SIEMENS
Ingenuity for life

# PROFINET Redundancy Functions

PROFINET

https://support.industry.siemens.com/cs/ww/en/view/109756450

Siemens Industry Online Support

**Security Informa-tion**

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.

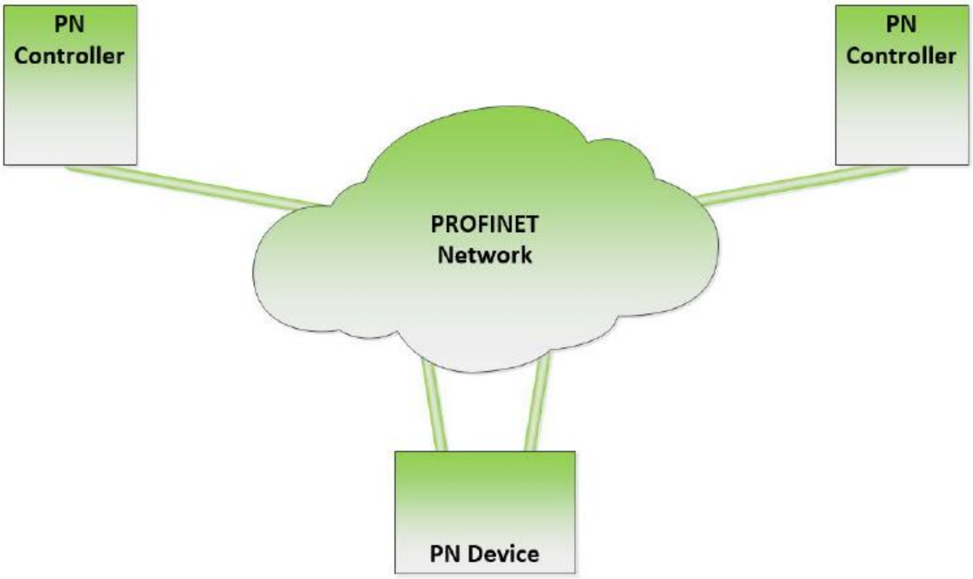
# Contents

# 1 Basic Information

With the introduction of the PROFINET communication standard it was not possible to use the redundancy functions like those of the PROFIBUS Slave Redundancy until the PROFIBUS User Organization (PNO) approved the PROFINET System Redundancy as standard for the redundant communication of PROFINET controllers and PROFINET devices in 2011.

In the following we explain the PROFINET redundancy functions in their basic configuration.

Figure 1-1 Overview of the PROFINET system redundancy



The PROFINET system redundancy standard distinguishes between four configurations with the designations NAP S1, S2, R1 and R2.

A NAP (**N**etwork **A**ccess **P**oint) is a PN interface of an IO device. Taking the example of an ET 200SP or ET 200MP, this is the PN interface of the interface module. You should note here that a NAP is not the interface module but the PN interface.

The S (single) describes an IO device with one PN interface. An R (redundant) indicates that the IO device has two NAPs:

- Either two interface modules each with a PN interface or
- One interface module with two independent PN interfaces.

A NAP S device can connect with a single network. A NAP R device can connect with a redundant network like a double line or a double ring.

The last number indicates the maximum number of communication relationships of one PN interface (NAP). This is described as an AR (Application Relationship) in the PNO standard. With a NAP S1 and a NAP R1, each PN interface can establish just one communication connection to exactly one IO controller (IOC).

An IOC in the SIMATIC product portfolio is, for example, a PN interface of an S7-400 or an S7-1500. The controller as such is called a redundant IO controller.

With a NAP S2 and R2, two IO controllers (IOCs) can be assigned to one NAP - a PN interface of an interface module, for example. It should be noted here that the NAP in operation uses only one of the two connections actively for IO data exchange and switches to the other connection only if there is a failure.

**Remark:**
With system redundancy, the IO controller (IOC) – in other words the PN interface of the PLC – and the interface module of the IO device must both support the corresponding PROFINET system redundancy function. It is not possible to redundantly connect an IO device that supports NAP S2, like the ET 200SP with a High Feature interface module, to two standard S7-1500 controllers, because this type of PLC does not support NAP S2. This configuration would be limited to the smallest common configuration – in this case NAP S1 – and would permit connection of the ET 200SP to only one of the two controllers.

Figure 1-2 Overview of the PROFINET system redundancy configurations

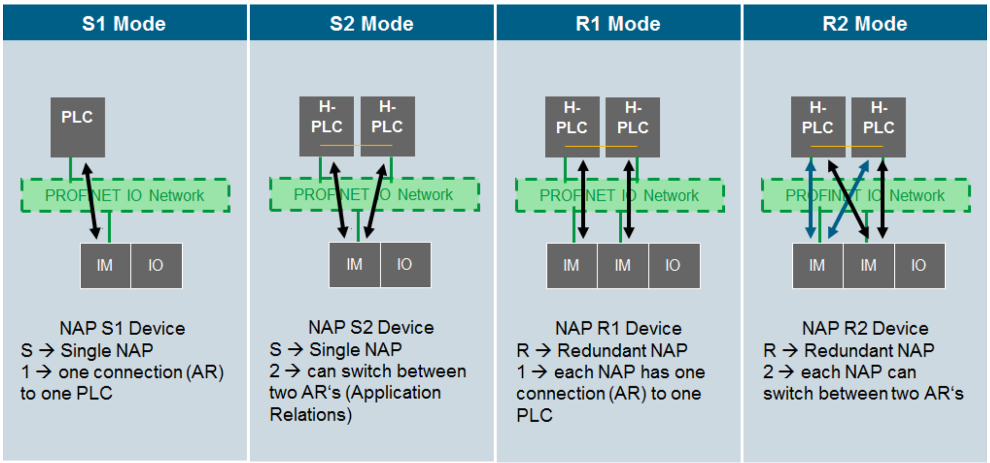


Table 1-1 Terms

| Term | Explanation |
|---|---|
| Host | Controller (an S7-1516, for example) |
| IO controller (IOC) | PROFINET interface of the host - The PROFINET interface must not be confused with the port connections. |
| IO device (IOD) | IO station (ET 200SP, for example) |
| Interface module (IM) | Header module of an IO station (ET 200SP, for example) |
| Application relationship (AR) | The AR corresponds to the communication relationship between an IO controller and an IO device. |
| Access point (AP) | A NAP corresponds to a PROFINET interface of an IO device. The PROFINET interface must not be confused with the port connections. |

# 2 PROFINET System Redundancies

## 2.1 PROFINET System Redundancy S1

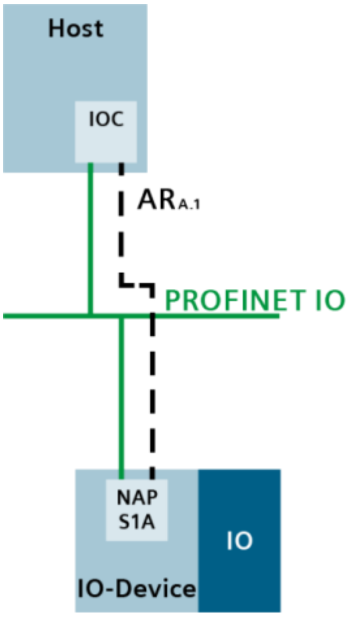
NAP S1 describes an IO device with exactly one PROFINET interface. Taking the example of an ET 200SP or ET 200MP that would be an IO device with one interface module and with one PN interface.

Via its PN interface this interface module has a communication relationship (AR) to a controller (IOC), the PN interface X1 of an S7-1516F, for example.

In the case of failure (disconnection, PLC failure) the device cannot switch over to another communication connection. This is not a redundant configuration, but describes the actual PROFINET standard.

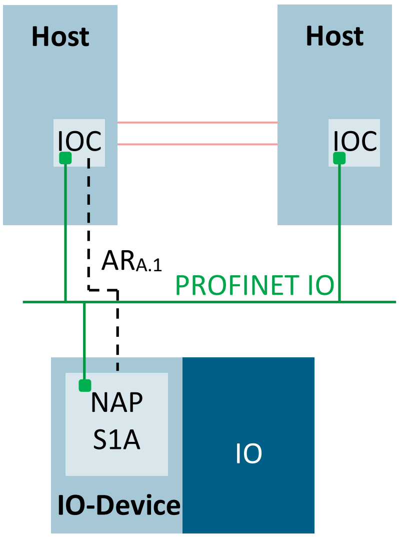
**Remark:**
PROFINET NAP S1 is supported by every standard IO device and is mentioned in the PROFINET system redundancy standard only for the sake of completeness. This does not affect the availability of a plant configuration.

Figure 2-1 NAP S1 principle



When you connect a NAP S1 device to a redundant control system (S7-400H, for example), such an IO device can only be assigned to one of the two controllers (IOC). In the case of failure (failure of the corresponding PLC, for example), the remaining controller cannot take over this IO device even though the IO device and the PN interface of the controller are physically in the same network.

Figure 2-2 Connection of a standard IO device to a redundant system



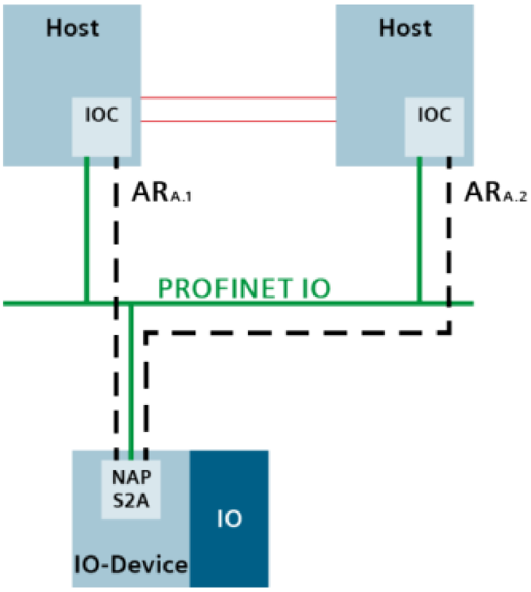
## 2.2 PROFINET System Redundancy S2

With a NAP S2 configuration, an IO device has exactly one PROFINET interface (NAP), in the case of an ET 200SP this corresponds to an interface module with one PN interface.

This one interface module can establish up to two communication relationships (ARs) with two IO controllers (IOCs) – exactly on AR per IOC. During operation, of these two connections one is used for the IO data exchange (primary AR) and the other is held in reserve (backup AR). In the PNO system redundancy standard one speaks of an AR set with two ARs.

If there is a fault with the primary AR, the control system switches to the backup connection. The data exchange then runs over the second configured IO controller (IOC).

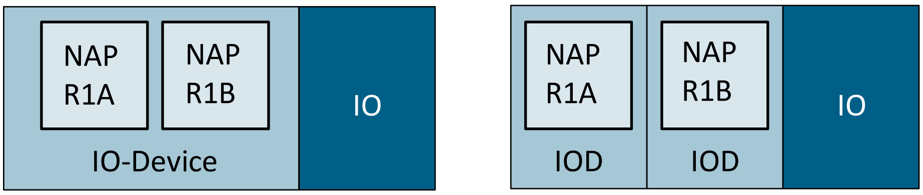
Figure 2-3 NAP S2 principle



## 2.3 PROFINET System Redundancy R1

NAP R1 describes an IO device with two PN interfaces. In the case of a SIMATIC IO station this would be one interface module with two PN interfaces or two interface modules each with one PN interface but the same IOs.

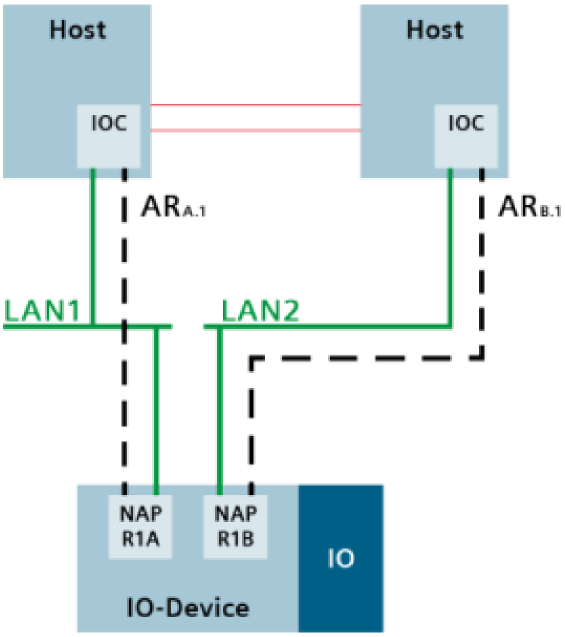
Figure 2-4 NAP R IO device configuration



This configuration is primarily for designed for use on redundant networks like redundant lines or rings. However, this is not an absolute requirement because, according to the standard, both IOCs and both NAPs are also allowed to be in the same single network (line, ring, star).

Each of these two NAPs has a communication relationship (AR) to its own IO controller (IOC). According to this, compared to the NAP S2 the redundancy is achieved not through two communication relationships per interface but through doubling of the PN interfaces.

Figure 2-5 NAP R1 principle

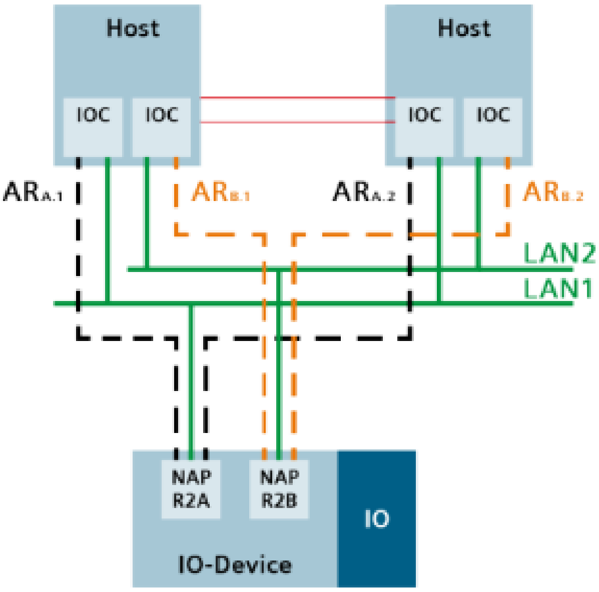


In this way a PN interface (NAP) cannot switch between the two IO controllers (IOCs) because it has only one communication relationship (AR) to one IO controller (IOC). Instead, in the case of failure of the active communication relationship (primary AR) there is switchover to the second available PN interface (NAP). As already with NAP S2 one speaks here in the PNO system redundancy standard of an AR set with two ARs.

## 2.4 PROFINET System Redundancy R2

The NAP R2 configuration combines the two solutions NAP R1 and S2 in that it can process two PN interfaces (NAPs) per IO device and each of these interfaces can process two communication relationships (ARs) to two IO controllers (IOCs). Compared to NAP S2 and NAP R1, in this case access can be made to four possible communication relationships, which is called an AR set of four ARs in the PNO system redundancy standard.

Figure 2-6 NAP R2 principle



To which communication relationship is switched to in the case of failure depends on the type of failure and via which route a stable IO communication can be provided the quickest.

# 3 Delimitation to Ethernet Redundancy Protocols

The PROFINET system redundancy is a redundancy protocol between an IO device and one or two IO controllers. This system redundancy protocol is independent of the single or redundant network used and in principle it does not matter whether and which redundancy protocols are used in the network.

It often happens that such network redundancy protocols are confused with the PROFINET system redundancy protocol or are place on the same level with it. The following protocols have the task, despite a network fault (failure switch, disconnected connection...), of maintaining the communication via alternative routes in the entire network:

- MRP - Media Redundancy Protocol
- MRPD - Media Redundancy for Planned Duplication
- HSR - High-availability Seamless Redundancy
- PRP - Parallel Redundancy Protocol
- …

The system redundancy responsible for faults in the direct IO controller <-> IO device communication relationship, if a controller or an interface module fails, for example.