REF542plus

Installation Manual for Web Interface

Installation manual

ABB

1MRS755865

Issued: 22.01.2004
Version: A/28.02.2006

Multifunctional Protection and Switchbay
Control Unit

Installation Manual for Web Interface

Installation manual

REF542plus

Contents

Copyrights

The information in this document is subject to change without notice and should not be construed as a commitment by ABB Oy. ABB Oy assumes no responsibility for any errors that may appear in this document.

In no event shall ABB Oy be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, nor shall ABB Oy be liable for incidental or consequential damages arising from use of any software or hardware described in this document.

This document and parts thereof must not be reproduced or copied without written permission from ABB Oy, and the contents thereof must not be imparted to a third party nor used for any unauthorized purpose.

The software or hardware described in this document is furnished under a license and may be used, copied, or disclosed only in accordance with the terms of such license.

Trademarks

ABB is a registered trademark of ABB Group. All other brand or product names mentioned in this document may be trademarks or registered trademarks of their respective holders.

Guarantee

Please inquire about the terms of guarantee from your nearest ABB representative.

1. Introduction

1.1. This manual

Before attempting any operation with the REF542plus, read carefully this manual first.

This manual describes how to install the WebREF function of the REF542plus. Please note that Web Page views and pictures are to be considered exemplary.

This manual is addressed to engineering and commissioning personnel and to anyone who needs to administrate the WebREF with REF542plus via the Ethernet network and the Web Browser interface.

1.2. Use of symbols

This publication includes the following icons that point out safety-related conditions or other important information:

The warning icon indicates the presence of a hazard which could result in personal injury.

The caution icon indicates important information or warning related to the concept discussed in the text. It might indicate the presence of a hazard which could result in corruption of software or damage to equipment or property.

The information icon alerts the reader to relevant facts and conditions.

It should be understood that operation of damaged equipment could, under certain operational conditions, result in degraded process performance leading to information or property loss. Therefore, comply fully with all notices.

1.3. Intended audience

This manual is intended for installation personnel, administrators and skilled operators to support installation of the software.

1.4.   Product documentation

Name of the Manual	Document ID
Application Notes	1MRS755870
CAN Manual	1VTA100189-Rev 1, en
Configuration Manual	1MRS755871
iButton Programmer User Manual	1MRS755863
Manual Part 3, Installation and Commission	1 VTA100004
Manual Part 4, Communication	1VTA100005
Motor Protection with ATEX Certification, Manual	1MRS755862
Operator's Manual	1MRS755869
Protection Manual	1MRS755860
Technical Catalogue	1MRS755859
Technical Reference Modbus RTU	1MRS755868
Web Manual, Installation	1MRS755865
Web Manual, Operation	1MRS755864

1.5.   Revision history

Version	Date	Comment
1VTA100264 Release 1.0	22.01.2004	First release
1VTA100264 Release 1.1	14.05.2004	Update
A	28.02.2006	Document updated • language • layout

Applicability

This manual is applicable to REF542plus Release 2.0, software version V4D02f. Please consider also the Users Manual WebREF 1VTA 100180.

2.   Safety Information

The safety warnings should always be observed. Non-observance can result in death, personal injury or substantial damages to property. Guarantee claims might not be accepted when safety warnings are not respected.

The WebREF isn't designed for connecting to the Internet. It is further using internet technologies.

ABB cannot take any warranty for any damages resulting from the WebREF function, in case the REF542plus Ethernet network is connected to a company intranet or the Internet.

In case the customer decides, on his own risk, to connect to intranet or the Internet, special security advices have to be considered. To setup switches and gateways with the IPSec feature is mandatory as described in this manual.

Do not make any changes to the REF542plus configuration unless you are familiar with the REF542plus and its configuration tool. This might result in disoperation and loss of warranty.

3.   Supported browsers

The WebREF supports Microsoft Internet Explorer 5.x, 5.5 and 6.x for Windows.

To parse the xml-files and requests, the browser needs the MSXML 3.0 parser, which comes with IE 5.5 and higher. By user IE 5.x it is necessary to install MSXML 3.0 in replace mode, which can be downloaded from http://www.microsoft.com/downloads.

To install MSXML 3.0 in replace mode:

From the command prompt, enter: pathname > xmlinst –u, where the pathname is the folder where xmlinst.exe is installed. This command uninstalls any registry entries for MSXML.

From the command prompt, enter: regsvr32 msxml3.dll. This registers MSXML 3.0.

From the command prompt, enter: pathname > xmlinst. This installs the latest version of MSXML in replace mode.

3.1.   Problems with browsers or operating systems

Adobe SVG Viewer 3.0 supports javascript-api, which is necessary to change the SLDs, only with IE under Windows. If the SVG viewer is running on a Macintosh system or a Netscape Browser, the plugin can only display svg-files, but no interaction such as moving or clicking elements.

Most of the other used technologies and browser functions are also Netscape 6.x and Mozilla 1.x compatible. For more information about svg-support in browsers have a look at www.adobe.com/svg.

You can download, if necessary, the SVGview.exe from the Adobe's download page to your PC. Simply install the SVG viewer by starting the execution file.

3.2.   Advice on using Internet Explorer

It is recommended to put the address of WebREF on the "Trusted sites" list of the browser. Otherwise, problems with displaying the SLD and other interfaces can occur. Select **Internet Options** in the **Tools** menu of your browser. Select the security options in the pop up window and click **trusted sites**. Add the IP addresses of the devices and index pages to the menu. See Fig. 3.2.-1.
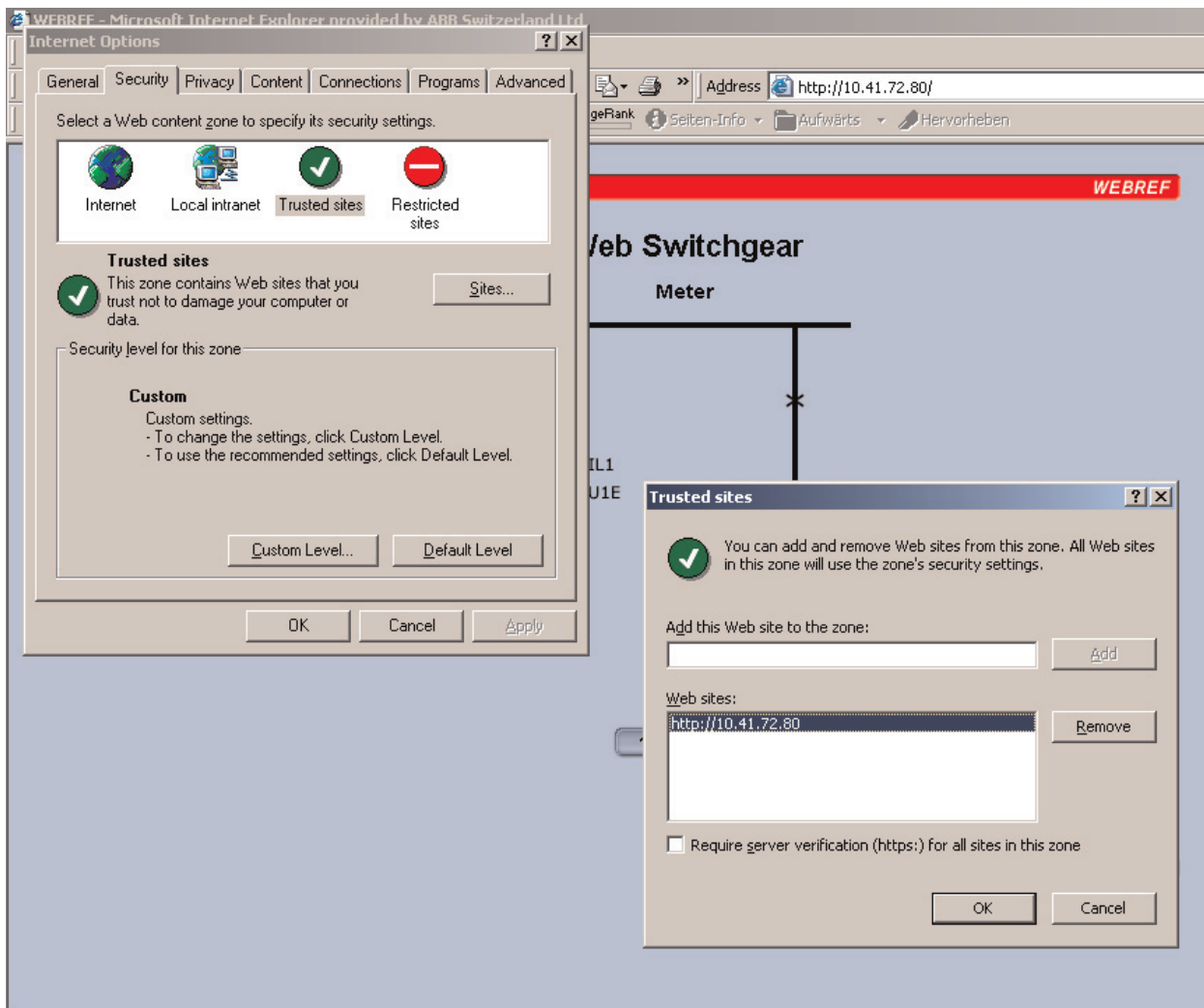
A051090

Fig. 3.2.-1   Trusted sites selection in the Internet browser

A further setting required for user authentication services is the enable setting for proxy connections, See Fig. 3.2.-2. It can be found in the Internet Options; Advanced. Browse to HTTP1.1 settings and enable Use HTTP 1.1 through proxy connections.
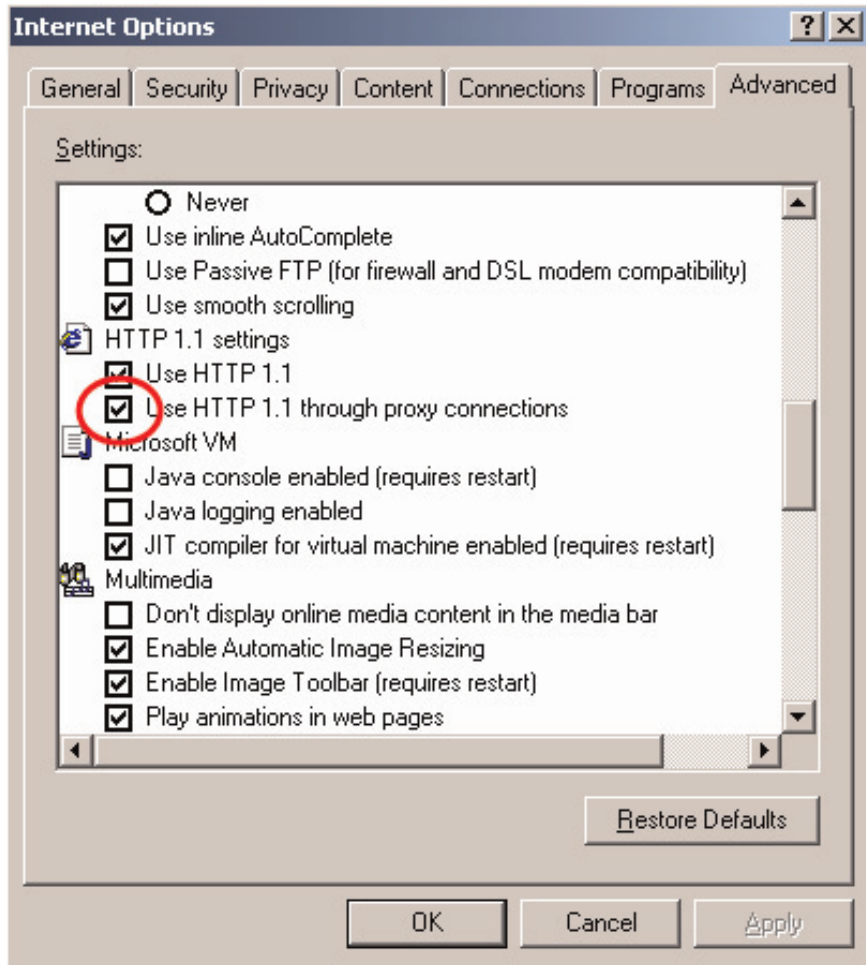
Fig. 3.2.-2   Enable the setting for proxy connections

4. Web access and security requirements

Web access to REF542plus has to be protected with IPSec authentication (IP level), if the substation is connected to a company's intranet. In this case, a gateway which provides the IPSec feature to be installed is recommended, as shown in Fig. 4.-1.
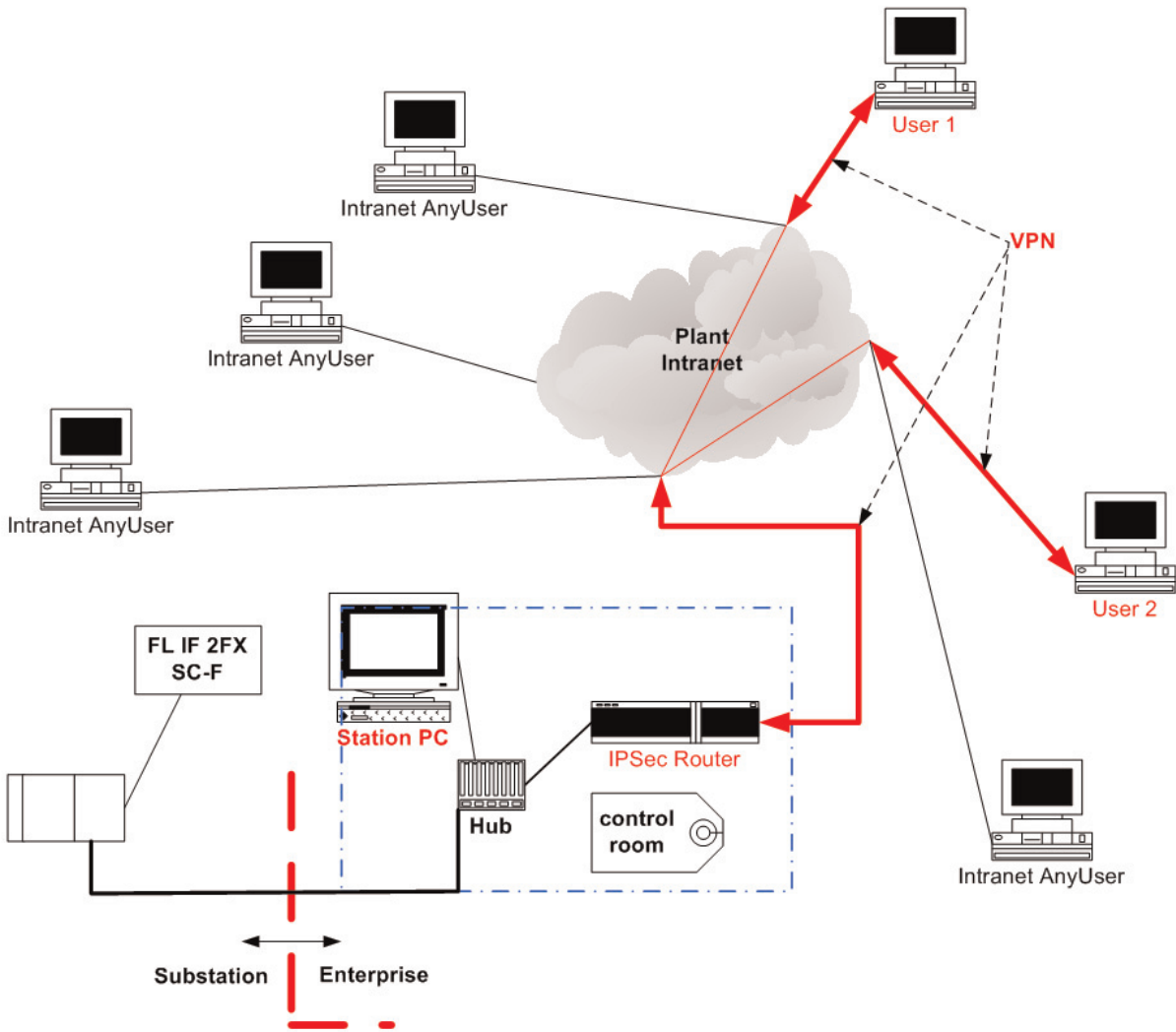
A051276

Fig. 4.-1 Example of a connection to an enterprise network

It assures that only certified clients, that is Web browsers, can access the IP address of REF. That is, "pinging" to the IP address is in this case not possible.

4.1.   User authentication

The user has to authenticate himself by giving a user name and password. The user name and password have to be communicated to the core unit to check the authentication. For security reasons, to avoid access from intruders and not authenticated users, the information (user name and password) is encrypted with a non-convertible key.

Therefore, digest authentication algorithms are used in the configuration tool and REF542plus core unit. This way passwords are not communicated as plain text through the communication line because they are already converted on the PC level with an AES algorithm encryption key and converted back on the device level. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. The encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form called the plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.

4.2.   Security for writing operations

Web-enabled REF542plus allows some writing operations. This means that the user can change information on the server, such as the telephone numbers for SMS messaging or start FTP through the web interface.

This writing operation needs an authentication based on user name and password. For security reasons, the digest authentication is applied. This way passwords are not communicated as plaintext through the communication line.

4.3.   Security for saving passwords

Web-enabled REF542plus allows interaction with the device for different types of user rights. Operation requiring special rights needs an authentication based on the user name and password. All the passwords are stored in the SCL file on the PC. This file is prepared by the Configuration Tool and then sent to the device. For security purposes, all the passwords are not stored as plaintext but as already encrypted.

Selecting a suitable password is crucial and part of the security aspects of the application. A password should be handled like a key and should never be public. The password should be changed randomly and it should not contain names or words in order to increase access security for hackers and unwanted actions. It is further recommended to have figures and special characters in the password to increase the security level for any intruders.

> The password must have a minimum of 8 characters, otherwise the password is not accepted.

4.4.   Attack from remote

An attack from remote, meaning from outside the local REF network, should be prevented. Therefore, unauthorized users should not be able to get access to REF542plus. A remote attack is only possible when the devices are connected to company intranet or Internet. Installing the IPSec function is recommended.

4.5.   Number of devices allowed per subnet

The number of devices per subnet is limited. The limitation is set to 256 devices.

The practical subnet size should be defined by the application and have a practical size of 10 devices. In case a GSM Modem is connected, one device per total network is sufficient.

5.   WebREF Configuration

With the Configuration Tool of REF542plus the WebREF function can be enabled and configured. To have the single line diagrams correctly displayed on the Web page, some requirements in the graphical design of SLD are needed. They are described in more detail in this chapter.

The language files can be configured according to the user needs. It can be selected, which is the preferred default language to be displayed when starting the pages of the device, and also which is the second preferred language. The second language is the one selectable on the Web page header. In addition, any kind of language file, including the non-character based languages, can be generated for display.

The GSM and the network configuration are handled by the Configuration Tool as well.

5.1.   SLD design constraints

Drawing of busbar symbol has to be on the same vertical coordinates and the whole width of the drawing field should be used.

- The vertical Y-coordinates should be the same (Example: 7)
- Use the whole width X-coordinates (Example: 0, 118)

REF542plus   **Multifunctional Protection and Switchbay**   1MRS755865
                        Control Unit
                        Installation Manual for Web Interface

                        Installation manual
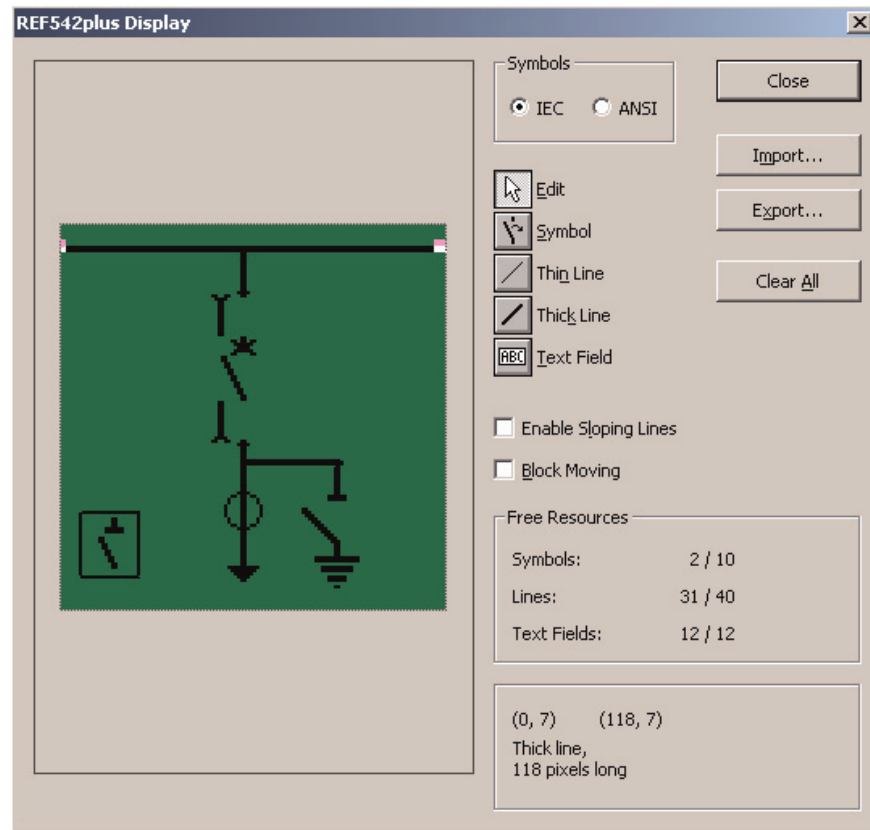
A051094

Fig. 5.1.-1   SLD design constraints

5.2.   Switchboard overview

The switchboard overview is generated automatically. No configuration to get
the page is necessary. To get the overview on the right shape, some rules have
to be respected:

- The overview is oriented according to the IP addresses. The lower IP
  address is left of the device you want to monitor and the higher IP address
  is right to the station you want to monitor.

- The size of the overview is the size of a subnet. In the subnets, click **Next**
  to continue.

- There are 3 SLDs displayed per page. You can continue and move back
  with the **Next** button.

- When drawing SLD in the Configuration Tool, use the full width of the
  drawing area in order to prevent a discontinued (only from visual point of
  view) busbar in the overview. See Section 5.1. SLD design constraints .

5.3. Web communication configuration

Select the **Configure** menu in the ABB REF542conf - New dialog and click **Enable Web Interface** to see the functions needed to enable any WebREF configuration.
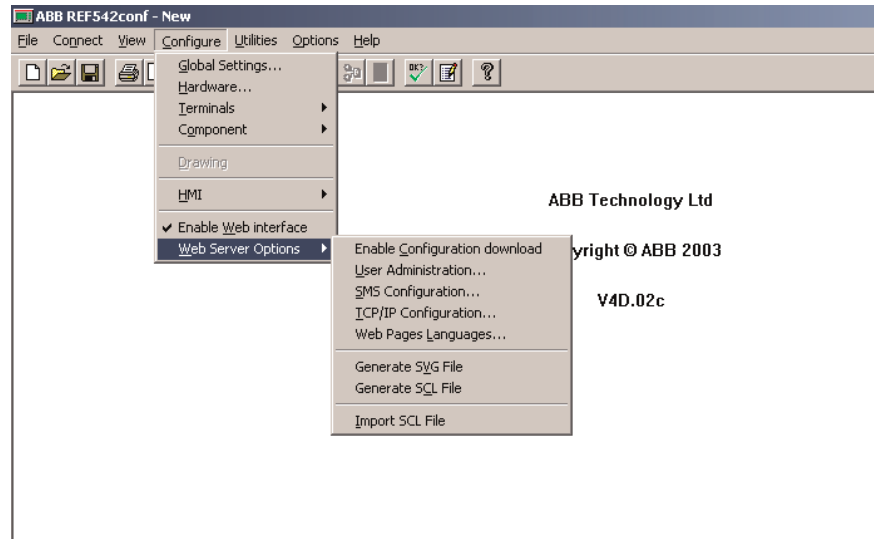
Fig. 5.3.-1   Configuration for the web communication

5.4. Enable configuration download

The Web file transfer can be enabled and disabled by clicking **Configure > Web Server Options > Enable Configuration Download**. In case it is not enabled, the Web configuration files are not uploaded to REF542plus. In this case, the transfer time is shorter because the Web function is not loaded or it is already loaded not but modified.

If the **Enable Configuration Download** is selected, the files will be transferred with the standard REF542plus configuration and updated accordingly on the REF542plus unit.

> When WebTransfer is not selected the WebREF configuration is not uploaded or modified.

5.5. User administration

By selecting **Configuration > Webserver Options > User Administration**, the user can apply user name and password for interacting with the GSM setting page and Language file up and download page. In here, the passwords can be changed and users removed.

5.5.1. Security features on writing operations, passwords and user names

The Web-enabled REF542plus allows some writing operations for the GSM page. This means that the user can change information on the server, such as the telephone numbers for SMS messaging, can be changed through the Web Interface.

This writing operation needs an authentication based on a user name and password. The digest authentication has been chosen. This way, the passwords are not communicated and stored as plain text through the communication line, but encrypted by the AES algorithm encryption based on a fixed key word stored in the Configuration Tool and device firmware.

All these passwords are stored in the SCL file. This file is prepared by the Configuration Tool and then sent to the device.

With the password and user name, the system decides with which privileges a user or application is permitted to interact with the protected system and prevents such interaction in case of a negative decision. Different login mechanism has to be chosen to have a clear user authentication.

Selection of a suitable password is crucial and part of the security aspects of the application. The password should be handled like a key and it should never be public. The password should be changed randomly and should not contain names or words to increase access security for hackers and unwanted actions. It is further recommended to have figures and special characters in the password to increase security.

The password must have a minimum of 8 characters, otherwise the password is not accepted.

5.5.2. Add user

By clicking the Add User radio button a dialog will pop up to enter a new user. Type the user name, password and confirm password by retyping it. By clicking **OK**, the user is added and displayed with user name in the User Administration dialog. The password must have a minimum of 8 characters, otherwise the password is not accepted.
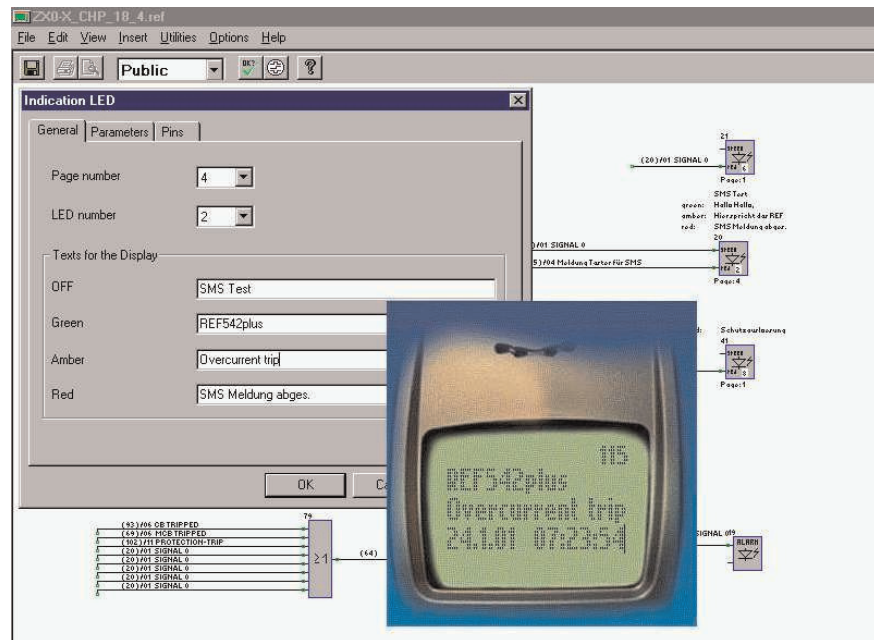
5.5.3. Remove user

By selecting the current user and clicking the **Remove User** button, the user is removed without further notice.

5.5.4.   Edit user

This function is needed to change passwords and user names according to the customer needs. By selecting the current user and clicking the **Edit User** button, the password can be changed.

5.6.   SMS configuration

A051096

Fig. 5.6.-1   Gateway configuration for SMS messages to a GSM modem

REF542plus can be either configured to function as a gateway for SMS messages to the GSM modem, or as a normal SMS message source.

As the gateway function is configured, REF542plus will receive all SMS messages from the Ethernet network and forward them to the GSM modem for transmitting into the GSM network. REF542plus is forwarding all the SMS messages that are sending to this (Gateway) IP address. Also, the SMS messages generated by the gateway itself are sent to the GSM for transmitting.

As the SMS message source is configured, REF542plus will send its SMS message to the Gateway IP address. The gateway is then forwarding this message to the GSM modem.

5.6.1.　　REF as SMS gateway
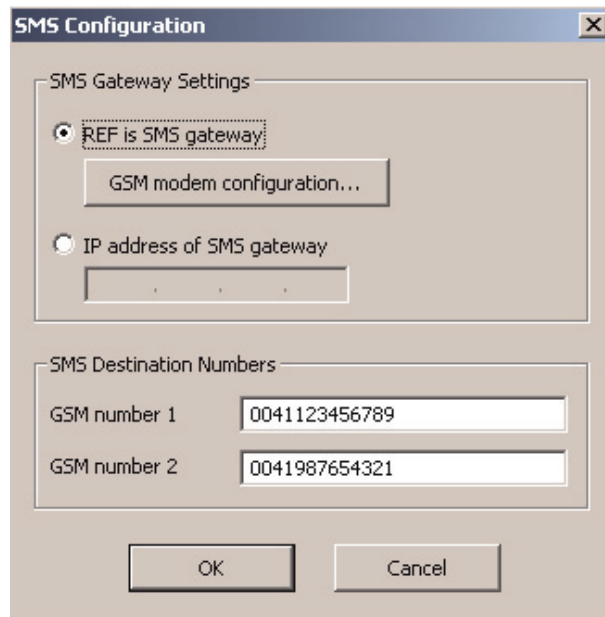
A051097

Fig. 5.6.1.-1　　SMS gateway setting

A REF542plus, with the GSM physically connected via the serial interface, is the SMS gateway. Only a REF542plus which has a GSM physically connected can be a SMS gateway. Therefore, a REF542plus used for gateway has to be configured as REF is SMS gateway and the MODEM has to be configured. All other REF542plus devices have to be configured with the IP address of SMS gateway set to the gateway's IP and the GSM number(s).

More then one REF gateway is possible per subnet.

It is recommended not to overload the queue of SMS messages more than one SMS gateway per subnet. The queue is designed to have not more than 10 SMS messages per gateway at the same time.

5.6.2.　　GSM modem configuration

The modem configuration is fixed in the actual version. By clicking the GSM modem configuration radio button, a dialog for selecting the modem type and baud rate is provided. The modem type and values cannot be selected. For the applications with this version, the INSYS GSM 2.0 is recommended.

The phone card should be the type without a PIN code. The reason for this is that WebREF is not requesting for PIN at power up.

> Phone cards which do not allow "Disable request for PIN at powerup" can not be used. A phone card without a PIN code has to be used.
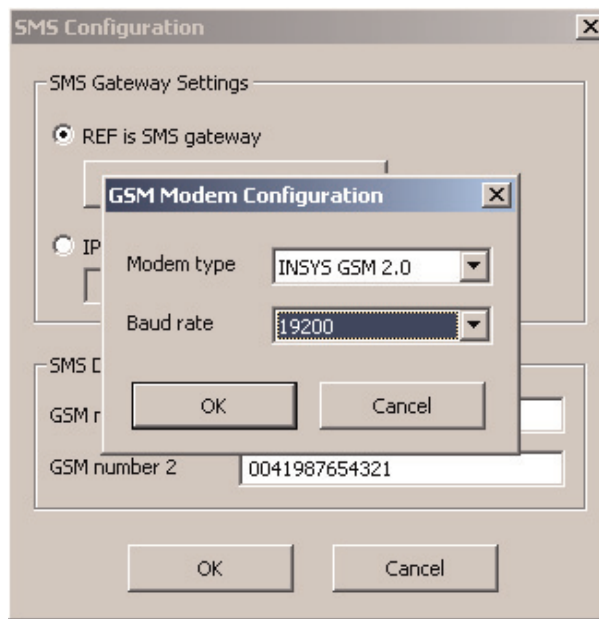
A051098

Fig. 5.6.2.-1   Setting of the modem type and baud rate

5.6.3. IP address of SMS gateway

A051099

Fig. 5.6.3.-1   IP address for the SMS gateway

When REF542plus has no GSM physically connected, the IP address of SMS gateway button has to be selected. Also, the IP address of the gateway has to be typed. Verify that the address is correctly typed because this can cause malfunction of the SMS messaging.

5.7.   Ethernet network settings

In this setting the Ethernet network access can be configured by setting the IP address, subnet mask and default gateway.
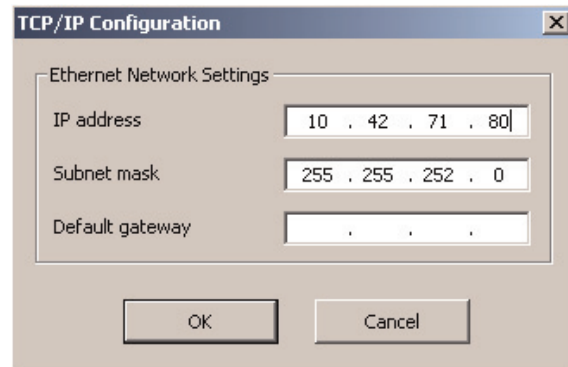

A051100

Fig. 5.7.-1   Parameter setting for the ethernet network

In the TCP/IP configuration these 3 options can be set for each REF542plus. In case there is no router in place, the default gateway address can be left open. The subnet mask is set to a default value 255.255.252.0.

For more information, refer to the Section 6.4.2. TCP/IP configuration.

5.8.   Language file generation

The language file can be modified according to the language request by the application. Therefore, the English language file can be used as basic for the modification. Some general rules have to be respected for the modification:

- Never change text inside brackets.
  - Example: **<Title>**Messverte**</Title>**
- Never change what is inside (content) SAdr
  - Example: <SAdr>**005**</SAdr>
- Never change filenames
  - Example: <Page2>**control_page.htm**</Page2>
- Never change items containing the "Underline" character
  - Example: <<DataSetName>**BinaryIO_Outputs**</DataSetName>

Everything else can be translated when respecting the rules above. For the information on how to generate the different language files, see Section 9. Appendix A: Generate language files and the listed examples.

> ℹ️ The Alarm page needs a special handling in order to have the configured alarm text translated. See
> Section 9. Appendix A: Generate language files

5.9. Web pages language selection

Web-enabled REF542plus Web pages can be displayed in two different languages, in English and in a second user defined language. This means that independently of device configuration and firmware, the user can set a completely arbitrary second language on the server (even with different symbols, like Chinese or Japanese) simply providing the translated language files.

5.9.1. Special language configuration
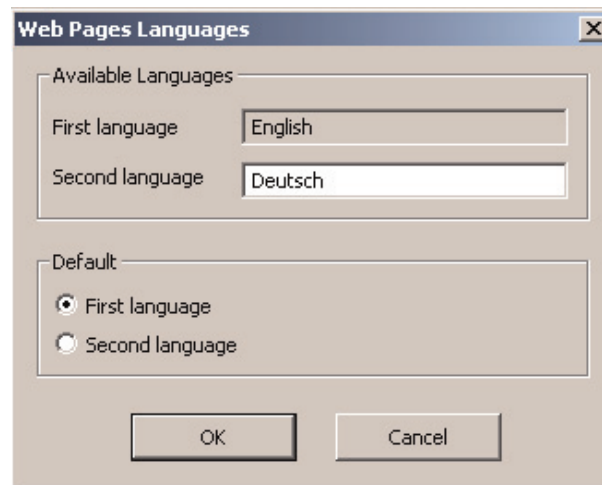
A051101

Fig. 5.9.1.-1   Configuration for the second language

By clicking **Configure > Web Server Option > Web Pages Languages**, the user can define a second language. The text typed in the Second Language field of the dialog is corresponding text for the language button on the Web page.

Limitations: The text typed in this field is limited to 16 characters. The text to be typed must be character based.

A051102

Fig. 5.9.1.-2   Selection of the language from the Web page

Furthermore, the default language can be selected. The default language is the language displayed when a new WebREF session is opened.
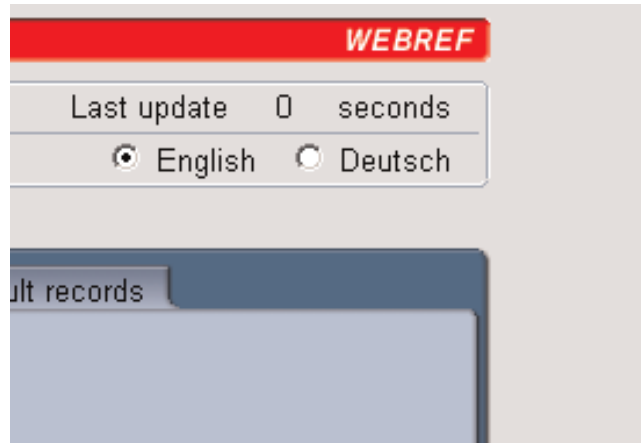
Note that the English version is always present and cannot be unselected by the Configuration Tool.

5.9.2.   Language files upload

This is the list of the English files, which can be used in case the customer wants to have a not supported language. The language files are only available in English version. In Section 9. Appendix A: Generate language files , the modification from the English version can be seen.

Default English language files can be requested from the SA-D Supportline. Also a batch file for downloading all the needed files to the REF542plus can is available.

Table 5.9.2.-1   English language files

	File name
1	BinaryIO_Inputslang_2.xml
2	BinaryIO_Outputslang_2.xml
3	service_statisticslang_2.xml
4	service_versionslang_2.xml
5	service_tcpipsetlang_2.xml
6	service_hwidentlang_2.xml
7	helplang_2.xml
8	measlang_2.xml
9	faultreclang_2.xml
10	alarmslang_2.xml
11	striplang_2.xml
12	menulang_2.xml

Table 5.9.2.-1   English language files (Continued)

	File name
13	messaginglang_2.xml
14	languagelang_2.xml
15	prot_currentlang_2.xml
16	prot_voltagelang_2.xml
17	prot_motorlang_2.xml
18	prot_distancelang_2.xml
19	prot_differentiallang_2.xml
20	prot_otherslang_2.xml

After their modification, they need to be uploaded to REF542plus via FTP. That requires a correct configuration of the Ethernet port with the IP address. When the language upload is enabled, the FTP server is enabled and it can be used as described below.

For security reasons, the FTP session is time limited to 5 minutes. After timeout, the user has to login again with the user name and password.

The following is the procedure for uploading language files:

1. Open the Web browser, click the Language tab on the Configuration property sheet and enable language file transfer by clicking the **Enable** button.

2. Type your user name and password in the Enter Network Password dialog and click **OK** (user names and passwords are defined by the Configuration Tool and they are then automatically stored in the SCL files).
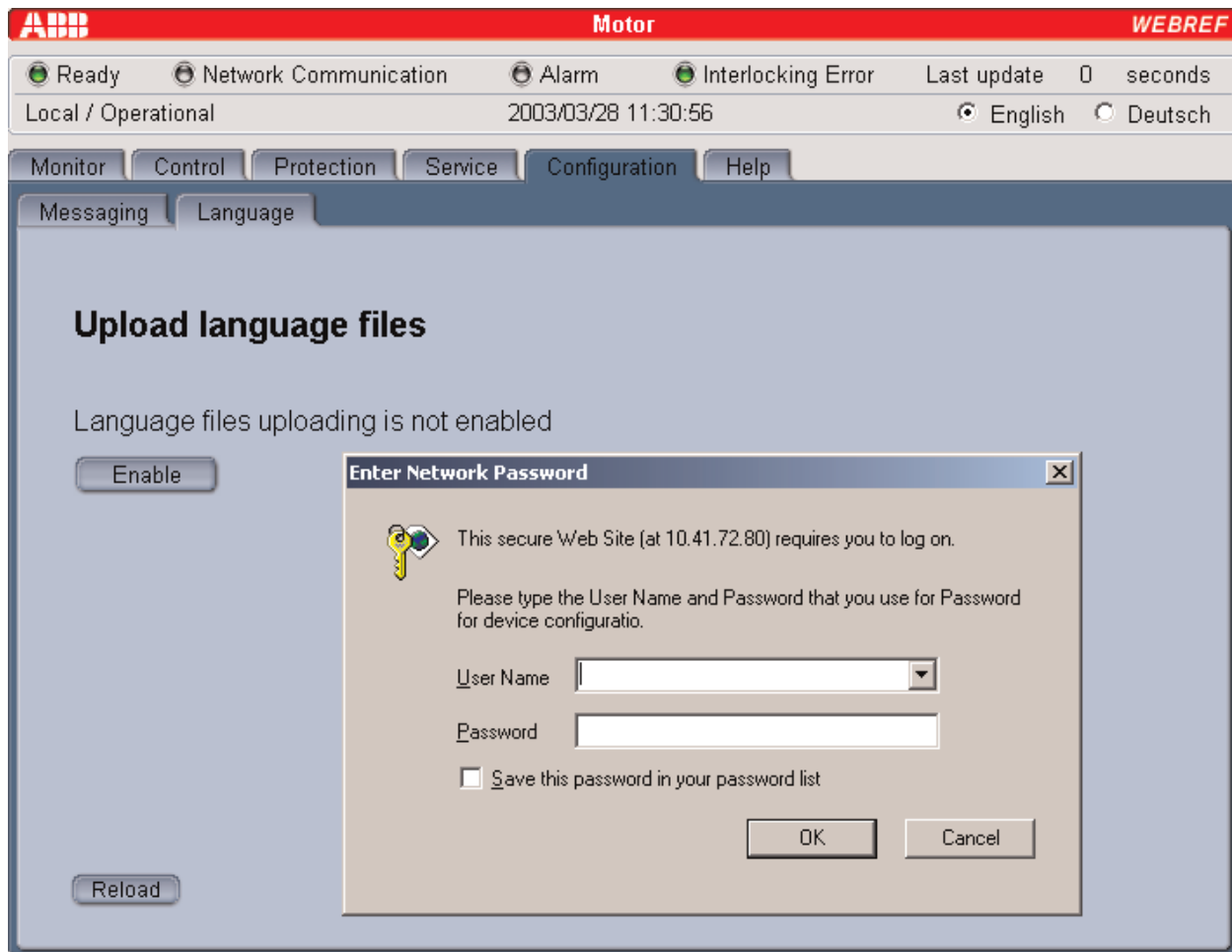
A051103

Fig. 5.9.2.-1   Uploading procedure for the language file

When user name and password are typed in, it will reside in the fields until the browser is closed. For security reasons and to avoid to have unwanted modifications, it is recommended to close your browser completely, after the configuration operation is done.
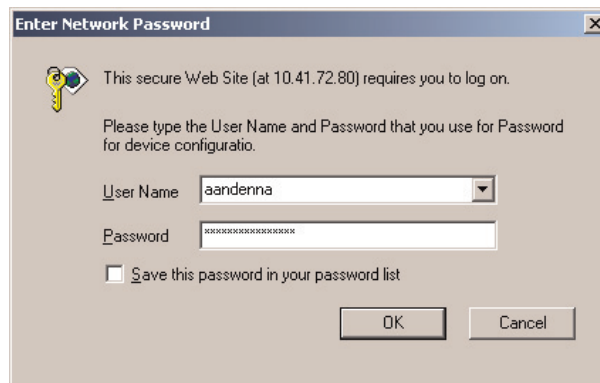
A051104

Fig. 5.9.2.-2   Insert the user name and the password

3. Open the Command prompt on the PC connected to the same network of the device.

4. Move to the path in which the language files to be uploaded and "file system files.bat" file are located.

5. Execute the following command:

ftp -s:"file system files.bat" <REF IP address>
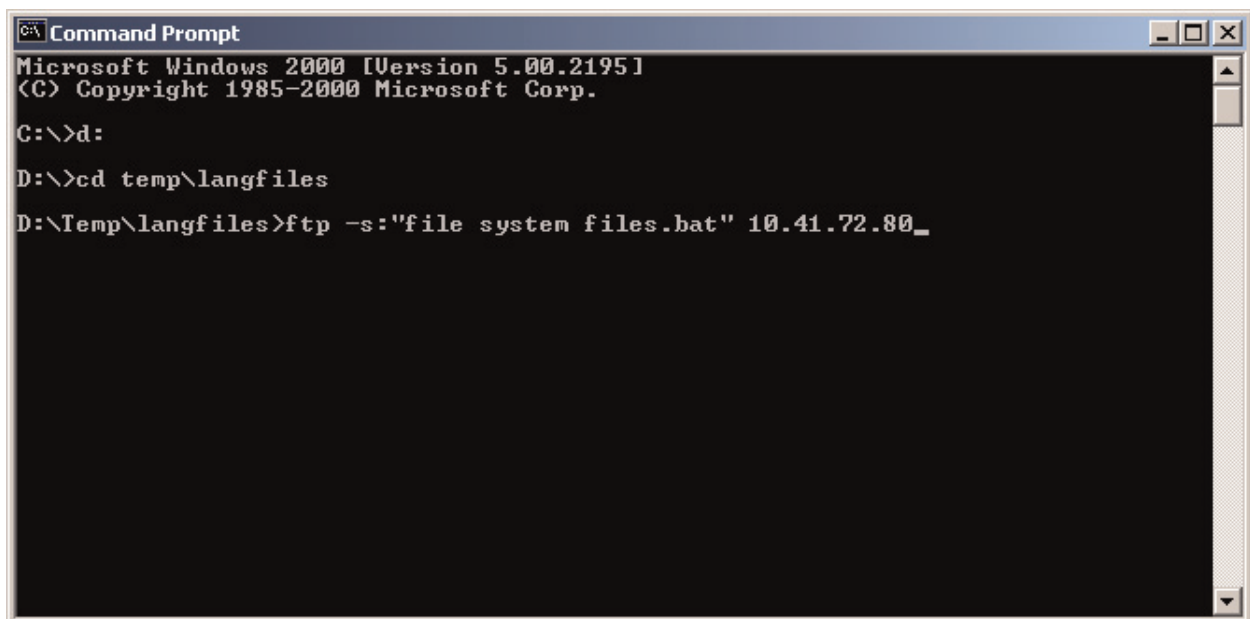
A051105

Fig. 5.9.2.-3   Execute command for the file transfer via ftp

After some seconds, the output should be:

A051106

Fig. 5.9.2.-4   Log file during the file transfer

Language files are now stored in the REF542plus Web server.

6. Communication requirements and network installation

6.1. REF542plus Ethernet physical interface

REF542plus is provided with a standard Ethernet physical connector RJ-45 female. The connector is compliant with IEEE8802.3 10BASE-T standard.

6.1.1. Assignment of the RJ-45 female connector
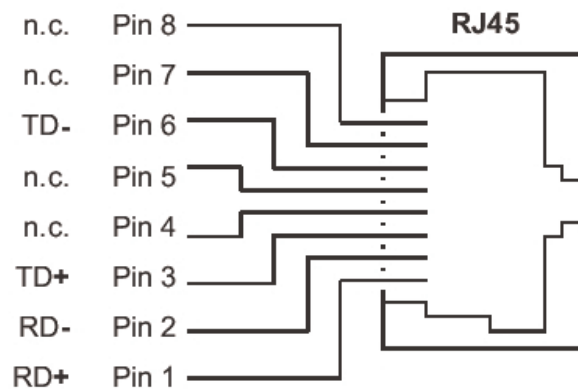
A051107

Fig. 6.1.1.-1   RJ-45 female connector pin assignment

6.1.2. Connecting REF542plus

To connect the Ethernet cable to REF542plus, plug the RJ-45 male connector into the female connector (port X70 of REF542plus core unit) according to the keying until it snaps into place.
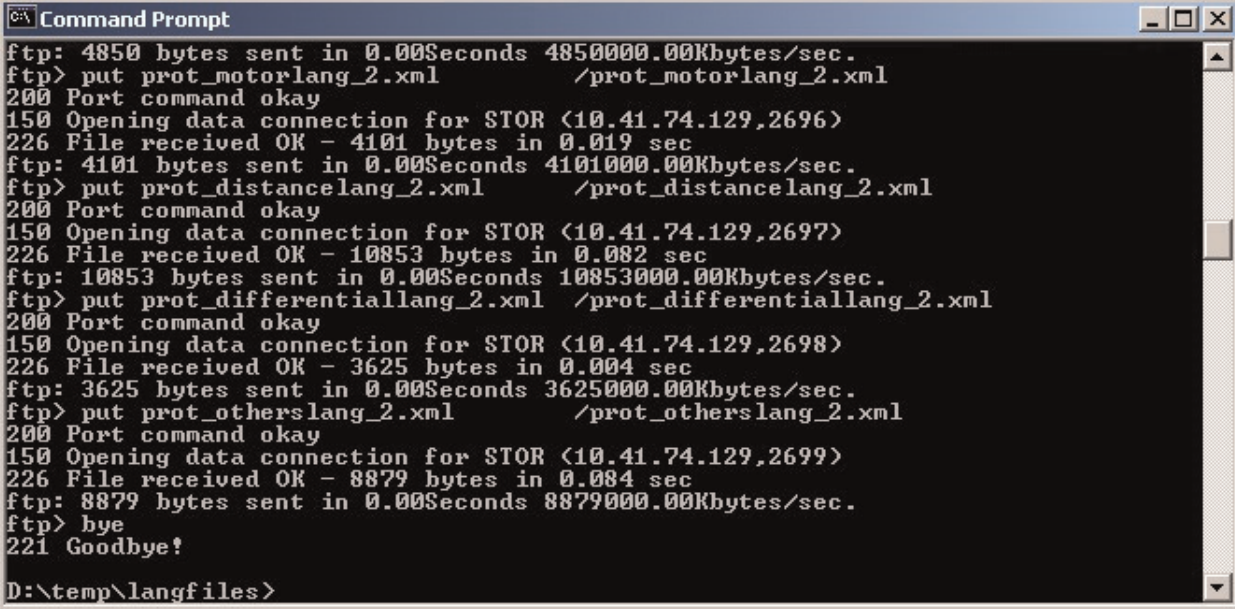
To remove the connector, press the snap-in device in the direction of the connector and then remove the connector.

6.2. Network devices required

To build a network, several additional devices are needed. The requirements for network devices are described in this paragraph. In addition, there is an ABB recommendation for each device.

6.2.1. Network cables

The cable connected directly to REF542plus Ethernet port has to be a shielded twisted-pair Industrial Ethernet cable, compliant with IEEE8802.3 10BASE-T standard and of category 5 (CAT-5), with an impedance of 100 Ω and standard RJ-45 male connectors at both ends.

Fig. 6.2.1.-1 shows the pin assignment in case:

- Cross Over connection cable: the cable connects REF542plus directly to a PC in a point-to-point fashion and REF542plus is not connected in a network. The same cable is needed to connect two hubs between them.

- 1:1 or straight through cable: the cable connects REF542plus to a standard Ethernet device such as hub or switch and REF542plus belongs to an Ethernet network.
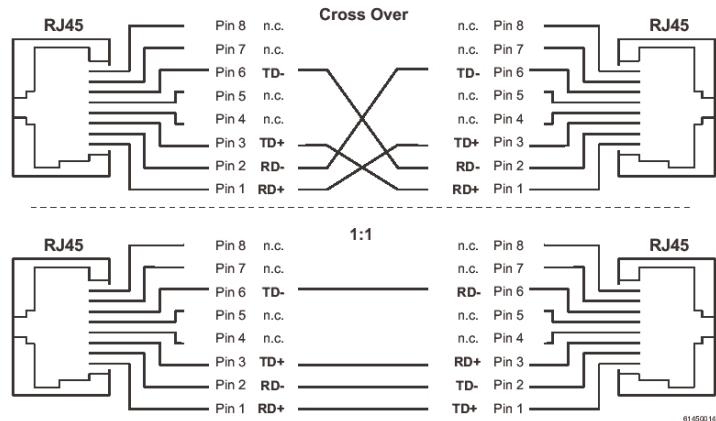
A051108

Fig. 6.2.1.-1   Pin assignment of Cross Over and 1:1 cable

> **i** ABB cable recommendation for REF542plus connection to a switch

- Phoenix Contact FL CAT5 FLEX, CAT 5-S/UTP cable (J-LI02YS(ST)C H 2 x 2 x 26 AWG), light-duty, flexible installation cable 2 x 2 x 0.14 mm², stranded, shielded, outer sheath: 5.2 mm diameter, preassembled on both sides with RJ 45 connector, crossover or line assignment.

- For connections with switch outside the switch gear, the heavy version is suggested: CAT 5-S/UTP cable (J-02YS(ST)C HP 2 x 2 x 24 AWG), heavy-duty installation cable 2 x 2 x 0.22 mm², solid conductor, shielded, outer sheath: 7.8 mm diameter, inner sheath: 5.2 mm diameter, preassembled on both sides with RJ-45 connector, crossover or line.

6.2.2. Using media converter

The Ethernet network in which REF542plus devices are connected may be based on different solutions about physical cables, depending on the particular plant topologies, requirements, environment, customers, connection with other subsystems, and so on.

Multifunctional Protection and Switchbay Control Unit   **REF542plus**

Installation Manual for Web Interface

Installation manual

⚠ Although transient suppression circuitry is present on Ethernet RJ-45 port of REF542plus, the high amplitude transients can potentially damage the port and its link partners. It is recommended to use RJ-45 ports only inside the switchgears or inside environments sufficiently protected.

⚠ For the substation applications, it is not recommended to use RJ-45 to interface to field devices across distances, which could produce high levels of ground potential rise (that is greater than 2.5 kV) during the line to ground fault conditions.

Therefore, for the highest noise immunity requirements in industrial applications, mixed topology solutions based both on twisted pairs and optical connections (for longer distances and/or outside the switch gear) would be better. See Section 6.3. Network topology and Section 6.3.6. Integration within the switchgear for more information about topologies.

The version of fiber optic cable to use depends on the required distance range. Fiber optic distances up to 50 m (164.04 ft.) can be covered with plastic optical fiber (POF) by using easy to operate polymer fiber technology. For distances up to 100 m (328.08 ft.), HCS fiber, also easy to assemble, can be used together with optical connection conforms to the F-SMA standard. If longer distances are to be covered or if an existing glass fiber installation is used, the glass fiber optic can normally cover transmission distances up to 3000 m (9842.52 ft.) by using multimode glass fiber HCS with connection conforms to the ST® (B-FOC) standard.

ABB recommendation for Media Converters:

* Phoenix Contact FL MC 10/100BASE-T/FO POF, FL MC 10/100BASE-T/FO G850, and so on.

6.2.3.   Hubs

ABB recommendation for hubs:

* Phoenix Contact FL HUB 10BASE-T can be used to expand a network quickly and cost-effectively. It has four twisted pair ports. It can be used together with other hubs to create a multi-port repeater with up to 20 ports.
* The FL HUB AGENT version also has an agent, which can provide comprehensive system diagnostics for all the connected ports.

6.2.4.   Switches

A switch is a device that channels incoming data from any of multiple input ports to the specific output port that will take the data towards its intended destination. On a LAN, the switch determines from the physical device address (MAC) in each incoming message frame to which output port to forward it to and back.

Even if for WebREF both the hubs and switches are allowed, for the industrial networking environments, a fully switched Ethernet architecture is the most appropriate choice.

In a fully switched network, there are no hubs and therefore each network has a dedicated segment for every node. Because the only devices on each segment are the switch and node, the switch picks up every transmission before it reaches another node and then forwards the data only over the appropriate network segment. In a fully switched network, the nodes only communicate with the switch and never directly with each other. For more information on the network structures, see Section 6.3. Network topology .

ABB recommends for switches:

*   For small plants, ABB recommends Phoenix Contact FL SWITCH 8TX, Ethernet switch, 8 front Ethernet ports in RJ-45 format, automatic detection of data transmission rate of 10/100 Mbps, coupling network segments with different transmission rates, auto-crossing function, DIN rail mountable.
*   For medium-large plants and especially if the network has composed of several sub-networks, ABB recommends Phoenix Contact Modular Switch System, that can be seamlessly expanded from 8 ports up to 24 ports, offering a flexible cable outlet - either at the bottom or at the front - depending on the requirements of the installation and location. Interface modules are available for twisted pair, glass fiber or even cost-effective Ethernet installations by using polymer and HCS fibers.
*   For harsh environments and/or particularly critical applications, ABB recommends OnTime Networks switches (U200 series or R200), or RuggedCom switches (RuggedSwitch^{TM} - RS8000T or RS1600T).

6.2.5.   Router

A router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to.

See Section 6.5. Communication system security for more information about the use of standard Ethernet router and security requirements.

ABB recommendation for routers:

- For connections directly from the substation and installation in the switch gear, ABB recommends Westermo ED-20. It is an industrialized DIN Rail mounted serial to Ethernet router. The device will allow access to a remote Ethernet network via a PSTN, ISDN or radio modem.

- For connections to corporate intranet and/or installation in control room (or not harsh industrial environment), ABB recommends any off-the-shelf standard Ethernet router integrated in PC (software router) or hardware device may be used (for example CISCO). The rack version for modularity and performance reasons it is suggested rather than the software version running on PC.

6.3. Network topology

6.3.1. Bus topology

A typical bus topology is illustrated in Fig. 6.3.1.-1
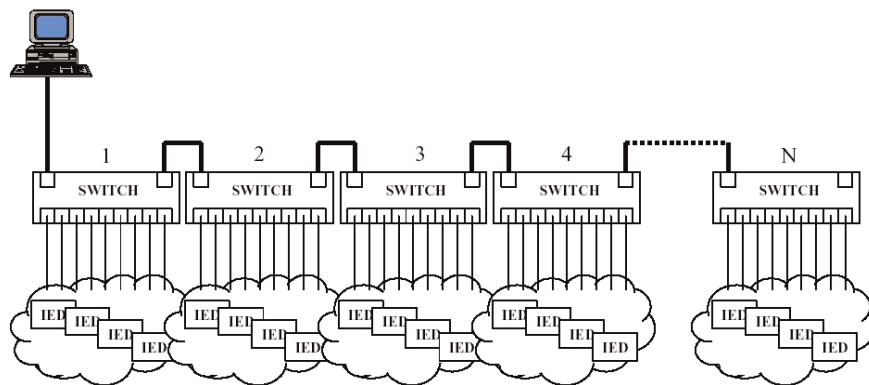
A051109

Fig. 6.3.1.-1   Bus topology

Each switch is connected to the previous switch or next switch in the cascade via one of its ports (uplink port).

The bus topology is recommended for small plants for its cost effective advantage. The main disadvantage is to have a big latency to reach the last device of the bus from the PC.

6.3.2. Star topology

A typical star topology is illustrated in Fig. 6.3.2.-1.

REF542plus

**Multifunctional Protection and Switchbay
Control Unit**

1MRS755865

Installation Manual for Web Interface

Installation manual

A051110

Fig. 6.3.2.-1   Star topology

Switch N is referred to as the "backbone" switch, since all the other switches
uplink to it in order to form a star configuration.

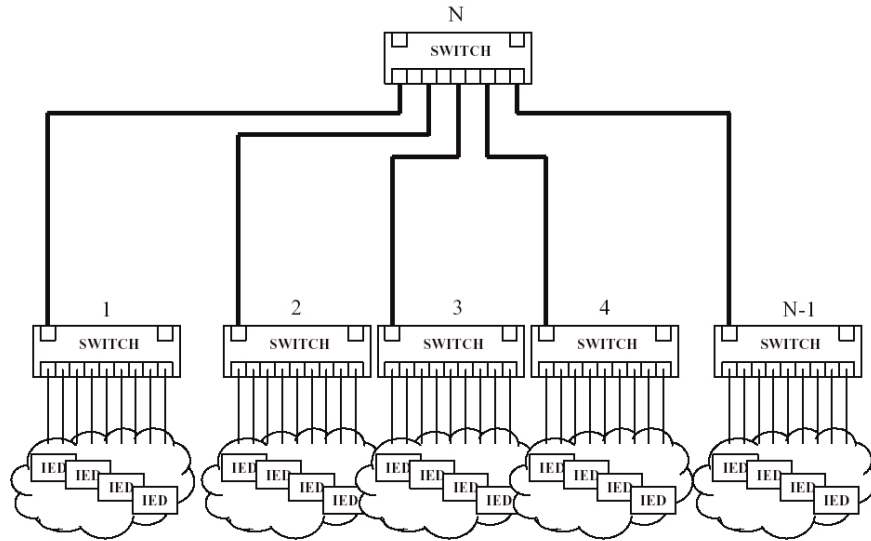This architecture is recommended for medium or large plants, especially if
they are already organized in subsystems (example: one subsystem for each
switch gear).

> **ℹ** Number of devices for subnet
>
> The number of devices per subnet is limited. The limitation is set
> to 256 devices. A practical subnet size should be defined by the
> application and should have a size of approximately 10 devices.
> In case a GSM Modem is connected, one device per total
> network is sufficient.

6.3.3.   Example of star topology with REF542plus

WebREF is particularly suitable for low-end solutions. The Fig. 6.3.3.-1
shows a typical architecture for low-end systems based on a single network in
star-topology.

Not all depicted devices are mandatory. Example: for an unmanned plant the
operator PC is not mandatory and a laptop can be used only for service,
maintenance, and so on, while the modem sends all information to a remote
control room.
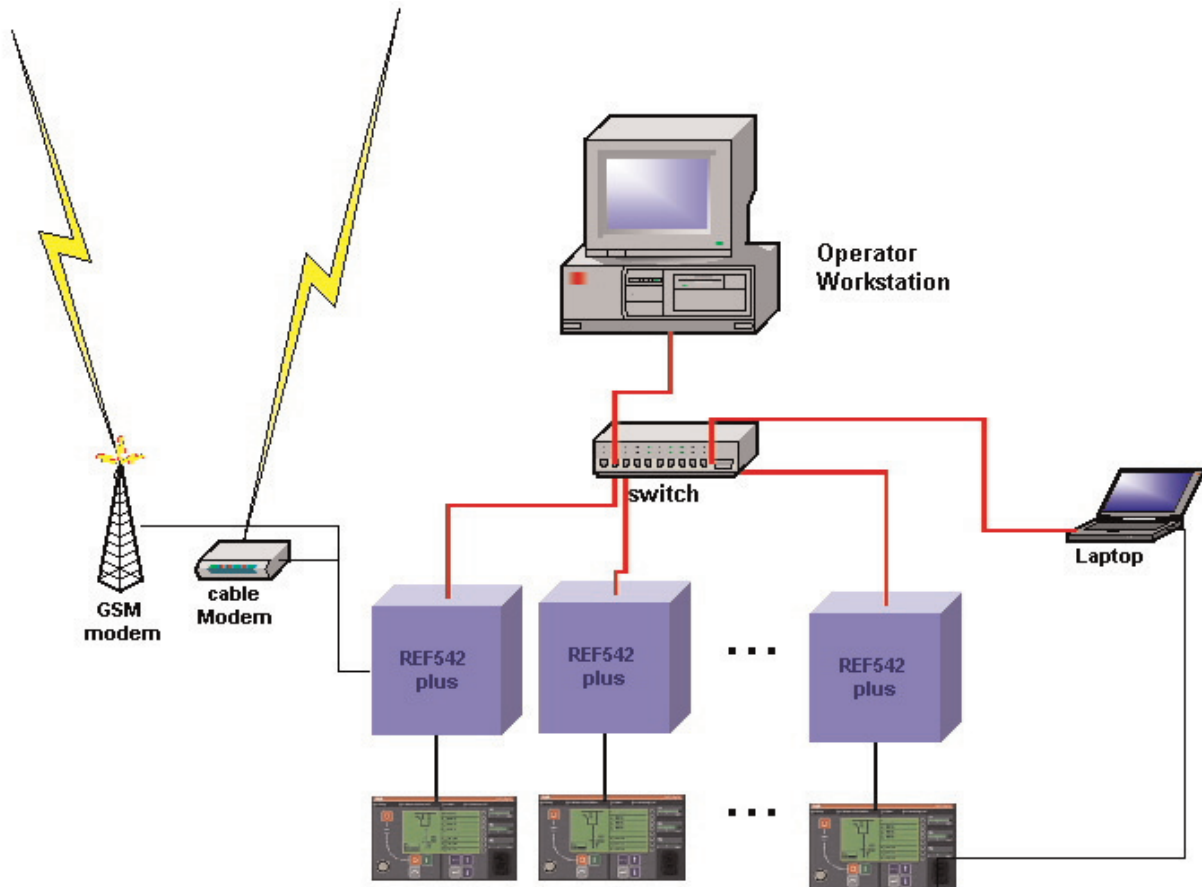
A051111

Fig. 6.3.3.-1   Example of star topology

6.3.4.   Ring topology

A typical ring topology is illustrated in Fig. 6.3.4.-1.

It is very similar to the bus topology except that the loop is closed from the switch N back to switch 1. This provides some level of redundancy, if any of the ring connections should fail.

This topology is more cost effective of the star topology, but less than the bus one. In addition, it offers a redundancy in the loop, but in this case it requires the use of switch able to change to linear topology in case of a fault.
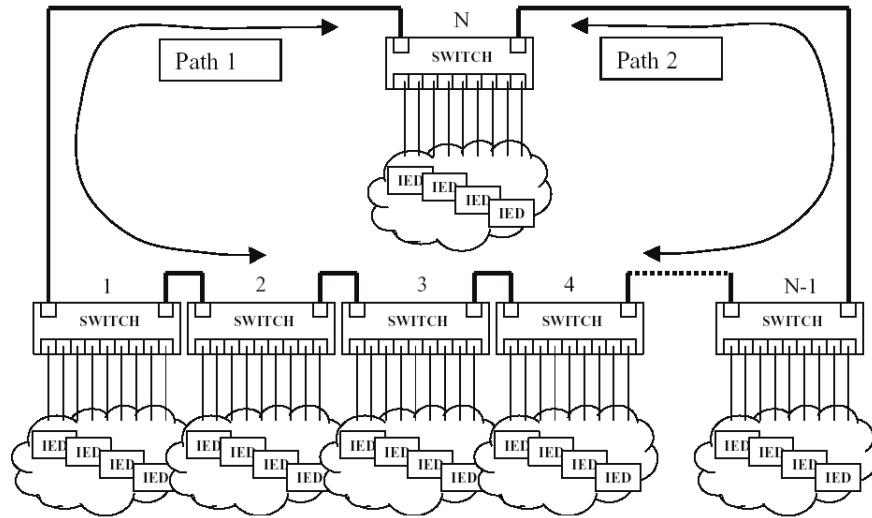
Fig. 6.3.4.-1   Ring topology

6.3.5.   Example of redundant ring topology with REF542plus

Considering the Fig. 6.3.5.-1, the structure is made connecting backbone
ports of switches (generally provided in industrial Ethernet switches).
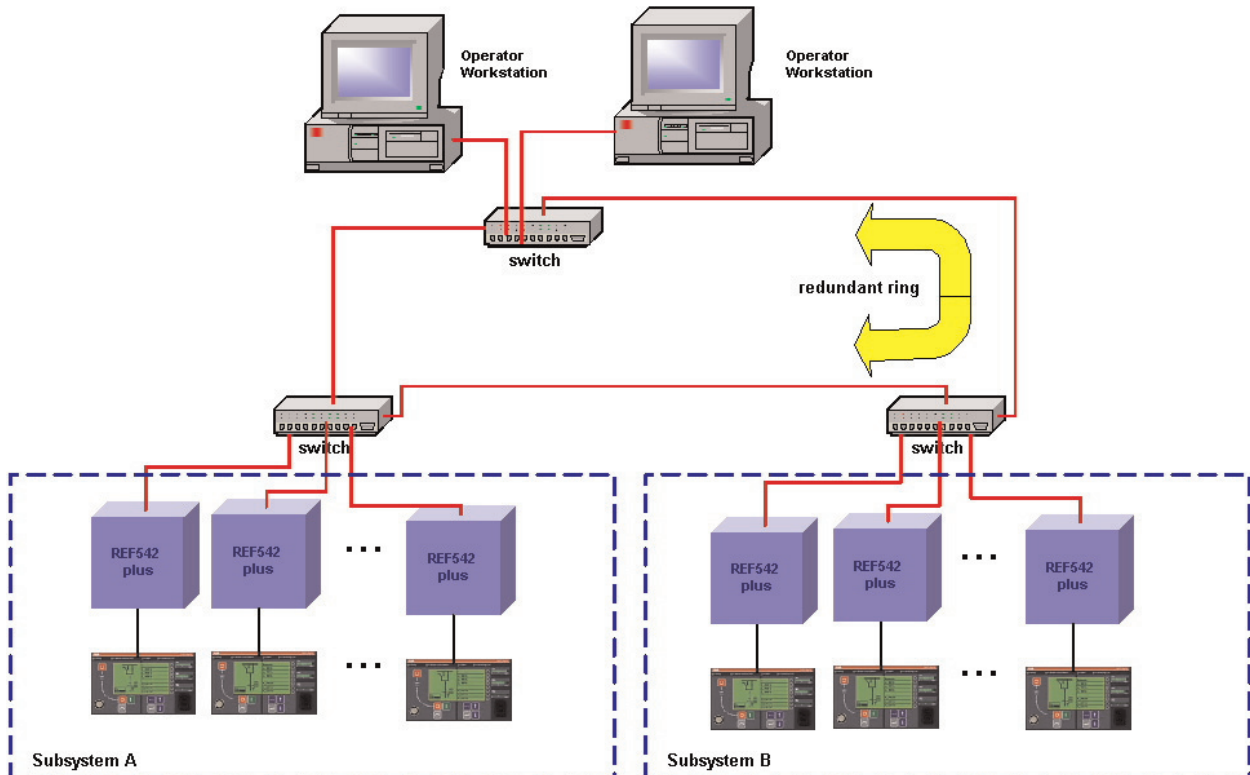
A051113

Fig. 6.3.5.-1   *Example of redundant ring structure*

Each REF542plus is connected by means of a single electrical connection to the switch of its subsystem. The fibre optics cables are recommended for the loop.

By means of the ring structure, it is possible to build a redundant communication system at station level, see Fig. 6.3.6.-1. This is because if any subsection of the loop fails, the ring structure is changed to a linear structure automatically. For this reason, the ring structure is particularly suitable for large plants.

6.3.6.   Integration within the switchgear

With reference to Fig. 6.3.6.-1, for the integration of the Ethernet network inside the switchgear, following basic rules are suggested:

- To use one or more industrial Ethernet switches placed in empty LV cubicles of the switch gear (that is the bus-rise panel) or in an additional empty LV panel. It is preferable to use DIN-rail mounted Ethernet devices. Also, it is preferred, if the Ethernet switch already has the possibility of optical uplink, otherwise the media converters (always DIN-rail mounted) are needed.

- To connect REF542plus devices and the switch by means of shielded and twisted pair cable CAT5 with RJ-45 male connectors.

- To connect the switch externally by means of an optical cable, Plastic Fibre Optic or Glass Fibre Optic depending on the distance and the environment.

- Ethernet cables have to be placed on the roof of the switchgear. Also other solutions can be used (that is using lateral side holes of the LV cubicle). Do not use paths in the power part of the switchgear.
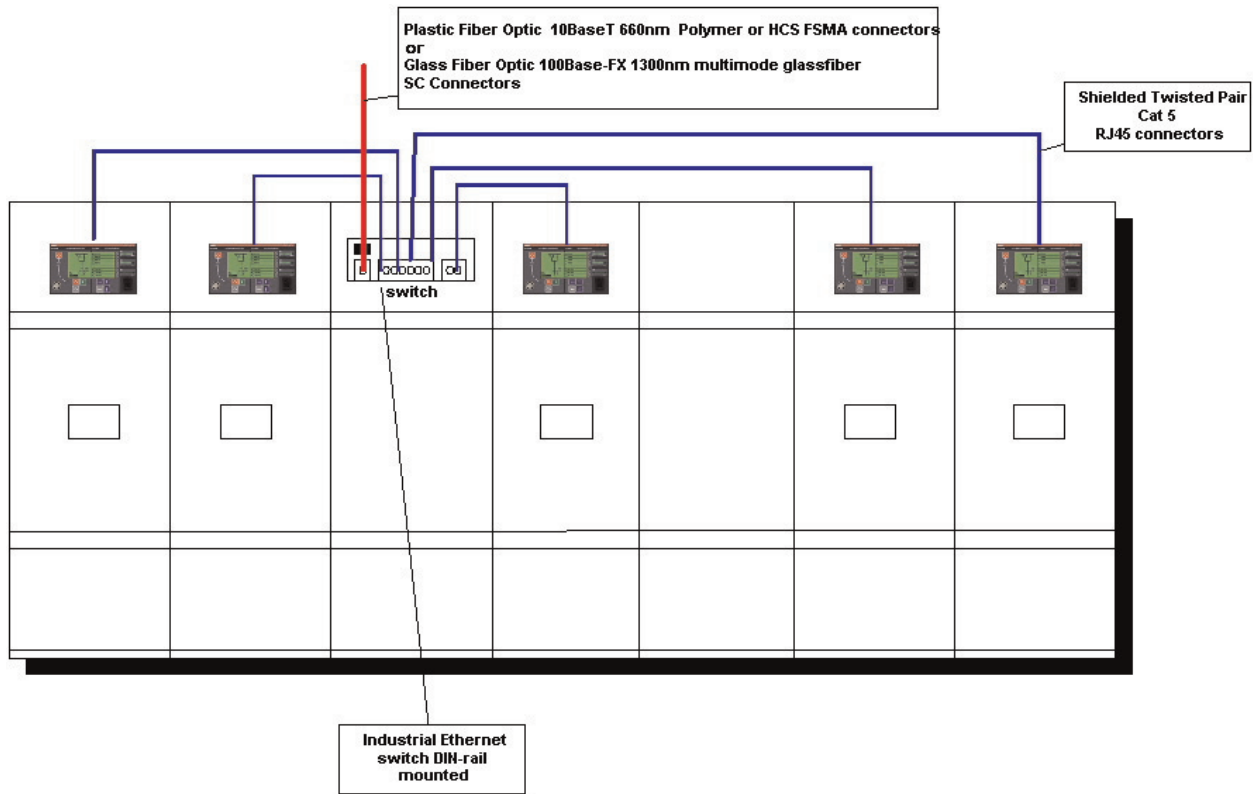
Fig. 6.3.6.-1   *Integration within the switchgear*

6.3.7.   Example of complex topology

Fig. 6.3.7.-1 shows an example of complex topology in which several network solutions are used.

The network is based on a star topology where a modular switch is used as a backbone for the substation. This modular switch is then connected by an optical uplink (glass fibre) to the control room and by optical links (plastic fiber) to the two subnetworks.

Even if the modular switch is the backbone of the communication system, for the cost reasons, the first subnetwork is directly connected to the modular switch and not to a separate switch as in a real star topology.
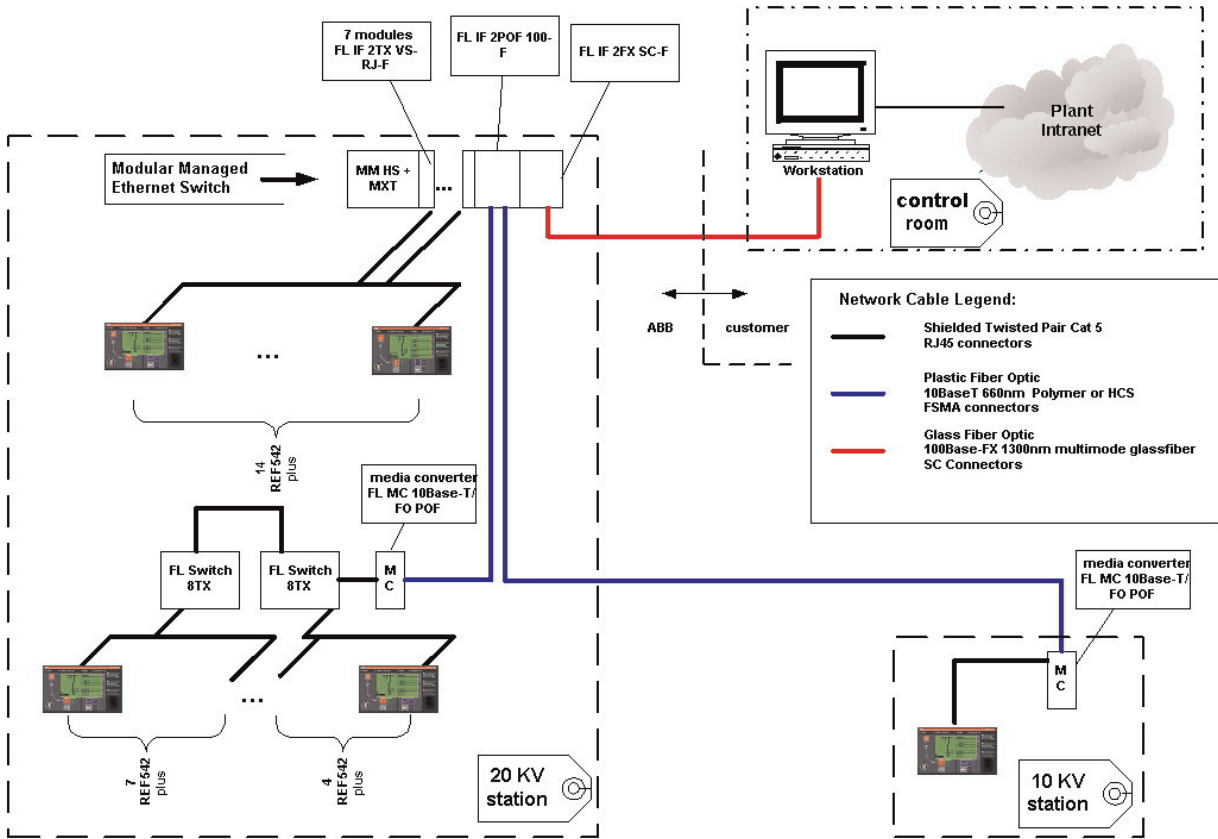
Fig. 6.3.7.-1   Example of complex topology

6.4.   Network address configuration

6.4.1.   MAC address configuration

MAC address is programmed to the core unit in the production phase.

6.4.2.   TCP/IP configuration

For more information regarding IP Address, Subnet mask and Default Gateway address, see Section 7. Terminology.

The IP address is stored in the configuration file (.ref) downloaded by the REF542plus engineering tool. The tools runs on a PC connected point-to-point with the serial port of RHMI.

The REF542plus has a default IP address. To configure the new IP address the operator has to configure the IP address before to connect the REF542plus to the network. This in order to avoid address conflicts between the default IP address and IP addresses already configured in the Ethernet network. The REF is fully TCP/IP standard compatible.

6.4.3.   IP address
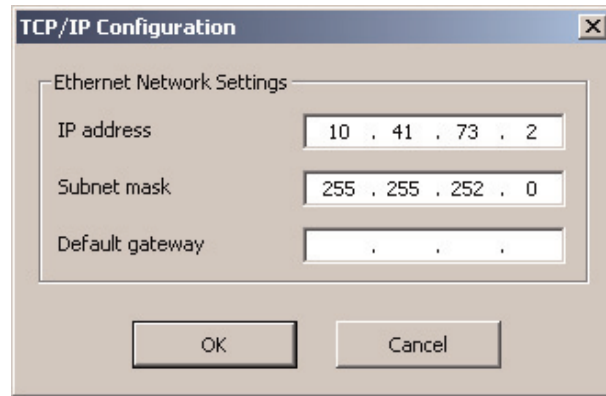
A051117

Fig. 6.4.3.-1   Configuration of the IP address

REF542plus determines only the last two numbers as an IP address. In this case 2 means the device has the number 2 in its sub network. It results in that a maximum of 254 devices per subnet are possible.

> The IP address with the number 10.41.75.255 determines a broadcast address. It is not allowed to configure any addresses with this end figure, because all the users above the subnet mask range are then addressed.

6.4.4.   Subnet mask

The subnet mask can be set as it is needed, but only the 3rd number is determined.
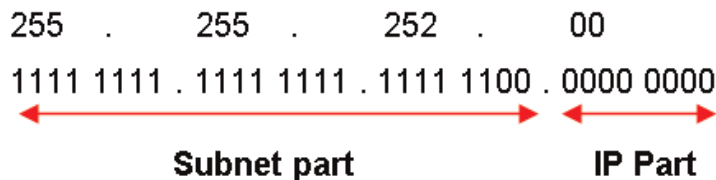
A051172

Fig. 6.4.4.-1   Definition of the subnet mask

It means that a maximum of 254 different sub networks can be configured in REF. The REF is only building a switchgear overview for the matching subnet part. The identification of the subnet part and IP part is REF542plus specific, but is not in conflict with any standard.

> The subnet mask with the number 255.255.255.x determines only one subnet and not any other subnetwork can have access to it. It is allowed to configure sub networks with that mask.

6.4.5. Default gateway configuration

This parameter specifies the gateway IP address. This is the address to use when forwarding packets to a network other than the one the switch belongs to, see Section 6.4.2. TCP/IP configuration for REF542plus parameters' configuration.

> The default gateway configuration is only required if it is intended to address the network configurable devices from a management station separated from them by a router.

> The default Gateway IP address has to be inside the subnet mask.

6.4.6. Example of a subnet configuration

How to create two sub networks: The two networks are identified through the 3rd address identifier.

Table 6.4.6.-1   Example of two sub networks

Subnet 1	Subnet 2
10.41.72.1	10.41.73.1
10.41.72.2	10.41.73.2
10.41.72.3	10.41.73.3

REF is building in this case two switchgear overviews from the two different subnet identifiers, because only the matching 3rd identifiers are moved to one subnet. To see with one computer both the Subnet 1 and Subnet 2, the 3rd identifier in the subnet mask of the computer must set to 255.255.254.00 or below which is IP standard.

Table 6.4.6.-2   Example of subnets and subnet masks

Subnet 1	0100 1000=48h =72
Subnet 2	0100 1001=49h =73
Subnet mask	1111 1110=FEh =254
Subnet mask	1111 1100=FDh =252 (Next possible alternative)

The next possible alternative mask address allows also a wider range of IP addresses to have access to subnet 1 and 2. It means that also other computers can have access to them.

In the example, it would allow the 3rd IP address identifier 48h;49h;4ah;4bh which is in decimal 72;73;74;75.

6.4.7.   Examples of communication system addressing

Communication system addressing should be based on the following network design rules:

• The router and REF542plus devices belonging to the LAN plant have to have the same subnet mask address.

• The default gateway address configured in each REF542plus has to be equal to the IP address of the router.

• The IP addresses of REF542plus have to be consecutive.
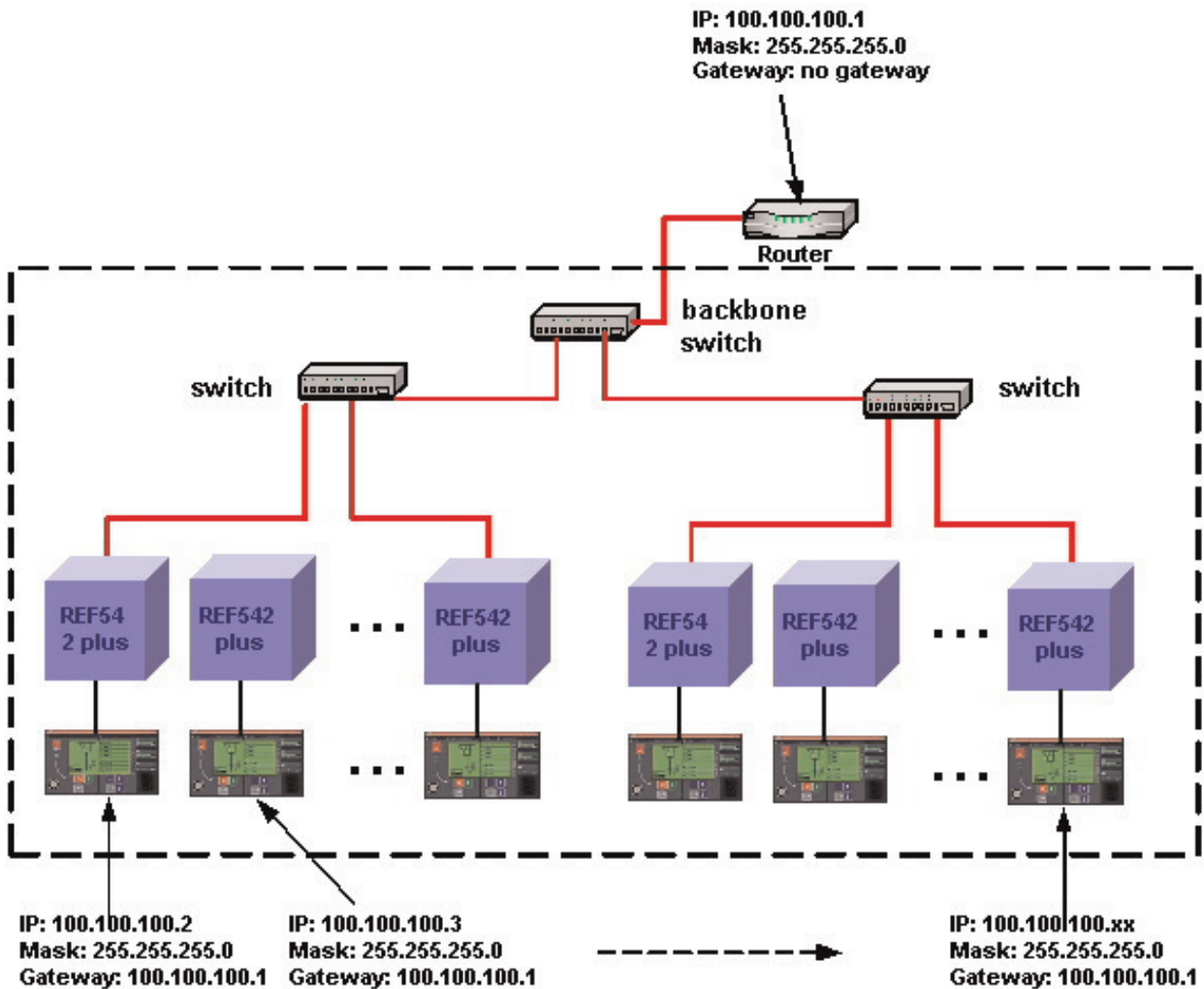
A051118

Fig. 6.4.7.-1   Example of network addressing with router

Fig. 6.4.7.-2 shows an example in which a PC is used to interface the LAN plant with the Corporate WAN. The PC is mandatory and it has run as a server if the Corporate WAN uses DHCP, see PC addressing in Fig. 6.4.7.-2.

This is the typical case in which the PC is a workstation in control room or a dedicated server PC belonging to the network in control room. If a remote connection, that is ISDN, is needed, a router has to be connected to Ethernet network 2 and not directly to 1.

Note the DHCP configuration for the server in the example. This is necessary to have a "transparent" access to REF542plus from the Corporate WAN side.

PC ADDRESSING

Ethernet card 1
IP: 100.100.100.1
Mask: 255.255.255.0
Gateway: no gateway

Ethernet card 2
IP: 205.138.44.162
Mask: 255.255.255.240
Gateway: 205.138.44.161

DHCP range
From 100.100.100.2
To 100.100.100.254
Mask 255.255.255.0
No gateways assignis to client

IP: 100.100.100.2
Mask: 255.255.255.0
Gateway: 100.100.100.1

IP: 100.100.100.3
Mask: 255.255.255.0
Gateway: 100.100.100.1

IP: 100.100.100.xx
Mask: 255.255.255.0
Gateway: 100.100.100.1

A051119

Fig. 6.4.7.-2   *Example of network addressing with PC server*

6.5. Communication system security

Required for customers connecting to intranet or Internet only.

6.5.1.　　　　Access through standard Ethernet router

It is mandatory to connect the LAN plant to the Internet or to intranet by means of a router offering at least the basic security functions, such as IPSec, password protection and so on. See
Section 5.5.1. Security features on writing operations, passwords and user names about Security for more information on the security issues.
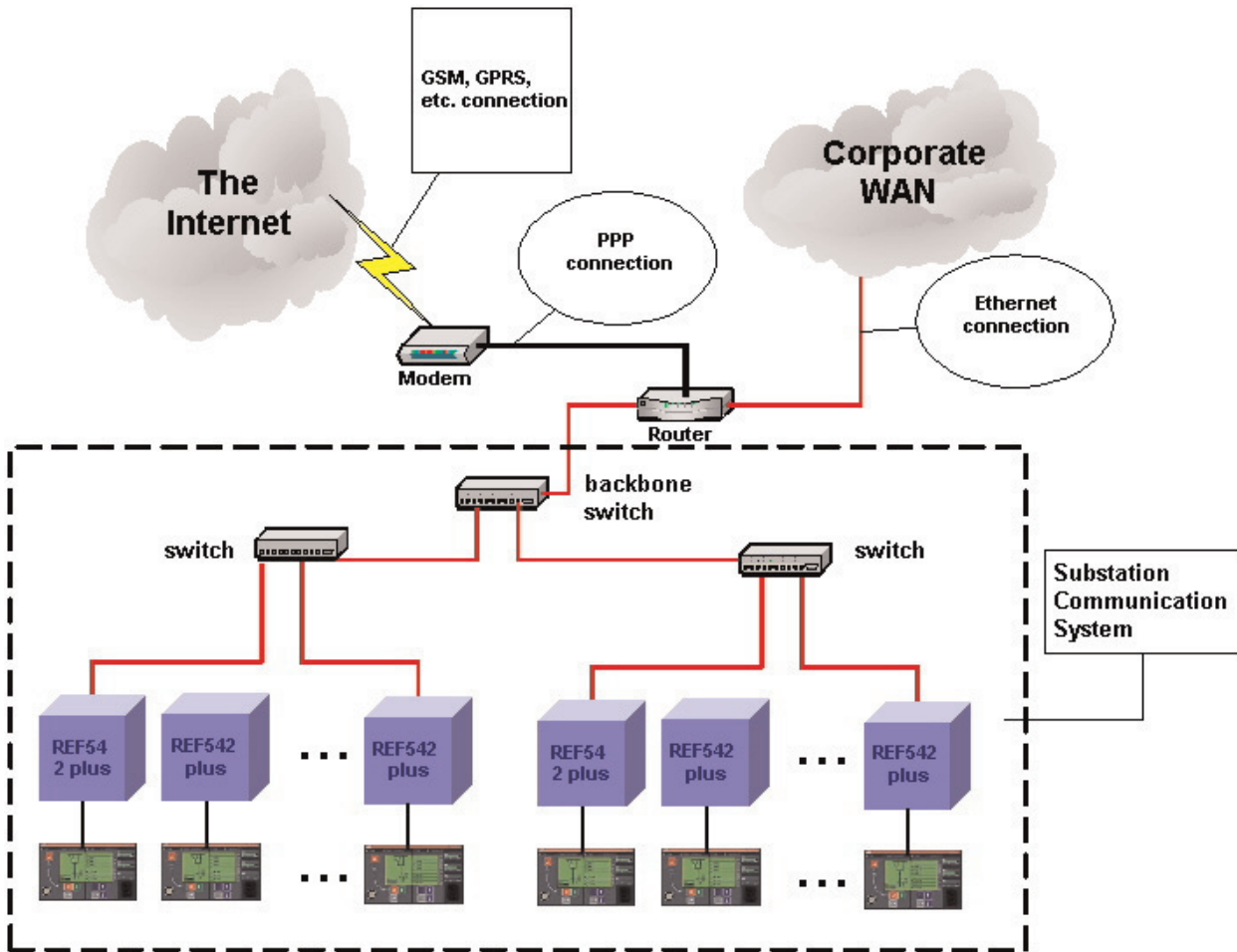
Fig. 6.5.1.-1　　　Connection to the Internet or to Intranet

6.5.2.　　　　IPSec function

The principle features of IPSec are the encryption and authentication of all traffic at the IP layer. A further functional area is the key management. Authentication assures that a received packet was really sent by the source indicated in the packet header, and that the data in the packet coincide with the data sent. By using encryption, listening of the data by third parties has no effect. The key management is responsible for the secure exchange of the

keys. This feature needs to be enabled on the operating system on client's side as well. Otherwise, the incoming data is not processed as pinging is not a function.

IPSec major benefits are:

- IPSec is below the transport layer and therefore transparent to applications. The software on user or end system does not need to be adapted, if IPSec is implemented in a firewall or router.
- IPSec can be implemented in a firewall or router providing a security tunnel between the two isolated networks. While the strongest security is transparently provided for the traffic between the two networks, the inner network traffic is not affected or delayed.

7. Terminology

Term	Description
Configuration Tool	Software program to configure the REF542plus. This program runs on a PC.
Default Gateway	The default gateway address is your router or switch IP address that does the address forwarding in case the IP address of the receiver in not the subnet of the sender.
IP Address	An IP (Internet Protocol) address is a unique identifier for a node or host connection on an IP network. An IP address is represented as 4 decimal values separated by decimal points. This is known as "dotted decimal" notation. Example: 140.179.220.200The IP address and the subnet mask determine which part belongs to the network address and which part belongs to the node address.
Subnet mask	To have a subnet in an IP Network can be done for a variety of reasons, including organization, use of different physical media (such as Ethernet, FDDI, WAN, etc.), preservation of address space, and security. The most common reason is to control network traffic. In an Ethernet network, all nodes on a segment see all the packets transmitted by all the other nodes on that segment. Performance can be adversely affected under heavy traffic loads, due to collisions and the resulting retransmissions. A router is used to connect IP networks to minimize the amount of traffic each segment must receive.Applying a subnet mask to an IP address allows you to identify the network and node parts of the address. The 1s in the mask represents the network bits, and the 0s represents the node bits. Performing a bitwise logical AND operation between the IP address and the subnet mask results in the Network Address or Number.
Web Interface	Monitoring interface, which retrieves data from the REF542 plus. The interface is based on an Internet browser running on a standard PC with Win 2000 or NT installed.

8.   Abbreviations

Abbreviation	Description
AES	Advanced Encryption Standard
IP	Internet Protocol
LAN	Local area network
LED	Light-Emitting Diode
LV	Low voltage
RHMI	Remote human-machine interface as control unit
SCL	Substation Configuration Language (defined by IEC 61850)
SLD	Single-line diagram

9.   Appendix A: Generate language files

To modify the language file, it is requested from the engineering person to have some basic knowledge of handling files. The files have to be stored when modified and then downloaded, see Table 9.-1. No compilation or linking is required.

> If you have done a translation of the files into a new language, please send it to SA-D Supportline, which will insert it in the Intranet Online Support site.

The following language files can be modified by the engineer to the second language as user defined:

Table 9.-1   Modified language files

	File Name
1	BinaryIO_Inputslang_english.xml
2	BinaryIO_Outputslang_english.xml
3	service_statisticslang_english.xml
4	service_versionslang_english.xml
5	service_tcpipsetlang_english.xml
6	service_hwidentlang_english.xml
7	helplang_english.xml
8	measlang_english.xml
9	faultreclang_english.xml
10	alarmslang_english.xml
11	striplang_english.xml
12	menulang_english.xml
13	messaginglang_english.xml
14	languagelang_english.xml
15	prot_currentlang_english.xml
16	prot_voltagelang_english.xml
17	prot_motorlang_english.xml
18	prot_distancelang_english.xml
19	prot_differentiallang_english.xml
20	prot_otherslang_english.xml

Some general rules have to be respected:

- Never change text inside brackets.

  Example: **<Title>**Messwerte**</Title>**

- Never change what is inside (content) SAdr

  Example: <SAdr>**005**</SAdr>

- Never change filenames

    Example: <Page2>**control_page.htm**</page2>

- Never change items containing the "Underline" character

    Example: <DataSetName>**BinaryIO_Outputs**</DataSetName>

Everything else can be translated when respecting the rules above.

Finally, the translated files have to be stored in your local PC with the "Name_2.xml" filename as shown in Table 9.-2. The word "_English" has to be removed from the filename.

See examples:

Table 9.-2   Example of file names

	File name
1	BinaryIO_Inputslang_2.xml
2	BinaryIO_Outputslang_2.xml
3	service_statisticslang_2.xml
4	service_versionslang_2.xml
5	service_tcpipsetlang_2.xml
6	service_hwidentlang_2.xml
7	helplang_2.xml
8	measlang_2.xml
9	faultreclang_2.xml
10	alarmslang_2.xml
11	striplang_2.xml
12	menulang_2.xml
13	messaginglang_2.xml
14	languagelang_2.xml
15	prot_currentlang_2.xml
16	prot_voltagelang_2.xml
17	prot_motorlang_2.xml
18	prot_distancelang_2.xml
19	prot_differentiallang_2.xml
20	prot_otherslang_2.xml

A special handling is needed for the Alarm page. This is a dynamic page, which means that the text to be modified on the page is not static, because the text depends on the configuration and can be any text instead. (Example: LED 1: TRIP 10KV Outgoing West). For details see Section 9.1. Alarmslang page.
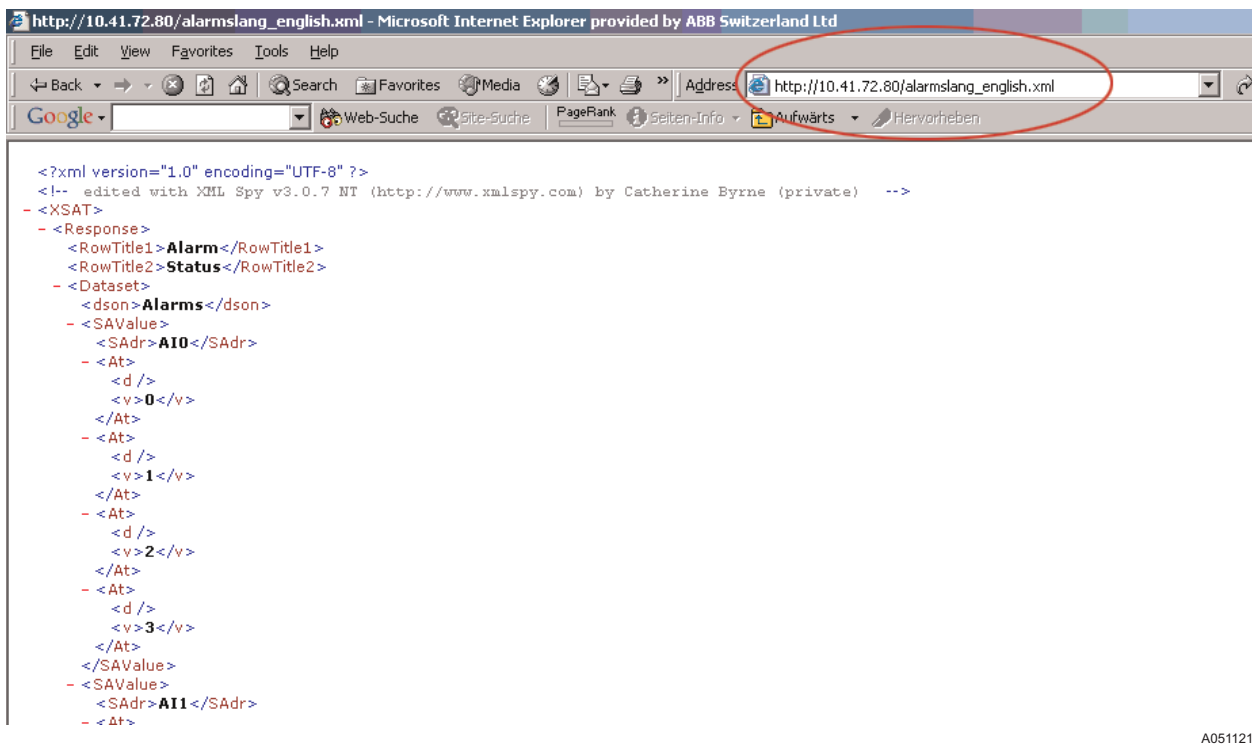
9.1. Alarmslang page

This page has a configuration depending text content and needs a special handling for translation. Here is described one of the several methods:

1. Open the Internet browser and browse the REF542plus device where you want to update the language of the Alarm page.
2. Type in XML file name (alarmslang_english.xml) of the Alarms page language file to see its contents.
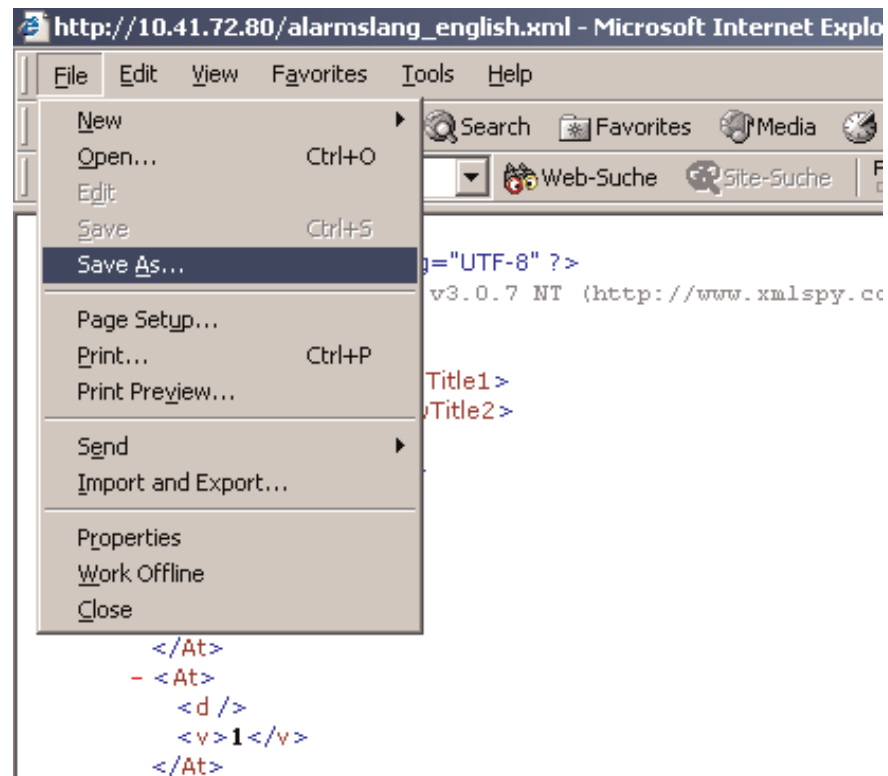
   Example:

   http://10.41.72.80/alarmslang_english.xml

A051121

*Fig. 9.1.-1   Example of the alarm slang page*

3. Save the file content to your directory where you can locally modify the files.

A051122

Fig. 9.1.-2   Saving the alarm slang page

4. Now the alarms language file is stored as configured. It means that the content of the alarm text done with the Configuration tool is available for modification.

5. Open your editor for example Notepad and modify the text. Translate Title, Rowtitle1 and Rowtitle2 into your language. In addition translate the D-tag (descriptor) and the U-tag (Unit) for each SAvalue tag into your language.

6. Change the file encoding to "UNICODE" to have the support for all the special characters.
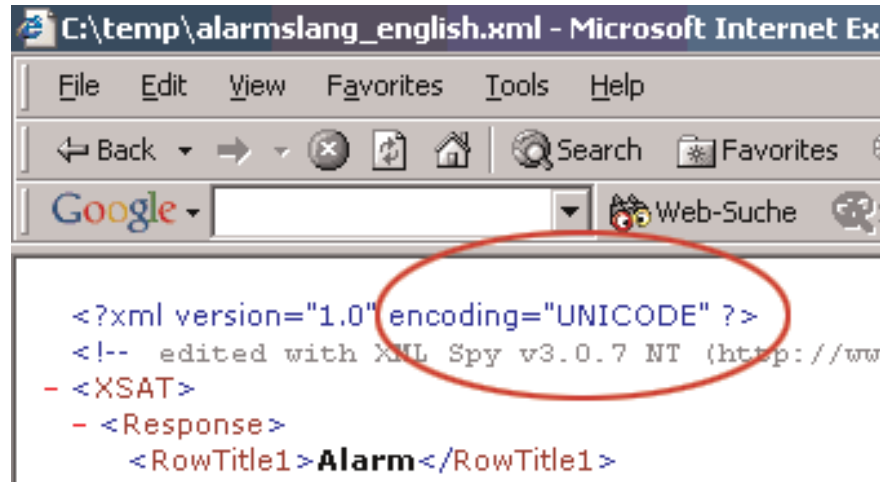
Fig. 9.1.-3   Define the UNICODE file encoding

7. Save the modified file with the "Name_2.xml" name conversion. It means that the _English extension needs to be replaced from the filename with "_2". Filename: alarmslang_2.xml instead of alarmslang_English.xml.

9.2. BinaryIO_Inputslang page

- Translate Title, Rowtile1 Rowtitle2 and DataSetName.
- Translate the D-tag (descriptor) and the U-tag (Unit) for each SAvalue tag into your language as wanted.
- Store the modified file under the filename: BinaryIO_Inputslang_2.xml.

9.3. BinaryIO_Outputslang page

- Translate Title, Rowtile1 Rowtitle2 and DataSetName.
- Translate the D-tag (descriptor) and the U-tag (Unit) for each SAvalue tag into your language as wanted.
- Store the modified file under the filename: BinaryIO_Outputslang_2.xml.

9.4. Faultreclang page

- Translate Title, Rowtile1, Rowtitle2 and DataSetName.
- Translate the D-tag (descriptor) and the U-tag (Unit) for each SAvalue tag into your language as wanted.
- Store the modified file under the filename: faultreclang_2.xml

9.5. Helplang page

Translate the Title and store the modified file under the filename: helplang_2.xml.

9.6. Languagelang Page

- Translate the Title and HelpItem.
- Store the modified file under the filename: languagelang_2.xml

9.7. Measlang page

- Translate the Title, Rowtitle1 and Rowtitle2
- Translate the D-tag (descriptor) and the U-tag (Unit) for each SAvalue tag into your language.
- Store the modified file under filename: measlang_2.xml.

9.8. Menulang page

- Translate the menu header as requested.
- Do not change the contents of the filename: <Page3>**prot_voltage_frame.htm**</page3>
- Store the modified file under the filename: menulang_2.xml

9.9. Messaginglang page

- Translate the Title and Text
- Store the modified file under the filename: messaginglang_2.xml

9.10. Prot_currentlang page

- Translate the Title, Rowtitle1, Rowtitle2 and Dson into your language.
- Translate the D-tag (descriptor) and the U-tag (Unit) for each SAvalue tag into your language.
- Store the modified file under filename: prot_currentlang_2.xml.

9.11. Prot_differentiallang page

- Translate the Title, Rowtitle1,Rowtitle2 and Dson into your language.
- Translate the D-tag (descriptor) and the U-tag (Unit) for each SAvalue tag into your language.
- Store the modified file under filename: prot_differentiallang_2.xml

9.12. Prot_distancelang Page

Translate Title, Rowtitle1,Rowtitle2 and Dson into your language.

Translate for each SAvalue tag the D-tag (descriptor) and the U-tag (Unit) to your language. Store the modified file under filename: prot_distancelang_2. xml

9.13. Prot_voltagelang page

- Translate the Title, Rowtitle1, Rowtitle2 and Dson into your language.
- Translate the D-tag (descriptor) and the U-tag (Unit) for each SAvalue tag into your language.
- Store the modified file under the filename: prot_voltagelang_2.xml.

9.14. Prot_otherslang page

- Translate the Title, Rowtitle1, Rowtitle2 and Dson into your language.
- Translate the D-tag (descriptor) and the U-tag (Unit) for each SAvalue tag into your language.
- Store the modified file under the filename: prot_otherslang_2.xml

9.15. Service_hwidentlang page

- Translate the Title, Rowtile1, Rowtitle2 and DataSetName.
- Translate the D-tag (descriptor) for each SAvalue tag into your language as wanted.
- Store the modified file under the filename: service_hwidentlang_2.xml.

9.16. Service_ statisticslang page

- Translate the Title, Rowtile1, Rowtitle2 and DataSetName.
- Translate the D-tag (descriptor) for each SAvalue tag into your language as wanted.
- Store the modified file under the filename: service_statisticslang_2.xml

9.17. Service_ versionslang page

- Translate the Title, Rowtile1, Rowtitle2 and DataSetName.
- Translate the D-tag (descriptor) for each SAvalue tag into your language as wanted.
- Store the modified file under the filename: service_versionslang_2.xml..

9.18. Service_ tcpipsetlang page

- Translate the Title, Rowtile1, Rowtitle2 and DataSetName.
- Translate the D-tag (descriptor) for each SAvalue tag into your language as wanted.
- Store the modified file under the filename: service_tcpipsetlang_2.xml.

9.19. Striplang page

Translate the Title and Rowtile1 to 4.

Translate the D-tag (descriptor) for each SAvalue tag into your language as wanted.

Store the modified file under the filename: striplang_2.xml.

ABB