An Ontology-Driven Framework for Security and Resiliency in Cyber Physical Systems

Rohith Yanambaka Venkata, Patrick Kamongi and Krishna Kavi

University of North Texas
Denton, Texas-76203
Email: [ry0080, pk0158, krishna.kavi]@unt.edu

***Abstract*—Cyber-Physical Systems (CPS) can be described as an integration of computation and physical processes, where embedded systems monitor and control physical processes. Advances in technologies, such as networking and processors have enabled the adoption of CPS in safety-critical systems like smart grids and autonomous vehicles. Cyber-attacks, as the name suggests, target components in the cyber space with the intention of disrupting the functionality of the physical components. In this paper, we present an Ontology-driven framework that captures the relationship between cyber and physical systems to semantically reason about the impact of cyber-attacks on the physical systems. We demonstrate the idea using a reference Red-Light Violation Warning (RLVW) Vehicle to Infrastructure (V2I) network. Our proposed Ontology provides the ability to identify vulnerabilities in cyber systems that may impact a given physical system, enumerate potential mitigation steps and help design resilient physical systems that can meet their design specifications despite the occurrence of a cyber-attack.**

Keywords–Cyber Physical Systems; CPS; Security; Resiliency; Ontology.

I. Introduction

Cyber-Physical Systems (CPS) are systems that involve coordination between two components: cyber (or computational) and physical systems. Ashibani et al. [1] describe CPS as a combination of tightly integrated physical processes (such as actuation), networking and computation. The physical processes are monitored and controlled by cyber subsystems through network interconnects.

The proliferation of CPS has gained increased traction with the advances in networking and embedded system technologies like system-on-chip (SoC) and wireless transmitters. With the increased capability and complexity in CPS, they have found application in domains such as smart cities, transportation, and power grids. However, this growth has come at the cost of potential cyber-attacks [2]. Often, security and resiliency are either not paid the attention they deserve or are disregarded altogether. As a result, cyber-attacks on CPS are becoming increasingly prevalent, as evidenced by recent attacks targetting critical infrastructure:

- A cyber-attack in 2016 crippled a power grid in Ukraine, affecting at least 100,000 people. The attackers used software-based attacks to shut down the Remote Terminal Units (RTUs) that control circuit breakers, causing a power outage for about an hour [3].
- A German steel mill was the target of a cyber-physical attack in 2014, when malicious actors took control of the mill's production software and caused material damage to the mill [4].
- On 21 October 2016, an attack on DNS service provider Dyn caused issues for a list of well-known services such as Twitter, GitHub, Reddit, Spotify, Netflix, and PayPal. A Mirai botnet compromised tens of millions of IP addresses. All in all, about 100,000 devices were involved. This was the then largest attack ever recorded with network traffic volume reaching 1.2Tbps.
- Perhaps the most recognizable of all the attacks was the STUXNET worm that infected Iranian nuclear power plants [5]. The worm caused the centrifuges to spin too quickly and for too long, damaging or destroying the delicate equipment in the process. This is an excellent example of how cyber-attacks affect physical systems.

It is evident from these examples that an attack targetting the cyber domain (cyber-attacks) can adversely impact the normal operation of the physical systems that they control. The impact is especially acute in safety-critical systems.

One way to understand the impact of cyber-attacks on physical systems is by modeling CPS systems using Ontologies. 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 components such as individuals (instances of objects), classes, attributes, and relations as well as restrictions, rules, and axioms. Ontologies not only introduce a shareable and reusable knowledge representation but, can also add new knowledge about a domain [6]. Ontologies provide numerous advantages.

- Ontologies enable automated reasoning about data [6].
- They provide the ability to represent data formats, including unstructured, semi-structured or structured data, enabling smooth data integration, easy concept and text mining, and data-driven analytics [6].
- Adding additional relationships, integrating multiple Ontologies and cross domain concept matching are also possible.

CPS enable technological advances in diverse critical domains such as healthcare, traffic flow management, and smart manufacturing. Design needs vary across the domains of operation. So, Ontologies may be able to capture complex dependencies and relationships between the cyber and physical components

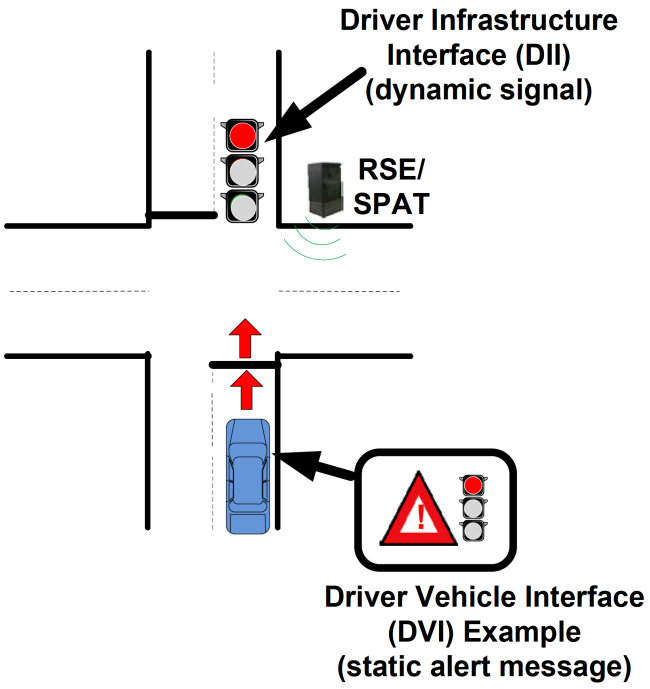

Figure 1. The Red Light Violation Warning system [8].

and potentially identify common design principles across multiple domains. Cyber-attacks may or may not affect the physical system of a CPS. To understand the impact of attacks on the functioning of physical components, the relationships captured by the Ontology can be used to semantically reason about security and resiliency of the physical components.

In this paper, we present our Ontology-driven framework that captures some of the physical and cyber components of a Vehicle-to-Infrastructure (V2I) reference architecture [7], including design goals and requirements specification from their design artifacts. This includes information such as functional, security and resiliency requirements. The objective is to understand the relationship between the cyber and physical components of the V2I CPS system to be able to reason about security and resiliency of the physical system. The Ontology will help understand the impact of cyber-attacks on the physical components. This information can then be used to identify mitigation techniques (in physical or cyber domains) and design changes that can help improve the security and resiliency of the physical system.

The paper is split into 6 sections. In section II, we briefly describe the reference architecture that is used to validate the Ontology. Section III outlines some of our previously-developed tools that perform vulnerability management. The CPS Ontology and the reasoning process are briefly described in section IV. A case study using the Red-Light Violation Warning (RLVW) and the CPS Ontology is presented in section V, followed by the conclusion in section VI.

II. Reference architecture - Red Light Violation Warning (RLVW)

The RLVW safety application involves providing a cooperative vehicle and infrastructure system that assists drivers in avoiding crashes at signalized intersections by first advising the driver of a signalized intersection, followed by a warning to the vehicle's driver if, based on their speeds and distance to the intersection, they may violate an upcoming red light. As a vehicle equipped with a Driver Vehicle Interface (DVI), a screen on the dash that displays alerts from the infrastructure as the vehicle approaches an intersection equipped with a Road Side Equipment (RSE)-controlled traffic light. It receives messages about the signal phase and timing (SPaT), intersection geometry, and position correction information [7]. SPaT, a traffic signal control information that conveys the current movement state of each active phase in the system can aid in safety, mobility and monitoring the environment [9]. The driver is alerted or warned if the RLVW application determines that given current operating conditions, the driver is predicted to violate the red light.

The RLVW system is one of six safety applications developed by the United States Department of Transportation [7]. The goal of the RLVW application is to improve roadway safety by reducing red-light running and collisions at signalized intersections [7]. The infrastructure and vehicle components include both cyber and physical components. Figure 1 shows various components of the RLVW application. We will evaluate our Ontology with this architecture as a baseline. This application contains:

1) Infrastructure component: The infrastructure component is responsible for warning drivers of an approaching intersection well in advance. In addition, drivers also need to be warned if their approach is likely to result in a red light violation.

2) Vehicle component: The vehicle component is responsible for sensing the world, conveying intent (to other vehicles and the infrastructure) and situational awareness. All of this information needs to be sent to the infrastructure.

- Sensing the world includes measuring speed, getting current Global Positioning System (GPS) coordinates and determining the lane currently being driven on.
- Conveying intent is vital in a connected vehicle environment (especially Vehicle to Vehicle network). The information exchanged may influence the behavior of other entities in the network.
- Situational awareness involves attributing context to the data collected by a physical component. For example, if a sensor measures the speed of the vehicle to be 60 miles per hour, the relevant cyber component needs to determine if this is a safe speed given the current context. This speed may be acceptable on a highway but, not within city limits.

3) Design goals: In this section, we look at some of the design goals and specifications of the RLVW application before we present a preliminary outline of our Ontology design in the subsequent sections.

Figure 2 outlines some of the important design goals of the communication model being considered. The three primary objectives of V2I is to prevent/minimize fatalities, injuries and property damage. One of the ways this can be achieved is by using the RLVW application, which attempts to satisfy the design goals by reducing red light running and traffic collisions. The various design specifications and their relationships are reflected in Figure 2.

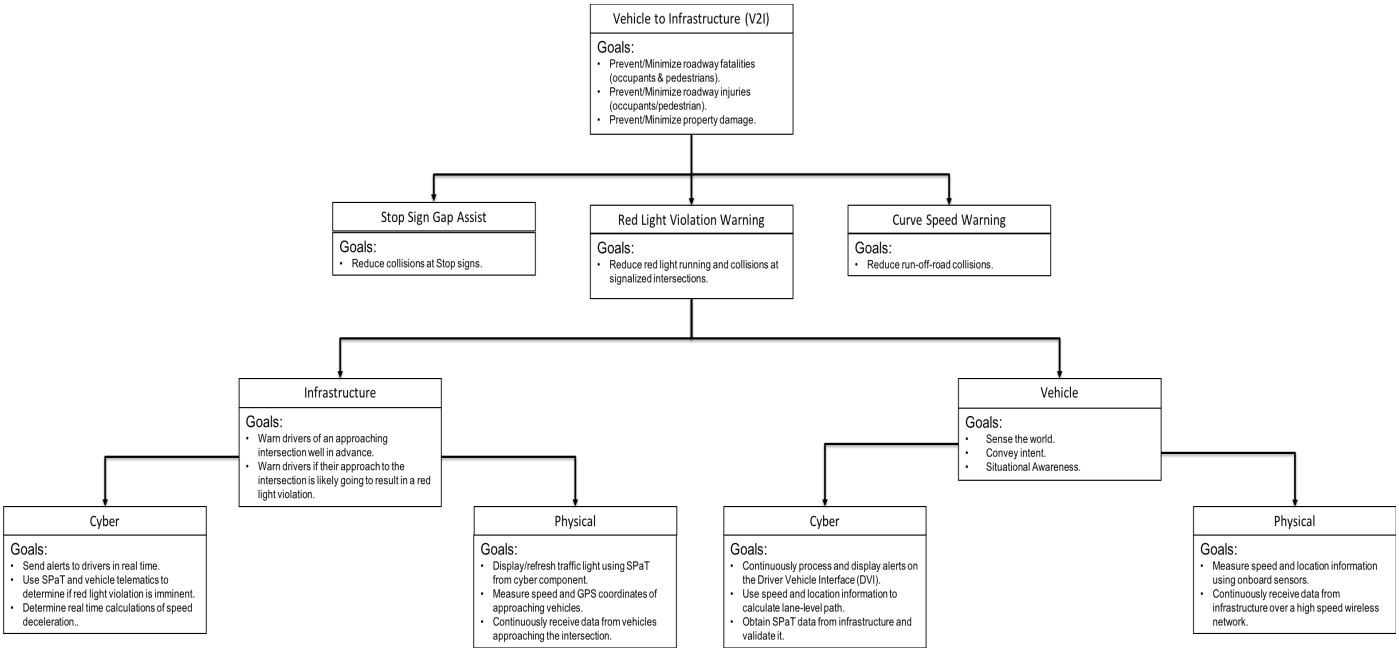

Figure 2. Design goals for RLVW.

The National Institute of Standards and Technology (NIST) has published a framework that provides guidance in designing, building, verifying, and analyzing complex CPS systems [10]. The CPS Framework captures the generic functionalities that CPS provide, and the activities and artifacts needed to support conceptualization, realization, and assurance of CPS [10]. The framework describes the following series of steps within a reference architecture.

- The domain of the CPS needs to be identified.
- Facets or views on CPS encompassing identified responsibilities in the system engineering process [10] need to be identified. These include conceptualization, realization, and assurance. They contain well-defined activities and artifacts (outputs) for addressing design goals (or concerns) [10].
- Aspects need to be consolidated. Aspects are high-level groupings of cross-cutting concerns. Concerns are interests in a system relevant to one or more stakeholders. These may include Functional, Business, Timing, Data, Trustworthiness, etc [10].

Our objective is to reason about security and resiliency so, we focus only on the trustworthy concerns. Trustworthiness is the demonstrable likelihood that the system performs according to designed behavior under any set of conditions as evidenced by characteristics including, but not limited to, safety, security, privacy, reliability and resilience [10]. In the next section, we briefly describe vulnerability assessment for cyber systems using some of our previous work.

III. Vulnerability-based Threats Assessment

Given a deployed Cyber-Physical System that leverages one or more IT (or cyber) components for normal operations, security evaluation of the IT system is a priority.

In our previous work, we have designed solutions (VULCAN [11], and NEMESIS [12]) to automate essential security management tasks to assist in identifying, assessing and mitigating the threats that may affect any given IT system (this apply to the Cyber components that power a Cyber-Physical System).

Let us consider an example of an IT component (that is part of a Cyber-Physical System) such as the "Qualcomm SD 820 Firmware". Our VULCAN Framework [11], enable us to model and represent such an IT component using a Common Platform Enumeration (CPE) standard [13].

An Ontology Knowledge Base (OKB), which is a populated Ontology, plays a central role within the VULCAN framework by capturing various critical public data feeds of IT products (e.g., Application/Software, Operating System, and Hardware) vulnerability, attack, and mitigation information using an evolving and semantically rich Ontology model.

The vulnerability index generated by VULCAN captures information about publicly known vulnerabilities (including their insightful information) that affect our assessed IT component. Figure 3 shows a simplified view of the generated vulnerability index to highlight a few vulnerabilities (including their vulnerability description, severity score and Common Weakness Enumeration (CWE) [14] identifier) that affects our assessed IT product (viz., Qualcomm SD 820 Firmware). This System-on-Chip (SoC) is commonly used in level 3 and level 4 autonomous vehicles.

With the amount of semantically rich information captured within the generated vulnerability index of the assessed IT component, we can reason and infer various insights in regards to the current vulnerability status of the "Qualcomm SD 820 Firmware" and how many of its vulnerabilities have a damaging impact (if exploited by a malicious actor) to the core of the Cyber-Physical System in operation.

Using this vulnerability index, our NEMESIS architecture can assist in performing various threat modeling, and risk assessment tasks of the for the IT product. This information

may be useful towards designing and CPS that are inherently resilient to the modeled threats.

Table I illustrates a sample view of how NEMESIS classifies vulnerabilities (that affect the assessed IT component "Qualcomm SD 820 Firmware") into possible threat types (using STRIDE threat model [15]) that could arise from their exploitation. For instance, "CVE-2018-3594" [16] vulnerability was identified by VULCAN that it affects our assessed IT component, then NEMESIS determines that this vulnerability could lead to "Tampering, Information Disclosure, Repudiation, and Elevation of Privilege" STRIDE threat types (as shown in Table I).

TABLE I. QUALCOMM SD 820 FIRMWARE: THREAT CLASSIFICATION SAMPLE

Vulnerability	S	T	R	I	D	E
CVE-2018-3594	0	1	1	1	0	1
CVE-2017-18140	0	0	1	0	0	0
CVE-2016-10414	0	1	0	0	0	0
CVE-2016-10446	0	1	0	1	0	1
CVE-2016-10434	1	1	1	0	1	1

In Table II we illustrate how NEMESIS ranks all the classified threat types by the average severity of all the found vulnerabilities that can lead to each of the STRIDE threat types. For instance, "Information Disclosure" threat type is the most severe threat that the assessed IT component "Qualcomm SD 820 Firmware" is exposed to.

TABLE II. QUALCOMM SD 820 FIRMWARE: THREAT TYPES RANKING

Threat Type	Severity [0-10]
Tampering	8.19
Denial of Service	5.0
Spoofing	7.5
Information Disclosure	9.0
Repudiation	8.57
Elevation of Privilege	8.78

Security practitioners can use the information for assessing IT products (or cyber component of CPS) to strategize cyber mitigations and resiliency measures to counter any of the perceived threat types that could impact the critical missions of the operational Cyber-Physical System.

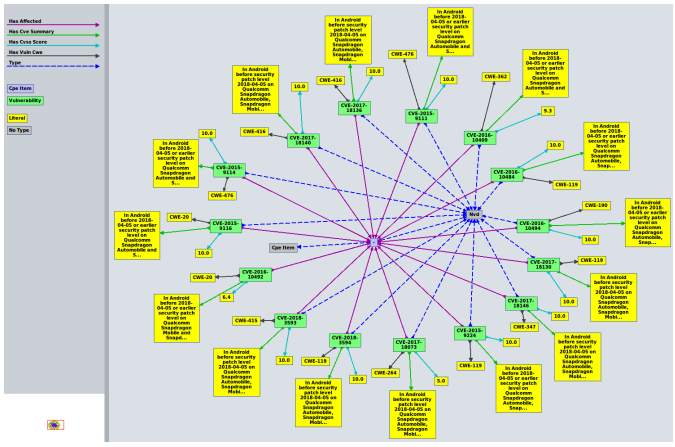

Figure 3. Qualcomm SD 820 Firmware – Vulnerability Index Sample

IV. CPS Ontology Design and Reasoning Process

Cyber systems usually include processors, memory modules, network interfaces and software products. We briefly discussed vulnerability assessment and management for cyber systems by introducing some of our previous work in Section III. also previously demonstrated the ability to enforce differentiated levels of security for Internet of Things (IoT) devices [17]. Now, our goal is to understand how these cyber (or IT) vulnerabilities affect physical systems. The challenge is to capture the relationship between cyber and physical components to semantically reason about security and resiliency. The Ontology will be able to provide an insight into potential mitigation techniques, which may involve changes in the design or patching and updating software packages in the cyber domain.

- Design goals and components of a CPS domain need to be identified in consultation with domain experts.
- The relationships between various components in the domain need to be identified within the context of the design goals identified in the previous step.
- Given all components and their relationships, threat modeling needs to be performed so that only threats relevant to the given CPS are considered.
- The CPS needs to be redesigned if required.
- The redesigned system needs to be validated to ensure it still complies with the design specifications.

We have constructed an Ontology for the trustworthiness concern based on NIST's CPS framework. Figure 4 depicts a preliminary design for the CPS Ontology that is capable of reasoning against a limited set of vulnerabilities that we will discuss in Section V. The Ontology was implemented using OWL web semantic language [18] on Protege Ontology editor [19].

The design specifications from Figure 2 were translated into an Ontology. The RLVW concept contains five different knowledge points: physical components and cyber components which are self-explanatory, Abstract, Vehicle and Infrastructure. The infrastructure and vehicle components are mapped to the cyber and physical concepts. A knowledge point called Abstract captures all the design goals of a CPS domain (The RLVW safety application in this scenario). The two components of interest in this Ontology are the traffic light and RSE. The traffic light interacts with the RSE to display traffic lights and transition between them.

Design goals may be security requirements (from Security Service Level Agreements or SSLAs), Resiliency goals and Functional requirements. Lee et al., [20] describe an Ontology to capture SSLAs, which can be used to understand security agreements of a service provider or to audit compliance to design specifications [20].

V. Case Study

Let us evaluate this Ontology using a few simple examples. We use the STRIDE threat modeling discussed in Section III and the design specifications from Section 2. The configuration of system components is as follows:

- Qualcomm 820a SoC powers a vehicle.
- The DVI is controlled by Android Auto operating system [21].

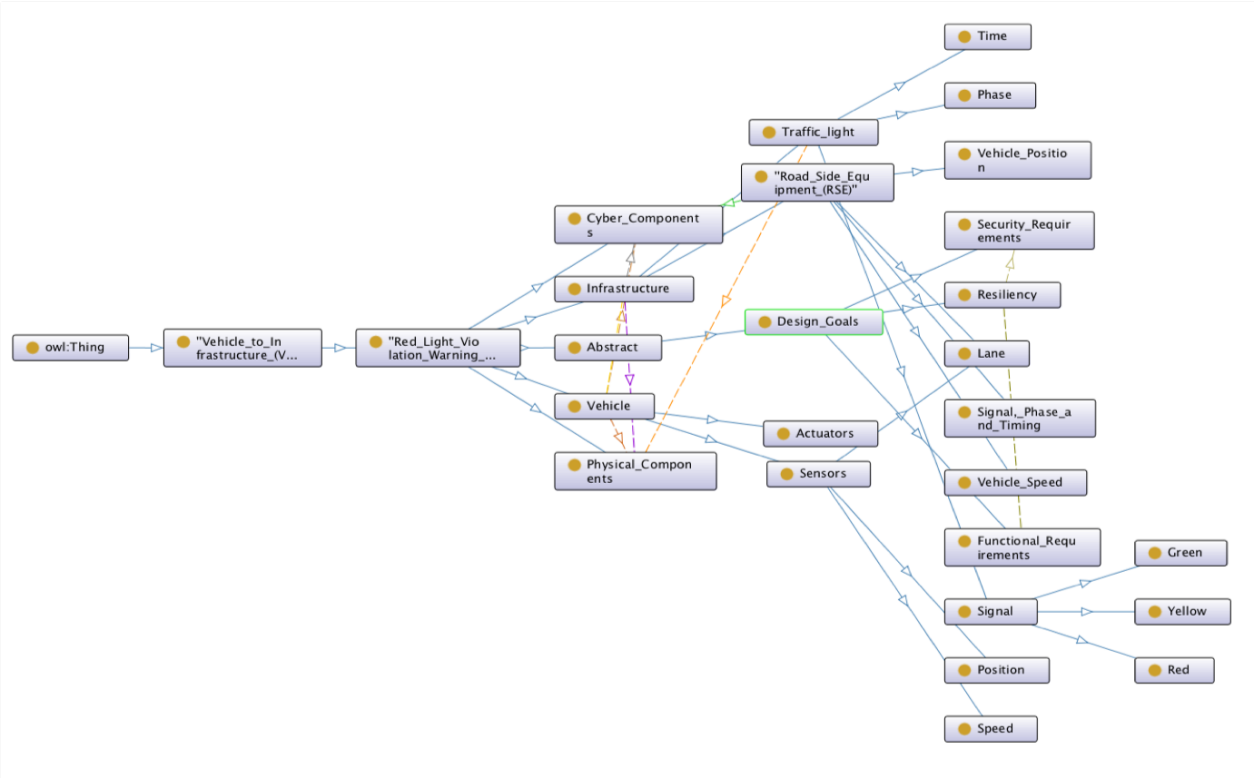

Figure 4. An example of the CPS ontology.

- RSE is a facility server running Ubuntu 16.04 LTS.
- No identification scheme exists to authenticate entities in the network.
- The data exchanged is not validated (neither by RSE nor the vehicle).
- The traffic light is not designed with any fail-safe modes.
- No personally-identifiable information is collected/stored.

A. An attack on the RSE

Let us consider the RLVW application discussed before. We were able to determine using the CPE identifier for Snapdragon 820a that five significant vulnerabilities could affect the SoC as discussed in section III. One of the most important steps in threat modelling for CPS is to assign a context to a threat/vulnerability i.e, try to understand how a vulnerability affects a physical system. In the first example, let us consider a scenario where an adversary attacks the RSE (as depicted in Figure 5). RSE is no longer trustworthy. Potential attacks are:

- **Spoofing :** The adversary may masquerade as the RSE, sending false data to vehicles or the traffic light. The lights may flash randomly or be turned off. The vehicle may not receive a warning from the RSE even if a potential red light violation is detected. For example, CVE-2018-1111 [22] may be used to create malicious DHCP packets to compromise the server.
- **Tampering :** Data is maliciously modified before being sent to vehicles or the traffic light. The potential impact is similar to that of the Spoofing attack. For example, an adversary may use CVE-2017-1000366 [23] to create a specially crafted environment variable to perform a buffer overflow attack.
- **Repudiation :** Non-repudiation is a state of affairs where a source of specific information denies ever creating/issuing it. In this case, the RSE can deny ever having issued an alert to a vehicle or the traffic light. In this case, the Ontology will help us understand that this attack is not relevant to us because it is easy to validate the RSE by using data from the vehicle. This may not be as critical as spoofing or tampering in our system.
- **Information Disclosure :** Since no personally identifiable information is collected, this attack does not substantially impact the physical system. However, if the RSE captures images of the vehicle that violated the red-light, information disclosure may violate privacy goals. If information about the cyber domain is leaked, VULCAN can help mitigate it.
- **Denial of Service :** The adversary may use any of the CVEs previously discussed to render the RSE unresponsive. This means that the vehicles may not receive alerts and the traffic lights are not controlled. The impact may be similar to that of the Spoofing attack.
- **Elevation of Prvilege :** Elevation of privilege or privilege escalation attacks involve gaining escalated access to a resource that is normally protected from a user. This is a cyber-attack so, VULCAN or NEMESIS

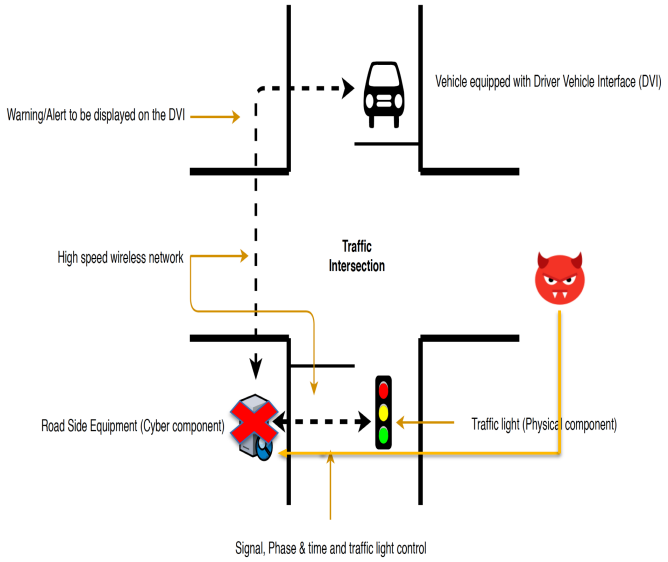

Figure 5. An attack on the RSE.

may be able to suggest mitigation techniques.

B. Mitigation techniques

The Ontology will be able to reason about potential mitigation techniques for a given cyber-vulnerability logically. This also includes changes to the design specification. Let us look at some of them:

- For most of the cyber-attacks like elevation of privilege, updating software packages, applying patches should suffice.
- Cyber system can be designed to protect against spoofing attacks by authenticating network entities using a digital certificate-based identification scheme.
- Physical systems can be designed to protect against spoofing attacks by using a physical unclonable function (PUF) based identification scheme.
- The traffic light can be built to flash yellow lights if no response is received from the RSE for a preset amount of time.
- SPaT data can be transmitted by the RSE so that the vehicles can validate the alerts that were sent.
- Similarly, speed and location information can be sent by the vehicles approaching the intersection. The RSE can validate the data collected by the sensors on the vehicle with the data collected by the RSE. Cross-validation may prove to be a useful design feature.

The Ontology can suggest mitigation techniques. Cost Vs Risk estimates may be used to pick the appropriate mitigation scheme. The insight provided by the Ontology can be used to design resilient physical systems.

C. An attack on the cyber component of a vehicle

We briefly discussed how specific threats that target the cyber component of the RSE might impact the CPS. Similarly, the cyber component of a vehicle (such as the Qualcomm 820a SoC) may be targetted by spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege attacks, which may violate the trustworthy concern of the V2I system. However, due to the limitation in space, we are unable to elaborate on this further.

VI. Conclusion

In this paper, we have presented an argument for modeling CPS using Ontologies. As systems grow more complex, understanding the relationship between various components becomes harder but, more critical.

We have introduced an Ontology-driven framework that is capable of capturing the relationship between cyber and physical domains. We use the example of a V2I communication model to demonstrate the capability of the Ontology. This Ontology, designed in consultation with domain experts helps identify potential vulnerabilities in the cyber domain that may impact a physical system. Also, it helps in identifying possible mitigation steps (in the cyber or physical domain) that can be used to protect against the threats modeled and also help design resilient physical systems that may provide reduced functionality to meet design specifications (resilient) despite the occurrence of a cyber-attack.

In the future, we intend to develop a more detailed Ontology framework that captures complex relationships between various components. This will also include tools that will be able to translate design specifications from the NIST framework into our Ontology to reason about the trustworthiness of a CPS design.

References

[1] Y. Ashibani and Q. H. Mahmoud, "Cyber physical systems security: Analysis, challenges and solutions," Computers and Security, vol. 68, 2017, pp. 81 – 97. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404817300809

[2] Z. DeSmit, A. E. Elhabashy, L. J. Wells, and J. A. Camelio, "An approach to cyber-physical vulnerability assessment for intelligent manufacturing systems," Journal of Manufacturing Systems, vol. 43, 2017, pp. 339 – 351, high Performance Computing and Data Analytics for Cyber Manufacturing. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S027861251730033X

[3] "Why the Ukraine power grid attacks should raise alarm," Mar. 2017, URL:https://www.csoonline.com/article/3177209/security/why-the-ukraine-power-grid-attacks-should-raise-alarm.html/ [accessed: 2018-06-16].

[4] K. Zetter, "A cyber-attack has caused confirmed physical damage for the second time ever," URL:https://www.wired.com/2015/01/german-steel-mill-hack-destruction/ [accessed: 2018-06-13].

[5] K. Zetter, "An unprecedented look at STUXNET, the world's first digital weapon," URL:https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ [accessed: 2018-06-16].

[6] "What are Ontologies?" URL:https://ontotext.com/knowledgehub/fundamentals/what-are-ontologies/ [accessed: 2018-06-13].

[7] B. Christie, "Vehicle-to-infrastructure (V2I) safety applications performance requirements, vol. 3, red light violation warning (RLVW)," United States. Dept. of Transportation. ITS Joint Program Office; United States. Federal Highway Administration, techreport, 2015.

[8] B. Christie, "Vehicle-to-Infrastructure (V2I) Safety Applications: Performance Requirements, Vol. 1, Introduction and Common Requirements," United States. Dept. of Transportation. ITS Joint Program Office; United States. Federal Highway Administration, Tech. Rep., 2015.

[9] United States Dept. of Transportation, URL:https://www.its.dot.gov/presentations/pdf/SPaT.pdf [accessed: 2018-06-10].

[10] Cyber-Physical Systems Public Working Group, "Framework for Cyber-Physical SystemsRelease 1.0," National Institute of Standards and Technology, Tech. Rep., 2016.

[11] P. Kamongi, S. Kotikela, K. Kavi, M. Gomathisankaran, and A. Singhal, "Vulcan: Vulnerability assessment framework for cloud computing," in Proceedings of The Seventh International Conference on Software Security and Reliability. SERE (SSIRI) 2013. IEEE, June 2013, pp. 218–226.

[12] P. Kamongi, M. Gomathisankaran, and K. Kavi, "Nemesis: Automated architecture for threat modeling and risk assessment for cloud computing," in The Sixth ASE International Conference on Privacy, Security, Risk and Trust (PASSAT). ASE, December 2014.

[13] National Institute of Standards and Technology, "Common platform enumeration (cpe)," https://nvd.nist.gov/cpe.cfm, June 2018.

[14] MITRE, "Common weakness enumeration (cwe)," http://cwe.mitre.org, June 2018.

[15] "The STRIDE Threat Model," http://msdn.microsoft.com/en-US/library/ee823878(v=cs.20).aspx, June 2018.

[16] National Institute of Standards and Technology, https://nvd.nist.gov/vuln/detail/CVE-2018-3594, June 2018.

[17] R. Y. Venkata and K. Kavi, "CLIPS: Customized Levels of IoT Privacy and Security," in Proceedings of the 12^{th} The Twelfth International Conference on Software Engineering Advances Oct 12–14, 2017, Athens, Greece, pp. 41–47.

[18] "OWL web semantic language," URL:https://www.w3.org/OWL/ [accessed: 2018-06-10].

[19] M. A. Musen and the Protégé team, "The protégé project: A look back and a look forward," AI Matters, vol. 1, no. 4, Jun 2015, pp. 4–12, 27239556[pmid]. [Online]. Available: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4883684/

[20] C.-Y. Lee, K. Kavi, R. Paul, and M. Gomathisankaran, "Ontology of secure service level agreement," 2015 IEEE 16th International Symposium on High Assurance Systems Engineering, 2015, pp. 166–172.

[21] Google, "The Android Auto Operating System," URL:https://www.android.com/auto/ [accessed: 2018-06-08].

[22] National Institute of Standards and Technology, "CVE-2018-1111," URL:https://nvd.nist.gov/vuln/detail/CVE-2018-1111 [accessed: 2018-05-18].

[23] National Institute of Standards and Technology, "CVE-2017-1000366," URL:https://nvd.nist.gov/vuln/detail/CVE-2017-1000366 [accessed: 2018-05-18].