HSP
Hardware Service Pack
Getting Started

Copyright

Contents

1   Introduction

The Hardware Service Pack (HSP) is an ETAS product for firmware management of ETAS hardware. It is an easy to use tool for adding new functionality to the hardware.

With HSP, users can

- Check the current firmware state,
- Check the current firmware compatibility state,
- Update/ downdate the firmware and
- Get the update activities logged

of the connected ETAS hardware by an intuitive process.

1.1   What's new

For new features of this HSP version, support of new products, and for information about firmware support use in the HSP program the menu options **Help** $\rightarrow$ **Release Notes Service Package...** and **Help** $\rightarrow$ **Release Notes HSP-UT...**

1.2   Product Overview

1.2.1   Product Structure

The **H**ardware **S**ervice **P**ack is a tool for the firmware management of ETAS hardware. HSP consists of two main parts:

- HSP Update Tool (HSP-UT) and
- HSP Service Packages (HSP-SP and LABCAR-FWP).
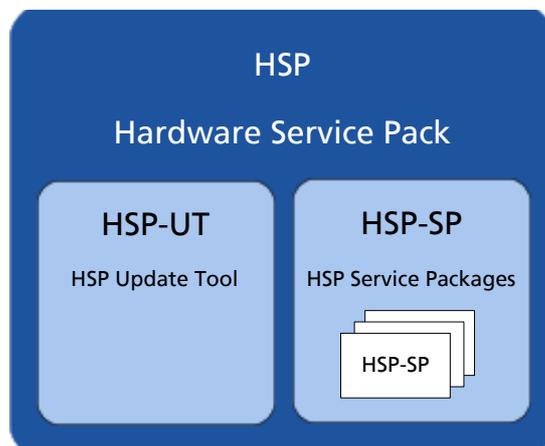
Fig. 1-1   Hardware Service Pack product structure

The **HSP U**pdate **T**ool (**HSP-UT**) is the user interface for the firmware update process. This tool allows users to view the state of firmware in a given ETAS hardware component. Based on this information, users update the firmware. Please refer to the release note for the current HSP-UT version for information about supported ETAS hardware modules.

The **HSP S**ervice **P**ackages (**HSP-SP**) contains the actual firmware, i. e. the files that will be downloaded to the hardware.

Additional the following drivers and supplements are contained in HSP:

- The **ES520 Driver (UCI)** contains the PC drivers needed by the ES520 for correct function with INCA and HSP-UT.

- The **ES580 (CAN and J2534)** contains the PC drivers needed by the ES580 (CAN-LINK II) for correct function with INCA.

- The **ES581.3 (CAN and J2534)** contains the PC drivers needed by the ES581.3 for correct function with a SW application, e.g. INCA, HSP-UT, etc.

- The **ES581.4 (USB and J2534)** contains the PC drivers needed by the ES581.4 for correct function with a SW application, e.g. INCA, HSP-UT, etc.

- The **ES582 (USB)** contains the PC drivers needed by the ES582 for correct function with a SW application, e.g. INCA, HSP-UT, etc.

- The **ES583 (USB)** contains the PC drivers needed by the ES583 for correct function with a SW application, e.g. INCA, HSP-UT, etc.

- The **ES584 (USB)** contains the PC drivers needed by the ES584 for correct function with a SW application, e.g. INCA, HSP-UT, etc.

- The **ES63x** component contains new sensor lines for the ES63x Lambda Module supporting new Lambda sensors.

- The **ES5xx/ES8xx/ES9xx** driver installation: Since INCA V7.1 INCA service packs automatically install the most recent version of ETAS ECU and Bus Interfaces Distribution Package (ED-EBI and EBI-IP). You may need to execute the ETAS ECU and Bus Interfaces installations manually only if you use Non-ETAS software that supports ETAS hardware.

- The **LambdaConfigTool** component contains the configuration tool "LambdaConfigTool" for the LA3/LA4 Lambda Meter. This tool is independent from the HSP-UT.

1.2.2   Product Versioning

The version of the Hardware Service Pack (HSP) is changed if either HSP Update Tool (HSP-UT) or if any of the HSP Service Packages (HSP-SP) was changed.

1.2.3   Product Feature

The main features of HSP Update Tool are:

- Detailed information about firmware status for several systems available
- Detailed information about software application and firmware compatibility
- After selection of product group firmware update in three steps only
- Free selection of the systems for firmware update among the displayed hardware
- User information by icons for easy readability of firmware status
  - for the complete system
  - for each updateable component in the system
- Icons are changing during the update process their status
- Up to 64 systems can be updated within the same update process
- Log files documents the updates
- Program window layout is configurable
- Integrated online help

1.3   User Information

1.3.1   User Profile

This manual is intended for qualified personnel working in the fields of automotive control unit development and calibration.

HSP users should be familiar with the operating system Microsoft Windows. All users should be capable of executing menu functions, activating buttons etc. Users should also be acquainted with the Windows file storage system, particularly the relations between files and directories. The user must know about and have mastered the basic functions of the Windows File and Program Manager and Windows Explorer. The user should also be familiar with "Drag & Drop".

All users who are not familiar with the basic techniques of Microsoft Windows should familiarize themselves with them before using HSP. Details of working with Windows are contained in the relevant manuals by Microsoft Corporation.

1.3.2   Structure of the Documentation

The HSP documentation consists of an online help which describes the operation, and a Getting Started manual. This manual describes installation, contains an overview of the most important features of operation, and background information.

The HSP Getting Started consists of the following chapters:

- "Introduction" (this chapter),
- "Program Installation" on page 11,
- "Using the HSP Update Tool" on page 17,
- "ETAS Network Manager" on page 20,
- "ETAS Contact Addresses" on page 40 and
- "Index" on page 41.

1.3.3   HSP Online Help - Quick Guide

Use the **Help** → **Help** menu option to invoke the general help function. Press the <F1> function key to call context-sensitive help.

The **Help** → **Quick Start** menu option and the **Help** → **Symbols** menu option gives an direct access to online help topics.

The **Help** → **Technical Suppor**t menu option opens an info box about HSP support (hotline contact).

The **Help** → **Supported Hardware** menu option gives an direct access to an overview of supported hardware.

The **Help** → **Release Notes HSP** menu option, the **Help** → **Release Notes HSP-UT** menu option gives an direct access to the HSP Releases Notes or to the HSP-UT Release Notes.

The **Help** → **User's Guide ES580** menu option opens the ES580 User's Guide.

The **Help** → **Info ...** menu option gives information about the HSP Update Tool version and additional tool installed components.
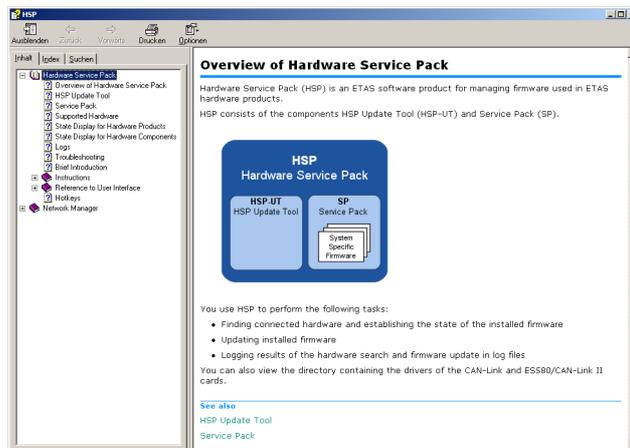
The three tabs of the help window provide you with the following options:

- The "Contents" tab allows you to browse the help topics by categories.
- The "Index" tab lists all index entries. Browse the entire list, or enter a search term to limit the scope of listing.
- The "Search" tab allows you to search for individual words or terms included in a help topic. Type a search string and let the help function list the entries it has found related to this term.

1.3.4 Working with the Manual

Getting Started is available electronically and can be viewed on the screen at any time. Using the index, full-text search, and hypertext links, you can find references fast and conveniently (see `HSP GettingStarted-En.pdf`).

Presentation of Information

All actions to be performed by the user are presented in a so-called "Use-Case" format. This means that the objective to be reached is first briefly defined in the title, and the steps required to reach the objective are then provided in a list. This presentation appears as follows:

Definition of Objective:

Any preliminary information...

- Step 1

  Any explanation for Step 1...

- Step 2

  Any explanation for Step 2...

- Step 3

  Any explanation for Step 3...

Any concluding remarks...

Specific example:

To create a new file:

When creating a new file, no other file may be open.

- Choose **File** → **New**.

  The "Create file" dialog box is displayed.

- Type the name of the new file in the "File name" field.

  The file name must not exceed 8 characters.

- Click **OK**.

The new file will be created and saved under the name you specified. You can now work with the file.

Typographical Conventions

The following typographical conventions are used in this document:

Select **File** → **Open**	Menu commands are shown in boldface.
Click **OK**	Buttons are shown in boldface.
Press <ENTER>	Keyboard commands are shown in angled brackets, in block capitals.
The "Open File" dialog box is displayed.	Names of program windows, dialog boxes, fields, etc. are shown in quotation marks.
Select the file `setup.exe`.	Text in drop-down lists on the screen, program code, as well as path and file names are shown in the Courier font.

Important notes for the user are shown as follows:

Note

Important note for the user.

2 Program Installation

2.1 Overview

2.1.1 Program Files and Windows User Rights

Main Installation File (HSP)

The HSP main installation file installs the Hardware Service Pack including the HSP-UT and HSP-SP.

> **Note**
>
> *You need Windows administrator rights for installing the Hardware Service Pack HSP.*

You can install HSP in localized versions of the Graphical User Interface (GUI).

Service Package Files (HSP-SP)

If a compatible HSP version is installed on your PC there is the possibility to install additional HSP Service Packages (HSP-SP) with Windows standard user rights.

> **Note**
>
> *For installing the HSP Service Packages you need only Windows standard user rights.*

2.1.2 Documentation

A printed version of the HSP documentation is not available. All HSP documentation is available in Adobe PDF file format. To read and print the manuals use the Adobe Acrobat Reader.

File	Description
`HSP-UT ReleaseNotes-En.pdf`	HSP Update Tool release notes (only english language)
`HSP-UT ReleaseNotes-Jp.pdf`	HSP Update Tool release notes (only japanese language)
`HSP GettingStarted-En.pdf`	HSP Getting Started (this document)
`HSP GettingStarted-Jp.pdf`	HSP Getting Started (this document in japanese language)

2.1.3   System Requirements

Item	Description
Required PC hardware (IBM-compatible)	2 GHz Dual-Core PC, 2 GByte RAM, Network adapter, Graphics (1280 x 1024), 128 MB RAM
Required operating system	Windows 10, Windows 8.x, Windows 7 (32-bit version or 64-bit version in 32-bit compatibility mode)
Free disk space	2 GByte

Note

The CPU as well as the main memory requests must satisfy the minimum requirements of the used operating system.

2.1.4   Restrictions

Operating system

Product release tests were performed under Windows 7 and Windows 8.x. No tests were performed on multi-processor machines.

Using multiple masters

When updating the ETAS hardware with HSP no access by other ETAS applications may be carried out on this hardware.

Windows User Rights

For restrictions because of Windows user rights refer to chapter 2.1.1 on page 11.

Using some hardware components

HSP-UT does not support the CAN-Link II or ES580 card. HSP-UT cannot detect the presence of the card and consequently cannot update its firmware.

Note

For complete description of restrictions by using some hardware components refer to the HSP Update Tool Release Notes.

2.1.5   Supported ETAS Products

Read the list of supported hardware or the HSP Update Tool release notes for detailed informations.

2.2   Installation Procedure

2.2.1   Installing HSP

Note

You need Windows administrator rights for installing the Hardware Service Pack HSP.

There is no difference in procedure between HSP installation from a CD and from a network drive.

To start the HSP installation:

- Double click on the setup.exe file in the HSP installation package.
- Follow the instructions displayed by the installation wizard.

Note

The language selection made in the HSP installation is a global setting for all ETAS applications

2.2.2   Installing HSP Service Packages (HSP-SP)

If a compatible HSP version is installed on your PC it is possible to install additional Service Packages (HSP-SP) with Windows standard user rights.

Note

For installing the HSP Service Packages you need only Windows standard user rights.

The HSP Service Packages are available for all users of a PC, i.e. all installed packages are available for selection in the HSP-UT regardless of user.

The file format of all HSP Service Package files is "*.spi".

There are three ways to select, import and install the HSP Service Packages:

- select and click an HSP-SP file "*.spi" in Windows Explorer

   or

- select in HSP program "File → Import Service Package"

   or

- select in HSP program "Tools → Service Package Manager".

Note

The complete handling to install HSP Service Packages is described in the Online Help of HSP.

2.3   LAN handling Support

The Hardware Service Pack supports the improved LAN handling of INCA with different configurations for hardware access by Ethernet:

- Usage of different network adapters:
    - one network adapter for the company LAN and
    - one network adapter for the ETAS-Hardware or
- Usage of one network adapter:
    - automatic switch between company LAN and usage in automotive.

For working with HSP it is necessary to configure the network environment of your PC for the ETAS hardware. The ETAS Network Manager supports your configuration.

To start ETAS Network Manager:

- Select in the HSP Main Window start menu **Tools** → **ETAS Network settings**.

  The ETAS Network Manager is started.

To select a network adapter:
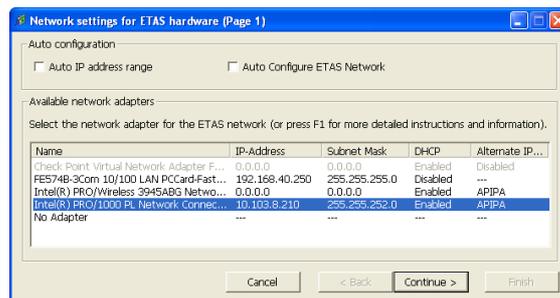
- Select a network adapter from the "Available Network Adapters" field.
- Make the necessary settings in the "Network Settings for ETAS hardware" window.
- Click **Finish**.

Details for using ETAS Network Manager are described in chapter 4 on page 20.

2.4   Uninstall Procedure

2.4.1   Uninstalling HSP

> **Note**
>
> *Windows administrator rights are required for uninstalling the HSP (HSP-UT with all HSP-SP files).*

This procedure describes how to uninstall the HSP Update Tool and all installed Service Packs.

To uninstall HSP:

- Select in the Windows start menu **Start** → **System Control** → **Programs and Functions**.
- Select **HSP Update Tool**.
- Click **Uninstall**.

  The Windows Installer window is displayed:
- Click **Yes** to start the HSP uninstallation.

  The uninstall process is started.

2.4.2   Uninstalling HSP Service Packages (HSP-SP)

> **Note**
>
> *For uninstalling of selected HSP Service Packages you need only Windows standard user rights.*

Using the HSP Service Package Manager as a part of HSP all users can uninstall a selected HSP Service Package version (e.g. previous/older released service package) without uninstalling the HSP-UT.

> **Note**
>
> *The complete handling to uninstall HSP Service Packages is described in the Online Help of HSP.*

2.5   Lambda Meter Configuration Tool

The Hardware Service Pack contains also the ETAS "Lambda Meter Configuration Tool". The "Lambda Meter Configuration Tool" enables the firmware update of the LA3 / LA4 modules, allows convenient setting of modules' parameters and offers the opportunity to download customer specific characteristic curves. The HSP installation procedure automatically installs the "Lambda Meter Configuration Tool" into the HSP directory on the PC.

To start Lambda Config Tool:

- Select in the Windows start menu **Start** → **Programs** → **ETAS** → **HSP** → **Supplements** → **Lambda Meter Configuration Tool.**

  The "Lambda Config Tool" is started.

3   Using the HSP Update Tool

This section describes how to update the firmware on ETAS hardware.

In this manual, the word 'update' is used to describe the process of downloading a binary file, the actual firmware, from the PC to dedicated memory in ETAS hardware. The downloaded firmware does not necessarily have to be a newer version than the firmware originally located on the hardware.

3.1   Starting the HSP Update Tool (HSP-UT)

The HSP-UT can be started either by double-clicking the HSP-UT icon on the desktop or from the **Start** menu under **Programs** → **ETAS** → **HSP** → **HSP Update Tool**. The "HSP Update Tool" window of the HSP-UT opens. In the following description this window is named "Main" window.

When you select a particular version of the Hardware Service Pack, you are automatically selecting the matching version of the Service Package, i. e. the actual firmware used by the HSP-UT.
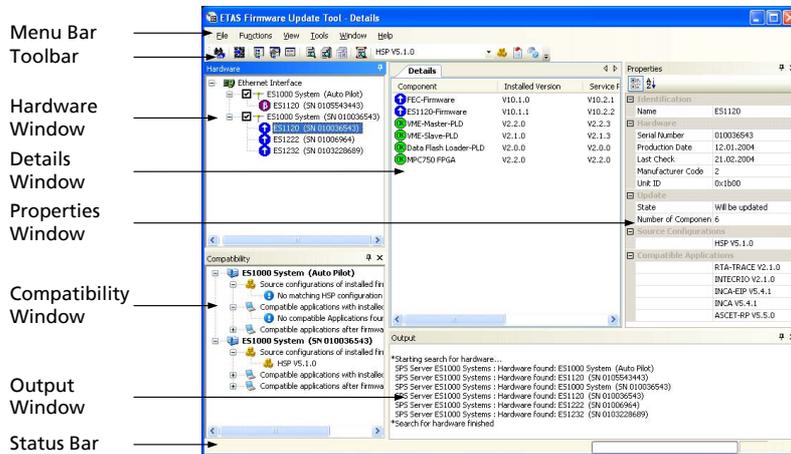
Please refer to the HSP online help for details on menu options and button functionality.

> **Note**
>
> *Before starting the HSP-UT please make sure that no ETAS Target Server is active, i. e., that no Target Server icon is visible in the Windows task bar.*

3.2   "HSP Update Tool" Window

The "HSP Update Tool" window is also named "Main" window.

3.3   Update Procedure

The sequence for updating the firmware is dependent on number of ETAS systems connected on the PC:

1. Connect the hardware to the PC and to power supply

> **Note**
>
> *Neither the power supply nor the Ethernet connection may be interrupted during a firmware update!*

2. Select the HSP version[1] or the LABCAR-FWP version[2]

3. Click "Search for hardware"

4. Checking the firmware state and select hardware systems whose firmware you want to update

5. Start firmware update

6. Additionally you can check the current firmware state of one of the connected hardware systems after a hardware search operation was done.

7. Quit the HSP Update Tool after firmware check or update is completed.

3.4   Document the Firmware State

The HSP Update Tool automatically creates two types of log files, the "Firmware State Log File" and the "Firmware History Log File", offering the possibility to document the firmware state and the firmware update activities.

Contents of the log files can be viewed within HSP-UT window. As the files are in plain text format, they can simply be printed using text editors like Notepad.

3.4.1   Firmware State Log File

This feature makes it possible to document the current firmware state or a specific update sequence, i. e. the firmware state before and after the firmware update.

The Firmware State Log File will automatically be created the first time a search for hardware will be performed after installation of HSP. Afterwards this file will be overwritten with every search for hardware performed. If a successful update follows on a search for hardware the content will be appended with this information.

The content of the latest successfully executed update will remain when restarting HSP.

3.4.2   Firmware State History Log File

This feature makes it possible to "browse" the history on successfully executed firmware updates.

The Firmware State History Log File will also be automatically created the first time an update has been done after installation of HSP and contains all previous versions of the firmware state log file. If a new firmware state log file is created, the content of this file is appended at the beginning of the history file.

[1.] only HSP version V6.1 and higher
[2.] only HSP version V7.0 and higher

When required it is possible to delete the content of this file. There is a maximum allowed size for this file. When the size reaches 500 kB the oldest update information will be truncated.

3.5   Driver Installation

3.5.1   ES520 Driver Installation

If there is no ES520 driver (UCI) installed on your PC or an installed driver is not up to date you can install the required driver which is delivered with HSP. The installed driver allows to perform a firmware update on your ES520 hardware and to use it with ETAS software on this PC.

3.5.2   ES580 or CAN-Link II Card Driver Installation

If there is no ES580 or CAN-Link II card driver installed on your PC or an installed driver is not up to date you can install the required driver which is delivered with HSP. The installed driver allows to perform a firmware update on your ES580 or CAN-Link II card hardware and to use it with ETAS software on this PC.

The driver is available in a 32-bit- and 64-bit version.

3.5.3   ES581 and ES581.4 Driver Installation

If there is no ES581 driver (USB) installed on your PC or an installed driver is not up to date you can install the required driver which is delivered with HSP.

The installed driver allows to perform a firmware update on your ES581 hardware and to use it with ETAS software on this PC.

Users of the ES581 with third party applications have additionally to install an J2534 conform driver (Pass Thru Interface) which is also delivered with HSP.

3.5.4   ES583.1 Driver Installation

If there is no ES583.1 driver (USB) installed on your PC or an installed driver is not up to date you can install the required driver which is delivered with HSP.

The installed driver allows to perform a firmware update on your ES583.1 hardware and to use it with ETAS software on this PC.

3.5.5   ES5xx/ ES8xx/ ES9xx Driver Installation

Since INCA V7.1 INCA service packs automatically install the most recent version of ETAS ECU and Bus Interfaces (ED-EBI and EBI-IP). You may need to execute the ETAS ECU and Bus Interfaces installations manually only if you use Non-ETAS software that supports ETAS hardware.

3.6   Quit the HSP Update Tool

Quit the HSP Update Tool after firmware check or update is completed.

Note

Leaving the tool running may interfere with other ETAS applications.

4   ETAS Network Manager

The ETAS Network Manager is used for creating a configuration that will be used by the ETAS IP Manager. The IP Manager is responsible for dynamic IP addressing of the ETAS hardware used in your network.

4.1   Overview

ETAS software supports different configurations for hardware access via Ethernet:

- Using multiple network adapters:
    - one network adapter for the company network,
    - one or more network adapters for the ETAS hardware.
- Using one network adapter
    - automatic toggling between the company network and the ETAS hardware.

Note

You do not require a separate network adapter to connect the ETAS hardware to your PC. You can use the same network adapter both for the company network and the ETAS network.

The ETAS Network Manager supports you in selecting the network adapter for the ETAS hardware.

The ETAS Network Manager gives you an overview of the network adapters available for your PC and the type of IP address assignment. If more than one network adapter is available in the system, you can select the network adapter to use for connecting the ETAS hardware to your PC. You can also specify the address range for the IP assignment for the ETAS hardware.

You do not need administrator rights to select the network adapter and the network environment configuration for the ETAS hardware. You can toggle between the ETAS network and the company network without rebooting your PC.

Note

With Network Manager, you cannot create or modify the configuration for the network adapter. Instead modify the network settings of your PC via the Control Panel (see the documentation for your operating system).
Please note that this requires administrator rights.

4.2   ETAS Hardware Addressing

The ETAS network allows you to connect several devices (including those that are the same type) to your PC. The connected devices are identified in the local ETAS network by their unique IP address.

An IP Manager integrated in the ETAS software looks up which IP addresses are available in a pre-configured address pool and assigns available IP addresses to the connected ETAS hardware.

The address range for the address pool is specified using the ETAS Network Manager.

4.3   Network Adapter Addressing

4.3.1   Type of Network Adapter Addressing

The type of network adapter addressing done within the company network depends on the operating system being used and the network adapter configuration:

Operating System	Type of Network Adapter Addressing			
	Manual	DHCP	DHCP+APIPA	DHCP+ alternative IP address
Windows XP	yes	yes	yes	yes
Windows Vista	yes	yes	yes	yes
Windows 7	yes	yes	yes	yes

The ETAS network supports the following types of network adapter addressing:

Operating System	Type of Network Adapter Addressing			
	Manual	DHCP	DHCP+APIPA	DHCP+ alternative IP address
Windows XP	yes	no	yes	yes
Windows Vista	yes	no	yes	yes
Windows 7	yes	no	yes	yes

If you wish to use the network adapters both for the company network and the ETAS network, you cannot use the network adapters that exclusively support DHCP addressing for this dual operation.

Note

DHCP can be used only in combination with APIPA or an alternative IP address!

4.3.2   Addressing the Network Adapter Manually

Addressing a network adapter depends on the operating system.

For instructions on addressing your PC's network adapter, see the documentation for your operating system.

To address the network adapter manually, you need administrator rights. Please contact your system administrator, if necessary.

If the network adapter is addressed manually, i.e., it has a static IP address, it may happen that you accidentally end up searching for or initialize ETAS hardware, although the PC is connected to the company network. The Network Manager allows you to stipulate that if this happens, you are to receive a warning before an IP address is assigned to an ETAS hardware.

4.3.3 Addressing the Network Adapter via DHCP

Addressing via DHCP requires that the DHCP server be available. Should the DHCP server not be available, or if there is no DHCP server (as in the ETAS network), the network adapter has not been configured.

In this instance, each operating system has a feature that automatically assigns the network adapter an IP address:

*Windows XP / Windows Vista / Windows 7*

Windows XP, Windows Vista and Windows 7 automatically check whether there is a connection to the DHCP server. If there is none, it either assigns the IP address automatically via APIPA, or it uses the user-specified alternative IP address. The ETAS network always uses either the APIPA address or the alternative IP address.

When toggling between the DHCP network and ETAS hardware, make sure that the operating system is able to detect a connection failure because only then will reconfiguration be initiated. This may take up to 10 seconds. It takes the operating system 60 seconds to entirely reconfigure from a DHCP address to an APIPA address or to the alternative address. If the network adapter is once again connected to the DHCP network, configuring to a DHCP address takes place right after the connection has been detected.

Addressing a network adapter via DHCP without alternative addressing is not supported.

4.4 User Interface

4.4.1 Configuration Dialog Window 1 — Selection of Network Adapter ("Network settings for ETAS hardware (page 1)")
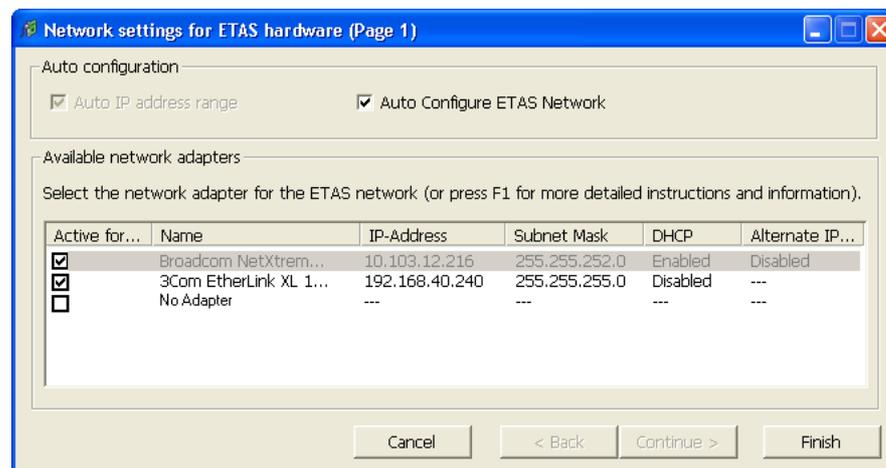
The following information on the available network adapters is displayed:

- **Auto IP Address Range** checkbox

  If you tick this checkbox, the next configuration step is skipped, and the ETAS Network Manager automatically assigns default IP address ranges that will be used by the selected network adapter for addressing the ETAS hardware. If the IP address range is automatically changed by the IP Manager, a message is displayed in the system tray.

- **Auto Configure ETAS Network** checkbox

  If you tick this checkbox, you can enable or disable several network adapters at once for auto-configuration through the IP Manager.

  When you tick the checkbox, the "Auto IP Address Range" checkbox is activated. In the list of available network adapters, the "Active for ETAS Network" column is inserted, where you can determine which network adapters shall be available for auto-configuration through the ETAS Network Manager.

  The ETAS Network Manager will go through the list (top-down) and use the first adapter which has a valid IP configuration for ETAS[1] and configure the IP address range automatically. If a configured network adapter fails, e.g. because the network adapter is being disabled or physically not available, the IP Manager will configure the next available network adapter automatically, and a message is displayed in the system tray, indicating the new configuration.

- **Active for ETAS Network** column

  This column is only visible if the "Auto Configure ETAS network" checkbox is ticked. In the checkbox in this column you can determine which network adapters shall be enabled for autoconfiguration by the ETAS Network Manager (see „Auto-Configuring Network Adapter for ETAS Hardware" on page28).

- **Name** column

  Name of the network adapter. This entry cannot be edited in this window.

  This column also contains an entry with the name "No Adapter". If you want to disable the IP Manager, e.g. because there is no Ethernet hardware connected to the PC, you can tick this entry in the "Active for ETAS Network" column.

- **IP Address** column

  IP address of the network adapter. This entry cannot be edited in this window.

- **Subnet Mask** column

  Setting for the subnet mask. This entry cannot be edited in this window.

- **DHCP** column

  Shows whether the network adapter is configured for DHCP:
 - Enabled

    The network adapter is configured for DHCP.
  - Disabled

    The network adapter is configured with a fixed IP address.

- **Alternate IP Configuration** column

  Shows the alternative IP address of the network adapter if it is configured for DHCP. This indication depends on the operating system being used.

[1.] An IP configuration is valid if the network adapter either uses a fix IP address, or if DHCP and APIPA are enabled.

– APIPA

Automatic Private IP Addressing: method for automating the IP config-uration for network connections

– ---

An alternative IP address does not exist.

– User defined

The user can define a user-specific alternative IP address.

4.4.2   Configuration Dialog Window 2 — Defining the Address Pool
("Network settings for ETAS hardware (page 2)")
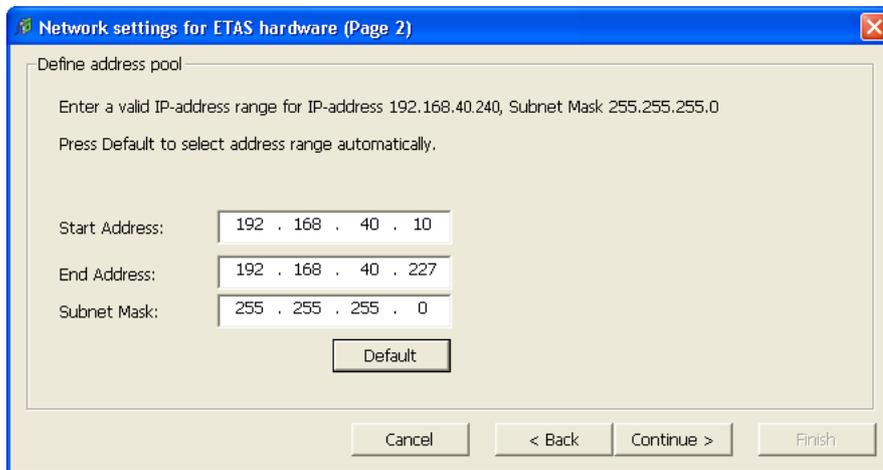
In general, all values can be modified by directly typing them in the correspond-ing field, or by selecting the default setting from a list box.

The following network parameters can be set:

• **Start Address**

The first IP address in the IP address range for the ETAS hardware

• **End Address**

The last IP address in the IP address range for the ETAS hardware

• **Subnet Mask**

Associated Subnet Mask

Reserved IP Addresses

The following IP addresses are reserved for certain ETAS hardware in the IP address range that the ETAS hardware (192.168.40.1 - 192.168.40.254 with Subnet Mask 255.255.255.0) is currently using:
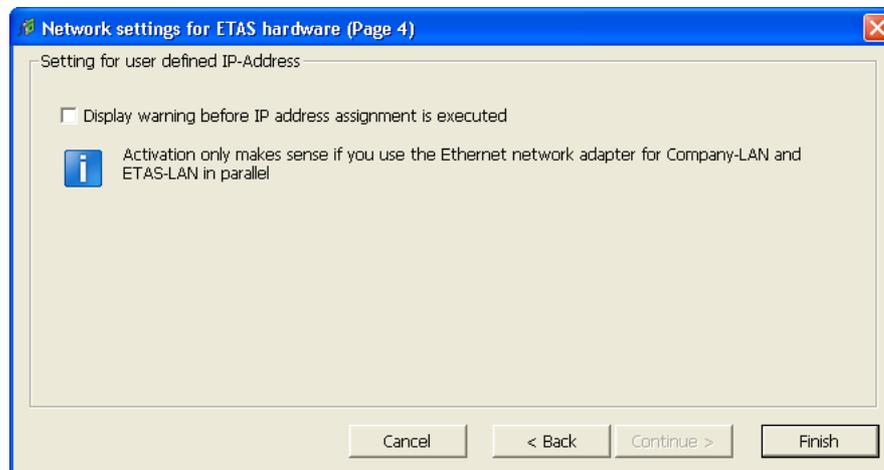
IP_Address	ETAS Hardware
192.168.40.10	ES1120
192.168.40.11	ES1130
192.168.40.12	ES780

IP_Address	ETAS Hardware
192.168.40.13	Reserved
192.168.40.14	LABCAR-RTPC
192.168.40.15	ES1135

These addresses are assigned exclusively to these devices and thus may not be used for other ETAS hardware. This has to be taken into consideration when defining the address pool.

4.4.3   Configuration Dialog Window 4 — Displaying Warning ("Network settings for ETAS hardware (Page 4)")

This dialog window appears only if the selected network adapter is addressed manually.

The following parameters can be set:

- **Display warning before IP address assignment is executed**

  Use this checkbox to specify that a warning be displayed before an IP address is assigned to an ETAS hardware device.

Note

Enabling this warning is useful only if you want to run the PC both in the company network or on an ETAS measurement module in the ETAS network using this network adapter.
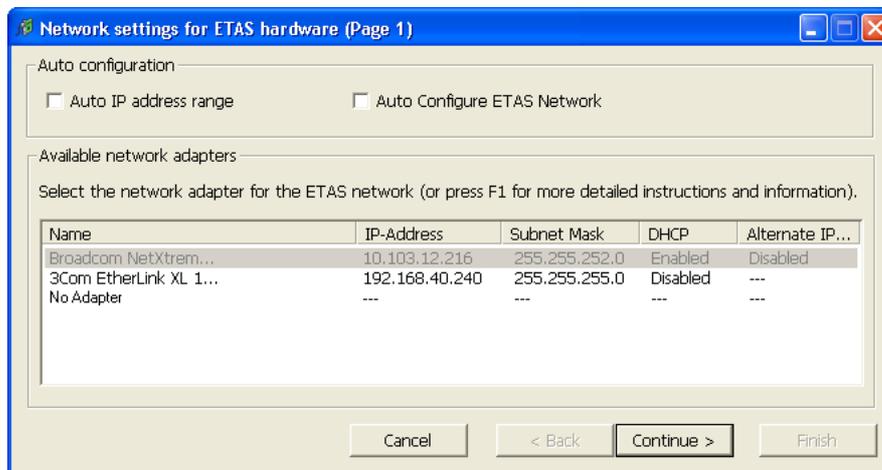
4.5   Configuring Network Addresses for ETAS Hardware

4.5.1   Manually configuring the Network Adapter

To configure the network adapter for ETAS hardware:

1. In the Windows Start menu, go into the program folder of your ETAS software (below **Start** → **Programs** → **ETAS**), and select **ETAS Network Settings.**

   The "Network settings for ETAS hardware (Page 1)" dialog window is opened.


2. In the "Available Network Adapters" area, select the network adapter you want to use for the corporate network and the ETAS network. If no network adapter is installed on the PC, the dialog window contains no entries.

   Note

   The type of addressing of the network adapter must be supported by the ETAS network. Otherwise, you cannot select the network adapter.

3. Click **Continue**.

    The "Network settings for ETAS hardware (Page 2)"
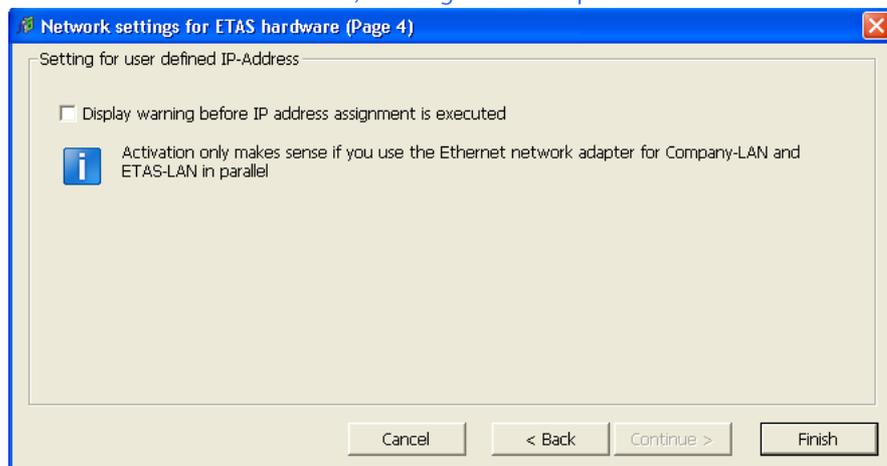   dialog window opens.
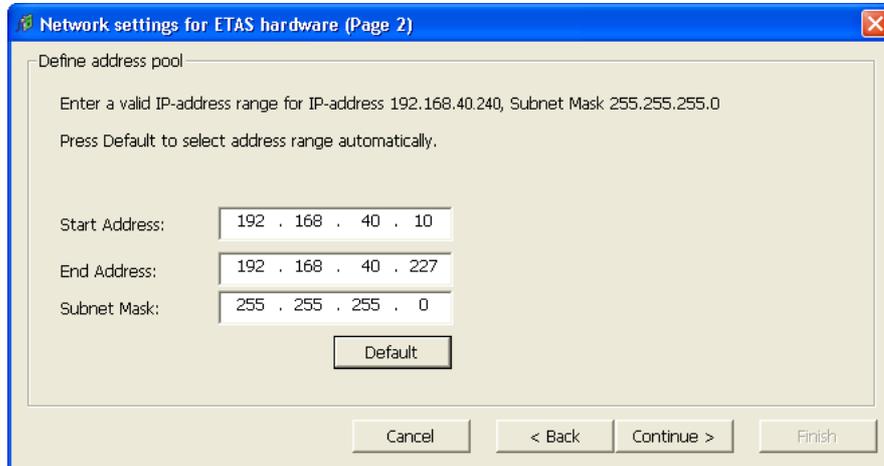
4. Enter the IP address range for the ETAS hardware
    and the subnet mask, or click **Default** to have the
    Network Manager automatically complete the IP
    address range and the subnet mask.

    You may accept these settings or overwrite them.

5. Click **Continue**.

    The "Network settings for ETAS Hardware (Page
    4)" dialog window opens.

6. If you want to define that a warning is displayed before the ETAS hardware is assigned an IP address, enable "Display warning before IP address assignment is executed".

Note

Enabling this warning is useful only if you want to run the PC both in the company network or on an ETAS measurement module in the ETAS network using this network adapter.

7. Click **Finish**.

8. Restart the ETAS software to make the changes become effective. If the Network Manager was started automatically during a hardware search or initialization, you do not have to restart the ETAS software to apply the changes.

4.5.2   Auto-Configuring Network Adapter for ETAS Hardware

The ETAS Network Manager offers the automatic assignment of IP address ranges in the ETAS network through the IP Manager. You can either use auto-configuration of a selected network adapter, or, if more than one network adapter is available, let the IP Manager auto-configure the ETAS network, including the selection of the adapter to be used.

How to auto-configure a selected network adapter for ETAS hardware

1. In the Windows Start menu, go into the program folder of your ETAS software (below **Start** → **Programs** → **ETAS**), and select **ETAS Network Settings.**

   The "Network settings for ETAS hardware (Page 1)" dialog window is opened.
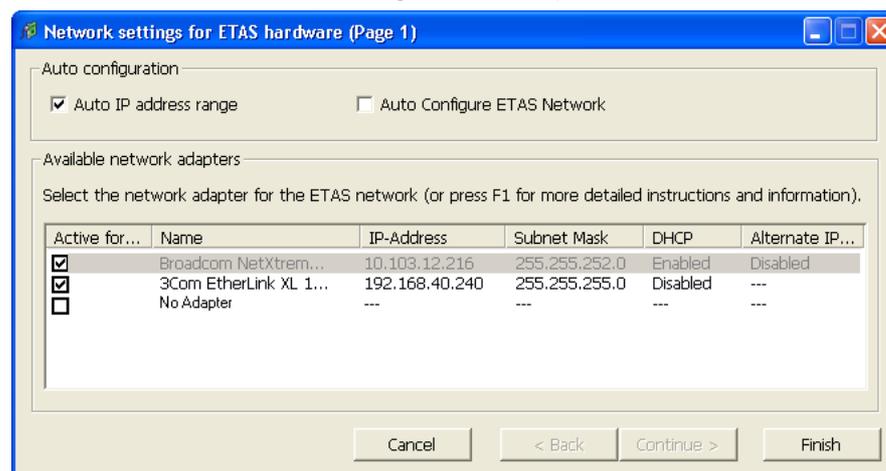
2. In the "Available Network Adapters" area of the "Network settings for ETAS hardware (Page 1)" dialog window, select the network adapter you want

to use for the corporate network and the ETAS net-
work. If no network adapter is installed on the PC,
the dialog window contains no entries.

> **Note**
>
> *The type of addressing of the network adapter must
> be supported by the ETAS network. Otherwise, you
> cannot select the network adapter.*

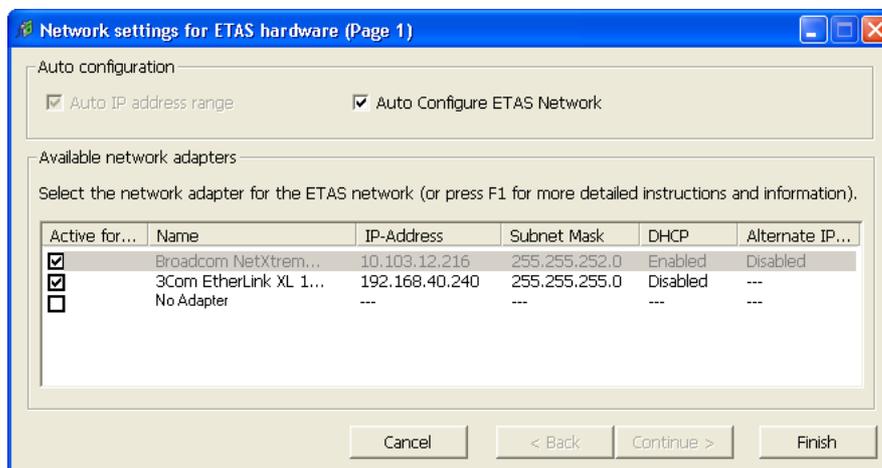3. Tick the "Auto IP Address Range" checkbox.

4. Click **Finish**.

The ETAS Network Manager automatically assigns
default IP address ranges that will be used by the
selected network adapter for addressing the ETAS
hardware.

If later on, the IP address range is automatically changed by the IP Manager, a
message is displayed in the system tray.

**How to auto-configure a network adapter, with multiple network adapt-
ers being available**

1. In the Windows Start menu, go into the program
folder of your ETAS software (below **Start**   → **Pro-
grams**   → **ETAS**), and select **ETAS Network Set-
tings.**

The "Network settings for ETAS hardware (Page 1)"
dialog window is opened.

2. In the "Network settings for ETAS hardware (Page
1)" dialog window, tick the "Auto Configure ETAS
Network" checkbox.

The "Auto IP Address Range" checkbox is activated,
and in the list of available network adapters, the
"Active for ETAS Network" column is inserted.

3. Enable all network adapters that shall be available for auto-configuration through the IP Manager by ticking the corresponding checkbox in the "Active for ETAS Network" column.

4. Click **Finish**.

Starting with the network adapter that is currently selected in the dialog window, the ETAS Network Manager will go through the list (top-down), and use the first adapter which has a valid[1] IP configuration for ETAS and configure the IP address range automatically. If a configured network adapter fails, e.g. because the network adapter is being disabled or physically not available, the IP Manager will configure the next available network adapter automatically, and a message is displayed in the system tray, indicating the new configuration.

4.5.3   Enabling APIPA in the Registry

Note

You need administrator rights to make changes in the Registry.

To enable APIPA in the Registry:

1. Click **Start**, and then click **Run**.

2. Enter regedit, and click **OK**.

    The Registry editor opens.

3. Click the entry for a network adapter in the Registry key:

    Global key (refers to all network adapters)

    HKEY_LOCAL_MACHINE\SYSTEM\
    CurrentControlSet\
    Services\Tcpip\Parameters

    Interface or card-specific key

    HKEY_LOCAL_MACHINE\SYSTEM\
    CurrentControlSet\
    Services\Tcpip\Parameters\
    Interfaces\adapter_name

Note

If neither of these keys exists, the APIPA mechanism is enabled. If the global key exists but is not enabled, the setting of the global key is decisive. If the global key does not exist or is set to enabled, the card-specific key is decisive.

4. Set the value for
    IPAutoconfigurationEnabled to 1.

    The APIPA mechanism is enabled.

[1.] An IP configuration is valid if the network adapter either uses a fix IP address, or if DHCP and APIPA are enabled.

4.6   Troubleshooting Ethernet Hardware Access

In certain cases you might have problems accessing ETAS hardware via the Ethernet interface. For instance, if APIPA, a mechanism for IP addressing, has not been enabled on your system, you cannot select a network adapter in the Network Manager. You can find descriptions of potential problems and their solutions in "Troubleshooting General Problems" on page 32.

5 Troubleshooting General Problems

This chapter gives some information of what you can do when problems arise that are not specific to an individual software or hardware product.

5.1 Problems and Solutions

5.1.1 Network Adapter cannot be selected via Network Manager

Cause: APIPA is disabled

The alternative mechanism for IP addressing (APIPA) is usually enabled on all Windows XP and Vista systems. Network security policies, however, may request the APIPA mechanism to be disabled. In this case, you cannot use a network adapter which is configured for DHCP to access ETAS hardware. The ETAS Network Manager displays a warning message.

The APIPA mechanism can be enabled by editing the Windows registry. This is permitted only to users who have administrator privileges. It should be done only in coordination with your network administrator.

To enable the APIPA mechanism:

- Open the Registry Editor:
  - Windows XP:
    Click **Start** and then click **Run**. Enter `regedit` and click **OK**.
  - Windows Vista:
    Click **Start**, enter `regedit` in the entry field, and push <ENTER>.

  The registry editor is displayed.

- Open the folder `HKEY_LOCAL_MACHINE\SYS-TEM\`
  `CurrentControlSet\Services\`
  `Tcpic\Parameters\`

- Click **Edit** → **Find** to search for the key `IPAuto-configurationEnabled`.

If you cannot find any instances of the registry key mentioned, the APIPA mechanism has not been disabled on your system, i.e. there is no need to enable it. Otherwise proceed with the following steps.

- Set the value of the key `IPAutoconfigurationEnabled` to 1 to enable the APIPA mechanism.

  You may find several instances of this key in the Windows registry which either apply to the TCP/IP service in general or to a specific network adapter. You only need to change the value for the corresponding network adapter.

- Close the registry editor.

- Restart your workstation in order to make your changes take effect.

5.1.2   Search for Ethernet Hardware fails

Cause: The versions of the Hardware and the ETAS MC Software are not compatible

If you are using ETAS hardware with ETAS MC software, you can use the ETAS HSP Update Tool to check the firmware version of your hardware:

- Make sure you use the ETAS HSP Update Tool with the latest HSP (Hardware Service Pack) version.

- Also use the HSP Update Tool to check whether the hardware is compatible with the MC software used.

- Make sure any additional drivers for that hardware are installed correctly.

You can get the required HSP from the ETAS internet pages under www.etas.com.

If you still cannot find the hardware using the HSP Update Tool, check whether the hardware offers a Web interface and whether you can find using this interface. Otherwise check whether one of the following causes and solutions might apply.

Cause: Personal Firewall blocks Communication

For a detailed description on problems caused by personal firewalls and possible solutions see "Personal Firewall blocks Communication" on page 35.

Cause: Client Software for Remote Access blocks Communication

PCs or notebooks which are used outside the ETAS hardware network sometimes use a client software for remote access which might block communication to the ETAS hardware. This can have the following causes:

- A firewall which is blocking Ethernet messages is being used (see „Cause: Personal Firewall blocks Communication" on page33)

- By mistake, the VPN client software used for tunneling filters messages. As an example, Cisco VPN clients with versions before V4.0.x in some cases erroneously filtered certain UDP broadcasts.

  If this might be the case, please update the software of your VPN client.

Cause: ETAS Hardware hangs

Occasionally the ETAS hardware might hang. In this case switch the hardware off, then switch it on again to re-initialize it.

Cause: ETAS Hardware went into Sleep Mode

In order to save power, some ETAS devices will go to sleep mode if they do not see that they are connected to another device/computer.

To solve that, connect your Ethernet cable from your computer to the "HOST"/ "Sync In" port on the device. After the device turns on, connect to the device using the web interface and change the settings so that the device stays always on. Consult the device's manual for details on how to do that.

Cause: Network Adapter temporarily has no IP Address

Whenever you switch from a DHCP company LAN to the ETAS hardware net-work, it takes at least 60 seconds until ETAS hardware can be found. This is caused by the operating system's switching from the DHCP protocol to APIPA, which is being used by the ETAS hardware.

Cause: ETAS Hardware had been connected to another Logical Network

If you use more than one PC or notebook for accessing the same ETAS hardware, the network adapters used must be configured to use the same logical network. If this is not possible, it is necessary to switch the ETAS hardware off and on again between different sessions (repowering).

Cause: Device driver for network card not in operation

It is possible that the device driver of a network card is not running. In this case you will have to deactivate and then reactivate the network card.

To deactivate and reactivate the network card:

- To deactivate the network card first select in the Windows start menu the following item:
  - Windows XP:
    Control Panel → **Network Connections**
  - Windows Vista:
    Control Panel → **Network and Internet** → **Network and Sharing Center**
- Right click on the used network adapter and select **Disable** in the context menu.
- In order to reactivate the network adapter right click on it again and select **Enable**.

Cause: Laptop power *management deactivates the network card*

The power management of a laptop computer can deactivate the network card. Therefore you should turn off power monitoring on the laptop.

To switch off power monitoring on the laptop:

- From the Windows Start Menu, select
  - Windows XP:
    Control Panel → **System**.
    Then select the **Hardware** tab and click on **Device Manager**.
  - Windows Vista:
    Control Panel → **System and Maintenance** → **Device Manager.**
- In the Device Manager open the tree structure of the entry **Network Adapters**.
- Right click on the used network adapter and select **Properties** in the context menu.
- Select the **Power Management** tab and deactivate the **Allow the computer to turn off this device to save power** option.

- Select the **Advanced** tab. If the property **Auto-sense** is included, deactivate it also.
- Click **OK** to apply the settings.

Cause: Automatic disruption of network connection

It is possible after a certain period of time without data traffic that the network card automatically interrupts the Ethernet connection. This can be prevented by setting the registry key `autodisconnect`.

To set the registry key `autodisconnect`:

- Open the Registry Editor.
- Select under `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\lanmanserver\parameters` the Registry Key `autodisconnect` and change its value to `0xffffffff`.

5.1.3 Personal Firewall blocks Communication

Cause: Permissions given through the firewall block ETAS hardware

Personal firewalls may interfere with access to ETAS Ethernet hardware. The automatic search for hardware typically cannot find any Ethernet hardware at all, although the configuration parameters are correct.

Certain actions in ETAS products may lead to some trouble if the firewall is not properly parameterized, e.g. upon opening an experiment in ASCET or searching for hardware from within INCA or HSP.

If a firewall is blocking communication to ETAS hardware, you must either disable the firewall software while working with ETAS software, or the firewall must be configured to give the following permissions:

- Outgoing limited IP broadcasts via UDP (destination address 255.255.255.255) for destination ports 17099 or 18001
- Incoming limited IP broadcasts via UDP (destination IP 255.255.255.255, originating from source IP 0.0.0.0) for destination port 18001
- Directed IP broadcasts via UDP to the network configured for the ETAS application, destination ports 17099 or 18001
- Outgoing IP unicasts via UDP to any IP in network configured for the ETAS application, destination ports 17099 through 18020
- Incoming IP unicasts via UDP originating from any IP in the network configured for the ETAS application, source ports 17099 through 18020, destination ports 17099 through 18020
- Outgoing TCP/IP connections to the network configured for the ETAS application, destination ports 18001 through 18020

> **Note**
>
> *The ports that have to be used in concrete use cases depend on the hardware used. For more precise information on the port numbers that can be used please refer to your hardware documentation.*

The Windows operating systems come with a built-in personal firewall. On many other systems it is very common to have personal firewall software from third party vendors, such as Symantec, McAffee or BlackIce installed. The proceedings in configuring the ports might differ for each personal firewall software used. Therefore please refer to the user documentation of your personal firewall software for further details.

As an example for a firewall configuration, you will find below a description on how to configure the widely used Windows XP firewall if the hardware access is prohibited under Windows XP with Service Pack 2.

Solution for Windows XP Firewall, Users with Administrator Privileges

If you have administrator privileges on your PC, the following dialog window opens if the firewall blocks an ETAS product.

To unblock a product:

- In the "Windows Security Alert" dialog window, click on **Unblock**.

  The firewall no longer blocks the ETAS product in question (in the example: ASCET). This decision survives a restart of the program, or even the PC.

Instead of waiting for the "Windows Security Alert" dialog window, you can unblock ETAS products in advance.

To unblock ETAS products in the firewall control:

- From the Windows Start Menu, select **Settings** → **Control Panel**.

- In the control panel, double-click the **Windows Firewall** icon to open the "Windows Firewall" dialog window.
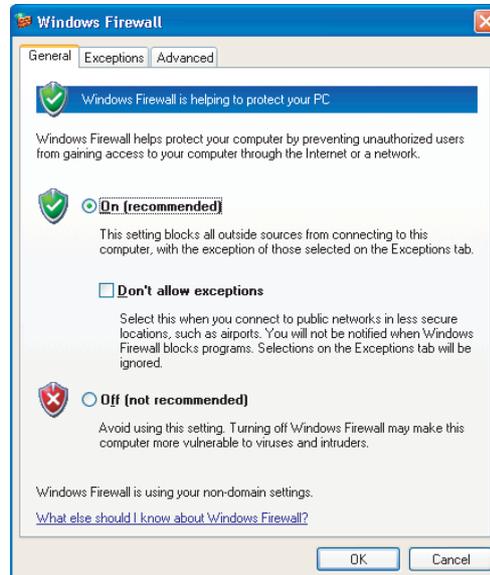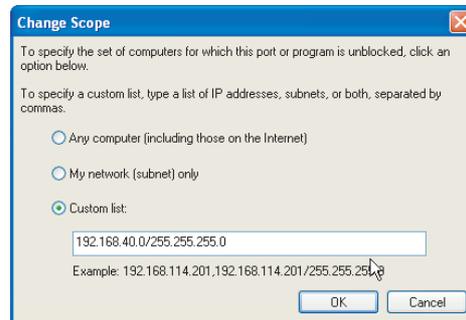

- In the "Windows Firewall" dialog window, open the "Exceptions" tab.
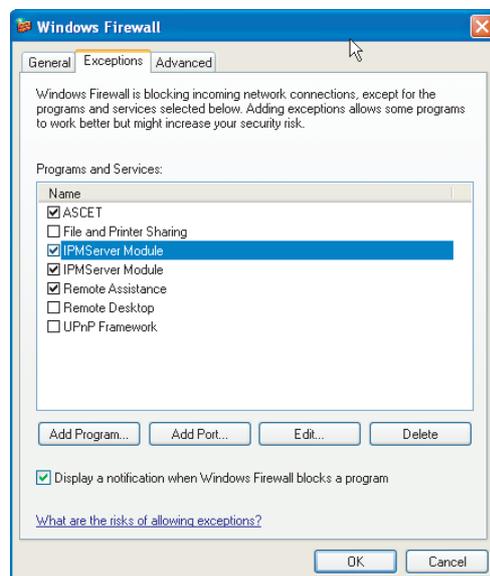
This tab lists the exceptions not blocked by the firewall. Use **Add Program** or **Edit** to add new programs, or edit existing ones.

- Make sure that the ETAS products and services you want to use are properly configured exceptions.

– Open the "Change Setup" window.

– To ensure proper ETAS hardware access, make sure that at least the IP addresses `192.168.40.xxx` are unblocked.

– Close the "Change Setup" window with **OK**.

• Close the "Windows Firewall" dialog window with **OK**.

The firewall no longer blocks the ETAS product in question. This decision survives a restart of the PC.

Solution for Windows XP Firewall, Users without Administrator Privileges

This section addresses users with restricted privileges, e.g., no system changes, write restrictions, local login.

Working with an ETAS software product requires "Write" and "Modify" privileges within the `ETAS`, `ETASData`, and ETAS temporary directories. Otherwise, an error message opens if the product is started, and a database is opened. In that case, no correct operation of the ETAS product is possible because the database file and some `*.ini` files are modified during operation.

The ETAS software has to be installed by an administrator anyway. It is recommended that the administrator assures that the ETAS program/processes are added to the list of the Windows XP firewall exceptions, and selected in that list, after the installation. If this is omitted, the following will happen:

• The "Window Security Alert" window opens when one of the actions conflicting with a restrictive firewall configuration is executed.

To unblock a program (no Admin privileges):

- In the "Windows Security Alert" dialog window, activate the option **For this program, don't show this message again**.

- Click **OK** to close the window.

  An administrator has to select the respective ETAS software in the "Exceptions" tab of the "Windows Firewall" dialog window to avoid further problems regarding hardware access with that ETAS product.

6   ETAS Contact Addresses

ETAS HQ

ETAS GmbH

Borsigstraße 24	Phone:	+49 711 3423-0
70469 Stuttgart	Fax:	+49 711 3423-2106
Germany	WWW:	www.etas.com

ETAS Subsidiaries and Technical Support

For details of your local sales office as well as your local technical support team and product hotlines, take a look at the ETAS website:

ETAS subsidiaries	WWW:	www.etas.com/en/contact.php
ETAS technical support	WWW:	www.etas.com/en/hotlines.php

Index