Model Systems Engineering Document

ITS Application: Communications

May 24, 2019
Prepared by Athey Creek Consultants

Contents

Acronyms

ATIS	• Advanced Traveler Information System
ATMS	• Advanced Traffic Management Software
ARC-IT	• National Architecture Reference for Cooperative and Intelligent Transportation
CAV	• Connected and Automated Vehicle
DSCR	• Dedicated Short-range Communications
DMS	• Dynamic Message Signs
FAT	• Factory Acceptance Test
FIRST	• Freeway Incident Response Safety Team
ITS	• Intelligent Transportation System
LAN	• Local Area Network
MnDOT	• Minnesota Department of Transportation
RSU	• Roadside Unit
RTMC	• Regional Transportation Management Center
SEA	• Systems Engineering Analysis
VPN	• Virtual Private Network
WAN	• Wide Area Network

Purpose and Description of ITS Application: Communications

Document Purpose

This document is intended to support the Systems Engineering Analysis (SEA) activities for the Minnesota Department of Transportation (MnDOT) and other local transportation agencies within Minnesota as they consider, plan, develop, design, implement, and operate communications. The content of this document will be a systems engineering analysis resource to support project compliance as set forth in 23 CFR Section 940 (Rule 940). This document can be used in conjunction with the Minnesota Statewide Regional Intelligent Transportation System (ITS) Architecture and related systems engineering resources to complete an ITS Systems Engineering project-specific checklist as part of the initial analysis of applications considered for implementation. To access the available checklists for ITS-related deployments, visit the MnDOT Systems Engineering web page at: https://www.dot.state.mn.us/its/systemsengineering.html.

In situations where projects are not consistent with this systems engineering document, the contents of this document may be used as a base to support the development of project specific systems engineering documents, including a concept of operations, functional requirements, and test plans specific to the project.

Communications Overview

Communications provide the mechanism to transfer information, video, images, control commands, and other data and data types from one system or device to another. As shown in Figure 1, communications support many ITS and Connected and Automated Vehicles (CAV) applications.

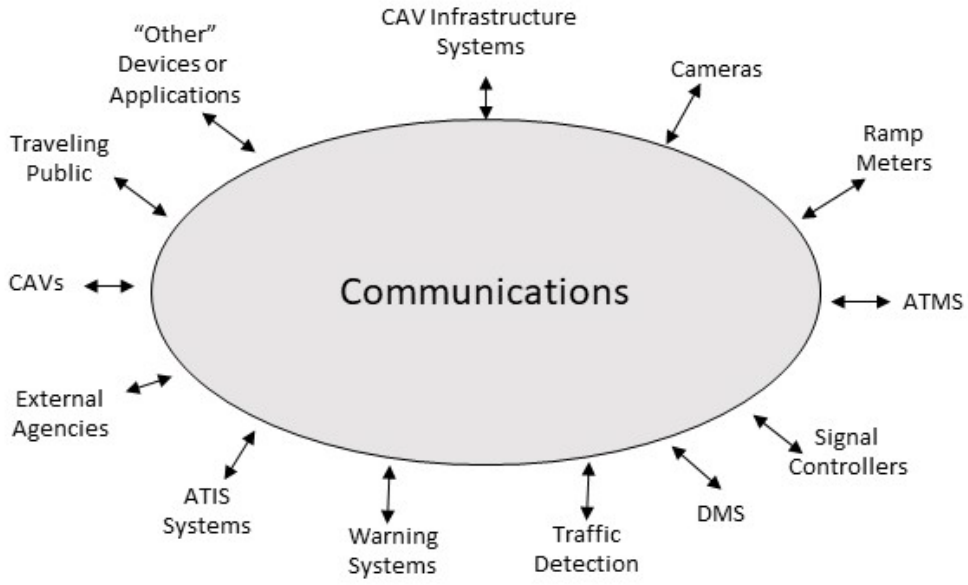


Figure 1: Illustration of the Role of Communications

Communications Needs and Typical Conditions

Communications Needs

Operations of ITS and CAV applications rely upon communications. Transportation agencies that operate ITS and CAV applications typically operate a number of communications components based on the unique needs of the individual applications, systems, or field devices communicating. The following table describes the most common challenges and needs facing ITS and CAV applications and identifies related communications needs.

Table 1: ITS and CAV Applications' Challenges and Needs, and Resulting Needs for Communications

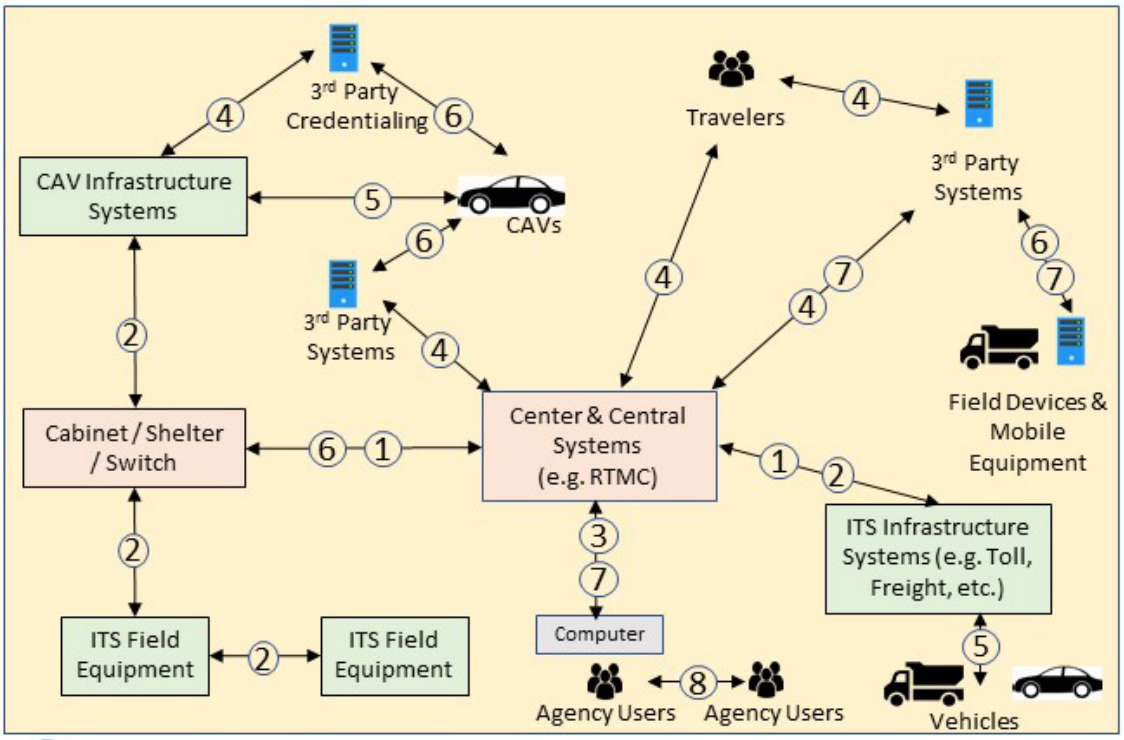
Challenge/Applications' Needs	Communications Need
- Dynamic Message Sign (DMS), video, ramp metering, traffic detection, and warning applications require data to be communicated over long distances from local cabinets/controllers to central locations.	Need #1: Long distance, high bandwidth, high data transfer rate, with minimal signal loss
- The field devices associated with various applications are generally placed in or near the roadway to support specific functions. Communications need to exchange data between the devices and the cabinets and controllers where supporting systems are located, and long-distance communications typically terminate. - These short distance communications need to be installer and maintainer friendly to accommodate connections that follow poles, connected into devices, etc.	Need #2: Flexibility in deployment to support various terrains and obstacles
- DMS, traffic detection, and video applications sometimes require wireless communications to the field devices and/or controllers, where wireline is not practical or possible.	Need #3: Wireless connectivity to devices
- Agency operators will access internal systems that require communications to central servers and/or databases and need communications supporting the software systems.	Need #4: Internal security for users
- Some ITS and CAV safety applications require extremely low latency and high availability communications to support warning systems.	Need #5: Low latency high availability communications
- Some CAV applications require sophisticated security and credentialing management to ensure the security of vehicles and systems. To accomplish this, infrastructure systems need to communicate with internet based credentialing services and with CAVs through wireless communications.	Need #6: Credentialing enabled security
- ITS and CAV applications can be vulnerable to cyber security attack, and mechanisms to secure the communications are needed.	Need #7: Security at the communication terminations to prevent unwanted intrusions

Challenge/Applications' Needs	Communications Need
- Agencies need to communicate data, information, and video to third party providers and the traveling public. Similarly, there are situations where agency owned communications mediums/ technologies are not financially or physically viable and public communications are needed. Finally, agency employees need access to public information exchanges.	Need #8: Unsecured use of public Internet
- Agencies need to establish communications with devices and systems where secure and encrypted communications are required but where agency operated networks are not practical, and public communications (e.g. internet, cellular phone) are practical.	Need #9: Secured use of public communications mediums

Communications Environment/Components

In order to address the communications needs identified in Table 1, transportation agencies commonly use internally operated wireline and wireless/radio communications technologies supplemented with public subscription-based wireline and wireless communications to accomplish the two-way exchange of data, information, and control that is needed to operate ITS and CAV systems. Networking capabilities will continue to evolve how networks share infrastructure. For example, MnDOT currently uses a Virtual Private Network (VPN) through public internet to communicate with ITS devices running on private wireless cell phone modems. Functionally, it acts as an extension of the MnDOT Regional Transportation Management Center - RTMCnet™. However, technically the communications equipment is a part of both the public internet and private cell phone infrastructure.

In summary, transportation agencies rely on multiple communications components that collectively comprise the overall communications application. Figure 2 illustrates eight communications components/technologies that collectively meet the communications needs defined in Table 1. Figure 2 illustrates the ***typical devices, systems, and users*** that rely upon the various communications components. The intent of Figure 2 is not to represent all users of each component, but rather to illustrate the full set of communications components used to support ITS and CAV applications in Minnesota.



1. Long range (backbone) communications
2. Short range, wireline or wireless communications
3. Local area network (LAN) or wide area network (WAN) depending on location
4. Public Internet
5. Short-range wireless, secured communications
6. Commercial wireless communications (e.g. private cellular phone companies)
7. Virtual Private Network (VPN) over public Internet
8. Agency operated wireless (voice) radio network

Figure 2: Illustration of Primary Communications Components/Technologies

Communications Components Descriptions and Typical Conditions

Table 2 presents descriptions of the communications components as illustrated in Figure 2 above and provides brief summaries of the typical conditions where each component is used.

Table 2: Communications Components that Comprise the Communications Application

Component	Description/Function
1. Long-range (backbone) communications	• Ethernet connections using fiber or copper mediums to support two-way communications of large volumes of data, in minimum time, over long distances with minimal loss. • May be agency owned/operated or shared with others, therefore security and intrusion prevention is provided by the systems/devices at the connections (e.g. modems, terminators, access points).
2. Short-range wireline or wireless communications	• Ethernet or serial connections using fiber or copper mediums to support two-way communications over short distances. • May also include short-range wireless communications such as wi-fi, microwave, or FM radio. • Typically, these are agency owned/operated, therefore security and intrusion prevention is provided by the systems/devices at the connections (e.g. modems, terminators, access points). • Physical components are suitable for connecting to local devices, passing through conduit, or other configurations to support deployments.
3. DOT operated LAN or WAN	• Private communications network that allows device to device connections and user application to device connection with standard security concerns. • Access to outside systems or public communications are through a firewall.
4. Public internet	• Use of the public internet allows information (e.g. video, data) to be shared with agencies and individuals that are not connected to the LAN or WAN. • Public internet allows agency personnel to access non-agency websites (e.g. to access weather information from weatherchannel.com). • Communications have limited security and all agency-operated systems would interface to the Internet through a firewall.
5. Short-range, wireless, low latency communications	• Communications technologies to support connectivity between infrastructure systems and vehicles. Infrastructure systems may include, but are not limited to, CAV infrastructure systems, tolling infrastructure systems, and freight/pre-clearance infrastructure systems that communicate with vehicles.

Component	Description/Function
	• Typically provide extremely low latency communications and are able to support credentials-based security protocols. • Range is generally 300 meters or less, line of sight.
6. Commercial wireless communications	• Services provided by third party providers to perform wireless communications over commercial networks such as cellular and/or wi-fi. • Agencies may procure metered or unlimited communications and all aspects are performed by the third party.
7. VPN over Public Internet	• Secure and encrypted communications over less secure networks and the public internet. • Mediums may involve private cellular phone carriers and various connections with the public internet.
8. Agency operated wireless (voice) radio network	• Wireless communications are used to communicate with individuals while in the field or mobile (e.g. Freeway Incident Response Safety Team (FIRST) vehicle operators, Regional Transportation Management Center (RTMC) operators, managers and other responders). • Typically, these are agency operated radio networks, but may utilize public radio in specific situations.

Operational Concepts

The previous section defined a series of needs (see Table 1) addressed by the communications application. This categorization of needs will be further used in this section to relate each need to one or more communications components (see Table 2) that potentially address the need. Table 3 maps each need to one or more communications components that has the potential to satisfy the need.

The intended use of the table below is to support future ITS and CAV deployments. In situations where the needs for communications are understood, the table below would allow system development to identify candidate communications components to be included in the design process.

Table 3: Mapping of Applications' Needs to Communications Components

Need	Communication Components/Technologies							
	Long-range communications	Short-range wireless or wireline	DOT operated LAN or WAN	Public internet	Short-range, wireless, low latency communications	Commercial wireless communications	VPN over Public Internet	Agency operated wireless radio
Need #1: Long distance w/ minimal signal loss	■			■				
Need #2: Flexibility in deployment		■				■	■	
Need #3: Wireless connectivity					■	■	■	■
Need #4: Internal security for users			■					
Need #5: Low latency high availability communications					■			
Need #6: Credentialing enabled security				■	■			
Need #7: Security at the communication terminations to prevent unwanted intrusions	■	■	■		■	■	■	■
Need #8: Use of public internet				■				
Need #9: Secured use of public communications mediums				■		■	■	

Operational Scenarios/Roles and Responsibilities

Operational Scenarios

Scenarios for the use of communications are intended to provide example descriptions about how decisions about the use of communications will be reached and examples of the roles of communications.

- Scenario A: Deployment of a New Permanent Video Camera
- Scenario B: Deployment of a Temporary Video Camera in a Rural Work Zone
- Scenario C: Deployment of Roadside Unit as part of a CAV Infrastructure System
- Scenario D: Media access to MnDOT Video

Scenario A: Deployment of a New Permanent Video Camera

A site has been identified in the Twin Cities where MnDOT intends to deploy and operate a video camera. This site is along the path of fiber optic communications, and there is a connection point to the fiber backbone near an existing cabinet with communications switch. Project designers review the communications needs and identify needs #1, #2, and #7 (See Table 1) are pertinent to this deployment. The designers determine that the fiber backbone will address the need for long-distance communications (need #1) and that an ethernet communications solution between the cabinet and the camera will meet the need for flexibility in deployment (need #2). The fiber and ethernet solutions both meet the need for security (need #7). Technicians and installers coordinate the connections to the existing fiber and installation of the new ethernet at the same time as the video camera installation.

Scenario B: Deployment of a Temporary Video Camera in a Rural Work Zone

A work zone is planned for a rural portion of the state, not served by land-line communications. The project team has identified the need for deployment and operation of a video camera to monitor traffic and the operational status of local equipment. The goal is for operators in the RTMC to monitor and control the video camera. Project designers have identified the most relevant needs for this deployment to be needs #3, #7, and #9 (See Table 1). With deployment of a MnDOT owned communication solution not practical, the project designers decide to select VPN over public internet and commercial wireless carriers and deploy a cellular modem at the site of the video camera and establish communications relying on the private network.

Scenario C: Deployment of Roadside Unit as part of a CAV Infrastructure System

A site has been identified in the Twin Cities where MnDOT intends to deploy and operate an RSU in order to broadcast message to and receive messages from CAVs. This site is along the path of fiber optic communications, and there is a connection point to the fiber backbone near an existing cabinet with communications switch. Project designers review the communications needs and identify needs #1, #2, #6, and #7 (See Table 1) are pertinent to this deployment. The designers determine that the fiber backbone will address the need for long-distance communications (need #1) and that an ethernet communications solution between the cabinet and the RSU will meet the need for flexibility in deployment (need #2). The fiber and ethernet solutions both meet the need for security (need #7). The CAV infrastructure system needs to connect to the credentialing service MnDOT subscribes to through internet communications (need #6), so an Internet access is installed at the RSU. Finally, the RSU will be equipped with a radio transmitter to send 5.9 GHz messages. At this time, the licensed option for 5.9 GHz

communications is Dedicated Short-range Communications (DSRC) so this protocol is deployed. Technicians and installers coordinate the connections to the existing fiber and installation of the new ethernet and RSU radio broadcaster at the same time as the overall CAV Infrastructure System.

Scenario D: Media access to MnDOT Video

MnDOT is in the process of maintaining their feed of video to local media outlets that will display the live video during their news broadcasts. MnDOT determines that communication need for public internet exchange (need #8 in See Table 1) is the primary need for this delivery of service and elects to continue delivering video to media outlets using the public internet to connect the video management system with the media outlets. In order to provide sufficient video quality, MnDOT determines the required amounts of bandwidth and the needed transmission speed; and arranges commercial public internet connections between the MnDOT servers and the public internet. The media providers will be responsible for determining their required public internet connections.

System Requirements

System requirements are verifiable details that define what a system will do, but not how the system will do it. Requirements for communications components vary by the component, with some requirements applying universally across all components and others being specific to one or more components.

Communications requirements are listed in the table below first by describing the requirement (column 1) then by mapping each requirement to the appropriate communications component (See Table 2). Three types of requirements are included:

- ***Performance related communications requirements*** – Requirements that describe performance levels and functional activities that must be performed by the communications;
- ***Security related communications requirements*** – Requirements that describe what the communications must do to address security topics; and
- ***Design related communications requirements*** – Requirements related to design and deployment aspects of communications components.

Table 4: Communications Requirements Presented by Component

Requirement	Communication Components/Technologies							
	Long-range communications	Short-range wireless or wireline	DOT operated LAN or WAN	Public internet	Short-range, wireless, low latency communications	Commercial wireless communications	VPN over Public Internet	Agency operated wireless radio
Performance Related Communications Requirements								
1. Communications shall transfer data (e.g. text, pictures, video, commands, etc.) from sender applications to receiver applications.	■	■	■	■	■	■	■	
2. Communications shall interface with encoders and decoders to enable conversion of data and information to/from digital signals.	■	■	■	■	■	■	■	
3. Communications shall transfer voice from sender to receiver devices.						■		■

Requirement	Communication Components/Technologies							
	Long-range communications	Short-range wireless or wireline	DOT operated LAN or WAN	Public internet	Short-range, wireless, low latency communications	Commercial wireless communications	VPN over Public Internet	Agency operated wireless radio
4. Communications design shall address required bandwidth (capacity) for MnDOT to make video available to media partners with sufficient quality.				■				
5. Communications design shall address required bandwidth (capacity) for internal agency operated communications components.	■	■	■					
6. Communications design shall address required data transfer speed needs of the applications supported.	■	■	■	■	■	■	■	■
7. Communications design shall address consistency needs of the applications supported.	■	■	■		■	■		■
8. Communications design shall address reliability needs of the applications supported.	■	■	■		■	■		■
9. Communications design shall address recovery needs of the applications supported.	■	■	■		■			■
Security Related Communications Requirements								
10. Communications shall restrict access to servers or devices outside the agency, except through firewall protection.	■	■	■		■		■	
11. Communications shall provide a secure data exchange without requiring devices and systems interacting with the device to maintain their own firewall protection.	■	■	■		■			

Requirement	Communication Components/Technologies							
	Long-range communications	Short-range wireless or wireline	DOT operated LAN or WAN	Public internet	Short-range, wireless, low latency communications	Commercial wireless communications	VPN over Public Internet	Agency operated wireless radio
12. Communications shall use secure methods for encrypting data in transit to accommodate data exchange outside the agency firewall.	■	■	■	■	■	■	■	■
13. Communications shall rely upon and require firewall or related protection within applications connected through the communications solution.	■	■	■	■	■	■	■	■
14. Communications designs shall include security and/or firewall capabilities within the applications serving as senders and receivers (to accommodate lack of security control in the communications).				■		■		
15. Communications shall comply with agency security policy to block malicious attempts and cybersecurity attacks.	■	■	■		■	■	■	
Design Related Communications Requirements								
16. Communications shall follow design standards for conduit protection, burial depth, and grounding.	■	■	■		■	■		■
17. Wireless communications deployment design shall include an interference analysis.					■			■
18. Communications design shall include documentation of hardware and field elements.	■	■	■		■			■

Requirement	Communication Components/Technologies							
	Long-range communications	Short-range wireless or wireline	DOT operated LAN or WAN	Public internet	Short-range, wireless, low latency communications	Commercial wireless communications	VPN over Public Internet	Agency operated wireless radio
19. Communications devices shall be mounted on appropriate support structures.	■	■	■		■			■
20. Communications designs shall obtain any required licenses for devices or communications.					■			■
21. Communications design shall use application specific approaches to avoid 'cross-talk' interference (e.g. MnPass application may use GPS tag coordination).		■						

Relationship to the National ARC-IT and Minnesota ITS Architecture

The Minnesota Statewide Regional ITS Architecture presents a vision for how ITS systems work together, share resources, and share information. The 2018 update to the ITS Architecture represents the latest status of Minnesota, as captured through outreach meetings and input from stakeholders statewide. As such, the Minnesota ITS Architecture was a valuable input to the development of this documents, supporting:

- Definition of needs for communications;
- Communication components supporting the needs;
- Concepts for the use of communications; and
- Overall input to the requirements.

The Minnesota ITS Architecture enabled the Project Team to build upon the content of the architecture and clarify specifics for this document.

In addition to the role of supporting the development of this document, the Minnesota Statewide Regional ITS Architecture and the National Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) will continue to serve as a resource for the agencies that utilize this document as they prepare for deployment. Table 5 below identifies the needs/potential solutions included in the Minnesota ITS Architecture that are addressed through concepts for the use of communications described in this document, as well as references to service packages and processes as defined in the National ARC-IT. Finally, the far right column identifies the communications need(s) that were influenced or derived based on each service package.

Table 5: Summary of Local and National ITS & CAV Architecture References Mapped to Communications Needs

MN Statewide Regional ITS Architecture: Need/Potential Solutions	ARC-IT: Service Packages	ARC-IT: Processes	Communications Needs Influenced by each Service Package
• SUP02 Managing and sharing transportation data	• SU03 Data Distribution	• Provide Transportation Center Data Sharing Services	• Need #1: Long distance, high bandwidth, high data transfer rate, with minimal signal loss • Need #4: Internal security for users
• SUP02 Managing and sharing transportation data	• SU03 Data Distribution	• Provide Field Data Sharing Services	• Need #1: Long distance, high bandwidth, high data transfer rate, with minimal signal loss • Need #2: Flexibility in deployment to support various terrains and obstacles • Need #3: Wireless connectivity to devices • Need #7: Security at the communication terminations to prevent unwanted intrusions
• SUP02 Managing and sharing transportation data	• SU03 Data Distribution	• Provide Vehicle Data Sharing Services	Need #5: Low latency high availability communications Need #6: Credentialing enabled security
• SUP02 Managing and sharing transportation data	• SU03 Data Distribution	• Provide Personal Data Sharing Services	Need #8: Unsecured use of public Internet

MN Statewide Regional ITS Architecture: Need/Potential Solutions	ARC-IT: Service Packages	ARC-IT: Processes	Communications Needs Influenced by each Service Package
• SUP02 Managing and sharing transportation data	• Roadway Communications Support (Functional Object)	• Support Roadway System Communications	• Need #1: Long distance, high bandwidth, high data transfer rate, with minimal signal loss • Need #2: Flexibility in deployment to support various terrains and obstacles • Need #3: Wireless connectivity to devices • Need #7: Security at the communication terminations to prevent unwanted intrusions
• SUP02 Managing and sharing transportation data	• SU08 Security and credentials management	• Support Connected Vehicle Center Communications • Support Data Distribution Communications • Support Service Monitor Communications	• Need #6: Credentialing enabled security • Need #8: Unsecured use of public Internet • Need #9: Secured use of public communications mediums
• SUP02 Managing and sharing transportation data	• SU08 Security and credentials management	• Support Wide Area Connected Vehicle Communications	• Need #5: Low latency high availability communications • Need #6: Credentialing enabled security

MN Statewide Regional ITS Architecture: Need/Potential Solutions	ARC-IT: Service Packages	ARC-IT: Processes	Communications Needs Influenced by each Service Package
• ATIS10 Operate a statewide web-based and telephone based 511 system	• TI01 Broadcast Traveler Information	• Wide Area Information Disseminator System (physical object) • Disseminate Traveler Information	• Need #5: Low latency high availability communications • Need #6: Credentialing enabled security • Need #8: Unsecured use of public Internet

Model Test Plan

This section presents a model test plan to support testing and validation activities during the integration and deployment stages of communications to confirm that the system is developed, installed, and operating as specified by the system requirements.

Each communication deployment will be different, and the testing and validation performed will likely vary depending upon the complexity of the system and the familiarity with the vendor products.

The table below provides a series of testing instructions related to the requirements presented above. The intent is that agencies using this model systems engineering document will incorporate these tests into their overall testing and validation plans, adapting them as needed.

Column 3 in the table below describes 'testing instructions' for each requirement. The communication requirements include a range of requirement types and therefore the testing instructions vary. The following bullet list explains the approach to different testing instructions:

- *Advisory requirement – no testing required:* This is noted for requirements that are primarily operational advice and therefore no formal testing is required;
- *Design:* these test instructions are used to describe testing in the form of design reviews or documentation reviews describing the ramp metering. These are typically not physical tests, but rather reviews of processes or documents;
- *Factory Acceptance Test (FAT):* These represent recommendations for FATs to allow the agency deploying the communications to verify the quality assurance / quality control and ramp metering operational parameters at the site of manufacturing and assembly. This can involve the procuring agency on-site at the vendor factory testing the actual equipment to be delivered or the reports of previous tests of components, software, or features;
- *Field:* These represent recommendations for tests to be conducted in MnDOT offices or the field to test the actual deployment and functionality of the communications.

Table 6: Model Test Plan for Communications

	System Requirement	Testing Instructions	Type of Result	Comments / Notes
1.	Communications shall transfer data (e.g. text, pictures, video, commands, etc.) from sender applications to receiver applications.	Field – Confirm that communications transfer data from sender applications to receiver applications.	Pass/Fail	Test for: • Long-range communications • Short-range wireless or wireline • DOT operated LAN or WAN • Public internet • Short-range, wireless, low latency communications • Commercial wireless communications • VPN over public internet
2.	Communications shall interface with encoders and decoders to enable conversion of data and information to/from digital signals.	Field – Confirm that communications interface with encoders and decoders to enable conversion of data and information to/from digital signals.	Pass/Fail	Test for: • Long-range communications • Short-range wireless or wireline • DOT operated LAN or WAN • Public internet • Short-range, wireless, low latency communications • Commercial wireless communications • VPN over public internet
3.	Communications shall transfer voice from sender to receiver devices.	Field – Confirm that communications transfer voice from sender to receiver devices.	Pass/Fail	Test for: • Commercial wireless communications • Agency operated wireless radio
4.	Communications design shall address required bandwidth (capacity) for MnDOT to make video available to media partners with sufficient quality.	Design – Confirm that the communications design addresses required bandwidth (capacity) for MnDOT to make video available to media partners with sufficient quality.	Content Review	Test for public internet only

	System Requirement	Testing Instructions	Type of Result	Comments / Notes
5.	Communications design shall address required bandwidth (capacity) for internal agency operated communications components.	Design – Confirm that the communications design addresses required bandwidth (capacity) for internal agency operated communications components.	Content Review	Test for: • Long-range communications • Short-range wireless or wireline • DOT operated LAN or WAN
6.	Communications design shall address required data transfer speed needs of the applications supported.	Design – Confirm that the communications design addresses required data transfer speed needs of the applications supported.	Content Review	Test for all communication components / technologies
7.	Communications design shall address consistency needs of the applications supported.	Design – Confirm that the communications design addresses consistency needs of the applications supported.	Content Review	Test for: • Long-range communications • Short-range wireless or wireline • DOT operated LAN or WAN • Short-range, wireless, low latency communications • Commercial wireless communications • Agency operated wireless radio
8.	Communications design shall address reliability needs of the applications supported.	Design – Confirm that the communications design addresses reliability needs of the applications supported.	Content Review	Test for: • Long-range communications • Short-range wireless or wireline • DOT operated LAN or WAN • Short-range, wireless, low latency communications • Commercial wireless communications • Agency operated wireless radio

	System Requirement	Testing Instructions	Type of Result	Comments / Notes
9.	Communications design shall address recovery needs of the applications supported.	Design – Confirm that the communications design addresses recovery needs of the applications supported.	Content Review	Test for: • Long-range communications • Short-range wireless or wireline • DOT operated LAN or WAN • Short-range, wireless, low latency communications • Agency operated wireless radio
10.	Communications shall restrict access to servers or devices outside the agency, except through firewall protection.	Field – Confirm that communications restrict access to servers or devices outside the agency, except through firewall protection.	Pass/Fail	Test for: • Long-range communications • Short-range wireless or wireline • DOT operated LAN or WAN • Short-range, wireless, low latency communications • VPN over public internet
11.	Communications shall provide a secure data exchange without requiring devices and systems interacting with the device to maintain their own firewall protection.	Field – Confirm that communications provide a secure data exchange without requiring devices and systems interacting with the device to maintain their own firewall protection.	Pass/Fail	Test for: • Long-range communications • Short-range wireless or wireline • DOT operated LAN or WAN • Short-range, wireless, low latency communications
12.	Communications shall use secure methods for encrypting data in transit to accommodate data exchange outside the agency firewall.	Field – Confirm that communications use secure methods for encrypting data in transit to accommodate data exchange outside the agency firewall.	Pass/Fail	Test for all communication components / technologies
13.	Communications shall rely upon and require firewall or related protection within applications connected through the communications solution.	Field – Confirm that communications rely upon and require firewall or related protection within applications connected through the communications solution.	Pass/Fail	Test for all communication components / technologies

	System Requirement	Testing Instructions	Type of Result	Comments / Notes
14.	Communications designs shall include security and/or firewall capabilities within the applications serving as senders and receivers (to accommodate lack of security control in the communications).	Field – Confirm that security and/or firewall capabilities are present within the applications serving as senders and receivers (to accommodate lack of security control in the communications).	Pass/Fail	Test for: • Public internet • Commercial wireless communications
15.	Communications shall comply with agency security policy to block malicious attempts and cybersecurity attacks.	Field – Confirm that communications comply with agency security policy to block malicious attempts and cybersecurity attacks.	Pass/Fail	Test for: • Long-range communications • Short-range wireless or wireline • DOT operated LAN or WAN • Short-range, wireless, low latency communications • Commercial wireless communications • VPN over public internet
16.	Communications shall follow design standards for conduit protection, burial depth, and grounding.	Field – Confirm that the communications design follows standards for conduit protection, burial depth, and grounding.	Pass/Fail	Test for: • Long-range communications • Short-range wireless or wireline • DOT operated LAN or WAN • Short-range, wireless, low latency communications • Commercial wireless communications • Agency operated wireless radio
17.	Wireless communications deployment design shall include an interference analysis.	Design – Confirm that the wireless communications deployment design includes an interference analysis.	Content Review	Test for: • Short-range, wireless, low latency communications • Agency operated wireless radio

	System Requirement	Testing Instructions	Type of Result	Comments / Notes
18.	Communications design shall include documentation of hardware and field elements.	Design – Confirm that the communications design includes documentation of hardware and field elements.	Content Review	Test for: • Long-range communications • Short-range wireless or wireline • DOT operated LAN or WAN • Short-range, wireless, low latency communications • Agency operated wireless radio
19.	Communications devices shall be mounted on appropriate support structures.	Field – Confirm that communications devices are mounted on appropriate support structures.	Pass/Fail	Test for: • Long-range communications • Short-range wireless or wireline • DOT operated LAN or WAN • Short-range, wireless, low latency communications • Agency operated wireless radio
20.	Communications designs shall obtain any required licenses for devices or communications.	Design – Confirm that the communications design includes required licenses for devices or communications.	Content Review	Test for: • Short-range, wireless, low latency communications • Agency operated wireless radio
21.	Communications design shall use application specific approaches to avoid 'cross-talk' interference (e.g. MnPass application may use GPS tag coordination).	Design – Confirm that the communications design uses application specific approaches to avoid 'cross-talk' interference (e.g. MnPass application may use GPS tag coordination).	Content Review	Test for short-range wireless or wireline