

RECEIVED

ON: **January 20, 2015**

and Checked for

CONFORMANCE

BY: **KMH** DATE: **1-29-2015**



CONSTRUCTION LEADERS

SUBMITTAL NO. : 004
Smart Work Zone

Item No.	Specification	Description
1	900.645-02	Smart Work Zone

PROJECT:
HARTFORD LATERAL SLIDE
PROJECT NO.: IM 091-2(79)
CONTRACT NO.: TBD

OWNER:
STATE OF VERMONT AGENCY OF TRANSPORTATION

ENGINEER OF RECORD:
STATE OF VERMONT AGENCY OF TRANSPORTATION

CONTRACTOR:
PCL CIVIL CONSTRUCTORS, INC.

JANUARY 20, 2015



January 15, 2015

Jeremy Mackling
PCL Civil Constructors, Inc.
3810 Northdale Blvd, Suite 200
Tampa, FL 33624

Re: Hartford IM 091-2(79)
Smart Work Zone (SWZ), Submittal No.1

Dear: Jeremy

Please find attached the Smart Work Zone submittal packet. Be advised that this electronic submittal is the only one I am submitting at this time. If hard copies are required let me know how many and I can generate those for you. Please forward those to the appropriate individuals.

The map showing the equipment types and locations is located at the front of the submittal packet. The locations for the PCMS's, PTZ's and the trailer mounted sensors are preliminary and may change depending upon actual site conditions, etc.

Please contact me with any questions or concerns.

Respectfully,

Scott Deschamps

Scott Deschamps
Director of Operations

WE ARE AN EQUAL OPPORTUNITY EMPLOYER

115 INDUSTRIAL LANE-BERLIN BARRE, VT 05641 (802) 223-8948 FAX (802) 229-1848



Smart Work Zone

Hartford, Vermont
IM-091-2(79)

PCL CONSTRUCTION

Submitted by:
Worksafe Traffic Control Industries, Inc.
115 Industrial Ln-Berlin, Barre, Vt. 05641
3 Garvin Falls Road, Bow, NH. 03304
800-547-0808

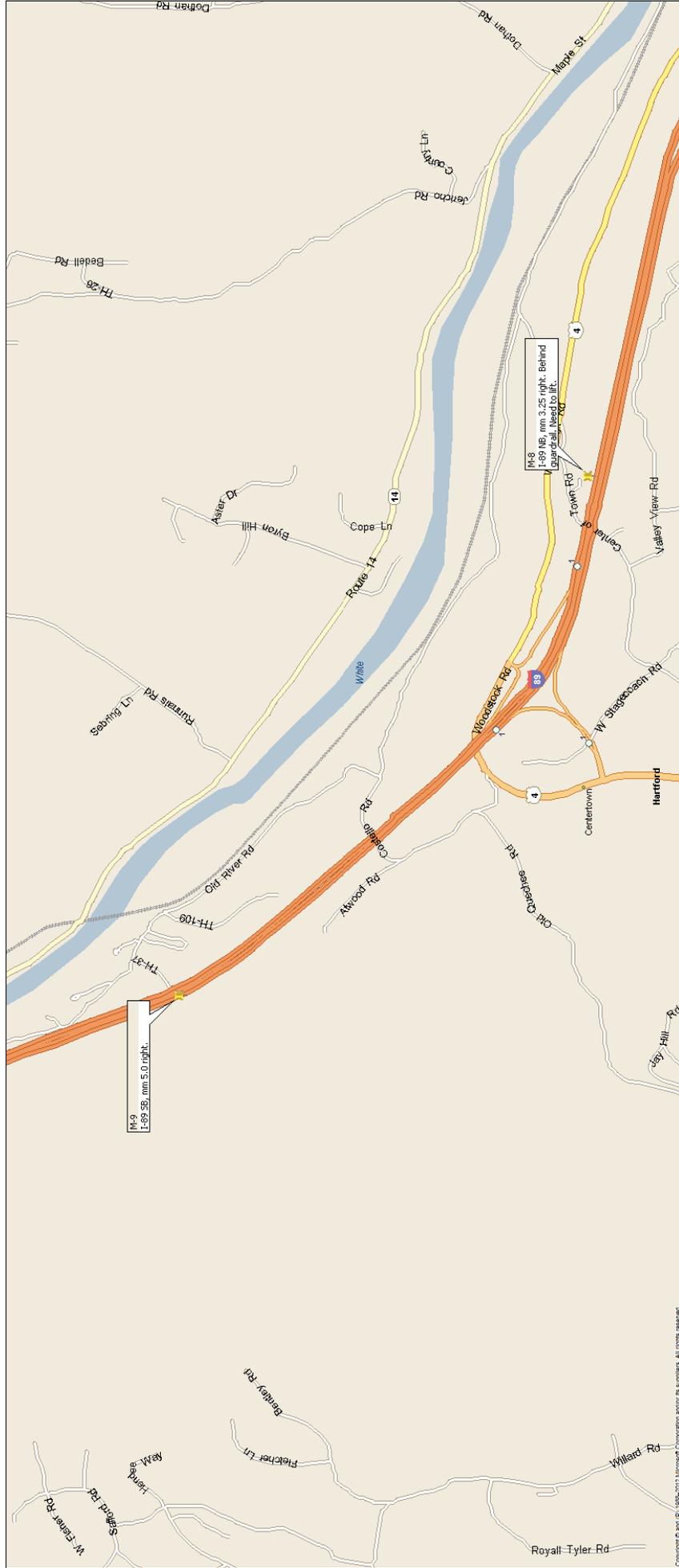


Table of Contents

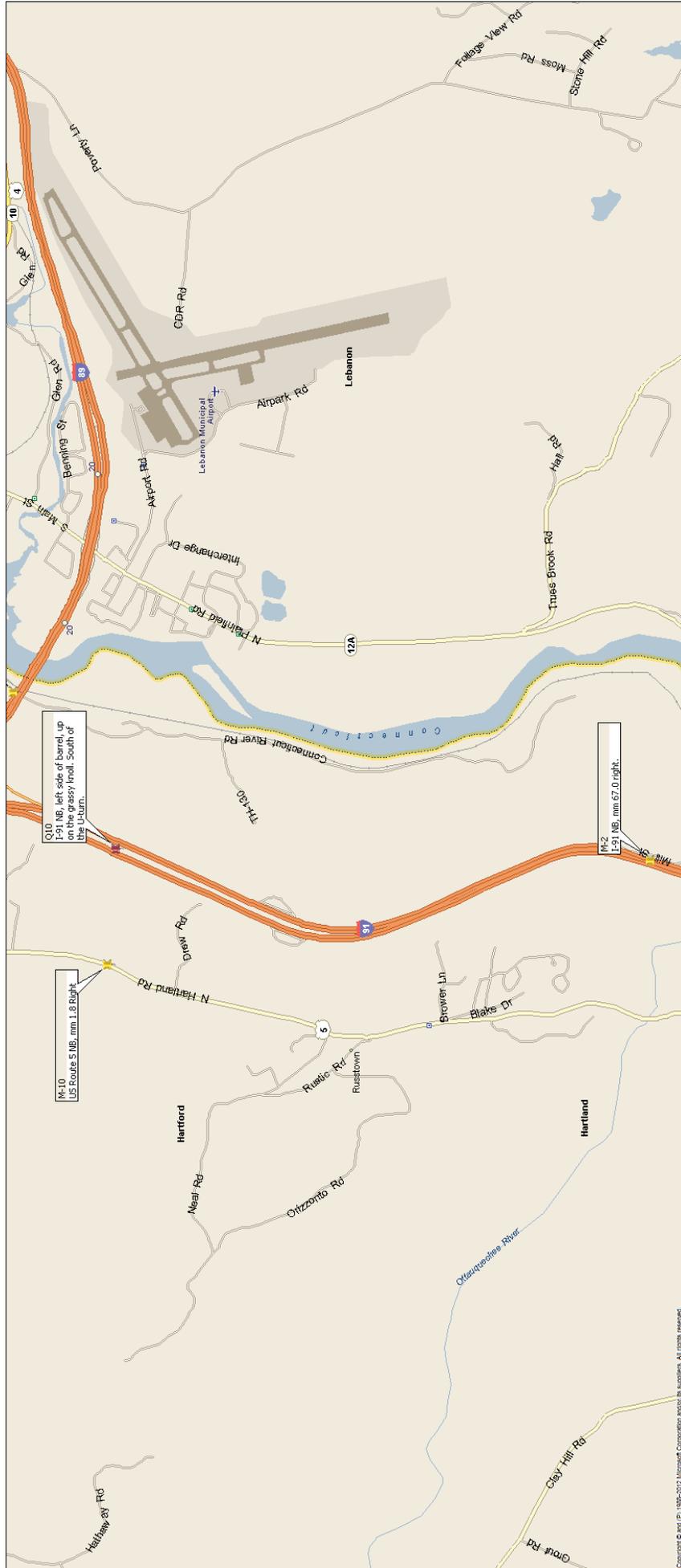
1. Proposed Equipment Layout Map
2. Contact Information
3. Project Experience
4. Portable Changeable Message Sign (PCMS) Specification
5. PCMS User Manual
6. Portable Queue Trailer (PQT) Specification
7. PQT User Manual
8. EZ Cam Video Trailer Specification
9. AXIS Pan-Tilt-Zoom (PTZ) Camera Specification
10. AXIS PTZ User Manual
11. ASTI Computerized Highway Information Processing System (CHIPS)
12. ASTI CHIPS US patent
13. SWZ System Failure Protocol

**THE FINAL LOCATIONS OF ALL MESSAGE
BOARDS, QUEUE SENSORS AND
CAMERAS SHALL MEET THE APPROVAL
OF THE ENGINEER**

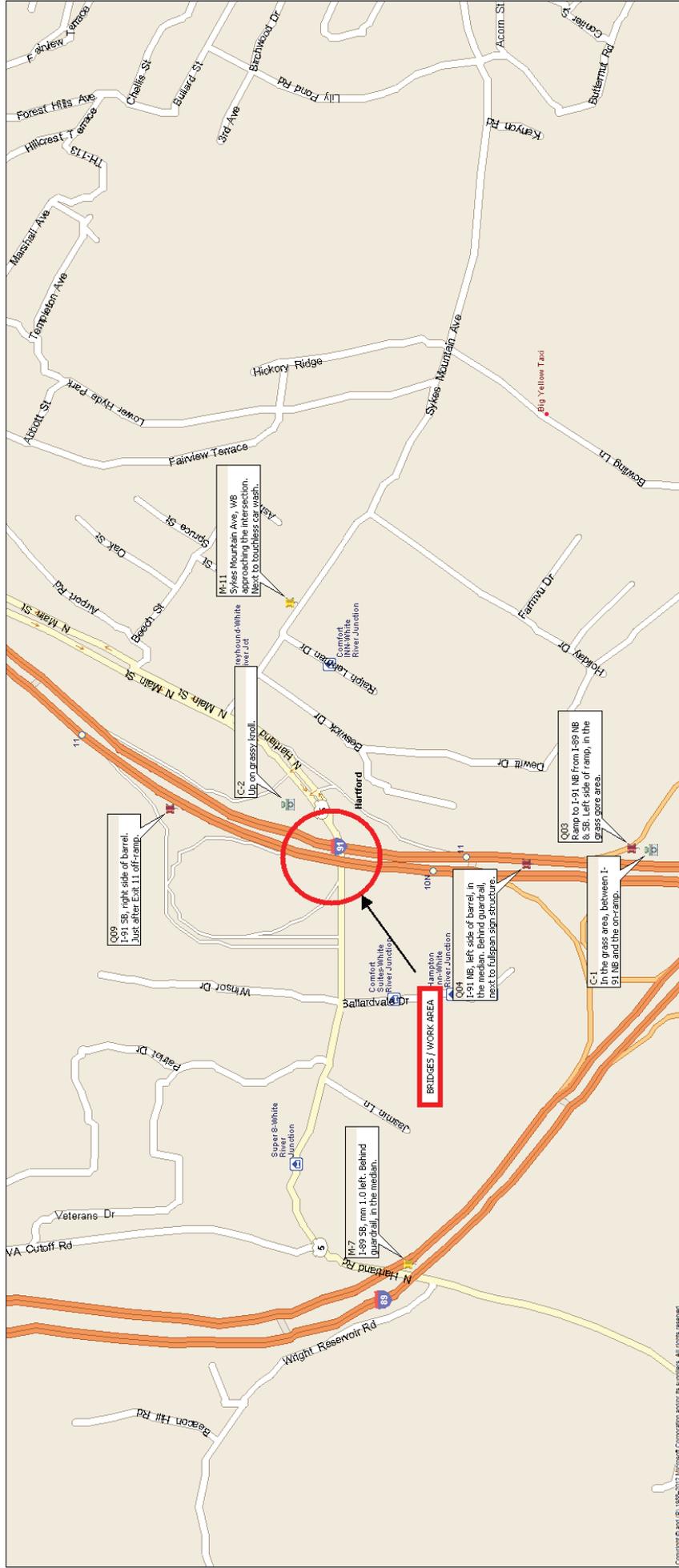
I-89 North Leg; North of WRJ



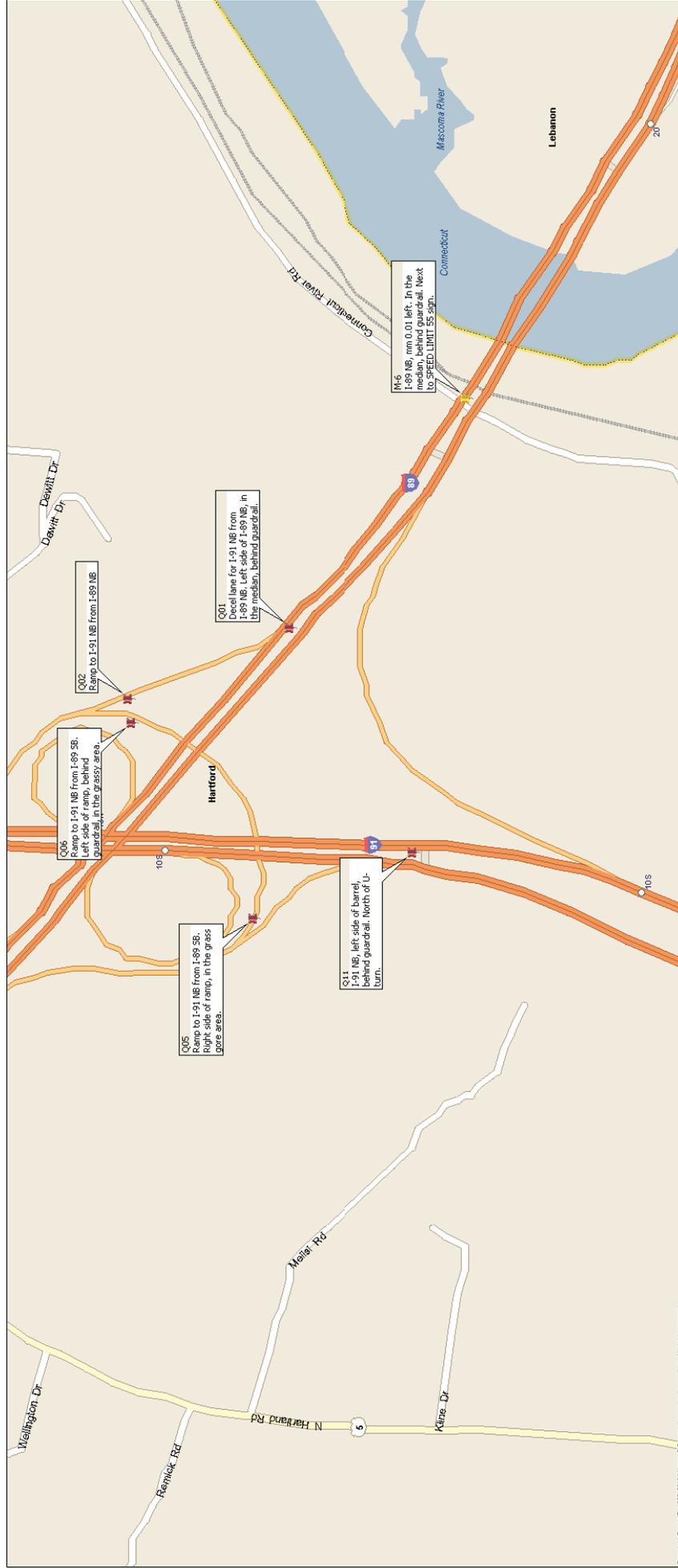
I-91 South Leg; South of WRJ



I-89 / I-91 Interchange (Northern section) & Interchange 11



I-89 / I-91 Interchange (southern section)



Copyright © 2011 (P) 1988-2011 Microsoft Corporation. All rights reserved.

Equipment Summary

Portable Changeable Message Signs (PCMS) = 12 each

Portable Queue Trailers (PQT) = 11 each

Portable Pan-Tilt-Zoom Camera (PTZ) = 2 each



**Hartford, Vermont IM-O91-1(65)
Smart Work Zone (SWZ)**

Contact Information:

PCL Construction:

Project Manager: Jeremy Mackling 813-810-1142 (cell)

Worksafe T.C.I., Inc.

Scott Deschamps	800-547-0808 or 802-288-6051 (cell)
Debra Ricker	800-547-0808 or 802-839-0896
Zebulon Chandler	800-547-0808
Mike Perry	603-224-0880

ASTI Technicians:

Peter Krikelis	302-328-3220
Les Spade	302-420-5724 (cell)
Don Henry	302-420-5721 (cell)

VTRANS Contacts:

State Resident Engineer:	Chris Barker	802-279-8161 (cell)
ConnectVT ITS Administrator:	Robert T. White	802-522-9867
Traffic Operations Engineer:	Amy L. Gamble	802-477-3251
VTrans Project Manager:	Mark Gerrish	802-461-5570
Transportation Operations Ctr.:	Larry Dodge	802-793-2251
	Gregory Fox	



Project Experience – Temporary Smart Work Zones

New Hampshire Projects:

- **Salem-Manchester A000(123), 13933-C**

Exit 1, I-93 widening project. September 2007 – March 2010

Contractor: SPS New England

Project Engineer: Robert Naftoly 978-462-6543

Project Supervisor: Henry Mulvey 978-375-9778

NHDOT Contract Administrator: Mark Caesar 603-818-9892

mcaesar@dot.state.nh.us

NHDOT ITS Manager: Denise Markow 603-227-0016

dmarkow@dot.state.nh.us

- **Manchester-Bedford 14607**

I-293 & I-93 resurfacing project. April 2008 – November 2008

Contractor: Brox Industries

Project Manager: Norman Saucier 978-454-9105

Project Supervisor: Mike Sheehan 978-815-2970

NHDOT Contract Administrator: Steve Quirion squirion@dot.state.nh.us

NHDOT ITS Manager: Denise Markow 603-227-0016

dmarkow@dot.state.nh.us

- **Rochester 10620-G**

Exit 12, Spaulding Turnpike widening project. April 2008 – September 2009

Contractor: S.U.R. Construction, Inc.

Project Supervisor: Andy Lepage 603-817-8585

NHDOT Contract Administrator: Jim Hersey jhersey@dot.state.nh.us

NHDOT ITS Manager: Denise Markow 603-227-0016

dmarkow@dot.state.nh.us

- **Salem-Manchester 14633-E**

Exit 5, I-93 widening project. July 2008 – June 2009

Contractor: Severino Trucking Co., Inc.

Project Supervisor: Bernie Lee 603-234-8516

NHDOT Contract Administrator: Matt Lampron mlampron@dot.state.nh.us

NHDOT ITS Manager: Denise Markow 603-227-0016

dmarkow@dot.state.nh.us

- **Merrimack 12105**

F.E. Everett Turnpike, Bridge widening project. October 2008 – December 2010
Contractor: R.S. Audley, Inc.

Project Supervisor:	Boyd Watkins	603-419-0005
NHDOT Contract Administrator:	Steve Lemire	slemire@dot.state.nh.us
NHDOT ITS Manager:	Denise Markow	603-227-0016 dmarkow@dot.state.nh.us

- **Salem-Manchester 13933-G**

Exit 3, I-93 widening project. June 2009 – present
Contractor: George Cairns & Sons, Inc.

Project Supervisor:	Garry Cairns	603-421-1888
NHDOT Contract Administrator:	Conrad Skov	cskov@dot.state.nh.us
NHDOT ITS Manager:	Denise Markow	603-227-0016 dmarkow@dot.state.nh.us

- **Rochester 10620-I**

Spaulding Turnpike widening project. September 2009 – present
Contractor: Severino Trucking Co., Inc.

Project Supervisor:	Bernie Lee	603-234-8516
NHDOT Contract Administrator:	Gene Sawyer	603-948-2093 gsawyer@dot.state.nh.us
NHDOT ITS Manager:	Denise Markow	603-227-0016 dmarkow@dot.state.nh.us

- **Salem-Manchester I-93 Corridor**

I-93 corridor widening project. March 2010 – present
Contractor: George Cairns & Sons, Inc.

Project Supervisor:	Garry Cairns	603-421-1888
NHDOT Contract Administrator:	Conrad Skov	cskov@dot.state.nh.us
NHDOT ITS Manager:	Denise Markow	603-227-0016 dmarkow@dot.state.nh.us

- **Lebanon 11700A**

Exit 20, I-89 Interchange widening project. April 2010 – present
Contractor: R.S. Audley, Inc.

Project Supervisor:	Dan Bocash	603-419-0007
NHDOT Contract Administrator:	Peter Kehoe	603-419-0047 pkehoe@dot.state.nh.us
NHDOT ITS Manager:	Denise Markow	603-227-0016 dmarkow@dot.state.nh.us

- **Bow-Concord 13742B**

I-93 Bridges over I-89. August 2011 – present

Contractor: R.S. Audley, Inc.

Project Supervisor:	Ben Zogopoulous	603-419-0011
NHDOT Contract Administrator:	Chuck Flanders	603-234-0597 cflanders@dot.state.nh.us
NHDOT ITS Manager:	Denise Markow	603-227-0016 dmarkow@dot.state.nh.us

Vermont Projects:

- **Richmond-So. Burlington IM-089-2(39)**

I-89 Structure repair/resurfacing project. May 2008 – July 2008

Contractor: Pike Industries, Inc.

Project Manager:	Bill Laporte	802-223-3002
Project Supervisor:	Mike Cronin	802-839-6407
VTRANS Resident Engineer:	Bob Sukert	802-279-0217 bob.sukert@state.vt.us
VTRANS Director of ConnectVermont:	Robert White	802-828-2781 robertt.white@state.vt.us

- **State of Vermont – VTRANS**

Contract to provide maintenance services and remote control access for Variable Message Signs statewide. February 2011 – February 2013

VTRANS Director of ConnectVermont:	Robert White	802-828-2781 robertt.white@state.vt.us
---------------------------------------	--------------	--

Massachusetts Projects:

- **Sagamore Bridge Project**

U.S. Route 6, Bridge deck repairs/resurfacing project. March 2010 – May 2010

Contractor: R. Zoppo Corporation

Project Manager:	Bill Clifford	781-344-8822
Project Supervisor:	Frank Monahan	617-839-9117
MassDOT Traffic Engineer:	Neil Boudreau	617-973-8211 neil.boudreau@state.ma.us

- **Medford I-93 Superstructure Project**

Medford I-93 Superstructure Replacement and Related Work (Project #606255)
Real Time Traffic Management System (RTTM) project. March 2011 – Sept. 2011

Contractor: J.F. White Contracting/Kiewit Corporation Venture

Project Manager: Peter Rapp 508-879-4700

Project Supervisor: Sean Whalen 845-240-8238

MassDOT Traffic Engineer: Neil Boudreau 617-973-8211

neil.boudreau@state.ma.us

H.O.C. Manager: Eric Podolski 617-310-4700

eric.podolski@state.ma.us

VER-MAC INC.



PCMS-1210

PORTABLE MESSAGE BOARDS

Our character matrix three-line full size controller message signs are one hundred percent NTCIP-compliant and can be easily controlled by any NTCIP-compliant traffic management software. Our robust design, plug and play components, and energy efficient technology provide a sign that requires minimal maintenance and has a low cost to own.

TECHNICAL BRIEFS DESIGN SPECIFICATIONS OVERALL DIMENSIONS

Overall length: 4470 mm (176")
Overall width: 2184 mm (86")
Display panel: 1804 mm x 3387 mm (71"x 133")
Traveling height: 2946 mm (116")
Operating height: 4572 mm (180")
Weight: 1085 kg (2390 lb.)

TEMPERATURE RANGE

Operational: -40° to + 74°C (-40° to +165° F)
Storage: -40° to + 85°C (-40° to +185° F)

ELECTRICAL INTERFERENCE

The PCMS 1210 is not affected by any normal (standard) type of RF interference

RELATIVE HUMIDITY RANGE

Operating 10% to 95% RH, non-condensing

TRAILER MATERIAL

51 mm x 102 mm x 3.175 mm steel tubing (2" X 4" X 1/8")
Diamond plate catwalk mounted on display side of trailer to simplify maintenance.

CABINETS

Aluminum sign and control cabinets
Locked with padlocks
Plastic battery boxes
Weather stripping seals each compartment against moisture

AXLE

Single 1588 kg (3500 lb.) axle

HITCH

Heavy-duty hitch capacity with 72 mm (3") pintle eye
Optional: 51 mm (2") ball coupler

- 1361 kg (3000-lb) maximum tongue load
- Heavy-duty safety chains with safety hooks meeting safety standards

TIRES & WHEELS

Tires: Load Range D 381 mm (15")
Wheel Size: 381 mm (15")
6-stud tire rims
Optional: Anti-theft locking mechanism
LEVELING JACKS

Four-screw jacks each rated at 907 kg (2000 lbs)
Optional: Tongue wheel jack
TRAILER LIGHTS

State-of-the-art halogen lighting as per USDOT standards and specifications

Custom-made connections complying with customer specifications
LIFT MECHANISM

Electro-hydraulic lift
SOLAR PANELS

Various configurations of solar panels and batteries available
High efficiency single-crystal silicon cells anti-reflective coated for improved efficiency
BATTERIES

6-volt 220 amp/hour deep-cycle batteries wired to provide a 12-volt system
Optional: Various batteries and configurations available
CONTROLLER
MENU DISPLAY (LCD)

Current usage and battery voltage
Solar array current output (to the battery) and voltage
Sign status (error detection)
Current message display
CONTROLS

Main power switch
Raise / lower switch
Can switch from laptop to cellular
(local communication RS- communication 232)
LCD Display
Keyboard
Charger switch
DISPLAY DIMENSIONS

The total display area is 1753 mm high x 3327 mm wide (69" x 131")

SPEED OF MESSAGE CHANGE

All three lines can be changed completely in less than 100 milliseconds with no visual disturbance.
LEGIBILITY

Messages displayed are easily readable from more than 305 meters
(1000 feet)
DISPLAY

590nm (\pm 2nm) amber-colored LEDs with a viewing angle of 30 degrees (standard)
LEDs have a rated life of 100,000 hours
Each amber-colored LED encased in an enhanced optical lens to maximize legibility from any distance (creating bolder characters)
4 LEDs per pixel in enhanced optical lens
Each pixel shaded by a removable black plastic visor to minimize washout in direct sunlight
3 lines of up to 8 characters per line
A character is based on a 5 x 7 pixel of 457 mm (18")
LED output adjusts automatically to ambient light conditions
100 brightness levels (1%-100% in increments of 1%)
The display is enclosed in an aluminum cabinet and protected by a polycarbonate face with UV protection
KEYBOARD

Graphic touchscreen LCD Controller
SOFTWARE

Changeable messages (default 255) (*1-999)
Permanent messages (default 258) (*1-999)
Volatile messages (default 64) (*1-999)
Permanent Font sizes (15)
Custom Changeable Font sizes (*5)
Auto font
Per character font sizing

Per character & line flashing
Admin & User level password
Auto brightness (photocell)
Manual 0%-100% brightness levels (increments of 1%)
Scheduling
Scrolling
Special dynamic data features trigger messages, display motorist speed, actual temperature, time & date & live countdown.
Supports NTCIP 1203 v2
Backward compatibility with NTCIP 1203 v1
Supports all new NTCIP 1203 v2 MULTI tags including optimization and combination <http://www.ntcip.org/>
Protocol translation engine allows live conversion from legacy protocol to NTCIP
Firmware acts as a virtual hub, allowing concurrent per interface protocol
Local communication settings
Drop address and communication speed (PMPP)
IP address, mask, gateway and port number for SNMP/UDP/IP transport setup

***Requires Factory Settings**

PASSWORD PROTECTION

Admin & User level password

PAINT

State-of-the-art powder coating system

- « Highway safety orange » is the standard color used

Optional: Other colors available to comply with different regulations or match client fleet standard

- Powder coating quality
 - o Certified UV protection paint
 - o Impact resistant
 - o Humidity resistant
 - o Salt spray resistant

MAINTENANCE

Battery fluids should be checked and topped off at least once a month

- Solar panels must be free of dust and snow

WARRANTY

1-year warranty on complete trailer
2-year warranty on electronics
6-month manufacturer's warranty on batteries
Limited warranty on solar panels varies from one manufacturer to another

TECH SUPPORT

24/7 technical support



VER-MAC

TMG Touchscreen Controller for VMS

Guide to Use

VER-MAC INC.
1781 Bresse
STE-FOY (QUÉBEC)
G2G 2V2
Canada
1-888-488-SIGN

Introduction3
 Using a touchscreen.....3
User Profiles for the TMG3
Menu Structure and Operating Instructions5
 Getting started.....5
 Authentication and Login6
HOME:7
 QuickPick:7
ACTIVATE MESSAGE8
 Task scenario 1: *Selecting and displaying a message from either Library or Collection*.....8
 Task scenario 1:1 *Removing a message from Collection*9
BLANK SIGN9
MESSAGE EDITOR.....10
 Task scenario 1: *Creating a new message*12
 Task scenario 1:1: *Inserting a page with a graphic image into a message*12
 Task scenario 2: *Editing (modifying) a message*13
 Task scenario 2:1 *Displaying a Radar speed reading in a message*14
OPTIONS14
PARAMETERS16

Introduction

Ver-Mac's TMG Touchscreen Controller for Signs is a compact microcomputer with a 7inch LCD touchscreen. It has been designed to allow easy setting of messages for display and for accessing in-built diagnostics and maintenance aids on Variable Message Signboard (VMS) units.

The TMG comes with a library of over 100 pre-defined messages and more than 30 graphic images. There is also on the Home screen a QuickPick collection of images.

The TMG has *multiple language capabilities*. The soft keyboard and fonts can be easily and rapidly adapted to input text (complete with accents) for VMS messages in different languages. These include Arabic and Hindi. However at the moment the interface is available only in English.

Using a touchscreen

You activate the functions of the TMG Touchscreen Controller by either touching the icons on the screen with your fingertip or a soft stylus-like instrument (e.g. the eraser tip of a lead pencil). *Never* use sharp pointed plastic, and *most definitely not* a metal object.

Smudges and fingerprints can be removed with a fully coated lens cleaner and a soft cloth.

User Profiles for the TMG

There are three User profiles.

1. Viewer – allows a User to quickly check that all is well with the VMS unit
2. Guest - allows a User to blank the sign, quickly select and display a message from:
 - a) the QuickPick image bank
 - b) the Library (bank of permanent messages) *or*
 - c) the Collection (messages previously created for the particular VMS unit)

Guests also can:

- a) access Maintenance and run tests on the different hardware components of the panel, whenever necessary
 - b) personalize (change) their Password
3. Admin. - has *full* set of rights and privileges



: Before starting to use the TMG, you should consult the table (below) get to know the User Rights and Privileges that match your User profile

USER RIGHTS AND PRIVILEGES - TMG Touchscreen controller			
	Viewer	Guest	Administrator
Log in/out			
Password	None		
HOME			
HOME	<i>Limited Rights</i>	<i>Full Rights</i>	
Overview	Read Only		
QuickPick			
OPERATIONS			
Activate Message	<i>No Rights</i>	<i>Limited Rights</i>	<i>Full Rights</i>
Library – View Access Sort Select	Not displayed	 	
Collection – View Access Sort Select		 	
Delete Message			
Blank Sign			
Blank Sign	Not displayed		
Message Editor			
Message Editor	Not displayed	Not displayed	
<i>Full</i> Message creation/modification rights			
Options			
Options	Not displayed		
Brightness: Auto/Manual Mode - select/set			
Maintenance: run test & check			
Pixel Test: run test & check			
Devices : check list of Active Devices			
Parameters			
Parameters	Not displayed	One icon only	
Change Guest Password: access & set			
Change Admin Password: access & set			
Clock: access & set			
Network Communications: access & set			
Special Code: access & set			
Diagnostic: Ver-Mac Support reference			

Menu Structure and Operating Instructions

The table below shows the different Operations available on the TMG Touchscreen Controller:

OPERATIONS BUTTONS		
Icon	Name	Available Options
	HOME	displays: 1) Log out icon and Battery indicator; 2) Operations buttons; 3) Message Preview; 4) Operating state; 5) QuickPick; 6) Status bar
	ACTIVATE MESSAGE	gives access to: Message Sources: a) Library; b) Collection enables User to: i) Sort; ii) Select; iii) Activate; iv) Delete Message
	BLANK THE SIGN	removes the message currently displayed on the signboard
	MESSAGE EDITOR	gives access to: a) all Message Creation/Modification tools; b) Page Template; c) flexible Keyboard layout
	OPTIONS	gives access to: a) Brightness; b) Maintenance; c) Pixel Test; d) Device enables User to: i) check, ii) make adjustments to and/or iii) run tests on unit hardware
	PARAMETERS	gives access to <i>settings for the VMS unit</i> : a) Change Password for Guest/Admin; b) Clock; c) Network; d) Diagnostic; e) Special Code

When you access the Home screen, the Operations buttons that display (or not) correspond to the privileges allocated to your User profile.

Getting started

- ❖ Make sure that the TMG Touchscreen Controller is connected to the VMS unit and switch the power **ON**.

When the main power switch is turned on, the system goes through a power-up and initialization procedure. This *takes approximately 2 minutes*, during which time the splash screen «**Ver-Mac**» displays. It is followed by the message, «**Loading...** ».

- ❖ When **Security** displays, the start-up sequence is complete and the TMG is ready for use

If there has been no touchscreen activity for approximately 5 minutes, the TMG shuts down to conserve power and restore Password security.

- ❖ To re-establish your connection, you touch anywhere on the screen and then you have to log in once again.

Authentication and Login

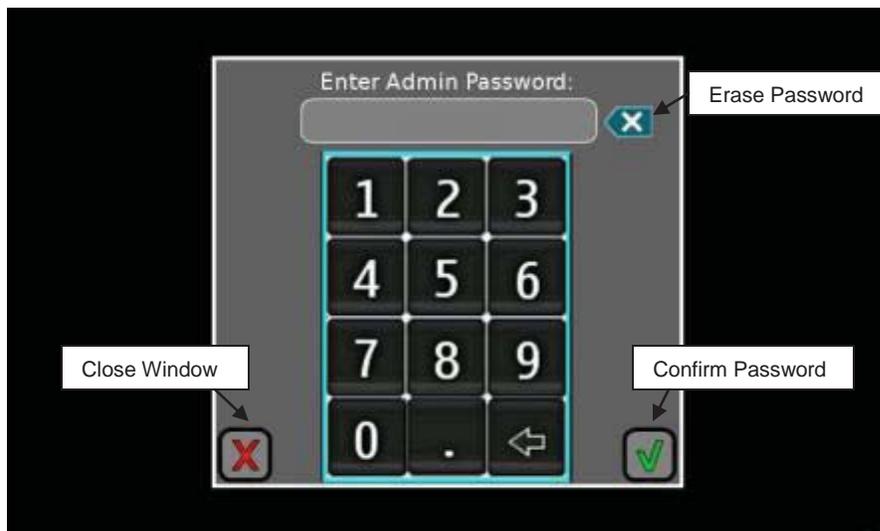
There are three levels of access corresponding to three User profiles within the TMG:

- a. **Viewer** - verification procedures only
- b. **Guest** – limited device operating functions (**password-protected*)
- c. **Administrator** – full access to device functions (**password-protected*)



Note: Passwords for the TMG must be numbers.

1. In the Security window (above) you first select your User profile (touch the appropriate icon)



2. In the next screen (above) touch and enter the numbers of your Password
3. When you have finished, touch , the Green checkbox, to confirm

If you have entered the wrong Password, the Error message « Invalid password» displays and you return to **Security**, where you can start again.

After the first login, users can change and personalize their password (see **Change Password**)

- ❖ To log out, touch , the Log out icon, located top right in all Operations screens

HOME



This is the screen that displays when you have successfully completed Login.

From this screen you can *view* the current state of the VMS and, depending to your User profile, select the area of Operations that you need.

Note: All Users access this screen following Login, but the display of Operations buttons varies.

QuickPick:

This feature contains the indications that are used most frequently on all signboards, no matter what their size.

- ❖ To select and display you *touch once* on the required indication
- ❖ Screen briefly shows message «Wait...»
- ❖ Your selection shows on Preview *and* displays on the VMS

ACTIVATE MESSAGE



For pre-existing messages stored in the Library or the Collection, and for images in the Graphic image bank:

To select, touch it once
Then, *to display, touch it once again*

Menu options in Select Message screen

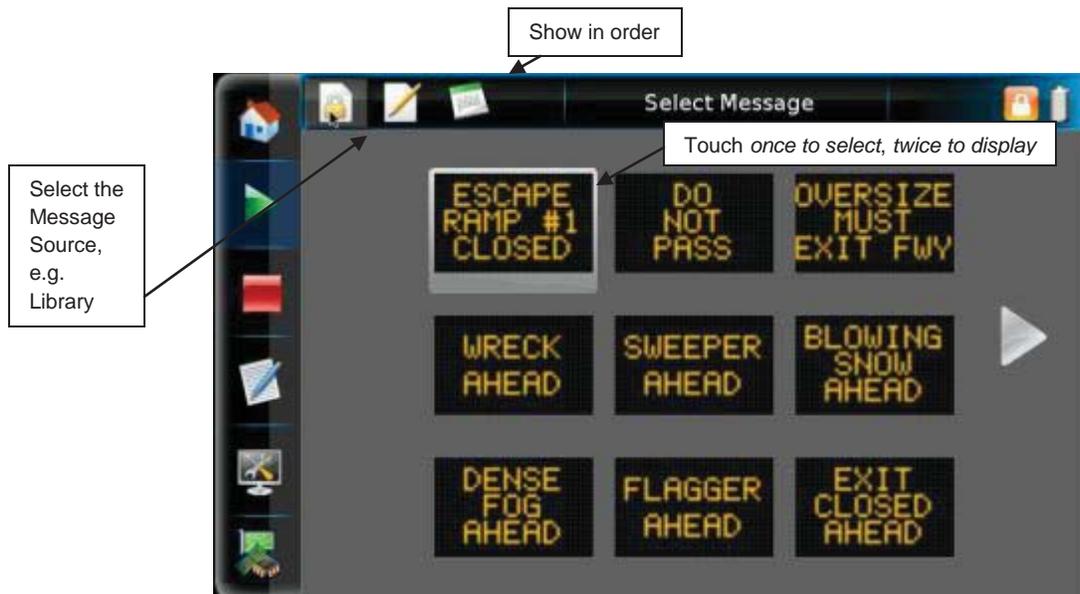


From left to right: (a) Message Source (Open Library or Open Collection); (b) Sort: Alphabetical Order or Order of creation (most recent to oldest); (c) Delete Message

Note: The menu option Sort applies to the Collection only. Messages in the Library are in Alphabetical order.
The menu option Delete Message is available only to Admin. Users

Task scenario 1: *Selecting and displaying a message from either the Library or the Collection*

1. From Operations buttons, touch , the Activate Message icon.
Message «Loading...» appears briefly and then the Select Message screen (below) displays



2. To select the message source, touch , the Open Library *or* , the Open Collection icon
Using the Forward/Back buttons, you can browse the messages
3. ***Touch a message once to select and view it***
Then ***touch it once more to display it automatically*** on the VMS
Message «Please wait...» appears briefly, then you are returned to Home screen
4. Your selected message is now displayed on the Preview for you to check before closing your session (touch ) *or* moving to other Operations (touch the appropriate button)

Note: You *cannot close* your session *if any window is open* on the screen.

Task scenario 1:1 *Removing a message from the Collection*

Reminder: This Operation is available to Admin users only

- ❖ First touch to select the message you want to delete
- ❖ Then touch , the Delete Message icon, and message is removed
You return again to the Collection where you can select and delete other messages

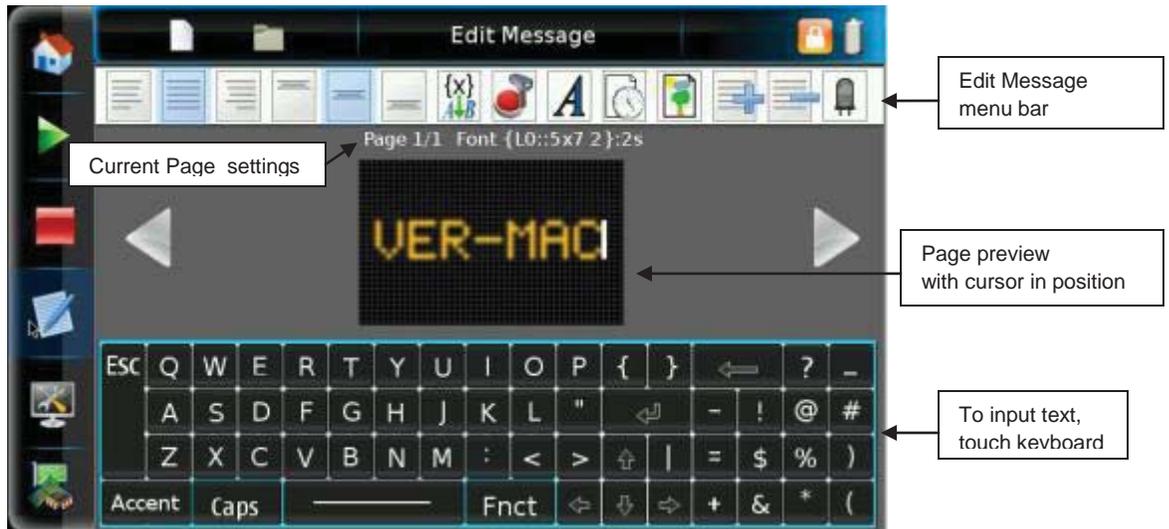
Note: This operation only removes the message from the Collection: it does not remove the message from the sign itself if it is the current message being displayed

BLANK SIGN

- ❖ From Home screen, touch , the Blank Screen icon
This removes the message currently displayed on the VMS
- ❖ The Preview also goes dark, indicating that the sign is now blank (no illumination)

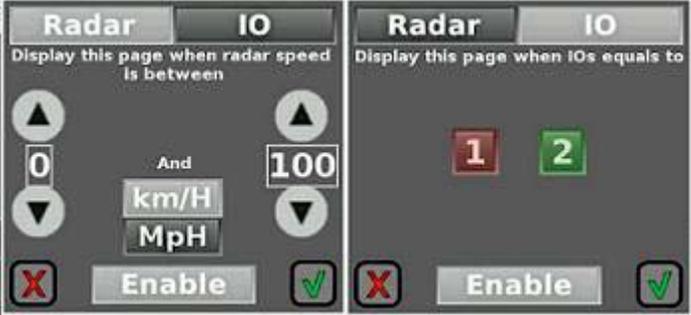
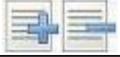
MESSAGE EDITOR

When you need to create a message touch , the Message Editor icon and screen (below) displays:



Toolbar:  

1. **New Message:** Display blank Preview screen with cursor
2. **Open Message:** Display all previously created and changeable messages for the VMS

EDIT MESSAGE menu bar		
Functions	Icons	Outcome
Text Alignment:	 <p>(a) (b) (c)</p>	<p>a) Align text along the Left margin of page b) Center text – margins both sides of page are equal c) Align text along the Right margin</p> <p> To adjust, touch the line(s)</p>
Page Layout:	 <p>(a) (b) (c)</p>	<p>a) Align page to Top b) Center (positioned mid-page) c) Align page to Bottom</p>
Insert Dynamic Data		<p> UNDER DEVELOPMENT</p>
Message triggered by: Radar and/or Input-Output Device		 <ol style="list-style-type: none"> Select device(s), Radar or IO [Note: If device is OFF, touch Enable] Set Message page display conditions – <ul style="list-style-type: none"> Radar: touch boxed numbers, enter the speeds with keypad and touch check  to confirm Input/Output device : touch activated (green) or not (red) and touch check  to confirm <p>[Note: For IOs: you must also set the message to display under normal conditions (no activated IOs). It can be a blank VMS.]</p>
Fonts		 <ol style="list-style-type: none"> Select Font (Forward/Back buttons) Set Character and Line Spacing and touch check  <p> Fonts #21 & #22 are for Arabic; Font #24 for Hindi. Keyboard changes when these fonts are selected and set.</p>
Timing - Page Display		<p>Using numeric touchpad enter the Page time ON (1 – 25 sec). Touch  when finished</p>
Graphics		<p>From the Image bank, select and insert an image as a page in a message</p>
Message structure		<p>Add Page to / Remove Page from message you are creating/modifying</p>
Line Blink time (0.5sec)		<ol style="list-style-type: none"> To have one line of the message flash, touch the line and then Blink icon. To have the message flash, repeat procedure for each line in turn

Task scenario 1: *Creating a new message*

1. Access Edit Message screen (see above) and using the keyboard, input the text of your 1st page

 Preview already shows a message?
To clear it, touch , the New Message icon on the toolbar

2. Adjust the page features (touch icons on Edit Message menu bar and follow the instructions)

If necessary add another page, (touch  icon) and repeat the process

3. When your new message is finished, touch . Message «Loading ... » appears briefly. By default this selects and lists your new message as #1 in the Collection of messages for the VMS

 You should now check that your new message is the way you want it.
If not, return to Edit Message (touch ) to make the changes. Then repeat Step 3 above and continue the process

4. To display your newly created message on the VMS, *touch it once*
Message «Please wait...» appears briefly, then you are returned to Home screen

Task scenario 1:1: *Inserting a page with a graphic image into a message*

Note: Graphics require a whole page for each image. The graphic image page can be a message in its own right or can be a page in a multi-page message.

1. In Edit Message screen open a blank message page (as in *Creating a new message* (above))
2. Now, instead of using the keypad and writing text, you touch , the Insert Graphic icon on the menu bar and display the graphic image bank (below):



3. *Touch the image you want once to select it*
Then *touch* the selected image *again* to insert it on your page
4. You are returned to the Edit Message screen where you can create more pages for the message *or* as in Steps 3 and 4 above (touch , Activate Message etc.) proceed to display the message

Task scenario 2: *Editing (modifying) a message*

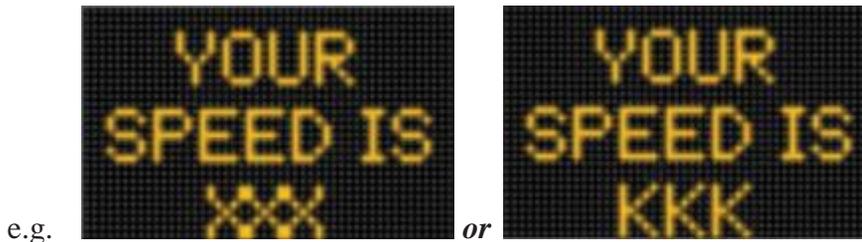
1. Access Edit Message screen and touch , Open Message
Message «Loading...» appears briefly and then the message Collection is displayed
2. Sort the collection (touch  *or* ) and *touch to select* the message you want
Then to return to Edit message screen, *touch once again* the selected message
3. According to what you want to do, touch the necessary function icon from the Edit Message menu bar
Follow the instructions and make the change(s)
4. The continue the process as outlined in Steps 3 & 4 above

Task scenario 2:1: *Displaying a Radar speed reading in a message*

Note: This is *not* the same as having a **page of message triggered by radar input**

The procedure for inserting the *actual* speed reading from a radar device into a message on a VMS is much the same as that outlined in **Scenario 1: *Creating a message*** (above).

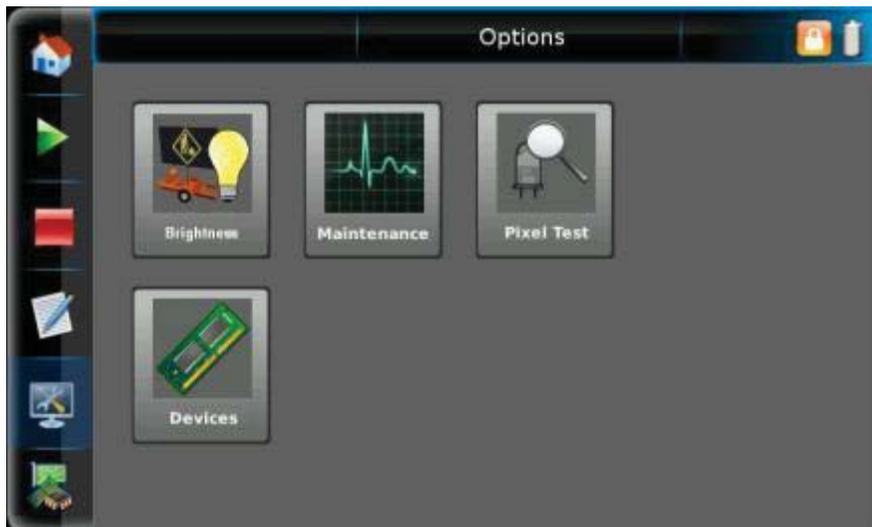
1. Using the keyboard, input any text you want on the page
2. Then, where you want the reading to appear, type either KKK for the reading in kilometers *or* XXX for miles,



3. Complete and display your message in the usual way (Steps 2 to 4 above)OPTIONS

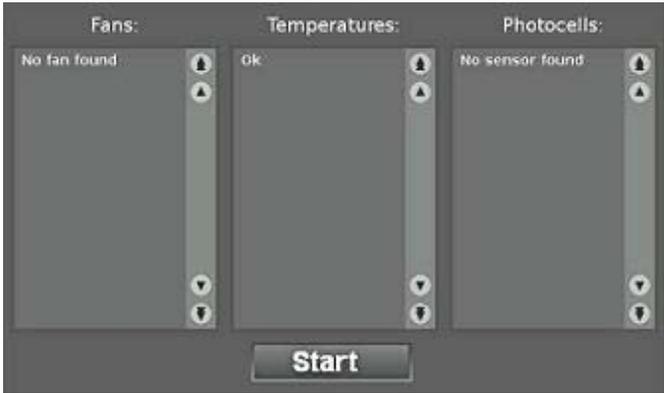
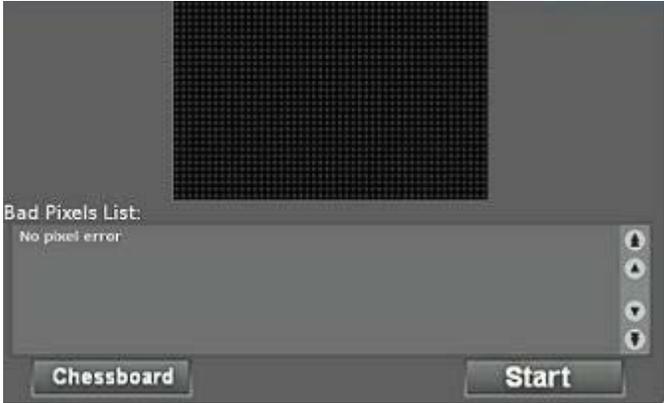
When you need to test or check the state of some or all of the hardware components of the VMS unit touch , the Maintenance icon.

This opens the screen (below) where you touch and select the icons for the Option(s) you want to access:



Note: This screen is accessible to *both* Guest and Admin users

OPTIONS

Icon	Window that opens	Procedure
		<p>Brightness:</p> <p>Select the mode (Automatic/Manual):</p> <ol style="list-style-type: none"> 1. Based on information from the photocells, Automatic adjusts brightness of the light emitted by the LEDs and displays the current reading. 2. User can adjust or set Brightness level by selecting Manual and using arrows
		<p>Maintenance:</p> <p>Runs a check on the three (3) hardware components of the VMS that may affect its performance:</p> <ol style="list-style-type: none"> 1. Fans that aerate the sign case 2. Sensors that detect Temperature <i>inside</i> the VMS case 3. Photocell sensors that detect the ambient light conditions (the light conditions <i>outside</i> the VMS panel)
		<p>Pixel Test:</p> <p>There are 2 types of test:</p> <ol style="list-style-type: none"> 1. Checks <i>all</i> pixels and locates (x/y coordinates) any that are faulty 2. To help you to <i>visually locate</i> a faulty pixel (stuck On/OFF), select Chessboard. This test focuses section by section.
		<p>Devices:</p> <p>This window lists all the peripheral devices that make up the VMS unit and are active.</p>

PARAMETERS

Parameters are certain settings and invisible aspects of the VMS which can affect the actual state of the panel and/or its operations.

To access this information and display the Parameters screen (below), touch the icon, 



PARAMETERS

Icons		Procedure
 <p>Change Guest Password</p>	<p>For both procedures (Change Guest Password and Change Admin Password), the window that opens is similar to password window that displays at Login.</p>	<p>A keypad and instructions are displayed. These vary according to your User status.</p>
 <p>Change Admin Password</p>	<p>Note: Guest users can change their own password. This is the only Parameter operation available to them: none of the other Parameters icons are displayed.</p>	<p>Messages confirm the new settings</p>
 <p>Clock</p>		<p>According to the geographic location of the VMS unit</p> <ol style="list-style-type: none"> 1. Touch to select the correct time zone for the location 2. Adjust <i>current Date and Time</i> (touch numbers in rectangles and input with keypad or use ▲▼ arrows)
 <p>Network</p>		<ol style="list-style-type: none"> 1. Touch Type to select (DHCP /static IP) 2. Touch EDIT , access keyboard to input changes  <ol style="list-style-type: none"> 3. Touch APPLY
 <p>Special Code</p>	<p>This function is reserved for adding additional features as instructed and guided by Ver-Mac Support</p>	<p>Input coded information using the keypad</p>
 <p>Diagnostic</p>	<p>With assistance from Ver-Mac support, this aids in debugging any problems that cannot be resolved otherwise.</p>	<p>Note: Under normal circumstances <i>users do not need to access this procedure</i></p>

QUEUE

SMARTER SOLUTIONS

SMARTER TECHNOLOGY

TRAILER MOUNTED QUEUE DETECTION

Industrial grade trailer to give years of dependable service

Provide data including speed, volume, and occupancy

Adjustable solar array for maximum exposure to sun

Optional digital cellular communications

Microwave detection reliably detects up to 10 lanes of traffic

Available as a portable unit or permanent mount

Removable tongue

Battery bank sized for 30-day autonomy



The Queue Trailer is a portable trailer that provides a versatile and lightweight platform with a small footprint to mount a microwave radar unit to detect speed, volume and occupancy for up to ten lanes of traffic. When equipped with ASTI's communication package the Queue Trailer can provide data remotely to a variety of information-gathering components.

ASTI TRANSPORTATION SYSTEMS

18 BLEVINS DRIVE NEW CASTLE, DE 19720 PHONE:302 328 3220

TRAILER MOUNTED QUEUE DETECTOR ASSEMBLY

DESCRIPTION – This work is the furnishing installation and maintenance of a traffic queue detector trailer having the capability of sensing slow or stopped traffic and relaying the real-time traffic conditions to the CHIPS System via radio communications, as indicated on the Traffic Control Plan and as directed. This work also includes performing a site survey to confirm the optimum radio communications.

SENSOR –

- (a) Microwave Queue Detector with the following specifications:

Operating Frequency:	10.525 GHz (X-band)
Detection Zones:	Up to 8 traffic lanes simultaneously
Detection Range:	100 m
Measured Quantities:	Speed, occupancy, volume, presence
Communications:	Wireless modem or RS-485 connection
Power:	6 watts @ 9-36 VDC
Weight:	5 lbs.
Physical Dimensions:	32 cm. H x 23 cm W x 7.6 cm D
Zone Resolution:	3 m
Time Resolution:	2.5mSec
Ambient Operating Temp:	-40C to +50C
Humidity:	Up to 95% RH
Shock:	10 g 10ms half sine wave
Elevation Angle:	15 to 45 degrees
Azimuth:	12 degrees
Transmitted Power at 3m:	<100dBuV/m @ 10.525Ghz

- (b) Trailer – Provide an all-encompassing trailer that is used to house and deploy the queue detector receiver, communications module, photovoltaic system and antenna with the following specifications:

Color	Highway safety orange
Dimensions	
Length	122”
Width	96”
Travel Height	72”
Operating Height	17’
Trailer Deck	1/8 Formed Steel

Mast	17-foot retractable mast for mounting antenna, solar panel, and sensor.
Pivot Support Arms	Cable Wench 14 Guage Steel, Hinged Telescoping Door Support, Battery Lock Down Assy., Battery Access Panel, Vented, Lockable 28" x 24" x 11 ¾ " (L x W x H)
Lifting Mechanism	
Battery Box	
Dimensions	
Stabilizers	Four 27-inch adjustable outriggers.
Mast	17-foot retractable mast for mounting antenna, solar panel, and sensor.
Axle	2,000 lb. Capacity
Leaf Springs	1,400 lb. Capacity
Roller Bearings	Yes
Hubs	Yes
Tires	7.35 x 14
Fenders	16 Guage Rolled Steel
Hitch	2" Ball
Safety Chains	¼ Inch with 2,500 lb. Slip Safety Hooks
Tongue	.250" thick x 2 ½" Square Tubing
Overall Length	60"
Removable	Yes
Trailer Lighting	Class A Trailer Lights with License bracket.
Reflectors	One on each side, two amber At front, two red at rear
Finish	The trailer shall have grease and wax removed prior to one coat of Trio Etching Primer and one coat of Acrylic Omaha Channel.

- (c) Communications - 220 Mhz Radio Communications Module FCC approved radio transmitter, capable of transmitting and receiving real time traffic queue information, with the following specifications

PHYSICAL CHARACTERISTICS:

Weight:	2 lb.
Size:	6.8 x 3.3 x 2
RF Antenna Connector	50 Ohm TNC
GPS Antenna Connector	SMA
Serial Interface	RS-232 DB-9F / 1200-230400 bps

ENVIRONMENTAL:

Operating Temperature Range	-30°C to +70°C (10% duty cycle limit above 60°C)
Humidity	5% - 95% Non-condensing

RF FEATURES:

- 224 mW RF output (+23.5 dBm)
- Full duplex transceiver
- Dual-band support for both 800 MHz cellular and 1.9 GHz PCS bands
- Adheres to CDMA authentication as specified in CDMA2000 1X

PACKET MODE FEATURES (1xRTT):

- Data rates up to 153.6 kbps (forward channel) and 76.8 kbps

POWER MANAGEMENT FEATURES:

Input Voltage	9 VDC to 28 VDC
Input Current	20 mA to 350 mA
Typical Transmit/Receive	300ma at 12VDC
Dormant connection idle for 10-20 seconds	60 ma at 12 VDC
Low power mode	20 mA at 12 VDC

- (d) Antenna – Fiber Glass Omni Directional antenna with a minimum 5 dB gain tuned to the Master Traffic Control Center radio frequency. Plated, rust resistant mounting hardware for mounting antenna to the queue detector trailer mast.

Frequency:

- Cellular 824-894 MHz
- Lowband SMR 806-870 MHz
- Highband SMR 870-960 MHz
- GPS 1575.42 +/- 2 MHz

GPS Gain	27 dB Amplifier, 5 dBi Antenna
VSWR	2:1 max over range
Noise Figure	2.0 dB max, 1.7 dB typical
Operating Temp	-30o to +80o C
Nominal Impedance	50 ohms
Maximum Power	10 Watts for 800/900 MHz
Amplifier Bias	Dual 3.3/5 VDC +/-10%
Current	20 mA max, 10 mA typical

- (e) Coaxial Cables and Data Cables – Cables and hardware as required to interconnect antenna, queue detector, and receiver radio communications module as indicated. Coaxial cable will be 20 feet in length, 50 ohm RG8 with PL259 connectors.
- (f) Power Supply – Solar assisted battery banks with the following specifications for operating the queue detector receiver and communications module.

The photovoltaic system will have the following minimum requirements.

Two 4D Marine type batteries with a total of 370-amp hour rating

Nominal Voltage	
Nominal capacity at 20 hours	Rated 185 amp hour
Minutes of discharge at 25 amps	176 minutes
Dimensions	11.97" x 6.6" x 9.35" (L x W x H)
Weight	63 lbs. Ea.
Terminals	Threaded Post with Wing Nut

Charge Controller	
Operating voltage	12 VDC
Maximum voltage	25 VDC
Minimum voltage	1.5 VDC
Input current	18 amps maximum
Battery voltage	0 VDC minimum
Charge stop voltage	14.35 VDC (+/- 1%)
Current consumption (+/- 5%)	
Charging	55 mA
Analyzing	9 mA
Idle	<1 mA
Operating temperature	-40 F to +150 F
Operating Humidity	Up to 100%
Dimensions	2" x 2" x 1.5" (L x W x H)

Weight 5 oz. (114.7 g)

Solar Panel

Dimensions 47.3" x 20.8" x 1.3"
(L x W x H)

Weight 16.7 lbs.

Electrical Parameters

Max power

Watts 100 W

Volts 16.5 V

Amperage 9.6 A

Cell Size 4.8 x 4.8

Number in sires 36

Termination Junction box

Material type

Substrate White ABS

Frame Aluminum channel

Mounting Bracket Side of pole

Portable Queue Trailer User Guide

1. Find a suitable site for trailer.

A suitable site is level with a setback of 20 feet from the first lane of traffic with no poles or signs to interfere with the radar beam. The area must also have no overhead safety concerns. The trailer needs to be in an area that can have visible sun on the solar panels for at least 7 hours without shadowing from trees or mast when fully extended.

2. Position the trailer so that is parallel to the traffic that is wished to be counted.



3. Use leveling jack stands to level the trailer for proper alignment of the SmartSensor HD



Leveling jack stands

4. Turn the winch clockwise to raise the mast and sensor to the full height of 25 feet.



Winch



midway extended



fully extended

5. Apply power to the actuator switch by turning the On/Off switch to ON in the grey enclosure. Adjust the SmartSensor HD angle with the actuator switch in the control compartment.



Angle actuator switch



Correct SmartSensor HD angle.

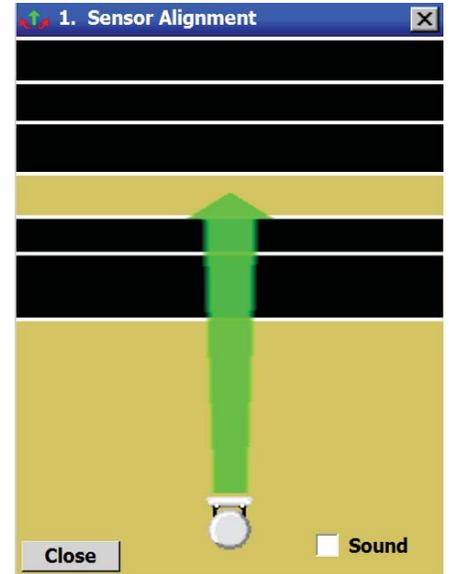
6. Use Laptop with SmartSensor Manager HD software, serial cable, and Click 200 to adjust SmartSensor for correct Sensor Alignment.



Laptop connected to Click 200

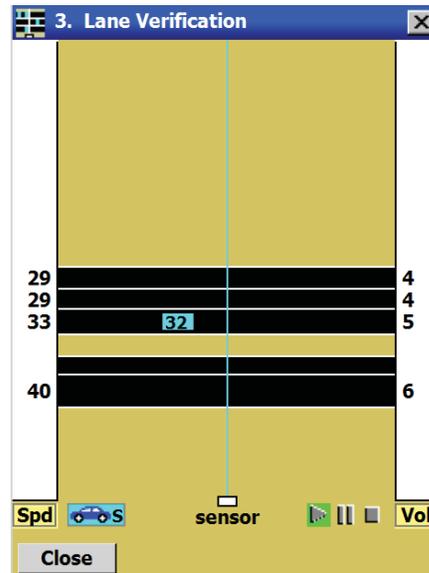
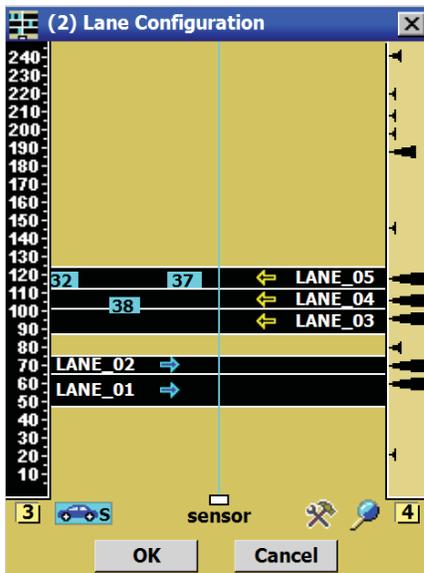


Click 200



Correctly aligned SmartSensor HD

7. Utilize SmartSensor Manager HD software to configure SmartSensor HD for all lanes and classifications required.



8. After all configuring of SmartSensor HD is done. Connect Click 200 to CDMA modem for remote connectivity if required.



Sierra Wireless PinPoint XT CDMA modem.

Click 200

Gray ribbon cable is connected to CDMA modem.

9. Close the grey enclosure and lock the 2 twist locks on the side. Close the battery and control compartment lid. Lock if required.



Twist locks

10. Rotate the solar panels to the south for optimal solar charging with no shadowing from the mast.



Solar alignment pin



Travel position



Rotated to face South

Preparing of portable Queue Trailer for stowage or travel.

I. Rotate solar panel to travel position with the least resistance or panel to the front.



II. Turn the winch counter clockwise to lower the mast and sensor to the lowest point of 9 and half feet.



III. Turn the On/Off switch to OFF in the grey enclosure. Raise three of the leveling jacks.



Points of interest.



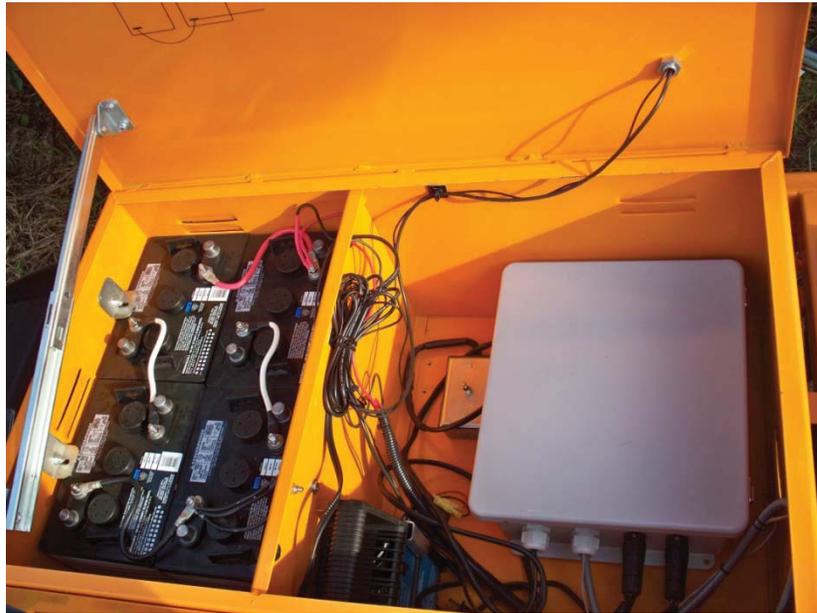
SmartSensor HD
Angle Actuator

Solar Panel
Mast Winch

Control
Compartment

Battery
Compartment

Control / Battery Compartment



Battery Compartment



4 6Vdc AGM batteries
In a series / parallel
connection for
12Vdc system voltage

Control Compartment



1 AC Battery charger
1 Angle Actuator switch
1 grey Control Enclosure

Control Enclosure



ProStar 30M Solar Charge Controller

PinPoint XT Verizon CDMA /GPS Modem

SmartSensor HD Sensor Cable

Click 200 Surge Protector

On/ Off Switch



Portable Queue Trailer

ASTI Transportation Systems, Inc.

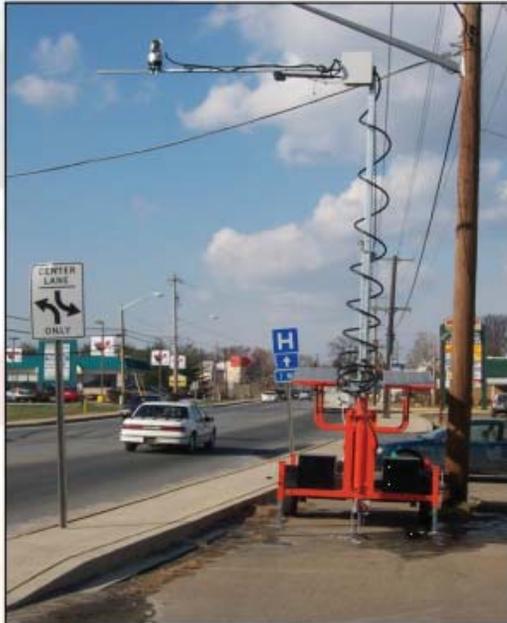
EZ CAM Portable Video Surveillance Trailer

The **EZ CAM** provides a portable, self-contained, all weather, trailer mounted equipment platform. Through the use of wireless communication the **EZ CAM** provides the end user a rapidly deployable real time video system viewable from a remote location.

The **EZ CAM** shall include an operational height of 32 feet above ground level, day/night camera with pan/tilt/zoom capability, adjustable solar array, battery backup providing year round autonomy, extendable outriggers with a footprint of 110 square feet.

The **EZ CAM** can be used as a stand alone camera system or tied into a larger existing CCTV system. The pan/tilt/zoom feature can be controlled via an IP address on your browser or an ASTI customized webpage providing individual icons selecting each camera for viewing.

This unit can be equipped with an "over the road" extendable mast arm.



LPR Trailer



EZ Cam



ASTI Transportation Systems, Inc. 18 Blevins Drive, New Castle, DE 19720
(302) 328-3220 www.asti-trans.com

Portable Video Surveillance Trailer **General Specifications**

A. INTENT STATEMENT

The purpose of these specifications is to describe a portable, self-contained, all weather, trailer mounted equipment platform. The function is to host and power a camera system on an aerial mast, for traffic management applications (ITS). The unit shall contain its own solar/battery power supply, capable of continuous operation, day and night, for extended periods of time. The unit shall be mounted on a two-wheel trailer capable of being towed at normal highway speeds as well as being operated in a stationary, stable position. The unit shall conform to all Federal and State requirements for vehicle lighting.

B. OPERATING CRITERIA

- The mast shall have an operational height of 32 ft. above ground level.
- The solar array(s) shall be adjustable from 0° - 60° and rotate 360°.
- The trailer shall have extendable outriggers with a footprint of 110 sq. feet.

C. EQUIPMENT COMPONENTS

1. TRAILER

- The trailer frame shall be constructed of structural steel tubing and channel. The unit shall be of sufficient strength and design to adequately support the weight of the entire unit.
- All frame members to be fully welded, any captive tubes shall have weep holes on the bottom side.
- The trailer shall be fabricated per attached drawings.
- The trailer deck shall be 40 sq. ft. All open deck space shall be covered with 1/8" steel diamond plate.
- The draw bar shall be triple member, "A" frame design per attached drawings.
- The draw bar shall extend 5ft from the front edge of the trailer frame and be equipped with (2) two 1/4" x 24" proof coil, plated safety chains with hooks.
- The trailer frame shall incorporate (4) four, laterally extendable outriggers. The outriggers shall be fabricated from 1 1/2" x 2 1/2" x 3/16" steel tubing. Each outrigger shall extend 32" from its stowed position. The outriggers shall be secured in their stowed and extended positions by 3/8" hitch pins with lanyards securely attached to the trailer frame.
- The trailer shall include (4) four, 3500 lb., drop leg, top wind screw jacks with 15" drop extension and 15" screw travel (REF. SHELBY Model #6101B). The jacks shall be

mounted: (4) four on outriggers. The outriggers shall be constructed of 1-1/2"x2-1/2"x3/16" steel tubing. They shall be galvanized and extend 30" out from the trailer frame. The draw bar shall have (1) 2000 lb, 13", top wind, swing away type screw jack (REF. HAMMERBLOW model #TWS 151 DS)

- The hitch shall be a 2" ball coupler, 5000 lb. rated, bolted to draw bar. (REF FULTON Model #22200).
- The axle shall be 2000 lb. rated and equipped with (2) two, double eye, 1200 lb. rated leaf springs. The hubs shall be roller bearing type with 5.45 bolt pattern. (REF. AXIS PRODUCTS Model #72/58).
- The wheels shall be 14" x 5" white spoke, with a 5.45 lug pattern.
- The tires shall be F78-14ST 205-75 load range "C".
- The trailer shall be equipped with (2) two combination stop/turn/marker light assemblies with a 4-pole, flat trailer lighting plug. (REF. OPTRONICS Model #ST-9RS).
- The rear of the trailer shall be marked with (4) four lineal feet of FHWA approved, conspicuity marking tape.
- The entire trailer shall be properly cleaned and prepped. It shall receive (1) one prime coat and (2) two topcoats of Federal Standard 595 Safety Orange, acrylic enamel with urethane additives.
- The fenders shall be black, high impact polyethylene. They shall have an integral full inner splash shield and flat stepping surfaces.

2. PEDESTAL BASE

- The pedestal mount shall be fabricated per attached drawings.
- The mast receiver tube shall attach to the vertical supports via (2) two, 1" pillow bearings (REF. PEER Model #HSP-205-16).
- The receiver tube shall pivot on the pillow bearings 90°. The pivot pin shall be 1" cold rolled steel and lock into the bearings by means of (2) two eccentric locking rings.
- The receiver tube shall tilt to its vertical position by means of a 1050 lb. winch with safety brake (REF. FULTON Model K1050). Optional power winch available.
- The winch shall raise the tube by means of a 3/16" galvanized wire rope, routed through a series of (2) two 2" x 1/2" pulley sheaves for compounding the lift.
- The tube shall lock in its vertical position by means of a 5/8", spring loaded, forged steel pin.
- The entire pedestal base shall be properly cleaned and prepped. The entire unit shall receive (1) one prime coat, and (2) two topcoats of Omaha Orange acrylic enamel with urethane additive.
- The pedestal assembly shall be attached to the trailer frame using (6) six 1/2" x 1 1/2" grade 5 bolts and locking nuts.

3. MAST

- The mast assembly shall consist of (3) three concentric sections of square steel tubing
- Each mast segment shall be raised by means of (3) three separate lengths of 3/16" galvanized wire rope with a 2" x 1/2" pulley sheave at the top of each tube.
- The (2) upper telescopic segments shall be shimmed in such a manner that the segments have free play while extending, and become "snug" within the outer tube when fully extended.
- The shims shall also serve as stops to retain each segment within the other.
- The shims shall be powder coated with a nylon polymer.
- All segments shall be galvanized.
- The top segment shall include a camera mounting platform. The platform shall be a 6"x6"x3/16" steel plate weld to a 1-1/2"x1-1/2"x4" piece of perforated steel tubing. The tube shall fit into the open end of the top segment and be attached w/ a 3/8" hitch pin.
- The lower two segment shall provide a means to attach NyCoil spiral conduit to each segment.
- The cabled segments shall extend in unison by means of a 1550 lb. winch with safety brake. Optional 1700 lb power winch available.
- The lower segment shall include a 1/2" – 13 x 1 1/2" stud on center of the bottom. This stud will extend through a hole in the bottom plate of the receiver tube to retain the assembly within the receiver by means of a washer and locking nut.
- A teflon disc shall be inserted between the bottom of the lower mast segment and the inside bottom of the receiver tube for smooth rotation.
- The mast assembly shall be capable of 360° rotation. The lower segment shall include a handlebar type rotation lever.
- The rotating mast assembly shall be locked into desired position within the pedestal base receiving tube by means of a heavy duty, "T" handle, locking clamp, stud size 5/8" minimum.
- The entire assembly and receiver tube shall be lowered to a horizontal position for transport. The retracted mast assembly will rest in a cradle and be retained by means of a 5/8", spring loaded, forged steel pin, extending through (1) one side bracket of the cradle, locking the mast beneath.
- The cradle shall incorporate a retaining pin to secure all mast segments from extending outward during transport. The pin shall be 1/2" diameter x 1 1/2" long round steel. The retracted mast assembly shall have 5/8" diameter, concentric, mating holes through the lower side of each segment. The 1/2" pin will extend upward through all mast segments while in the transport position.

4. POWER SUPPLY – SOLAR

- The (4) four solar generating modules shall be mounted on an apparatus which allows for independent positioning of each module per attached drawing.
- Each module shall be adjustable from 0° - 60° tilt and 360° rotation.

- The mounts (four) shall consist of a machined aluminum, 2” I.D. split pillow block socket joint and a steel 2” ball on the solar panel bracket.
- The module shall be secured in desired position by a ratcheting locking lever, clamping the pillow blocks together.
- The ball-in-socket assemblies shall be mounted atop (4) four formed tubular mounting posts.
- The solar module bracket and the tubular mounting post shall have a connecting rod to secure the solar modules for transport. This rod shall be tubular steel, zinc plated, attached with 3/8” hitch pins.
- The solar array shall consist of (4) four, 110 watt, photovoltaic modules (REF. SHELL model # SM110).
- A solar charging circuit shall protect the battery supply from over-charge and over-discharge conditions (ASTI supplied).

5. POWER SUPPLY – BATTERY

- The battery bank shall consist of (12) twelve, 6 VDC, deep cycle batteries. The batteries shall be wired in a series/parallel configuration to yield a 12 VDC output. (REF. TROJAN Model #T-605).
- The batteries shall be securely retained in their compartments by (6) six, powder coated, hold down brackets (2 per bracket). Use of the compartment lid as a hold down is not acceptable.
- The battery compartments will hold (6) six batteries each. The enclosures shall be black, corrosion proof, high impact polyethylene. The enclosures shall be weatherproof, ventilated and lockable.
- All battery wiring shall be color coded: Red – positive, Black – negative, White w/ trace – series jumper.
- All batteries shall be mounted below deck level for improved ballasting and impact protection.
- Battery charger.

6. STORAGE COMPARTMENTS: (2) 50 gallon, high impact plastic storage bins shall be mounted on each side of the trailer for equipment storage.

7. CAMERA – The PTZ network camera enables advanced remote monitoring with pan, tilt and zoom control over IP networks.

AXIS Q6032-E PTZ Dome Network Camera

Advanced, outdoor-ready PTZ dome for demanding surveillance.



- > 35x optical zoom and 220° tilt
- > Outdoor-ready and Arctic Temperature Control
- > D1 resolution, day/night and H.264
- > Auto-tracking
- > High Power over Ethernet (IEEE 802.3at)

AXIS Q6032-E PTZ Dome Network Camera is an outdoor-ready, high-performance PTZ dome designed for quick, easy and reliable installation in demanding surveillance applications. It is ideal for use at airports and seaports, as well as for city and perimeter surveillance.

The IP66- and NEMA 4X-rated AXIS Q6032-E provides cost-efficient installation since no external housing is required. With Axis' Arctic Temperature Control, the camera not only can function at -40 °C (-40 °F) but also power up at that temperature following a power failure.

AXIS Q6032-E has 35x optical and 12x digital zoom. It has a fast and precise pan/tilt response. The camera can also tilt 20° above the horizon for an extended tilt range of 220°, enabling better views, especially over uneven terrain. Intelligent video functionalities include auto-tracking, which enables the camera to automatically detect and follow a moving object within its field of view.

Day and night functionality, progressive scan, 128x wide dynamic range and D1 resolution (720x480 in 60 Hz, 720x576 in 50 Hz) contribute to the camera's superb video quality. The H.264 compression format ensures that image quality is not compromised while providing great savings in bandwidth and storage use.

AXIS Q6032-E is powered through High Power over Ethernet using the supplied High PoE midspan. Power over Ethernet simplifies installation since only one cable is needed for carrying power, as well as video and pan/tilt/zoom controls. With High PoE, the camera can operate even during a power failure as the network can be connected to an Uninterruptible Power Supply.



Note: Mounting brackets are sold separately

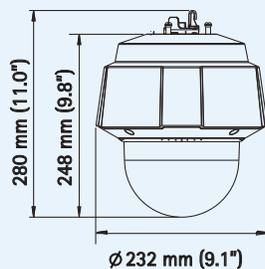
Technical specifications – AXIS Q6032-E PTZ Dome Network Camera

Camera	
Models	AXIS Q6032-E 60 Hz; AXIS Q6032-E 50 Hz
Image sensor	1/4" ExView HAD progressive scan CCD
Lens	f=3.4 – 119 mm, F1.4 – 4.2, autofocus, automatic day/night Horizontal angle of view: 55.8° – 1.7°
Minimum illumination	Color: 0.5 lux at 30 IRE F1.4 B/W: 0.008 lux at 30 IRE F1.4
Shutter time	1/30000 s to 0.5 s (60 Hz), 1/30000 s to 1.5 s (50 Hz)
Pan/tilt/zoom	E-flip, 100 preset positions Pan: 360° endless, 0.05° – 450°/s Tilt: 220°, 0.05° – 450°/s 35x optical zoom and 12x digital zoom, total 420x zoom
Pan/tilt/zoom functionalities	Guard tour Control queue On-screen directional indicator
Video	
Video compression	H.264 (MPEG-4 Part 10/AVC) Motion JPEG
Resolutions	D1 720x480 to 176x120 (60 Hz) D1 720x576 to 176x144 (50 Hz)
Frame rate H.264	H.264: Up to 30/25 fps (60/50 Hz) in all resolutions Motion JPEG: Up to 30/25 fps (60/50 Hz) in all resolutions
Video streaming	Multiple, individually configurable streams in H.264 and Motion JPEG Controllable frame rate and bandwidth VBR/CBR H.264
Image settings	Wide dynamic range (WDR), electronic image stabilization (EIS), manual shutter time, compression, color, brightness, sharpness, white balance, exposure control, exposure zones, backlight compensation, fine tuning of behavior at low light, rotation, aspect ratio correction, text and image overlay, privacy mask, image freeze on PTZ
Network	
Security	Password protection, IP address filtering, HTTPS encryption*, IEEE 802.1X network access control*, digest authentication, user access log
Supported protocols	IPv4/v6, HTTP, HTTPS*, SSL/TLS*, QoS Layer 3 DiffServ, FTP, SMTP, Bonjour, UPnP, SNMPv1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS
System integration	
Application Programming Interface	Open API for software integration, including VAPIX® from Axis Communications available at www.axis.com
Intelligent video	Video motion detection, auto-tracking
Alarm triggers	Intelligent video, PTZ position
Alarm events	File upload via FTP, HTTP and email Notification via email, HTTP and TCP PTZ position, local storage
Video buffer	56 MB pre- and post-alarm
General	
Casing	IP66- and NEMA 4X-rated metal casing (aluminum), acrylic (PMMA) clear dome, sunshield (PC/ASA)
Processors and memory	ARTPEC-3, 128 MB RAM, 128 MB Flash
Power	High Power over Ethernet (High PoE) IEEE 802.3at, max. 60 W AXIS T8124 High PoE Midspan 1-port: 100-240 V AC, max. 74 W
Connectors	RJ-45 for 10BASE-T/100BASE-TX PoE IP66-rated RJ-45 connector kit included
Local storage	SD/SDHC memory card slot (card is not included)
Operating conditions	-40 °C to 50 °C (-40 °F to 122 °F) Arctic Temperature Control enables camera start-up at temperatures as low as -40 °C (-40 °F)
Approvals	EN 55022 Class B, EN 61000-3-2, EN 61000-3-3, EN 61000-6-1, EN 61000-6-2, EN 55024, FCC Part 15 Subpart B Class B, ICES-003 Class B, VCCI Class B, C-tick AS/NZS CISPR 22, KCC Class B, EN 60950-1 IEC 60529 IP66, NEMA 250 Type 4X IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-78, IEC 60068-2-14, IEC 60068-2-30, IEC 60068-2-6, IEC 60068-2-27, IEC 60068-2-60, ISO 4892-2 Midspan: EN 60950-1, GS, UL, cUL, CE, FCC, VCCI, CB, KCC, UL-AR
Weight	3.5 kg (7.7 lb.)
Included accessories	AXIS T8124 High PoE Midspan 1-port, IP66-rated RJ-45 connector kit, clear dome cover, sunshield, Installation Guide, CD with User's Manual, recording software, installation and management tools, Windows decoder 1-user license

*This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (www.openssl.org)

More information is available at www.axis.com

Dimensions

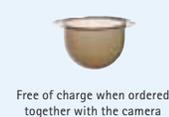


Optional accessories

AXIS T91A Mounting Accessories



AXIS Q603x-E Smoked Dome B



AXIS T8310 Video Surveillance Control Board



AXIS T90A Illuminators



AXIS P8221 Network I/O Audio Module



AXIS Camera Station and video management software from Axis' Application Development Partners. For more information, see www.axis.com/products/video/software/

USER'S MANUAL

AXIS Q6032-E Dome Network Camera



Notices

This manual is intended for administrators and users of the AXIS Q6032-E Dome Network Camera, and is applicable for firmware release 5.06 and later. It includes instructions for using and managing the camera on your network. Previous experience of networking will be of use when using this product. Some knowledge of UNIX or Linux-based systems may also be beneficial for advanced users, for developing shell scripts and applications. Later versions of this document will be posted to the Axis Website, as required. See also the product's online help, available via the Web-based interface.

Liability

Every care has been taken in the preparation of this manual. Please inform your local Axis office of any inaccuracies or omissions. Axis Communications AB cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. Axis Communications AB makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Axis Communications AB shall not be liable nor responsible for incidental or consequential damages in connection with the furnishing, performance or use of this material.

Intellectual Property Rights

Axis AB has intellectual property rights relating to technology embodied in the product described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the patents listed at <http://www.axis.com/patent.htm> and one or more additional patents or pending patent applications in the US and other countries.

This product contains licensed third-party software. See the menu item "About" in the product's user interface for more information.

This product contains source code copyright Apple Computer, Inc., under the terms of Apple Public Source License 2.0 (see <http://www.opensource.apple.com/apssl/>). The source code is available from: <http://developer.apple.com/darwin/projects/bonjour/>

Equipment Modifications

This equipment must be installed and used in strict accordance with the instructions given in the user documentation. This equipment contains no user-serviceable components. Unauthorized equipment changes or modifications will invalidate all applicable regulatory certifications and approvals.

Trademark Acknowledgments

Apple, Boa, Bonjour, Ethernet, Internet Explorer, Linux, Microsoft, Mozilla, Netscape Navigator, OS/2, Real, SMPTE, QuickTime, UNIX, Windows, WWW are registered trademarks of the respective holders. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Axis Communications AB is independent of Sun Microsystems Inc. UPnP™ is a certification mark of the UPnP™ Implementers Corporation.

Support

Should you require any technical assistance, please contact your Axis reseller. If your questions cannot be answered immediately, your reseller will forward your queries through the appropriate channels to ensure a rapid response. If you are connected to the Internet, you can:

- download user documentation and firmware updates
- find answers to resolved problems in the FAQ database. Search by product, category, or phrases
- report problems to Axis support by logging in to your private support area
- visit Axis Support at www.axis.com/techsup

Contents

Notices	2
Product Description	4
Key features	4
Overview	5
Status Indicators	6
Accessing the Camera	7
Access from a browser	7
Setting the root password	8
Video Streams	11
How to stream H.264	11
Motion JPEG	11
Alternative methods of accessing the video stream	12
Setup Tools	13
Basic Setup	13
Video	14
Video Stream	14
Camera Settings	16
Overlay Image	17
Privacy mask	17
Live View Config	18
Layout	18
Dome	20
Preset Positions	20
Auto Tracking	20
Guard Tour	21
OSDI Zones	21
Advanced	21
Events	23
Event Servers	23
Event Types	23
Recording List	28
System Options	29
Security	29
Network	31
Storage	35
Maintenance	36
Support	36
Advanced	37
About	38
Resetting to the Factory Default Settings	38
Troubleshooting	39
Checking the Firmware	39
Upgrading the Firmware	39
Emergency Recovery Procedure	39
AXIS Support	40
Symptoms, possible causes and remedial actions	41
LED Indicator flash routine	43
Technical Specifications	44
General performance considerations	46
Glossary of Terms	47
Index	53

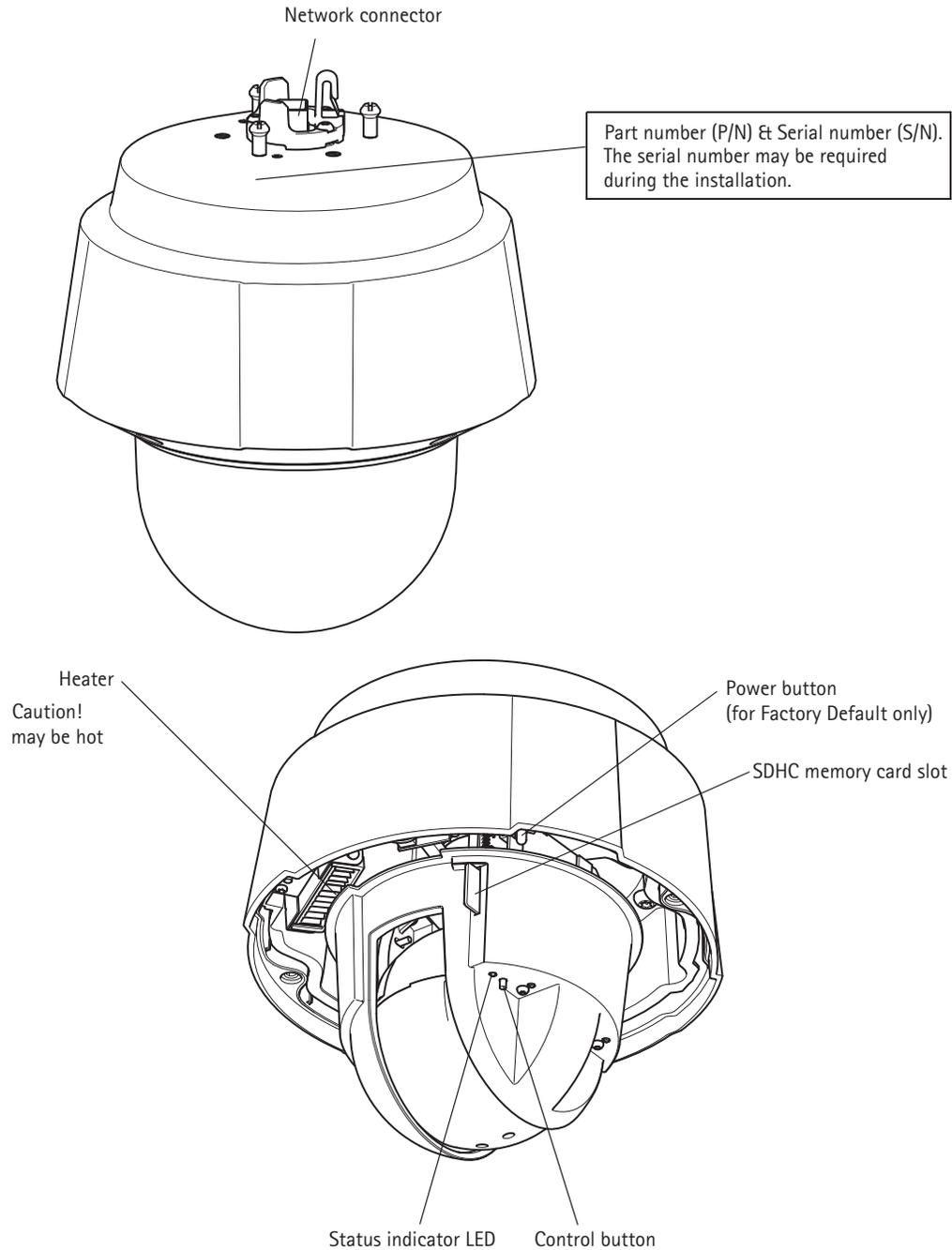
Product Description

This manual applies to AXIS Q6032-E PTZ Dome Network Camera.

Key features

- **Outdoor-ready**
 AXIS Q6032-E is designed for quick and easy installation in demanding indoor and outdoor environments. There is no need to purchase and mount a separate outdoor housing. It eliminates the cost and complexity of pre-mounting a camera in an enclosure and minimizes the risk of incorrect mounting, which helps to ensure optimal camera performance.
 With an IP66 and NEMA 4X rating, it is dust tight and offer protection against high-pressure water jets.
 AXIS Q6032-E has a built-in heater, fans and a removable sunshield, allowing the camera to be used in temperatures ranging from -40 °C up to 50 °C (-40 °F up to 122 °F).
- **Arctic Temperature Control**
 Arctic Temperature Control is a new and unique functionality from Axis that is introduced for the first time in AXIS Q6032-E. It allows the camera to not only function at -40 °C (-40 °F) but also power up at that temperature.
- **35x zoom with autofocus**
 AXIS Q6032-E offers a powerful 35x optical and 12x digital zoom with autofocus, providing crisp, clear and rich detail of both zoomed in and zoomed out images. License plates, for example, can be clearly read from a distance of 160 m (525 ft.).
- **High PoE (Power over Ethernet)**
 AXIS Q6032-E is powered through High PoE, which simplifies installation since only one cable is needed for carrying power, as well as video and pan/tilt/zoom controls. With High PoE, the camera can operate even during a power failure as the network can be connected to an Uninterruptible Power Supply. A High PoE midspan is supplied with the camera.
- **Multiple H.264 and Motion JPEG streams**
 AXIS Q6032-E offers the most efficient video compression format H.264 (MPEG-4 Part 10/AVC), which saves up to 80% in bandwidth and storage use compared with Motion JPEG without compromising image quality. The camera also supports Motion JPEG for increased flexibility.
- **Local storage**
 The camera comes with a built-in slot for an SD/SDHC memory card, enabling several days of recordings to be stored locally without any external equipment.
- **Progressive Scan**
 Progressive scan provides full resolution images of moving objects without distortion.
- **Fast pan & Tilt**
 With a maximum speed of 450°/second, and high precision, low-speed movement at 0.05°/second, AXIS Q6032-E can follow a walking person at a distance of 400 m (1300 ft.) and pan/tilt to any preset in less than 1.5 seconds.
- **Extended tilt range of 20° above the horizon**
 The camera can tilt 20° above the horizon for a total tilt range of 220°, making it possible for the camera to see higher than where it is mounted. This is especially beneficial when monitoring over uneven terrain. The extended tilt range (over the standard 180°) also makes installation easier since the camera does not have to be mounted 100% upright.
- **Intelligent video capabilities**
 AXIS Q6032-E has both video motion detection and auto tracking, which allows a moving object within the camera's field of view to be detected and followed automatically.
- **Advanced security and network management**
 AXIS Q6032-E offers the highest degree of security, including HTTPS encrypted video streams without affecting performance and IPv6 support in addition to IPv4. IPv6 is a requirement in many large installations.

Overview



Network connector – RJ-45 Ethernet connector. Supports High Power over Ethernet (IEE 802.3at). Use Axis T8124 Midspan (included). Shielded cable shall be used to comply with EMC.

Control button – The control button is used for

- Connecting to AXIS Internet Dynamic DNS Service, see page 32. To connect, press the button once.
- Restoring the camera to factory default settings, see *Resetting to the Factory Default Settings*, on page 38.

Power button – Press the button to temporarily power camera when dome cover is removed. The power button is also used with the control button to restore the camera to factory default settings, see *Resetting to the Factory Default Settings*, on page 38.

Serial number label – Part number (P/N) and Serial number (S/N). The serial number may be required during installation.

SDHC Memory card slot – A standard or high capacity SD memory card (not included) can be used for local recording with removable storage. To insert and remove an SD card, the camera's top cover must first be removed; for instructions please refer to the Installation Guide.

Note:

Before removal, the SD card should be unmounted to prevent corruption of recordings. To unmount the SD card, go to **Setup > System Options > Storage > SD Card** and click **Unmount**.

Status Indicators

After the startup and self test routines the indicators flash as follows.

Unit	Color	Indication
AXIS Q6032-E	Unlit	Steady connection/normal operation
	Amber	Steady for system initiating. Flashes during firmware upgrade or reset to factory default.
	Amber/red	No network connection
	Red	Firmware upgrade failure
	Green	Steady for 10 sec. after successful restart

See also *LED Indicator flash routine*, on page 43.

Unit	LED	Color	Indication
AXIS T8124	Port	Unlit	No camera connected
		Amber	Insufficient power for camera and heater. Check cable
		Flashing	Power overload
		Green	Camera connected, normal behavior
	AC input	Steady green	AC power connected

Accessing the Camera

To install the network camera, refer to the Installation Guide supplied with your product.

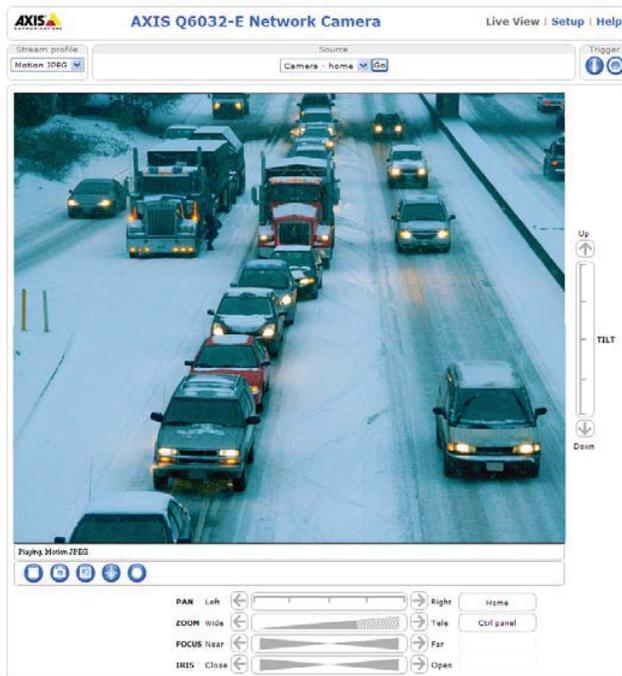
The network camera can be used with most operating systems and browsers. The recommended browsers are Internet Explorer with Windows, Safari with Macintosh and Firefox with other operating systems. See *Technical Specifications*, on page 44.

Notes:

- To view streaming video in Microsoft Internet Explorer, set your browser to allow ActiveX controls and install AXIS Media Control (AMC) on your workstation.
- QuickTime™ is also supported for viewing streaming H.264 video.
- If your workstation restricts the use of additional software components, the camera can be configured to use a Java applet for viewing Motion JPEG.
- The network camera includes one (1) decoder license for viewing H.264 video streams. This is automatically installed with AMC. The administrator can disable the installation of the H.264 decoder, to prevent installation of unlicensed copies.

Access from a browser

1. Start a browser (Internet Explorer, Firefox).
2. Enter the IP address or host name of the camera in the **Location/Address** field of your browser.
To access the camera from a Macintosh computer (Mac OS X), click on the Bonjour tab and select the network camera from the drop-down list.
3. If this is the first time you are accessing the camera, see *Access from the Internet*, on page 8. Otherwise enter your user name and password, set by the administrator.
4. The camera's Live View page appears in your browser.



Note:

The layout of the Live View page may have been customized to specific requirements. Consequently, some of the examples and functions featured here may differ from those displayed on your own Live View page.

Access from the Internet

Once connected, the camera is accessible on your local network (LAN). To access the camera from the Internet you must configure your broadband router to allow incoming data traffic to the camera. To do this, enable the NAT-traversal feature, which will attempt to automatically configure the router to allow access to the camera. This is enabled from Setup > System Options > Network > TCP/IP Advanced.

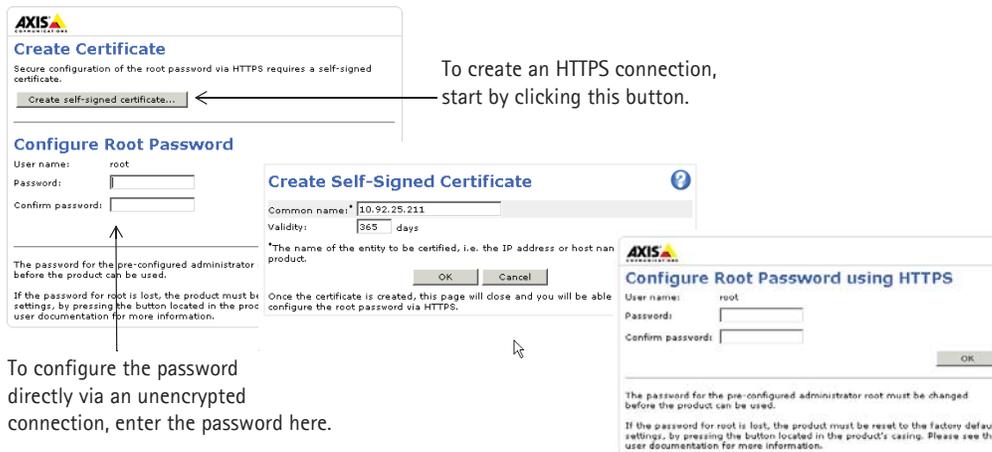
For more information, please see *NAT traversal (port mapping) for IPv4*, on page 33 See also the AXIS Internet Dynamic DNS Service at www.axiscam.net For Technical notes on this and other topics, visit the Axis Support web at www.axis.com/techsup

Setting the root password

To gain access to the product, you must set the password for the default administrator user - 'root'. This is done in the 'Configure Root Password' dialog, which is displayed when the network camera is accessed for the first time. To prevent network eavesdropping the root password can be set via an encrypted HTTPS connection, which requires an HTTPS certificate

Note:

HTTPS (Hypertext Transfer Protocol over SSL) is a protocol used to encrypt the traffic between web browsers and servers. The HTTPS certificate ensures encrypted exchange of information.



To set the password via a standard HTTP connection, enter it directly in the first dialog shown above.

To set the password via an encrypted HTTPS connection, follow these steps:

1. Click **Create self-signed certificate**.
2. Provide the requested information and click **OK**. The certificate is created and the password can now be set securely. All traffic to and from the network camera is encrypted from this point on.
3. Enter a password and then re-enter it to confirm the spelling. Click **OK**. The password has now been configured.

Notes:

- The default administrator user name 'root' is permanent and cannot be deleted.
- If the password for root is lost, the camera must be reset to the factory default settings. See page 38.
- If prompted, click **Yes** to install AXIS Media Control, which allows viewing of the video stream in Internet Explorer. You will need administrator rights on the computer to do this. If using Windows 7 or Windows Vista, you must also run Internet Explorer as administrator; right-click the Internet Explorer icon and select **Run as Administrator**.

The Live View page

How you customize the Live View page determines which buttons are visible. Not all the buttons described below will show up, unless configured to do so. These are configured under **Setup > Live View Config > Layout**.



The Stream Profile drop-down list allows you to select a customized or pre-programmed stream profile on the Live View page. Stream profiles are configured under **Setup > Video > Stream Profiles**, see *Stream Profiles*, on page 16 for more information.



The Trigger buttons can trigger an event directly from the Live View page. The buttons are configured under **Setup > Live View Config > Layout**.



The Snapshot button saves a snapshot of the video image on display. Right-click on the video image to save it in JPEG format on your computer. This button is primarily intended for use when the AXIS Media Control viewer toolbar is not available.



Activate the camera's Fan manually with this button.



Activate the camera's Heater manually with this button.

AXIS Media Control viewer toolbar

The AXIS Media Control viewer toolbar is available in Internet Explorer only. See *AXIS Media Control (AMC)*, on page 12 for more information. AMC displays the following buttons:



The Play button connects to the Axis product and starts playing a media stream.



The Stop button stops the video stream.



The Snapshot button takes a snapshot of the current image. The location where the image is saved can be specified in the AMC Control Panel.



Click the View Full Screen button and the video image will fill the entire screen. Press Esc (Escape) on the computer keyboard to cancel full screen view.



The Record button is used to record the current video stream. The location where the recording is saved can be specified in the AMC Control Panel.

Pan/Tilt/Zoom Controls

The Live View page also displays the Pan/Tilt/Zoom (PTZ) controls. The administrator can enable/disable controls for specified users under **System Options > Security > Users**.

With the PTZ Control Queue enabled the time each user is in control of the PTZ settings is limited. Click the buttons to request or release control of the PTZ controls. The PTZ Control Queue is set up under **Dome > Control Queue**.



Click the **Emulate joystick mode** button and click in the image to move the camera view in the direction of the mouse pointer.



Click the **Center mode** button and click on a position in the image to center the camera view on that position.

Up



Pan and Tilt bars – Click a position directly on the bar to steer the camera view directly to the new position in one smooth movement or click on the arrows at the ends of the bars to steer the camera in steps.

Zoom bar – Click a position directly on the zoom bar to zoom all the way to the new position in one movement or click the arrows at the ends of the bar to zoom in steps.

Focus bar – Click a position directly on the focus bar to set focus at a new position in one movement or click the arrows at the ends of the bar to change focus in steps.

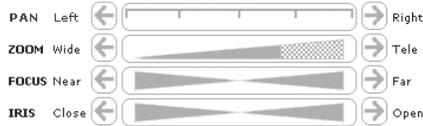
Iris bar – Click a position directly on the iris bar to change the degree the iris opens to in one movement or click the arrows at the ends of the bar to change the iris in steps.



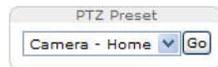
TILT



Down



Click the **Ctrl panel** button to open the PTZ control panel which provides additional PTZ controls. User-defined buttons can also appear in the Control panel, see *Controls*, on page 22.



Select a **PTZ preset** position to steer the camera view to the saved position, see *Preset Positions*, on page 20.



Click the **Start/Stop Auto Track** button to manually start and stop the auto tracking feature.

Video Streams

The network camera provides several image and video stream formats. Your requirements and the properties of your network will determine the type you use.

The Live View page in the network camera provides access to H.264 and Motion JPEG video streams, and to the list of available stream profiles. Other applications and clients can also access these video streams/images directly, without going via the Live View page.

How to stream H.264

This video compression standard makes good use of bandwidth, and can provide high quality video streams at less than 1 Mbit/s.

Deciding which combination of protocols and methods to use depends on your viewing requirements, and on the properties of your network. The available options in Axis Media Control are:

Unicast RTP	This unicast method (RTP over UDP) is used for live unicast video, especially when it is important to always have an up-to-date video stream, even if some images are dropped.	<p>Unicasting is used for video-on-demand broadcasting, so that there is no video traffic on the network until a client connects and requests the stream.</p> <p>Note that there are a maximum of 10 simultaneous unicast connections.</p>
RTP over RTSP	This unicast method (RTP tunneled over RTSP) is useful as it is relatively simple to configure firewalls to allow RTSP traffic.	
RTP over RTSP over HTTP	This unicast method can be used to traverse firewalls. Firewalls are commonly configured to allow the HTTP protocol, thus allowing RTP to be tunneled.	
Multicast RTP	<p>This method (RTP over UDP) should be used for live multicast video. The video stream is always up-to-date, even if some images are dropped.</p> <p>Multicasting provides the most efficient usage of bandwidth when there are large numbers of clients viewing simultaneously. A multicast broadcast cannot however, pass a network router unless the router is configured to allow this. It is not possible to multicast over the Internet, for example. Note also that all multicast viewers count as one unicast viewer in the maximum total of 10 simultaneous connections.</p>	

Axis Media Control negotiates with the camera to determine the transport protocol to use. The order of priority, listed in the AMC Control Panel, can be changed and the options disabled, to suit specific requirements.

Important!

H.264 and is licensed technology. The network camera includes one H.264 viewing client license. Installing additional unlicensed copies of the viewing client is prohibited. To purchase additional licenses, contact your Axis reseller.

Motion JPEG

This format uses standard JPEG still images for the video stream. These images are then displayed and updated at a rate sufficient to create a stream that shows constantly updated motion.

The Motion JPEG stream uses considerable amounts of bandwidth, but provides excellent image quality and access to every image contained in the stream. The recommended method of accessing Motion JPEG live video from the network camera is to use the AXIS Media Control (AMC) in Internet Explorer in Windows.

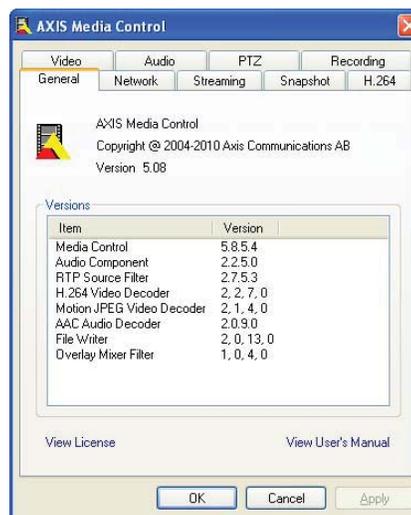
AXIS Media Control (AMC)

AXIS Media Control (AMC) in Internet Explorer in Windows is the recommended method of accessing live video from the network camera.

The AMC Control Panel can be used to configure various video settings. Please see the AXIS Media Control User's Manual for more information.

The AMC Control Panel is automatically installed on first use, after which it can be configured. Open the AMC Control Panel from:

- Windows Control Panel (from the Start menu)
- Alternatively, right-click the video image in Internet Explorer and click **Settings** to access the AMC window.



Alternative methods of accessing the video stream

You can also access video/images from the network camera in the following ways:

- Motion JPEG server push (if supported by the client, Firefox, for example). This option maintains an open HTTP connection to the browser and sends data as and when required, for as long as required.
- Still JPEG images in a browser. Enter the path - `http://<ip>/axis-cgi/jpg/image.cgi`
- Windows Media Player. This requires AXIS Media Control and the H.264 decoder to be installed. The paths that can be used are listed below in the order of preference:
 - Unicast via RTP: `axrtpu://<ip>/axis-media/media.amp`
 - Unicast via RTSP: `axrtsp://<ip>/axis-media/media.amp`
 - Unicast via RTSP, tunneled via HTTP: `axrtsphttp://<ip>/axis-media/media.amp`
 - Multicast: `axrtpm://<ip>/axis-media/media.amp`
- To access the video stream from QuickTime™ the following paths can be used:
 - `rtsp://<ip>/axis-media/media.amp`
 - `rtsp://<ip>/axis-media/media.3gp`

<ip> = IP address

Notes:

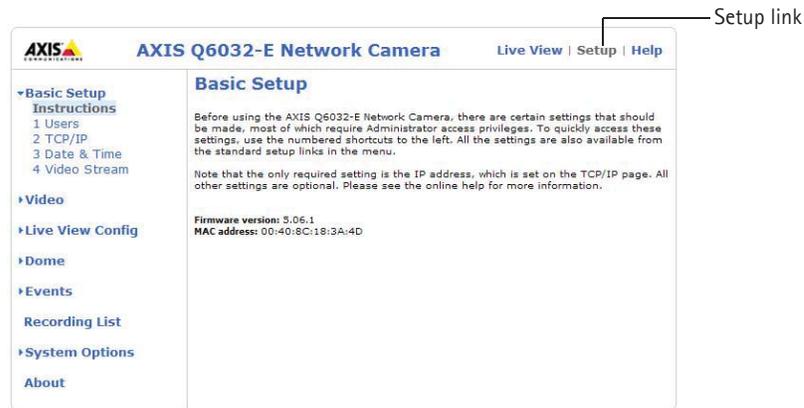
- The network camera supports QuickTime 6.5.1 and later
- QuickTime adds latency to the video stream (up to 3 seconds)
- It may be possible to use other players to view the H.264 stream using the paths above, although Axis does not guarantee this
- <ip> = IP address

Setup Tools

AXIS Q6032-E can be configured by users with administrator or operator rights. To access the product's Setup tools, click **Setup** in the top right-hand corner of the Live View page.

- Administrators have unrestricted access to all settings.
- Operators have access to Video & Audio, Live View Config, PTZ, Events and Recording List.

See also the online help available by clicking  on each Setup page.



Basic Setup

Basic Setup provides shortcuts to the settings that should be made before using the network camera:

1. Users, see page 29.
2. TCP/IP, see page 31.
3. Date & Time, see page 31.
4. Video Stream, see page 14.

Video

Click [?](#) to access the online help that explains the Setup tools.

Video Stream

The video stream settings appear under three different tabs:

- Image
- H.264
- MJPEG

Image

Image Appearance

Use these settings to modify the image resolution and compression. Setting the compression level affects the image quality and the amount of bandwidth required, the lower the compression, the higher the image quality with higher bandwidth requirements. The image can also be rotated.

See the online help files [?](#) for more information.

Video Stream

To avoid bandwidth problems on the network, the frame rate allowed to each viewer can be limited. Select the **Unlimited** radio button option to allow the highest available frame rate; or select the **Limited to** radio button and enter a value (1-30) fps in the field.

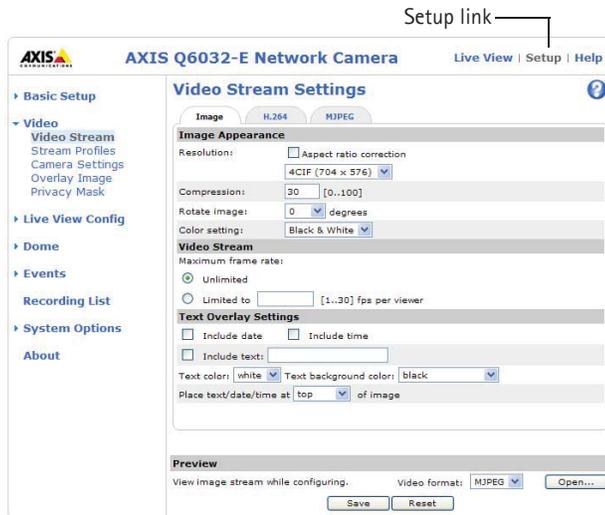
Text Overlay Settings

Use these settings to include text, date, and time as overlay in the video stream. See the online help files [?](#) for information on available options.

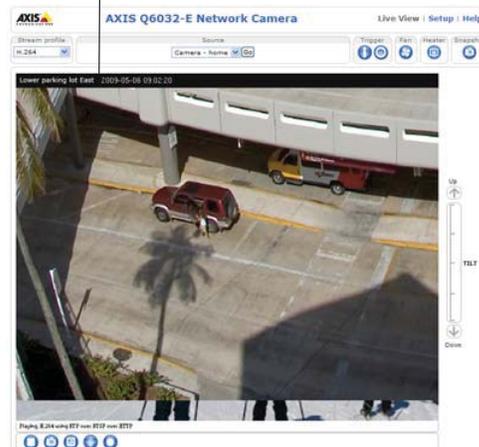
Preview

For a preview of the image before saving, select video format and **Open**. When satisfied with the settings, click **Save**.

To place an overlay image at specific coordinates, see *Overlay Image*, on page 17.



Text, date & time overlay



H.264

GOV Settings

The GOV structure describes the composition of the video stream and setting the GOV-length to a higher value saves considerably on bandwidth but may have an adverse effect on image quality.

Bit Rate Control

The bit rate can be set as **Variable Bit Rate (VBR)** or **Constant Bit Rate (CBR)**. VBR adjusts the bit rate according to the image complexity, using up bandwidth for increased activity in the image, and less for lower activity in the monitored area.

CBR allows you to set a fixed **Target bit rate** that consumes a predictable amount of bandwidth. As the bit rate would usually need to increase for increased image activity, but in this case cannot, the frame rate and image quality are affected negatively. To partly compensate for this, it is possible to prioritize either the frame rate or the image quality. Not setting a priority means the frame rate and image quality are equally affected.

Note:

To determine a reasonable bit rate, go to **Setup > Video > Video Stream > Image**. Under Overlay Settings, check the **Include** checkbox and enter the code **#b** in the **Include text:** field. The current bit rate will display as a text overlay on the Live View page.

To preview the image stream while configuring the GOV settings and Bit rate control, select **Open** under **Preview**.

MJPEG

Sometimes the image size is large due to low light or complex scenery. Adjusting the **Maximum frame size** helps control the bandwidth and storage used by the Motion JPEG video stream in these situations. Defining the frame size as **Default** provides consistently good image quality at the expense of increased bandwidth and storage usage during low light. Limiting the frame size optimizes bandwidth and storage usage, but may give poor image quality. To prevent increased bandwidth and storage usage, the maximum frame size should be set to an optimal value.

Stream Profiles

There are four pre-programmed stream profiles available for quick set-up. These settings can be adjusted and new, customized profiles can be created. Each profile has a descriptive name, describing its usage and/or purpose. The profiles can be accessed from the Live View page.

- To create a new stream profile, click **Add** to bring up the **Stream Profile Settings** dialog.
 1. Enter a unique name and a description for your profile.
 2. Select a **Video encoding** type (H.264 or MJPEG) from the drop-down list.
 3. Modify the stream settings under the **Image**, **H.264** and **MJPEG** tabs. See *Video Stream*, on page 14.
 4. Click **OK** to save the profile.
- To copy an existing stream profile, click **Copy** and enter a new name. Change the stream profile settings as above.
- To modify an existing stream profile, click **Modify** and change the settings as above. The original settings for the pre-programmed profiles can always be restored by clicking **Restore**.
- To remove a stream profile, click **Remove**. Pre-programmed profiles cannot be removed.

Camera Settings

This page provides access to the image settings for the network camera.

Image Appearance

Color level – Select an appropriate level by entering a value in the range 0-100. Lower values mean less color saturation, whilst the value 100 gives maximum color saturation.

Brightness – The image brightness can be adjusted in the range 0-100, where a higher value produces a brighter image.

Sharpness – Controls the amount of sharpening applied to the image. A sharper image might increase image noise, especially in low light conditions. A lower setting reduces image noise, but the image would be less sharp.

Contrast – Controls the contrast of the image.

White balance

White balance is used to compensate for the different colors present in different light sources, to make the colors in the image appear the same. The network camera can be set to automatically identify the light source and compensate for its color. Alternatively, the type of light source can be manually selected from the drop-down list. Please see the online help files  for a description of each available setting.

Wide dynamic range – Wide dynamic range can improve the exposure when there is considerable contrast between light and dark areas in the image.

Exposure Settings

Configure the exposure settings to suit the image quality requirements in relation to lighting, frame rate and bandwidth considerations.

Exposure control – This setting is used to adapt to the amount or type of light used. **Automatic** is the default setting and can be used in most situations. The shutter speed is automatically set to produce optimum image quality.

Max exposure time – Select the maximum exposure time from the drop-down list. Increasing the exposure time will improve image quality, but may decrease the frame rate. There may also be an increase in motion blur. Checking **Allow slow shutter** decreases the shutter speed in low light to improve image brightness.

Enable Backlight compensation – Enable this option if a bright spot of light, for example a light bulb, causes other areas in the image to appear to dark.

Exposure zones – This setting determines which part of the image is used to calculate the exposure. For most situations, the **Auto** settings can be used.

IR cut filter – Set the filter to **Off** to allow the camera to “see” infrared light; it increases the light sensitivity, for example at night. The image is shown in black & white when the IR cut filter is off. Set to **Auto** to automatically switch between **On** and **Off** according to the lighting conditions

Max gain – Measured in decibels (dB). A high level of amplification may provide a better image in very low light situations. A high gain will also increase the amount of image noise.

Image Settings

Autofocus enabled – Autofocus is enabled by default.

Stabilizer – When monitoring an environment that is subject to vibrations (such as traffic control), images may appear to be unsteady. Depending on the environment, select the frequency (High or Low) that gives the best improvement in image quality.

Image freeze on PTZ – Select **All movements** to freeze the image while the camera is moving during a pan, tilt or zoom operation. Once the camera reaches its new position the current image is shown. **Presets** freezes the image only when the camera moves between preset positions.

View Image Settings – Click **View** to view the video stream with the current configuration. Once satisfied, click **Save**.

Overlay Image

An overlay image is a static image superimposed over the video image. The overlay image can be used to provide extra information, or to mask a part of the video image. See the online help for supported image formats and sizes.

To use your own image, e.g. a logo, it must first be uploaded to the network camera. Click **Browse** and locate the image file on the computer. Click **Upload**. When uploaded, the file can be selected in the **Use overlay image** drop-down list.

Image Overlay Placement

To place the overlay image at specific coordinates, check **Include overlay image at the coordinates** and enter the X and Y coordinates.

View Image Settings

Click **View** to view the overlay image in the video stream.

Once satisfied, click **Save**.

Privacy mask

A privacy mask is an area of solid color that prohibits users from viewing parts of the monitored area. Up to eight privacy masks can be used. Privacy masks cannot be bypassed via the VAPIX® Application Programming Interface (API).

Privacy Mask List

The Privacy Mask List shows all the masks that are currently configured in the network camera and if they are enabled.

Add / Edit Privacy mask

To define a new mask:

1. Click **Add mask**. A rectangle appears on the image.
2. Use the mouse to move the rectangle. To resize, click and pull the bottom right-hand corner.
3. Choose a color, black, white, gray or red, from the **Privacy mask color** drop-down list.
4. Enter a descriptive name in **Mask name**.
5. Click **Save**.

To edit a privacy mask, select the mask and reshape, move or change color as needed.

Live View Config

Layout

Stream Profile

From the **Stream Profile** drop-down list, select the stream profile that is to be used for the Live View page. Listed are the pre-programmed stream profiles as well as the ones created under **Video > Stream Profiles**. See *Stream Profiles*, on page 16, for more information.

Default Viewer

From the drop-down lists, select the default method for viewing video images for your browser. The camera attempts to show the video images in the selected video format and viewer. If this is not possible, the camera overrides the settings and selects the best available combination.

Browser	Viewer	Description
Internet Explorer	AMC	Recommended viewer in Windows Internet Explorer (H.264/Motion JPEG).
	QuickTime	H.264
	Java applet	A slower imaging alternative to AMC. Requires one of the following installed on the client: <ul style="list-style-type: none"> JVM (J2SE) 1.4.2 or higher JRE (J2SE) 5.0 or higher
	Still image	Displays still images only. Click the Refresh button in your browser to view a new image.
Other browsers	Server Push	Recommended viewer for other browsers (Motion JPEG).
	QuickTime	H.264
	Java applet	A slower imaging alternative to Server Push (Motion JPEG only).
	Still image	Displays still images only. Click the Refresh button in your browser to view a new image.

Viewer Settings

Check the **Show viewer toolbar** box to display the AXIS Media Control (AMC) or the QuickTime viewer toolbar under the video image in your browser.

The administrator can disable the installation of the **H.264 decoder** included with AXIS Media Control. This is used to prevent the installation of unlicensed copies. Further decoder licenses can be purchased from your Axis dealer.

Enable **Show crosshair** in **PTZ joystick mode** and a cross will indicate the center of the image in PTZ joystick mode.

Check **Use PTZ joystick mode as default** to enable joystick mode. The mode can be changed temporarily from the PTZ control panel.

Check **Enable recording button** to enable recording from the Live View page. The recordings are saved to the location specified in the AMC Control Panel, see *AXIS Media Control (AMC)*, on page 12.

Action Buttons

Check the boxes to display the action buttons in the Live View page.

The **manual trigger button** can be used to manually trigger and stop an event. See *Events*, on page 23.

The **snapshot button** can be used to save a snapshot from the video stream. This button is mainly intended for use with browsers other than Internet Explorer, or when not using AXIS Media Control to view the video stream. AXIS Media Control for Internet Explorer has its own snapshot button.

The **auto tracking button** in the Live View page (Start/Stop Auto Track) manually stops and starts the auto tracking feature.

The **fan button** is used to manually start the camera's fan. Specify the number of minutes the fan should run for.

The **heater button** is used to manually start the camera's heater. Specify the number of minutes the heater should run for.

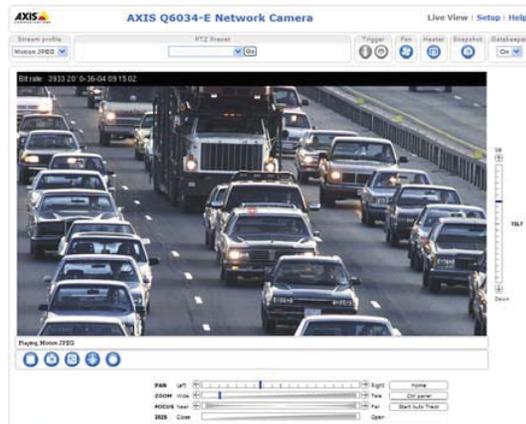
User Defined Links

User defined links can link to web pages, or can be used to run scripts or activate and control external devices connected to the network camera. Once configured, the link appear on the Live View page.

To set up a link, check the **Show custom link** box, select the **cgi** or **web link** radio button, enter the URL and a descriptive name in the provided field.

A link defined as a web link will open in a new window, while a cgi link will run for example a script in the background.

User defined CGI links can be used to issue API requests. For more information on the VAPIX Application Programming Interface (API), see the Video developer pages at Axis Web site www.axis.com/developer.



User defined link

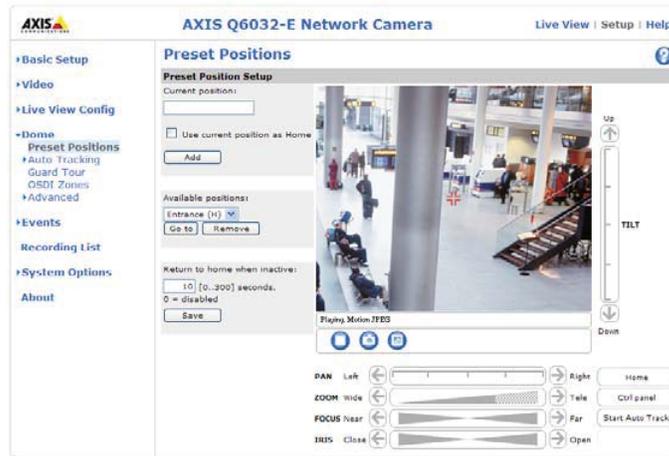
Dome

Preset Positions

A preset position is a pre-defined camera view that can be used to quickly steer the camera to a specific location.

From **Preset Position Setup**, use the Pan, Tilt and Zoom (PTZ) controls to steer the camera view to the required position. When satisfied with the camera's position, enter a descriptive name and click **Add**. The camera position, iris and focus settings are then saved as a preset position.

This position can be assumed at any time, by selecting the preset's name from the **Available positions** drop-down list. Preset positions can be selected in **Live View** page, from **Event Types** and in the **Guard Tour**.



One position can be set as the **Home** position, which is readily accessible by clicking the **Home** button in both the **Preset Positions** window and the **Live View** window. The name will have (H) added, for example, Entrance (H).

The network camera can also be configured to return to the **Home** position when the camera has been inactive for a specified length of time. Enter the length of time in the field **Return to home when inactive** and click **Save**. Setting the time to zero prevents the camera from automatically returning to the **Home** position.

The preset position name can be included in the overlay image text, see *Text Overlay Settings*, on page 14.

Auto Tracking

The network camera can detect movement in the camera's field of view, for example a moving vehicle or person. If auto tracking is enabled, the camera will automatically pan and tilt to follow the moving object or, in case there is lots of simultaneous movement, the area with the most movement. Auto tracking continues until the moving object stops or disappears from the monitored area. Movement in areas blocked by privacy masks and in exclude areas does not trigger auto tracking.

It is strongly recommended to enable the **PTZ Control Queue** if Auto Tracking and Guard Tour are simultaneously enabled. In the PTZ Control Queue, the Guard Tour has lower priority than Auto Tracking so the camera will not abandon Auto Tracking to start a Guard Tour.

Configuration

Start and Stop Auto Tracking – To enable auto tracking, click **Start**. To disable auto tracking, click **Stop**.

Movement trigger sensitivity – Set to Low, Medium or High. Medium is usually a good choice, but in some situations a low or high sensitivity might be more suitable, depending on the size of the moving objects and the image contrast.

Exclude Areas

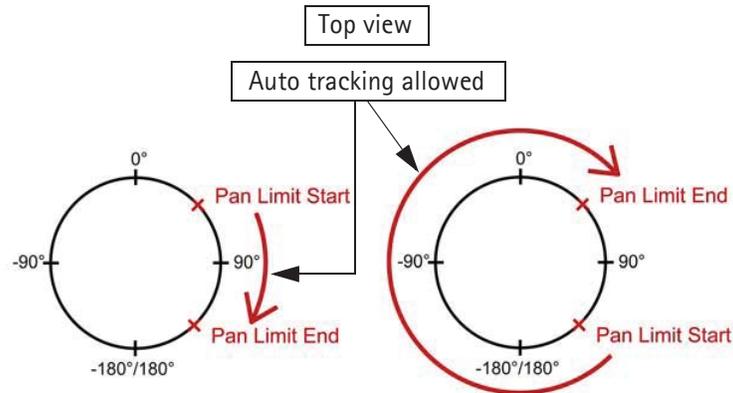
Exclude areas are areas where movement is to be ignored. Note that movement in an area blocked by a privacy mask is always ignored.

To create an exclude area, click **Add area**. The area (the blue rectangle) can be resized and moved to the desired position. Enter a descriptive name and click **Save**. To enable or disable an area, click the name of the area and click **Enable/Disable**.

Max Limits

The pan and tilt limits restrict the area where auto tracking is allowed. This may prove useful, for example, to avoid tracking birds in the sky. Click **Enable Tilt Limit** and **Enable Pan Limit** to enable the pan and tilt limits, respectively.

Enter the limits (in degrees) of the **Lower tilt angle** and **Upper tilt angle**, or click the links and move the blue horizontal bars in the preview window. To set the pan limits, enter the values (in degrees) in the **Pan limit start** and **Pan limit end** fields, or click the links and move the blue vertical bars in the preview window. Auto tracking is allowed between the pan start and end limits going clockwise, see the illustration below.



Guard Tour

A guard tour displays the video stream from different preset positions, one-by-one, in a pre-determined order or randomly, and for configurable time periods. The guard tour will keep running after the user has logged off or closed the browser.

OSDI Zones

On-screen Direction Indicator (OSDI) Zones can be included in the overlay text (see page 14) to aid the user to navigate the camera. Each OSDI Zone is set up with coordinates and a descriptive name.

The camera uses the coordinates of the center of the image to set the lower left and upper right zone areas. First navigate to where you would like the lowermost left point of the OSDI Zone to be located. By clicking **Get** the coordinates are set. Proceed to where the upper right point of the zone should be located and click its **Get** button. Give the zone a descriptive name and click **OK**.

To include the name of OSDI Zone in the overlay text, go to **Video > Video Stream > Text Overlay Settings**. Check the **include text** box and enter the modifier **#L** in the field. See **File Naming & Date/Time Formats** in the online help [?](#) for more information about modifiers.

Advanced

Limits

Define the pan, tilt, zoom and focus limits for the network camera. Movements to the left and right, up and down, can be restricted to narrow the area under surveillance. The near focus limit can be set to avoid focusing on objects too close to the camera.

Once a limit has been saved, this position cannot be exceeded by the network camera unless the values have been reset and saved to a greater value first (reset the default values of the mechanical restrictions).

Move speed sets the speed of the camera's Pan/Tilt movements. The default setting is maximum speed.

Enable proportional speed – When using a joystick (or emulating one with the mouse), this setting can be used to reduce the maximum pan/tilt movement speed, i.e. the speed the camera moves at when the joystick is pushed all the way out in any pan/tilt direction. This is useful when the camera is zoomed in on an object and a pan/tilt movement is performed.

See the online help  for more information.

Controls

Panel Shortcut Command Buttons can be configured to provide direct access to commands issued via the VAPIX® Application Programming Interface. The buttons will be displayed in the PTZ control panel, which is available on the Live View page by clicking the **Ctrl panel** button.



Enable/Disable controls – Uncheck the boxes to disable the pan, tilt, zoom, focus and iris controls.

Note:

Disabling PTZ controls will affect preset positions. For example, if the tilt control is disabled, the camera cannot move to preset positions that require a tilt movement.

Control Queue

The administrator can set up a queue for the PTZ controllers. Once set up, the **PTZ Control Queue** buttons appear on the Live View page offering one viewer exclusive control for a limited amount of time. Other users will be placed in queue.

Events

Pre-defined parameters, known as an **event** or **Event Type** can trigger certain actions in the camera. A common event type is an alarm that causes the camera to upload images. Many event types use an **Event Server**, to receive uploaded images.

An event that is triggered by a signal, such as a detection of motion or system event, is called a **triggered event**, see page 24.

A **scheduled event** runs at pre-programmed times.

An **Action** refers to what happens when the event occurs.

This section describes how to configure the camera to perform certain actions when events occur.

Event Servers

Event servers are used to receive uploaded image files and/or notification messages. To set up Event Server connections in your camera, go to **Setup > Events > Event Servers** and enter the required information for the server type.

Server type	Purpose	Information required
FTP Server	<ul style="list-style-type: none"> Receives uploaded images 	<ul style="list-style-type: none"> Descriptive name Network address and Upload path User Name and Password
HTTP Server	<ul style="list-style-type: none"> Receives notification messages Receives uploaded images 	<ul style="list-style-type: none"> Descriptive name URL (IP address or host name) User Name and Password Proxy settings
TCP Server	<ul style="list-style-type: none"> Receives notification messages 	<ul style="list-style-type: none"> Descriptive name Network address (IP address or host name) Port number

For details on each setting, see the online help  available from each web page.

When the setup is complete, the connection can be tested by clicking the **Test** button (the connection test takes approximately 10 seconds).

Event Types

An **Event Type** describes how and when the camera is to perform certain actions.

Example: If somebody passes in front of a camera and an event has been configured to detect and respond to motion, the camera can record and save images to an FTP server, and can send a notification e-mail to an e-mail address. Images can be sent as e-mail attachments.

Triggered Event

A triggered event can be activated by:

- A Manual trigger - using the manual trigger button on the Live View page or through the VAPIX® Application Programming Interface (API)
- Movement in a motion detection window
- On boot - for example after power loss
- Pan Tilt Zoom - when the camera stops at a preset position
- Disk full - when the local storage disk (SD memory card) has less than 1MB of free memory left
- Auto Tracking - Auto Tracking detects movement in the camera's field of view and will follow the motion, e.g. a person or vehicle, until it disappears from the monitored area.
Specify whether to trigger the event when motion starts or when motion stops
- Fan malfunction

How to set up a triggered event

The following example describes how to set up the camera to upload images when a door is opened.

1. Click **Add triggered** on the **Event types** page.
2. Enter a descriptive **Name** for the event, such as Door open.
3. Set the **Priority** - High, Normal or Low.
4. Set the **Respond to Trigger** parameters to define when the event is active, for example, after office hours.
5. Select the trigger alternative from the **Triggered by** drop-down list. For example, motion detection.
6. Set the **When Triggered** parameters, that is, define what the camera will do if the main door is opened. To upload images, select **Save stream** and enter the required information. See *Save stream*, on page 24.
7. Click **OK** to save the event in the **Event Types** list.

Please see the online help  for descriptions of each available option.

Note:

Up to 10 event types can be configured in the camera, and up to three of these can be configured to upload images. File names can be formatted according to specific requirements. See *File Naming & Date/Time Formats* in the online help .

Save stream

To upload images to an FTP or HTTP server, save the video stream to the local storage card or to send images by email, check the **Save stream** box.

Image frequency - Set the image frequency to a desired frame rate. The frame rate will be the best possible, but might not be as high as specified, especially if uploading via a slow connection.

Pre-trigger and Post-trigger buffers

This function is very useful when checking to see what happened immediately before and/or after a trigger, for example, 20 seconds before and/or after a door was opened. All uploaded images are JPEG images.

Include pre-trigger buffer - Images stored internally in the server from the time immediately preceding the trigger. Check the box to enable the pre-trigger buffer and specify the buffer length in seconds, minutes or hours.

Include post-trigger buffer - Contains images from the time immediately after the trigger. The post-trigger buffer is configured in the same way as the pre-trigger buffer.

Notes

- Pre-trigger and Post-trigger buffers will be lost if the connection to the event server fails
- The maximum length of the pre-/post-buffer depends on the video image size and selected frame rate
- If the pre- or post-buffer is too large for the camera's internal memory, the frame rate is reduced and individual images may be missing. If this occurs, an entry is created in the unit's log file

Continue image upload (unbuffered) – Upload video images for a fixed length of time or for as long as the trigger is active.

Select type – Upload images to an FTP or HTTP server, send images by e-mail or save the video stream to the local storage disk.

Create folder – Images uploaded to FTP and HTTP servers can be saved to designated folders. Folders can for example be named using the current date and time, see File Naming & Date/Time formats in the online help [?](#) .

Base file name – Used to name all uploaded images. Add a suffix or use your own file format to give the images unique names, see File Naming & Date/Time formats in the online help [?](#) .

Use stream profile – Select the stream profile to upload, send as e-mail or save to the local disk. When saving to the local disk, the video format (JPEG or H.264) must first be selected.

Scheduled Event

A Scheduled event can be activated at preset times, in a repeating pattern on selected weekdays.

How to set up a scheduled event

The following example describes how to set up a scheduled event.

1. Click **Add scheduled** on the **Event Types** page. The **Triggered Event Type Setup** page appears
2. Enter a descriptive **Name** for the event, such as Scheduled e-mail upload.
3. Set the **Priority** (High, Normal or Low).
4. Set the **Activation Time** parameters (24h clock) for the event. For example, select Recurrence pattern and let the event start on Sundays at 13.00 with a duration of 12 hours.
5. Set the **When Activated** parameters, that is, define what the camera should do when the event is active. To upload images, select **Save stream** and enter the required information. See *Save stream*, on page 24.
6. Click **OK** to save the Event in the Event Types list.

Please see the online help [?](#) for descriptions of each available option.

Motion Detection

Motion detection is used to generate an alarm whenever movement occurs (or stops) in the video image. A total of 10 Include and/or Exclude windows can be configured.

- Included windows target specific areas within the whole video image
- Excluded windows define areas within an Include window that should be ignored (areas outside Include windows are automatically ignored)

Once configured, the motion detection windows appear in the list of available triggers, for triggering events. See *How to set up a triggered event*, on page 24.

Note:

Using the motion detection feature may decrease the camera's overall performance.



Set up a motion detection include window

The following example describes how to configure the camera for motion detection.

1. Go to Setup > Events > Motion Detection.
2. Create a new motion detection window:
 - a. Using AXIS Media Control (Internet Explorer): Select the radio button **Configure Included Windows** and click **New**. Select the new window in the list of windows and enter a descriptive name.
 - b. Using the Java applet: Click **Add Window**. Select the **Include** radio button and enter a descriptive name in the field.
3. Adjust the size (drag the bottom right-hand corner) and position (click on the text at the top and drag to the desired position) of the active window.
4. Adjust the **Object Size**, **History** and **Sensitivity** profile sliders (see table below for details). Any detected motion within an active window is then indicated by red peaks in the **Activity** window (the active window has a red frame).
5. Click **Save**.

To exclude parts of the Include window, select the **Exclude** option and position the Exclude window as required, within the Include window.

To delete an Include or Exclude window:

- a. Using AXIS Media Control (Internet Explorer): Select the window in the list of windows and click **Del**.
- b. Using the Java applet: Select the window and click on the cross in the upper right corner.

Please see the online help [?](#) for descriptions of each available option.

	Object Size	History	Sensitivity
High level	Only very large objects trigger motion detection	An object that appears in the region will trigger the motion detection for a long period	Ordinary colored objects on ordinary backgrounds will trigger the motion detection
Low level	Even very small objects trigger motion detection	An object that appears in the region will trigger motion detection for only a very short period	Only very bright objects on a dark background trigger motion detection
Default value	Low	High	High

- Avoid triggering on small objects in the video image by setting the **object size** level to high.
- Use several small Motion Detection windows rather than one large window, if triggers on small movements or objects are desired.
- To reduce the number of triggers if there is a lot of movement during a short period of time, select a high **history** level.
- To only detect flashing light, select low **sensitivity**. In other cases, a high **sensitivity** level is recommended.

Recording List

Starttime	Length	Triggered by	Locked
2009-05-06 08:48:05...	00:00:37	New Event	yes
2009-05-06 08:23:48...	00:00:30	New Event	no
2009-05-06 08:22:53...	00:00:10	New Event	no
2009-05-05 13:43:15...	00:00:10	New Event	yes
2009-05-05 13:36:47...	00:00:10	New Event	no
2009-05-05 12:40:46...	00:00:10	New Event	no

The Recording List web page contains a list of recordings made to the SD memory card. It shows each recording's start time, length, the event type, and indicates if the recording is locked so that it can neither be deleted nor recorded over.

To view a recording, select it from the list and click **Play**.

For detailed recording and video information, select an individual recording from the list and click **Properties**.

Use the **Lock/Unlock** button to define whether a recording can be removed or recorded over, or if the recording is important and needs to be saved for future use. Locking the recording can help prevent its accidental removal.

The **Remove** button is used to delete unlocked recordings.

Recordings are made to the SD memory card once an event has been set up on under **Setup > Event Types > Add triggered /Add scheduled > Save stream > Select type**. Select Local Storage from the drop-down list.

See **Setup > System Options > Storage > SD Card** to mount, format and monitor the status and available recording space of the SD memory card.

Please refer to the Installation Guide supplied with the product for instructions on how to insert and remove the SD memory card.

Notes:

- The SD memory card is optional and not included in the product.
- To play recordings in Windows Media Player download and install AXIS Matroska File Splitter from www.axis.com/techsup/software

System Options

Security

Users

User access control is enabled by default. An administrator can set up other users, by giving these user names and passwords. It is also possible to allow anonymous viewer login, which means that anybody may access the Live View page, as described below:

The user list displays the authorized users and user groups (levels):

Viewer	Provides the lowest level of access, which only allows access to the Live View page.
Operator	An operator can view the Live View page, create and modify events, and adjust certain other settings. Operators have no access to System Options.
Administrator	An administrator has unrestricted access to the Setup tools and can determine the registration of all other users.

HTTP/RTSP Password Settings – Select the type of password to allow. You may need to allow unencrypted passwords if there are viewing clients that do not support encryption, or if you recently upgraded the firmware and the existing clients do support encryption, but need to log in again, and be configured to use this functionality.

User Settings

- Check the checkbox to enable **anonymous viewer login** to allow any viewer direct access to the Live View page.
- Check the checkbox to enable **anonymous PTZ control login** to allow anonymous users to join a queue for gaining control of the PTZ controls.
- **Enable Basic Setup** – before using the network camera, there are certain settings that should be made, most of which require Administrator access privileges. To quickly access these settings, use the Basic Setup in the menu. All settings are also available from the standard setup links in the menu. Basic Setup is enabled by default but can be disabled and removed from the menu.

IP Address Filter

Enable **IP Address Filtering** to allow or deny access to the network cameras. Once enabled, the IP addresses in the list are allowed or denied access according to the choice made in the drop-down list **Allow/Deny the following IP addresses**.

The administrator can add up to 256 IP address entries to the list (a single entry can contain multiple IP addresses). The users from these IP addresses need to be specified in the user list with the appropriate access rights. This is done from **Setup > System Options > Security > Users**.

HTTPS

The network cameras support encrypted browsing using HTTPS.

A **self-signed certificate** can be used until a Certificate Authority-issued certificate has been obtained. Click the **Create self-signed Certificate** button to install a self-signed certificate. Although self-signed certificates are free and offer some protection, true security is only implemented after the installation of a signed certificate issued by a Certificate Authority.

A signed certificate can be obtained from an issuing Certificate Authority by clicking the **Create Certificate Request** button. When the signed certificate is returned, click the **Install signed certificate** button to import the certificate. The properties of any certificate request currently resident in the camera or installed can also be viewed by clicking the **Properties** button. The HTTPS Connection Policy must also be set in the drop-down lists to enable HTTPS in the camera.

For more information, refer to the online help  .

IEEE 802.1X

IEEE 802.1X is a standard for port-based Network Admission Control providing secure authentication of wired and wireless network devices. IEEE 802.1X is based on EAP (Extensible Authentication Protocol).

To access a network protected by IEEE 802.1X, devices must authenticate themselves. The authentication is performed by a third-party entity called an authentication server, typically a RADIUS server, examples of which are FreeRADIUS and Microsoft Internet Authentication Service. In Axis implementation, the network device and the authentication server authenticate themselves with the help of digital certificates using EAP-TLS (Extensible Authentication Protocol - Transport Layer Security). The certificates are provided by an Certification Authority (CA). You need:

- a CA certificate to validate the identity of the authentication server
- a CA-signed client certificate and a private key to authenticate the network device.

To allow the network device to access a network protected by IEEE 802.1X:

1. Obtain a CA certificate, a client certificate and a client private key (contact your network administrator).
2. Go to **Setup > System Options > Security > IEEE 802.1X** and upload the CA certificate, the client certificate and the client private key.
3. Under **Settings**, select the EAPOL version, provide your EAP identity and private key password.

Check the box to enable IEEE 802.1X and click **Save**.

Certificates

CA Certificate – The CA certificate is used to validate the identity of the authentication server. Enter the path to the certificate directly, or locate the file using the **Browse** button. Then click **Upload**. To remove a certificate, click **Remove**.

Client Certificate/Client private key – The client certificate and private key are used to authenticate the network device. They can be uploaded as separate files or in one combined file (e.g. a PFX file or a PEM file). Use the Client private key field if uploading one combined file. For each file, enter the path to the file, or locate the file using the **Browse** button. Then click **Upload**. To remove a file, click **Remove**.

Settings

Eapol version – Select the EAPOL version (1 or 2) as used in your network switch.

Eap identity – Enter the user identity (maximum 16 characters) associated with your certificate.

Private key password – Enter the password (maximum 16 characters) for the private key.

Enable IEEE 802.1X – Check the box to enable the IEEE 802.1X protocol.

Date & Time

Current Server Time

Displays the current date and time (24h clock). The time can be displayed in 12h clock format in the overlay (see below).

New Server Time

Select your time zone from the drop-down list. If you want the server clock to automatically adjust for daylight savings time, select the **Automatically adjust for daylight saving time changes** option.

From the **Time Mode** section, select the preferred method to use for setting the time:

- **Synchronize with computer time** - Sets the time from the clock on your computer.
- **Synchronize with NTP Server** - The camera will obtain the time from an NTP server every 60 minutes.
- **Set manually** - This option allows you to manually set the time and date.

Note:

If using a host name for the NTP server, a DNS server must be configured under **TCP/IP** settings. See *Basic TCP/IP Settings*, below.

Date & Time Format Used in Images

Specify the formats for the date and time (12h or 24h) displayed in the video streams. Use the predefined formats or use your own custom date and time formats. See **Advanced File Naming & Date/Time Formats** in the online help  for information on how to create your own date and time formats.

Network

Basic TCP/IP Settings

AXIS Q6032-E supports both IP version 4 and IP version 6. Both versions may be enabled simultaneously, and at least one version must always be enabled. When using IPv4, the IP address for the camera can be set automatically via DHCP, or a static IP address can be set manually. If IPv6 is enabled, the network cameras receive an IP address according to the configuration in the network router. There are also options for setting up notification of changes in the IP address, and for using the **AXIS Internet Dynamic DNS Service**. For more information on setting the IP address, please see the online help .

Network Settings

Click **View** for an overview of the IP configuration of the network camera.

IPv4 Address Configuration

Enable IPv4 – Check to enable IPv4.

Obtain IP address via DHCP – Dynamic Host Configuration Protocol (DHCP) is a protocol that lets network administrators centrally manage and automate the assignment of IP addresses on a network. DHCP is enabled by default. Although a DHCP server is mostly used to set an IP address dynamically, it is also possible to use it to set a static, known IP address for a particular MAC address.

Note:

DHCP should only be enabled if using dynamic IP address notification, or if your DHCP server can update a DNS server, which then allows you to access the network camera by name (host name). If DHCP is enabled and you cannot access the unit, run **AXIS IP Utility** to search the network for connected Axis products or reset the network camera to factory default settings and then perform the installation again.

Use the following IP address – To use a static IP address for the network camera, check the radio button and then make the following settings:

- **IP address** – Specify a unique IP address for your network camera. (To check if the IP address you intend to use is available or not, click the **Test** button)
- **Subnet mask** – Specify the mask for the subnet the network camera is located on
- **Default router** – Specify the IP address of the default router (gateway) used for connecting devices attached to different networks and network segments.

IPv6 Address Configuration

Enable IPv6 – Check to enable IPv6. Other settings for IPv6 are configured in the network router.

Services

Enable ARP/Ping setting of IP address – The IP address can be set using the ARP/Ping method, which associates the unit's MAC address with an IP address. Check this box to enable the service. Leave disabled to prevent unintentional resetting of the IP address.

Notes:

- The ARP/Ping service is automatically disabled two minutes after the unit is started, or as soon as an IP address is set. In order to reset the IP address, the camera must be restarted to activate ARP/Ping for an additional two minutes.
- Pinging the unit is still possible when this service is disabled.

AXIS Internet Dynamic DNS Service – Enable this option to use AXIS Internet Dynamic DNS service to assign a host name for easy access to your network camera (requires access to the Internet).

Click **Settings** to register the camera with AXIS Internet Dynamic DNS service, or to modify the existing settings. The domain name currently registered at AXIS Internet Dynamic DNS service for your product can at any time be removed.

For more information, please refer to the online help  .

Advanced TCP/IP Settings

DNS Configuration

DNS (Domain Name Service) provides the translation of host names to IP addresses on your network.

Obtain DNS server address via DHCP – Automatically use the DNS server settings provided by the DHCP server. Click the **View** button to see the current settings.

Use the following DNS server address – Enter the desired DNS server by specifying the following:

- **Domain name** – Enter the domain(s) to search for the host name used by the network camera. Multiple domains can be separated by semicolons (;). The host name is always the first part of a Fully Qualified Domain Name, for example, **myserver** is the host name in the Fully Qualified Domain Name **myserver.mycompany.com** where **mycompany.com** is the Domain name.
- **DNS servers** – enter the IP addresses of the primary, and secondary DNS servers.
Note: This is not mandatory with regard to secondary DNS servers.

NTP Configuration

Obtain NTP server address via DHCP – Check this radio button to automatically look up and use the NTP server settings as provided by DHCP. Click the **View** button to see the current settings.

Use the following NTP server address – To create manual settings, check this radio button and enter the host name or IP address of the NTP server.

Host Name Configuration

The network cameras can be accessed using a host name, instead of an IP address. The host name is usually the same as the assigned DNS Name.

Link-Local IPv4 Address

This is enabled by default and assigns the network cameras an additional IP address for use with UPnP™. The camera can have both a Link-Local IP and a static/DHCP-supplied IP address at the same time – these will not affect each other.

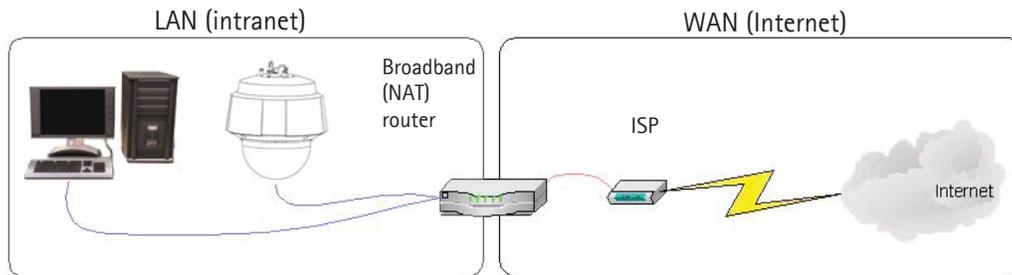
HTTP and HTTPS

The default HTTP/HTTPS port numbers (80 and 443 respectively) can be changed to any port within the range 1024-65535. This is useful for simple security port mapping, for example.

NAT traversal (port mapping) for IPv4

A broadband router allows devices on a private network (LAN) to share a single connection to the Internet. This is done by forwarding network traffic from the private network to the "outside", that is, the Internet. Security on the private network (LAN) is increased since most broadband routers are pre-configured to stop attempts to access the private network (LAN) from the public network/Internet.

Use **NAT traversal** when your network cameras are located on an intranet (LAN) and you wish to make it available from the other (WAN) side of a NAT router. With NAT traversal properly configured, all HTTP traffic to an external HTTP port in the NAT router is forwarded to the camera.



Notes:

- For NAT traversal to work, this must be supported by the broadband router. The router must also support UPnP™.
- The broadband router has many different names: "NAT router", "Network router", "Internet Gateway", "Broadband sharing device" or "Home firewall" but the essential purpose of the device is the same.

Enable/Disable – When enabled, the network camera attempts to configure port mapping in a NAT router on your network, using UPnP™. Note that UPnP™ must be enabled in the camera (see **System Options > Network > UPnP**).

Use manually selected NAT router – Select this option to manually select a NAT router and enter the IP address for the router in the field provided.

If a router is not manually specified, the network cameras automatically search for NAT routers on your network. If more than one router is found, the default router is selected.

Alternative HTTP port – select this option to manually define an external HTTP port. Enter the port number in the field provided. If no port is entered here a port number is automatically selected when NAT traversal is enabled.

Notes:

- An alternative HTTP port can be used/be active even if NAT traversal is disabled. This is useful if your NAT router does not support UPnP and you need to manually configure port forwarding in the NAT router.
- If you attempt to manually enter a port that is already in use, another available port is automatically selected.
- When the port is selected automatically it is displayed in this field. To change this enter a new port number and click Save.

FTP

The FTP server running in the network cameras enables the upload of new firmware, and user applications. Check the box to enable the service.

RTSP

The RTSP protocol allows a connecting client to start an H.264 stream. Check the box to enable the server and enter the RTSP port number to use. The default setting is 554. Note that H.264 video streams will not be available if this service is not enabled.

SOCKS

SOCKS is a networking proxy protocol. The network camera can be configured to use a SOCKS server to reach networks on the other side of a firewall/proxy server. This functionality is useful if the network camera is located on a local network behind a firewall, and notifications, uploads, alarms, and such need to be sent to a destination outside the local network (such as the Internet). See the online help  for more information.

Quality of Service (QoS)

Quality of Service (QoS) guarantees a certain level of a specified resource to selected traffic on a network. Quality can be defined as a maintained level of bandwidth, low latency, and no packet losses. The main benefits of a QoS-aware network can be summarized as:

- The ability to prioritize traffic and thus allow critical flows to be served before flows with lesser priority.
- Greater reliability in the network, thanks to the control of the amount of bandwidth an application may use, and thus control over bandwidth races between applications.

The QoS in Axis network video products marks the data packets for various types of network traffic originating from the product. This makes it possible for network routers and switches to reserve a fixed amount of bandwidth for these types of traffic. The network camera marks the following types of traffic:

- video
- event/alarm
- management network traffic

QoS Settings

For each type of network traffic supported by your Axis network video product, enter a DSCP (Differentiated Services Codepoint) value. This value is used to mark the traffic's IP header. When the marked traffic reaches a network router or switch, the DSCP value in the IP header tells the router or switch the type of treatment to apply to this type of traffic, for example, how much bandwidth to reserve for it. Note that DSCP values can be entered in decimal or hex form, but saved values are always shown in decimal.

For more information on Quality of Service, please see the Axis support web at www.axis.com/techsup

SMTP (email)

Enter the host names (or IP addresses) and port numbers for your primary and secondary mail servers in the fields provided, to enable the sending of notifications and image email messages from the camera to predefined addresses via SMTP.

If your mail server requires authentication, check the box for **Use authentication to log in to this server** and enter the necessary information. See the online help  for more information.

SNMP

The Simple Network Management Protocol (SNMP) allows remote management of network devices. An SNMP community is the group of devices and management station running SNMP. Community names are used to identify groups.

Depending on the level of security required, select the version of SNMP to use.

SNMP v1/v2

Select either SNMP V1 that includes no security, or SNMP v2c that uses very simple security.

The community name can be specified as a password for read or read/write access to all supported SNMP objects. The community is the group of network devices using SNMP. The default password for the **Read Community** is **public** and the default password for the **Write community** is **write**.

Traps for SNMP v1/v2

Traps are used by the camera to send messages to a management system for important events or status changes.

If **Enable traps** is selected, enter the email address where the trap message is to be sent as well as the **Trap community** that should receive the message.

There are four types of traps available for the network camera.

- Cold start
- Warm start
- Link up
- Authentication failed

SNMP v3

SNMP v3 provides encryption and secure passwords. HTTPS must be enabled. To use traps with SNMP v3 an SNMP v3 management application is required.

If the **Enable SNMP v3** option is enabled, provide the Initial user password. Note that the initial password is activated only when HTTPS is enabled and can only be set once.

If HTTPS is enabled, SNMP v1 and SNMP v2c should be disabled.

When SNMP configuration is ready, click **Save** to use the new settings or **Reset** to return to the default values.

UPnP™

The network camera includes support for UPnP™. UPnP™ is enabled by default, and the network camera then is automatically detected by operating systems and clients that support this protocol.

RTP/H.264

These settings are the port range, IP address, port number, and Time-To-Live value to use for the video stream(s) in multicast H.264 format. Only certain IP addresses and port numbers should be used for multicast streams. For more information, please see the online help.

Bonjour

The network camera includes support for Bonjour. When enabled, the camera is automatically detected by operating systems and clients that support this.

Storage

SD Card

The **Disk Management** window is used to set up and manage local storage. it is used to connect memory cards for recording video, monitoring a disk's status, enabling automatic cleanup and preventing the memory card from being overwritten.

Storage Device

Storage device is used to identify and monitor the status of the SD card. it shows the size of the SD card and how much free space is available for storage. It is also used to mount and format SD cards for local storage.

Storage Device Settings

Storage device settings is used to configure removal of recorded video. Automatic disk cleanup can be enabled and set up according to a schedule, and an SD card can be locked to prevent storage removal.

Maintenance

Maintain Server

Restart – The camera is restarted without changing any settings.

Restore – The unit is restarted and most current settings are reset to factory default values. The settings that do not reset are:

- the boot protocol (DHCP or static)
- the static IP address
- the default router
- the subnet mask
- the product interface language
- the system time
- the 802.1x settings

Default – The default button should be used with caution. Pressing this returns the camera's settings to the factory default values (including the IP address).

Dome Status – Click the test button to check the pan, tilt, zoom mechanics and camera for errors. If you receive an error message, contact Axis Customer Services at www.axis.com/techsup

Upgrade Server

See *Upgrading the Firmware*, on page 39.

Support

Support Overview

The **Support Overview** page provides valuable information on troubleshooting and contact information, should you require technical assistance.

System Overview

System Overview is an overview of the camera's status and settings. Information that can be found here includes the camera's firmware version, IP address, security, event and image settings and recent log items. Many of the captions are also links to the proper **Setup** page to conveniently make adjustments in the camera's settings.

Logs & Reports

When contacting Axis support, please be sure to provide a valid Server Report with your query. The Access Log is automatically included in the server report.

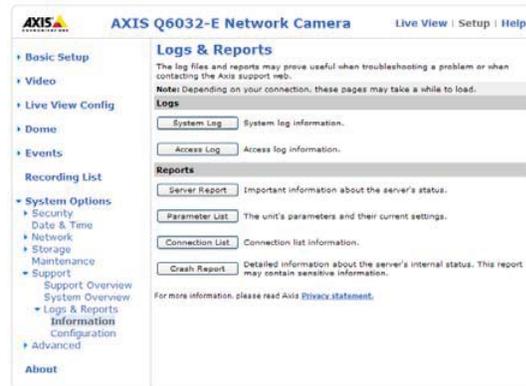
Information

The Server Report and Parameter List may prove useful when troubleshooting a problem or when contacting the Axis support.

- **System Log** – Provides information about system events.
- **Access Log** – By default, the Access Log lists all failed attempts to access the camera but can be configured to list all connections to the camera, whether successful or not. Go to **Support > Logs & Reports > Configuration** and select the desired level of information from the list. See *Configuration*, on page 37 for more information.

The Access Log is useful for various purposes such as tracking all access to the camera, simple web attraction tracking, system analysis and troubleshooting.

- **Server Report** – Provides information about the server status and should always be included when requesting support.
- **Parameter List** – Shows the unit's parameters and their current settings.
- **Connection List** – Lists all clients that are currently accessing video. It is also used for system analysis and troubleshooting.
- **Crash Report** – Generates an archive with debugging information. Note that the report takes several minutes to generate.



Configuration

From the drop-down lists, select the level of information to be added to the **System Log** and **Access Log** files.

The default information level for the Access Log is set to Critical & Warnings, i.e. failed connections. However, in an error situation and when requesting support, set it to the highest information level – Critical & Warnings & Info.

For the Log Level for Email, select from the drop-down list the level of information to send as email and enter the destination email address.

Advanced

Scripting

Scripting is an advanced function that enables you to customize and use scripts.

Caution!

Incorrect scripting may cause unexpected behavior or even cause loss of contact with the unit. If a script does cause problems, reset the unit to its factory default settings. A backup file may be of use to return the unit to its latest configuration.

Axis strongly recommends that you do not use this function unless you understand the consequences. Note that Axis support does not provide assistance for problems with customized scripts.

For more information, please visit the Developer pages at www.axis.com/developer

File upload

Files (e.g. web pages and images) can be uploaded to the network camera and used as custom settings. Uploaded files are accessed through `http://<ip address>/local/<user>/<filename>` where <user> is the selected user access group (viewer, operator or administrator) for the uploaded file.

Plain Config

Plain Config is for the advanced user with experience of Axis network camera configuration. All parameters can be set and modified from this page. Help is available from the standard help pages.

About

Here you can find basic information about your network camera. You can also view third party software licenses.

Resetting to the Factory Default Settings

To reset the camera to the original factory default settings, go to the **System Options > Maintenance** web page (as described in *Maintenance*, on page 36). Alternatively, use the **Control** button and the **Power** button on the side of the camera as described below:

Using the Control button and the Power button

This will reset all parameters, including the IP address, to the Factory Default settings:

1. Remove the dome ring and dome cover, this will automatically disconnect power from the camera.
2. Press and hold the Control button and the Power button at the same time.
3. Continue to hold down the Control button and the Power button until the Status indicator flashes amber (this may take up to 15 seconds).
4. Release the Control button. When the Status indicator changes to green (which may take up to 1 minute) the process is complete and the camera has been reset. The unit now has the default IP address 192.168.0.90

Note:

The Status indicator will display green for 10 seconds only. After that it will be unlit. Refer to the Status indicator table on page 6 for more information.

5. Release the Power button.
6. Replace the dome ring and dome cover, this will automatically reconnect power to the camera.
7. Re-assign the IP address, see the Installation Guide for instructions.

Troubleshooting

Checking the Firmware

Firmware is software that determines the functionality of network cameras. One of your first actions when troubleshooting a problem should be to check the current firmware version. The latest version may contain a correction that fixes your particular problem. The current firmware in your camera is displayed on the page **Setup > Basic Setup** or under **About**.

Upgrading the Firmware

When you upgrade your camera with the latest firmware from the Axis web site, your camera receives the latest available functionality. Always read the upgrade instructions and release notes available with each new release, before updating the firmware.

Note:

Preconfigured and customized settings are retained for use when the new firmware is running (providing that the features are available in the new firmware) although this is not guaranteed by Axis Communications.

1. Save the firmware file to your computer. The latest version of the firmware is available free of charge from the Axis web site at <http://www.axis.com/techsup>
2. Go to **Setup > System Options > Maintenance** in the camera's web pages.
3. In the **Upgrade Server** section, click **Browse** to locate the desired firmware file on your computer. Click **Upgrade**.

Note:

- After starting the upgrade process, you should always wait at least 5-10 minutes before restarting the camera, even if you suspect the upgrade has failed.
- Your dealer reserves the right to charge for any repair attributable to faulty upgrading by the user.
- AXIS Camera Management can be used for multiple upgrades. Please see the Axis website at www.axis.com for more information.



Emergency Recovery Procedure

If power or the network connection to the camera is lost during the upgrade, the process will fail and the unit becomes unresponsive. A flashing red status indicator indicates a failed upgrade. To recover the unit, follow the steps below. The serial number is found on the label on the product casing and is included on an extra label included in the package.

1. **Unix/Linux** - From the command line, type the following:

```
arp -s <IP address of camera> <Serial number> temp
ping -s 408 <IP address of camera>
```

Windows - From a command/DOS prompt, type the following:

```
arp -s <IP address of camera> <Serial number>
ping -l 408 -t <IP address of camera>
```
2. If the unit does not reply within a few seconds, restart it and wait for a reply. Press CTRL+C to stop Ping.
3. Open a browser and type in the camera's IP address. In the page that appears, use the **Browse** button to select the upgrade file to use, for example, axisq6032_e.bin. Then click the **Load** button to restart the upgrade process.
4. After the upgrade is complete (1-10 minutes), the unit automatically restarts and shows a steady green (for about 10 seconds) on the status indicator before returning to its normal unlit status.
5. Reinstall the camera, for more information, see the Installation Guide provided with the product.

If the emergency recovery procedure does not get the camera up and running again, contact Axis support at www.axis.com/techsup

AXIS Support

If you contact Axis Customer Services, please help us to resolve your problems expediently by providing a Server Report and a brief description of the problem.

The Server Report contains important information about the server and its software, as well as a list of the current parameters. The Access log files are also included in the Server Report. Go to **Setup > System Options > Support > Support Overview** to generate a Server Report.

Symptoms, possible causes and remedial actions

Problems setting the IP address	
When using ARP/Ping	Try the installation again. The IP address must be set within two minutes after power has been applied to the camera. Ensure the Ping length is set to 408. See the Installation Guide.
The camera is located on a different subnet	If the IP address intended for the camera and the IP address of your computer are located on different subnets, you will not be able to set the IP address. Contact your network administrator to obtain an appropriate IP address.
The IP address is being used by another device	Disconnect the camera from the network. Run the Ping command (in a Command/DOS window, type ping and the IP address of the unit). If you receive: Reply from <IP address>: bytes = 32; time = 10 ms..... - this means that the IP address may already be in use by another device on your network. You must obtain a new IP address and reinstall the unit. If you receive: Request timed out - this means that the IP address is available for use with your camera. In this case, check all cabling and reinstall the unit.
The camera cannot be accessed from a web browser	
Cannot log in	When HTTPS is enabled, ensure that the correct protocol (HTTP or HTTPS) is used when attempting to log in. You may need to manually type http or https in the browser's address field.
The IP address has been changed by DHCP	If the camera and client are on the same network. Run AXIS IP Utility to locate the camera. Identify the camera using its model or serial number. Alternatively: 1) Move the camera to an isolated network or to one with no DHCP or BOOTP server. Set the IP address again, using AXIS IP Utility or the ARP Ping command. 2) Access the unit and disable BOOTP and DHCP in the TCP/IP settings. Return the unit to the main network. The unit now has a fixed IP address that will not change. 3) As an alternative to 2), if dynamic IP address via DHCP or BOOTP is required, select the required service and then configure IP address change notification from the network settings. Return the unit to the main network. The unit will now have a dynamic IP address, but will notify you if the address changes.
Other networking problems	Test the network cable by connecting it to another network device, then Ping that device from your workstation. See instructions above.
Camera is accessible locally, but not externally	
Broadband router configuration	To configure your broadband router to allow incoming data traffic to the camera, enable the NAT-traversal feature which will attempt to automatically configure the router to allow access to the camera. This is enabled from Setup > System Options > Network > TCP/IP Advanced. Note that the router must support UPnP™.
Firewall protection	Check the Internet firewall with your system administrator.
Default routers required	Check if you need to configure the default router settings.
Problems with the H.264 format	
No H.264 displayed in the client	Check that the correct network interface is selected in the AMC control panel (streaming tab). Check that the relevant H.264 connection methods are enabled in the AMC control panel applet (streaming tab). In the AMC Control Panel, select the H.264 tab and click the button Set to default H.264 decoder.
No multicast H.264 displayed in the client.	Check with your network administrator that the multicast addresses used by the camera are valid for your network. Check with your network administrator to see if there is a firewall preventing viewing.
Multicast H.264 only accessible by local clients.	Check if your router supports multicasting, or if the router settings between the client and the server need to be configured. The TTL (Time To Live) value may need to be increased.
Poor rendering of H.264 images.	Color depth set incorrectly on clients. Set to 16-bit or 32-bit color. In text overlays are blurred, or if there are other rendering problems, you may need to enable Advanced Video Rendering from the H.264 tab in the AMC Control Panel. Ensure that your graphics card is using the latest device driver. The latest drivers can usually be downloaded from the manufacturer's web site.
Color saturation is different in H.264 and Motion JPEG	Modify the settings for your graphics adapter. Please see the adapter's documentation for more information.

Lower frame rate than expected	Reduce number of applications running on the client computer.
	Limit the number of simultaneous viewers.
	Check with the system administrator that there is enough bandwidth available. See also the online help.
	Check in the AMC control panel applet (H.264 tab) that video processing is not set to Decode only I frames.
	Lower the image resolution.
Why do I not get 30 frames per second?	See <i>General performance considerations</i> , on page 46
Image degeneration	Decrease the GOV length, see the online help for more information.
The status indicator flashes red and the camera is inaccessible	
A firmware upgrade has been interrupted or the firmware has in some other way been damaged.	See <i>Emergency Recovery Procedure</i> , on page 39.
No images are displayed on web page	
Problem with AXIS Media Control (<i>Internet Explorer only</i>)	To enable the updating of video images in Internet Explorer, set your browser to allow ActiveX controls. Also, make sure that AXIS Media Control is installed on your workstation.
Installation of additional ActiveX component restricted or prohibited	Configure your camera to use a Java applet for updating the images under Live View Config > Layout > Default Viewer for Internet Explorer. See the online help for more information.
Video/Image problems, general	
Image too dark or too light.	Check the video image settings. See the online help on Video Stream and Camera Settings
Missing images in uploads	This can occur when trying to use a larger image buffer than is actually available. Try lowering the frame rate or the upload period.
Slow image update	Configuring pre-buffers, motion detection, high-resolution images, high frame rates will affect the performance of the camera.
Poor performance	Poor performance may be caused by heavy network traffic, multiple users accessing the unit, low performance clients, use of features such as motion detection, event handling and image rotation other than 180 degrees.
Image not clear	Check that the dome cover is clean. Do <u>not</u> clean a dome cover that looks clean to the eye and never polish the surface. Excessive cleaning can damage the surface. For general cleaning of a dome cover it is recommended to use a non-abrasive, solvent-free neutral soap or detergent with water and a soft cloth. Rinse well with clean lukewarm water. Dry with a soft cloth to prevent water spotting. Never use harsh detergents, gasoline, benzene or acetone etc. and avoid cleaning in direct sunlight or at elevated temperatures.
Poor quality snapshot images	
Screen incorrectly configured on your workstation	In Display Properties, configure your screen to show at least 65000 colors, that is, at least 16-bit. Using only 16 or 256 colors will produce dithering artifacts in the image.
Overlay/Privacy mask is not displayed	
Incorrect size or location of overlay or privacy mask.	The overlay or privacy mask may have been positioned incorrectly or may be too large. Refer to Overlay Image Settings in the online help for more information.
Browser freezes	
Netscape 7.x or Mozilla 1.4 (or later) can sometimes freeze on a slow computer	Lower the image resolution.
Problems uploading files	
Limited space	There is only limited space available for the upload of your own files. Try deleting existing files to free up space.
Motion Detection triggers unexpectedly	
Changes in luminance	Motion detection is based on changes in luminance in the image. This means that if there are sudden changes in the lighting, motion detection may be triggered mistakenly. Lower the sensitivity setting to avoid problems with luminance.
Storage/Disk management problems	
Video cannot be recorded	Check that the SD Card is not write protected (i.e., Read only).
SD Card cannot be mounted	If the SD Card cannot be mounted, reformat it and then click Mount .

For further assistance, please contact your reseller or check the support pages on the Axis web site at www.axis.com/techsup

LED Indicator flash routine

Case	Color	Description
Normal boot sequence	Unlit	Power on RFL check*
	Amber	Kernel booting System initiating
	Green	Shows steady green for 10 sec. for normal operation after restart.
	Unlit	Steady connection/normal operation
Hard Factory Default	Unlit	Power on RFL check*
	Amber	Steady - Kernel booting Flashes - Firmware restore Steady - System initiating
	Green	Shows steady green for 10 sec. for normal operation after restart.
	Unlit	Steady connection/normal operation
Flash Upgrade	Unlit	Steady connection/normal operation
	Amber	Flashes - Firmware upgrade
	Unlit	Reset RFL check*
	Amber	Steady - Kernel booting Flashes - Firmware restore Steady - System initiating
	Green	Shows steady green for 10 sec. for normal operation after restart.
	Unlit	Steady connection/normal operation
No Network	Unlit	Power on RFL check*
	Amber	Kernel booting System initiating
	Amber/red	Flashes - No network
	Green	Shows steady green for 10 seconds for normal operation after restart
	Unlit	Steady connection/normal operation
AXIS DynDNS	Unlit	Steady connection/normal operation
	Green	Flashes- Dyn DNS connecting Steady - DynDNS connection successful
	Unlit	Steady connection/normal operation
Bad Checksum	Red	Flashes - RFL check* failed See <i>Emergency Recovery Procedure</i> , on page 39.

* RFL (Resident Firmware Loader) check is a checksum method used to ensure that the software loading and starting the firmware works correctly.

Technical Specifications

Function/group	Item	Specification
Camera	Models	AXIS Q6032-E 60 Hz AXIS Q6032-E 50 Hz
	Image sensor	1/4" ExView HAD Progressive Scan CCD
	Lens	<ul style="list-style-type: none"> • f 3.4 mm – 119 mm • F1.4 – 4.2 • Autofocus • Automatic day and night functionality • Horizontal angle of view: 55.8° - 1.7°
	Light sensitivity	<ul style="list-style-type: none"> • Color: 0.5 lux at 30 IRE F1.4 • B/W: 0.008 lux at 30 IRE F1.4
	Shutter time	<ul style="list-style-type: none"> • 60 Hz: 1/30 000 s – 0.5 s • 50 Hz: 1/30 000 s – 1.5 s
	Pan/Tilt/Zoom	<ul style="list-style-type: none"> • E-flip • 100 preset positions • Pan: 360° endless, 0.05 – 450°/s • Tilt: 220°, 0.05 – 450°/s • 35x optical zoom and 12x digital zoom, total 420x zoom
	Pan/Tilt/Zoom functionalities	<ul style="list-style-type: none"> • Guard Tour • Control queue • On-screen directional indicator
Video	Video compression	<ul style="list-style-type: none"> • H.264 (MPEG-4 Part 10/AVC) • Motion JPEG
	Resolutions	60 Hz: 704x480 to 176x120 50 Hz: 704x576 to 176x144
	Frame rate H.264	Up to 30/25fps (60/50 Hz) in all resolutions
	Frame rate Motion JPEG	Up to 30/25fps (60/50 Hz) in all resolutions
	Video streaming	<ul style="list-style-type: none"> • Multiple, individually configurable streams in H.264 and Motion JPEG • Controllable frame rate and bandwidth • VBR/CBR H.264
	Image settings	<ul style="list-style-type: none"> • Wide Dynamic Range (WDR), Electronic Image Stabilization (EIS), manual shutter time, compression, color, brightness, contrast, sharpness, white balance, exposure control, exposure zones, backlight compensation, fine tuning of behavior at low light, aspect ratio correction • Rotation 0°, 180° • Text and image overlay • Privacy mask • Image freeze on PTZ
	Users	<ul style="list-style-type: none"> • 20 simultaneous users • Unlimited number of users using multicast (H.264/MPEG-4)
Network	Security	Password protection, IP address filtering, HTTPS encryption, IEEE 802.1X network access control, digest authentication, user access log
	Supported protocols	IPv4/v6, HTTP, HTTPS, SSL/TLS, QoS Layer 3 DiffServ, FTP, SMTP, Bonjour, UPnP, SNMPv1/v2c/v3(MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, etc.* *This product includes software developed by the Open SSL Project for use in the Open SSL Tool kit (www.openssl.org)

AXIS Q6032-E – Technical Specifications

Function/group	Item	Specification
System Integration	Application Programming Interface	Open API for software integration, including VAPIX® from Axis Communications, specification available at www.axis.com
	Intelligent Video	Video motion detection, auto tracking
	Alarm triggers	Video motion detection, PTZ position, memory card full, auto tracking, manual trigger, on boot, fan malfunction
	Alarm events	<ul style="list-style-type: none"> • File upload via FTP, HTTP and email • Notification via email, HTTP and TCP • PTZ position • Local storage • Guard Tour • Auto tracking
	Video buffer	56 MB pre- and post alarm
	Video access from web browser	<ul style="list-style-type: none"> • Camera live view • Video recording to file (ASF) • Sequence tour for up to 20 Axis video sources, • Windows Vista, XP, 2000, 2003 server • DirectX 9c or higher • For other operating systems and browsers see www.axis.com/techsup
	Installation, management and maintenance	<ul style="list-style-type: none"> • AXIS Camera Management tool on CD and web-based configuration • Configuration of backup and restore • Firmware upgrades over HTTP or FTP, firmware available at www.axis.com
General	Casing	IP66-rated and NEMA 4X-rated metal casing (aluminum) Acrylic (PMMA) clear dome cover Sunshield (PC/ASA)
	Processors, memory	ARTPEC-3, 128 MB RAM, 128 MB Flash
	Power	<ul style="list-style-type: none"> • Camera: High Power over Ethernet, max 50 W • Midspan (included): AXIS T8124 High Power over Ethernet Midspan 1-port 60 W, 100-240 V AC, max 74 W
	Connectors	<ul style="list-style-type: none"> • RJ-45 Ethernet 10BASE-T/100BASE-TX • IP66-rated RJ-45 connector kit included
	Local storage	SD/SDHC memory card slot (card not included)
	Operating conditions	<ul style="list-style-type: none"> • Operating conditions camera unit -40 °C to 50 °C (-40 °C to 122 °F) Arctic Temperature Control enables camera start-up at temperatures as low as -40 °C (-40 °F) • Operating conditions midspan Full power 60W: -10 °C to 45 °C (heater in camera unit active) Half power 30W: -10 °C to 55 °C (heater in camera unit inactive) • Humidity up to 93% RH (non-condensing)
	Storage conditions	<ul style="list-style-type: none"> • Storage conditions camera unit -40 °C to 60 °C (-40 °F to 140 °F)
	Approvals	<ul style="list-style-type: none"> • EN 55022 Class B, EN 61000-3-2, EN 61000-3-3, EN 61000-6-1, EN 61000-6-2, EN 55024, FCC Part 15 Subpart B Class B, ICES-003 Class B, VCCI Class B, C-tick AS/NZS CISPR 22, KCC Class B • IEC 60529 IP66 • IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-78, IEC 60068-2-14, IEC 60068-2-30, IEC 60068-2-6, IEC 60068-2-27, IEC 60068-2-60 • ISO 4892-2 • Midspan: EN 60950-1, GS, UL, cUL, CE, VCCI, CB, KCC, CSA, UL-AR
	Dimensions (HxWxD)	235 mm x 230 mm x 230 mm (9.3" x 9.1" x 9.1")
	Weight	<ul style="list-style-type: none"> • 3.5 kg (7.7 lb.)

Function/group	Item	Specification
	Included accessories	AXIS T8124 High PoE Midspan 1-port, IP66-rated RJ-45 connector kit, IP66-rated RJ45 connector kit, clear and smoked dome cover, sunshield, Installation Guide, CD with User's Manual, recording software, installation and management tools, Windows decoder 1-user license
	Video management software (not included)	AXIS Camera Station – Video management software for viewing and recording up to 50 cameras See www.axis.com/products/video/software/ for more software applications via partners
	Optional accessories	<ul style="list-style-type: none"> • AXIS T91A Mounting accessories • AXIS T8310 Video Surveillance Control Board • AXIS Camera Station • AXIS T90A Illuminators • Multi-user decoder license pack

General performance considerations

When setting up your system, it is important to consider how various settings and situations will affect performance. Some factors affect the amount of bandwidth (the bit rate) required, others can affect the frame rate, and some affect both. If the load on the CPU reaches its maximum, this will also affect the frame rate.

The following factors are among the most important to consider:

- High image resolutions and/or lower compression levels result in larger images. Bandwidth affected.
- Access by large numbers of Motion JPEG and/or unicast H.264 clients. Bandwidth affected.
- Simultaneous viewing of different streams (resolution, compression) by different clients. Effect on frame rate and bandwidth.
- Accessing both Motion JPEG and H.264 video streams simultaneously. Frame rate and bandwidth affected.
- Heavy usage of event settings affects the camera's CPU load. Frame rate affected.
- Enabled motion detection. Frame rate and bandwidth affected.
- Heavy network utilization due to poor infrastructure. Bandwidth affected.
- Viewing on poorly performing client PCs lowers perceived performance. Frame rate affected.

Glossary of Terms

ActiveX – A standard that enables software components to interact with one another in a networked environment, regardless of the language(s) used to create them. Web browsers may come into contact with ActiveX controls, ActiveX documents, and ActiveX scripts. ActiveX controls are often downloaded and installed automatically as required.

Angle – The field of view, relative to a standard lens in a 35mm still camera, expressed in degrees, e.g. 30°. For practical purposes, this is the area that a lens can cover, where the angle of view is determined by the focal length of the lens. A wide-angle lens has a short focal length and covers a wider angle of view than standard or telephoto lenses, which have longer focal lengths.

ARP (Address Resolution Protocol) – This protocol is used to associate an IP address to a hardware MAC address. A request is broadcast on the local network to discover the MAC address for an IP address.

ARTPEC (Axis Real Time Picture Encoder) – This chip is used for image compression.

ASIC (Application Specific Integrated Circuit) – A circuit designed for a specific application, as opposed to a general purpose circuit, such as a microprocessor.

Aspect ratio – A ratio of width to height in images. A common aspect ratio used for television screens and computer monitors is 4:3. High-definition television (HDTV) uses an aspect ratio of 16:9.

Autoiris (DC-Iris) – This special type of iris is electrically controlled by the camera, to automatically regulate the amount of light allowed to enter.

Bitmap – A bitmap is a data file representing a rectangular grid of pixels. It defines a display space and color for each pixel (or 'bit') in the display space. This type of image is known as a 'raster graphic.' GIFs and JPEGs are examples of image file types that contain bitmaps.

Because a bitmap uses this fixed raster method, it cannot easily be rescaled without losing definition. Conversely, a vector graphic image uses geometrical shapes to represent the image, and can thus be quickly rescaled.

Bit rate – The bit rate (in kbit/s or Mbit/s) is often referred to as speed, but actually defines the number of bits/time unit and not distance/time unit.

Bonjour – Also known as zero-configuration networking, Bonjour enables devices to automatically discover each other on a network, without having to enter IP addresses or configure DNS servers. Bonjour is a trademark of Apple Computer, Inc.

Broadband – In network engineering terms, this describes transmission methods where two or more signals share the same carrier. In more popular terminology, broadband is taken to mean high-speed data transmission.

CCD (Charged Coupled Device) – This light-sensitive image device used in many digital cameras is a large integrated circuit that contains hundreds of thousands of photo-sites (pixels)

that convert light energy into electronic signals. Its size is measured diagonally and can be 1/4", 1/3", 1/2" or 2/3".

CGI (Common Gateway Interface) – A specification for communication between a web server and other (CGI) programs. For example, a HTML page that contains a form might use a CGI program to process the form data once it is submitted.

CIF (Common Intermediate Format) – CIF refers to the analog video resolutions 352x288 pixels (PAL) and 352x240 pixels (NTSC). See also *Resolution*.

Client/Server – Client/server describes the relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfils the request. Typically, multiple client programs share the services of a common server program. A web browser is a client program that requests services (the sending of web pages or files) from a web server.

CMOS (Complementary Metal Oxide Semiconductor) – A CMOS is a widely used type of semiconductor that uses both negative and positive circuits. Since only one of the circuit types is on at any given time, CMOS chips require less power than chips using just one type of transistor. CMOS image sensors also allow processing circuits to be included on the same chip, an advantage not possible with CCD sensors, which are also much more expensive to produce.

Codec – In communications engineering, a codec is usually a coder/decoder. Codecs are used in integrated circuits or chips that convert e.g. analog video and audio signals into a digital format for transmission. The codec also converts received digital signals back into analog format. A codec uses analog-to-digital conversion and digital-to-analog conversion in the same chip.

Codec can also mean compression/decompression, in which case it is generally taken to mean an algorithm or computer program for reducing the size of large files and programs.

Compression – See *Image compression*.

CVBS – analog video format (composite video).

DC-Iris (Autoiris) – This special type of iris is electrically controlled by the camera, to automatically regulate the amount of light allowed to enter.

DHCP (Dynamic Host Configuration Protocol) – DHCP is a protocol that lets network administrators automate and centrally manage the assignment of Internet Protocol (IP) addresses to network devices in a network.

DHCP uses the concept of a 'lease' or amount of time that a given IP address will be valid for a computer. The lease time can vary, depending on how long a user is likely to require the network connection at a particular location.

DHCP also supports static addresses for e.g. computers running web servers, which need a permanent IP address.

DNS (Domain Name System) – DNS is used to locate and translate Internet domain names into IP (Internet Protocol) addresses. A domain name is a meaningful and easy-to-remember name for an Internet address. For example the domain name www.example.com is much easier to

remember than 192.0.34.166. The translation tables for domain names are contained in Domain name servers.

Domain Server – Domains can also be used by organizations who wish to centralize the management of their (Windows) computers. Each user within a domain has an account that usually allows them to log in to and use any computer in the domain, although restrictions may also apply. The domain server is the server that authenticates the users on the network.

Duplex – See *Full-duplex*.

Ethernet – Ethernet is the most widely installed local area network technology. An Ethernet LAN typically uses special grades of twisted pair wires. The most commonly installed Ethernet systems are 10BASE-T and 100BASE-T10, which provide transmission speeds up to 10 Mbps and 100 Mbps respectively.

ETRAX (Ethernet Token Ring AXIS) – Axis' own microprocessor.

Factory default settings – These are the settings that originally applied for a device when it was first delivered from the factory. If it should become necessary to reset a device to its factory default settings, this will, for many devices, completely reset any settings that were changed by the user.

Firewall – A firewall works as a barrier between networks, e.g. between a Local Area Network and the Internet. The firewall ensures that only authorized users are allowed to access the one network from the other. A firewall can be software running on a computer, or it can be a standalone hardware device.

Focal length – Measured in millimeters, the focal length of a camera lens determines the width of the horizontal field of view, which in turn is measured in degrees.

FTP (File Transfer Protocol) – An application protocol that uses the TCP/IP protocols. It is used to exchange files between computers/devices on networks.

Frame – A frame is a complete video image. In the 2:1 interlaced scanning format of the RS-170 and CCIR formats, a frame is made up of two separate fields of 262.5 or 312.5 lines interlaced at 60 or 50 Hz to form a complete frame, which appears at 30 or 25 Hz. In video cameras with a progressive scan, each frame is scanned line-by-line and not interlaced; most are also displayed at 30 and 25 Hz.

Frame rate – The frame rate used to describe the frequency at which a video stream is updated is measured in frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

Full-duplex – Transmission of data in two directions simultaneously. In an audio system this would describe e.g. a telephone systems. Half-duplex also provides bi-directional communication, but only in one direction at a time, as in a walkie-talkie system. See also *Simplex*.

Gain – Gain is the amplification factor and the extent to which an analog amplifier boosts the strength of a signal. Amplification factors are usually expressed in terms of power. The decibel (dB) is the most common way of quantifying the

gain of an amplifier.

Gateway – A gateway is a point in a network that acts as an entry point to another network. In a corporate network for example, a computer server acting as a gateway often also acts as a proxy server and a firewall server. A gateway is often associated with both a router, which knows where to direct a given packet of data that arrives at the gateway, and a switch, which furnishes the actual path in and out of the gateway for a given packet.

GIF (Graphics Interchange Format) – GIF is one of the most common file formats used for images in web pages. There are two versions of the format, 87a and 89a. Version 89a supports animations, i.e. a short sequence of images within a single GIF file. A GIF89a can also be specified for interlaced presentation.

GOV (Group Of VOPs) – A group of VOPs is the basic unit of an H.264 video stream. The GOV contains different types and numbers of VOPs (I-VOPs, P-VOPs) as determined by the GOV length and GOV structure. See also *VOP*.

GOV length – The GOV length determines the number of images (VOPs) in the GOV structure. See also *GOV* and *VOP*.

GOV structure – The GOV structure describes the composition of an H.264 video stream, as regards the type of images (I-VOPs or P-VOPs) included in the stream, and their internal order. See also *GOV* and *VOP*.

H.264 – A standard for video compression, also known as MPEG-4 Part 10.

Half-duplex – See *Full-duplex*.

HDTV – High-definition television, high resolution digital video.

HTML (Hypertext Markup Language) – HTML is the set of "markup" symbols or codes inserted in a file intended for display in web browser. The markup tells the browser how to display the page's words and images for the user.

HTTP (Hypertext Transfer Protocol) – HTTP is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the web. The HTTP protocol runs on top of the TCP/IP suite of protocols.

Hub – A (network) hub is used to connect multiple devices to the network. The hub transmits all data to all devices connected to it, whereas a switch will only transmit the data to the device it is specifically intended for.

IEEE 802.11 – A family of standards for wireless LANs. The 802.11 standard supports 1 or 2 Mbit/s transmission on the 2.4 GHz band. IEEE 802.11b specifies an 11 Mbit/s data rate on the 2.4 GHz band, while 802.11a allows up to 54 Mbit/s on the 5 GHz band.

Image compression – Image compression minimizes the file size (in bytes) of an image. Two of the most common compressed image formats are JPEG and GIF.

Interlacing – Interlaced video is video captured at 50 pictures (known as fields) per second, of which every 2 consecutive fields (at half height) are then combined into 1 frame.

Interlacing was developed many years ago for the analog TV world and is still used widely today. It provides good results when viewing motion in standard TV pictures, although there is always some degree of distortion in the image.

To view interlaced video on e.g. a computer monitor, the video must first be de-interlaced, to produce progressive video, which consists of complete images, one after the other, at 25 frames per second. See also *Progressive scan*.

IP (Internet Protocol) – The Internet Protocol is a method transmitting data over a network. Data to be sent is divided into individual and completely independent "packets." Each computer (or host) on the Internet has at least one address that uniquely identifies it from all others, and each data packet contains both the sender's address and the receiver's address.

The Internet Protocol ensures that the data packets all arrive at the intended address. As IP is a connectionless protocol, which means that there is no established connection between the communication end-points, packets can be sent via different routes and do not need to arrive at the destination in the correct order.

Once the data packets have arrived at the correct destination, another protocol – Transmission Control Protocol (TCP) – puts them in the right order. See also *TCP*.

IP Address – An IP address is simply an address on an IP network used by a computer/device connected to that network. IP addresses allow all the connected computers/devices to find each other and to pass data back and forth.

To avoid conflicts, each IP address on any given network must be unique. An IP address can be assigned as fixed, so that it does not change, or it can be assigned dynamically (and automatically) by DHCP.

An IP address consists of four groups (or quads) of decimal digits separated by periods, e.g. 130.5.5.25. Different parts of the address represent different things. Some part will represent the network number or address, and some other part will represent the local machine address.

See also *IP (Internet Protocol)*.

I-VOP – See *VOP*.

JPEG (Joint Photographic Experts Group) – Together with the GIF file format, JPEG is an image file type commonly used on the web. A JPEG image is a bitmap, and usually has the file suffix '.jpg' or '.jpeg.' When creating a JPEG image, it is possible to configure the level of compression to use. As the lowest compression (i.e. the highest quality) results in the largest file, there is a trade-off between image quality and file size.

kbit/s (kilobits per second) – A measure of the bit rate, i.e. the rate at which bits are passing a given point. See also *Bit rate*.

LAN (Local Area Network) – A LAN is a group of computers and associated devices that typically share common resources within a limited geographical area.

Linux – Linux is an open source operating system within the UNIX family. Because of its robustness and availability, Linux has won popularity in the open source community and among commercial application developers.

Local storage – If a camera or video encoder supports local

storage, an SD card can be inserted into the SD card slot to locally record and store a video stream.

MAC address (Media Access Control address) – A MAC address is a unique identifier associated with a piece of networking equipment, or more specifically, its interface with the network. For example, the network card in a computer has its own MAC address.

Manual iris – This is the opposite to an autoiris, i.e. the camera iris must be adjusted manually to regulate the amount of light allowed to reach the image sensor.

Mbit/s (Megabits per second) – A measure of the bit rate, i.e. the rate at which bits are passing a given point. Commonly used to give the 'speed' of a network. A LAN might run at 10 or 100 Mbit/s. See also *Bit rate*.

Monitor – A monitor is very similar to a standard television set, but lacks the electronics to pick up regular television signals.

Motion JPEG – Motion JPEG is a simple compression/decompression technique for networked video. Latency is low and image quality is guaranteed, regardless of movement or complexity of the image. Image quality is controlled by adjusting the compression level, which in turn provides control over the file size, and thereby the bit rate.

High-quality individual images from the Motion JPEG stream are easily extracted. See also *JPEG*.

Megapixel – See *Pixel*.

MPEG (Moving Picture Experts Group) – The Moving Picture Experts Group develops standards for digital video and audio compression. It operates under the auspices of the International Organization for Standardization (ISO). The MPEG standards are an evolving series, each designed for a different purpose.

MPEG-2 – MPEG-2 is the designation for a group of audio and video coding standards, and is typically used to encode audio and video for broadcast signals, including digital satellite and Cable TV. MPEG-2, with some modifications, is also the coding format used by standard commercial DVD movies.

Multicast – Bandwidth-conserving technology that reduces bandwidth usage by simultaneously delivering a single stream of information to multiple network recipients.

Network connectivity – The physical (wired or wireless) and logical (protocol) connection of a computer network or an individual device to a network, such as the Internet or a LAN.

NTSC (National Television System Committee) – NTSC is the television and video standard in the United States. NTSC delivers 525 lines at 60 half-frames/second.

NWay – A network protocol that automatically negotiates the highest possible common transmission speed between two devices.

PAL (Phase Alternating Line) – PAL is the dominant television standard in Europe. PAL delivers 625 lines at 50 half-frames/second.

Ping – Ping is a basic network program used diagnostically to

check the status of a network host or device. Ping can be used to see if a particular network address (IP address or host name) is occupied or not, or if the host at that address is responding normally. Ping can be run from e.g. the Windows Command prompt or the command line in UNIX.

Pixel – A pixel is one of the many tiny dots that make up a digital image. The color and intensity of each pixel represents a tiny area of the complete image.

PoE (Power over Ethernet) – Power over Ethernet provides power to a network device via the same cable as used for the network connection. This is very useful for IP-Surveillance and remote monitoring applications in places where it may be too impractical or expensive to power the device from a power outlet.

PPP (Point-to-Point Protocol) – A protocol that uses a serial interface for communication between two network devices. For example, a PC connected by a phone line to a server.

PPTP (Point-to-Point Tunneling Protocol) – A protocol (set of communication rules) that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. In this way a corporation can effectively use a WAN (Wide Area Network) as a large single LAN (Local Area Network). This kind of interconnection is known as a virtual private network (VPN).

Pre/post alarm images – The images from immediately before and after an alarm. These images are stored in a buffer for later retrieval.

Progressive scan – Progressive scan, as opposed to interlaced video, scans the entire picture, line by line every sixteenth of a second. In other words, captured images are not split into separate fields as in interlaced scanning.

Computer monitors do not need interlace to show the picture on the screen, but instead show them progressively, on one line at a time in perfect order, i.e. 1, 2, 3, 4, 5, 6, 7 etc., so there is virtually no 'flickering' effect. In a surveillance application, this can be critical when viewing detail within a moving image, such as a person running. A high-quality monitor is required to get the best from progressive scan. See also *Interlacing*.

Protocol – A special set of rules governing how two entities will communicate. Protocols are found at many levels of communication, and there are hardware protocols and software protocols.

Proxy server – In an organization that uses the Internet, a proxy server acts as an intermediary between a workstation user and the Internet. This provides security, administrative control, and a caching service. Any proxy server associated with a gateway server, or part of a gateway server, effectively separates the organization's network from the outside network and the local firewall. It is the firewall server that protects the network against outside intrusion.

A proxy server receives requests for Internet services (such as web page requests) from many users. If the proxy server is also a cache server, it looks in its local cache of previously downloaded web pages. If it finds the page, it is returned to the user without forwarding the request to the Internet. If the page is not in the cache, the proxy server, acting as a client on behalf of the user, uses one of its own IP addresses to request the page

from another server over the Internet. When the requested page is returned, the proxy server forwards it to the user that originally requested it.

P-VOP – See *VOP*.

Resolution – Image resolution is a measure of how much detail a digital image can hold: the greater the resolution, the greater the level of detail. Resolution can be specified as the number of pixel-columns (width) by the number of pixel-rows (height), e.g. 320x240.

Alternatively, the total number of pixels (usually in megapixels) in the image can be used. In analog systems it is also common to use other format designations, such as CIF, QCIF, 4CIF, etc.

RTCP (Real-Time Control Protocol) – RTCP provides support for real-time conferencing of groups of any size within an intranet. This support includes source identification and support for gateways like audio and video bridges as well as multicast-to-unicast translators.

RTCP offers quality-of-service feedback from receivers to the multicast group as well as support for the synchronization of different media streams.

RTP (Real-Time Transport Protocol) – RTP is an Internet protocol for the transport of real-time data, e.g. audio and video. It can be used for media-on-demand as well as interactive services such as Internet telephony.

RTSP (Real Time Streaming Protocol) – RTSP is a control protocol, and a starting point for negotiating transports such as RTP, multicast and Unicast, and for negotiating codecs.

RTSP can be considered a 'remote control' for controlling the media stream delivered by a media server. RTSP servers typically use RTP as the protocol for the actual transport of audio/video data.

Router – A device that determines the next network point to which a packet should be forwarded on its way to its final destination. A router creates and/or maintains a special routing table that stores information on how best to reach certain destinations. A router is sometimes included as part of a network switch. See also *switch*.

Server – In general, a server is a computer program that provides services to other computer programs in the same or other computers. A computer running a server program is also frequently referred to as a server. In practice, the server may contain any number of server and client programs. A web server is the computer program that supplies the requested HTML pages or files to the client (browser).

Sharpness – This is the control of fine detail within a picture. This feature was originally introduced into color TV sets that used notch filter decoders. This filter took away all high frequency detail in the black and white region of the picture. The sharpness control attempted to put some of that detail back in the picture. Sharpness controls are mostly superfluous in today's high-end TVs. The only logical requirement for it nowadays is on a VHS machine.

Simplex – In Simplex operation, a network cable or communications channel can only send information in one direction.

SMTP (Simple Mail Transfer Protocol) – SMTP is used for sending and receiving e-mail. However, as it is 'simple,' it is limited in its ability to queue messages at the receiving end, and is usually used with one of two other protocols, POP3 or IMAP. These other protocols allow the user to save messages in a server mailbox and download them periodically from the server.

SMTP authentication is an extension of SMTP, whereby the client is required to log into the mail server before or during the sending of email. It can be used to allow legitimate users to send email while denying the service to unauthorized users, such as spammers.

SNMP (Simple Network Management Protocol) – SNMP forms part of the Internet Protocol suite, as defined by the Internet Engineering Task Force. The protocol can support monitoring of network-attached devices for any conditions that warrant administrative attention.

Sockets – Sockets are a method for communication between a client program and a server program over a network. A socket is defined as 'the endpoint in a connection.' Sockets are created and used with a set of programming requests or 'function calls' sometimes called the sockets application programming interface (API).

SSL/TSL (Secure Socket Layer/Transport Layer Security)
These two protocols (SSL is succeeded by TSL) are cryptographic protocols that provide secure communication on a network. SSL is commonly used over HTTP to form HTTPS, as used e.g. on the Internet for electronic financial transactions. SSL uses public key certificates to verify the identity of the server.

Subnet/subnet mask – A subnet is an identifiably separate part of an organization's network. Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network (LAN). Having an organization's network divided into subnets allows it to be connected to the Internet with a single shared network address.

The subnet mask is the part of the IP address that tells a network router how to find the subnet that the data packet should be delivered to. Using a subnet mask saves the router having to handle the entire 32-bit IP address; it simply looks at the bits selected by the mask.

Switch – A switch is a network device that connects network segments together, and which selects a path for sending a unit of data to its next destination. In general, a switch is a simpler and faster mechanism than a router, which requires knowledge about the network and how to determine the route. Some switches include the router function. See also *Router*.

TCP (Transmission Control Protocol) – TCP is used along with the Internet Protocol (IP) to transmit data as packets between computers over the network. While IP takes care of the actual packet delivery, TCP keeps track of the individual packets that the communication (e.g. requested a web page file) is divided into, and, when all packets have arrived at their destination, it reassembles them to re-form the complete file.

TCP is a connection-oriented protocol, which means that a connection is established between the two end-points and is maintained until the data has been successfully exchanged between the communicating applications.

Telnet – Telnet is a simple method with which to access

another network device, e.g. a computer. The HTTP protocol and the FTP protocols allow you to request specific files from remote computers, but do not allow you logon as a user of that computer. With Telnet, you log on as a regular user with whatever privileges you may have been granted for specific applications and data residing on that computer.

UDP (User Datagram Protocol) – UDP is a communications protocol that offers limited service for exchanging data in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP). The advantage of UDP is that it is not required to deliver all data and may drop network packets when there is e.g. network congestion. This is suitable for live video, as there is no point in re-transmitting old information that will not be displayed anyway.

Unicast – Communication between a single sender and a single receiver over a network. A new connection is established for each new user.

URL (Uniform Resource Locator) – An "address" on the network.

Varifocal lens – A varifocal lens provides a wide range of focal lengths, as opposed to a lens with a fixed focal length, which only provides one.

VPN (Virtual Private Network) – This creates a secure "tunnel" between the points within the VPN. Only devices with the correct "key" will be able to work within the VPN. The VPN network can be within a company LAN (Local Area Network), but different sites can also be connected over the Internet in a secure way. One common use for VPN is for connecting a remote computer to the corporate network, via e.g. a direct phone line or via the Internet.

VOP (Video Object Plane) – A VOP is an image frame in an H.264 video stream. There are several types of VOP:

- An I-VOP is complete image frame.

- A P-VOP codes the differences between images, as long as it is more efficient to do so. Otherwise it codes the whole image, which may also be a completely new image.

WAN (Wide-Area-Network) – Similar to a LAN, but on a larger geographical scale.

W-LAN (Wireless LAN) – A wireless LAN is a wireless local area network that uses radio waves as its carrier: where the network connections for end-users are wireless. The main network structure usually uses cables.

Web server – A web server is a program, which allows web browsers to retrieve files from computers connected to the Internet. The web server listens for requests from web browsers and upon receiving a request for a file sends it back to the browser.

The primary function of a web server is to serve pages to other remote computers; consequently, it needs to be installed on a computer that is permanently connected to the Internet. It also controls access to the server whilst monitoring and logging server access statistics.

WEP (Wireless Equivalent Privacy) – A wireless security protocol, specified in the IEEE 802.11 standard, which is

designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to that usually expected of a wired LAN. Security is at two different levels; 40-bit and 128-bit encryption. The higher the bit number, the more secure the encryption.

WPA-PSK (Wi-Fi Protected Access – Pre-Shared Key) – This wireless encryption method uses a pre-shared key (PSK) for key management. Keys can usually be entered as manual hex values, as hexadecimal characters, or as a Passphrase. WPA-PSK provides a greater degree of security than WEP.

YPbPr – analog video signal for component video.

Zoom lens – A zoom lens can be moved (zoomed) to enlarge the view of an object to show more detail.

Index

A

Access Log 37
 Action Buttons 9, 19
 Administrator 13, 29
 Alarm 26
 AMC 7
 ARP/Ping 32
 Auto Tracking 24
 AXIS Media Control viewer toolbar 9

B

Backlight compensation 16
 Backup 36
 Bit Rate 15
 Bonjour 7, 35
 Brightness 16
 Buffer Size 24
 Buffers 24

C

Camera tampering 25
 CGI link 19
 Color level 16
 Connection List 37
 Constant Bit Rate 15
 Contrast 16
 Control button 38
 Control Queue 22

D

Date & Time 31
 Default Viewer 18
 Disk full 24
 Disk Management 35
 DNS Configuration 32
 DNS Server 32
 Domain Name 32

E

Emergency recovery 39
 Enable ARP/Ping 32
 Event Servers 23
 Event Types 23
 Events 23
 Exposure control 16
 Exposure zones 16

F

Factory Default Settings 38
 Fan 9, 24
 Firmware 39
 Frame Rate 14
 FTP 33
 FTP Server 23

G

GOV Settings 15
 Guard Tour 21

H

H.264 14, 15
 Heater 9
 Host Name 32
 HTTP Server 23
 HTTPS 8, 29, 33

I

IEEE 802.1X 30
 Image freeze on PTZ 17
 IP Address Filtering 29
 IPv4 31, 33
 IPv6 32
 IR cut filter 17

L

LED 43
 LED Indicator 6, 43
 Live View 9
 Live View Config 18
 Local storage 4
 Logs & Reports 37

M

Mask 17
 MJPEG 14, 15
 Motion Detection 26
 Motion detection 24
 Move speed 21

N

NAT traversal 8, 33
 Network Settings 31
 NTP Configuration 32
 NTP Server 31

O

Operator 29
 OSDI Zones 21
 Overlay Settings 14

P

Pan Tilt Zoom 24
 Pan/Tilt/Zoom Controls 10
 Parameter List 37
 Password Settings 29
 Port Status 28
 Post-trigger Buffer 24
 Preset positions 20
 Pre-trigger Buffer 24
 Proportional speed 22
 PTZ (Pan Tilt Zoom) 20
 PTZ control panel 10

Q

QoS 34
QuickTime 11, 18

R

Recording List 28
Recovery 39
Referrals 29
Restore 36
RTSP 34

S

Scheduled Event 25
Security 29
Self-signed certificate 8
Server Report 37
Server Time 31
Sharpness 16
SMTP 34
Snapshot button 9
SNMP 34
Stabilizer 17
Storage 35
Storage Device 35
Support 36, 40
System Log 37
System Options 29

T

TCP Server 23
TCP/IP Settings 31
Time Mode 31
Troubleshooting 39

U

Upgrade Server 36
UPnP 33, 35
Users 29

V

VAPIX 19, 22
Variable Bit Rate 15
Video Stream 14
Viewer 29

W

White balance 16
Wide dynamic range 16



&



ASTI Transportation Systems, Inc.
CHIPS
Computerized Highway Information Processing System

May 2013

ASTI Transportation Systems, Inc.
18 Blevins Drive
New Castle, DE 19720

CONTENTS

I.	Introduction to Smart Work Zone Systems, Real Time Traffic Management Systems and Temporary ITS Systems	
1.1	Introduction to ASTI.....	3
1.2	Company Description.....	4
1.3	Project Roles and Organization Chart.....	5
II.	Benefits of RTTMS, SWZS and Temporary ITS Systems	
2.1	Enhanced Safety within the Work Zone.....	6
2.2	Financial Impacts.....	7
2.3	Increased Mobility.....	8
2.4	Public Perception.....	8
III.	The System	
3.1	System Overview.....	9-14
3.2	The Hardware.....	9-14
3.3	The Software.....	9-14
3.4	Web Based Solution.....	9-14
IV.	High Project Experience	
4.1	The “Carnageddon” I-405 in Los Angeles.....	14
4.2	Super Bridges I93FAST14 in Boston.....	15
4.3	The I-595 Express Corridor in Fort Lauderdale.....	15
4.4	The I-93 Corridor SWZS in New Hampshire.....	16

I. Introduction to Smart Work Zone Systems, Real Time Traffic Management Systems and Temporary ITS Systems

1.1 Introduction to ASTI Transportation Systems, Inc.

ASTI Transportation Systems, Inc. is one of the original suppliers of the Smart Work Zone System in the United States. Since incorporation back in 1991, ASTI has been a premier provider of various sensor types as well as multiple notification systems based on some form of a data collection device. Originally Advanced Sensor Technologies Incorporated, ASTI started by supplying meteorological equipment to the smaller airports, Coast Guard, and other industrial companies. Other instrumentation included visibility ceilometers, transmissometers using forward and/or back scatter technology.

It was these technologies that led to the Georgia Fog Project with the University of Florida where they were looking to put visibility protection on the stretch of I-95 between Georgia and Florida. There were numerous fatalities as a result of the continuing fog concerns. ASTI was then able to redesign the meteorological equipment to utilize the existing technology to scale back and accommodate the needs of the highway. This then spread to as far as Puerto Rico with a project on Route 10. This was the beginning of ASTI's move into the highway market.

By 1993, Advanced Sensor Technologies Incorporated reincorporated as ASTI Transportation Systems, Inc. to better serve the highway industry. This moved ASTI into a system approach thus moving away from the sensor approach.

ASTI entered the ITS market when ITS America was still under IVHS or Intelligent Vehicle Highway Society of America.

ASTI started doing pilot projects with FHWA's Strategic Highway Research Program or SHRP. This program requested the ability to capture over-height vehicles entering the highway through the use of a sensor technology. It was requested that vehicles be detected over the legal of 13 feet 6 inches. ASTI trademarked the "Safety Pass" which was capable of capturing vehicles that hit these limits. It was these types of pilot projects that led to the introduction of the "Queue Trailer".

The ASTI Queue Trailer started off as a side fire collection device. This device was being utilized to collect the pertinent data. However, it was being utilized in a transmitter and receiver type of setting. This required sensors on both sides of the highway which did not always provide the most feasible form of data collection. The sensors also needed to "see" each other to create a solid infrared beam and data was being collected upon beam breakage. All of the data that was being collected was being utilized to update message signs via a point to point wireless system. The point to point wireless systems put a drain on the portable systems as well as required a constant adjustment to ensure all points of interest were "seeing" each other within a line of sight set up.

It was this automated notification system and process that eventually led to providing a total solution called a Smart Work Zone System.

1.2 Company Description

The Smart Work Zone System became a fully automated means of notifying the traveling public of various condition types that lie immediately ahead of their trip. Through the use of data collection sensors and updating of message signs, ASTI was able to provide a total safety solution to the highway industry.

Today, ASTI Transportation Systems, Inc. is a wholly owned subsidiary of New Enterprise Stone & Lime, Inc. or NESL. New Enterprise Stone & Lime owns a myriad of production facilities, quarries and contracting services as well as the Highway Safety Division. This division includes Precision Solar Controls or PSC, Protection Services Inc or PSI, Work Area Protection or WAP, Stabler Companies Inc or SCI and ASTI Transportation Systems, Inc.

With numerous offices throughout the United States that are all focused on the highway safety industry, ASTI is able to provide unparalleled levels of service to their clients. ASTI's family of companies allows them to utilize their experience and local support to fully service systems supplied in all states within the United States.

With Precision Solar Controls providing the message board manufacturing, Work Area Protection providing the traffic control device manufacturing and ASTI providing the latest data collection and web based solutions, the company as a whole is capable of providing both the highest quality system as well as the highest level of immediate support. With one point of contact for all of these services, ASTI is able to provide the convenience and response required on the largest and highest profile projects.

For over 20 years ASTI has been providing the highway safety industry with the highest quality Smart Work Zone Systems, Real Time Traffic Management Systems and Temporary ITS Systems on a national and international scale.

1.3 Project Roles and Organizational Chart

ASTI provides a single point of contact on the sensors, the changeable message signs, the camera trailers, the wireless communication infrastructure, the software and data collection, the web based project page and all other facets of the Smart Work Zone solution.

The ASTI team consists of high level software developers, military developed engineers, sensor experts, network engineers and video detection experts. All of the ASTI team has an extensive background in the ITS industry as everyone has served several years on the team including the original founder of the company.

It is through this team that ASTI is able to provide the knowledge required to trouble shoot all aspects of the system. This translates to immediate results while in the field or remotely from a support level. How does this translate to the client, if the system goes down for any reason, the ASTI support is capable of getting the system back up and running very quickly. This means your temporary loss of data or video is just that, temporary. It is due to this response time that ASTI strongly supports performance requirements being written in to specifications.

The typical ASTI/Worksafe TCI, Inc. Smart Work Zone System or Real Time Traffic Management System organizational chart looks like this:



II. Benefits of RTTMS, SWZS and Temporary ITS Systems

2.1 Enhanced Safety within the Work Zone

Some would say the two biggest factors that a Smart Work Zone or Real Time Traffic Management system provides is Reduced Congestion and a Reduction in Rear End Collisions. However, the system often provides a much safer environment for the workers on that project that is not often considered when looking at these systems from a Department of Transportation perspective.

These systems provide a high level of congestion reduction as the traveling public is now able to re-route their trip based on congestion ahead messaging far enough in advance of the work zone or prior to an exit thus allowing them to change their course.

Due to the real time nature of these systems, they are able to trigger changeable message signs far enough in advance of the work zone that motorists are able to slow down and avoid a possible conflict.

However, there is something to consider with real time. If there aren't enough sensors to capture the event then the system cannot work effectively. This is where the design of the system is very important. An experienced supplier of these systems has a good feel for the correct amount of sensors to achieve a very reactive system. The more sensors there are on the road, the more likely the system is able to capture the stopped traffic sooner. If a vehicle stops in between the sensors then it will take a few seconds to a few minutes for the system to begin acknowledging the concern. This is where sensor placement is also crucial to a successful deployment.

With the reduced congestion and more aware drivers approaching the work zone, the workers that are present are now in a much better working environment as it relates to the motoring public. Therefore, the use of the Smart Work Zone has created better trip planning through a web based solution, better re-routing if needed, a safer road environment ahead as there are no surprises and the system has created a better working environment for the construction of the work zone.

Regarding the actual placement of the devices, each device is placed within a certain amount of feet from the roadway or nearest lane. There are often times requirements within the specification that require the devices to be placed behind a guardrail or temporarily mounted to a pole. This offset allows the devices to be out of the right of way of traffic as well as being in a safe and secure placement ensuring their safety and performance.

2.2 Financial Impacts

By reducing congestion and reducing accidents, the Smart Work Zone System is capable of allowing the contractor to now focus on their job both safely and efficiently. With fewer vehicles entering the work zone the contractor is now able to do lane closures and temporary stoppages much more efficiently. This efficiency translates to quicker job completion for both the contractor and the Department of Transportation. There are several projects that provide a financial bonus to a shorter duration project. These bonuses impact the contractor providing the service but also assist the Department of Transportation with shorter lane closure durations, less personnel focused and required on that project and potential savings in payment.

There is also a financial impact associated with an accident. When an accident occurs, there are several layers of events that follow and several layers of support that follow as well.

- Police, Fire and Ambulance are often called to the scene.
- DOT personnel have accident protocols in place that require their involvement.
- There is an intangible cost associated with lost time from all of those involved.
- There is a potential cost associated with an airlift if immediate evacuation is required.
- Accidents require a clean-up crew to handle the spills or broken materials.
- A tow truck provider is called to the scene to remove the damaged vehicles.
- Worst case scenario is an accident leading to a fatality.

So, is the question what is the cost of the Smart Work Zone System or is the more appropriate question what could the Smart Work Zone System save?



2.3 Increased Mobility

Mobility – The ability to move or be moved freely and easily.

It has been proven time and time again that ITS applications in work zones have greatly improved the mobility through that work zone.

ITS within the work zone provides the traveling public with the ability to make decisions for travel routes or adjusting travel times. By doing so, the traffic within the work zone has either been drastically reduced or has been reduced to a smoothing flow. This reduction and calming effect leads to a safer environment for the traveler, the contractor, the flaggers, the emergency response crews and anyone else entering the work zone.

2.4 Public Perception

ASTI provides both an administration level project website as well as a public website with all Real Time Traffic Management projects. The administration level project website provides the Department of Transportation Personnel with the ability to not only see what's going on with the project or that particular corridor but more importantly gives them the control required to respond to situations. Through the website, they can update message signs individually or as a group within seconds. This provides immediate dissemination of information for incidents or notifications such as Amber Alerts. They are also capable of pan/tilt/zoom controls of the video present on the project. The video reinforces the data that is being collected in an immediately viewable aspect. The sensors are constantly collecting data and the website now provides them with lane by lane speed, volume, and occupancy and classification data.

The public site provides a great service to the public as they can now view the current traffic conditions on that particular route. With a color coding infrastructure, the website provides instance feedback on roadway conditions. RED is showing traffic conditions have stopped, YELLOW is showing traffic conditions have slowed and GREEN is showing traffic conditions are flowing. The public also has the ability to see current messages being posted on the changeable message signs in the event they are interested in seeing a more detailed description of what is occurring within that work zone. If video is available, they can now quickly see current traffic conditions. Some states prefer to have the website linked to their 511 page which now combines two streams of information into one. If users are provided with email or texting notification of current conditions then that service is enhanced by providing the same information within the work zone project.

The public is now empowered with information and can utilize that information to make an informed decision on the trip ahead. This also provides a calming effect as the motorist is now aware of the conditions and is not sitting in their vehicle getting anxious on the unknowns.

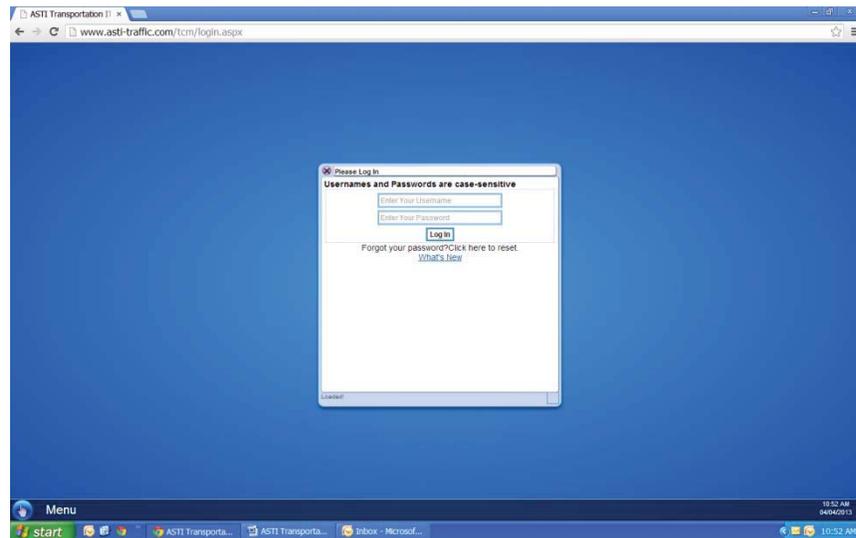
It is highly recommended that all Real Time Traffic Management Systems get a press release to the public to not only share the information available but to also display the most current technologies being utilized to aid the motorist on their daily commute.

This information sharing is a tremendous tool to keep the motorist informed of what the State is doing to assist them during their travels. The end result of the information sharing is a smoother flow of traffic, a reduction in accidents, a safer work zone and a more comfortable driving experience.

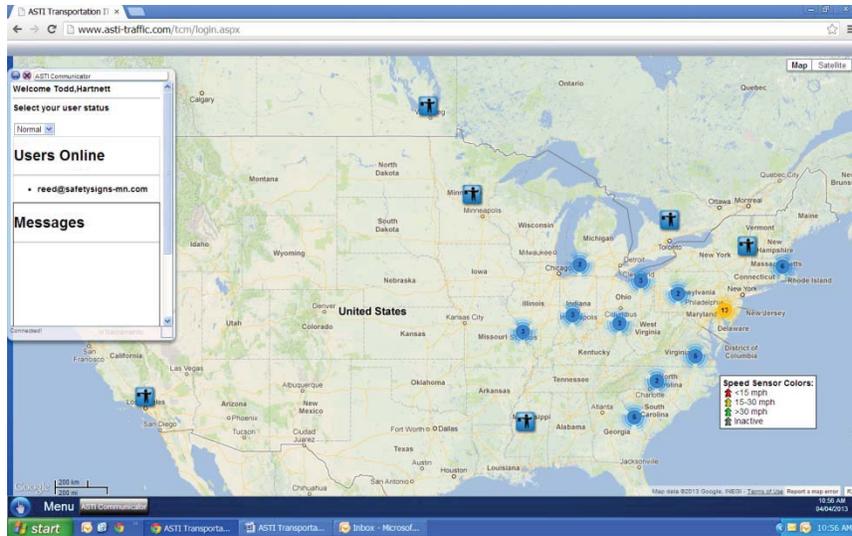
III. The System

3.1 System Overview, the Hardware, the Software and the Website

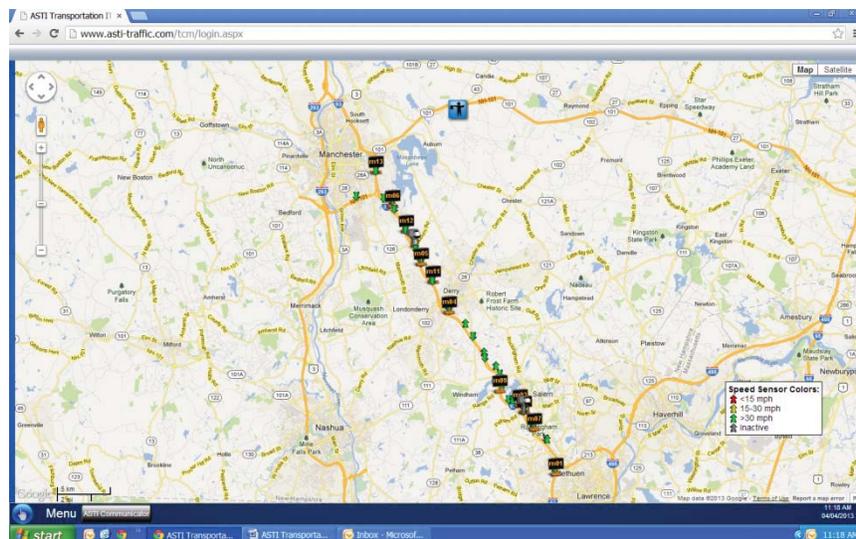
Each Real Time Traffic Management System is provided with a project website. The project website provides all administration users with a username and password that is a secure form of controlling the system. All events are stored for future reporting.



Once the user has logged in, the website will then take that user to the map overview of their particular project. Also, loading immediately is the ASTI “IM” feature. This IM feature allows the user to see all other users that are currently online and available to “chat”. This is also an immediate response location for ASTI customer service. An ASTI user is always logged on during regular business hours to field all online service calls. The chat feature also allows other Department of Transportation personnel to discuss their system thoughts in private or public. This brings other system users together in the event that is desired.

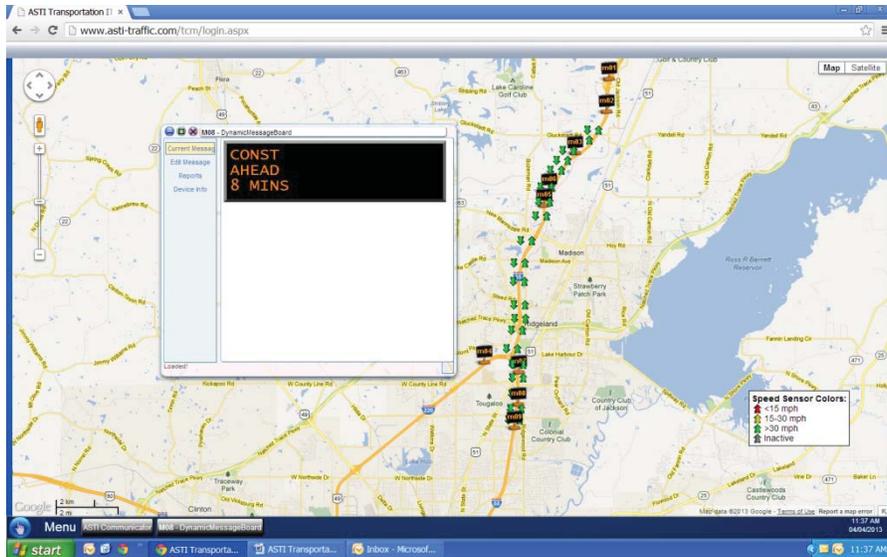


Upon selection of the individual project, the user will then zoom into the area which will provide visualization of the sensors, message signs and cameras.



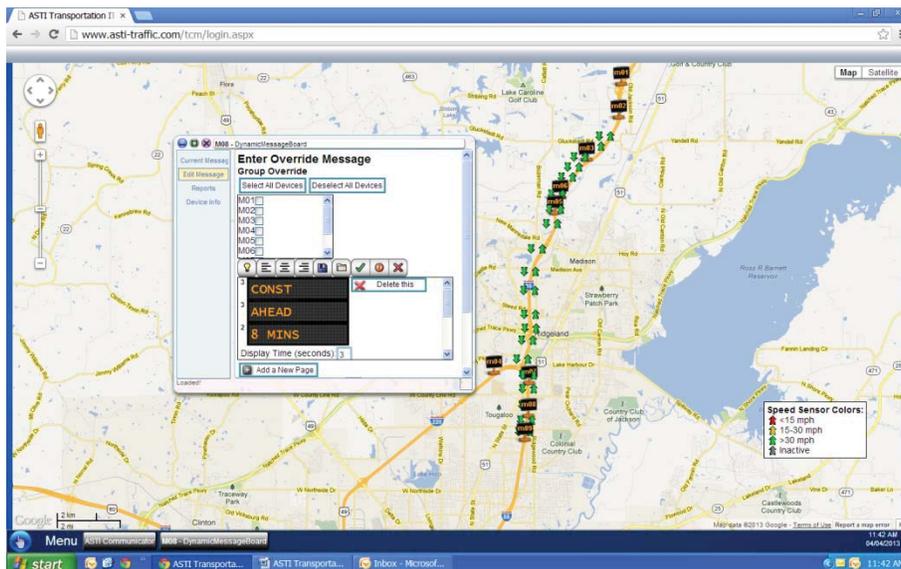
It is at this screen that the user can get a total project overview and also then select a specific unit within the field. If one unit is displaying a different color or is being grayed out, then this is typically showing a concern. The concern could be a traffic related event; the units could have lost power or could have lost communication with the backend software. In any of these events, the contractor and DOT personnel are immediately aware of the situation. The user can then select the icon for that respective device for more detail.

Regarding the message signs, the user can select a message sign which will then populate the current message being displayed.

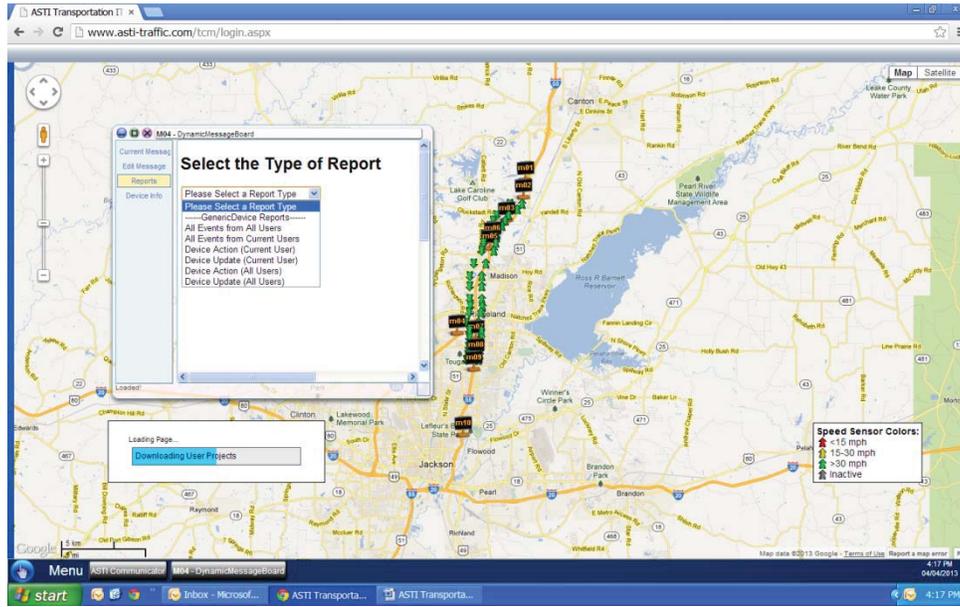


Depending on how the system has been setup, the message displayed could be the result of a travel time message, a congestion message, a dynamic merge message or an incident management message that has put the message sign in an override state. The override state is the result of the contractor or DOT personnel responding to a specific need that pulls the system out of its automated mode. This message needs to be set in place for a period of time and once that time has expired, the system will then go back into automated mode.

Once the user has selected the message sign of interest, they can select to **EDIT THE MESSAGE**. From here the user has the ability to select from their stored messages, enter a new message, save a new message to their library and set the timing of the message. The user can also choose to send the message to all boards on their project or within their fleet by simply hitting “Select All Devices”. A blank message can also be sent by easily blanking all characters.



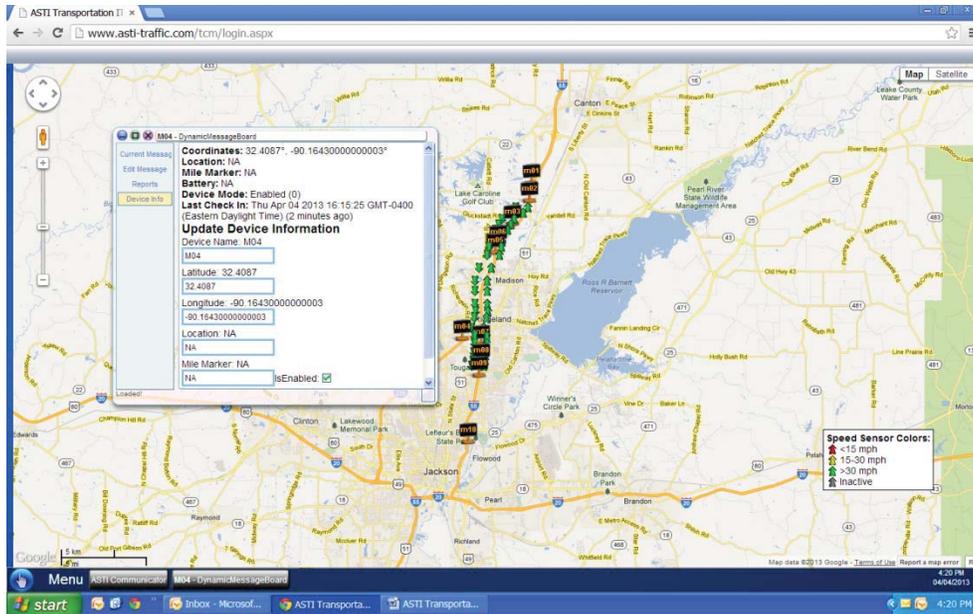
From this screen the user is able to select the REPORTS tab and then choose their desired report. There are several types of reports that can be selected all offering detailed data from the particular device/unit in the field. These reports can be utilized to generate forecasting data and trends within the traffic on that particular day or in relation to a similar event. All report is displayed in an Excel spreadsheet format and can be saved at your desired location, printed for hard copy storage or viewed only.



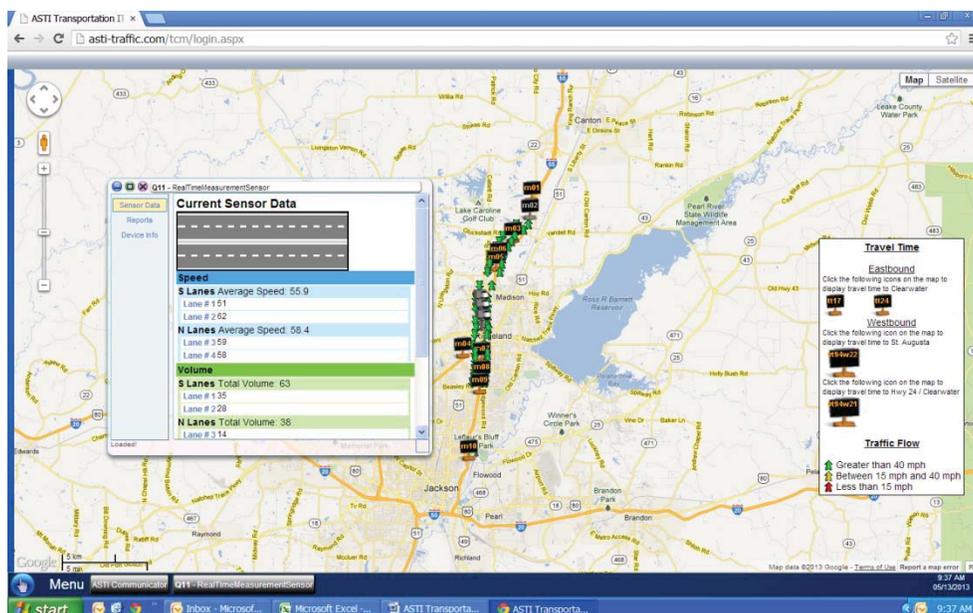
The final tab is the DEVICE INFO tab and that provides the user with all of the pertinent device information such as the latitude and longitude data that was collected from the GPS transponder in the event digital cellular modems are being utilized. For simplicity in locating the unit in field and coordinating with the software, there's also a location to manually enter the nearest mile marker for the unit.

This section also offers the last check in time of the polling cycle from the backend software as well as the battery voltage.

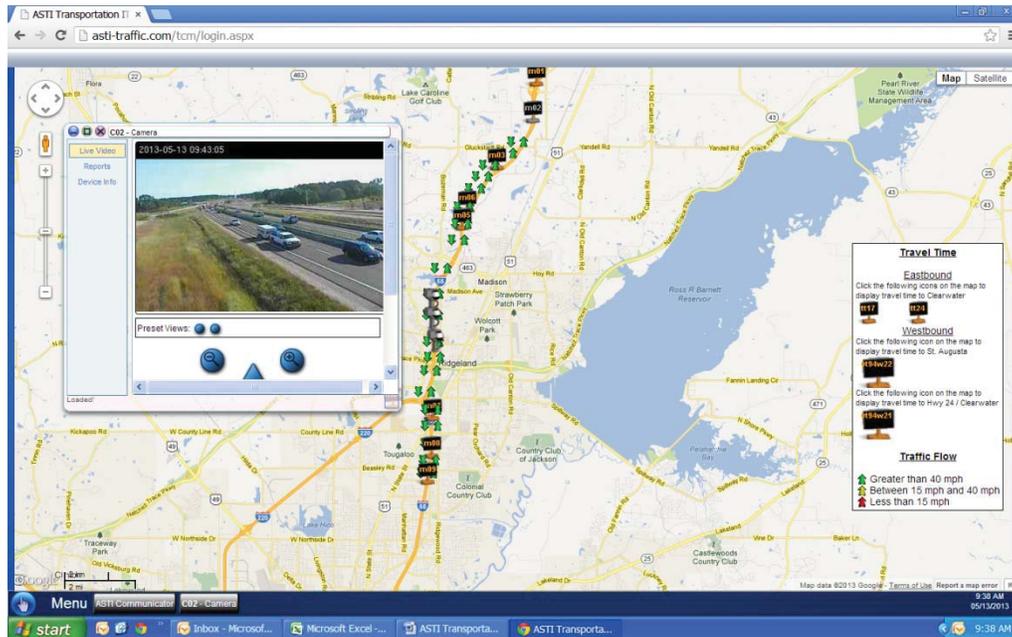
The battery voltage is a very important feature of the unit as this allows ASTI to monitor voltage levels on all units in the field and generate an email to the service/maintenance contractor on the project in the event the voltage drops below a certain level. This proactive approach helps to ensure the unit is being maintained prior to a drop in battery voltage causing an interruption in service due to lost power.



The sensor utilized on all of the ASTI Smart Work Zone System projects is the Wavetronix Smart Sensor. When a longer span of lane coverage is required the HD sensor allows ASTI to capture multiple lanes of traffic and often see both directions of the highway. This enables ASTI to provide a more cost effective solution as opposed to providing sensors on each side of the multiple direction highways. The sensor data collected is then displayed through the website in a lane by lane configuration. The traffic is also captured in a roadway/vehicle display format. Speed, volume and occupancy are displayed on a user friendly pop up graphic display. The user can also select the reporting feature from here to generate an XML spreadsheet including a time and date stamp. This reporting tool enables the user to forecast and trend traffic based on that particular day, year and event.



If a system has included video as part of the project requirements, the video is easily selected and viewed through the website as well. Most of the ASTI project video is served through a single contact thus increasing the frames per second to the maximum a digital cellular modem can provide. This semi-streaming video is displayed via a pop up window upon selecting the video icon. If the user is an administrator of the system, they can then easily take over the controls of the camera and pan/tilt/zoom to their specific desire.



IV. High Profile Project Experience

4.1 The “Carmageddon” Interstate 405 in Los Angeles, California

The project on I-405 consisted of the demolition of the Mulholland Bridge. The demolition of the bridge was done in two phases with the southern side of the bridge being demolished first, followed by approximately 11 months of south-side bridge reconstruction. Upon completion of the south side, the northern side of the bridge was demolished and rebuilt in the same manner. The Mulholland Bridge needed to be removed to accommodate the widening of the I-405 freeway as part of the 10-mile northbound carpool lane construction project. The \$1 billion project was a joint effort between Metro and Caltrans, and was being constructed by Kiewit Infrastructure West Co. The project required the use of a temporary ITS solution provided by ASTI to ensure all traffic was managed in the most efficient means possible. Through the use of portable queue detection, travel time and congestion management signage, and temporary video, ASTI was able to provide an effective solution to Kiewit, Metro and Caltrans.

4.2 Super Bridges I-93 FAST 14 in Boston, Massachusetts

The 93FAST14 project involved the replacement of fourteen deteriorated bridge superstructures on Interstate 93 throughout Medford. Due to the impact that this was going to have on the traveling public, Mass DOT implemented the use of Smart Work Zone technology. ASTI Transportation Systems, being the leader in this industry, was the chosen provider of this technology.

The goal of the system was to monitor the project work zone and disseminate real time information to DOT personnel, the Highway Operations Center (HOC) and the traveling public. It was anticipated that the traffic conditions would deteriorate due to queuing by high traffic volumes, work zone vehicle interference, inclement weather and grade changes.

The Smart Work Zone System on this project was not only providing minute by minute data collection through the use of Wavetronix sensors but also going a step further to integrate BlueToad-Bluetooth technology and the integration of the State's NAVTEQ data collection to deliver the highest quality and most real time data possible. This allowed DOT personnel to make incident management decisions as well as provide the traveling public with the most current information available. Having the ability to make these decisions far enough in advance of the work zone empowered the traveling motorist with re-routing capabilities, more efficient trip planning and quite simply a safer trip through the work zone environment.

4.3 The Interstate 595 Express Corridor in Fort Lauderdale, Florida

From FDOT I-595.com Website: The I-595 Express Corridor Improvements Project consists of the reconstruction of the I-595 mainline and all associated improvements to frontage roads and ramps from the I-75/Sawgrass Expressway interchange to the I-595/I-95 interchange, for a total length along I-595 of approximately 10.5 miles, and approximately 2.5 miles on Florida's Turnpike from Peters Road to Griffin Road. The design and construction cost of the project is approximately \$1.2 billion. The major project components include:

- Three ground level reversible [express toll lanes](#), serving express traffic to/from the I-75/ Sawgrass Expressway from/to east of S.R. 7, with a direct connection to the median of Florida's Turnpike. These lanes will be operated as managed lanes with variable tolls to optimize traffic flow, and will reverse direction during peak travel times (eastbound in the a.m. /westbound in the p.m.).
- [Continuous connection of S.R. 84](#) frontage road between Davie Road and S.R. 7.
- The addition of [auxiliary lanes](#) on I-595 along with combined ramps, [cross-road bypasses](#), and [grade-separated entrance and exit ramps](#) to minimize merge, diverge and weaving movements.
- Widening / reconstruction of 2.5 miles of the Florida's Turnpike mainline and improvements to the [I-595/Florida's Turnpike interchange](#).

- Construction of the New, a component of the Broward County Greenway System.
- 13 [sound barriers](#) providing noise abatement for 20 communities.
- Implementation of an [Express Bus Service](#) within the corridor.

On this project, ASTI provided the TransCore Miramar office with a temporary ITS solution custom to the project needs. With a custom, two line PCMS configuration and point to point wireless solution, this project was one of the more unique projects that ASTI took on. This included custom build units that integrated Wavetronix HD sensors, Vicon Cameras and the custom DMS into a complete Work Zone ITS product. These units were then tied directly into the SunGuide System for FDOT's complete control over the ITS components within the work zone.

4.4 The Interstate 93 Corridor SWZS in New Hampshire

From NHDOT Press Release: The New Hampshire Department of Transportation (NHDOT) has deployed a Smart Work Zone System as part of the Interstate 93 Exit 1 rebuilding project. The primary goal of this system is to provide a safe and efficient travel corridor through the work zone by alerting motorists about what is happening along the road ahead.

The Exit 1 Smart Work Zone consists of changeable message signs that provide information to motorists as they travel through the work zone, traffic sensors that measure vehicle volumes and speed, and a mounted camera that provides images of traffic through the construction corridor.

Motorists will be able to check travel conditions in the work zone via the Internet and will receive vital incident or road construction information through changeable message signs strategically located within three miles north and south of the project area. Motorists will be able to use this information to prepare for stopped or slowed traffic ahead, or they may choose an alternative route. The idea is to let the motorist decide what action to take. Also benefiting from the Smart Work Zone will be emergency personnel responding to incidents on I-93 in the vicinity of Exit 1 in Salem.

The Smart Work Zone has a website link that may be accessed through the I-93 project website at www.rebuildingi93.com. This website link provides the traveling public an Internet location to view the messages displayed on the message signs, the speeds measured through the work zone and an image of the traffic on I-93.

Intern'l Class:

G08G 1/00 20060101 G08G001/00

Claims

1. A method for obtaining real time traffic related information on a highway location using a plurality of roadside devices said roadside devices comprising traffic sensors, the method comprising: i. providing a plurality of roadside devices comprising at least one traffic sensor along said highway for detecting traffic flow past said highway location and connecting said roadside devices to the Internet; ii. providing a central control computer also connected to the Internet via a modem, wherein said central control computer is programmed to provide a plurality of active virtual ports connected to the Internet through said modem, iii. obtaining a device Internet address for said central control computer and for each of said plurality of roadside devices and assigning a virtual port in said central control computer to each of said devices address; iv. establishing an Internet connection between each of said at least one roadside device and said central control computer whereby said central control computer accesses said each of said roadside devices through said assigned virtual port.
2. The method according to claim 1 wherein the step of connecting said plurality of roadside devices to the Internet is performed using digital cellular modems.
3. The method according to claim 1 wherein said plurality of roadside devices further comprises means to communicate a message to a passing motorist.
4. The method according to claim 3 wherein said message communicating means comprises a variable message board (VMS) also connected to the Internet.
5. The method according to claim 4 wherein said Internet connection is performed using a digital cellular modem.
6. The method according to claim 1 wherein said plurality of roadside devices comprises a plurality of roadside traffic sensors and at least one variable message board, each of said roadside traffic sensors having a unique Internet address and each of said at least one variable message board also having a unique Internet address and wherein the central control computer communicates with each of said roadside devices using a plurality of software generated unique virtual port, and wherein said communication occurs quasi-simultaneously.
7. The method according to claim 6 wherein said central computer is connected to the Internet using an Ethernet port.
8. The method according to claim 6 wherein said Internet address is an IP address.
9. The method according to claim 6 wherein said Internet address is a URL address.
10. A real time traffic control system comprising: a plurality of roadside sensors arrayed along the highway and connected to the Internet and each having a unique Internet address; a central control computer also having a unique Internet address and connected to the Internet, said control computer programmed to create on demand a plurality of individual virtual communication ports, each of said virtual communication ports corresponding to each of said unique device addresses, whereby said computer communicates in a quasi-simultaneous manner with said plurality of roadside devices.

11. The control system according to claim 10 further comprising at least one information communicating means also having a unique address and also connected to the Internet.
12. The system according to claim 11 wherein said roadside sensors and said information communication means are connected to the Internet through a digital cellular modem.
13. A method for communicating with a plurality of roadside display devices positioned along a highway, the method comprising: i. providing a plurality of roadside display devices along the highway for displaying messages to passing motorists and connecting the plurality of roadside display devices to the Internet; ii. providing a central control computer also connected to the Internet, wherein the central control computer is programmed to provide a plurality of active virtual ports connected to the Internet, iii. obtaining a device Internet address for each of the plurality of roadside display devices and assigning at least one of the plurality of active virtual ports in the central control computer to the device Internet address of each roadside display device; iv. establishing an Internet connection between each of the plurality of roadside display devices and the central control computer whereby the central control computer accesses each of the roadside display devices through the assigned virtual port.
14. The method according to claim 13, wherein the step of connecting the plurality of roadside display devices to the Internet is performed using digital cellular modems.
15. The method according to claim 13, wherein each of the roadside display devices have a unique Internet address and wherein the central control computer communicates with each of the roadside display devices using a plurality of software generated unique virtual ports, and wherein the communication occurs quasi-simultaneously.
16. The method according to claim 15, wherein the Internet address is an Internet protocol (IP) address or a uniform resource locator (URL) address.
17. The method according to claim 13, further comprising: polling the roadside display devices in a quasi-simultaneous manner in order to verify information displayed by the plurality of roadside display devices.
18. A real time roadside display device verification system comprising: a plurality of roadside display devices arrayed along a highway and connected to the Internet, each roadside display device having a unique device address; a central control computer also having a unique Internet address and connected to the Internet, the control computer programmed to create on demand a plurality of individual virtual communication ports, each of the virtual communication ports corresponding to each of the unique device addresses, whereby the computer communicates in a quasi-simultaneous manner with the plurality of roadside display devices.
19. The system according to claim 18, wherein the roadside display devices are connected to the Internet through a digital cellular modem.
20. The system according to claim 18, wherein the central control computer is configured to poll the roadside display devices in a quasi-simultaneous manner in order to verify information displayed by the plurality of roadside display devices.

Description

CROSS REFERENCE TO RELATED APPLICATIONS.

[0001] This application claims the benefit of priority to U.S. Provisional Application No. 60/647,511 filed on Jan. 27, 2005, the contents of which are incorporated herein by reference in their entirety.

FIELD OF THE INVENTION

[0002] This invention relates to a centrally controlled highway traffic advisory system and associated method and more particularly to a system and associated method for simultaneously addressing a plurality of remote sensors and displays from a remote location via the Internet.

BACKGROUND OF THE INVENTION

[0003] Highway construction zones and accidents are often a major source of congestion in highways as they interrupt the normal traffic flow due to temporarily restricting the available highway lanes. Reduction of the number of available traffic lanes and re-routing the traffic to improvised new traffic lanes cause conditions that are unexpected by the motorist.

[0004] To alleviate such congestion systems have been developed that advise the motorist well ahead of the construction or other incident zones of traffic problems ahead, and anticipated congestion and reduced speed requirements. Such systems may be either temporary, using free standing signaling devices such as remotely controllable traffic lights or variable message boards (VMS) in communication with a remote central controller together with movable roadside traffic flow sensors, or fixed using permanently installed variable message boards in combination with a remote controller and either permanent or temporary roadside traffic sensors. Roadside traffic flow sensors have been known to include occupancy detectors which detect vehicle flow interruption in a highway lane, traditional speed detectors and video cameras.

[0005] Typically such systems include a central control, usually located in the vicinity of the incident or construction zone but also possibly remote thereof. The central control is almost always a computer adapted to receive status information from different roadside devices and able to remotely control such devices so as to, in the case of a VMS for example, display messages to the motorists well ahead of the problem zone.

[0006] Communications between the central control and the roadside devices may be by hard wire connection, telephone link, or radio frequency transmitter/receiver (Transceiver). In such case, the roadside device and the central control include modems for communicating with each other. "Advanced Portable Traffic Management System Work Zone Operational Test" by Nookala et al describes a highway safety system that incorporates the use of widespread spectrum radio, cellular phone and Integrated Services Digital Network (ISDN) phone links. The spread spectrum radio is used to link roadside nodes to the central control computer. The signal transfers from node to node, the nodes acting both as relay and a means of communication between nodes. Together with the ISDN link and cellular phone the system performs as part of an Ethernet network. Each remote terminal (roadside) is equipped with an Ethernet EHUB which allows multiple devices to share the Ethernet. The system includes establishment of a web page to provide traffic information accessible by motorists planning a trip through the Internet.

[0007] Thus there presently are known a number of sophisticated systems used in traffic control. However what these systems have in common is the sequential polling of the different roadside devices regardless of the communication mode adopted in the system. A much more efficient mode of communication would be the quasi-simultaneous polling of all devices particularly if such polling could

be implemented in a continuous mode.

SUMMARY OF THE INVENTION

[0008] There is, therefore, provided in accordance with the present invention a method for obtaining real time traffic related information on a highway location by:

[0009] i. Providing a plurality of roadside devices comprising at least one traffic sensor along the highway for detecting traffic flow past a desired highway location and connecting the roadside devices to the Internet using a modem.

[0010] ii. Providing a central control computer also connected to the Internet via a modem, wherein the central control computer is programmed to provide a plurality of active virtual ports connected to the Internet through the modem.

[0011] iii. Obtaining a device Internet address for the central control computer and for each of the plurality of roadside devices and assigning a virtual port in the central control computer to each of the devices address.

[0012] iv. Establishing an Internet connection between each of the roadside devices and the central control computer whereby the central control computer accesses each of said roadside devices through the assigned virtual port.

[0013] The connection of the roadside devices to the Internet is preferably done using digital cellular modems, and, in at least one embodiment of this invention, variable message boards along the highway are used to communicate messages to passing motorists. The variable message boards are also connected to the central control computer using an Internet connection.

[0014] Still in accordance with the present invention, the plurality of roadside devices comprises a plurality of roadside traffic detectors and at least one variable message board, each of said roadside traffic sensors having a unique Internet address and each of said at least one variable message board also having a unique Internet address; the central control computer communicates with each of said roadside devices using a plurality of software generated unique virtual ports.

[0015] There is further contemplated according to this invention, a real time traffic control system comprising a plurality of roadside sensors arrayed along the highway each having a unique Internet address and each connected to the Internet. The system further comprises a central control computer also having a unique Internet address and connected to the Internet. The control computer is programmed to create on demand a plurality of individual virtual communication ports, each corresponding to one of the unique device addresses, whereby the computer communicates in a quasi-simultaneous manner with the roadside devices. Digital cellular modems are used to connect the roadside devices to the Internet.

BRIEF DESCRIPTION OF THE DRAWINGS

[0016] FIG. 1 is a schematic figure representing a system according to this invention implemented along a highway.

[0017] FIG. 2 is a flow diagram of exemplary steps for polling sensors and updating message boards in accordance to various aspects of the present invention.

[0018] FIG. 3 is a schematic diagram showing the establishment of communication with sensors and the

outflow of information in accordance with an aspect of the present invention.

[0019] FIG. 4 is a schematic diagram showing the inflow and handling of information from sensors received in the central computer in accordance with aspects of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0020] The invention will next be described with reference to the figures wherein same numerals are used to identify same elements in all figures. The figures illustrate the invention and are not intended to act as engineering or construction drawings, therefore they are not to scale and do not include all elements that may be included in such drawings, as inclusion of such elements would unduly clutter the drawings.

[0021] Referring next to FIG. 1 there is shown a highway 10 on which there have been deployed a plurality of means 12 to communicate a message to passing motorists. Such means typically comprise roadside display devices such as variable message boards, which, by way of illustration rather than limitation, may be either portable devices of the type disclosed in U.S. Pat. No. 5,231,393 issued to Strickland et al. in 1993 or fixed, or combinations of the two. Such roadside display devices typically provide for a plurality of messages to be displayed to passing motorists, and the message displayed may be pre-programmed actuated upon receipt of a pre-arranged code signal or composed and transmitted to the device from a remote location. However the message communication means may also comprise traffic signals (including traffic metering devices and conventional traffic lights), highway advisory radio or any other means that will notify a motorist of potential traffic issues ahead. We will refer to all such display devices from hereon as VMS.

[0022] Also deployed along the highway there is shown a plurality of roadside traffic detection sensors 14. Roadside sensors 14, by way of illustration rather than limitation may be speed sensors, occupancy sensors, sensors that determine the type of traffic passing through a designated zone, i.e. long (trucks) or short (passenger) vehicles, video cameras and/or combinations thereof. The roadside sensors may operate using infrared radiation, radar or any other convenient detection system.

[0023] Collectively we will refer to roadside displays/VMS and sensors as roadside devices.

[0024] Associated with each of the roadside devices, is a modem 16 such as a broadband data modem. Modem 16 may be a Code Division Multiple Access (CDMA), a Global System for Mobile computing (GSM) or an equivalent thereof. Each of the modems 16 provides a connection, preferably a high speed connection, between the roadside device and a global information network (e.g., the Internet) through a digital cellular data phone line, e.g., via the nearest cellular phone tower 24. As used herein, the term "Internet" refers to all such networks including, by way of illustration rather than limitation, the Internet, Internet2, and other such networks. Each of the roadside devices has an individual Internet address (herein "address"), preferably an Internet protocol (IP) address, that identifies the location of the device over the Internet.

[0025] A centrally located controller 18, i.e. a computer, usually located in a secure and convenient place unrelated to the zone or zones where the roadside devices are deployed, is also connected to the Internet. Such connection is most likely but not exclusively, a hard wired connection to a high speed Internet access provider. Obviously the controller can be located anywhere where Internet access is possible which in practical terms means almost anywhere in the world.

[0026] The central control computer is programmed to poll the roadside devices and obtain therefrom traffic information or send thereto instructions. For example the central control device may poll the

traffic sensors and obtain data relating to real time local traffic flow. The central control computer may then send to the VMS's a command to display a message advising motorists of traffic conditions ahead.

[0027] The central control computer may be further programmed to provide certain commands and display messages automatically to the VMS's, such messages depending on the traffic information obtained from the traffic sensors, or the central control may display the information to an operator and the operator may in turn select the appropriate message to be communicated to the motorists on the highway. It is still within the scope of the present invention to provide a remote control computer connected to the central control computer and able to communicate with the central control computer via the Internet thereby to provide access to the central control computer from a remote location.

[0028] Alternatively, the central control computer does not have to be in a fixed location, but can be any properly programmed computer in a location with access to the Internet.

[0029] FIG. 2 depicts a flow chart 200 of exemplary steps for polling sensors and displaying messages on VMS's in accordance with one embodiment of the present invention. At block 202, a polling/message display application (herein the "application") is initiated, virtual ports are reserved, and timers are started. In an exemplary embodiment, the application resides on the central control computer and may be initiated by a user in a conventional manner. Upon initiation, the application reserves virtual ports within the central control computer and starts timers that control polling of the sensors and display of messages on the VMS's. A virtual port may be reserved for each unique one of the sensors and the VMS's for communications between the central computer and the sensors and VMS's. For example, if there are four (4) sensors and three (3) VMS's, the application may reserve seven (7) virtual ports for communication with these devices. In an exemplary embodiment, an identifier for each device and an associated virtual port are stored in a table. In addition, the address for each device may be stored in the table.

[0030] At block 204, the application sets a sensor device flag and indicates the number of sensors (Q) to be polled by the central control computer. The application then enters a loop, blocks 206-214, for sequentially establishing communication with the individual sensors. A counter 205 increments a sensor value N after each pass through the loop. The loop starts with establishing communication with a first sensor (N=1) and ends after establishing communication with a last sensor (N=Q).

[0031] The following is sample coding loop from the application for polling roadside sensors such as for example a queue detector: TABLE-US-00001 For intLoopCounter = 1 to TOTALQ MDIForm 1.udpPeerQ(intLoopCounter).SendData(strToSend) MDIForm 1.StatusBar1.Panels(1) = "Sending-> " &.Fields("RadioAddress") & Chr(&HFF) & Chr(&H8F) & Chr(&H1) & Chr(&H2) & Chr(&H2) MDIForm 1.StatusBar1.Panels(2) = "" Next intLoopCounter.

[0032] At block 206, a virtual port number and an address for the sensor are obtained. The virtual port number and the address for the current sensor may be obtained from the table discussed above with reference to block 202.

[0033] At block 208, a control for the sensor is created at the central control computer. Parameters such as port number, address, and polling string are passed to the control for defining communications between the central control computer and the sensor. In an exemplary embodiment, the control is a Windows Socket (Winsock) control. The Winsock control may be created through a subroutine that is called with the statement "MDIForm 1.udpPeerQ (intLoopCounter) .SendData(strToSend)" in the above sample coding loop.

[0034] At block 210, the central control computer establishes a connection with the sensor and sends polling data to the sensor through the established connection. In an exemplary embodiment, the

connection is in accordance with a User Datagram Protocol (UDP). In accordance with this embodiment, the polling data may be sent by a SendData method associated with a SocketWrapper object that pushes a datagram which traverses the Internet as one packet that takes one path to the sensor or as multiple packets that follow multiple paths to the sensor. In alternative exemplary embodiments, the connections may be in accordance with TCP/IP or other such communication protocol. As a practical matter, the central control computer may be connected to the Internet and communications from the central control computer may travel from the central computer over the Internet to a transmitter (cellular tower) where it is transmitted to a modem associated with the device to which communications are being sent.

[0035] At block 212, a data receiving period begins for receiving responses to the polling data from the sensor, e.g., through the Winsock control for that sensor.

[0036] At block 214, the application checks if the sensor is the last sensor (e.g., $N=Q$). If the sensor is the last sensor (e.g., $N=Q$), processing proceeds at block 216. Otherwise, if the sensor is not the last sensor (e.g., $N<Q$), processing proceeds at block 204 with the steps of blocks 204-214 repeated for the next sensor.

[0037] At block 216, the receiving period for the sensors, which began at block 212, ends. In an exemplary embodiment, data from a sensor may be received at essentially anytime after poll data is sent to that sensor and ends sometime after the last sensor is polled. Thus, there is an overlap period during the receiving period in which data from multiple sensors may be received by the central control device. After the receiving period ends, the control created at block 208 may be terminated.

[0038] In the exemplary embodiment, the virtual ports established within the central control computer enable the central control computer to receive packet of data from multiple sensors in any sensor order and in any packet order. For example, data may be received from a first sensor 1 followed by data from a third sensor followed by data from a second sensor. In another example, a first packet may be received from a first sensor followed by a first packet from a second sensor followed by a second packet from the first sensor. In another example, a second packet from a first sensor may be received before the first packet of the first sensor is received. Thus, communications from the sensors may be received in a quasi-simultaneous manner.

[0039] Timers may be implemented to handle non-responsive sensors, e.g., for identifying a sensor for maintenance if the sensor has not responded for a particular period of time or number of cycles. In an exemplary embodiment, when a sensor responds a time/stamp is placed on the data and written to a database. This time stamp is checked every minute (with another timer, not shown) and compared to the current time. If the device has not responded for a predetermined period of time, the application generates an alarm. This alarm can be a visual alarm, an audible alarm, an e-mail being sent etc.

[0040] FIG. 3 illustrates conceptually the steps performed in blocks 208 and 210. Blocks 300a-n represent the controls that were created in the central control computer in block 208. The controls 300a-n establish communication with associated sensors and send poll data to those sensors (block 210). Communication between the controls 300a-300n are established via the Internet 302. As illustrated in FIG. 3, multiple controls 300a-n may exist concurrently (e.g., as multiple threads) for communication with the sensors. Similar steps may be performed for communicating with VMS's.

[0041] FIG. 4 is a flow diagram illustrating the receipt of data from the sensors during the data receiving period that begins at block 212 (FIG. 2) and ends at block 216. As illustrated in FIG. 4, communications may be received from multiple sensors 400a-n concurrently (quasi-simultaneously), e.g., over the Internet 402. As stated above, each created control (e.g., Winsock control) is associated with a virtual port. When a sensor checks in, it checks in through its virtual port. The control for that virtual port then

takes over at block 404, e.g., through a set of application programming interface routines (API) called by the application to request and carry out lower-level services performed by the computer's operating system. The individual controls (represented by controls 406a-c) process data received at their virtual port (e.g., using the API) by attaching the address of the sensor and their virtual port number to the data and passing the data, address, and virtual port number to a decoding routine 408. The decoding routine 408 decodes the received data--taking into account the address and virtual port information--to obtain polling results. This enables decoding of the data regardless of the order in which it is received. A similar process may be performed to receive information from the VMS's. Once the received information is decoded appropriate action may be taken such as developing messages and identifying VMS's to display those messages.

[0042] Referring back to FIG. 1, at block 218, one or more VMS's are identified for updating based on the results received from the sensors in response to the polling data. For example, if twenty sensors provide responses to the polling data and, based on those responses, there are four VMS's to be updated, those four VMS's are identified for updating. As one example, the information may indicate that traffic is stopped as detected by sensors "A" and "B" located at mile 25 of the highway. Once this information is displayed to an operator the operator may set a single VMS located along the highway a number of miles upstream of the stopped traffic to display a message advising the motorists of the situation and possibly suggesting alternate routes. In accordance with this example, this VMS would be identified as the sole VMS for update.

[0043] The central computer may also be programmed to send certain pre-recorded messages to selected VMS's depending on the status indication of roadside sensors such as speed or queue detectors. For example, receipt and decoding by the central control computer of a message indicating speed of traffic as less than a preset limit could trigger an automatic response in the form of a command sent to a VMS setting an appropriate preselected speed limit or a caution indication. Such messages may constantly change as the data received by the roadside traffic sensors provide new information regarding traffic flow, or may change at predetermined desired intervals.

[0044] At block 220, the application sets a VMS device flag and indicates the number of VMS's (R) that will be sent message data by the central control computer. The application then enters a loop, blocks 220-228, for sequentially establishing communication with the individual VMS's and sending messages thereto. A counter 221 increments a VMS value M after each pass through the loop. The loop starts with establishing communication with a first message board (M=1) and ends after establishing communication with a last message board (M=R). The message data may be sent using a coding loop similar to the sample coding loop described above.

[0045] At block 222, a virtual port number and an address for the VMS are obtained. The virtual port number and the address for the VMS may be obtained from the table discussed above with reference to block 202.

[0046] At block 224, a control for the VMS is created at the central control computer. Parameters such as port number, address, and a message board string are passed to the control for defining communications between the central control computer and the VMS. As described above, the control may be a Windows Socket (Winsock) control.

[0047] At block 226, the central control computer establishes a connection with the VMS and sends message data to the message board through the established connection. As described above, the connection may be a UDP, TCP/IP, or other such connection. The message data may include a textual message for display on the VMS or an indicator that instructs the VMS to display a prerecorded textual message. In addition, such as in the case of a traffic metering device VMS, the message data may

include timing information for controlling STOP/GO lights on the traffic metering device or an indicator that instructs the traffic metering device to control lights based on predefined timing information.

[0048] At block 228, the application checks if the VMS is the last VMS (e.g., $M=R$). If the VMS is the last VMS (e.g., $M=R$), processing ends at block 230 (or proceeds at block 204 in a continuous loop until the application ends). Otherwise, if the VMS is not the last VMS (e.g., $M<R$), processing proceeds at block 220 with the steps of blocks 204-214 repeated for the next VMS.

[0049] In an exemplary embodiment, the VMS's may be polled to verify that the VMS's are displaying the correct information. In accordance with this embodiment, the VMS's may be polled using a routine similar to the routine for polling the sensors described above with reference to blocks 204-216. All VMS's may be polled to identify the messages currently being displayed for comparison with expected messages stored by the central control computer. Alternatively, only those VMS's that were updated most recently may be polled.

[0050] When information (e.g., a datagram) is sent over the Internet from the control computer to the device modems, the datagram may be broken into smaller packets and sent to the end device, or the whole datagram may go as one piece. If broken up, it is reassembled once it gets there. This applies for traffic traveling from the computer to the devices and from the devices to the computer. The operating system software on the computer puts the packets back together if they are broken apart, and the connecting device modem puts the packets together once they all reach it. Thus, information going to or coming from more than one device arrives at or leaves from the computer in a quasi-simultaneous manner when using more than one port.

[0051] Because data transmitted through the Internet is split into distinct smaller individual packets arriving at their destination along various separate routes, because the system does require confirmation of linking with a device or of successful transmission of the datagram, and through the use of the virtual ports, the central control computer is able to poll different roadside devices without waiting for the complete transmission/reception to and from each of the roadside devices. This process is referred to herein as "quasi-simultaneous" as distinguished from a process where the computer sequentially polls each device, that is, sends out a message and waits for the completion of the transaction prior to addressing another roadside device.

[0052] This applies for traffic traveling from the central control computer to the roadside devices and from the roadside devices to the central control computer. The central control computer operating system puts the packets back together if they are broken apart and the modem attached to the roadside device will put the packets together once they all reach it.

[0053] The central control computer and the roadside devices are preferably but not necessarily on what is referred to a permanently on status. This means that the link between the central control and the roadside devices is always "on" and there is constant communication between the central control computer and all of the devices quasi-simultaneously, thereby providing real time traffic information. Because the central control computer is always connected to all the devices it is able to receive information continuously from all the devices.

[0054] The foregoing system and process have been described with reference to a Microsoft operating system and routines and subroutines available through such system. While at present this is a preferred operating system, the present invention is not to be limited to use with this operating system exclusively. Rather this one example of the present invention which is readily implemented at this time. However other operating systems and subroutines may be used to create the multiplicity of virtual ports used in accordance with the present invention to communicate with a plurality of devices in a quasi-

simultaneous fashion through an Internet connection.

* * * * *





Smart Work Zone Protocol for system failure notification

Any time the website is going to be down, **SWZ equipment moved, traffic pattern changed**, incidents occur, or any other problems that will affect the system the following list of people need to be notified, preferably via email. This includes changing the pattern of traffic for work to be done.

VTrans Personnel:

Vtrans Project Manager: Mark Gerrish 802-461-5570
Mark.Gerrish@state.vt.us

ITS Traffic Manager: Robert T. White 802-522-9867
RobertT.White@state.vt.us

Traffic Operations Ctr: Larry Dodge
Larry.Dodge@state.vt.us

Gregory Fox
Gregory.Fox@state.vt.us

Chris Barker
Resident Engineer
chris.barker@state.vt.us
Nate Dagesse
Chief Inspector
ndagesse@eivtech.com

Worksafe Personnel:

Scott Deschamps scottd@worksafetci.com
800-547-0808 802-288-6051

Debra Ricker debrar@worksafetci.com
800-547-0808

ASTI Personnel:

Peter Krikelis pete@asti-trans.com
302-328-3220

Don Henry don@asti-trans.com
302-328-3220