Requirements Traceability in Cyber Physical Systems using Semantic Inference

Rohith Yanambaka Venakata, Rohan Maheshwari, Dr. Krishna Kavi

Cyber Physical Systems

- The integration of existing communication and information technologies with physical systems
- CPS systems are increasingly benefitting from IoT and 5G expansion
- Their role in Industrial Control Systems puts upon a heavy load of data transmission between their cyber and physical components.

Problem

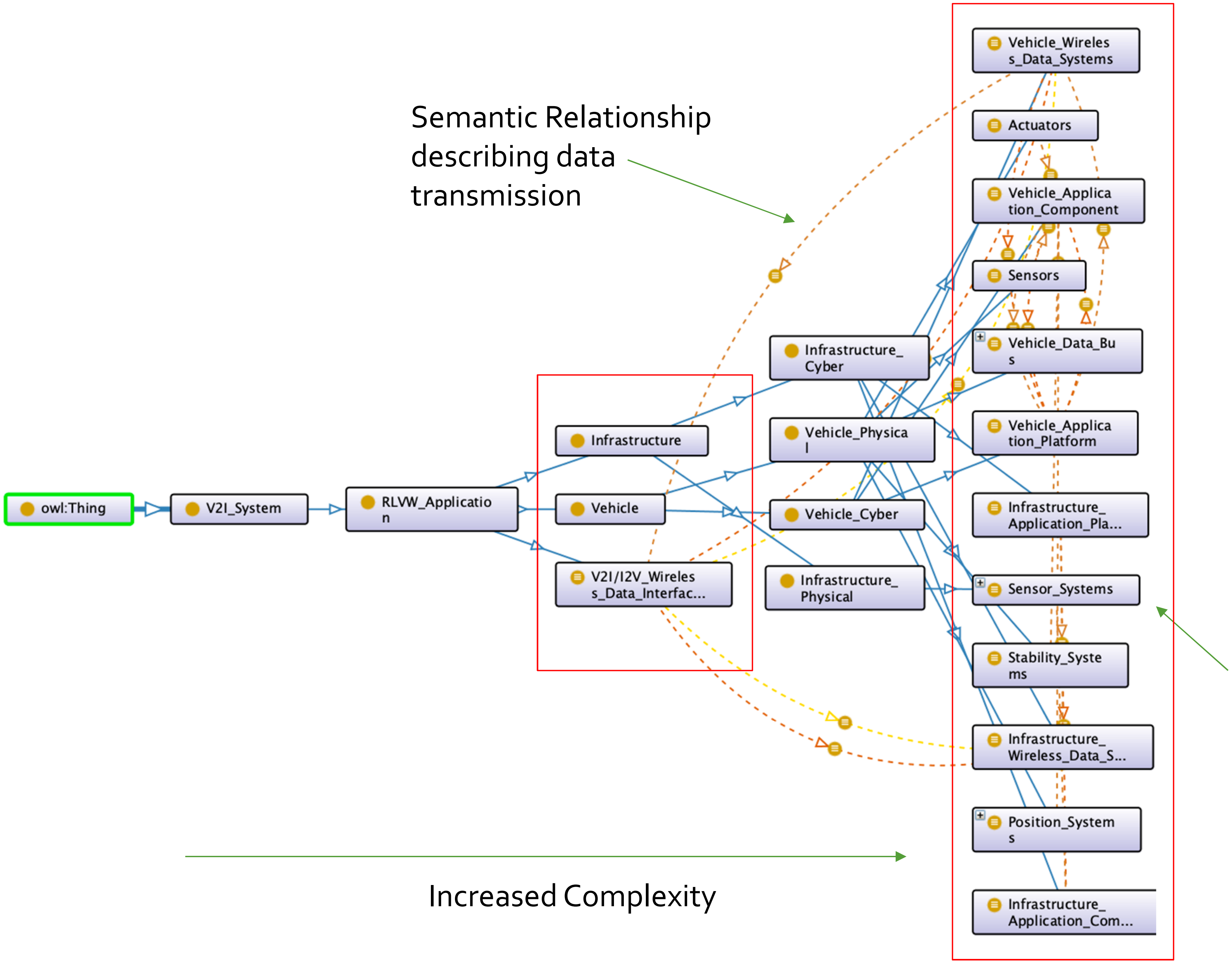
- CPS systems are increasingly benefiting from the expanding IoT network as they are implemented in the infrastructure.
- Rapid integration of CPS systems as a single unit has brought upon changes in architecture that implies vulnerabilities.
- Cyber attacks are more severe when the gained privileges cover access to a larger system.
- As new components are added to a CPS domain, the region of attack becomes unclear and difficult to mitigate.

Motivation

- Vulnerabilities in CPS systems increase the amount of possible access nodes in both the cyber and physical sub domains.
- The increased attack surface calls for threats to be identified in two categories: Infrastructure Security and Information Security.
- It is important to develop a new framework that can account for:
  - Increased connection points
  - New data transmission phases
  - CPS components

Ontologies

- Ontologies provide a reliable technique to visualize 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
  - Role allocation
- Ontologies provide a systematic methodology to understand the internal communication systems
  - Leads to identification, classification, and scoring of threats


owl:Thing
V2I_System
RLVW_Application
Infrastructure
Vehicle
V2I/I2V_Wireless_Data_Interfac...
Infrastructure_Cyber
Vehicle_Physical
Vehicle_Cyber
Infrastructure_Physical
Vehicle_Wireless_Data_Systems
Actuators
Vehicle_Application_Component
Sensors
Vehicle_Data_Bus
Vehicle_Application_Platform
Infrastructure_Application_Pla...
Sensor_Systems
Stability_Systems
Infrastructure_Wireless_Data_S...
Position_Systems
Infrastructure_Application_Com...

Semantic Relationship describing data transmission

Increased Complexity

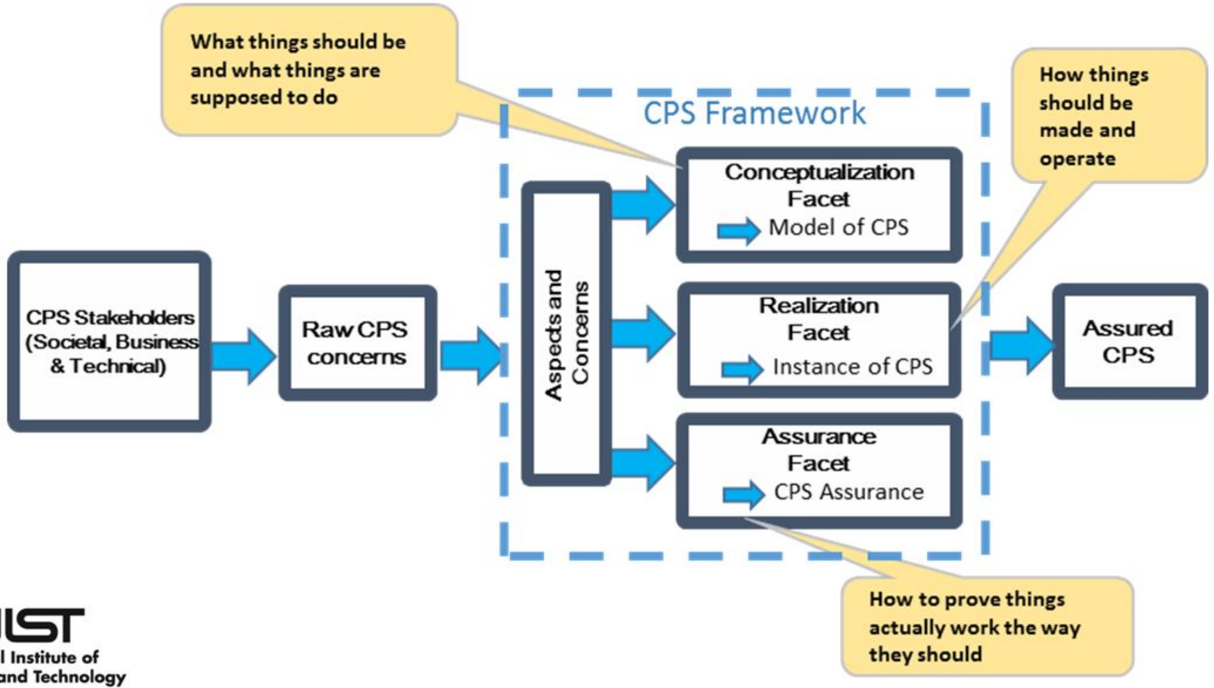
Hardware Component sending sensor data to IWDS

Proposal

- We propose a Role Application framework in which we dissect security threats and vulnerabilities relative to the layer they are violating.
- We use different Ontologies in our framework to semantically reason about concepts, properties and restrictions associated with CPS components at each phase.

NIST Framework

- National Institute of Standards and Technology (NIST) has developed a framework that provides guidance in designing, building, verifying, and analyzing complex CPS systems.
- Conceptualization Phase
- Realization Phase
  - Abstract Realization
  - Concrete Realization
- Assurance Phase


What things should be and what things are supposed to do
CPS Framework
How things should be made and operate
CPS Stakeholders (Societal, Business & Technical)
Raw CPS concerns
Aspects and Concerns
Conceptualization Facet
Model of CPS
Realization Facet
Instance of CPS
Assurance Facet
CPS Assurance
Assured CPS
How to prove things actually work the way they should

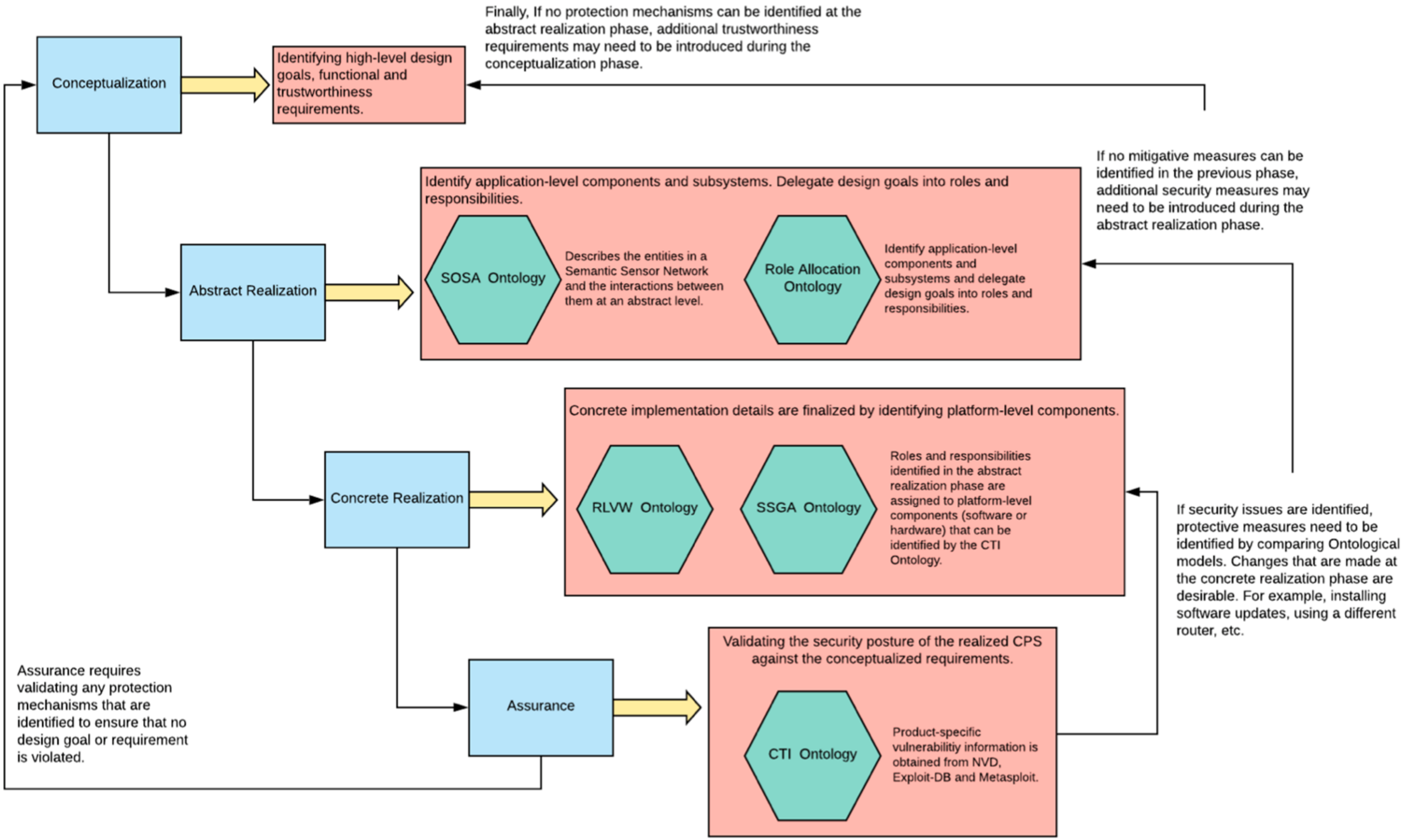
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

SOSA Ontology

- The Sensor-Observation-Sampling-Actuation Ontology (SOSA), conceptualizes all entities, activities and properties that typically constitute a CPS
- A general-purpose framework for modeling the interactions between various entities involved in the functions of observation, sampling and actuation in Semantic Sensor Networks (SSNs)
- This is a W3C Standard specification
- Accomplishes the Abstract Phase of the NIST Framework

Cyber Threat Information Ontology

- The communication and processing in CPS subsystems are not directly included in the SOSA ontology
- This exposes the cyber and physical components of the CPS to security attacks.
- CTI extracts the Common Platform Enumeration data (CPE) from the conceptualized components from SOSA
- Requests the National Vulnerability Database (NVD) for Common Vulnerability Enumeration data (CVE) that contains:
  - Attack vectors
  - Access nodes
  - Severity metrics
- Accomplishes Assurance Phase



Identifying high-level design goals, functional and trustworthiness requirements.

Finally, If no protection mechanisms can be identified at the abstract realization phase, additional trustworthiness requirements may need to be introduced during the conceptualization phase.

Identify application-level components and subsystems. Delegate design goals into roles and responsibilities.

Describes the entities in a Semantic Sensor Network and the interactions between them at an abstract level.

Identify application-level components and subsystems and delegate design goals into roles and responsibilities.

If no mitigative measures can be identified in the previous phase, additional security measures may need to be introduced during the abstract realization phase.

Concrete implementation details are finalized by identifying platform-level components.

Roles and responsibilities identified in the abstract realization phase are assigned to platform-level components (software or hardware) that can be identified by the CTI Ontology.

If security issues are identified, protective measures need to be identified by comparing Ontological models. Changes that are made at the concrete realization phase are desirable. For example, installing software updates, using a different router, etc.

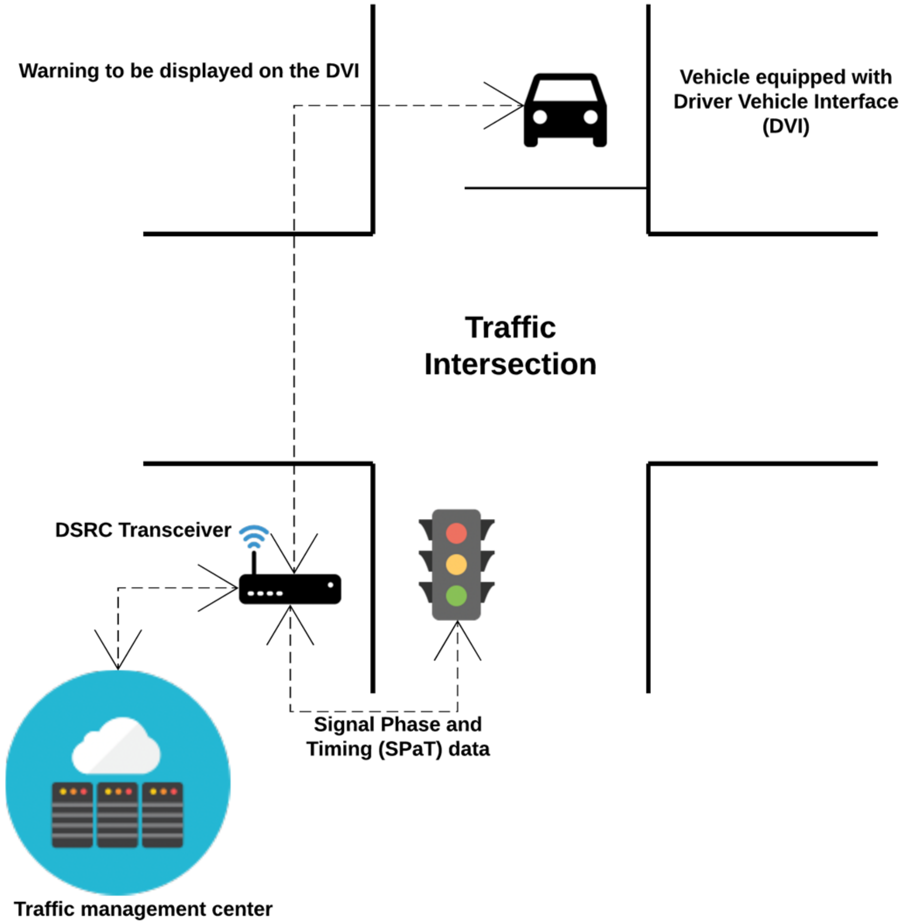
Validating the security posture of the realized CPS against the conceptualized requirements.

Product-specific vulnerabilitiy information is obtained from NVD, Exploit-DB and Metasploit.

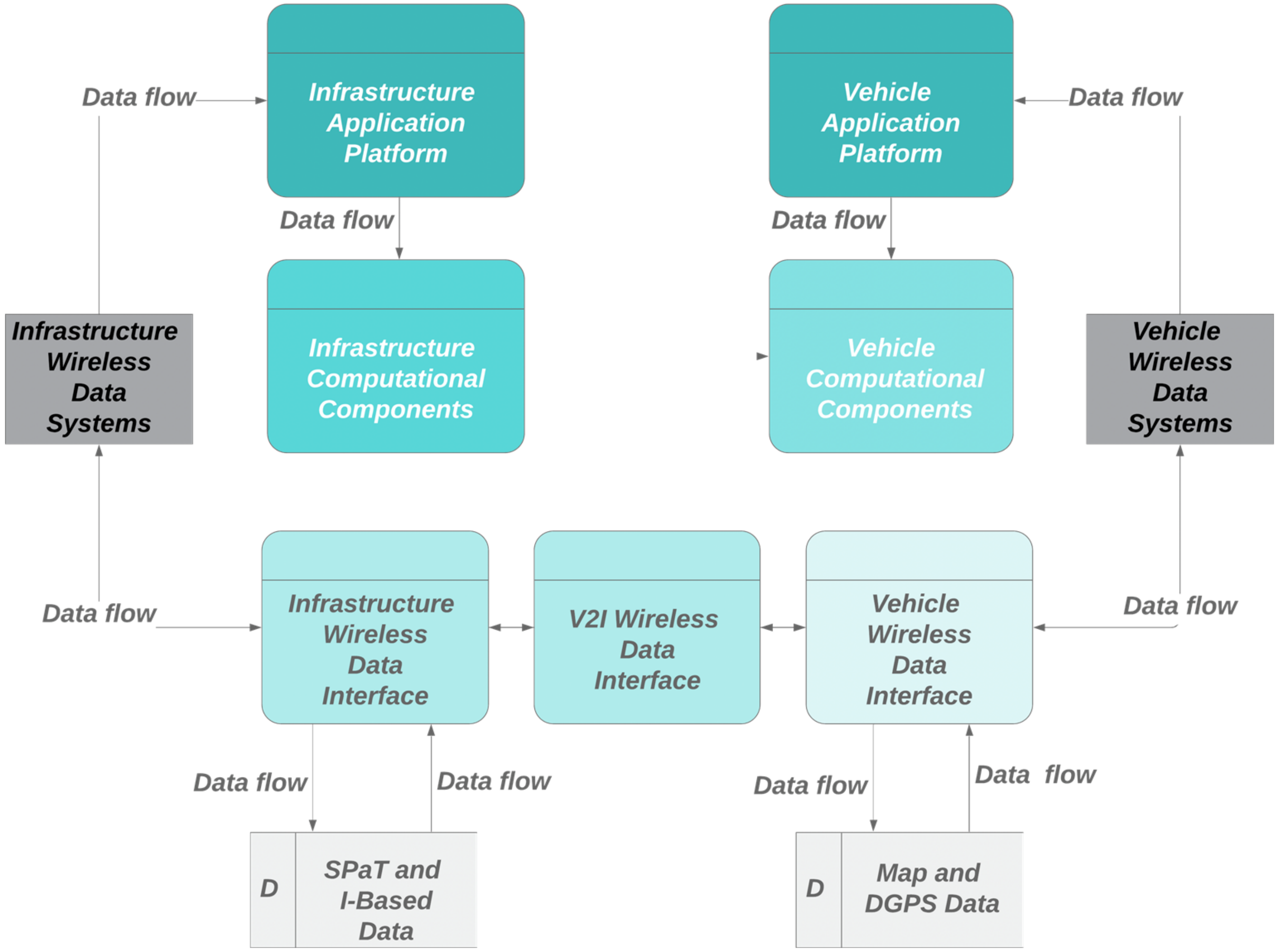
Assurance requires validating any protection mechanisms that are identified to ensure that no design goal or requirement is violated.

Case Study: Red Light Violation Warning (RLVW)

- The RLVW application enables a connected vehicle approaching an instrumented signalized intersection to receive information from the infrastructure.
- The application in the vehicle uses:
  - Speed and acceleration profile
  - Signal timing and geometry information
- This information dictates the likelihood that the vehicle will enter the intersection in violation of a traffic signal.

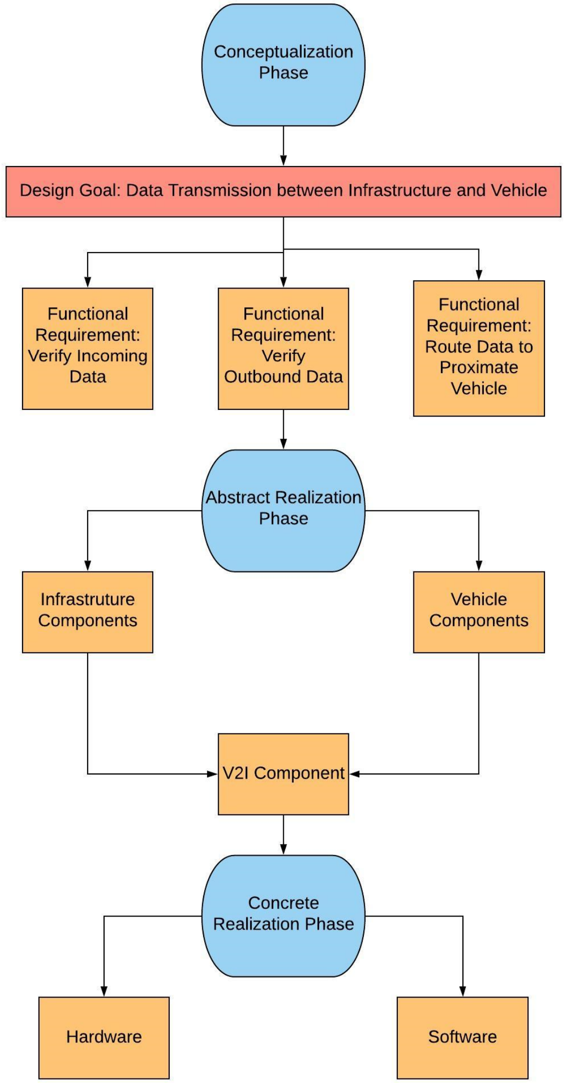

Warning to be displayed on the DVI
Vehicle equipped with Driver Vehicle Interface (DVI)
Traffic Intersection
DSRC Transceiver
Signal Phase and Timing (SPaT) data
Traffic management center

V2I Wireless Data Systems Network


Infrastructure Application Platform
Vehicle Application Platform
Data flow
Data flow
Data flow
Data flow
Infrastructure Wireless Data Systems
Infrastructure Computational Components
Vehicle Computational Components
Vehicle Wireless Data Systems
Data flow
Infrastructure Wireless Data Interface
V2I Wireless Data Interface
Vehicle Wireless Data Interface
Data flow
Data flow
Data flow
Data flow
Data flow
D
SPaT and I-Based Data
D
Map and DGPS Data

Approach

- The SIMON framework describes three layers of threat identification:
  - Classifying design goals
  - Subsystems
  - Hardware/software
- The number of nodes used in this model can demonstrate the complexity of CPS.
- The complexity of the CPS indicates new intermediate layers forming between the CPS Model layers.
- It is desirable to assign roles and responsibilities to components in the abstract and concrete realization phases based on functional and security requirements.
- This approach will provide requirements traceability, which will aid in increasing resiliency by reducing the attack surface.


Conceptualization Phase
Design Goal: Data Transmission between Infrastructure and Vehicle
Functional Requirement: Verify Incoming Data
Functional Requirement: Verify Outbound Data
Functional Requirement: Route Data to Proximate Vehicle
Abstract Realization Phase
Infrastruture Components
Vehicle Components
V2I Component
Concrete Realization Phase
Hardware
Software

Conceptualization

- Design Goal: Communicate relevant data between the Infrastructure and Vehicle application components.
- The system is responsible for maintaining authenticity of transmitted data through security measures.
- The three sub design goals of the V2I system are:
  - Verify Incoming Data (VID)
  - Verify Outbound Data (VOD)
  - Data Routing to Proximate Vehicles (DRPV)

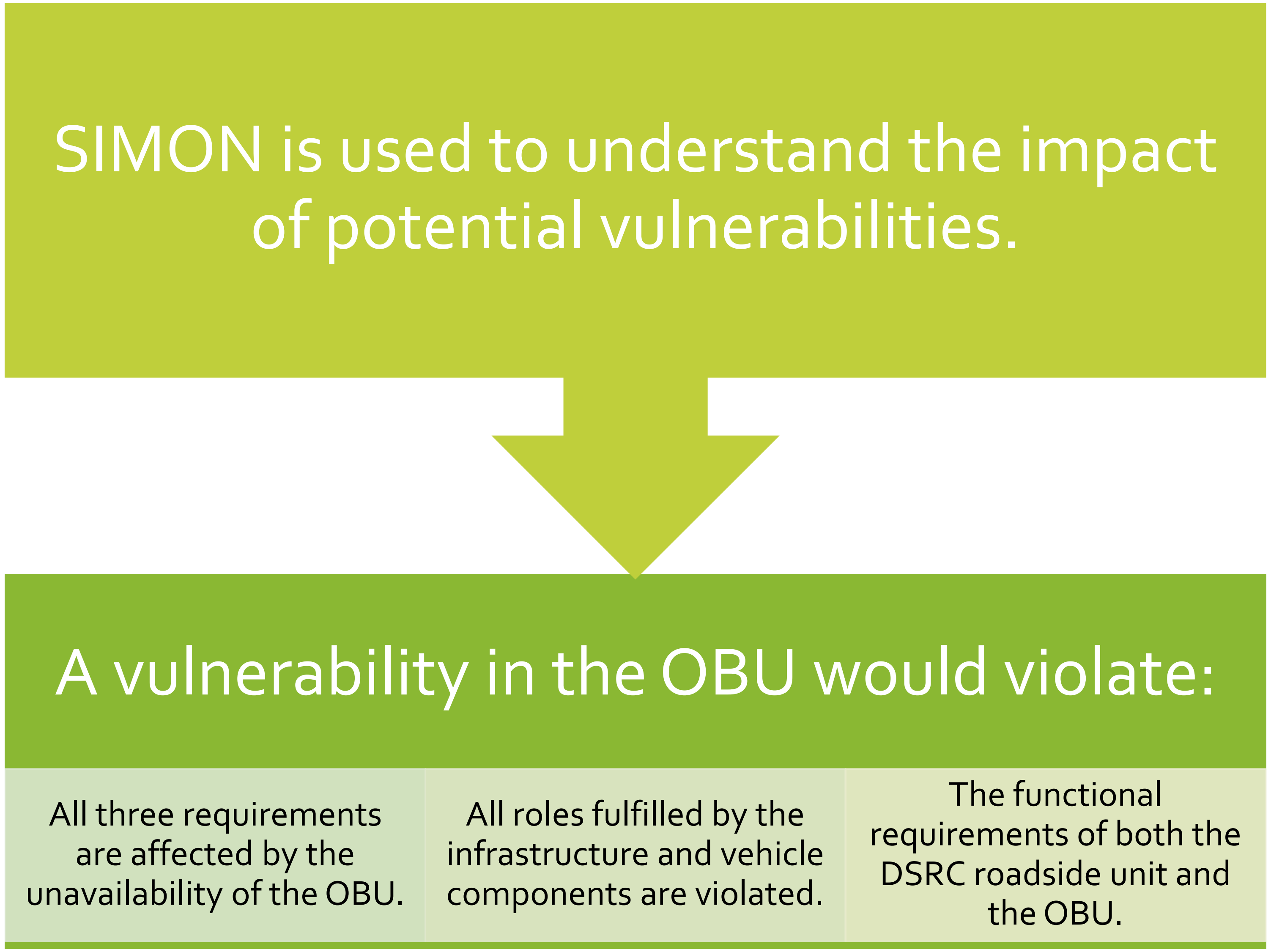
Abstract Realization

- Abstract Realization contains transmission capabilities and roles of the categorized components in previous phase.
- These components exist on both the vehicle and infrastructure side of the V2I system:
  - Applicational Platform
  - Wireless Data Systems
  - Wireless Data Interface

Concrete Realization

- Core data transmission occurs in the hardware and software components of the V2I components.
  - DSRC On Board Unit (OBU)
  - DSRC Transceiver
  - Wireless Sensor Network (WSN)

Assurance



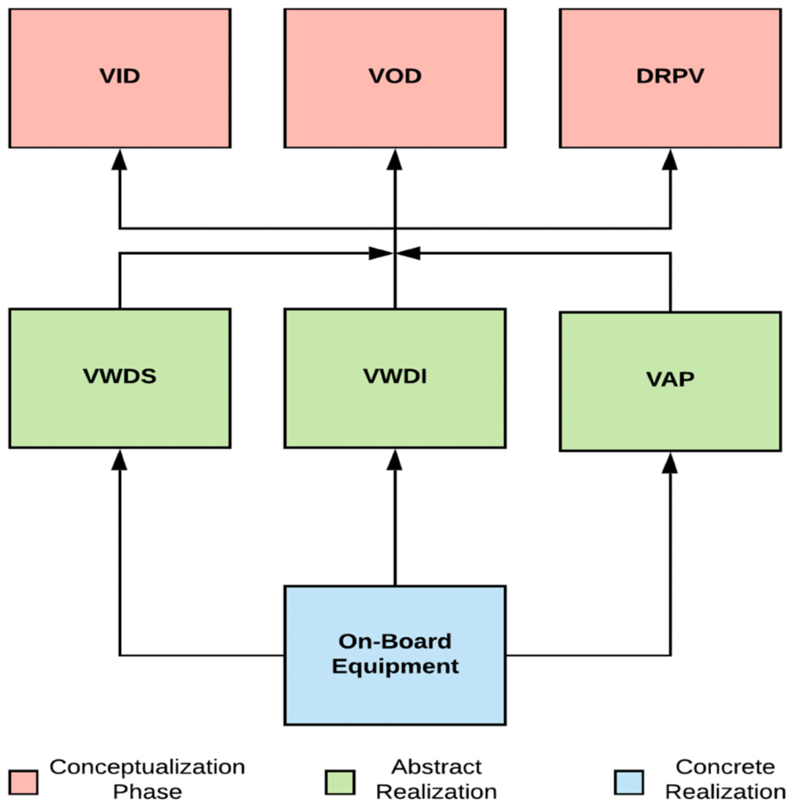
SIMON is used to understand the impact of potential vulnerabilities.

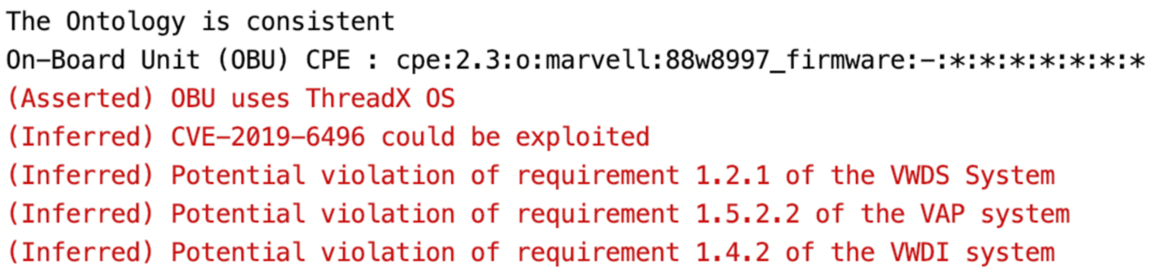
A vulnerability in the OBU would violate:

All three requirements are affected by the unavailability of the OBU.

All roles fulfilled by the infrastructure and vehicle components are violated.

The functional requirements of both the DSRC roadside unit and the OBU.





```
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
```

Assurance

- CPS attacks identified in the companion “SIMON” study
- V2X Remote DSRC Interjection Threat
- V2X Handler Elevation of Privilege Threat

Conclusion

- Proposed a framework for CPS design validation using semantic inference.
- Utilized the SOSA Ontology and CTI Ontology to accomplish each stage of the NIST Framework
- Harnessed SIMON to reason about the acquired data to trace vulnerabilities back to the requirements they violate.

Future Work

- Explore the possibility of extending ontological capabilities to automatically translate design goals into semantic models.
- Test proposed framework in other CPS domains.