ITS Risk Analysis

Prepared by:

Lockheed Martin Federal Systems
Odetics Intelligent Transportation Systems Division

Prepared for:

Federal Highway Administration
US Department of Transportation
Washington, D. C. 20590

June 1996

TABLE OF CONTENTS

EDL# 5402 – “National ITS Architecture Documents: Implementation Strategy; U.S. Department of Transportation”

EDL# 5403 - "National ITS Architecture Documents: Standards Requirements; U.S. Department of Transportation"

EDL# 5404 – “National ITS Architecture Documents: Standards Development Plan; U.S. Department of Transportation”

EDL# 11863 - "National ITS Architecture Documents: Market Packages - A Tool for Viewing, Accessing and Utilizing the National ITS Architecture; U.S. Department of Transportation".

Table of Contents

Executive Summary

Introduction

Risk analysis plays a key role in the implementation of an architecture. Early definition of the situations, processes, or events that have the potential for impeding the implementation of key elements of the ITS National Architecture is a critical element to the success of that implementation.

The focus of risk assessment for an architecture differs somewhat from that for marketing and deploying a specific product. Much more attention must be given to institutional and organizational issues that could prevent the implementation of various aspects of the architecture. On the technical side, the risk assessment must pay attention not only to the feasibility of a technology to meet the user service requirements, but also must consider the capability of multiple approaches or technologies to meet the requirements. Also, the capability for new products and technologies to be introduced over time is important to the sustained success of the overall deployment.

Methodology

The risk analysis used the following three step approach: Identify, Assess, and Mitigate.

Risk Identification

Identification was accomplished by a structured search for a response to the question - *What events may reasonably occur that will impede the achievement of key elements of the ITS architecture?* In addition to a word description, identification included: classification into one of the eight categories, each category being subdivided into several classification; which element of the architecture was affected; selection of one of five risk bearers; and which portion of the product life cycle was affected.

Risk Rating

Rating identifies the importance of the risk to the goals of the architecture. It comes as a response to the questions - *What is the probability that this risk will occur?* and *What is the severity of the impact on the architecture if a risk is allowed to take place?*

Rating was accomplished by estimating the probability of occurrence and severity of risk impact. Each of these two groupings was rated as either High, Moderate, or Low.

A combined, overall rating was established as the final element of risk rating. The output of this task was a listing of all risks categorized into three groups: Red risks (High), Yellow risks (Moderate), and Blue risks (Low).

Risk Mitigation

Mitigation establishes a plan which reduces or eliminates risk impact to the architecture's deployment. The question is - *What should be done, and whose responsibility it is to eliminate or minimize the risk?* Options available for mitigation are: control, avoidance, or transfer.

Identification

The identification process consisted of gathering the Red risks identified by the four architecture teams in Phase I and augmenting this list with a set of previously defined yellow risks for further analysis. Their applicability for the combined Phase II architecture was determined. This large body of completed analysis provided an excellent starting point. This yielded a total of 61 risks that were analyzed. As the program continued and the architecture completed the risks were re-evaluated and their descriptions have been updated.

Assessment

During the assessment step the combined list of risks from phase I were reassessed. This yielded a total of 10 Red risks, 36 Yellow risks, and 3 Blue risks out of the 61 risks that were analyzed. Twelve risks were combined after analyzing across the 4 teams.

A total of 10 risks have been identified and assessed as Red. The table on the following page summarizes information on risk identification and rating. Only Operating Costs & Maintainability is not represented in the set of red risks. The risks are also evenly spread across the architectural elements: Center, In-Vehicle, Communication, and Highway Infrastructure. Of the 4 possible life cycle stages, only Production is not represented by a red risks. Half of the risks are assigned to Deployment & Sales.

Of the stakeholders that will bear these risks, the consumers bear more than the other groups. The risks are also spread fairly evenly across the three scenarios (Urban, Inter-urban, and Rural) as well as the three time frames used in the evaluation (5-years, 10-years, and 20-years from 1992).

Mitigation

Mitigation strategies for each Red risk have been defined. These typically involve a set of actions to be taken by the sector(s) which shoulder the responsibility for the reduction of that risk. An example of the one developed for the Technical Immaturity risk of the AVSS products is given below:

TF-2.1 Technology Immaturity

Mitigation Category: Transfer
Mitigation Handler: Government, Private Producer

While the private sector will naturally develop some AVSS features such as lateral and longitudinal collision warning, they have little reason to develop other features such as intersection collision warning. Government can play a key role in speeding the development of advanced technology for safety systems.

- The government should fund testing and evaluation of Advanced Vehicle Safety Systems (AVSS) related technologies to speed maturity and deployment.
- In partnership with private producers, a government backed test and development program should include the use of an intersection grid track for operational testing.
- Employ advanced software modeling and simulation programs that address all known threatening situations.

While a lot of technology choices exist for implementing AVSS type systems, they have until recently been developed for the military. To adapt them to a commercial environment will require careful testing and integration with commercial technologies.

Summary

ITS spans a wide array of services, sectors, and users. The risks identified spread across sectors and phases of deployment. No one area stands out as an overall high risk area. The risks inherent in deployment of ITS may slow one aspect or another, but the overall effort will continue to develop and deploy.

Red Risk Summary

Category	Classification	Description	Architecture Affected	Probability of Occurrence	Severity of Impact
Technical Feasibility	Technology Immaturity	While incorporating or adapting existing technologies, the architecture may require new or currently immature	In vehicle	M	H

		technologies (e.g.: wireless wide area data communications, vehicle guidance and control components) which may result in the use of unproved or unacceptable system components.			
Technical Feasibility	AHS Functional Failure	Failure on an automated highway will seriously impact safety. Failure will also dramatically increase congestion on the AHS. Therefore, it will be necessary to design AHS so that systems can only fail soft, i.e., with safe reversion to manual control. This requires stringent fail safety criteria.	In vehicle	M	H
Market Acceptance	Privacy concerns	Concerns about the misuse of information related to the tracking of individual traveler Origin-Destination data, travel speeds, vehicle occupancy, etc. could impede market acceptance unless assurances are made to the public concerning data security and how data will be used and stored.	Total System	H	M
Market Acceptance	Rural Market	The rural ITS market, in areas which are not serviced by cellular telephone, needs satellite communications for MAYDAY and for traffic surveillance via Automate Road Signing Beacons, but the market size for this equipment will be small. The risk is that this may cause the cost of these products (equipment purchase plus user fees) to be too expensive to be viable.	Communications	M	H
Market Acceptance	Cost of Communications Does Not Drop	Wide area wireless data communications capabilities may not be deployed widely enough or pricing options and costs may remain too high for many ITS consumers thus market penetration will not rise as expected.	Communications	H	H
Operational Performance	Insufficient timeliness of information	Without rapid and efficient dissemination of traffic information, the end user may encounter problems that he or she purchased the system for the purpose of avoiding.	Communication	H	H
Institutional and Legal	Perceived Harmful By-Products: Safety, Environment	Adverse health, safety, and environmental impacts may be associated with the deployed systems. This may result in failure to gain the support of public and advocacy groups, (e.g. widespread use of collision avoidance radars in vehicles could cause radiation fears).	In vehicle, Highway Infrastructure, TMC	M	H
Organizational	Requires New Public & Private Partnerships	Reluctance by either the public or the private sectors could prevent deployment of TMS and ISP public-private partnerships.	TMC	H	M
Budget & Financial	Competition for Limited Capital Funds	Lack of government funds and clearly demonstrable benefits could prevent initial construction of TMS and other infrastructure by limiting the capital funds available for deployment of key architecture elements.	TMC	M	H
Budget & Financial	Decisions affected by budgetary instability	The risk to highway infrastructure improvement occurs in the O&M stage due to the lack of a steady, dependable flow of funding.	Highway Infrastructure, TMC	M	H

1.0 Introduction

The primary objective of this analysis is to identify the critical risks which could delay or prevent the deployment of the ITS system architecture and recommend mitigation plans which will eliminate or reduce these risks to the deployment process.

Analysis of an architecture is a complex task which requires consideration of a large number of potential issues. Unlike deployment of a physical system which typically involves a predominance of tangible issues such as technology, cost, manufacture, and maintenance, architecture analysis requires consideration of additional elements such as organizations, individuals, laws, opinions, economics, events and activities. These present a variety of ”what if” conditions which can have a serious risk impact and are difficult to quantify.

Risk identification and assessment covers a wide field, and consequently, the evaluators must have access to those elements which shape the development of the architecture and its deployment. Figure 1 illustrates these influences and their relationship to this study. Infusion of appropriate information to the risk analysis is being accomplished by direct involvement of team members participating in these various tasks.

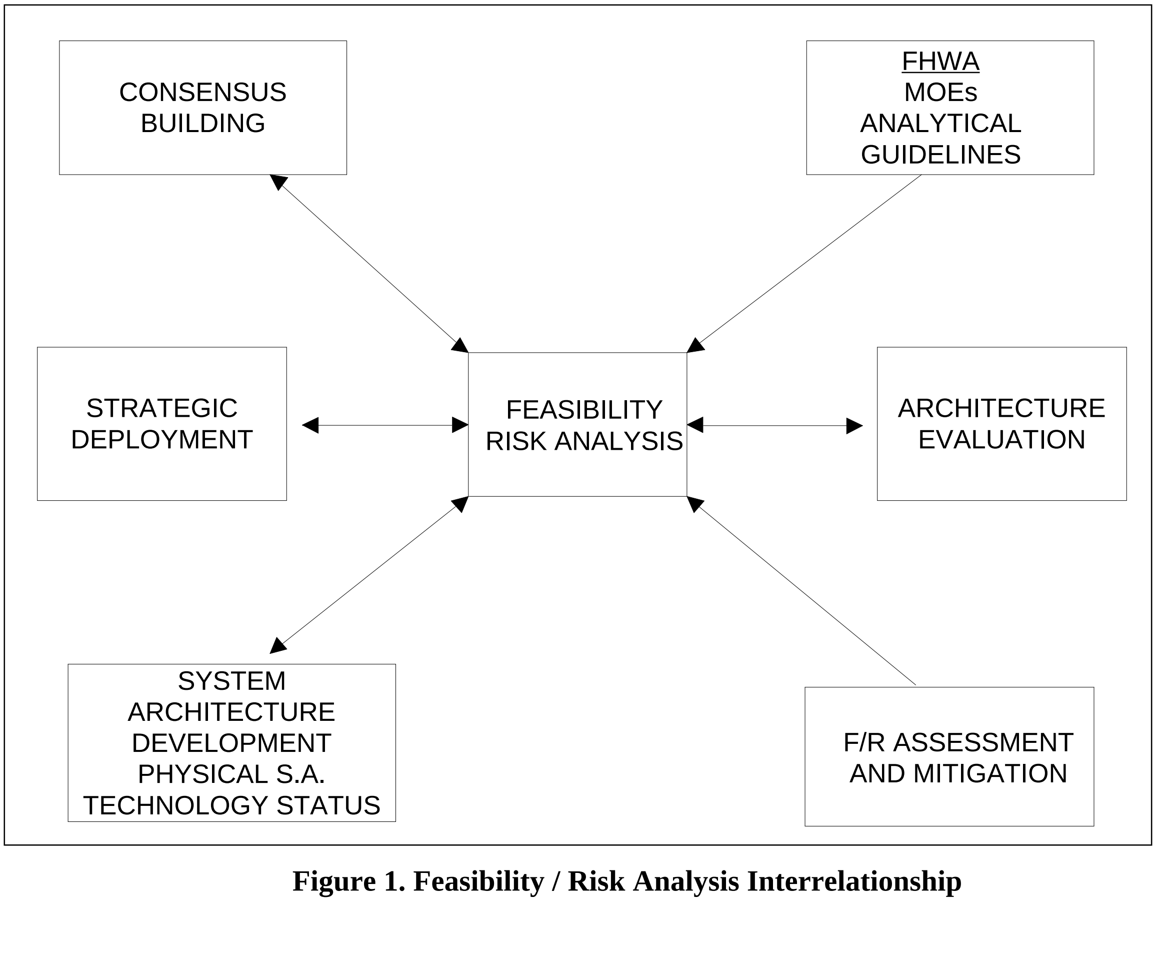

Figure 1. Feasibility / Risk Analysis Interrelationship

2.0 Risk Analysis Methodology

2.1 Methodology Overview

The Risk analysis consists of three tasks -- Identification, Rating, Mitigation. These represent a sequential process, which lends itself to organized procedures, with specific tasks and objectives.

Risk Identification

Risks are identified in response to the following question: *What events may reasonably occur that will impede the achievement of key elements of the ITS architecture?*

Occurrences having outcomes that are irrelevant to the architecture's goals present no risk. The primary output of the identification process includes a description of each risk, applicable risk category, stakeholder affected, and life cycle of the product at which the risk is most likely to occur.

Risk Rating

Rating identifies the potential of a risk to impact the goals of the architecture. The basic questions to be answered are: *What is the severity of the impact on the architecture if a risk is allowed to take place?* and *What is the probability that this risk will occur?*

Risks are rated on the basis of probability of occurrence, and the severity of impact. Through the application of appropriate processes, the risks are categorized into Red (high), Yellow (moderate), and Blue (low) categories.

Risk Mitigation

A plan that would reduce or eliminate the highest risks. The key question is: *What should be done and who is responsible to eliminate or minimize the risk?*

The mitigation plan includes a description of the actions that can be taken to mitigate the red rated risk and assigns a primary handler for the action.

The actual methodology for the these steps entails more complexity than is apparent from this overview. The process is shown in Figure 2 with details discussed in the following sections.

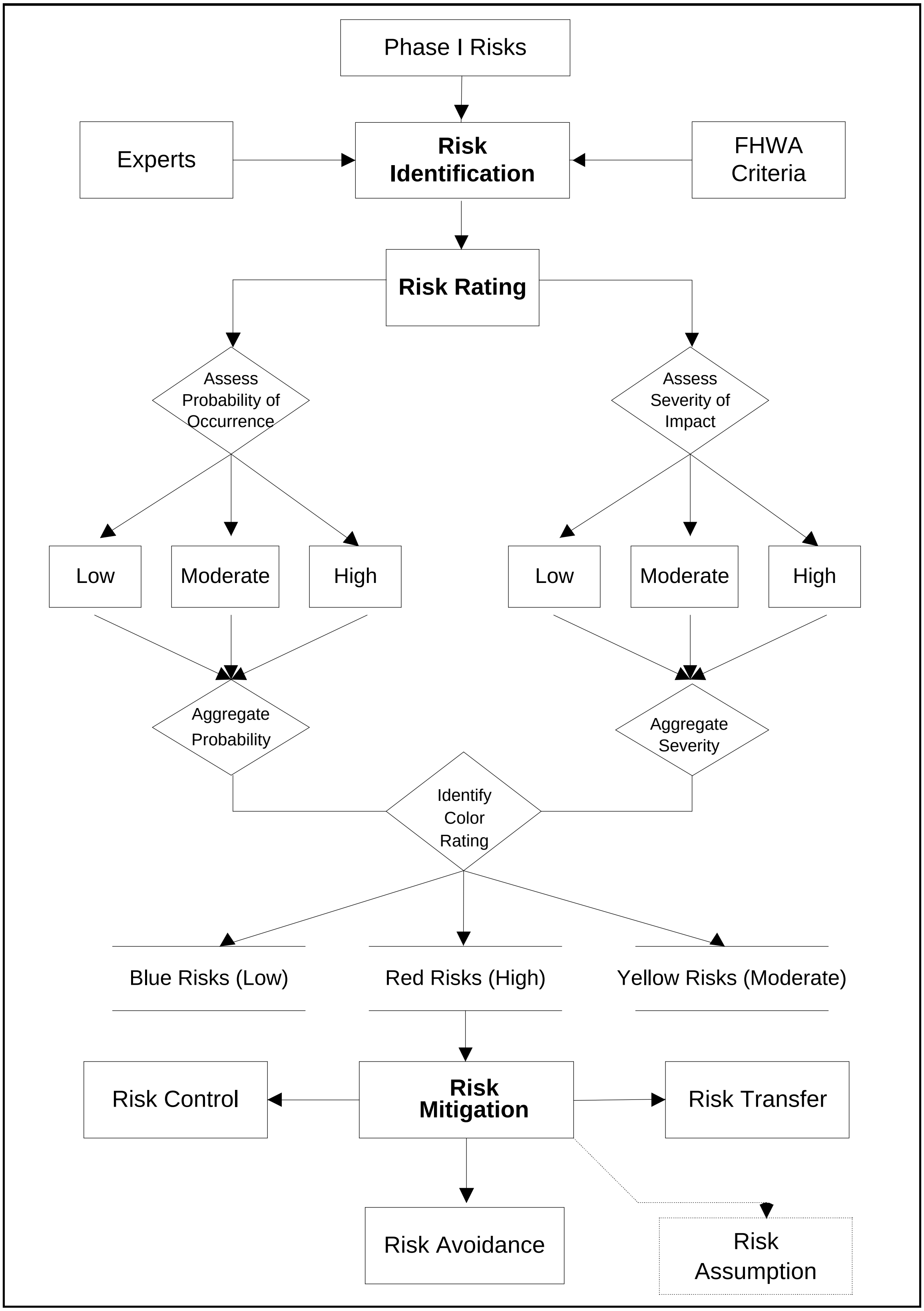

Figure 2. Risk Analysis Process

2.2 Risk Identification

The objective of this step is to identify and describe all potentially important risks pertaining to the architecture and its deployment.

These must be addressed over the life span of the deployment of architecture elements, from research through deployment, operation, and maintenance. Risks must be classified according to the major subsystems and components and to which stakeholders are most likely to bear the risk.

The issues to be addressed relate to those risks that will be important to the deployment of ITS services using the architecture. The general method for identifying these risks will be the examination of several elements in order to identify, describe, and categorize each risk. These elements are identified as follows:

- Life Cycle stages which include research, development, production, deployment or sales, and operation and maintenance.
- Which stakeholders are most likely to bear the risk: government, private producers, information service providers, commercial consumers, or private consumers.
- Major subsystems and components of the architecture. This may also include example deployments.
- Risk categories for each stage of the ITS life cycle. This can include elements such as: technical feasibility, cost to produce, market acceptance, operational performance, operating costs and maintainability, institutional and legal, organizational, budget, and financial.

The High (Red) and some of the Moderate (Yellow) risks identified by the four Phase I architecture teams have been reevaluated to determine if they are valid for the combined Phase II architecture. This large body of completed analysis provides a good starting point. Then any new risks will be identified using the methodology outlined in this section.

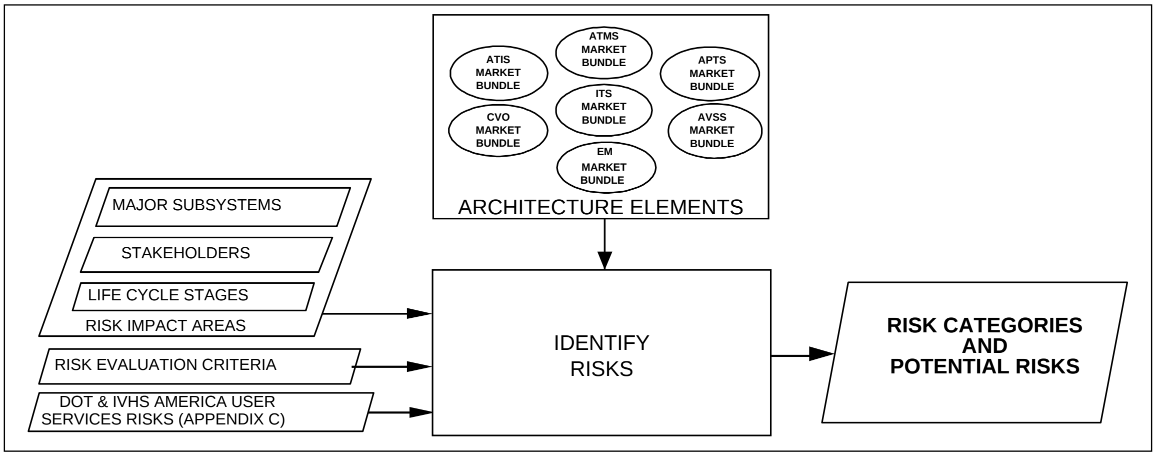

Figure 3. Risk Identification Approach

Risk identification will be addressed by a structured, multi-step approach (See Figure 3) based on logical, functional or physical groupings of the architecture elements.

The analytical procedure for risk identification will follow the outline listed below.

1) Consolidate the risks identified by the phase I teams and determine their applicability against the Phase II combined architecture. Some risks may have been specific to one of the Phase I architectures.

2) Generate tables of risk categories by life cycle stages and by affected stakeholder group. This initial set of risks will be generated by consensus work groups within the teams. Build upon the categories/risks that are applicable from step 1 and add any additional items that may arise from an analysis of the Phase II architecture.
3) Using the output from step 2 generate descriptions of the identified risks (both the carry-overs from Phase I and any new risks). This task is performed by individual or work groups from the team with relevant expertise. The objective is to obtain a more concise definition of the risk category, a brief description of the risk, and the areas of the architecture and/or its functionality which could be affected.

The quantity of combinations to be analyzed is reduced by a rational examination of each of the three timeframes. Supporting this approach is the spiral or iterative method of architecture development, and the modeling and evaluation tasks. These provide alerts to any new combinations for risk analysis.

All three time frames are considered in the analysis. This dimension contains critical considerations attendant with growth in technical capability, increasing acceptance by users and operators, increasing pressures for congestion reduction, and the potential for cost reduction inherent in market growth conditions.

The outputs from the risk identification process are tabulated under the following headings:

1) Risk ID - A code number for reference and data retrieval purposes. It consists of a letter designation corresponding to the risk category, a number corresponding to one of the primary system elements affected by the risk designation, and a sequential number. For example, BF-1.7 corresponds to the seventh entry for risks in the Budget & Finance category which impact the TMC, primarily.
2) Category - These 8 categories, suggested by the Phase I Guidelines, span a complete range of risk areas:
   - Technical Feasibility
   - Cost to Produce
   - Market Acceptance
   - Operational Performance
   - Operating Costs and Maintainability
   - Institutional and Legal
   - Organizational
   - Budget or Financial
3) Description - A concise description of the risk, intended to provide a stand-alone, non-technical description generated by the risk identifier.
4) Architecture Affected - The first, underlined entry indicates the source and location of the risk. Subsequent entries identify other areas of the architecture that are affected by the risk.
5) Risk Bearer - or Stake Holder. They are:
   - Government (Federal, State, Local or other)
   - Private Producers
   - Information Service Providers
   - Commercial Consumers
   - Private Consumers

2.3 Risk Rating

The objective of this step in the risk evaluation process is to assign to each identified risk a rating which considers the probability of occurrence of the risk, and the severity of impact if the risk occurs.

Risks are classified on the basis of probability of occurrence, defined as the likelihood of the risk occurring; and severity of impact, defined as the risk to be borne if no preventative action is taken.

Probability of occurrence will be rated on the basis of FHWA-supplied definitions of High, Moderate, and Low risks (see below). Severity of impact should be addressed by considering the primary categories of performance, cost, and likelihood of implementation. The last item focuses on whether the system or service will be fielded or not.

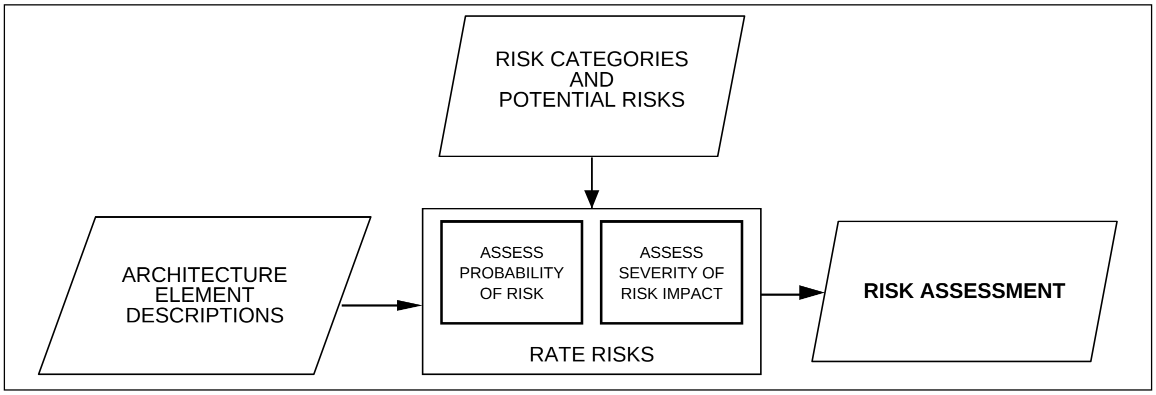
RISK CATEGORIES AND POTENTIAL RISKS
ARCHITECTURE ELEMENT DESCRIPTIONS
ASSESS PROBABILITY OF RISK
ASSESS SEVERITY OF RISK IMPACT
RATE RISKS
RISK ASSESSMENT

Figure 4. Risk Rating Approach

The risk ratings that were assigned to the Phase I risks are reassessed against the Phase II architecture. A rating will be applied for each of the 3 timeframes (5, 10, 20 year) and 3 scenarios (urban, inter-urban, and rural). For example, determine the likelihood that a particular risk will occur in the 10 year time frame in the urban scenario and what will be the impact in that situation compared with other situations.

The rating assessment is assigned first by individual team members followed by interactive group review for finalization of the assessments.

Three classifications will be used to denote Red (High),Yellow (Moderate), and Blue (Low) criticality. The final output of this task will be a report on all Red and Yellow risks.

To accomplish the risk rating the following approach as shown in Figure 4 on page 13 is used:

1) Determine the Probability of Risk occurrence and assign values of Low, Moderate, or High based on the following scale:

• Low:	0-9% likelihood of occurrence
• Moderate:	10-29% likelihood of occurrence
• High:	30-100% likelihood of occurrence

2) Determine the Severity of risk impact to any of the following aspects of the architecture: performance, cost, and likelihood of implementation. High, Moderate, and Low values are assigned to each of the three impact categories. They are then aggregated for each risk by selecting the highest of the separate impact ratings.

   High, Moderate, and Low are assigned based on the following scale:

• Low:	Insignificant or negligible risks

- Moderate: Will result in “significant” disruption of system implementation, increase of costs, or degradation of performance
- High: Will result in architecture failure or termination, extremely poor performance or extremely high costs

3) Determine the summary risk rating for each risk identified. The summary rating will be determined using the rating scheme defined in Table 1.

Table 1.Risk Rating Scheme

RATING	PROBABILITY	SEVERITY
RED	High High Moderate	High Moderate High
YELLOW	High Moderate Low	Low Moderate High
BLUE	Moderate Low Low	Low Moderate Low

4) Finally, a report on all Red and Yellow risks is generated with the following information:
   - Description of the Risk
   - The assigned risk category
   - The ratings for probability and severity
   - The life cycle stage in which the risk occurs
   - Assessment of which stakeholder groups are most affected.

In the area of market penetration, risks are assessed by analyzing the product or service’s ability to capture a threshold percentage of the competing markets. Estimation of these thresholds are based on the conclusion drawn from case studies in comparative industries (cellular phones, portable computers, cable TV, credit/debit card services).

2.4 Risk Mitigation

The objective of this step is to identify risk mitigation strategies for each of the risks identified and rated as red. The mitigation categories to be considered are: risk control, risk avoidance, risk transfer, and risk assumption.

The key issues in Risk Mitigation involve the actions that must be undertaken to reduce or eliminate each risk identified previously. The actions taken fall into one or a combination of the following categories:

- Risk Control
- Risk Avoidance
- Risk Transfer
- Risk Assumption

Risk Assumption refers to the conscious decision by the affected party to accept the risk. It must also identify what stakeholder group would be responsible for, or would undertake any of the risk mitigation actions.

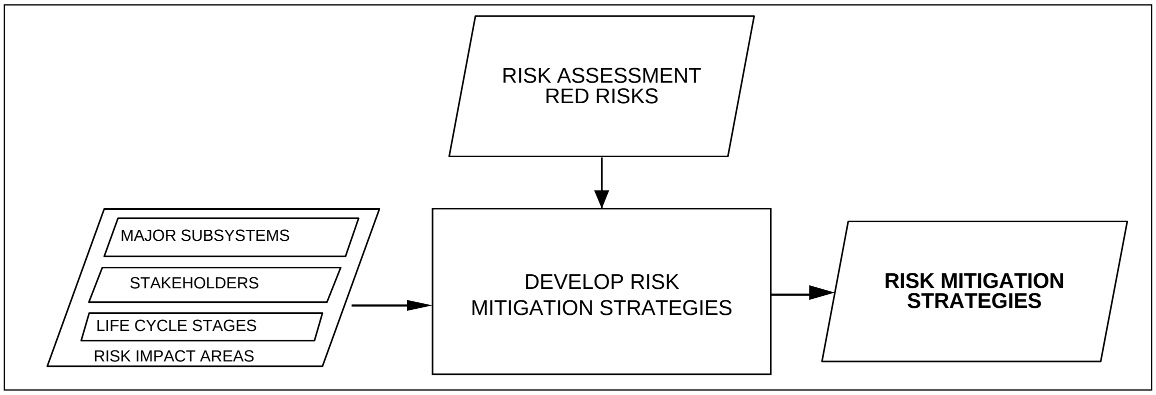

Figure 5. Risk Mitigation Approach

As illustrated in Figure 5 the risks assessed as red are examined with respect to the major impact areas to develop effective mitigation strategies or courses of action which could be taken to reduce or eliminate risk impacts. As an alternative to mitigation the team may consider, and if appropriate, recommend risk assumption. This is considered a viable option only in those cases where the level of risk can be safely assumed.

To compile a risk mitigation strategy the following tasks are performed:

1) Each risk defined as Red (High) in the previous analysis is evaluated against the categories of risk control, risk avoidance, risk transfer, and risk assumption. This provides a first level of evaluation.
2) A second level of evaluation is conducted at joint meetings, where the inputs of a variety of groups within the teams will be coordinated.
3) The output is a mitigation plan that incorporates details of tasks, timing and responsibilities to mitigate the risk.

The output of this analysis will be the specific recommendations for mitigating Red (High Level) risks.

3.0 Identification of Risks

This section addresses two risk groupings. The first grouping includes risks identified by the architecture teams including risks which were identified during Phase I by the four different architecture teams as well as any new risks identified during Phase II. The second group consists of specific risk statements identified at the outset of the program for the purpose of evaluating the architecture design. As one would suspect, there could be commonalties, however, the structure and definition of the second group makes it convenient to treat the analysis of the two groups on a separate basis.

Because risks have been gathered from several different sources an attempt at consolidation has been made in order to facilitate a better understanding of the risks. The Phase I Risks that have been brought over from the 4 different Phase I teams are identified followed by any new risks that have been identified during Phase II.

3.1 Structure for Risk Identification

To aid the risk identification process, risks are identified by the major subsystems of the architecture. Then the risks are considered from the perspectives of who would bear the risk and at what stage the risk would occur.

The four major architectural groupings used to categorize the risks are:

- Center - including centers for traffic management, transit management, emergency management, independent service providers, and commercial vehicle fleets
- In-Vehicle - including private vehicles, transit vehicles, emergency vehicles, and commercial vehicles
- Communication Infrastructure - including both wireless and wireline components
- Roadway Infrastructure - including all of the roadside components as well as parking facilities, commercial vehicle stations, and toll plazas.

All potential risks were identified by stakeholder groups most likely to bear the risk. Different stakeholders will bear risks differently so by considering risks in terms of stakeholders a more effective mitigation plan can be devised. The five major stakeholder considered are listed in Table 2.

Table 2.Risk Bearers (Stakeholders)

Stakeholder	Definition
Government agencies (G)	Federal, State and Local agencies with primary responsibility of governing, regulating, managing, and funding ITS.
Private Producers (PP)	Manufacturers or builders of ITS related products, financed by the private sector or funded by government agencies, motivated by profit or fee.
Information service providers (ISP)	Providers of ITS traveler information either financed by private institutions and motivated by service fee, or contracted by government agencies to provide ITS services for a fee.
Commercial consumers (CC)	Users of the ITS while plying their business.
Private consumers (PC)	Users of the ITS for personal purposes.

The risks are identified by life cycle stage of the architecture implementation. Different risks can occur at various stages of the ITS architecture implementation. Four distinct life cycle stages were considered and are listed in Table 3.

Table 3.Risk Life Cycle Stages

Stage	Definition
Research and Development (R&D)	Covers the period that starts when an idea is conceived through the proof-of-concept to the development of a prototype.
Production (P)	Covers the period during manufacture or construction of an ITS architecture element or component.
Deployment and Sales (D&S)	Covers the period during which the component or service is being marketed, sold, and installed.
Operations and Maintenance (O&M)	Covers the period after installation when an ITS architecture element or component is in operation and is being routinely maintained and repaired, if necessary.

Using the FHWA guidelines risks were finally grouped into eight different categories:

- Technical Feasibility: Concerned with whether a product or system can be developed and then manufactured in quantity.
- Cost to Produce: Deals with issues that tend to raise production costs.
- Market Acceptance: Considers whether a product or service can be sold to a purchaser in the market place.
- Operational Performance: Focuses on how a system performs after it is deployed.
- Operating Costs and Maintainability: Covers the ability to obtain and afford desired functionality of product over its lifetime.
- Institutional and legal: Includes situations and events that involve non-participatory stakeholders.
- Organizational: Includes situations that occur within participating agencies and organizations.
- Budget or Financial: Covers issues related to limited financial resources.

3.2 Phase I Risks

This is the first step in the Phase II Risk Analysis. The red risks identified by the four Phase I teams are listed as well as several of the yellow risks from the Loral and Rockwell phase I studies.

The tables were presented to the Technical Review Team in a similar format to foster discussion about there risks and to trigger thoughts about any new risks. The risks shown here need to be assessed against what is now known about ITS - the architecture and deployment strategies. The risks will be shown again in section 4 where assessments are recorded.

The risks in the following tables are sorted by the category under which each risk was identified.

An attempt has been made to standardize the data from the four teams. For instance, the Westinghouse subsystem called “Transit Fleet Management” was changed to “TMC (Transit)” to be more compatible with the other teams’ Phase I risks. Rockwell identified and classified risks by market bundle which may have spanned subsystems. All of the red risks belonged to the Advanced Vehicle Safety System (AVSS) market bundle. In the list of yellow risks the market bundle for which the risk was written has been added to the risk description. Risk IDs have been added to the risks in a manner consistent with Loral's Phase I naming convention described in Section 2.2 "Risk Identification". This Risk ID will make it easier to track the risks in later parts of this document.

3.2.1 Phase I Red Risks

Table 4 through Table 7 on pages 18 through 21 contain the risks that were rated "Red" by the Phase I architecture teams.

Some edits have been made to the descriptions and other fields to bring the risks more inline with the Phase II architecture.

3.2.2 Phase I Yellow Risks

Table 8 and Table 9 on pages 21 through 23 list some of the yellow risks identified during Phase I by the Loral and Rockwell teams. These risks will be analyzed against the Phase II architecture.

The yellow risks identified during phase I were risks in which the combination of Probability of Occurrence and Severity of Impact was either "High/Low", "Moderate/Moderate", or "Low/High".

The methodology for selecting yellow risks for inclusion in the following tables was different for the Loral and Rockwell Phase I documents. For Loral phase I, the list of 248 yellow risks in Appendix A of the Feasibility Study were reviewed. A yellow risk was selected for this list if the "Probability of Occurrence" value and all of the "Severity of Risk Impact" values were "M". The thought being that if one of those two values had been changed to an H, then they would have appeared as Red risks in the Phase I analysis. A risk was also selected if any of its values were an "H". This still produced a list of 75 risks. This list has been further reduced by selecting the risks that had an "H" for any of its values and by selecting the risks that were applied to "All" timeframes and scenarios.

For the Rockwell phase I document, the risks that were identified as Red risks in section 4 but were changed to yellow in section 5 were selected. Rockwell originally identified 28 red risks but after developing the mitigation strategies for them found that many could be reclassified if the strategies were employed. The result was that there were only 4 red risks left (see previous table) and of the remaining 24 risks, 16 were yellow and 8 were blue.

Table 4.Loral Phase I Red Risks

Risk ID	Category	Classification	Description	Architecture Affected	Risk Bearer	Life Cycle Stage
MA-1.1	Market Acceptance	Different Participation Levels by Areas or Regions	Every region or locality may adopt a different system or use different communication technology resulting in incompatibilities when drivers move from one area to another. This will reduce overall effectiveness of any system and the resulting benefits to the user.	TMC, ISP	CC, PC	D&S
MA-2.1	Market Acceptance	Acceptance of Increased Public Transit	The demand for public transit is inelastic. As long as users of the private auto are unrestricted, the transit alternative is unlikely to be adopted.	In-vehicle	ISP, CC, PC	D&S
MA-2.2	Market Acceptance	Acceptance of Commercial Vehicle Electronic Clearance	Commercial drivers may try to avoid being electronically tracked and verified.	In-vehicle	PP, CC, PC	D&S
MA-3.2	Market Acceptance	Cost of Communications Does Not Drop	Wide area wireless data communications capabilities may not be deployed widely enough or pricing options and costs may remain too high for many ITS consumers thus market penetration will not rise as expected.	Communications	CC, PC	D&S
MA-4.1	Market Acceptance	Inter-operability	Vehicles with proprietary smart cards and route guidance IVUs that use proprietary communication standards may not be interoperable to all areas of the country.	Highway Infrastructure	G, ISP, CC, PC	D&S
O-1.1	Organizational	Requires New Public & Private Partnerships	Reluctance by either the public or the private sectors could prevent deployment of TMS and ISP public-private partnerships.	TMC	G, ISP	D&S
BF-1.1	Budget & Financial	Competition for Limited Capital Funds	Lack of government funds and clearly demonstrable benefits could prevent initial construction of TMS and other infrastructure by limiting the capital funds available for deployment of key architecture elements.	TMC	G, ISP	D&S
BF-1.2	Budget & Financial	Competition for Limited Capital Funds	Non-ITS interests may have enough power to limit capital funds for architecture deployment.	TMC	G	D&S

Table 5.Rockwell Phase I Red Risks

Risk ID	Category	Classification	Description	Architecture Affected	Risk Bearer	Life Cycle Stage
TF-2.1	Technical Feasibility	Technology Immaturity	While incorporating or adapting existing technologies, the architecture may require new or currently immature technologies (e.g.: wireless wide area data communications, vehicle guidance and control components) which may result in the use of unproved or unacceptable system components.	In-Vehicle	PP	R&D
MA-2.3	Market Acceptance	Human Factors Problems	Inherent human factor demands or limitations may result in package not being accepted.	In-vehicle	PP, ISP	O&M
OM-2.1	Operating Costs and Maintainability	Software and Hardware Reliability	The architecture relies on hardware and software that are not robust and frequently fail, thereby resulting in significant maintenance costs being expended.	In-vehicle, TMC	PP, CC, PC	O&M
IL-2.1	Institutional and Legal	Perceived Harmful By-Products: Safety,	Adverse health, safety, and environmental impacts may be associated with the deployed systems. This may result in failure to gain the support of public and	In-vehicle, Highway	G, CC, PC	O&M

		Environment	advocacy groups, (e.g. widespread use of collision avoidance radars in vehicles could cause radiation fears).	Infrastructure, TMC		

Table 6.Hughes Phase I Red Risks

Risk ID	Category	Classification	Description	Architecture Affected	Risk Bearer	Life Cycle Stage
TF-2.2	Technical Feasibility	Inadequate Intersection Collision Avoidance	Failure of a collision avoidance system will seriously impact safety of the few vehicles involved. Therefore, the standards for safety and performance have been set very high.	In-Vehicle	PC	O&M
TF-2.3	Technical Feasibility	AHS Functional Failure	Failure on an automated highway will seriously impact safety. Failure will also dramatically increase congestion on the AHS. Therefore, it will be necessary to design AHS so that systems can only fail soft, i.e., with safe reversion to manual control. This requires stringent fail safety criteria.	In-vehicle	PC	O&M
TF-3.1	Technical Feasibility	MAYDAY reliability	MAYDAY messages must be successfully transmitted and received or the ”comfort level” of the user will be permanently lost. The risk is that a MAYDAY system which is perceived to be unreliable will not be bought.	Communications	CC, PC	O&M
MA-3.1	Market Acceptance	Rural Market	The rural ITS market, in areas which are not serviced by cellular telephone, needs satellite communications for MAYDAY and for traffic surveillance via Automate Road Signing Beacons, but the market size for this equipment will be small. The risk is that this may cause the cost of these products (equipment purchase plus user fees) to be too expensive to be viable.	Communications	CC, PC	O&M

Table 7.Westinghouse Phase I Red Risks

Risk ID	Category	Classification	Description	Architecture Affected	Risk Bearer	Life Cycle Stage
TF-1.1	Technical Feasibility	Complex system integration	Private producers will have to cope with integrating new products with a multitude of existing products, some of which are proprietary	TMC	PP	R&D
TF-2.4	Technical Feasibility	Stringent safety standards	Safety standards must be maintained while adding to driver mental load.	In-Vehicle	PP	R&D, P
PC-1.1	Cost to Produce	Compatibility with multiple standards	Need standards and protocols which allow for compatibility of the traffic control systems while continuing to allow the private sector protection of its products.	TMC	G, PP	P
PC-2.1	Cost to Produce	Stringent performance standards	Performance of the equipment must meet expectations and the equipment must not be prone to failure or vulnerable to sabotage.	In-Vehicle	PP	R&D, P
PC-1.2	Cost to Produce	Compatibility with multiple standards	Open standards may remove the market niche for some vendors, making them reluctant to be compatible.	TMC (Transit)	G, PP	R&D
PC-0.1	Cost to Produce	Market fragmentation	If the standards process is delayed a large number of incompatible services will be implemented.	Total System	G, PP	D&S
MA-4.2	Market Acceptance	Privacy concerns	Using video surveillance for information on the location of individual vehicles may be perceived as an invasion of privacy by the public.	Highway Infrastructure	G, PP	D&S
MA-1.2	Market Acceptance	Inter-operability of	There is a lack of inter-operability between subsystems which will take time	TMC (Transit)	G, PP, ISP	D&S

		equipment	to change.			
MA-0.1	Market Acceptance	Privacy concerns	Concerns about the misuse of information related to the tracking of individual traveler Origin-Destination data, travel speeds, vehicle occupancy, etc. could impede market acceptance unless assurances are made to the public concerning data security and how data will be used and stored.	Total System	G, PC	D&S
OP-3.1	Operational Performance	Insufficient timeliness of information	Without rapid and efficient dissemination of traffic information, the end user may encounter problems that he or she purchased the system for the purpose of avoiding.	Communication	CC, PC	O&M
OM-1.1	Operating Costs & Maintainability	Lack of openness complicates product mix & match	The transit system owner will not be able to purchase off-the-shelf subsystems and just plug them together.	TMC (Transit)	G, ISP	O&M
IL-4.1	Institutional & Legal	Legal privacy issues	There is a possibility that inappropriate levels of information will be available about the activities of private citizens.	Highway Infrastructure	G	D&S
BF-1.3	Budget & Financial	Decisions affected by budgetary instability	Expansion of responsibilities to provide ITS user services will exceed local resources for O&M.	TMC	G, PC	D&S
BF-4.1	Budget & Financial	Decisions affected by budgetary instability	The risk to highway infrastructure improvement occurs in the O&M stage due to the lack of a steady, dependable flow of funding.	Highway Infrastructure	G, PC	D&S
BF-1.4	Budget & Financial	Slow market growth hampers payback	There will be a long learning curve to convince the transit customers to purchase the new equipment.	TMC (Transit)	PP	R&D, P, D&S
BF-0.1	Budget & Financial	Decisions affected by budgetary instability	Removal of federal funding from the architecture development process and the associated standards setting process, could damage the ITS development and implementation.	Total System	G, PP, ISP, CC, PC	R&D, D&S

Table 8.Loral Phase I Yellow Risks

Risk ID	Category	Classification	Description	Architecture Affected	Risk Bearer	Life Cycle Stage
TF-1.2	Technical Feasibility	Number of & skill level of developers, maintainers, operators	An insufficient number of skilled workers will hamper deployment and limit the effectiveness of the system through an inability to properly maintain and operate.	TMC	G	D&S, O&M
TF-1.3	Technical Feasibility	Complex system integration	Unable to package or integrate different components or subsystems so that they continue to provide the capabilities that they can provide separately.	TMC	G	R&D
TF-1.4	Technical Feasibility	Algorithm development	Algorithm development is required to provide the improved performance of traffic control systems.	TMC	PC	R&D
TF-4.1	Technical Feasibility	AHS sensor reliability	The sensors required to make AHS operate must be developed with sufficient reliability to provide operation in all climatic conditions.	Highway Infrastructure	G	D&S
MA-2.4	Market Acceptance	High cost of emergency notification and personal security	Current estimates of emergency notification costs are in the range of $200 to $400. This may still be too high in comparison with the other vehicle options competing for the $2000 consumers generally spend on vehicle electronics.	In-vehicle	ISP, PC	D&S
OP-3.2	Operational Performance	Insufficient timeliness of information	During peak periods of usage time, critical information handling may be slowed significantly.	Communications	ISP	D&S

OM-1.2	Operating Costs & Maintainability	High maintenance costs	Cables for traffic control and surveillance communications may result in significant operational and maintenance costs. Operators may be inclined not to deploy to the levels required by ITS operations.	TMC	G	O&M
IL-2.2	Institutional & Legal	Spectrum availability	Limits number of users of wireless ITS services	In-Vehicle	PP	D&S
IL-3.1	Institutional & Legal	Spectrum limits market	Limited bandwidth restricts number of ITS users.	Communications	ISP	D&S
IL-3.2	Institutional & Legal	Impacts market of competitive industries	Availability of “MAYDAY or “PANIC BUTTON” may decrease demand for cellular phones or vice versa.	Communications	PP	D&S
IL-3.3	Institutional & Legal	Disruption to installed infrastructure & equipment	Backhoe cuts fiber cable that runs along highway right-of-way, disrupting service.	Communications	G, ISP	O&M
O-1.2	Organizational	Requires changes in standard operating Procedures	Govt. and bureaucracy employees may resist changes in procedures and unions may challenge efforts to privatize.	TMC	G, ISP	D&S
O-3.1	Organizational	One or more regions choose not to participate	Continental coverage of US dependent on other regional carriers offering the same wireless technology.	Communications	ISP	R&D
BF-1.5	Budget & Financial	Inability to attract capital markets	Private sector may not be willing to invest in TMC if public fund is not in place.	TMC	G, ISP	D&S
BF-2.1	Budget & Financial	Slow market growth hampers payback	Producers may experience financial losses if market growth rate is less than projected.	In-Vehicle	PP	D&S

Table 9.Rockwell Phase I Yellow Risks

Risk ID	Category	Classification	Description	Architecture Affected	Risk Bearer	Life Cycle Stage
TF-1.5	Technical Feasibility	Security requirement	ATIS, Adequate system security may not be accomplished due to multiple and open system access (e.g., to databases) which makes it possible for tampering or misuse by unauthorized parties.	TMC	PC	O&M
TF-2.5	Technical Feasibility	Complex functional requirements	AVSS, Inability of the architecture/ technologies to perform complex functions needed by the packages.	In-Vehicle	PP, ISP	R&D, D&S
TF-2.6	Technical Feasibility	Stringent Safety Standards	AVSS, New safety standards needed by the architecture may not be attainable or may result in unacceptable technical performance.	In-Vehicle	ISP, CC, and PC	O&M
TF-2.7	Technical Feasibility	Security Requirement	AVSS, The architecture may not be able to provide sufficient security, against tampering or misuse by unauthorized parties, while maintaining desired performance.	In-Vehicle, TMC, Highway Infrastructure	CC, PC	O&M
PC-2.2	Cost to Produce	Stringent Performance Standards	AVSS, Performance standards imposed by the architecture may be stringent (e.g., to ensure compatibility of products). This may result in high costs to produce the products.	In-Vehicle	CC, PC	O&M
MA-1.3	Market Acceptance	Low payback for	ATIS, Both private and commercial users may not get sufficient payback when utilizing this package. This may result in them discontinuing the	TMC	CC	D&S, O&M

		purchasers	service, or may dissuade others from obtaining this service.			
MA-1.4	Market Acceptance	Privacy concerns	ATIS, The architecture requires knowledge of vehicle's(both private and commercial) location. This requires collection and storage of the location information and may hinder package acceptance by individuals and organizations who may desire to keep their location information confidential.	TMC	CC, PC	O&M
MA-2.5	Market Acceptance	Interoperability of Equipment	AVSS, The architecture may not fully consider interoperability of equipment among vehicles, regions, and infrastructures. This may limit marketability of those products and services.	In-Vehicle, Highway Infrastructure	ISP, CC, PC	D&S, O&M
OP-2.1	Operational Performance	Insufficient timeliness of Information	ATMS, Information must be communicated to computers or to human decision makers in a timely fashion. The architecture/service value may be compromised if the information is not provided promptly.	In-Vehicle, TMC	CC, PC	O&M
IL-1.1	Institutional & Legal	Legal & privacy issues	CVO, Use of this package requires knowledge and possibly storage of users' location, plans, and financial data. While this data is confidential, there is always the possibility of leaks and hence user's reluctance to subscribe to the package.	TMC	ISP, CC	O&M
O-1.3	Organizational	One or more jurisdictions choose not to cooperate	ATIS, ATMS, and APTS require cooperation between many jurisdictions for deployment. Traditional barriers may inhibit successful deployment.	TMC, Highway Infrastructure	G, ISP	D&S, O&M
BF-2.2	Budget & Financial	Decisions affected by budgetary instability	APTS, Budget instability and uncertainty in the public sector will hinder the timely progress of evolutionary deployment. Affected especially will be those products with extended life cycles needing long term maintenance and replacement in the distant future.	In-Vehicle, TMC	G	O&M
BF-2.3	Budget & Financial	Inability to Attract Capital Markets	AVSS, This architecture may not be able to attract capital investments to finance development and deployment of the package.	In-Vehicle	PP	R&D
BF-2.4	Budget & Financial	Excessive Liability	AVSS, This package may create excessive liability for the private producers, service providers and ultimately the government.	In-Vehicle	G, PP	D&S, O&M

The acronyms in the Description column above refer to market bundles used in the Rockwell phase I architecture and are defined as follows:

- ATIS Advanced Traveler Information Service
- ATMS Advanced Traffic Management System
- APTS Advanced Public Transit System
- CVO Commercial Vehicle Operation
- EM Emergency Management
- AVSS Advanced Vehicle Safety System

4.0 Results of Risk Assessment

The design approach for the architecture is built around the goal of mitigating the numerous risks facing the deployment, acceptance, and operation of the ITS user services. Some of the user services are new and may be perceived as high risk since they have neither been tested in actual marketplaces.

The architecture is such that maximum utilization of existing infrastructure can be made, both in transportation and communication. The infrastructures that are emerging independent of the ITS architecture can also be leveraged. The purpose of this approach is to reduce the impact of the uncertainty inherent in offering the ITS services by both the private and public sectors. This approach lends itself naturally to incremental, evolutionary growth. It obviates the need for early unwarranted fiscal commitments by both sectors. By relying on technologies and infrastructures of proven, well understood performance with well established models, the stakeholder’s expectations can be more easily met.

A flexible and modular architecture mitigates the risks associated with variability across the national landscape and the disparate needs of thousands of jurisdictions.

This section presents the architecture risks that have been assessed as yellow or red. Building off of the identification process this section will contain tables that described the assessed probability and severity of a risks impact. This section will also identify the life cycle to which the risk is assigned and the scenario/timeframe in which a particular risk is yellow or red.

4.1 Assessment of Red and Yellow Risks

The risks identified in Section 3, both the carry overs from phase I and any new risks that have been added have been assessed using the methodology described in Section 2.

Risks are assessed for three time frames: 1997, 2002, and 2012. They are also assessed across the different scenarios: Urban, Inter-Urban, and Rural. In some cases a specific risk is pertinent to several combinations within the time and scenario matrix. These risks can be consolidated but only after completing the rating process to avoid masking the criticality of a risk within a particular time/scenario.

Contained in this section are the risks that were assessed as Red or Yellow according to the methodology described earlier. Mitigation strategies for the Red risks is provided in Section 5.

As mentioned earlier, the phase I risks have been distributed earlier for input into their assessment against the phase II architecture. That feedback from the Technical Review Team has been incorporated here.

4.1.1 Red and Yellow Risk Tables

Table 10 on page 26 shows all risks either rated red in Phase I or initially added as red in Phase II. Based upon the current architecture a new rating has been applied to each. Use the Risk ID field to tie each risk back to its description in Section 3. The rationale for the new rating is given in section 4.1.2, including the rationale behind changing formerly red risks to lower ratings. Table 11 on page 27 shows the reassessment of all yellow risks chosen for reevaluation. As will be noted, no yellow risks were raised to red status.

The “Aggregate Severity of Impact” field is the compilation of the Performance Impact, Cost Impact, and Implementation Likelihood fields.

Table 10.Assessment of Phase I Red Risks

Risk ID	Classification	Scenario & Timeframe	Probability of Occurrence	Performance Impact	Cost Impact	Implementatio n Likelihood	Aggregate Severity of Impact	Rating
MA-1.1	Different Participation Levels by Areas or Regions	All - 5, 10	M	M	L	M	M	Y
MA-2.1	Acceptance of Increased Public Transit	Urban - All	M	M	L	M	M	Y
MA-2.2	Acceptance of Commercial Vehicle Electronic Clearance	Inter-urban - 5,10	M	L	M	M	M	Y
MA-3.2	Cost of Communications Does Not Drop	All - 10, 20	H	H	H	M	H	R
MA-4.1	Inter-operability	All - 5	M	M	L	M	M	Y
O-1.1	Requires New Public & Private Cooperative Ventures	All - 5, 10	H	M	L	M	M	R
BF-1.1	Competition for Limited Capital Funds	All	M	H	M	M	H	R
BF-1.2	Competition for Limited Capital Funds	See BF-1.1 above						
TF-2.1	Technology Immaturity	All - 10, 20	M	M	H	M	H	R
MA-2.3	Human Factors Problems	Urban - All	M	L	M	L	M	Y
OM-2.1	Software and Hardware Reliability	Urban, Inter-urban - All	L	L	M	L	M	B
IL-2.1	Perceived Harmful By-Products: Safety, Environment	All - 10, 20	M	M	H	M	H	R
TF-2.2	Inadequate Intersection Collision Avoidance	Urban - 20	L	H	M	L	H	Y
TF-2.3	AHS Functional Failure	Urban - 20	M	H	M	L	H	R
TF-3.1	MAYDAY reliability	All	L	M	H	M	H	Y
MA-3.1	Rural Market	Rural - 10	M	M	H	L	H	R
TF-1.1	Complex system integration	Urban - All	M	L	M	M	M	Y
TF-2.4	Stringent safety standards	All - 5, 10	M	M	L	M	M	Y
PC-1.1	Compatibility with multiple standards	Urban, Inter-urban - 5, 10	L	L	L	M	M	B
PC-2.1	Stringent performance standards	Urban - 10, 20	M	M	L	M	M	Y
PC-1.2	Compatibility with multiple standards	All - 5, 10	L	M	L	M	M	B
PC-0.1	Market fragmentation	See MA-1.1 on previous page						
MA-4.2	Privacy concerns	All	M	M	M	M	M	Y
MA-1.2	Inter-operability of equipment	Urban, Inter-urban - 5, 10	M	M	L	M	M	Y
MA-0.1	Privacy concerns	All	H	M	M	M	M	R

OP-3.1	Insufficient timeliness of information	Urban, Inter-urban - 5, 10	H	H	M	M	H	R
OM-1.1	Lack of openness complicates product mix & match	Urban - 5, 10	M	L	M	M	M	Y
IL-4.1	Legal privacy issues	Urban, Inter-urban - All	M	L	L	M	M	Y
BF-1.3	Decisions affected by budgetary instability	See BF-4.1 below						
BF-4.1	Decisions affected by budgetary instability	All	M	H	H	M	H	R
BF-1.4	Slow market growth hampers payback	Urban - 5, 10	L	M	L	H	H	Y
BF-0.1	Decisions affected by budgetary instability	All - 5	M	M	M	M	M	Y

Table 11.Assessment of Phase I Yellow Risks

Risk ID	Classification	Scenario & Timeframe	Probability of Occurrence	Performance Impact	Cost Impact	Implementation Likelihood	Aggregate Severity of Impact	Rating
TF-1.2	Number of & skill level of developers, maintainers, operators	Urban, Inter-urban - 5	M	M	M	M	M	Y
TF-1.3	Complex system integration	See TF-1.1						
TF-1.4	Algorithm development	All	M	M	M	M	M	Y
TF-4.1	AHS sensor reliability	All	M	M	M	M	M	Y
MA-2.4	High cost of emergency notification and personal security	Rural - 5, 10	H	L	L	L	L	Y
OP-3.2	Insufficient timeliness of information	See OP-3.1						
OM-1.2	High maintenance costs	Urban - All	H	L	L	L	L	Y
IL-2.2	Spectrum availability	All	M	M	M	M	M	Y
IL-3.1	Spectrum availability limits market	All	M	M	M	M	M	Y
IL-3.2	Impacts market of competitive industries	All	M	M	M	M	M	Y
IL-3.3	Disruption to installed infrastructure & equipment	All	M	M	M	M	M	Y
O-1.2	Requires changes in standard operating Procedures	All	M	M	M	M	M	Y
O-3.1	One or more regions choose not to participate	Urban, Inter-urban - 5	L	H	H	H	H	Y
BF-1.5	Inability to attract capital markets	All	M	M	M	M	M	Y
BF-2.1	Slow market growth hampers payback	All	M	M	M	M	M	Y
TF-1.5	Security requirement	Urban - 5	L	H	M	M	H	Y
TF-2.5	Complex functional requirements	Urban - 20	M	M	M	L	M	Y

TF-2.6	Stringent Safety Standards	See TF-2.4						
TF-2.7	Security Requirement	Urban - 20	L	H	M	L	H	Y
PC-2.2	Stringent Performance Standards	See PC-2.1						
MA-1.3	Low payback for purchasers	All	M	M	M	M	M	Y
MA-1.4	Privacy concerns	See MA-4.2						
MA-2.5	Interoperability of Equipment	Urban - 10, 20	M	M	L	L	M	Y
OP-2.1	Insufficient timeliness of Information	See OP-3.1						
IL-1.1	Legal & privacy issues	All	M	M	L	M	M	Y
O-1.3	One or more jurisdictions choose not to cooperate	See O-3.1						
BF-2.2	Decisions affected by budgetary instability	See BF-1.1						
BF-2.3	Inability to Attract Capital Markets	See BF-1.5						
BF-2.4	Excessive Liability	Urban, Inter-urban - 20	M	L	M	L	M	Y

4.1.2 Risk Assessment Descriptions

This section describes the reevaluation of Phase I risks and gives rationales for reducing some of the risk assessments. Also, some risks were combined after analyzing across the 4 teams.

4.1.2.1 Red to Yellow

The following risks were lowered in overall rating from red to yellow.

MA-1.1 Different Participation Levels by Areas or Regions

The Performance Impact was changed from High to Moderate resulting in a lower "Yellow" rating. This was done because even systems that are not nationally compatible provide significant benefit (i.e. performance) in their own regional coverage. If roaming is sufficiently beneficial then (as happened with cellular phones) the industry will create it.

MA-2.1 Increased Acceptance of Public Transit

The Performance Impact was changed from High to Moderate resulting in a lower "Yellow" rating. The public transit services provide many performance improvements relating to more efficient operation of the system. If ridership does not increase these operational benefits are still obtained, hence the performance impact is only moderate.

MA-2.2 Acceptance of Commercial Vehicle Electronic Clearance

The probability of the risk occurring is Moderate instead of High due operational test experience which shows real benefits and significant user acceptance. Performance impact on the architecture is minimal because of the stand-alone feature of these services. Cost impact is Moderate because the basic cost benefit of the system can be achieved at moderate participation levels.

MA-4.1 Interoperability

The probability of this risk occurring is reduced to Moderate because interoperability across all areas of the country will not be required in the earlier timeframe. Initial systems will tend to be islands of automation. The standards will evolve over time and manufacturers wanting to capture as much of the existing market as possible will develop a migration strategy for owners of the early equipment.

MA-2.3 Human Factors Problems

The probability and severity of impact are reduced to moderate by the fact that before these products are fielded they will have undergone strenuous testing to determine their acceptability by the human users.

TF-2.2 Inadequate Intersection Collision Avoidance

The probability that this risk will occur is Low. This part of the architecture will not be available for some time and it comprises only a small part of the overall services that are achievable by the architecture.

TF-3.1 MAYDAY Reliability

The probability that this risk will occur, that users will perceive the MAYDAY feature as unreliable in the early time frame and not try again as the product matures, is Low.

TF-1.1 Complex System Integration

The probability that systems cannot be integrated properly is moderate instead of high. While the challenge is significant to integrate new equipment and software with existing components it is a challenge for which integrators plan and which they routinely meet.

TF-2.4 Stringent Safety Standards

The probability of occurrence is moderated by the fact that development practices are employed by developers to take these requirements into account.

PC-2.1 Stringent Performance Standards

The probability of occurrence is reduced to moderate. This risk applies to the automatic control systems required for the advanced vehicle safety subsystems. The risk is moderated due to the late time frame at which these products will be deployed. Continued research and early prototyping of the technology will reduce the subsequent production costs.

MA-4.2 Privacy Concerns

The probability of occurrence is reduced to moderate. Video camera surveillance has been in place for some time now in many types of businesses and public places without causing the public any concern. The customers that will appreciate the performance benefits of ITS services will also appreciate the added sense of security that comes with the increased video surveillance.

MA-1.2 Inter-operability of Equipment

The probability that the ITS services that make up the architecture will not be deployed because of a lack of interoperable equipment between TMCs is moderate at best. Interoperability between subsystems will be accomplished as the need for it is defined. Early deployments involve stand-alone systems. The need for tight interoperability is not as high as it will be in later years after the standards (such as NTCIP) have been developed and put into practice.

OM-1.1 Lack of Openness Complicates Product Mix & Match

The probability that this will occur is reduced to Moderate because the products purchased to supply a center are being marketed to all metropolitan areas. The pool of spares and compatible upgrade equipment is, therefore, very large. This also lessens the impact to performance.

IL-4.1 Legal Privacy Issues

The probability that this will occur is reduced to Moderate because such issues are addressed in the architecture itself by governing the ways that information is disseminated among subsystems. Also, other risks are written that cover this issue from the market acceptance point of view.

BF-1.4 Slow Market Growth Hampers Payback

The probability that slower market growth of transit information services will affect the achievement of overall ITS services is low. In general, the perceived benefits will increase the market acceptance. The financing for such services is also shared between the government agencies that have transit operations and private ISPs that will be developing products for this market.

BF-0.1 Decisions Affected by Budgetary Instability

The severity of cost impact has been reduced to Moderate. As Phase II of the National Architecture Program draws to a close this risk and its associated impact becomes over come by events.

4.1.2.2 Yellow to Red

None of the Yellow Risks identified in Phase I and listed in Table 8 and Table 9 were reassessed to a Red rating. Several, however, were combined into red risks.

4.1.2.3 Red to Blue

The following risks were lowered in overall rating from red to blue.

OM-2.1 Software and Hardware Reliability

The probability of occurrence is Low. This risk was originally against the Advanced Vehicle Safety System. Most of the services that make up these packages in the combined architecture will not be available until the later time frames. The standards and practices are already in place to develop safe reliable systems. Once these products and services move from the concept and prototype stage to full production the standards for constructing reliable equipment and software will be applied.

PC-1.1 Compatibility with Multiple Standards

The probability that product manufacturer's will not be able to protect their own unique products is negligible. In fact, most of the manufacturers will play a role in the definition of the eventual standards. The impact, especially cost, of maintaining compatibility with multiple standards is low because of the larger potential market that can be realized with such compatibility.

PC-1.2 Compatibility with Multiple Standards

The probability that manufacturers of transit products and services for ITS will not be able to maintain their niche market is negligible. The increased market potential that a national architecture delivers will more than justify the cost to build to an open system. Manufacturers will still be able to add extensions to the products that are unique to their brand to gain a competitive edge.

4.1.2.4 Risks Combined after Assessment

After a review of the red and yellow risks from the Phase I architecture teams it became apparent that there were several overlapping risks. These have been combined in the following ways:

PC-0.1 Market Fragmentation

This risk is covered by risk *MA-1.1 Different Participation Levels by Areas or Regions.* The market's fragmentation has no impact to cost. The cost is high in the early time frames because the technology is new - regardless of the standards developed.

BF-1.3 Decisions Affected by Budgetary Instability

This risk is covered by risk *BF-4.1 Decisions Affected by Budgetary Instability*. While one risk is for the TMC and the other is for the highway infrastructure, they are both written to address the issue of funding the Operations and Maintenance phase of the life cycle.

TF-1.3 Complex System Integration

This risk is covered by risk *TF-1.1 Complex System Integration.*

OP-3.2 Insufficient Timeliness of Information

This risk is covered by risk *OP-3.2 Insufficient Timeliness of Information.*

TF-2.6 Stringent Safety Standards

This risk is covered by risk *TF-2.4 Stringent Safety Standards.*

PC-2.2 Stringent Performance Standards

This risk is covered by risk *PC-2.1 Stringent Performance Standards.*

MA-1.4 Privacy Concerns

This risk is covered by risk *MA-4.2 Privacy Concerns.*

O-1.3 One or More Jurisdictions Choose Not to Cooperate

This risk is covered by risk *O-3.1 One or More Jurisdictions Choose Not to Cooperate.*

BF-1.2 Competition for Limited Capital Funds

This risk has been combined with risk *BF-1.1 Competition for Limited Capital Funds.*

BF-2.2 Decisions Affected by Budgetary Instability

This risk is covered by risk *BF-1.1 Decisions Affected by Budgetary Instability.*

BF-2.3 Inability to Attract Capital Markets

This risk is covered by risk *BF-1.5 Inability to Attract Capital Markets.*

4.2 Red Risk Summary

After reassessing the red risks from Phase I, a total of 10 risks have been rated as Red for Phase II. Of the remaining 22 Phase I red risks, 3 have been assessed as Blue and 16 are now Yellow. Three were combined with some of the other risks.

The red risks will be discussed in the following sections by the category in which the risk was identified.

Table 12 on page 34 summarizes information on risk identification and rating of the 10 red risks. As will be seen in the next sections, the risks are evenly spread across the 8 possible categories. Only "Cost to Produce" and "Operating Costs & Maintainability" is not represented in the set of red risks. These risks are also evenly spread across the Architectural Elements: Center, In-Vehicle, Communication, and Highway Infrastructure. Of the 4 possible life cycle stages, only Production is not represented by a red risks. Half of the risks are assigned to Deployment & Sales.

Of the Stakeholders that will bear these risks, the consumers bear more than the other groups. The risks are also spread fairly evenly across Scenario and Time Frame.

This section lists the risk classification and description that came from each category.

4.2.1 Technical Feasibility

Two Technical Feasibility risks were assessed a Red Rating.

Risk ID	Classification	Description
TF-2.1	Technology Immaturity	While incorporating or adapting existing technologies, the architecture may require new or currently immature technologies (e.g.: wireless wide area data communications, vehicle guidance and control components) which may result in the use of unproved or unacceptable system components.
TF-2.3	AHS Functional Failure	Failure on an automated highway will seriously impact safety. Failure will also dramatically increase congestion on the AHS. Therefore, it will be necessary to design AHS so that systems can only fail soft, i.e., with safe reversion to manual control. This requires stringent fail safety criteria.

4.2.2 Cost to Produce

None of the Costs to Produce risks were assessed as Red at the System Architecture level; however, some significant risks may exist for various elements of the architecture.

4.2.3 Market Acceptance

Three Market Acceptance risks were assessed as Red.

Risk ID	Classification	Description
MA-0.1	Privacy concerns	Concerns about the misuse of information related to the tracking of individual traveler Origin-Destination data, travel speeds, vehicle occupancy, etc. could impede market acceptance unless assurances are made to the public concerning data security and how data will be used and stored.
MA-3.1	Rural Market	The rural ITS market, in areas which are not serviced by cellular telephone, needs satellite communications for MAYDAY and for traffic surveillance via Automate Road Signing Beacons, but the market size for this equipment will be small. The risk is that this may cause the cost of these products (equipment purchase plus user fees) to be too expensive to be viable.
MA-3.2	Cost of Communications Does Not Drop	Wide area wireless data communications capabilities may not be deployed widely enough or pricing options and costs may remain too high for many ITS consumers thus market penetration will not rise as expected.

4.2.4 Operational Performance

One Operational Performance risk was assessed as Red.

Risk ID	Classification	Description
OP-3.1	Insufficient timeliness of information	Without rapid and efficient dissemination of traffic information, the end user may encounter problems that he or she purchased the system for the purpose of avoiding.

4.2.5 Operating Costs and Maintainability

None of the Operating Costs and Maintainability risks were assessed as Red at the System Architecture level; however, some significant risks may exist for various elements of the architecture.

4.2.6 Institutional and Legal

One Institutional and Legal risk was assessed as Red.

Risk ID	Classification	Description
IL-2.1	Perceived Harmful By-Products: Safety, Environment	Adverse health, safety, and environmental impacts may be associated with the deployed systems. This may result in failure to gain the support of public and advocacy groups, (e.g. widespread use of collision avoidance radars in vehicles could cause radiation fears).

4.2.7 Organizational

One Organizational risk was assessed as Red.

Risk ID	Classification	Description
O-1.1	Requires New Public & Private Partnerships	Reluctance by either the public or the private sectors could prevent deployment of TMS and ISP public-private partnerships.

4.2.8 Budget or Financial

Two risks from Budget or Financial were assessed as Red. BF-1.1 represents the combination with BF-1.2. BF-4.1 represents the combination with BF-1.3.

Risk ID	Classification	Description
BF-1.1	Competition for Limited Capital Funds	Lack of government funds and clearly demonstrable benefits could prevent initial construction of TMS and other infrastructure by limiting the capital funds available for architecture deployment.
BF-4.1	Decisions affected by budgetary instability	The risk to highway infrastructure improvement occurs in the O&M stage due to the lack of a steady, dependable flow of funding.

Table 12.Red Risk Summary

Risk ID	Category	Classification	Description	Architecture Affected	Risk Bearer	Life Cycle Stage	Scenario & Time frame	Probability of Occurrence	Severity of Impact	Rating
TF-2.1	Technical Feasibility	Technology Immaturity	While incorporating or adapting existing technologies, the architecture may require new or currently immature technologies (e.g.: wireless wide area data communications, vehicle guidance and control components) which may result in the use of unproved or unacceptable system components.	In vehicle	PP	R&D	All - 10, 20	M	H	R
TF-2.3	Technical Feasibility	AHS Functional Failure	Failure on an automated highway will seriously impact safety. Failure will also dramatically increase congestion on the AHS. Therefore, it will be necessary to design AHS so that systems can only fail soft, i.e., with safe reversion to manual control. This requires stringent fail safety criteria.	In vehicle	PC	O&M	Urban - 20	M	H	R
MA-0.1	Market Acceptance	Privacy concerns	Concerns about the misuse of information related to the tracking of individual traveler Origin-Destination data, travel speeds, vehicle occupancy, etc. could impede market acceptance unless assurances are made to the public concerning data security and how data will be used and stored.	Total System	G, PC	D&S	All	H	M	R
MA-3.1	Market Acceptance	Rural Market	The rural ITS market, in areas which are not serviced by cellular telephone, needs satellite communications for MAYDAY and for traffic surveillance via Automate Road Signing Beacons, but the market size for this equipment will be small. The risk is that this may cause the cost of these products (equipment purchase plus user fees) to be too expensive to be viable.	Communications	CC, PC	O&M	Rural - 10	M	H	R
MA-3.2	Market Acceptance	Cost of Communications Does Not Drop	Wide area wireless data communications capabilities may not be deployed widely enough or pricing options and costs may remain too high for many ITS consumers thus market penetration will not rise as expected.	Communications	CC, PC	D&S	All - 10, 20	H	H	R
OP-3.1	Operational Performance	Insufficient timeliness of information	Without rapid and efficient dissemination of traffic information, the end user may encounter problems that he or she purchased the system for the purpose of avoiding.	Communication	CC, PC	O&M	Urban, Interurban - 5, 10	H	H	R
IL-2.1	Institutional and Legal	Perceived Harmful By-Products: Safety, Environment	Adverse health, safety, and environmental impacts may be associated with the deployed systems. This may result in failure to gain the support of public and advocacy groups, (e.g. widespread use of collision avoidance radars in vehicles could cause radiation fears).	In vehicle, Highway Infrastructure, TMC	G, CC, PC	O&M	All - 10, 20	M	H	R
O-1.1	Organizational	Requires New Public & Private Partnerships	Reluctance by either the public or the private sectors could prevent deployment of TMS and ISP public-private partnerships.	TMC	G, ISP	D&S	All - 5, 10	H	M	R
BF-1.1	Budget & Financial	Competition for Limited	Lack of government funds and clearly demonstrable benefits could prevent initial construction of TMS and other	TMC	G, ISP	D&S	All	M	H	R

		Capital Funds	infrastructure by limiting the capital funds available for deployment of key architecture elements.							
BF-4.1	Budget & Financial	Decisions affected by budgetary instability	The risk to highway infrastructure improvement occurs in the O&M stage due to the lack of a steady, dependable flow of funding.	Highway Infrastructure, TMC	G, PC	D&S	All	M	H	R

5.0 Risk Mitigation

This section presents mitigation strategies for each of the red rated risks. The mitigation actions that were defined by the Phase I teams for each of the red risks were used as the starting points for this effort. The Phase II architecture and Implementation Strategy were examined in order to improve the original mitigation strategy.

5.1 Mitigation Strategies

The risks are listed here in the order in which they were presented in Table 12 on page 34 by the Risk ID and Classification. The mitigation strategies have been placed into the following general categories: Control, Avoidance, and Transfer. Then the stakeholder group is identified that will bear the primary responsibility for mitigating the risk.

TF-2.1 Technology Immaturity

Mitigation Category: Transfer
Mitigation Handler: Government, Private Producer

While the private sector will naturally develop some AVSS features such as lateral and longitudinal collision warning, they have little reason to develop other features such as intersection collision warning. Government can play a key role in speeding the development of advanced technology for safety systems.

- The government should fund testing and evaluation of Advanced Vehicle Safety Systems (AVSS) related technologies to speed maturity and deployment.
- In partnership with private producers, a government backed test and development program should include the use of an intersection grid track for operational testing.
- Employ advanced software modeling and simulation programs that address all known threatening situations.

While a lot of technology choices exist for implementing AVSS type systems, they have until recently been developed for the military. To adapt them to a commercial environment will require careful testing and integration with commercial technologies.

TF-2.3 AHS Functional Failure

Mitigation Category: Control
Mitigation Handler: Government

In the ITS architecture the Advance Vehicle Safety Systems user services are implemented primarily by in-vehicle equipment. With the exception of the Intersection Collision Avoidance user service, there is little real-time high-speed control communication (apart from sensing and setting operational parameters) between the vehicle subsystem to any other subsystem (except for communication with other adjacent vehicles). This will reduce the number of external interconnections, thereby reducing the probability of failure, and the need for extra systems/hardware. For those cases where functional failure could have a real safety impact:

- Set very high standards for safety and performance.
- The government established safety/performance standards should incorporate system self test prior to AVSS operation. This will provide a measure of assurance that the system is functional.

MA-0.1 Privacy concerns

Mitigation Category: Control
Mitigation Handler: Government, Information Service Providers

There exists concern from the Private Sector that the proper management of this risk adds additional burden to the consumer. At the same time, another view is that the mismanagement of this risk could result in broad mistrust of ITS.

- Control access to databases containing private information. Use that information only in ways that the sources of the information have been informed about. Require that users opt-in for services where private data needs to be stored.
- Introduce encryption and authentication functions in the communication layer to protect private data.
- Use only cooperative vehicle probes.
- Enact state legislation to protect personal data in government databases that might otherwise be exposed to state Freedom Of Information Act requests.
- Educate consumers on how information is used within ITS, along with the associated risks and benefits.

MA-3.1 Rural Market

Mitigation Category: Control
Mitigation Handler: Government

Government backed standards development efforts will encourage modularity and hence increase quantities to more rapidly develop this market.

- Establish Government subsidies or joint cost-sharing to help pay for equipment and services.
- Develop standards at a functional level and encourage modularity. By doing this, economies of scale can be achieved.
- Provide for innovative market packaging (e.g., combine convenience with personal safety) to increase acceptance.

MA-3.2 Cost of Communications Does Not Drop

Mitigation Category: Control
Mitigation Handler: Information Service Providers, Government

- Design the architecture to minimize communication costs e.g. location of processing, choice of messages, flexibility to adapt to a competitive and rapidly evolving wireless data communication marketplace, use of data compression in the communication layer of the architecture.
- Conduct a detailed analysis of communication alternatives on the basis of technical feasibility, deployment costs, cost to consumers, and open vs. proprietary standards.
- Conduct an analysis of consumers willingness to pay for ITS related services requiring increased communications cost
- Identify alternatives for reducing service costs to consumers e.g. partial federal subsidies, public utility business structures, variable rates and deregulation.

OP-3.1 Insufficient Timeliness of Information

Mitigation Category: Control
Mitigation Handler: Information Service Providers, Private Producers

The architecture requires control of this risk at the TMS, ISP and Vehicle subsystems.

- Simulate and analyze architecture deployment for given operating scenarios to determine critical links and bottlenecks.
- Allow jurisdictions to tailor deployment to eliminate bottlenecks.
- Minimize message latency, optimize processing along critical path.
- Limit volume of data flow by applying data compression technologies where applicable.
- Plan/allocate additional capacity to allow for growth.

IL-2.1 Perceived Harmful By-Products: Safety, Environment

Mitigation Category: Transfer
Mitigation Handler: Government, Private Producer

The probability of actually producing harmful byproducts as a result of ITS technologies or the architecture is very low, (and in-fact ITS should reduce the number of present harmful by products of transportation). If the public perceives that ITS is contributing to these harmful by-products, acceptance of ITS could be seriously hampered. The risk is transferred to the government and producers to educate the public and build in features that address any anxiety the public may have.

- Develop outreach programs, public educational seminars, and consensus briefings to gain acceptance.
- Incorporate emissions monitoring in the deployment strategy. Focus on safety benefits and tradeoffs.

O-1.1 Requires New Public & Private Partnerships

Mitigation Category: Control
Mitigation Handler: Government

These partnerships will grow and prosper as the benefits to both sides become apparent. The earlier these benefits can be brought to light the better. This should be a key goal and priority of operational test and early deployment programs.

- Utilize operational tests to establish business, financial, and transactional relationships for public-private partnerships.
- Establish financial incentives to facilitate cooperation and project coordination.
- Demonstrate how sharing information reduces congestion and makes it a win-win situation.

BF-1.1 Competition for Limited Capital Funds

Mitigation Category: Avoidance
Mitigation Handler: State Governments

Establishing public-private partnerships may be affected by the previous risk, *O-1.1 Requires New Public & Private Partnerships.*

- Secure alternate funding e.g. bond issues, incentives for private sector such as tax abatements, long term operations contracts, advertising revenues (legislation may be necessary).
- Continue activities to secure federal funding on the basis of realistic mobility plans for near-term and future time frames. Utilize regional Federal representatives as a resource to support and critique plans and proposals.
- Privatize all or part of the TMS, transferring the burden to the private sector.

BF-4.1 Decisions affected by budgetary instability

Mitigation Category: Avoidance
Mitigation Handler: Government, Information Service Providers

A lack of a steady, dependable flow of funding will hamper the efficient operation and maintenance of the highway infrastructure. The ones who will ultimately suffer will be the private and commercial users of the transportation network. Government agencies must avoid this by performing the trade-off analyses early.

- Secure alternate funding e.g. establish public/private partnerships.
- Perform rigorous trade-offs between initial procurement price and operations and maintenance costs (life-cycle analysis).

5.2 Mitigation Summary

In summary all 10 red risks identified have mitigation strategies which can contain the risk and if followed can lessen either the probability of occurrence or severity of the risk.

ITS spans a wide array of services, sectors, and users. The risks inherent in deployment of ITS may slow one aspect or another, but the overall effort will continue to develop and deploy.

A.0 List of Acronyms

A	
ABS	Antilock Brake System
ADA	Americans with Disabilities Act
AFD	Architecture Flow Diagram
AID	Architecture Interconnect Diagram
AHS	Automated Highway System
AMPS	Advanced Mobile Phone System
APTS	Advanced Public Transportation System
ATIS	Advanced Traveler Information System
ATM	Asynchronous Transfer Mode
ATMS	Advanced Traffic Management System
AVCS	Advanced Vehicle Control System
AVI	Automated Vehicle Identification
AVL	Automated Vehicle Location
AVO	Automated Vehicle Operation
C	
CAAA	Clean Air Act Amendment
CASE	Computer Aided Systems Engineering
CCTV	Closed Circuit TV
CDMA	Code Division Multiple Access
CDPD	Cellular Digital Packet Data
CMS	Changeable Message System
COTR	Contracting Officer Technical Representative
CSP	Communication Service Provider
CVAS	Commercial Vehicle Administration Subsystem
CVCS	Commercial Vehicle Check Subsystem
CVISN	Commercial Vehicle Information Systems and Networks
CVS	Commercial Vehicle Subsystem
CVO	Commercial Vehicle Operations
D	
DAB	Digital Audio Broadcast
DD	Data Dictionary
DDE	Data Dictionary Element
DFD	Data Flow Diagram
DGPS	Differential Global Positioning System
DOD	Department of Defense
DOT	Department of Transportation
DMV	Department of Motor Vehicles
DSRC	Dedicated Short Range Communications
DTA	Dynamic Traffic Assignment

E

ECPA	Electronic Communications Privacy Act
EDI	Electronic Data Interchange
EPA	Environmental Protection Agency
EM	Emergency Management Subsystem
EMC	Emergency Management Center
EMMS	Emissions Management Subsystem
ESMR	Enhanced SMR
ETA	Expected Time of Arrival
ETTM	Electronic Toll and Traffic Management

F

FARS	Fatal Accident Reporting System
FCC	Federal Communications Commission for the U.S.
FHWA	Federal Highway Administration
FIPS	Federal Information Processing Standard
FOT	Field Operational Test
FMS	Fleet Management Subsystem
FPR	Final Program Review
FTA	Federal Transit Administration

G

GIS	Geographic Information System
GPS	Global Positioning System

H

HAR	Highway Advisory Radio
HAZMAT	HAZardous MATerial(s)
HOV	High Occupancy Vehicle
HUD	Head–Up Display

I

IEEE	Institute of Electrical and Electronics Engineers, Inc.
IVIS	In Vehicle Information System
IP	Internet Protocol
IPR	Interim Program Review
ISO	International Standards Organization
ISP	Information Service Provider
ISTEA	Intermodal Surface Transportation Efficiency Act
ITE	Institute of Transportation Engineers
ITI	Intelligent Transportation Infrastructure
ITS	Intelligent Transportation Systems
ITS AMERICA	Intelligent Transportation Society of America
IVHS	Intelligent Vehicle Highway Systems

L

LAN	Local Area Network
LCD	Liquid Crystal Display
LED	Light Emitting Diode

LEO	Low–Earth Orbit satellite system
LPD	Liability and Property Damage
LRMP	Location Reference Messaging Protocol
LRMS	Location Reference Messaging Standard
M	
MAN	Metropolitan Area Network
MAUT	Multiattribute Utility Theory
MMI	Man–Machine Interface (or Interaction)
MOE	Measure Of Effectiveness
MPO	Metropolitan Planning Organization
MPH	Miles per Hour
MTC	Metro Traffic Control
N	
NA	National Architecture
NAR	National Architecture Review
NEMA	National Electrical Manufacturers Association
NHPN	National Highway Planning Network
NHTSA	National Highway Traffic Safety Administration
NII	National Information Infrastructure (aka Information Superhighway)
NTCIP	National Transportation Communications for ITS Protocol
O	
OEM	Original Equipment Manufacturer
OSI	Open Systems Interconnection
OTP	Operational Test Plan
P	
PCS	Personal Communications System
PDA	Personal Digital Assistant
PIAS	Personal Information Access Subsystem
PMS	Parking Management Subsystem
PS	Planning Subsystem
PSA	Precursor System Architecture
PSPEC	Process Specification
PSTN	Public Switched Telephone Network
Q	
QFD	Quality Functional Deployment
R	
R&D	Research and Development
RDS	Radio Data Systems
RDS–TMC	Radio Data Systems incorporating a Traffic Message Channel
RTA	Regional Transit Authority
RS	Roadway Subsystem
RTS	Remote Traveler Support Subsystem

S

SAE	Society of Automotive Engineers
SDO	Standards Development Organization
SMR	Specialized Mobile Radio
SONET	Synchronous Optical Network
SOV	Single Occupancy Vehicle
STMF	Simple Transportation Management Framework
SQL	Standard Query Language

T

TAS	Toll Administration Subsystem
TCS	Toll Collection Subsystem
TDM	Travel Demand Management
TDMA	Time Division Multiple Access
TIGER	Topologically Integrated Geographic Encoding & Referencing files
TMC	1. Traffic Management Center 2. Traffic Message Channel. See RDS–TMC
TMS	Traffic Management Subsystem
TRMC	Transit Management Center
TRMS	Transit Management Subsystem
TRT	Technical Review Team
TRVS	Transit Vehicle Subsystem

V

VMS	Variable Message Sign
VRC	Vehicle/Roadside Communications
VS	Vehicle Subsystem

W

WAN	Wide Area Network
WIM	Weigh–in Motion
WWW	World Wide Web