



INCA V7.3

Installation Guide

Copyright

The data in this document may not be altered or amended without special notification from ETAS GmbH. ETAS GmbH undertakes no further obligation in relation to this document. The software described in it can only be used if the customer is in possession of a general license agreement or single license. Using and copying is only allowed in concurrence with the specifications stipulated in the contract.

Under no circumstances may any part of this document be copied, reproduced, transmitted, stored in a retrieval system or translated into another language without the express written permission of ETAS GmbH.

© **Copyright 2020** ETAS GmbH, Stuttgart

The names and designations used in this document are trademarks or brands belonging to the respective owners.

INCA V7.3 - Installation Guide R01 EN - 03.2020

Content

1	Introduction	5
1.1	Intended Use	5
1.2	Safety Information	5
1.3	Privacy	5
1.4	Documentation Conventions	5
2	Preparing to Install	7
2.1	Package Contents	7
2.2	System Requirements	7
2.3	Privileges	8
2.4	Firewall Configuration	9
2.5	Configuring the Virus Scans	9
3	Customizing the Installation	10
3.1	Setting the Configuration Behavior of Service Pack Installer	10
3.2	Setting the Configuration Behavior of INCA	11
3.3	Setting the Licensing Behavior	13
3.4	Using Command Line Parameters	15
	3.4.1 Silent Mode	15
	3.4.2 No Restart Mode	15
4	Installing the Program	16
4.1	Using the Service Pack Installer	16
4.2	Using the Single Installation	16
4.3	Using the Installation Wizard	17
	4.3.1 Selecting the Installation Components	17
	4.3.2 Specifying the INCA Destination Directories and Language	17
	4.3.3 Filling in the User Information Form	18
4.4	Updating the Program	18

5	Licensing the Software	19
6	Addressing and Configuring the Network Adapter	20
7	Uninstalling the Program	21
8	Troubleshooting	22
8.1	Personal Firewall Blocks Communication	22
8.1.1	Cause: Permissions Given through the Firewall Block ETAS Hardware ...	22
8.1.2	Cause: Permissions Given through the Firewall Block XCP on Ethernet ...	23
8.1.3	Cause: Permissions Given through the Firewall Block Diagnostics over IP (DoIP)	23
8.1.4	Change Personal Firewall Settings	23
8.2	Network Adapter Cannot Be Selected via Network Manager	25
8.3	Updating the Program Failed	26
9	ETAS Contact Addresses	27
Index	28

1 Introduction

This manual addresses system administrators and users with administrator privileges who install, maintain, or uninstall INCA. It describes both the installation on a single computer via DVD and the installation on several computers via a company network.

1.1 Intended Use

INCA was developed and approved for automotive applications and procedures as described in the user documentation for INCA and INCA add-ons. For use in other application areas, contact your ETAS sales representative.

1.2 Safety Information

Adhere to the ETAS Safety Advice for INCA and to the safety instructions given in the online help and PDF manuals.

ETAS GmbH cannot be made liable for damage which is caused by incorrect use and not adhering to the safety instructions.

1.3 Privacy

Please note that personal data is processed when using INCA. As the controller, the purchaser undertakes to ensure the legal conformity of these processing activities in accordance with Art. 4 No. 7 of the General Data Protection Regulation (GDPR/EU). As the manufacturer, ETAS GmbH is not liable for any mishandling of this data.

For further information refer to chapter "[Filling in the User Information Form](#)" on [page 18](#) and to the online help of the respective product.

1.4 Documentation Conventions

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...

1. Step 1
Any explanation for Step 1...
2. Step 2
Any explanation for Step 2...

3. Step 3

Any explanation for Step 3...

Any concluding remarks...

Typographic Conventions

The following typographic conventions are applied:

Choose File → Open .	Menu options are printed in bold, blue characters.
Click OK .	Button labels are printed in bold characters.
Press <ENTER>.	Key commands are printed in small capitals enclosed in angle brackets.
The "Open file" dialog box appears.	The names of program windows, dialog boxes, fields, etc. are enclosed in double quotes.
Select the <code>setup.exe</code> file.	Text strings in list boxes, in program code and in path and file names are printed using the <code>Courier</code> font.
A conversion between Logic and Arithmetic data types is <i>not</i> possible.	Emphasized text portions and newly introduced terms are printed in <i>italic</i> font face.

Important notes for the users are presented as follows:



Note

Important note for users.

2 Preparing to Install

This chapter contains information on the scope of delivery as well as hardware and software requirements to install the program.

2.1 Package Contents

The DVD-ROM or installation package has the following contents:

- INCA, MDA, and ETKTools
- INCA add-ons
- Hardware Service Pack (HSP)
- Documentation:
 - Online help
 - Manuals in PDF format
 - Video tutorials

2.2 System Requirements

The table below contains the minimum and the recommended requirements. The minimum requirements ensure that the program will run smoothly with smaller projects. The recommended requirements ensure that the program will operate very efficiently. Consider that large ECU projects and experiments require more memory.

For information on the causes influencing the INCA performance, see "Performance Tips and Tricks", which you will find in the **Manuals** folder of your INCA installation.

Note

See the release notes for the latest information on the system requirements.

	Minimum System Requirements	Recommended System Requirements
General hardware	<ul style="list-style-type: none"> • Network adapter • DVD-ROM drive (in case of installation from DVD) 	<ul style="list-style-type: none"> • Network adapter • DVD-ROM drive (in case of installation from DVD)
Processor	<ul style="list-style-type: none"> • 2 GHz 	<ul style="list-style-type: none"> • 3 GHz quad core processor or equivalent
RAM	<ul style="list-style-type: none"> • 2 GB 	<ul style="list-style-type: none"> • 16 GB

	Minimum System Requirements	Recommended System Requirements
Graphics card	<ul style="list-style-type: none"> Resolution of at least 1024 x 768 256 MB RAM 16 bit colors and DirectX 9 	<ul style="list-style-type: none"> Resolution of at least 1280 x 1024 1 GB RAM 32 bit color and DirectX 9
Required free disk space	<ul style="list-style-type: none"> 5 GB (not including the size for user data) 	<ul style="list-style-type: none"> >10 GB
Operating system	<ul style="list-style-type: none"> WINDOWS® 8.1 (64 bit) WINDOWS® 10 (64 bit) 	<ul style="list-style-type: none"> WINDOWS® 10 (64 bit)
English, French, Japanese, Chinese and German operating systems are supported.		

2.3 Privileges

Administrator Privileges

You need administrator privileges for the following cases:

- Installing the program
- Accessing a specific version via COM API without re-registering the program

User Privileges

To work with the program, each user must have read and write access for the following folders and directories:

- Registry folder and all subfolders:
 - for INCA:


```
HKEY_LOCAL_MACHINE\SOFTWARE\ETAS
```
 - for some 32 bit components related to INCA operation:


```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ETAS
```
- TEMP directory used by INCA; the TEMP directory is determined during the INCA installation.
- Installation directory
- Shared components in ETASShared13 (e.g. c:\Program Files\Common Files\ETAS\ETASShared13)
- Directory for the program data (e.g. c:\ETASData) and all subdirectories
- Common files (c:\Program Files\Common Files\ETAS)

- Directory for the ETAS log files (e.g. `c:\ETAS\LogFiles, %AppData%\ETAS\Setup`) and all sub directories

In case of remote access, the same user privileges are required.

2.4 Firewall Configuration

The firewall used on the client PC must be configured in such a way that it does not block the communication to the measure and calibration hardware used by INCA. For further information on configuring the ports, refer to the user documentation of your firewall software.

Details on the ports which must be given permission by the firewall can be found in section "Troubleshooting" on page 22.

2.5 Configuring the Virus Scans

Virus scans may reduce the system performance significantly, sometimes to such an extent that the system seems to freeze and recordings get unusable.

To avoid performance losses caused by virus scans

1. Exclude the following program paths¹ from online virus scans:
 - `c:\Program Files\ETAS`
 - `c:\ETAS`
 - `d:\ETASData`
 - Temp directory used by INCA
2. Set scheduled virus scans to times when INCA will not be used.

¹. The exact paths may be different on your PC as they can be configured during installation.

3 Customizing the Installation

To provide the users with the installation files, you can copy the data from the DVD to a network drive. A network installation has the advantage of allowing you to adjust the installation files even before actually installing the program on the computer. This allows you to set company-specific defaults.

You can change certain default settings before conducting the network installation. This is done by adjusting the configuration file

`InstallationDefaultSettings.xml`. This file is located in the installation directory and can be opened with a text editor.



CAUTION

Every licensed program from ETAS uses its own configuration file. Existing information (e.g., temp folder, registry entry) defined from other programs will be overwritten from the current installation respectively the configuration file. Ensure that you always indicate the same settings for all installations.

You can also adapt the settings of the service pack installer, which contains the file `Installation.xml`, located in the installation directory of the service pack installer.

3.1 Setting the Configuration Behavior of Service Pack Installer

In the configuration file `Installation.xml` of the service pack installer, you can define which programs and add-ons will be installed. This file is located in the installation directory of the service pack installer. There are three different types of XML tags within the file:

1. `<Product>` marks all programs which will be installed.
This tag has two different attributes:
 - `action: "install"` to install the program and `"default"` for no actions.
 - `name`: The name of the program to be installed (INCA or MDA).
2. `<Category>` marks two different sections within a `<product>` tag (see table):
This tag has two different attributes:
 - `action: "install"` to install the following add-ons and `"default"` for no actions.
 - `name: "01_General AddOns (free) "` for free add-ons and `"02_Licensed AddOns"` for licensed add-ons.
3. `<Addon>` marks all available add-ons.

This tag has two different attributes:

- `action: "inherited"` takes the settings from the parent tag ("`install`" or "`default`") and "`exclude`" won't install the add-on.
- `name`: See the following table for all available add-ons.

Following Add-ons are available:

General Add-ons	Licensed Add-ons
AddOn_DriveRecorder	AddOn_MCE
AddOn_eCDM	AddOn_FlexRay
AddOn_Video-Tutorials	AddOn_LIN
	AddOn_QM-Basic
	AddOn_INCA-EIP
	AddOn_INCA-SIP
	AddOn_ODX
	AddOn_CANTransmit
	AddOn_INCA-VoiceRecorder
	AddOn_INCA-TOUCH

3.2 Setting the Configuration Behavior of INCA

In the file `InstallationDefaultSettings.xml`, you can define different settings of the INCA installation.

Following custom parameters or variables are available:

- `CONTINUE_ON_TRACE_OVERFLOW`
 - `true`

INCA skips the measure data if the trace buffer identifies a trap and the data might be outdated.
 - `false`

Default setting: In case of an stack overflow, the ECU does not send any data during the reinitialization.
- `IPM_AUTO_IP_RANGE`
 - `true`

Activates the "Auto IP address range" checkbox in the Network Manager by default. The ETAS Network Manager will automatically assign default IP address ranges that will be used by the selected network adapter for addressing the ETAS hardware.

- `false`

Deactivates the "Auto IP address range" checkbox in the Network Manager by default. The user will explicitly either have to set concrete IP address ranges or accept the defaults.
- `IPM_AUTO_CONFIG_NIC`

With this parameter, you can enable or disable several network adapters at once for auto-configuration through the Network Manager.

 - `true`

Activates the "Auto Configure ETAS Network" checkbox in the Network Manager by default. This makes it possible to activate multiple network adapters at once for auto-configuration. The Network Manager will use the first adapter which is enabled for auto-configuration and which has a valid IP configuration for ETAS¹. It will then configure the IP address range automatically.
 - `false`

Deactivates the "Auto Configure ETAS Network" checkbox in the Network Manager by default. The user will have to select the network adapter explicitly which shall be used for the ETAS network.
- `IPM_DEFAULT_OFFSET_START` and `IPM_DEFAULT_OFFSET_END`

The default IP address range used by the ETAS tools for the IP assignment of ETAS hardware can be defined using these settings. The default value can be either empty or a 32 bit decimal value. In case the default value is empty, these settings will not be considered by INCA. As the names of the settings indicate, they are offsets relative to the NIC subnet. This means that they are valid for every NIC configuration unless they fall outside the subnet host range. In case of undefined or invalid settings, ETAS network manager will use fall-back values to define the IP range. Fall-back values are `.2` for the start IP address offset and last valid host for the NIC subnet for the end IP address offset (e.g. 192.168.40.2 - 192.168.40.254)
- `PRODINSTDIR`

Defines the installation path for INCA.
- `LIMA_INIFILE`

Defines the installation path for the `licensing.ini` file. The `licensing.ini` file contains your license information.
- `DO_PRELOAD`

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

On INCA startup, the .NET framework will be preloaded to improve the duration of the opening process of the Variable Selection Dialog.

- **PRODDATAINSTDIRALL**
Defines the path of the working files (e.g. configuration files, databases).
- **ETAS_TEMPPATH**
Defines the path of the temporary files.
- **ETAS_LOGPATH**
Defines the path of the log files.
- **ETAS_LANGUAGE**
Defines the desired language.
- **CREATE_UNINSTALLATION_SHORTCUT**
Automatically creates an uninstallation shortcut on your desktop.
- **ENABLE_ERROR_REPORTING**
Enables or disables the ZIP&SEND function in case of a program error.
- **EMAIL_ERROR_REPORT_TO**
Defines the recipient of the reporting e-mail (ZIP&SEND function). More than one address can be defined, separated by "," (comma).
- Following variables includes personal and company information. Set any default values to automatically insert them into the form within the installation.
FirstName, LastName, Company, Department, AreaCode, Phone, Language, EMail, Street, ZIPCode, City, Country.

3.3 Setting the Licensing Behavior



CAUTION

Every licensed program from ETAS uses its own license file. Existing settings defined from other programs will be overwritten from the current installation respectively license file.

Ensure that you always indicate the same settings for all installations.

To provide the users a fully licensed program version from a network drive, you need to adapt the file `Licensing.ini`. This file is located in the installation directory of the INCA installation package and can be opened with a text editor.

You can define the following custom parameters or variables:

- **LicenseFileName**
Defines the absolute path to the location of the license file which will be added.

- `LicensesToBorrow`

Use this setting if licenses can be borrowed from a license server. To enable the borrow mechanism, enter the name of the product or feature license (e.g. INCA, MDA). If you enter more than one license name, the names must be separated by blanks.
- `BorrowExpiryMode`

Specifies whether the borrowed license expires on a certain date or after a certain amount of days:

 - `Interval`

If the `BorrowExpiryMode` is set to `Interval`, the borrowed license will expire after a certain amount of days which is defined in the parameter `BorrowExpiryInterval`.
 - `Date`

If the `BorrowExpiryMode` is set to `Date`, the borrow period will expire at a certain date which is defined in the parameter `BorrowExpiryDate`.
- `BorrowExpiryDate`

If the `BorrowExpiryMode` is set to `Date`, this parameter specifies the date when the borrow period expires. The format is `yyyy-mm-dd`.
- `BorrowExpiryInterval`

If the `BorrowExpiryMode` is set to `Interval`, this parameter specifies the length of the borrow period in days.
- `BorrowAutomaticExtensionInterval`

This parameter specifies the borrow interval in days that is applied when an automatic extension of the borrow period is executed (as defined under `ExecuteBorrowAutomaticExtensionInterval`).
- `ExecuteBorrowAutomaticExtensionInterval`

Defines at what point in time the borrow period will be extended. The parameter defines the number of days till the expiration of the current borrow period. When the borrowed license expires, the borrow period will be extended to the interval specified under `BorrowAutomaticExtensionInterval`. The borrow period will only be extended if `AutoborrowActive` is set `true`.
- `AutoborrowActive`

If this parameter is set `true`, the borrow period will be automatically extended to the interval specified under `BorrowAutomaticExtensionInterval`.
- `Ports`

In order for multiple users to work in parallel, different ports must be defined.

3.4 Using Command Line Parameters

`Setup.exe /?` and `Setup.exe /help`

Displays the available command line parameters. A full description of the command line parameters and of the error codes which can occur during an installation are described within the `setup.pdf` provided in the installation root directory.

3.4.1 Silent Mode

`/silent`: Executes the installation silent. This means, there won't be displayed any dialog window of the installation routine. All commands are hidden. For example, you can use this option to install INCA on a computer without interrupting the users work.

3.4.2 No Restart Mode

`/NoRestart`: Use this parameter in combination with the silent parameter to omit a restart that might be necessary at the end of the installation. If the restart is omitted, this will be recorded in a log message. If the silent parameter is set, either the Allow Restart or the No Restart Parameter must be set too.

4 Installing the Program

Before starting the installation, make sure that all requirements described in chapter "[Preparing to Install](#)" on [page 7](#) are fulfilled. There are two different ways to install INCA on your computer. You can use the service pack installer or the single installation.

Note

The fully qualified file name of all components of the setup and the directory name are subjects of a restriction and must fall below a certain character length. The character length is calculated individually. If there is an error during setup, please try another and shorter path or file name.

4.1 Using the Service Pack Installer

The service pack installer combines installations of different programs and add-ons in one user dialog window.

To install INCA

1. Close all open ETAS programs.
2. Depending on your company-specific regulations, the installation files are provided on DVD or on a network drive.

By using the DVD, the installation routine starts automatically. If this is not the case, execute the `Autostart.exe` file on the DVD manually.

If you install the program from a network drive, also execute the `Autostart.exe` file.

3. Select your preferred setup language by clicking on the corresponding flag icon.
4. Click on **Installation**.
5. Click on **INCA V7.3/MDA Vx.y/Add-ons**.
6. Select your desired add-ons and programs from the list.
7. Click on **Install**.

All your desired programs and add-ons will be installed in silent-mode. For more information about the Silent Mode, see chapter "[Silent Mode](#)" on [page 15](#).

4.2 Using the Single Installation

If you only use the single INCA installer, there is another installation routine than using the service pack installer.

To install INCA

1. Close all open ETAS programs.
2. Depending on your company-specific regulations, the installation files are provided on DVD or on a network drive.

Execute the `setup.exe` file from your INCA installation directory.

By default, `setup.exe` is located at `<root>\01_INCA_V7.3.<x>\00_Prod_INCA_73<x>`.

If you install the program from a network drive, also execute the `setup.exe` file.

3. Select your preferred setup language and click on `Next`.



Note

The actual location might differ depending on the IT policy of your company. So please ask your tool administrator about the details.

4.3 Using the Installation Wizard

The following chapters provide information about selected INCA settings while using the installation wizard.

4.3.1 **Selecting the Installation Components**

If you use the installation wizard, you can select the components to be installed.

4.3.2 **Specifying the INCA Destination Directories and Language**

If you use the installation wizard, you can select the desired language and the destination directories for the program and data files.

The *program files*, *program data*, *log files* and *temp files* are stored in different directories. If you uninstall or update the program later, only the program files will be deleted or overwritten. The program data will still be available. The program data includes the following:

- Databases
- User interfaces
- Demo files
- Measure files
- User profiles

**CAUTION**

Selecting the `Program Files` directory for INCA data files may lead to problems in INCA since the access to the program folder depends on the Windows user rights.

Do not save INCA data files in the `Program Files` directory. Select a folder in a data area where all users have read and write access rights.

**Note**

The language you select in this dialog will change the global language settings for all already installed ETAS products.

4.3.3 Filling in the User Information Form

If you use the installation wizard, you can enter your user information.

**Note**

You do not need to fill in the fields of the form. INCA reuses the entered information for further use cases.

4.4 Updating the Program

Use the service pack installer to update the program. You are able to upgrade or downgrade your current INCA version.

Follow the instructions in Chapter "[Using the Service Pack Installer](#)" on page 16 to get a list of available updates. If there are updates available, the new "Package Version" and a red icon are shown in the corresponding row.

5 Licensing the Software

A valid license is required for using INCA. You can obtain the license file required for licensing either from your tool coordinator or through a self service portal on the ETAS Internet Site under <http://www.etas.com/support/licensing>. To request the license file you have to enter the activation number which you received from ETAS during the ordering process.

In the Windows Start menu, select

E → ETAS → ETAS License Manager.

Follow the instructions given in the dialog. For further information, for example about the ETAS license models and borrowing a license press **F1** in the ETAS License Manager.

6 Addressing and Configuring the Network Adapter

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 (ETAS network).

In the Windows Start menu, select

E → ETAS INCA 7.3 → INCA V7.3 Tools → ETAS Network settings.

Follow the instructions given in the dialog. For further information about addressing and configuring the network adapter press **F1** in the ETAS Network Manager.

7 Uninstalling the Program

To uninstall INCA, choose **Add/Remove Programs** or **Programs and Features** in the Windows Control Panel.

If you only like to remove individual components, start `INCA setup.exe` from the installation directory again. It will open the maintenance mode of INCA setup.

To uninstall components individually

1. Select **Modify** in the list and click on **Next**.
2. Select or unselected your desired add-ons and click on **Next**.
The installation wizard shows your changes.
3. Click on **Modify** to confirm your selection.

8 Troubleshooting

8.1 Personal Firewall Blocks Communication

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, McAfee 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.

Personal firewalls may interfere communication with hardware or protocols, i.e., INCA doesn't get any response from the ECU or can't send a request. The automatic search for hardware typically cannot find any Ethernet hardware at all, although the configuration parameters are correct. If a firewall is blocking communication to ETAS hardware or any protocol, you must either disable the firewall software while working with ETAS software, or the firewall must be configured to give the permissions for the following use cases.

8.1.1 Cause: Permissions Given through the Firewall Block ETAS Hardware

- 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 refer to your hardware documentation.

8.1.2 Cause: Permissions Given through the Firewall Block XCP on Ethernet

- Outgoing IP multicasts for XCP Slave Detection via UDP to any IP in network, destination IP 239.255.0.0, port 5556.
- Incoming IP multicasts for XCP Slave Detection via UDP from any IP in network, destination IP 239.255.37.45, port 3745.

8.1.3 Cause: Permissions Given through the Firewall Block Diagnostics over IP (DoIP)

- Outgoing TCP/IP connections for DoIP to the DoIP network, destination port 13400.
- Outgoing IP unicasts via UDP for DoIP to the DoIP network, destination port 13400.
- Outgoing IPv4 limited broadcasts for DoIP via UDP (destination address 255.255.255.255) for destination port 13400.
- Outgoing IPv6 broadcasts for DoIP via UDP from any IP in the network, destination IP FF02:1, port 13400.
- Incoming IP unicasts via UDP for DoIP originating from the DoIP network, destination port 13400.

8.1.4 Change Personal Firewall Settings

As an example for a firewall configuration, you will find below a description on how to configure the Windows 10 firewall.

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

Note

Please consult your IT responsible and/or check the IT security policies of your company before changing your firewall configuration and reconnecting the computer to the network!

To unblock a product

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

The firewall no longer blocks the ETAS product in question. 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

1. In the Windows search field, enter **Control Panel**.
2. Select **Control Panel**.
The "Control Panel" window opens.
3. In the "Control Panel" window, click on **System and Security** → **Windows Defender Firewall** to open the "Windows Firewall" dialog window.
4. In the "Windows Firewall" dialog window, in the left column, click on **Advanced Settings**.
The "Windows Firewall with Advanced Security" window opens.
In this window all inbound and outbound rules are listed. Make sure that the ETAS products and services you want to use are properly configured exceptions.
5. To add a new rule, in the left column, right-click **Inbound Rules** or **Outbound Rules** (depending on your requirement).
6. In the right column, click on **New Rule**.
7. In the upcoming window, choose **Port** and follow the instructions to set the new rule. You find all required information in the beginning of this chapter.

Solution using the Example of the Windows 7 Firewall, Users without Administrator Privileges

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

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 this 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. 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)

1. In the "Windows Security Alert" dialog window, activate the option **For this program, don't show this message again**.
2. 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.

8.2 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 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 only permitted to users who have administrator privileges. It should only be done in coordination with your network administrator.

To enable the APIPA mechanism

1. Open the Windows "Registry Editor".
2. Open the folder `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\`
3. Click **Edit** → **Find** to search for the key `IPAutoconfigurationEnabled`.

If you cannot find any instances of this registry key, 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.

4. 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.

5. Close the registry editor.
6. Restart your workstation in order to make your changes take effect.

8.3 Updating the Program Failed

Cause: One of the required INCA or INCA add-on installations failed

If one of the required INCA or INCA add-on installations fails, the installation of the complete service pack cannot be finished.

To solve the issue, do the following

1. Check the log files for details about the issue. The following log files are stored under <ETAS Default log directory>\ServicePack\
 - SP_SETUP_YEAR_MONTH_DAY.log
 - SP_SETUP_YEAR_MONTH_DAY_DEBUG.log

If there is no `DefaultLogPathName` key in the registry, the logs are stored in the `%temp%` folder.

2. Check if all ETAS programs are closed.
3. To install the whole service pack or selected add-ons again, tick the checkbox **Re-Install mode** in the Service Pack Installer.
4. Click **Re-Install**.

If the installation still fails, contact your local support.

Additional to the service pack installer logs, there are log files related to the last product/add-on installation at `%AppData%\ETAS\SETUP`. Check the end of the log for any indication for the failure reason.

9 ETAS Contact Addresses

ETAS Headquarter

ETAS GmbH

Borsigstraße 24

Phone: +49 711 3423-0

70469 Stuttgart

FAX: +49 711 3423-2106

Germany

Internet: 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 Internet: www.etas.com/en/contact.php

ETAS technical support: Internet: www.etas.com/en/hotlines.php

Index

A

APIPA25

E

ETAS License Manager 19

ETAS Network Manager11,20,25

F

Firewall configuration9,22

H

HSP7

I

INCA add-on 5,7

INCA components 17

install.ini 10

N

Network adapter7,11,20,25

S

Service pack26

System requirements7