Requirements Traceability in Cyber Physical Systems using Semantic Inference

Rohith Yanambaka Venkata, Rohan Maheshwari and Krishna Kavi

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

***Abstract*—The distinguishing feature of Cyber Physical Systems (CPS) is the coupling of computational and physical systems, where embedded cyber systems monitor and control physical processes. CPS is responsible for an important role in critical infrastructure, and everyday life. They include smart networked systems with embedded sensors, processors and actuators that sense and interact with the physical world and support real-time, guaranteed performance in safety-critical applications. The cyber-physical nature, coupled with safety-critical application greatly increases the attack surface and the impact of cyber attacks. Understanding the interaction between various subsystems in a CPS is vital in evaluating its security posture and identifying the measures to mitigate threats. To that end, the ability to trace a CPS design from the requirements elicitation phase to the implementation phase, otherwise known as requirements traceability may prove to be invaluable. This paper presents an Ontological approach to requirements traceability in CPS by building upon our previous work on defining the Semantic Inference Model for Security in CPS using Ontologies (SIMON), a design framework for CPS systems.**

Keywords–CPS Security; Ontology; CPS Privacy, CPS Resiliency.

I. INTRODUCTION

CPS systems are increasingly benefiting from the expanding IoT network as they are implemented in the infrastructure. Their role in Industrial Control Systems puts upon a heavy load of data transmission between their cyber and physical components [1]. They face an increasingly difficult challenge across domains as the relationship with the infrastructure heightens in complexity. Independently, cyber and physical systems have developed a resiliency towards outsider threats since the structure of these systems have not required adaption [2]. However, the rapid integration of these systems as a single unit has brought upon changes in architecture that implies vulnerabilities [3].

In an age where the relationship between cyber and physical systems are conflating to create new applications of IoT, the ramifications of security threats are more severe than before. The intertwining of existing communication and information technologies with physical systems such as power plants, healthcare systems, and transportation has increased the autonomous capability to the infrastructure. The implementation of software in these domains has resulted in increased risk of unauthorized access to these newly integrated systems. Consequently, cyber attacks are more severe when the gained privileges cover access to a larger system.

Cyber and physical systems follow a framework that characterizes the path that data takes from a physical to application layer. When considering the amalgamation of these two systems, it can be inferred that new transmission phases will be implemented in order for CPS systems to communicate internally. Therefore, the encryption protocols over the current stages will not cover the introduced vulnerabilities in the layers connecting the cyber and physical components of a system. Therefore, data traveling between these respective planes will be vulnerability to outside attacks and manipulation. The outcome of which can compromise the functionality of the additional components now involved.

Vulnerabilities in CPS systems increase the amount of possible access nodes in both the cyber and physical sub domains. As new components are added in the CPS domain to bridge the cyber and physical components, the region of attack becomes unclear and difficult to mitigate. In fact, because CPS systems require connectivity and reliability on a larger scale than sub domain systems such as the internet, their security protocols contain a higher level of complexity [3]. The increased attack surface calls for threats to be identified in two categories: Infrastructure Security and Information Security. In order to do so, it is important to develop a new framework that can account for threats and vulnerabilities in the increased connection points, data transmission phases, and components involved in CPS systems.

With a plethora of functional requirements, data paths, and components involved in CPS networks, Ontologies provide a reliable technique to visualizing these concerns. Ontologies are a system of components that are connected through the semantic web. Relationships between components and their functionality are described using logical axioms, taxonomies, and other classification tools. These relationships along with objective ruling systems and characteristics of CPS components allow Ontologies to reason about possible vulnerabilities as well the attack path taken to compromise the system. When considering a new CPS domain, Ontologies provide a systematic methodology to understanding the internal communication systems as well as identifying and classifying security threats.

In this paper, we propose a role application framework in which we dissect security threats and vulnerabilities relative to the layer they are violating. In our previous work [4], we presented a semantic inference framework that supplemented the NIST CPS framework [5] divided CPS engineering into three layers as follows: Conceptualization, Abstract Realization, and Concrete Realization [4].

In the Conceptualization Phase, we will organize design goals and top priority functional requirements that describe the CPS system's overarching goals. This way, it will be apparent how individual threats impact the capabilities of the CPS system.

Moving into the Abstract Realization Phase, the supporting functional requirements will be denoted in the order they assist the execution of the design goals. Each requirement will be broken down into roles and responsibilities that are to be met by the CPS components. In addition to listing the objectives of the requirements, there will also be security properties that

 ISBN: 978-1-61208-752-8

define the level of resiliency required to ensure reliability in the component. This process will occur recursively until all components are assigned roles. At this stage, we can proceed into the next layer.

In the Concrete Realization Phase, the components organized in the Abstract Realization Phase will be divided into the individual hardware and software components that allow for functionality of the CPS component. The technical identification and mitigation of security threats in the CPS domain will occur here. Once an issue is located in the CPS system, the traceability of the requirements and all linked quantities can be used to identify where a change in the system needs to be made.

The rest of the paper is organized as follows. Section II outlines the structure of the Semantic Inference Model for Security in Cyber Physical Systems using Ontologies (SIMON) framework. In addition, the main contribution of this paper, the role allocation Ontology is also discussed in this section. Section III demonstrates the capabilities of the role allocation framework using the Red Light Violation Warning System (RLVW) as a case study.

II. SIMON Framework

In a companion paper in this conference, we presented the SIMON framework [4] that combines (and extends) existing standard specification Ontologies, such as Semantic Sensor Networks (SSN), and new ones as required by the domain of interest. For the sake of completeness, we will replicate some key aspects of SIMON in this paper. First, we will review some of the Ontologies and frameworks used in our research and then, present a role allocation procedure that enables requirements traceability.

A. NIST CPS Framework

National Institute of Standards and Technology (NIST) has developed a framework that provides guidance in designing, building, verifying, and analyzing complex CPS systems [5]. The framework captures generic functionalities that CPS provide, the activities and artifacts needed to support conceptualization, realization and assurance of CPS design [5]. Designing a CPS system involves:

- **Conceptualization -** Capturing all activities related to high-level goals, functional requirements and organization of CPS as they pertain to what a CPS should be and what they are supposed to do. It provides a conceptual model of the CPS system under consideration.
- **Realization -** 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. No implementation details pertaining to products (components and sub-components) are identified. For example, we may identify that the network communications needed in the system will be handled by a wireless data 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 will be used as an edge router that functions as the wireless data communication application 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 CPS built in the realization phase satisfies the model developed in the conceptualization phase [5]. This includes evaluating claims, argumentation and gathering evidence required to address important requirements of design, policy, law and regulation [5]. In our case, we use reasoners to infer and derive assurances (or violations) of the goals and functional requirements are met. We use additional Ontologies to capture cyber threat data so that vulnerabilities, cyber attacks and possible mitigative measures 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.

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 the overarching design goals from the conceptualization phase into roles and responsibilities for entities identified in either of the realization phases will help achieve this property.

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 defines a set of conceptualized functional requirements for the underlying sub-systems to realize. In addition, each role may define a set of security requirements to be fulfilled. In the concrete realization phase, a detailed example is presented in Section III.

The trustworthiness requirements as described by the NIST CPS Framework can be categorized as:

- **Privacy:** Privacy requirements address concerns pertaining to the prevention of entities gaining access to data stored in, created by or transiting through a CPS system or its components [5].
- **Reliability:** Address concerns related to the ability of a CPS to deliver stable and predictable performance in the expected conditions [5].
- **Resilience:** Address concerns related to the ability of a CPS to withstand instability, unexpected conditions, and gracefully return to predictable, but possibly degraded performance [5].
- **Security:** Concerns related to the ability of the CPS to ensure that all of its processes, mechanisms, both physical and cyber, and services are afforded internal or external protection from unintended and unauthorized access, change, damage, destruction, or use [5]. Security can best be described through three lenses:

 ISBN: 978-1-61208-752-8

- **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 access to and use of a system.

SIMON can be used to modify the CPS design at any of the various phases to address any design violations discovered by our reasoners. We use different Ontologies in our framework to describe the concepts, properties and restriction associated with CPS systems at each of the design phases described in the next section.

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

The Sensor-Observation-Sampling-Actuation Ontology (SOSA), 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 that provides a formal, general-purpose framework for modeling the interactions between various entities involved in the functions of *observation, sampling and actuation* in SSNs [6].

The *core structure* of SOSA Ontology design pattern encompasses all of the three modeling perspectives; the activities of observing, sampling, and actuating [6]. 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.

D. Cyber Threat Information Ontology

The SOSA Ontology outlined in the previous section helps capture the intricacies of the coupling between the cyber and physical elements in CPS systems. The activities of observing and sampling must be followed by communicating the data and processing 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 obtains and contextualizes Cyber Threat Information (CTI) from three sources:

- **The National Vulnerability Database (NVD) -** A U.S. government repository of standards based vulnerability management data [7].
- **Exploit Database -** An archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers [8].
- **Metasploit -** A framework for developing, testing and executing software exploits [9].

The cyber threat Ontology is underpinned by the STIX structured language, 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 faster and more effectively [10].

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 that are used by a reasoner to infer additional information that may be hard to define using 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 CTI Ontology also inherits characteristics from two additional Ontologies:

- **Cyber Observable Expression (CybOX)** - A standardized language for encoding and communicating information about cyber observables [10]. Using CybOX language, 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.[11].

III. Case Study: Red Light Violation Warning System (RLVW)

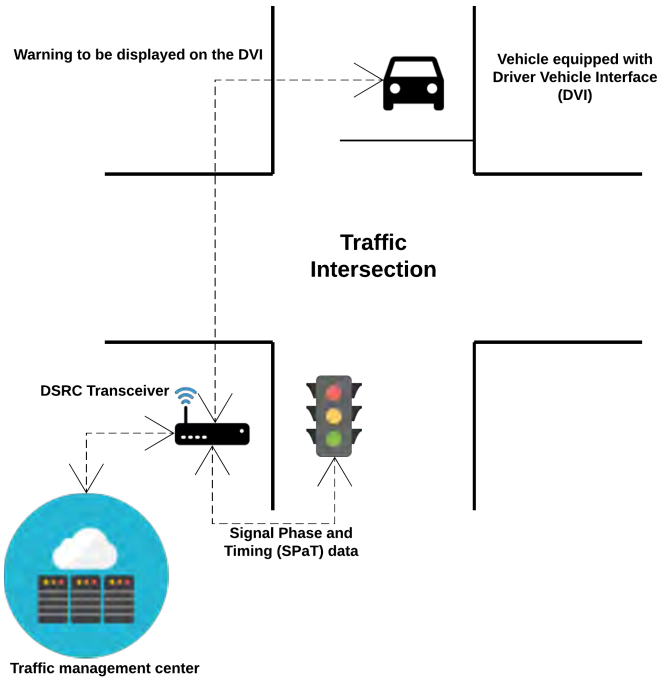

Figure 1. The RLVW system

As a case study to show the use of our framework, we use the Red Light Violation Warning (RLVW) safety application as described in the US Department of Transportation document [12]. The 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

 ISBN: 978-1-61208-752-8

occur, a warning can be provided to the driver. Figure 1 shows an overview of the RLVW system.

The SIMON framework describes three layers of threat identification by classifying design goals, subsystems that support those goals, and hardware/software that enable functionality of the subsystems. The number of nodes used in this model can demonstrate the complexity of CPS. The more nodes and edges established in this system, the more intermediate layers are formed between the CPS Model layers. In doing so, more vulnerabilities are introduced into the system due to larger access points throughout the CPS. To mitigate this, it is desirable to assign roles and responsibilities to components in the abstract and concrete realization phases based on functional and security requirements. Such an approach will provide requirements traceability, which will aid in increasing resiliency by reducing the attack surface.

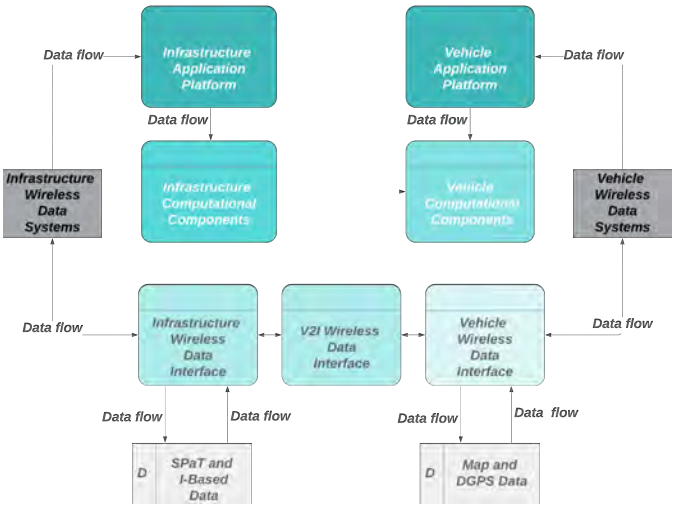

Figure 2. The V2I Wireless Data Systems Network

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 their respective WDI and Application Platforms (APs). The V2I WDI incorporates algorithms and data exchanged to perform calculations to recognize high-risk situations in advance. 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 [12]. The system is also responsible for maintaining authenticity of transmitted data through security measures. Corrupted data can result in compromising driver safety and their informations privacy. The three primary 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 transmitted 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 results in traffic violations or accidents.

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 quantitatively satisfy the aspirational properties of the V2I WDI System, it is important to categorize each component into 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 dedicated 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 Cyber Physical 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. So to understand these challenges, we form a general hierarchy of the V2I WDI network that maps each component to the requirement it fulfils [12]. This will unravel the group of threats associated at each layer of the system. Figure 2 shows an overview of the V2I wireless data interconnect.

1) 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 design goal 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.

 ISBN: 978-1-61208-752-8

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 the security, privacy, 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 design goal 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):** Receives messages from the Vehicle Application Component through the Vehicle Application Platform, 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 design goal 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 the bridge between the cyber and physical components of this side of the CPS, thus making it one of the least resilient and most vulnerable parts of the CPS.

  The VAP role is equivalent to the IAP role previously discussed. Since they are very similar in the conceptual goals they support, it stands to reason that the VAP role should support security, privacy, resiliency and reliability requirements.

2) 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, which would be 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. 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 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

 ISBN: 978-1-61208-752-8

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 [13].

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 is required to be supported by the OBU. However, multiple roles/responsibilities may be fulfilled by a single realization. For example, using 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 [14]. 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.

D. Assurance Phase

The assurance phase deals with obtaining confidence that the CPS system built in the concrete realization phase satisfies the models 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 3 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, SIMON's CTI Ontology discussed in sectionII-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 of privacy,

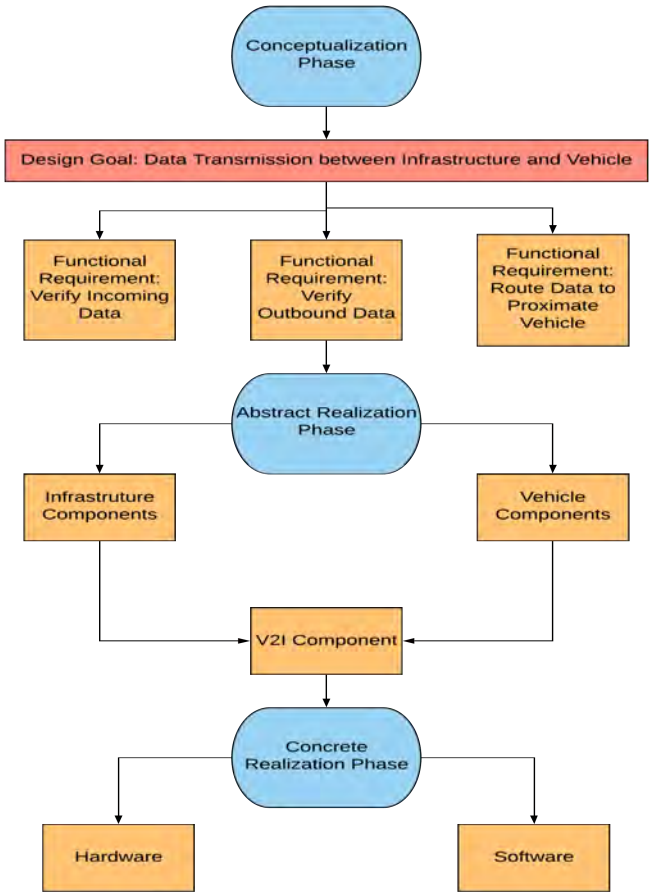

Figure 3. Role allocation hierarchy

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 [15], 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.

 ISBN: 978-1-61208-752-8

- 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.

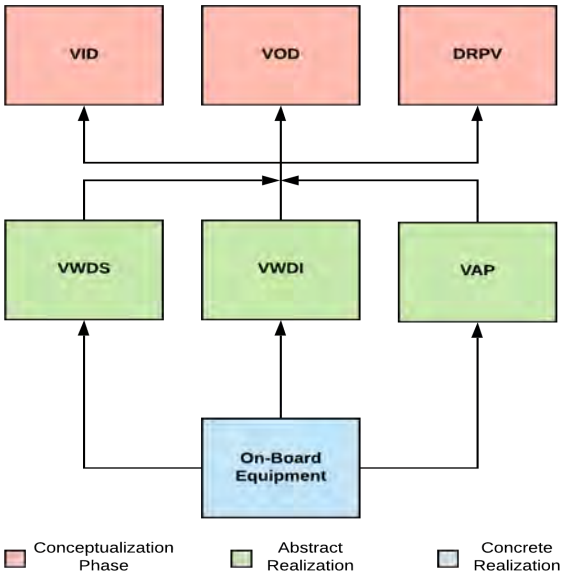

Figure 4. DoS attack on the OBU

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 4 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 [4]. These insights would be invaluable to CPS system designers.

```
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

IV. Conclusion and Future Work

In this paper, 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. However, we are 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.

Acknowledgement

This research is supported in part by the NSF Net-centric Industry-University Cooperative Research Center at UNT and the industrial members of the Center.

References

[1] A. A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, "Challenges for Securing Cyber Physical Systems," *Center for Hybrid and Embedded Software Systems*, pp. 1–3, 2009.

[2] F. AlDosari, "Security and Privacy Challenges in Cyber-Physical Systems," *Scientific Research Publishing*, pp. 4–6, 2017.

[3] B. Li and L. Zhang, "Security analysis of cyber-physical system," *AIP Conference Proceedings*, pp. 1–4, 2017.

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

[5] 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.

[6] 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.

[7] "National vulnerability database." URL: https://nvd.nist.gov/ [accessed: 2019-06-11].

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

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

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

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

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

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

[14] D. Snchez-lvarez, M. Linaje, and F.-J. Rodrguez-Prez, "A Framework to Design the Computational Load Distribution of Wireless Sensor Networks in Power Consumption Constrained Environments," *Sensors(Basel)*, pp. 2–5, 2018.

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

 ISBN: 978-1-61208-752-8