FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

System-Level Design Under Confidentiality and Integrity Constraints

Janos Sztipanovits
Istvan Madari
ISIS-Vanderbilt

Berkeley UNIVERSITY OF CALIFORNIA
Massachusetts Institute of Technology
NSF
MICHIGAN
VANDERBILT UNIVERSITY

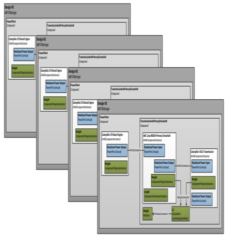
Content

1. **Goals**
2. Theory: Decentralized Label Model
   - Security types
   - Formal Framework
3. Validation
   - CVRIA – Connected Vehicle Pilot
   - Analysis Architecture
4. Next Steps

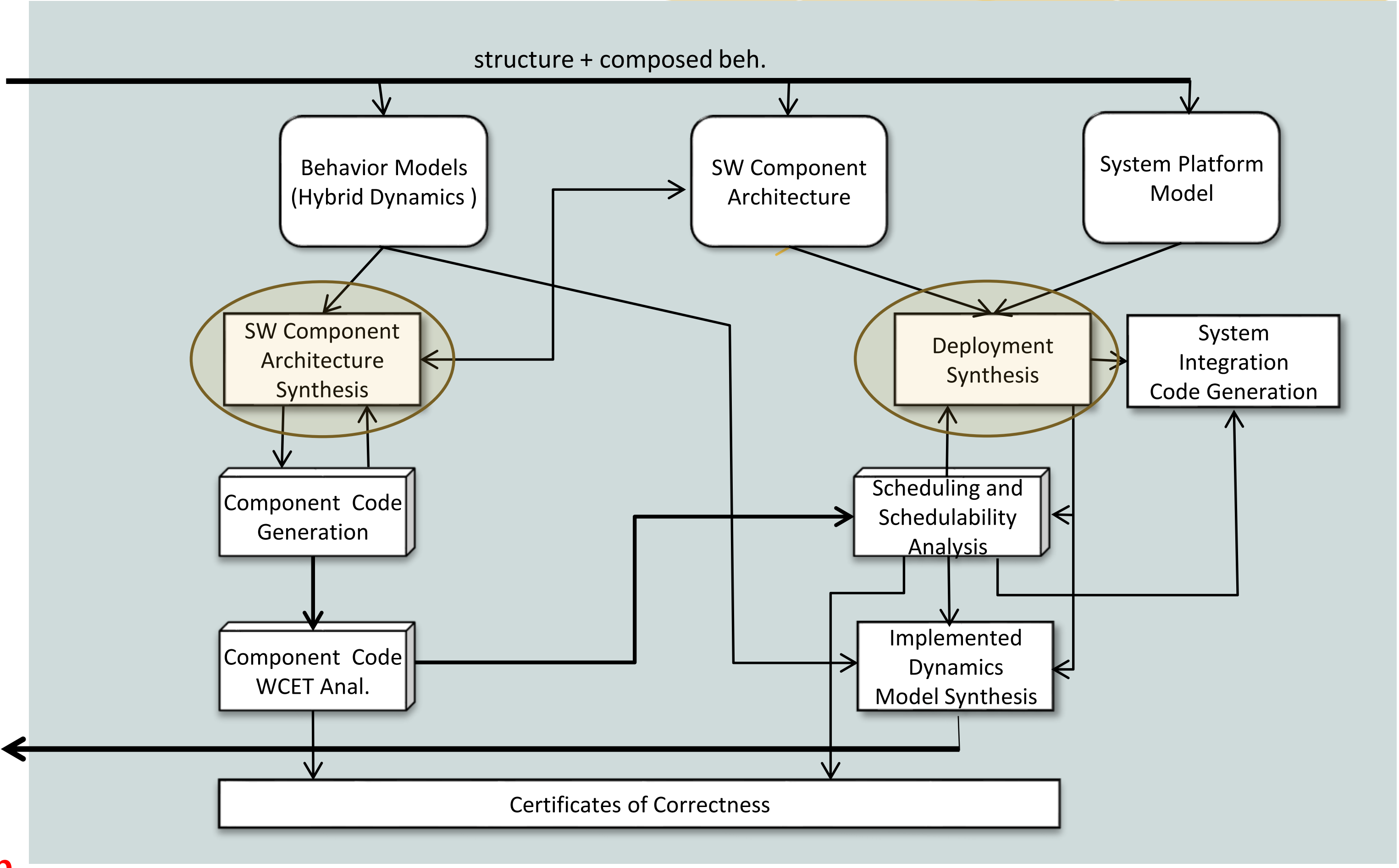
What Is Our Goal?

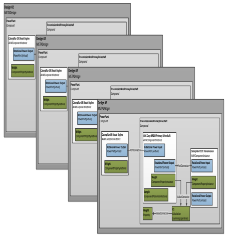
- **The system-level synthesis problem for the "cyber" side of CPS:**
  - Derive specification for the behavior of the system components that will be implemented using networked computing
  - Derive a functional model for the information architecture and componentize the system
  - Select computing/networking platform
  - Derive deployment model assigning components of the information architecture to processing and communication platforms
  - Generate code for software components and derive WCET and WCCT
  - Perform timing analysis
- **Making security part of system-level co-design (correct-by-construction)**
  - Co-design of functionality, performance, timing and security
  - Our goal is to address security requirements as part of the design trades embedded in the system-level design process

Typical System-level Synthesis Steps of Information Architecture



Design Architectures with ideal comp. dynamics

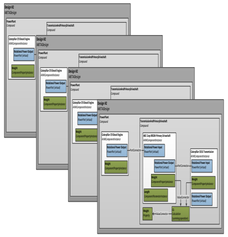

structure + composed beh.
Behavior Models (Hybrid Dynamics)
SW Component Architecture
System Platform Model
SW Component Architecture Synthesis
Deployment Synthesis
System Integration Code Generation
Component Code Generation
Scheduling and Schedulability Analysis
Component Code WCET Anal.
Implemented Dynamics Model Synthesis
Certificates of Correctness



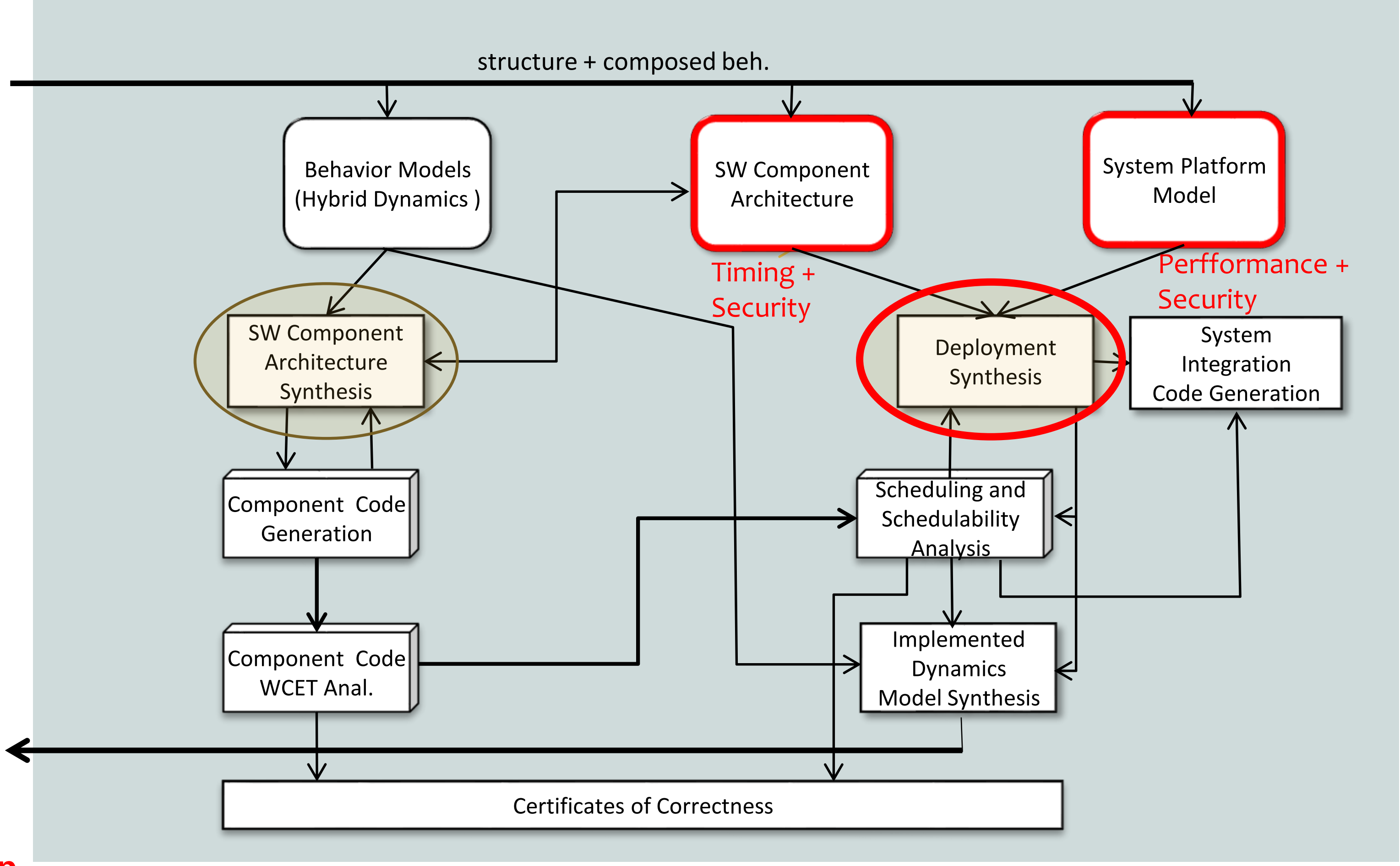
Design Architectures with **deployed comp. dynamics**

- CAN Bus
- TT bus

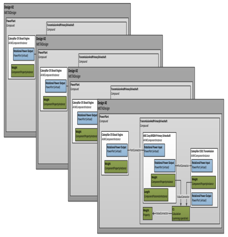
Typical System-level Synthesis Steps of Information Architecture



Design Architectures with ideal comp. dynamics



structure + composed beh.
Behavior Models (Hybrid Dynamics)
SW Component Architecture
System Platform Model
Timing + Security
Perfformance + Security
SW Component Architecture Synthesis
Deployment Synthesis
System Integration Code Generation
Component Code Generation
Scheduling and Schedulability Analysis
Component Code WCET Anal.
Implemented Dynamics Model Synthesis
Certificates of Correctness



Design Architectures with **deployed comp. dynamics**

- CAN Bus
- TT bus

FORCES FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Synthesis Problem

- How to map a logical Information Architecture (components + information flows) on a physical Platform Architecture such that

  - Functional requirements (the information architecture)
  - Performance requirements (timing)
  - Security requirements (confidentiality and integrity)

  are satisfied simultaneously?

Challenges

- Modeling language suite ✓
  (behavior, information flows, SW components, architecture, timing, platform, deployment) - reuse previous work as example
- Security Requirement Modeling ✓
  (need to be composable with other modeling aspects)
- Common Semantic Domain and Formal Framework ✓
  (functional, performance and security models need to be anchored to a semantic domain suitable for synthesis)
- Synthesis Framework and Co-design flow ✓
  (mapping system-level synthesis problem on the formal framework and tools)
- **Integrated Tool Suite and Validation**
  (target domain rich enough for testing the co-design tool suite)

Content

1. Goals
2. **Theory: Decentralized Label Model**
   - Security types
   - Formal Framework
3. Validation
   - CVRIA – Connected Vehicle Pilot
   - Analysis Architecture
4. Next Steps

Security Concerns Addressed

- **Integrity attacks**
  - Manipulate data (value, timestamp, source identity,..)
- **Confidentiality attack**
  - Leak critical data to unauthorized persons/systems
- **Integrity and confidentiality restrictions impose constraints on information flows.**
  - How to model these restrictions?
  - How to integrate these restrictions with others (functional and timing) and formulate a co-design problem?

Decentralized Label Model (DLM) for Information Flow Control

- Myers, Liskov (1997): Introduced **security-typed languages** by labeling variables with information flow security policies
- Method was developed for programming languages, the result is *Jif, a security-typed version of Java.*
- DLM provides mechanism for static/dynamic type checking of security labels in information flows to detect policy violations.
- Example: *Jif*, a security-typed version of Java
- **Introduce security-types in modeling languages**

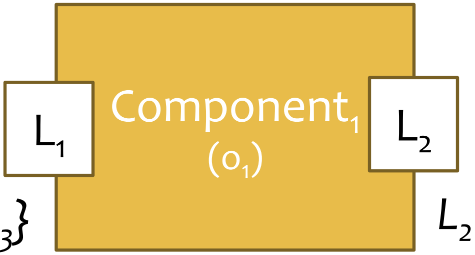
DLM Concepts

- New semantic concepts introduced:
  - *Principles* that represent authority entities.
  - *Labels expressing* security classes encountered in most information flow models.
  - *Policies* that are elementary security primitives used in *labels.*
  - *Labeled entities* that have attached labels, such as *values, slots (variables, objects, i/o channels)*. Copies of *values* can be relabeled, *slots* cannot.
  - *Operators* that can *relabel* or *declassify* values in information flows.
- The model can be naturally applied to system-level information flow modeling languages by assigning security types to input/output ports

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Working With Security Labels

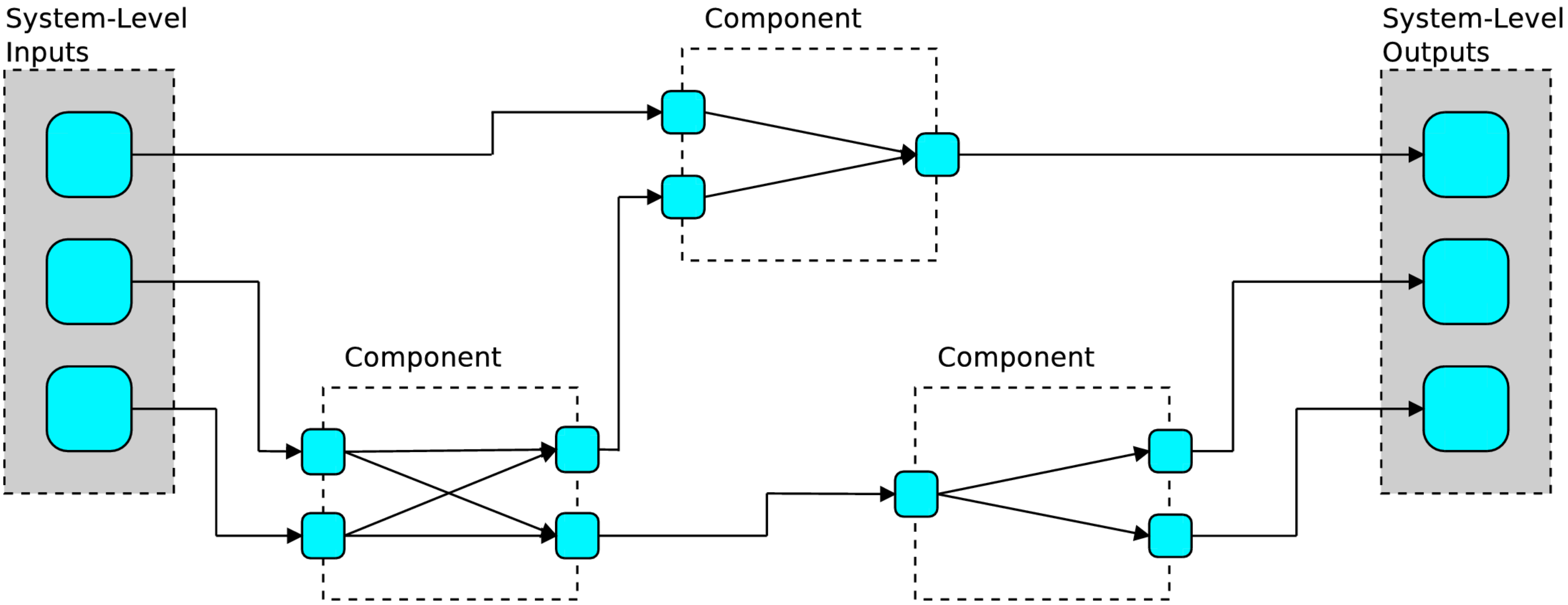
- *Labels* contain a set of *policies*. Each *policy* includes an *owner* and a set of *readers* allowed by the *owner*. The *effective reader set* for a *label* is the intersection of every *reader set* in it.
  $L = \{o_1: r_1, r_2; o_2: r_2, r_3\}$
- *Processing blocks* running under the authority of an *owner* can *declassify* the *owner's policy* by adding *readers.*



$L_1 = \{o_1: r_1, r_2; o_2: r_2, r_3\}$

$L_2 = \{o_1: r_1, r_2, r_{3,} ; o_2: r_2, r_3\}$

Information Flows in an Information Architecture

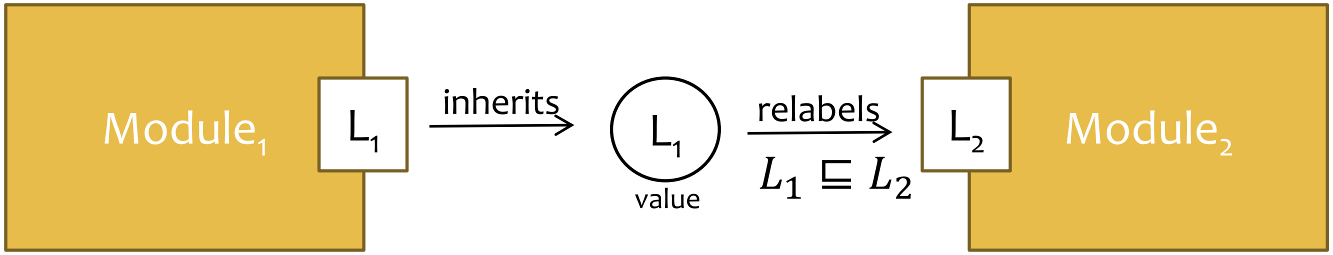


→ Logical Information Flow

🟦 Annoted with Security Label

Security Type Propagation Rules

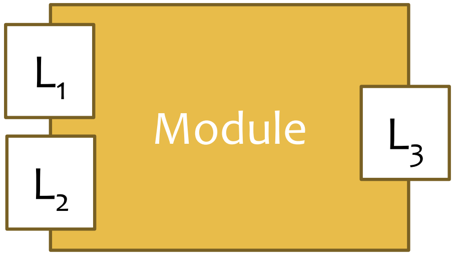
- *Propagation rule-1 (restriction):*



$owners(L_1) \subseteq owners(L_2)$
$\forall o \in owners(L_1), readers(L_1, o) \supseteq readers(L_2, o)$

(L$_1$ has more readers and fewer owners than L$_2$)

- *Propagation rule-2 (join):*



L$_3$ is the *join* of L$_1$ and L$_2$
$L_3 \ = \ L_1 \sqcup L_2$

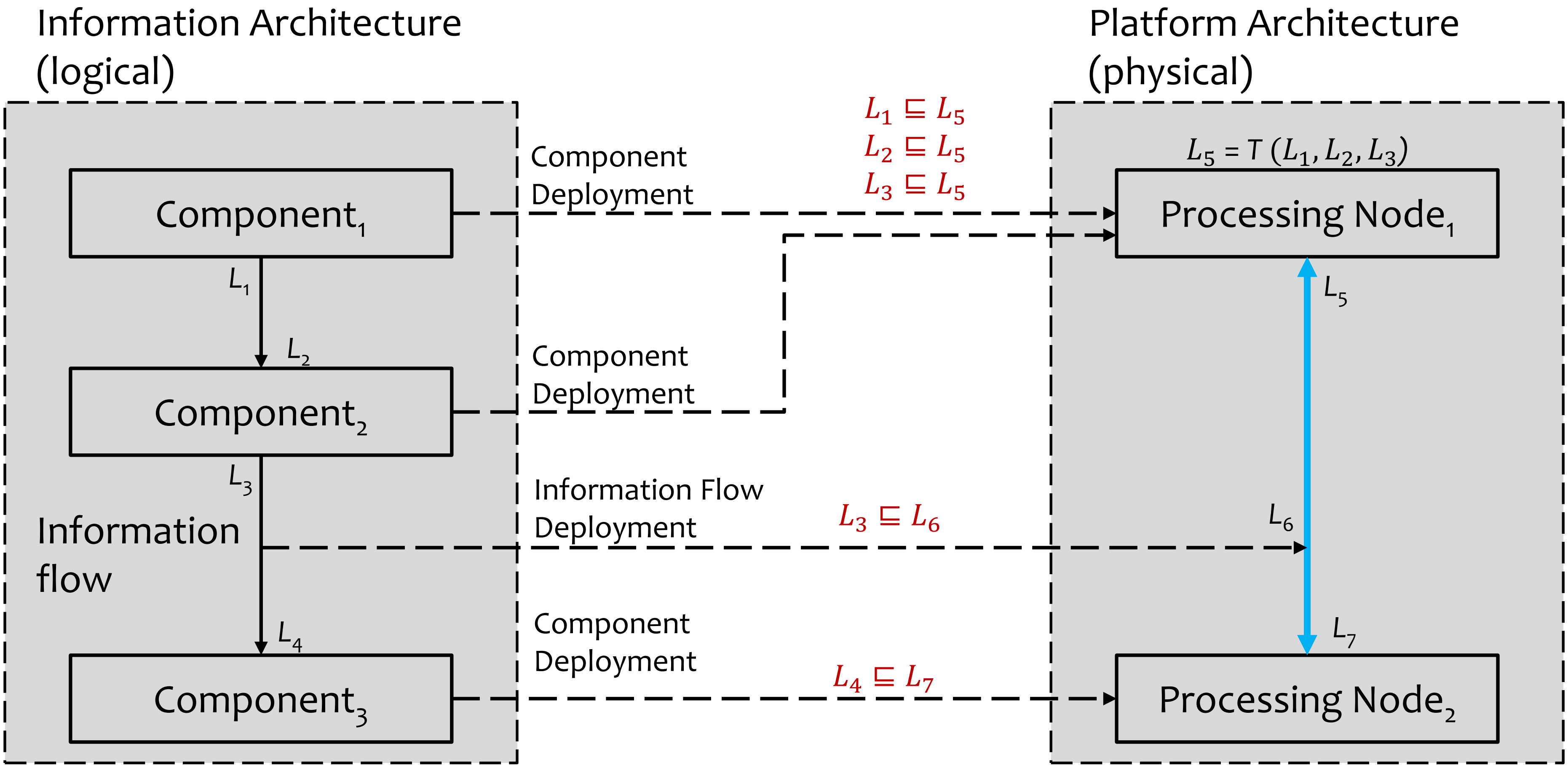
$owners(L_1 \sqcup L_2) = owners(L_1) \cup owners(L_2)$

$readers(L_1 \sqcup L_2, o) \ = readers(L_1, o) \cap readers(L_2, o)$

(*join* L$_1$ and L$_2$ is the least restrictive label that maintains all the flow restrictions specified by L$_1$ and L$_2$)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Information Architecture Deployed on a Physical Platform



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Content

1. Goals
2. **Theory: Decentralized Label Model**
   - ○ Security types
   - ○ **Formal Framework**
3. Validation
   - ○ CVRIA – Connected Vehicle Pilot
   - ○ Analysis Architecture
4. Next Steps

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

FORMULA

- Ethan Jackson (ISIS grad student 2004-2008; MSR 2009 – Present)
- Algebraic Data Types (ADT), Open World Logic Programs (OLP) provide common semantic domain for DSMLs and model transformations.
- Constraint Logic Programming provides execution semantics for model transformations.
- Z3 backend for model finding.

Policies and Labels

A policy consists of an owner principal and a set of allowed reader principals:

owner: reader1 reader2

A label is a (possibly empty) set of policies:

L = { policy1; policy2; ...}

Our encoding views a label as a tree where the label's identifier is the root, the policy owners make up the second level, and the corresponding readers make up the third level :

```
Label  ::= new (name:String).
Policy ::= new (lbl:Label, owner:Principal).
Reader ::= new (pl:Policy, reader:Principal).
```

Propagation Rules Examples

We can compute the effective readers set for each label:

```
EffReader(lbl, reader) :-
  lbl is Label, reader is Principal, no CantRead(lbl, reader).
CantRead(pl.lbl, r) :-
  pl is Policy, r is Principal,
  no { r' | ActsForTR(r, r'), Reader(pl, r') }.
```

We can compare the restrictiveness of labels based on their effective reader sets:

```
AtLeastAsRestrictive(lbl1, lbl2) :-
  lbl1 is Label, lbl2 is Label,
  no { x | EffReader(lbl1, x), CantRead(lbl2, x) }.
```

We can also “propagate” policies by computing the join ($\sqcup$) of two labels: the least restrictive label that is at least as restrictive as both labels.

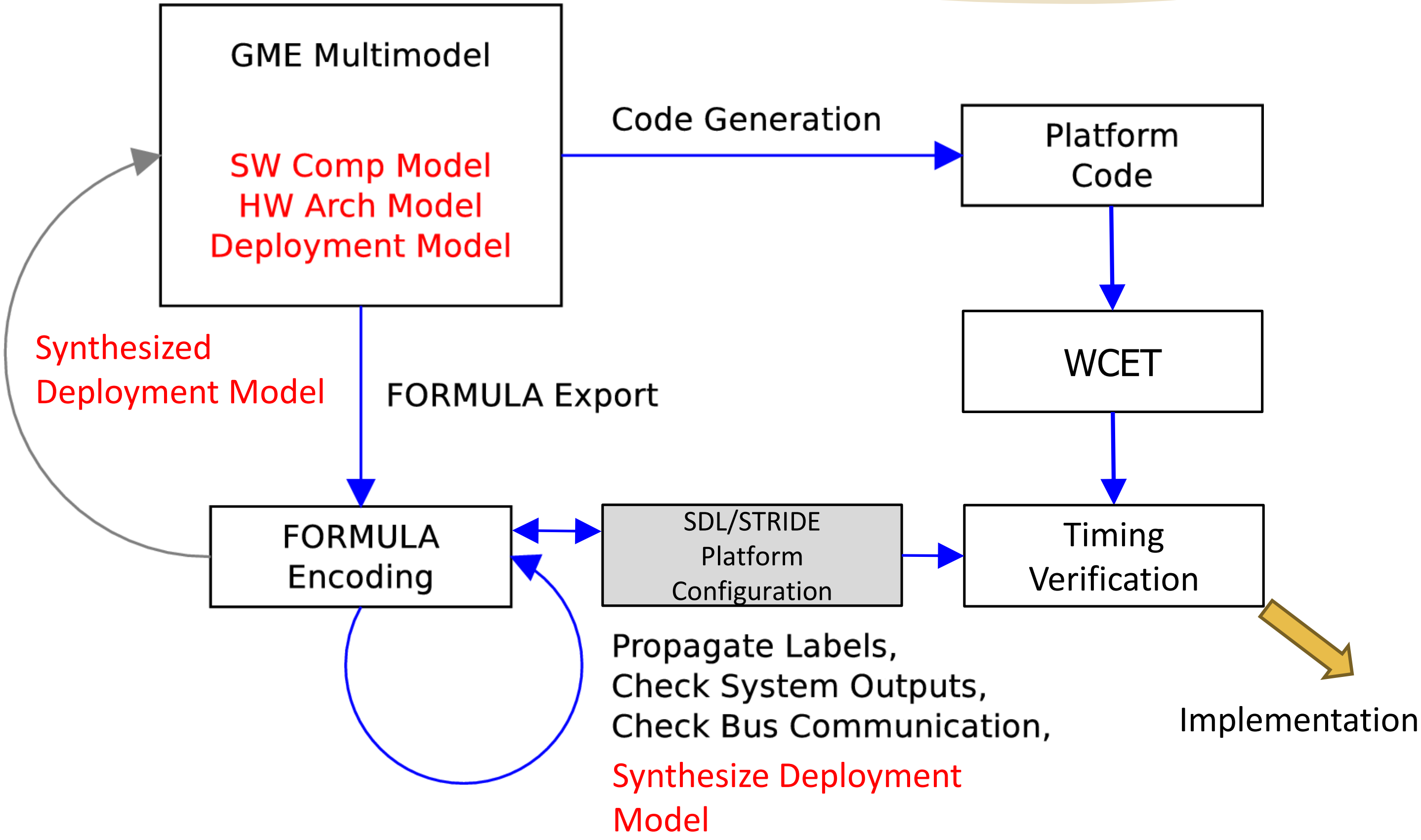
Content

1. Goals
2. Theory: Decentralized Label Model
   - Security types
   - Formal Framework
3. **Validation**
   - CVRIA – Connected Vehicle Pilot
   - Analysis Architecture
4. Next Steps

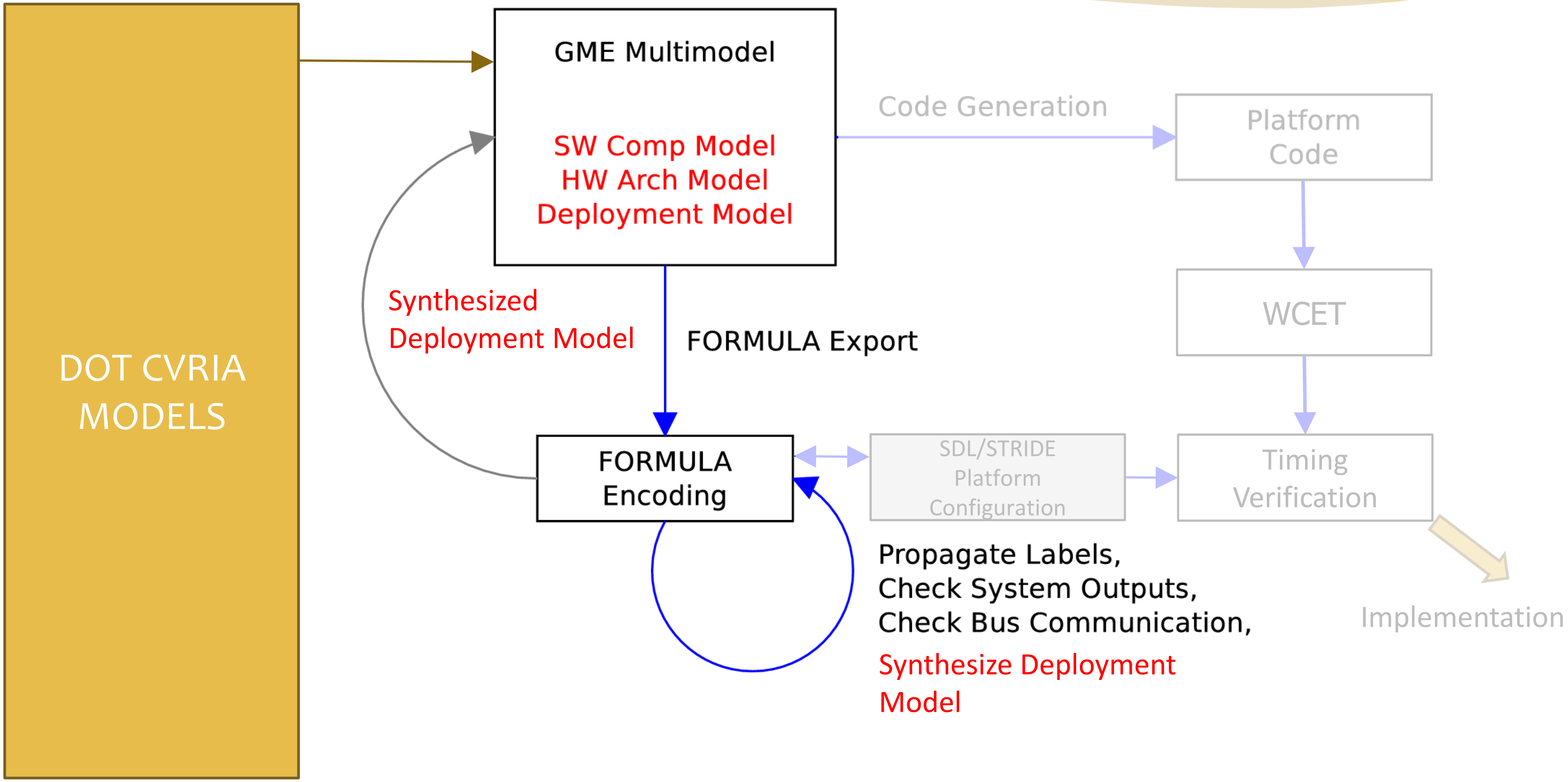
Validation Is Hard

- Results from the theory so far
  - Extending information flow models with security types (DSML)
  - Type checking rules (propagation and transformation)
  - Formulation of system-level design problems (deployment synthesis, security controls)
  - Mapping to formal framework (FORMULA, Z3)
  - Demonstrating in small examples
- Validation
  - What are the policy/performance tradeoffs?
  - Is the method practical for real-life system-level design problems?
  - What is the feasibility of creating a useable tool chain?
  - Scaling limitations?
- Primary Challenge: Finding real-life use case with existing models

Validation of the System-level Design Workflow



Validation of the System-level Design Workflow



DOT CVRIA MODELS

GME Multimodel

SW Comp Model
HW Arch Model
Deployment Model

Code Generation

Platform Code

WCET

Synthesized Deployment Model

FORMULA Export

FORMULA Encoding

SDL/STRIDE Platform Configuration

Timing Verification

Propagate Labels,
Check System Outputs,
Check Bus Communication,
Synthesize Deployment Model

Implementation

Content

1. Goals
2. Theory: Decentralized Label Model
   - Security types
   - Formal Framework
3. **Validation**
   - **CVRIA – DoT - Connected Vehicle Pilot**
   - Analysis Architecture
4. Next Steps

Views of CVRIA

Views	Applications
Enterprise - Describes the relationships between organizations and the roles those organizations play within the connected vehicle environment	Principals, Labels, Policies
Functional - Describes abstract functional elements (processes) and their logical interactions (data flows)that satisfy the system requirements	Components, Information flows Label assignments
Physical - Describes physical objects (systems and devices) and their application objects as well as the high-level interfaces between those physical objects	Platform properties
Communications - Describes the layered sets of communications protocols that are required to support communications among the physical objects that participate in the connected vehicle environment	Communication channel properties

http://www.iteris.com/cvria/

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

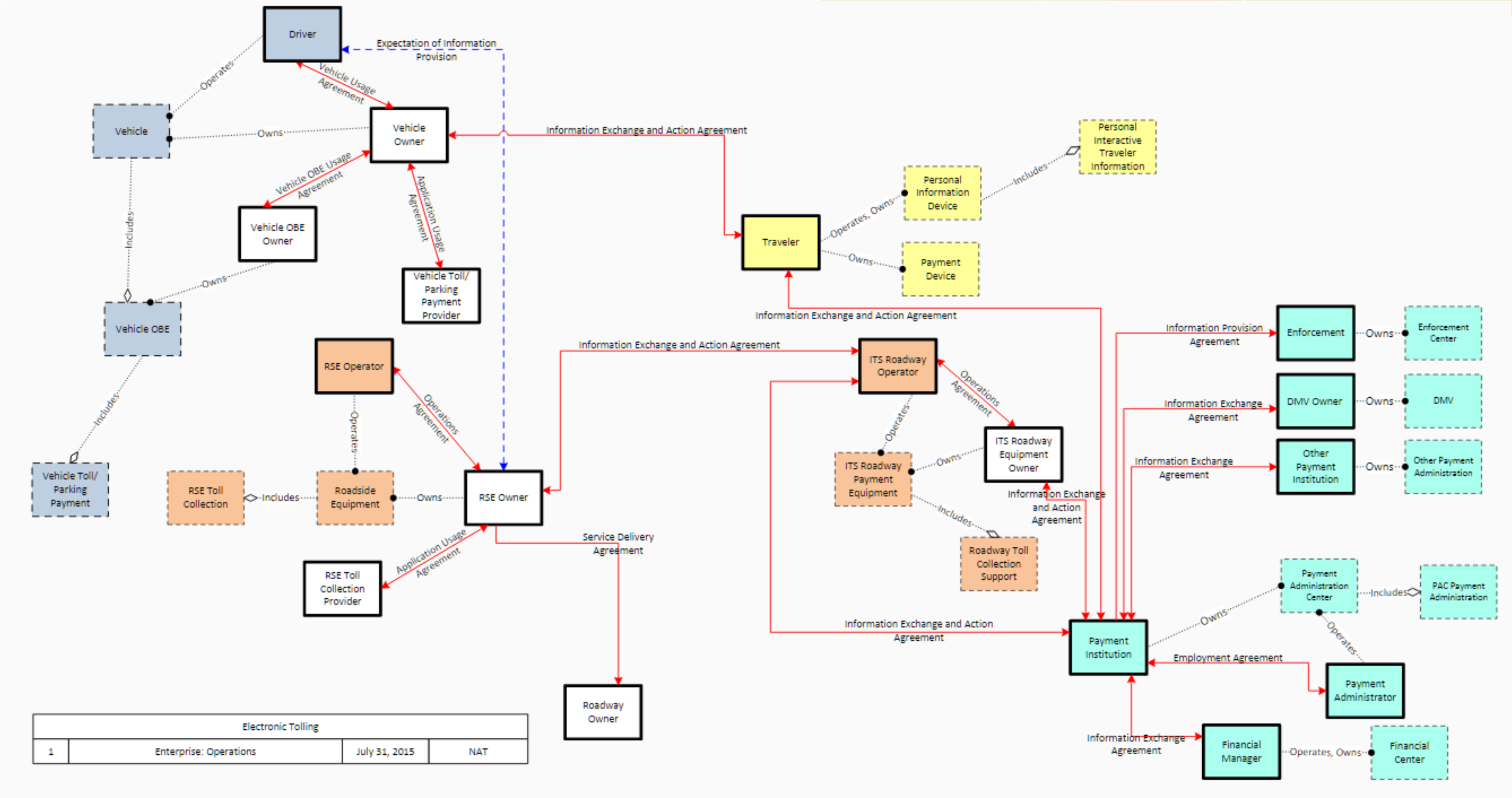
Validation Using CVRIA Models

- It provides a large set of use cases and architecture models. In general the models contain:
  - Organizational, physical, functional, and communication models (e.g.: toll collection, vehicles, drivers, equipment)
  - Dataflows, information flows, data structures between components
  - Mappings across different layers
- Validation concept
  - Import relevant subset of CVRIA models into our formal modeling environment (FORMULA)
  - Integrate CVRIA DSMLs with security DSL constructs
  - Based on the security labels:
    - Perform type checking (using FORMULA constraint check)
    - Propagate security labels (using FORMULA)
    - Find deployment properties (using FORMULA Z3 solver)

Example Application: Electronic Toll Collection

- Collect tolls electronically
- Detect and process violations
- Fees may be adjusted to implement demand management strategies
- Communication between roadway equipment and the vehicle is required
- Fixed-Point to Fixed-Point interfaces between toll collection equipment and transportation authorities and financial infrastructure supporting fee collection
- Toll violations are identified and electronically posted

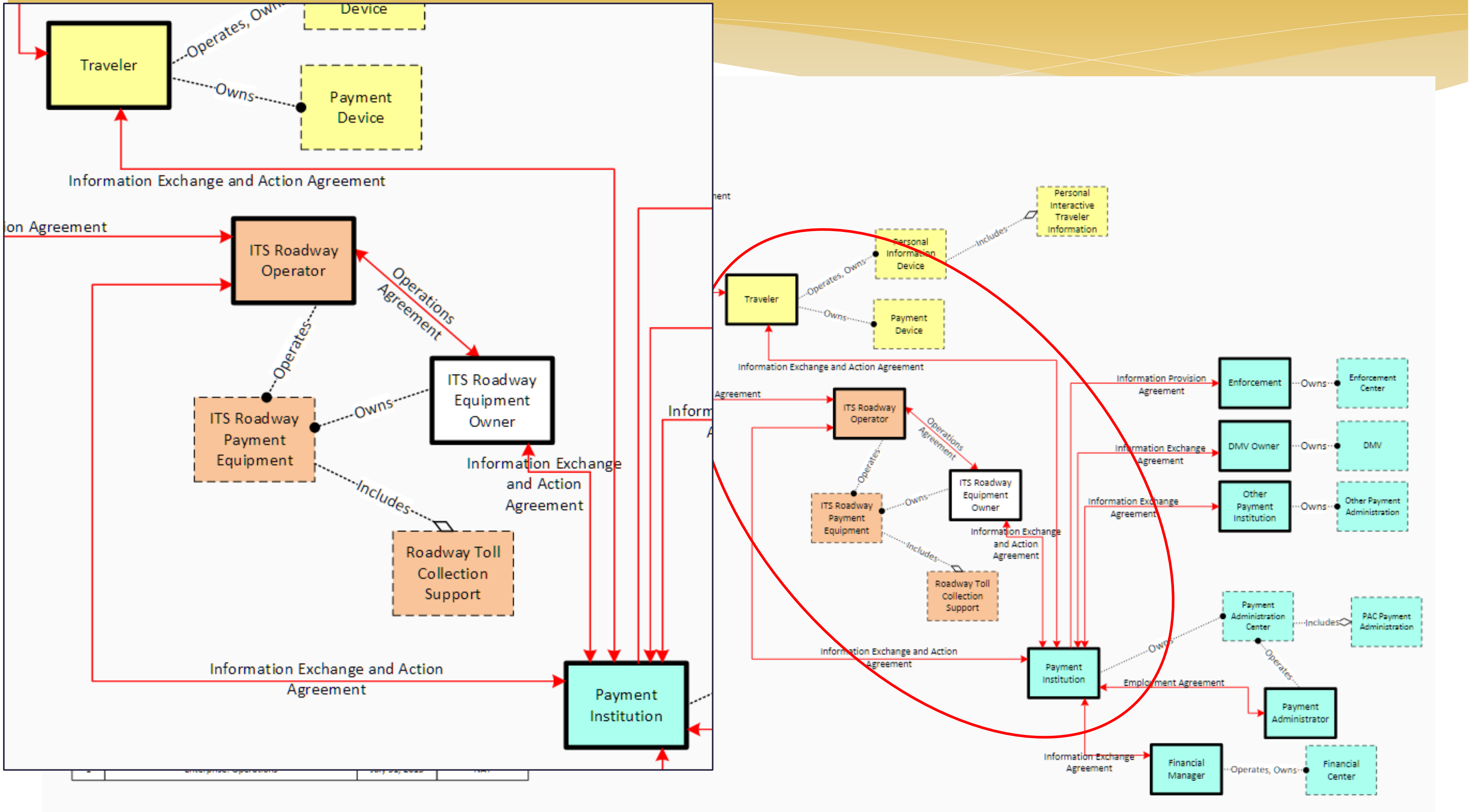
Enterprise View


Driver
Expectation of Information Provision
Operates
Vehicle Usage Agreement
Vehicle
Owns
Vehicle Owner
Information Exchange and Action Agreement
Vehicle OBE Usage Agreement
Application Usage Agreement
Includes
Vehicle OBE Owner
Vehicle Toll/ Parking Payment Provider
Owns
Vehicle OBE
Includes
Vehicle Toll/ Parking Payment
RSE Operator
Operations Agreement
Operates
RSE Toll Collection
Includes
Roadside Equipment
Owns
RSE Owner
Application Usage Agreement
RSE Toll Collection Provider
Service Delivery Agreement
Roadway Owner
Information Exchange and Action Agreement
Traveler
Operates, Owns
Personal Information Device
Includes
Personal Interactive Traveler Information
Owns
Payment Device
Information Exchange and Action Agreement
ITS Roadway Operator
Operations Agreement
Operates
ITS Roadway Equipment Owner
Owns
ITS Roadway Payment Equipment
Includes
Roadway Toll Collection Support
Information Exchange and Action Agreement
Information Exchange and Action Agreement
Information Provision Agreement
Enforcement
Owns
Enforcement Center
Information Exchange Agreement
DMV Owner
Owns
DMV
Information Exchange Agreement
Other Payment Institution
Owns
Other Payment Administration
Payment Institution
Owns
Payment Administration Center
Includes
PAC Payment Administration
Operates
Employment Agreement
Payment Administrator
Information Exchange Agreement
Financial Manager
Operates, Owns
Financial Center

Electronic Tolling			
1	Enterprise: Operations	July 31, 2015	NAT

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

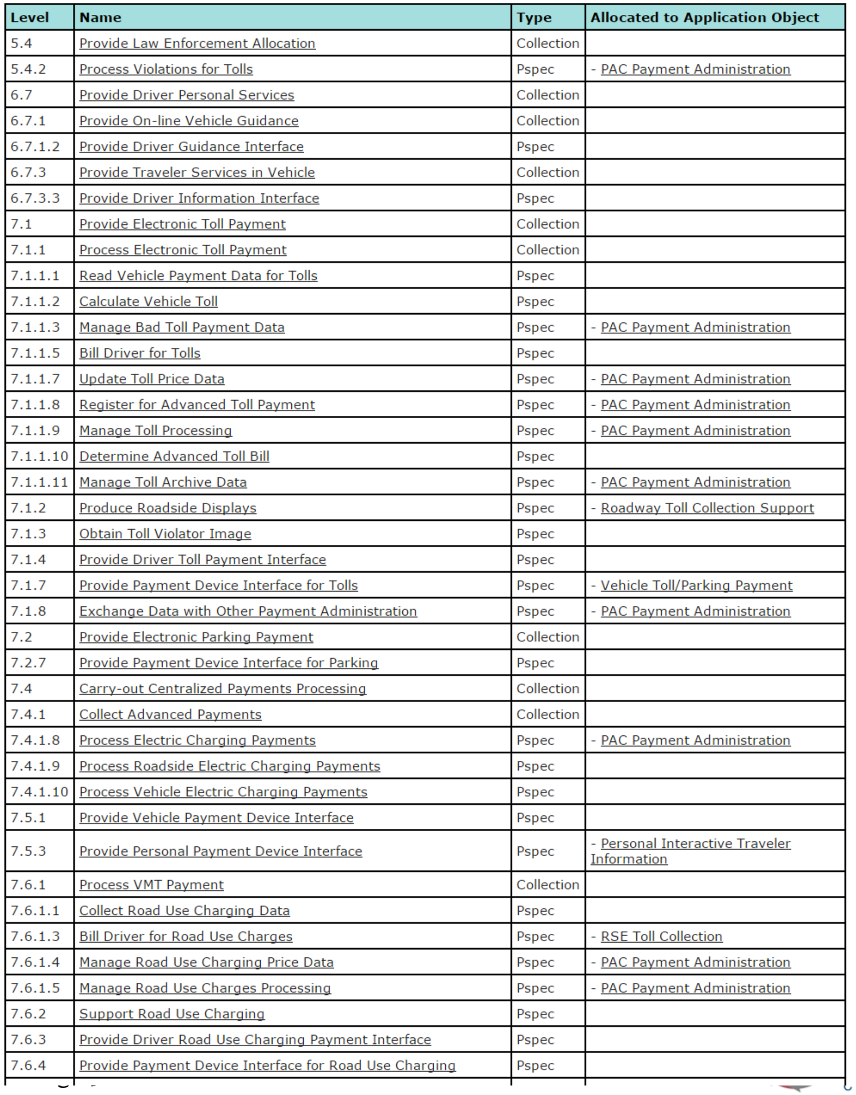
Traveler - Payment Institution Relationship


Traveler
Operates, Own
Device
Owns
Payment Device
Information Exchange and Action Agreement
ion Agreement
ITS Roadway Operator
Operations Agreement
Operates
ITS Roadway Payment Equipment
Owns
ITS Roadway Equipment Owner
Information Exchange and Action Agreement
Includes
Roadway Toll Collection Support
Information Exchange and Action Agreement
Payment Institution
Inform
ent
Traveler
Operates, Owns
Personal Information Device
Includes
Personal Interactive Traveler Information
Owns
Payment Device
Information Exchange and Action Agreement
Agreement
ITS Roadway Operator
Operations Agreement
Operates
ITS Roadway Payment Equipment
Owns
ITS Roadway Equipment Owner
Information Exchange and Action Agreement
Includes
Roadway Toll Collection Support
Information Provision Agreement
Enforcement
Owns
Enforcement Center
Information Exchange Agreement
DMV Owner
Owns
DMV
Information Exchange Agreement
Other Payment Institution
Owns
Other Payment Administration
Information Exchange and Action Agreement
Payment Institution
Owns
Payment Administration Center
Includes
PAC Payment Administration
Operates
Employment Agreement
Payment Administrator
Information Exchange Agreement
Financial Manager
Operates, Owns
Financial Center

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

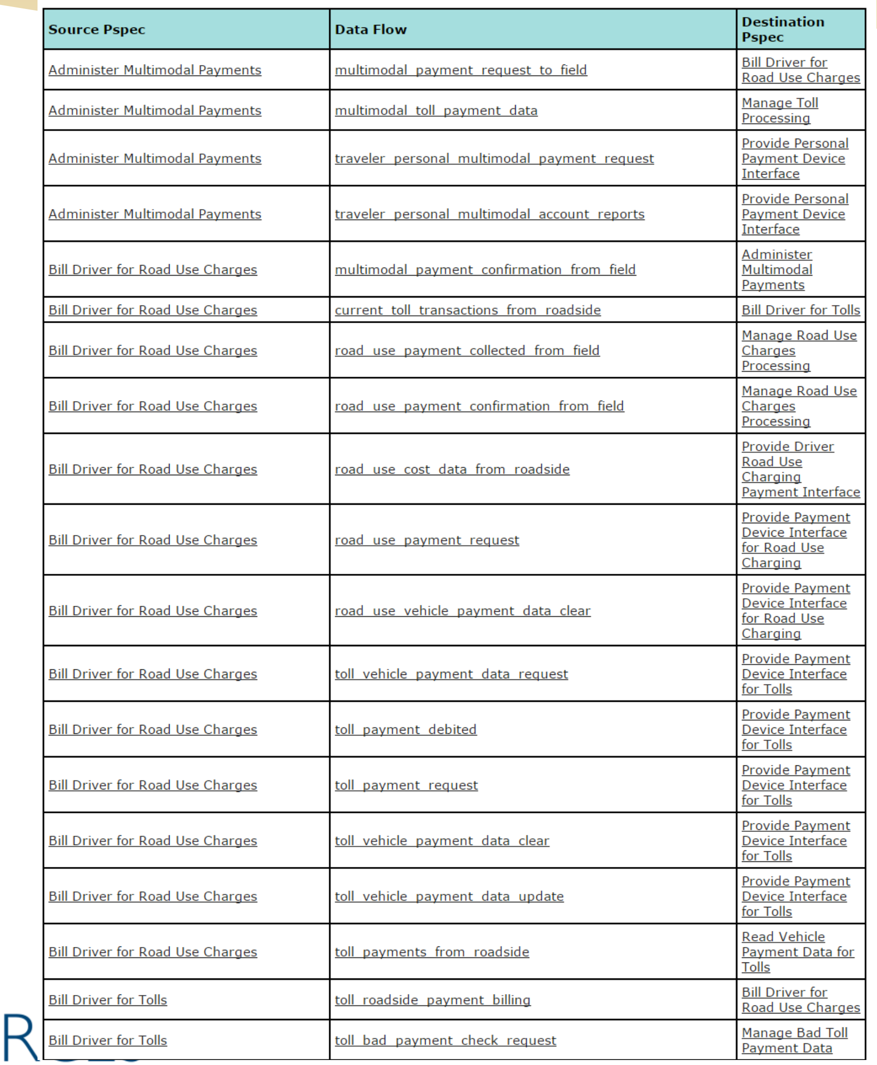
Electronic Toll Collection: Functional View

Processes: 48



Level	Name	Type	Allocated to Application Object
5.4	Provide Law Enforcement Allocation	Collection	
5.4.2	Process Violations for Tolls	Pspec	- PAC Payment Administration
6.7	Provide Driver Personal Services	Collection	
6.7.1	Provide On-line Vehicle Guidance	Collection	
6.7.1.2	Provide Driver Guidance Interface	Pspec	
6.7.3	Provide Traveler Services in Vehicle	Collection	
6.7.3.3	Provide Driver Information Interface	Pspec	
7.1	Provide Electronic Toll Payment	Collection	
7.1.1	Process Electronic Toll Payment	Collection	
7.1.1.1	Read Vehicle Payment Data for Tolls	Pspec	
7.1.1.2	Calculate Vehicle Toll	Pspec	
7.1.1.3	Manage Bad Toll Payment Data	Pspec	- PAC Payment Administration
7.1.1.5	Bill Driver for Tolls	Pspec	
7.1.1.7	Update Toll Price Data	Pspec	- PAC Payment Administration
7.1.1.8	Register for Advanced Toll Payment	Pspec	- PAC Payment Administration
7.1.1.9	Manage Toll Processing	Pspec	- PAC Payment Administration
7.1.1.10	Determine Advanced Toll Bill	Pspec	
7.1.1.11	Manage Toll Archive Data	Pspec	- PAC Payment Administration
7.1.2	Produce Roadside Displays	Pspec	- Roadway Toll Collection Support
7.1.3	Obtain Toll Violator Image	Pspec	
7.1.4	Provide Driver Toll Payment Interface	Pspec	
7.1.7	Provide Payment Device Interface for Tolls	Pspec	- Vehicle Toll/Parking Payment
7.1.8	Exchange Data with Other Payment Administration	Pspec	- PAC Payment Administration
7.2	Provide Electronic Parking Payment	Collection	
7.2.7	Provide Payment Device Interface for Parking	Pspec	
7.4	Carry-out Centralized Payments Processing	Collection	
7.4.1	Collect Advanced Payments	Collection	
7.4.1.8	Process Electric Charging Payments	Pspec	- PAC Payment Administration
7.4.1.9	Process Roadside Electric Charging Payments	Pspec	
7.4.1.10	Process Vehicle Electric Charging Payments	Pspec	
7.5.1	Provide Vehicle Payment Device Interface	Pspec	
7.5.3	Provide Personal Payment Device Interface	Pspec	- Personal Interactive Traveler Information
7.6.1	Process VMT Payment	Collection	
7.6.1.1	Collect Road Use Charging Data	Pspec	
7.6.1.3	Bill Driver for Road Use Charges	Pspec	- RSE Toll Collection
7.6.1.4	Manage Road Use Charging Price Data	Pspec	- PAC Payment Administration
7.6.1.5	Manage Road Use Charges Processing	Pspec	- PAC Payment Administration
7.6.2	Support Road Use Charging	Pspec	
7.6.3	Provide Driver Road Use Charging Payment Interface	Pspec	
7.6.4	Provide Payment Device Interface for Road Use Charging	Pspec	

Dataflows: 85

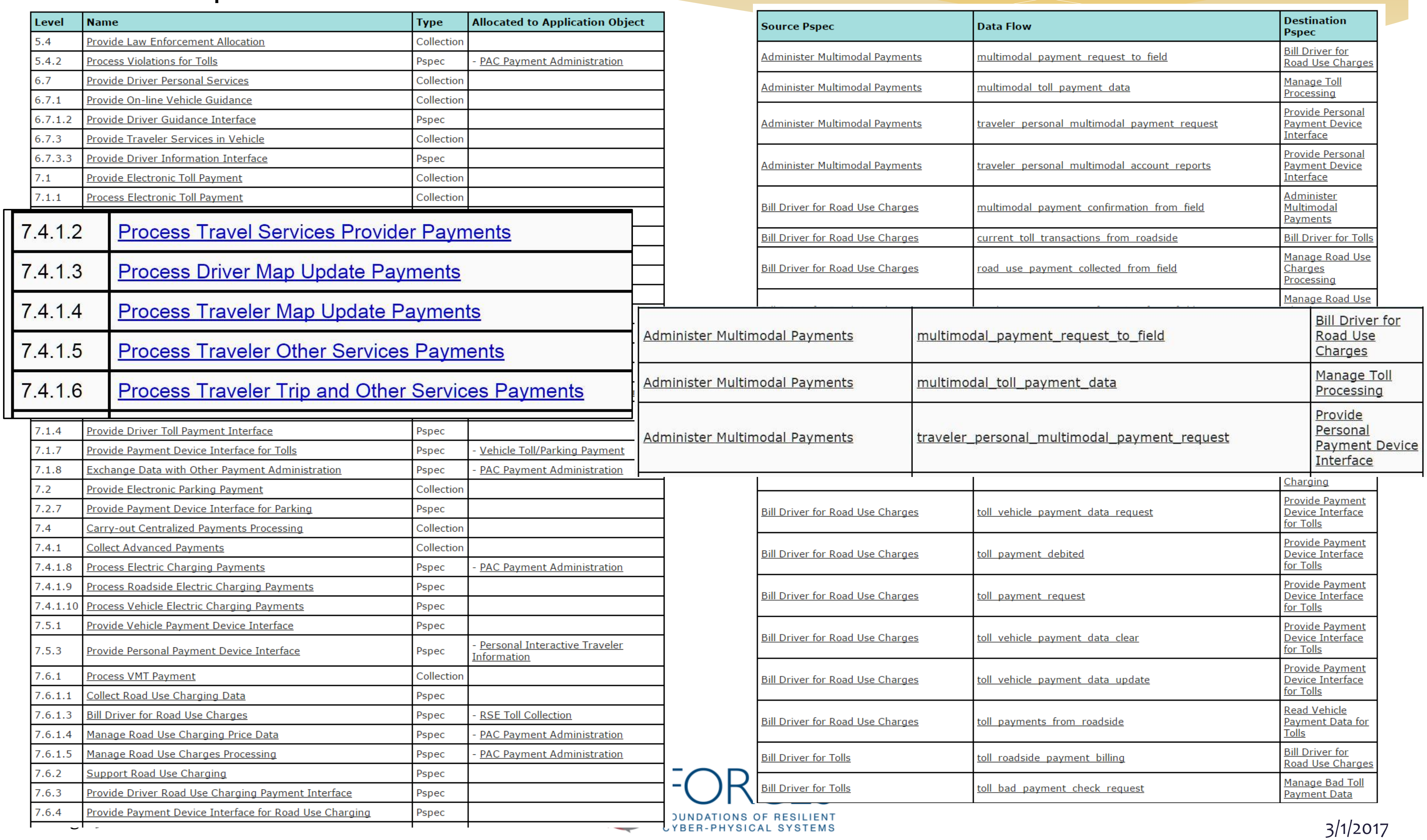


Source Pspec	Data Flow	Destination Pspec
Administer Multimodal Payments	multimodal_payment_request_to_field	Bill Driver for Road Use Charges
Administer Multimodal Payments	multimodal_toll_payment_data	Manage Toll Processing
Administer Multimodal Payments	traveler_personal_multimodal_payment_request	Provide Personal Payment Device Interface
Administer Multimodal Payments	traveler_personal_multimodal_account_reports	Provide Personal Payment Device Interface
Bill Driver for Road Use Charges	multimodal_payment_confirmation_from_field	Administer Multimodal Payments
Bill Driver for Road Use Charges	current_toll_transactions_from_roadside	Bill Driver for Tolls
Bill Driver for Road Use Charges	road_use_payment_collected_from_field	Manage Road Use Charges Processing
Bill Driver for Road Use Charges	road_use_payment_confirmation_from_field	Manage Road Use Charges Processing
Bill Driver for Road Use Charges	road_use_cost_data_from_roadside	Provide Driver Road Use Charging Payment Interface
Bill Driver for Road Use Charges	road_use_payment_request	Provide Payment Device Interface for Road Use Charging
Bill Driver for Road Use Charges	road_use_vehicle_payment_data_clear	Provide Payment Device Interface for Road Use Charging
Bill Driver for Road Use Charges	toll_vehicle_payment_data_request	Provide Payment Device Interface for Tolls
Bill Driver for Road Use Charges	toll_payment_debited	Provide Payment Device Interface for Tolls
Bill Driver for Road Use Charges	toll_payment_request	Provide Payment Device Interface for Tolls
Bill Driver for Road Use Charges	toll_vehicle_payment_data_clear	Provide Payment Device Interface for Tolls
Bill Driver for Road Use Charges	toll_vehicle_payment_data_update	Provide Payment Device Interface for Tolls
Bill Driver for Road Use Charges	toll_payments_from_roadside	Read Vehicle Payment Data for Tolls
Bill Driver for Tolls	toll_roadside_payment_billing	Bill Driver for Road Use Charges
Bill Driver for Tolls	toll_bad_payment_check_request	Manage Bad Toll Payment Data

Electronic Toll Collection: Functional View

Processes: 48

Dataflows: 85



Level	Name	Type	Allocated to Application Object
5.4	Provide Law Enforcement Allocation	Collection	
5.4.2	Process Violations for Tolls	Pspec	- PAC Payment Administration
6.7	Provide Driver Personal Services	Collection	
6.7.1	Provide On-line Vehicle Guidance	Collection	
6.7.1.2	Provide Driver Guidance Interface	Pspec	
6.7.3	Provide Traveler Services in Vehicle	Collection	
6.7.3.3	Provide Driver Information Interface	Pspec	
7.1	Provide Electronic Toll Payment	Collection	
7.1.1	Process Electronic Toll Payment	Collection	
7.1.4	Provide Driver Toll Payment Interface	Pspec	
7.1.7	Provide Payment Device Interface for Tolls	Pspec	- Vehicle Toll/Parking Payment
7.1.8	Exchange Data with Other Payment Administration	Pspec	- PAC Payment Administration
7.2	Provide Electronic Parking Payment	Collection	
7.2.7	Provide Payment Device Interface for Parking	Pspec	
7.4	Carry-out Centralized Payments Processing	Collection	
7.4.1	Collect Advanced Payments	Collection	
7.4.1.8	Process Electric Charging Payments	Pspec	- PAC Payment Administration
7.4.1.9	Process Roadside Electric Charging Payments	Pspec	
7.4.1.10	Process Vehicle Electric Charging Payments	Pspec	
7.5.1	Provide Vehicle Payment Device Interface	Pspec	
7.5.3	Provide Personal Payment Device Interface	Pspec	- Personal Interactive Traveler Information
7.6.1	Process VMT Payment	Collection	
7.6.1.1	Collect Road Use Charging Data	Pspec	
7.6.1.3	Bill Driver for Road Use Charges	Pspec	- RSE Toll Collection
7.6.1.4	Manage Road Use Charging Price Data	Pspec	- PAC Payment Administration
7.6.1.5	Manage Road Use Charges Processing	Pspec	- PAC Payment Administration
7.6.2	Support Road Use Charging	Pspec	
7.6.3	Provide Driver Road Use Charging Payment Interface	Pspec	
7.6.4	Provide Payment Device Interface for Road Use Charging	Pspec	

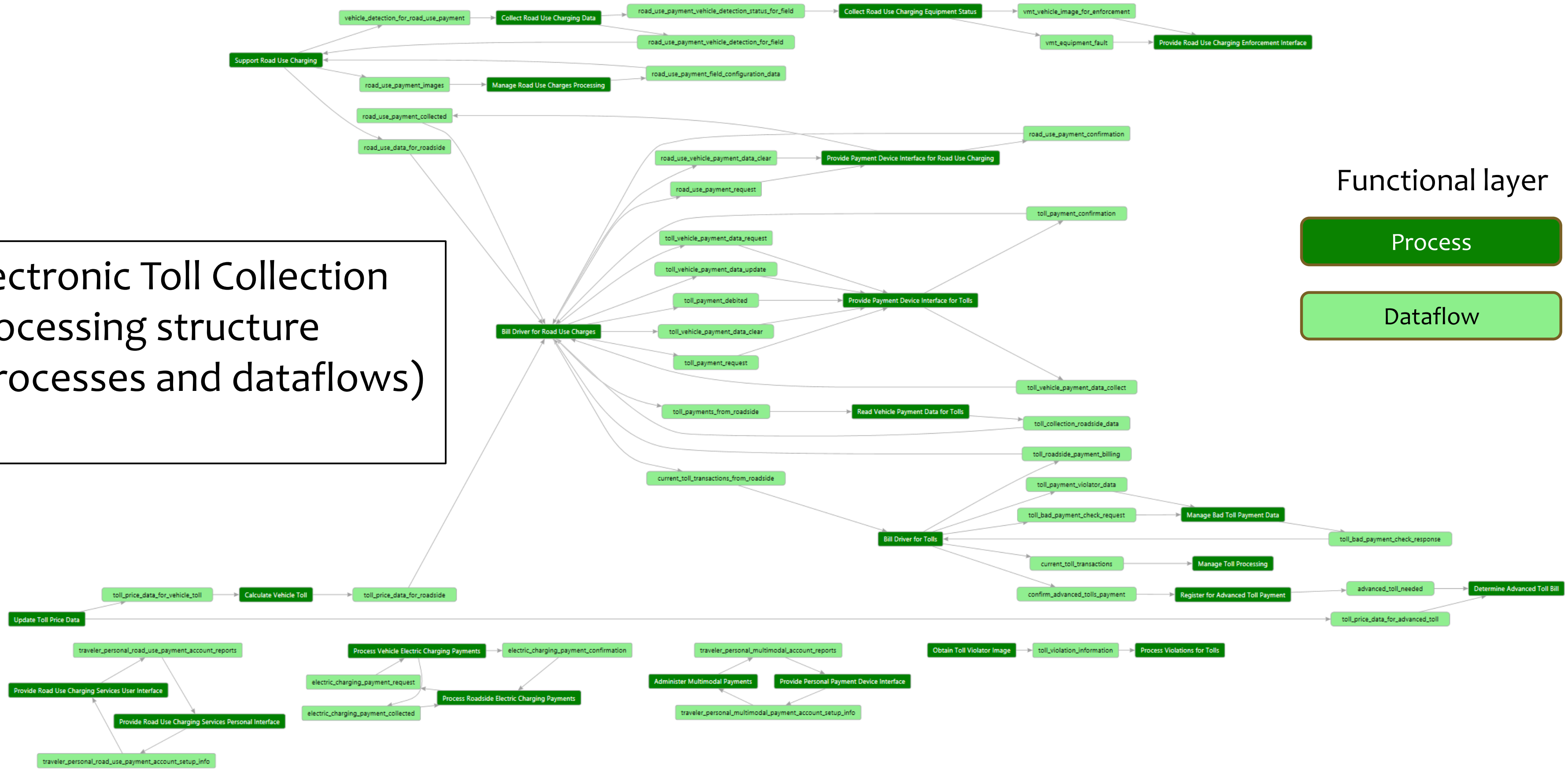
7.4.1.2	Process Travel Services Provider Payments
7.4.1.3	Process Driver Map Update Payments
7.4.1.4	Process Traveler Map Update Payments
7.4.1.5	Process Traveler Other Services Payments
7.4.1.6	Process Traveler Trip and Other Services Payments

Source Pspec	Data Flow	Destination Pspec
Administer Multimodal Payments	multimodal_payment_request_to_field	Bill Driver for Road Use Charges
Administer Multimodal Payments	multimodal_toll_payment_data	Manage Toll Processing
Administer Multimodal Payments	traveler_personal_multimodal_payment_request	Provide Personal Payment Device Interface
Administer Multimodal Payments	traveler_personal_multimodal_account_reports	Provide Personal Payment Device Interface
Bill Driver for Road Use Charges	multimodal_payment_confirmation_from_field	Administer Multimodal Payments
Bill Driver for Road Use Charges	current_toll_transactions_from_roadside	Bill Driver for Tolls
Bill Driver for Road Use Charges	road_use_payment_collected_from_field	Manage Road Use Charges Processing
		Manage Road Use
		Charging
Bill Driver for Road Use Charges	toll_vehicle_payment_data_request	Provide Payment Device Interface for Tolls
Bill Driver for Road Use Charges	toll_payment_debited	Provide Payment Device Interface for Tolls
Bill Driver for Road Use Charges	toll_payment_request	Provide Payment Device Interface for Tolls
Bill Driver for Road Use Charges	toll_vehicle_payment_data_clear	Provide Payment Device Interface for Tolls
Bill Driver for Road Use Charges	toll_vehicle_payment_data_update	Provide Payment Device Interface for Tolls
Bill Driver for Road Use Charges	toll_payments_from_roadside	Read Vehicle Payment Data for Tolls
Bill Driver for Tolls	toll_roadside_payment_billing	Bill Driver for Road Use Charges
Bill Driver for Tolls	toll_bad_payment_check_request	Manage Bad Toll Payment Data

Administer Multimodal Payments	multimodal_payment_request_to_field	Bill Driver for Road Use Charges
Administer Multimodal Payments	multimodal_toll_payment_data	Manage Toll Processing
Administer Multimodal Payments	traveler_personal_multimodal_payment_request	Provide Personal Payment Device Interface

Electronic Toll Collection – Functional View Processing Structure

Electronic Toll Collection Processing structure (processes and dataflows)



Support Road Use Charging
vehicle_detection_for_road_use_payment
Collect Road Use Charging Data
road_use_payment_vehicle_detection_status_for_field
Collect Road Use Charging Equipment Status
vmt_vehicle_image_for_enforcement
vmt_equipment_fault
Provide Road Use Charging Enforcement Interface
road_use_payment_vehicle_detection_for_field
road_use_payment_field_configuration_data
road_use_payment_images
Manage Road Use Charges Processing
road_use_payment_collected
road_use_data_for_roadside
road_use_payment_confirmation
road_use_vehicle_payment_data_clear
Provide Payment Device Interface for Road Use Charging
road_use_payment_request
toll_payment_confirmation
toll_vehicle_payment_data_request
toll_vehicle_payment_data_update
toll_payment_debited
Provide Payment Device Interface for Tolls
Bill Driver for Road Use Charges
toll_vehicle_payment_data_clear
toll_payment_request
toll_vehicle_payment_data_collect
toll_payments_from_roadside
Read Vehicle Payment Data for Tolls
toll_collection_roadside_data
toll_roadside_payment_billing
current_toll_transactions_from_roadside
toll_payment_violator_data
toll_bad_payment_check_request
Manage Bad Toll Payment Data
Bill Driver for Tolls
toll_bad_payment_check_response
current_toll_transactions
Manage Toll Processing
confirm_advanced_tolls_payment
Register for Advanced Toll Payment
advanced_toll_needed
Determine Advanced Toll Bill
toll_price_data_for_advanced_toll
toll_price_data_for_vehicle_toll
Calculate Vehicle Toll
toll_price_data_for_roadside
Update Toll Price Data
traveler_personal_road_use_payment_account_reports
Provide Road Use Charging Services User Interface
Provide Road Use Charging Services Personal Interface
traveler_personal_road_use_payment_account_setup_info
Process Vehicle Electric Charging Payments
electric_charging_payment_confirmation
electric_charging_payment_request
Process Roadside Electric Charging Payments
electric_charging_payment_collected
traveler_personal_multimodal_account_reports
Administer Multimodal Payments
Provide Personal Payment Device Interface
traveler_personal_multimodal_payment_account_setup_info
Obtain Toll Violator Image
toll_violation_information
Process Violations for Tolls

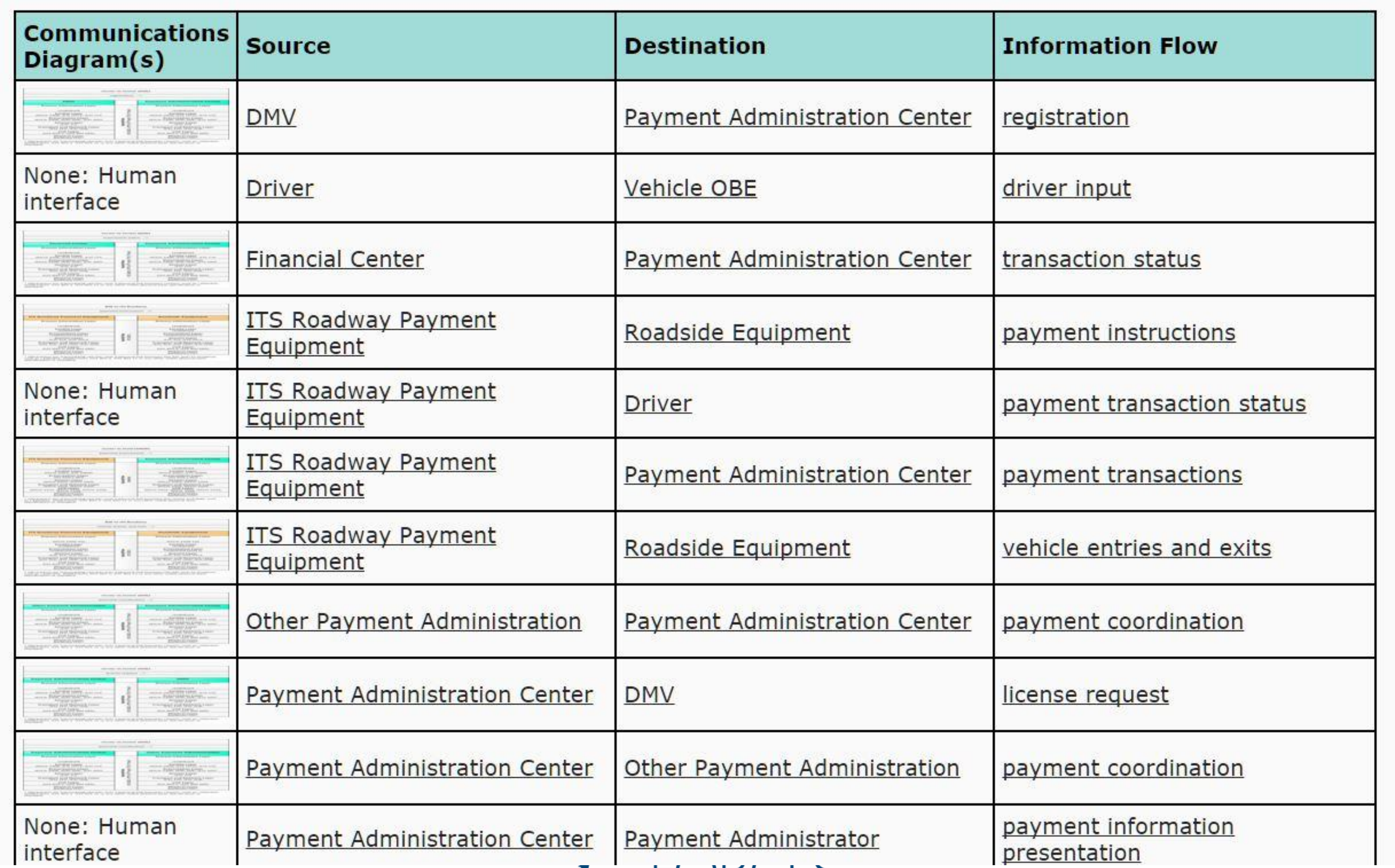
Functional layer

Process

Dataflow

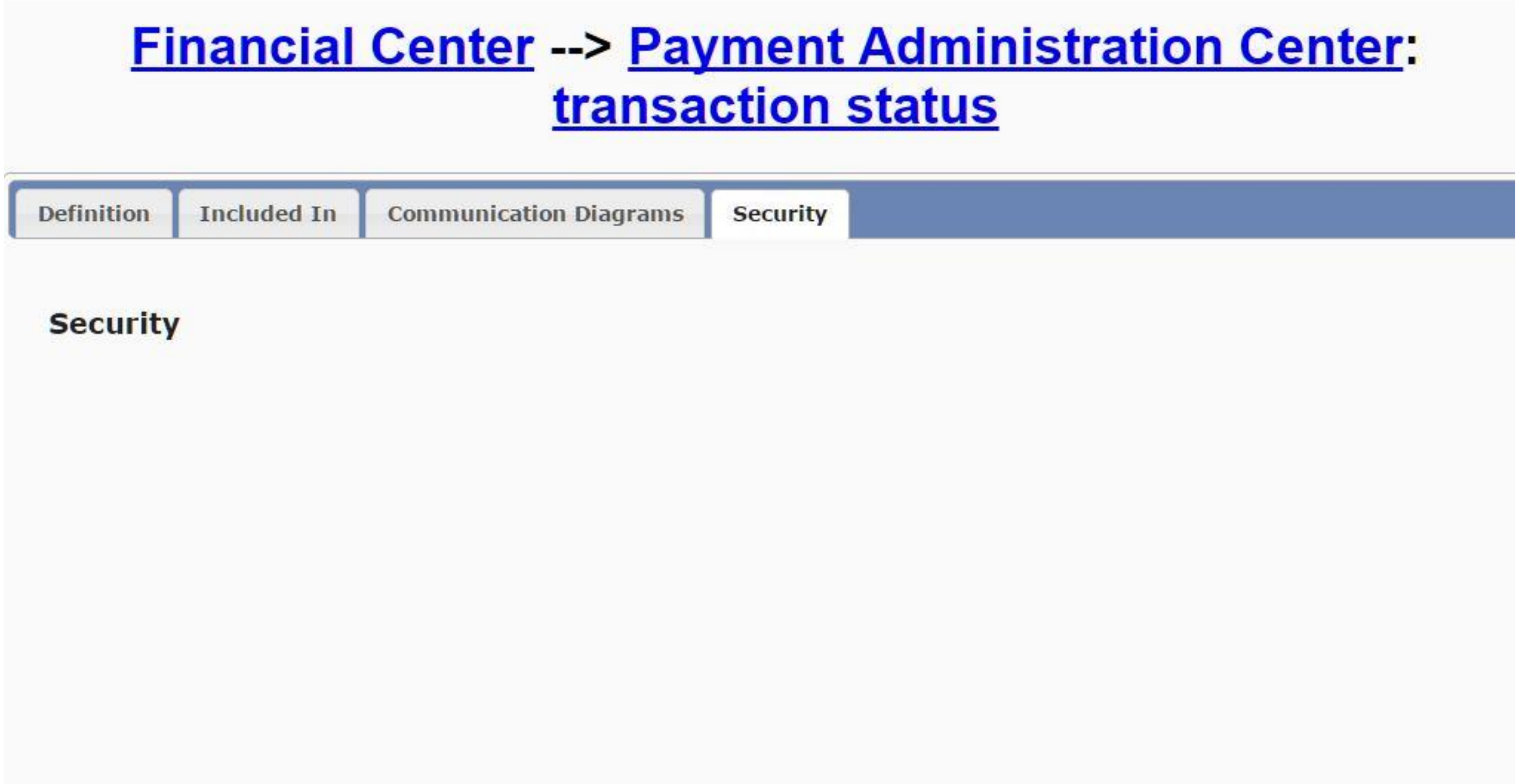
FORCES
FOUNDATIONS OF RESILIENT
CYBER-PHYSICAL SYSTEMS

Electronic Toll Collection – Communication View



Communications Diagram(s)	Source	Destination	Information Flow
	DMV	Payment Administration Center	registration
None: Human interface	Driver	Vehicle OBE	driver input
	Financial Center	Payment Administration Center	transaction status
	ITS Roadway Payment Equipment	Roadside Equipment	payment instructions
None: Human interface	ITS Roadway Payment Equipment	Driver	payment transaction status
	ITS Roadway Payment Equipment	Payment Administration Center	payment transactions
	ITS Roadway Payment Equipment	Roadside Equipment	vehicle entries and exits
	Other Payment Administration	Payment Administration Center	payment coordination
	Payment Administration Center	DMV	license request
	Payment Administration Center	Other Payment Administration	payment coordination
None: Human interface	Payment Administration Center	Payment Administrator	payment information presentation

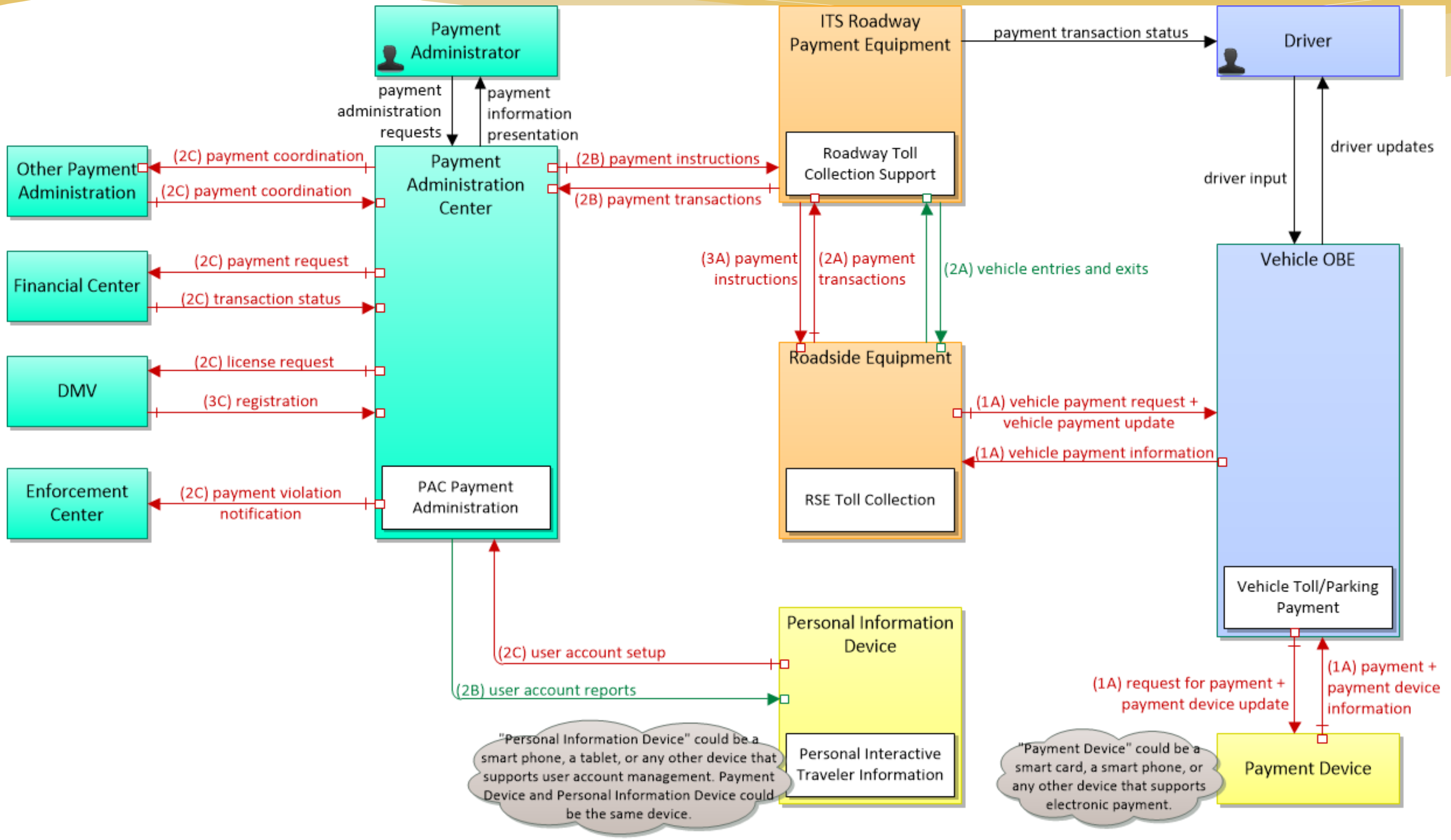
Electronic Toll Collection – Communication View Security



Financial Center --> Payment Administration Center: transaction status

Security

Electronic Toll Collection: Physical View Platform Architecture



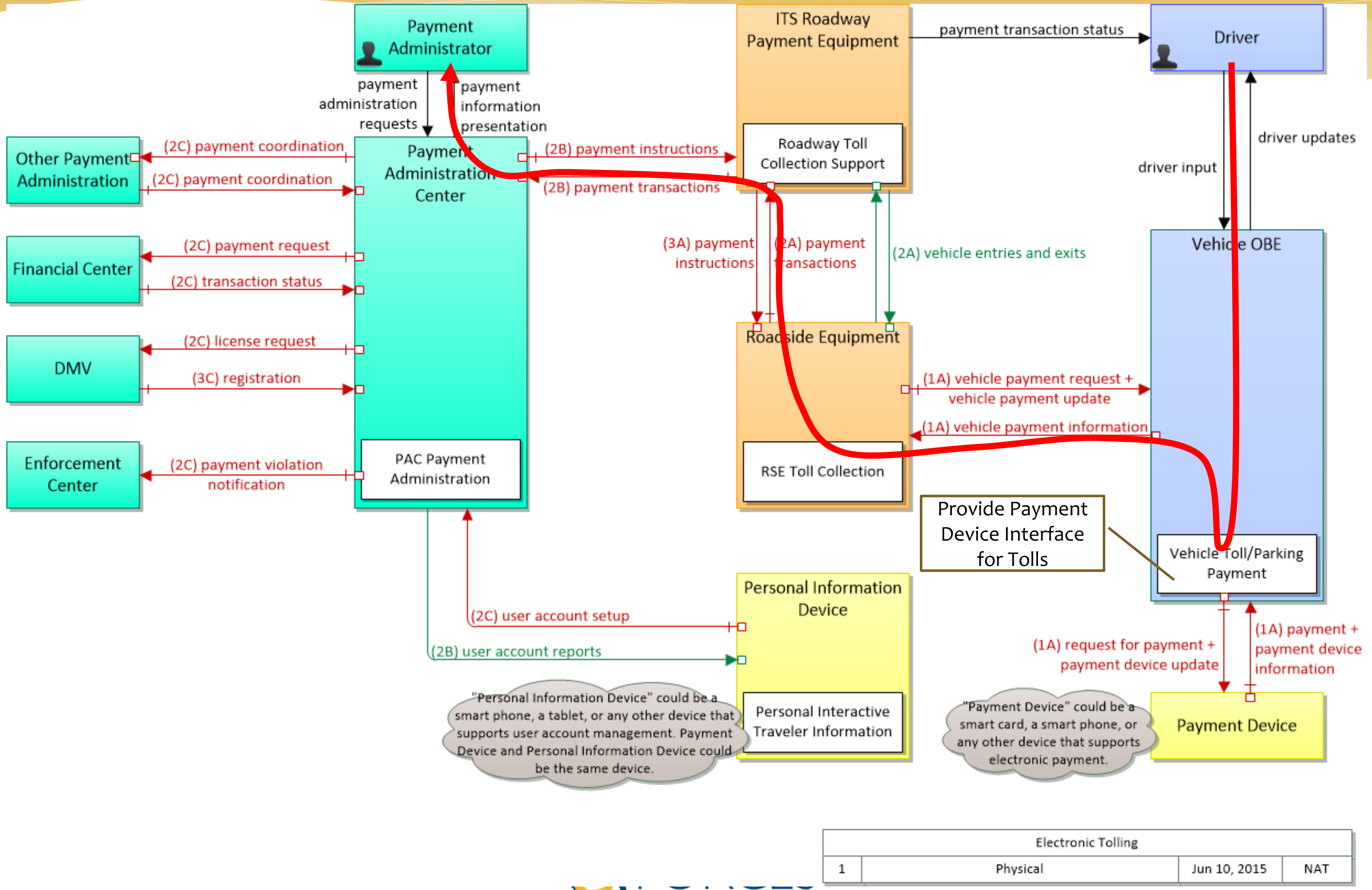
Payment Administrator
payment administration requests
payment information presentation
Other Payment Administration
(2C) payment coordination
(2C) payment coordination
Payment Administration Center
Financial Center
(2C) payment request
(2C) transaction status
DMV
(2C) license request
(3C) registration
Enforcement Center
(2C) payment violation notification
PAC Payment Administration
ITS Roadway Payment Equipment
Roadway Toll Collection Support
(2B) payment instructions
(2B) payment transactions
payment transaction status
Driver
driver input
driver updates
(3A) payment instructions
(2A) payment transactions
(2A) vehicle entries and exits
Roadside Equipment
(1A) vehicle payment request + vehicle payment update
(1A) vehicle payment information
RSE Toll Collection
Vehicle OBE
Vehicle Toll/Parking Payment
(2C) user account setup
(2B) user account reports
Personal Information Device
Personal Interactive Traveler Information
"Personal Information Device" could be a smart phone, a tablet, or any other device that supports user account management. Payment Device and Personal Information Device could be the same device.
(1A) request for payment + payment device update
(1A) payment + payment device information
"Payment Device" could be a smart card, a smart phone, or any other device that supports electronic payment.
Payment Device

http://www.iteris.com/cvria/html/applications/app109.html#tab-3

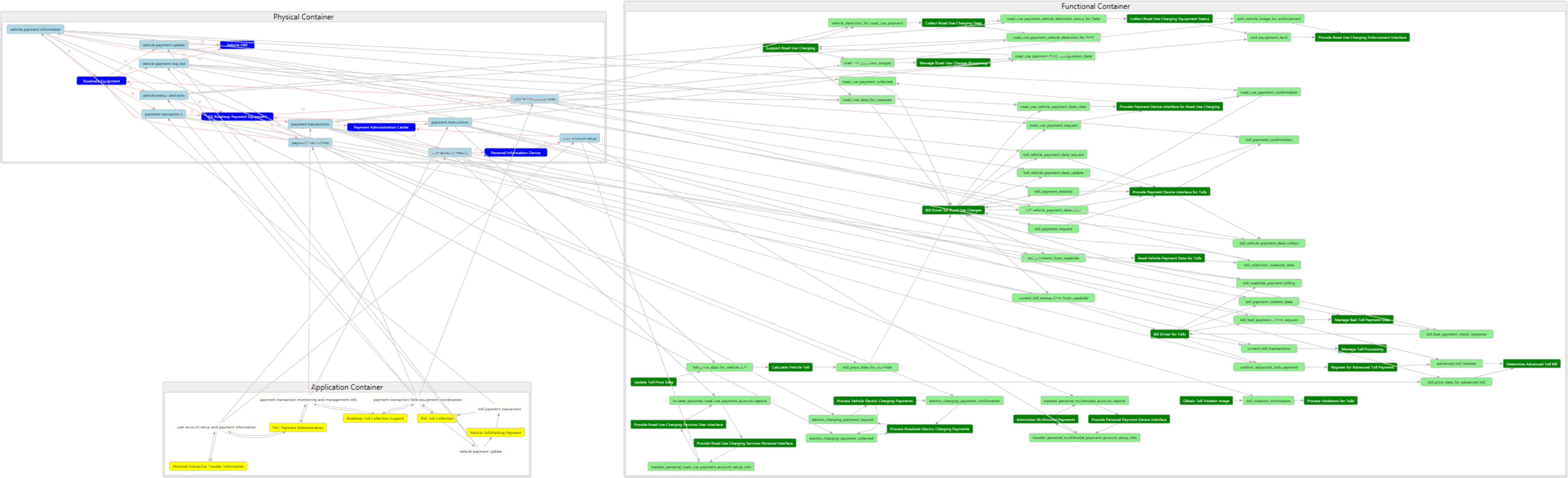
Electronic Tolling			
1	Physical	Jun 10, 2015	NAT

FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Dataflow Example


Payment Administrator
payment administration requests
payment information presentation
ITS Roadway Payment Equipment
Roadway Toll Collection Support
payment transaction status
Driver
driver input
driver updates
Other Payment Administration
(2C) payment coordination
(2C) payment coordination
Payment Administration Center
(2B) payment instructions
(2B) payment transactions
Financial Center
(2C) payment request
(2C) transaction status
(3A) payment instructions
(2A) payment transactions
(2A) vehicle entries and exits
Vehicle OBE
DMV
(2C) license request
(3C) registration
Roadside Equipment
(1A) vehicle payment request + vehicle payment update
(1A) vehicle payment information
Enforcement Center
(2C) payment violation notification
PAC Payment Administration
RSE Toll Collection
Provide Payment Device Interface for Tolls
Vehicle Toll/Parking Payment
Personal Information Device
(2C) user account setup
(2B) user account reports
(1A) request for payment + payment device update
(1A) payment + payment device information
"Personal Information Device" could be a smart phone, a tablet, or any other device that supports user account management. Payment Device and Personal Information Device could be the same device.
Personal Interactive Traveler Information
"Payment Device" could be a smart card, a smart phone, or any other device that supports electronic payment.
Payment Device
Electronic Tolling
1
Physical
Jun 10, 2015
NAT

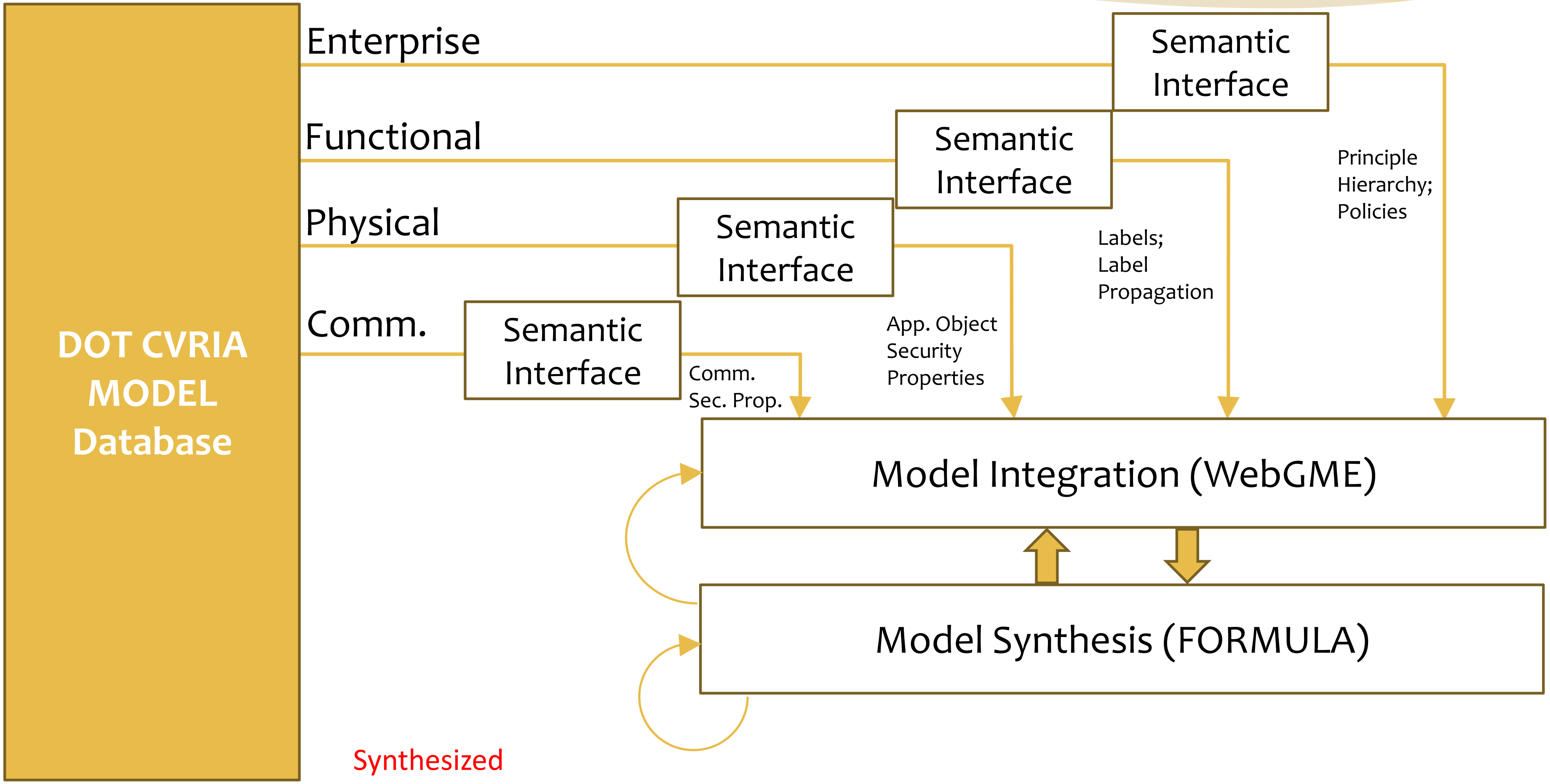
Electronic Toll Collection – A Glimps of Functional to Physical Deployment Mappings


Physical Container
vehicle payment information
vehicle payment update
Vehicle OBE
vehicle payment request
Roadside Equipment
vehicle entries and exits
payment transactions
US Roadway Payment Equipment
payment transactions
Payment Administration Center
payment instructions
vehicle entries and exits
payment instructions
user account setup
user account reports
Personal Information Device
U
Application Container
payment transaction monitoring and management info
payment transaction field equipment coordination
toll payment transaction
Roadway Toll Collection Support
RSE Toll Collection
user account setup and payment information
PAC Payment Administration
Vehicle Toll/Parking Payment
vehicle payment update
Personal Interactive Traveler Information
Functional Container
vehicle_detection_for_road_use_payment
Collect Road Use Charging Data
road_use_payment_vehicle_detection_status_for_field
Collect Road Use Charging Equipment Status
vmt_vehicle_image_for_enforcement
road_use_payment_vehicle_detection_for_field
vmt_equipment_fault
Provide Road Use Charging Enforcement Interface
Support Road Use Charging
road_use_payment_images
Manage Road Use Charges Processing
road_use_payment_field_configuration_data
road_use_payment_collected
road_use_payment_confirmation
road_use_data_for_roadside
road_use_vehicle_payment_data_clear
Provide Payment Device Interface for Road Use Charging
road_use_payment_request
toll_payment_confirmation
toll_vehicle_payment_data_request
toll_vehicle_payment_data_update
toll_payment_debited
Provide Payment Device Interface for Tolls
Bill Driver for Road Use Charges
toll_vehicle_payment_data_clear
toll_payment_request
toll_vehicle_payment_data_collect
toll_payments_from_roadside
Read Vehicle Payment Data for Tolls
toll_collection_roadside_data
toll_roadside_payment_billing
current_toll_transactions_from_roadside
toll_payment_violator_data
toll_bad_payment_check_request
Manage Bad Toll Payment Data
Bill Driver for Tolls
toll_bad_payment_check_response
current_toll_transactions
Manage Toll Processing
toll_price_data_for_vehicle_toll
Calculate Vehicle Toll
toll_price_data_for_roadside
confirm_advanced_tolls_payment
Register for Advanced Toll Payment
advanced_toll_needed
Determine Advanced Toll Bill
Update Toll Price Data
toll_price_data_for_advanced_toll
traveler_personal_road_use_payment_account_reports
Process Vehicle Electric Charging Payments
electric_charging_payment_confirmation
traveler_personal_multimodal_account_reports
Obtain Toll Violator Image
toll_violation_information
Process Violations for Tolls
Provide Road Use Charging Services User Interface
electric_charging_payment_request
Administer Multimodal Payments
Provide Personal Payment Device Interface
Process Roadside Electric Charging Payments
Provide Road Use Charging Services Personal Interface
electric_charging_payment_collected
traveler_personal_multimodal_payment_account_setup_info
traveler_personal_road_use_payment_account_setup_info

Scaling

Applications	Applications	101	E.g.: Electronic Toll Collection
	Application objects	245	RSE Toll Collection, PAC Payment Administration,..
	Information flows	436	Driver Input, Payment Coordination,..
Physical View	Physical objects	112	Payment Device, Payment Administrator,..
	Information flows	1076	Payment Device Update, Payment Transactions,…
Functional View	Processes	609	Calculate Vehicle Toll, Collect Advanced Payments,..
	Dataflows (flattened)	8556	Toll Payment Debited, Toll Payment Request,..

Validation Workflow for System-level Design Using CVRIA



Synthesized Deployment Model

FORCES FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Next Steps

- Completion of 2 CVRIA application examples, one of them is time sensitive
- Completion of the synthesis tasks
- Running performance evaluations (how security policies influence timing properties of application execution)