EtherNet/IP Scanner for SIMATIC

S7-1200/ S7-1500/ EtherNet/IP

https://support.industry.siemens.com/cs/ww/en/view/109782314

Siemens Industry Online Support

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

 **DANGER**	**indicates that death or severe personal injury will result if proper precautions are not taken.**

 **WARNING**	**indicates that death or severe personal injury may result if proper precautions are not taken.**

 **CAUTION**	**indicates that minor personal injury can result if proper precautions are not taken.**

NOTICE	**indicates that property damage can result if proper precautions are not taken.**

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by personnel qualified for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

 **WARNING**	**Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.**

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit https://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under https://www.siemens.com/industrialsecurity.

Table of contents

1 Preface

Purpose

This document contains information about the LCCF_EnetScanner function block for SIMATIC S7-1200 and S7-1500. It will explain its usage and parameterization as well as provide some basic background information about the implemented services defined by the ODVA®.

Core content

The following core issues are covered in this document:

- Purpose of the function block
- Parameterization
- Data exchange with EtherNet/IP adapters

Required basic knowledge

General knowledge in communications over Ethernet, programming and configuring the S7-1200 or S7-1500 with the TIA Portal is assumed and will not be part of this document. It is also assumed that the terms Server and Client and their meaning are familiar to the reader. Furthermore, the reader shall be proficient in the technology of PROFINET as several concepts will be referred to.

Delimitation

The document does not describe:

- How to setup Ethernet networks
- How to assign IP addresses and the split into subnets
- How to configure the controllers in this example
- How to configure the LCCF_EnetAdapter function block for SIMATIC S7
- How to take network traces and/ or analyze network traffic

Basic knowledge about the above topics is assumed.

Validity

This document is valid for the following components

- TIA Portal
- SIMATIC S7 Controller

The following hardware and software are used throughout this document.

Table 1-1: used components

Name	Part number	Version
SIMATIC S7-1215C	6ES7 215-1AG40-0XB0	V4.2 (or above)
SIMATIC S7-1512C	6ES7 512-1CK00-0AB0	V2.6 (or above)
ET200SP MF	6ES7155-6MU00-0CN0	V5.0 (or above)
TIA Portal STEP7 Prof.		V15.1 Update 4
MFCT		V1.0

In this application example the S7-1500 is operated as EtherNet/IP Scanner, while the S7-1200 is operated as EtherNet/IP adapter.

The application example for the LCCF_EnetAdapter function block can be downloaded using the SIOS ID: 109782315

https://support.industry.siemens.com/cs/ww/en/view/109782315

2 Introduction

2.1 Description

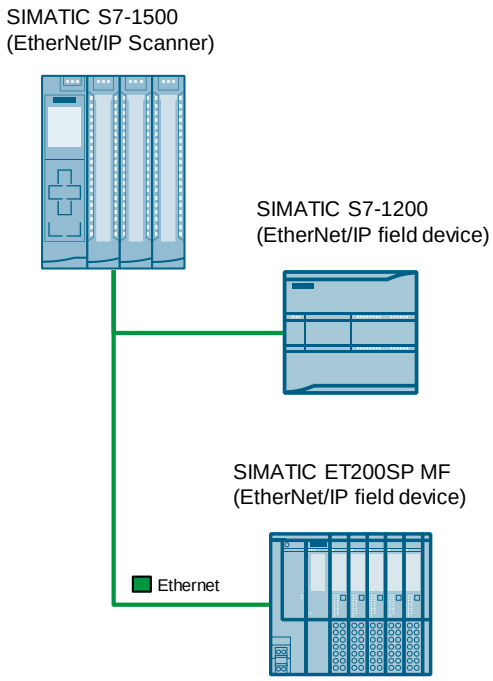
Although, according to the number of installed nodes PROFINET is the largest Ethernet based fieldbus in the world, EtherNet/IP is at number 3. Especially in several regions of the world EtherNet/IP has a dominating role. SIMATIC controller inherently don't have support for field devices using EtherNet/IP.

In this application example a possible solution is demonstrated and explained, how such EtherNet/IP field devices can still be used with SIMATIC controller. Here SIMATIC controller applies to both S7-1500 and S7-1200.

In this example the S7-1200 will be operated as such EtherNet/IP field device together with the ET200SP MF interface module. The S7-1500 shown in the below schematic is operated as the device controlling the field devices.

NOTE The roles of the S7-1200 and S7-1500 can be exchanged without changes in the description as the LCCF_EnetScanner function block exists for both systems.

Figure 2-1: simplified setup



As mentioned above the ET200SP MF and the S7-1200 controller are operated as field devices providing sensor signals to the S7-1500 controller and accepting control signals from the S7-1500.

The real setup also contains a SCALANCE X208 switch for easier connectivity. However, the switch is not necessary as a line topology (as shown above) is also possible.

2.2 EtherNet/IP

Even though in the above schematic setup the cables are named with PROFINET/ IE, any other Ethernet based protocol can co-exist on the same network. Especially if such protocol uses IP as networking protocol and either TCP or UDP as transport protocol.

EtherNet/IP is such a protocol. It is Ethernet based (IEEE 802.3) and uses IPv4 as networking protocol as well as TCP and UDP as its transport protocol. EtherNet/IP is an open standard maintained by the ODVA® (Open DeviceNet Vendor Association). Yet it should not be mixed up with so called TCP native/ socket communications.

EtherNet/IP is a best effort approach to achieve higher performance and lower jitter compared to regular TCP communications while maintaining maximum interoperability to the other TCP or UDP based communication protocols.

The IP in the name EtherNet/IP is not to be mixed up with IPv4. It is an abbreviation for CIP (Common Industrial Protocol). This CIP is embedded into the payload of the TCP or UDP packets used to exchange data between two or more devices.

The devices creating an EtherNet/IP network are called:

- Scanner, which are scanning the network. They are collecting the information, such as sensor data, from the other field devices. In PROFINET terms this would be equivalent to a Controller or a Master on other networks
- Adapter, which are providing such sensor data to the Scanner. The adapters translate the EtherNet/IP protocol into a proprietary intra device protocol. The adapt the protocols. The PROFINET equivalent term is Device or Slave on other networks.

As the Open User Communication allows a SIMATIC programmer to create the payload for packets send via UDP or TCP, the SIMATIC can implement the necessary features and functions to provide EtherNet/IP as loadable function block. This functionality can be used with any Open User Communication capable interface of the SIMATIC, such as integrated PROFINET ports as well as Industrial Ethernet CMs and CPs.

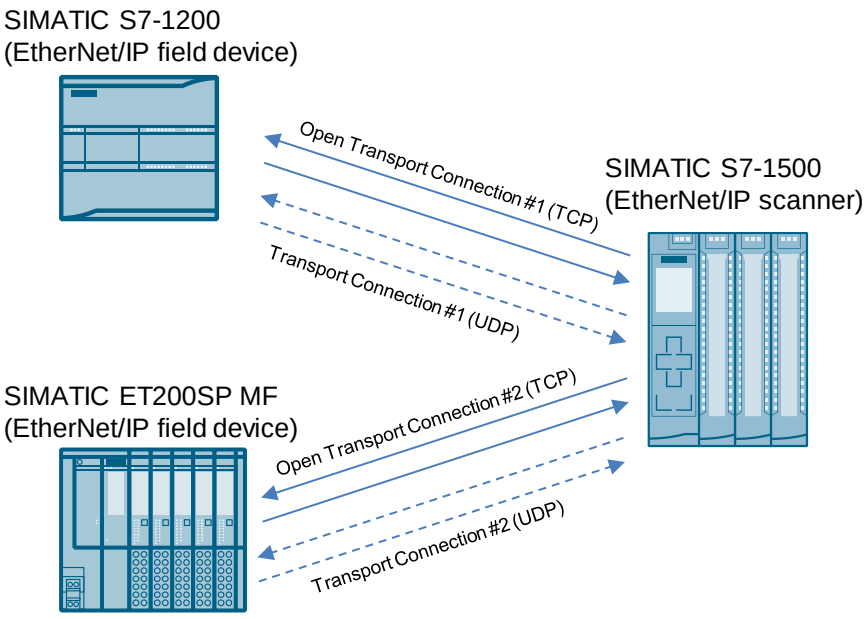
2.3 Function principle

The application example demonstrates the necessary steps to configure the SIMATIC S7-1500 to operate as EtherNet/IP Scanner with the help of the LCCF_EnetScanner function block.

The communication will use both transport protocols mentioned above. The Scanner is configured to exchange data with two Adapters. One adapter is the ET200SP MF in EtherNet/IP fieldbus mode. The second adapter is represented by the S7-1200 using the also available LCCF_EnetAdapter function block.

This is schematically shown on the next page's figure.

Figure 2-2: schematic functional principle



The communication is established by the Scanner using a TCP connection. After registering the Scanner with the Adapters, a transport connection is negotiated with each of the Adapters. Once this is successfully done, the transport connection is opened, and the data exchange takes place using UDP datagrams.

There are two more terms associated with EtherNet/IP.

- Originator: is the device, which initiates the transport connection. This is typically the Scanner.
- Target: is the device, which accepts the transport connection. This is typically the Adapter.

In this application example the transport connection uses UDP transport and unicast communications. With EtherNet/IP the target may also vote for a multicast connection. The target would then send the sensor data to many devices (incl. the originator) instead of only to the originator.

NOTE In this application example the terms Adapter and Target as well as Originator and Scanner are used as synonyms. This is correct for this application example. In other scenarios this might not hold true anymore.

2.4 Scope of delivery

The application example consists of the document and a TIA Portal project. It also contains the MFCT project for an exemplary configuration of the ET200SP MF as well as an EDS file for each of the field devices.

The program in the TIA Portal program can be easily adopted into a “S7-1200 as Scanner” scenario, as the LCCF_EnetScanner function block uses the identical parameterization.

The parameterization for the Scanner will consist of the two adapters. It will be explained which settings from the EDS files are mapped into the configuration of the LCCF_EnetScanner block.

3 Commissioning

3.1 Preparation

As preparation for the application example to function, the above-mentioned hardware components should be placed into a rack or on a solid table to prevent slip or fall.

WARNING

Risk of electric shock

To operate this application example the connection of the above hardware to electrical power is required. Disregarding local regulations and common sense may cause an electric shock and because of that injury or death.

Always follow the rules for working with electrical equipment. If in doubt, have someone familiar with these rules and regulations set up the hardware for you.

Further download the TIA Portal project and make sure you have the MFCT installed and properly functioning. Another good idea is to have a text editor, such as Notepad on your computer, as several values will be taken from the EDS files, which are in turn text files.

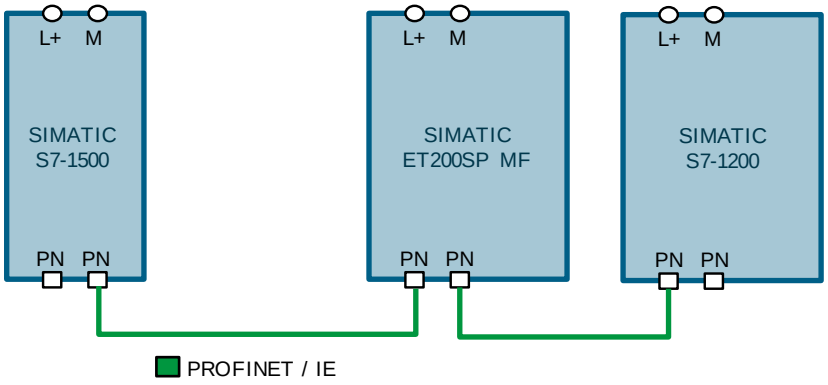
3.2 Connecting the hardware components

As mentioned above please observe electrical guidelines and rules when connecting power to the components, which is the first step to take.

Secondly setup the Ethernet cables. There are two options to do that.

The first option is the Line topology as shown below:

Figure 3-1: Line topology setup

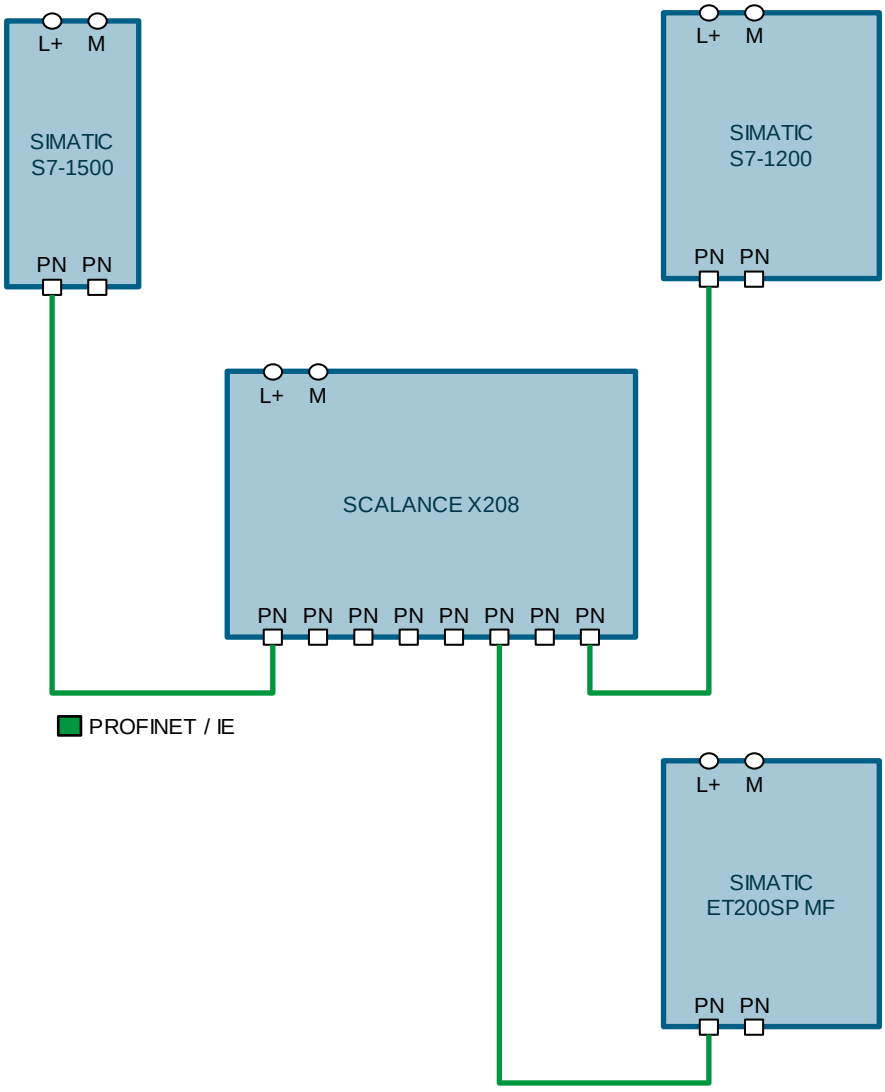


NOTE

The line topology is an easy to setup topology. Although it does not allow network debugging as easy on a protocol level.

Another topology is the star topology, which in the application example is used. It is shown in the next schematic.

Figure 3-2: Star topology setup



NOTE

The star topology is using a network switch as the center point. If the used switch allows port mirroring/ port spawning network protocol analysis is much easier.

In this document some network traces will be shown to illustrate the explained mechanisms.

Network traces are taken used the application Wireshark®.

4 Configuration/Engineering

4.1 Creating and managing projects

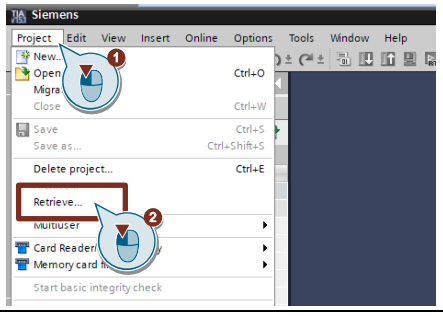
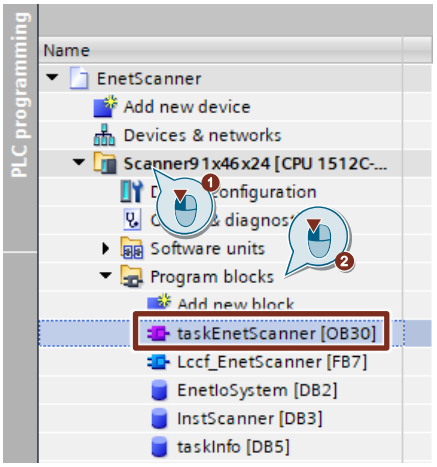
To follow along with this application example the TIA Portal project should have been downloaded from SIOS.

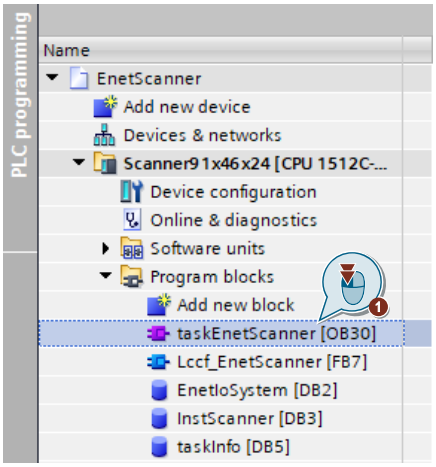
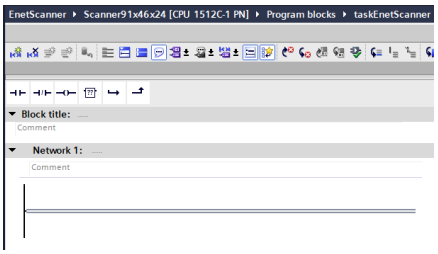
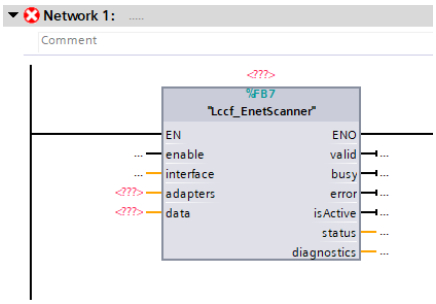
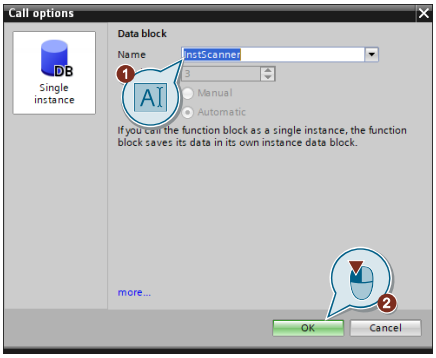
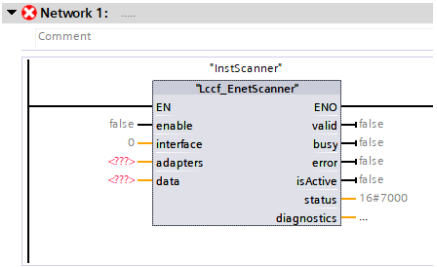
NOTE

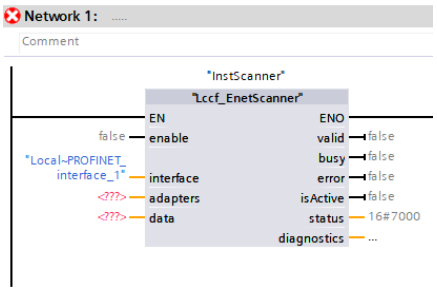
A new TIA Portal project may also be created as it allows to adopt the hardware platform accordingly.

However, it is not part of this document to explain the setup of the hardware being used as EtherNet/IP Scanner.

Table 4-1: Configuration instructions

Step	Instruction	Result
1.	Start TIA Portal	
2.	Retrieve the downloaded TIA Portal project (EnetScanner.zap15_1) 	This will extract the compressed TIA Portal archive into a folder of your selection.
3.	Open the contained SIMATIC S7-1500 controller 	You will see the function block LCCF_EnetScanner in the program folder as well as two data blocks. • EnetIoSystem • InstScanner You will also see a Cyclic Interrupt OB.

Step	Instruction	Result
4.	Open the existing OB “taskEnetScanner” with a double-click on it. 	The block opens in the editor. 
5.	Place a call to the LCCF_EnetScanner onto the network.  TIA Portal will request an instance DB. Type in the name of the existing instance DB or select it from the drop-down list. 	As the result the block call is placed with the instance DB. In this example the instance DB is named “InstScanner” 

Step	Instruction	Result
6.	Assign the interface you want to use to the actual parameter of the block call 	

NOTE

It is recommended to use the TIA Portal maintained global constants for the interface identifier. Otherwise the function block may not work properly.

However, any Open User Communication (OUC) capable interface may be used, including Industrial Ethernet CM or CP extension cards.

At this point the LCCF_EnetScanner function block is not operable. The configuration of the EtherNet/IP field devices needs to be done and an area to for the sensor and control data needs to be declared.

4.2 Creating the EtherNet/IP IO system

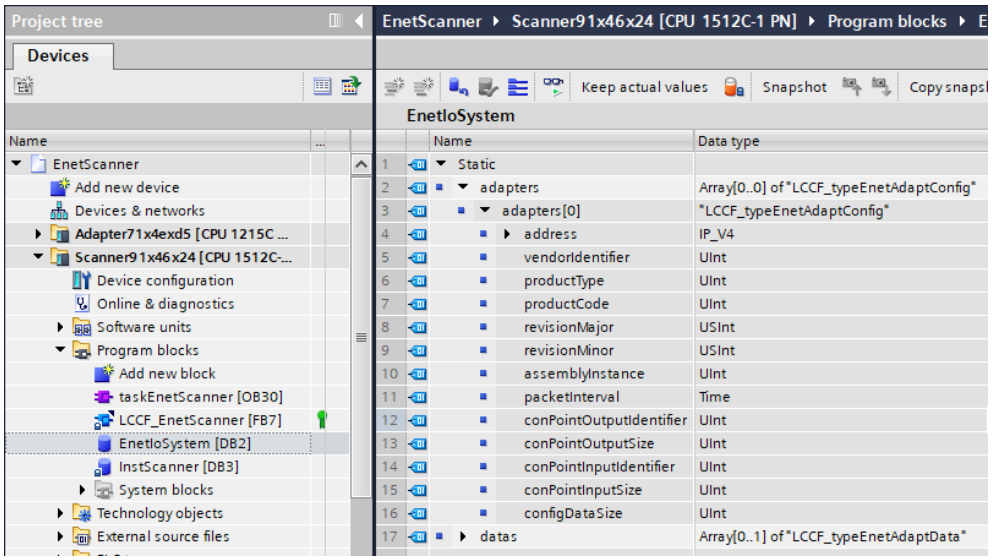
Similar to PROFINET or PROFIBUS there is a managing device in an EtherNet/IP network. In this application example it is realized by the S7-1500. The managing system is called the Scanner.

For the Scanner to know, which managed devices, called Adapters, are in the scope, it requires some information. Theis information is describing the parameters of the data exchange. They contain as minimum:

- Addressing information of the Adapter
- Update rates for both Inputs and Outputs
- Amount of data to be exchanged

As for EtherNet/IP there is no graphical way to configure the EtherNet/IP IO system in TIA Portal the LCCF_EnetScanner function block accepts the configuration in the form of an array of Adapter descriptions. The descriptions are best stored in a global DB. In this application example the DB is called “EnetIoSystem”, which stores the array with the adapter descriptions in it.

Figure 4-1: Datablock “EnetIoSystem”



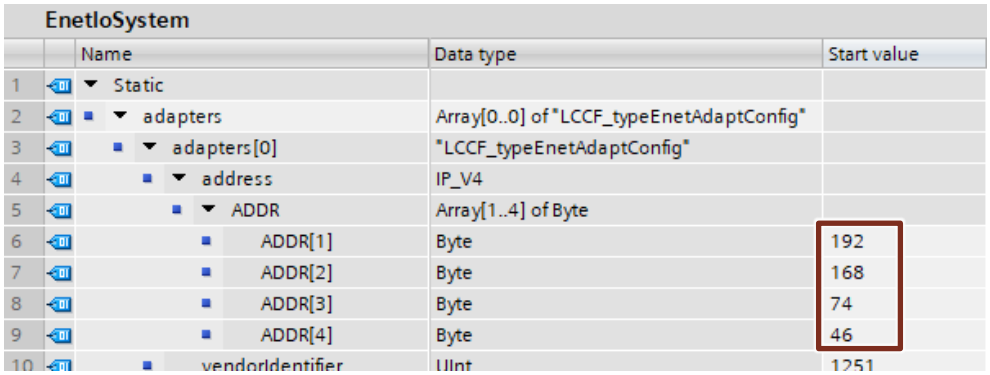
In this chapter the application example explains how this configuration is created and where to get the information from.

4.2.1 Creating an Adapter description

The above shown data block contains an array of type LCCF_typeEnetAdaptConfig. This type contains all the relevant information the LCCF_EnetScanner function block needs to operate the herein described Adapters.

As mentioned before, it contains addressing information, which are most important. One of these addresses is the IPv4 address the Adapter can be reached at.

Figure 4-2: IP address of an adapter



The address is stored using the system provided datatype IP_V4. The Adapter configuration shown above is the configuration of the ET200SP MF. It has the IP address 192.168.74.46, which is also shown in the below IP address overview.

Table 4-2: IP addresses

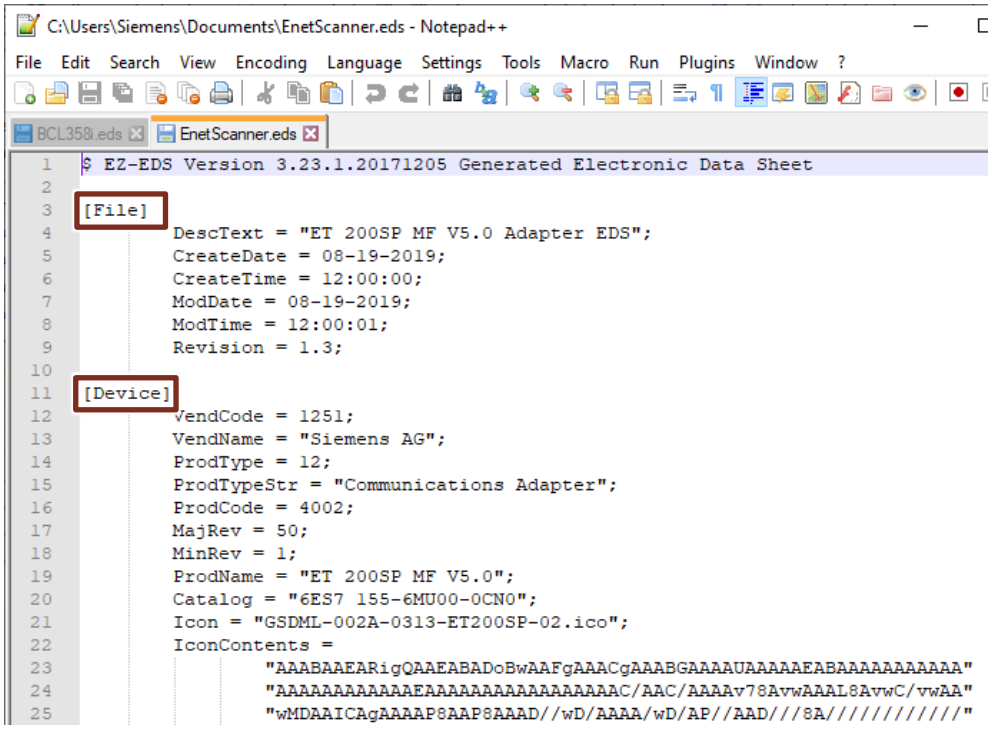
Role	System	IP address
EtherNet/IP Scanner	S7-1500	192.168.74.12
EtherNet/IP Adapter	ET200SP MF	192.168.74.46
	S7-1200	192.168.74.45

Further addressing information are necessary. They will be retrieved from an electronic data sheet (EDS), which is like a GSD file known from PROFINET and PROFIBUS systems.

4.2.2 EDS files

The EDS file format is standardized by the ODVA® and is text based and human readable. It contains several clusters of information. These clusters are called segments. They are identified by their name and marked by '[' and ']' characters (squared brackets)

Figure 4-3: EDS file for ET200SP MF



Throughout this document the marked areas will be called sections. The sections contain assignments to items.

The Adapter description required for the LCCF_EnetScanner function block, is mostly taken from such EDS files. In the following this document explains, which sections and items are relevant to LCCF_EnetScanner and therefore, necessary to enter into the adapter description.

After that the procedure is repeated for the second adapter

Device parameters

The device describing parameters are relevant for the Scanner, as it uses this information to verify the real existing device against the configured device. In case there is a mismatch the operation of this device is not started.

Such information is:

- vendorIdentifier, in the EDS file called “VendCode” is an ODVA® assigned number to the manufacturer of this device
- productType, in the EDS file called “ProdType” is a standardized number identifying the type of the device
- productCode, the “ProdCode” called number identifies this product together with its type and vendor ID.
- revisionMajor, the major revision number, together with the minor revision number serves the purpose of compatibility check
- revisionMinor, as above serves the minor revision number the purpose of a compatibility check.

They can be found at the section [Device] as shown in the below figure.

Figure 4-4: EDS file [Device] section

```
11  [Device]
12          VendCode = 1251;
13          VendName = "Siemens AG";
14          ProdType = 12;
15          ProdTypeStr = "Communications Adapter";
16          ProdCode = 4002;
17          MajRev = 50;
18          MinRev = 1;
19          ProdName = "ET 200SP MF V5.0";
20          Catalog = "6ES7 155-6MU00-0CN0";
21          Icon = "GSDML-002A-0313-ET200SP-02.ico";
22          IconContents =
```

For the application example the transfer into the configuration inside the EnetIoSystem data block looks like this:

Figure 4-5: [Device] section parameters

adapters	Array[0..0] of "Lccf_typeEnetAdaptConfig"	
adapters[0]	"Lccf_typeEnetAdaptConfig"	
address	IP_V4	
vendorIdentifier	UInt	1251
productType	UInt	12
productCode	UInt	4002
revisionMajor	USInt	50
revisionMinor	USInt	1

Further parameters are taken from different other sections of the EDS file.

Data sizes and update times

In the [Params] section, several parameter sets are defined, which are used later in the EDS file.

The relevant information for the configuration of the EnetIoSystem are here

- Update interval
- Size of Inputs and Outputs

Figure 4-6 [Params] section RPI and Output Data size

```
[Params]
        Param9 =
                0,                      $ reserved, shall equal 0
                ,,                      $ Link Path Size, Link Path
                0x0020,                 $ Descriptor
                0xC8,                   $ Data Type
                4,                      $ Data Size in bytes
                "RPI",                  $ name
                "",                     $ units
                "RPI",                  $ help string
                2000,20000000,10000,    $ min, max, default data sizes
                ,,,,                    $ mult, div, base, offset scaling
                ,,,,                    $ mult, div, base, offset links
                ;                       $ decimal places
        Param768 =
                0,                      $ reserved, shall equal 0
                ,,                      $ Link Path Size, Link Path
                0x0000,                 $ Descriptor
                0xC7,                   $ Data Type
                2,                      $ Data Size in bytes
                "Output Data",          $ name
                "Bytes",                $ units
                "",                     $ help string
                0,496,496,              $ min, max, default data values
                ,,,,                    $ mult, div, base, offset scaling
                ,,,,                    $ mult, div, base, offset links
                0;                      $ decimal places
        Param769 =
                0,                      $ reserved, shall equal 0
                ,,                      $ Link Path Size, Link Path
                0x0000,                 $ Descriptor
                0xC7,                   $ Data Type
                2,                      $ Data Size in bytes
                "Input Data",           $ name
```

In the above shown figure the parameter, marked with 1 describes the RPI called “Requested Packet Interval” or update rate in µs.

The update rates in the range between 2.000µs (2ms) and 20.000.000µs (20s) are valid for this device. The default setting is 10.000µs (10ms).

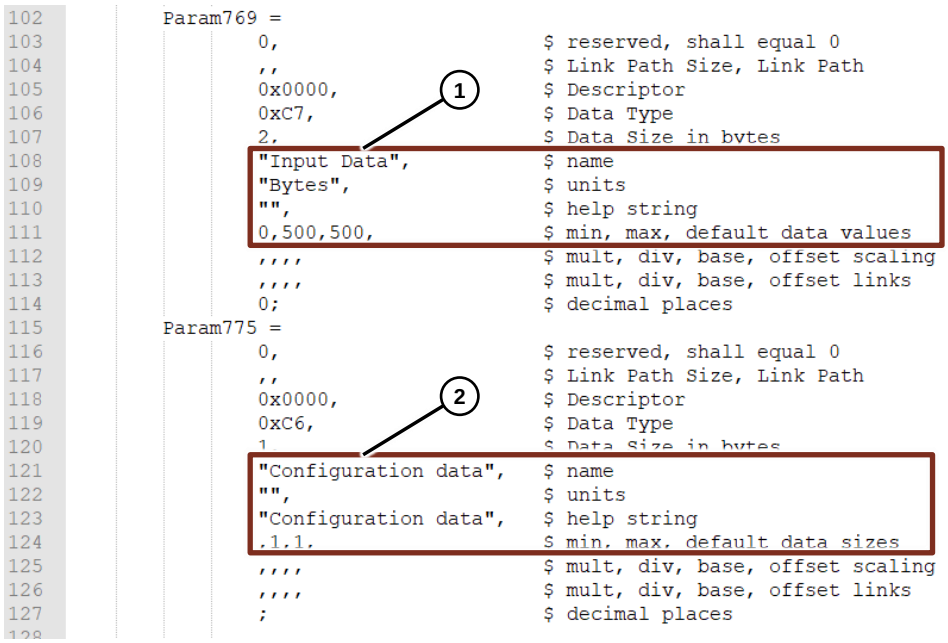
The parameter marked with 2, describes the size of the Output data in Bytes. The valid range is in between 0 Bytes and 496 Bytes, where the default is equal to the maximum size.

NOTE

The maximum size of 496 Bytes is a limitation given by the ODVA® specification for EtherNet/IP. It is introduced for compatibility reasons to ControlNet, which is another network using the same communication mechanisms defined in CIP as EtherNet/IP.

Further down in the [Params] section you will find the other relevant information for the Input data size and the configuration data size. They are shown in the below figure.

Figure 4-7: [Params] section Input Data and Configuration Data size



Same as in the previous figure the with 1 marked area shows a relevant parameter. In here the size of the Input Data is defined. The valid range is between 0 and 500 Bytes.

The second marked area contains the size of the configuration data. The configuration may not exist. Therefore, the minimum size is not provided. The configuration data may not exceed 1 Byte in maximum.

NOTE

The values for RPI and I/O sizes from the EDS file provide a valid range. The user can choose any value in between the minimum and maximum possible value.

The above retrieved values are to be entered into the appropriate positions of the adapter description as shown on the next page.

This application example will use the values in the below table

Table 4-3: Configured values for ET200SP MF

Parameter name	valid range	chosen value
RPI	2ms – 20s	50ms
Output Size	0 – 496 Bytes	20 Bytes
Input Size	0 – 500 Bytes	20 Bytes
Configuration Size	None – 1	None

NOTE

The Output direction is also called the “Originator To Target” direction (short OT direction), while the Input direction is called the “Target To Originator” direction (short TO direction).

Figure 4-8: EnetIoSystem configuration for RPI and data sizes

EnetIoSystem

	Name	Data type	Start value
1	Static		
2	adapters	Array[0..0] of "LCCF_typeEnetAdaptConfig"	
3	adapters[0]	"LCCF_typeEnetAdaptConfig"	
4	address	IP_V4	
5	vendorIdentifier	UInt	1251
6	productType	UInt	12
7	productCode	UInt	4002
8	revisionMajor	USInt	50
9	revisionMinor	USInt	3
10	assemblyInstance	UInt	775
11	packetInterval	Time	T#10ms
12	conPointOutputIdentifier	UInt	768
13	conPointOutputSize	UInt	20
14	conPointInputIdentifier	UInt	769
15	conPointInputSize	UInt	20
16	configDataSize	UInt	0

In the above shown figure the settings are made for the three connection points, which are:

- conPointOutput → Originator to Target direction
- conPointInput → Target to Originator direction
- configData

Three more settings are of relevance before the LCCF_EnetScanner function block can communicate with the ET200SP MF module.

AssemblyID and Connection Point IDs

They are called the Assembly instances, AssemblyIDs, or pointIdentifier. The EDS file contains them in a somewhat cryptic way in the [Connection Manager] section.

In the below shown figure the with “Path” commented line (line 202) is of particular interest as it contains the access path to the assembly objects.

Figure 4-9 [Connection Manager] section AssemblyIDs

```
154 [Connection Manager]
155         Object_Name = "Connection Manager Object";
156         Object_Class_Code = 0x06;
157
158         Connection1 =
159                 0x04010002,             $ 0-15    = supported transport classes
160                                         $ 16      = trigger: cyclic
161                                         $ 17      = trigger: change of state

195                                         $ 31      = T->O priority: reserved
196                 Param9,Param768,Assem768,       $ O->T RPI, size, format
197                 Param9,Param769,Assem769,       $ T->O RPI, size, format
198                 ,,                      $ proxy config size, format
199                 ,,                      $ target config size, format
200                 "Connection00 Exclusive",      $ Connection Name
201                 "Connection00 Exclusive Owner"      $ help string
202                 "20 04 25 00 07 03 2D 00 00 03 2D 00 01 03";    $ Path
```

The access path is a series of hexadecimal numbers, which follows a specified format.

This series is split into segments which are in the order of:

1. Class Segment (ID: 20hex) addressing the Assembly class (ClassID = 04hex)

   ```
   "20 04 25 00 07 03 2D 00 00 03 2D 00 01 03";    $ Path
   ```

2. Instance Segment (ID 24hex or 25hex) addressing the Configuration Assembly (0307hex = 775dec)

   ```
   "20 04 25 00 07 03 2D 00 00 03 2D 00 01 03";    $ Path
   ```

3. Connection Point Segment (ID 2Chex or 2Dhex) addressing a Connection Point (300hex = 768dec)

   ```
   "20 04 25 00 07 03 2D 00 00 03 2D 00 01 03";    $ Path
   ```

4. Connection Point Segment (ID 2Chex or 2Dhex) addressing a Connection Point (301hex = 769dec)

   ```
   "20 04 25 00 07 03 2D 00 00 03 2D 00 01 03";    $ Path
   ```

The order of the connection points is also predefined and is always in the same order. First the OT direction (Originator to Target), which is, from the point of view of the Scanner, the Output direction.
Followed by the TO direction (Target to Originator), which is the Input direction for the Scanner.

NOTICE

Wrong decoding of the Connection Point or Instance IDs can occur.

As the byte ordering is “big endian” in the EDS file, the numbers may be mistakenly ordered in “little endian” and therefore decoded wrong. This may end up addressing the wrong connection points causing non-functional behavior of the LCCF_EnetScanner block.

Make sure the byte ordering is adjusted.

```
"20 04 25 00 07 03 2D 00 00 03 2D 00 01 03";    $ Path
```

As example the instance segment’s value is 25 00 07 03, where

- 25 00 is the segment identifier for the instance segment.
- 07 03 is the value for the instance. Here the bytes must be swapped otherwise the decimal representation of 07 03hex is 1795dec.
  This would address a different instance instead of the correct instance 775.

NOTE

The direction can also be derived from the EDS file as it is described there in the correct order.

```
195                                  $ 31      - T->O priority: reserved
196             Param9,Param768,Assem768,       $ O->T API, size, format
197             Param9,Param769,Assem769,       $ T->O API, size, format
198             ,,                             $ proxy config size, format
199             ,,                             $ target config size, format
200             "Connection00 Exclusive",      $ Connection Name
201             "Connection00 Exclusive Owner",      $ help string
202             "20 04 25 00 07 03 2D 00 00 03 2D 00 01 03";    $ Path
```

The O->T direction is listed before the T->O direction.

Do not assume, that the numbers in the Paramxxx or Assemxxx name always indicate the Connection Point identifier. Here this is the case, however this is not always like this, as these numbers are arbitrary numbers.

Now that the connection point identifier and the assembly identifier are known, they can be transferred into the EnetIoSystem data block for the adapter as shown below.

NOTE

The AssemblyIDs or connection point identifiers are specific for each device type. They may be different for different devices. This means ET200SP MF always use, 775, 768 and 769 for their identifiers. A F6Nano motion controller uses the identifiers 1, 100 (64hex) and 101 (65hex).

Figure 4-10: EnetIoSystem configuration for RPI and data sizes

EnetIoSystem

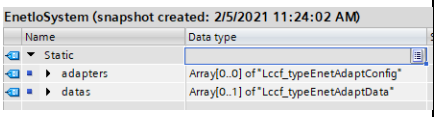
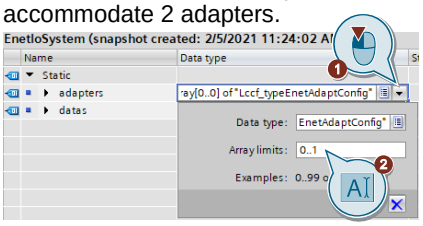
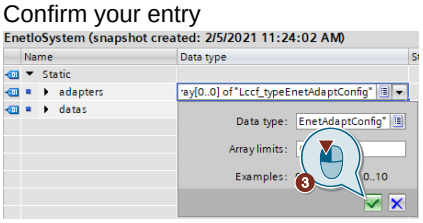
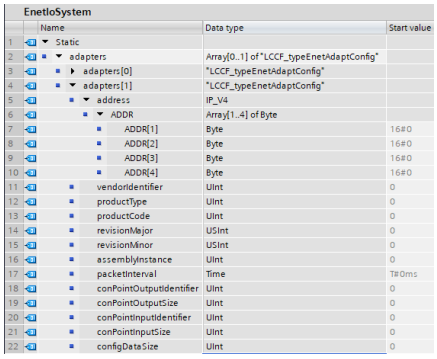
	Name	Data type	Start value
1	Static		
2	adapters	Array[0..0] of "LCCF_typeEnetAdaptConfig"	
3	adapters[0]	"LCCF_typeEnetAdaptConfig"	
4	address	IP_V4	
5	vendorIdentifier	UInt	1251
6	productType	UInt	12
7	productCode	UInt	4002
8	revisionMajor	USInt	50
9	revisionMinor	USInt	3
10	assemblyInstance	UInt	775
11	packetInterval	Time	T#10ms
12	conPointOutputIdentifier	UInt	768
13	conPointOutputSize	UInt	20
14	conPointInputIdentifier	UInt	769
15	conPointInputSize	UInt	20
16	configDataSize	UInt	0

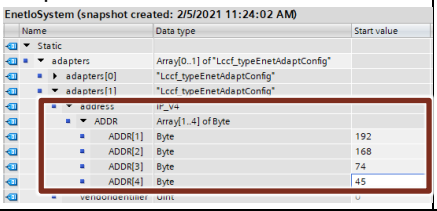
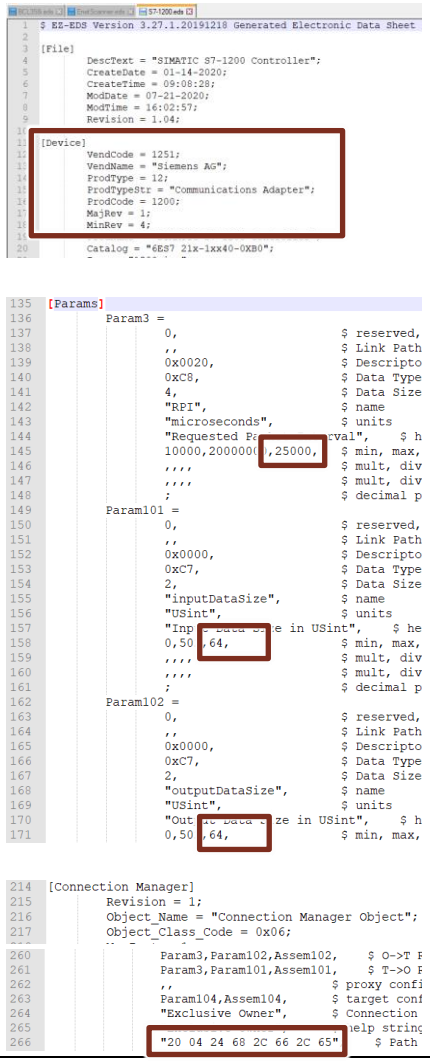
This finishes the configuration of the ET200SP MF as EtherNet/IP adapter for the LCCF_EnetScanner function block.

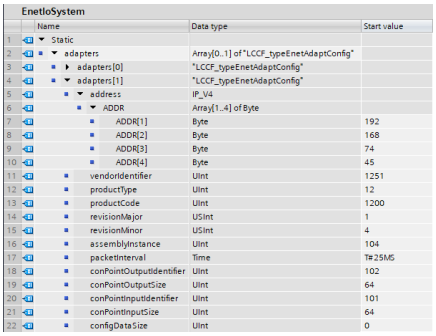
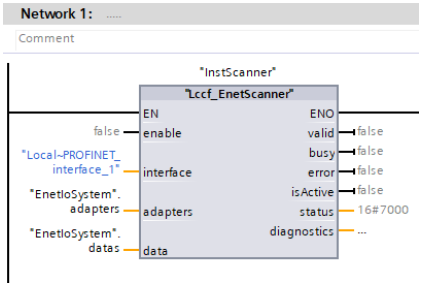
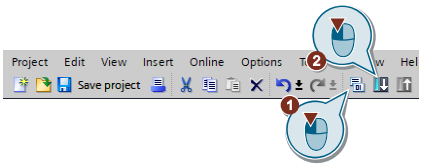
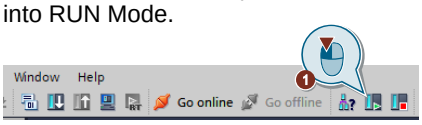
Finalizing the parameterization

As the LCCF_EnetScanner block has not been completely parameterized, the document will now show the next necessary steps to achieve this.

Table 4-4: LCCF_EnetScanner block parameterization

Step	Instruction	Result
1.	Verify that the EnetIoSystem data block contains at least two variables. 	The variable “adapters” contains the just prepared description for the ET200SP MF. The second variable contains the data areas to exchange the data with the adapters.
2.	Extend the “adapters” array to accommodate 2 adapters.  Confirm your entry 	You will get a new entry for the second adapter. 

Step	Instruction	Result
3.	Enter the IP address of the second adapter. 	In this document it is the S7-1200 with 192.168.74.45
4.	Open the EDS file of the second adapter with you text editor program (e.g. Notepad). Note the relevant data from the differerent sections 	The following data are used in this application example From sections [Device] • VendorCode = 1251 • ProductType = 12 • ProductCode = 1200 • Revision = 1.004 [Params] • Output Size = 64 Bytes • Input Size = 64 Bytes • RPI = 25 ms (25.000µs) [Connection Manager] • Instance ID = 104 (68hex) • OT Assembly ID = 102 (66hex) • TO Assembly ID = 101 (65hex)

Step	Instruction	Result
5.	Transfer the noted data to the EnetIOSystem data block	as a result, the EnetIoSystem should look like the below: 
6.	Assign the variables to the corresponding parameters of the LCCF_EnetScanner. 	The LCCF_EnetScanner is now parameterized with its minimum set of parameters.
7.	Compile and download the program to the PLC.  If it hasn't been already, put the PLC into RUN Mode. 	

After this procedure the PLC should be running and executing the LCCF_EnetScanner function block in a cyclic interrupt.

The use of a cyclic interrupt helps maintaining an execution in a more stable interval. With this the update rates do not differ too much, and the jitter is kept to a minimum.

NOTE

When operating the S7-1200 as EtherNet/IP adapter the configuration data can be used to transfer additional data, such as parameter sets. This will be done once on startup and acyclic at a fixed rate of every 5s. The configuration data size is set to 64 bytes fixed in the EDS file.

```
Param104 =
        0,                      $ reserved, shall equal 0
        ,,                      $ Link Path Size, Link Path
        0x0000,                 $ Descriptor
        0xC7,                   $ Data Type
        2,                      $ Data Size in bytes
        "configDataSize",       $ name
        "USint",                $ units
        "Configuration Data Size in USint",    $ help string
        64,64,64,               $ min, max, default data values
        ,,,,                    $ mult, div, base, offset scaling
        ,,,,                    $ mult, div, base, offset links
        ;                       $ decimal places
```

The entry to be made in the EnetIoSystem data block for adapters[1] looks like below:

EnetIoSystem

	Name	Data type	Start value
1	Static		
2	adapters	Array[0..1] of "LCCF_typeEnetAdaptConfig"	
3	adapters[0]	"LCCF_typeEnetAdaptConfig"	
4	adapters[1]	"LCCF_typeEnetAdaptConfig"	
5	address	IP_V4	
6	ADDR	Array[1..4] of Byte	
7	ADDR[1]	Byte	192
8	ADDR[2]	Byte	168
9	ADDR[3]	Byte	74
10	ADDR[4]	Byte	45
11	vendorIdentifier	UInt	1251
12	productType	UInt	12
13	productCode	UInt	1200
14	revisionMajor	USInt	1
15	revisionMinor	USInt	4
16	assemblyInstance	UInt	104
17	packetInterval	Time	T#25MS
18	conPointOutputIdentifier	UInt	102
19	conPointOutputSize	UInt	64
20	conPointInputIdentifier	UInt	101
21	conPointInputSize	UInt	64
22	configDataSize	UInt	64

As the configuration data are targeting the adapter instance the same as for the assemblyInstance.

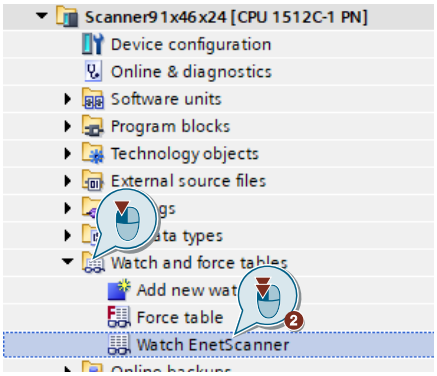
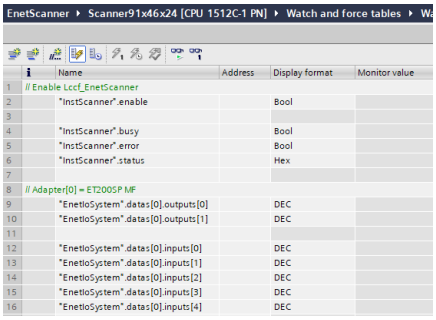
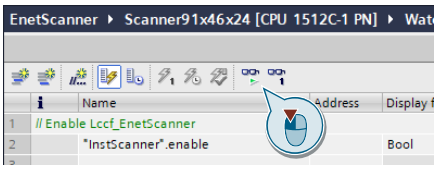
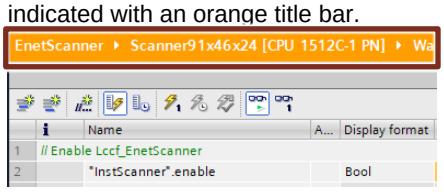
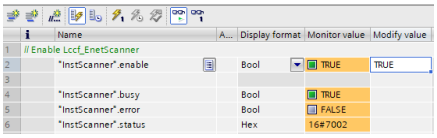
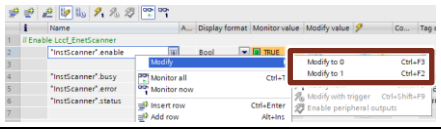
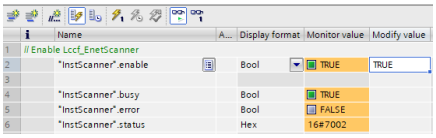
5 Operating

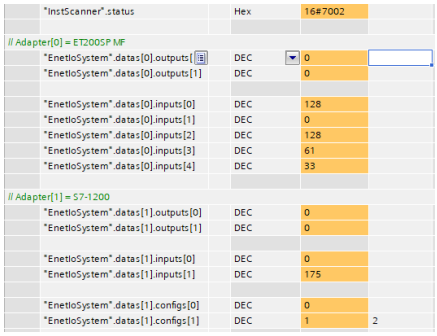
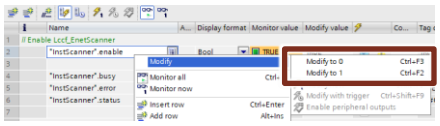
5.1 Start the application

The application will be operated by simply toggle the “enable” input parameter of the LCCF_EnetScanner function block to “TRUE” and monitor the exchanged data.

For this follow the below instructions as a watch table has been prepared in the application examples TIA Portal project.

Table 5-1:

Step	Instruction	Result
1.	Open the prepared watch table “Watch EnetScanner” 	The watch table opens 
2.	Switch the watch table online to be able to monitor and modify values 	The watch table switches online. This is indicated with an orange title bar. 
3.	Modify the “enable” variable to “TRUE” This can be done either by typing the value “1” or “TRUE” into the “Modify value” column  or by using the context menu 	as a result, the LCCF_EnetScanner establishes connections to the configured adapters and starts the data exchange. The status of the LCCF_EnetScanner is reported as 16#7002, which means busy. The appropriate flags are set as well accordingly. 

Step	Instruction	Result
4.	Modify the output data and monitor the input data for each adapter 	
5.	To stop the LCCF_EnetScanner toggle the “enable” parameter to “FALSE”. 	As a result of that, the input values are frozen, the update stops. The LCCF_EnetScanner shuts down the connections to all configured adapters.

NOTE When the second adapter has the configuration data configured, you may also change the configuration data during operation. The configuration data will be updated in 5s. intervals.

5.2 Troubleshooting

In case the result is not as expected the cause could be found on both sides of the communication path.

Before you try to change any of the program or configuration, check the physical installation first.

5.2.1 Physical check

Verify the following causes for malfunctions or not functioning at all.

1. Is the SIMATIC powered up?
2. If used, is the SCALANCE switch powered up?
3. Are the network cables properly inserted into the LAN sockets of the devices? This can be determined by evaluating the port LEDs of the devices. At least the Link LED should be illuminated.

Table 5-2: physical checks

observation	possible cause	remedy
SIMATIC is not reachable from TIA Portal	SIMATIC is not powered up.	• Check power supply and wiring with the installation manual. • Correct wiring Power the Power Supply up
	SIMATIC doesn't have network connection	• Check network cable to be inserted properly into the network socket (P1.X1 or P1.X2) Check and correct network settings of your PC
SIMATIC cannot communicate with SIMATIC EtherNet/IP adapters	Network switch is not powered up	Check and correct power supply to the network switch.
	network cables are not properly inserted into the Adapter	• Check all network cable sockets to have their "link" lights illuminated. • If necessary, remove the network cable from the LAN socket and reinsert until you hear a click. • Replace the network cable

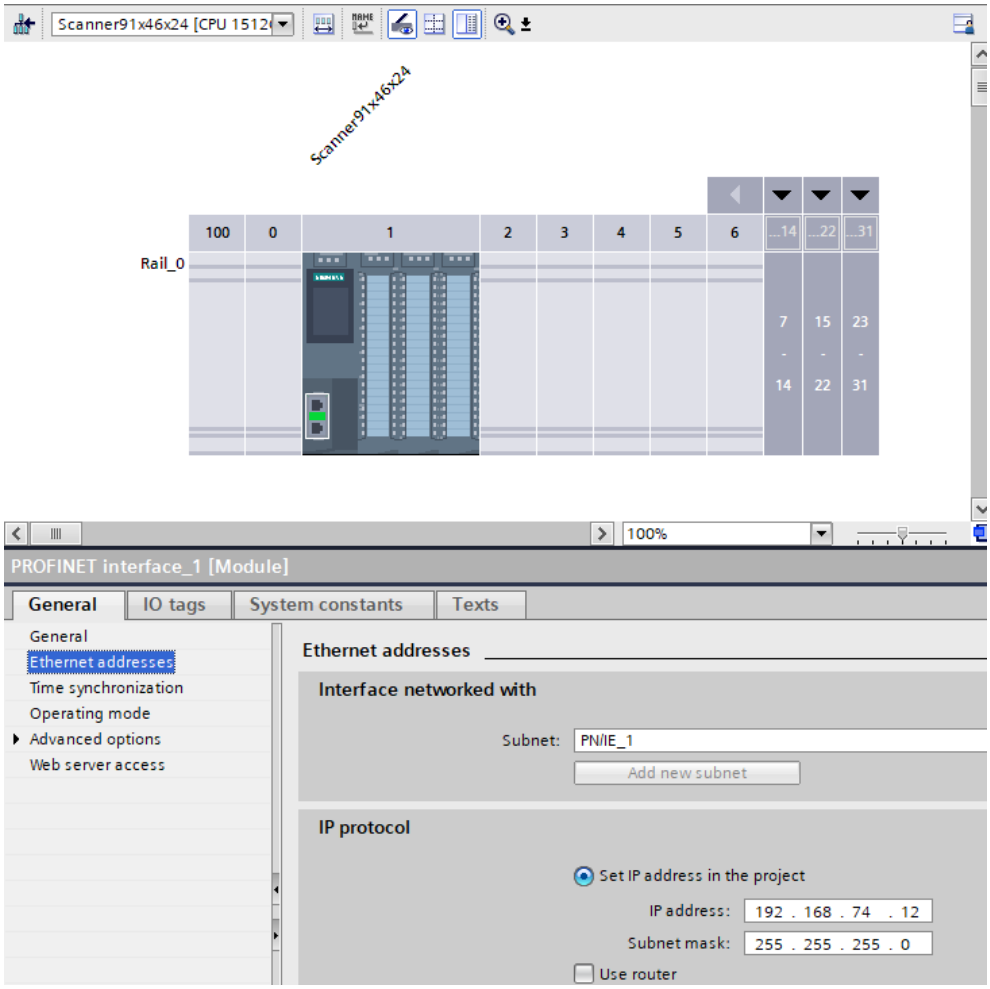
If you checked everything and there is no communication at all, then perform the checks recommended in the next chapter.

5.2.2 Network Settings

Missing communication can be caused by any partner along the line of communication. Therefore, make sure the network settings for the devices are compatible to each other.

In this application example the Ethernet settings for the scanner as well as for the two configured adapters are shown below.

Figure 5-1: Network settings – Scanner PLC



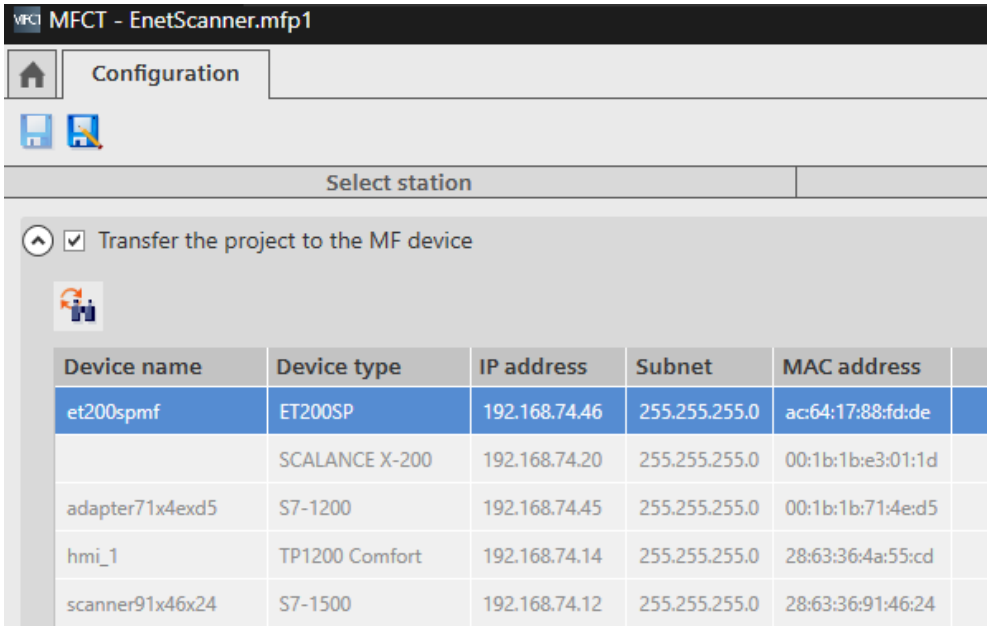
Important settings are the IP address and the subnet mask. As shown above the are:

- IP: 192.168.74.12
- Mask: 255.255.255.0

Compatible IP addresses differ on a network with subnet mask 255.255.255.0 only in the last octet. Otherwise, a communication without network router is not possible.

For the ET200SP MF adapter the MFCT (MultiFieldbus Configuration Tool) is used. The settings are shown below

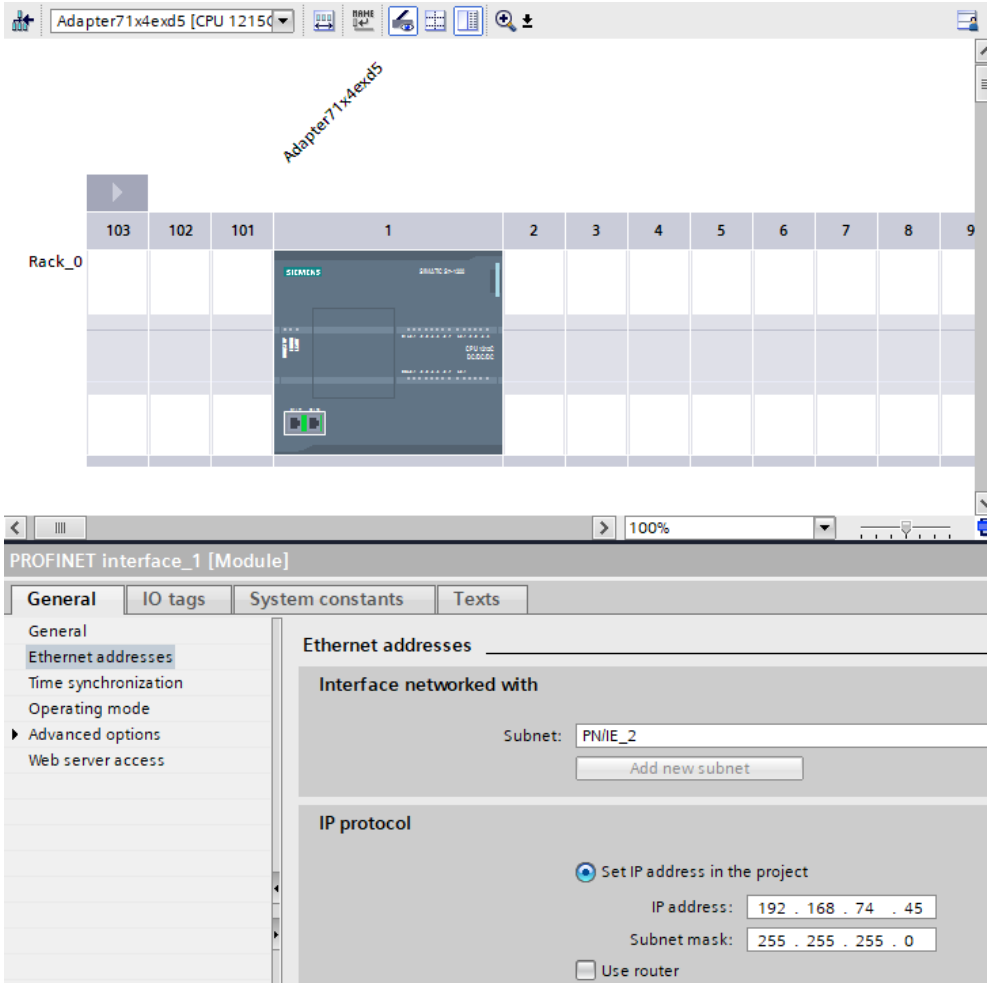
Figure 5-2: Network Settings for Adapter[0]/ ET200SP MF



Make sure the IP address settings are compatible to the settings of your scanner device. In this application example the ET200SP MF has compatible settings with:

- IP: 192.168.74.46
- Mask: 255.255.255.0

Figure 5-3: Network Settings for Adapter[1]/ S7-1200



Here the settings are shown above to be:

- IP: 192.168.74.45
- Mask: 255.255.255.0

5.2.3 SIMATIC Program

Answering the following questions may give you a hint on what needs to be corrected.

Table 5-3: LCCF_EnetScanner checks

observation	possible cause	remedy
status information doesn't change their values, when enable is set to true	The block is not executed	place an unconditional call to the block in cyclic interrupt program
error is true, the moment enable is set to true	Parameterization error	check the status code and correct the parameterization
valid becomes false after a certain time	Connection problems	check the status code and follow the specific recommendations further down in the document.

The LCCF_EnetScanner block reports certain error codes to inform the user about issues in the execution. This document describes the status codes the LCCF_EnetScanner block reports in the chapter “Parameters”

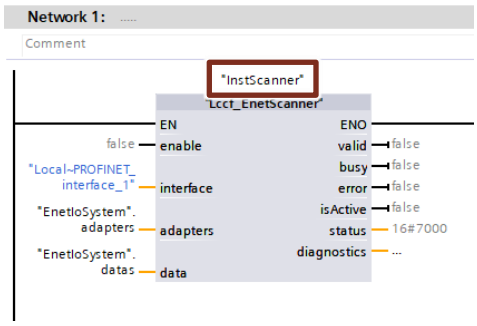
6 LCCF_EnetScanner block

6.1 Parameters

The LCCF_EnetScanner has been designed to require a minimum of parameters to make its use as easy as possible. Still a minimum external configuration is necessary, which is explained in the following chapter.

A call to the LCCF_EnetScanner block requires an instance DB to store operation relevant data internally as shown in the below figure.

Table 6-1: block call to “LCCF_EnetScanner”

LAD	SCL
	

The instance DB is generated automatically by the TIA Portal, when you place the call to the block. In this application example the instance DB is named “InstScanner”.

Besides the instance DB the other shown parameters are necessary and are explained in the below table.

Table 6-2: Parameter of the LCCF_EnetScanner block

Name	Direction	Data Type	Description
enable	Input	BOOL	Rising edge enables the functionality of the block. Any previously reported fault will be cleared, and conditions re-evaluated. Falling edge shuts the block down and stops any communications.
interface	Input	HW_ANY	Hardware Identifier of the interface to use for the communication. This typically uses a system defined constant. It is possible to use any “Open User Communication” supporting interface. This includes Industrial Ethernet CMs and CPs
adapters	InOut	Array[*] of LCCF_typeEnetAdaptConfig	List of configured adapters to exchange data with. Each array element represents one EtherNet/IP adapter and is of type

Name	Direction	Data Type	Description
			LCCF_typeEnetAdaptConfig. Refer to the chapter 4.2.1 “Creating an Adapter description” for details
data	InOut	Array[*] of LCCF_typeEnetAdaptData	List of data areas for each configured EtherNet/IP adapter to exchange data with.
valid	Output	BOOL	TRUE indicates that the values in the mapping variables are valid. FALSE some or all values are invalid and should NOT be used for process control.
busy	Output	BOOL	TRUE indicates the CIP Client block is actively processing requests. FALSE indicates the block is not processing requests.
error	Output	BOOL	TRUE indicates that an error occurred during the operation of the block. Depending on the type of the error indicated by status (see below) cycling of the enable flag may clear the error. FALSE indicates no error.
isActive	Output	BOOL	TRUE indicates the active data exchange with all configured devices FALSE indicates, that at least one device is not communicating with the Scanner.
status	Output	WORD	Status information about the operational state of this block. For details see the chapter Block status messages below
diagnostics[1]	Output	LCCF_typeDiagnostic	A structure containing additional information in case of an error, which are relevant for debugging the CIP server block. The content is of value for the developer.

[1] The parameter „diagnostics“ may be hidden in the block call.

6.1.1 Block status messages

The LCCF_EnetScanner block reports a status information to the user, which follows a standardized pattern.

The status code is split into the error flag and a status information value.

Table 6-3: Error and status message format

15	14		12	11			8	7							0
Error	Info/ Warning			Class Code				Specific Status Codes							
16#7 = Information 16#8 = Error				0 = Information											
				2 = Parameter related											
				4 = Internal Cause											
				6 = External Cause											

The LCCF_EnetScanner reports specific status codes. They are listed and explained in the following table.

Table 6-4: status messages

Valid	Busy	Error	Status Code (in hex)	Cause	Remedy
TRUE	TRUE	FALSE	16#0000	Success/ OK	--
FALSE	FALSE	FALSE	16#7000	No Call/ Idle	Block is called with enable = FALSE. Create rising edge on enable to start execution
FALSE	TRUE	FALSE	16#7001	Initial call	Block starts initialization and performs parameter check
TRUE	TRUE	FALSE	16#7002	Follow Up call	Block continues operation
TRUE	TRUE	FALSE	16#7202	More data areas have been parameterized, than adapter have been configured	Adjust the array boundaries for the data area to be the same as the adapter definitions. When keep operating, the excessive data areas are not touched and remain unchanged.
TRUE	TRUE	FALSE	16#72x7	Parameterized RPI was at least once exceeded by the adapter[x].	This warning indicates an overload and should be avoided by increasing the RPI.
TRUE	TRUE	FALSE	16#72x8	Scanner cannot realize the desired update rate for adapter[x]	This warning indicates an overload situation on the scanner side and should be avoided. This can be achieved by increasing the RPI.

Valid	Busy	Error	Status Code (in hex)	Cause	Remedy
TRUE	TRUE	FALSE	16#76x2	Overload situation, updates for adapters may have been lost	This warning indicates an overload situation on the scanner side. This can be avoided by increasing the “Communication load” setting in the CPU properties or increasing the call up interval of the used cyclic interrupt.
FALSE	FALSE	TRUE	16#8006	Cannot setup I/O socket.	It appears that the required UDP connection resource cannot be acquired from the system. Check and make sure, there are at least one unused UDP resource available. Consult the technical data for the used CPU model to learn how many such resources the CPU has.
FALSE	FALSE	TRUE	16#8201	Invalid interface specified	The specified interface doesn’t support the acquisition of operation relevant information. This interface cannot be used to be operated as scanner. Specify a different interface.
FALSE	FALSE	TRUE	16#8202	Number of configured adapters exceed maximum possible adapters	Reduce the number of adapters in this system to the maximum allowed number.
FALSE	FALSE	TRUE	16#8203	Number of configured data areas is lower than number of configured adapters.	Adjust the array boundaries to be identical for both number of configured adapters and available data areas.
FALSE	FALSE	TRUE	16#82x7	Parameterized input buffer is smaller than configured for adapter[x]	Adjust the configured T→O direction data size.
FALSE	FALSE	TRUE	16#82x8	Parameterized output buffer is smaller than configured for adapter[x]	Adjust the configured O→T direction data size.
FALSE	FALSE	TRUE	16#82x9	Parameterized configuration data	Adjust the configured configuration data size.

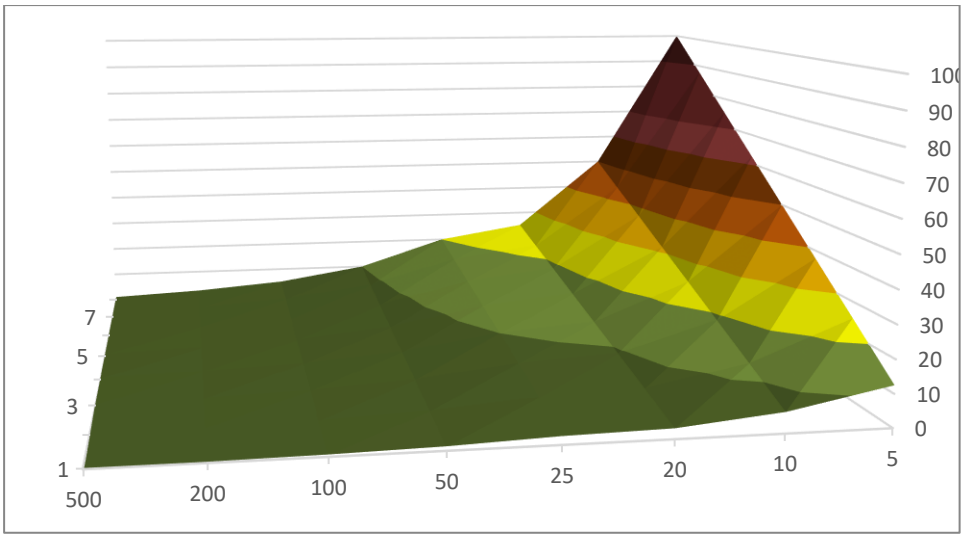
Valid	Busy	Error	Status Code (in hex)	Cause	Remedy
				buffer is smaller than configured for adapter[x]	
FALSE	FALSE	TRUE	16#86xA	Incompatible buffer types for adapter [x]	The configured T→O buffer type is incompatible to the parameterized Input buffer type. Adjust both the size and type either of the configuration or for the parameterized buffer.
FALSE	FALSE	TRUE	16#86xB	Incompatible buffer types for adapter [x]	The configured O→T buffer type is incompatible to the parameterized Output buffer type. Adjust both the size and type either of the configuration or for the parameterized buffer.
FALSE	FALSE	TRUE	16#86xC	Incompatible buffer types for adapter [x]	The configured configuration data buffer type is incompatible to the parameterized configuration data buffer type. Adjust both the size and type either of the configuration or for the parameterized buffer.

6.1.2 Technical data

For better planning of the automation program the user must be aware, that the operation of the LCCF_EnetScanner block has impacts on both memory loading and cycle time of the remaining automation program.

As all the protocol handling is done as part of the user program, the cycle time will be extended by the time the selected CPU model requires to execute the protocol stack. As one could imagine the more adapters are configured the more time is necessary to compute the communications. Another performance influencing factor is the RPI. The shorter the RPI is, the more often communication to the adapters need to be done.

Figure 6-1: PLC load depending on RPI and number of adapters



NOTE

The above diagram doesn't show real loadings nor do the value are based on real measurements for a specific CPU.

The diagram only illustrates the loading dependencies.

As shown in the above diagram, lower RPI cause more updates per time unit. This in turn causes a higher load o the PLC. The number of configured adapters also has an influence on the PLC load in the way, that the higher the number is, the higher the load will be (proportional).

SIMATIC S7-1500

The average load shown in the below table are based on measurements taken on a CPU 1512C used throughout the application example loaded with the two adapters.

Table 6-5: Execution times for LCCF_EnetScanner

adapters	min. load	average load	max. load
ET200SP MF	0,6 ms	1,5 ms	3,2 ms
ET200SP MF S7-1200	1 ms	2 ms	5 ms

The measured load is based on a 10ms cyclic interrupt and the data exchange configured in the application example.

Table 6-6: configured data exchange sizes

Adapter	Outputs	Inputs	Configuration
ET200SP MF	20 Bytes @50ms	20 Bytes @50ms	None
S7-1200	64 Bytes @25ms	64 Bytes @25ms	64 Bytes @5s

Besides program execution time memory consumption should be taken into consideration, when selecting the CPU model for a specific automation task. The LCCF_EnetScanner block contributes to the memory loading a certain amount of memory plus the data required per configured adapter. The following tables will provide the detailed information.

Table 6-7: Memory consumption S7-1500

Block	Load Memory	Work Memory
LCCF_EnetScanner	474.426 Bytes	23.395 Bytes
instance DB	36.927 Bytes	25.044 Bytes

Memory is also consumed for each adapter configured and data areas to be provided for it.

Table 6-8: Memory consumption for EtherNet/IP IO system

Adapter	Load Memory	Work Memory
1	4.453 Bytes	1.348 Bytes
2	5.635 Bytes	2.532 Bytes
3	6.816 Bytes	3.708 Bytes

NOTE

With the SIMATIC S7-1500 up to 16 EtherNet/IP adapters can be controlled. This limitation is a compromise between many factors such as update rates, CPU load, memory consumption and others.

If a specific application requires more the S7-1500 allows for more OUC connection resources, which can be used.

SIMATIC S7-1200

For the S7-1200 controller the technical data are listed below

Table 6-9: Memory consumption S7-1200

Block	Load Memory	Work Memory
LCCF_EnetScanner	478.544Bytes	23.922 Bytes
instance DB	25.176 Bytes	13.260 Bytes

The Configuration of the EtherNet/IP IO system also requires some memory. When configured with the description and the data organized as array in the same data block, the required memory is listed below.

Table 6-10: Memory consumption for the EtherNet/IP IO system

Adapters	Load Memory	Work Memory
1	4.330 Bytes	1.284 Bytes
2	5.511 Bytes	2.468 Bytes
3	6.694 Bytes	3.644 Bytes

NOTE

With the LCCF_EnetScanner block the S7-1200 controller can control up to 8 EtherNet/IP adapters. This is a compromise between many factors, such as update rates, CPU load and memory consumption.

The S7-1200 controllers allow for more than 8 OUC resources, which can be used in specific applications.

NOTICE

Risk of overloading the controller

Configuring too many EtherNet/IP adapters can overload the controller and cause the loss of control over the process, as the time required to retrieve sensor signals may be larger than allowed for safe process control.

Evaluate the requirements of the process and select an appropriate, if in doubt the larger, CPU model.

6.2 What’s next?

The current implementation leaves some room for further developments. Such implementations include:

- Support for modular adapters
- Identification of available adapters (read in network)
- Improved status display for configured adapters
- Inhibit individual adapters

7 Appendix

7.1 Service and support

Industry Online Support

Do you have any questions or need assistance?

Siemens Industry Online Support offers round the clock access to our entire service and support know-how and portfolio.

The Industry Online Support is the central address for information about our products, solutions and services.

Product information, manuals, downloads, FAQs, application examples and videos – all information is accessible with just a few mouse clicks:
support.industry.siemens.com

Technical Support

The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers – ranging from basic support to individual support contracts. Please send queries to Technical Support via Web form:
www.siemens.com/industry/supportrequest

SITRAIN – Digital Industry Academy

We support you with our globally available training courses for industry with practical experience, innovative learning methods and a concept that's tailored to the customer's specific needs.

For more information on our offered trainings and courses, as well as their locations and dates, refer to our web page:
www.siemens.com/sitrain

Service offer

Our range of services includes the following:

- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts

You can find detailed information on our range of services in the service catalog web page:
support.industry.siemens.com/cs/sc

Industry Online Support app

You will receive optimum support wherever you are with the "Siemens Industry Online Support" app. The app is available for iOS and Android:
support.industry.siemens.com/cs/ww/en/sc/2067

7.2 Industry Mall

The Siemens Industry Mall is the platform on which the entire siemens Industry product portfolio is accessible. From the selection of products to the order and the delivery tracking, the Industry Mall enables the complete purchasing processing – directly and independently of time and location:
mall.industry.siemens.com

7.3 Links and literature

Table 7-1

	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Download page of this entry https://support.industry.siemens.com/cs/ww/en/view/109782314

7.4 Change documentation

Table 7-2

Version	Date	Modifications
V1.0	03/2021	First version
V1.1	04/2021	Corrected/ Updated screenshots
V1.2	02/2022	Updated screenshots due to error correction in the blocks Updated technical data