Concept of Operation

ConOps: Key Concepts

1. Test Bed Geographic Reference

2. Data Context

3. Security, Privacy by Design

4. Data Exchange Pattern

5. Data Bundles

ConOps: Key Concepts

Geographic Reference

- The Test Bed is defined by a 2 degree by 3 degree rectangle
- Overlay grid of 10 millidegree^2 "tiles"
- This yields 60,000 identically sized and shaped tiles
- Each tile is identified by a pair of geo reference points for the NW and SE corners of the tile.
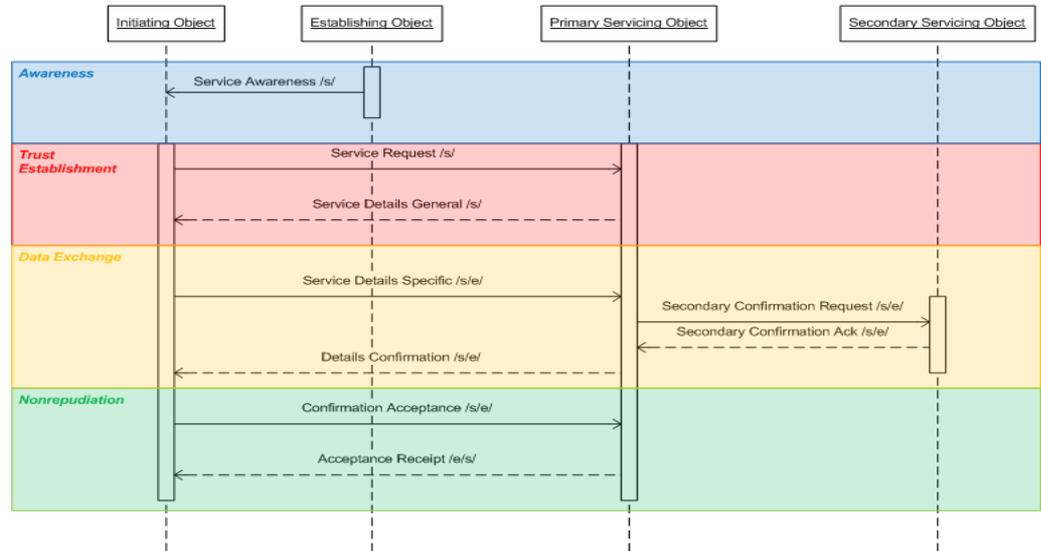
ConOps: Concept - Security by Design

Security and Privacy by Design are guiding principles and two of the foundational concepts behind the goals and overall design of the Unified implantation of the CVRIA in Michigan.

ConOps: Concept - Data Exchange Pattern

- Each Information Flow will follow this pattern

- There are four stages of the pattern

Service Awareness ►

Trust Establishment ►

Data Exchange ►

Non-Repudiation ►

Phases of a Peer-to-Peer Data Exchange Message Sequence

| Initiating Object | Establishing Object | Primary Servicing Object | Secondary Servicing Object |

Awareness
Service Awareness /s/

Trust Establishment
Service Request /s/
Service Details General /s/

Data Exchange
Service Details Specific /s/e/
Secondary Confirmation Request /s/e/
Secondary Confirmation Ack /s/e/
Details Confirmation /s/e/

Nonrepudiation
Confirmation Acceptance /s/e/
Acceptance Receipt /e/s/

ConOps: Concept - Bundles

- Individual data objects (records) can be concatenated into a single consolidated data object call a "bundle"
- Contents of the APDU Header and APDU Body will be tailored for each information flow.

  □ Security Header
  □ APDU Header
  □ APDU Body
  □ Security Trailer

- Contents of the Bundle Header and Bundle Main Body will be tailored for each information flow.

Header Segment		1609.2 Header	
		APDU Type = (see table below)	
		Body Length	
		Bundle Generation Time	
		Bundle Generation Location	
		Total Bundle Count	
Body Seg.	SAE J2735 EVSM 1	Safety Pilot BSM	Other Data Elements
	SAE J2735 EVSM 2	Safety Pilot BSM	Other Data Elements
	SAE J2735 EVSM 3	Safety Pilot BSM	Other Data Elements
	SAE J2735 EVSM 4	Safety Pilot BSM	Other Data Elements
	SAE J2735 EVSM 5	Safety Pilot BSM	Other Data Elements
	SAE J2735 EVSM 6	Safety Pilot BSM	Other Data Elements
	SAE J2735 EVSM 7	Safety Pilot BSM	Other Data Elements
	SAE J2735 EVSM 8	Safety Pilot BSM	Other Data Elements
		1609.2 Trailer	

ConOps: Information Flows

Information flows will be described in a consistent framework…

- A tailored Message Sequence Diagram will be presented.
- Each of the four phases of the tailored message sequence will be sequentially described.
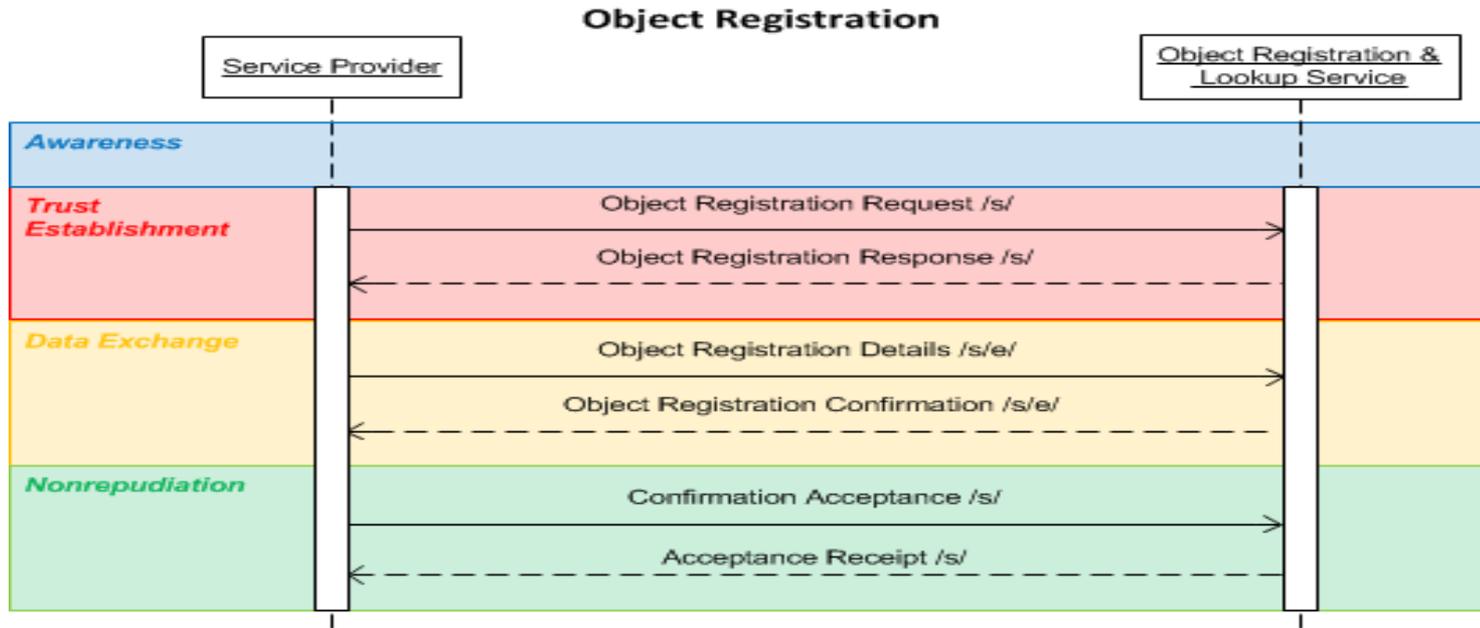- Each phase description may include a high level description of message contents
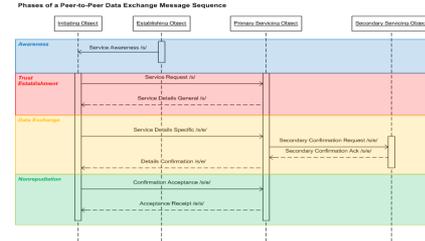
Phases of a Peer-to-Peer Data Exchange Message Sequence

Object Registration – Trust Establishment

The Object Registration – Trust Establishment function provides a mechanism for a Southeast Michigan Test Bed objects to register with the Object Registration & Discovery Service their intent to have other Test Bed object made aware of their service offering.
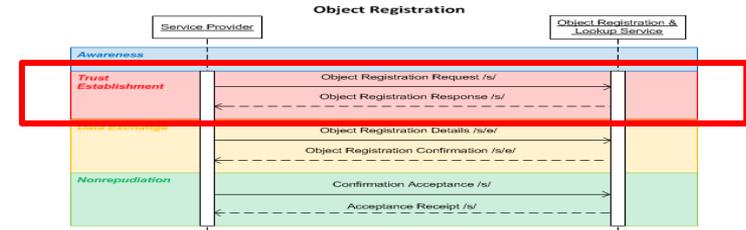
Trust establishment will require that the Test Bed object previously obtain the appropriate security credential from the Security Credential Management Service (SCMS). Registered objects do not need to unregister, as the registration itself has a specified lifespan. Using the appropriate security credentials, the Test Bed object will generate, sign and send the following Service Registration Request Message to the Object Registration & Discovery Service.

Field	Description
EVSD Type[1]	- "Fundamental EVSM Bundle Deposit" indicating that each record consists of Safety Pilot BSM & Other Data Elements - "Road Weather EVSM Bundle Deposit" indicating that each record consists of the Safety Pilot BSM & Road Weather Data Elements - "Environment EVSM Bundle Deposit" indicating that each record consists of the Safety Pilot BSM & Environmental Data Elements - "Electrical Vehicle EVSM Bundle Deposit" – indicating that each record consists of the Safety Pilot BSM & Electrical Vehicle Data Elements
Bundle Generation Time	The timestamp of when the bundle was generated. Bundles with a Bundle Generation Time value indicating that the bundle was generated before the time threshold based on the current value of the configurable (default 20 minutes) "EVSD Bundle Life Span" interval will be discarded.
Bundle Generation Location	The geographical location where the bundle was generated. Bundles with a Bundle Generation Location value indicating that the bundle was generated outside the defined Southeast Michigan Test Bed geographic region will be discarded. Bundles with a Bundle Generation Location value indicating that the bundle was generated within the defined Southeast Michigan Test Bed geographic region will be accepted.
Total Bundle Count	The number of bundles that are part of the delivery. This field is not used for bundle deposits, as each deposited bundle will be sent in a separate transaction.
EVSD Messages	One or more Enhanced Vehicle Situation Data Messages of the type indicated in EVSD Type

U.S. Department of Transportation

ConOps: Object Registration Flow

Object Registration

| Service Provider | Object Registration & Lookup Service |

Awareness

Trust Establishment
- Object Registration Request /s/
- Object Registration Response /s/

Data Exchange
- Object Registration Details /s/e/
- Object Registration Confirmation /s/e/

Nonrepudiation
- Confirmation Acceptance /s/
- Acceptance Receipt /s/

ConOps: Object Registration Flow *(TE 2 of 2)*

Object Registration – Trust Establishment

The Object Registration – Trust Establishment function provides a mechanism for a Southeast Michigan Test Bed objects to register with the Object Registration & Discovery Service their intent to have other Test Bed object made aware of their service information. Trust establishment will require that the Test Bed object have previously obtained the appropriate security credential from the Security Credential Management Service (SCMS). Registered objects do not need to unregister, as the registration itself has a specified lifespan. Using the appropriate security credentials, the Test Bed object will generate, sign and send a Service Registration Request to the Object Registration & Discovery Service. It will include a temporary "Flow Identifier" token which will subsequently be used to "tag" the various transactions in this information flow.

The Object Registration & Discovery Service will authenticate the signature and validate the Service Registration Request. The validation result will be included in an Object Registration Response, which will be returned to the registering Test Bed object. The Test Bed object will authenticate the signature and validate the Object Registration Response. At this point in the information flow, either the flow has been terminated due to an error condition or both entities have established trust.

Deposit of Enhanced Vehicle Situation Data Bundles

ConOps: EVSD Deposit Flow *(DX 2 of 4)*

Deposit of Enhanced Vehicle Situation Data Bundles
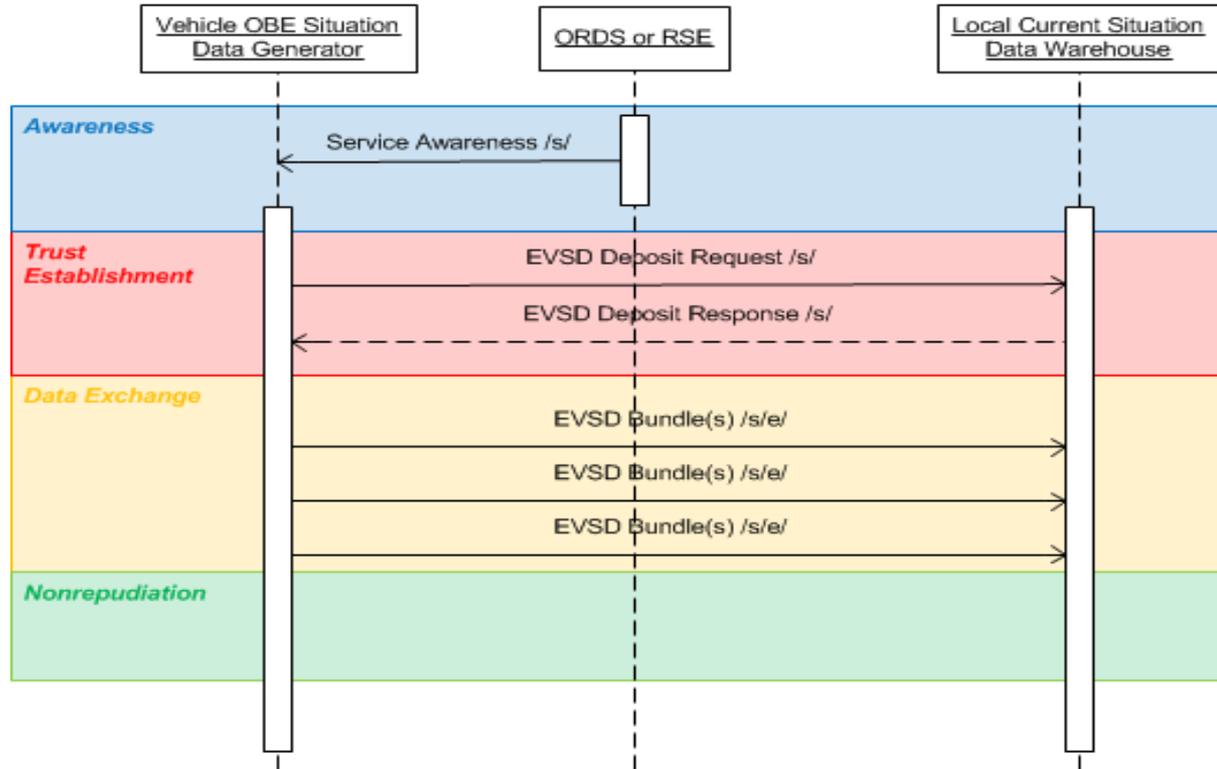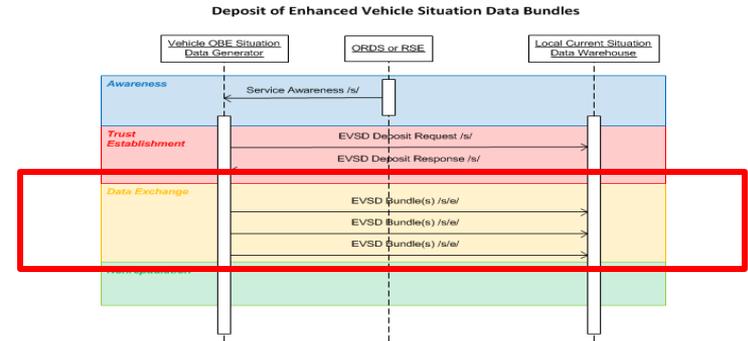
Enhanced Vehicle Situation Data Bundle Deposit – Data Exchange

The Local Current Situation Data Bundle Deposit function is the process by which authorized Vehicle OBE Situation Data Generation objects will deposit their bundles at the Local Current Situation Data Warehouse; and the Local Current Situation Data Warehouse receives and authenticates incoming bundles.

The Local Current Situation Data Warehouse will validate and authenticate all received situation data bundles. It is incumbent upon each provider to maintain awareness of its credential state and to proceed accordingly. Parsing and validation of received bundles will be constrained to the structure and contents of the bundle header and trailer segments.

ConOps: EVSD Deposit Flow (DX 3 of 4)

Bundles with an improperly formatted header/trailer or with invalid header/trailer contents will be discarded. Bundles which cannot be authenticated by supporting security services will be discarded. A record of each bundle discard along with required metadata will be generated and captured.

The logical structure of the Enhanced Vehicle Situation Data Bundle is shown below. Please note that the final number of records per bundle will be chosen to keep the overall message file that contains the bundles to something that will fit into 8-10 IEEE 802.2 segments. This might vary somewhat based on the particular bundle type.

ConOps: EVSD Deposit Flow *(DX 4 of 4)*

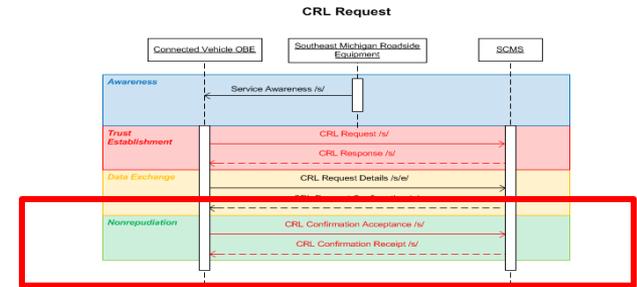| Field	Description
EVSD Type[1]	'Fundamental EVSM Bundle Deposit" indicating that each record consists of Safety Pilot BSM & Other Data Elements "Road Weather EVSM Bundle Deposit" indicating that each record consists of the Safety Pilot BSM & Road Weather Data Elements "Environment EVSM Bundle Deposit" indicating that each record consists of the Safety Pilot BSM & Environmental Data Elements "Electrical Vehicle EVSM Bundle Deposit" – indicating that each record consists of the Safety Pilot BSM & Electrical Vehicle Data Elements
Bundle Generation Time	The timestamp of when the bundle was generated. Bundles with a Bundle Generation Time value indicating that the bundle was generated before the time threshold based on the current value of the configurable (default 20 minutes) "EVSD Bundle Life Span" interval will be discarded.
Bundle Generation Location	The geographical location where the bundle was generated. Bundles with a Bundle Generation Location value indicating that the bundle was generated outside the defined Southeast Michigan Test Bed geographic region will be discarded. Bundles with a Bundle Generation Location value indicating that the bundle was generated within the defined Southeast Michigan Test Bed geographic region will be accepted.
Total Bundle Count	The number of bundles that are part of the delivery. This field is not used for bundle deposits, as each deposited bundle will be sent in a separate transaction.
EVSD Messages	One or more Enhanced Vehicle Situation Data Messages of the type indicated in EVSD Type

CRL Request

CRL Request

SCMS — CRL Retrieval — Non-Repudiation

Non-repudiation will require that the querying Test Bed object generate, sign, and send a CRL Confirmation Acceptance to the SCMS. It will contain a unique identifier derived from the received CRL Request Confirmation. The SCMS will authenticate the signature and validate the CRL Confirmation Acceptance. Validation results will be indicated in the CRL Confirmation Status and embedded into the CRL Confirmation Receipt, which will be generated and returned to the registering Test Bed object.   The exchange of the CRL Confirmation Acceptance and CRL Confirmation Receipt are new information flow transactions between the requesting Test Bed object and the SCMS. They were not defined in the SCMS Design document for the SPMD, and therefore, are indicated in red in the information flow diagram (Figure 12).

ConOps: Example Operational Scenarios

1. **Vehicle Situation Data** …generated by a CV OBEs and deposited in the Situation Data Clearinghouse. Delivered, based on subscribed criteria to the Situation Data Processing Center, and possibly one or more Third Party Application Centers

2. **Traveler Situation Data Broadcast** …an traveler (advisory) message and its associated dispatch instructions are generated by the Situation Data Processing Center or a Third Party Application Center and send to the Situation Data Warehouse.   The Warehouse validates and sorts these messages into data stores based on the geographic area associated with the advisory message.   Each RSE periodically requests advisory messages within a geographic boundary and constructs a radio "playlist" based on each messages dispatch instructions. Passing vehicles are able to receive these messages.

ConOps: Example Operational Scenarios

3. **Traveler Situation Data Broadcast** …an traveler (advisory) message and its associated delivery instructions are generated by the Situation Data Processing Center or a Third Party Application Center and send to the Regional Historic Situation Data Warehouse.   The Warehouse validates and sorts these messages into data stores based on the geographic boundary associated with the advisory message.   Connected Vehicles may periodically requests advisory messages within a geographic boundary. The Warehouse will bundle and deliver these messages to the requesting vehicle.

4. **Field Situation Data** …RSEs will generate periodic snapshots of Signal Phase & Timing (SPaT) messages. These will be bundled by each RSE, along with the current MAP, and deposited at the Regional Historic Situation Data Warehouse. Connected Vehicles may periodically requests advisory messages within a geographic boundary. The Warehouse will bundle and deliver these messages to the requesting vehicle.

Before and After
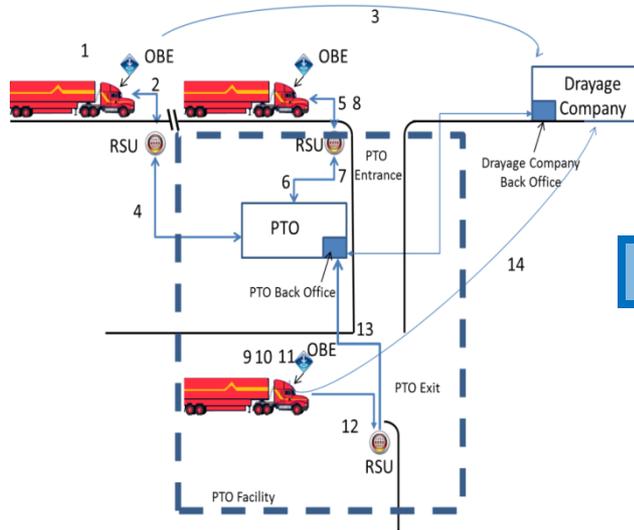
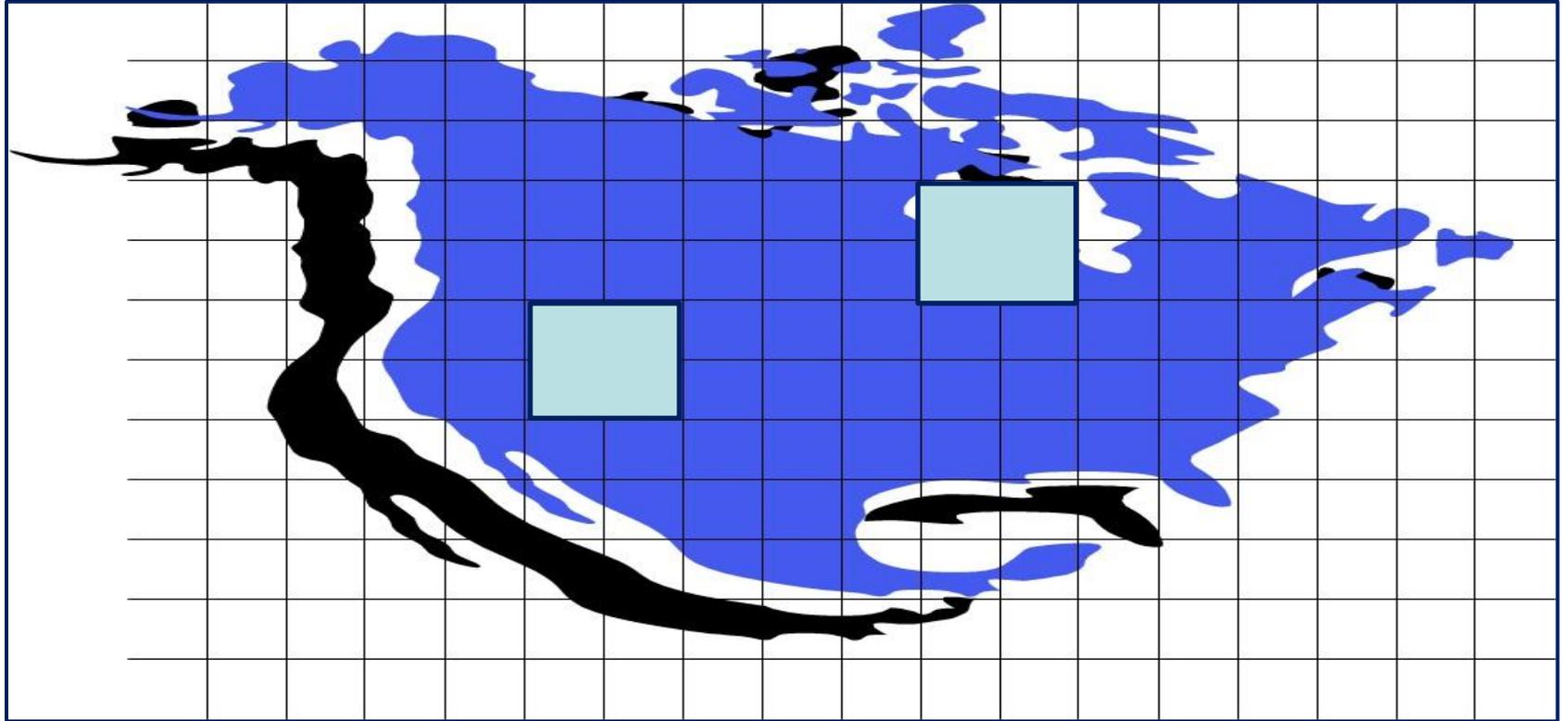**Standalone System**
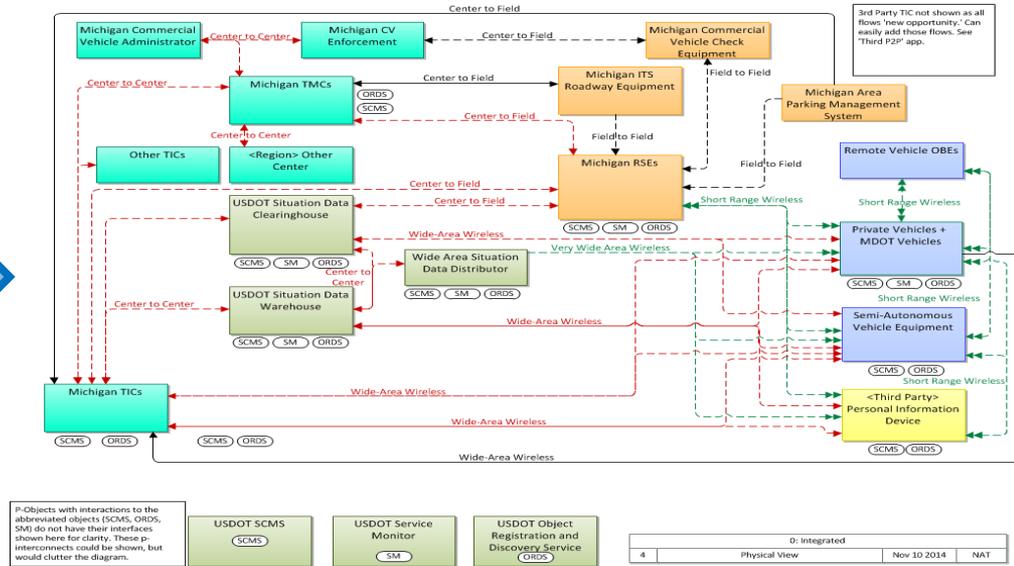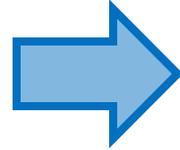
Part of the Reference Implementation

Operational Scenario

- Transaction type applications accomplished with shared physical objects in vehicles
  - Objects installed for crash avoidance
  - Include location awareness, human interface, and radio services
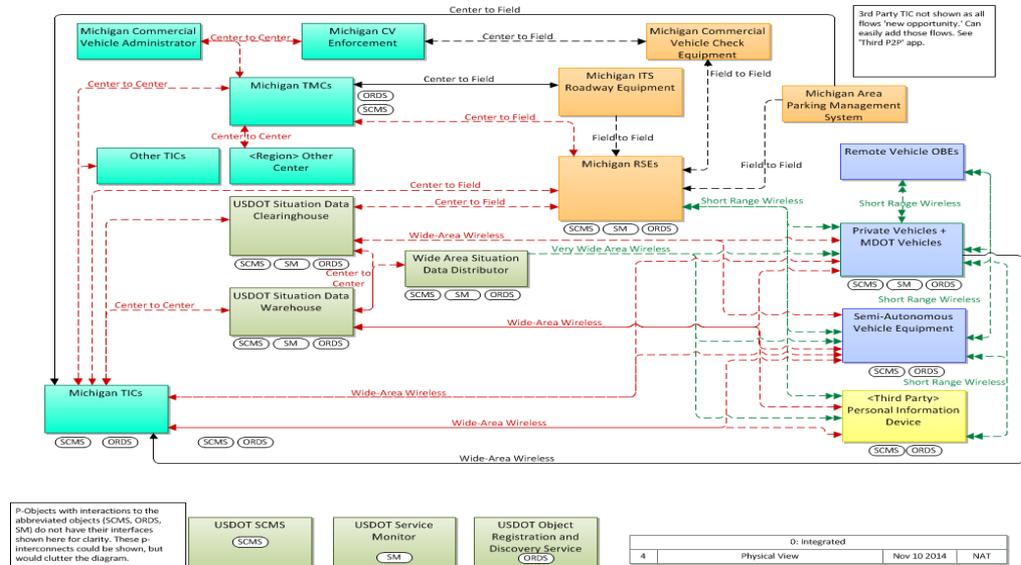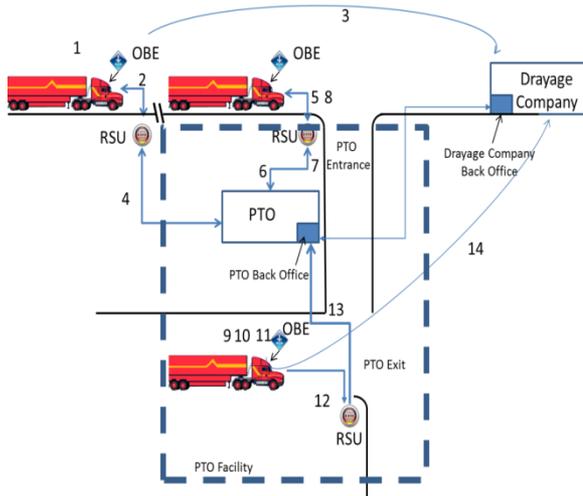 - Create unique application objects to serve application needs

Awareness

Trust Establishment

- Use anonymous messages signed with 1609.2 certificates

Data Exchange

- Common application data protocol units nationwide
- Standards-based data unit definitions
  - Example: Commercial Vehicle Operations

Non-Repudiation

- Equal record nationwide

Cyber Physical Systems – Virtual Organization