Siemens
Industry
Online
Support

APPLICATION EXAMPLE

Switching System IP Address in S7-1500R/H Redundant System

S7-1500R/H V1.0 / System IP

SIEMENS

Legal information

Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG ("Siemens"). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. **The application examples are not subject to standard tests and quality inspections of a chargeable product and may contain functional and performance defects or other faults and security vulnerabilities. You are responsible for the proper and safe operation of the products in accordance with all applicable regulations, including checking and customizing the application example for your system, and ensuring that only trained personnel use it in a way that prevents property damage or injury to persons. You are solely responsible for any productive use.**

Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. Any further use of the application examples is explicitly not permitted and further rights are not granted. You are not allowed to use application examples in any other way, including, without limitation, for any direct or indirect training or enhancements of AI models.

Disclaimer of liability

Siemens shall not assume any liability, for any legal reason whatsoever, including, without limitation, liability for the usability, availability, completeness and freedom from defects of the application examples as well as for related information, configuration and performance data and any damage caused thereby. This shall not apply in cases of mandatory liability, for example under the German Product Liability Act, or in cases of intent, gross negligence, or culpable loss of life, bodily injury or damage to health, non-compliance with a guarantee, fraudulent non-disclosure of a defect, or culpable breach of material contractual obligations. Claims for damages arising from a breach of material contractual obligations shall however be limited to the foreseeable damage typical of the type of agreement, unless liability arises from intent or gross negligence or is based on loss of life, bodily injury or damage to health. The foregoing provisions do not imply any change in the burden of proof to your detriment. You shall indemnify Siemens against existing or future claims of third parties in this connection except where Siemens is mandatorily liable.

By using the application examples you acknowledge that Siemens cannot be held liable for any damage beyond the liability provisions described.

Other information

Siemens reserves the right to make changes to the application examples at any time without notice and to terminate your use of the application examples at any time. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.

The Siemens terms of use (https://www.siemens.com/global/en/general/terms-of-use.html) shall also apply.

Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity 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 cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry.

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

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

Table of contents

 © Siemens 2024

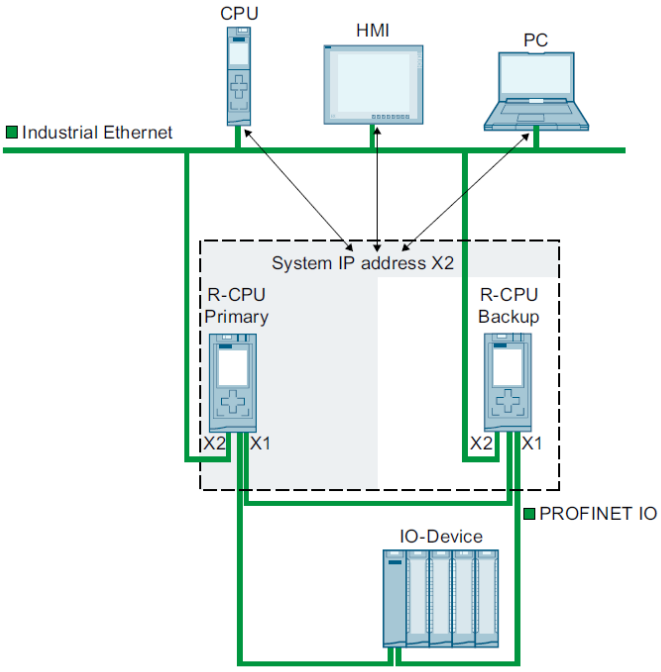
1. Introduction

1.1. Overview

The system IP address of the S7-1500R/H redundant system is a virtual IP address that is used for communication with other devices (such as HMI devices, CPUs, or PCs) and ensures that communication can continue even in case of failure of one of the CPUs of the redundant system.

For the partner device, the communication to the redundant system through the system IP address is transparent. In fact, the partner does not need to be aware that there are two redundant CPUs, as with the system IP, the redundant system is reached as a whole.

Each PROFINET interface (X1, X2, X3, W1) of the redundant CPUs can have its own system IP address.



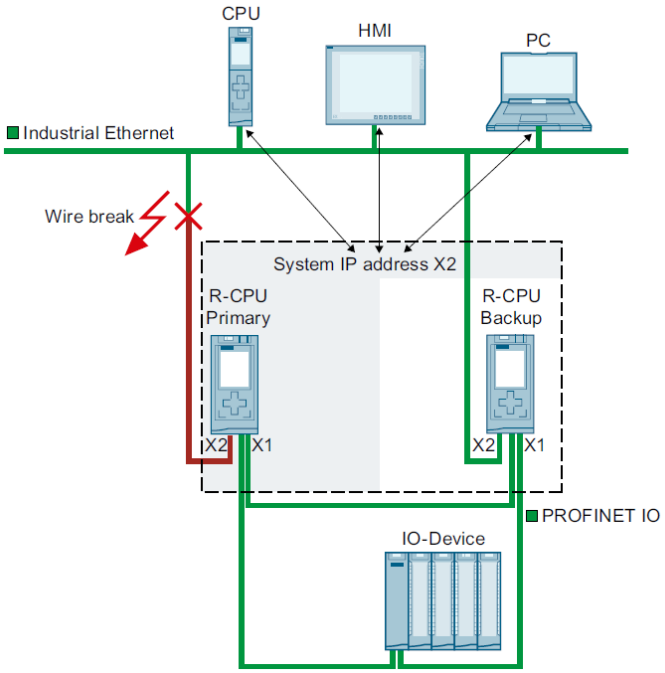
With firmware version < V4.0, by using the system IP address, the partner devices communicate only with the primary CPU of the redundant system. In RUN-Redundant state, if the primary CPU fails, the communication can continue through the new primary CPU (previously backup CPU) in the RUN-Solo state after the switchover process has finished.

The partner devices do not need to be aware of this switchover, as they continue to reach the redundant system through the same IP address, the system IP.

© Siemens 2024 |

1.2. Use case and solution

However, because with firmware version < V4.0, the system IP address is always hosted on the primary CPU, if the physical connection between this primary CPU and the partner devices is interrupted (e.g., wire break or switch failure), there is no communication anymore.



In such situations, it can make sense to switch the system IP to the backup CPU. As consequence, the communication with the partner devices can be reestablished.

With firmware version < V4.0, the only way to solve this situation is to force a STOP of the primary CPU, so that an automatic switchover takes place, and the backup CPU becomes the new primary CPU, thus also starting to host the system IP address. However, the switchover process also affects all other communications through other interfaces that might have been working correctly on the previous primary CPU. This could potentially impact industrial processes.

As of firmware version V4.0, this situation can be solved without affecting the role assignment of the primary CPU. Via two new modes of instruction RH_CTRL, the user can control which of the two redundant CPUs activates a configured system IP address. By monitoring the quality of the connection, users can decide for themselves on which CPU the system IP address must be activated.

This document provides different ways to program this connection monitoring. These depend on the device used, the network topology and the preferences of the user.

1.3. "RH_CTRL" instruction

Switching of the system IP addresses via the new modes of "RH_CTRL" instruction available with firmware V4.0 can be only used if the three following preconditions are fulfilled:

- S7-1500R/H redundant system is in the RUN-Redundant state,
- The system IP address is enabled on the considered interface,
- OPC UA Server is disabled (independent from the interface used). It is not supported currently.

The two new modes are:

- **Mode 15**: Activate the configured system IP address on the PROFINET interface with the specified HW ID (Xn or W1).
- **Mode 16**: Query of the activation status of the system IP address on the interface with the specified HW ID (Xn or W1).

S7-1500R/H redundant system has several interfaces on which a system IP address can be enabled. Each interface can be managed independently with these new modes of the "RH_CTRL" instruction.

For example, RH_CTRL supports switching of the system IP of the X2 PROFINET interface to the backup CPU and keeping the system IP of the X1 PROFINET interface hosted on the primary CPU.

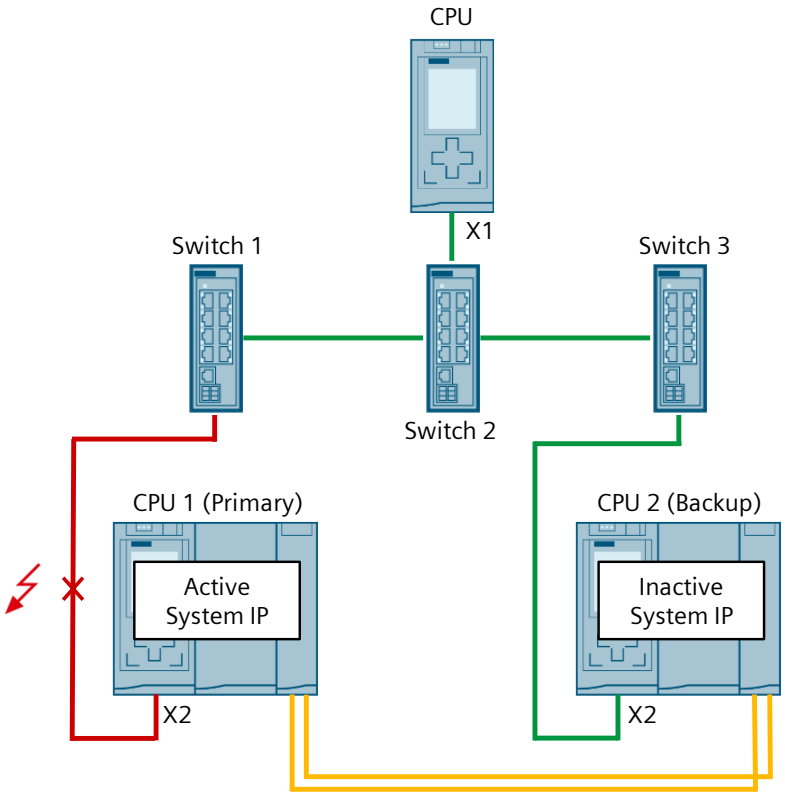
1.4. Possible scenarios

Possibles scenarios to illustrate the benefits of these new "RH_CTRL" modes.

NOTE Switching the system IP address between CPUs of the R/H redundant system does not guarantee that the communication with the devices will be reestablished. The device must be able to reach the CPU hosting the system IP address over a physical connection. Otherwise, the switching will have no effect.

1.4.1. Wire break of an ethernet cable

Failure scenario: due to a wire break, the device (e.g., CPU) is not able to reach the primary CPU (CPU 1) of the S7-1500R/H redundant system anymore. Therefore, the communication is interrupted.

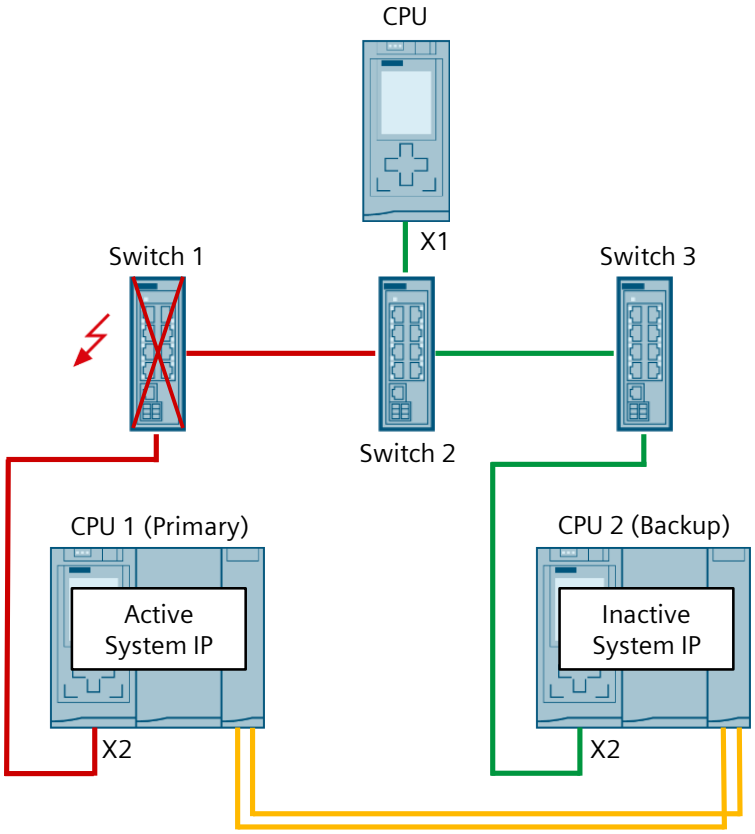


Because there is no connection failure between the backup CPU (CPU 2) and the device (CPU), a switching of the System IP on X2 interface can be triggered. As consequence, CPU 2 becomes the new host of the system IP address and the communication with the device can be reestablished.

If the wire break happened in the cable between the partner CPU and Switch 2, the switching of the System IP would have no effect. It is important to monitor the quality connection from the S7-1500R/H redundant system to the device (see chapter IntroductionConnection monitoring).

1.4.2. Switch failure

Failure scenario: due to a switch failure, the device (e.g., CPU) is not able to reach the primary CPU (CPU 1) of the S7-1500R/H redundant system anymore. Therefore, the communication is interrupted.



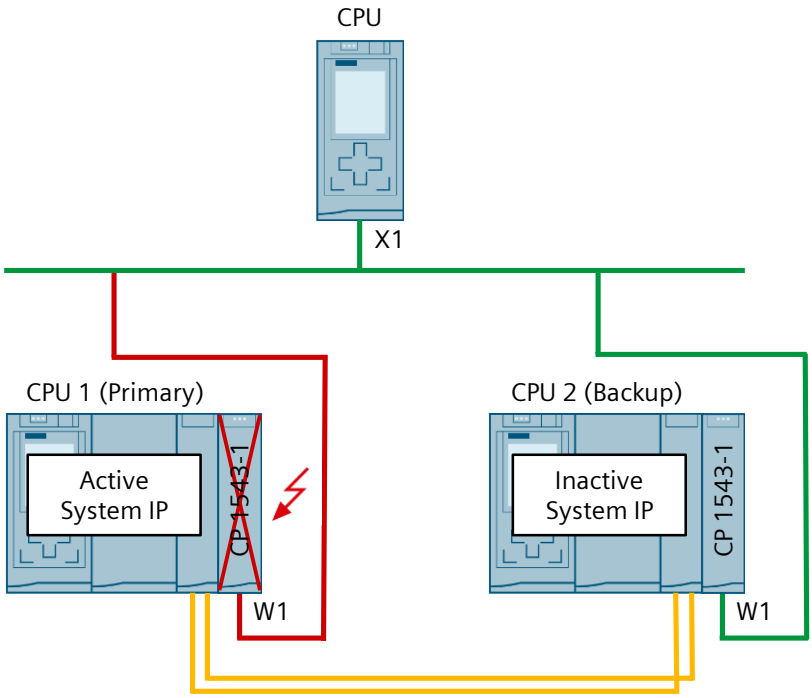
Because there is no connection failure between the backup CPU (CPU 2) and the device (CPU), a switching of the System IP on X2 interface can be triggered. As consequence, CPU 2 becomes the new host of the system IP address and the communication with the device is reestablished.

If Switch 2 failed, the switching of the System IP would have no effect. Again, it is important to monitor the quality connection from the S7-1500R/H redundant system to the device (see chapter IntroductionConnection monitoring).

1.4.3. Failure of a CP 1543-1 with S7-1500H

Failure scenario: due to a CP 1543-1 failure, the device (e.g., CPU) is not able to reach the primary CPU (CPU 1) of the S7-1500H redundant system anymore. Therefore, the communication is interrupted.

In case of S7-1500H: due to the mandatory active backplane, a CP 1543-1 failure does not trigger a CPU STOP. If the CP of the CPU currently hosting the system IP address on the W1 interface fails, the communication to the device is interrupted.



Because there is no connection failure between the CP 1543-1 of the backup CPU (CPU 2) and the device (CPU), a switching of the System IP on W1interface can be triggered. As consequence the CP 1543-1 of the backup CPU (CPU 2) becomes the new host of system IP address (W1) and the communication with the device is reestablished.

In case of S7-1500R: a CP 1543-1 failure causes a CPU STOP, therefore there is a CPU role switching. The system IP switching is performed automatically.

2. Engineering

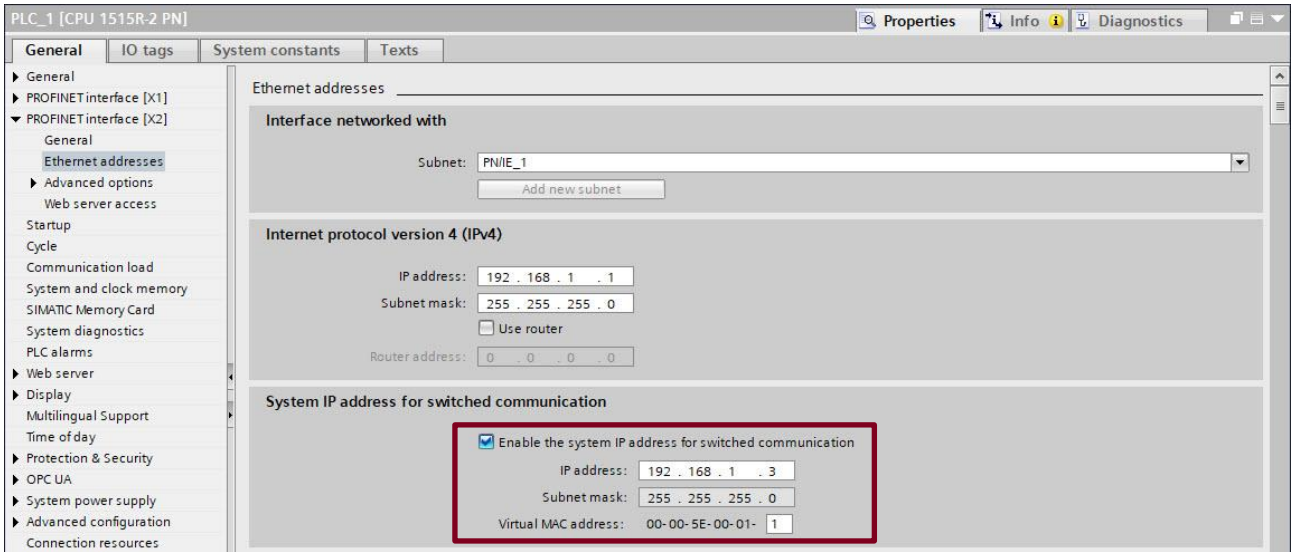
2.1. Enabling system IP address

S7-1500R/H redundant system has several interfaces in which the system IP can be enabled. Listed below are the interfaces of the redundant controllers that support firmware V4.0:

	Interface X1	Interface X2	Interface X3	W1 Virtual interface with CP 1543-1
CPU 1513R-1 PN	Yes	No	No	Yes
CPU 1515R-2 PN	Yes	Yes	No	Yes
CPU 1517H-4 PN	Yes	Yes	Yes	Yes
CPU 1518HF-4 PN	Yes	Yes	Yes	Yes

NOTE Regarding W1 Virtual interface, the system IP address can be enabled only on one pair of CP 1543-1 even if the system supports using multiple CPs.

Example: here the system IP address is enabled on the interface X2.



2.2. Connection monitoring

The connection between the S7-1500R/H redundant system and the partner device must be monitored by the user program. In case of connection failure, the switching of the system IP address can be triggered.

There are multiple ways to monitor a connection, it depends on many factors: complexity and topology of the network, type of communication partner or programming preferences of the user.

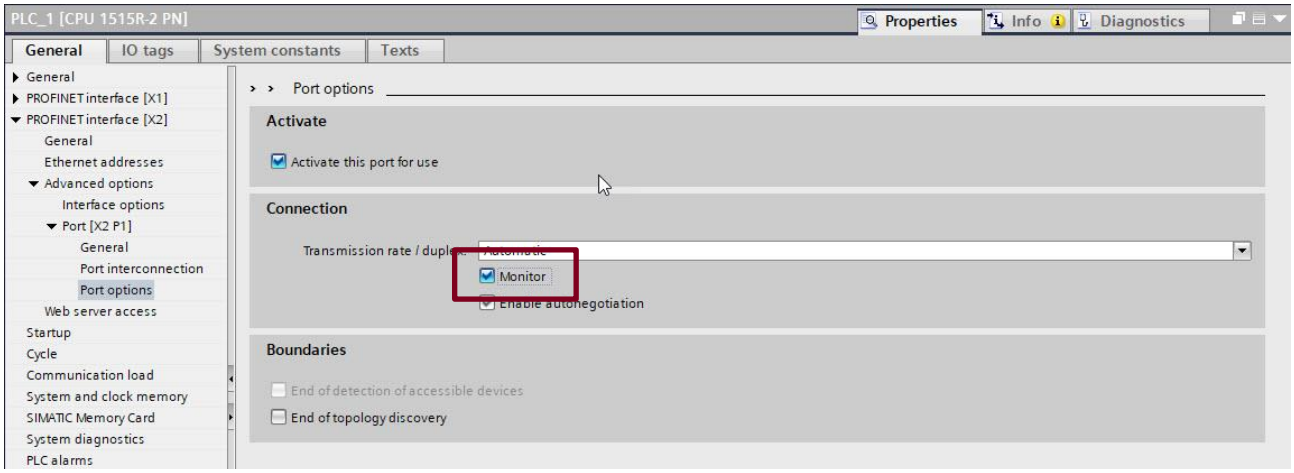
In this chapter some possibles solutions are explained.

2.2.1. Port link monitoring

The principle is to check if the port(s) of the interface of the CPU that is hosting the system IP address is correctly connected (link Up or Down) to the device. To monitor a port link, several options are available.

Enabling the "Monitor" option on the "Port options"

When enabling this option, a diagnostic message is generated when the link is down (e.g. with a wire break or a removed connector). And the OB 82 (Diagnostic error interrupt) is triggered by the firmware.



Reading the port link status using PROFINET Data Records

The user can also use the Library for PROFINET data records (LPNDR). This library provides instructions (e.g., **LPNDR_ReadGlobalInfo**) that provide such diagnostic and monitoring information.

Limitations

- For larger networks, monitoring only the controller ports is not sufficient. Indeed, if a switch in the middle of the network, but not directly connected to the CPU, fails, the port link status will not help, because no link down will be reported in that case (see for example the architecture of the chapter "switch failure"). For such configurations, ports of all involced devices in the network would have to be monitored to evaluate the status of the connection.

- Additionally, this method does not work when using the system IP address with the W1 virtual interface, in the case an additional CP 1543-1 communication processor is used.

2.2.2. Simple Network Management Protocol (SNMP)

The status of SNMP-capable network devices can be monitored via SNMP (Simple Network Management Protocol) and, if necessary, controlled by network management systems.

The instruction of the LSNMP library allows the S7-1500R/H redundant system to act as a simple SNMP manager to query information from network components. With this information, the communication path and therefore, the physical connection are monitored.

This method is common in large networks, but all devices to be monitored in the network must be SNMP-capable.

2.2.3. Lifebeat monitoring

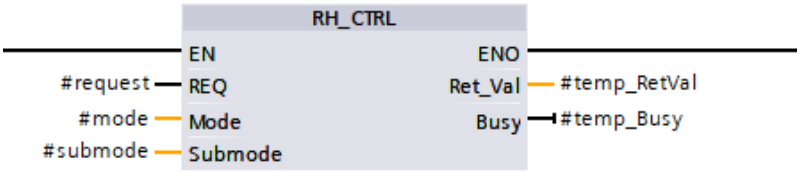
Programming a lifebeat monitoring information between the S7-1500R/H redundant system and the device is also a solution.

The lifebeat monitoring information offers a applicative solution, independent of the architecture and network used, to identify the quality of the connection. After a delay (timer) if no new information is received (watchdog), then a switching of the system IP is initiated.

There are multiple ways to program such information, depending on the type and/or the functionalities of device (e.g., handshake between both devices, diagnostic of the OUC connection via the block T_DIAG).

2.3. User program implementation

Once a physical connection failure has been detected by using one of the methods explained or any other, the "RH_CTRL" instruction is called to switch the system IP address from the CPU that is currently hosting it, to the other CPU.



HW ID as Submode

When using modes 15 and 16 with the "RH_CTRL" instruction, the submode parameter must be used to specify the interface in which the system IP will be activated or that will be queried.

The submode parameter is defined as a WORD, whereas the HW ID is defined as an UINT. To convert the HW ID from the UINT datatype to the WORD datatype, a MOVE instruction can be used.

To determine the HW identifier of a PROFINET interface:

1. Select the required interface in the device or network views of TIA Portal
1. Select the "System constants" tab in the inspector window

Block call

Continuing with the example of the wire break used in the introduction, at the time the fault is detected, the system IP address of PROFINET interface X2 was being hosted on the primary CPU, so it will be switched to the backup CPU.

1. Call the "RH_CTRL" instruction with mode 15 and HW ID (submode) of the PROFINET interface X2 on the backup CPU to activate the system IP address on required interface.

2. Call the "RH_CTRL" instruction cyclically with mode 16 and HW ID (submode) of the interface X2 on the backup CPU to query the activation status. Through the Ret_Val parameter, the block will notify whether the system IP is currently hosted on the interface (16#05), the system IP is not hosted on the interface (16#06), or the switching of the system IP is in progress (16#07).

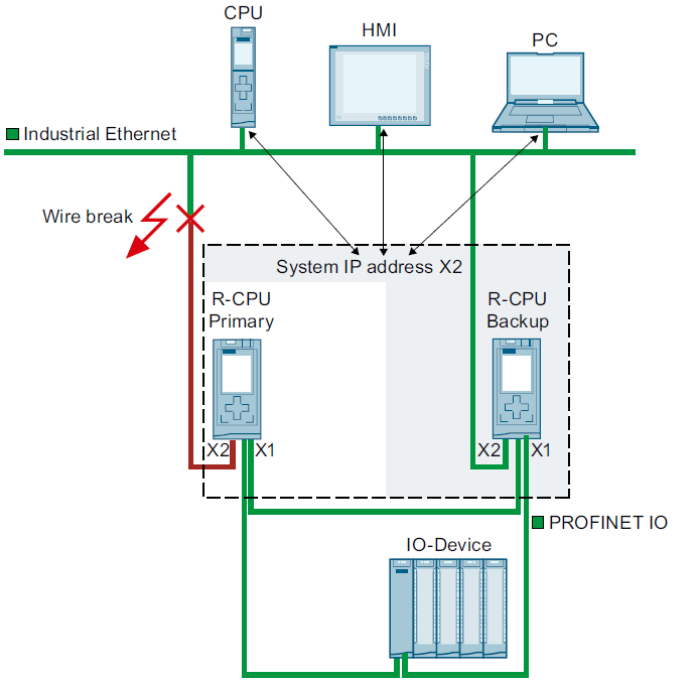
Error handling

The "RH_CTRL" instruction will provide information via the Ret_Val parameter in case of an error:

Ret_Val	Description
16#8091	The provided HW ID of the interface is not valid.
16#80A1	The R/H system is not the RUN-Redundant state.
16#80A3	The system IP address is not configured or enabled for the requested interface.
16#80A4	The switching of system IP is currently in progress and the call with mode 15 is ignored.
16#80A5	The switching of system IP is not possible due to an activated OPC UA Server.

Result

After successful completion of the system IP switchover, the S7-1500R/H redundant system is again reachable by the devices, for example: through the interface X2 of the backup CPU. See picture below.



NOTE The switching itself within the R/H-system takes few milliseconds. After that, the system IP on the new host is theoretically reachable. But for the real connection reestablishment to the new system IP host depends on also other factors like how fast the remote partner will detect connection abort towards former system IP host and establish a new connection to the new host.

2.4. Further considerations

Some further considerations to consider when using this feature:

- Even if the minimum firmware version is V4.0 to use this feature, and only documented into TIA Portal version V20, it is possible to program it with previous TIA Portal versions.
- When a system IP address is enabled on the backup CPU, performance (such as data throughput) may decrease compared to the previously activated system IP address on the primary CPU. When starting up, it is important to check whether the performance when communicating via the backup CPU is sufficient for the user application.
- When switching a system IP address to the redundant CPU, the "RH_CTRL" instruction deactivates the affected system IP address of the CPU on which it has been previously active. Deactivating will result in the termination of all communication connections that use the affected system IP address as an endpoint. The connections will be reestablished (if physically possible) once the switchover has been completed.
- Even if the system IP address is switched to the backup CPU, the role of primary CPU is not. With this feature, the system IP address is just no longer limited to being hosted by the primary CPU of the redundant system.
- As seen before, switching a system IP address from the primary CPU to the backup CPU or vice versa may only solve connectivity issues caused by the S7-1500R/H redundant system disconnected from the network. In other cases of failure (e.g., complex networks via switches) the connectivity problem might not be solved by switching the system IP address.
  If S7-1500R/H redundant system lose the RUN-Redundant state (e.g. failover or stop of a CPU), all configured system IP addresses will be activated on new primary CPU. So, default behavior of system IP become active again, if system lose redundancy.

3. Appendix

3.1. Service and support

SiePortal

The integrated platform for product selection, purchasing and support - and connection of Industry Mall and Online support. The SiePortal home page replaces the previous home pages of the Industry Mall and the Online Support Portal (SIOS) and combines them.

- Products & Services
  In Products & Services, you can find all our offerings as previously available in Mall Catalog.
- Support
  In Support, you can find all information helpful for resolving technical issues with our products.
- mySieportal
  mySiePortal collects all your personal data and processes, from your account to current orders, service requests and more. You can only see the full range of functions here after you have logged in.

You can access SiePortal via this address: sieportal.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: support.industry.siemens.com/cs/my/src

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: siemens.com/sitrain

Industry Online Support app

You will receive optimum support wherever you are with the "Industry Online Support" app. The app is available for iOS and Android:

3.2. Links and literature

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to this entry page of this application example https://support.industry.siemens.com/cs/ww/en/view/109972846
\3\	Library for PROFINET data records https://support.industry.siemens.com/cs/ww/en/view/109753067
\4\	Libraries for Communication for SIMATIC Controllers https://support.industry.siemens.com/cs/ww/en/view/109780503
\5\	How do you program the TSEND_C and TRCV_C instructions for open user communication over the integrated PROFINET interface of the S7-1200/S7-1500 CPU? https://support.industry.siemens.com/cs/ww/en/view/67196808
\6\	How do you configure and program an S7 connection and the "PUT" and "GET" instructions for data transfer between two S7 CPUs? https://support.industry.siemens.com/cs/ww/en/view/82212115
\7\	How do you program and parameterize Modbus/TCP communication between S7-1500 CPUs and S7-1200 CPUs? https://support.industry.siemens.com/cs/ww/en/view/102020340

3.3. Change documentation

Version	Date	Modification
V1.0	12/2024	First version