RITA Intelligent Transportation Systems
Joint Program Office

Core System:
Risk Assessment Report (RAR)

www.its.dot.gov/index.htm
October 28, 2011

U.S. Department of Transportation
Research and Innovative Technology Administration

Produced by Lockheed Martin
ITS Joint Program Office
Research and Innovative Technology Administration
U.S. Department of Transportation

Notice

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD MM YYYY)
28 10 2011

2. REPORT TYPE
(Risk Report)

3. DATES COVERED
N/A

4. TITLE AND SUBTITLE
Core System: Risk Assessment Report (RAR)

5a. CONTRACT NUMBER
GS-23F-0150S

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

5d. PROJECT NUMBER
DTFH61-10-F-00045

5e. TASK NUMBER
6

5f. WORK UNIT NUMBER

6. AUTHOR(S)
Core System Engineering Team

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Lockheed Martin
9500 Godwin Drive
Manassas, VA 20110

8. PERFORMING ORGANIZATION REPORT NUMBER
11-USDOTSE-LMDM-00056

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
US Department of Transportation
Research and Innovative Technology Administration
ITS Joint Program Office
1200 New Jersey Ave., S.E.
Washington D.C. 20590

10. SPONSORING/MONITOR'S ACRONYM(S)

11. SPONSORING/MONITOR'S REPORT NUMBER(S)

12a. DISTRIBUTION/AVAILABILITY STATEMENT
This document is available to the public through the National Technical Information Service, Springfield, Virginia 22161.

12b. DISTRIBUTION CODE

13. SUPPLEMENTARY NOTES
Risk Assessment Report (RAR) for the Core System portion of the *connected vehicle* program

14. ABSTRACT (Maximum 200 words)
This document describes a set of high-level risks that could affect deployment or implementation of the Core System as part of the United States Department of Transportation's (USDOT) next generation integrated transportation system. It describes a set of risks and provides a subjective analysis of their potential impact to the system These are in addition to risks and issues presented and discussed in other *connected vehicle* program documents.

15. SUBJECT TERMS
Risk, security, governance, core system, connected vehicle, enterprise, stakeholders, communications, certificate

16. SECURITY CLASSIFICATION OF:

a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**
Unclassified	Unclassified	Unclassified

17. LIMITATION OF ABSTRACT
None

18. NUMBER OF PAGES
33

19a. NAME OF RESPONSIBLE PERSON
Walt Fehr

19b. TELEPHONE NUMBER
(202) 366-0278

CHANGE LOG

Revision	*Change Summary*	*Author*	*Date*
-	Initial Release	Lockheed Martin	9/20/2011
A	Update to incorporate feedback	Lockheed Martin	10/21/2011
B	Update to incorporate feedback from 10/25/2011	Lockheed Martin	10/28/2011

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1.0 INTRODUCTION

1.1 Identification

This document is the Risk Assessment Report (RAR) for the Core System for the United States Department of Transportation's (USDOT) *connected vehicle* program.

1.2 Document Overview

The USDOT initiated this Systems Engineering (SE) project for the Core System as part of the *connected vehicle* program. The purpose of the Risk Assessment Report is to identify critical technical and cost risks that may impact the *connected vehicle* program deployment.

A common definition of a risk is the probability that a decision or action will result in a negative or unwanted consequence, where the probability of each possible outcome is known or can be estimated (see Vehicle Infrastructure Integration (VII) Risk Management Plan, version 3.0). In this document the risks will be identified along with a discussion of their potential impact on deployment. Each risk will have a qualitative discussion of its impact (e.g., high, medium, or low impact) and its likelihood (e.g., high, medium or low likelihood) that the risk will materialize. Actions or mitigation measures will then be listed.

Table 1-1 below summarizes the High Core System Risks based on the combination of impact and likelihood. More detail on these and all of the other identified risks are provided in Section 4.0.

Table 1-1: High Core System Risks

4.1.1	Timely Deployment
4.1.2	Relationships between Core Systems and external Enterprises
4.2.1	Role and Makeup of the Core Certification Authority
4.2.2	External Support System (ESS) for Security
4.2.3	Operations and Maintenance (O&M) of the Security External Support System (ESS)
4.2.4	Security Management

The Core System Risk Assessment Report consists of the following sections:

- Section 1.0: provides an overview of the document and the Core System
- Section 2.0: lists the reference documents
- Section 3.0: describes how the risks are organized and 'scored' for this report
- Section 4.0: provides the detailed listing of each risk including the Risk statement, a root cause, the Consequence, Likelihood it will happen, a graphical summary of the overall risk, and a list of any actions that can be taken to mitigate or reduce the risk.
- Section 5.0: is the Glossary.

1.3 Core System Overview

The USDOT's *connected vehicle* program envisions the combination of the applications, services and systems necessary to provide the safety, mobility and environmental benefits through the exchange of data between mobile and fixed transportation users. It consists of the following:

- **Applications** that provide functionality to realize safety, mobility and environmental benefits,
- **Communications** that facilitate data exchange, and
- **Core Systems**, which provide the functionality needed to enable data exchange between and among mobile and fixed transportation users, and
- **Support Systems,** including security credentials certificate and registration authorities that allow devices and systems to establish trust relationships.

The Core System's main mission is to enable safety, mobility and environmental communications-based applications for both mobile and non-mobile users. The scope of the Core System includes those enabling technologies and services that will provide the foundation for application transactions. The Core System works in conjunction with External Support Systems like the Certificate Authority for Dedicated Short Range Communications (DSRC) security, as defined in IEEE Standard 1609.2. The system boundary for the Core System is not defined in terms of devices or agencies or vendors, but by the open, standardized interface specifications that govern the behavior of all interactions between Core System Users.

The Core System supports a distributed, diverse set of applications. These applications use both wireless and wireline communications to provide:

- Wireless communications with and between mobile elements including vehicles (of all types), pedestrians, cyclists, and other transportation users
- Wireless communications between mobile elements and field infrastructure
- Wireless and wireline communications between mobile elements, field infrastructure, and back office/centers

The Federal Communications Commission (FCC) allocated 75 Megahertz (MHz) of spectrum in the 5.9 Gigahertz (GHz) frequency range for the primary purpose of improving transportation safety. In addition to safety of life and public safety applications, the FCC's Final Report and Order also allowed private and non-safety applications to make use of the spectrum on a lower priority basis.

A critical factor driving the conceptual view of the Core System and the entire *connected vehicle* environment is the level of trustworthiness between communicating parties. While the Core System is being planned for anonymity, it is also providing a foundation from which to leverage alternative communications methods for non-safety applications. These alternatives are typically available on the market today and the levels of anonymity and privacy inherent to these systems are typically governed by agreements between communication providers and consumers. So while privacy is not compromised for an individual, what happens between that individual and their communication provider (e.g., 3G service provider) very well may compromise privacy. Some application providers may require personal information in order to function which would require the Application User to opt-in to use that application.

Within the *connected vehicle* environment the Core System concept distinguishes communications mechanisms from data exchange and from the services needed to facilitate the data exchange. The Core System supports the *connected vehicle* environment by being responsible for providing the services needed to facilitate the data exchanges. The contents of the data exchange are determined by applications unless the data exchange is used as part of the facilitation process between the user and the Core System.

The Core System provides the functionality required to support safety, mobility, and environmental applications. This same functionality may also enable commercial applications but that is not a driving factor for the development of the Core System. The primary function of the Core System is the facilitation of communications between System Users and some of the communications must also be secure. The Core System may also provide data distribution and network support services depending on the needs of the Core System deployment.

A critical factor driving the conceptual view of the Core System and the entire *connected vehicle* environment is the level of trustworthiness between communicating parties. A complicating factor is the need to maintain the privacy of participants, though not necessarily exclusively through anonymous communication.

For additional information on the Core System, please reference the Core System Concept of Operations (ConOps) document.

2.0 REFERENCED DOCUMENTS

- Core System Concept of Operations (ConOps), Rev D, October 7, 2011.
- Core System Requirements Specification (SyRS) Rev E, October 14, 2011.
- System Architecture Document (SAD), Rev C, 2011.
- Vehicle Infrastructure Integration (VII) Risk Management Plan, version 3.0.
- VII Privacy Policies Framework, Version 1.0.2, February 16, 2007.
- An Approach to Communications Security for a V2V/V2I Communications Data Delivery System, Technical Description and Identification of Policy and Institutional Issues, September 2011, FHWA-JPO-11-130.
- Core System Security White Paper, March 29, 2011.
- Core System Policy White Paper, March 29, 2011.

3.0 RISK ASSESSMENT

3.1 Evaluation Explanation

The Risk Assessment Grid Chart is made up of an X Axis, called Consequences (or impacts) and a Y Axis, call Likelihood (or probability). Each X and Y Axis is made up of 5 grid cells (1-5), with the lower numbers representing less risk than higher ones as represented in Figure 3-1. The green section represents lower numbers (e.g., 2, 3; 3, 1), while the red section represents higher numbers (e.g., 5, 3; 4, 4).

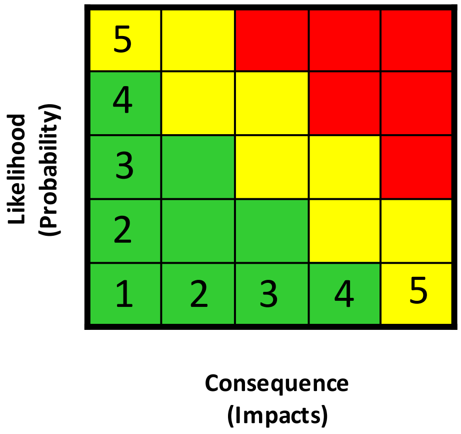


Figure 3-1: Risk Assessment Grid

The Y Axis as Likelihood (or probability) is evaluated as a percentage as follows:

Table 3-1: Likelihood Evaluation Table

Likelihood Score	Probability Range	Overall Probability
1	1%-19%	Very Low
2	20%-39%	Low
3	40%-59%	Medium
4	60%-79%	High
5	80%-100%	Very High

The X Axis as Consequences (or impacts) is typically made up of Cost, Schedule, and Technical factors with a mean score for the overall Consequence score. Each program varies widely, but this is an example below:

Table 3-2: Consequence Evaluation Table

Consequence Score	Mitigation Cost	Schedule (Months)	Technical Evaluation
1	$1K – $25,000.	1-2	Existing technology meets requirements
2	$25,000 - $100,000	2-3	Minor evolution of existing technology needed to meet requirements, all issues addressed and near resolution.
3	$100,000 - $500,000	3-5	Moderate evolution of existing technology need to meet requirements, issues addressed but not resolved.
4	$500,000 - $1M	5-6	Significant evolution of existing technology, major performance issues remain, critical requirements not met.
5	$1M and over	6 and over	New "State of the Art," Limited technology experience, current system does not meet critical requirements.

Likelihood (Probability) Scores can be typically supported by rationale, whereas Consequence (Impact) factors are more difficult to determine especially in the Design Phase. Consequence factors are better evaluated at the Development and Implementation Phase where costs and schedules are more pronounced. For the purpose of this document, Consequence factors will use Schedule and Technical Evaluation factors to determine impacts, but not cost.

The overall risk score will consist of Green for Low, Yellow for Medium, and Red for High.

4.0 RISKS FOR THE CORE SYSTEM

The risks for the Core System will be separated into two categories. One category are risks that are associated with an individual Core System, the second category are risks that are associated with the collection of multiple Core Systems and their relationships.

The following risks are those that are associated with an individual Core System:

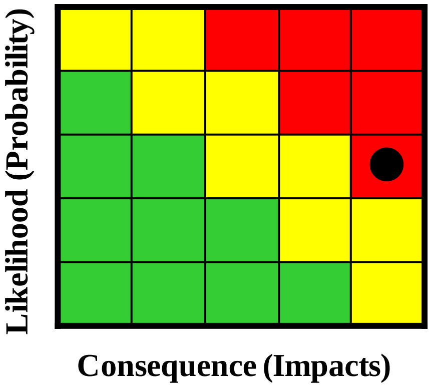
1) Timely Deployment [High Risk]
2) Relationships between Core Systems and external Enterprises [High Risk]
3) Adequate Operations and Maintenance Personnel [Medium Risk]

The following risks are those that are associated with multiple Core Systems and their relationships:

1) Role and Makeup of the Core Certification Authority [High Risk]
2) External Support System (ESS) for Security [High Risk]
3) Operations and Maintenance (O&M) of the Security External Support System (ESS)) [High Risk]
4) Security Management [High Risk]
5) System Performance Management [Medium Risk]
6) Privacy [Medium Risk]
7) Device Certification [Medium Risk]

4.1 Risks Associated with an Individual Core System

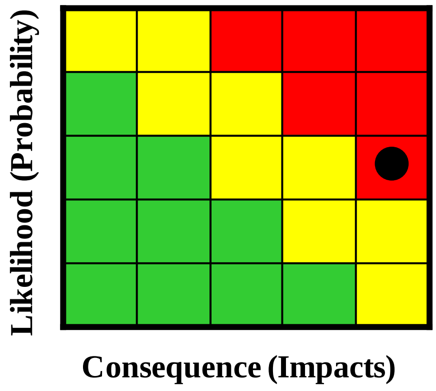
4.1.1 Timely Deployment



Risk Statement
IF the deployment for functioning Core Systems is not complete by the time mobile system users are beginning to use the *connected vehicle* environment THEN the Core Services including trust management and data distribution will not be available to System Users and applications that rely on having common trust and standardized data may be affected. Are the next steps for implementing the design of the Core System documented and scheduled? Are the schedules for the Core System deployment in alignment with the deployment of other parts of the *connected vehicle* program such as the vehicle-based safety systems? Allowing the design and implementation of the Core System to fall behind the development of *connected vehicle* related devices and applications could jeopardize the successful implementation of the overall *connected vehicle* environment.
Root Cause Driver
Planned Deployment issue.
Consequence (Impacts)
(Score: 5) If the Core System is not deployed along with the *connected vehicle* applications, then System Users may have to resort to devices with non-standard interfaces or stand-alone applications resulting in a patchwork of systems that cannot interoperate.
Likelihood (Probability)
(Score: 3) This is an institutional issue which may take time to accomplish. Planning involves various interest groups. At this point, with few specific decisions about the deployment of the Core System being discussed or documented the likelihood is high that this risk will occur.
Overall Score: Red (High)

Risk Reduction Actions/Events	
1	DOT should conduct an analysis to determine when the Core System should be deployed relative to other devices and applications being developed in order to provide the best benefits.
2	The Core System documentation needs to be made available to research programs like the safety pilot, test bed, and other private researchers to support prototyping and to determine how to design and implement Core System(s).
3	Standards organizations need to begin evaluating how to incorporate Core System interfaces.

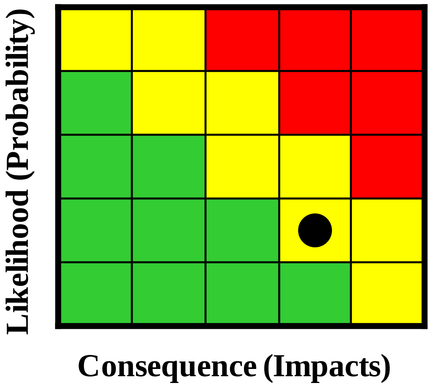
4.1.2 Relationships between Core Systems and external Enterprises



Risk Statement
IF the enterprise relationships between the Core System and external entities are not developed, deployed, operational, and maintained THEN the Core System would likely not operate correctly and efficiently. The System Architecture Document defines relationships for governance of the Core Systems, including a Core Certification Authority and External Support Systems. This affects all aspects of the Core System included trust management and data distribution services. Related to Risk: • Section 4.2.1, Role and Makeup of the Core Certification Authority
Root Cause Driver
Stakeholder Operational Agreements
Consequence (Impacts)
(Score: 5) The Core System has dependencies on external Enterprise relationships working correctly as designed, otherwise the Core System is impacted operationally and over time through undefined maintenance agreements and operating agreements.
Likelihood (Probability)
(Score: 3) External Enterprise objects like the Core Certification Authority will involve many different stakeholder organizations, including public and private sector organizations. The likelihood is high that the diverse group of stakeholders will not be able to coalesce and establish the necessary structure to govern the Core System(s) and the security external support systems or sustain their operations over the long term.
Overall Score: Red (High)

Risk Reduction Actions/Events	
1	Assess the System Architecture Document (SAD) external Enterprise Objects and their relationships to ensure cooperation and interoperability.
2	Develop the institutional/policy concepts necessary to establish the Core Certification Authority and External Support Systems while continuing to develop the technical aspects of the Core System to ensure interoperability.

4.1.3 Adequate Operations and Maintenance Personnel



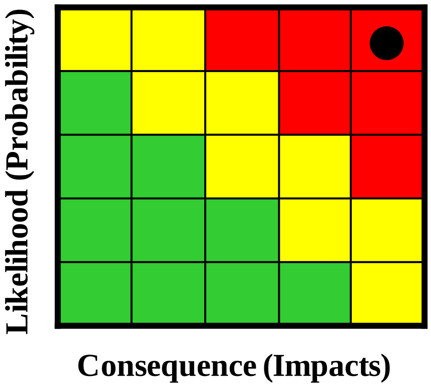
Risk Statement
IF new personnel need to be hired and trained or retraining is needed for existing personnel to operate and maintain a Core System THEN appropriate annual budgets and training time must be available so that Core System critical updates will not lag behind which could cause security and incompatibility issues over time.
Root Cause Driver
That there is budget for personnel to operate and maintain the Core Systems.
Consequence (Impacts)
(Score: 4) There are operations and maintenance personnel to handle the day-to-day operations of the Core System and there may a need for these personnel to be trained. There are also training costs that are needed as well. Without a personnel budget, the Core System cannot operate.
Likelihood (Probability)
(Score: 2) Adequate and complete budgets are needed to operate/maintain the Core System. The assumption is that if a jurisdiction is installing a Core System that they have considered personnel for operations and maintenance, so the likelihood is somewhat low.
Overall Score: Yellow (Medium)

Risk Reduction Actions/Events	
1	The US DOT will need to conduct an assessment to determine what personnel are needed to operate and maintain Core System equipment, servers, accounts, etc. This makeup of the workforce will depend on the scale of the services being provided by a Core, including, to some degree, the estimated number of System Users (particularly center based system users with which a Core System would interact in order to setup geo-casts, setup new subscriptions, investigate misbehavior, etc.); as well as the hours of operation of that Core System.
2	The US DOT, as part of the institutional/policy development for the Core System governance should also establish policy guidelines (see risk 4.2.1) that address the minimal staffing requirements for any agency or entity contemplating hosting a Core System. This could be part of the role of the Core Certification Authority - to ensure that the required levels were in place and were maintained over time.

4.2 Risks Associated with Multiple Core Systems

The following risks are those that are associated with multiple Core Systems and their relationships:

4.2.1 Role and Makeup of the Core Certification Authority

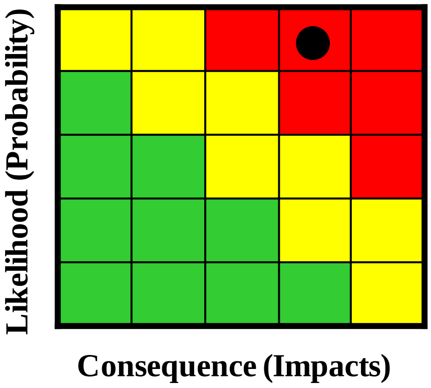


Risk Statement
IF the Core Certification Authority (CCA) is not established and operational THEN the Core System will likely have policy and interdependence issues with other Core Systems as well as with external support systems. The System Architecture Document defines roles for the Core Certification Authority and suggests the importance of bringing together a number of diverse stakeholders in order to establish this Authority. The success of the Core System depends on having a trusted Authority to establish the governance models, standards for operations, and provide leadership concerning the institutional issues surrounding the operation of the Core System. The Core Certification Authority would need to monitor upgrades as they come along to determine when there is an interoperability issue with other Core Systems or System Users. As noted in the SAD's Enterprise View - Governance, the make-up of the CCA is probably many different bodies, all of which need to be identified. Related to Risks: • Section 4.1.2, Relationships between Core Systems and external Enterprises • Section 4.2.4, Security Management • Section 4.2.5, System Performance Management • Section 4.2.7, Device Certification
Root Cause Driver
Establishment and operation of the Core Certification Authority is needed.
Consequence (Impacts)
(Score: 5) If the Core Certification Authority is not available, then Core System policies, conflicts, jurisdictional issues, interdependencies, application standards, etc., for Core Systems may not be resolved in a manner that supports the overall interoperability of the *connected vehicle* environment.

Likelihood (Probability)
(Score: 5) This is an institutional issue which will take time to resolve. There will likely be a need for a national charter for this authority. The task of establishing the CCA will include establishing budgets, defining roles, identifying governance processes, and determining personnel needs. It will also need buy-in from local jurisdictions, device/system developers, and other various interest groups. This effort will take time to establish the CCA. Given the institutional complexity of this activity and the number of stakeholders that must work together the likelihood is high that it will take longer to establish the institutional issues than to get the technical issues worked out and ready to support deployment of the *connected vehicle* environment.
Overall Score: Red (High)

Risk Reduction Actions/Events	
1	US DOT should continue the policy research already underway for the overall governance needs for the *connected vehicle* environment and use the enterprise objects and relationships described in the System Architecture Document (SAD) to better inform the investigations into what formal or informal processes are needed, what roles might need to be filled, how the CCA will be chartered, how budgets will be established, etc.
2	Using this assessment the national oversight and governance authority can be scoped.

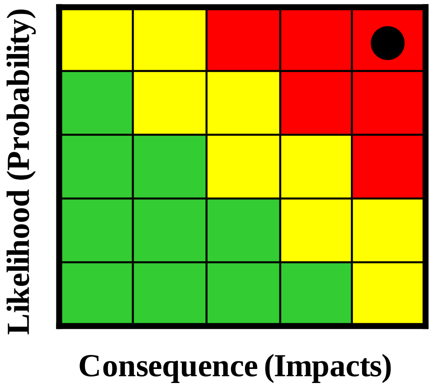
4.2.2 External Support System (ESS) for Security



Risk Statement
IF the External Support Systems for providing a security credentials Registration Authority (RA) and Certificate Authority (CA) are not developed, established, and deployed THEN the System Users will not be able to receive valid IEEE 1609.2 (DSRC) security Certificates nor will the Core System or System Users be able to receive IEEE 1609.2 (DSRC) Certificate Revocation Lists (CRLs) in order to quickly identify any misbehaving users and maintain an operational system. Related to Risk: • Section 4.2.3, Operations and Maintenance (O&M) of the Security External Support System (ESS)
Root Cause Driver
Inadequate Planning for Security Distribution
Consequence (Impacts)
(Score: 4) The Core System's misbehavior management is impacted if the IEEE 1609.2 (DSRC) CRLs are not distributed to the Core. *Connected vehicle* services like Vehicle-to-Vehicle (V2V) Safety are impacted if there is not a defined way to distribute certificates and CRLs to System Users.
Likelihood (Probability)
(Score: 5) The automobile companies and Core System have expectations that the IEEE 1609.2 (DSRC) Certificates are to be distributed by an external authority. This is an institutional issue which may take time to accomplish. The establishment of this external support system involves various interest groups, including System Users and the likelihood is high that this will not be in place in time for full-scale deployment of devices and applications in the *connected vehicle* environment.
Overall Score: Red (High)

Risk Reduction Actions/Events	
1	Assess which Certificate Authority functions for the ESS need to be developed, established, and deployed and set up a plan.
2	Determine who will operate the ESS and what is the funding model will be for both the initial roll-out and ongoing support phases.
3	Determine who has oversight and governance to ensure that the Core System is compatible with the ESS functions.

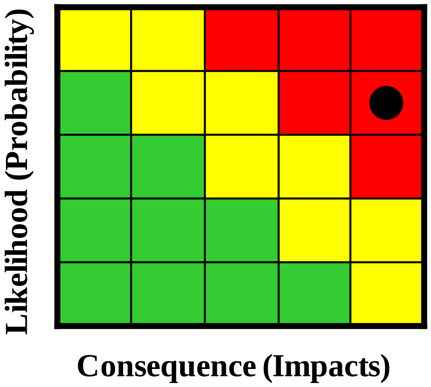
4.2.3 Operations and Maintenance (O&M) of the Security External Support System (ESS)



Risk Statement
IF the ESS RA and CA roles and responsibilities for operations, maintenance, and funding are not established THEN the ESS may not be efficiently managed. The Core System would be impacted if it is relying on an ESS for security credentials management, particularly regular, accurate CRLs to ensure that the Core's system users are adequately protected. Related to Risk: - Section 4.2.2, External Support System (ESS) for Security
Root Cause Driver
ESS RA and CA Enterprise roles and responsibilities need to be defined for efficient operation and maintenance.
Consequence (Impacts)
(Score: 5) The ESS roles and responsibility for operations and maintenance need to be defined especially for the IEEE 1609.2 (DSRC) Certificate distribution and CRL distribution, otherwise the Core System is impacted by poor operations and maintenance of CRL distribution and all *connected vehicle* environment users are impacted by poor O&M of the certificate distribution process.
Likelihood (Probability)
(Score: 5) This is an institutional issue which must be planned for and may take time to accomplish. The establishment of this ESS involves various interest groups, including System Users to define roles and responsibilities. With the great number of stakeholders that must agree on how this is done and continue to ensure that this security system is operational the likelihood is high that this risk will occur.
Overall Score: Red (High)

Risk Reduction Actions/Events	
1	Assess what the roles and responsibilities for the ESS are.
2	Develop a business model for continued solvency of the ESS, including how long term O&M will be funded and sustained.

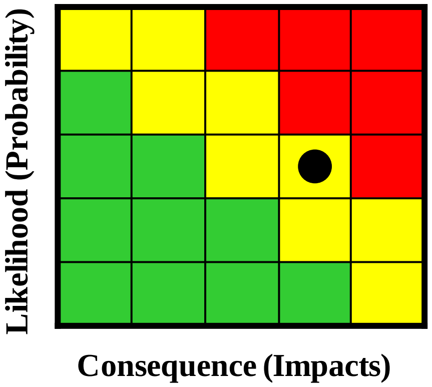
4.2.4 Security Management



Risk Statement
IF the Security Management Standards or Policies are not established nationally, including agreements on what constitutes misbehavior and how bad actors are removed THEN Core Systems and System Users could be vulnerable to the actions of unidentified malicious System Users, and the data provided to System Users may be suspect. Such policies need to include registration, expiration, revocation, and renewal of both IEEE 1609.2 (DSRC) as well as X.509 certificates. Revocation policies need to define what constitutes misbehavior and identify the appropriate response(s) for incidence of misbehavior. This should include how to handle devices that do not operate according to their specification but may simply have malfunctioned, as well as devices that operate in such a way as to indicate they may have been tampered with. Related to Risk: • Section 4.2.1, Role and Makeup of the Core Certification Authority
Root Cause Driver
Governance, Security Credentials Policy
Consequence (Impacts)
(Score: 5) Core Systems with different Security Management Standards or Policies may be incompatible.
Likelihood (Probability)
(Score: 4) This is an institutional issue which will involve planning among diverse interest groups, including System Users. The results of the Safety Pilot and other operational tests need to be used as inputs to this issue; however, at this time the likelihood is still high that this risk will occur.
Overall Score: Red (High)

Risk Reduction Actions/Events	
1	Use the lessons learned from Safety Pilot and Certification pilot to assess the need for a national policy or standard dealing with security management of the *connected vehicle* environment.
2	Investigate a potential role for the Core Certification Authority to provide oversight in establishing the security management Standards or Policies for the Core Systems, individually and collectively.
3	Establish criteria or thresholds to govern how misbehavior in the Core System is identified and how the information is provided to the ESS DSRC Certificate Authority for removal.
4	Establish a policy for the ESS DSRC Certificate Authority to accept or reject the Core System's CRL Change Request recommendation(s).

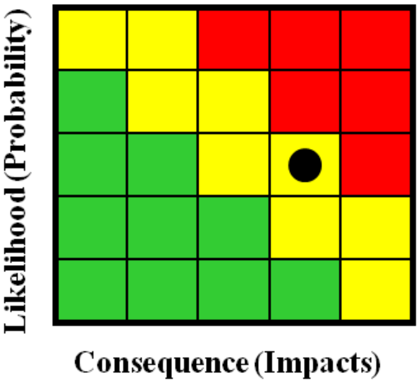
4.2.5 System Performance Management



Risk Statement
IF the System Performance Management standards are not established nationally THEN Core Systems could be governed inconsistently which could cause incompatibility issues or operational conflicts. With a concept of multiple core systems distributed across the country all supporting safety, mobility, and environmental applications, there should be a consideration to establish a framework of performance criteria to ensure that the overall environment is successful. Without it services could be inconsistent and system users could experience areas of spotty coverage or limits on what they can do. V2V Safety would not be affected necessarily. A policy regarding Quality of Service (QoS) for network traffic (e.g., probe data, map data, web traffic) carried over the telecommunications network that may span across geographic boundaries may be needed. While not strictly a Core System issue this affects the overall success of the environment. Where Core Systems must coordinate their services, having a QoS policy, or at least the framework to define such a policy, will increase the ability of the implementers and operators of Core Systems to work together efficiently. Related to Risk: • Section 4.2.1, Role and Makeup of the Core Certification Authority
Root Cause Driver
National System Performance Management standards
Consequence (Impacts)
(Score: 4) Core Systems with different System Performance Management standards may be incompatible.
Likelihood (Probability)
(Score: 3) This is an institutional issue involving various stakeholder interest groups, including System Users. This issue will be worked along with other policy/governance discussions such as the establishment of the Core Certification Authority but there is a moderate likelihood that this risk will occur.
Overall Score: Yellow (Medium)

Risk Reduction Actions/Events	
1	DOT should assess System Performance Management needs for a national policy or standard.
2	Investigate whether the Core Certification Authority could be used as oversight for establishing System Performance Management Standards or Policies for the Core Systems.

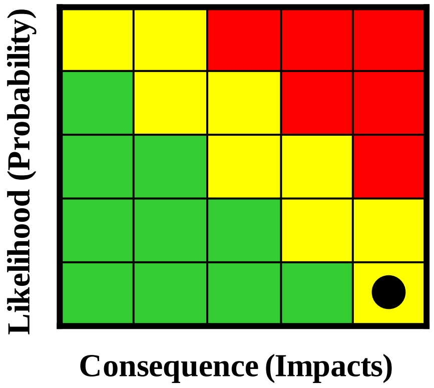
4.2.6 Privacy



Risk Statement
IF appropriate privacy laws and policies are not established and enforced on a consistent basis nationally THEN privacy violations may occur and system users could opt-out of using the Core System(s) if they believe their privacy is at risk. The Core System documentation supports the VII Privacy Policies Framework and specifies a system that protects data that may contain Personally Identifiable Information (PII) from unnecessary access. The framework should be modified to be consistent with the current vision of the *connected vehicle* environment. Primarily this means adapting the framework's concepts to an architecture with multiple Core Systems each potentially managed by a separate entity. Policy and/or laws or ordinances then need to define how entities manage PII and also how entities interoperate and share PII when necessary. These laws and policies should also identify when sharing of PII is justified, if ever. Additional provisions may need to be defined to maintain the privacy of communications between System Users as their data passes through a network. There may be a need to establish a mechanism to determine what data needs to be protected, including enforcement of the policies and standards.
Root Cause Driver
Lack of National Privacy Standards or Policies for *connected vehicle* Applications and Core Systems.
Consequence (Impacts)
(Score: 4) National privacy laws and policies, including enforcement of those policies, are needed to ensure no privacy violations occur. The Core System does protect data, by limiting the PII data that it collects or communicates and by securing (i.e. encrypts) the PII data it does have but any breaches with respect to personal data could cause a relatively high impact.
Likelihood (Probability)
(Score: 3) Privacy exists at some level, but national privacy laws and policies may have to be refined or established to include a discussion on enforcement of violations to the policy. VII Privacy Policies Framework provides the background and a good foundation to continue research in this area as well as legislation for online privacy that is being debated so the probability of this risk remains relatively low.
Overall Score: Yellow (Medium)

Risk Reduction Actions/Events	
1	As *connected vehicle* technology matures, assess and investigate the types of data likely to come to or through the Core System that need to be kept private.
2	As *connected vehicle* technology matures, assess whether national privacy laws or policies need to be updated/written to include enforcement of violations.

4.2.7 Device Certification



Risk Statement
IF the Device and Application Certification for On-Board Equipment (OBE), Retrofit, and Aftermarket DSRC Devices is not available and consistent THEN those devices would not be interoperable with other devices and with the Core System. Devices will need to be certified to ensure that they meet the standards or specifications defined for interaction with the Core System and with each other. Similarly for applications that interact with the Core, there needs to be a means by which an authority can certify that the applications meet national standards or define specifications for application behavior wherever they are deployed. Related to Risk: • Section 4.2.1, Role and Makeup of the Core Certification Authority
Root Cause Driver
National Certification Process needed for DSRC Devices and Applications.
Consequence (Impacts)
(Score: 5) The On-Board Equipment (OBE), Retrofit, and Aftermarket DSRC Devices and Applications may not be compatible or interoperable, thus increasing collisions and reducing transportation.
Likelihood (Probability)
(Score: 1) There has been some progress with Device Certification for the Pilot Program. This needs to continue for all devices, as well as certifying Applications for those devices.
Overall Score: Yellow (Medium)

Risk Reduction Actions/Events	
1	Assess Application Certification, as well as continuing to mature the Device Certification.
2	Determine the potential need for a national authority to govern and certify DSRC devices and their Applications.

5.0 GLOSSARY

Table 5-1. Glossary

Term	**Definition**
Consequences (or impacts)	is typically made up of Cost, Schedule, and Technical factors with a mean score for the overall Consequence score.
Likelihood (or probability)	is defined as the percentage that the risk will occur
Risk	is a potential event, considering the probability that a decision or action will result in a negative or unwanted consequence, where the probability of each possible outcome is known or can be estimated. See Vehicle Infrastructure Integration (VII) Risk Management Plan, version 3.0
Risk Management	is the systematic approach to setting the best course of action under uncertainty by identifying, assessing, controlling, and monitoring risk issues. See Vehicle Infrastructure Integration (VII) Risk Management Plan, version 3.0