Electronic Locking System (ELS)
ELMcontrol Software User's Manual

Version 1.47
04/2012

CHATSWORTH
PRODUCTS, INC.

800-834-4969
techsupport@chatsworth.com
www.chatsworth.com

Table of Contents

1. Introduction

This manual provides the information necessary to install, configure and use the Electronic Locking System *ELMcontrol* software. The information in this document is subject to change without notice. CPI is not liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Because of the dymanic nature and continued enhancement of CPI products, the illustrations and descriptions in this manual may differ from the various products you receive.

Please address comments on this publication to:

ELS Product Manager
Chatsworth Products, Inc.
9353 Winnetka Avenue
Chatsworth, CA 91311
800-834-4969
Fax: 252-514-2977

2. License Agreement

PLEASE READ THIS LICENSE AGREEMENT CAREFULLY BEFORE INSTALLATION OF SOFTWARE AND USING THE PRODUCT OR SERVICE.

THIS LICENSE AGREEMENT CONTAINS CHATSWORTH PRODUCTS' STANDARD TERMS AND CONDITIONS. WHERE PERMITTED BY THE APPLICABLE LAW, BY KEEPING YOUR CHATSWORTH PRODUCT BEYOND THIRTY (30) DAYS AFTER THE DATE OF DELIVERY, YOU FULLY ACCEPT THE TERMS AND CONDITIONS SET FORTH IN THIS LICENSE AGREEMENT.

IN ADDITION, WHERE PERMITTED BY THE APPLICABLE LAW, YOUR INSTALLATION OF THE SOFTWARE AND/OR USE OF THE PRODUCT OR SERVICES CONSTITUTES FULL ACCEPTANCE OF THE TERMS AND CONDITIONS OF THE LICENSE AGREEMENT CONTAINED HEREIN. THESE INCLUDE WARRANTY DISCLAIMERS, INDEMNIFICATION TERMS AND LIMITATIONS OF LIABILITY.

IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT, INCLUDING ANY WARRANTY DISCLAIMERS, INDEMNIFICATION TERMS OR LIMITATIONS OF LIABILITY, THEN YOU SHOULD NOT USE THE SOFTWARE AND SHOULD RETURN IT TO THE SELLER FOR A REFUND OF THE PURCHASE PRICE.

THE LAW IN YOUR JURISDICTION MAY LIMIT THE EXTENT TO WHICH YOUR RETENTION, INSTALLATION OR USE CONSTITUTES ACCEPTANCE OF THE TERMS AND CONDITIONS HEREIN; AND AS TO THE ENFORCEABILITY OF LIMITATIONS UPON OR EXCLUSIONS OF WARRANTIES, AND UPON INDEMNIFICATION TERMS OR LIMITATIONS OF LIABIILITY, OTHERWISE SET OUT IN THIS AGREEMENT.

This is a License Agreement between Chatsworth Products, Inc. (hereinafter "Chatsworth Products") and you, the end user. Chatsworth Products and you accept the terms and conditions set forth herein, a perpetual, limited, non-exclusive License (hereinafter "License").

License Grant

Chatsworth Products hereby grants you, the end user, a limited, non-exclusive, free to copy, install and use the CPI Electronic Locking System (ELS) *ELMcontrol* software, amendments thereof and its associated files (hereinafter collectively referred to as the "Software") for personal and commercial purposes only. Chatsworth Products provides the License solely for end-user use. You may not reverse engineer, decompile, or disassemble the software. The software is licensed as a single product. Its component parts may not be separated for use on more than one computer. You may not rent or lease the software individually, separately or independently unless it is used in conjunction with the operation of the CPI Electronic Locking System (ELS) hardware.

You may make copies of the software and transfer your rights under this agreement, provided that each recipient of the software also agrees to the terms of this agreement.

Copyright ©

The copyright of the Software at all times belongs to and remains with Chatsworth Products. Without prior approval of Chatsworth Products, no part of the Software may be reproduced, distributed or transmitted in any form or by any means, electronic or mechanical, for any purpose other than stated in the License. All title and copyrights in and to the Software (including but not limited to any images, photographs, animations, video, audio, text, and applets, incorporated into the Software), and any copies of the Software are owned by Chatsworth Products (or one or more of its licensors). The Software is protected by copyright laws and international treaty provisions. Therefore, you must treat the Software like any other copyrighted material except that you may make copies of the Software, subject to the limitations set forth herein.

NO WARRANTY—LIMITATION OF LIABILITY—INDEMNIFICATION—COVENANT NOT TO SUE

I. THE SOFTWARE IS PROVIDED "AS IS," AND NEITHER CHATSWORTH PRODUCTS NOR ANY OF ITS LICENSORS MAKES ANY EXPRESS OR IMPLIED REPRESENTATIONS OR WARRANTIES TO YOU REGARDING THE USABILITY, CONDITION OR OPERATION THEREOF. NEITHER CHATSWORTH PRODUCTS NOR ANY OF ITS LICENSORS WARRANTS THAT THE SOFTWARE WILL MEET ANY PARTICULAR CRITERIA OF PERFORMANCE OR QUALITY AND/OR THAT IT WILL BE FREE FROM VIRUSES OR OTHER DEFECTS. CHATSWORTH PRODUCTS AND ITS LICENSORS EXPRESSLY DISCLAIM ALL IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION, THE WARRANTY OF MERCHANTIBILITY AND THE WARRANTY OF FITNESS FOR A PARTICULAR USE AND THE WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE AND THE WARRANTY OF NON-INFRINGEMENT AND/OR ANY WARRANTY ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

II. YOUR INSTALLATION AND USE OF THE SOFTWARE IS AT YOUR OWN RISK. YOU ASSUME FULL RESPONSIBILITY AND RISK OF LOSS RESULTING FROM YOUR DOWNLOADING, INSTALLING, AND/OR USE OF FILES OR OTHER MATERIAL. YOU AGREE THAT NEITHER CHATSWORTH PRODUCTS NOR ANY OF ITS LICENSORS WILL BE LIABLE FOR DAMAGES (INCLUDING BUT NOT LIMITED TO DIRECT, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR SPECIAL DAMAGES) ARISING OUT OF YOUR INSTALLATION OF, USE OF, OR INABILITY TO USE THE SOFTWARE, AND YOU HEREBY WAIVE ANY CLAIMS OF ANY KIND WITH RESPECT THERETO, WHETHER BASED IN CONTRACT, BREACH OF WARRANTY, TORT OR ON ANY OTHER GROUNDS, EVEN IF CHATSWORTH PRODUCTS (OR ANY SUCH LICENSOR) HAS BEEN ADVISED OF THE POSSIBILITY OF DAMAGES, AND WHETHER OR NOT CAUSED BY CHATSWORTH PRODUCTS' OR ITS LICENSORS' NEGLIGENCE. THE SOLE AND ENTIRE LIABILITY OF CHATSWORTH PRODUCTS AND ITS LICENSORS, AND YOUR EXCLUSIVE REMEDY WITH RESPECT TO THE USE OF THE SOFTWARE OR ANY BREACH OF THIS AGREEMENT, SHALL BE THE REPLACEMENT OF ANY SOFTWARE FOUND TO BE DEFECTIVE.

III. YOU AGREE TO RELEASE, WAIVE, DISCHARGE AND COVENANT NOT TO SUE CHATSWORTH PRODUCTS, ITS LICENSORS, OWNERS, DIRECTORS, OFFICERS, EMPLOYEES, AGENTS, SUPPLIERS OR AFFILIATED COMPANIES, FOR ANY AND ALL LIABILITIES ARISING FROM OR POTENTIALLY ARISING FROM ANY CLAIM, DEMAND OR ACTION BASED UPON ANY LOSSES, LIABILITIES, DAMAGES OR COSTS, INCLUDING BUT NOT LIMITED TO DAMAGES THAT ARE DIRECT OR INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL, AND INCLUDING ATTORNEYS FEES AND LEGAL COSTS, THAT MAY RESULT FROM INSTALLATION, OPERATION OF, USE OF, OR THE INABILITY TO USE CHATSWORTH PRODUCTS' SOFTWARE, OR FROM THE FAILURE OF CHATSWORTH PRODUCTS' SYSTEM TO REPORT A GIVEN EVENT OR CONDITION, WHETHER OR NOT CAUSED BY CHATSWORTH PRODUCTS' NEGLIGENCE, EXCEPT AS NECESSARY TO ENFORCE THE EXPRESS TERMS OF THIS LICENSE AGREEMENT.

IV. YOU WILL INDEMNIFY, DEFEND AND HOLD HARMLESS CHATSWORTH PRODUCTS, ITS LICENSORS, OWNERS, DIRECTORS, OFFICERS, EMPLOYEES, AGENTS, SUPPLIERS OR AFFILIATED COMPANIES, AGAINST ANY AND ALL CLAIMS, DEMANDS OR ACTIONS BASED UPON ANY LOSSES, LIABILITIES, DAMAGES OR COSTS, INCLUDING BUT NOT LIMITED TO DAMAGE THAT ARE DIRECT OR INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL, AND INCLUDING ATTORNEYS FEES AND LEGAL COSTS, THAT MAY RESULT FROM INSTALLATION, OPERATION OF, USE OF, OR THE INABILITY TO USE CHATSWORTH PRODUCTS' SOFTWARE, OR FROM THE FAILURE OF CHATSWORTH PRODUCTS' SYSTEM TO REPORT A GIVEN EVENT OR CONDITION, WHETHER OR NOT CAUSED BY CHATSWORTH PRODUCTS' NEGLIGENCE.

V. WITHOUT WAIVING ANY PROVISION IN THIS LICENSE AGREEMENT, IF A CIRCUMSTANCE ARISES WHERE CHATSWORTH PRODUCTS AND/OR ITS LICENSORS ARE FOUND TO BE LIABLE FOR ANY LOSS OR DAMAGE ARISING OUT OF MISTAKES, NEGLIGENCE, OMISSIONS, INTERRUPTIONS, DELAYS, ERRORS OR DEFECTS IN THE SOFTWARE SUBJECT TO THIS AGREEMENT, THEN SUCH LIABILITY SHALL NOT EXCEED THE TOTAL AMOUNT PAID BY THE CUSTOMER UNDER THIS LICENSE AGREEMENT OR $250.00, WHICHEVER IS GREATER. YOU HEREBY RELEASE CHATSWORTH PRODUCTS AND ITS LICENSORS FROM ANY AND ALL OBLIGATIONS, LIABILITIES AND CLAIMS IN EXCESS OF THIS LIMITATION.

VI. NEITHER CHATSWORTH PRODUCTS NOR ANY OF ITS LICENSORS SHALL BE HELD RESPONSIBLE IN ANY WAY OR BY ANY MEANS, EITHER DIRECTLY OR INDIRECTLY, FOR ANY COMMUNICATIONS DIFFICULTIES OUTSIDE OF CHATSWORTH PRODUCTS' CONTROL WHICH COULD LEAD TO THE INTERRUPTION OF DATA DELIVERY SERVICE TO YOUR ELECTRONIC MAIL ADDRESS, PAGER, TELEPHONE OR ANY OTHER RECEIVING DEVICES OR THIRD-PARTY DATA STORAGE AND/OR DELIVERY SERVICES.

VII. IN PARTICULAR, YOU WILL NOT RELY ON ANY REPRESENTATION OR WARRANTY, EXPRESSED OR IMPLIED, MADE BY ANY PERSON OTHER THAN AN AUTHORIZED REPRESENTATIVE OF CHATSWORTH PRODUCTS, IN EVALUATING THE SOFTWARE.

VIII. THE LAW IN SOME JURISDICTIONS MAY LIMIT OR PRECLUDE WARRANTY EXCLUSIONS OR LIMITATIONS, INDEMNIFICATION TERMS AND/OR LIMITATIONS ON LIABILITY, SO NOT ALL OF THE ABOVE LIMITATIONS MAY APPLY TO YOU.

Disclaimer

Although the Software is scanned for the known viruses, you should scan the Software for viruses or other defects, prior to installation on your system. Chatsworth Products does not accept any liability for damage or loss as a result of the installation or use of the Software, including but not limited to any damage or loss resulting from any such viruses or defects.

Notwithstanding its efforts Chatsworth Products reserves the right to change the Software and publish new release versions. Chatsworth Products assumes no responsibility in notification to the end-user of new release updates or versions of the Application.

Web site use

Customer may use services provided by CHATSWORTH Products on an Internet web site that could be connected to the use of the Software subject to this Agreement. The use of such web site may only be made by authorized users with a proper identification and password or serial number.

In using such a web site, you are further BOUND BY THE TERMS AND CONDITIONS LOCATED ON THE WEB SITE. YOU MUST READ ALL OF THE TERMS AND CONDITIONS BEFORE PROCEEDING TO USE THE WEB SITE. IF YOU DO NOT AGREE TO ANY OF THE TERMS AND CONDITIONS ON THE WEB SITE, THEN YOU SHOULD CEASE USING THE WEB SITE, AND INFORM CHATSWORTH PRODUCTS THAT YOU DO NOT INTEND TO USE AND/OR CONTINUE USING THAT WEB SITE. YOUR USE OF THE WEB SITE IS AN ACKNOWLEDGMENT THAT YOU AGREE TO ALL THE TERMS AND CONDITIONS THEREIN.

Deemed acceptance and applicable law

The installation or use of the Software is deemed acceptance of the terms and conditions contained in the License Agreement. This License Agreement shall be effective and binding upon Chatsworth Products and you, the end user, upon installation or use of the Software. The term of this Agreement shall commence on the date of installation or use by you and shall continue indefinitely if you remain in compliance with all of the terms and condition set forth herein. If you do not agree to the terms of the License, please do not install or otherwise use the Software.

Choice of Forum and Choice of Law

In the event that a dispute arises out of or in connection with this License Agreement, then any claims or suits of any kind concerning such disputes shall only and exclusively be brought in either the Court of Los Angeles County, California or the United States District Court in Los Angeles, California.

Regardless of the place of contracting or performance, this License Agreement and all questions relating to its validity, interpretation, performance and enforcement shall be governed by and construed in accordance with the laws of the State of Delaware, without regard to the principles of conflicts of law.

3. Warranty

Chatsworth Products, Inc. (CPI) guarantees manufactured products and each part or component thereof against all defects in material and/or workmanship. CPI agrees to remedy any manufacturing defect either through replacement or repair at no charge, provided that the defective unit is returned, transportation prepaid, to the CPI factory. The warranty extends for a period of one year from the date of installation or initial use, provided that this period shall not exceed 18 months from the original date of shipment from the factory.

Any product that has been repaired or replaced shall be similarly warranted on its repair or replacement for the remaining product warranty period or 90 days from the date of repair or replacement, whichever expires last.

This warranty does not extend to products that have been subjected to neglect, accident or improper use, nor to units that have been altered by non-CPI personnel.

No warranties other than those set forth in this section are given or implied with respect to the products furnished. CPI shall, in no event, be liable for consequential damages, for loss, damage or expense directly or indirectly arising from the use of the products, for any inability to use materials or from any other cause.

4. Service and Support

For answers to your questions, please email Technical Support at **techsupport@chatsworth.com**, or call toll-free at **800-834-4969** (US. & Canada) Monday to Friday, 5 a.m. to 5 p.m., Pacific Time.

5. System Overview

The *ELMcontrol* software allows easy configuration, control and monitoring of the CPI Electronic Locking System (ELS) from a computer with a Microsoft Windows® operating system.

The ELS includes a Communications Module (P/N 16147-050) and any combination of up to 64 Electronic Lock Control Modules (P/N 16147-052), 512 Electronic Lock Upgrade Kits (P/N 16147-060, 16147-061, 16147-062 and 16147-063), 64 Keypad Modules (P/N 16147-008) and 64 Proximity Card Reader Modules (P/N 16147-054). All modules connect with CAT 5 patch cords to form a Controller Area Network (CAN) Bus. (Keypad Modules connect with a special S1 to RJ-11 cable; one cable is included with the module.).

Data is exchanged between the computer hosting the *ELMcontrol* software and the Communications Module via an Ethernet LAN connection or a direct serial interface (RS232). The communications protocol is Simple Network Management Protocol SNMPv1 (RFC1157). (The Communications Module provides SNMPv1 and SNMPv2c to allow the integration of the system into third party SNMP manager programs.) The SNMP is available at the network interface as well as at the serial interface. The serial interface provides some additional configuration functions needed for the initial set up of the system (e.g. LAN IP address and workstation login passwords). For security reasons the data exchange is possible on authorized computers or by authorized persons, only.

The computer hosting the *ELMcontrol* software must be connected to the system before any configuration changes will take effect. The configuration settings for the ELS modules are directly checked and saved in the ELS modules by the *ELMcontrol* software.

6. Software Installation

The installation of *ELMcontrol* requires Microsoft Windows® 98, Microsoft Windows® ME, Microsoft Windows® NT 4.0, Microsoft Windows® 2000 or Microsoft Windows® XP on the workstation. The network protocol TCP/IP is required for Ethernet LAN connection to the ELS.

6.1. Installation from the CPI-ELMcontrol CD

- Put the CPI-*ELMcontrol* CD into the CD-ROM-drive. If the AutoRun feature for CDs is enabled, the *ELMcontrol* installation program ('Setup.exe') starts automatically. If you see a dialog box, then the installation program has started. If the installation program does not appear, then AutoRun may be disabled. In this case start 'Windows Explorer', double-click the CD-ROM drive to open it and double-click the 'Setup.exe' file to begin the installation.

- Click on the button **ELMcontrol installation**.

- Follow the installation instructions.

6.2. Download and Installation From the Website

- Download the *ELMcontrol* Software from CPI Website (http://www.chatsworth.com/Support-and-Downloads/Downloads/Software/). You will get a compressed file (ZIP format).

- Extract the contained files into a directory on your hard disk.

- Start the 'Setup.exe' file.

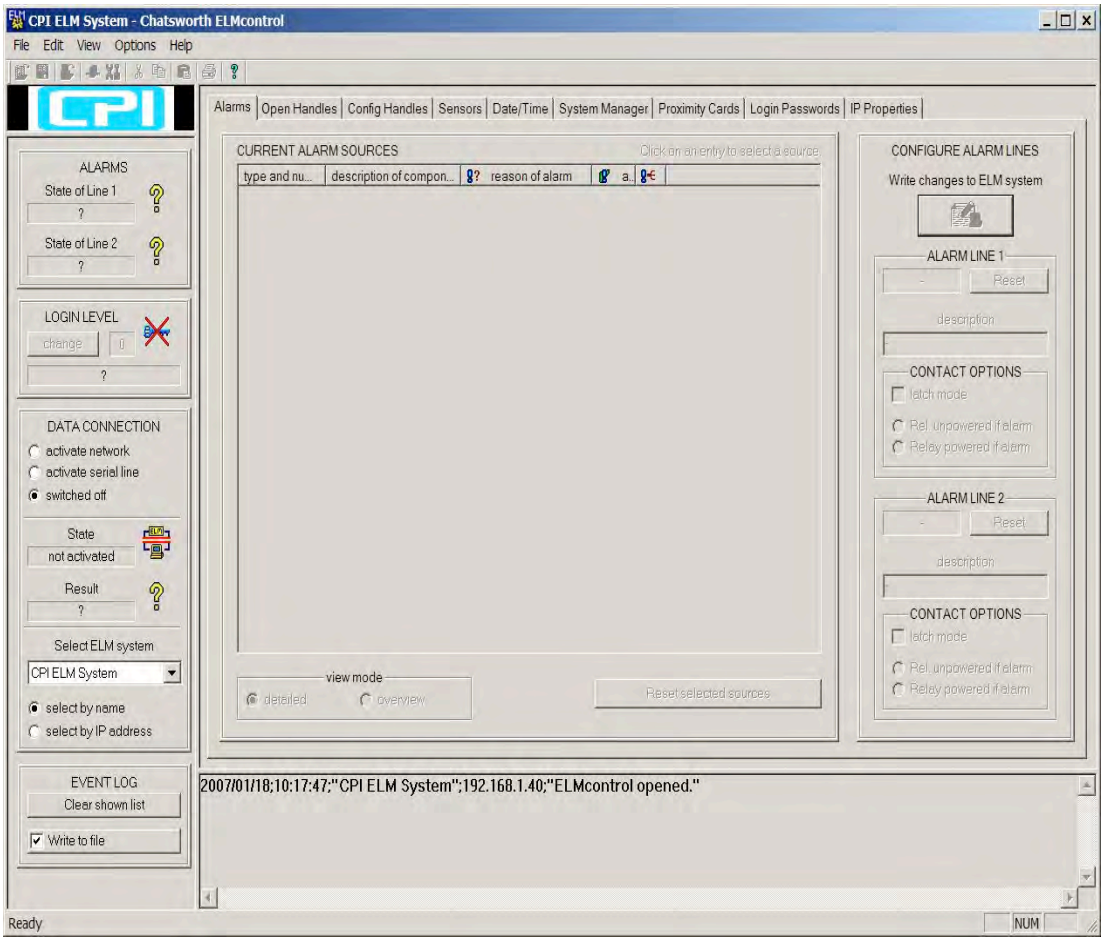
- Follow the installation instructions.

7. User Interface

The user interface of *ELMcontrol* includes different sections. In the left column there are alarm annunciators, settings for and display of data connections to the system, and event log controls.

In the top part of the right column there are several tabs for viewing, installing and controlling different components and features of the system (e.g. alarms, modules and handles).

Events, relevant processes, warnings and errors are indicated and recorded in the lower window.



7.1. Selection of the Workspace Language

The initial installation of *ELMcontrol* sets the workspace language to the language of the operating system. Currently *ELMcontrol* supports English, German, Italian and French. If the installation program detects an operating system of another language, English will be set as default. The preferred language can be selected in *ELMcontrol* as follows:

- Select the menu **Options** from the main menu strip.
- Select the menu entry **Language.**

The following window is displayed:

- Click the button of the language you want to select and click on **Ok**.

The change of language will take effect the next time the program is started.

7.2. Data Connections

Data is exchanged between the computer hosting the *ELMcontrol* software and the ELS modules via a network or serial interface with the Communications Module (P/N 16147-050).

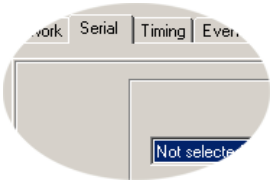
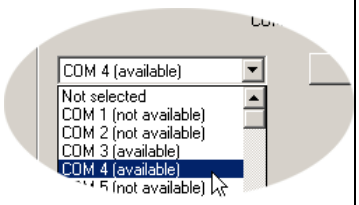
A serial connection is required to configure a network IP address for the Communications Module and to select workstation login passwords. All other configuration data can be exchanged via the network or the serial connection.

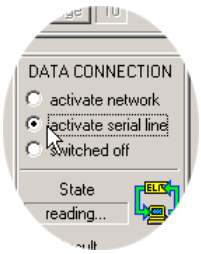
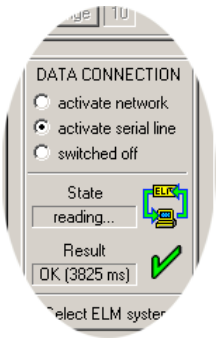
7.2.1. Quick Guides for Getting Started

The following instructions give an overview of important settings that allow a data connection between *ELMcontrol* and the ELS modules. The following sections include a detailed presentation.

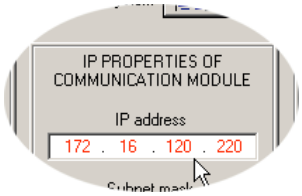
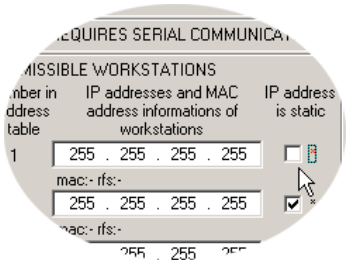
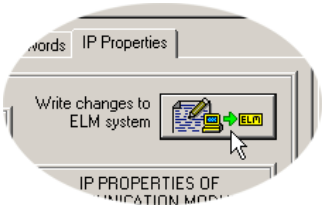
First, verify that the necessary cable connections are made, the ELS modules are on and *ELMcontrol* has been started on the workstation.

7.2.1.1. A Quick Guide for Setting up a Serial Connection

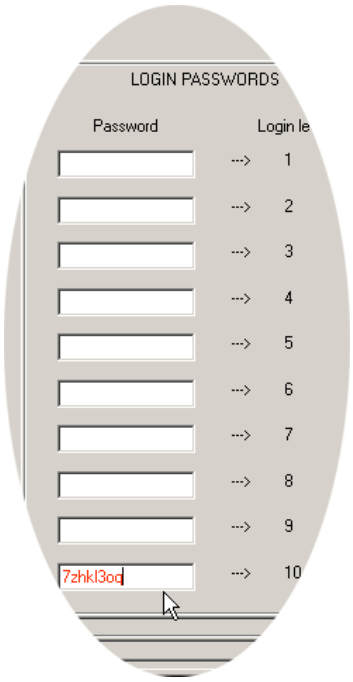
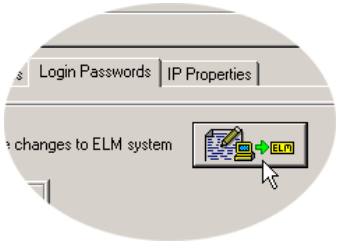
Nr.	WHAT TO DO?	HOW TO DO?	WHEN TO DO?
1	*Choose the serial port of the workstation to which the Communications Module is connected.*	Select **Options** / **Configuration** from the main menu. 	*Only necessary after an initial installation or if switching to another serial port.*
		Click the **Serial** tab of the displayed window. 	
		Go to the **COM PORT** area and check the correct port. 	
		Click the **Ok** button. 	

2	Activate the connection.	Click the **activate serial line** button in the **DATA CONNECTION** area of the user interface.		Always necessary
3	Check the connection.	The **Result** field in the **DATA CONNECTION** area should show **OK**.		

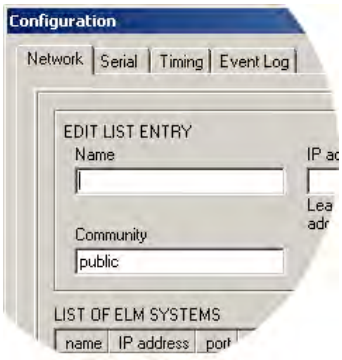
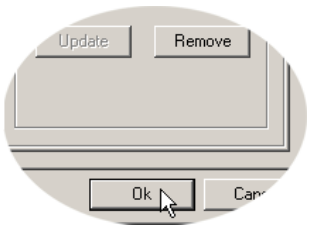
7.2.1.2. A Quick Guide for Setting up a Network Connection

Nr.	WHAT TO DO?	HOW TO DO?	WHEN TO DO?
1	*Establish a serial connection to configure the IP properties of the Communications Module.*	See section 7.2.1.1. *A Quick Guide for Setting up a Serial Connection*, above.	*Only necessary under the following conditions:* *-Initial installation* *-Exchange of the Communications Module* *-Firmware update of the Communications Module* *-If changing the IP configuration*
2	*IP-Configuration of the Communications Module*	Click the **IP properties** tab on the user interface. 	
		Enter the IP address that should be used by the Communications Module into the **IP address** field of the **IP PROPERTIES OF COMMUNICATION MODULE** area. 	
		Uncheck at least one of the **IP address is static** check boxes in the **PERMISSIBLE WORKSTATIONS** area. 	
		Click the **Write changes to ELM system** button. 	

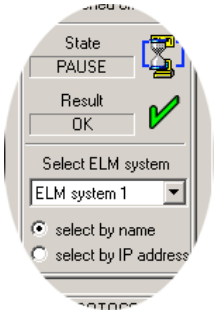
A Quick Guide for Setting up a Network Connection – continued

Nr.	WHAT TO DO?	HOW TO DO?	WHEN TO DO?
3	*Setting a login password*	Click the **Login Passwords** tab on the user interface. 	*Only necessary under the following conditions:* *-Initial installation* *–Exchange of the Communications Module* *-Firmware update of the Communications Module* *-To change login passwords*
		Enter a password for login level 10 into the corresponding input field of the **LOGIN PASSWORDS** area. *Remember the password. You will use the password to access the system from a workstation.* 	
		Click the **Write changes to ELM system** button. 	

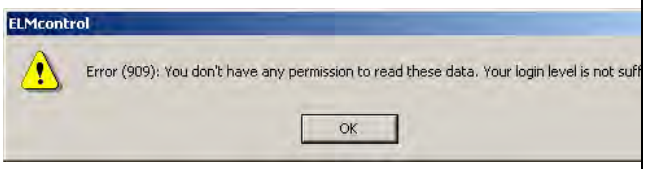
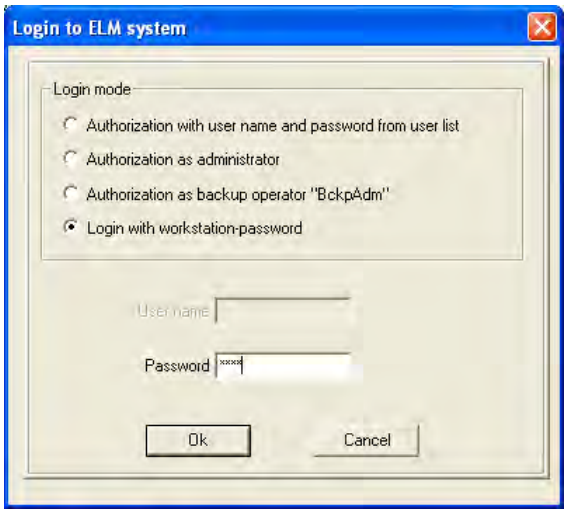
A Quick Guide for Setting up a Network Connection – continued

Nr.	WHAT TO DO?	HOW TO DO?	WHEN TO DO?
4	*Include the name of the system in the list of ELM systems*	Select **Options** / **Configuration** from the main menu. 	*Only necessary if the system is not already included in the list of ELM systems.* *If a serial data connection was established before, then a proper list entry already exists.* *If the name is a domain name which can be translated by DNS (Domain Name Service) into an IP address then entering an IP address is not required.*
		Click the **Network** tab of the displayed window. 	
		In the **EDIT LIST ENTRY** area, enter a name for the system into the **Name** field and enter the IP address of the Communications Module into the **IP address** field. Click on the **Update** button. (The new entry appears in the **LIST OF ELM SYSTEMS** table.) 	
		Click the **Ok** button. 	

A Quick Guide for Setting up a Network Connection – continued

Nr.	WHAT TO DO?	HOW TO DO?	WHEN TO DO?
5	*Select the system you wish to access from the ELM system list.*	From the user interface, go to the **DATA CONNECTION** area and click on the arrow beside the field **Select ELM system** and select the system you wish to access from the list in the display. 	*Only necessary if the list of ELM systems contains more than one sysem, and the system required is not selected.* *If a serial data connection was established to the system before, then the system is already selected.*
6	Activate the connection.	From the user interface, go to the **DATA CONNECTION** area and click on the **activate network** button 	Always necessary
7	Check the connection.	The **Result** field in the **DATA CONNECTION** area should show **OK**. *The workstation is connected to the system (Communications Module) with a network connection using the ELMcontrol software.* 	

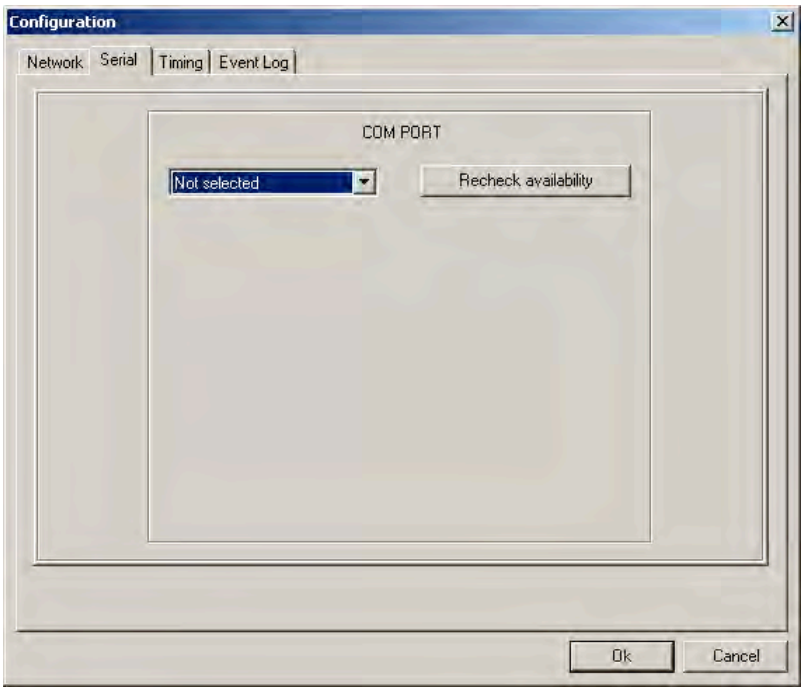
A Quick Guide for Setting up a Network Connection – continued

Nr.	WHAT TO DO?	HOW TO DO?	WHEN TO DO?
8	Login to the system	 Click the **Ok** button to quit the message box.	*Only necessary if this message box is displayed.* *This is always the case after initial installation or after a firmware update of the Communicati ons Module.*
		Click on the **change** button in the **LOGIN LEVEL** area on the user interface. 	
		 Select the button: Login with workstation-password. Enter the password (entered at number 3 above) and click the **Ok** Button.	
9	*Check the login level.*	The authorized level is shown in the **LOGIN LEVEL** area of the user interface. 	

7.2.2. Setting Up a Serial Connection

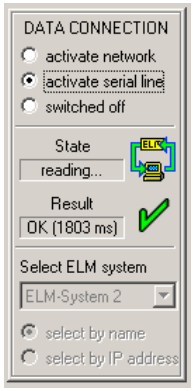
Install the *ELScontrol* software on a workstation following the steps in section 6. Then, connect the Communications Module to the workstation using the included Null Modem Cable. Use the *ELScontrol* software to configure a serial connection as follows:

- Select the menu **Options** from the main menu.
- Select the **Configuration** menu.
- Click the **Serial** tab of the displayed window.
- Select the serial port where the Communications Module (P/N 16147-050) is connected to the workstation and click on **Ok**.



After selecting the serial port, activate the data connection as follows:

- To start the system scan click the button **activate serial line** in the **DATA CONNECTION** area on the user interface.



The **State** field in the area **DATA CONNECTION** shows the current scan in process. The **Result** field indicates whether the last scan cycle was free of error and how much time the cycle took.

The system connected to the serial port is automatically added to the list of selectable ELM systems in the **DATA CONNECTION** area and is displayed under **Select ELM system**.

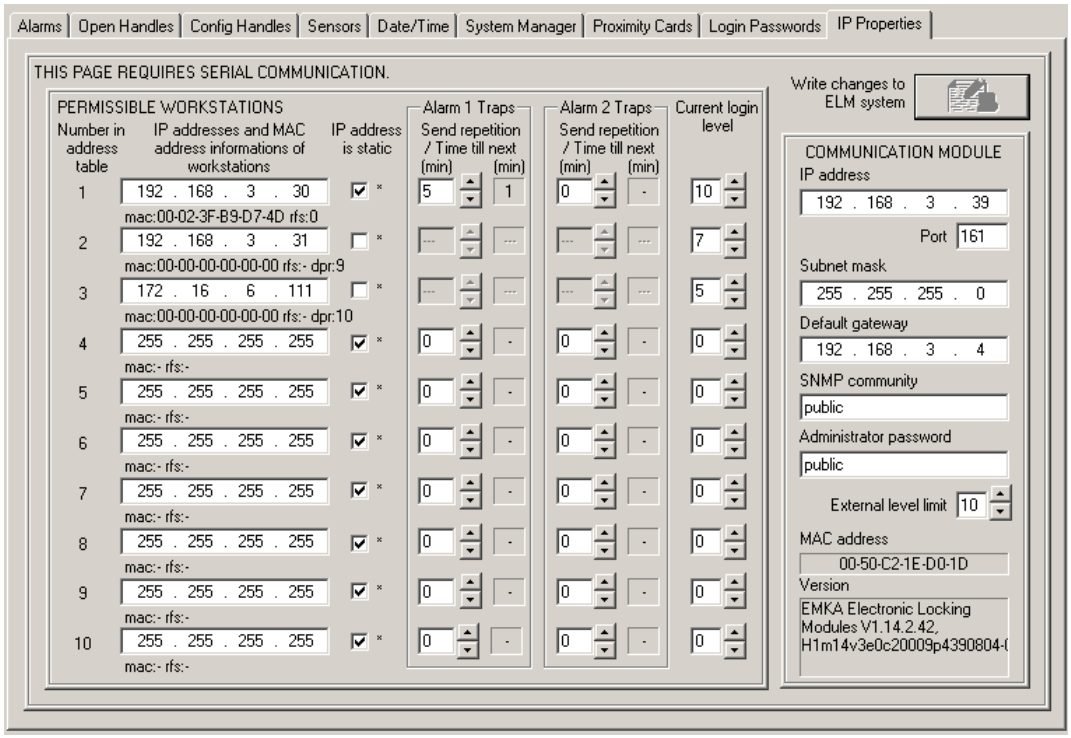
7.2.3. Setting Up a Network Connection

7.2.3.1. Network Setup of the System IP Properties

The Communications Module (P/N 16147-050) must be IP-configured through a serial connection before a network connection can be established. Basic configuration requires the setting of an IP address, workstation permissions and at least one login password.

Set up a serial connection between a workstation with the *ELMcontrol* software and the Communications Modules (see section 7.2.2. Setting up a Serial Connection).

Click the index-tab **IP Properties,** that leads you to the below index card.



The index card **IP Properties** allows configuration of all network parameters used by the Communications Module. The settings from this index card are stored in the Communications Module.

The area **COMMUNICATION MODULE** includes the following settings:

IP address
Enter the IP address of the Communications Module.

Port
Enter the port number that the Communications Module will use. The SNMP standard port is 161.

Subnet mask
Set up of a subnet mask is required if the Communications Module will send SNMP-traps.

Default gateway
The IP address of the gateway is required if the Communications Module will send traps to targets located in a different network.

SNMP community
Enter the default SNMP community string that will be accepted by the Communications Module.

Administrator password
Enter the administrator password. For more information about login as administrator see section 7.3. Permissions.

Note, that a workstation login ["login as workstation"] is not possible if the SNMP community is different from the administrator password. The different login methods are explained in section 7.3.1. Login Methods.

External level limit
Enter the maximum permitted login level when accessing the system from the WAN (wide area network).

MAC address
The MAC address of the Communications Module is shown for information purposes only, no changes are possible.

Version
Displays the actual hardware and software version of the Communications Module.

The area **PERMISSIBLE WORKSTATIONS** list the workstations that can exchange data with the Communications Module and receive SNMP-traps. Designate a specific IP address for each workstation, how often SNMP-traps are sent to the workstation and a login limit for the workstation as follows:

IP addresses and MAC address information of workstations; IP address is static
To allow a specific workstation to access the system, enter the static IP address of the workstation and check the button **IP address is static**. This space will be reserved for the workstation. **Traps can be sent to workstations with static IP addresses, only.**

If you delete the check mark under **IP address is static**, the Communications Module automatically enters the IP address of a workstation that successfully logs-in by means of a valid **workstation password** (see section 7.3 Permissions). This process allows the use of workstations that get a changing IP address by means of DHCP (Dynamic Host Configuration Protocol). To those workstations, however, the system cannot send any traps. If all of the "dynamic chart positions" are filled, the oldest entry will be deleted when a new workstation successfully logs on.

Below every IP address field the MAC address of the workstation (**mac**) and the last data exchange with the workstation in minutes (**rfs**) is shown. For a "dynamic chart position" there is an additional display of the dynamic priority (values **0** to **10**) for the corresponding workstation (**dpr**). If all chart positions are full, the "dynamic workstation" with the lowest priority is automatically deleted from the chart when an additional workstation that is not listed in the chart successfully logs on.

Alarm Traps can be designated for workstations with static IP addresses, only.

Alarm 1 Traps – Send repetition
Enter the interval in minutes for traps being sent by the system to the corresponding workstation when the condition of alarm line 1 is **active** or **latched** (see section 7.9. Configuration of Alarm). The interval can be **1** to **254** minutes. No trap is sent if the value is **0**.

Alarm 1 Traps – Time till next
This display shows the time in minutes remaining until the next trap is sent when alarm line 1 is **active** or **latched**.

Alarm 2 Traps - Send repetition
Enter the interval in minutes for traps being sent by the system to the corresponding workstation, when the condition of alarm line 2 is **active** or **latched** (see section 7.9. Configuration of Alarm). The interval can be **1** to **254** minutes. No trap is sent if the value is **0**.

Alarm 2 Traps - Time till next
This display shows the time in minutes remaining until the next trap is sent when alarm line 2 is **active** or **latched**.

Current login level
This display shows the current login level of the workstation. The selected level is active until the next login by workstation password from this workstation (see section 7.3 Permissions).

All changes in the input fields become effective only after a click on the button **Write changes to ELM system.** If you fail to click this button all changes are lost as soon as you leave the index card **IP Properties.**

7.2.3.2. Network Setup of a Workstation

Workstations that connect to the system through the network (LAN) must be configured for network connection using the TCP/IP protocol. Installation and configuration of the TCP/IP-protocol is explained in the documentation for the Windows® - operating system. The IP address of the workstation may be static or assigned by a DHCP-server. The workstation must be on the same LAN as the Communications Module.

More than one system can be accessed through the LAN from the workstation. The *ELMcontrol* software creates a list of systems and stores the list on the workstation.

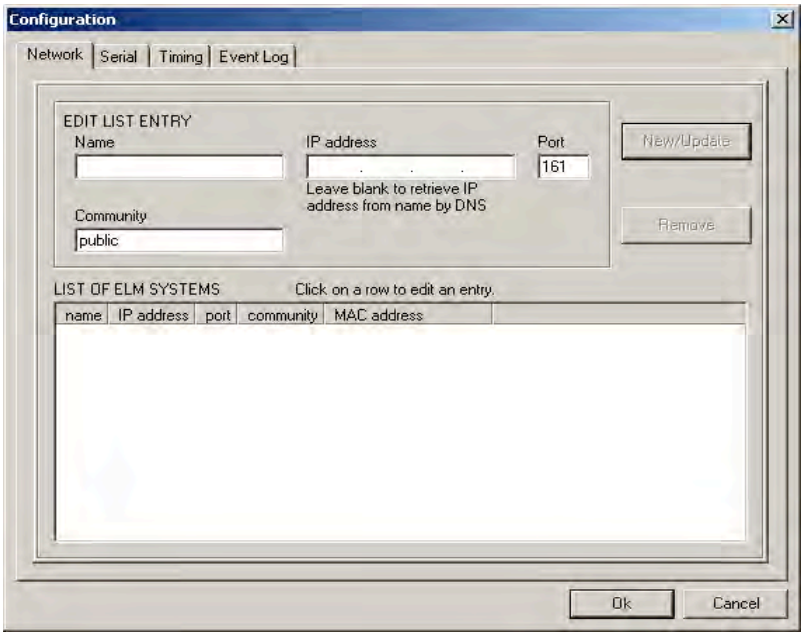
Every list entry contains a name, IP address, IP port, a SNMP community string and a MAC address. The name of the selected list entry is shown in the title strip of the user interface. All data and operations in the display refer to the selected system that is currently active. Referring to the relevant list selection *ELMcontrol* stores some status information in the workstations registry memory.

To establish a network connection between *ELMcontrol* and a system an entry representing the system must be included in the list of ELM systems. Each entry represents a different Communications Module and associated ELS modules. Such an entry is automatically made during a serial connection. You can add to, review and edit the list of ELM Systems as follows.

Reviewing the ELM System List

- Select **Options** from the main menu strip.
- Select **Configuration**.
- Click the index tab **Network** on the display.

  You will get to the following window:



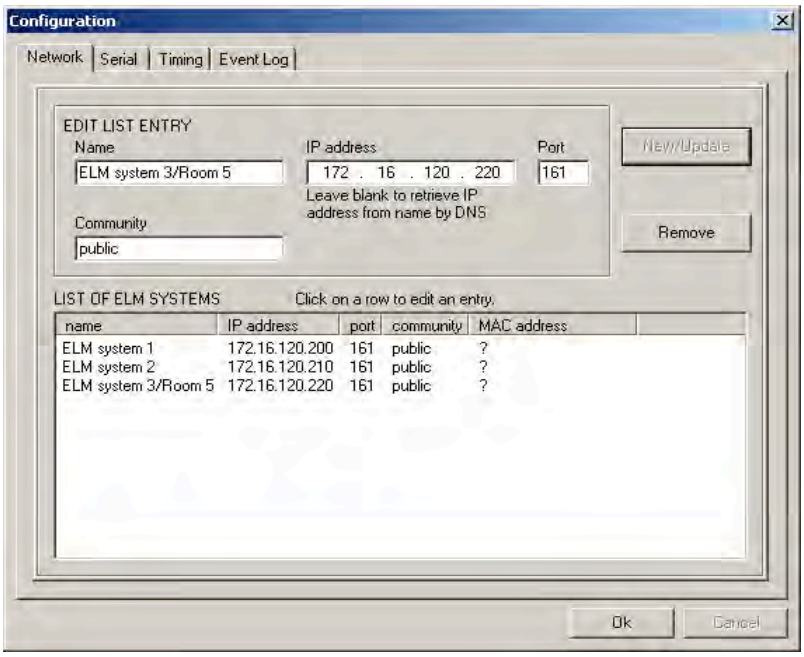
- For each system, add an entry to the list as follows:

New entry:

  - Enter a name for the system in the field **Name**. This is the name that will be displayed on the user interface.
  - Enter the IP address of the Communications Module of the system in the field **IP address**. If the name is a domain name that can be translated by Domain Name Service (DNS), leave the IP address field blank.

- Enter the **Port** which is used by the Communications Module. Default is 161.
- Click the **Update** button. The entry appears in the table **LIST OF ELM SYSTEMS** and in the drop down list in the **DATA CONNECTION** area of the user interface**.**

For example, the following illustration shows a list with three systems to manage. Please be aware that the MAC address is automatically added by *ELMcontrol* as soon as a data connection has been set up.



<u>To edit an entry:</u>

- Click on the row in the table that you want to edit.
- Make changes in the **EDIT LIST ENTRY** fields.
- Click the **Update** button.

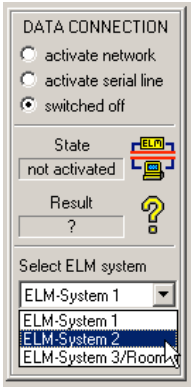
<u>To remove an entry:</u>

- Click on the row in the table that you want to remove.
- Click the **Remove** button.

After all systems have been entered click the **Ok** button to close the window **Configuration**.

7.2.3.3. Switching Between ELM Systems

- Go to the user interface, to the area **DATA CONNECTION** and click on the arrow beside the field **Select ELM system** and select the system from the list in the display that you want to access. Each system name represents a different Communications Module and associated ELS modules.

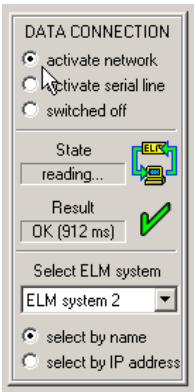


Select the IP address (**select by IP address** button) or by means of the name of system (**select by name** button).

You can easily switch over from one system on the list to another. All data exchanged over the LAN is related to the selected system. If there is only one system on the list it is automatically selected.

7.2.3.4. Activating the Network Connection

- To start a scan of the selected system go to the area **DATA CONNECTION** on the user interface and click the button **activate network**.



The **State** field in the **DATA CONNECTION** area shows the current scan process. The **Result** field indicates whether the last scan cycle was free of error and how much time the cycle took.

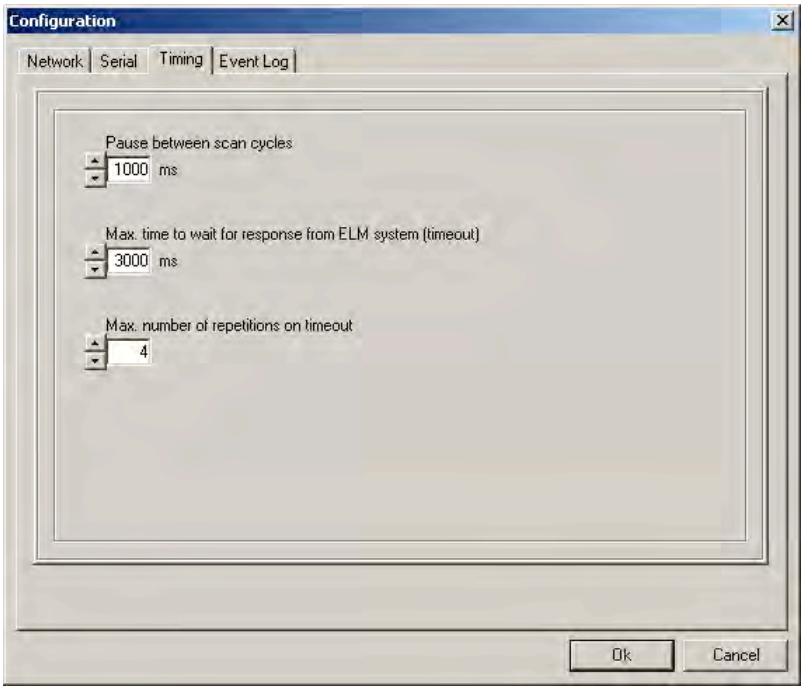
- Login to the system (see section 7.3. Permissions).

7.2.4. Setting Up Timing Conditions

Once a data connection is made, the data from the system is read in cycles.

To set or edit Timing Conditions:

- Select the menu **Options** from the main menu strip.
- Select **Configuration** from the menu strip.
- Click the index tab **Timing** in the display



- Set the variables as follows:
  - **Scan between scan cycles** – defines the length of time between each scan cycle. The scan pause influences the data update rate and the load of data connections. The scan pause is preset at 1000 ms (1 s). It can be set between 50 ms and 9950 ms.
  - **Maximum time to wait for response from ELM system (timeout)** – defines the length of time the software will wait for a response from the Communications Module. The timeout is preset at 3000 ms (3 s). It can be set between 50 ms and 9950 ms.
  - **Maximum number of repetitions on timeout** – if the Communications Module does not respond by the timeout, the request will be repeated this number of times. A warning message is recorded in the event log with each request. When the maximum number is reached, the request is

ended and an error message is recorded in the event log. The preset number is 4. It can be set between 0 and 99.

- With a click on the **Ok** button the changed values are taken over and the window **Configuration** is closed.

7.3. Permissions (Login Levels)

A user's **login level** determines the type and amount of data exchanged between *ELMcontrol* (as well as other PC applications) and the ELS.

The current login level is shown in the area **LOGIN LEVEL** on the left side of the screen.

There are eleven login levels numbered from 0 - 10. The degree of permission increases with a higher login level number. Level 0 (standard setting) stands for basic system-identification. Reading data requires level 1. Writing data requires level 2. Unrestricted access requires level 10 – the highest login level.

For the Standard-Firmware-Version of the Communications Module (16147-050), the permissions for reading and changing the access codes or Access Control Numbers (ACN) for the handles/electronic locks change with each login level. Each handle can have five access codes (ACN 1, ACN 2, ACN 3, ACN 4 and ACN 5). Input of an access code number for opening a handle by means of a workstation login is possible with login level 1 or higher (see section 7.5. Configuring Handles and section 7.6. Open Handles). Permissions for reading and changing access codes (ACN) for other login levels are defined in the table on the next page.

The individual login levels are provided the following permissions:

Login Level		**Permissions**	
No.	**This level applies under following conditions:**	***Scan data from ELM system***	***Write data to ELM system***
0	Pre-settings, workstation unknown or login with unknown password	No data readable - with exception of the system identification	No data writable
1	Login with login password for level 1	Data completely readable - with exception of the access codes for handles and the user passwords	As level 0
2	Login with login password for level 2	As level 1	Data completely writable - with exception of the access codes for handles and the user passwords
3	Login with login password for level 3	As level 2	As level 2
4	Login with login password for level 4	Data completely readable - with exception of access codes ACN 2, ACN 3, ACN 4, ACN 5 for handles and the user passwords	Data completely writable - with exception of access codes ACN 2, ACN 3, ACN 4, ACN 5 for handles and the user passwords
5	Login with login password for level 5	Data completely readable - with exception of access codes ACN 3, ACN 4, ACN 5 for handles and the user passwords	Data completely writable - with exception of access codes ACN 3, ACN 4, ACN 5 for handles and the user passwords
6	Login with login password for level 6	Data completely readable - with exception of access codes ACN 4, ACN 5 for handles and the user passwords	Data completely writable - with exception of access codes ACN 4, ACN 5 for handles and the user passwords
7	Login with login password for level 7	Data completely readable - with exception of access code ACN 5 for handles and the user passwords	Data completely writable - with exception of access code ACN 5 for handles and the user passwords
8	Login with login password for level 8	Data completely readable - with exception of the user passwords	Data completely writable - with exception of the user passwords
9	Login with login password for level 9	Data completely readable - with exception of the user passwords	Data completely writable - with exception of the user passwords
10	Login with login password for level 10	No limitations	No limitations

7.3.1. Login Methods

There are four login methods for the system: login as workstation, login as user and login as administrator.

7.3.1.1. Login as User

On the Login Passwords tab you can manage a list of up to 100 user accounts. Each user account has a name, a password and login level. Management of the user list is possible via a serial or network connection. Details are covered in section 7.3.2.2. 7.2.3.2. User Management. Reading the user passwords and writing to the list requires login level 10.

A user login requires a matching name and password.

The **name of the user** will be included in event log entries for actions triggered by the user (e.g. opening of a door).

A login level assigned to a user is typically assigned to a single application program. Different application instances running on the same workstation may have different user logins and therefore may run with different login levels. The authorization is made by means of the SNMP community string of SNMP data requests.

7.3.1.2. Login as Administrator

By applying the administrator password the login level 10 is assigned. The administrator password is set using a serial connection. See section 7.2.3.1. 7.2.3.1. Network Setup of the System IP Properties for details.

Note, that a "login as workstation" is not possible if the SNMP community is different from the administrator password.

7.3.1.3. Login as Backup Operator

The backup operator is able to perform system backup and restore operations only. See section 7.4.4 Configuration Data Files.

A user named "BckpAdm" must be defined and login level 10 must be assigned to this user. See section 7.3.2.2. 7.2.3.2. User Management for details of how to define a user login.

7.3.1.4. Login as Workstation

On the Login Passwords tab there is a chart at the right side of the screen with 10 passwords called the **workstation login passwords**. Each workstation password is linked to a different login level. Assign workstation passwords using a serial data connection as explained in section 7.3.2.1. Workstation login passwords.

The workstations that are allowed to logon to the system are listed on the IP Properties tab in a table at the left side of the screen named **permissible workstations** as explained in section 7.2.3.1. 7.2.3.1. Network Setup of the System IP Properties.

When a workstation login is used, the login level is the level defined by the workstation password from the Workstation Login Passwords table on the Login Passwords tab. Login is allowed if the password matches and if the workstation is listed in the Permissible Workstations table on the IP Properties tab. If the workstation is not listed in the Permissible Workstations table and the workstation password is valid, it will be listed in the table if there is a dynamic address position available. Note that the workstation IP login level can be changed with a serial connection at the IP Properties tab.The login operation is covered in section 7.3.3. Login to the System.

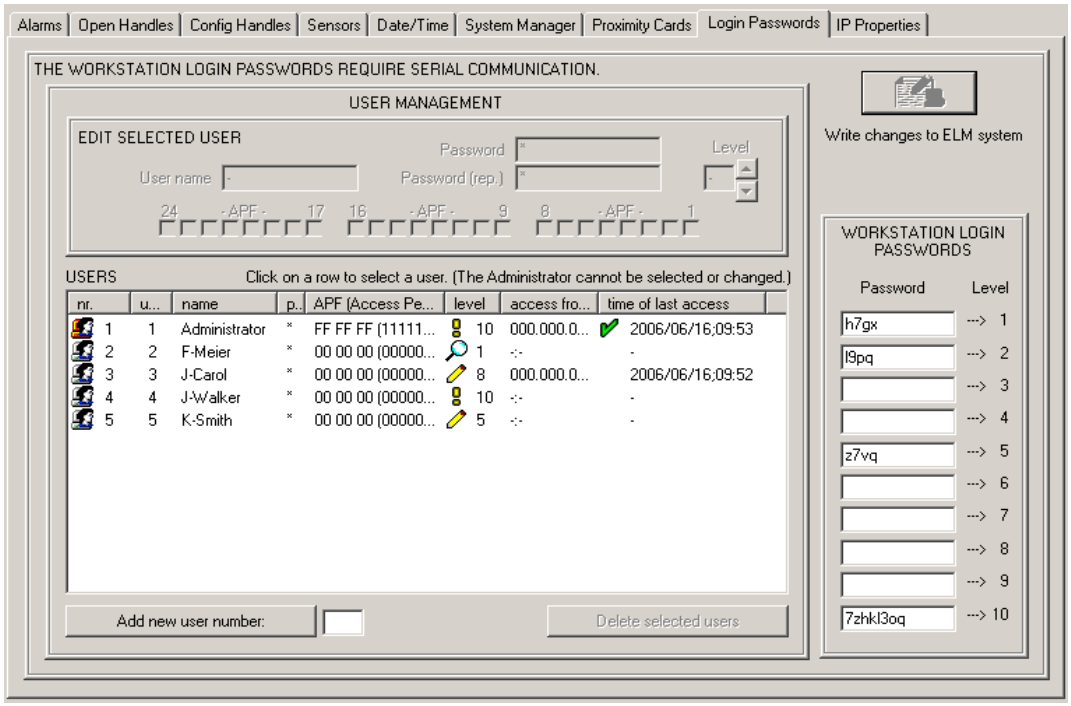
When using a workstation login, the **IP address of the workstation** will be included in event log entries for actions triggered from that workstation (e.g. opening of a door).

A login level assigned to a workstation applies to all application programs running on that workstation because the authorization criterion is the source IP address of SNMP data requests.

7.3.2. Login Passwords

Users and passwords are entered on the index card **Login Passwords**. The only exception is the administrator password, which has to be specified on the index card **IP Properties** (see section 7.2.3.1. 7.2.3.1. Network Setup of the System IP Properties.

- Click the index tab **Login Passwords**.


Alarms
Open Handles
Config Handles
Sensors
Date/Time
System Manager
Proximity Cards
Login Passwords
IP Properties
THE WORKSTATION LOGIN PASSWORDS REQUIRE SERIAL COMMUNICATION.
USER MANAGEMENT
EDIT SELECTED USER
User name
Password
Password (rep.)
Level
24 - APF - 17 16 - APF - 9 8 - APF - 1
USERS
Click on a row to select a user. (The Administrator cannot be selected or changed.)
nr. u... name p.. APF (Access Pe... level access fro... time of last access
1 1 Administrator * FF FF FF (11111... 10 000.000.0... 2006/06/16;09:53
2 2 F-Meier * 00 00 00 (00000... 1 -:- -
3 3 J-Carol * 00 00 00 (00000... 8 000.000.0... 2006/06/16;09:52
4 4 J-Walker * 00 00 00 (00000... 10 -:- -
5 5 K-Smith * 00 00 00 (00000... 5 -:- -
Add new user number:
Delete selected users
Write changes to ELM system
WORKSTATION LOGIN PASSWORDS
Password
Level
h7gx ---> 1
l9pq ---> 2
---> 3
---> 4
z7vq ---> 5
---> 6
---> 7
---> 8
---> 9
7zhkl3oq ---> 10

7.3.2.1. Workstation Login Passwords

Workstation login passwords are entered in the area **Workstation Login Passwords** on the right side of the Login Passwords tab using a serial connection. Enter a password into the corresponding input field for each level that requires a workstation login. The password may include letters and numbers and must have a minimum of four and a maximum of eight characters.

A serial connection is required.

All changes become effective only after clicking the button **Write changes to ELM system** button. If this is not done changes will be lost.

7.2.3.2. User Management

User accounts are entered in the area **User Management** on the Login Passwords tab. The administrator is listed here also. The administrator entry cannot be changed or deleted.

The table **Users** shows all registered users of the system. You can sort the list according to each of the represented columns by clicking on the respective top of the column. Click again on the same place and the order is reversed.

The table contains the following information:

Number
A consecutive number makes navigation within the table easier.

User ID-Number
The number of the table row which stores the data of the user is displayed for information.

Name
This is the name of the user. Names have to be unique. The name is used for login and will be included in certain event log entries.

Password
This is the individual password for login.

APF (Access Permission Flags)
These 24 flags form a method of authorization for opening a handle or latch. Each of the 24 flags can independently be set or deleted. Each handle or latch (see section 7.5. Configuring Handles and Latches) also has 24 flags called the **ARF** (Access Requirement Flags).
The opening of a handle is permitted when a user APF matches a handle ARF.
With the help of the ARF/APF you can form groups from handles and users with different opening permissions which can be subdivided hierarchically.

Level
The login level which the user can attain at the login procedure. Different supplementary symbols show a rough survey of the kind of the permission which is assigned to the login level.

Access from IP socket
The address and the port number of the workstation from which the user accessed the system last is displayed here.

Time of last access
The last access time of the user is shown. If the time is less than a minute, the symbol ✔ is displayed to show which users are currently operating.

Adding users

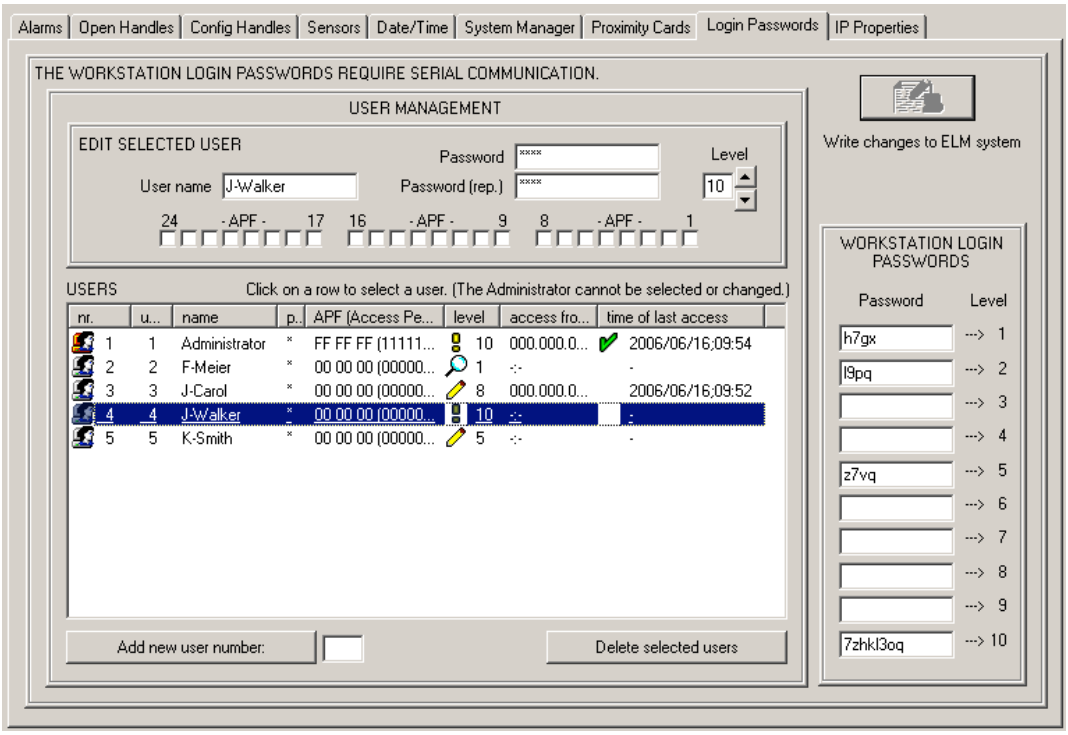
- Click the button **Create new user.**

A new user entry is added to the list. As name the standard name "user" appended by an ongoing number, is applied.

Then change the settings of the new user entry according to your needs, as follows.

Change settings

- To change the settings for a user first select the entry that shall be modified by a click with the left mouse button on the corresponding row in the table.



In the area **EDIT SELECTED USER** the parameters of the user entry can be changed.

- The sum of the name and password must not exceed 15 characters in length.
- Adjust the desired login level. You can disable a user account without deleting it from the list by putting the level on 0 (this is the presetting when adding a new user entry.)
- Mark all the flags of the APF which you want to set.
- After the chosen changes have been made click on the button **Write changes to ELM system**.

The table is updated after the next reading cycle (scan).

If the button **Write changes to ELM system** is not clicked any changes made are dismissed as soon as you select another user entry or if you leave the index card **Login Passwords**.

Deleting users

- First select the desired user entry by clicking with the left mouse key on the desired entry in the table. With the control key (Ctrl) or the shift key pressed at the same time you can select several entries or areas.
- Click the button **Delete selected users.**

If you add a new user number equal to an existing user number, the older entry will be deleted.

7.3.3. Login to the System

You must have a valid workstation or user password to login to the system.

- Click on the **change** button in the area **LOGIN LEVEL** on the user interface.

The following input-window is shown:

Choose the desired login method (see section 7.3.1. Login Methods). Enter a valid password. A user login requires the user name and password. Click on the **Ok** button. The corresponding login level is shown in the **LOGIN LEVEL** area of the user interface.

The new login level reverts to **0** if the password is not accepted.

7.4. System Configuration With the System Manager

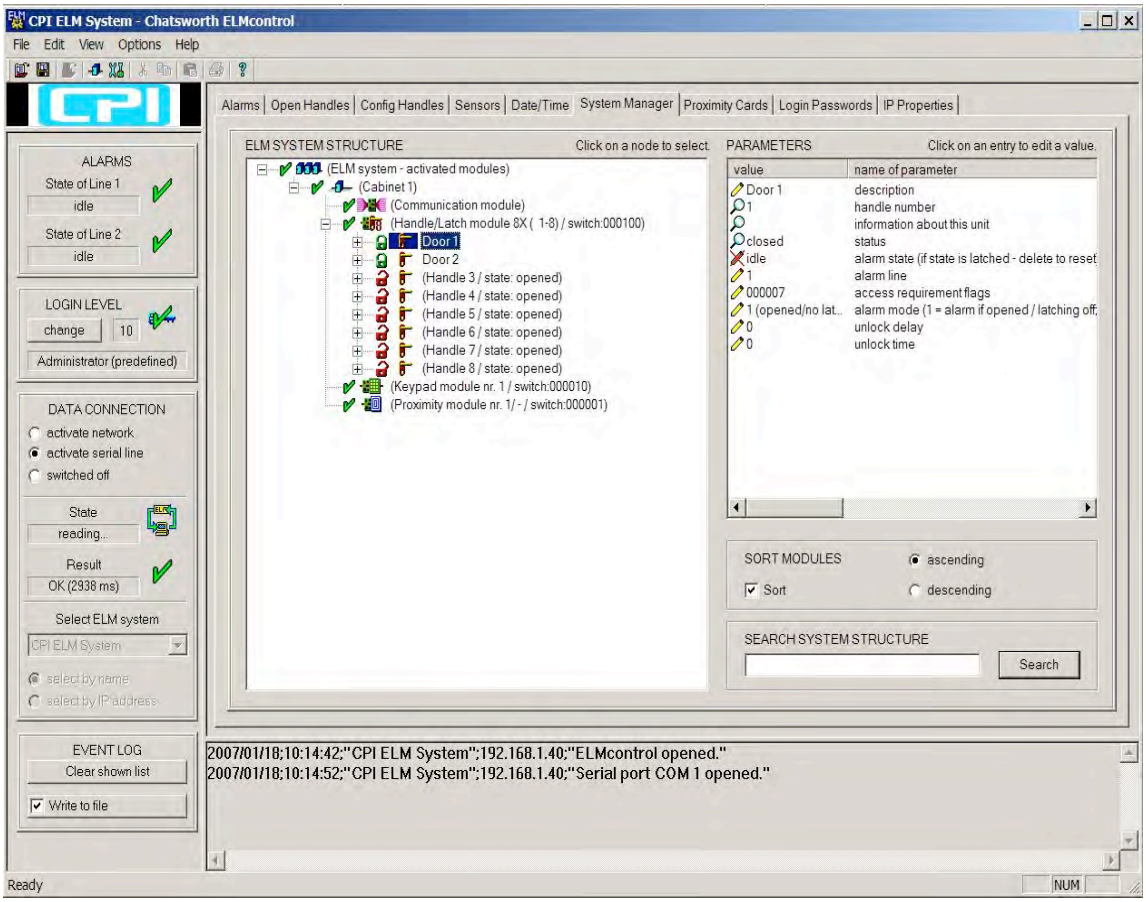
The index card **System Manager** allows the entire configuration of the system. The System Manager can only be used with a high login level.

The system is presented from the point of view of a physical structure. All modules are shown with their components (e.g. Handles). For a better survey modules can be grouped with "cabinets".

On initial startup of a system it is necessary to register all modules (except the Communication Module) in the System Manager. The following section (7.4.1 Presentation of the System-Structure*)* explains the presentation of a configured system within the System Manager. The following section (7.4.2 Configuration of the System-Structure*)* gives examples of the individual steps necessary for registering and activating ELS modules.

7.4.1. Presentation of the System Structure

All cabinets and modules of the system together with the corresponding peripheral components are shown in the **ELM SYSTEM STRUCTURE** area of the index card System Manager in a hierarchic structure (tree-structure).



The nodes of the tree which are subdivided into sub-nodes have the symbols „**+**" or „**-** ", respectively. A mouse-click on this symbol shows or hides the sub-nodes.

The nodes of the tree-structure have different parameters. A node can be selected by mouse-click. The parameters of the selected node are shown in the area **PARAMETERS.**

- Parameters which are marked by the symbol  can be changed. You can change the value of these parameters by clicking on the value in the display. You will then see an input-field to which another value can be entered. For completion press **ENTER** or mouse-click beside the input field. The new value is then automatically transferred to the ELM system.

- Parameters which are marked by the symbol  are currently blocked for an input. Other parameters must be set before changing these parameters.

- Parameters with the symbol  are only shown, they cannot be changed. The symbol refers to missing authority for the display of the value.

The first parameter of a node is the **Description.** *ELMcontrol* automatically generates a description for every node which gives information about the relevant values and the most important parameters. This automatically generated description is placed in parenthesis; it can be replaced by your own text. If all characters of the description are removed *ELMcontrol* will enter the system-generated description.

The description can also be seen at the tree-structure on the right hand side beside the node-type symbol. On the left hand side beside the node-type symbol you will find a symbol that informs of the status of the node.

The tables below explain the meaning of the symbols for node-types and status in the tree-structure:

Node-type-symbol	***Meaning of the node***	***Parameter within the automatically generated description***	***Status symbols and meaning***	
	All cabinets of the system, root node of the whole structure	-		Cabinets and modules are activated and they are running trouble-free.
				At least one activated module within one cabinet is defective.
				At least one activated module within the whole system reports active alarm.
				At least one activated module within the whole system reports latched alarm
				The status of at least one module within the whole system is unknown.
				At least one module of the system is ready for activation.
				At least one module of the system needs further configuration in order to be ready for activation.
				At least one module of the system has been disabled due to an addressing conflict with another module of the same type.

Node-type-symbol	***Meaning of the node***	***Parameter within the automatically generated description***	**Status symbols and meaning**	
	Cabinet	Number of cabinet		Modules of this cabinet are activated and they are running trouble-free.
				At least one activated module within this cabinet is defective.
				At least one activated module within this cabinet reports active alarm.
				At least one activated module within this cabinet reports latched alarm
				The status of at least one module within the whole system is unknown.
				The cabinet contains at least one module ready for activation.
				At least one module of the cabinet needs further configuration in order to be ready for activation.
				At least one module of the cabinet has been disabled due to an addressing conflict with another module of the same type.

Node-type-symbol	***Meaning of the node***	***Parameter within the automatically generated description***	***Status symbols and meaning***	
	Communications Module (P/N 16147-050)	-		The module is running trouble-free.
				The module is defective.
				At least one of the two alarm lines reports active alarm.
				At least one of the two alarm lines reports latched alarm.
				The status of the module is unknown.
				There is no valid firmware running on the module.

Node-type-symbol	***Meaning of the node***	***Parameter within the automatically generated description***	**Status symbols and meaning**	
	Electronic Lock Control Module for 8 swing handles (P/N 16147-052)	Area of handle numbers, position of the six CAN-address switches		The module is running trouble-free.
				The module is defective.
				At least one handle or latch of this module reports active alarm.
				At least one handle or latch of this module reports latched alarm.
				The status of the module is unknown, or the module was not completely configured.
				The module is not activated, but it is ready for activation.
				The module needs further configuration in order to be ready for activation.
				The module has been disabled due to an addressing conflict with another module of the same type.
				The module is currently in detection mode.

Node-type-symbol	***Meaning of the node***	***Parameter within the automatically generated description***	***Status symbols and meaning***	
	Keypad Module (P/N 16147-008)	Number of the keypad station (component number), position of the six CAN-address switches		The module is running trouble-free.
				The module is defective.
				The status of the module is unknown, or the module was not completely configured.
				The module is not activated, but it is ready for activation.
				The module needs further configuration in order to be ready for activation.
				The module has been disabled due to an addressing conflict with another module of the same type.
				The module is currently in detection mode.

Node-type-symbol	***Meaning of the node***	***Parameter within the automatically generated description***	***Status symbols and meaning***	
	Proximity Card Reader Module (P/N 16147-054)	Number of the reading station (component number), ID-number of the card at the reading station, position of the six CAN- address switches		The module is running trouble-free.
				The module is defective.
				The status of the module is unknown, or the module was not completely configured.
				The module is not activated, but it is ready for activation.
				The module needs further configuration in order to be ready for activation.
				The module has been disabled due to an addressing conflict with another module of the same type.
				The module is currently in detection mode.

Node-type-symbol	***Meaning of the node***	***Parameter within the automatically generated description***	***Status symbols and meaning***	
	Swing Handle with electronic lock Made with: Electronic Lock Upgrade Kit (P/N, 16147-060, 16147-061, 16147-062, or 16147-063)	Handle/latch number, present status: open/closed		The handle/latch is open.
				The handle/latch is closed.
				The handle/latch reports an active alarm.
				The handle/latch reports a latched alarm.
				Number and status of the handle are unknown. (The handle module was not completely configured.)

Node-type-symbol	***Meaning of the node***	***Parameter within the automatically generated description***	***Status symbols and meaning***	
	Access Code Number (ACN) for a swing handle	Number of the access code, related swing handle number, digit string of the ACN		The access code was registered and can be used.
				The status of the access code is unknown.
				The access code was not registered.
				The registered digit string of the access code consists of more digits than allowed,

The sequence of the modules within each cabinet corresponds to the sequence of modules listed in the module table. By checking the **Sort** button in the area **SORT MODULES** the sequence can be changed. By means of the buttons **ascending / descending** the sorting order of modules can be reversed. Cabinets are always sorted in ascending order.
A corresponding lexicographical sorting of descriptions of the nodes is carried out.

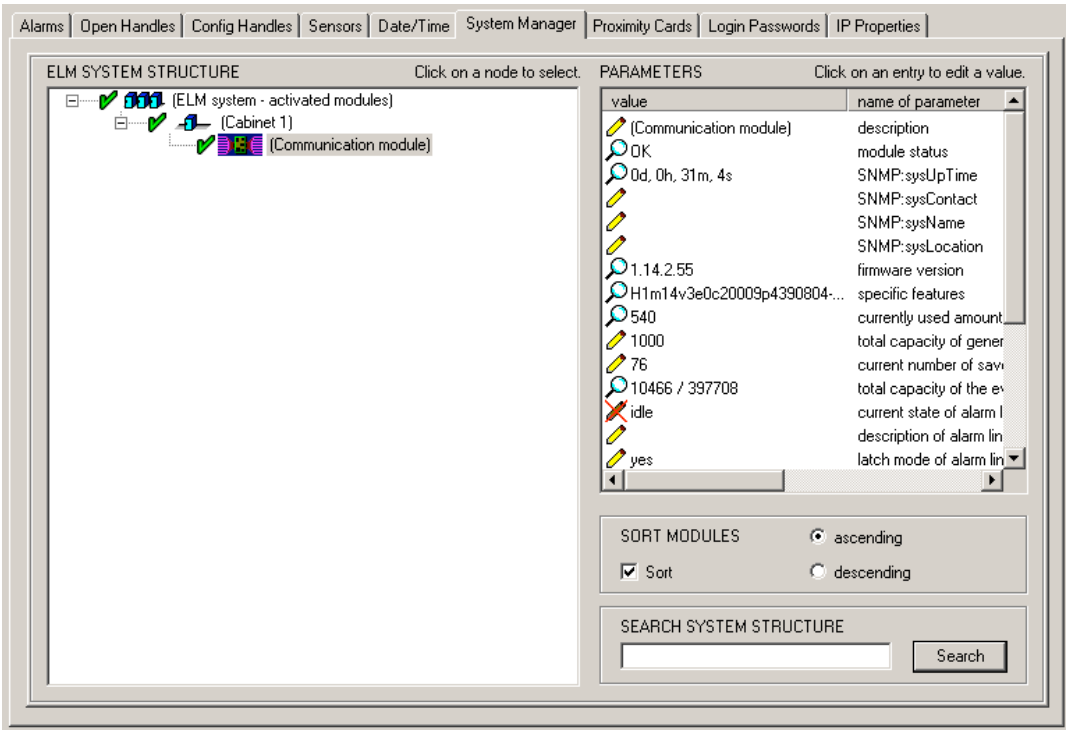
In the area **SEARCH SYSTEM STRUCTURE** you can enter a sequence of characters, activate the button **search** and this entry is searched among all node names. The first node to be found is shown and checked. Repeat the **search** to find further results.

You can change the assignment of a module to a cabinet by using *Drag&Drop* for shifting the module node to another cabinet node. To shift a module node, click and hold the left mouse button on the corresponding module node, drag the node to another cabinet node, and unclick the mouse button.

7.4.2. Configuration of the System Structure

At the first application of an **ELM system** there are no modules included in the system structure of active modules, except for the Communications Module.

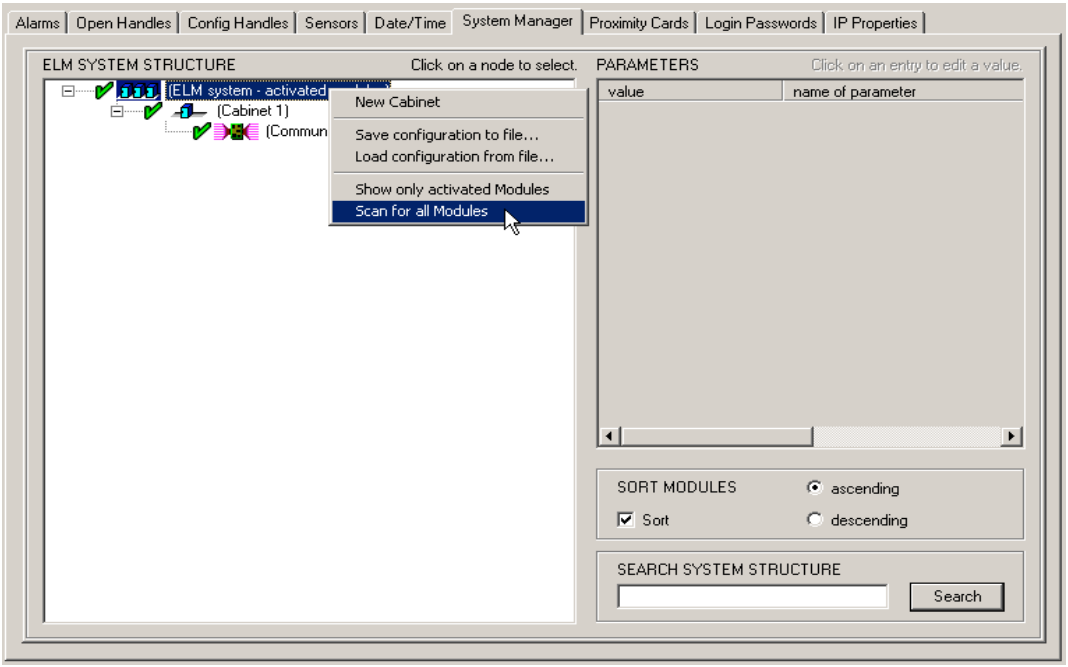
ELMcontrol automatically generates the node **Cabinet 1** as a sub node of the **ELM system** root node, and assigns the Communications Module to this node.



7.4.2.1. Scanning the System for Modules

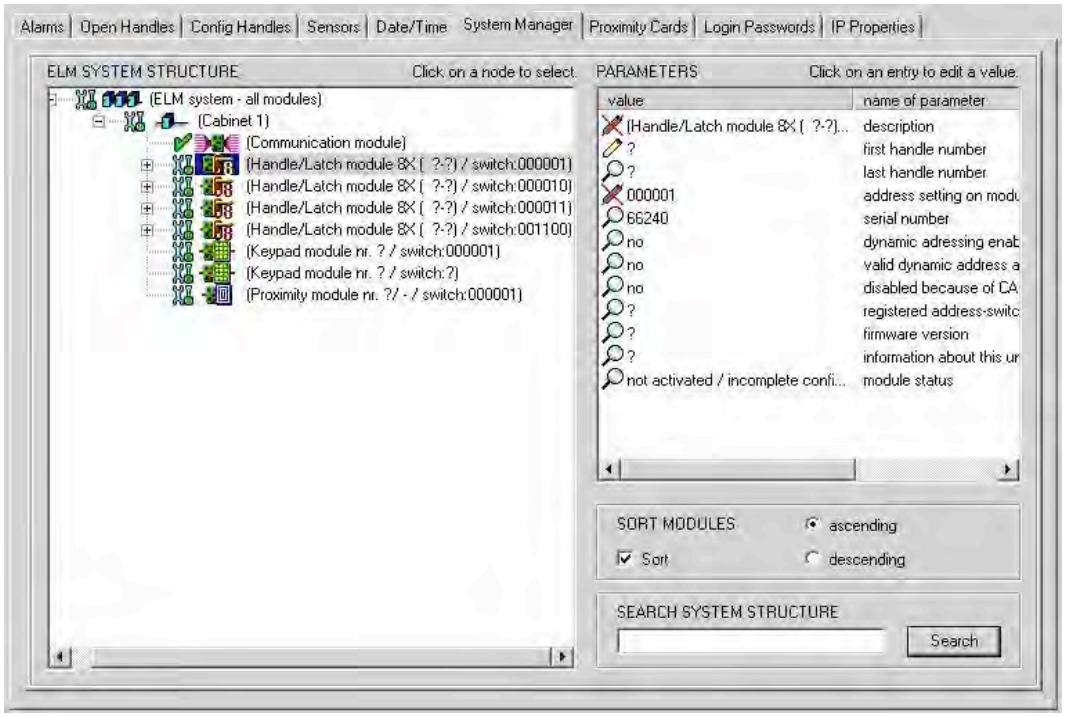
- Click with the right mouse button on the node **ELM system**.

A context menu is opened.



- Choose **Scan for all Modules**

A search process is started. All found modules are displayed. These modules are assigned by default to the cabinet which contains the Communications Module.



At the first application none of the found modules are activated except for the Communications Module.

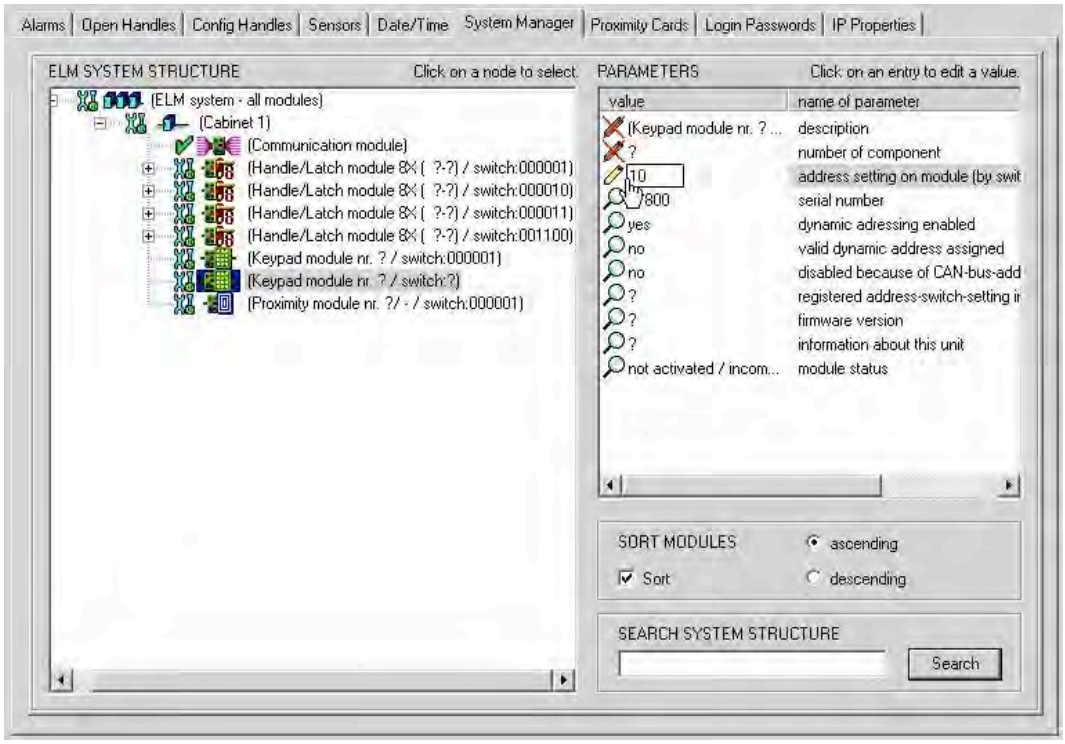
The activation of modules as well as registering further cabinet nodes to the system structure is shown below with examples.

7.4.2.2. Activation of Modules

- After a scan operation, click on a module you want to activate.

Activating Keypad Modules (P/N 16147-008)
In the following example the last of the two Keypad Modules of the list is used. This module is prepared for "dynamic addressing". Before activation an address and a component number must be assigned to the module.

- Click on the **PARAMETER** value **address setting on module**

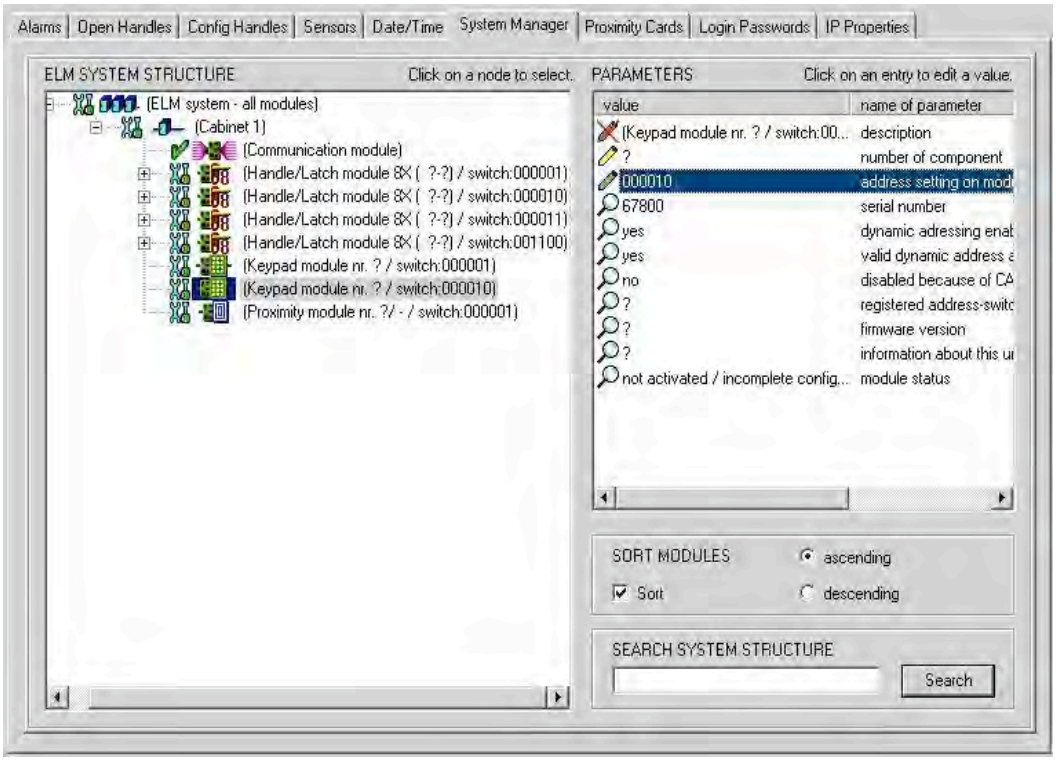


- Enter a binary address for the keypad module into the input field. The value you are putting in must be between **0** and **111111** (leading zeros can be left out). This corresponds to a decimal range of 0-63. The address must be different from the addresses of all other Keypad Modules in the system.

- Complete your input with **ENTER** or by mouse click beside the input field.

- Click with the right mouse button on the node **ELM system** and select **Scan for all modules**.

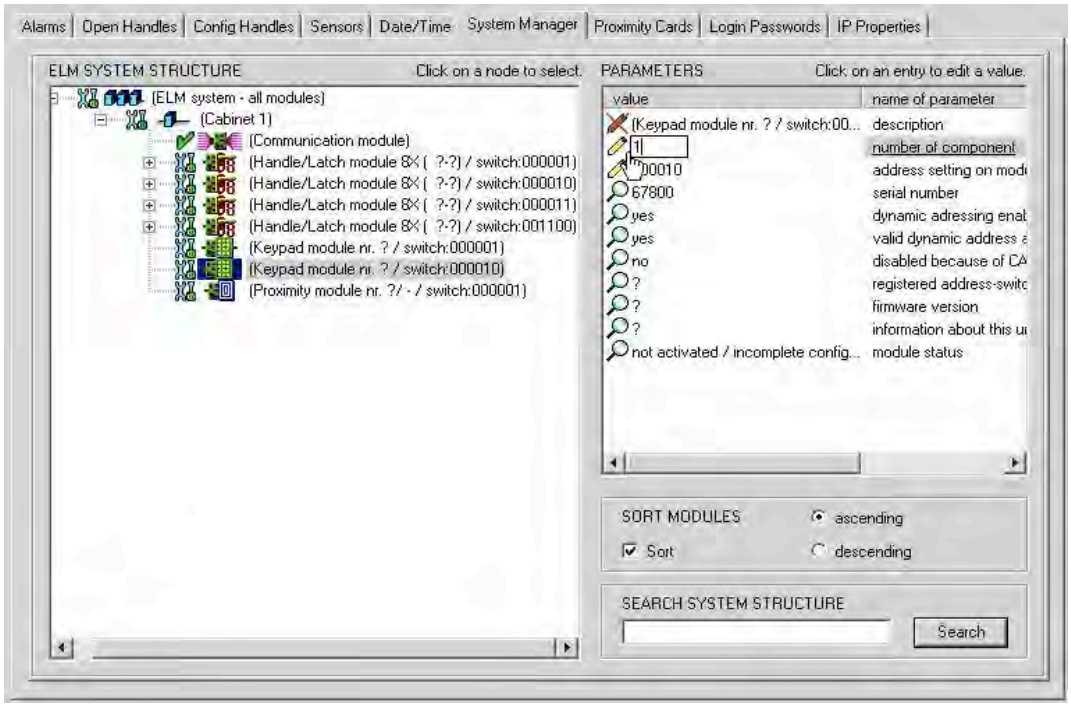
After rescanning, the updated list shows that the selected module now has a valid CAN bus address. For the presented example **10** was entered (decimal value 2). This address is stored within the module and will be valid until the value is changed or deleted.



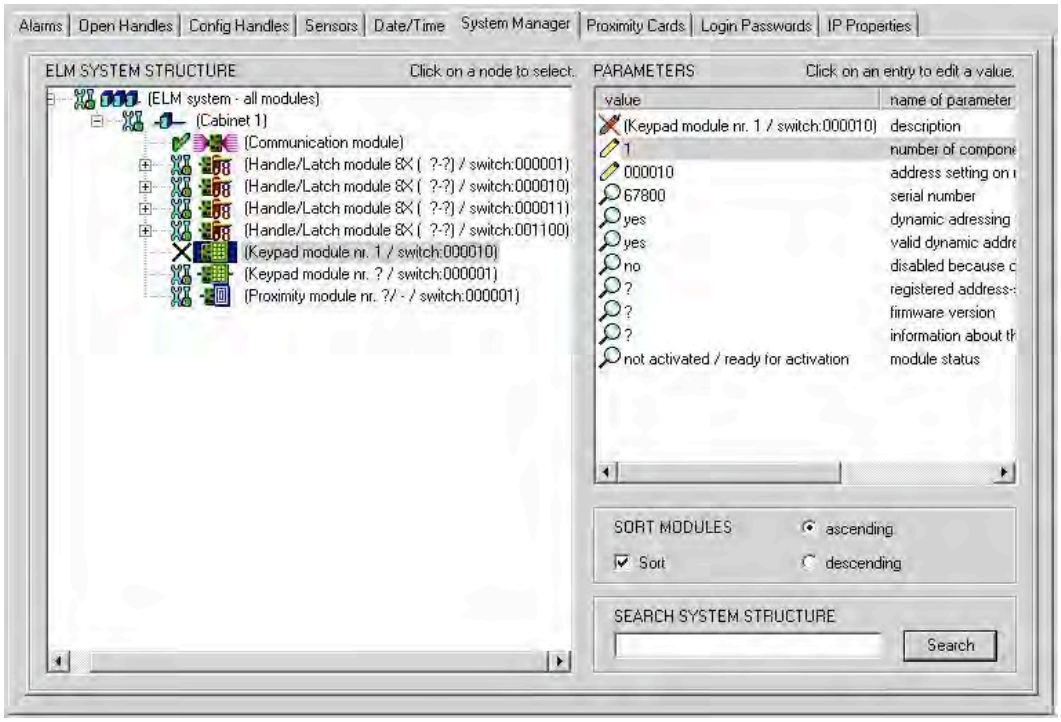
A component number must also be assigned. This component number ranges from 1 to 64. It identifies and distinguishes this Keypad Module from other keypads in the system. If a handle is opened using of this keypad, the component number will be stored in the event log.

Click on the **PARAMETER** value **number of component**.

- Enter the number (1 to 64) of the Keypad Module (in our example: **1**).

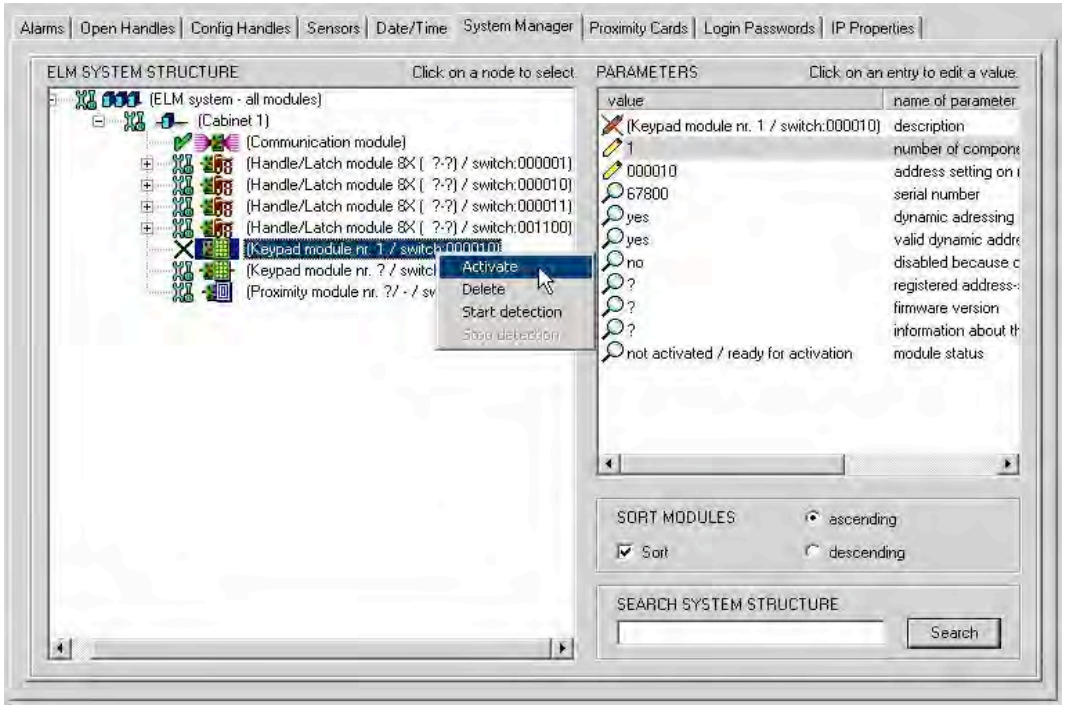


- Complete your input with **ENTER** or by mouse click beside the input field.

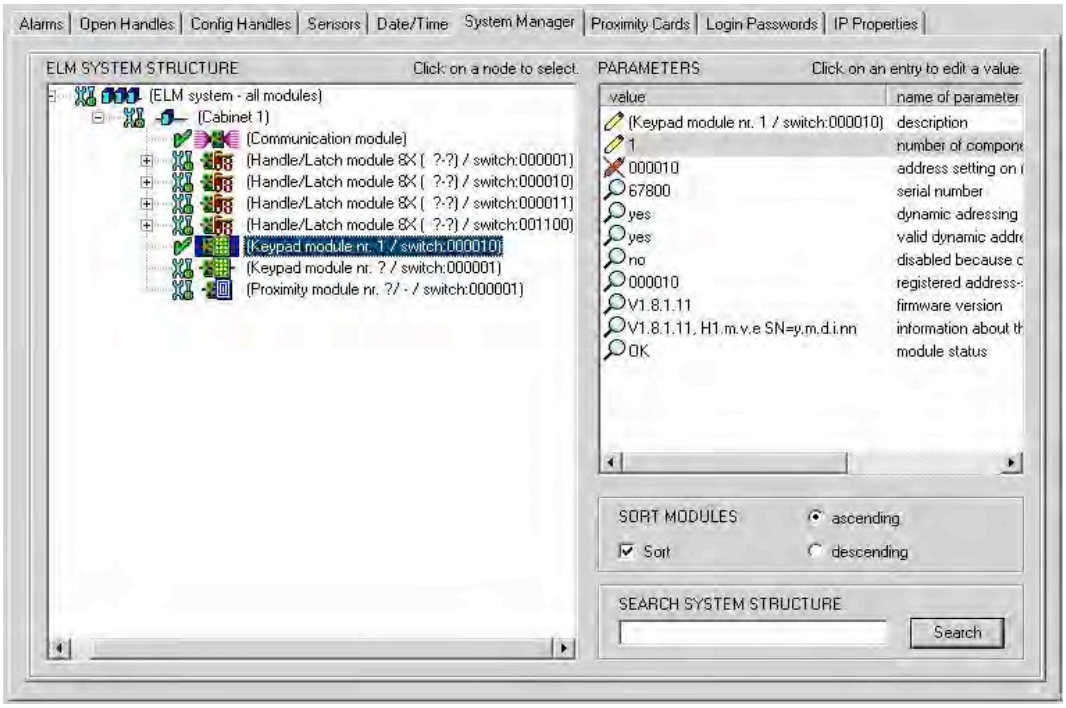


Now all settings necessary for activation have been made and the module status points **ready for activation.**

- Click with the right mouse button on the node of the module and select **Activate** from the context menu.



The module is immediately activated. If the module runs error-free the **PARAMETER** value **Ok** is displayed as **module status** and the status symbol ✔ is shown beside the node.



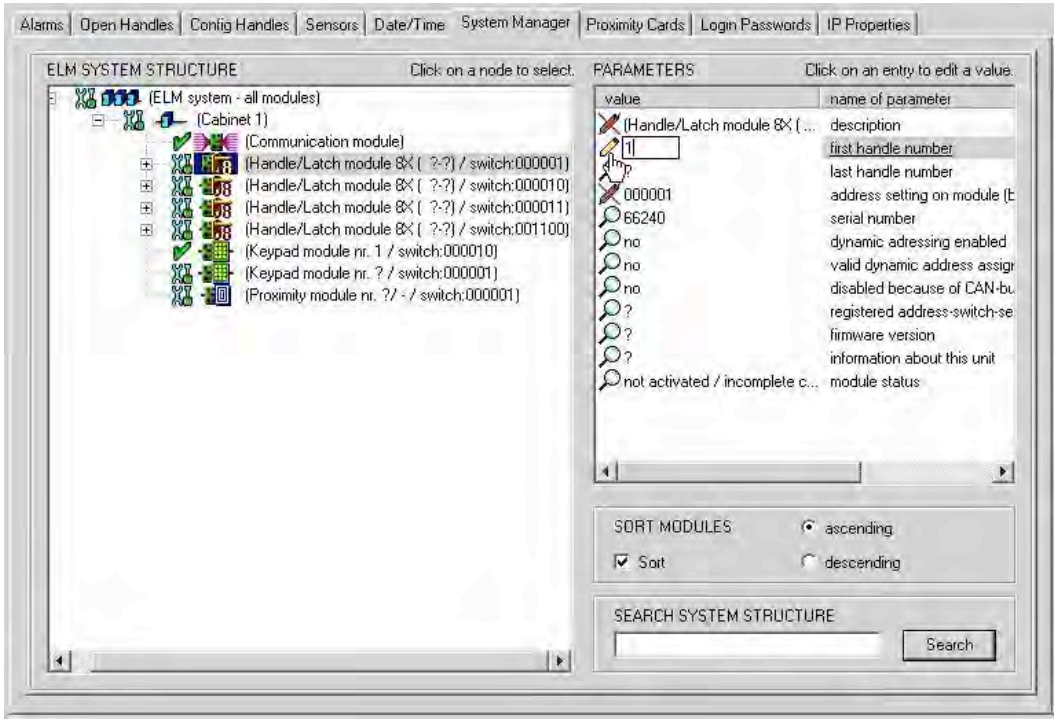
- Repeat this process for all other Keypad Modules in the system giving each module a unique address and number.

<u>Activating Electronic Lock Control Modules (P/N 16147-052)</u>
The activation and configuration of an Electronic Lock Control Module is shown below.

- Click on the handle module you want to activate.

In the following example the first handle module of the list is used. This module is prepared for "static addressing". This means that unlike the keypad in the example above, the address is already fixed by the DIP switches 1-6 on the module. Therefore before the activation just a component number must be assigned to this module. If dynamic addressing was enabled, a binary address between 0 and 111111 (0-63) would be entered instead.

- Click on the **PARAMETERS** value **first handle number.** Put in the number you want to give the first handle that is connected to this module (the example uses: **1**).

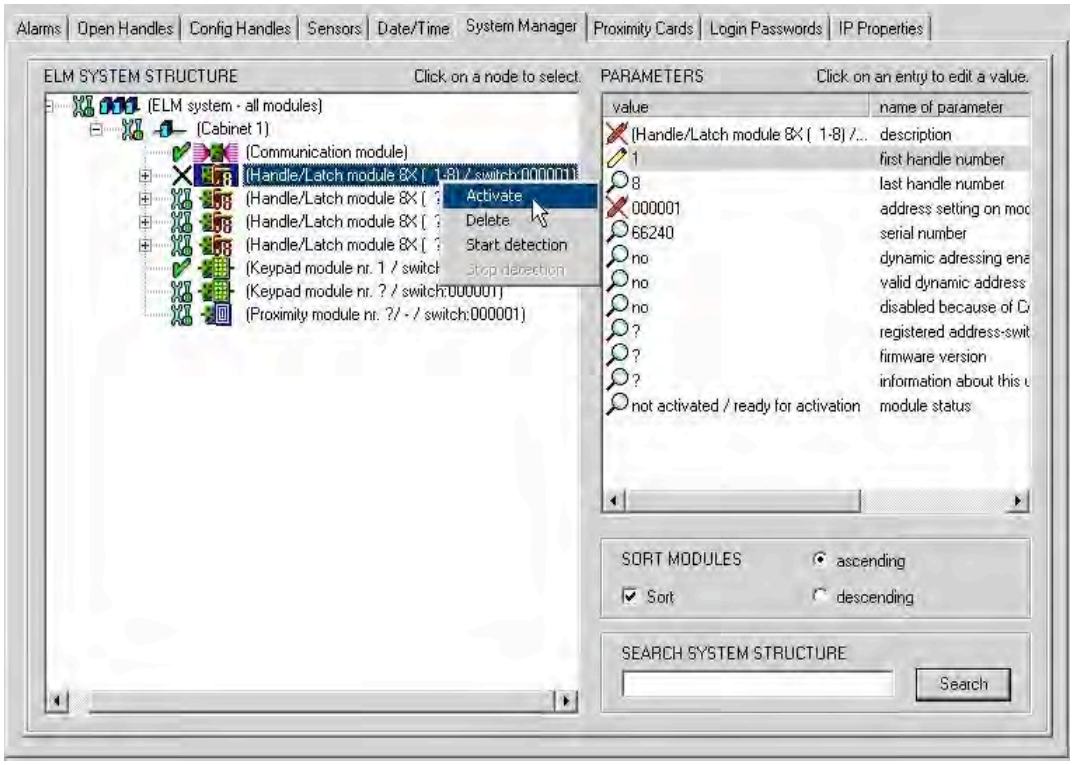


- Complete your input with **ENTER** or by a mouse click beside the input field.

The other handles connected to the module are automatically numbered in ascending order (1-8).

Now all settings necessary for activation have been made and the module status points **ready for activation.**

- Click with the right mouse button on the node of the module and select **Activate** from the context menu.



The module is immediately activated. If the module runs error-free the message **Ok** is displayed as **module status** and the status symbol ✔ is shown beside the node.

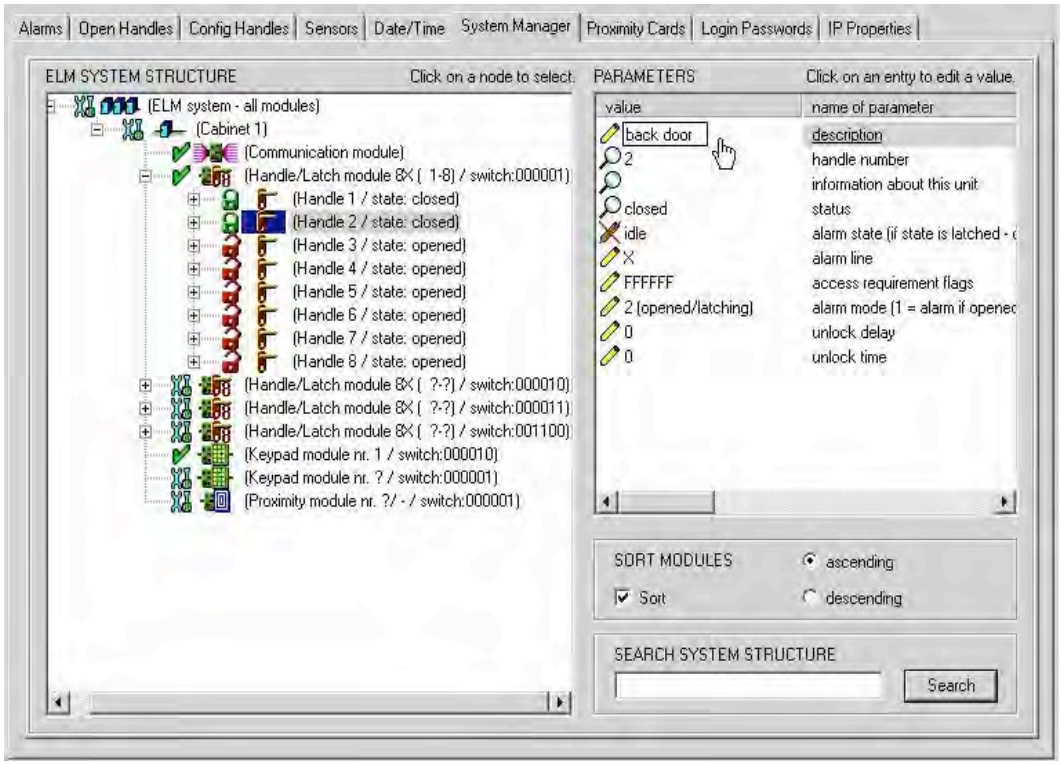
Activating Electronic Lock Upgrade Kits (P/N 16147-060, 16147-061, 16147-062, 16147-063)

In the following example we show how to make changes to the name of a handle and how to enter an access code to the System Manager.

- Click on the **+** symbol beside the handle module node.

All handles connected to this module are displayed as sub nodes.

- Click on the node of the handle to be edited (in our example: **Handle 2**).
- Click on the **PARAMETERS** value **Description.**



- Put in a new description (in our example: **back door**).
- Complete your input with **ENTER** or by a mouse click beside the input field.

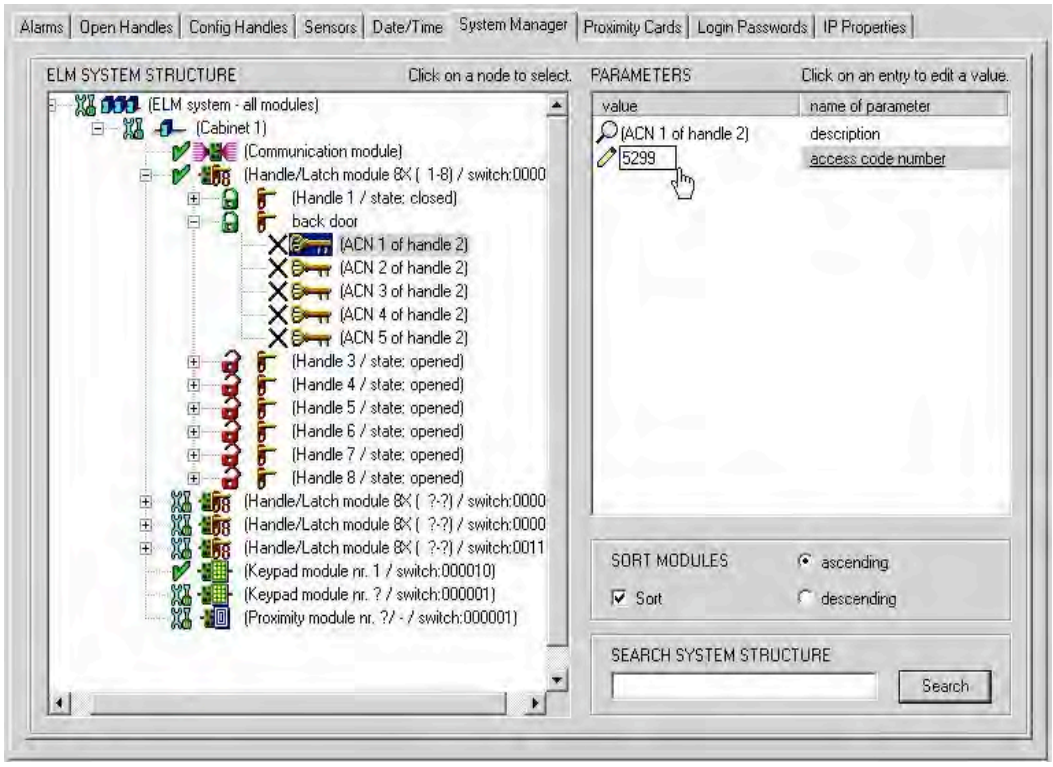
The new description is used for the handle node.

- Click on the **+** symbol beside the node of handle 2.

All five possible access codes numbers (ACN) of the handle are shown as sub nodes of the handle.

- Select an access code number (ACN) and click on the **PARAMETERS** value **access code number**.

- Put in a code number consisting of four to six numbers (in our example: **5299**).



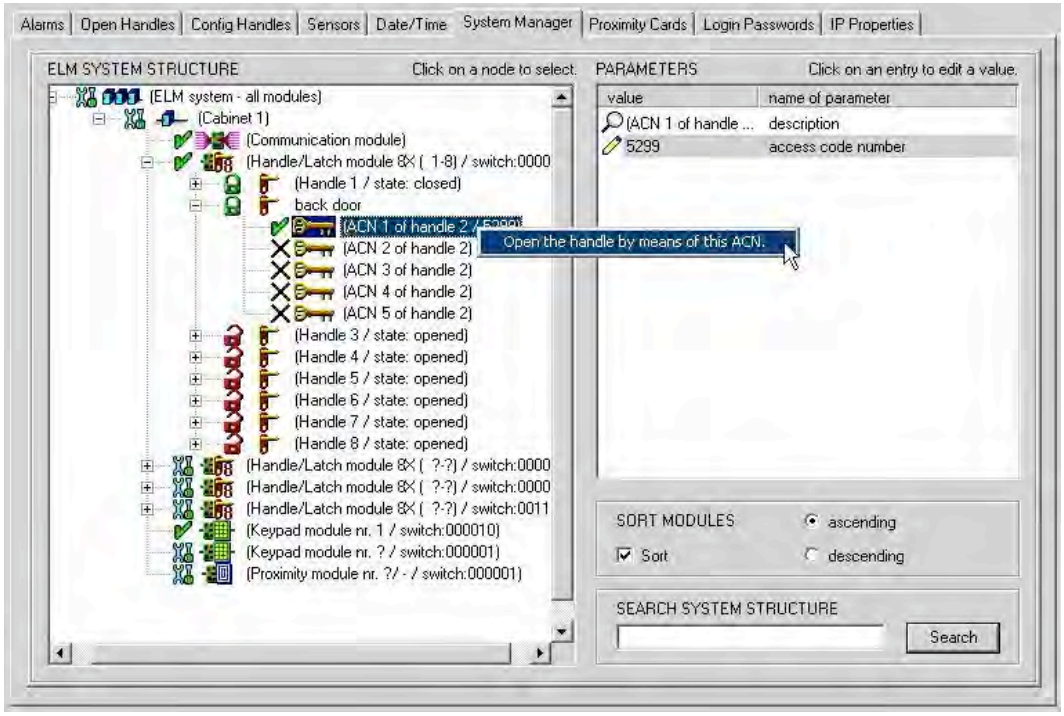
- Complete your input with the button **ENTER** or by a mouse-click beside the input field.

The assigned access code (5299) will open the handle (back door) from a Keypad Module or by entering the code on the tab Open Handles or within the System Manager.

Repeat this step to configure other handles or use the tab Configure Handles. An access code must be assigned to each handle before it will operate.

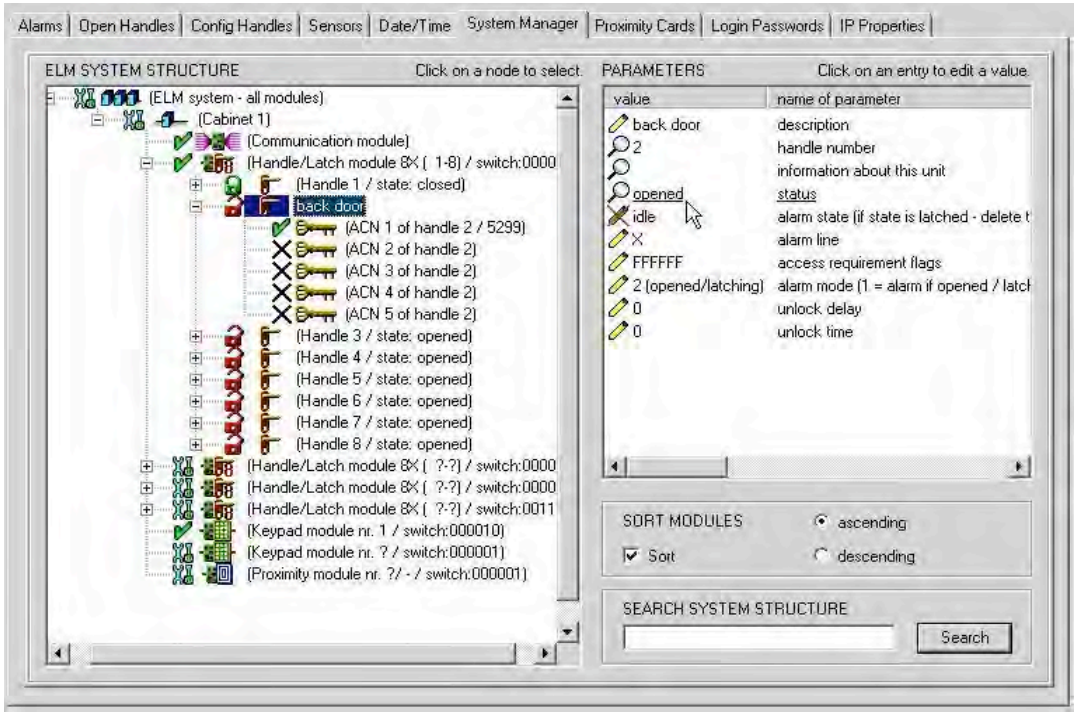
Test the operation of the Electronic Lock Control Module and the handle within the system manager as follows:

- Click with right mouse key on the ACN under the handle.



- Select **Open handle by means of this ACN.**

The handle should open and the report the status of the handle as open.



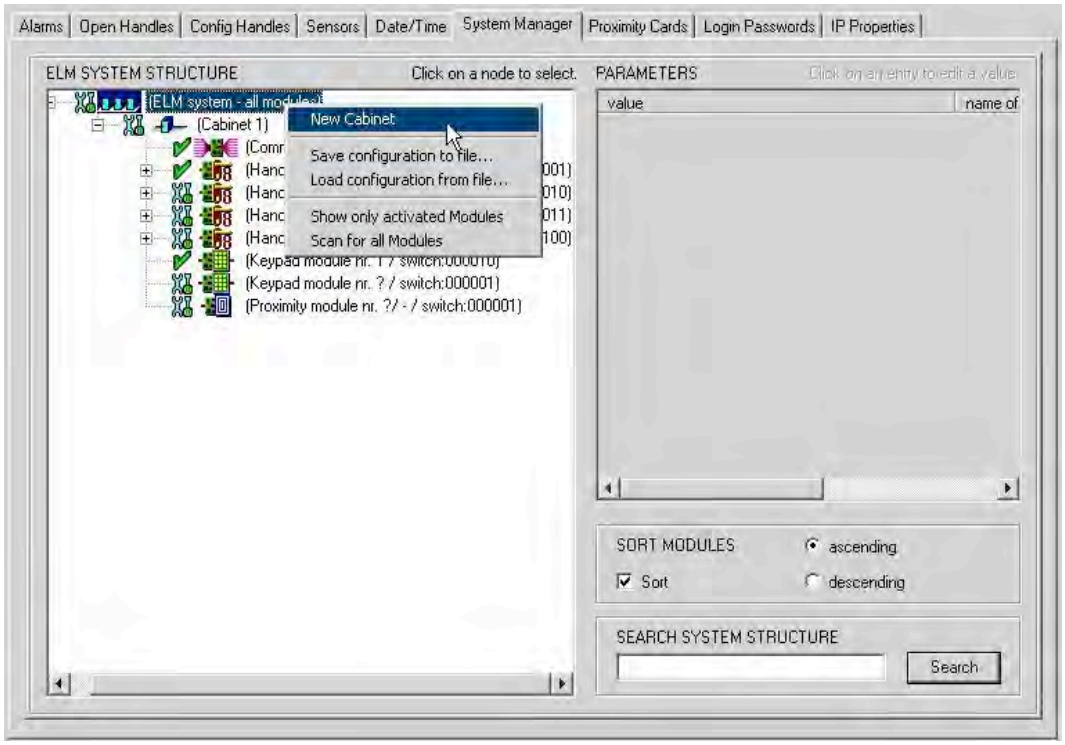
7.4.2.3. Registration of Cabinets

You can add additional "cabinets" in the System Manager tree-stucture to organize nodes according to their physical locations in the network as follows.

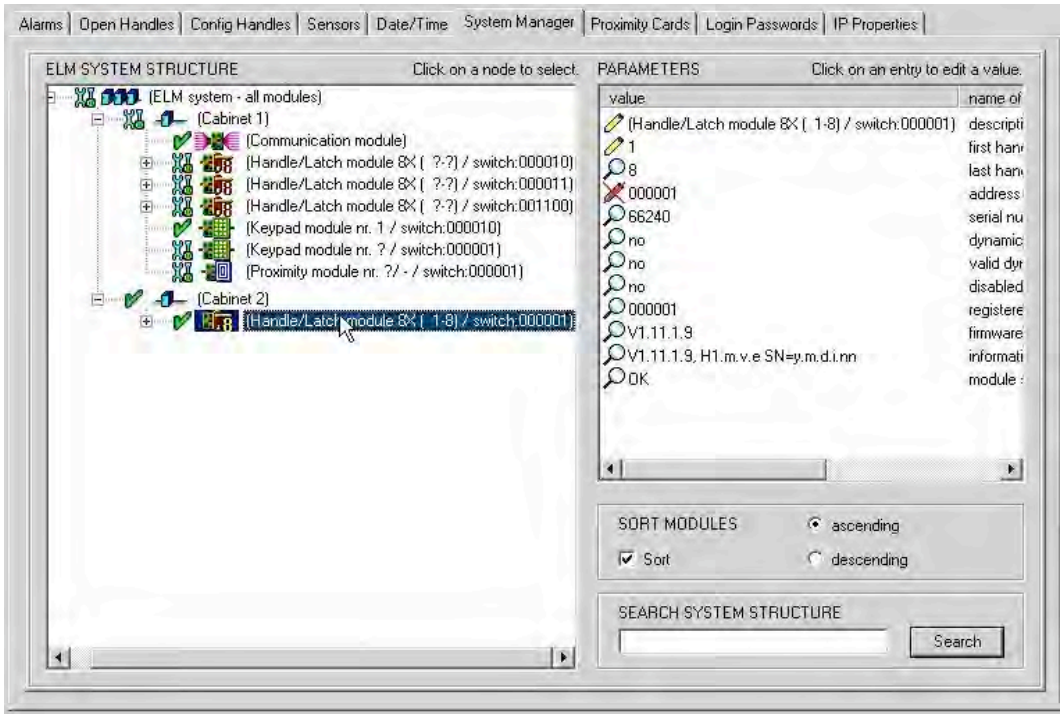
- Click with the right mouse button on the node **ELM system**.

A context menu is opened.

- Select **New Cabinet**.

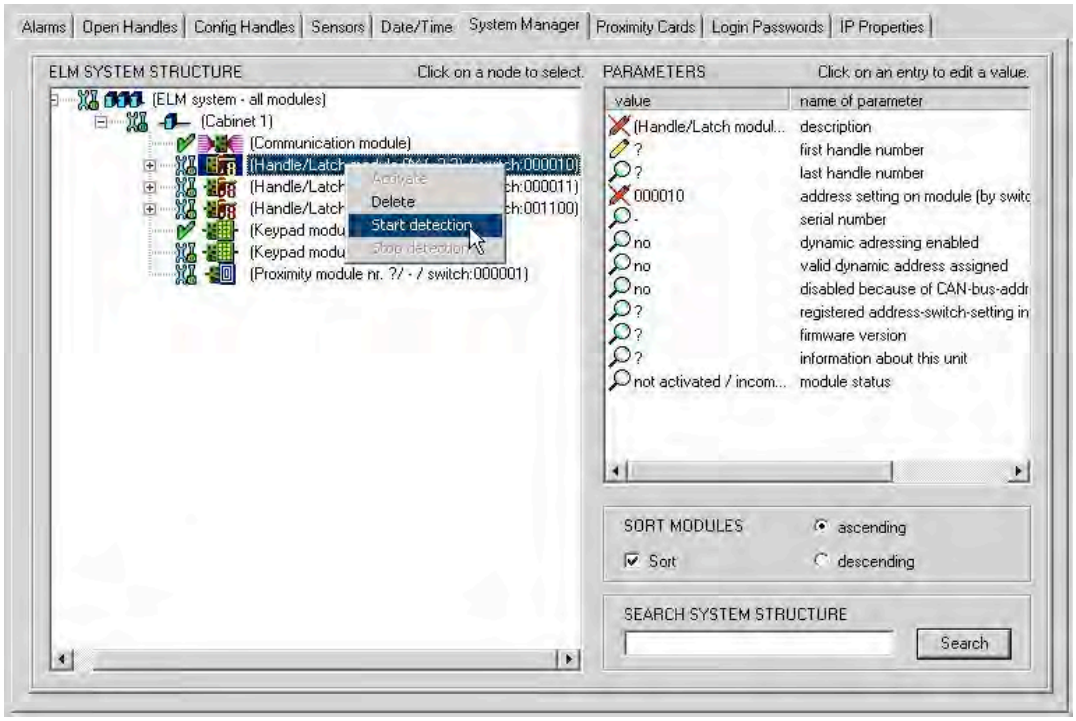


ELMcontrol generates a new node **Cabinet 2**. You can click, hold and drag modules to the new cabinet. The following image shows the result of shifting a module node to the new cabinet node.



7.4.2.4. Detection of Modules

- To identify the physical location of a module, click with the right mouse key on the module's node and select **Start detection** from the context menu.



For 255 seconds an LED on the module will flash. The LEDs on the other modules (apart from the Communications Module) permanently shine. The remaining period of time is displayed in the module status and in the module node.

- To stop the flashing LED, click with the right mouse button on the module's node and choose **Stop detection.**

7.4.2.5. Deactivation and Deletion of Modules

- If you want to delete a module from the list click on the module node with the right mouse key and select **Delete** from the context menu. If you delete a cabinet node all associated modules will also be deleted.

When an active module is deleted, it is immediately deactivated by the system. Please note that the module keeps its system address when it is deleted.

The Communications Module and the related cabinet cannot be deleted. If you delete the cabinet which contains the Communications Module then all the other modules (if any) will be removed from the cabinet.

7.4.3. Module Types and Parameters

The configuration parameters of the module types are listed in the following table:

Module type	***Parameter***	***read/ write***	***Meaning***
All	Description		Description of the module
	Firmware-version		Software version number of the module
	Module status		Status of the module (status of error)
All, except for Communications Module (P/N 16147-050)	Registered address-switch setting in table of modules		Binary CAN bus address which is registered to the table of modules by the system when the module is activated. This address must match the address setting on the module (either static or dynamic).
	Address setting on module		Binary CAN bus address which is assigned to the module, either static or dynamic. This value is writable if "dynamic addressing" is active (DIP switches 1-6 on the module are "on"). Otherwise the DIP switch setting 1-6 is displayed and used as address by the module.
	Serial number		A serial number stored within the module. This number is entered at production.
	Dynamic addressing enabled		(yes/no) Shows whether the module is set to dynamic addressing mode.
	Valid dynamic address assigned		(yes/no) Shows whether a valid dynamic address is assigned to the module.
	Disabled because of CAN-bus-addressing conflict		(yes/no) If two or more modules are set to the same address, then all except for one will be disabled.

Configuration parameters of module types – continued

Module type	***Parameter***	***read/ write***	***Meaning***
 Communica-tions Module (P/N 16147-050)	Specific features		Indications of specific properties -Hardware-Version-Number -Clock frequency (in Hz) -Baud-Rate of the serial connection (in Bit/s)
	SNMP:sysUpTime		SNMP variables according to the MIB-II system group
	SNMP:sysContact		
	SNMP:sysName		
	SNMP:sysLocation		
	Currently used amount of the general purpose file storage in bytes		Used amount and total capacity of the general purpose file storage of the Communications Module. You may change the total capacity by entering a different value. Please note that the capacity of the event log storage is in a reversed relationship to the capacity of the file storage.
	Total capacity of general purpose file storage in bytes		
	Current number of saved event log entries		Currently stored event log entries and total capacity of the event log storage. Enter '0' if you want to clear the event log storage.
	Total capacity of the event log ring-buffer; maximum number of entries / bytes		
	Current state of alarm line 1		Status of alarm line 1 Status being = **latched**, for a reset of the alarm delete the text in the input field. (see section 7.9. Configuration of Alarm)
	Description of alarm line1		Optional text description for alarm line 1 (see section 7.9. Configuration of Alarm)
	Latch mode of alarm line 1		**yes** = latch mode for alarm line 1 is switched on **no** = latch mode for alarm line 1 is switched off (see section 7.9. Configuration of Alarm)

	Relay for alarm1 shall be off if no alarm 1 is present		**yes** = relay off, because there is no Alarm 1 reported **no** = relay on, if there is Alarm 1 (see section 7.9. Configuration of Alarm)
	Current state of alarm line 2		Status of alarm line 2 Status being = **latched**, for a reset of the alarm delete the text in the input field. (see section 7.9. Configuration of Alarm)
	Description of alarm line 2		Optional text description for alarm line 2 (see section 7.9. Configuration of Alarm)
	Latch mode of alarm line 2		**yes** = latch mode for alarm line 2 is switched on **no** = latch mode for alarm line 2 is switched off (see section 7.9. Configuration of Alarm)
	Relay for alarm line 2 shall be off if no alarm is present		**yes** = relay off, because there is no Alarm 2 reported **no** = relay on, if there is Alarm 2 (see section 7.9. Configuration of Alarm)
	MAC address of Communications Module		MAC address of the network of the Communications Module (see section 7.2.3.1. 7.2.3.1. Network Setup of the System IP Properties)
	IP address of Communications Module		IP address of the network of the Communications Module (see section 7.2.3.1. 7.2.3.1. Network Setup of the System IP Properties)

Configuration parameters of module types – continued

Module type	***Parameter***	***read/ write***	***Meaning***
Keypad Module P/N (16147-008)	Number of component	✎	Number of the key pad unit (1-64)
Electronic Lock Control Module for 8 swing handles (P/N 16147-052)	First handle number	✎	Number of the first handle of this module
	Last handle number	🔍	Number of the last handle of this module
Proximity Card Reader Module (P/N 16147-054)	Number of component	✎	Number of the proximity unit (1-64)
	1. length of card-ID	✎	(see section 7.8. Proximity Cards)
	1. start address of the card-ID	✎	(see section 7.8. Proximity Cards)
	2. length of card-ID	✎	(see section 7.8. Proximity Cards)
	2. start address of card-ID	✎	(see section 7.8. Proximity Cards)
	Card-ID mask	✎	(see section 7.8. Proximity Cards)
	Keeping period	✎	(see section 7.8. Proximity Cards)
	ID of current card	🔍	ID-number of the card that is held before the proximity reading station

7.4.4. Configuration Data Files

The configuration data of the system can be stored in a separate backup file on the workstation and can be downloaded from the workstation to the system.

The configuration data files include the configuration of all modules with the complete number of components and their parameters as well as the data for all proximity cards. The data that can be set via serial connection only (e.g. the IP-configuration of the Communications Module and the workstation login passwords) is not included in the configuration file.

Two different configuration file formats are available.

Text File

A text format allows changes of the configuration in a text editor. Note that the text format of the configuration file includes all access codes for all handles and all alarm-settings.

The file consists of multiple entries. Each entry includes a configuration parameter in the form of an SNMP-Identification Number, together with the SNMP-data type and the value of the parameters. These three elements are placed in one line, separated by semicolon and preceded by comment lines indicated by the characters "//". The comments indicate the component or module and explain the parameter.

Examples:

```
//module table entry number: 1
//(Handle module 8X (1-8) / switch:000001)
//first handle number
.1.3.6.1.4.1.13595.1.2.4.2.1.3.1;2;1
```

This example is the specification of the first handle number for the handle module with address 1 (switch: 000001). The SNMP-OID of this parameter is *.1.3.6.1.4.1.13595.1.2.4.2.1.3.1*. The data type is 2 (INTEGER) and the value is *1*.

```
//(Handle module 8X (1-8) / switch:000001)
//(Handle 2)
//description
.1.3.6.1.4.1.13595.1.2.1.2.1.3.2;4;back door
```

This example shows the text description for handle 2, which is "back door". The data type of this parameter is 4 (OCTETSTRING). This handle is the second handle of the handle module with address 1 (switch: 000001).

```
//(Handle 1)
//(ACN 4 of handle 1)
//access code number
.1.3.6.1.4.1.13595.1.2.1.2.1.7.1;4;2112
```

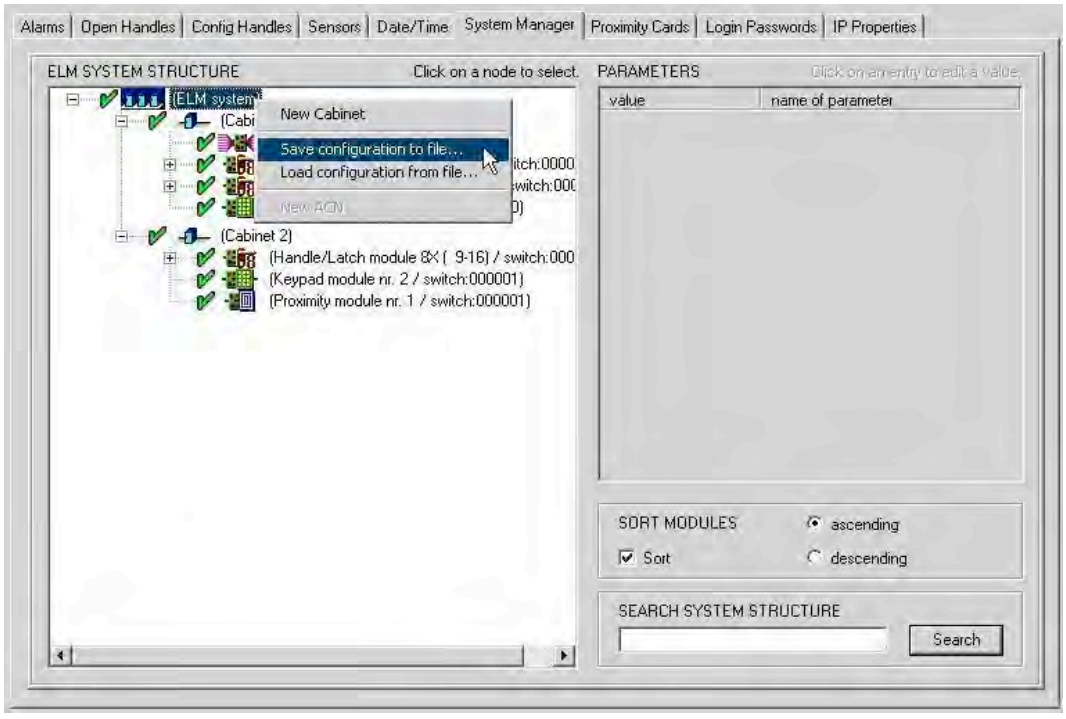
This example shows the forth access code number (ACN 4) for opening handle 1 is 2112.

Encrypted File

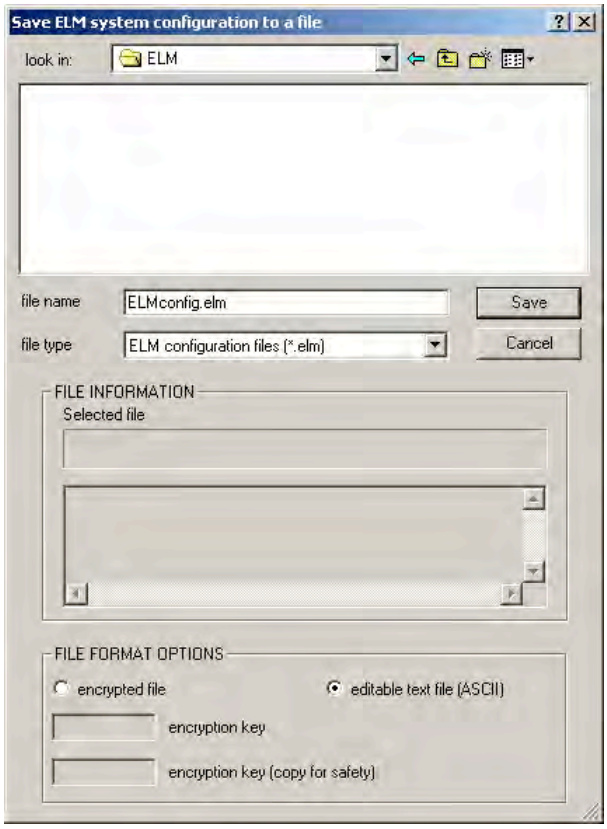
An encrypted file format protects the information contained in the file against unauthorized viewing and changes. The file is saved by a password and then encoded. The algorithm that is used for encoding is Triple-DES according to standard ANSI X9.52.

7.4.4.1. Storing Configuration Data to a File

- Under the **ELM System Structure** area on the System Manager tab, click with the right mouse button on the node **ELM system**.
- Select **Save configuration to file** from the context menu. It is also possible to call up the function from the main menu (**File**/**Save**) or click on the icon of the tool bar.



You get to the following window:



- Select a directory, name the file, and assign a file type for the configuration file. *ELMcontrol* prescribes the file type "**.elm**", but you can choose a different name for the file type.

- Select the **encrypted file** button in the **FILE FORMAT OPTIONS** area to encode the file. Enter a password in the **Encryption Key** field. Verify the password in the **Encryption Key (copy for safety)** field. Remember your password.

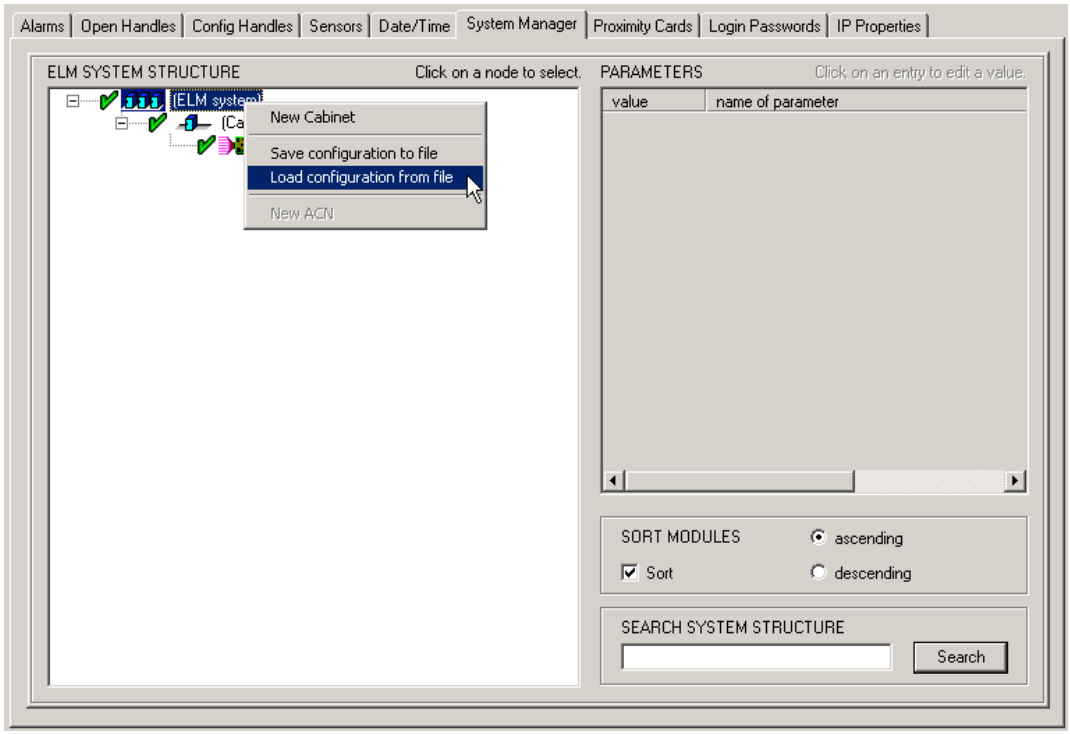
- Click the key **Save**.

Configuration data is scanned from the system and saved to the file.

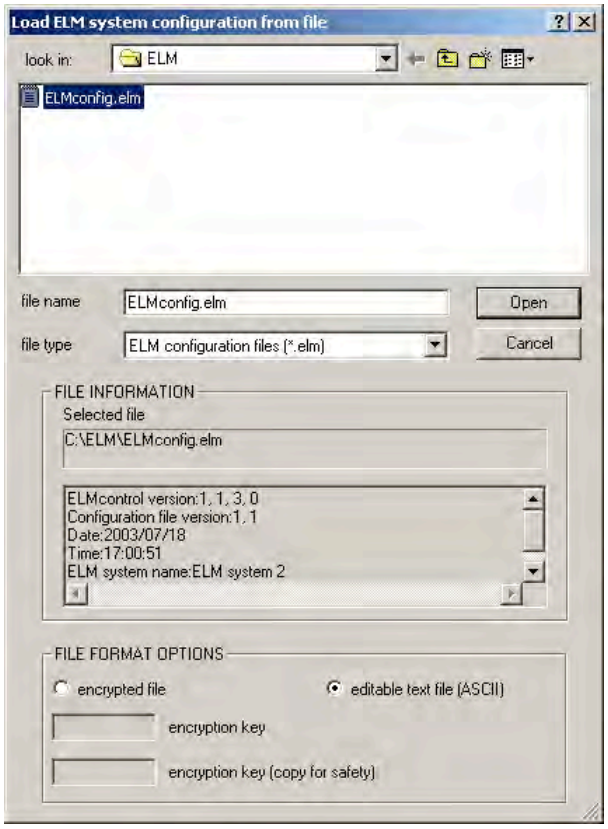
7.4.4.2. Loading Configuration Data From a File

Loading a configuration file is only possible after the existing configuration of the system has been deleted.

- Delete all entered cabinets or modules. Only the Communications Module and Cabinet1 should remain in the tree-structure under the **ELM SYSTEM STRUCTURE** area on the System Manager tab.
- Right click on the **ELM system** node.
- Select **Load configuration from file** from the context menu. You can also use (**File**/**Open**) from the main menu or click on the icon in the tool bar.



You get to the following window.



- Select a configuration file.

ELMcontrol recognizes the format of the selected file. If the file is text format with free access (not encoded) file information is shown in the **FILE INFORMATION** area.

- If the file is encoded with a password, enter the password in the Encryption Key field in the **FILE FORMAT OPTIONS** area.

- Click the key **Open**.

Configuration data is scanned from the file and loaded to the system.

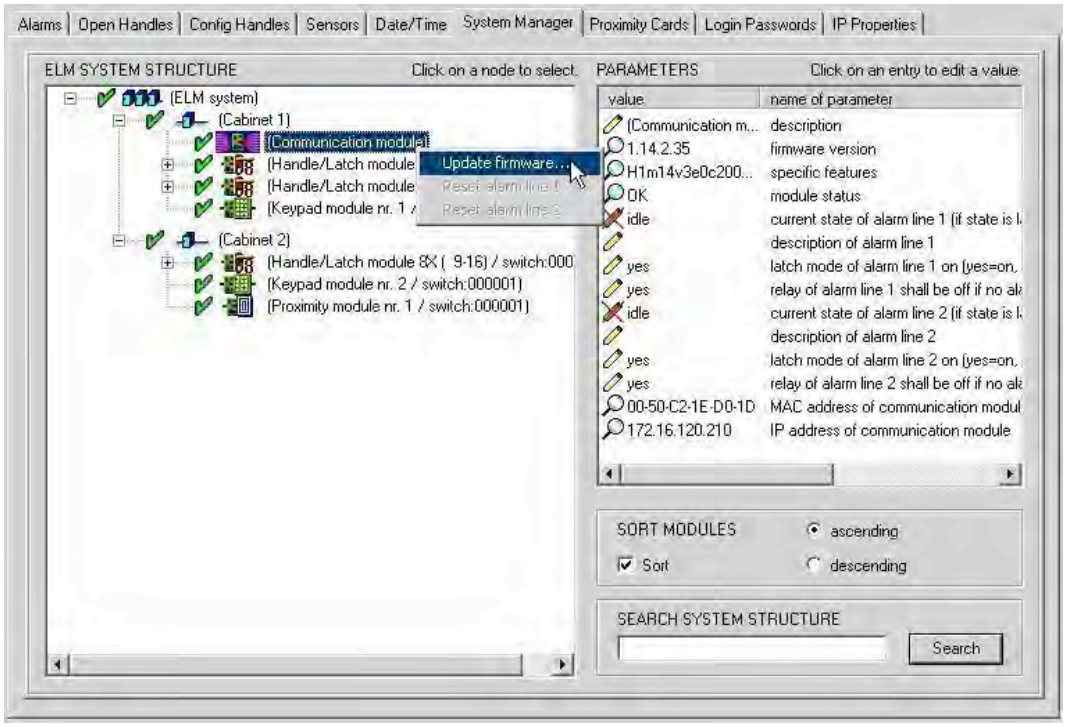
7.4.5. Updating Firmware of a Communications Module

When setting up a data connection with a Communications Module, the *ELMcontrol* software determines compatibility with the module's firmware. If the firmware is not compatible a corresponding message is generated that list the current firmware version and the required minimum firmware version.

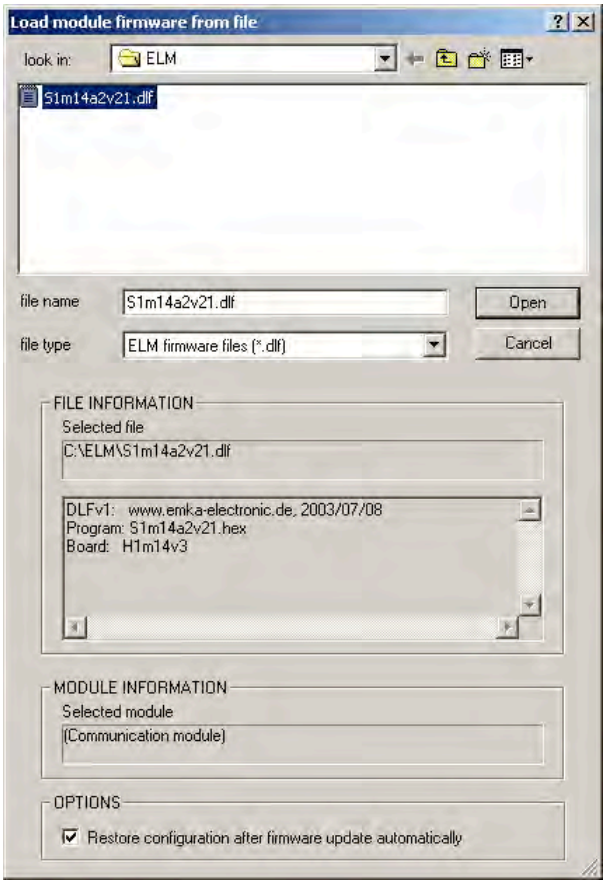
Download the current firmware version from the CPI Website at http://www.chatsworth.com/Support-and-Downloads/Downloads/Software/. Update firmware from the System Manager tab using a serial connection.

A firmware update deletes all configuration data. Before the firmware is updated, *ELMcontrol* can automatically save the existing configuration in a file and restore it afterwards, if requested. Restoring includes configuration of all modules with every component and their parameters as well as the data of all proximity cards. However, the IP-configuration and the login-passwords cannot be restored. These settings must be entered manually using a serial connection after the firmware update is complete.

- Obtain a copy of the new firmware file from the CPI Website or Technical Support.
- Right click the Communications Module node under the **ELM SYSTEM STRUCTURE** area on the System Manager tab.
- Select **Update firmware** in the context menu. You can also use (**File/Update Firmware**) from the main menu or click on the icon in the tool bar.



You get to the following window.



- Select a firmware file. The file type is "**dlf**".

In the **FILE INFORMATION** area, the firmware upgrade version and compatible module is shown.

Restore configuration after firmware update automatically is pre-selected in the **OPTIONS** area. Selecting this option will automatically save a system configuration file before installing the firmware upgrade. After the upgrade, the system configuration will be loaded on the system. You must complete the IP configuration and login passwords manually using a serial connection.

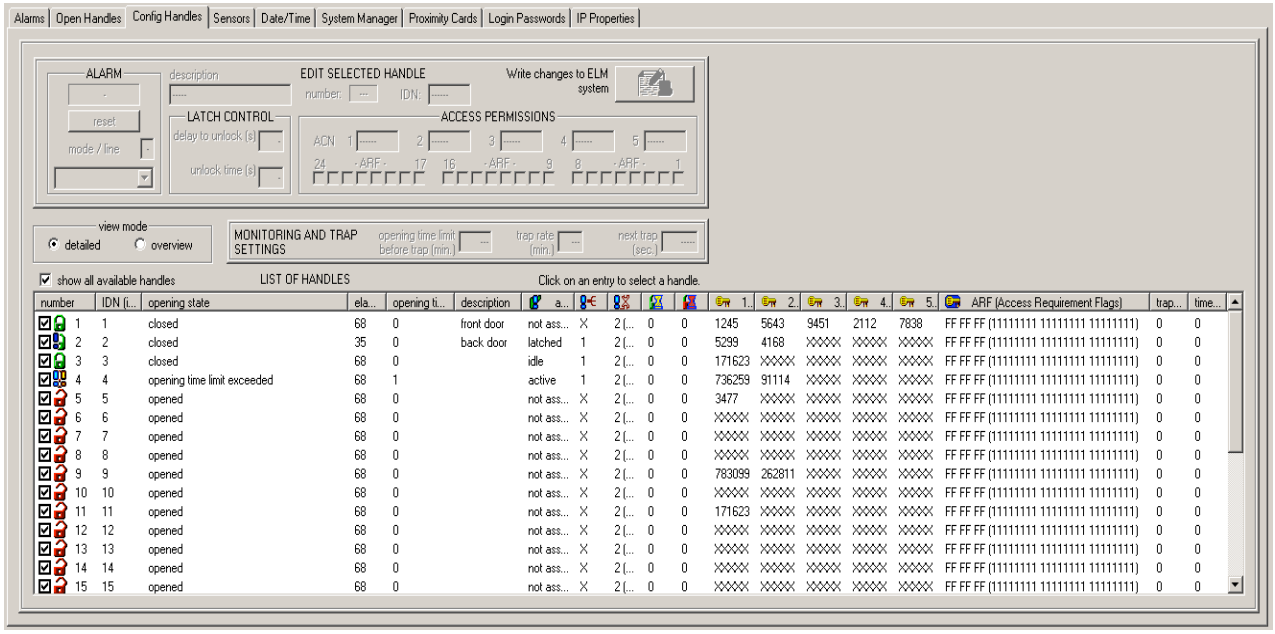
- Click the key **Open**.

The firmware update is started.

7.5. Configuring Handles and Latches

Use the **Configure Handles** tab to configure handles.

- Click on the index tab **Configure Handles**. You will see the following screen:



The table **LIST OF HANDLES** shows the handles attached to the system. You can sort the list according to each of the displayed columns of the table by a click on the corresponding top of the column. Click again on the same place and the order is reversed.

The **View mode** toggles between a multi-column **Overview** or a list with all **Details** (shown).

The table includes the following information:

Number
Every handle has a number, which is defined during the configuration of the Electronic Lock Control Module. This number serves as an identification of the handle and is used when opening the handle with a Keypad Module or Proximity Card Reader Module.

Status symbol
There is a symbol at the left side of the handle number. It indicates the present status of the handle.

The following status symbols are shown individually or in combination:

 *The handle is open.*

The handle is closed.

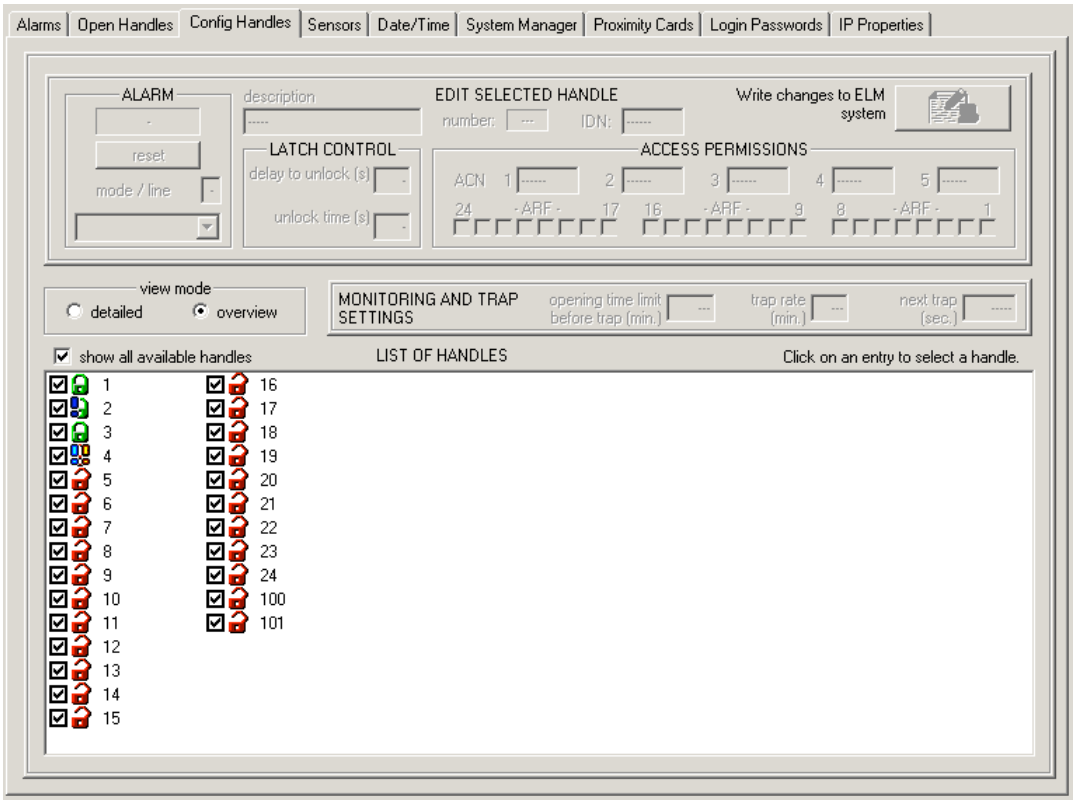
The handle reports an active alarm. (light blue exclamation mark)

The handle reports latched alarm. (dark blue exclamation mark)

The handle module is defective. (red exclamation mark)
The system administrator should check the correct setting of the module parameters in the system-manager and should exchange defective modules.

Number and status of the handle are unknown.
ELMcontrol has not read all necessary information from the system (i. e. the scan process is not complete).

The view mode **Overview** shows the handle number and the status symbol for every handle, only.



Scan process
There is a check box at the left hand side of the status symbol which changes the handle scan process as follows.

☑ *complete scan of all handle data*
ELMcontrol scans all data of the handle and shows under the **Details** view mode all properties delivered by the system for the present login level.

☐ *scan of the handle status, only*
ELMcontrol scans only handle data from the system that is necessary for monitoring the present status of the handle. This refers to the opening status, alarm status and the error status of the handle module. *ELMcontrol* only shows the corresponding status symbols of the handle. This reduces the scan process and allows a faster update rate of the handle display because less data is exchanged. You cannot change the handle parameters (e. g. access code numbers) with this type of scan because *ELMcontrol* does not exchange the corresponding data with the system.

- For a change of scan, check or uncheck the check box next to the handle with a mouse click or by highlighting the handle and pressing the space bar.

Above the table **LIST OF HANDLES** you will find the check box **show all available handles.** If this check box is marked all handle numbers which can be assigned to Electronic Lock Control Modules known to the system are listed in the table. For example, if one eight handle module is connected, eight handles will be shown in the list even if eight handles are not physically connected to the module. With the check box **show all available handles** unmarked the table of handles shows only the handles that have the ***complete scan of all handle data*** check box marked.

- To delete certain handles from the table, the scan process for these handles should be set to ***scan of handle status, only*** (uncheck the handle scan check box) and uncheck the **show all available handles** check box.

IDN (identification number)
1..6-digit number which can independently be assigned to a handle or latch

Opening state
The present status (**open / opening time limit exceeded / closed / delayed to unlock / unlocked**) is shown. This requires the use of handles, which have a contact for signaling the status of the handle to the handle module.

Elapsed time in current state (minutes)
The time elapsed since the handle has entered the current opening state.

Opening time limit (minutes)
The time limit allowed for a handle to be opened. Exceeding this limit causes sending of SNMP trap(s) if the **Trap rate** setting (see below) for this handle is not 0. The time limit

before entering the state **opening time limit exceeded** can be defined in 1 minute steps from 0 to 9999 minutes; 0 means "no limit".

Description
Every handle can be given a description with a maximum of 31 characters.

Alarm state
The handle can be in one of the following alarm status:

Alarm status	*Meaning*
not assigned	The handle is not connected with an alarm line.
idle	The handle is connected with an alarm line. The handle is closed at present; no releasing condition (handle open) exists. The handle does not cause an alarm.
active	The handle causes an "active" alarm. This means that the handle is connected to an alarm line and the releasing condition (handle open) exists at present. The alarm line assigned to the handle is also in a condition of "active" alarm.
latched	The handle causes a "latched" alarm. The handle is connected to an alarm line and the alarm type "latched" is switched on. The handle is closed at present; at a previous time, however, it was open. The alarm line assigned to the handle is also in a "latched" status if no other components connected with this alarm line report "active" alarm.
?	The alarm status is unknown. *ELMcontrol* has not read all information from the system necessary for terminating the scan process.

Alarm line
Shows the number of the assigned alarm line. If the handle was not assigned to an alarm line the character **X** is displayed.

Alarm mode
The setting is only effective in cases where an alarm line is assigned to the handle/latch. The following modes are available:

Alarm mode	*Meaning*
1 (alarm if opened / latching off)	If the handle is opened, it causes an "active" alarm. The alarm will be cancelled when the handle is closed. The alarm state returns to "idle".
2 (alarm if opened / latching on)	If the handle is opened, it causes an "active" alarm. After closing the handle the alarm will continue as a "latched" alarm.
3 (alarm if unexpected opened / latching off)	If the handle is opened, it causes an "active" alarm but only if the opening was not authorized (burglary). The alarm will be cancelled when the handle is closed. The alarm state returns to "idle".

4 (alarm if unexpected opened / latching on)	If the handle is opened, it causes an "active" alarm but only if the opening was not authorized (burglary). After closing the handle the alarm will continue as a "latched" alarm.

Delay to unlock
For latches only: This parameter determines the delay period after initiating the opening (e.g. by entering the right access code on a key pad) until the beginning of the release period. The time period can be entered in 2 seconds steps from 0 to 510 seconds.

Unlock time
For latches only: This parameter defines the real release period. This period of time starts after expiry of the delay time (see above). During the unlock period the door can be opened at any time - but only once. An immediate locking is carried out when closing the door even if the unlock time hasn't expired yet. The time period can be entered in 2 seconds steps from 0 to 510 seconds.

Access Code Numbers (ACN 1 - ACN 5)
With one of the shown number codes the handle can be opened via keypad, proximity card, or PC (software). Codes that haven't been fixed are displayed by the sequence of characters **XXXXX.**

Access Requirement Flags (ARF)
These 24 flags form another method of authorization for opening a handle. The ARF can be used with a proximity card or keypad. Each of the 24 flags can be set or deleted independently. Each card (see section 7.8. Proximity Cards) as well as each user (see section 7.3.2.2. 7.2.3.2. User Management) has 24 flags, called the Access Permission Flags (APF).
A handle can be opened by a proximity card or keypad with a user account number when the handle's ARF matches the user's/proximity card's APF.
With the help of the ARF/APF you can form groups from handles and cards or users with different opening permissions which can be subdivided hierarchically.

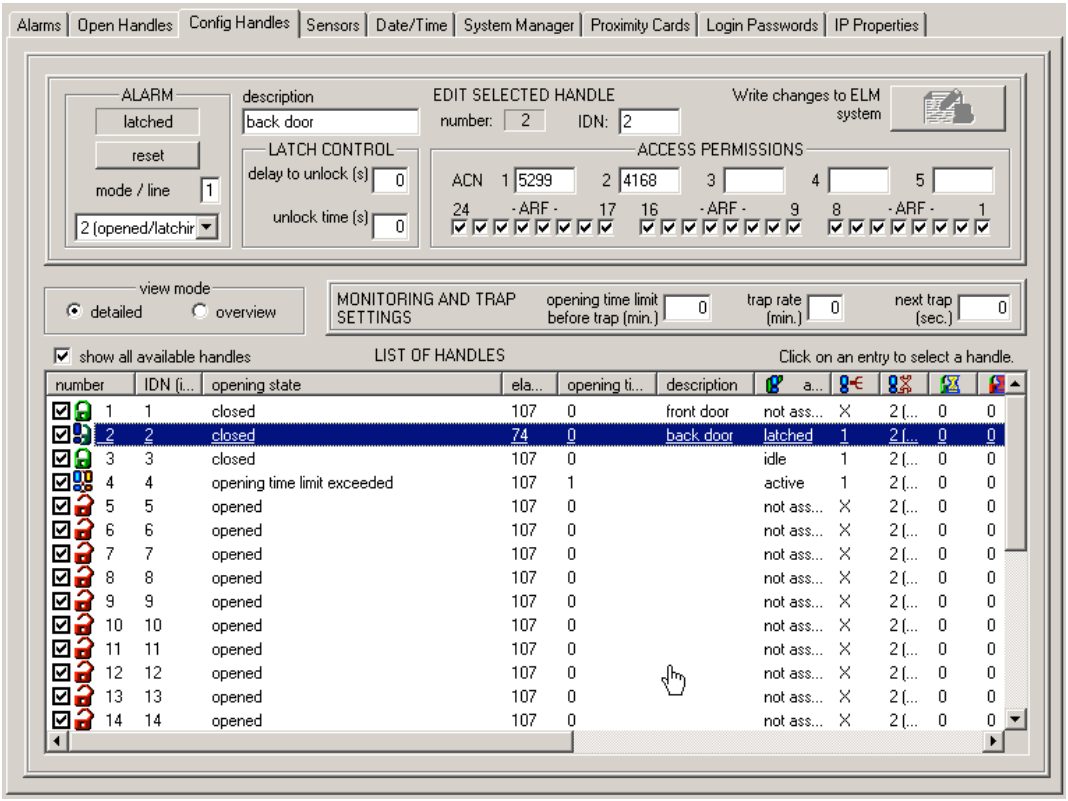
Trap rate
Trap mode and time interval for sending SNMP-traps at changes of opening state of the handle/latch.
The following values are possible:

- 0: The handle/latch does not send any SNMP-trap (default)
- 1: At each change of the opening condition a trap is sent once.
- 2 .. 250: At each change of the opening condition one trap is sent. But this trap is then repeated every 2 .. 250 minutes.

Time until next trap
At Trap rate settings of 2 .. 250 this is the time up to the next trap (in seconds).

Change Settings

- To change the settings of a handle select the handle that you want to edit with a click with the left mouse button on the desired row in the table. The line is marked in color. Note: the scan button for the selected handle must be marked (complete scan of all data).



The parameters of the selected handle are shown in the **EDIT SELECTED HANDLE** area.

Now you can edit the description, the access codes and flags, the connection to the alarm line and the type of alarm. In case of a latch you can additionally edit the delay time and the unlock time.

- The **description** is text with no more than 31 characters.
- An **ACN** is numbers only. The minimum length is 4 digits, and the maximum length is 6 digits. To delete an access code, remove all numbers from the corresponding field or put in the character **X.**
- Mark all the flags of the **ARF** that you want to set.
- The numbers 1 or 2 are possible **alarm line** numbers. To disconnect an alarm line use the character **X** or remove the number from the input field.

- Select the desired **alarm mode**.

- If the handle/latch should send SNMP-Traps when opened/closed, adjust the desired **trap rate**. At values of 2 ... 250 the remaining time to the **next trap** is shown**.** In this case you may overwrite this time value and so e.g. trigger the next SNMP-trap for test purposes at another time.

- After you have made the desired changes click the button **Write changes to ELM system**.

The entries are updated after the next scan (reading cycle).

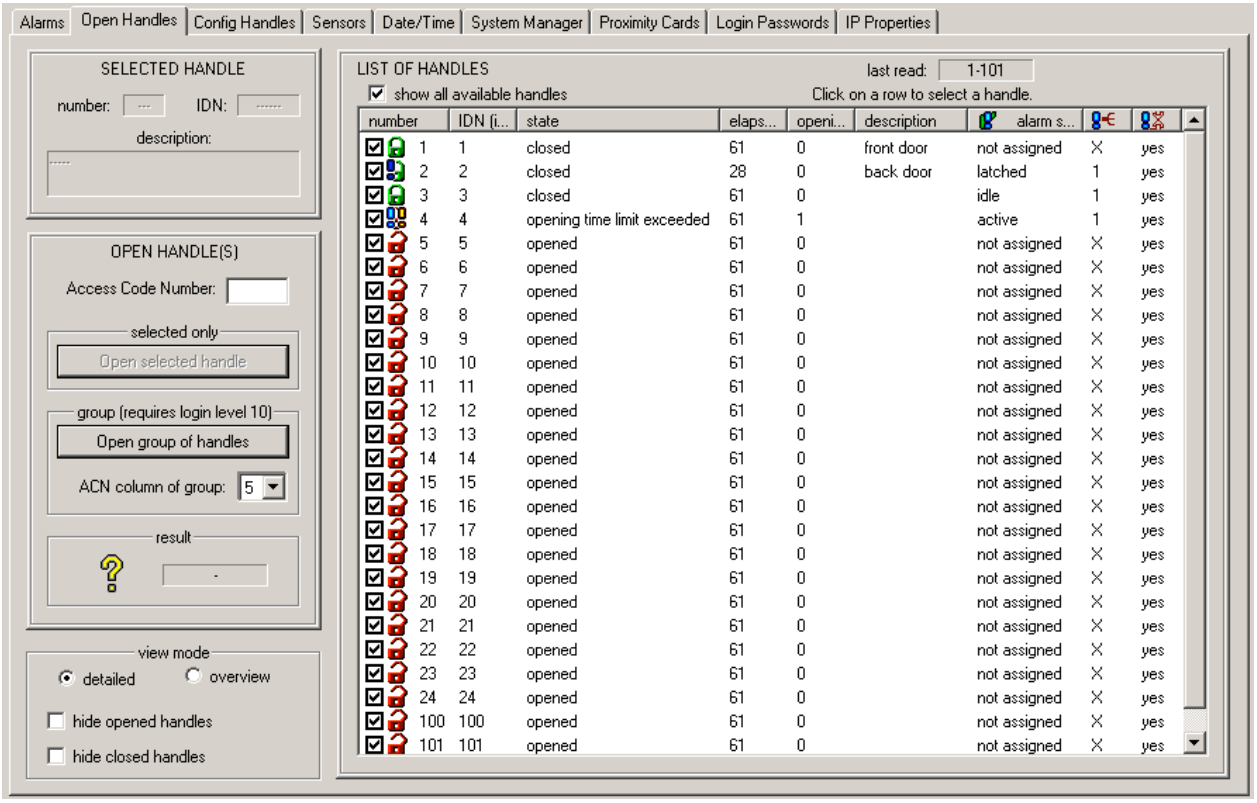
If the button **Write change to the ELM system** is not clicked any changes made are dismissed as soon as you select another handle or if you leave the index card **Configure Handles.**

Handles showing the alarm status "latched" can be put back to the status "idle" in the **ALARM** area by clicking the **reset** button. Handles showing the alarm status "active" can be put back to the status "idle" only if alarm mode 3 or 4 is assigned to the handle.

7.6. Open Handles and Unlock Latches

The index card **Open Handles** allows the opening of handles and the unlocking of latches from a workstation using the *ELMcontrol* software. Unlike the System Manager tab, you must have a valid ACN to open a handle. The index card **Open Handles** can be used with a low login level.

- Click on the index tab **Open Handles.** The following window shows the corresponding index card:



The Table **LIST OF HANDLES** shows the handles of the system.

The **View mode** can be a multi-column **Overview** or a list with all **Details** (shown). You can also hide open or closed handles by selecting the button **hide open handles** or **hide closed handles**.

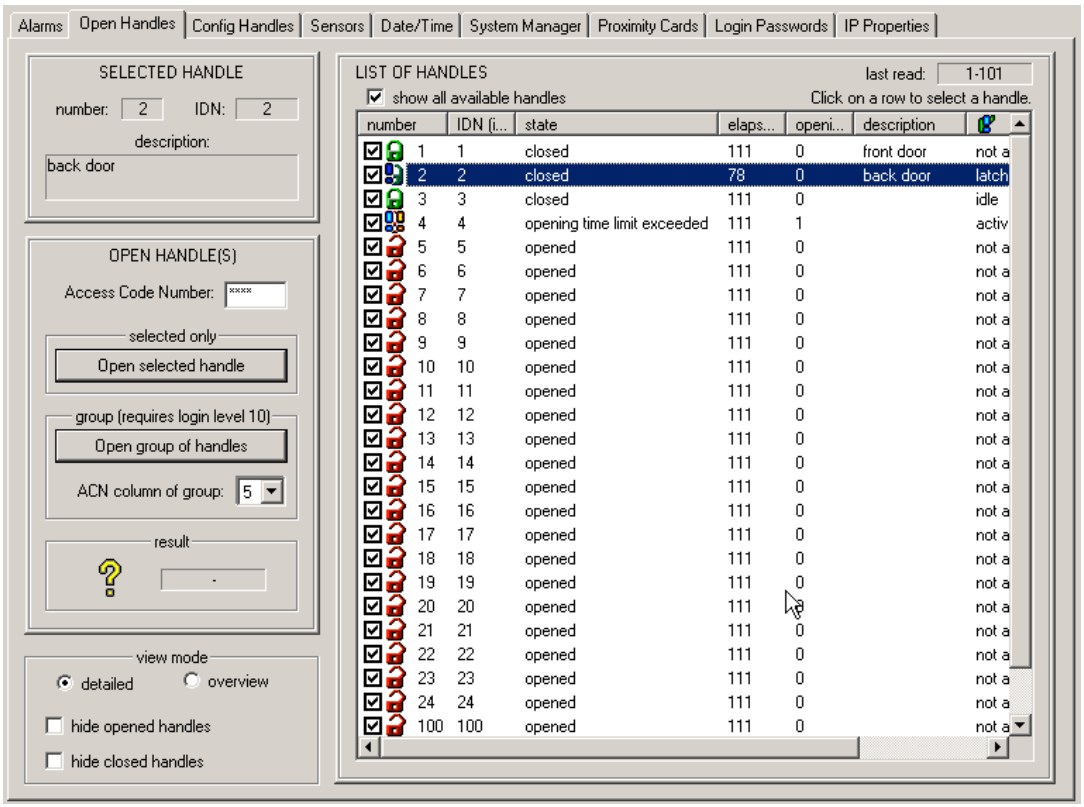
The table contains the following criteria:

Number
Status symbol
Scan process
Identification number
Opening state

Elapsed time in current state (minutes)
Opening time limit (minutes)
Description
Alarm state
Alarm line
Alarm latch mode

This information is also contained in the corresponding table on the index card **Configure Handles**, see section 7.5. Configuring Handles for criteria explanations.

- To open a handle select the corresponding handle by clicking with the left mouse button on the handle number in the table.



Number and description of the selected handle are shown in the **SELECTED HANDLE** area.

- In the **OPEN HANDLE(S)** area put in a permitted Access Code Number (ACN) for this handle.

- Click on the button **Open Selected Handle.**

After an analysis by the system you will see if the ACN is accepted in the **Result** field. As soon as the handle has been opened the change of the status of the handle (opened) is shown in the table of handles after the next reading cycle (scan).

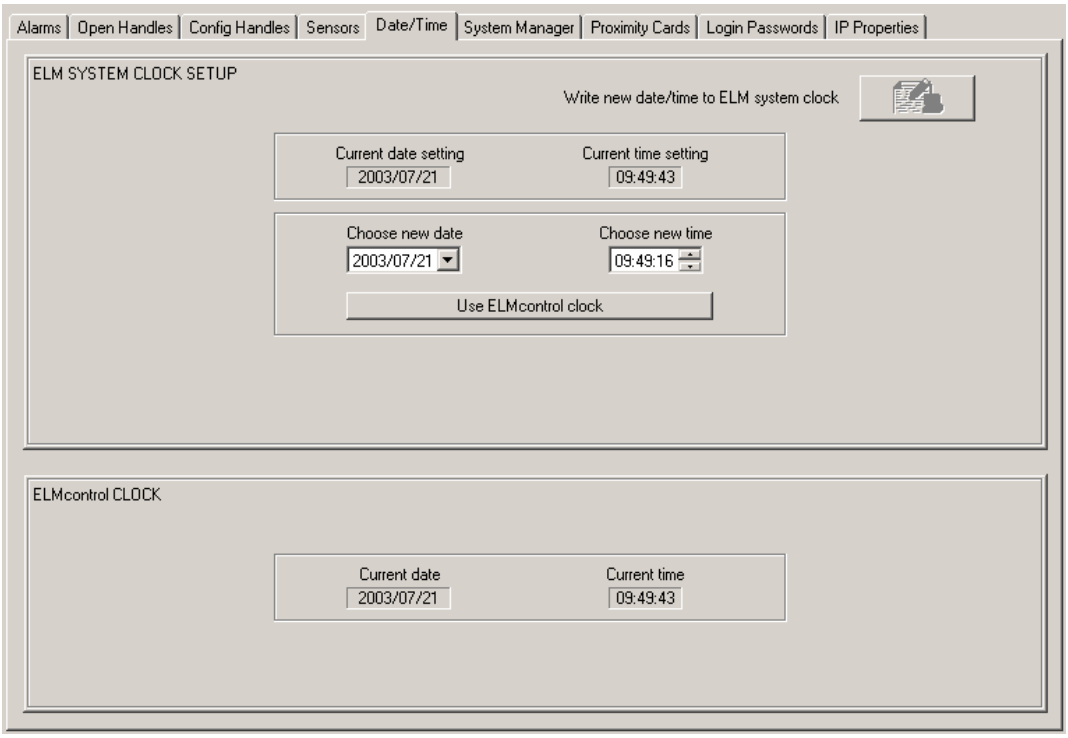
By clicking **Open group of handles** each handle having the entered **Acess Code Number** defined as its **ACN column of group** (choose from 1..5) will be opened.

Attention: Please keep in mind that if opening a group of single point latches then these latches may be powered from the same source. Make sure that the power supply can handle the requirement. The sum of current needed by these latches may also exceed the specified current limit of the latch controller module (depends on the used latch type).
Please note that for this reason, latches connected to latch controller modules for 8 single point latches may be excluded from opening for safety.

7.7. Setting of Date and Time

The system includes an internal clock (a timer with an accumulator that makes it independent from the operational voltage). Each event stored in the event log includes the date and time on the internal clock – the **ELM SYSTEM CLOCK**. The expiry date of proximity cards is also determined from this clock.

The index card **Date/Time** allows scanning and adjusting of the system clock.



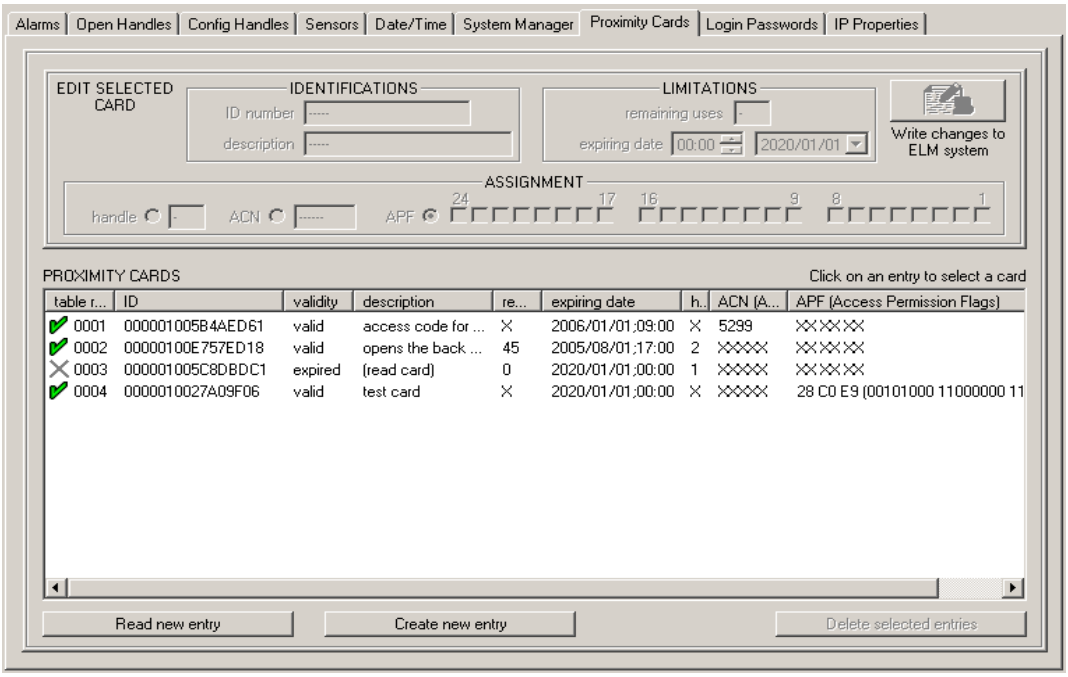
The actual time of the system clock is shown in the area **ELM SYSTEM CLOCK SETUP** in the fields **current date setting** and **current time setting.** Adjust the time using the input fields **Choose new date** or **Choose new time** and set the new date or time by clicking on the button **Write new date/time to ELM system clock**.

The **ELMcontrol CLOCK** area shows the time on the connected workstation – the workstation hosting the *ELMcontrol* software. Click on the button **Use ELMcontrol clock** in the **ELM SYSTEM CLOCK SETUP** area to synchronize the system clock with the clock on the workstation hosting the *ELMcontrol* software.

7.8. Proximity Cards

The Proximity Card Reader Module allows the opening of handles with proximity cards (Legic-System). The system can save a list of up to 1000 card entries with permission to open handles. The administration of these card entries is possible from the **Proximity Cards** tab.

- Click on the index tab **Proximity Cards**. You will get to the window below.



The table **PROXIMITY CARDS** shows all card entries for the system. You can sort the list according to each of the displayed columns of the table by a click on the corresponding top of the column. Click again on the same place and the order is reversed.

The table contains the following information:

Table row
The number of the table row, which stores the data of the card, is shown for information.

ID Number
The ID number of the entry identifies the card. It contains 2 to 16 hexadecimal digits.

Attention: A single card can be listed in the table several times with different ID numbers. Additonally, different cards can produce the same ID number at different proximity reading stations. Therefore the number of entries in the table does not necessarily correspond to the number of actually used cards.

When a card is held before the reading station of a Proximity Card Reader Module, the module determines the ID number of this card as follows:

- The Proximity Card Reader Module reads two areas from the memory of the card. The start address and the length of each area is defined in the system manager during the configuration of the Proximity Card Reader Module. Every area may comprise a maximum of 8 bytes or 16 digits. The total length of both areas is also limited to 8 bytes or 16 digits.
- Both areas are put together into one number consisting of 2 to 16 hexadecimal figures.
- This number is linked with the ID mask, which is also set during the configuration of the Proximity Card Reader Module. This mask consists of 16 hexadecimal figures. Starting on the left, a bit-wise logical addition (OR-link) is carried out. Bits of no relevance are set to the value 0.
- The result is the ID-number of the card.

Note: If more than one Proximity Card Reader Module is used in the system, be sure that the parameters of the modules (length of card ID, start address of the card Id, and card ID mask) are the same. If the modules' parameters are configured differently, it is possible to get different ID numbers from the same card or the same ID number from different cards. The result is different access rights at different reading stations for each card.

Status symbol
At the left hand side of the ID-number you will find a symbol that gives information on the validity of the card entry.

The following status symbols are displayed:

 *The card entry is valid.*

 *The card entry is run out.*

Validity
The use of every card entry can be limited to a specific number of uses and/or until a particular date and time. If these limits are not reached the card entry is **valid**, otherwise the card entry is **run out** and is not accepted by the reading station.

Description
Every card entry can be assigned a text as description with a maximum length of 31 characters.

Remaining uses

If the number of uses of a card entry is limited, the number of times the card can be used to open handles is listed. If the value is **0**, the card has run out. If the use of the card is unlimited the character **X** is shown.

Date of expiry
The expiration date and time of the card entry is displayed. After expiration a card entry becomes invalid.

Handle
If a handle is assigned to the card entry, the handle number is shown. If it is a valid card entry the corresponding handle opens upon reading of the card at a reading station. If no handle was assigned to the card entry the character **X** is displayed.

Access Code Number (ACN)
If an access code has been assigned to the card entry this access code is shown. To open a handle the handle number must be selected at a Keypad Module and the card must be read at a card reader. The **holding time** set for the Proximity Card Reader Module and the Keypad Module determines how much time is available for the process. The system checks the access code assigned to the card entry. If the access code is valid, the handle opens. If there is no access code assigned to the card entry the character sequence **XXXXX** is displayed.

Access Permission Flags (APF)
These 24 flags form another method of authorization for opening a handle with a proximity card. Each of the 24 flags can be set or deleted. Each handle (see section 7.5. Configuring Handles and Latches) also has 24 flags, called the Access Requirement Flags (ARF). **A handle can be opened by a proximity card when the APF for the card matches the ARF for the handle.** With the help of the ARF/APF you can form groups from handles and cards with different opening permissions which can be subdivided hierarchically.

Adding card entries

With the button **Create new entry** it is possible to add a new card entry to the list.

- Click the button **Create new entry.**

A card entry with a serial numbered ID number is added to the list.

- Change settings for the card entry consequently as explained below. Enter the ID number and all necessary parameters.

It is also possible to add the new card entry to the list by use of a reading station.

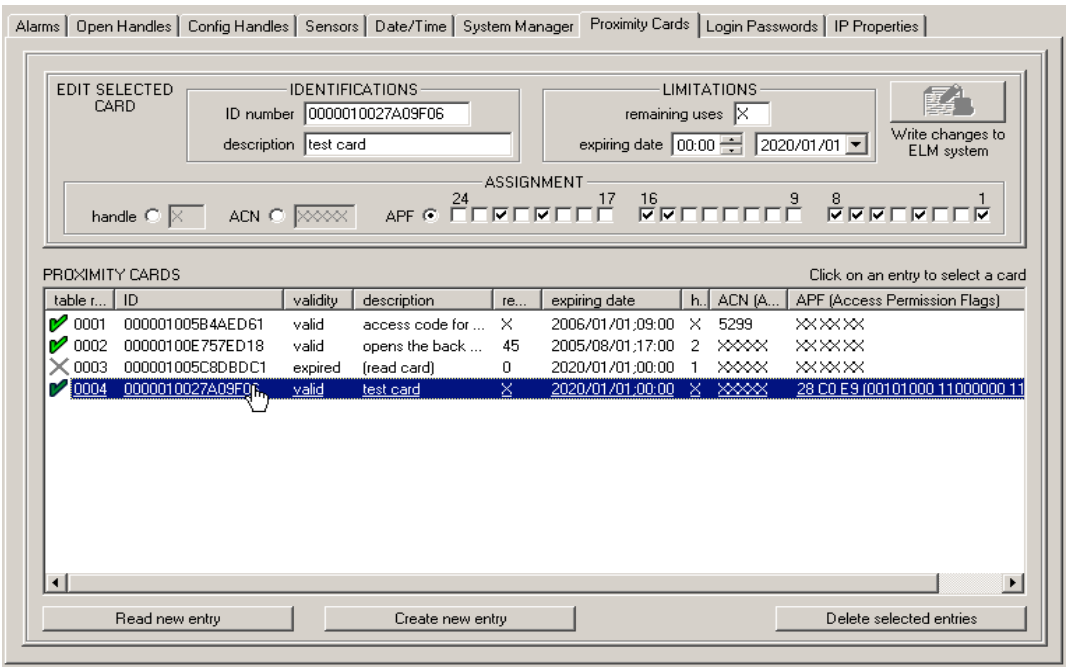
- Click on the button **Read new entry**. The button remains on.
- Then hold the card in front of a reading station.

A new card entry is added with the recognized ID number if there is no entry in the list with the same ID number.

- Scan other cards if required.
- Click on the button **Read new entry** to stop scanning cards.

Change settings

- To change the settings for a card entry first select the entry that will be modified by clicking the corresponding row in the table with the left mouse button.



In the **EDIT SELECTED CARDS** area the parameters of the card entry can be changed.

- Up to 16 hexadecimal figures (**0**-**9**, **A**-**F**) can be put in for the ID number. In case of an odd number of digits the figure **0** is put in the first place. The card entry is removed if the ID number field is left blank.
- For description enter text with a maximum of 31 characters.
- Assign either a handle number or an ACN or the APF to the card entry.
    - An access code consists of numbers only, comprising at least four and not more than six digits. To remove the access code please delete all characters in the corresponding input field or put in the character **X**.

- For the handle number you can put in **1** to **512**. If you want to cancel the assignment to a handle number please enter the character **X** or delete the number from the input field.

- Mark all the flags of the APF which you want to set.

- If you want to limit the number of uses for the card enter the corresponding number of uses into the field **remaining uses**. Values from **0** to **254** are possible. The value **0** causes blocking of the card entry. If you want to use the card entry an unlimited number of times, please delete the entry or put in the character **X**.

- Set the expiration date and time of the card in the corresponding fields.

- After the changes have been made click on the key **Write changes to ELM system**.

The corresponding entries to the table are updated after the next reading cycle (scan).

If the button **Write changes to ELM system** is not clicked any changes made are dismissed as soon as you select another entry or if you leave the **Proximity Cards** tab.

Deleting card entries

- First select the desired card entry by left clicking the row in the table with the mouse. With the control key (Ctrl) or the shift key being pressed at the same time you can select several entries or areas.

- Click on the button **Delete selected entries.**

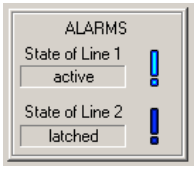
The entry can also be removed by deleting the ID number in the corresponding input field.

7.9. Configuration of Alarm

The system is capable of administering two alarm lines.

Every alarm line is connected to a relay on the Communications Module. The relays have switch over contacts and can be wired as either normally open (NO) or normally closed (NC). When the alarms are active or latched, the contacts are energized which closes the contacts wired in the NO mode and opens the contacts wired in the NC mode.

The status of both alarm lines is shown in the area **ALARMS** in the left column of the user interface when logged in to the system.

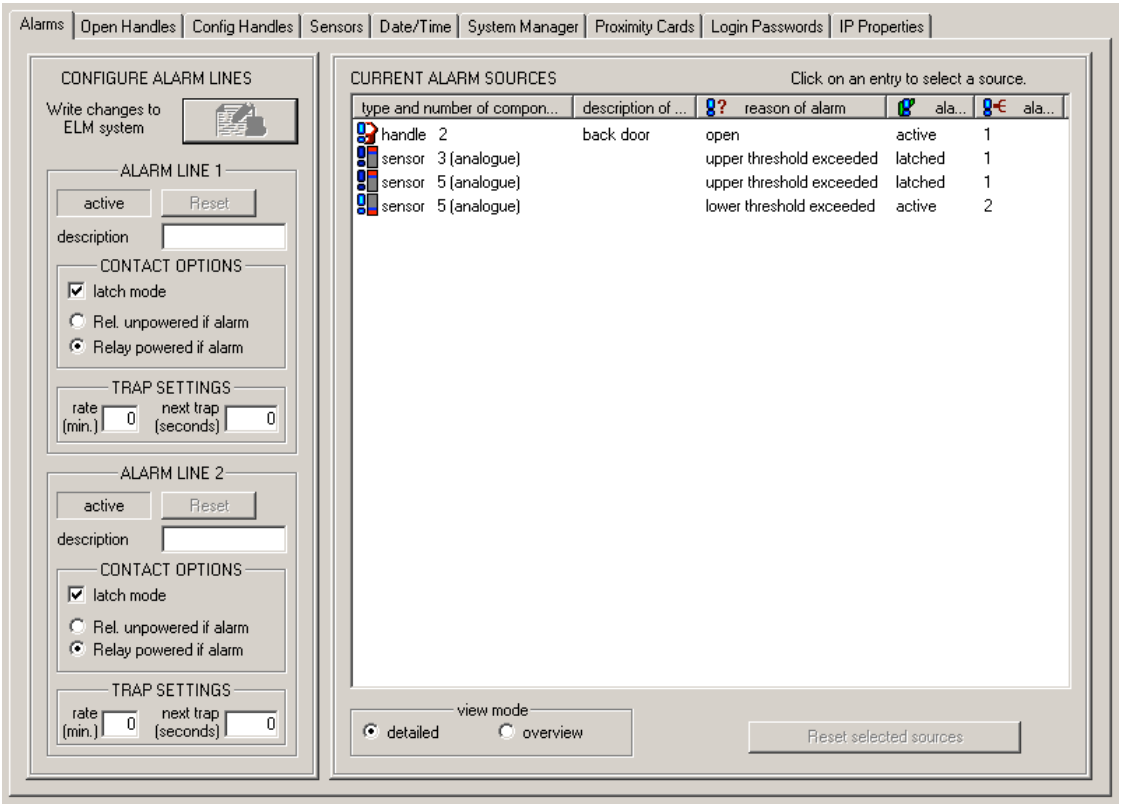


Every alarm line can show one of the following states:

Alarm status	***Meaning***
idle	No alarm.
active	At least one alarm source connected to this alarm line reports active alarm.
latched	At least one alarm source connected to this alarm line reports latched alarm. No component connected to this alarm line reports an active alarm.
?	The status of alarm is unknown. *ELMcontrol* has not yet read all necessary information from the system, i.e. the scan process is not complete.

The **Alarms** tab allows the configuration of the alarm lines and shows the current source of alarm.

- Click on the index tab **Alarms**. You get to the displayed window.



The **CONFIGURE ALARM LINES** area of the index card **Alarms** shows the current status and the configuration of both alarm lines. It allows the configuration of the following settings:

Description
Enter text up to 31 characters.

latch mode (**CONTACT OPTIONS** area)
This check box shows if alarm shall continue to be reported if all alarms of all components connected to this alarm line are discontinued. With the setting **latch mode** the alarm line is switched over to the alarm status **latched** after all connected components are transformed to the status **idle.** Otherwise the alarm line reports **idle**.

Use the **Reset** button to change alarm lines from the **latched** status to the **idle** status. The reset is carried out immediately.

Relay unpowered/powered if alarm (**CONTACT OPTIONS** area)
This button determines if the relay of the alarm line is powered with an **active** or **latched** alarm status, or whether the relay is powered with an **idle** alarm status. The last setting allows a transmission of an alarm report if the system is switched off.

trap rate (area **TRAP SETTINGS**)
Trap mode and time interval for sending SNMP-traps at changes of state of the alarm line.
The following values are possible:

- 0: The alarm line does not send any SNMP-trap (default)
- 1: At each change of the alarm line a trap is sent once.
- 2 .. 250: At each change of the alarm line one trap is sent. But this trap is then repeated every 2 .. 250 minutes.

next trap (area **TRAP SETTINGS**)
At trap rate settings of 2 .. 250 this is the time up to the next trap (in seconds). In this case you may overwrite this value and so e.g. trigger the next SNMP-trap for test purposes at another time.

- After the desired changes have been made, click on the button **Write changes to ELM system**, to save the new settings in the system.

The **CURRENT ALARM SOURCES** area of the index card **Alarms** contains a list of all components of the system that are current alarm sources. Every line describes an alarm source or the cause for alarm. Components which can release several alarms may be listed multiple times.

The **View mode** can be a multi-column **Overview** or a list with all **Details** (shown). You can also sort the list by clicking on the top of each column. With another click on the same place the order of sequences is reversed.

The table contains the following information:

Type and Number
The entry contains the type of component (handle) of the alarm source and the identification number of the component.

Status symbol
On the left hand side beside the types you find a symbol that informs about the current status of the alarm source (operating status, alarm status). The status symbols depend on the type of component. The meaning of the symbol is explained in the chapters dealing with the configuration of the components.

The view mode **Overview** shows only the type, the number, and the status symbol of every alarm source.

Description
Includes the description for the components of the alarm source if a description was entered when the components were configured.

Reason of alarm
The cause for alarm is shown.

Alarm status
The alarm source can be in the alarm states **active** or **latched**. The meaning of these states is explained in the sections dealing with the configuration of the components.

Alarm line
Shows the number of the assigned alarm lines.

Alarm sources in the alarm status **latched** can be switched over to the alarm status **idle** by clicking the **reset selected sources** button.

- First select the desired source by left clicking the desired row in the table with the mouse. With the control key (Ctrl) or the shift key being pressed at the same time you can select several entries or areas or paragraphs.

Click on the key **Reset selected sources**

7.10. Event Log

In the lower part of the user interface certain events, relevant processes, warnings and errors are shown and recorded. There are two categories of events listed in the *ELMcontrol*-protocol:

- Events which were caused by the *ELMcontrol* software (*ELMcontrol*-Event).
- Events which took place in a system and have been saved by the system - for the time being - in an internal protocol memory (ELM system-Event).

The entries into the ELM system-event log memory are read and logged by *ELMcontrol*. The event log-memory of the system is a ring type memory. If the memory is filled completely, the oldest event will be overwritten by a new event which needs to be saved. As soon as *ELMcontrol* recognizes that the log is full, it puts a corresponding note into the *ELMcontrol* –protocol that no further ELM system-Events could be registered.

7.10.1. Format of Log Entries

Every entry to the protocol (data log) consists of one line and comprises several paragraphs. The individual paragraphs are separated from each other by semicolon.

A log entry contains the following paragraphs:

ELMcontrol-Event

Paragraph	Format	Subject
1	Year/Month/Day (YYYY/MM/DD)	Date of *ELMcontrol* -Protocol entry (ELMcontrol-date)
2	Hour:Minute:Seconds (HH:MM:SS)	Time of the entry to the *ELMcontrol* (ELMcontrol-time)
3	Text in brackets	Name of the selected system
4	IP-Address	IP-Address of the selected system
5	Text in brackets	Explanations of the event

ELM System-Event

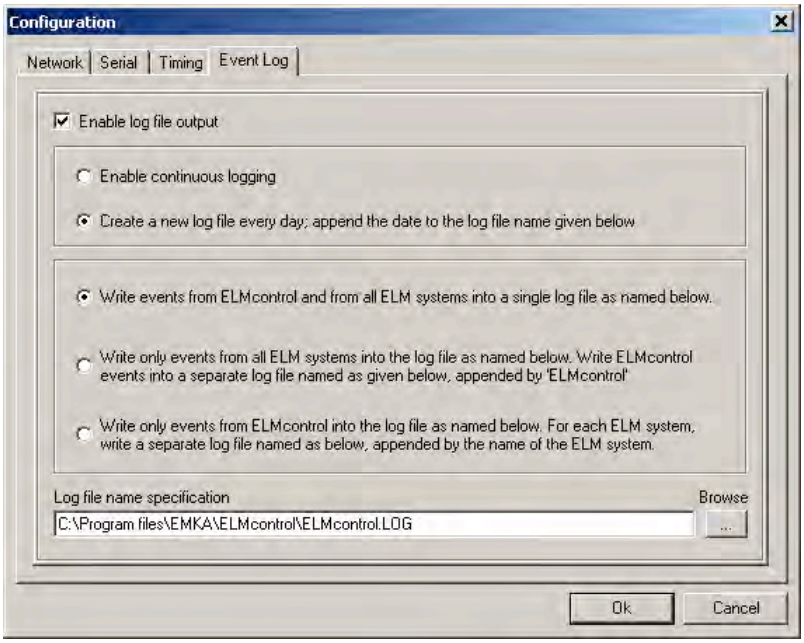
Paragraph	Format	Subject
1	Year/Month/Day (YYYY/MM/DD)	Date of *ELMcontrol* -Protocol entry (ELMcontrol-date)
2	Hour:Minute:Seconds (HH:MM:SS)	Time of the entry to the ELMcontrol (ELMcontrol-time)
3	Text in brackets	Name of the selected systems
4	IP Address	IP Address of the selected systems
5	"ELM system"	Further paragraphs contain information on ELM system-events
6	Number	Number of the event in the system-Protocol memory
7	Number	Capacity of the system-protocol memory (maximal number of events saveable in the system-Protocol memory)
8	Number	Number of series of the system-protocol memory (number of series the protocol memory is newly used)
9	Year/Month/Day (YYYY/MM/DD)	Date of the entry to the system-protocol memory (ELM system-Date)
10	Hour:Minute:Seconds(HH:MM:SS)	Time of the entry into the system-protocol (ELM system-time)
11	Text in brackets	Type of event

7.10.2. Configuration of Log Files

You can save the EVENT LOG to a file by clicking the button **Write to file** in the **EVENT LOG** area on the lower left hand side of the user interface. If the check box on the button Write to File is checked (the default setting after initial installation) log entries are automatically saved in one or several text files. The files can be configured as explained below.

- Select the menu **Options** from the main menu strip.
- Select the **Configuration** menu.
- Click the **Event log** tab of the displayed window.

The following window is displayed:



The check box **Enable log file output** corresponds to the button **Write to file** in the **EVENT LOG** area of the workspace. Writing log entries to file(s) can be enabled or disabled.

The buttons below determine whether all log entries are saved into one file or whether a daily file is saved (the default after initial installation). You can also set whether events from different sources will be saved to different files (not selected after initial installation). It is possible to separate ELMcontrol events from system events and to write a separate protocol file for every system.

The input field **Log file name specification** lets you specify the path and file name for log file(s). If only one file is written, the log file uses the designated file name. Otherwise the defined name is interpreted as a base name which is completed depending on the settings with the description of the event source and/or the current date.