

SIEMENS

Ingenuity for life

Industry Online Support

Home

PROFINET – MRP Ring: Important Configuration Recommendations When Using RSTP

SIMATIC ET 200, SIMATIC CFU

<https://support.industry.siemens.com/cs/ww/en/view/109759619>

Siemens
Industry
Online
Support



This entry is from the Siemens Industry Online Support. The general terms of use (http://www.siemens.com/terms_of_use) apply.

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.

The 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 <http://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 the customer's exposure to cyber threats.

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

Contents

1	PROFINET - MRP Ring: Important Configuration Recommendations When Using RSTP	3
1.1	Verification of PROFINET MRP Rings to Ensure Error-free Operation.....	5
2	Settings in the User Interface of SCALANCE Switch Products (Examples)	9
3	Terms Used	10
4	List of the Affected Products and Planned Firmware (FW) Correction Versions	11
4.1	SIMATIC CFU.....	11
4.2	Interface Modules	11
4.3	Gateways.....	12
4.4	Development Kits.....	12
5	Network Diagnostics Products	12
6	Support and Other Sources	12

1 PROFINET - MRP Ring: Important Configuration Recommendations When Using RSTP

As an established field bus communication technology, PROFINET offers many advantages and mechanisms like increased data throughput, enhanced plant availability, and integrity in other data networks.

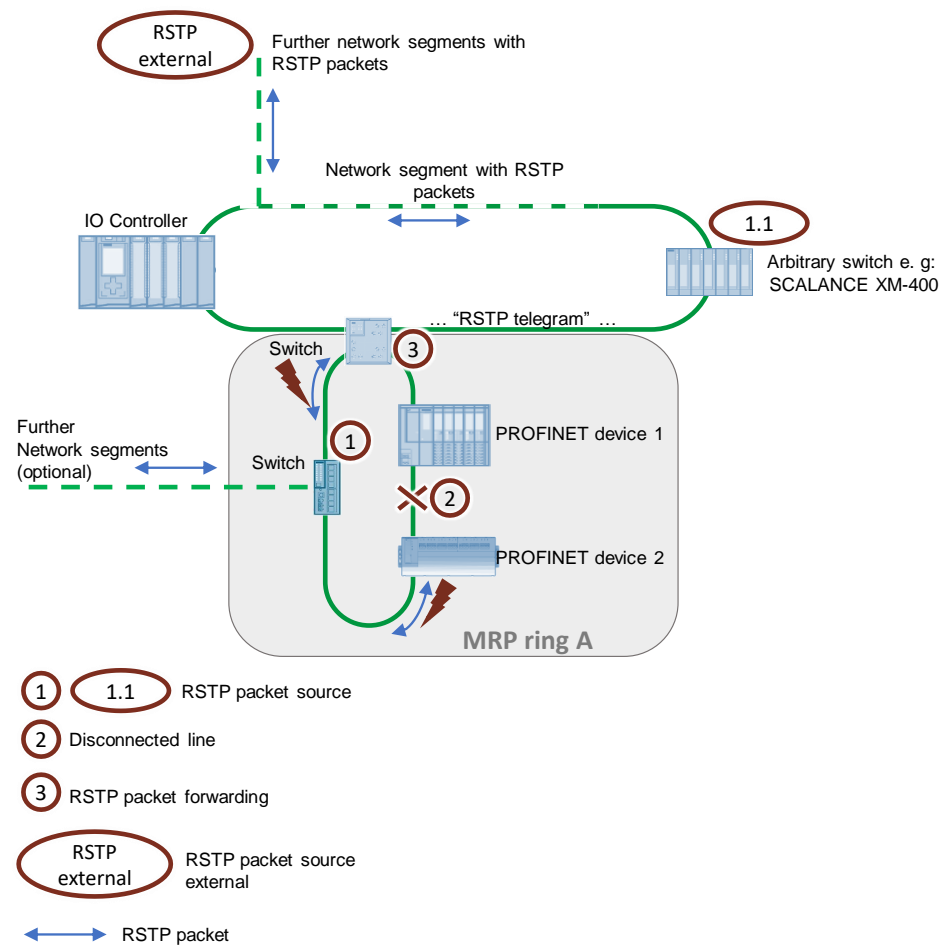
One of the classic ways of enhancing the availability of a PROFINET network segment is to use an MRP ring topology that can compensate the failure of an individual device without impairing the network.

According to the currently valid PROFINET standard there might be unintentional failure of an MRP ring if RSTP packages are in the MRP ring at the same time.

The following triggers for negatively influencing an MRP ring have been identified:

1. Return of a disconnected line connection between two neighboring affected PROFINET devices in the ring (**Figure 1-1**).

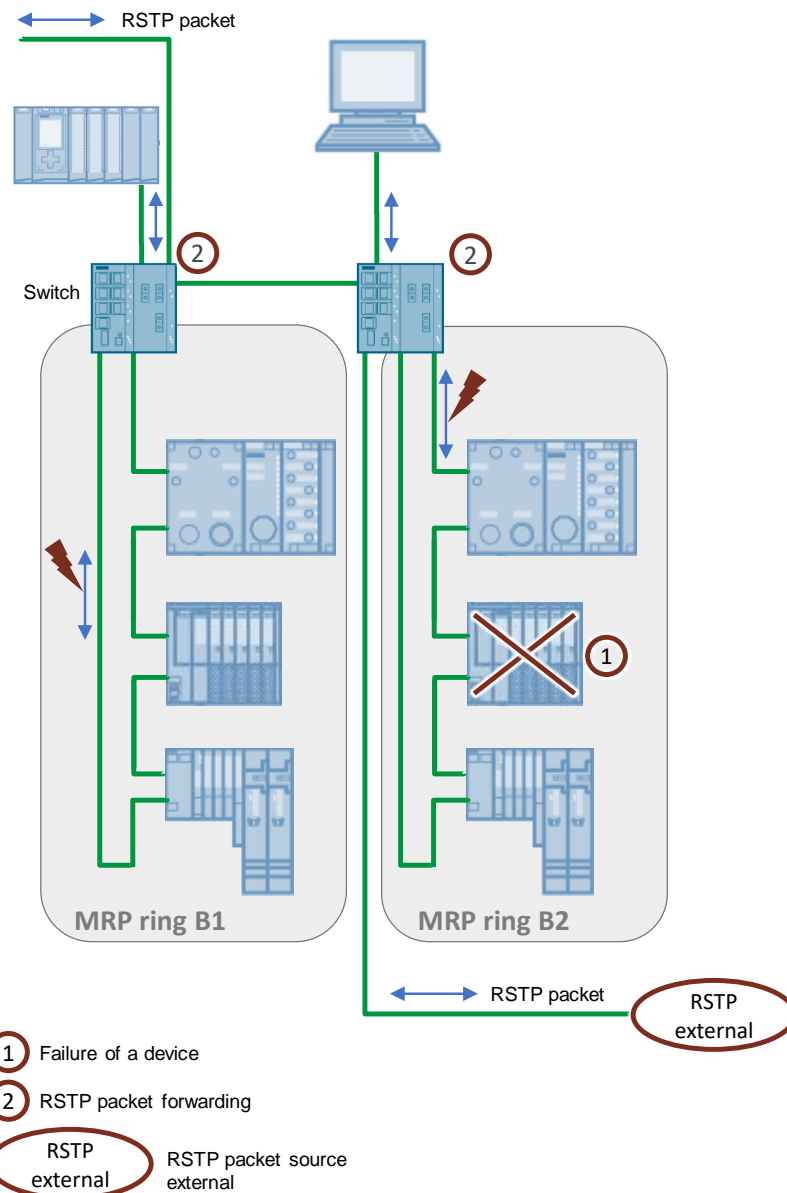
Figure 1-1



1 PROFINET - MRP Ring: Important Configuration Recommendations When Using RSTP

- Return or start of an affected PROFINET device whose neighbors are also affected PROFINET devices. This can be the result of a restart, a firmware update, switching off and on or a fault on the affected device (**Figure 1-2**).

Figure 1-2



A detailed list of the affected devices and their firmware versions is available in the additional information at the end of the document.

This document describes what is to be done for error-free function when PROFINET segments are connected with other RSTP-compatible network segments in an MRP ring topology.

For information

RSTP packages are often used in office environments and IT infrastructures to recognize and disable redundant paths in local networks. PROFINET forwards the RSTP packages transparently. Switching off of RSTP services must be made in agreement with the network administrators.

1.1 Verification of PROFINET MRP Rings to Ensure Error-free Operation

The objective is to operate MRP rings free of RSTP packages

Until corresponding firmware corrections are ready for the affected PROFINET devices, effective strengthening measures can be taken by appropriately configuring the connecting nodes (bridges) between the network segments concerned.

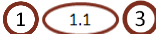
Although the SCALANCE switches are not directly affected they fulfill key tasks in the network and are used as a solution as shown in the following.

There are basically two measures depending on the source of the RSTP packages:

1) RSTP packages are created directly in the MRP ring

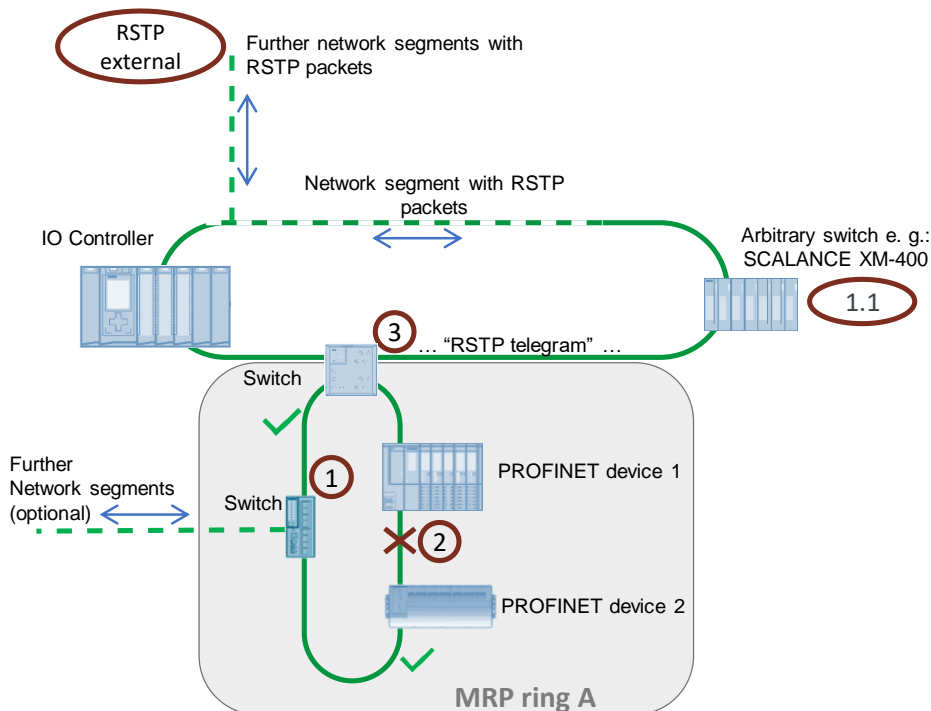
In this case the source of the RSTP packages (usually switches and/or bridges) has to be disabled:

RSTP generation (Spanning Tree) = "disabled".

See Figure 1-3 -> Components: 

1 PROFINET - MRP Ring: Important Configuration Recommendations When Using RSTP

Figure 1-3



- ① 1.1 RSTP packet source
- ② Disconnected line
- ③ RSTP packet forwarding
- RSTP external RSTP packet source external
- ↔ RSTP packet

The example presented here shows the special phenomenon that also neighboring switches that are not in the MRP ring are a source of RSTP packages by default setting even though this is not explicitly wanted in the network segmented. This is the case with SCALANCE XM-400 (1.1), for example.

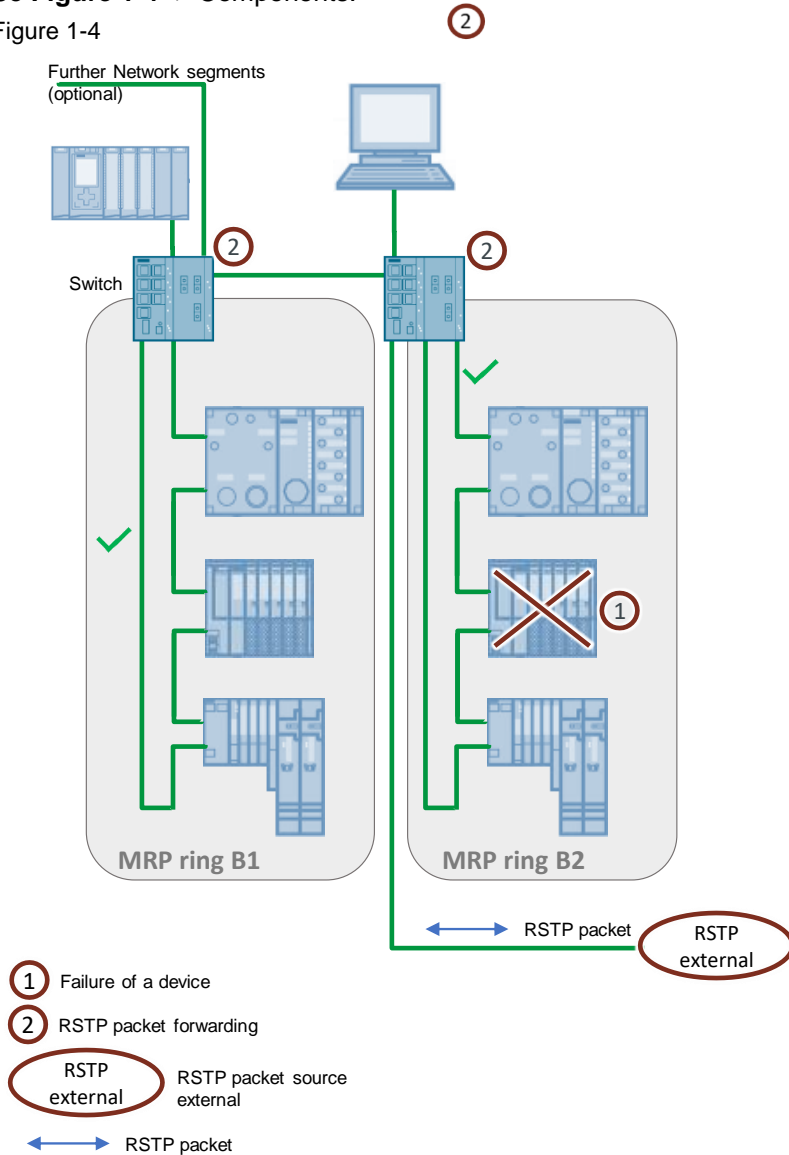
In addition, Measure 2) (see below) should be implemented for the components ① and ③ if RSTP packages are triggered from other network segments.

2) RSTP packages come into the MRP ring exclusively from neighboring network segments

Since in this case RSTP packages are generated outside the MRP ring, it suffices to block them, which means that they are not forwarded to the MRP ring:
Passive Listening = "disabled".

Se **Figure 1-4** -> Components:

Figure 1-4



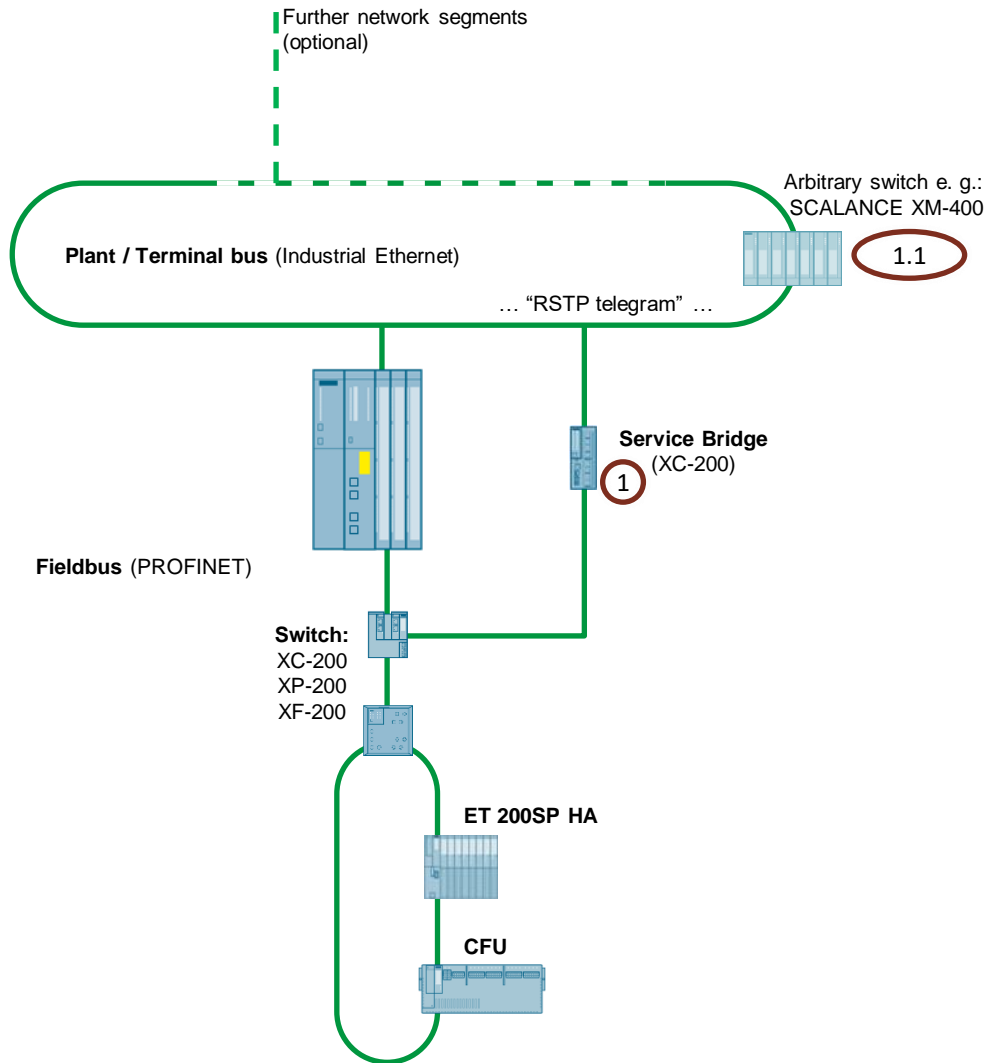
The settings recommended here assume that it is possible to do without RSTP frames in the affected MRP network segments. Please note that the "Passive Listening" setting applies to all ports. If you still need ports with RSTP frames, you can use two switches, for example, and split the network structures accordingly.

Furthermore, there are regulations for how to configure networks that prevent forwarding of RSTP packages - when using a service bridge (SIMATIC PCS 7), for example.

The network topology shown in **Figure 1-5** needs no further measures, because an S7 controller does not forward Ethernet communication between its interfaces and the service bridge (1) used blocks all RSTP packages in the basic setting.

1 PROFINET - MRP Ring:
Important Configuration Recommendations When Using RSTP

Figure 1-5



2 Settings in the User Interface of SCALANCE Switch Products (Examples)

Figure 2-1 RSTP generation ("Spanning Tree") = "disabled" taking the example of the SCALANCE XC200 series

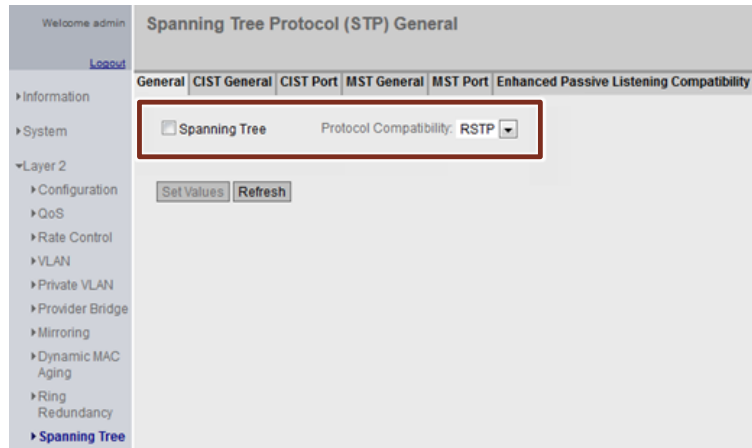
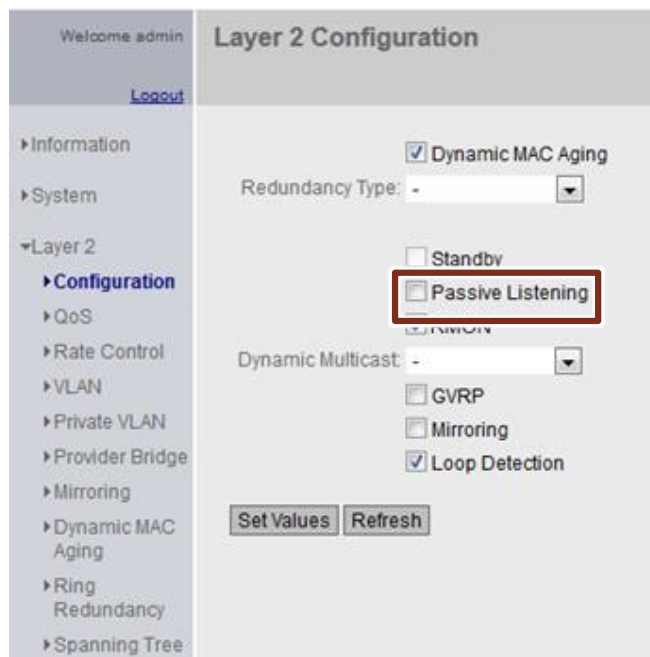


Figure 2-2 "Passive Listening" = "disabled" taking the example of the SCALANCE XC200 series



You must always make sure that when SCALANCE devices are replaced, the replacement devices have the corresponding parameters before being used in the network (using C-Plug interchangeable media, for example).

Note When using devices from other manufacturers with the same scope of functions, please get in touch with the indicated contact or support channels to get the required assistance.

3 Terms Used

RSTP

Rapid Spanning Tree Protocol. It is a further development of the Spanning Tree Protocol (STP).

RSTP generation ("Spanning Tree")

Generation of RSTP packages to disable redundant paths in local networks or enable them again if necessary (failure of a connection). (This procedure is used frequently in office environments).

Passive Listening

Forwarding of RSTP packages.

4 List of the Affected Products and Planned Firmware (FW) Correction Versions

4.1 SIMATIC CFU

Table 4-1

Article number	Product designation	Planned correction version
6ES7655-5PX11-0XX0	SIMATIC CFU PA	Cleared with coming FW version V1.1.1
6ES7655-5PX11-1XX0	SIMATIC CFU PA Bundle	Cleared with coming FW version V1.1.1
6ES7655-5PX11-1AX0	SIMATIC CFU PA Bundle Alu	Cleared with coming FW version V1.1.1

4.2 Interface Modules

ET 200SP

Table 4-2

Article number	Product designation	Planned FW correction version
6ES7155-6AU00-0CN0	IM 155-6 PN HF	Cleared with coming FW version V4.2
6ES7155-6AU00-0DN0	IM 155-6 PN HS	Cleared with coming FW version V4.0.1

ET 200SP HA

Table 4-3

Article number	Product designation	Planned correction version
6DL1155-6AU00-0PM0	IM 155-6 PN	Cleared with coming FW version V1.1

ET 200MP

Table 4-4

Article number	Product designation	Planned correction version
6ES7155-5AA00-0AC0	IM 155-5 PN HF	Cleared with coming FW version V4.2

ET 200AL

Table 4-5

Article number	Product designation	Planned correction version
6ES7157-1AB00-0AB0	IM 157-1 PN	Firmware version planned

4.3 Gateways

PN / PN coupler

Table 4-6

Article number	Product designation	Planned correction version
6ES7158-3AD10-0XA0	PN / PN coupler	Cleared with coming FW version V4.2

4.4 Development Kits

Evaluation Kit ERTEC 200P

Table 4-7

Article number	Product designation	Planned correction version
6ES7195-3BE00-0YA0	Evaluation Kit ERTEC 200P	Cleared with coming FW version V4.6

5 Network Diagnostics Products

BANY (Bus Analyzer)

Table 5-1

Article number	Product designation
9AE4140-1BA00	BANY Agent without TAP
9AE4140-1BA01	BANY Agent with TAP
9AE4140-2AA00	Bus Analyzer Agent XM-400

TAP (Test Access Port)

Table 5-2

Article number	Product designation
6GK5104-0BA00-1SA2	SCALANCE TAP104

6 Support and Other Sources

Further information about PROFINET MRP ring:

<https://support.industry.siemens.com/cs/ww/en/view/109739614>

Service Bridge Configuration file:

<https://support.industry.siemens.com/cs/ww/en/view/109747975>