attacker(s) gained access and how they migrate within a network. This framework helps identify those problem areas and contributes to the awareness of an organization's security posture at the perimeter and beyond. Organizations can use the framework to identify holes in defenses, and prioritize them based on risk.

ATT&CK can be extremely useful for evaluating an environment's level of visibility against targeted attacks with the existing tools deployed across an organization's endpoints. A technique is a specific behavior to achieve a goal and is often a single step in a string of activities employed to complete the attacker's overall mission. ATT&CK provides many details about each technique including a description, examples, references, and suggestions for mitigation and detection.

A tactic is an objective or mission of an adversary. It describes what an attacker hopes to achieve with a specific compromise. Each tactic contains an array of techniques that have been used by malware or threat actor groups in known compromises. There are 11 tactics and over 250 techniques identified in the framework.

ATT&CK aids in the strategic response to cyber risks by outlining the tactics, techniques and attack vectors that could be used to compromise a CPS system. This insight, in addition to the structure of threat intelligence offered by STIX, may prove to be invaluable in identifying, enumerating, quantifying and addressing risks in CPS.

Here is a brief look at some of the important characteristics of our CTI Ontology:

- **Attack:** This feature is mapped to the *Indicator* and *Observed Data* classes in the STIX Ontology and the *Observation, FeatureOfInterest* and *ObservableProperty* classes in the STIX Ontology. This characterizes a cyber attack by identifying a pattern and a set of adversarial behaviors or information observed on a system in the network.
- **Exploit:** Mapped to the *Vulnerability* and *Intrusion set* classes in the STIX Ontology and the *Sensor, Actuator* and *Sample* classes in the SOSA Ontology, the Exploit feature enumerates a flaw in a platform (Software or Hardware with a CPE entry in the NVD) that can be leveraged by an adversary to compromise a CPS system.
- **Ramification:** Incident response teams often desire to know the consequences/objectives of potential adversaries to prioritize responses to cyber attacks. In a similar vein, threat modeling at the design phase of a CPS system will equip CPS designers to understand the outcome of cyber attacks and design more secure or resilient systems. At present, threat classification is based on the Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service and Elevation of Privilege (STRIDE) model [24], where each type of threat is assigned its own class. The *Ramification* feature maps to a class in the STRIDE based on the nature of the threat. In addition, it also maps to the *ThreatActor, CourseOfAction* and *Vulnerability* classes in the STIX Ontology and the *Actuation, Observation, Procedure, FeatureOfInterest, Platform* and *ObservableProperty* classes in the SOSA Ontology.

Thus, our framework allows users to identify and enumerate cyber threats that affect a CPS system of interest. We rely on Ontologies because of the following benefits they offer:

- **Knowledge Representation:** The primary benefit of using an Ontology is its ability to define a semantic model of data within the context of an associated knowledge domain. This can be leveraged to achieve knowledge sharing and, more importantly, knowledge reuse, which is discussed in the next section.
- **Logical Reasoning:** Reasoning in Ontologies and knowledge bases is an important property. Reasoning refers to deriving facts that are not explicitly specified in the Ontology. Ontologies use description logic to facilitate tractable reasoning.
- **Modularity:** Our framework facilitates modularity by allowing CPS designers to use domain-specific properties (Ontologies like SOSA). Users have the option of using additional vocabulary, in addition to the W3C specification to model proprietary systems.
- **Extensibility:** CPS systems are constantly evolving. Advances in networking and embedded system technologies like system-on-chip (SoC) and wireless transceivers result in the emergence of new CPS applications. The structure of SIMON, coupled with its modular design, supports integrating or modifying CPS characteristics, and facilitates reasoning about the security posture of a system.

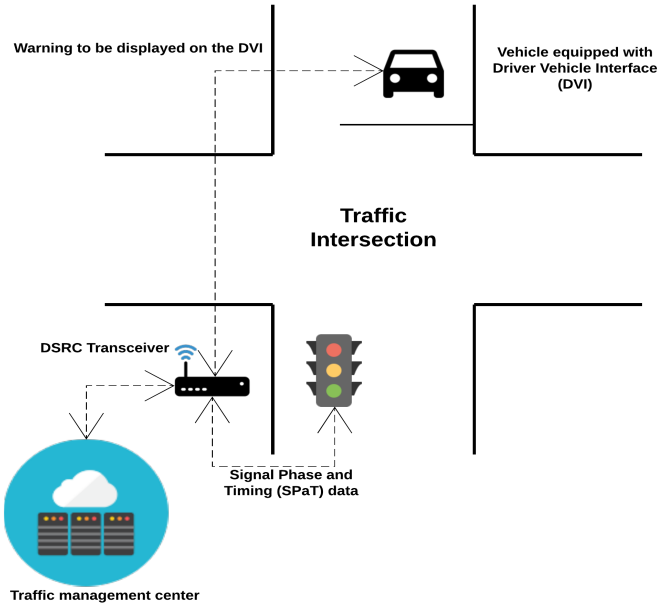

Figure 2. The RLVW system

IV. Vehicle To Infrastructure (V2I) Wireless Data Interface Ontology: A Case Study

As a case study to show the value of our framework, we use the Red Light Violation Warning (RLVW) safety application as described in the US Department of Transportation document [25]. The Red Light Violation Warning (RLVW) application enables a connected vehicle approaching an instrumented signalized intersection to receive information from the infrastructure regarding the signal timing and the geometry of the intersection. The application in the vehicle uses its speed and acceleration profile, along with the signal timing and geometry information, to determine if it appears likely that the vehicle will enter the intersection in violation of a traffic signal. If the violation seems likely to occur, a warning can be provided to the driver.

Figure 2 depicts the RLVW system. To identify the most vulnerable areas in this system, it is vital to understand the flow and origin of data (i.e., sensing and observation aspects of the system). Intelligent Transportation Systems (ITS) developers and automobile companies will be designing their CPS components to take advantage of the upcoming 5G data networks. Because such networks provide increased bandwidth and reduced latency, data will not only travel faster and in larger packets but will also be more vulnerable to attacks. For this case study, we developed an Ontology that highlights the data activity around the wireless portion of the RLVW protocol.

In addition to choosing this region, we have highlighted only the CPS components that have either wireless capabilities or using the data collected from the wireless components. Thus, the Ontology highlights the wireless data interface portion of the V2I system where our conditions are met.

The design of the Ontology itself was made with respect to a few different factors. One of which was the component usage of the 5G networks. Components at the top of the hierarchy had active roles in communicating data from the Infrastructure to the Vehicle or vice versa. Components towards the bottom had more specific roles in acquiring and processing certain types of data that were necessary for signal phase calculations, optimal deceleration distance, and Differential Global Positioning System (DGPS) calculations. Organizing the Ontology with this factor in mind will allow for developers to quickly find the affected component during an attack based on the V2I data usage of the attacker. If the attacker had access to large amounts of data, it is highly likely that a component making heavy usage of the 5G network was involved. Conversely, if the attack was less threatening and had access to a smaller amount of data, the component involved would most likely be at the bottom of the hierarchy.

Another factor in designing the Ontology was splitting the components responsible for generating data into data collection and data calculation roles. Often times, attacks involve limiting the capabilities of components to collect data, whereas others involve altering the calculations of the collected data. To distinguish between the two, we organize components into cyber and physical categories. The cyber components are responsible for calculations, whereas the physical components (i.e sensors, actuators) are responsible for collecting data.

Lastly, we assign data types to each of the hardware and software components. Not only does this help understand which components are making use of which data, but it provides indicators in times of attacks. To elaborate, if it is known what type of data an attack is making use of, we can use a traceability methodology to start from the bottom of the Ontology at that specific data type, and trace up the Ontology until we find potential components that could be involved in the attack. Then, modifications and countermeasures can be taken to patch these vulnerabilities.

The flow of data in the Ontology has revealed that the Infrastructure Wireless Data System (IWDS) and the Vehicle Wireless Data System (VWDS), which are connected through the V2I Wireless Data Interface, are the most vulnerable regions of the entire V2I CPS, because in this data flows through an open network. With the source and destination IP addresses of data packets unprotected, this can lead to numerous threats from any third party with a V2X communication handler.

Now, we describe how our framework and the Ontologies described in Section III can be used to evaluate the RLVW system. Our framework, which extends NIST CPS framework and includes the Conceptualization phase, Abstract and Concrete Realization phases, and Assurance phase.

A. Conceptualization Phase

The design goal of the Vehicle to Infrastructure (V2I) Wireless Data Interface (WDI) system is to communicate relevant data between the Infrastructure and Vehicle application components through WDI and Application Platforms (APs). The V2I WDI incorporates algorithms and data exchanged to perform calculations to recognize “high-risk” situations. This inference results in issuing driver alerts and warnings through specific protocols. The most primitive and fundamental goal of the V2I WDI is to calculate and communicate Signal, Phase and Timing (SPaT) information to the vehicle with support of driving advisories and warnings [25]. The system is also responsible for maintaining authenticity of transmitted data through security measures. Corrupted data can result in compromising driver safety and information privacy. In our view, the three primary trustworthy design goals of the V2I WDI system are:

- **Verify Incoming Data (VID):** Since the system serves as a bridge between the vehicle and infrastructure domains, its main design goal revolves around transmitting data between both components. Therefore, a key requirement of this system is to verify the authenticity of incoming data from either side of the system, to avoid Phishing and other instances of fraudulent data transfer. This should be accomplished through ingress filtering protocols set in place to verify packet source headers and IP addresses.
- **Verify Outbound Data (VOD):** The WDI system is also responsible for generating advisories and alerts tailored to each nearby vehicle. With this in mind, a supporting requirement for this design goal must be to implement Secure Socket Layer (SSL) protocols or an alternative cryptographic key to ensure outbound data is not tampered with before reaching its destination.
- **Data Routing to Proximate Vehicles (DRPV):** Because this system is involved with establishing multiple connections between the infrastructure and vehicles, there is no generic set of messages purposed for all vehicles. Each advisory is calculated using metrics provided by each vehicle, thus creating a functional requirement to ensure that each message is sent to the appropriate vehicle. Failure of this requirement can serve fatal if metrics are sent to the incorrect vehicle, which may result in traffic violations or accidents.

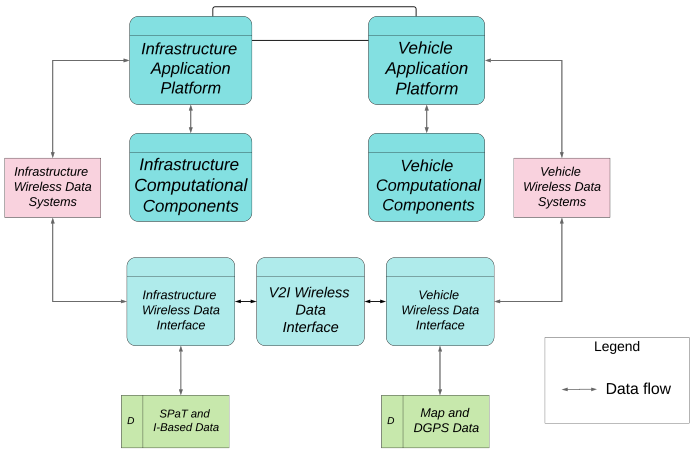

Figure 3. The V2I Wireless Data Systems Network

B. Abstract Realization Phase

The functional requirements listed in the conceptualization phase are purposed to describe the theoretical capabilities of

a CPS. When moving into the application layer components that satisfy the desired goals of the V2I WDI System, it is important to categorize each component along the respective requirement it resolves. This way, in the assurance phase, it can be tested how well the design goal of each component meets its functional requirement. Each component in the abstract realization phase will be assigned its own role.

Since the V2I WDI system is only a portion of the entire V2I domain, its design goal only covers data transmission. Therefore, only the transmission capabilities and roles of the categorized components will be discussed. Additionally, it is important to note that the sub components of both the infrastructure and vehicle contain similar components with only slightly varying goals. When working with CPS systems, the cyber and physical aspect of this CPS can be made resilient independently. However, the current issue that Intelligent Transportation System (ITS) developers face is maintaining that level of security when combining both sides of the system. This is because the integration of optimal designs when forming the system can lose the resiliency of both the cyber and physical aspects. To understand these challenges, we form a general hierarchy of the V2I WDI network that maps each component to the requirement it fulfils [25]. This will unravel the group of threats associated at each layer of the system. Figure 3 shows an overview of the V2I wireless data interconnect.

1) Verify Incoming Data (VID) Associated Components:

- **Infrastructure Wireless Data Systems (IWDS):** The Infrastructure Wireless Data Interface (IWDI) is responsible for sending and receiving data to/from nearby vehicles via the V2I Wireless Data Interface (VWDI). Its main role is to validate passing data by making sure position accuracy of incoming vehicles is up to the DoT standards. Additionally, the system calculates SPaT and Differential Global Positioning System (DGPS) metrics to be deployed to nearby vehicles via the IWDI.

  The IWDI role helps realize all activities related to communication with vehicles equipped with a VWDI. In other words, all three conceptual design goals are supported by the IWDI role. The conceptual design goals mandate that the security, privacy, and resiliency requirements be associated with the IWDI role.

- **Infrastructure Application Platform (IAP):** The IAP is the computational platform, which hosts the Infrastructure Application Component and provides the necessary hardware and software interfaces enabling communication with Infrastructure Wireless Data Systems, Infrastructure Data Systems, Roadside Signage System, Traffic Signal Controller, and Local/Back Office User Systems. Its main role is to channel all data gathered by sensors and physical systems to the cyber components. It can be considered the bridge between the cyber and physical components of the infrastructure side of the CPS, thus making it one of the least resilient and most vulnerable parts of the CPS.

  The IAP role is perhaps one of the most important in the RLVW system. It facilitates the interaction between the constituent systems in the infrastructure and the vehicle. It is apparent from the conceptual goals that the IAP role must meet the security, privacy, resiliency and reliability requirements.

- **Vehicle Wireless Data Systems (VWDS):** This component receives messages from the Vehicle Application Component through the Vehicle Application Platform, and formats and processes messages to be received by infrastructure components. This system also transmits data from the Vehicle Wireless Data Interface to the deeper hardware of the vehicle. This system also obtains GPS location and time. It may include a processor for GPS differential correction. Its main role is to convey information from the capture point at the Vehicle Wireless Data Interface to the internal components below and vice versa.

  The VWDS role is essential in ensuring communication between the sensors in the infrastructure space and the innards of VDWI. Hence, it must support the security and resiliency requirements outlined in the previous section.

- **Vehicle Application Platform (VAP):** The Vehicle Application Platform is the computational platform, which hosts the Vehicle Application Component and provides the necessary hardware and software interfaces enabling communication with Vehicle Wireless Data Systems, Vehicle Data Systems, and the Driver Warning Systems. Its main design goal is to channel all data gathered by vehicle sensors, actuators, and On-Board Diagnostics (OBD) data to the vehicular cyber components for processing and calculations. It can be considered as the counterpart to IAP on the infrastructure side. The security responsibilities of VAP are identical to those of IAP.

2) Verify Outbound Data (VOD) Associated Components:

- **Infrastructure Wireless Data Interface:** The IWDI is responsible for sending and receiving to nearby vehicles via the V2I Wireless Data Interface. Its main design goal is to refresh data transmission frequency at a configurable pace. It is also required to be equipped with countermeasures in case of corrupt or tampered data transmission. In these cases, it should issue warning messages to nearby vehicles to terminate data transmission and calculations using any information that comes from the Infrastructure.

  IWDI defines the functional requirements pertaining to communication with VWDI. The functional requirements of IWDI dictate that it should support security and resiliency.

- **Vehicle Wireless Data Interface:** The VWDI is responsible for sending and receiving to nearby Industrial Control Systems such via the V2I Wireless Data Interface. Its main design goal is to validate incoming data and request new packets from the infrastructure at a configurable frequency. It is also required to correct map and DGPS data for the infrastructure application component to produce the most precise RLVW metrics. In the case of inaccurate or corrupt data, the VWDI is required to terminate data transmission and issue alerts to the driver information interface.

  VWDI is the vehicle-side equivalent of IWDI. So, intuitively, this role should support the same security requirements as IWDI: security and privacy.

3) DRPV Associated Components:

- **V2I Wireless Data Interface:** Acts as a bridge for data transmission between the entire Infrastructure and

Vehicle components. It receives raw data from the Infrastructure and vehicle components. This communication is functional over a bi-directional Dedicated Short Range Communication (DSRC) network. Therefore, its security protocol is effective within 1000 meters of any attacker. Beyond that, connectivity is loose and vulnerable. Its main design goal relative to the RLVW application is to ensure secure data transmission between approaching vehicles and signalized intersections.

It is evident from the description of this application that it sustains all three design goals of the RLVW system. Its vital importance means that this role should support privacy, reliability, resilience and security.

C. Infrastructure Data Types and Significance

Starting with the Infrastructure, its physical components consists of the signalized intersection sensor systems that capture two main types of data [25].

D. SPaT

SPaT data (Signal Phase and Timing) contains information about the behavior of the traffic controllers regarding the state of the signal (viz., red, green or yellow), how long that state will remain, and time until next phase change.

E. Driving Conditions

The physical component of the infrastructure also produces data that characterizes the environmental conditions approaching vehicles may face. This data consists of weather data, visibility data, and road conditions for the vehicle to incorporate in its decision making computations, to improve precision in judgement as approaching the intersection.

F. Vehicle Data Types and Significance

The vehicle's physical components consists of the position and stability systems, actuators, and telematic sensors that transmit Differential GPS (DGPS) and Dynamic Telematic Data (DTD) [25].

1) Differential GPS: DGPS data contains map data of the vehicle's position relative to the approaching signalized intersection. The vehicle data systems transmit DGPS to the infrastructure in order to alert the traffic controllers of the instantaneous distance the vehicle is from the intersection.

2) Dynamic Telematic Data: DTD consists of information regarding the vehicle's speed and position, and reveals how the vehicle is behaving internally. This data is combined with DGPS and incoming SPaT data from the vehicles to make calculations using DVI equations and algorithms in order to make a precise judgement of whether the driver should increase or decrease speed to avoid traffic violations and or accidents at the intersection.

G. Concrete Realization Phase

Now that the baseline for the design goals and supporting components are established, we can identify technical aspects of the identified components to understand how these functional requirements are met. Mapping the hardware and software to their respective components will help unravel the classification of security threats, since it is at this phase where the core data transmission occurs. Up until now, the above layers cover high-level understandings of the V2I WDI System. Now, we will classify core hardware and software that is generalized for both sides of the system in order to understand the mechanics behind V2I data transmission.

- **DSRC On Board Unit (OBU):** The DSRC OBU is the dedicated communication device installed on V2X connected vehicles. This hardware is responsible for establishing and receiving SPaT and Roadside data at a configurable frequency between 5.8 GHz -5.9 GHz. It utilizes the widely adaptive ThreadX RTOS operating system designed specifically for Internet of Things (IoT) applications. The DSRC OBU assists in enabling the capabilities of the Vehicle Wireless Data Interface [26].
  The OBU resides in vehicles and is responsible for implementing the VWDS, VAP and VWDI roles from the abstract realization phase. All of the security requirements associated with each constituent abstract-level component must be supported by the OBU. For example, an encrypted communication channel will fulfill both privacy and confidentiality requirements mandated by the roles that this component supports.
- **DSRC Roadside Unit (RSU):** The RSU unit performs identical functions but on the other end of the V2I wireless network. It is responsible for receiving SPaT and Roadside data from the infrastructure technical systems, verifying the data, and transmitting it upon data request from nearby vehicles. The RSU unit enables the capabilities of the V2I Wireless Data Interface, acting as the cyber bridge between the Vehicle and Infrastructure cyber components.
  The RSU is responsible for supporting the roles of IWDS, IAP, and IWDI. The security requirements associated with each of the three roles need to be supported by the RSU.
- **Wireless Sensor Network (WSN):** The WSN is the sensor network on the infrastructure side that captures road conditions data, infrastructure-based vehicle detection, road conditions, speed data, visibility data, and weather data. It utilizes sensors and actuators for the detection aspect of the hardware and standard transceivers, antennas, and receivers for the communication aspect of the hardware [27]. The Infrastructure Wireless Data Systems are supported by this WSN network, acting as the source of raw data that is formatted and processed into metrics by the Data Systems.

The WSN resides in the intersection between infrastructure and vehicle subsystems, and facilitates communication between the IWDI and VWDI systems. It is required to support the security requirements associated with these two roles.

H. Assurance Phase

The assurance phase deals with obtaining confidence that the CPS system built in the concrete realization phase satisfies the goals described in the abstract realization and conceptualization phases. Validating the concrete CPS system involves ensuring that it meets the functional and security requirements associated with the roles that each component supports.

Figure 4 illustrates the hierarchy of role allocation in SIMON. Evaluating the security posture of a CPS system requires current CTI data from multiple sources. To that end,

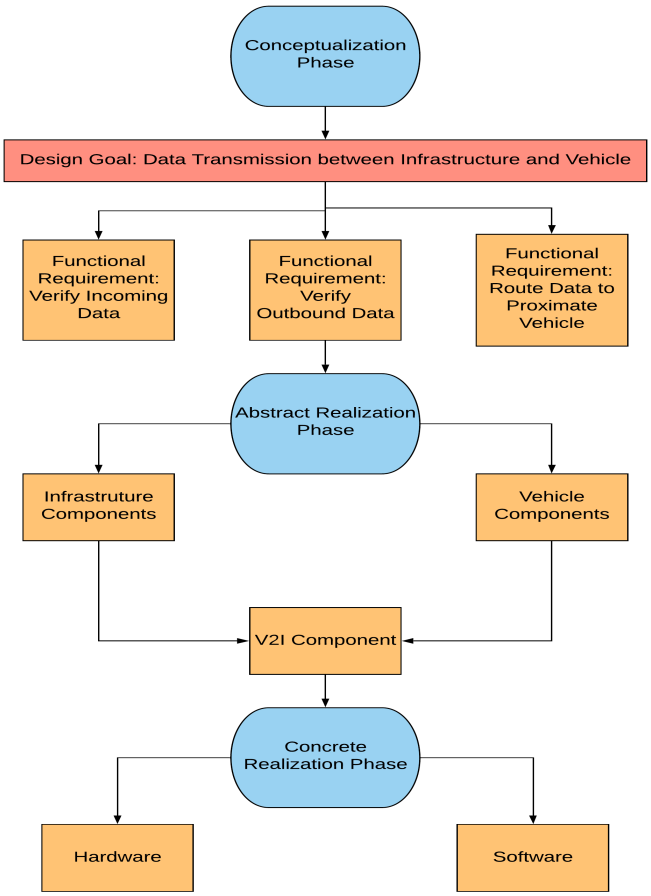

Figure 4. Role allocation hierarchy

SIMON's CTI Ontology discussed in Section III-D provides pertinent information.

Let us consider the example of an OBU running ThreadX RTOS. The OBU is responsible for sustaining the VWDS, VAP and VWDI roles, which necessitate the support for privacy, security and resiliency requirements. CTI is able to formulate a CPE identifier for this system using information obtained from the NVD. CPE:2.3:o:marvell:88w8997_firmware:-:*:*:*:*:*:*:* identifies the ThreadX-based firmware on a Marvell Avastar WiFi device. The Common Vulnerability Scoring System (CVSS) metrics from the NVD for this CPE indicate that the attack vector for a threat that exploits this vulnerability would be adjacent, which means that any infected devices in a local network could potentially compromise other devices in the network. Furthermore, the high severity score from the CVSS metrics indicates that a an attack that leverages this vulnerability could be catastrophic. If the system were to be affected by CVE-2019-6496 [28], an adversary may be able to launch a denial of service attack on the OBU. The vulnerability allows remote attackers to execute arbitrary code or cause a denial of service (block pool overflow) via malformed WiFi packets during identification of available WiFi networks. Exploitation of the WiFi device can lead to exploitation of the host application processor in some cases, but this depends on several factors, including host OS hardening and the availability of DMA.

To understand the impact of this vulnerability on the CPS system, the requirements traceability property offered by SIMON must be leveraged. This would show how the impact of a potential exploitation of this vulnerability would propagate up the three stages of design processes. Figure 5 shows various inferences that the reasoner makes in providing the insights presented below.

```
The Ontology is consistent
On-Board Unit (OBU) CPE : cpe:2.3:o:marvell:88w8997_firmware:-:*:*:*:*:*:*:*
(Asserted) OBU uses ThreadX OS
(Inferred) CVE-2019-6496 could be exploited
(Inferred) Potential violation of requirement 1.2.1 of the VWDS System
(Inferred) Potential violation of requirement 1.5.2.2 of the VAP system
(Inferred) Potential violation of requirement 1.4.2 of the VWDI system
```

Figure 5. DoS attack inference

- In the concrete realization phase, a vulnerability in the OBU would violate the functional requirements of both the DSRC roadside unit and the OBU. It is desirable to implement mitigative measures in the concrete realization phase because it wouldn't require a complete overhaul or re-engineering of systems previously implemented.
- In the abstract realization phase, all the roles fulfilled by the OBU and DSRC transceiver, VWDS, VAP, VWDI, IWDS, IAP, IWDI are violated. The corresponding security requirements pertaining to availability are affected. CVE-2019-6496, being a vulnerability exploited for DoS, confidentiality and integrity requirements may not be impacted.
- In the conceptualization phase, all three requirements (VOD, VID and DRPV) are affected by the unavailability of the OBU. thereby impacting the primary design goal of the RLVW system, which is to prevent roadway fatalities by ensuring date transmission between the infrastructure and vehicles.

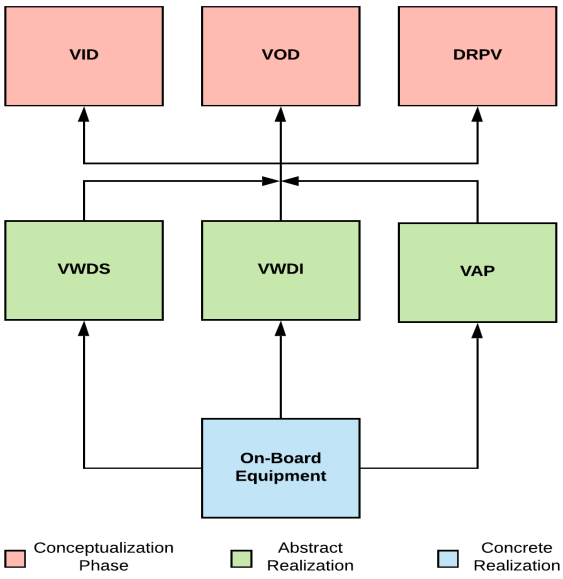

Figure 6. DoS attack on the OBU

A DoS attack on the OBU would violate the availability requirement for all three roles supported by the OBU (VWDS, VAP and VWDI), thereby violating the DRPV design principle of the CPS system. Figure 6 shows the how the design goals

of the RLVW system will be affected by such an attack on the OBU. The knowledge reuse property of SIMON can be used to compare various CPS systems to identify mitigative measures from other domains that can be reused in the CPS system under consideration. We have presented multiple examples in our prior work [1]. These insights would be invaluable to CPS system designers.

I. *Identifying Security Threats and Protection Mechanisms*

In this section, let us consider a few vulnerabilities and potential corrective measures in the RLVW system using SIMON. Now that the baseline for the V2I WDI region is set, we can analyze the proposed Ontology to classify potential threats in the flow of data.

1) V2X Remote DSRC Interjection Threat: The IWDS and VWDS communicate through the V2I WDI over a bidirectional DSRC network [25]. While DSRC provides a robust and low latency connection for short distance communication [29], its security protocol only prevents Distributed Denial of Service (DDoS) attacks from a short distance. Therefore, a third party with V2X communication handlers can interject data transmission remotely through Internet Protocol and Domain Name Service (IP/DNS) spoofing attacks to reroute outgoing Differential GPS (DGPS) data and Dynamic Telematic Data (DTD) from the vehicle. With this data in their possession, unauthorized V2X handlers can track drivers and read into vehicle logs, which creates privacy issues for the victim. The NIST Vulnerability Database highlights a similar issue with the configuration *cpe:2.3:a:cisco:application-policy-infrastructure- controller:8.31s6:*:*:*:*:*:*:** [17]. Existence of this vulnerability suggests that this simple attack is highly probable, if correct mitigation is not in place. A potential start for resolving this issue may involve ITS developers implementing a SSL certificate with outgoing data, which requires V2X handlers to have a certain cryptographic key in order to access the contents of the data packets [30].

```
The Ontology is consistent
Road side equipment CPE : cpe:2.3:a:cisco:application-policy-infrastructure-controller:8.31s6:*:*:*:*:*:*:*
Adversary may leverage CVE-2017-12352 to gian elevated privileges
Adversary may tamper with the RLVW warning data that is broadcast to vehicles
(Warning) Potential violation of functional requirement 1.1.5 of the Road side equipment
(Inferred) Potential violation of functional requirement 1.2.4.7 of the RLVW system
(Inferred) Potential violation of functional requirement 1.2.5.2 of the RLVW system
(Inferred) Potential violation of functional requirement 1.1 of the Driver Interface system
```

Figure 7. RLVW Inference.

The CTI Ontology obtains vulnerability information for components identified in the concrete realization phase using NIST CPE (Common Platform Enumeration) identifications. In this example, let us consider one vulnerability that can be exploited for privilege escalation with NIST Common Vulnerability Enumeration (CVE) identification, *CVE 2017-12352*, associated with the CISCO router with *cpe:2.3:a:cisco:application-policy-infrastructure-controller:8.31s6:*:*:*:*:*:*:** [17]. An adversary can exploit this vulnerability in certain system script files on Cisco Application Policy Infrastructure Controllers to gain elevated privileges and execute arbitrary commands with root privileges on an affected host operating system [31]. The vulnerability is due to insufficient validation of user-controlled input that is supplied to script files of an affected system [31]. A simple fix would be to install a software update for the application policy infrastructure controller. However, to demonstrate the capabilities of Ontological modeling and reasoning, we will assume that no software patches are available for this component.

Figure 7 shows how the CTI Ontology uses semantic reasoning to link vulnerabilities to the design goals identified during the conceptualization phase. While an elevation of privilege attack can lead to catastrophic failure of the affected system, we will focus on adversaries potentially spoofing their identities in this example.

The Extensible Authentication Protocol (EAP), a certificate-based authentication scheme, can validate the V2X handler that issues requests for DGPS and DTD data. This prevents most spoofing attacks.

```
The Ontology is consistent
Distinction identified between SSGA and RLVW VWDS
(Asserted) SSGA uses wireless message authentication scheme
(Inferred) EAP introduces latency
(Inferred) Potential violation of requirement 1.3.1 of the Driver Interface System
(Inferred) Potential violation of requirement 1.5.2.2 of the RLVE system
```

Figure 8. Comparing the Ontologies

Figure 8 illustrates how the message authentication scheme is capable of preventing the spoofing attack identified by the CTI Ontology. However, this scheme introduces latency, which may impact the timing requirement listed in the conceptualization phase of RLVW. Let us investigate if message authentication scheme is a viable solution for RLVW.

```
(Asserted) Timing Requirements 1.3.4.1 needs to be met
(Inferred) RLVW zone needs to be extended to 100 meters
(Asserted) DSRC radio has a maximum range of 120 meters
(Inferred) Additional requirements need to be added at abstract realization
```

Figure 9. Testing compliance

As evidenced from Figure 9, the Ontology determines that the RLVW requirement to warn drivers well in advance of a red light violation to provide ample stopping distance may be violated by the latency that is introduced by the authentication scheme. Furthermore, the Ontology also infers that the components used in this system are capable of supporting the timing requirement as the DSRC transceiver has a range of 120 meters. To address this, the Ontology recommends that the warning zone be increased from 80 meters before the intersection to 100 meters, which should provide ample time for EAP to authenticate the communication. A requirement needs to be added in the abstract realization phase to include an authentication scheme that also includes fail-safe measures if authentication is inconclusive. A domain expert needs to be consulted to ensure that all design goals are accurately captured in the SIMON framework.

2) V2X Handler Elevation of Priviledge Threat: Unfortunately, DSRC communication between V2I WDI and VWDS is not the only insecurity of the WDI region. The performance requirements set by the DoT do not mention any form of security over the functionality of the IWDS and VWDS [25]. In this section, we investigate the possibility of improving the resiliency of a CPS system against privilege escalation attacks by implementing a fail-safe mechanism. The proposed Ontology outlines the path of data through the Infrastructure Application Component (IAC) and Platform (IAP) that reveals no form of encryption on data produced by the physical components or verification when that data is transmitted through the cyber components. Therefore, V2X Handlers with identical communication functionality and IP addresses can

replace the role of the IWDS in the TCP handshake and give false acknowledgement to the IAP. V2X Handlers can then tamper with outbound SPaT and road data, which results in the vehicle application component producing false metrics. These metrics may result in a red light traffic violation or even roadside accidents. A similar vulnerability issue is noted with the configuration *cpe:2.3:o:cisco:ios-xe:16.10.1:*:*:*:*:*:*:** in the NIST Vulnerability Database [17], thus indicating the possibility of this threat occurring roadside. A general solution to this vulnerability can involve ITS developers implementing an ingress filtering protocol that requires the VWDS to check incoming data packets for their source headers, to ensure it matches the one of the origin and to reject the packet if it does not [30].

To authenticate entities within a network, Public Key Infrastructure (PKI) encryption may be used. This requires a Certifying Agency (CA) to generate and assign a public key to each component in the system. The CA is maintained by the DoT. The messages are authenticated using Message Authentication Code (MAC). PKI is a comprehensive security and authentication scheme requiring all entities to ensure confidentiality, integrity, non-repudiation and end-to-end monitoring and key life cycle management.

The CTI identifies the configuration of the V2X handler and maps it to *cpe:2.3:o:cisco:ios-xe:16.10.1:*:*:*:*:*:*:**. It is able to identify vulnerability *CVE 2019-1756* that can be leveraged by adversaries to launch an elevation of privilege attack to breach the communication channel between the IAC and IAP. A vulnerability in Cisco IOS XE Software could allow an authenticated, remote attacker to execute commands on the underlying Linux shell of an affected device with root privileges [32]. The vulnerability occurs because the affected software improperly sanitizes user-supplied input. An attacker who has valid administrator access to an affected device could exploit this vulnerability by supplying a username with a malicious payload in the web UI and subsequently making a request to a specific endpoint in the web UI. A successful exploit could allow the attacker to run arbitrary commands as the root user, allowing complete compromise of the system [32].

```
The Ontology is consistent
Road side equipment CPE : cpe:2.3:o:cisco:ios-xe:16.10.1:*:*:*:*:*:*:*
Adversary may leverage CVE-2019-1756 to gian elevated privileges by code injection
Adversary may tamper with SPaT data
(Asserted) Potential violation of functional requirement 1.1.5 of the Road side equipment
(Inferred) Potential violation of functional requirement 1.2.4.7 of the RLVW system
(Inferred) Potential violation of functional requirement 1.2.5.2 of the RLVW system
(Inferred) Potential violation of functional requirement 1.1 of the Driver Interface system
(Inferred) Potential violation of functional requirement 1.1.6 of the RLVW system
```

Figure 10. Elevation of Privilege Threat Inference

The potential impact of this vulnerability being exploited is shown in Figure 10. The framework is able to infer that the primary design goals of the RLVW application and the roadside equipment may be violated as a direct result of this vulnerability.

As discussed in the previous example, EAP and message authentication can be also be used in this example to protect the RLVW system. However, we are interested in identifying possible resiliency measures that can be employed by the RLVW system to protect against privilege escalation attack. To identify activities that can be used in the vehicle to detect spurious data from the infrastructure, let us consider an autonomous vehicle that is capable of perceiving the world around it.

We have defined a simple Ontology that models approximately 3118 attributes of an autonomous vehicle that includes driving actions like stop and go, a collision warning system, a lane change detection system, and so on. The insights provided by this Ontology can be used to prevent attacks like those discussed above by introducing resiliency into the design of the CPS system. The inference engine compares the RLVW system against three principles of a fully autonomous vehicle.

- **Sensing the world -** It is imperative for autonomous vehicles to possess the ability to perceive the world around them.
- **Conveying intent -** Assuming that other autonomous vehicles are present in the immediate vicinity, conveying intent such as lane change or impending change in driving action to other vehicles (and possibly pedestrians) is required.
- **Situational awareness -** Assigning a context to the information obtained by sensing the world is essential in making an informed decision. Comprehending events in the environment with respect to time and space is crucial.

```
1. Ensure vehicle meets requirement for sensing the world (1.2.1.1)
                - Cameras in the front windshield to detect traffic lights (Refer to requirement 1.3.3.2)
```

Figure 11. Measure to introduce resiliency into the RLVW system

The Ontology limits the inference to the design principle of sensing the world for the RLVW system as the other principles do not apply to it. Applying all three principles will negate the role of the infrastructure elements in this V2I system. To that end, the insights provided by the Ontology are shown in Figure 11.

While this is only a preliminary design of a specific region of the V2I CPS, the potential of an Ontology-based model is shown through the vulnerabilities it can classify. By describing various components through their roles, data types, and functionality, the Ontology can reason about new threats or vulnerabilities upon the addition of an unknown component to the system. If the properties of the unknown component, which in this case study is a V2X handler, become known, the Ontology can use reasoners to infer where this new component may interject by comparing properties of the new component with existing components in the CPS. When a match is found, the Ontology will classify the new component in a certain instance of the CPS. This knowledge can be used to implement new levels of security and mitigation in existing components to make it difficult for V2X handlers to either interject the CPS, or play the role of a component in the CPS [33].

V. Conclusion and Future Work

In this paper, we have presented an argument for modeling CPS using Ontologies. We also presented SIMON, a framework that is based on the NIST CPS framework but extends it in several ways. We have presented an extension to our previous work on CPS design validation using semantic inference. Reasoning about a CPS realization and validating that the realization does not violate functional as well trustworthiness goals is essential in improving the security posture of a CPS system. Currently, the SIMON framework is not capable of

automatically translating design goals into Ontological models. We are currently exploring the possibility of extending our work to support this function in the future.

We demonstrated that the role allocation Ontology is capable of delegating the functional and security requirements among subsystems at various design stages of a CPS system. It offers requirements traceability to understand the impact of a security threat in CPS. An RLVW system was used a case study to demonstrate the role allocation Ontology's capabilities. In the future, we intend to investigate other CPS domains. We use Ontologies during each design phase of the framework to check for compliance and provide recommendations by reusing knowledge. Increased traction in CPS adoption, their growing complexity, and heterogeneous nature necessitates accuracy in capturing the relationship between various components in a CPS. Reasoning about a CPS realization and validating that the realization does not violate functional as well as trustworthiness goals is essential in improving the security posture of a CPS system. The SIMON framework can aid in this process. We have only described the framework at a very high level, and we plan to integrate various Ontologies and reasoning engines in the near future. Although Ontologies are used extensively for knowledge representation in domains such as healthcare and bioinformatics, we aim to leverage their capabilities to define a domain-agnostic framework that can be extended to various CPS domains by attributing domain-specific properties (like SOSA).

ACKNOWLEDGEMENT

This research is supported in part by the NSF Net-centric Industry-University Cooperative Research Center at the University of North Texas and the industrial members of the center. The authors would also like to acknowledge the infrastructure and support provided by the Center for Agile Adaptive and Additive Manufacturing funded through State of Texas Appropriation (190405-105-805008-220).

REFERENCES

[1] R. Y. Venkata, R. Maheshwari, and K. Kavi, "SIMON: Semantic Inference Model for Security in CPS using Ontologies," *ICSEA-2019*, pp. 1–2, 2019.

[2] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—a survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, 2017.

[3] J. Prinsloo, S. Sinha, and B. von Solms, "A review of industry 4.0 manufacturing process security risks," *Applied Sciences*, vol. 9, p. 5105, Nov 2019.

[4] J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos, and M. Kantarcioglu, "Security and privacy in cyber-physical systems: A survey of surveys," *IEEE Design Test*, vol. 34, no. 4, pp. 7–17, 2017.

[5] Y. Ashibani and Q. H. Mahmoud, "Cyber physical systems security: Analysis, challenges and solutions," *Computers Security*, vol. 68, pp. 81 – 97, 2017.

[6] "What are ontologies?." URL: {https://ontotext.com/knowledgehub/fundamentals/what-are-ontologies/[accessed: 2019-06-11]}.

[7] D. A. Wollman, M. A. Weiss, Y. Li-Baboud, E. R. Griffor, and M. J. Burns, "Framework for cyber-physical systems," *Special Publication (NIST SP) - 1500-203*, 2017.

[8] P. Kamongi, M. Gomathisankaran, and K. Kavi, "Nemesis: Automated architecture for threat modeling and risk assessment for cloud computing," 12 2014.

[9] P. Kamongi, S. Kotikela, K. Kavi, M. Gomathisankaran, and A. Singhal, "Vulcan: Vulnerability assessment framework for cloud computing," in *Proceedings of the 2013 IEEE 7th International Conference on Software Security and Reliability*, SERE '13, (Washington, DC, USA), pp. 218–226, IEEE Computer Society, 2013.

[10] K. Janowicz, A. Haller, S. J. D. Cox, D. L. Phuoc, and M. Lefrançois, "SOSA: A lightweight ontology for sensors, observations, samples, and actuators," *CoRR*, vol. abs/1805.09979, 2018.

[11] B. Mozzaquatro, C. Agostinho, D. Goncalves, J. Martins, and R. Jardim-Goncalves, "An ontology-based cybersecurity framework for the internet of things," *Sensors*, vol. 18, p. 3053, Sep 2018.

[12] S. Fenz, "An ontology- and bayesian-based approach for determining threat probabilities," in *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, ASIACCS '11, (New York, NY, USA), pp. 344–354, ACM, 2011.

[13] D. Settas, A. Cerone, and S. Fenz, "Enhancing ontology-based antipattern detection using bayesian networks," *Expert Systems with Applications*, vol. 39, no. 10, pp. 9041 – 9053, 2012.

[14] P. Gonzalez-Gil, J. A. Martinez, and A. F. Skarmeta, "Lightweight data-security ontology for iot," *Sensors*, vol. 20, p. 801, Feb 2020.

[15] P. Bhandari and Manpreet Singh Gujral, "Ontology based approach for perception of network security state," in *2014 Recent Advances in Engineering and Computational Sciences (RAECS)*, pp. 1–6, 2014.

[16] M. Iannacone, S. Bohn, G. Nakamura, J. Gerth, K. Huffer, R. Bridges, E. Ferragut, and J. Goodall, "Developing an ontology for cyber security knowledge graphs," pp. 1–4, 04 2015.

[17] "National Vulnerability Database." URL: https://nvd.nist.gov/ [accessed: 2019-06-11].

[18] "Exploit-DB." URL: https://www.exploit-db.com [accessed: 2019-06-20].

[19] "Metasploit-penetration testing framework." URL: https://www.metasploit.com/ [accessed: 2019-06-20].

[20] S. Barnum, "Standardizing cyber threat intelligence information with the structured threat information expression (stix)," *MITRE*, 2014.

[21] "Cyber Observable Expression." URL: https://cyboxproject.github.io [accessed: 2020-06-10].

[22] "Common Attack Pattern Enumeration and Classification (CAPEC)." URL: https://capec.mitre.org/ [accessed: 2019-07-02].

[23] "Mitre ATTCK Framework." URL: https://attack.mitre.org [accessed: 2020-07-21].

[24] Microsoft Corporation, "The STRIDE threat model." URL: https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20) [accessed: 2019-07-08].

[25] Department of Transportation, "Performance Requirements, Vol. 3, Red Light Violation Warning (RLVW)," *Vehicle-to-Infrastructure (V2I) Safety Applications*, pp. 1–68, 2015.

[26] "Vehicle to Infrastructure interaction (V2I)." URL: http://www.mogi.bme.hu/TAMOP/jarmurendszerek_iranyitasa_angol/math-ch09.html [accessed: 2019-09-19].

[27] D. Sánchez-Álvarez, M. Linaje, and F.-J. Rodríguez-Pérez, "A Framework to Design the Computational Load Distribution of Wireless Sensor Networks in Power Consumption Constrained Environments," *Sensors(Basel)*, pp. 2–5, 2018.

[28] "National Vulnerability Database." URL: https://nvd.nist.gov/vuln/detail/CVE-2019-6496 [accessed: 2019-06-11].

[29] "Dedicated short range communications (dsrc) service," 2019. URL: https://www.fcc.gov/wireless/bureau-divisions/mobility-division/dedicated-short-range-communications-dsrc-service [accessed: 2019-06-11].

[30] "Ddos glossary," 2019. URL: https://www.cloudflare.com/learning/ddos/glossary/ [accessed: 2019-06-11].

[31] Cisco, "Cisco application policy infrastructure controller local command injection and privilege escalation vulnerability," 2017. URL: = https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171129-apic [accessed: 2019-07-22].

[32] Cisco, "Cisco ios xe software command injection vulnerability," *Cisco security advisory*, 2019. URL: = {https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190327-iosxe-cmdinject} [accessed: 2019-07-22].

[33] R. Y. Venkata and K. Kavi, "An Ontology-Driven Framework for Security and Resiliency in Cyber Physical Systems," *The Thirteenth International Conference on Software Engineering Advances*, pp. 4–6, 2018.