MICHIGAN
DEPARTMENT OF TRANSPORTATION

SPECIAL PROVISION
FOR
SYSTEM INTEGRATION AND TESTING

a. Description. This work consists of conducting system integration and acceptance testing work in accordance with the standard specifications, except as modified herein.

1. General. System integration and testing includes network integration of ITS devices into the communication network and testing to prove functionality and operation for local, subsystem and final system. This may include trunk and distribution fiber networks. This special provision contains testing requirements for all ITS devices and networks; however, all of these devices may not be included in this project. Disregard testing requirements for devices that are not part of this project.

2. Location. The integration services include all necessary configuration and programming work at communication aggregations points, subsystem locations, and the transportation operations center (TOC). All individual field device integration and equipment configurations are paid for under the individual device special provisions pay item.

3. Existing Systems. This project may include integration with existing ITS devices, systems, or networks. See applicable sections regarding network migration and network pre/post testing.

b. Materials. None specified.

c. Construction.

1. Prior to construction, in addition to the requirements outlined in equipment specific special provisions and the Special Provision for Basic Methods and Materials for Intelligent Transportation System Work, the Contractor must provide the following:

A. Equipment Integration Plan (EIP). After all equipment shop drawings have been approved, and 14 days prior to any ITS device field installation, submit a complete EIP to the Engineer for review and approval. The EIP must follow the procedures and integration requirements described in the Special Provision for Project Overview. Ensure any deviations from these specifications are noted in the EIP and are not executed in the field without the approval of the Engineer. Field installation and integration must not begin before approval of the EIP. The EIP includes, but is not limited to, the following:

(1) Revised ITS field device location plan in response to any device relocation or layout adjustment.

(2) Revised ITS field device interconnection and wiring layout plans in response to any construction field changes.

(3) Detailed step-by-step integration procedures for each local and TOC integration. Typical site integrations can be grouped in one integration procedure by approval of the Engineer.

(4) Typical devices interconnect diagrams for local, Hub/Node, and TOC locations. Ensure all device interconnect diagrams are generated in Visio, CAD, or Microstation and clearly identify equipment model numbers and cable types.

(5) Network Integration details, including but not limited to the following:

(a) Overall system network diagram, including full logical network and IP configuration details for all devices in a system diagram and tabulated formats.

(b) Bandwidth and traffic flow analysis for all network layers links including anticipated typical traffic flows.

(c) Network segmentation and virtual local area network (VLAN) configuration.

(d) Port assignments for all network and ITS devices.

(e) Provide proposed routing protocol and scheme including details of the method of operations and failover criteria, failover settings and routing costs. Include at a minimum:

(i) IP Unicast Routing;

(ii) IP Multicasting Routing;

(iii) Internet Group Management Protocol (IGMP); and

(iv) Constraint methods for multicast packet flooding.

(f) Provide a planned method of testing performance. Include at a minimum:

(i) Performance criteria description, proposed measurements, and methods of measurement;

(ii) Acceptance threshold and references for the values;

(iii) Network loading, 20, 50 and 90 percent full capacity at access, distribution and trunk layer; and

(iv) Measurement tools.

(g) Proposed configurations of Managed Field Ethernet Switches.

(h) Proposed coordination steps with the ITS Maintenance Contractor to have field switches integrated into MDOT’s Network Monitoring System (NMS).

(6) Equipment programming/configurations for each ITS device type included in

the Bill of Materials (BOM) and as specified in the Special Provision for Basic Methods and Materials for ITS Work.

(7) Advanced Traffic Management System (ATMS) Software Integration plan and proposed procedures.

(a) Procure material compatible with the MDOT Statewide ATMS Software.

(b) Confirmation testing and software integration into the ATMS will be paid for under the Special Provision for Integration, Advanced Traffic Management System Software.

(8) Fiber Network Integration plan. The fiber network integration portion of the EIP must include, but is not limited to, the following:

(a) Plan to test fiber optic cable prior to the connection into the Node switches and provide comparison between the calculated and anticipated measured optical link budgets, including adjustments for optical sensitivity.

(b) Proposed coordination steps with the ITS Maintenance Contractor for network integration into existing or proposed switches at Hub/Node and TOC locations including:

(i) Back-end network configurations;

(ii) Installation of fiber optic transceivers;

(iii) Network termination and end-to-end connectivity establishment; and

(iv) Port configuration including open shortest path first routing.

(c) Proposed termination of the distribution network into patch panels at local ITS cabinets as shown on the plans.

(d) Proposed configuration of new field switches in ITS cabinets that are logically nearest to the Node. Configuration for the ITS site next in the network architecture can only continue if previous link communications chain has been integrated and communications verified.

(9) Include a Network Migration Plan as part of the EIP if called for in the Special Provision for Project Overview. Submit a Network Migration Plan identifying the intended process for transitioning communications from the existing network architecture to the proposed network architecture including, but not limited to:

(a) A detailed action plan identifying each step in the installation and migration activities including testing.

(i) Pre-Migration Testing. Test existing network and ITS device availability before network and device migration. Work with the ITS Maintenance Contractor for pretesting. Ensure the results are used to compare pretesting to post test results. Propose expected changes in results in the Acceptance

Test Plan (ATP).

(ii) Post Migration Testing. Ensure testing is completed in accordance with the ATP requirements.

(b) A list of certified personnel performing the work at each location;

(c) Contact information for the main point of contact during regular business hours and emergencies;

(d) Switch installation and configuration details;

(e) A list of equipment to be removed;

(f) A contingency plan for each activity identifying recovery process from each situation outlined in the migration plan;

(g) An outline of downtime and risk mitigation strategies; and

(h) Coordination for reintegrating existing devices into ATMS if the proposed network configuration utilizes a new addressing scheme.

B. ATP.

(1) General Requirements.

(a) If a system mockup is required, submit a complete ATP to the Engineer at least 14 days prior to beginning the mockup. If a system mockup is not required, submit a complete ATP to the Engineer 14 days prior to installing any electronic devices in the field.

(b) The ATP must include individual test cases clearly showing passing criteria for all ITS devices as applicable per project.

(c) The ATP must include local, subsystem, and final system testing for all ITS devices to be integrated on this project.

(d) Ensure failures during testing are included in a report that documents the defective unit or setting and the corrective action taken. Minor failures may be addressed and retested at the Engineer's discretion. Major failures, which would require additional work to multiple units and sites, may cause the Engineer to stop testing until the issue has been resolved. No extension of time or additional payments will be given or made due to delays caused by failed acceptance testing.

(e) The ATP forms as well as any supplemental documentation completed during the testing are to be delivered to the Engineer upon system acceptance. Ensure the forms are signed by the Contractor as well as the Engineer or representative.

(2) ITS Local Device Assembly Test (LDAT). Before ITS sub-system tests (SST), conduct stand-alone tests of the equipment installed at each field site as approved by

the Engineer. The test must, at a minimum, exercise all stand-alone (non-network) functional operations of the field equipment with all of the equipment installed per the plans or as directed by the Engineer.

(3) ITS Sub-System Test (SST). Conduct SST to verify a section of the overall ITS system is functioning properly. Ensure SST testing is conducted at logical nodes or aggregation points to verify both communications and device functionality.

(4) ITS Final System Test (FST). FST is the last step in the ATP and serves as the basis for system acceptance. Ensure the FST is performed at the TOC following completion of the SST. After the successful completion of the FST, the burn-in period begins.

(5) Testing Requirements. Ensure the list of ITS devices and testing requirements identified in Table 1 are included in the ATP. Submit test procedures required for Fiber Optic and Licensed Wireless Link Backhaul as part of their own special provision requirements.

Table 1: List of ITS Devices Required for ATP

ITS Devices	Test Procedures Required
ITS Cabinet	LDAT, SST, FST
Surveillance System Assembly	LDAT, SST, FST
Dynamic Message Sign (DMS)	LDAT, SST, FST
Microwave Vehicle Detection System (MVDS)	LDAT, SST, FST
Managed Field Ethernet Switches (MFES)	LDAT
Uninterruptible Power Supply (UPS)	LDAT, SST, FST
Unlicensed Wireless Radios	LDAT
Cellular Modems/Cable Modems	LDAT, FST
Environmental Sensor Station (ESS) Equipment	LDAT, FST
IP Power Distribution Unit	LDAT, FST
Infrared Illumination Device	LDAT
Lane Control System (LCS)	LDAT, SST, FST
Dynamic Message Panel (DMP)	LDAT, SST, FST
Fiber Optic Hardware Assembly	LDAT

For each ITS device type, ensure there is a test case developed with pass/fail criteria. All functional requirements in the test case must pass during the witness testing to grant final acceptance. The sections below list all functional requirements per device to be included in each test case. During the review of the ATP report, the Engineer has the right to add or remove test case requirements, as applicable, to the project and within the functional requirements shown in the special provisions.

(a) ITS Cabinet.

(i) LDAT.

1) Visual inspection to check workmanship, confirm equipment has

been installed in accordance with approved layout drawings and equipment shop drawings, and verify the cabinet field wiring matches the cabinet wiring diagram and interconnect drawings are stored in the cabinet.

2) Verify proper operation of the Ground Fault Interrupter (GFI) outlet.

3) Verify proper operation of the lights and vent fans.

4) Verify all ITS devices are labeled as required with the device name and IP address.

5) Verify accuracy of the temperature and humidity reported by the cabinet monitoring system.

6) Test door alarms locally.

7) Set and verify network settings (i.e., IP address, subnet mask, and gateway).

8) Configure the cabinet monitor to issue Simple Network Management Protocol (SNMP) traps to a central computer when a cabinet door is open and when the temperature in the cabinet exceeds 120 °F.

a. Demonstrate the cabinet monitor system can successfully use a SNMP trap for door opening/closing.

(ii) SST. Verify communications to the SNMP card of the cabinet monitoring system.

(iii) FST.

1) Test Alarm Conditions. Demonstrate the cabinet monitoring system can successfully use SNMP traps to alert a computer at the TOC about an open door and a high temperature.

2) Verify the ability of users in the TOC to determine the temperature, humidity, and door status using a web browser.

(b) Surveillance System Assembly.

(i) LDAT. Ensure the following local field operational tests are performed at the camera assembly field site on each closed-circuit television (CCTV) camera. Provide a laptop computer testing the video and camera control through software that supports *NTCIP*. Notify the Engineer at least 14 working days in advance of the proposed date for the camera local device assembly test. After the camera assembly, including the camera hardware, DVE, power supply, and connecting cables, has been installed:

1) Camera Assembly (local control). Perform the following local field operational tests at the camera assembly field site in accordance with the test plans. After the camera assembly, including the camera hardware,

power supply and connecting cables, has been installed:

a) Verify physical construction has been completed as specified in the contract, on the plans and herein.

b) Inspect the quality and tightness of ground and surge protector connections, patch cords and jumpers.

c) Verify proper voltage of all the power supplies.

d) Verify installation of specified cables and connections between the camera, PTU and camera control receiver.

e) Set and verify the camera control address and network/IP settings.

f) Verify the presence and quality of the video image during day and night lighting conditions via a video streaming client on the laptop computer.

g) Verify title block information is correct.

h) Exercise the pan, tilt, zoom (PTZ), focus - auto and manual, iris opening, and manual iris control selection; and the operation, low-pressure alarm (if present), preset positioning, and power on/off functions.

i) Demonstrate pan/tilt speed and extent of movement meets the specifications, and verify latency of PTZ does not exceed 250 milliseconds

2) Camera Cable. Furnish all equipment, appliances, and labor necessary to test the installed camera cable between the camera assembly and the network communication device.

a) Perform tests on the camera Ethernet cable per the *ANSI/TIA/EIA-568-B.1* using a meter designed for Ethernet cable testing.

b) Perform all Ethernet cable testing after final termination and cable installation, but prior to the connection of any electronics or field devices.

c) Replace any cable that fails to meet these parameters, or if any testing reveals defects in the cable, and test the new cable as specified above.

3) Configure and test the CCTV camera using settings that were approved at equipment mockup (if required) per the Special Provision for Project Overview or as approved by the Engineer to ensure interoperability and security.

4) Coordinate all configuration settings with the Engineer and provide any exportable electronic configuration files for each camera. The file will contain the location of the camera, its serial number, final accepted configuration and will be named to clearly indicate the device location from which it was obtained.

(ii) SST. Verify communications to the surveillance system or DVE.

(iii) FST. Ensure the following remote operational tests are conducted at the TOC using *NTCIP* software.

1) Verify the camera IP address and system name.

2) Verify the presence and quality of the video image.

3) Exercise the PTZ, focus, iris opening, and manual iris control selection; and the operation, low-pressure alarm (if present), preset positioning, and power on/off functions.

(c) DMS. Integrate the DMS into the communications network within 14 calendar days of installation and successful post-delivery testing. DMS may be used by MDOT as soon as integration is complete through final acceptance testing.

(i) LDAT. Ensure DMS LDAT is conducted at each field location after the DMS has been installed and integrated into the system. The test cases, at minimum, must include inspection of the sign housing, power supply, and electrical distribution; DMS controller; DMS Auxiliary Control Panel (ACP); LED display modules; temperature and light control; and sign failure conditions.

1) DMS Controller.

a) Verify a “local/remote” switch with an LED indicator that places the controller in local mode such that it can be controlled from the front panel interface instead of via the primary communication channel.

b) Verify the reset switch to quickly restart the controller.

c) LED “Active” indicator blinks when the controller is operating.

d) Verify system status LCD displays time and date.

2) DMS ACP.

a) Verify a “local/remote” switch with an LED indicator that places the controller in local mode such that it can be controlled from the front panel interface instead of via the primary communication channel.

b) Reset switch to quickly restart the controller.

c) LED “Active” indicator blinks when the controller is operating.

d) Verify system status LCD displays time and date.

3) LED Display Module.

a) On command from either a remote computer or local laptop running the central control software, the sign controller must test the operation of all LED pixels and determine whether their functional status is “normal” or “stuck-off.”

- Run a diagnostic test to verify all the LED driver cards, power supply diagnostic cards, temperature sensor cards, fan sensor card, and photo sensor are functioning properly.

- Verify Real-time DMS message posting.

- Verify static test message display.

- Verify flashing test message display.

- Verify a multipage test message display.

- Verify manual blanking of the display.

4) Light Control (DMS Intensity Control).

a) Verify from the DMS controller the option of selecting from a minimum of 100 LED intensity levels. Ensure LED intensity levels are available in a range of 1 percent to 100 percent of the maximum display intensity, and in increments of 1 percent.

b) Does not cause any flickering of the LED display matrix.

c) Verify manual and automatic intensity control modes to be user selectable using the DMS control software, although the typical control mode must be “automatic.”

d) Verify manual intensity control from both local and remote locations.

5) Sign Failure Conditions.

a) Verify that in the event of communication error between the DMS sign controller and the system control computer; the DMS controller automatically blanks the sign.

b) Verify that in the event of a power failure, the DMS controller automatically blanks the sign.

c) Ensure all testing work, activity, and results are documented and reported with their details to the Engineer.

(ii) SST. Verify communications to the DMS controller.

(iii) FST. Ensure the DMS FST is conducted from the TOC using the ATMS software. In the event the ATMS software is not capable of testing some required functional specifications of the DMS, then the DMS specific manufacturer's software can be used. Test the following requirements remotely:

1) LED display module as described in the LDAT.

2) DMS intensity control as described in the LDAT.

3) Sign failure conditions as described in the LDAT.

(d) MVDS.

(i) LDAT.

1) Verify physical construction has been completed as specified in the contract and herein.

2) Verify network settings.

3) Inspect the quality and tightness of ground connections.

4) Verify lanes match actual field conditions using the MVDS vendor-supplied test software.

5) Verify speed, volume, and occupancy are within the requirements of the MVDS special provision. The use of a calibrated Lidar gun is required for the speed test. Follow manufacturer recommended procedures for calibration of the Lidar gun.

6) Each installed MVDS's volume counts and speed measurements are to be verified utilizing the MVDS vendor-supplied test software running on a laptop connected locally to the detector communication port. Compare the counts from the detector to visual counts or counts from permanent or temporary traffic detection devices of known accuracy. Compare the speed measured by the detector to the speeds measured by the Lidar gun.

7) Ensure all testing work, activity, and results are documented and reported with their details to the Engineer.

(ii) SST. Verify communications to the MVDS.

(iii) FST.

1) Verify network interface device is receiving and transmitting data from the remote site to across the ITS network.

2) Conduct FST from the head end ATMS software.

(e) MFES.

(i) LDAT.

1) Verify physical connections are performed as specified in the contract.

2) Verify all LED indicators for link, activity, and power are functioning.

3) Configure and test the MFES using settings that were approved at equipment mockup (if required) per the Special Provision for Project Overview or as approved by the Engineer to ensure interoperability and security. Coordinate all configuration settings with the Engineer and provide backup configuration files electronically. Configuration settings include system name, location, IP address, subnet mask, and default gateway.

4) Verify all active ports have been configured per the Special Provision for Project Overview. Check the speed, duplex, and Virtual Local Area Network (VLAN) settings.

5) Disable any ports not in use.

6) If any MFES installed in the project is connected to equipment that originates a multicast stream, develop an IP multicasting plan, including multicast addressing and quality of service parameters, using protocol independent multicast sparse mode (PIM-SM). Revise the plan until it is satisfactory to the Engineer and then configure the MFESs and other devices accordingly.

7) On Layer 3 MFESs, configure gateway IP addresses for all subnets that connect to that MFES. Configure open shortest path first (OSPF) routing and confirm that routes to those subnets are being advertised to adjacent MFESs. Configure access control lists (ACLs). Work with the Engineer to determine IP ranges, ports, and other settings to be used in configuring the ACLs.

8) On Layer 2 MFESs, configure VLANs as shown on the plans. Configure trunking ports between MFESs and access ports between MFESs and equipment. Set VLAN Trunk Protocol (VTP) to transparent mode on all MFESs. Configure port security to only allow the media access control (MAC) addresses of equipment connected to the MFES to pass traffic. Configure Rapid Spanning Tree Protocol (RSTP) to prevent bridging loops and provide redundant paths.

(f) UPS.

(i) LDAT.

1) Verify electrical connections have been completed as detailed in the contract and herein.

2) Provision UPS with IP address and network settings provided by the Engineer. Configure the UPS using settings that were approved at equipment mockup (if required) per the Special Provision for Project Overview or as approved by the Engineer.

3) Alarms.

a) Disable all audible alarms associated with the UPS.

b) Ensure that the communication module of the UPS reports alarm conditions to the TOC using SNMP over the Ethernet communication system.

4) Verify the UPS can run off battery backup. Test utility power loss, automatic low-battery, and high temperature shutdown features per manufacturer's instructions without damaging device. Verify the UPS returns to normal operations without a manual reset.

5) Demonstrate the UPS can successfully use a SNMP trap for utility power loss and return to normal operations.

(ii) SST. Verify remote communications to the SNMP card of the UPS.

(iii) FST. Test alarm conditions. Demonstrate the UPS can successfully use SNMP traps to alert a computer at the TOC about a power loss, low-battery, and high temperature shutdown.

(g) Unlicensed Wireless Radios.

(i) LDAT.

1) Furnish all test equipment required to test the wireless link. The furnishing of test equipment is an appurtenance of the system integration and testing pay item.

2) Testing based on the Contractor supplied Test Plan must begin 30 days prior to the date of acceptance notification to the Engineer that the wireless link meets all requirements of the specifications and complies with all appropriate standards listed in the contract and is ready for final inspection.

3) Verify physical construction has been completed per the contract.

4) Inspect the quality and tightness of ground connections.

5) Set and verify the radio has been configured with the proper site name, IP address, subnet mask, gateway, and VLAN settings.

6) Verify actual throughput meets requirements using two laptops with Iperf, Jperf, or similar approved software for each site.

7) Record the throughput, Signal-to-Noise Ratio (SNR), Received Signal Strength (RSS), Received Signal Strength Indication (RSSI) and noise level for each site.

8) The Contractor is responsible for meeting the throughput and other requirements for wireless links. Ensure wireless links that do not meet the performance requirements during acceptance testing are upgraded or replaced at no additional cost to the contract.

(h) Cellular Modem/Cable Modem.

(i) LDAT.

1) Verify physical construction has been completed per the contract.

2) Verify cable, connections, and antenna (as applicable) are properly installed.

3) Integrate and test to meet MDOT specifications for integration and as shown on the plans.

4) Set and verify virtual private network (VPN) settings, local IP address, port forwarding, Network Address Translation (NAT), and IP-based filtering.

5) Conduct an upload throughput test of the cellular modem using Iperf, Jperf, or similar approved software.

6) Test the data throughput between the MFES inside the ITS cabinet through the cable modem and to an internet connected computer using a standard software application designed for this purpose. The throughput test will be witnessed by the Engineer and System Manager, recorded, and signed off by both the Contractor and MDOT as adequate for the design intent. The expected value for data throughput will be provided by the Engineer upon coordination with the cable internet provider.

(ii) FST. Verify remote connectivity to the cell/cable modem. Ensure the modem can be monitored and configured remotely.

(i) ESS Equipment. Integrate and calibrate the sensors with the remote processing unit (RPU) located in the field cabinet as designated on the plans.

(i) LDAT.

1) After each ESS field location is fully installed and integrated, ensure the following tests are conducted for all environmental sensors and RPU.

2) Furnish test equipment at no additional cost to the contract, that can complete test procedures whose parameters are equal or better than the minimum test parameters specified by the sensor manufacturer. Provide a list of tools and test equipment (common and specialized, including any built-in testing facilities that are functionally equivalent to external test equipment) necessary to test the equipment.

3) Verify physical construction has been completed as detailed in the contract and herein.

4) Verify all cable, connectors, grounding, bonding, and lightning protection.

5) Sensor Testing. Conduct all sensor measurements using manufacturer's recommended testing equipment and compare the recorded data to the functional requirements shown in the Atmospheric sensors, Pavement Condition Sensors, and Sub-Surface Temperature Probe special provisions. Provide all test results to MDOT for review prior to final system acceptance.

6) RPU Testing.

a) Verify all sensors are connected to the RPU as shown on the plans.

b) Set and verify the IP address and network settings provided by the Engineer.

c) Verify accurate data collection and reporting from each sensor.

d) Verify the RPU displays real-time data for all sensors connected.

e) Verify the RPU displays the data for the entire system "at a glance" for analysis.

f) Verify a long-term history page is present to show historical data from any sensor connected to the RPU. A log of at least 3 days should be present.

g) Verify the RPU supports local maintenance of all devices physically connected to the RPU using a graphical user interface (GUI).

h) Verify the RPU allows remote configuration of any sensor physically connected to the RPU using web interface.

i) Verify the presence of eight camera views in the RPU menu.

j) Verify the user can switch the first eight images with a second set of eight views.

(ii) FST. After each ESS field location is fully installed and integrated, ensure the following tests are conducted from the TOC using ATMS or current residing Road Weather Information System (RWIS) central management software:

1) Verify remotely from the TOC that each sensor is reporting accurate data within the ranges shown in the contract.

2) Verify each ESS location is represented on the map on the RWIS central management system.

3) Verify the presence of eight camera views on the hosted site during the day and the night. Ensure night images are easily viewed when an infrared (IR) illumination device is present.

4) Verify the IP address and site name corresponds to the ESS site location.

5) Verify remote configuration of the RPU from a web-browser.

6) Verify remote configuration of the IP camera from a web-browser.

(j) IP Power Distribution Unit (PDU).

(i) LDAT.

1) Configure the PDU for access from the MDOT TOC or head-end.

2) Verify the user can reset the power to all the devices connected to the IP PDU.

3) Verify all devices recover and return to normal operation.

(ii) FST.

1) Verify the user can remotely reset the power to all the devices connected to the IP PDU.

2) Verify all devices recover and return to normal operation.

(k) IR Illumination Device.

(i) LDAT.

1) Verify physical construction has been completed per the contract.

2) Verify the camera images/video is clearly viewable at night during low ambient light conditions.

(l) LCS. Provide Parsons Transportation Group, MDOT's ATMS contractor, access to an LCS controller, either by remote access or by providing a physical

unit, for development and testing of the controller driver and ATMS software within 60 days of project award. Provide all firmware updates for this LCS controller throughout construction, testing and integration.

(i) LDAT. Ensure LCS LDAT is conducted at each field location after the LCS has been installed and integrated into the system. The test cases, at minimum, must include inspection of the sign housing, power supply, and electrical distribution; LCS controller; LCS ACP; LED display modules; temperature and light control; and sign failure conditions.

1) LCS Controller.

a) Set and verify the IP address and network settings provided by the Engineer.

b) Verify a “local/remote” switch with an LED indicator that places the controller in local mode such that it can be controlled from the front panel interface instead of via the primary communication channel.

c) Verify the reset switch to quickly restart the controller.

d) LED “Active” indicator blinks when the controller is operating.

e) Verify system status LCD displays time and date.

f) Verify what you see is what you get (WYSIWYG) functionality.

2) LCS ACP.

a) Set and verify the IP address and network settings provided by the Engineer.

b) Verify a “local/remote” switch with an LED indicator that places the controller in local mode such that it can be controlled from the front panel interface instead of via the primary communication channel.

c) Reset switch to quickly restart the controller.

d) LED “Active” indicator blinks when the controller is operating.

e) Verify system status LCD displays time and date.

f) Verify WYSIWYG functionality.

3) LED Display Module.

a) On command from either a remote computer or local laptop running the central control software, the sign controller must test the operation of all LED pixels and determine whether their functional status is “normal” or “stuck-off.”

- Run a diagnostic test to verify all the LED driver cards, power supply diagnostic cards, temperature sensor cards, fan sensor card, and photo sensor are functioning properly.

- Verify Real-time LCS message posting, including American Standard Code for Information Interchange (ASCII) text and graphics.

- Verify static test message display.

- Verify flashing test message display.

- Verify a multipage test message display.

- Verify manual blanking of the display.

- Verify posting of pre-stored graphic images

4) Light Control (LCS Intensity Control).

a) Verify from the LCS controller the option of selecting from a minimum of 100 LED intensity levels. Ensure LED intensity levels are available in a range of 1 percent to 100 percent of the maximum display intensity, and in increments of 1 percent.

b) Verify that intensity control does not cause any flickering of the LED display matrix.

c) Verify manual and automatic intensity control modes to be user selectable using the LCS control software, although the typical control mode must be “automatic.”

d) Verify manual intensity control from both local and remote locations.

5) Sign Failure Conditions.

a) Verify that in the event of communication error between the LCS sign controller and the system control computer; the LCS controller automatically blanks the sign.

b) Verify that in the event of a power failure, the LCS controller automatically blanks the sign when power is restored.

c) Verify that in the event of a power failure, all data in the LCS controller non-volatile memory is retained.

d) Ensure all testing work, activity, and results are documented and reported with their details to the Engineer.

(ii) SST. Verify communications to the LCS controller.

(iii) FST. Ensure the LCS FST is conducted from the TOC using the ATMS software. In the event the ATMS software is not capable of testing some required functional specifications of the LCS, then the LCS specific manufacturer's software can be used. Test the following requirements remotely:

1) LED display module as described in the LDAT.

2) LCS intensity control as described in the LDAT.

3) Sign failure conditions as described in the LDAT.

(m) DMP. Integrate the DMP system into the communications network.

(i) LDAT. Ensure DMP LDAT is conducted at each field location after the DMP has been installed and integrated into the system. The test cases, at minimum, must include inspection of the sign housing, power supply, and electrical distribution; DMP controller; LED display modules; temperature and light control; and sign failure conditions.

1) DMP Controller.

a) Verify a "local/remote" switch with an LED indicator that places the controller in local mode such that it can be controlled from the front panel interface instead of via the primary communication channel.

b) Set and verify the IP address and network settings provided by the Engineer.

c) Verify the reset switch to quickly restart the controller.

d) LED "Active" indicator blinks when the controller is operating.

e) Verify system status LCD displays time and date.

f) Verify WYSIWYG functionality.

2) DMP ACP.

a) Verify a "local/remote" switch with an LED indicator that places the controller in local mode such that it can be controlled from the front panel interface instead of via the primary communication channel.

b) Set and verify the IP address and network settings provided by the Engineer.

c) Reset switch to quickly restart the controller.

d) LED "Active" indicator blinks when the controller is operating.

e) Verify system status LCD displays time and date.

f) Verify WYSIWYG functionality.

3) LED Display Module.

a) On command from either a remote computer or local laptop running the central control software, the sign controller must test the operation of all LED pixels and determine whether their functional status is “normal” or “stuck-off.”

- Run a diagnostic test to verify all the LED driver cards, power supply diagnostic cards, temperature sensor cards, fan sensor card, and photo sensor are functioning properly.

- Verify Real-time DMP message posting.

- Verify static test message display.

- Verify flashing test message display.

- Verify a multipage test message display.

- Verify manual blanking of the display.

4) Light Control (DMP Intensity Control).

a) Verify from the DMP controller the option of selecting from a minimum of 100 LED intensity levels. Ensure LED intensity levels are available in a range of 1 percent to 100 percent of the maximum display intensity, and in increments of 1 percent.

b) Does not cause any flickering of the LED display matrix.

c) Verify manual and automatic intensity control modes to be user selectable using the DMP control software, although the typical control mode must be “automatic.”

d) Verify manual intensity control from both local and remote locations.

5) Sign Failure Conditions.

a) Verify that in the event of communication error between the DMS sign controller and the system control computer; the DMP controller automatically blanks the sign.

b) Verify that in the event of a power failure, the DMP controller automatically blanks the sign.

c) Verify that in the event of a power failure, all data in the DMP

controller non-volatile memory is retained.

d) Ensure all testing work, activity, and results are documented and reported with their details to the Engineer.

(ii) SST. Verify communications to the DMP controller.

(iii) FST. Ensure the DMP FST is conducted from the TOC using the ATMS software. In the event the ATMS software is not capable of testing some required functional specifications of the DMP, then the DMP specific manufacturer's software can be used. Test the following requirements remotely:

1) LED display module as described in the LDAT.

2) DMP intensity control as described in the LDAT.

3) Sign failure conditions as described in the LDAT.

(n) Fiber Optic Hardware Assembly (all sizes).

(i) LDAT.

1) Visual inspection to check workmanship, confirm equipment has been installed in accordance with approved layout drawings and equipment shop drawings, and verify the cabinet field wiring matches the cabinet wiring diagram.

2) Verify all fiber optic cables, pigtails, jumpers, and patch panels are labeled as shown on the plans per the ITS cabinet labeling scheme.

3) Verify all fiber optic cables, pigtails and jumpers are properly trained inside the fiber optic hardware assembly.

(o) Field Security Appliance (FSA).

(i) LDAT.

1) Verify physical construction has been completed per the contract.

2) Verify all LED indicators for link, activity, and power are functioning.

3) Set and verify VPN settings, local IP address, port forwarding, Network Address Translation (NAT), and IP-based filtering.

4) Configure the FSA to issue SNMP traps to MDOT's NMS.

a) Demonstrate the FSA can successfully send a SNMP trap.

5) Disable any ports not in use.

6) Configure port security to only allow the MAC addresses of equipment connect to the field security appliance.

(ii) SST. Verify communications to the FSA.

(iii) FST.

1) Test Alarm Conditions. Demonstrate that the FSA can successfully send an SNMP trap to MDOT's NMS

2) Verify remote connectivity to the FSA. Ensure the FSA can be monitored and configured remotely.

2. Post-Installation Testing Phase.

A. ATP Execution Requirements.

(1) After the ATP has been accepted, submit in writing a detailed ATP schedule to MDOT for witness testing in the field. Include time and duration for each test case in the schedule.

(2) Conduct pretesting to verify each device is performing in accordance with the passing criteria requirements submitted with each test case, prior to scheduling formal testing with the Engineer and MDOT.

(3) Maintain an ATP progress report tracker in a tabulated format and submit to MDOT when required and at the completion of testing.

(4) Maintain signed electric and hard copies of the witness testing and submit to MDOT with the as-built documentation.

(5) Provide all required test equipment. Prior to field testing, ensure all test equipment datasheets and calibration records are submitted to MDOT for approval.

B. Burn-in Period Requirements.

(1) Begin the burn-in period at a time after FST acceptance and as approved by the Engineer. Ensure all ITS items are accepted and training requirements met prior to the start of the burn-in-period.

(2) Conduct the burn-in-period for 60 days.

(3) Maintain a failure log that records the date, time, and location of major and minor failures that occur, and the corrective actions taken. Record the details of the failure and corrective action in this log. Make documentation available for inspection by the Engineer and provide to the Engineer at the end of the burn-in-period.

(4) Equipment failure reports will be generated by the Engineer and issued to the Contractor for corrective action.

(5) There may be no major failures during the burn-in-period. If one occurs, restart

the 60-day period after the major failure has been corrected to the Engineer's satisfaction. The following are major failures:

(a) Less than 95 percent of entire ITS system for the project is operational at any moment.

(b) Any failure that requires more than 48 hours to correct after providing notice to the Contractor.

(c) Frequent occurrence of minor failures indicating a major system flaw, as determined by the Engineer.

(d) Any failure of routing or core network communications equipment.

(6) A minor failure is any other failure. The 60-day acceptance test period must be stopped when a minor failure occurs and restarted without resetting to zero after the minor failure is corrected to the satisfaction of the Engineer.

C. General requirements. Furnish, install, and integrate all available software/firmware upgrades through final acceptance for all new devices.

d. Measurement and Payment. The completed work, as described, will be measured as a lump sum and paid for at the contract price using the following pay item.

Pay Item	**Pay Unit**
System Integration and Testing	Lump Sum

System Integration and Testing will be paid based on Table 2:

Table 2: System Integration and Testing Partial Payments

Accepted EIP and ATP	50%
FST Acceptance	85%
Final ITS Acceptance	100%

Fifty percent of the lump sum will be paid upon acceptance of the EIP and ATP by the Engineer, and completion of the mockup if required in the Special Provision for Project Overview.

An additional 35 percent of the lump sum will be paid upon acceptance of the FST, by the Engineer. Ensure all FST's are successfully tested and satisfied per the requirements noted above. Any tests that do not pass will prevent receiving partial payment, unless otherwise approved by the Engineer.

The remaining 15 percent will be paid upon Final ITS Acceptance by the Engineer. In addition to successful completion of the burn-in test, final acceptance requires delivery of all contract deliverables, including all project documentation referenced in the Special Provision for Basic Methods and Materials for ITS work and other special provisions.