Daniel Berger
Lower Hudson Valley Chapter Director
New York Civil Liberties Union

Re: Freedom of information request: Public Records Request/Automatic License Plate Readers

This letter is the response to your correspondence dated August 1, 2012 regarding Records Request/Automatic License Plate Readers.

Attached are the department's General Orders, Memorandum of Agreement with Westchester County, LPR operating manual and supporting documentation. Most questions in your request should be answered with these documents.
Other questions not address in the documentation were:
Number of reads. (Approximately 1700 per day, 51,000 per month.
Our department currently only has one unit.)
This data can be accessed for criminal investigations but that access is limited to the Operations Division Commander and one Patrol Sergeant.

If you have any further questions I may be reached at 914-241-3111 or by email at jdickan@bedfordny.gov

Respectfully Yours,

Jeffrey R. Dickan
Operations Lieutenant
Bedford Police Department
307 Bedford Road
Bedford Hills, NY 10507-1321
Phone 914-241-3111
Fax 914-666-7236

GENERAL ORDER SECTION 112-12

LICENSE PLATE READER (LPR)				
DATE ISSUED 10/28/09	DATE EFFECTIVE 10/28/09	DATE REVIEWED	REVISION NO.	PAGE 1 OF 2

PURPOSE

The following special order is established in order to institute uniformed policies and procedures for the use of the Remington ELSAG Automatic License Plate Reader in an effort to fully utilize this equipment's capability in apprehending vehicles involved in criminal/unlawful activity and to increase the effectiveness of Vehicle and Traffic Law enforcement.

POLICY

This Department will use the LPR in a uniform manner and deploy the LPR by trained personnel on every shift whenever possible. In addition, it shall be the policy of this Department to store the accumulated LPR data for a period of one year. This data shall be shared with any requesting agency and submitted to a central repository may be required.

PROCEDURE

1. Officers utilizing the LPR system will be trained prior to its use through individual on-the-job training. Officers will be trained in the use of the LPR system as well as checking updated information, maintenance and manually entering plates. Once Department personnel are trained, squad sergeants will determine which officer on his respective squad will operate the LPR vehicle.

2. Excluding exigent circumstances, the LPR shall be deployed during all AMBER alerts.

3. Since LPR data is not live, all "Hits" will be confirmed through DMV prior to making an arrest. All "Hits" will be confirmed prior to stopping the vehicle. Once a "Hit" is positively confirmed, current department arrest procedures will be followed.

4. All scofflaws will be confirmed through the Court prior to vehicle tow/impound. Only vehicles parked on public roadways or municipal parking lots are subject to impound. Moving scofflaws (vehicles being driven on the public roadway) will not be stopped as scofflaws for the purpose of an impound without probable cause for a traffic stop in accordance with the Vehicle and Traffic Law. Vehicles with suspended/revoked registrations parked and unoccupied in public municipal lots may be impounded in the same manner as scofflaw vehicles

5. At the conclusion of their respective tour of duty, officers must complete an LPR Activity Report. The report will be submitted to the LPR project manager directly or to his mailbox. This form contains data required for the LPR grant program.

MEMORANDUM OF AGREEMENT FOR THE WESTCHESTER INTELLIGENCE CENTER (WIC) AMONG THE PARTICIPATING FEDERAL, STATE AND LOCAL LAW ENFORCEMENT AGENCIES

1. Overview

a. Background:

The Westchester Intelligence Center ("WIC") was established as a crime intelligence center to foster and facilitate information sharing and collaboration among law enforcement agencies, particularly field intelligence officers, operating in Westchester County as a means of increasing the ability of law enforcement to rapidly triage criminal events that endanger public safety and quickly respond to situations as they develop.

The principal goal of WIC is to support local police agencies in their efforts to abate crime and augment public safety in Westchester County.

WIC operates under the auspices of the Westchester County District Attorney's Office ("WCDAO") and is staffed by members of multiple law enforcement agencies. WIC is headed by an Executive Director, who shall serve as the Administrator of this Agreement ("Administrator").

b. Purpose and Intended Benefits:

With the goal of enhancing public safety, while protecting individual privacy rights, the parties to this agreement seek to establish a mechanism for the sharing and exchange of criminal intelligence information and data for the advancement of legitimate law enforcement purposes, including crime solving and abatement, identification and location of suspects and known offenders, detection of predictive trends in criminal activity, and development of strategies to solve and prevent crimes.

c. Agency Participation:

Any federal, state or local law enforcement agency operating in Westchester County ("Agency") may participate in WIC.

2. Information and Resources to be Shared:

Subject to the confidentiality provisions outlined in this agreement, WCDAO will make the resources of WIC available to all participating Agencies. WIC will share information

and data – whether generated by WIC or provided to WIC by outside law enforcement agencies - with participating Agencies for legitimate law enforcement purposes only.

3. Requests for Information:

All requests for information and data from WIC shall be submitted to the Administrator or his/her designated representative. The Administrator shall be the final arbiter of whether the information and data requested by the Agency is available for dissemination.

4. Record Retention:

It is understood and agreed that the requesting Agency is responsible for the preservation of all records and/or reports generated by WIC at the request of the Agency, and shall be the repository of those records and reports.

Each Agency shall retain, as part of its own case files and records, any records and reports (electronic and physical copies) obtained from WIC. The retention shall be in accordance with that Agency's policies for record retention and in compliance with any and all applicable federal, state, county and local laws.

5. Confidentiality and Security:

- In accordance with its purpose WIC shall be permitted to disseminate information and data supplied by an Agency to authorized users under the terms provided herein except to the extent such information and data has been specifically identified as "confidential" by the providing agency.
- Information and data possessed by WIC is subject to disclosure in accordance with the laws governing the criminal justice system and by court order.
- Only authorized users are allowed to view and use the information and data possessed by WIC. Any authorized user who receives a request from a non-authorized user for information and data provided by WIC shall not release that information, but may refer the requestor to the Administrator.
- Each Agency will make reasonable arrangements to maintain the security of the information and data in its custody, by protecting it against such risks as unauthorized access, collection, use, disclosure or disposal.
- Each Agency will advise WCDAO and WIC immediately of any circumstances, incidents or events concerning the following: unauthorized access to or modification of information or data supplied by WIC; unauthorized use of such information and data; unauthorized disclosure of such information and data; and breaches of privacy, security and confidentiality with respect to the information and data or with respect to any computer system in its custody that is used to store or access such information and data.
- Each Agency must investigate and cure any of the aforementioned incidents of unauthorized use of WIC information and/or data.

- All employees of WIC and each participating Agency having access to information and data stored and maintained at WIC will be subject to a criminal investigation background check.
- Each Agency will inform the Administrator or his/her designee, in writing, when an employee or agent of the Agency is no longer authorized to access WIC as a representative of the Agency.

6. Third Party Dissemination of Information and Data:

There shall be no third-party dissemination by an Agency of information and data obtained through WIC without the express, written consent of the Administrator.

7. Accuracy:

Each Agency will make every reasonable effort to ensure the information and data it contributes to WIC is accurate, complete and up-to-date.

It is expressly understood and agreed that an Agency shall use the ordinary investigative tools to insure the objective reliability of any information and data received from WIC which is relied upon to conduct any police initiated encounters.

8. Modification or Termination – General:

This agreement may be modified or terminated at any time by agreement, in writing, of both parties.

9. Termination for Non-Compliance:

This agreement may be terminated at any time by either Party if the other Party fails to meet its obligations under this agreement.

It is expressly understood and agreed that this agreement will, at the election of the Administrator, cease immediately if a recipient Agency is found to be improperly using or disclosing the shared information and data. In addition, such improper use or disclosure will be subject to the penalties provided by applicable law.

10. Term of Agreement:

This agreement shall go into effect upon full execution hereof by both parties. It shall remain in effect unless and until terminated in accordance with paragraph 8 or 9.

11. Notices:

Any notices required by this agreement shall be in writing and shall be effective on mailing. All notices shall be sent by registered or certified mail, return receipt requested, or by overnight courier, and mailed to the following addresses:

WCDA:
Honorable Janet DiFiore
District Attorney of Westchester County
Westchester County Courthouse
111 Dr. Martin Luther King, Jr. Blvd.
White Plains, New York 10601

With copy to:
Robert Kelly
Executive Director
Westchester Intelligence Center
85 Court Street
White Plains, New York 10601

Agency:
Chief William Hayes
Bedford Police Department
307 Bedford Rd
Bedford Hills, NY 10507

12. Compliance with Law:

WIC and Agency will comply with all applicable federal, state and local laws, codes, ordinances, rules, and regulations in performing activities under this agreement.

13. Execution of Memorandum of Agreement:

By executing this agreement, WCDAO and Agency acknowledge that they have received a copy of this agreement and will comply with its terms and conditions. This Memorandum of Agreement may be executed in one or more counterparts, each of which will be deemed an original, but all of which together constitute one and the same instrument. A complete original will be kept on file with WIC.

Agreed to on behalf of WCDAO and WIC:

_____ _____

Robert Kelly, Date
Administrator, WIC

Agreed to on behalf of: Bedford Police Department
Law Enforcement Agency

_____ _____

Chief William Hayes Date
Name and Title of Authorized Representative

STATE OF NEW YORK
DIVISION OF CRIMINAL JUSTICE SERVICES
Four Tower Place
Albany, New York 12203-3764

DAVID A. PATERSON
GOVERNOR

DENISE E. O'DONNELL
COMMISSIONER

January 16, 2009

Chief Christian Menzel
Bedford Town Police Department
307 Bedford Road
Bedford Hills, NY 10507

RE: Letter of Agreement Regarding Transfer of License Plate Reader (LPR)

Dear Chief Menzel:

Congratulations! Your agency has been selected as an eligible recipient for a License Plate Reader (LPR) award from the NYS Division of Criminal Justice Services (DCJS) through a grant received from the Governor's Traffic Safety Council.

DCJS will purchase an LPR for your Law Enforcement Agency (Recipient) to commit to a two-year traffic safety improvement initiative. In addition, DCJS will provide a one-year manufacturer's warranty and vendor developed Operation Center Software license for use in crime reduction activities and the apprehension of offenders.

In order to insure successful implementation by June 30th, 2009, DCJS and ELSAG North America Law Enforcement Systems, LLC will be working together to coordinate LPR software downloads, equipment installation, and training.

Agencies in agreement with the terms set forth in the attached DCJS Letter of Agreement (LoA) will receive one (1) LPR Unit upon the completion of the following:

STEP 1: Submit the signed LoA to DCJS via fax (518.457.1186) **by midnight of Wednesday, January 28th, 2009** to the attention of Michele Mulloy.

The original, signed LoA should be mailed directly to the attention of:

Eileen Langer-Smith
Division of Criminal Justice Services
3rd Floor, 4 Tower Place – Stuyvesant Plaza
Albany, NY 12203

STEP 2: Designate an agency laptop with the following minimum requirements:

- Windows 2000 (Service Pack 4) or XP – No Vista
- Available USB (2.0 preferred) and Ethernet Port (10/100)
- 1Gb RAM
- 1.6 GHz + processor (Pentium 4 preferred)
- 60 gb Hard Drive

In order to participate in the LPR initiative, those agencies that do not currently have an available agency laptop which meets the above minimum requirements will need to purchase and receive delivery of one by Tuesday, March 31st, 2009.

STEP 3: Complete the attached Agency Coordinator Contact Form and fax it with the signed Letter of Agreement.

If you are in agreement with the attached LoA, please sign it and return the original to the Office of Program Development and Funding, attention Motor Vehicle Theft and Insurance Fraud Unit by midnight of Wednesday, January 28th, 2009.

If you have any questions or are unable to comply with any of the above requirements by the deadlines indicated, please contact Michele Mulloy at 518.485.0913. Thank you for your assistance.

Very truly yours,

Denise E. O'Donnell

Denise E. O'Donnell

Letter of Agreement to Participate in the Traffic Safety Improvement Initiative

This letter of agreement will have the duration of two years from the equipment delivery date to the Law Enforcement Agency (Recipient), and may be amended in writing upon the mutual consent of the Recipient and DCJS. This letter of agreement may be terminated at the discretion of the Commissioner of the Division of Criminal Justice Services.

This letter confirms the agreement between DCJS and the Recipient, wherein DCJS has agreed to transfer all right, title, and interest in the LPR to the Recipient, and the Recipient agrees to accept the transfer of all right, title, and interest in the LPR, upon the following conditions.

1. The Recipient agrees to appoint a staff member to coordinate the receipt and utilization of the LPR (see attached Agency Coordinator Contact Form). The Recipient agrees to notify DCJS in writing of any personnel changes in regards to the LPR program coordination. The coordinator will be required to submit quarterly report data to DCJS and make appropriate efforts to ensure that the LPR equipment is utilized a minimum of eight (8) hours per week.

2. The Recipient agrees to provide DCJS a standardized quarterly progress report for a minimum of two years regarding LPR usage (see attached LPR Quarterly Progress Report). Each LPR contains software capable of generating the statistics necessary to complete the reporting requirements. Training on how to obtain the report from the LPR unit will be provided by the vendor upon installation and with subsequent software upgrades. This report data is essential in the ongoing evaluation on the effectiveness of LPR technology.

   Quarterly reports are to be sent electronically or via fax to the designee of the Director of the Office of Program Development and Funding.

3. The Recipient agrees to provide an appropriate and compatible laptop computer for the use and operation of the LPR.

4. The Recipient agrees to accept all responsibility for the care and operation of the LPR. Furthermore, the Recipient agrees to provide for the maintenance and support of the LPR beyond the original one-year warranty and service contract. Prior to the expiration of the DCJS funded one-year warranty, the Recipient agrees to purchase the second year extended warranty which covers the latest version of the applicable software.

5. The Recipient agrees to develop and implement a departmental policy regarding the utilization of the LPR and provide said policy in writing to DCJS within 90-days of receiving the LPR.

6. The Recipient agrees to implement strategic crime prevention and control initiatives regarding highway safety issues and other motor vehicle related offenses as recommended in the 'Operation of License Plate Readers for Law Enforcement Agencies in New York State Suggested Guidelines' (*http://www.criminaljustice.state.ny.us/ofpa/pdfdocs/approvedjune2007lprmanual1.pdf*). DCJS shall seek the return of any LPR equipment which is not effectively utilized for initiatives in accordance with the strategy recommendations.

7. The Recipient agrees to provide mutual assistance to law enforcement agencies in neighboring and/or overlapping jurisdictions which request the use of LPR's for special operations (subject to availability).

8. The Recipient agrees to immediately deploy the LPR when responding to the recovery of an abducted child (Amber Alert). The agency agrees to comply with the guidelines as issued by the Missing and Exploited Children's Clearinghouse (MECC) which are used during an AMBER Alert. Agencies should:

   a. Provide notification to patrols.
   b. Search during an incident.
   c. Look back for encounter prior to the alert date.
   d. Obtain assistance from other agencies with LPR equipment.

9. Any notice to either party must be in writing, signed by the party giving it, and shall be served personally, electronically or by mail to the other party. Notice to DCJS is to be given to the Deputy Commissioner of the Office of Program Development and Funding and notice to the Recipient is to be given to the person signing this letter of agreement on behalf of the Recipient or that individual's replacement pending a cessation of employment from the Recipient agency.

For the Law Enforcement Recipient:

In Acknowledgment of and Agreement with the Provisions of this Letter of Agreement:

Title: CHIEF OF POLICE

TOWN OF BEDFORD POLICE
Law Enforcement Agency

Date: 1/28/2009

ELSAG NorthAmerica
A Finmeccanica Company

ELSAG NORTH AMERICA, LLC
EXTENDED LIMITED WARRANTY

Equipment Owner	Servicer
Town of Bedford	Elsag North America, LLC
307 Bedford Road	205 H Creek Ridge Road
Bedford Hills, NY 10507	Greensboro, NC 27406

Model Number	Serial Number
MPH-900	J07017165-E08030860-J07016057

Date Equipment Installed:	N/A	Date Coverage Begins:	2-24-11
Warranty Sales Price:	N/A	Date Coverage Ends:	2-23-13

COVERAGE

ELSAG North America, LLC ("ELSAG") warrants this ELSAG hardware product against defects in design, materials and workmanship under normal use in accordance with the specifications and documentation for the period designated above ("Warranty Period"). If a hardware defect arises and a valid claim is received within the Warranty Period, at its option and to the extent permitted by law, ELSAG will either (1) repair the hardware defect at no charge, using new or refurbished replacement parts, or (2) exchange the product with a product that is new or which has been manufactured from new or serviceable used parts and is at least functionally equivalent to the original product.

EXCLUSIONS AND LIMITATIONS

ELSAG does not warrant that the operation of the Product will be uninterrupted or error free. ELSAG is not responsible for damage arising from failure to follow instructions relating to the Product's use. This warranty does not apply: (a) to errors or defects caused by persons or entities other than ELSAG, including, without limitation, errors or defects in any third-party software or products and errors or defects caused by modifications to the Product (including upgrades and repairs) by someone other than ELSAG or an ELSAG Authorized Service Provider; (b) to any breach of the Product (camera and trunk box/processing unit) seal by someone other than ELSAG or an ELSAG Authorized Service Provider; (c) to pre-existing conditions in the installation environment or vehicle; (d) to damage from accident, abuse, misuse or introduction of foreign objects into the Product; (e) to unauthorized Product repairs, modifications or alterations; (f) to failure to follow the manufacturer's instructions; (g) to third party actions (i.e., fire, collision, vandalism, theft, etc.); (h) to elements of

acts of war or acts of God; (i) to battery leakage or improper use of any electrical source; (j) to cosmetic or structural damage to case or frame of the Product or to any non-operating part including decorative parts; (k) to any damage to the Product covered by an insurance policy (in such a case, this Warranty will cover any applicable deductible, subject to the terms of coverage and exclusions set forth herein); (l) to preventative maintenance; (m) to any damage which is not reported during the Term of this Warranty; (n) to costs associated with the installation, removal or reinstallation of the Product; and (o) to consumable parts, such as batteries , unless damage has occurred due to a defect in materials or workmanship. Items not covered under warranty (but available for purchase) include; camera glass and batteries.

TO THE EXTENT PERMITTED BY LAW, THIS WARRANTY AND REMEDIES SET FORTH ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, REMEDIES AND CONDITIONS, WHETHER ORAL OR WRITTEN, STATUTORY, EXPRESS OR IMPLIED. AS PERMITTED BY APPLICABLE LAW, ELSAG SPECIFICALLY DISCLAIMS ANY AND ALL STATUTORY OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND WARRANTIES AGAINST HIDDEN OR LATENT DEFECTS. IF ELSAG CANNOT LAWFULLY DISCLAIM STATUTORY OR IMPLIED WARRANTIES THEN TO THE EXTENT PERMITTED BY LAW, ALL SUCH WARRANTIES SHALL BE LIMITED IN DURATION TO THE DURATION OF THIS EXPRESS WARRANTY AND TO REPAIR OR REPLACEMENT SERVICE AS DETERMINED BY ELSAG IN ITS SOLE DISCRETION. No ELSAG reseller, agent or employee is authorized to make any modification, extension, or addition to this warranty. If any term is held to be illegal or unenforceable, the legality or enforceability of the remaining terms shall not be affected or impaired.

ELSAG's maximum liability under this Warranty, whether in contract, tort (including negligence or strict liability), or otherwise, shall be the cost of repair or replacement of the affected Products. EXCEPT AS PROVIDED IN THIS WARRANTY AND TO THE EXTENT PROVIDED BY LAW, ELSAG IS NOT RESPONSIBLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM ANY BREACH OF WARRANTY OR CONDITION, OR UNDER ANY OTHER LEGAL THEORY IN CONTRACT, TORT (INCLUDING NEGLIGENCE OR STRICT LIABILITY) OR OTHERWISE, INCLUDING BUT NOT LIMITED TO LOSS OF USE; LOSS OF REVENUE; LOSS OF ACTUAL OR ANTICIPATED PROFITS (INCLUDING LOSS OF PROFITS ON CONTRACTS); LOSS OF THE USE OF MONEY; LOSS OF ANTICIPATED SAVINGS; LOSS OF BUSINESS; LOSS OF OPPORTUNITY; LOSS OF GOODWILL; LOSS OF REPUTATION, WHETHER OR NOT ELSAG IS OR HAS BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES.

For technical support or to arrange for service on your ELSAG product, call our toll free 24 hour hotline at 1-866-9MPH900.

TOWN OF BEDFORD

425 CHERRY ST.
BEDFORD HILLS, NY 10507
PHONE # (914) 666-8283 FAX # (914) 666-8025
Federal ID: 136007284

PO Number : 156694
Date : 01/13/2011
Page: 1 of 1

Purchase Order

Vendor : [redacted]
ELSAG NORTH AMERICA LAW ENFORCEMENT SYSTEMS
412 CLOCK TOWER COMMONS
BREWSTER, NY 10509
205-H Creek Ridge Road
Greensboro, NC 27406

Ship To:
POLICE DEPT.
307 BEDFORD RD.
BEDFORD HILLS, NY 10507

Bill To:
POLICE DEPT.
307 BEDFORD RD.
BEDFORD HILLS, NY 10507

PHONE # (845) 278-5425 **FAX #**

Description: 2011 ONE YEAR RENEWAL OF WARRANTY

Qty.	Unit	Description	Unit Price	Amount
		ONE YEAR RENEWAL OF WARRANTY 001.3120.0432		2,000.00
			Total:	$2,000.00

Its state contract
at the price went down 1750.00

CONDITIONS - READ CAREFULLY

1. IMPORTANT: INVOICE, PACKAGES AND CORRESPONDENCE MUST BEAR THIS PURCHASE ORDER NO.
2. EACH SHIPMENT MUST BE COVERED BY SEPARATE INVOICE.
3. THE RIGHT IS RESERVED TO CANCEL THIS ORDER IF NOT FILLED WITHIN THE PRESCRIBED TIME.
4. THE CONDITIONS OF THIS ORDER ARE NOT TO BE MODIFIED BY ANY VERBAL UNDERSTANDING.
5. CHARGES FOR BOXING OR CARTAGE WILL NOT ALLOWED UNLESS PREVIOUSLY AGREED UPON.
6. ALL SHIPMENTS ARE TO BE MADE PREPAID.
7. WHERE APPLICABLE ATTACH DELIVERY SLIPS SIGNED BY THE MUNICIPAL EMPLOYEE RECEIVING THE MATERIALS.
8. IN ORDER TO EXPEDITE PAYMENT, YOUR INVOICE SHOULD BE RETURNED PROMPTLY AFTER THE SERVICES HAVE BEEN RENDERED OR THE MATERIALS HAVE BEEN FURNISHED.

Ordered By: CTIEN Req. Date: 01/13/2011 Req. Number: 18634 Approved By:

Authorized Official

1/20/11
Date

ELSAG North America
205-H Creek Ridge Road
Greensboro, NC 27406

INVOICE

Invoice Number: 13968
Invoice Date: Jan 15, 2011
Page: 1

Voice: 336-379-7135
Fax: 336-379-7164

Bill To:	Ship to:
Town of Bedford Police Dept 307 Bedford Road Bedford Hills, NY 10507 United States	Town of Bedford Police Dept 425 Cherry St Bedford Hills, NY 10507 United States

Customer ID	Customer PO	Payment Terms	
BEDFORD PD - NY	[redacted]	Net 15 Days	
Sales Rep ID	**Shipping Method**	**Ship Date**	**Due Date**
DIRECT SALES	Fed-Ex		1/30/11

Quantity	Item	Description	Unit Price	Amount
1.00	520003	Service Plan Year 3	875.00	875.00
1.00	520004	Service Plan Year 4	875.00	875.00

Subtotal	1,750.00
Sales Tax	
Total Invoice Amount	1,750.00
Payment/Credit Applied	
TOTAL	**1,750.00**

Check/Credit Memo No:

Overdue invoices are subject to late charges.

REMINGTON ELSAG LAW ENFORCEMENT SYSTEMS, LLC

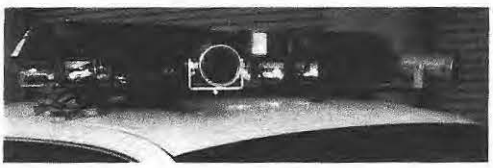
RELES MPH-900 Mobile LPR System

Remington ELSAG Law Enforcement Systems, the world leader in License Plate reading technology and deployment, offers the MPH900 as a solution for mobile automatic license plate reading. This system reads plates from a stationary location or at highway speeds and cross references them against an onboard hotlist. The system alarms within a second of identifying a plate on the hotlist and can process hundreds of plates per minute. An image and GPS coordinates of every plate scanned are stored and can be referenced later.

The MPH900 provides two sets of benefits:

Real-time Intervention
- Watch List Filtering
- Probable Cause generation for unbiased, targeted search
- Auto theft recovery
- Plate manipulation
- Rental Contract violations

Intelligence Gathering
- Link Analysis
- Recurring traffic pattern analysis
- Suspect surveillance
- "Late Hit" analysis
- Coordination with Mobile Plate Hunters



Instantly Alarms on a Wanted Plate

- Alarms can display on a laptop computer (sold separately) or on an M.D.T.
- Alarms can be broadcast to an operations center or to a support vehicle
- System can accommodate a hotlist of 4 Million lines of data, can combine data from different sources
- Has the ability to receive and transmit wireless updates
- Works day or night in all weather conditions

Pricing and Support

Item#	Description	LIST PRICE	OGS 1-9 Units	OGS 10-24 Units	OGS 25+ Units
MPH-900	MPH-900 LPR System	**$21,000**	$20,100	$18,425	$16,800

Technical Support and Maintenance are free for the first year and 5% (5% OGS - 10% non-OGS) of system cost thereafter. Support includes software upgrades.

We can be reached toll free at 1-866-967-4900 or **www.remingtonelsag.com**
870 Remington Drive, Madison, NC 27025

ELSAG North America

11/12/2009
QUOTATION

205 H Creek Ridge Rd
Greensboro, NC 27406

Duns # 196140821
Phone: 866-9MPH900 (967-4900)
Fax: 336-379-7164

Delivered to:
Town of Bedford Police
Jeff Dickan
307 Bedford Rd
Bedford, NY 10507

Quotation valid until: January 11, 2010
Prepared by: Kevin Bauersfeld
Projected Arrival Date: TBD

NASPO Multi-State Contract #PC62119 Award #19745
(California Participating Addendum)
WSCA # PC 62119 Hazardous Incident Response Equipment
(Contract term: 5/20/2007 - 5/10/2010)

Model #	Description	Cost	Units	Amount
MPH-900CamCable	Replacement Cable set for MPH-900, 15' power, Sheilded ethernet.	$150	1	$150.00
MPH-900INSTALL	Charge per vehicle for standard MPH-900 installation.	$900	1	$900.00
Phone Support	24 Hour Telephone Support by qualified MPH-900 technicians			**FREE**
ON-SITE TRAINING	Included in the purchase of both transportable and permanent MPH-900 installations available in group and individual sessions.			**FREE**
TRAINING CENTER MEMBERSHIP	Unlimited access to ELSAG North America training classes held either in the field or at Company Facilities.			**FREE**
			TOTAL	$1,050.00

Service Plan for goods and services provided by the above quote

			Due Date
Year I	Free	Hardware and Software	
Year II	$53	Hardware and Software	1 year after receipt
Year III	$53	Hardware and Software	2 years after receipt
Year IV	$53	Hardware and Software	3 years after receipt
Beyond	$32	Software Only	4 years after receipt

Service Plan Includes:
- Software Updates
- Annual Training/Service
- Parts & Labor

Approval Signature:_____

Terms: 2% Net 15 Days 1%30 Days Receipt of Goods

Cash Discount Value if paid in 15days	$21.00
Cash Discount Value if paid in 30 days	$10.50

MPH900™
Mobile Plate Hunter 900 Series

Software Installation Instructions for ENA MPH™900

Rev. C

If you need technical assistance, please contact us at

Elsag North America
412 Clock Tower Commons, Brewster, NY 10509 –
866 967 4900 or 1-866-9MPH900
336 379 7135

e-mail

techsupport@elsagna.com

Web:
WWW.ELSAGNA.COM

MPH900™
Mobile Plate Hunter 900 Series

About this guide

This guide explains how to install and configure the Mobile Plate Hunter 900 software.

Sections 1-2-3 include all system prerequisites and additional information you will need to install successfully the Mobile Plate Hunter 900 software.
Section 4 gives a few hints on how to upgrade from previous versions of the system

Section 5 6 and will guide you through the installation of the CarSystem Software Components

Section 7 will explain how to install the CarSystem when the wireless communication module is needed.
Sections 8 and 9 shows how to configure the Login and the system configuration.

Section 10 explains how to setup the Static IP Address in the host computer.

Section 11 is related to the installation of the Cartography module.

Sections 12 provide details on testing the Mobile Plate Hunter 900 after the setup procedure has been completed.

Sections 13 and 14 explain how to upgrade firmware and protocols on the MPH900 processor PUMA Lite configuration.

Sections 15 and 16 describe the Firmware and protocols loading procedures for AD3M cameras.

Sections 17-23 provides procedures on how to configure the AD3 system.

Revision History

Ver.	Date	Description	Author
1.2.0	3/02/2006	Kit 1.2.0 – CarSystem 2.9.0	Leeps
4.2.0	8/10/2006	Kit 4.2.0 – CarSystem 3.3.2	Masciangelo
4.3.0	11/08/2006	Kit 4.3.0 – CarSystem 3.4.0	Masciangelo
6.0.0	01/15/2008	Kit 6.0.0 – CarSystem 4.3.0 and Puma Lite configuration	Masciangelo
A	06/17/2008	CarSystem 4.5.0 Puma and AD3M manuals have been merged.	Masciangelo, Gonzalez
B	8/5/2008	Added Hot List from USB, AD3 recovery procedure, password reset and IP change procedures	Masciangelo, Gonzalez
C	12/12/2008	CarSystem 4.7.1; AD3 Firmware 2.0.0	Masciangelo, Gonzalez

MPH900™
Mobile Plate Hunter 900 Series

TABLE OF CONTENTS

MPH900™
Mobile Plate Hunter 900 Series

1 Introduction

This guide explains how to install the on board user interface, called CarSystem, onto the MDT, laptop or PC that is connected to the MPH™900 LPR (License Plates Readers) systems.
The document also explains how to load firmware and OCR configuration protocols onto the processor
The MPH™900 is a family of License Plate Reading System. The most recent products are:

- Puma Lite;
- AD3 M (dual sensor color and b/w cameras).

The current document is not applicable to Puma systems.

Puma Lite

The system components are:

- a pair of IR cameras,
- the MPH900 processor also called PUMA,
- a Mobile Data Terminal (MDT) hosting the on-board user interface,

AD3M

The system components are:

- a set of dual sensor (color and IR) LPR cameras
- a power and junction box
- a Mobile Data Terminal (MDT) hosting the on-board user interface.

The cameras are IP devices that include an OCR processor. Each camera is accessible via LAN through their Static IP address.

AD3M System Overview

Figure 1 shows the system components and their connections. Each vehicle can be equipped with up to 4 Smart LPR cameras (AD3-M).
Every camera is characterized by its own static IP address and a unique ID. Cameras have different focal length to adapt to different traffic conditions and application requirements. Available optics ranges from 12 mm to 50 mm for the black/white cameras. Usually there is a different parameters configuration (protocol) for every focal length.
The LPR cameras are connected to a junction and power supply box (AD3-MPW) through provided cables. The AD3-MPW device includes a LAN switch that connects all the cameras to the MDT or other on-board PC, the power supply module and an access point (WLAN) 802.11 G. The WLAN access point can be optionally used to connect the MDT to an Operation Center wirelessly or to connect external LPR cameras to the MDT. Up to 4 more cameras can be deployed remotely and linked to the same on-board PC.
The AD3-MPW device is powered from a vehicular 12 V source: It could be either directly the battery (permanent install) or a cigarette lighter socket (transportable).

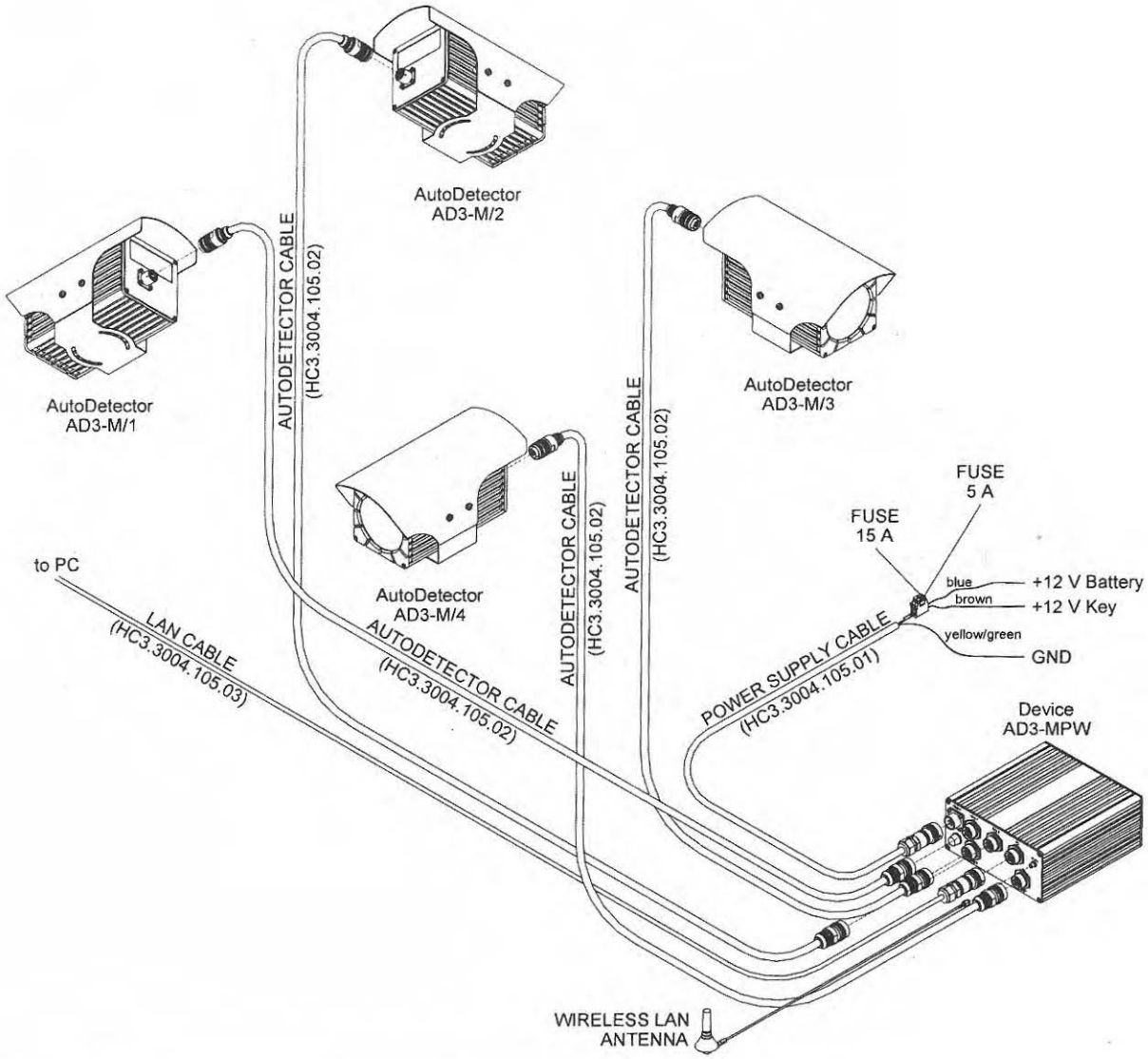


Figure 1: The picture shows the system hardware components and their connection.

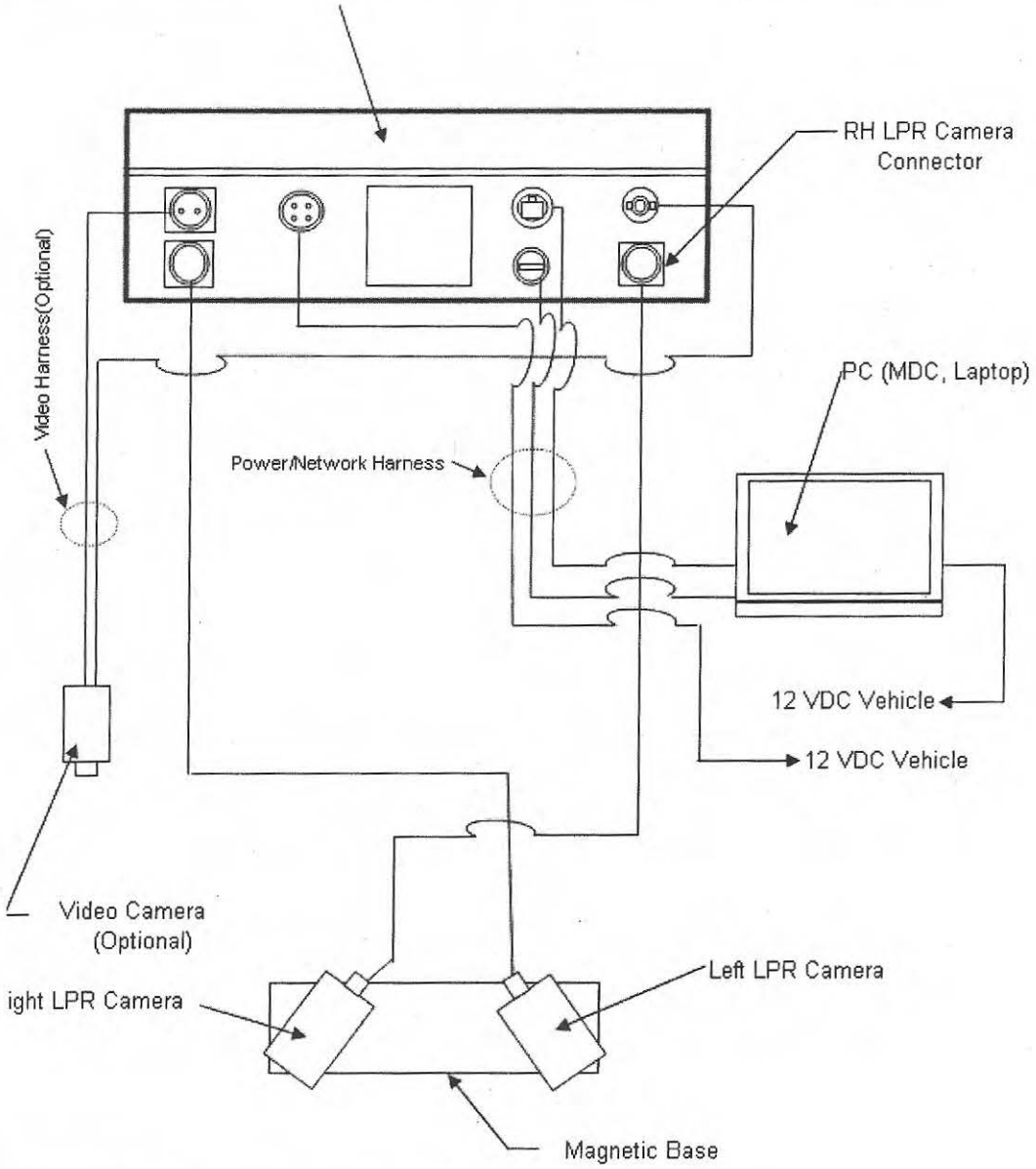


Figure 2: Schematics of Puma Lite system (transportable configuration).

2 Software License Agreement

This End User License Agreement (the "Agreement") is a legal agreement between you (the "End User"), and Elsag Spa (hereinafter "Elsag") regarding the use of Elsag proprietary software installed, pre-loaded or embedded with Elsag products (the "Software") for which there is no separate license agreement between you and Elsag itself. By opening or breaking the seal on the Software packet(s), and/or using the Software, you agree to be bound by the terms of this Agreement. If you do not agree to these terms, promptly return all Software items (disks, written materials, and packaging) and delete any preloaded or embedded Software.

LICENSE

This Agreement is not for the sale of Software or any other intellectual property. Elsag owns all title and intellectual property rights in and to Software. Elsag, the manufacturer and owner of the Software, reserves all rights not expressly granted under this Agreement.
This Agreement permits the End User to use one copy of the Software, for internal purposes only, on only one computer and only by a user, at a time.
If you have multiple licenses for the Software, you may use as many copies at any time as you have licenses. "Use" means loading the Software in temporary memory or permanent storage on the computer or Elsag product.
The End User hereby grants Elsag the right to perform an audit of the End User's use of the Software during normal business hours; the End User agrees to cooperate with Elsag in such audit, and the End User agrees to provide Elsag with all records reasonably related to the End User's use of the Software. The audit will be limited to verification of the End User compliance with the terms of this Agreement.

COPYRIGHT

The Software is owned by Elsag and is protected by Italian copyright laws and international treaties provisions. Therefore, the End User may not use, copy or distribute the Software without Elsag authorization.
The End User may make one copy of the Software solely for backup or archival purposes or transfer it to a single hard disk provided the End User keeps the original solely for backup or archival purposes.
The End User may not copy the printed materials accompanying the Software, nor print copies of any user documentation provided in any form.

RESTRICTIONS

The End User may not rent, lease, or loan the Software, but the End User may transfer his rights under this Agreement permanently, provided the End User transfers this Agreement, the Software and all accompanying printed materials, retains no copies, and the recipient agrees to the terms of this Agreement.
The End User may not reverse engineer, decompile, or disassemble the Software, except to the extent the foregoing restriction is expressly prohibited by applicable law. The End User may not modify or create derivative works based upon the Software.

LIMITED WARRANTY

Elsag warrants that the means on which the Software is furnished will be free under normal use from defects in materials and workmanship for a period of ninety (90) days from the date of receipt. This warranty is limited to the End User and is not transferable. Any implied warranties are limited to ninety (90) days from the date the End User receives the Software. The entire liability of Elsag, and the End User exclusive remedy, shall be replacement of the defective

means not meeting this warranty that is returned to Elsag with a copy of the End User receipt. This limited warranty is void if failure of the Software has resulted from accident, abuse or misapplication. Any replacement Software is warranted for the remaining original warranty period or thirty (30) days, whichever is longer.

Elsag does NOT warrant that the functions of the Software will meet your requirements or that operation of the Software will be uninterrupted or error free. The End User assumes responsibility for selecting the Software to achieve the End User intended results and for the use and results obtained from the Software.

TO THE EXTENT PERMITTED BY APPLICABLE LAW ELSAGDISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT WITH RESPECT TO THE SOFTWARE AND ALL ACCOMPANYING WRITTEN MATERIALS.
THE MAXIMUM LIABILITY OF ELSAG SHALL IN ANY EVENT NOT EXCEED THE SUM OF THE LICENSE FEE PAID FOR THE SOFTWARE.

NO LIABILITY FOR CONSEQUENTIAL DAMAGES

IN NO EVENT SHALL ELSAG BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR OTHER PECUNIARY LOSS) ARISING OUT OF USE OR INABILITY TO USE THE SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

ESSENTIALITY OF TERMS

The above provisions of Paragraph 4 on LIMITED WARRANTY, Paragraph 5 on NO LIABILITY FOR CONSEQUENTIAL DAMAGES constitutes essential parts and fundamental elements of the basis of this Agreement. Elsag would not be able to provide the Software without such limitations.

TERMINATION

This Agreement is effective until terminated. This Agreement will terminate immediately without notice from Elsag if the End User fails to comply with any of its provisions.
Upon termination the End User must destroy the Software and all copies thereof and the End User may terminate this Agreement at any time by doing so.

GENERAL

This Agreement is governed by the laws of Italy.
Any dispute between the End User and Elsag regarding this Agreement will be subject to the exclusive venue of the Court of Genoa (Italy).
This Agreement is the entire agreement between the End User and Elsag and supersedes any other agreement between them with respect to the Software.
If any provision of this Agreement is held invalid, the remainder of this Agreement will continue in full force and effect.

3 Prerequisites

The computer must be running Windows 2000 Professional, Service Pack 2 or higher or Windows XP professional, Service Pack 2.
The computer hardware minimal requirements are the following:

- Pentium 4 1 GHz with 512 MB
- 800X600 minimal display Resolution
- 5 GB hard disk space available
- LAN data port for connecting the PC to the Junction and Power box; if an on-board LAN is already present, a switch port must be available and the IP address of the cameras can be adapted for the existing IP class. USB 2.0 port
- 2xUSB ports
- Logged in user must have read/write access to the Elsag SpA folder in Program Files

The installer must be logged on with Administrator privileges.

For best performance, the hibernation option and screen-savers should be turned off.
It is not necessary to connect the cameras (as in Figure 1) during the software installation process.

GPS receiver installation

To use the localization feature you may use any NMEA compliant GPS. It needs to be configured prior to the install of MPH™ 900 software. Make note of which Com Port the GPS Antenna is using, you will need this information later to install the GPS module.

If the GPS receiver is a USB device, make sure to use always the same USB port of the on-board PC. Change of the physical port may result in a change of the logical port known to the system.

NOTE: The software driver must be installed **first** before connecting the GPS device to the MDT or computer. Failure to do so might result in the GPS not functioning.

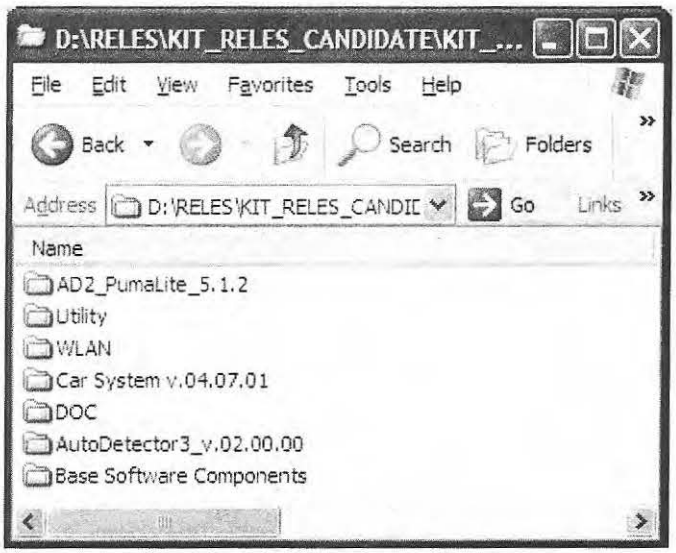


Fig. 3.1: Kit tree structure

The software kit is now unique for Puma_Lite and AD3M systems.
The directory Kit_Reles_[version] (see Fig. 3.1) contains the following subfolders:

- **Base Software Components** – This includes the off-the-shelf components installed for the Car System: MWP (proprietary Middleware package), MSDE (Microsoft Data Engine) and the current .NET package.
- **Car System v.[version]** – Installation files for the in-car PC software.
- **AD2_PumaLite_[version]**– This folder contains the Firmware to be loaded into the PUMA processor and, under Tools, the programs needed to load firmware and protocols.
- **DOC**- User manuals and Documentation is available in this folder.
- **AutoDetector3_[version]**– This folder contains the Firmware preloaded into the LPR cameras.
- **Utility** – Additional installation files including, GPS drivers, the Discovery tool to used to load firmware and protocols, the Java Engine.

The directory Kit_PROTOCOLS_PUMA_LITE_[version] contains the LPR protocols for the PUMA Lite. The protocols are organized by State.
USA_maps_[version] – This folder includes the setup kit for the optional on-board cartography module.
The directory **Kit_Protocols_AD3_[version]** includes the LPR protocols for AD3 cameras. The directory **KIT_PROTOCOLS_PUMA_LITE_[version]** includes LPR protocols for PUMA cameras.
It is advisable to copy the installation kit into the local machine before beginning the installation process.

4 Upgrade from previous versions

Upgrade from CarSystem 3.X.Y

If the *CarSystem* software is already installed in the PC, you may need to uninstall before proceeding with the installation of the new version.

The following procedure must be followed if the existing software comes from Reles_Kit_4.3.0 or Reles_Kit_5.0.0, corresponding to Car System 3.4.0.

- Uninstall CarSystem
- Uninstall MWP middleware
- Uninstall .NET Framework (optional)
- Restart computer

At this point, you can proceed to section 5 "Installation of the Base Software Components".

You don't need to re-install MSDE (step2).

Upgrade from CarSystem 4.X

- Uninstall *CarSystem*
- Uninstall maps
- Restart computer

At this point, you can proceed to the section "Installation of the software components".

You don't need to re-install MSDE (step2) or SQL 2005.

Upgrade from CarSystem 4.5.1

Note that the default installation folder has moved from **C:\Program Files\Elsag SpA\Car System** to **C:\Program Files\Car System**.
Also the maps version has changed to 2.2.0. *CarSystem* 4.7.1 is still compatible with maps 1.1.0.

5 Installation of the Base Software Components

In this section we describe the installation of the necessary off-the-shelf software components.

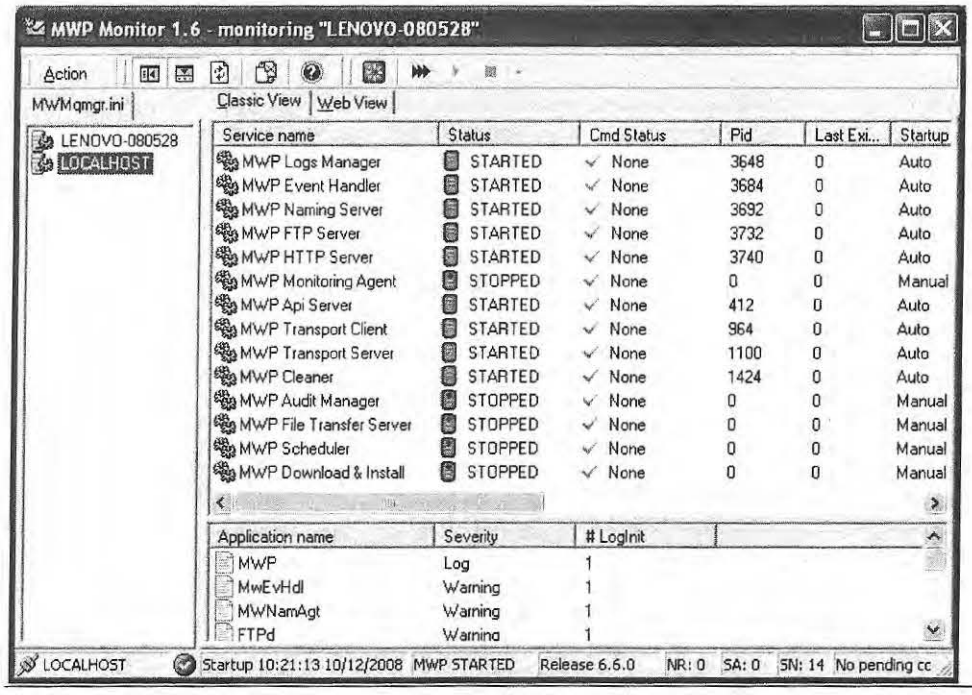
Temporarily disable any firewall, anti-virus and pop up blocking software currently running in the computer before launching the installation software.

Step 1

This is to install the proprietary middleware software.

- Run the Mwp66WinNT.exe setup program available under ..\Base Software Components\MWP v6.6
  - *Always select the default options.*
- Perform Windows system restart as requested.

After the Restart, launch the program Start-> Middleware MWP->Engine Monitor to check the correct installation of the Middleware. Double-click on LOCALHOST or the name of the computer as you can see from the figure below. The services you see in the figure below in red should be the only services stopped. Al others should be green. If the connection is successful and no other error messages are returned the installation has been successful and you can proceed to step 2.



Step 2

This step refers to the installation of the Microsoft Database Engine.
This step is required only if the Mission Report Module is installed. Otherwise skip setup 2 and perform step 3.

DbaMgr2k is a freeware program that allows connecting to the MSDE database and modifying application parameters, if needed.

1. Run the MSDE_Setup.exe setup program, under ..\Base Software Components \MSDE
2. Run the Setup_DbaMgr2k.exe setup program.
3. Perform Windows system restart.

After the restart, check that the MSSqlServer icon is present in the computer system tray (bottom – right of the screen) and that its small arrow is green.

It is possible to install the Microsoft SQL 2005 Express Edition database engine instead of MSDE.

Step 3

This is the Microsoft .NET framework. Install only if not already present in the system.

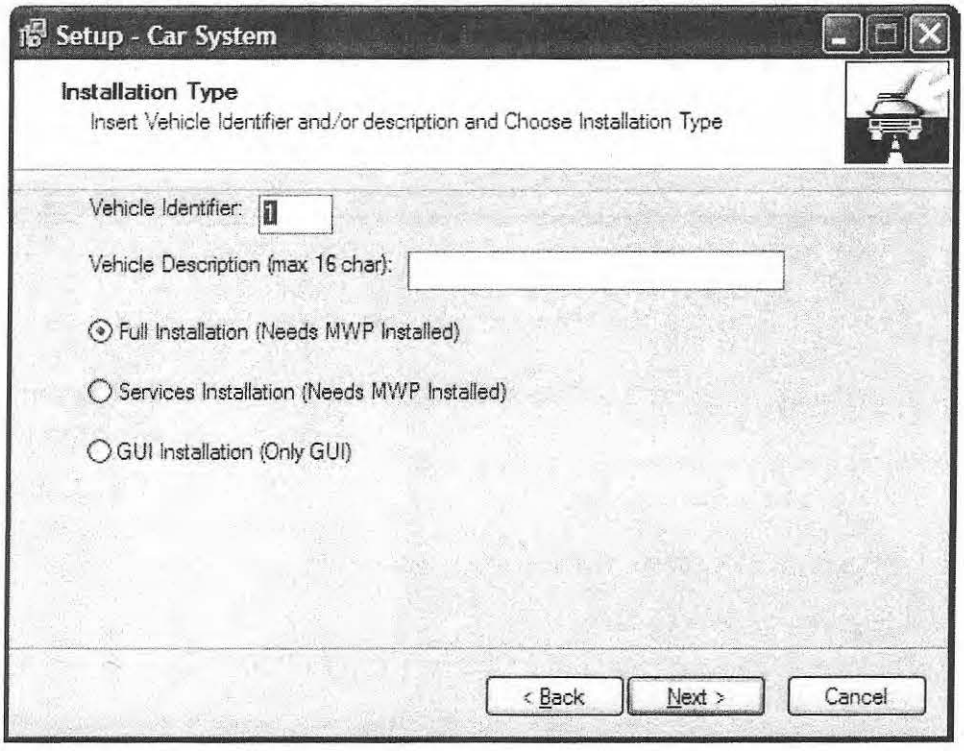
1. Run the dotnetfx.exe setup program from ..\Base Software Components\NET_FRAMEWORK_2.0

Note that the .Net Framework version is changed from 1.1 to 2.0. It is usually not necessary to uninstall the Framework if a previous version is already installed.

6 Installation of Stand Alone Car System

The stand alone ***CarSystem*** is not wirelessly connected to the Command Center. Optionally it's possible to transfer data to a Command Center via manual download and file transfer (i.e.: via flash drives).
Install the ***CarSystem*** components, according to the following steps:

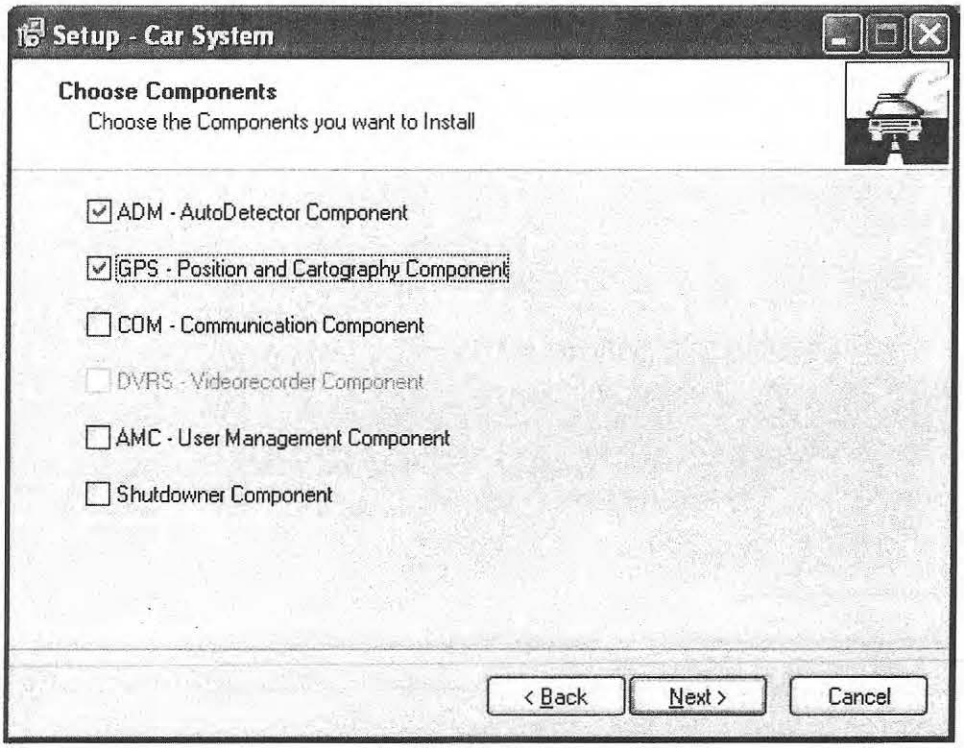
- Select RELES_CarSystem_Setup.exe from the ..\CarSystem_V<Version> folder and run the application
- You will have a Welcome window showing the ***CarSystem*** version number.
- Then the user will be requested to accept the License Agreement
- The next window will be the Installation Type: Enter a car number in the Vehicle Identifier field or leave 1 as default. The Vehicle Identifier is important to differentiate cars in the statistics reports when the application envisions more than one car. This is an internal identifier used when the unit is part of a fleet of vehicles coordinated by an Operation Center.



- Select Full Installation whenever the cameras are directly connected to a single MDT or on-board PC. If you are upgrading the system you can upgrade only the ***CarSystem*** Services or the User Interface. The CarSystem services are the software modules that communicate with the external devices, ranging from the

MPH™900X cameras to the GPS receiver. It is possible to split the services and the GUI into different computers networked together.

- Click next

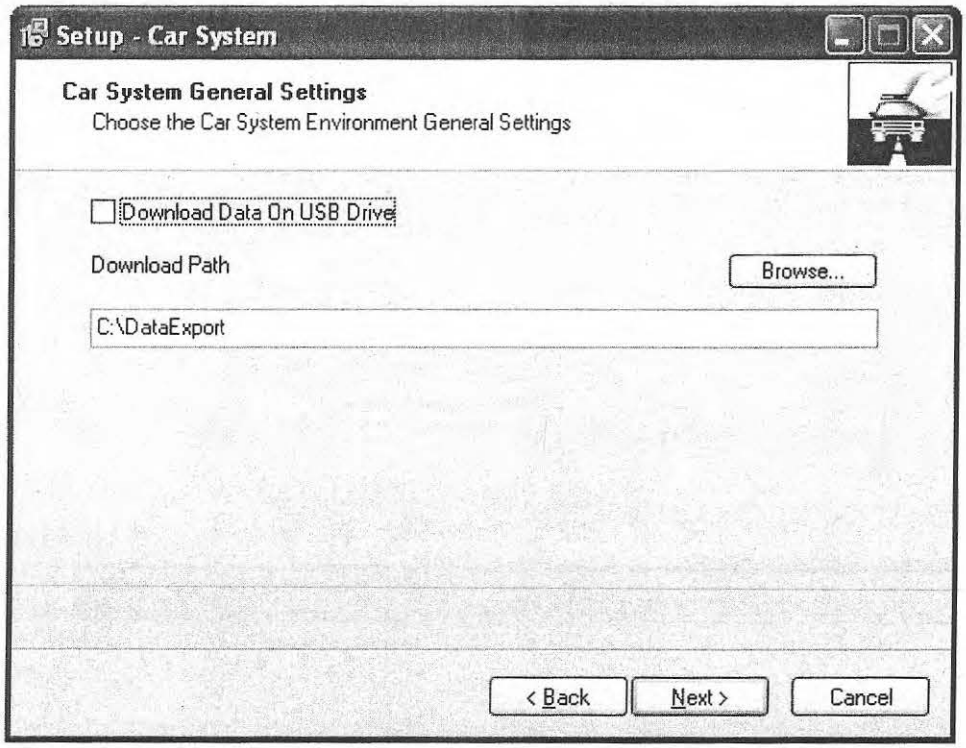


- Select *ADM-AutoDetector Component* to install LPR (License Plate Reader). This module is mandatory.
- Select *GPS – Position and Cartography Component*, if a GPS receiver is available and pre-installed
- Uncheck *COM Communication Component*; this option can be installed only with the optional Operation Center software on a remote server, if wireless communication (WLAN or Cellular) is available.
- Check *Shutdowner Component* if you want the ***CarSystem*** shutting down the XP computer when it closes.
- Check AMC-*User Management Component* if you want to setup user profiles for ***CarSystem***. If you uncheck this the ***CarSystem*** will automatically open up the user interface without requesting any password. If you want to add the Login system

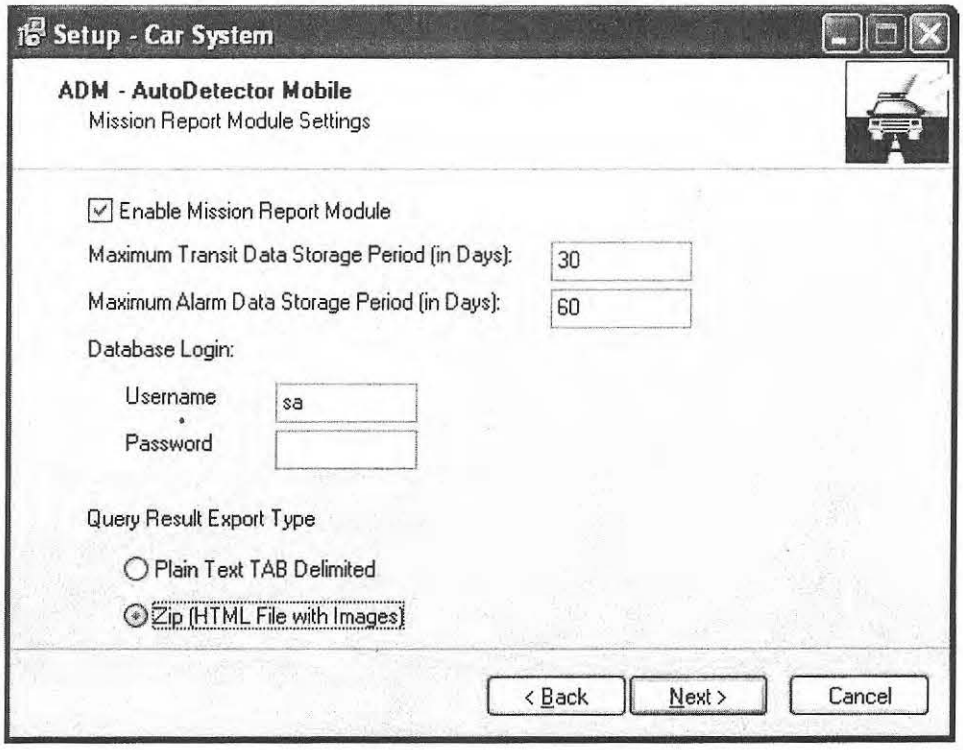
NEW

Click next

Below *Select Download Data On USB* if you want the data exported to a USB drive only. The *Download Path* option will be grayed out. Deselect it to download it to the C:\ drive and then Type in the path or Click Browse and select where you want the data to be exported to. This is only for a manual export of data and images from ***CarSystem***.



Click Next.



- Select *Enable Mission Report Module* to have the Mission Reporting features.
- Set *Maximum Transit Data Storage Period* (default is 5 days) and *Maximum Alarm Data Storage Period*. You may improve the Data Storage period to 30 days or more. That requires additional hard disk space occupation. Data older than the Maximum Data Storage Period are automatically discarded. Note that you can set different time periods for standard reads and alarms.

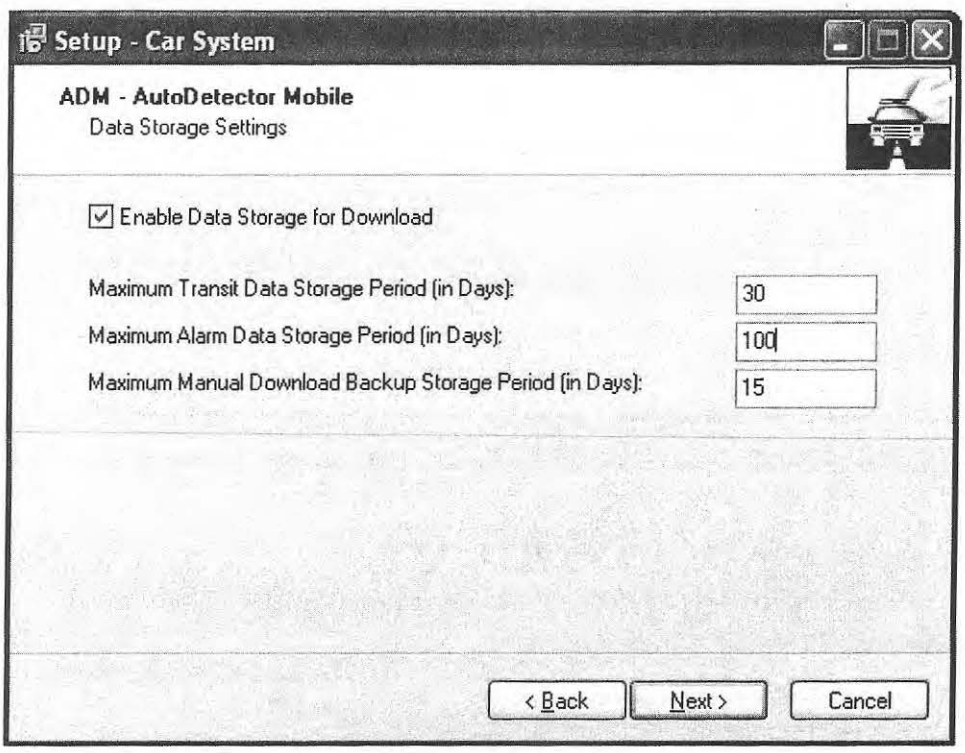
NEW

- The *Database Login* must be a valid Administrator level user of the MSDE or SQL database installed at step 2 or already existing in the computer. The MSDE default installation requires SA user with no password. The database Login is only used during installation but never at run time.
- For *Query Results Export Type* select Zip (HTML Files Images). In this case data and images will be exported as an HTML file with links to both b/w and color images).

Click next

Uncheck *Enable Data Storage for Download* unless the Manual Data Download feature is required. The feature allows the user to download read and alarm data in a proprietary format. Data can be imported into the optional MPH900 Operations Center module. This mode of operation is alternative to the automatic data download provided by the COM module.

This feature requires the installation of the optional Operations Center system on another computer.



NEW

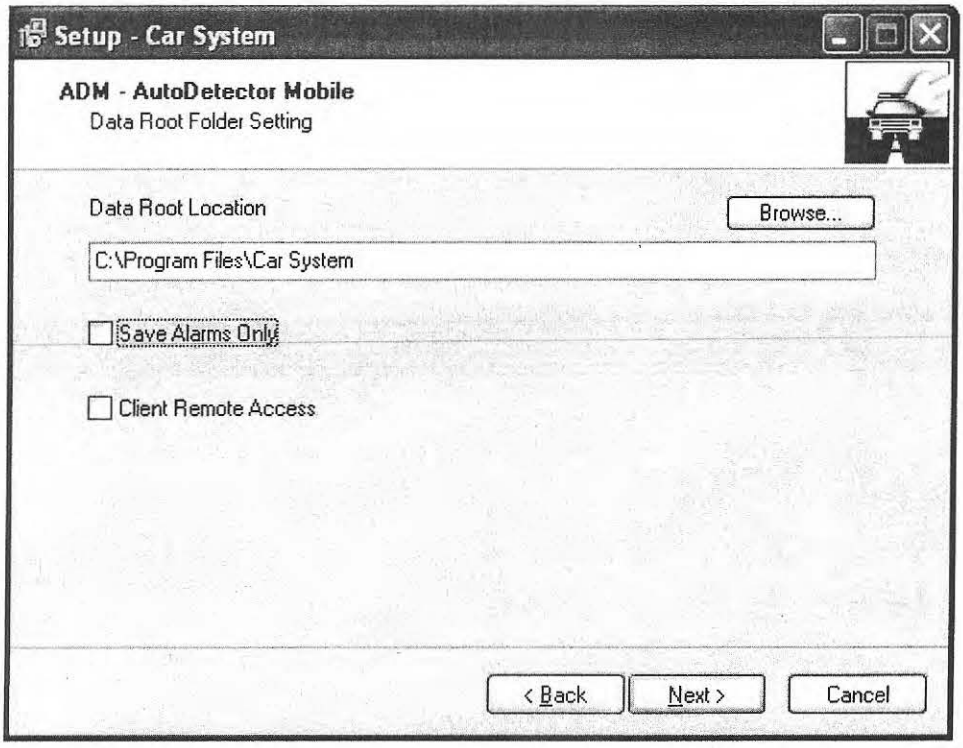
- *Maximum Data Storage period* is the time interval of local buffering of data to be downloaded to the Operations Center.
- *Maximum Alarm Data Storage Period* is the time in days you want to keep alarms.
- *Maximum Manual Download Backup Storage Period* is the time interval where already downloaded data are kept for backup in case the downloaded files are lost and a new copy is needed. Consider that each read is associated to two images for a total of about 70 KB. Determine the time intervals according to available hard disk space.

Click Next

For the Manual Data Download to be compatible with an existing Operations Center (Kit OPC_CARS_4.0.0 or earlier) a parameter must be modified after the completion of the CarSystem setup.

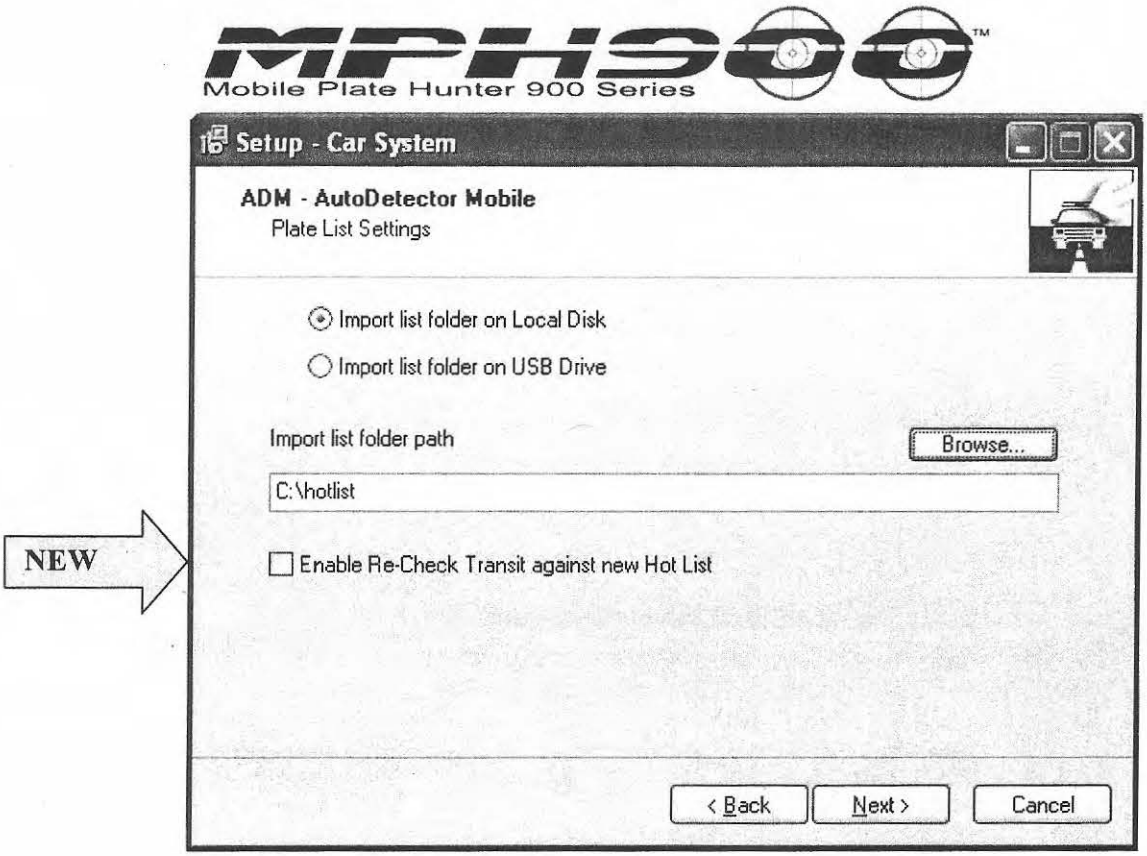
1) Open the LTBA.INI file under C:\Program File\CarSystem\Services\Config\
2) Modify the key MSDataFormat=0 to MSDataFormat=1 in the section [Mission Report]
3) Restart either MWP or the computer

The Operations Center software from Kit OPC_CARS_4.4.0 and above is compatible with the default installation; in this case there is no need to make the change.



Data Root Location allows the user to select the computer Drive and folder where to keep data, including images. The Drive must be local, network locations are not supported.

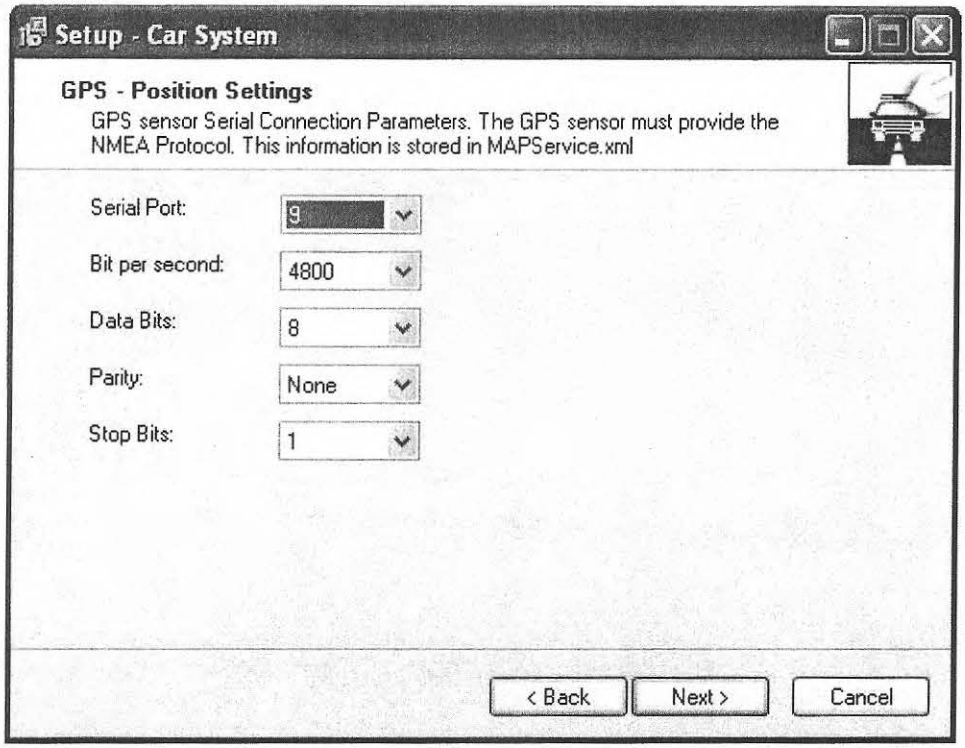
Click Next



In Plate List Settings you have the option to either load the hotlist to a specified folder on the system or you could load the hotlist directly from a USB drive by selecting "Import list folder on USB Drive. You could specify the import list folder in the box under "Import List folder path" or click browse to select the folder. The default path is C:\ListImport.
If you had a previous installation it is recommended that you change the path to C:\hotlist as in the image above.

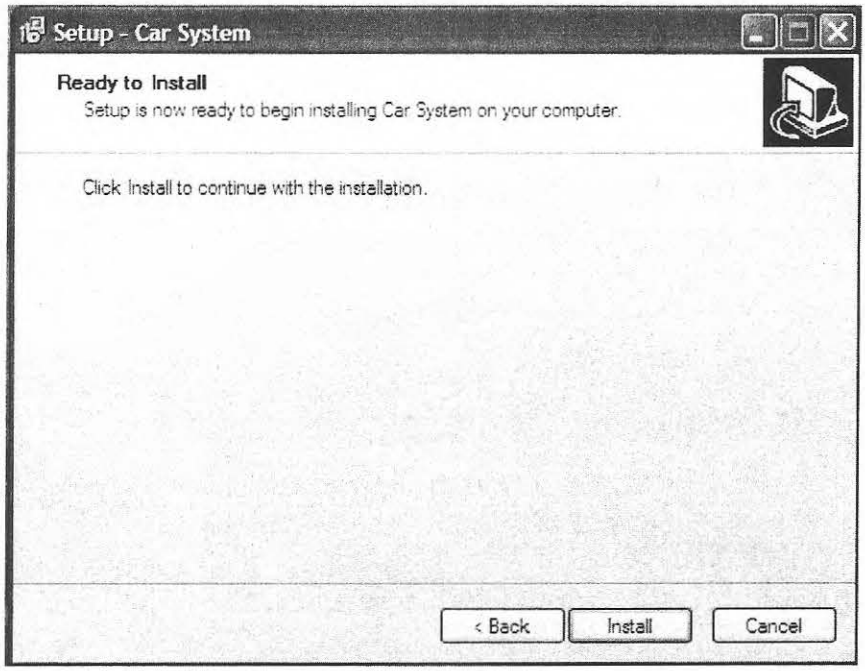
Uncheck Enable Re-Check Transit against new Hot List. This feature should not be used in this version of CarSystem.

Click Next.



- Enter Serial Port number of GPS (you can use the Device Manager from the Control Panel to find out the right port if the GPS antenna is connected to the computer). Default parameters other than the port are standard for NEMEA GPS.

  Click Next.



- Select Install

- Select Finish
- Windows system will restart.

7 Installation of the Car System with Communication component

In the previous section we described the default installation, which implies a manual import of the Hot List through a thumb drive. If the optional MPH900 Operation Center software is available, it is possible to configure an alternate architecture as shown in Figure 3: Schematics of wireless operations.

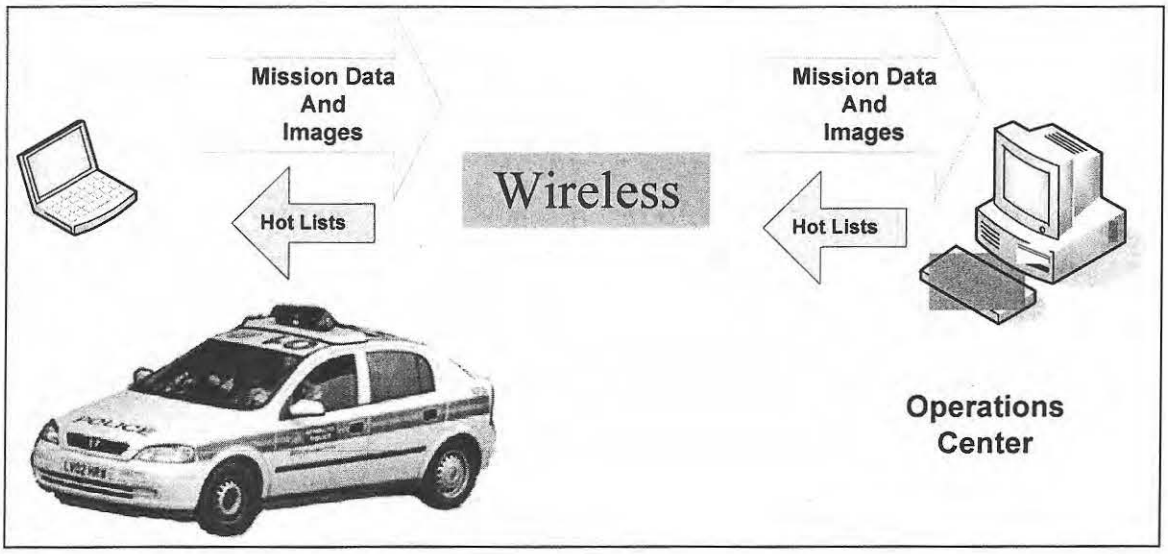


Figure 3: Schematics of wireless operations.

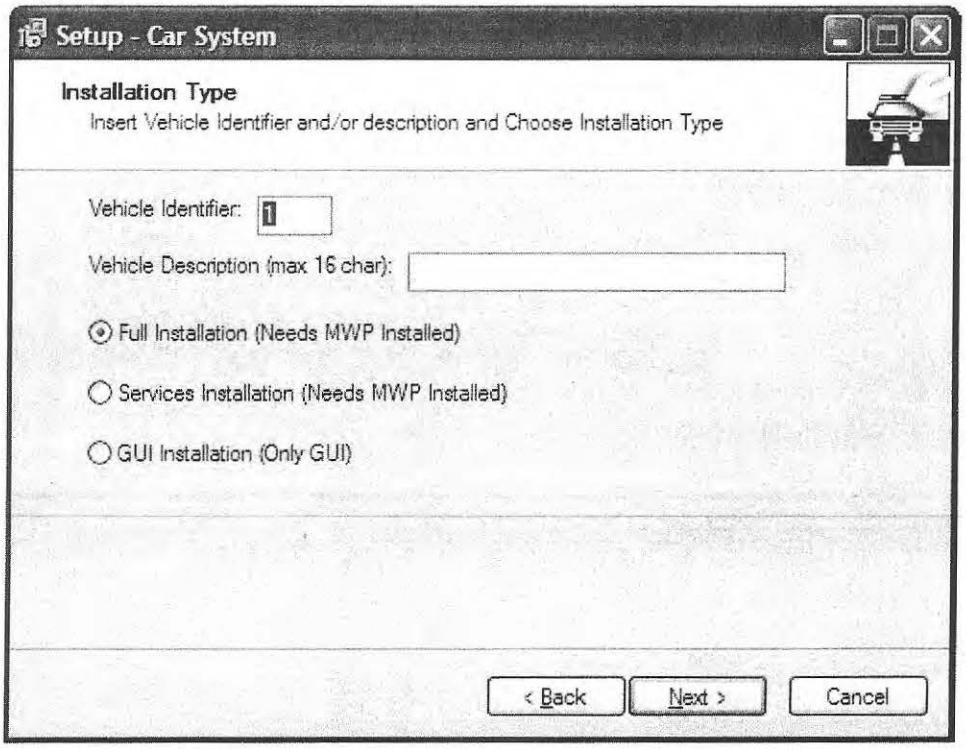
"Wireless" means any kind of WAN ranging from short range Wi-Fi to long range broadband cellular communications. The only requirements are the following;
The WAN (wide area network) or WLAN must support TCP/IP communication.
The network configuration must enable the FTP protocol. The car PC is the FTP client, while the Operations Center computer hosts the FTP server.

The installation of the Operations Center software and the availability of the WAN or WLAN are pre-requirements. In the following section we describe the CarSystem installation.
Up to Step 3 follow the standard procedure as shown in Section 5.

Install the ***CarSystem*** components, according to the following steps:

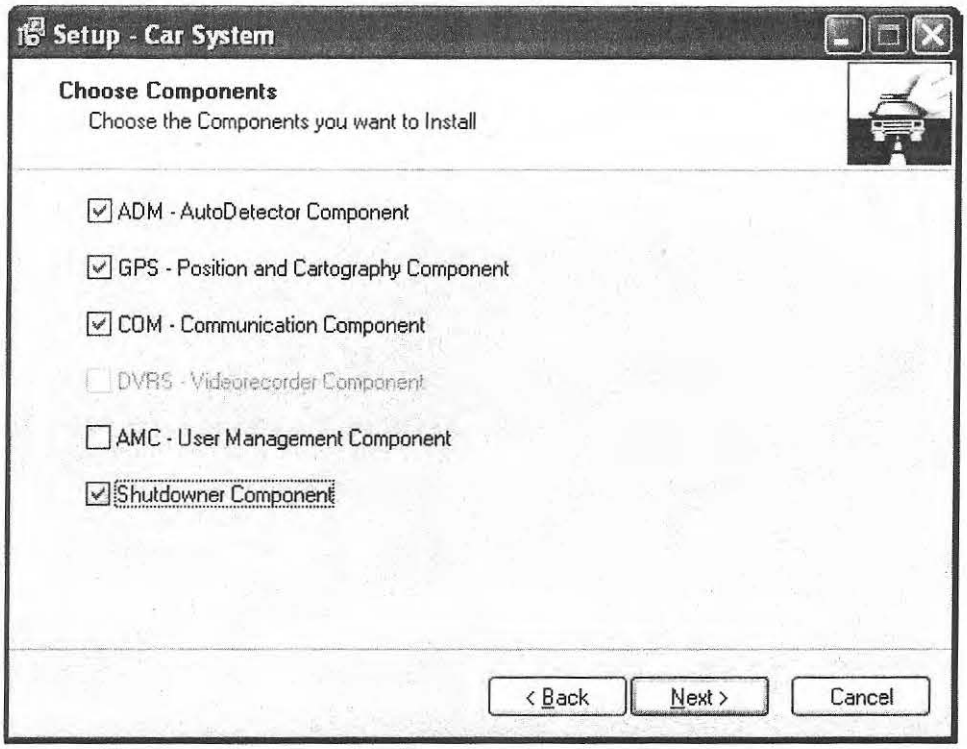
1) Select RELES_CarSystem_Setup.exe from the ..\CarSystem_V<Version> folder and run the application

2) You will have a Welcome window showing the CarSystem version number.
3) Then the user will be requested to accept the License Agreement
4) The next window will be the Installation Type: Enter a car number in the Vehicle Identifier field or leave 1 as default. The Vehicle Identifier is important to differentiate cars in the statistics reports when the application envisions more than one car. This is an internal identifier used when the unit is part of a fleet of vehicles coordinated by an Operation Center.



5) Select Full Installation whenever the cameras are directly connected to a single MDT or on-board PC. If you are upgrading the system you can upgrade only the CarSystem Services or the User Interface. The CarSystem services are the software modules that communicate with the external devices, ranging from the MPH™900 cameras to the GPS receiver. It is possible to split the services and the GUI into different computers networked together.

Click next



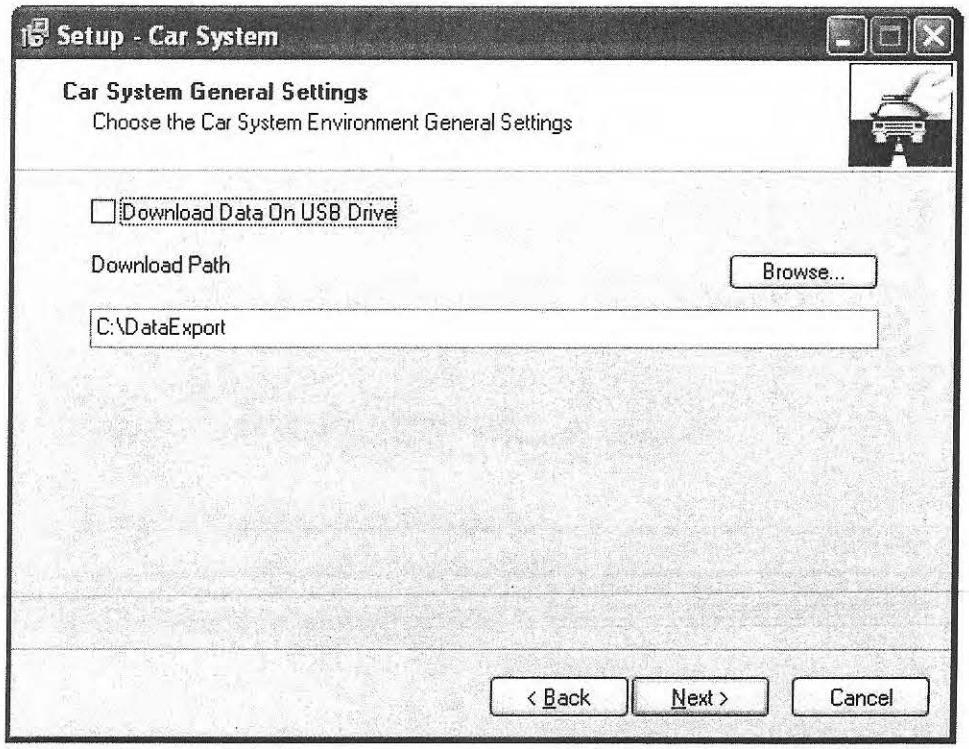
6) Select *ADM-AutoDetector Component* to install LPR (License Plate Reader). This module is mandatory.
7) Select *GPS – Position and Cartography Component*, if a GPS receiver is available and pre-installed
8) Select *COM Communication Component*.
9) Check *Shutdowner Component* if you want the CarSystem shutting down the XP computer when it closes.

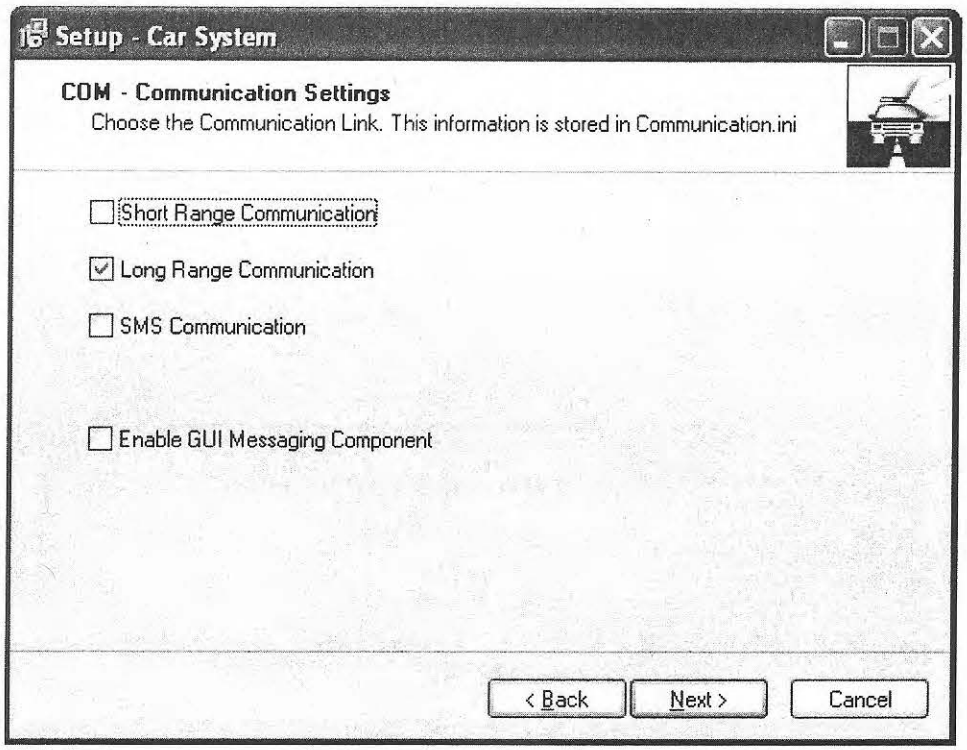
NEW

10) Check AMC-*User Management Component* if you want to setup user profiles for ***CarSystem***. If you uncheck this the ***CarSystem*** will automatically open up the user interface without requesting any password. If you want to add the Login system

Click next

11) Below *Select Download Data On USB Drive* if you want the data exported to a USB drive. The Download Path option will be grayed out. Deselect it to download it to the C:\ drive and then Type in the path or Click Browse and select where you want the data to be exported to. This is only for a manual export of data and images for ***CarSystem***, via the EXPORT function.





12) Select communication mode:

a. **Short Range Communication**: to operate by means of a short range device (e.g. Wi-Fi 802.11); connection is initiated when the vehicle is in the range of an Access Point and terminated when the vehicle exits the Access Point coverage area.
b. **Long Range Communication:** to operate by means of an Air Card device. The communication is optimized for "always-on" networks, such as any cellular broadband network.

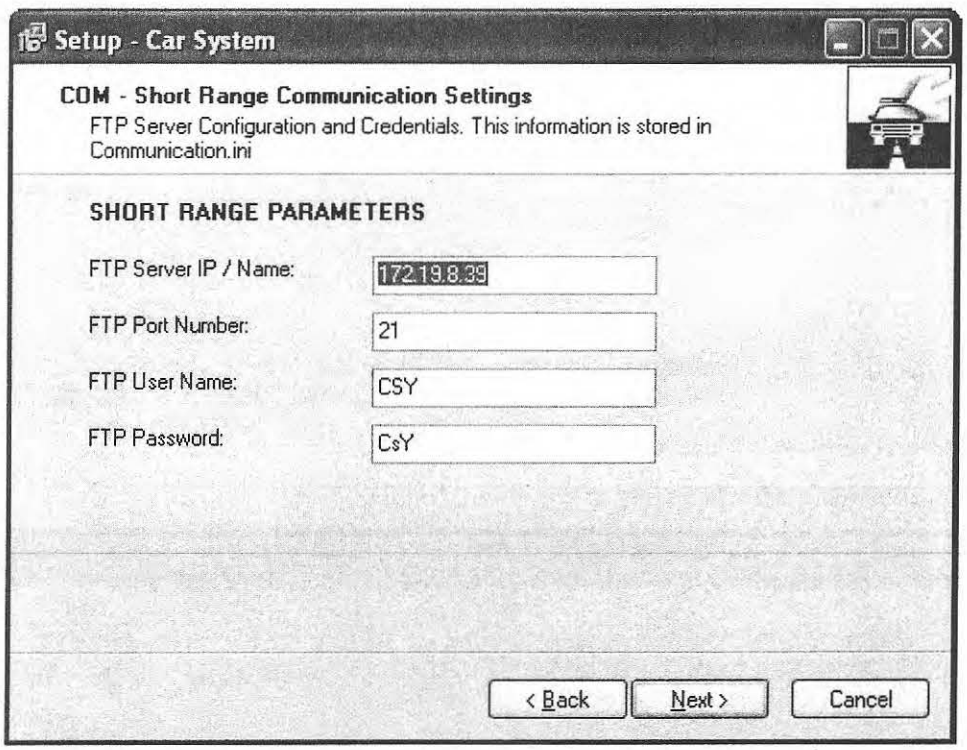
SMS Range Communication: to operate by means of GSM/Short Message Service; this feature requires the installation of a special GSM Modem.

Uncheck Enable GUI Messaging Component because this feature is not supported yet by the Command Center Software.

The following dialog box depends on the Communication type selection.

Short Range Communication Settings

Selecting "Short Range Communication" and Pressing "Next" the following window is presented.



- **FTP Server IP/Name**: the IP address or Name of the FTP server to communicate with;
- **FTP Port Number:** the port number of the FTP Server to communicate with; Use 21 unless there is a special need to change the FTP port.
- **FTP User Name:** the username to gain the access on the FTP server; This has to be CSY (Capital letter, case sensitive field)
- **FTP Password**: the password to gain the access on the FTP server; This has to be CsY (second character is a small letter).

The user has to fill all the required fields.

Long Range Communication Settings

Selecting "Long Range Communications" and pressing "Next" the following window is presented

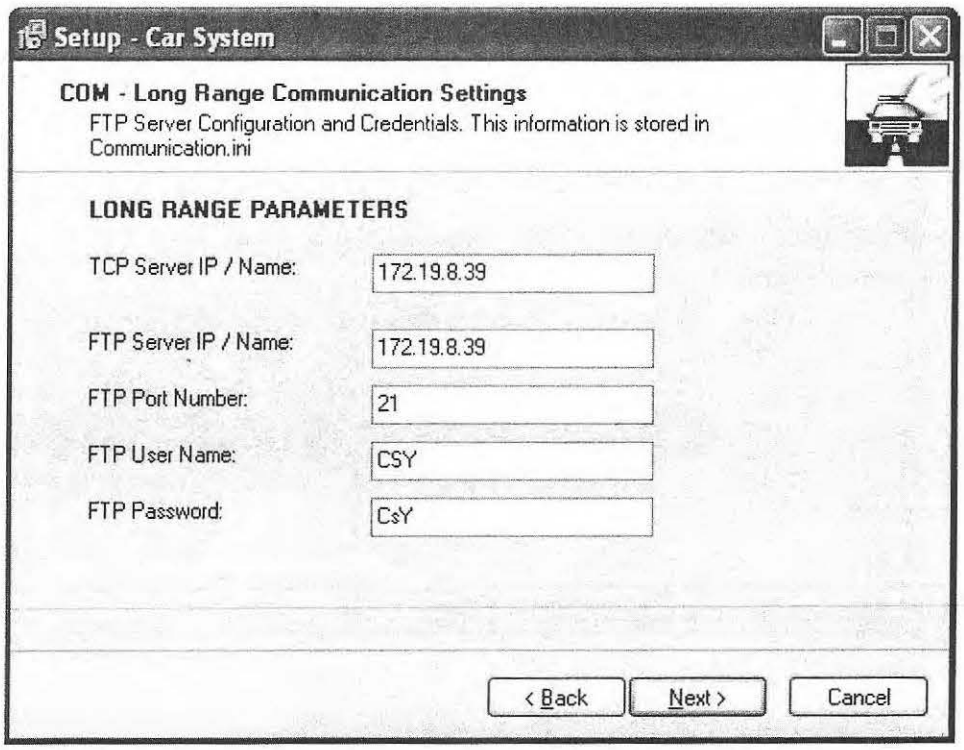


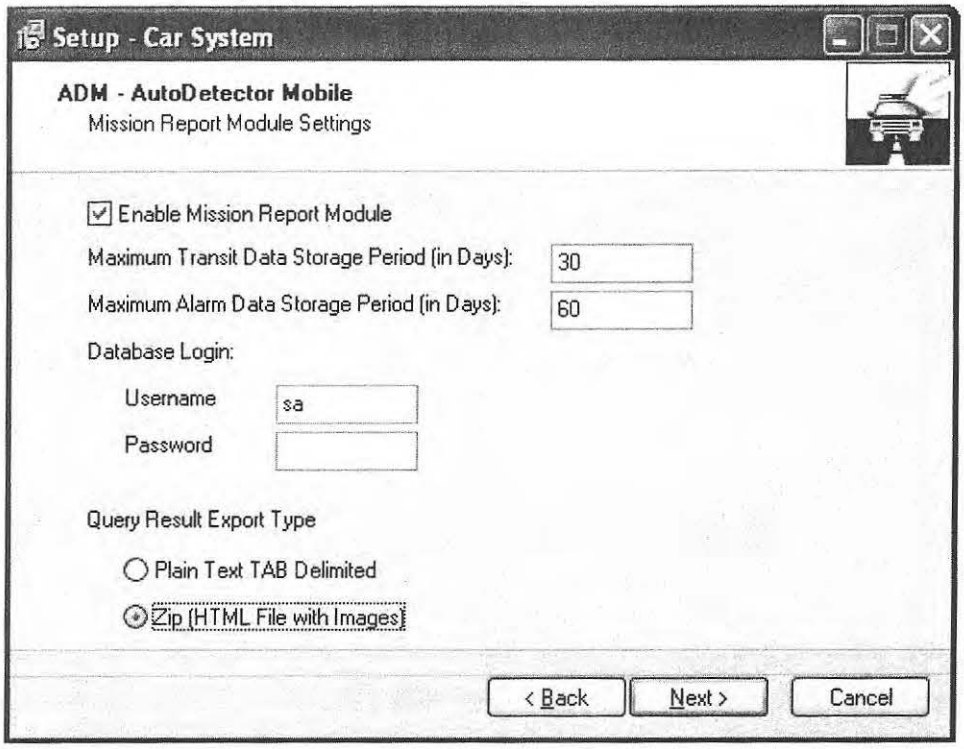
Figure 4– Long Range communication parameters

- **FTP Server IP/Name:** the IP address or Name of the FTP server to communicate with;
- **TCP Server IP / Name**: Not used. Just replicate the previous address.
- **FTP Port Number**: the port number of the FTP Server to communicate with; Use 21 unless there is a special need to change the FTP port.
- **FTP User Name**: the username to gain the access on the FTP server; This has to be CSY (Capital letter, case sensitive field)
- **FTP Password**: the password to gain the access on the FTP server; This has to be CsY (second character is a small letter).

The user has to fill all the required fields.

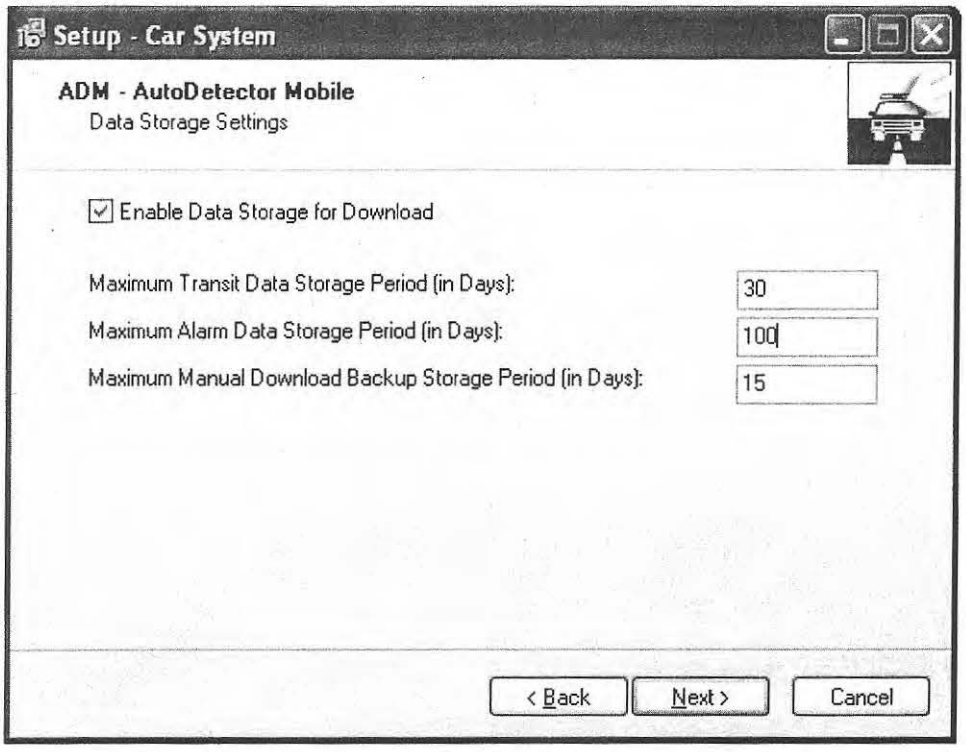
Click next.

The next dialog boxes are in common for both Communications modes.



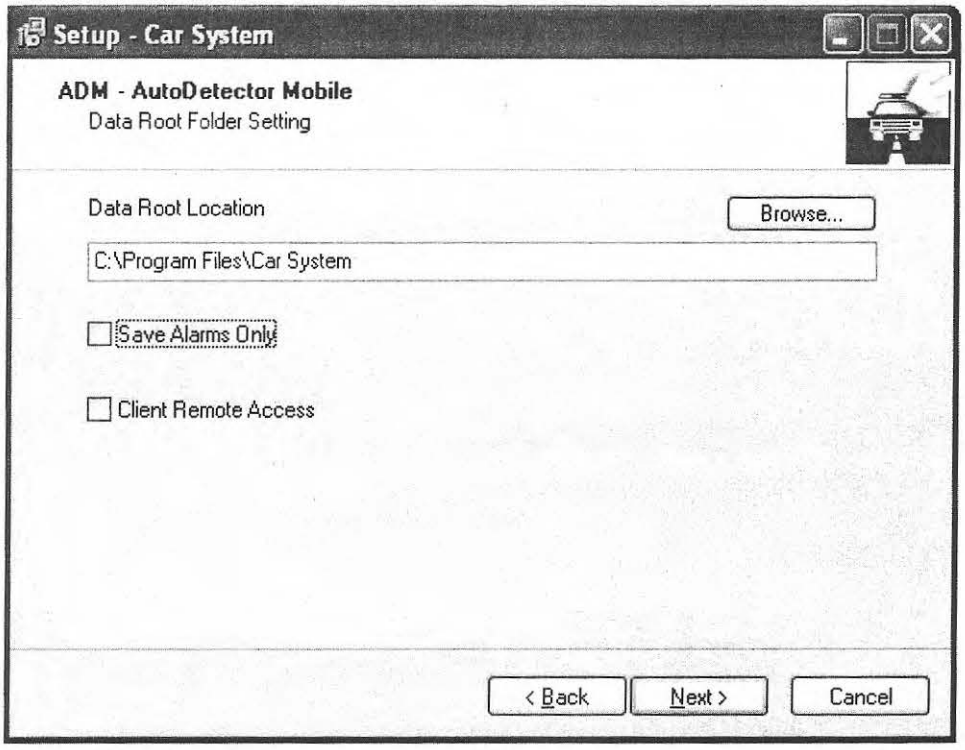
13) Select *Enable Mission Report Module* to have the Mission Reporting features.
14) Set *Maximum Transit Data Storage Period* (default is 5 days) and *Maximum Alarm Data Storage Period.* You may improve the Data Storage period to 30 days or more. That requires additional hard disk space occupation. Data older than the Maximum Data Storage Period are automatically discarded. Note that you can set different time periods for standard reads and alarms.
15) The Database Login must be a valid Administrator level user of the MSDE or SQL database installed or already existing in the computer. The MSDE default installation requires SA user with no password. The database Login is only used during installation but never at run time.

Click next.



16) Check *Enable Data Storage for Download.* This is mandatory when the Communication component is installed in order to provide local data storage for data waiting to be transmitted to the Operations Center.
17) *Maximum Data Storage Period* is the time interval of local buffering of data to be downloaded to the Operations Center.
18) *Maximum Alarm Data Storage Period* is the time in days you want to keep alarms
19) *Maximum Manual Download Backup Storage Period* is the time interval where already downloaded data are kept for backup in case the downloaded files are lost and a new copy is needed. Consider that each read is associated to two images for a total of about 70 KB. Determine the time intervals according to available hard disk space.

Click Next.

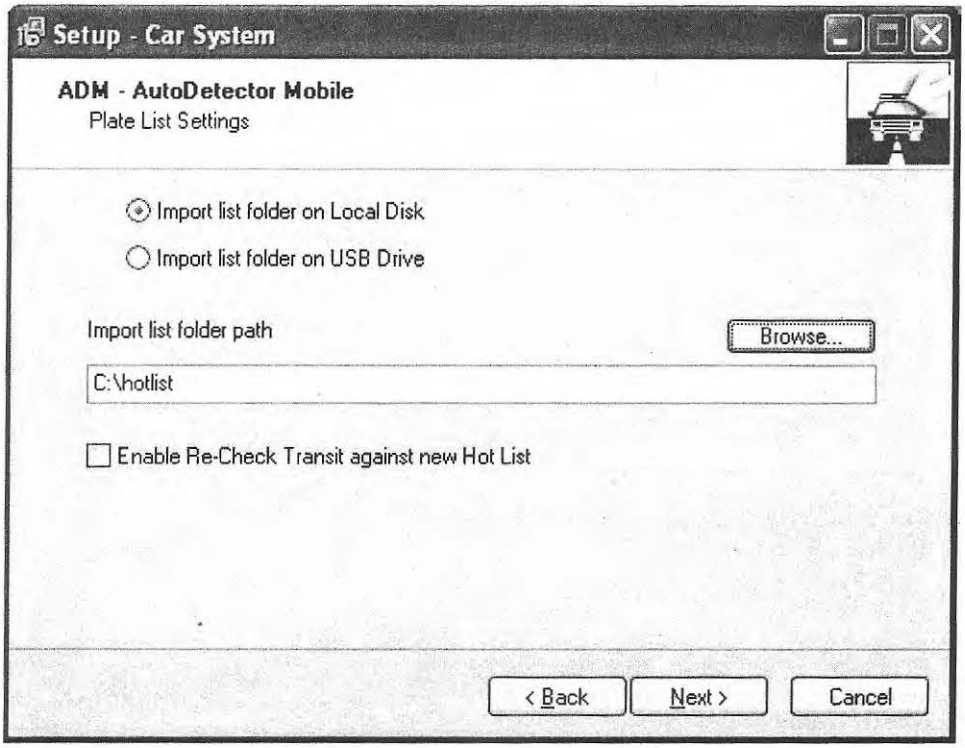


20) Data Root Location allows the user to select the computer Drive and folder where to keep data, including images. The Drive must be local, network locations are not supported.

NEW

Note that the default CarSystem installation folder is now C:\Program Files\ CarSystem

Click Next



In Plate List Settings you have the option to either load the hotlist to a specified folder on the system or you could load the hotlist directly from a USB drive by selecting "Import list folder on USB Drive. You could specify the import list folder in the box under "Import List folder path" or click browse to select the folder. The default path is

NEW

C:\ListImport.
If you had a previous installation it is recommended that you change the path to C:\hotlist as in the image above.

Uncheck Enable Re-Check Transit against new Hot List. This feature should not be used in this version of CarSystem.

Click Next

The rest of the CarSystem installation is the standard one already described in the previous sections.

Disable Sending alarm function (Long Range only)

It is necessary to manually change a parameter of the CarSystem configuration file to avoid a communication problem with the central server. (Only if Long Range has been selected).

1) Navigate to C:\Program Files\CarSystem\Services\Config
2) Edit the file LTBA.INI
3) Modify the value of the LTDWAlarmEnable parameter to 0 as shown below.

```
[COMMUNICATION_ENABLE]
;_____Enable Communication with Comm Service (possible values 0, 1)
COMMComunicationEnable=0
;_____Enable Communication with MDVRSService (possible values 0, 1)
MDVRSComunicationEnable=0
;_____ Event to send to the MDVRS (possible values 0=none, 1=alarm only, 2=all
transits)
MDVRSTransitSendEnable=2
;_____Enable Communication with LOCService (possible values 0, 1)
LOCComunicationEnable=1
;_____Enable Communication with EVT (possible values 0, 1)
EVTComunicationEnable=0

;_____Enable Send alarm to central via LongRange Channel(possible values 0, 1)
LTDWAlarmEnable=0
;_____Enable start upload data on folder full(possible values 0, 1)

LTDWSendFullFolderEnable=1
```

Restart MWP after this operation.

Change the Credentials file on the OPC Server (Long Range only)

This change has to be applied to the Server where the Operations Center revision 4.4.0 is installed. If Short Range communication mode is selected, no change is needed.

To change the credential files on the server, navigate to the following directory c:\smcv\CarSystemData\CS_CREDENTIALS\.

Copy the file *Car_00001_LR.xml* available in the CarSystem kit under..\Utility\LongRange_OPC and move it into the Server under

c:\smcv\CarSystemData\CS_CREDENTIALS\00001\

Replace the existing Car_00001_LR.xml file.

Add more Cars to the system (Both Long Range and Short Range)

If the Operations Center has to manage more than one car you have to follow this procedure:

1) Copy and paste the 00001 folder to the same directory and rename that copy to the new car id preferred (i.e. from 00001 to 00002)
2) Then rename the files within the folder to the relevant new car id.

Car_00001_LR.xml ← Change the 1 to the new car id

3) Edit the file and change the following line:

<IP>192.168.0.3</IP> ← Change this to the ip address of the Operation Center server

```
<?xml version="1.0" ?>
<MSG type="LIST_SVC_LR_CHANNEL">
        <SERVICE_NUM>1</SERVICE_NUM>
        <SERVICE SvcName="LTBA" OnBoardSvcId="1">
                <PORT>21</PORT>
                <IP>192.168.0.3</IP> ← Change this to the ip address of the ftp server
                <PROTOCOL>FTP</PROTOCOL>
                <USER>CarSystem</USER>
                <PWD>CarSystem</PWD>
        </SERVICE>
        </MSG>
```

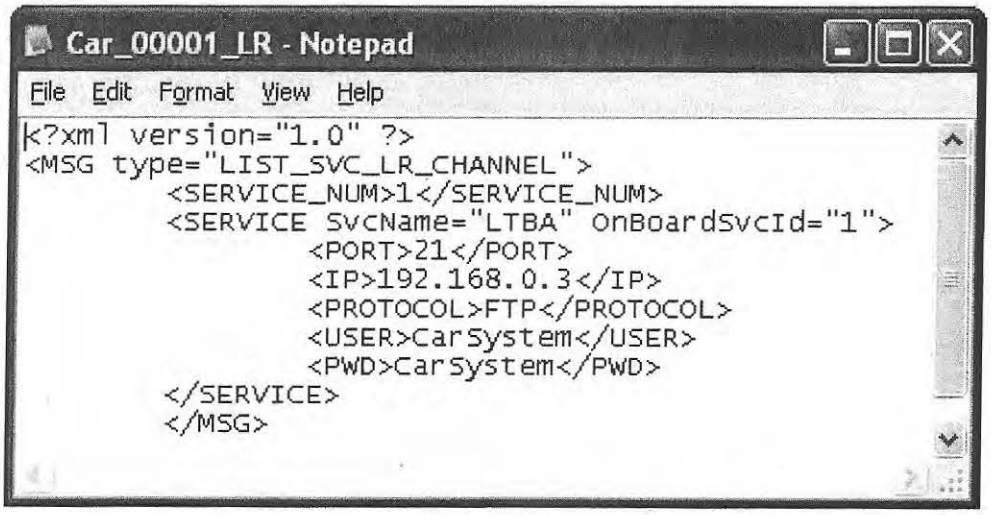


Figure 5: Example of the Long Range Credentials file.

If Short Range is selected, just apply the same procedure changing the file from Car_00001_LR.xml to Car_00001_SR.xml. In the end you must have one folder for each different CarId in the system.

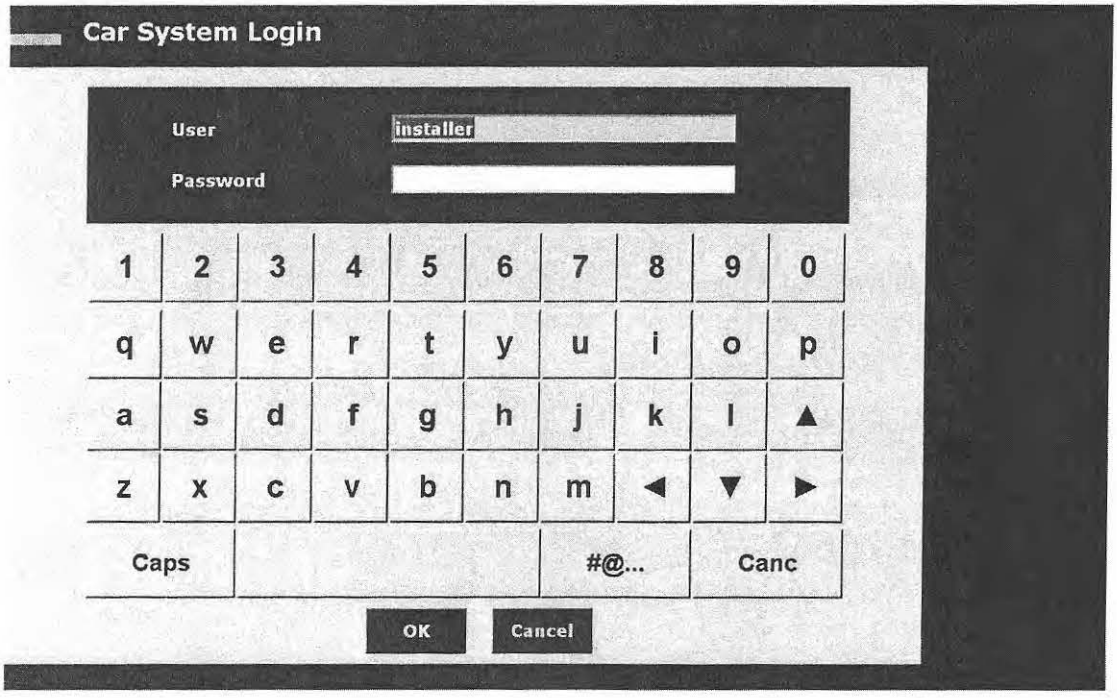
8 Set the Usernames and passwords

At this point you can launch the ***CarSystem*** for the first time, by clicking on the following icon available in the desktop of the Microsoft User used during installation..

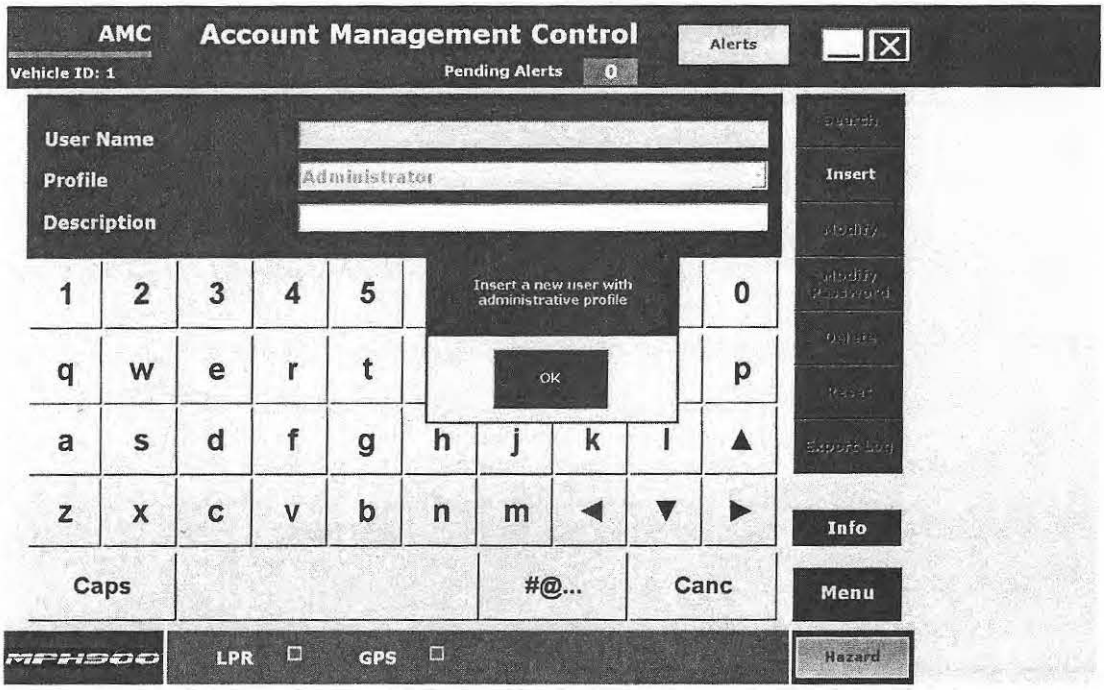
If you have selected *AMC – User Management Component* from the beginning of the setup then continue with this section. If not, you can skip this section and go to section 9.

Since the system is provided with a Login Control system, you need to define at least one Username and Password. The Account Management Control is proprietary and independent from the Windows security and username system,

The Login page shows up with the INSTALLER username, which is the default system start up username. A new User must be mandatory inserted to be able to access the system.
The INSTALLER password is **elsagdatamat1** (case sensitive).



Upon Login with the INSTALLER user you need to create at least an Administrator level user.



The user's password can be empty, if the Login control is not desired.

Every non-blank password will expire after 90 days.

The user will be requested to change password when necessary.

If you forget the administrator password and need to reset it, follow the directions below on how to reset the administrator password.

Warning: Resetting the administrator password will delete all user id's and passwords you have created. You will need to recreate them again.

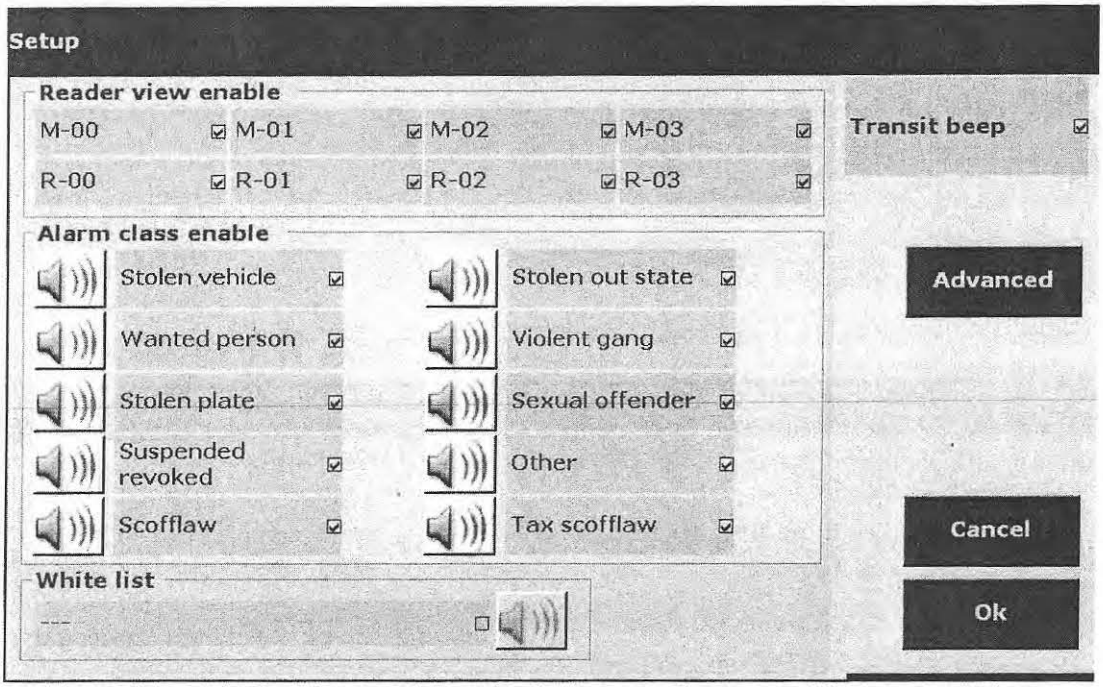
To reset the Administrator password a userdb file will need to be over written in the CarSystem.

In the <Kit\KIT_RELES_ADM3_2.3.0\Utility\UserDB folder is a file called users.db3 Copy this file and paste it to the directory C:\Program Files\Car System\Config and over write the existing file. This will put you back when you first installed the CarSystem above. Follow the directions in section 'Set Usernames and Passwords'.

9 CarSystem Configuration

Now you are ready to configure the system according to the purchased camera configuration. Up to 8 LPR cameras can be connected to the same ***CarSystem***, therefore it is necessary to customize the user interface to their specific number and positions. You can have 2 on-board cameras that are usually defined as RH (Right Hand) and LH (Left Hand). You can also control up to 4 Roadside wireless cameras from the same ***CarSystem*** interface.

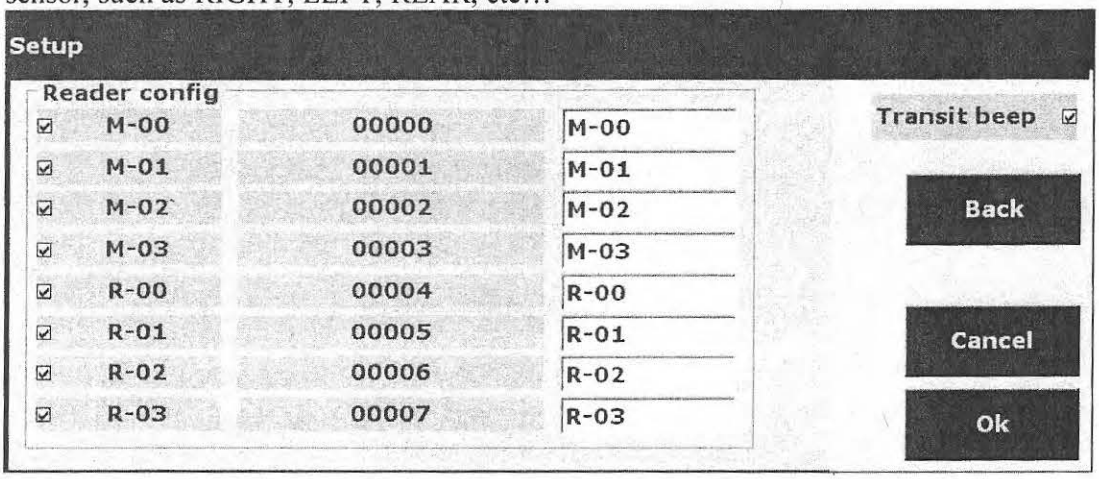
The configuration process is performed by clicking the Setup pushbutton on the main LPR page of the ***CarSystem***. On the following dialog Box select the Advanced option.



In this section of the Reader Config, uncheck the unused cameras. The correspondence from the camera Identifier and the physical cameras is done via the sensor internal ID according to the following table:

CarSystem ID	Camera ID	Note
M-00	0000	Mobile system Right
M-01	0001	Mobile system Left
R-00	0004	Roadside camera
R-01	0005	Roadside camera
R-02	0006	Roadside camera
R-03	0007	Roadside camera

In the right-most editable column it is possible to define a custom label to identify the sensor, such as RIGHT, LEFT, REAR, etc…



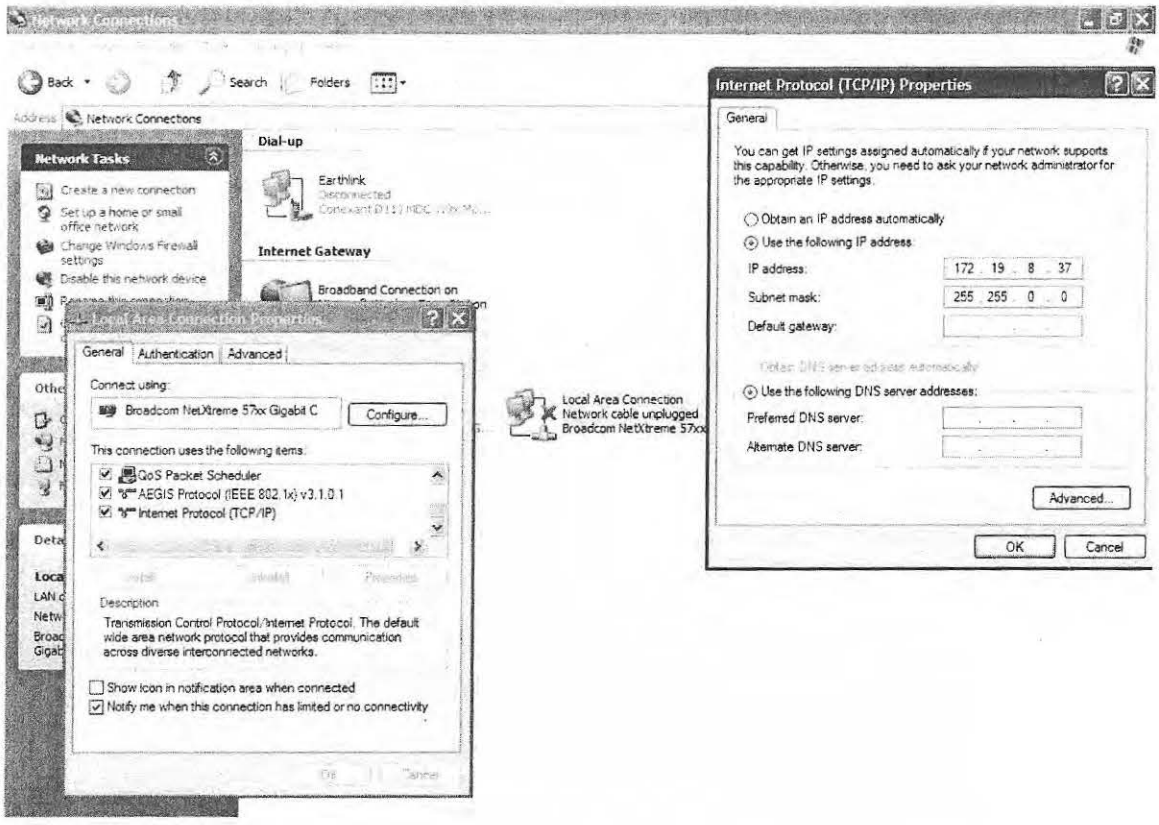
10 Set the Static IP Address

The MDT/laptop has to be connected to the MPH™900 sensors by means of a TCP/IP network. The computer has to have a Static IP address.
On request, it is possible to change the network subnet and the individual IP addresses of the sensors and the computer. Please contact Technical Assistance for that. The standard IP structure is the following:

Device	TCP-IP address	Note
Computer	172.19.8.37	Ethernet NIC connected to the AD3 junction box.
Left camera	172.19.8.31	
Right Camera	172.19.8.32	

The TCP/IP traffic must be enabled among the following addresses 172.19.8.31, 172.19.8.32, 172.19.8.37. Wireless networks and Computer Aided Dispatch programs may block TCP/IP traffic as a safety feature. In this case, the above mentioned TCP addresses must be unblocked.

MPH900™
Mobile Plate Hunter 900 Series



1. Select Start, Control Panel, Network Connections
2. Select the network adapter that will be used to connect to the processor
3. Right click the network adapter
4. Scroll to the bottom of the "This adapter uses these items:" window and select Internet Protocol (TCP/IP)
5. Select Properties
6. Check use the following IP Address
7. For IP Address Enter **172.19.8.37.**
8. For Subnet Mask Enter 255.255.0.0
9. Click OK

11 Installation of Cartography (optional)

In the kit folder, under USA_maps , it is possible to find the cartographic component. This component is location specific and you can install it only if your area maps are available. GPS must be installed to use this option.

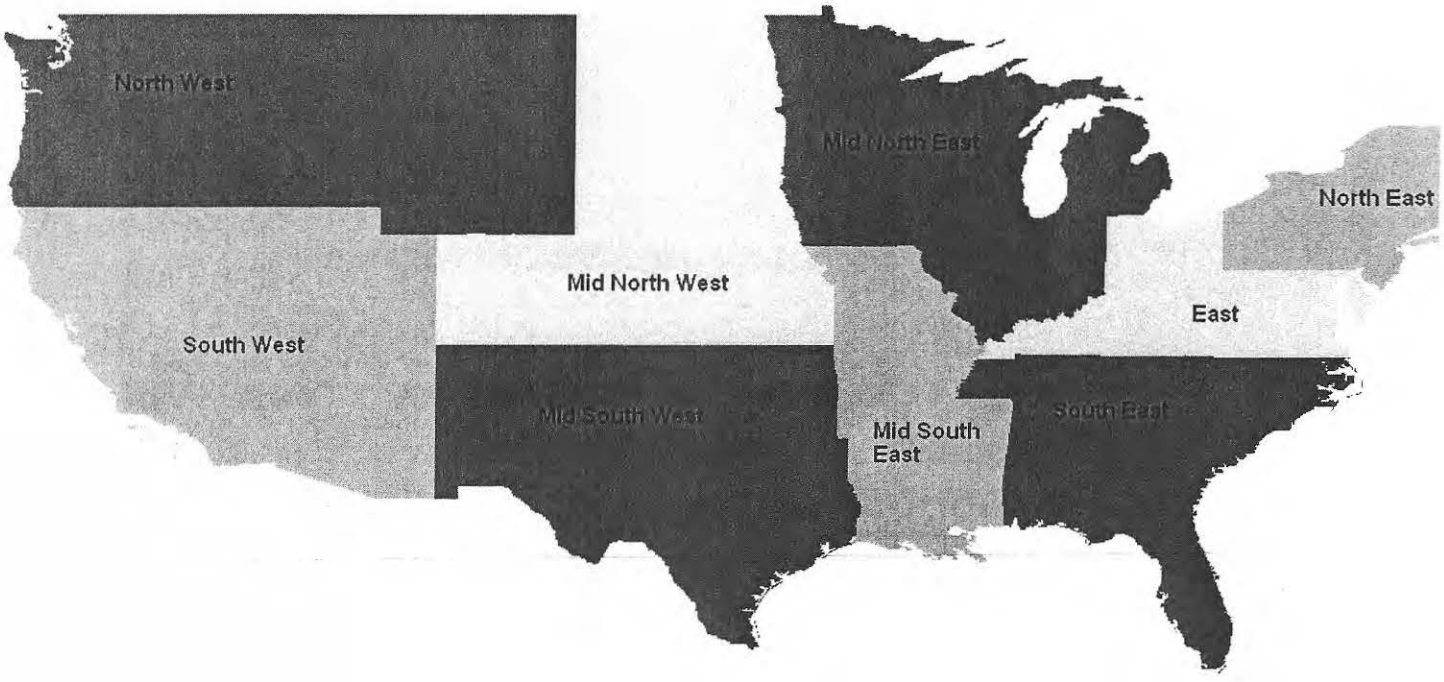


Figure 6: Cartography Tessellation of the USA. Select the right setup file according to this chart.

North West		
5 States	**WA**	Washington
	OR	Oregon
	ID	Idaho
	MT	Montana
	WY	Wyoming

Mid North West		
5 States	**ND**	North Dakota
	SD	South Dakota
	NE	Nebraska
	CO	Colorado
	KS	Kansas

MPH900™
Mobile Plate Hunter 900 Series

Mid North East		
6 States	IN	Indiana
	MI	Michigan
	WI	Wisconsin
	IL	Illinois
	MN	Minnesota
	IA	Iowa

North East		
9 States	ME	Maine
	VT	Vermont
	NH	New Hampshire
	MA	Massachussetts
	RI	Rhode Island
	CT	Connecticut
	NY	New York
	NJ	New Jersey
	PA	Pennsylvania

East		
7 States	DE	Delaware
	MD	Maryland
	DC	District of Columbia
	VA	Virginia
	WV	West Virginia
	OH	Ohio
	KY	Kentucky

South East		
6 States	FL	Florida
	GA	Georgia
	SC	South Carolina
	NC	North Carolina
	AL	Alabama
	TN	Tennessee

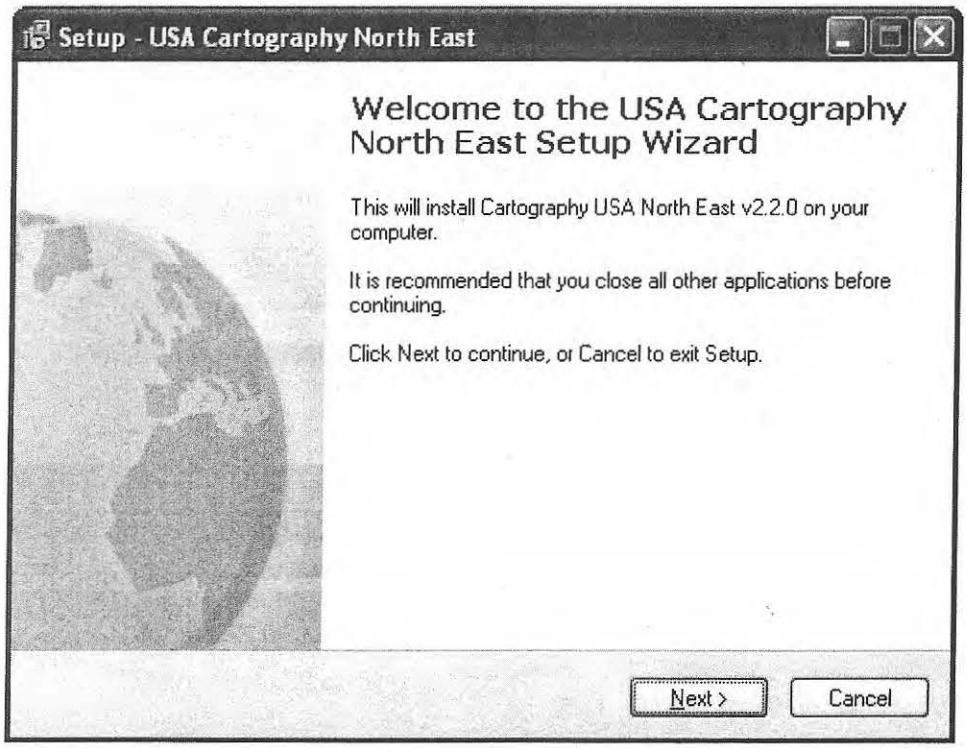
Mid South East		
4 States	AR	Arkansas
	MO	Missouri
	MS	Mississippi
	LA	Lousiana

Mid South West		
3 States	NM	New Mexico
	OK	Oklahoma
	TX	Texas

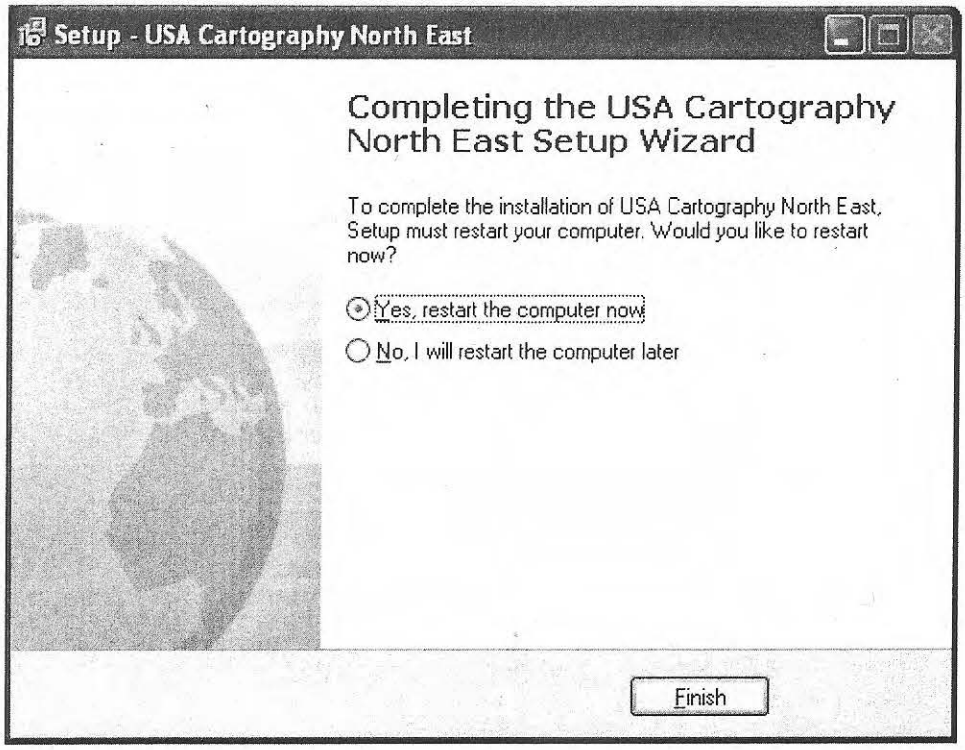
South West		
4 States	CA	California
	NV	Nevada
	UT	Utah
	AZ	Arizona

External		
7 States	AK	Alaska
	PR	Puerto Rico
	VI	Virgin Islands of the United States
	AS	American Samoa
	GU	Guam
	HI	Hawaii
	MP	Commonwealth of the Northern Mariana Islands

When select the right setup file you can continue on to the installation steps.



Click Next, there is no interaction needed.



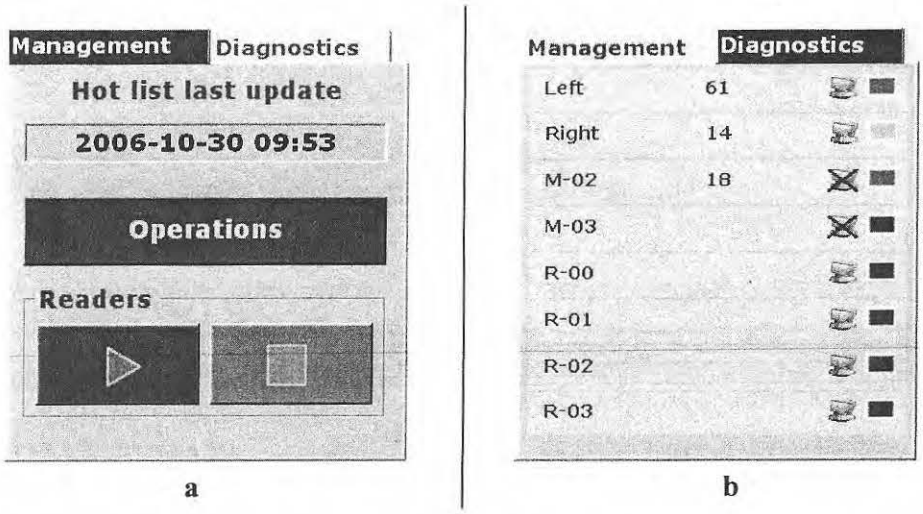
Click Finish, and then Restart the computer as prompted.

12 System Test

Once the software is installed, connect the junction box to the computer and launch the *CarSystem* software on the desktop.

The software should start and the LPR light should turn green.

Go to the "Diagnostics" tab and test that you can see the image from each camera.



a b

Select the Camera by clicking the camera name (left column) you wish to view. The status light will turn yellow while the camera is in Live mode.

Note that the camera will stop reading plates while in Live mode

Hot List download Test

1. Copy the test_hotlist.txt file from the utility folder and paste it into C:\Hot List on the computer connected to the RELES MPH900X junction box. The text file will be deleted shortly, while the ***CarSystem*** imports it.
2. The "Traffic Light" window will appear as in the following picture. On the main LPR window the Last Update Hot List field will be updated.

Note that the HL_Converter is not used anymore. Please uninstall it before running the Hot List download test.

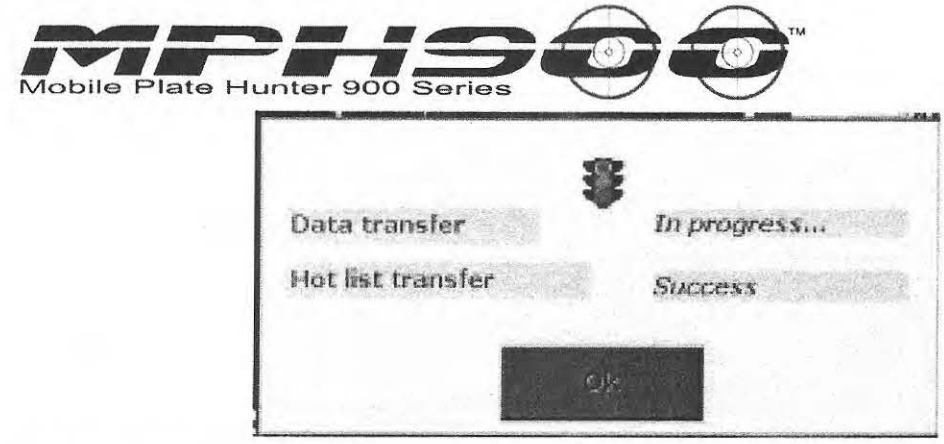


Plate read test

The objective of the test is to verify that the system is able to read a plate and generate an alarm. We must enter the plate in the temporary hot list and put the test plate in the camera field of view.

Click the Operations button.

- Add your test plate number in the plate field
- Select the State from the drop down box
- Click the insert button
- Place the plate in front of one of the cameras; when the plate is read you should hear the alarm sound.

13 PumaLite Configuration. How to upgrade the processor Firmware

The following preliminary step is necessary to prepare the diagnostics tools that are needed to download and upgrade the processor Firmware and to access the cameras in diagnostic mode.

Create Desktop Tool Icons

First of all, create a C:\Tools folder then copy under this folder the content of the folder

..\KIT_RELES_<version>\AD2_PumaLite_<version>\Tools\

- Then go to C:\Tools\o2cr_swupdLTBA
- Create a shortcut for LTBA_swUpdate.exe and copy it to the desktop.


LTBA-swUpdate.exe

- Go to C:\tools\ o2cr_console
- Create a shortcut for Console.exe and copy the shortcut to the desktop.


Console.exe

- Go to C:\tools\ o2cr_console
- Create a shortcut for Naming.exe and copy the shortcut to the desktop.


Naming.exe

- Go to C:\tools\ o2cr_swupdate
- Create a shortcut for GATE-swUpdate.exe and copy the shortcut to the desktop.


GATE-swUpdate.exe

First Upgrade of Firmware to PUMA Lite Configuration

In order to run CarSystem 4.X.Y the PUMA processor must be upgraded to the so-called PUMA Lite configuration. This special upgrade has to be done once: Subsequent firmware and protocols upgrade will require the procedure described in the next section.

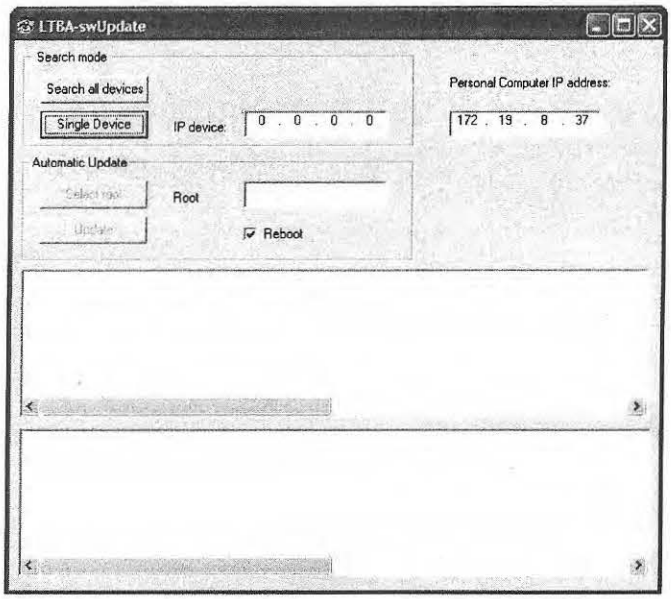
The PUMA Lite configuration is needed because the new CarSystem takes over some of the functionality of the old PUMA system such as Hot List matching and Data collection and archiving. Technically the PUMA hard-disk is not used anymore in the new configuration.

Note that the additional ("third") reading NTSC camera is not compatible with the PUMA Lite configuration. A Third camera PUMA system can't be upgraded to be compatible with CarSystem 4.X.Y.

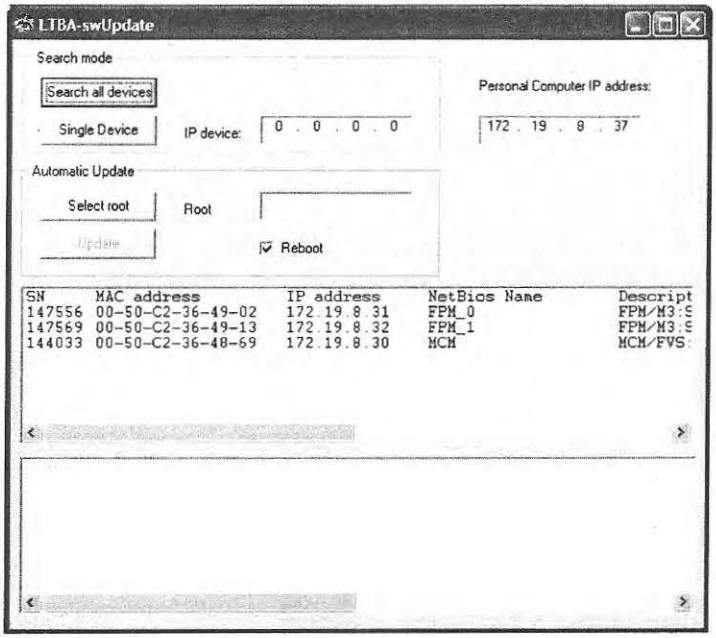
Before beginning, the MPH900 should be set up and running with a laptop attached.

1. Double click the "Shortcut to LTBA-swUpdate" icon.

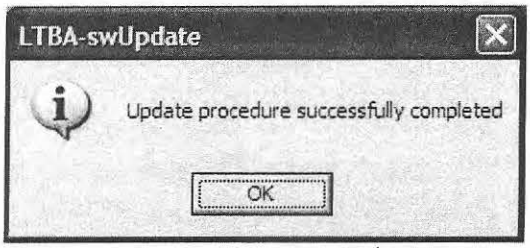
2. Make sure that the Personal Computer IP address on the right is 172.19.8.37. If it is not, change it to 172.19.8.37.



3. "Click the "Search all devices" button. 3 lines should show up in the middle pane



4. Click "Select Root"
5. Navigate to the KIT_RELES_6.1.0\AD2_PumaLite_5.1.2\PUMAtoPUMALite_Transition_Firmware \ directory, and highlight the \Base.00000.00 level.
6. Click OK
7. Click Update
8. The system will go through the load process and update the server. When it is complete a pop-up window will let you know that the update completed successfully.



Note that there will be 10 Iterations before a successful reboot as opposed to a normal Firmware updated. The Iterations are reported into the bottom pane.

After this step the new Firmware (5.1.2 or higher) has been loaded and you should have a Green light on the LPR signal of the CarSystem. The LPR system is not ready to read license plates until a valid US protocol is installed. Refer to the next section to learn how to install the right protocol.

How to upgrade the Protocols

The camera Protocols are a set of configuration files that include models of the license plates that must be recognized. For improved performances, localized state-specific protocols are available.
The set of protocols can be found on a separate kit issued by Remington Elsag.

The folder is called KIT_PROTOCOLS_PUMA_LITE_<version> <Version> can be 6.0.0 or higher. Under the root folder each available state specific configuration can be found under the state abbreviation. The \RELES folder includes the generic protocol useful when a state specific configuration is not available.

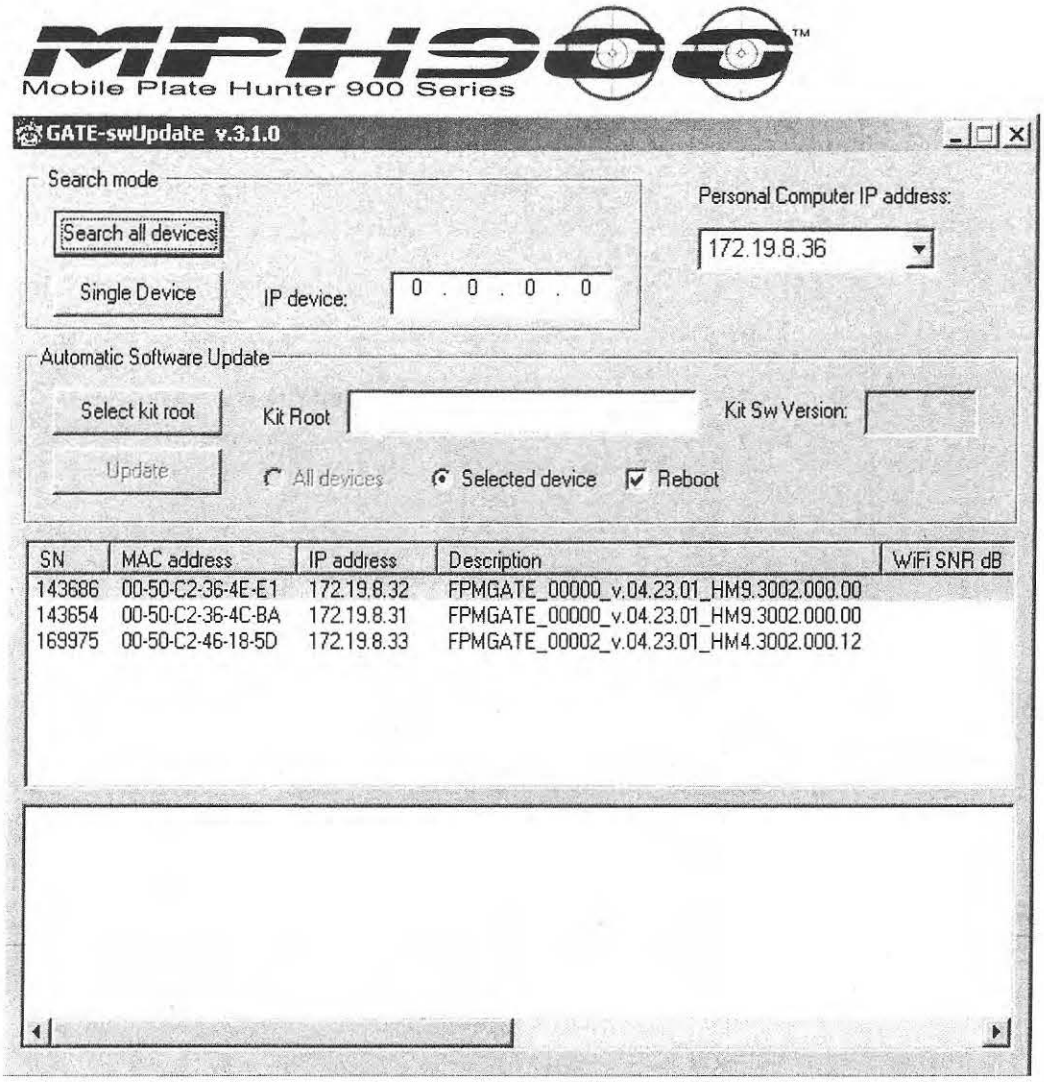
The protocol folder structure is the following:

KIT_PROTOCOLS_PUMA_LITE_6.0.0
- Arizona
  - FPM_0
  - FPM_1
- California
  - FPM_0
  - FPM_1
- RELES
  - FPM_0
  - FPM_1

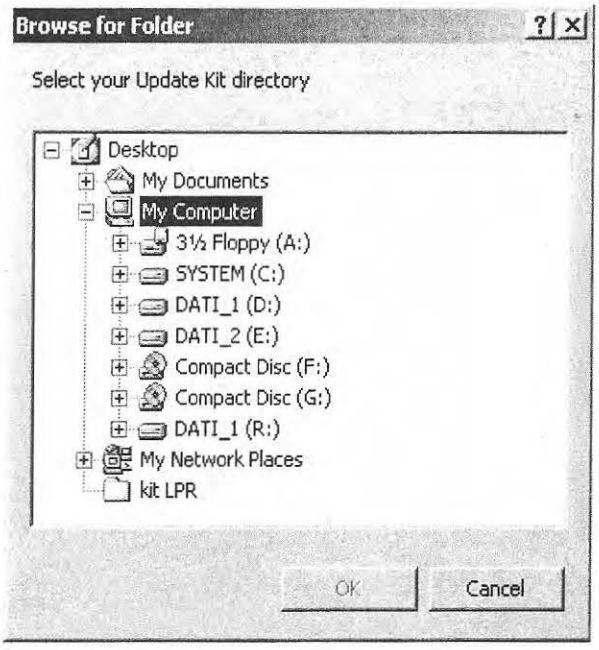
FPM_0 refers to the processing board controlling the RIGHT Hand camera (default IP: 172.19.8.31), while FPM_1 refers to the LEFT Hand board (default IP: 172.19.8.32).

The protocol update must be carried out separately on each camera processing board FPM_0 and FPM_1. This is the most important difference with respect to the previous system version (standard PUMA configuration). The other relevant difference is that we need to use a different Firmware loader, called GATE-swupdate instead of the usual LTBA-swUpdate.

1. Double click the "Shortcut to GATE-swUpdate" icon.
2. The following display screen will show up



3. You will see typically two lines, 172.19.8.31 and 172.19.8.32 corresponding to the RH and LH boards respectively.
4. Push the **Select kit root** button
5. A browser will open up as follows

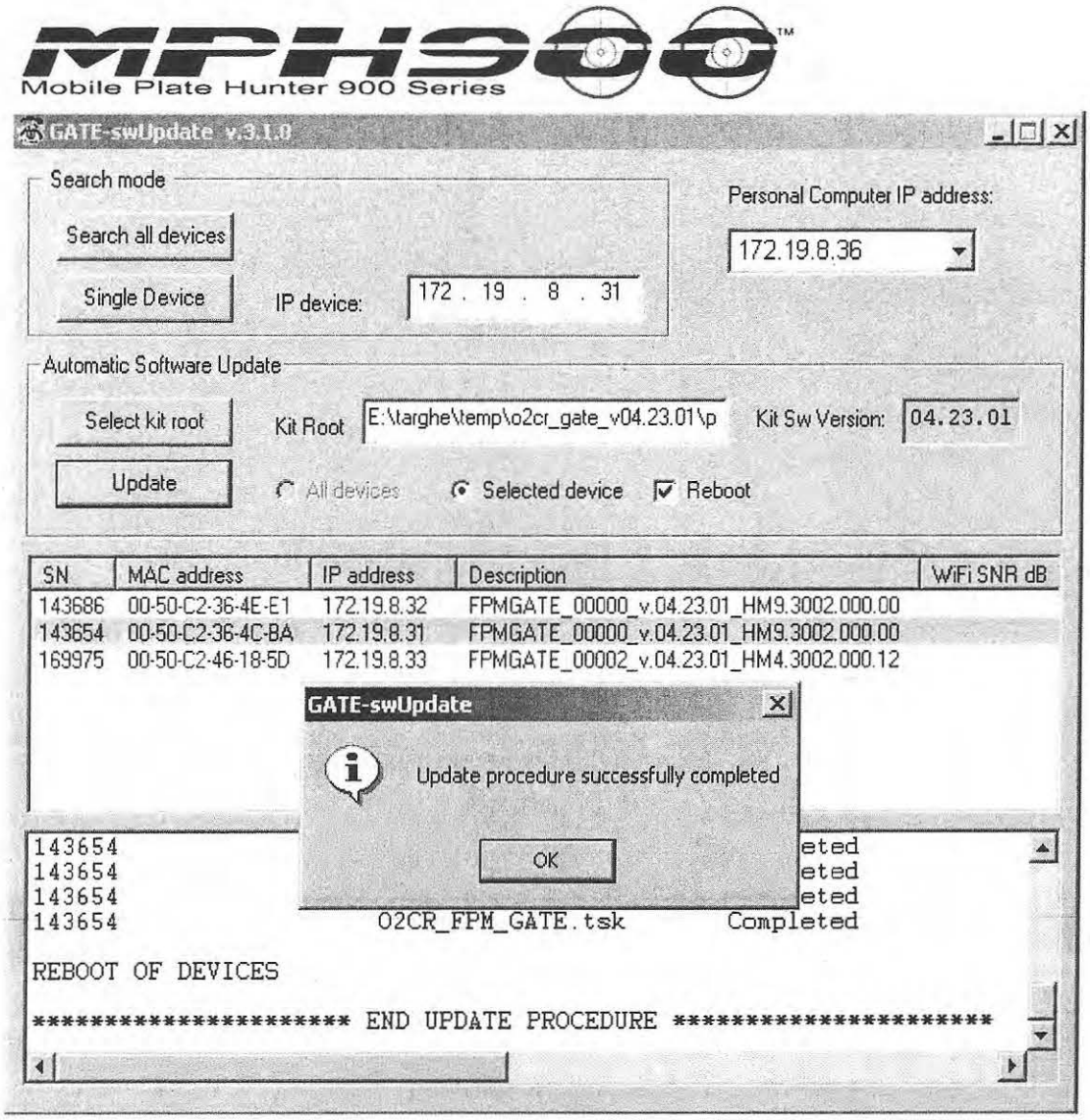


6. Navigate to locate the protocol folder at KIT_PROTOCOLS_PUMA_LITE_6.0.0 <State>

Then highlight the level

FPM_0

7. At this point the **Update** button is enabled and the version of the selected protocol or Firmware version is inserted in the **Kit SW Version** box. All the devices that already have this version are highlighted in blue.
8. Select the 172.19.8.31 line (FPM_0) by clicking on it.
9. Push **Update** to start the firmware download.
10. The bottom pane will show the status of the downloaded files in real time.
11. In case of at least one error the procedure terminates with the following message: *"Update Procedure Failed"*.
12. If all the files have been successfully downloaded, the final message will be *"Update procedure successfully completed"* and the device line will be blue highlighted.



13. Now select the device 172.19.8.32 (or FPM_1) and go back to step 4. Repeat the download procedure selecting the FPM_1 folder.

How to reload the processor Firmware when the PUMA Lite configuration has been already installed

After you upgraded the processor to the PUMA Lite configuration for the first time (Firmware AD2_PumaLite_5.1.2), you will have to follow a different procedure for subsequent Firmware reloads or upgrades.

The procedure is basically identical to the Protocol update method described in the previous section. The main points to remember are the following:

- The Firmware Loader to use is GATE-swUpdate.EXE
- The Firmware must be upgraded separately for each camera or camera control board (FPM_0, FPM_1).
- The location of the Firmware will be in the following folders
  ..\AD2_PumaLite_<version>\Firmware\FPM_0
  ..\AD2_PumaLite_<version>\Firmware\FPM_1

14 How to change default IP addresses of a PUMA Lite system

The proposed default IP addresses of the LPR processor are the following

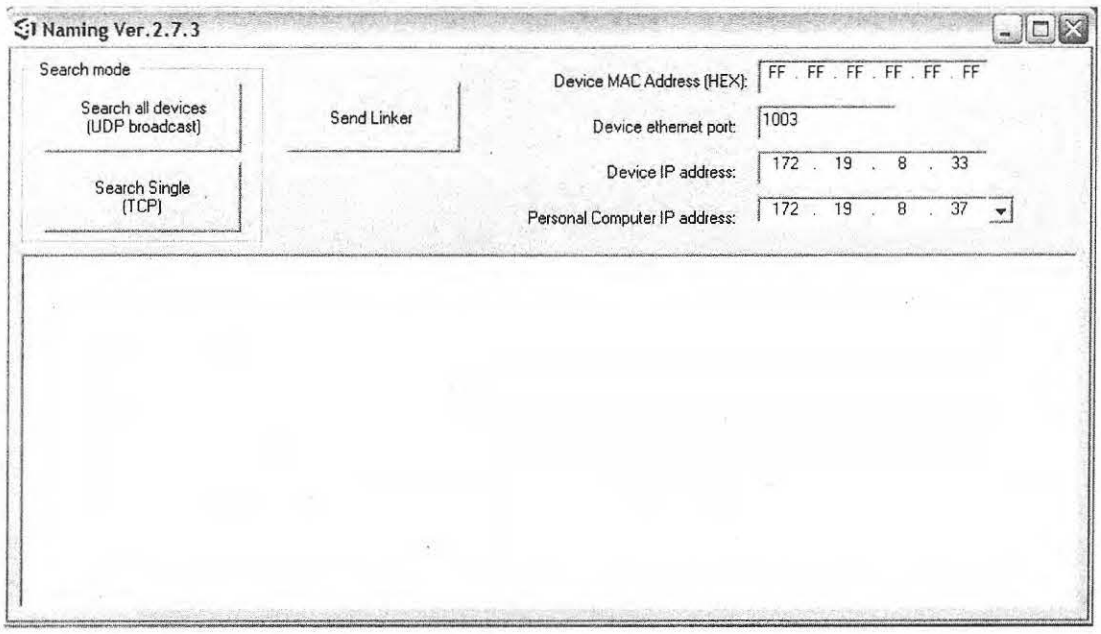
Network Interface Card	IP address	Subnet Mask	Connect to
MDT Main Ethernet	172.19.8.37	255.255.0.0	Puma Processor
MCM Temperature management Board	172.19.8.30	255.255.0.0	
RIGHT Camera FPM_0 Board	172.19.8.31	255.255.0.0	
LEFT Camera FPM_1 Board	172.19.8.32	255.255.0.0	

This scheme is not mandatory but can be changed to any other valid TCP/IP subnetwork. In this section we describe the procedure to change the default IP addresses to any other subset.

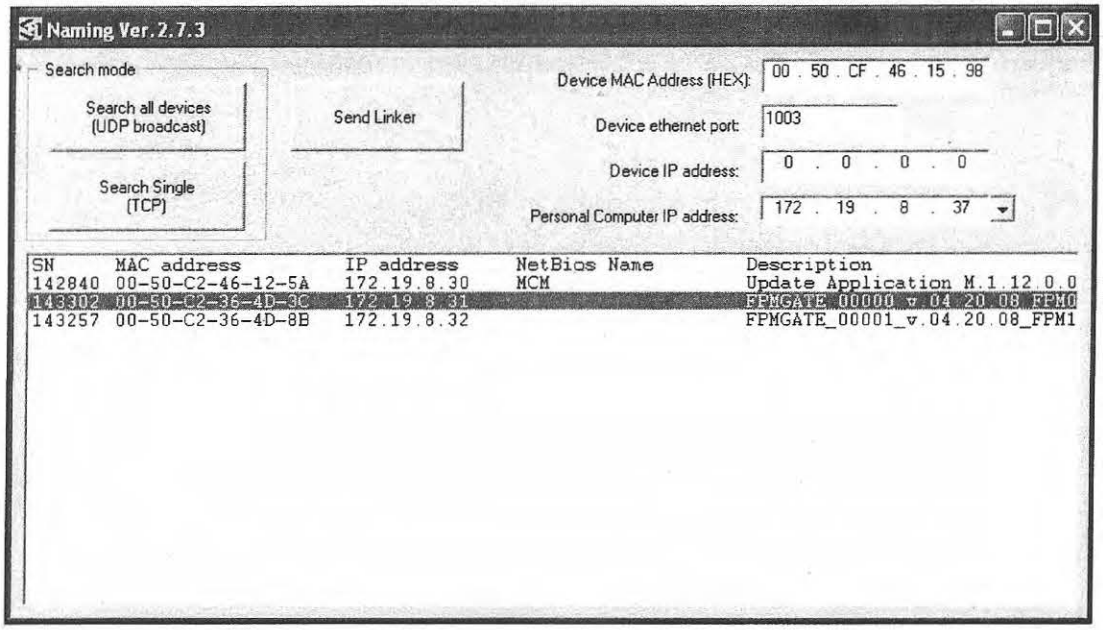
1. Double click the "Shortcut to NAMING.EXE" icon.


Naming.exe

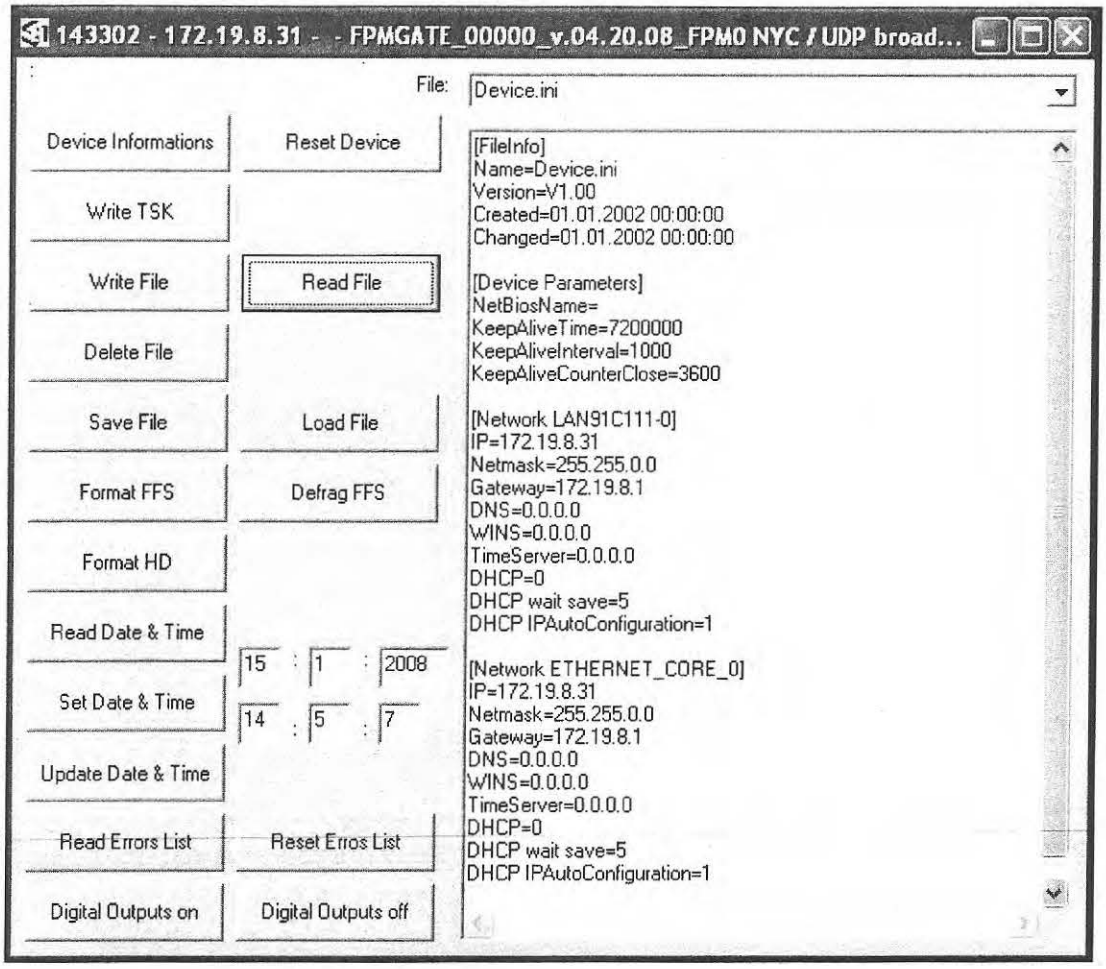
From the main screen make sure the Personal Computer IP Address is 172.19.8.37



2. The IP addresses of the boards has to be as shown in the picture Click the Search all Devices (UDP broadcast) button. You should then see all 3 devices listed on the screen as pictured above



3. Double-click on the MCM board line (172.19.8.30).



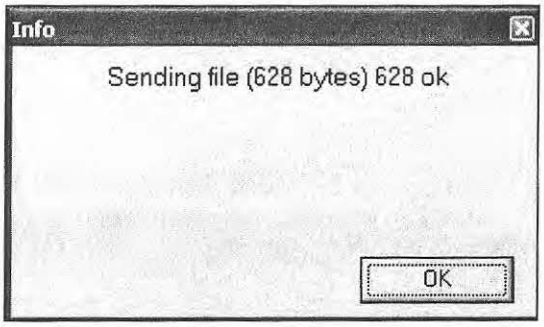
4. Select or Insert **device.ini** into the drop-down menu **File:** then click on **Read File.**
5. Identify the following file section and modify the IP and Netmask fields as desired

```
[Network LAN91C111-0]
IP=172.19.8.30
Netmask=255.255.255.0
Gateway=0.0.0.0
DNS=0.0.0.0
WINS=0.0.0.0
TimeServer=0.0.0.0
DHCP=0
DHCP wait save=5
DHCP IPAutoConfiguration=0

[Network ETHERNET_CORE_0]
IP=172.19.8.30
```

```
Netmask=255.255.255.0
Gateway=0.0.0.0
DNS=0.0.0.0
WINS=0.0.0.0
TimeServer=0.0.0.0
DHCP=0
DHCP wait save=5
DHCP IPAutoConfiguration=0
```

6. Press the **Write File** button and wait until a Success dialog box shows up. **Do not reboot the device now.**



7. Select or Insert **McmMonCfg.dat** into the drop-down menu then click on **Read File.**
8. Identify the following file section and insert the new IP addresses of the FPM_0 and FPM_1 boards according to the new scheme.

```
1               ! Enable
2               ! Numero di FPM presenti
172.19.8.31     ! IP address FPM 0
172.19.8.32     ! IP address FPM 1
1000            ! Periodo di Polling (in msec)
1               ! Porta di Input
0               ! Polarita` del segnale (0 => attivo basso; 1 => attivo alto)
1               ! Enable Log su File
5000            ! Max Size Log File (in KB)
#
```

9. Press the **Write File** button and wait until a Success dialog box shows up. **Do not reboot the device now.**
10. Close the window and, back on the main screen, press **Search all devices**
11. Double-click on the FPM_0 board line.
12. Select or Insert **device.ini** into the drop-down menu then click on **Read File.**

```
[Network LAN91C111-0]
```

```
IP=172.19.8.31
Netmask=255.255.255.0
Gateway=0.0.0.0
DNS=0.0.0.0
WINS=0.0.0.0
TimeServer=0.0.0.0
DHCP=0
DHCP wait save=5
DHCP IPAutoConfiguration=0

[Network ETHERNET_CORE_0]
IP=172.19.8.31
Netmask=255.255.255.0
Gateway=0.0.0.0
DNS=0.0.0.0
WINS=0.0.0.0
TimeServer=0.0.0.0
DHCP=0
DHCP wait save=5
DHCP IPAutoConfiguration=0
```

13. Identify the following file section and modify the IP and Netmask fields as desired. Insert the new IP address of the FPM_0 board. **Do not reboot the device now.**
14. Go back to step 10 and repeat the following steps selecting FPM_1.
15. When FPM_1 has been modified change the MDT IP address according to the new scheme.
16. Now you can reboot the (power off than power on) PUMA processor.
17. Launch NAMING again, hit **Search all devices.** The 3 boards will show up with the new IP addresses.
18. Launch CarSystem. The LPR light should be green. No changes are requested to the ***CarSystem*** configuration.

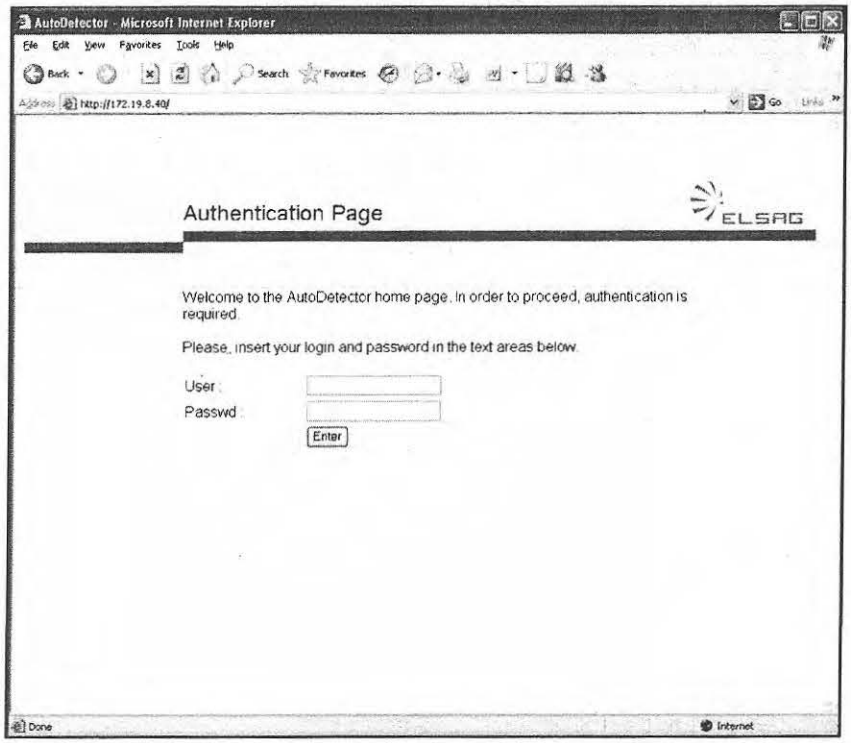
15 AD3M Configuration. How to upgrade the camera Firmware

Install the Discovery tool

The Discovery tool must be installed on the computer to access easily to the LPR cameras.
You can find the Discovery tool setup program in
..\Utility\Discovery\Discovery_Setup.exe.

Upgrade the Firmware

You need to open up the camera embedded Web Site through a standard Internet Browser. The camera Web Site can be found at http://<camera IP address>

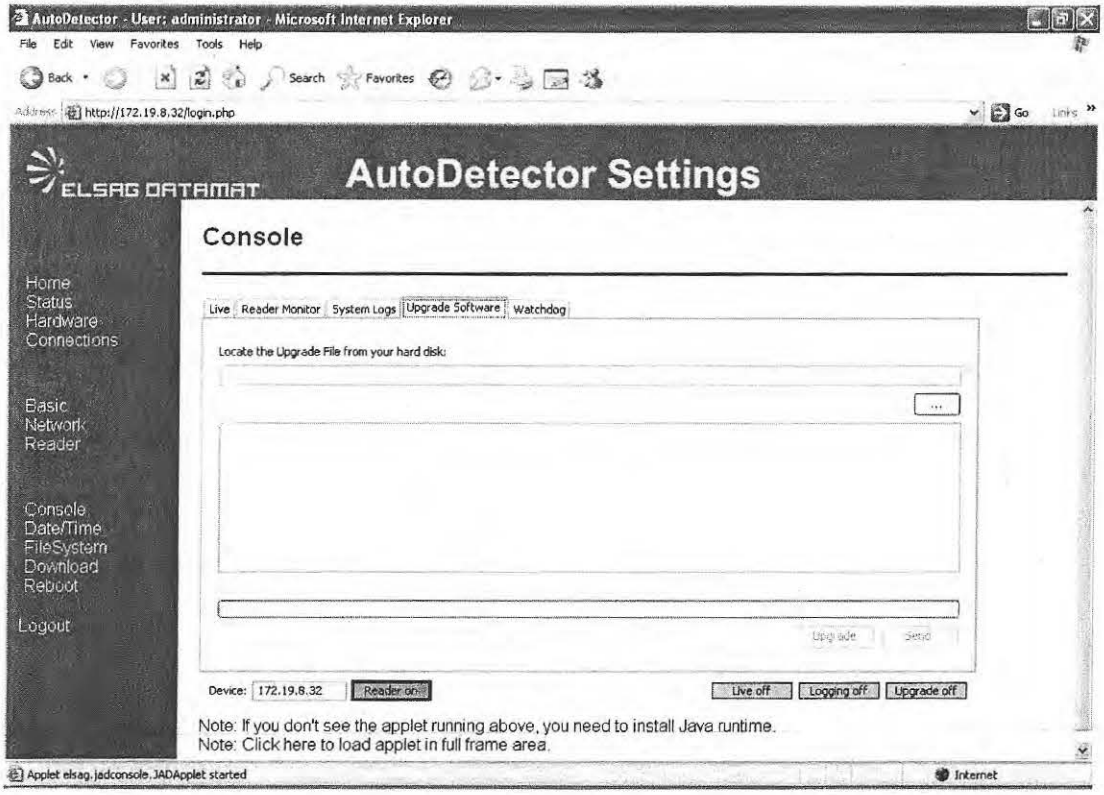


You must login as an administrator to perform a Firmware upgrade. The default username and password are

- ***administrator*** with password ***elsag***;

Launch the Console Page.
In order to use the Applet, the Java Runtime v.1.5.0_08 or further must be installed on the computer.

Select the Upgrade Software Tab.



At this point the new firmware must be selected. This is a file included in the kit folder under AutoDetector3_v<version>\Firmware:

- **Ad3_sw_app_v.<version>.kit**: Select this if you want to update firmware keeping the current camera configuration. The camera configuration includes IP address, camera ID.
- **Ad3_sw_sys_v.<version>kit**: Select this if you want to update firmware and reset the camera configuration to the factory default.

After choosing the package to be uploaded, the operator has to click the **Send** button to upload the package on the reader. By pressing this button, the progress bar on the bottom of the Console Applet will show the transfer status.

After the transfer has completed, the operator has to click the **Upgrade** button to perform the software upgrade. The camera will send the upgrade logs which will be displayed on the text box console. The bottom right box will show the Upgrade On signal on a red background.

After the upgrade operation, the reader will reboot with the new software/configuration
The upgrade time is about 3 minutes, not including reboot.
Close the browser window while the camera is rebooting and open a new session to verify that the new Firmware has been correctly loaded.

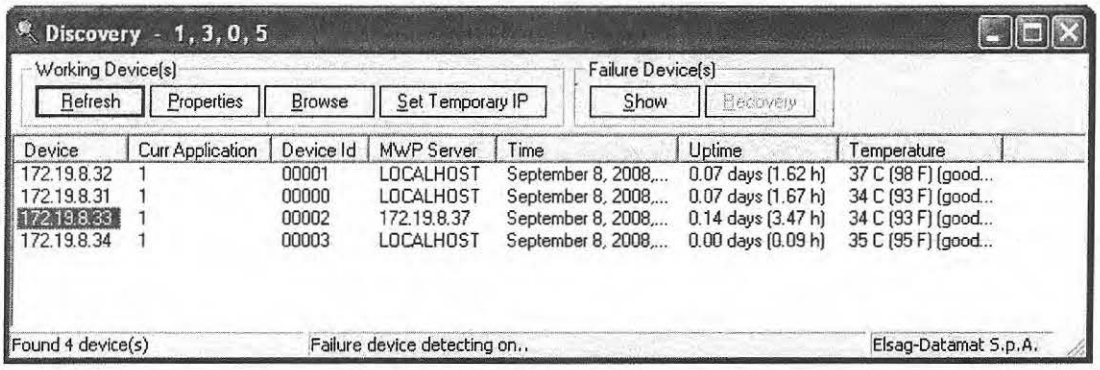
Repeat the procedure for any LPR camera in the system

16 AD3M. How to upgrade the camera Protocols

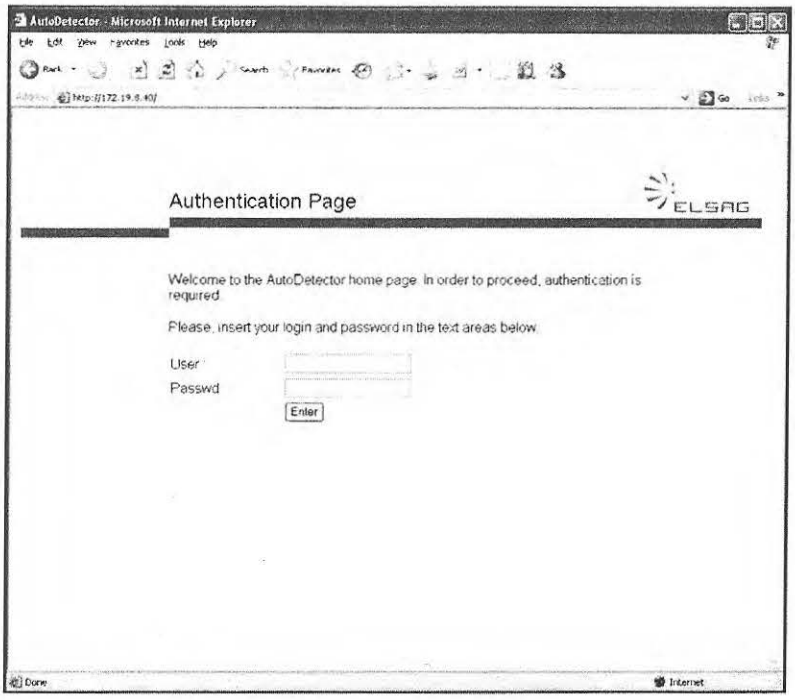
The camera Protocols are a set of configuration files that include models of the license plates that must be recognized. For improved performances, localized state-specific protocols are available.
The set of protocols can be found on a separate kit issued by ENA.

1.) Open the **LPR Discovery.exe** icon on your laptop

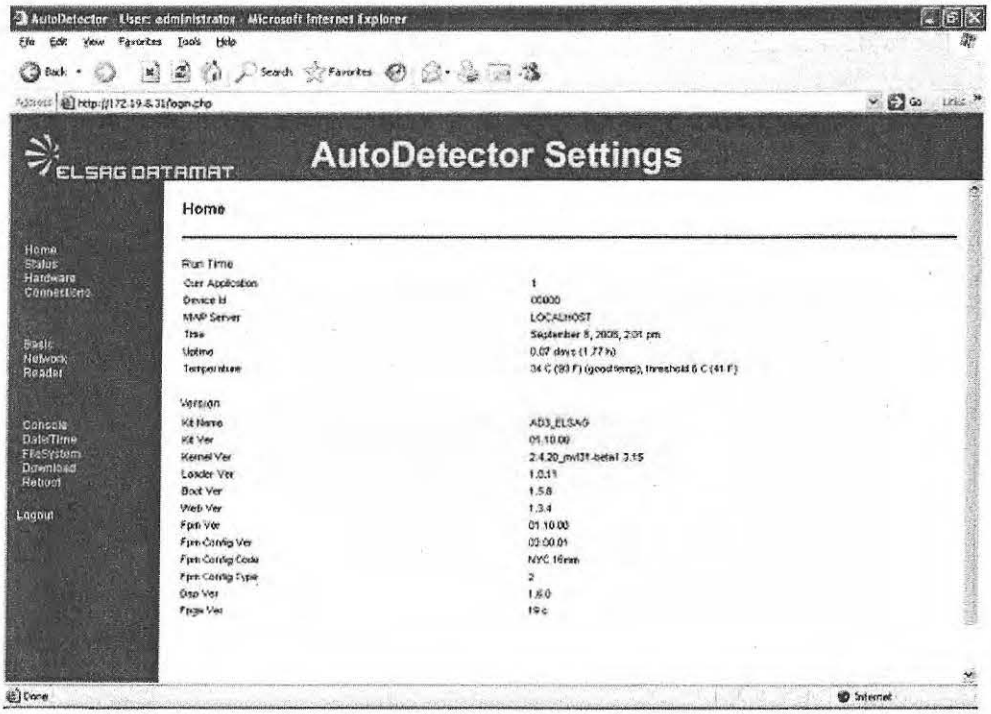
This will show each camera in operation with the IP address (Device) and Device ID:



2.) Select one of the cameras and click **Browse**
You will be prompted by an Authentication Page:
User: administrator
Password: elsag

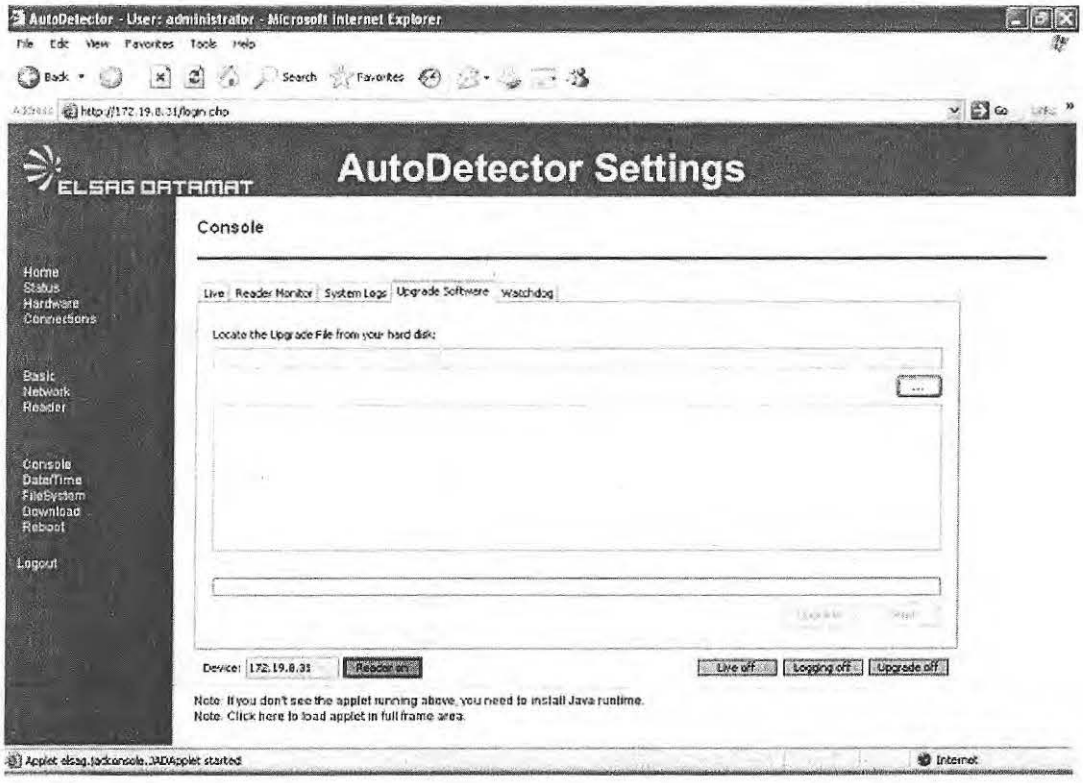


It will open up to the Home page showing the contents of the camera:



3.) Under Tools on the side menu, select **Console**

→ Click **Upgrade Software** to change the current protocol of the camera.



→ Click on the "…." button to search for the desired protocol.

-Locate the ***Protocol library*** under Local Disk and select the most recent version of the protocol specific to the area you are located.

For example, a valid protocol file is:

AD3_AZ_16mm_v.02.00.00.kit

This means that this is an Arizona configuration for a 16 mm (Right hand) camera and the protocol version is 2.0.0. Typically, 25 mm cameras are used for the left side and 16 mm for the right side. An updated version of the Arizona protocol may appear as **AD3_AZ_16mm_v.02.00.02.kit**, meaning it is the second version of the protocol.

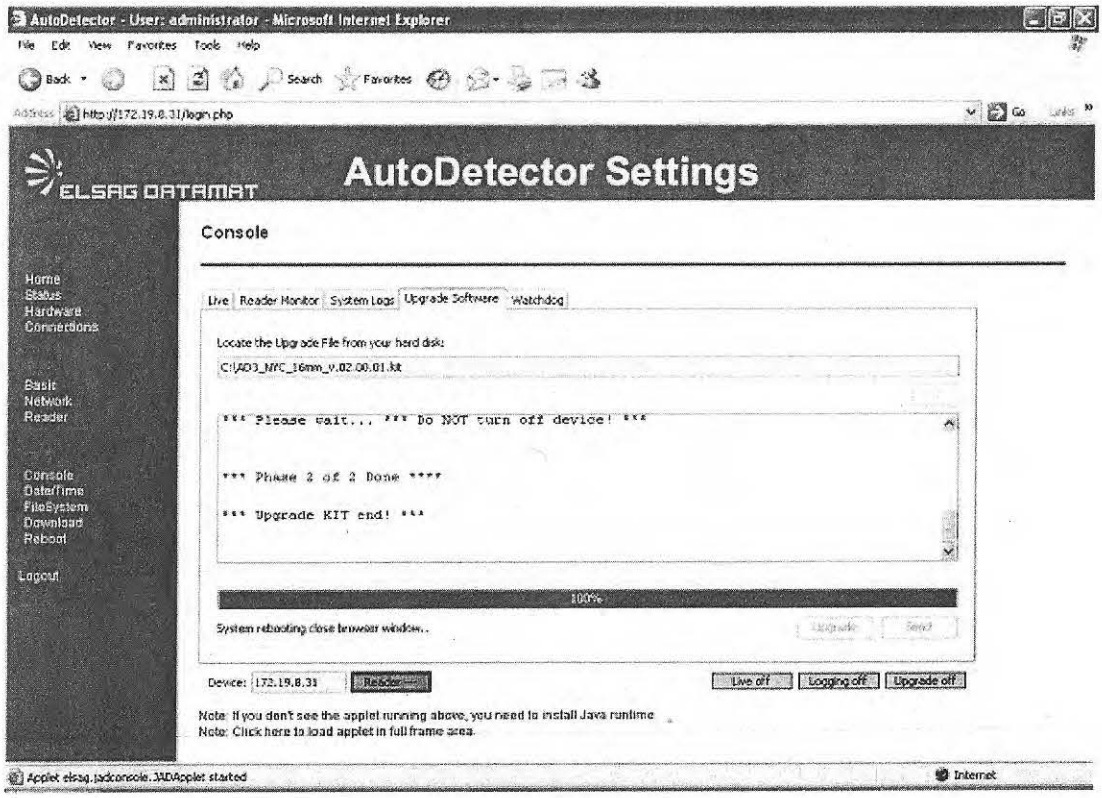
You will want to select the most updated version of the protocol specific to the area you are located.

→ Select **Send**

→ Select **Upgrade**

-Click OK for the pop up box "*Are you sure you want to upgrade this system*?"

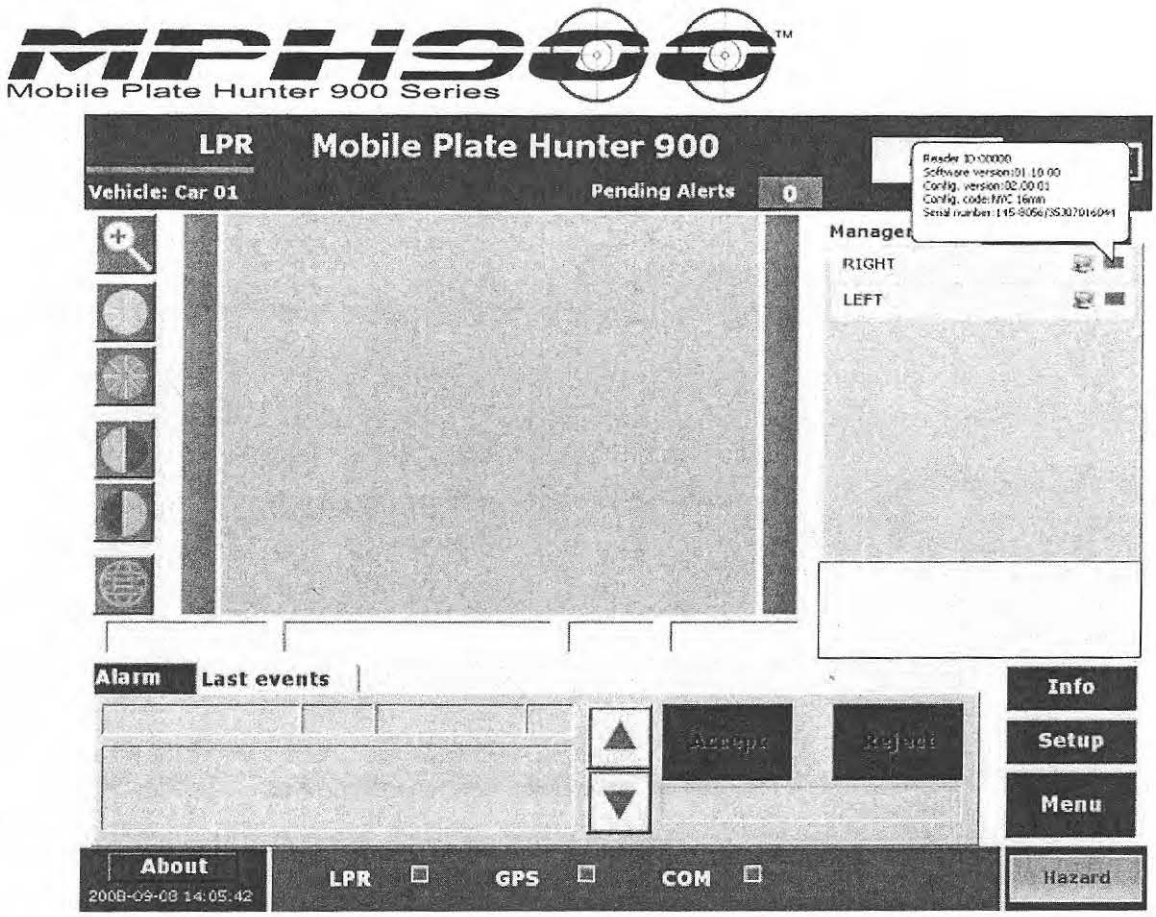
-Once the console reads "*System rebooting close browser window..*" you can exit and begin to update the next camera.



A complete upgrade for one camera takes approximately 2 minutes.

In Car System, you should see the light for the camera indicating if the camera is on (green) or off (red). While the camera is upgrading the protocol, the light will be red. After a successful upgrade, it returns to green. To check that the camera has been properly updated, drag the curser over the green light and it will tell you the current protocol on the camera.

For example, **NYC 16mm version 02.00.01**, as shown below

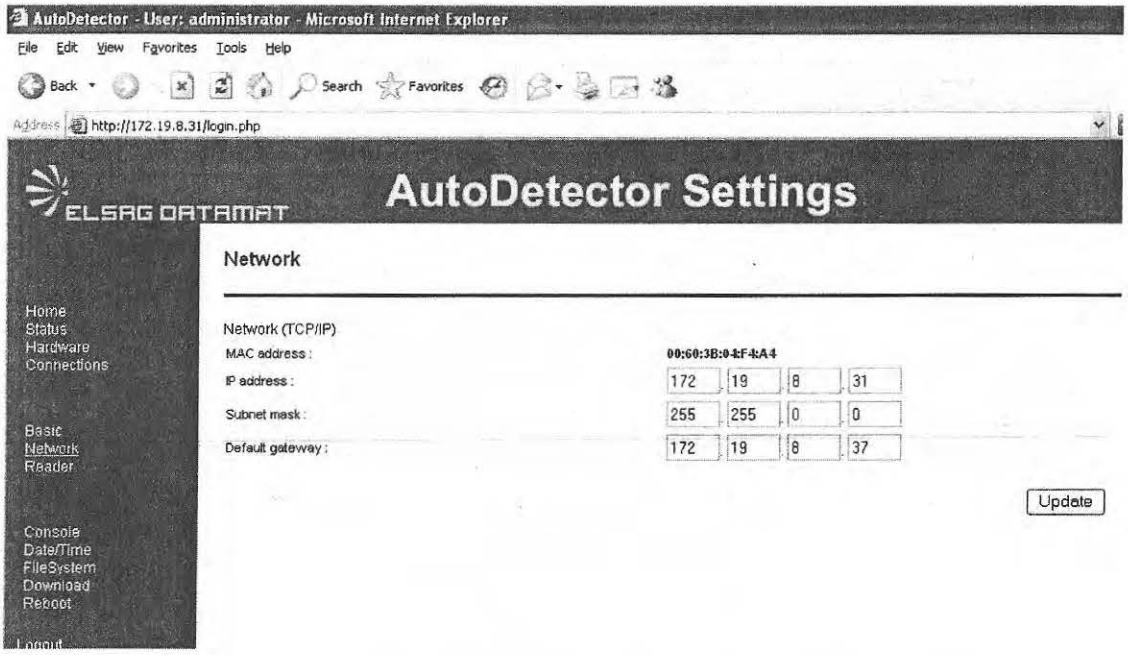


4) Repeat this process for each camera in operation (16mm, 25mm, 50mm, etc).

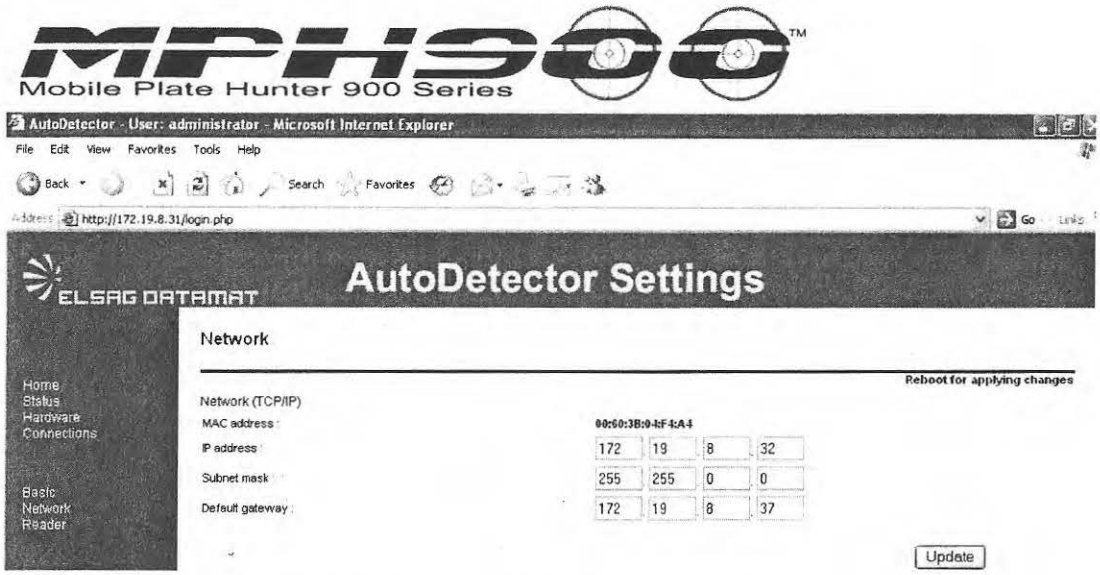
17 Changing default IP address of AD3M.

It might become necessary to change the IP address of the cameras. If so, you need to open up the camera's embedded Web Site through a standard Internet Browser with the discovery tool as done in the previous steps.

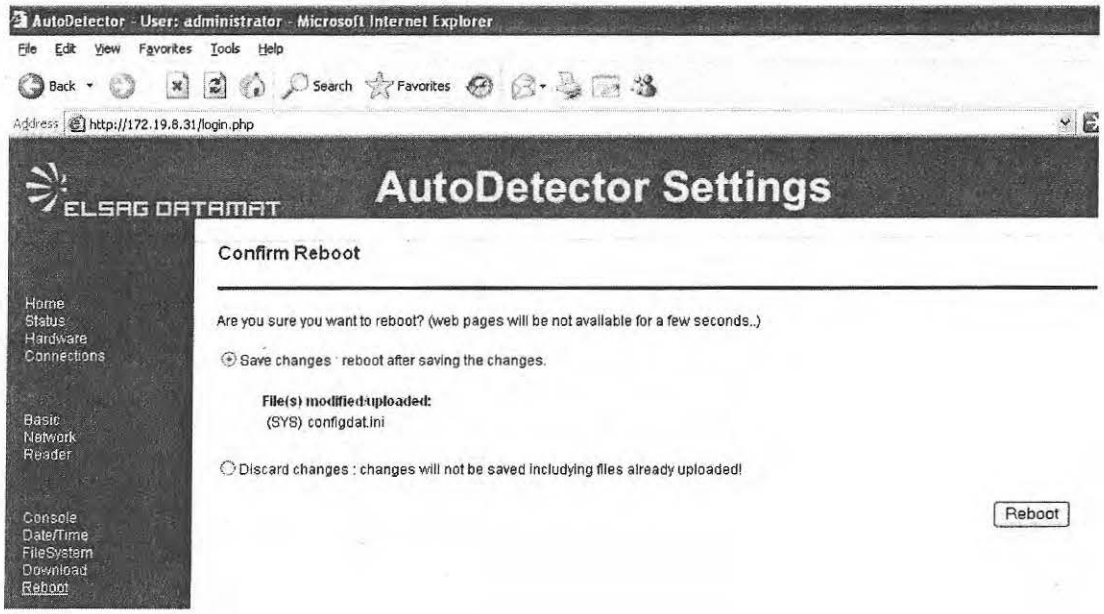
Once logged in click on Network on the right side of browser and will bring you to the site below.



Change the IP address to the address suitable for your network. Make sure that the subnet mask and gateway are correct for your network. Normally the gateway corresponds to the host PC connected to the cameras. Then click Update.
You will then get a flashing prompt to 'Reboot for applying changes'.



Then click on Reboot on the left side and you will be presented with the following window:



Click Reboot. Once the changes have been applied the browser will return the following below and the camera will reboot. Do the same to the other camera if necessary.


MPH900
Mobile Plate Hunter 900 Series
AutoDetector - User: administrator - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://172.19.8.31/login.php
ELSAG DATAMAT
AutoDetector Settin
Home
Status
Hardware
Connections
Basic
Network
Reader
Console
Date/Time
FileSystem
Download
Reboot
Logout
Reboot
commit : set runlevel 2...
commit SYS begins...
commit : sourceroot=/tmp/commit/SYS/
commit : targetroot=/etc/FPM/sys/
commit : copy /tmp/commit/SYS/configdat.ini /etc/FPM/sys/configdat.ini
commit : LPR_save SYS /etc/FPM/sys/ -m > /dev/null
commit : LPR_save SYS /etc/FPM/sys/ -m > /dev/null return 0
System restarting..

MPH900™
Mobile Plate Hunter 900 Series

18 How to change CarId after the installation

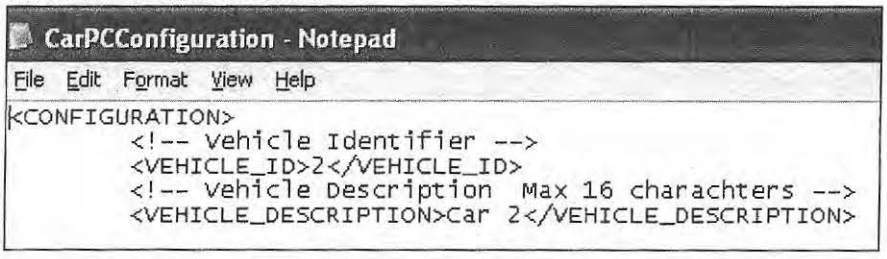
In a fleet of mobile units connected to a central system the CarId must be different for every unit.
Normally it is possible to select the CarId during the software installation but sometimes it is required to change it later. The following procedure explains how to do that without uninstalling and reinstalling the whole CarSystem.

Before changing the CarId in Car System, you must transfer over any data to the OPC server before continuing. Also erase data no longer needed. Changing the CarId will not change information in data files already stored in the PC. If you don't erase old data, there could be malfunctions in the data transfer process after the CarId change.

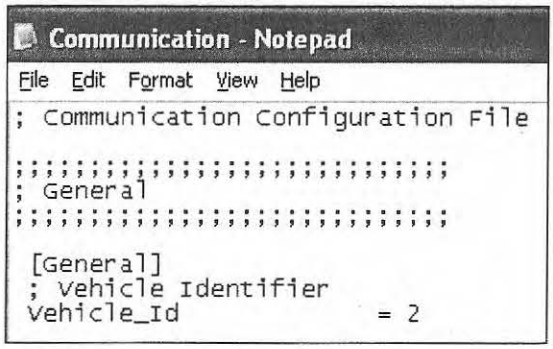
To change the Car Id, there are 6 files that need to be edited in Car System, in case the Communication component is installed. The following files and their path are listed below.
C:\Program Files\Car System\config**carpcconfiguration.xml**
C:\Program Files\Car System\services\config**communication.ini**
C:\Program Files\Car System\services\config**LTBA.ini**
C:\Program Files\Car System\services\config**LTDW.ini**
C:\Program Files\Car System\services\config**MapServices.xml**
C:\Program Files\Car System\services\config**MessageHandler.ini**

Below are screenshots of sections of the files that needs to be edited.
Carpcconfiguration.xml

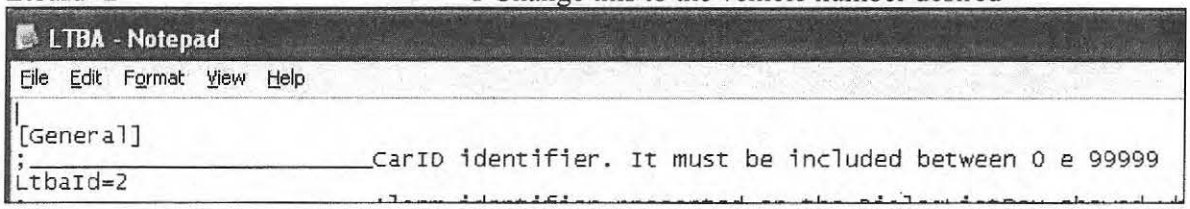
<VEHICLE_ID>2</VEHICLE_ID> ←Change the number 2 to the new vehicle number
<VEHICLE_DESCRIPTION>Car 2</VEHICLE_DESCRIPTION> ← Change Car 2 to the vehicle Desc.



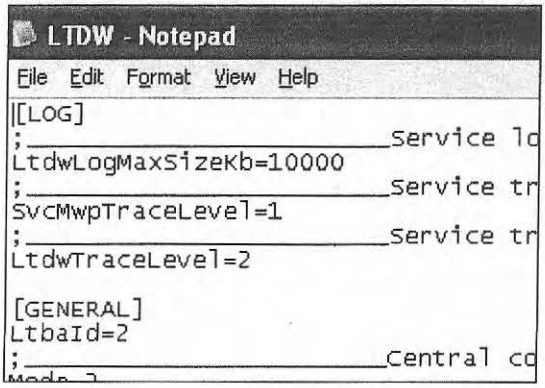
Communication.ini:
Change the following parameter:
Vehicle_Id =2 ←Change this to the vehicle number desired



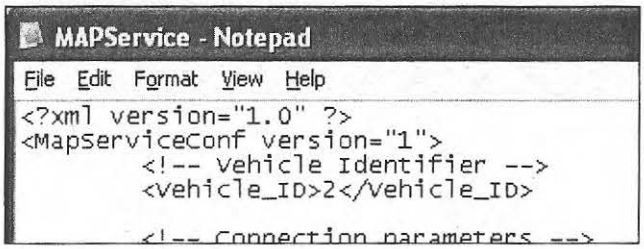
LTBA.ini:
Change the following parameter:
LtbaId=2 ←Change this to the vehicle number desired



LTDW.ini:
Change the following parameter:
Ltbaid=2 ←Change this to the vehicle number desired



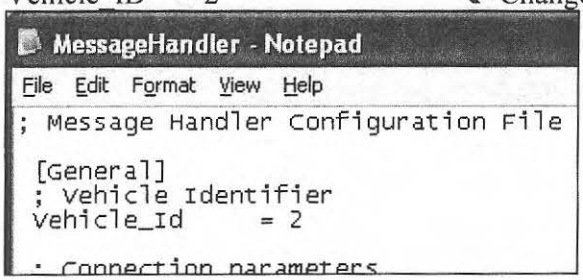
MapService.Xml:
Change the following parameter:
<vehicle_ID>2</vehicle_ID> ←Change this to the vehicle number desired



MessageHandler.ini:

Change the following parameter:

Vehicle_ID =2 ← Change this to the vehicle number desired



Reboot the PC.

19 Loading automatically the HotList from a USB flash drive

If the Hotlist loading system is manual, the default input source folder is C: \hotlist.
It is now possible to load the new Hotlist directly from a thumb drive without any User action.

To activate this function, you need to change the source of the Hotlist path; you can do this by opening the LTBA.ini file in C:\Program Files\Car System\Services\Config and edit the following section:

[LoadPlateList]
;_____Input path for hot list file
HotListSourceDirPath=c: \hotlist

Change to the following below:
[LoadPlateList]
;_____Input path for hot list file
HotListSourceDirPath=**USB\hotlist**

Restart MWP.

In this example the Hotlist will be searched on the \hotlist subfolder of the thumb drive, as soon as the thumb drive will be plugged into the PC, no matter what drive letter will be associated to the USB device.

As opposed to the standard system, the Hotlist file will not be erased by the thumb drive so that the same drive will be usable for multiple vehicles.

20 Discovery Application – Software recovery functionality

Normally the **Discovery Application** shows working devices connected to the PC-LAN, as mentioned above. This list can be refreshed pressing the **refresh** button or the **F5** keyboard button. With this view, in the footer at the bottom of discovery window there are two types of information: the **number of working devices** (on the left) and the presence of **failure devices** (in the middle).
Failure devices are readers that can't boot due to internal software damages. In this case devices broadcast alarm signal by LAN. The **Discovery Application** receives the signal and warns the operator with the flashing message showing in the footer:

"FAILURE DEVICES PRESENT...."

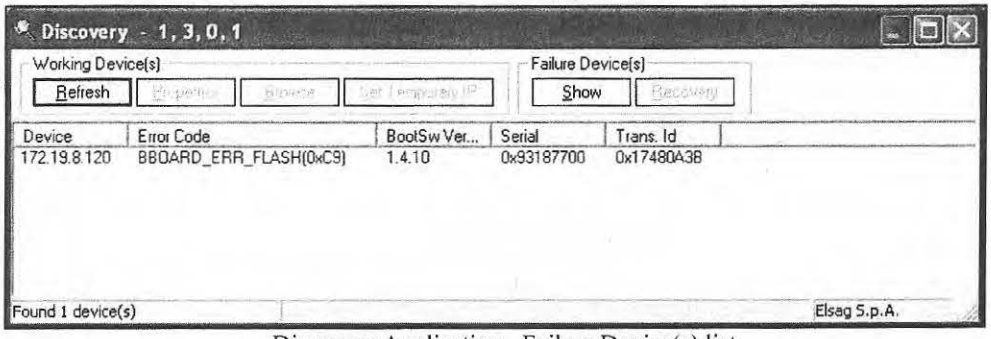
In the **Failure Device(s)** group box there are two buttons that make the user is able to operate on LPR devices that have registered some problems.
When this message is present, the operator can switch **Discovery interface** in **Recovery mode** by pressing **Show** button in the **Failure Device(s)** group box. It's necessary to wait some time (seconds), and then the failure devices will appear in the window.

– Discovery Application - Discovery Failure Device(s) waiting box

When a device goes into failure, it continuously goes into the following sequence:

1. Boot.
2. Search for a DHCP server, if found it, get Ip Address.
3. If DHCP server is not found, use internal default Ip (128.0.0.1)
4. Send broadcast alarm for few seconds
5. Reboot (go to 1).

Then the operator can press **Stop** button in the dialog box. In this way, the operator can see a list of failure devices connected to the PC-LAN.



– Discovery Application - Failure Device(s) list

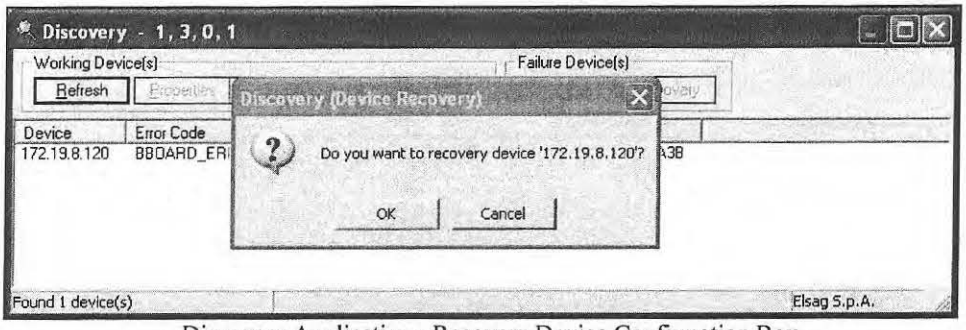
Some information is displayed:

Devices: IP address devices.
Error code: Type of error.
Boot SW Version: Boot version.
Serial: internal (not useful)
Trans Id.: internal (not useful)

To recovery devices in the list, the operator must:

1. Select one device in the list
2. Verify PC IP address that must be in the same class of the reader one.
3. Press **Recovery** Button

A confirmation box will appear.

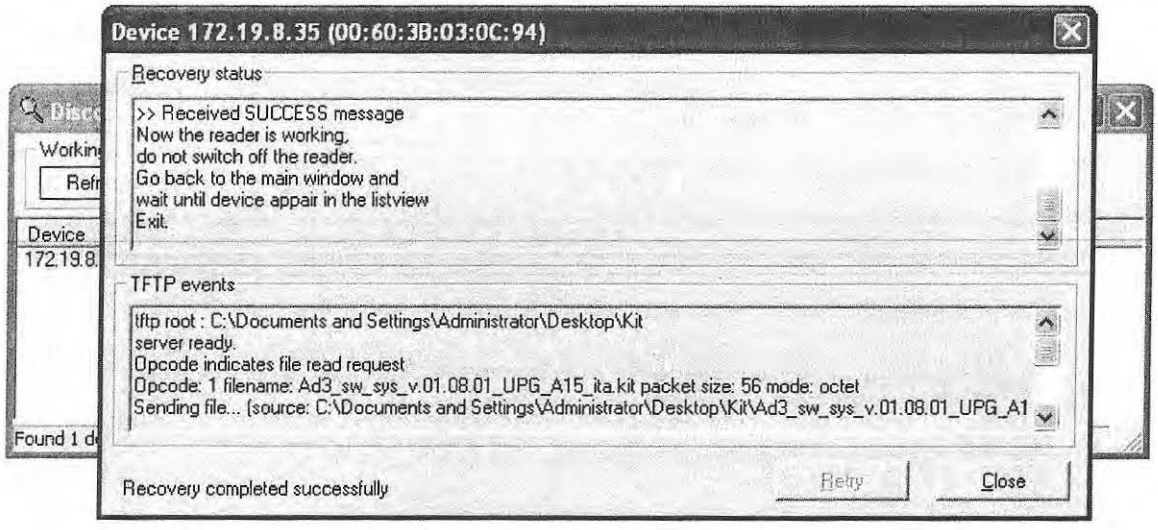


– Discovery Application - Recovery Device Confirmation Box

Press the **OK** button and a new box to select a Kit to upload will appear.

– Discovery Application - Recovery Device Kit Selection

The operator must choose the kit of type "**SYS**". This kit contains all software necessary. After the kit selection, the upload procedure begins.



– Discovery Application - Recovery Upload Procedure

It's necessary to wait some time (seconds), if the program can't connect to the reader try with **Retry** Button.
At the end the reader reboot automatically with the new software.

ATTENTION:
When upload process is ended, the **Close** button becomes active, but the reader is still working, do not switch off the power. It is necessary to wait the end of the update. To understand when the process is ended go to the main window by pressing the **Close** button, and, using the **Refresh** button, wait until the device appear in the window.

With this procedure the device loses all Network and Basic configuration. New Network and Basic configuration will be the default (Ip 172.19.8.30; Id 00001). You must then use the browser and log into the camera to re-configure it.

21 Changing the Default view from B/W to Color

Presently, the ***CarSystem***'s default image view is in BW for compatibility with PUMA BW only cameras. If you prefer color you can change the default view from BW to color. It is done by editing the LTBAConfiguration.xml file.

Go to C:\Program Files\Car System\Config and right click on LTBAConfiguration.xml and select edit.

At the bottom of the page in the section:
<!-- Default View (COLOR - BW) -->
<DEFAULT_VIEW_IMG>**BW**</DEFAULT_VIEW_IMG>

Change >BW< to >COLOR<
<!-- Default View (COLOR - BW) -->
<DEFAULT_VIEW_IMG>**COLOR**</DEFAULT_VIEW_IMG>

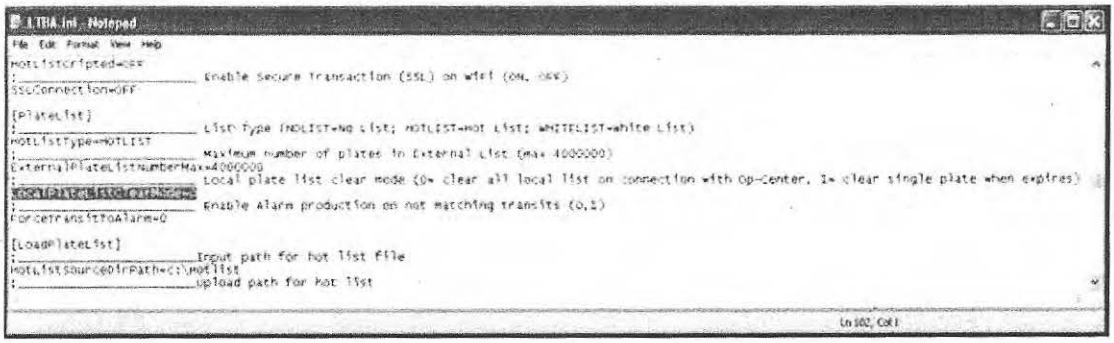
All images will now be displayed in color. You can still toggle back to black and white to view the BW image.

22 How to make the local Hot List permanent

In the normal mode of Operation the local Hot List, generated manually inserting plates through the ***CarSystem*** GUI, is deleted every time an external Hot List is imported.
You cam modify the default behavior by changing a parameter in LTBA.ini

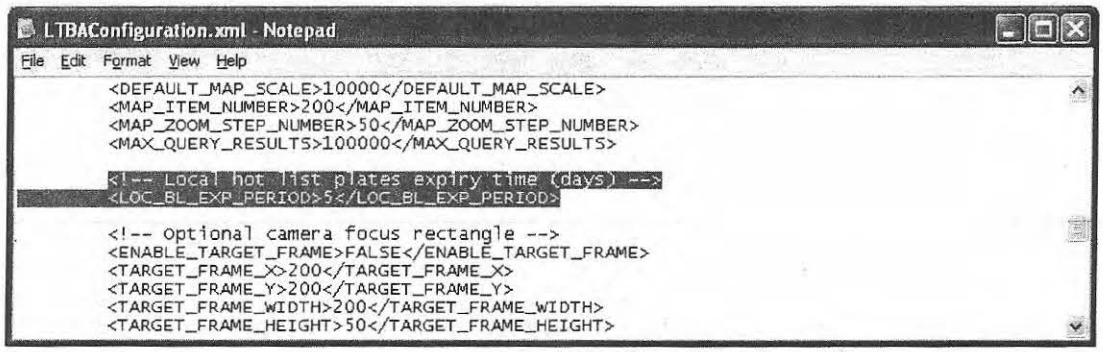
In ..\Carsystem\Services\Config\ open the file LTBA.ini and edit the following line:

LocalPlateListClearMode=0 <= Change to 1 0= clear manual list 1= keep manual list



Changing to 1 will keep all locally added plate list in the ***CarSystem*** until it expires. The default is 5 days. This can be changed in ..\Car System\Config\LTBAConfiguation.xml file in the following section:

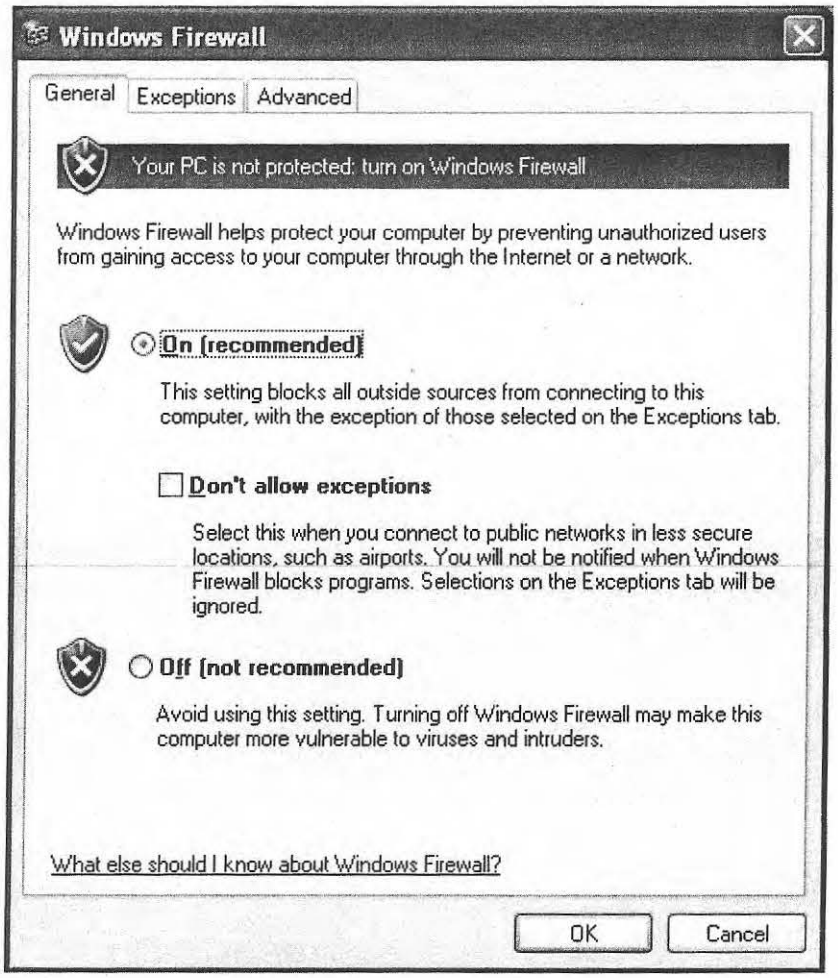
<!-- Local hot list plates expiry time (days) -->
<LOC_BL_EXP_PERIOD>5</LOC_BL_EXP_PERIOD>



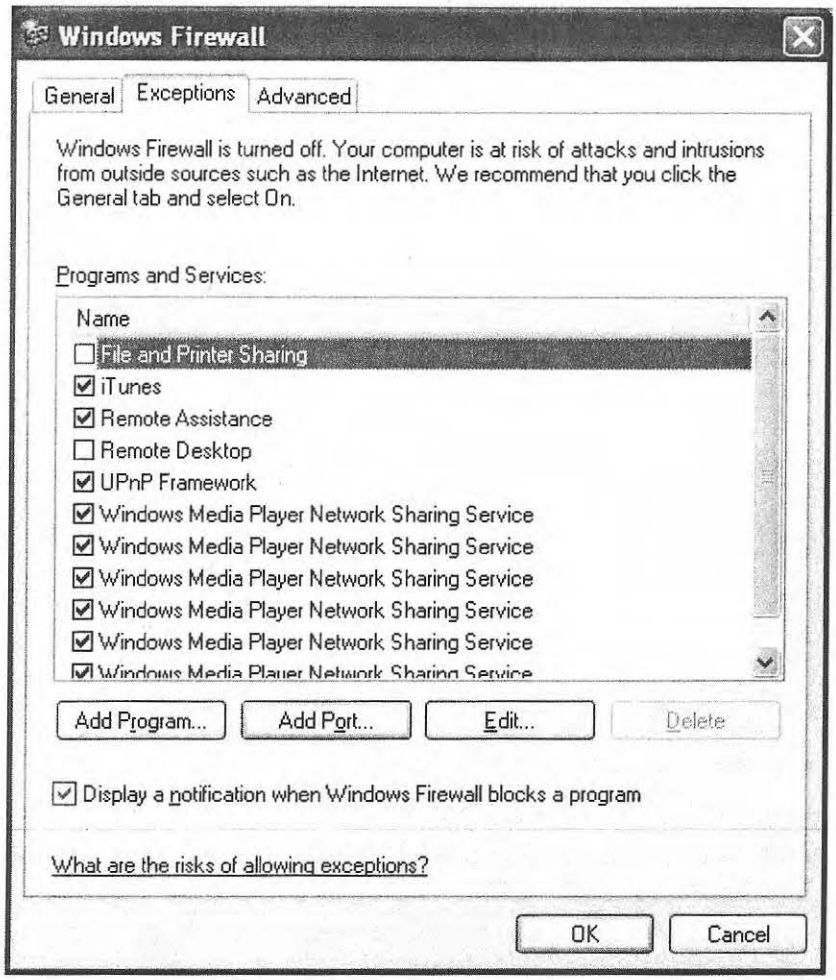
23 How to configure the XP Firewall

This settings apply to both AD3 and Puma-Lite configuration.

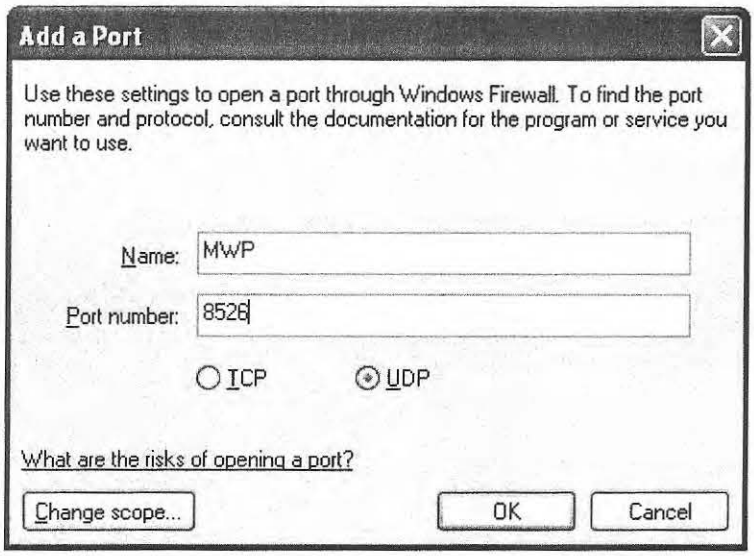
Go to Start - Settings – Control Panel. Click on Windows Firewall and click the On radio button.



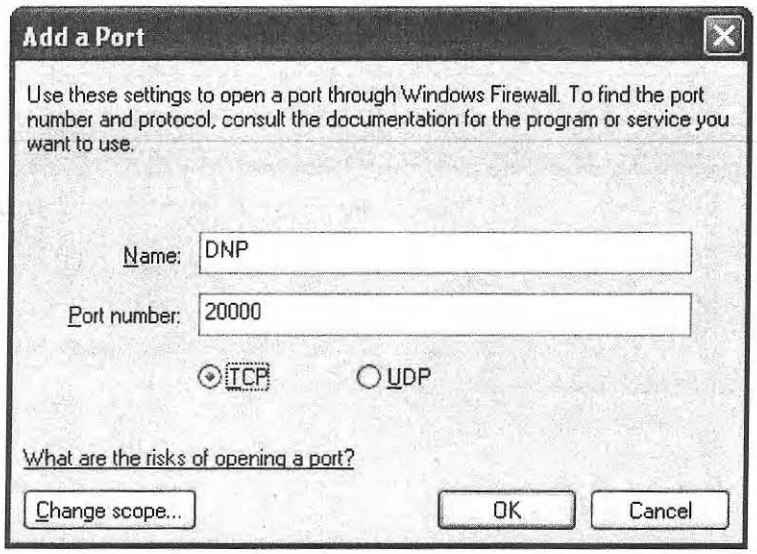
Click on the *Exceptions* tab and click Add Port.



In the Name field type in MWP and in the Port Number box type in 8526. Select the UDP button and click OK.



Click Add a Port again and in the Name box type DNP. In the Port Number box type 20000and select TCP button and click OK.



Click OK to the Windows Firewall dialogue box.