CVRIA and ITS Station Primer

1 Background

1.1 Connected Vehicle Reference Implementation Architecture

The USDOT initiated the development of the Connected Vehicle Reference Implementation Architecture (CVRIA) in order to accomplish three main goals:

1) Define a common framework (i.e. an architecture) for implementation of connected vehicle functions and interfaces, consistent with the National ITS Architecture
2) Identify and prioritize interfaces for standards development
3) Provide input to analysis to produce a policy foundation for architecture, standards, and certification

The CVRIA presents the Architecture of the Connected Vehicle Environment (CVE). While the architecture presents the CVE's functionality, the relationships that enable applications and the physical devices that implement them, all of these things are viewed through the lens of the applications that provide services to participants in the CVE:

To the CVRIA, an application is a connected vehicle application if:

1) The application uses an interface that passes data originating from an entity whose identity is independently authenticated but not necessarily known, and
2) That interface attaches to at least one entity in the transportation environment.

Using this definition, a proprietary signal control application, or transit management application that might be deployed today in a closed environment is not a connected vehicle application, while a similar application that relied on 3rd party authentication would be. The notion of 3rd party authentication as the basis for security has roots in the Internet and has been a part of connected vehicle and previous related program research for over a decade. This basic concept, that some*thing* is trustworthy, but that it does not need to be identified to the party that requires to trust that *thing*, is the underlying enabler in an environment where it is impractical for all those interacting to form personal relationships (e.g., you will never know the identities of most of the drivers around you).

Applications and supporting functionality were identified based on the various research activities underway and completed as part of the Research and Innovative Technology Administration's (RITA) connected vehicle research program. The architecture was constructed by examining these activities and producing a baseline definition for each application based on its likely implementation. These baseline definitions present a likely, but not the only method, for implementing a given application. Typically, the farther into the operational transportation environment one goes, the more variability one could expect in eventual implementation. Thus center-focused applications are more likely to be implemented as expected in the architecture, while vehicle-based applications expect more variability.

Primary sources of application concepts and needs were:

- Vehicle-to-vehicle (V2V) safety applications documented in the VSC-A Final Report
- Vehicle-to-infrastructure (V2I) safety applications documented in various V2I Concepts of Operations produced for USDOT
- Mobility applications documented in the Concepts of Operations developed under the Dynamic Mobility Applications program
- Environmental applications documented as part of the AERIS program
- Supporting functions described as part of the Core System systems engineering work, as well as the Security Credentials Management System implemented for the Model Deployment Safety Pilot
- Various other safety, mobility and environmental applications considered as part of the J2735 Systems Engineering draft

The CVRIA uses ISO/IEC/IEEE 42010:2011: Systems and software engineering – Architecture description as a framework for architecture construction. The CVRIA represents the CVE in four ways:

1) It describes the context in which applications operate by defining the enterprise interactions that affect application development, deployment, operations and maintenance in the Enterprise Viewpoint.
2) It describes the functions and data exchanges necessary to enable applications in the Functional Viewpoint.
3) It describes the physical entities that implement the functions and data exchanges in the Physical Viewpoint.
4) It defines the layered communications environment that applications use to deliver services in the Communications Viewpoint.

1.2 ITS Station Architecture

ETSI/CEN/ISO have produced a large body of standards work, and standards in development aimed to produce a set of communication standards for Co-operative Intelligent Transport Systems (C-ITS). ISO/CEN has documented architecture, communications and facilities of C-ITS in a series of ISO standards, while the ETSI has standardized a compatible variant in ETSI TC ITS.

ETSI/CEN/ISO does have a singular release 1, which includes a set of standards in support of applications, message and data specifications, application and message support, and conformance testing. This set of 44 standards focuses on communications and the interfaces between devices, as well as the management and security services necessary on board those devices. (This is a simplification; some of these standards speak of *functionalities*, not devices, but in order to implement a standard you need a *thing*). They identify an additional 27 pre-existing ITS-related standards that are more focused on traditional ITS and applications but are (or may be) related to ITS Station concepts.

ETSI/CEN/ISO's focus on the abstract begins with the definition of its node of concern: the bounded, secured, managed domain (BSMD). The BSMD that participates in C-ITS, aka the ITS Station, is the primary topic of concern for these standards and for the subsequent analysis in this primer.

2 References

2.1 CVRIA reference material

1. The Connected Vehicle Reference Implementation Architecture, http://www.iteris.com/cvria
2. Accelerated Vehicle to Infrastructure (V2I) Safety Applications Concept of Operations, Revised Draft, 5/29/2012
3. Accelerated Vehicle to Infrastructure (V2I) Safety Applications System Requirements Document, 6/18/2012
4. Border Information Flow Architecture, 5/16/2012
5. CCSDS 311.0-M-1 – Reference Architecture for Space Data Systems, Recommended Practice, September 2008
6. Concept Development and Needs Identification for Intelligent Network Flow Optimization (INFLO) Concept of Operations, Draft V3.0, 6/14/2012
7. Concept of Operations for Road Weather Connected Vehicle Applications, Draft V1.4.2, 6/26/2012
8. Concept of Operations for Transit Connected Vehicle, 3/31/2012
9. Concept of Operations: Data Capture and Management Research Data Exchange, 8/3/2011
10. Connected Vehicle Safety Applications for Highway Rail Intersections Concept of Operations, 9/21/2012
11. Core System Concept of Operations, 10/24/ 2011
12. Core System System Architecture Document (SAD), Revision C, 10/14/2011
13. Dynamic Eco-Lanes: Operational Concept, V1.1, 8/12/2012
14. Dynamic Low-Emissions Zones: Operational Concept, V1.1, 8/12/2012
15. Eco-Signal Operations: Operational Concept, V1.1, 8/12/2012
16. Freight Advanced Traveler Information System (FRATIS) Concept of Operations, Final 4/20/2012
17. Harmonization Task Group #1 Deliverable #1, Current Status of Security Standards, 8/29/2012
18. ISO/IEC/IEEE 42010 – Systems and software engineering – architecture description, 12/01/2011.
19. Integrated Dynamic Transit Operations (IDTO) Concept of Operations, Final V3.0, 5/11/2012
20. J2735 Systems Engineering Version, Candidate Standard for Consideration by SAE, Version v01, 12/15/2012
21. Multi-Modal Intelligent Signal System (MMITSS) Concept of Operations, V2.0, 9/14/2012
22. Object Management Group (OMG) Systems Modeling Language (OMG SysML^{TM}), version 1.1, November 2008
23. R.E.S.C.U.M.E. (Response, Emergency Staging and Communications, Uniform Management, and Evacuation) Concept of Operations, V1.0, 5/29/2012
24. Safety Pilot System Requirements Description, Roadside Equipment, V1.2, 1/19/2011
25. Safety Pilot System Requirements Description, Vehicle Awareness Devices, V3.6, 1/25/2012

26. Security Credential Management System Design, 4/13/2012
27. Signal Phase & Timing and Related Messages for V-I Applications Concept of Operations, Draft, 8/8/2011
28. Smart Roadside Initiative Concept of Operations, 5/21/2012
29. The Vehicle Data Translator V3.0 System Description (FHWA-JPO-11-127), V3.0, 5/1/2011
30. V2I Safety Concept of Operations, 8/10/2012
31. Vehicle Information Exchange Needs for Mobility Applications White Paper (FHWA-JPO-12-021), Final, 2/13/2012
32. Vehicle Infrastructure Integration (VII) Privacy Policies Framework, Version 1.0.2, February 16, 2007
33. Vehicle Safety Communications – Applications Final Report, 9/1/2011
34. Vision and Operational Concept for Enabling Advanced Traveler Information Services (Enable ATIS), Final 5/13/2012

2.2 ITS Station Architecture

1. ISO TC204 WG16 workspace: http://calm.its-standards.info
2. ETSI TCITS Working Portal: http://portal.etsi.org/its
3. CEN/ISO TS 17425, Intelligent Transport Systems - Co-operative systems - Data exchange specification for in-vehicle presentation of external road and traffic related data
4. CEN/ISO TS 17426, Intelligent Transport Systems - Cooperative Systems - Contextual speeds
5. CEN/ISO TS 17427, Intelligent Transport Systems - Cooperative Systems - Roles and responsibilities in the context of co-operative ITS based on architecture(s) for co-operative systems
6. CEN/ISO TS 18750, Intelligent Transport Systems - Cooperative ITS - Definition of a global concept for local dynamic maps
7. CEN/ISO TS 19091, Intelligent Transport Systems - Cooperative ITS - Using V2I and I2V Communications for Applications Related to Signalized Intersections (SPaT, MAP, SRM, SSM)
8. CEN/ISO TS 19321, Intelligent Transport Systems - Cooperative ITS - Dictionary of In-vehicle Information (IVI) data structures
9. ISO 16788, Intelligent Transport Systems - Communications access for land mobiles (CALM) - ITS IPv6 Security
10. ISO 16789, Intelligent Transport Systems - Communications access for land mobiles (CALM) - ITS IPv6 Optimization
11. CEN/ISO TS 17419, Intelligent Transport Systems - Cooperative Systems - Classification and management of ITS applications in a global context
12. CEN/ISO TS 17423, Intelligent Transport Systems - Cooperative Systems - Application requirements for selection of communication profiles
13. TS 17429, Intelligent Transport Systems - Cooperative Systems - Profiles for processing and transfer of information between ITS stations for applications related to transport infrastructure management, control and guidance
14. ISO 17515-1, Intelligent Transport Systems - Communications access for land mobiles (CALM) - LTE

15. ISO 21210, Intelligent Transport Systems - Communications access for land mobiles (CALM) - IPv6 Networking
16. ISO 21215, Intelligent transport systems - Communications access for land mobiles (CALM) - M5
17. ISO 21217, Intelligent Transport Systems - Communications access for land mobiles (CALM) - Architecture
18. ISO 21218, Intelligent Transport Systems - Communications access for land mobiles (CALM) - Medium service access points
19. ISO 24102-1, Intelligent Transport Systems - Communications access for land mobiles (CALM) - ITS station management - Part 1: Local management
20. ISO 24102-2, Intelligent Transport Systems - Communications access for land mobiles (CALM) - ITS station management - Part 2: Remote management
21. ISO 24102-3, Intelligent Transport Systems - Communications access for land mobiles (CALM) - ITS station management - Part 3: Service access points
22. ISO 24102-4, Intelligent Transport Systems - Communications access for land mobiles (CALM) - ITS station management - Part 4: Station-internal management communication
23. ISO 24102-5, Intelligent Transport Systems - Communications access for land mobiles (CALM) - ITS station management - Part 5: Fast service advertisement protocol (FSAP)
24. ISO 24102-6, Intelligent Transport Systems - Communications access for land mobiles (CALM) - ITS station management - Part 6: Flow management
25. ISO 25111, Intelligent Transport Systems - Communications access for land mobiles (CALM) - General requirements for using public networks
26. ISO 29281-1, Intelligent Transport Systems - Communications access for land mobiles (CALM) - Non-IP networking - Part 1: Fast networking & transport layer protocol (FNTP)
27. ISO 18377, Intelligent Transport Systems - Communications access for land mobiles (CALM) - Conformance requirements
28. ETSI TS 102 985 1, Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for non-IP networking (ISO 29281); Part 1: Protocol implementation conformance "statement (PICS) proforma
29. ETSI TS 102 985 2, Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for non-IP networking (ISO 29281); Part 2: Test suite structure & test purposes (TSS&TP)
30. ETSI TS 102 985 3, Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for non-IP networking (ISO 29281); Part 3: Abstract test suite and partial PIXIT (ATS) specification
31. ETSI TS 102 797 1, Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for ITS station management (ISO 24102); Part 1: Protocol Implementation Conformance Statement (PICS) proforma
32. ETSI TS 102 797 2, Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for ITS station management (ISO 24102); Part 2: Test suite structure & test purposes (TSS&TP)

33. ETSI TS 102 797 3, Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for ITS station management (ISO 24102); Part 3: Abstract test suite (ATS) and partial PIXIT proforma
34. ETSI TS 102 760-1, Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for Access Technology Support (ISO 21218); Part 1: Protocol Implementation Conformance Statement (PICS) proforma
35. ETSI TS 102 760-2, Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for Access Technology Support (ISO 21218); Part 2: Test suite structure & test purposes (TSS&TP)
36. ETSI TS 102 760-3, Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for Access Technology Support (ISO 21218); Part 3: Abstract test suite (ATS) and partial PIXIT proforma
37. CEN/ISO TS (new WI), Intelligent Transport Systems - Cooperative ITS - Test suite architecture
38. CEN/ISO TS (new WI) Part 1, Intelligent Transport Systems - Cooperative ITS - Test specifications for CEN/ISO TS 17429 - Part 1: Protocol Implementation Conformance Statement (PICS) proforma
39. CEN/ISO TS (new WI) Part 1, Intelligent Transport Systems - Cooperative ITS - Test specifications for CEN/ISO TS 17429 - Part 2: Test suite structure & test purposes (TSS&TP)
40. CEN/ISO TS (new WI) Part 1, Intelligent Transport Systems - Cooperative ITS - Test specifications for CEN/ISO TS 17429 - Part 3: Abstract test suite (ATS) and partial PIXIT proforma
41. CEN/ISO TS (new WI) Part 1, Intelligent Transport Systems - Cooperative ITS - Test specifications for CEN/ISO TS 19091 - Part 1: Protocol Implementation Conformance Statement (PICS) proforma
42. CEN/ISO TS (new WI) Part 1, Intelligent Transport Systems - Cooperative ITS - Test specifications for CEN/ISO TS 19091 - Part 2: Test suite structure & test purposes (TSS&TP)
43. CEN/ISO TS (new WI) Part 1, Intelligent Transport Systems - Cooperative ITS - Test specifications for CEN/ISO TS 19091 - Part 3: Abstract test suite (ATS) and partial PIXIT proforma
44. CEN/ISO TS (new WI) Part 1, Intelligent Transport Systems - Cooperative ITS - Test specifications for CEN/ISO TS 19321 - Part 1: Protocol Implementation Conformance Statement (PICS) proforma
45. CEN/ISO TS (new WI) Part 1, Intelligent Transport Systems - Cooperative ITS - Test specifications for CEN/ISO TS 19321 - Part 2: Test suite structure & test purposes (TSS&TP)
46. CEN/ISO TS (new WI) Part 1, Intelligent Transport Systems - Cooperative ITS - Test specifications for CEN/ISO TS 19321 - Part 3: Abstract test suite (ATS) and partial PIXIT proforma

3 Architecture Comparison

3.1 Scope

3.1.1 CVRIA

The CVRIA defines what we know about the evolving Cooperative Intelligent Transportation Systems (C-ITS) or Connected Vehicle Environment. The architecture description contained within http://www.iteris.com/cvria was developed based on the USDOT's extensive connected vehicle program, including a plethora of research efforts into safety, mobility and environmental applications. It includes many other inputs however, including relevant standards developed by the USDOT and other entities, and parallel or similar C-ITS efforts in Europe and Australia.

The CVRIA identifies the people and entities that have an interest in C-ITS (stakeholders), frames the concerns those stakeholders have as a series of questions, and then addresses those questions in a series of views. Each view of the CVRIA conforms to a viewpoint specification, of which there are four:

- Enterprise: relationships between organizations
- Functional: logical interactions between functions
- Physical: connections between physical objects and their application objects
- Communications: layered communications protocols between application objects

Views are broken up by application, and modeled in graphical language to facilitate stakeholder use. The architecture is impossible to understand in any one view; it is far too broad and too deep to be completely depicted. Instead, each view looks at particular aspects of the architecture; when taken in total, all views + all definitions + all characteristics of objects on these views

Consider the analogy of a house to the CVRIA. A house has organized collections of structural, electrical, plumbing, and mechanical components that work together to allow the house to function. Each Viewpoint looks at exactly one of these sets of components. In other words, there is a structural viewpoint, electrical viewpoint, and so forth.

Imagine that one could see one type of system by wearing the appropriate pair of glasses; e.g. electrical glasses, mechanical glasses. Looking in a window of the house with electrical glasses shows one diagram that forms part of the Electrical View. In order to understand the house's electrical systems, one must look in every window with the electrical glasses. In order to understand the entire house, one must look in every window, and with every set of glasses. The electrician might only care about the Electrical Viewpoint, and the plumber the Plumbing Viewpoint.

Similarly, in order to understand the entirety of the CVRIA, one must understand every model of the Functional, Physical, Enterprise and Communications Viewpoints. Different stakeholders may care about only certain Viewpoints, depending on how they interact with the CVRIA.

In order to organize the broad goals and concepts included in C-ITS, the CVRIA uses an application perspective. This is not a viewpoint per se, but rather a way of looking at subsets of each view focused on a specific connected vehicle application. The applications are derived from documentation like Concepts of Operation, System Requirements, standards, and other documents that have been written to describe parts of the connected vehicle environment. It should be noted that this is not an exhaustive list - new applications will be developed over time but these provide a comprehensive look at the connected vehicle environment.

3.1.2 ITS Station Architecture

The standards and standards in development related to the ITS Station Architecture provide specifications for the internal architecture of a participant in Intelligent Transport Systems. Specifically, these documents define specifications for:

- Information layer standards for common V2V and V2I application scenarios
- ITS Station communications security, connectivity, data exchange and management functionality
- Test specifications for conformance testing of ITS Station communications and management

The ITS Station architecture is transportation service agnostic. It defines the functionalities that implement transportation services. The justification for definition revolves around the characteristics inherent to ITS communications, which ISO 21217 describes as:

- station mobility leads to complex time-varying networking topologies, and time-varying properties of wireless communication channels (fading, hidden-nodes, etc.);
- variety of stations connected via various networking and access technologies including the Internet, various public and private networks, Bluetooth and WiFi, dedicated technologies, such as 5.8 GHz DSRC for road tolling:
  - a station with multiple access and networking technologies can maintain session continuity through a change of either or both;
  - two stations with different access technologies can establish end-to-end connectivity
- variety of communication requirements resulting from different ITS applications with different priorities, e.g. road safety, traffic efficiency, mobility and infotainment, e.g. with respect to communications capacity (data rate), communications reliability, communications availability;
- variety of communication requirements resulting from user needs, e.g. with respect to communications
- cost (in terms of money), communications privacy, communications security;
- variety of communication requirements resulting from regional regulations and policies;
- global applicability, where intended.

The ITS Station architecture does not provide any viewpoint specifications akin to the CVRIA's, however the various relevant standards to provide content that could be compared to the CVRIA's viewpoints. Mostly, the ITS Station concept is modeled *functionally*, though functions can be logically bound to *physical* subsystems, as there are interfaces between those functions. Another large focus is on *communication* between ITS stations. Typically the ITS station communications standards provide more detailed information than the CVRIA's communications viewpoint, although in some cases the CVRIA references documents that provide as much or more information (for instance SAE J2735 vs. the V2V and V2I documents in the Release 1 collection). Lastly, some of the Release 1 documents reference the relationships between institutions, very similar to the CVRIA's enterprise view, though limited in scope to the particular scenarios addressed.

3.2 Concerns Addressed

Concerns are concepts that are of interest or importance to one or more stakeholders. Concerns may apply to any phase of the system life cycle. However, some concerns may apply more during system design, implementation, operations, or maintenance and not during other phases of the system's life. A concern could be manifest in many forms, such as in relation to one or more stakeholder needs, goals, expectations, responsibilities, requirements, design constraints, assumptions, dependencies, quality attributes, architecture decisions, risks or other issues pertaining to the system.

3.2.1 CVRIA

Since the CVRIA follows ISO 42010, which specifies the identification of stakeholders and concerns, it is relatively easy to identify these aspects of the CVRIA. The CVRIA addresses the following concerns (those in **bold** most heavily focused on, while those in ~~strikethrough~~ are planned, with schema at least partially defined, but not complete:

CVRIA Concerns Addressed		
Safety, Mobility, Environmental, Convenience Missions		
~~Performance~~	**Interfaces**	**Functionality**
Information Security	**Operational Security**	Personnel Security
Organization/Resources	**Personal Safety**	**Personal Privacy**
~~Feasibility~~	Risks	**Flexibility**
Deploy-ability	**Maintainability**	

3.2.2 ITS Station Architecture

ISO/CEN/ETSI does not strictly follow ISO 42010, however a reading of the relevant standards indicates that it does address the following concerns:

ITS Station Concerns Addressed		
Safety, Sustainability, Efficiency, Comfort **Missions**		
Performance	**Interfaces**	**Functionality**
Information Security	**Operational Security**	**Personnel Security**
Organization/Resources	**Personal Safety**	~~Personal Privacy~~
Feasibility	Risks	**Flexibility**
Deploy-ability	**Maintainability**	

While personal privacy is not currently listed, there is a legal requirement that it be covered at some point as a result of directive 2010/40/EU.

3.3 Stakeholders Targeted

A system stakeholder is an individual, team, or organization (or classes thereof) with interests in, or concerns relative to, a system. Concerns are those interests which pertain to the system's development, its operation or any other aspects that are critical or otherwise important to one or more stakeholders (see ISO 42010-2011).

3.3.1 CVRIA

The Concept of Operations for the Core System defined three types of Users: Mobile, Field and Center. This differentiation was perceived to be helpful in the context of the Core because the services it provides vary depending on the user. This differentiation is maintained for the purposes of CVE architectural analysis, due to the significant differences in operations experienced by mobile and non-mobile, and center vs. field users.

Differentiation was considered for Acquirers, Maintainers, Developers and Managers. There are certainly differences in how an entity might procure a mobile CVE device vs. a backoffice device. That said, these stakeholders share the same concerns across all viewpoints, and differentiation would only serve to overly complicate the architectural analysis. Consequently no distinction is made between Mobile, Field and Center Acquirers, Developers or any other stakeholder class. It should be noted however that when stakeholder engagement activities are considered that representatives with interest in those three areas have all been engaged.

CVRIA Stakeholders		
Mobile User	**Field User**	**Center User**
Acquirer	Maintainer	**Manager**
Tester	Policy-Setter	**Application Developer**
Device Developer	Service Provider	Standards Development Organization
Transportation Planner	Enforcement	End-of-Lifecycle Manager

3.3.2 ITS Station Architecture

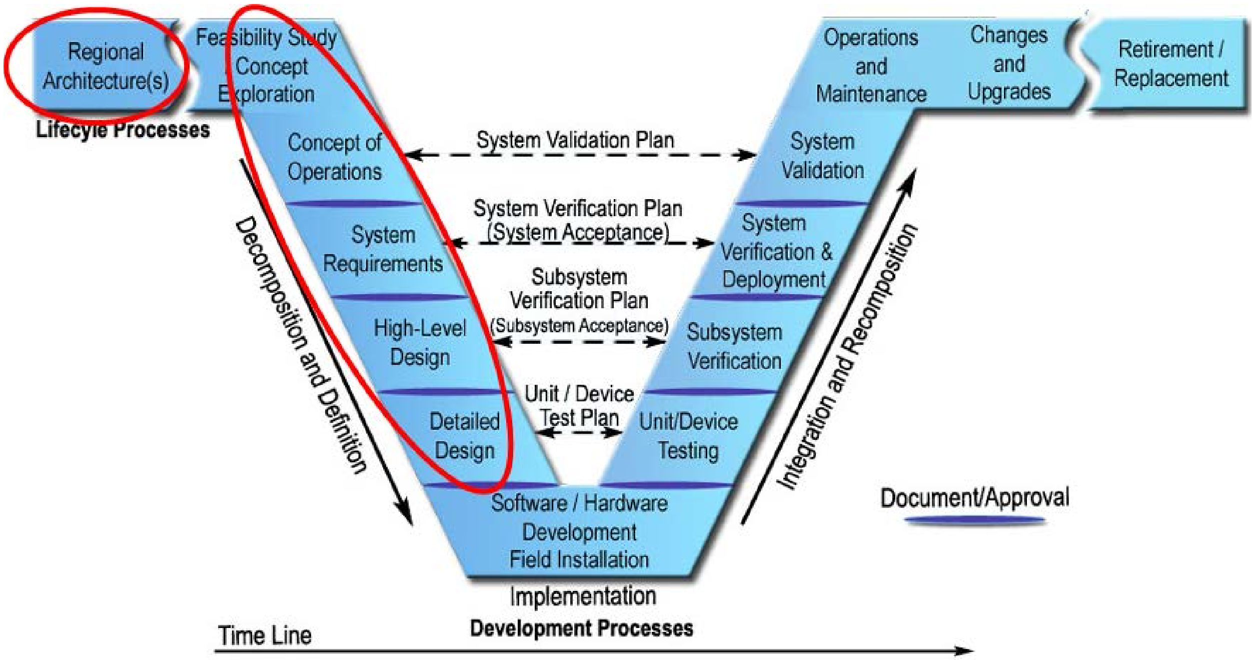
Scope differences with respect to CVRIA account for most of the differences in stakeholders. The ITS-Station concept gets at how to build interoperable devices, while the CVRIA focuses on application benefits. This leads to the ITS Station Architecture addressing more the concerns of the builders, rather than the user or operators of such devices. While many of the same stakeholders appear in this list, the relevance of the ISO/CEN/ETSI standards to those in bold is notably higher.

ITS Station Architecture Stakeholders		
Mobile User	Field User	Center User
Acquirer	Maintainer	Manager
Tester	**Policy-Setter**	**Application Developer**
Device Developer	Service Provider	**Standards Development Organization**
Transportation Planner	Enforcement	End-of-Lifecycle Manager

3.4 Practical Use

3.4.1 CVRIA

The CVRIA's initial specification was written at such a level as to provide appropriate documentation for project architectures and concepts of operation. Subsequent developments have increased the depth of CVRIA material however; the vision for CVRIA's scope incorporates the whole of the SE-process pre-implementation, and possible use post-implementation for validation/verification. Current ITS implementers also have access to the Turbo architecture tool, which develops regional architectures and regional operational concepts.



3.4.1.1 CVRIA Mini-Tool

The CVRIA team developed the CVRIA Mini-Tool as an adjunct to the Southeast Michigan 2014 project. The Mini-Tool facilitates the creation of a layered physical architecture, extending the baseline CVRIA methodology, and providing products useful at architecture, Concept of Operations, and design phases. It also addresses the enterprise viewpoint, enabling project managers to identify what agreements and other relationships are needed to realize their projects.

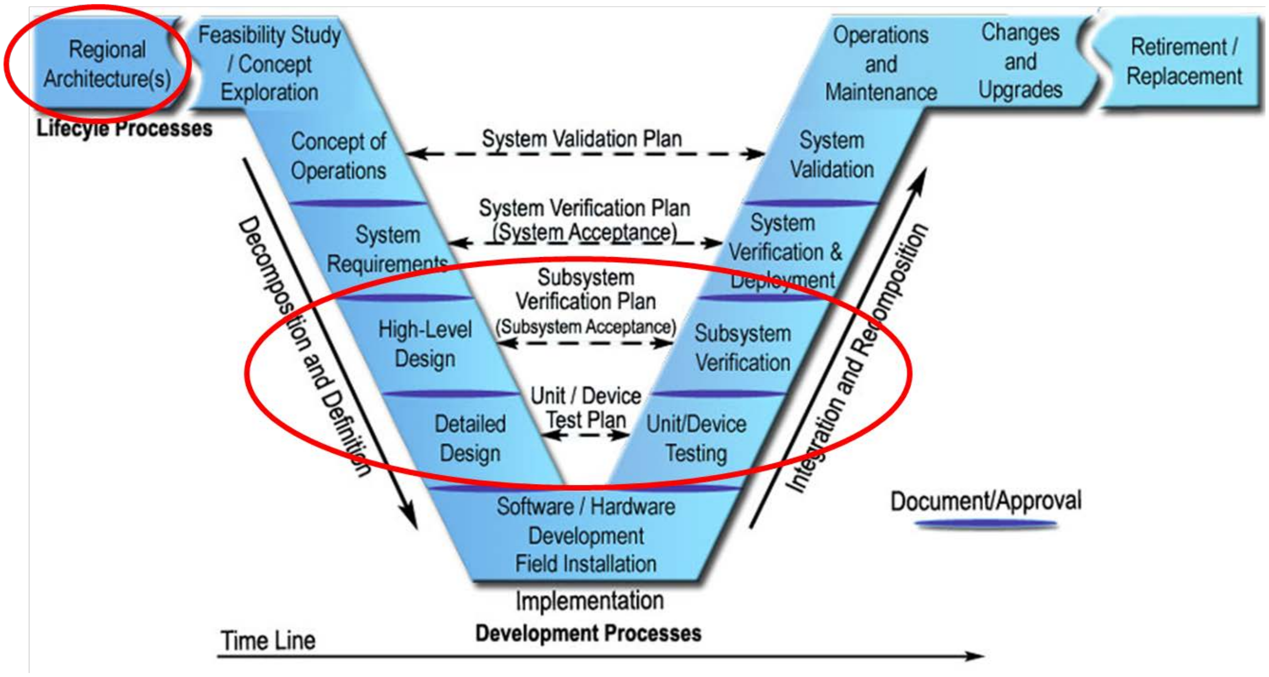
The CVRIA Mini-Tool is very much focused on projects, deployments, and implementations from a local or regional perspective.

3.4.1.2 SET-IT

The Systems Engineering Tool for Intelligent Transportation (SET-IT) is the project architecture tool for the CVRIA. Version 1.0 was released in January 2015, with updates for new functionality every six weeks thereafter. SET-IT is project-focused, with announced plans to support communications specification information down through detailed design. SET-IT produces a Concept of Operations document from a properly defined architecture, and will provide the basis for design documents in subsequent releases as additional functionality is added.

3.4.2 ITS Station Architecture

The scope of the ITS Station Architecture focuses on the design of objects/devices that implement C-ITS. Users of the European ITS Framework (FRAME) have access to a set of tools that enable the development of regional architectures, analogous to US Regional Architecture products produced by the Turbo architecture tool.



Documentation relevant to the ITS-Station is contained in a large mass of standards. A minimum of 44 standards are included as the sum of the ITS Station architecture work; an additional 27 are potentially relevant depending on the application, with many more in development. A small number (about 10) of these standards are freely available, but the remainder must be individually acquired. With an approximate acquisition cost of $150 each, a curious developer would need to expend $5000-$10000 and absorb the contents of roughly 50 documents in order to implement all functions and interfaces expected to be part of the ITS Station concept.

Note that paying for standards and reading lots of documentation is nothing new in the standards arena, nor is it unusual in the communications environment into which ITS encroaches.

3.5 Policy Issues

3.5.1 CVRIA

CVRIA considers applications (as defined by USDOT) as the combination of systems and software that provide transportation benefit. It also considers supporting services, or facilitating applications, that help enable those applications. Many of these imply policy issues:

1. Core Authorization, which defines the relationship between the controller of the roadside and the grantor of credentials (SCMS). If IEEE 1609.2 Service Specific Permissions are used at the roadside to verify authorization to grant service, there needs to be a mechanism for managing those permissions. Policy Issues:
    a. Who manages the SSP, and what is the entity’s relationship to the SCMS?
    b. How does the grantor of authorization (the local entity managing the roadside) interact with the manager of the SSP?

2. Data Distribution implies a centralized data dissemination system. This may be security policy related because the operator of the data distributor is the likely entry point for legal or otherwise interception of data, and as focal point must function in order for some services to work. Policy issues:
   a. How are the rights to operating data distribution systems apportioned? Who decides who has access to what data?
   b. If vehicles are mandated to provide some data (BSMs for example), and someone deploys listeners/collectors, can they sell that accumulated data? Under what circumstances?
   c. Is there any data that must be made available to all, for no charge?
3. Object Registration and Discovery, which enables the CVE participants to learn of one another, what services each is offering and potential conditions surrounding those services (this is not in the CVRIA today, but is part of the Southeast Michigan 2014 project and will be included in CVRIA v2.0). Like the DDS, ORDS is a focal point and must operate in order for services to operate. Policy issues:
   a. Should access to ORDS be required to operate? If so, how is ORDS funded?
   b. Are there restrictions/requirements on who can own/operate an ORDS? Who sets those?

3.5.2 ISO/CEN/ETSI

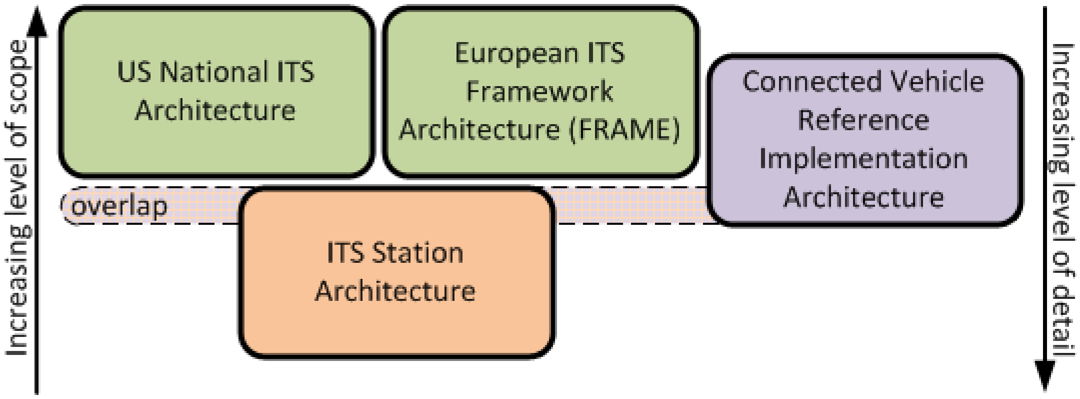
None currently identified.

4 Analysis

CVRIA is service/application focused, while the CEN/ISO/ETSI standards start from the unit of technical implementation platform?

4.1 Scope

CVRIA is a US effort, the ITS Station Architecture is internationally driven. This difference in origin provides differing focus and attention to concerns. ITS Station Architecture users are referenced to FRAME, the European ITS Architecture, which is more analogous to the US National ITS Architecture. The CVRIA will be integrated to the US National ITS Architecture in 2016, but prior to then includes only the subset of the US National ITS Architecture that includes connected vehicle concepts.


Increasing level of scope
US National ITS Architecture
European ITS Framework Architecture (FRAME)
Connected Vehicle Reference Implementation Architecture
overlap
ITS Station Architecture
Increasing level of detail

For all their differences, the CVRIA and the ITS Station Architecture are remarkably compatible. The basic building block of the CVRIA is the *physical object*, or p-object for short. The basic building block of ITS Station Architecture is the ITS-Station Unit, or ITS-SU. It is fair to say that generally, *a p-object could be implemented as an ITS-SU*. In fact, any ITS-SU could be easily captured in CVRIA methodological language, so that one might say that *any ITS-SU is a p-object*. The converse is not the case however. A p-object could also be implemented in such a way as to not satisfy the conditions of being an ITS-Station.

This leads to the obvious question, *what makes an ITS-Station*?

An ITS-Station is either a host, or a host and a router. Exactly what that means depends on which of the various related standards are implemented. The general principle within this architecture is that *if you do <X>, here's how you have to do it: <series of requirements>*. Requirements for each such function or interface are the subject of an individual standard. So for example, if an ITS Station claims remote management capability, it must be conformant to ISO 24102-2… Remote management, and would presumably be tested against portions of ETSI TS 797.

However, if we apply one of the HTG6 definitions, that C-ITS only occurs between entities that have communication enabled through third party trust authentication, then a more refined answer is, *an ITS Station is the device that meets whichever standards are required in order to get credentials*. Since the ITS Station architecture security requirements are still under development, the identification of the relevant standards cannot be done today.

4.2 Overlap

The CVRIA's communications viewpoint is the greatest source of overlap, but there is really not much of conflict here. The current CVRIA viewpoint specification is fairly shallow; very high level in scope: it defines the protocols necessary to realize a given application, all of which are easily captured in the ITS Station architecture; while there are likely standards referenced in the CVRIA that are not referenced in the ITS Station architecture (in particular, the message set standards that are US-centric), this is not an overwhelming or unbridgeable gap. It might be considered an opportunity for harmonization.

Both architectures seem reliant on IEEE 1609.2 for security when using 5.x GHz DSRC.

4.3 Complements

The real benefit of a comparison between the ITS Station Architecture and CVRIA is a realization of just how much the two approaches complement the other. The ITS Station reference architecture provides a detailed, logical framework for implementation. It is really focused on the building of *things*; whereas the CVRIA is focused on the realization of benefits through analysis of application concepts. The following list attempts to call these things out:

1. CVRIA provides a reasonably easy to understand, graphical modeling language that is excellent for transitioning between planning and design from a user service benefit perspective. The ITS Station Architecture provides specifications for how the individual units that provide those services might be built.
2. CVRIA touches on a lot of issues without a lot of depth, that are (or will be) well defined in the ITS Station architecture. For instance:
    a. Security services inside the p-object
    b. Management services inside the p-object
    c. Communications mechanism choices, priorities inside the p-object
3. CVRIA considers all objects peers, while the ITS Station architecture classifies objects as ITS Stations or not. If the ITS Station requirements could be clearly defined and made available, CVRIA might leverage them.
4. CVRIA focuses on the delivery of application services: benefits to users. These might be implemented by ITS Stations, and in fact might be considered more secure or stable if done so.
5. ISO TS 17419 (E) illustrates application and device registration, certification, certificate issuance institutional relationships that the CVRIA might leverage

4.4 Issues

Since CVRIA and the ITS Station Architecture are at such different levels of detail, an ideal scenario for the worldwide deployment of C-ITS might include the synergistic integration, or at least harmonization at boundaries, of the two architectures. This would yield benefits to stakeholders of all level of interest, from planners to chip makers. Unfortunately, there are some barriers to that approach:

1. The ITS Station concepts are bound within a series of standards, which are only available for a fee. The CVRIA and its tools are available for no charge, so integration has an intellectual property ownership challenge to CVRIA users. This might be solved by limiting the integration to drawing formalized boundaries, but that would constrict the scope of the CVRIA in an undesirable way. For example, SET-IT might be evolved to consider details inside a-objects, and further details inside p-objects. Drawing a boundary would forbid that expansion. Additionally, the USDOT has typically been loathe to provide too much specification to US road operators, while drawing such a fixed barrier would seem to imply a tacit mandate of the ITS station approach.
2. The ITS Station architecture's approach to security is vastly different than the US V2V security infrastructure specified in the recently released NHTSA report: Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application. The security system described

within this report, the SCMS, will be included in the CVRIA. This system addresses requirements with regard to personal privacy, anonymity and the presumption of minimal enforcement engagement that are significantly more stringent than what is discussed in the ISO/CEN/ETSI documents. Granted, this is partially the subject of Harmonization Task Group 6.

3. The CVRIA development team is developing, and the USDOT is providing for free, a set of tools enabling the adoption of the architecture, SET-IT. It may be practical to enable functionality in SET-IT that allows the user to specify a given p-object is to be implemented as an ITS-Station, and that associated requirements be attached to that object. While a similar intellectual property issue as item #1, the real issue is the international acceptance of such a toolset.
4. Perception. The CVRIA illustrates likely methods for accomplishing missions. It does not specify how an implementer has to do anything. The ITS Station architecture is all about specification, but with the exception of an initial set of application, message and data specifications focusing on V2V and V2I (see ISO/CEN/ETSI references 3, 4, 5, 7), does not address the accomplishment of user service missions.

Appendix A

Reference material related to the CVRIA that is not otherwise published, but used for reference in the preparation of this primer.

A.1 CVRIA Stakeholder definitions

Users

The User stakeholder is the operator of the Mobile, Field, or Center device or system. Owing to the significant logistical differences between these three types of devices and systems, their associated stakeholders are identified individually.

Mobile User

The Mobile User operates a personal information device (e.g. smart phone) or operates or rides in a vehicle that participates in the CVE. Mobile Users include automobile, bus, truck, construction and emergency vehicle drivers and passengers, as well as cyclists and pedestrians.

Field User

The Field User owns, operates and/or maintains the intelligent infrastructure distributed near or along the transportation network which performs surveillance, information provision, local transactions, and control functions.

Center User

The Center User owns, operates, and/or maintains back office systems that provide services in the CVE. Center User stakeholders include public and commercial transportation, transit and fleet managers, vehicle and device manufacturers (that want operational diagnostic information), information service providers, emissions, commercial vehicle and other regulatory managers, toll administrators, maintenance and construction operators, public safety, insurance and transportation data aggregators.

Acquirer

The acquirer is the entity that procures a device that participates in the CVE.

Examples of public entities that may assume the Acquirer role include state Departments of Transportation (DOTs), transit agencies, commercial vehicle administration agencies, or regional coordination entities that include elements of multiple such agencies. Examples of private entities that may assume the Acquirer role include private individuals (e.g., vehicle owner, mobile device owner), commercial fleet management companies, vehicle manufacturers or information service providers (e.g., traveler information).

Maintainer

The Maintainer is the entity that ensures continuous device or application operation by ensuring the availability of resources including power, environmental control, hardware, software patches and upgrades required for devices and applications to operate properly.

For Center and Field systems, the Maintainer role will often be funded by the same entity that serves as the Manager. The Maintainer may be part of the same agency as the Manager, or it may be contracted to a separate entity under control of the Manager. For Mobile components, the Maintainer stakeholder is less predictable: it may be the owner or operator of the device, or it may be a third party.

Manager

The Manager is responsible for planning the deployment and managing the operations of the components of the CVE. The Manager does not interact directly with the CVE. Changes that require operational modification (to enforce policies imposed by the Policy Setter for example) are determined by the Manager, but depending on scope and required functionality are implemented by the Developer, Maintainer or User.

The Manager role will be part of an agency or it may be contracted to a separate entity under control of an agency.

Tester

The Tester is responsible for verifying that devices and applications meet their specifications, and in particular that the interfaces they implement conform to the standards specified for those interfaces.

Policy-Setter

The Policy-Setter determines policies that affect CVE component and application deployment, implementation or operations. This could be a local entity such as a DoT, a regional body or a federal entity such as the Federal Communications Commission (FCC).

Application Developer

The Application Developer creates applications that provide services within the CVE.

Device Developer

The Device Developer creates devices and systems (Mobile, Field and Center) that will interact through applications to provide services of value to Mobile, Center and Field Users.

Service Provider

The Service Provider provides a service that is used by the Mobile, Field and Center Users to access or deliver other services. Examples of Service Providers are RSE owner/operators, cellular network providers, and security providers such as the operator of a certificate authority.

Standards Development Organization

The Standards Development Organization (SDO) develops and maintains the standards used to define interfaces between devices in the CVE.

Transportation Planner

Transportation planners analyze and plan for improvement of the transportation system, primarily in the form of roadway modification, construction and enhancement using ITS technologies.

Enforcement

Enforcement entities identify users that are in violation of regulations. For the CVE, this includes those entities that enforce traffic regulations, road usage and emissions.

End-of-Lifecycle Manager

Entities involved in disposal, recycling and recovery activities are focused on what happens to devices when those devices are no longer being used.

A.2 CVRIA Concerns

The connected vehicle applications have three missions: improvements in safety, mobility, and environmental stewardship:

1. The safety mission is aimed to increase situational awareness and reduce or eliminate crashes.
2. The mobility mission is aimed to enable the management of the transportation network toward optimum performance.
3. The environmental mission is aimed to enable reductions in the environmental impacts of travel.

Note that while commercially-focused applications may be enabled by the deployment of connected vehicle technology, commercial and convenience applications are not a mission goal.

Performance

This concern deals with characteristics such as speed (responsiveness of services), availability, reliability, capacity, and other quantitative measures.

Interfaces

This concern deals with how interfaces are defined and how users access and operate applications within the CVE.

Functionality

This concern deals with what functionality the CVE provides to users; how its components work together and how they transition between operational modes.

Security

Security includes three main areas:

Information Security

This concern deals with securing the origin, transmittal and destination of information.

Operational Security

This concern deals with protecting the physical devices participating in the CVE from physical and environmental threats.

Personnel Security

This concern is about ensuring that personnel do not inadvertently or maliciously cause harm to CVE assets and have the proper training necessary to respond to security related incidents.

Organization/Resources

This concern is about organization of CVE development and the resources required to develop, deploy, operate and maintain devices and applications.

Personal Concerns

Personal concerns are those relevant to an individual operator or user.

Personal Safety

This concern deals with protecting the individual from physical harm.

Personal Privacy

This concern is about protecting the individual's ability to selectively reveal personal information.

Feasibility

This concern deals with the ease and convenience of realizing a functional, beneficial CVE with regard to the current state of technology and available resources.

Risks

This concern deals with the chance of and repercussions of failure in system development and operation. This concern clarifies which level of risk is acceptable.

Flexibility

This concern deals with the ability to extend and expand the CVE to deal with new and potential unforeseen conditions or changes in its mission or scope.

Deployability

This concern deals with the issues surrounding deployment, including capital, human and other resource requirements, business models as well as transitions between development, deployment and operations.

Maintainability

This concern addresses issues of maintenance, in terms of resources required and impact on operations.