BPC 9102S – CHANGE NOTES

**Change notes for the BPC 9102S
Remote Field Controller**

Application note
1246285_en_14   © PHOENIX CONTACT 2022-09-07

1 General information

This document contains all changes made between firmware version 2021.9 and the current firmware version of the BPC 9102S Remote Field Controller
(Order No. 1246285).

Current firmware version: 2025.0.3

i	**Recommended:** To be able to use all new functions of a firmware version, always use all elements of the toolchain in the same version. The toolchain includes, for example, PLCnext Engineer, SDK and PLCnext CLI.

i	**Note:** In the context of a firmware update, the controller will be restarted. During this time, the plant availability can not be guaranteed.

i	**Attention when downgrading the firmware** Any BPC 9102S with a hardware-revision 03 or newer cannot be downgraded to a firmware version 2022.0.x or older ! This results in a defective hardware

i	**Attention HW:04 can not be downgraded** Any BPC 9102S with a hardware-revision 04 and therefore firmware-version 2023.6.4 can not be downgraded in firmware. Next possible update for such device is: FW: 2024.0.9 LTS FW 2025.0.2 or newer

2 Table of contents

i	**Attention! - If you updated the firmware from any previos firmware-version (2024.0.4 or 2023.6.3 or older) to FW 2025.0.2 or newer,** you can no longer downgrade/upgrade to the origin firmware-version. The next available update for a device with FW 2025.0.2 installed is: FW 2023.6.4 FW 2024.0.9 FW 2025.0.2 and newer.

i	Make sure you always use the latest documentation. It can be downloaded at phoenixcontact.net/product/1246285.

PHŒNIX CONTACT

INSPIRING INNOVATIONS

3 Changes in firmware version 2025.0.3

This section describes changes made between firmware version 2025.0.2 and firmware version 2025.0.3.
All parts of the previously released version are included in the current version.

Important information
Updating to firmware versions 2025.0.2 and newer from older firmware versions may have unexpected effects on the existing application or specific user settings.
It is strongly recommended to observe the following points before rolling out the firmware into productive operation:

– Intensive study of the change notes in this section and further documentation under Application-relevant changes 2025.
– Backup the project data and configurations before the update.
– Qualification of the application with regard to functionality or compatibility after the update.
– A downgrade back is possible, but an automatic restoration of all specific configurations cannot be guaranteed.

To be able to use all new functions of the firmware, you need PLCnext Engineer version 2025.0 LTS or newer.
Select the latest template for firmware version 2025.0 LTS in the PLCnext Engineer project.

In order to update to firmware version 2025.0.2 or newer at least a firmware version 2023.0 LTS or newer must be installed on the PLC. Older firmware versions will not accept the *.rauc firmware update file.

The following safety-related firmware versions must be used.
Please contact the Competence Center Services as to the details on safety firmware update procedure:
Phone: +49 5281 946 2777
E-mail: safety-service@phoenixcontact.com

| 02.10.0006 | ✔ |

Attention! - If you updated the firmware from any previos firmware-version (2024.0.4 or 2023.6.3 or older) to FW 2025.0.2 or newer,
you can no longer downgrade/upgrade to the origin firmware-version.
The next available update for a device with FW 2025.0.2 installed is:
FW 2023.6.4
FW 2024.0.9
FW 2025.0.2 and newer.

Observe the following general notes:

Changes in firmware version 2025.0

The firmware version 2025.0 contains updated parts of the underlying Linux® operating system and adapts the PLCnext Runtime System to these changes. This can have an impact on your application.

It is therefore absolutely necessary to familiarize yourself with these changes and the associated consequences before performing the update to firmware version 2025.0.

Note all the information in section 4 "Changes in firmware version 2025.0.2" and also read the additional information under Application-relevant changes 2025 and evaluate them for your own application.

3.1   Error corrections

– After updating to FW 2025.0.2, DNS name
resolution was unsuccessful, causing the
connection to the PLCnext Store, Proficloud,
or general internet to fail after the update.
This issue has been resolved; with the update
to FW 2025.0.3, the DNS name is correctly
resolved, and any internet connection
existing before the update remains active
after the update.

- After updating to FW 2025.0.2, an
unconfigured gateway '0.0.0.0' was set as
the active gateway on X3 - ETH LAN2.
This potentially caused an internet connection
drop. This behavior has been fixed.
A gateway '0.0.0.0' configured for X3 - LAN2
before an update to FW 2025.0.3
is considered 'unconfigured' and skipped.
As a result, a configured gateway on X4 - LAN3
remains active after the update.

- After updating to 2025.0.2 with an
"uncofigured" Gateway (0.0.0.0) on any
Ethernet-Port, the respective port could
no longer be configured in the new firmware.
This behavior has been fixed.

- FW 2025.0.2 could be brought into a
continuous reboot loop
(e.g., due to a faulty application).
The mechanism for detecting an infinite loop
did not intervene. This behavior has been
fixed with FW 2025.0.3.
A mechanism now detects a software-driven
infinite loop of reboots and only boots the
operating system, not the application,
to resolve possible errors and causes of
the reboot loop.

- Any self-created user in FW 2025.0.2 other
than the default user 'admin'
was unable to log in to the EHMI.
This issue has been resolved.

- Accessing an EHMI visualization with trend
charts caused exceptions and crashes in FW
2025.0.2. This issue has been fixed.

3.2   Known limitations and errors

> ℹ The known limitations and errors can be found in
> the PLCnext Info Center at:
> https://www.plcnext.help/te/Known_issues.htm
> Here you will find a constantly updated overview
> of all known issues.

3 Changes in firmware version 2025.0.2

This section describes changes made between firmware version 2024.0.6 and firmware version 2025.0.2.
All parts of the previously released version are included in the current version.

ℹ Important information
Updating to firmware versions 2025.0.2 and newer from older firmware versions may have unexpected effects on the existing application or specific user settings.
It is strongly recommended to observe the following points before rolling out the firmware into productive operation:

– Intensive study of the change notes in this section and further documentation under Application-relevant changes 2025.
– Backup the project data and configurations before the update.
– Qualification of the application with regard to functionality or compatibility after the update.
– A downgrade back is possible, but an automatic restoration of all specific configurations cannot be guaranteed.

ℹ To be able to use all new functions of the firmware, you need PLCnext Engineer version 2025.0 LTS or newer.
Select the latest template for firmware version 2025.0 LTS in the PLCnext Engineer project.

ℹ In order to update to firmware version 2025.0.2 or newer at least a firmware version 2023.0 LTS or newer must be installed on the PLC. Older firmware versions will not accept the *.rauc firmware update file.

ℹ The following safety-related firmware versions must be used.
Please contact the Competence Center Services as to the details on safety firmware update procedure:
Phone: +49 5281 946 2777
E-mail: safety-service@phoenixcontact.com

| 02.10.0006 | √ |

ℹ Attention! - Due to a hardware change in hardware-revision HW:04 a device with FW 2023.6.4 can not be downgraded/upgraded to any previsios firmware-version.
The next available update for a device with FW 2023.6.4 installed is:
FW 2024.0.9
FW 2025.0.2 and newer.

ℹ Attention! - If you updated the firmware from any previos firmware-version (2024.0.4 or 2023.6.3 or older) to FW 2025.0.2 or newer,
you can no longer downgrade/upgrade to the origin firmware-version.
The next available update for a device with FW 2025.0.2 installed is:
FW 2023.6.4
FW 2024.0.9
FW 2025.0.2 and newer.

ℹ Attention! - Before updating to firmware version 2025.0.2, a valid gateway must be set for each Ethernet interface. A "0.0.0.0" gateway for an Ethernet interface is not valid.

Observe the following general notes:

Changes in firmware version 2025.0

The firmware version 2025.0 contains updated parts of the underlying Linux® operating system and adapts the PLCnext Runtime System to these changes. This can have an impact on your application.

It is therefore absolutely necessary to familiarize yourself with these changes and the associated consequences before performing the update to firmware version 2025.0.

Note all the information in section 4 "Changes in firmware version 2025.0.2" and also read the additional information under Application-relevant changes 2025 and evaluate them for your own application.

3.1 New functions

App Manager

As announced, the app part types "Linux Daemons" and "Shared Libraries" are discontinued. The AppManager supports the new app part type "OCI Container" which is intended to become the successor of daemon apps. Additionally the AppManager does no longer include the path of *.so files announced as "sharedlibs" by the app_info.json into the ld.so.conf file of the Linux OS. Furthermore, a new RSC service IAppManagerService has been developed. This service can be used to retrieve information about installed apps and their state. In case of complex apps that are a combination of several apps the RSC service can be used to install the dependent apps in the necessary order.

Backup & Restore

The WBM has been extended by the page "Backup & Restore". On this page, different data sets, for example configuration or project files, can be selected and saved into an archive. Vice-versa an archive can be selected and its data sets can be restored. Backup & Restore uses the "PreparedForUpdate" state. At the moment only archives created with the same firmware version can be restored in order to ensure proper operation in case of future extensions.

Configurable alarms

– In combination with firmware 2025.0.2 (or newer) PLCnext Engineer 2025.0 (or newer) supports a system variable "ALARM_PROGRAM_STATUS" which provides information about the execution duration of the "AlarmProgram" instances.
– In combination with firmware 2025.0.2 (or newer) PLCnext Engineer 2025.0 (or newer) supports the use of variables to configure the alarm thresholds (previously only constants were supported).
– When configurable alarms (as defined in PLCnext Engineer) are confirmed or acknowledged via REST API a comment can be specified optionally. The alarm stores the latest comment. Specifying no comment keeps the previous comment, specifying an empty comment removes the previous comment.

GDS

– IN and OUT ports of a field bus component can be accessed via GDS data access services. This includes IOs of the following field busses:
  – Axioline
  – EtherNet/IP
  – INTERBUS

– Modbus TCP client
– PROFIBUS
– PROFINET

Additionally, the implementation of this feature enables to use elements of a field bus array in a GDS connector. Of course, the data types of the "startPort" and "endPort" have to be compatible.

GRPC

The PLCnext gRPC service supports to browse for existent gRPC services. There is no need to use the related protobuf files.

IEC 61131-3

The user program memory for IEC 61131-3 programs by PLCnext Engineer has been increased from 16 to 32 MB.

Licenses

For certain licenses (for example license is checked from an OCI container) and as a preparation for future features, CodeMeter Runtime from WIBU-Systems has been added to the firmware. The WIBU runtime is not automatically started by the firmware.

Modbus Client TCP

In combination with PLCnext Engineer 2024.6 (or newer) the firmware supports an Modbus TCP client. This client can be configured using PLCnext Engineer.
As factory default setting, the feature Modbus TCP client is deactivated. If necessary it can be activated via the WBM page "System Services".

OPC UA

The OPC UA client delivers diagnostic information. This information can be retrieved from the OPC UA server:

For each client connection there is one node (with child nodes) under Root.Objects.DeviceSet.<PLC-type>.eUA-Client.Connections, where <PLC-type> is the type name of the PLCnext Control device (e.g. "AXC F 2152" or "RFC 4072S"). These nodes belong to the newly introduced namespace "urn:<node-name>:PhoenixContact:eUA-Server/eUAClient/" where <node-name> is the name configured for the OPC UA server.

Podman

The Podman container system can also be operated by the Linux user "admin" without root rights being required.

Project Integrity

The project integrity check has been extended by a project signature. On the WBM page "Project Integrity" the con-

troller can be configured if and how the integrity or signature is checked and how to react in case of an integrity breach. PLCnext Engineer 2025.0 (or newer) projects can be configured with a private key and a certificate for signing projects when downloading the project. Using the WBM this certificate can be stored in the trust store "Code Signing". During this implementation also the safety project is included in the project integrity check.
A new RSC service has been implemented to read or write the project integrity configuration:
Arp::Plc::Domain::Services::IPlcConfigService.

PROFINET

The filter options "Station name", "IP address" and "Device state" are supported on the "Diagnostics" - "Profinet" WBM page tabs "Device list" and "Tree view".

SDK/C++

When creating a new project with the PLCnext CLI toolchain a header file named "<projectName>LibraryInfo.hpp" is created. This header file yields a version number of the library as an instance of the ArpVersion class. A user-specific version number can be entered and maintained during further development of the library. For ACF components this version number can be retrieved among other information by the RSC service Arp::Base::Rsc:Commons::ISystemInfoService.

WBM

The WBM page "Firmware update" has been reworked in order to use the "PreparedForUpdate" state. At the same time not only the firmware but also "PLCnext Engineer Software Packages" can be installed to the PLC. Consequently the WBM page has been renamed to "Update". In a future version this page can be extended to install further packages, for example safety-related firmware.

3.2 Changes

C++

– With the SDK version 2025.0 the language standard C++ 20 has been set in the compiler options ("-std=c++20"). The firmware itself is also compiled with this option set.
– For libraries created from C++, the firmware 2025.0 checks the version of the SDK used to compile these libraries. If the SDK version is 2024.6 or older then the library is not loaded and a notification is emitted. In these cases the libraries have to be recompiled with an appropriate SDK. Note that such libraries may also be part of a PLCnext Engineer project.

General

Firmware version 2025.0.2 brings some fundamentally updated parts of the underlying Linux® operating system and adapts the PLCnext Runtime System to these changes, resulting in higher RAM and CPU utilization. This in turn can have an impact on existing applications if these applications are close to the maximum RAM and CPU performance of the respective PLC type. For such applications, Phoenix Contact recommends also checking the RAM and CPU utilization when validating the functionality after a firmware and application update.

Firmware update

The Linux script "update-plcnext" has been removed (including its product-specific symlinks). Please use the WBM, DaUM, OPC UA or the RSC service IDeviceControlService::StartFirmwareUpdate() to install a different firmware version.

Linux

- The Linux system has been updated to version 6.1.
- The "boost" packages have been updated to version 1.84.0.
- Busybox has been removed entirely from the PLCnext Linux. Alternatives have been implemented for all necessary tools. Some of these alternatives have already been added with previous firmware versions.
  At the same time the following packages have also been removed:
  - text editor "vim" as well as "vi". Please use "nano" instead which is also set via Linux environment variable "EDITOR".
  - obsolete scripts related to gdbserver. These scripts have been added by Phoenix Contact but are no longer needed.
  - script "plcnext-update" (see above)
  - deprecated plug-in "stroke" of strongwan, existing configuration files (ipsec.conf) from 2024.6 or earlier firmware must be migrated to the new swanctl.conf syntax.
  - the "ipsec" script, to control an ipsec connection. The swanctl commands must be used.
  - the packages "cyrus-sasl" and "krb5" have been removed from the PLCnext Linux.
- Firmware 2024.0 shifted to OpenSSL 3.0. With firmware 2025.0 the outdated OpenSSL 1.1.1 binaries have been removed as announced.

- Since the Linux init system "SysV" has been replaced with "systemd" the firmware can no longer be started or stopped with the "/etc/init.d/plcnext" script. Please use the command "systemctl" instead, e.g. "sudo systemctl stop plcnext".
- The size of the "tmpfs" file system which is used for temporary files has been limited.
- Due to security reasons it is no longer possible to add users directly to the Linux system (using the command "useradd"). So the PLCnext user management is now the central authority to manage users.

LDAPS

In the past the firmware added PLCnext users with the role "Admin" also as Linux users to the Linux user management. Consequently, these users are stored in the PLCnext user management as well as (local) users in the Linux user management. Furthermore, logging in to Linux (SSH, SFTP) was not possible for PLCnext users defined via LDAP server.
By enabling the LDAP server to make use of the PLCnext user role "Admin", this procedure needed to be changed. As a consequence, before updating the firmware from ≤ 2024.6 to ≥ 2025.0, these users as well as users added directly to the Linux system need to be removed manually. Any files and folders created by these users must be removed, too, otherwise these files have an owner that is no longer known to the Linux user management. The same holds true for PLCnext user roles to which you have added the permission "arp.device/protocol.restricted_sftp:22". All these data will be removed by resetting the PLC to default settings.

Network/system

By changing the Linux init system from "SysV" to "systemd" Linux stores the IP configuration in different files and formats. As a consequence, PLCnext Linux is equipped with a conversion from the "SysV"-based configuration to the "systemd"-based configuration. When the PLC is booted this conversion starts. After a successful conversion the firmware saves itself a hash of the converted IP configuration. At its next execution the conversion compares the "SysV"-based configuration against the saved hash and converts only if necessary. The old IP configuration remains at the overlay file system, so that this configuration becomes active when downgrading to a firmware ≤ 2025.0. Furthermore, this conversion can handle all IP configurations set via PLCnext Engineer or the WBM. In case the "SysV"-based configuration file "/etc/network/interfaces" was manually changed (root rights necessary) it must be checked if these changes have been converted, too. Note that firmware 2025.0.2 (and newer) only saves changes to the IP configuration in the

new "systemd"-based configuration. Therefore when downgrading from firmware 2025.0.2 (or newer) to firmware 2024.6 (or older) the IP configuration may change while up/downgrading between firmware 2019.x and 2024.x keeps the IP configuration.

Note: When switching to DHCP via RSC service "IDeviceSettingsService" using the key "Interfaces.Ethernet.[AdapterIndex].IpAssign" (PLCnext Engineer uses this service at its "Online parameters" editor) firmware version 2025.0.2 keeps the set static IP address as well as the address set via DHCP while firmware version ≤ 2024.6 only makes use of the IP address set via DHCP.

OPC UA client

The performance of subscription (retrieving values from a remote OPC UA server) has been improved.

OPC UA server

The namespace "urn:<node-name>:PhoenixContact:eUA-Server/eUAClient/" where <node-name> is the name configured for the OPC UA server has been introduced with firmware 2024.6 and is only present if the OPC UA client is activated (WBM page "System Services"). This namespace uses index 2 (index 3 if OPC UA PubSub is activated additionally) at the "NamespaceArray" of the OPC UA server and all following namespaces are shifted by one index (if OPC UA client is activated).

PROFINET

PROFINET

In case of factory defaults behavior the PROFINET names of the PLC have been changed. In the past the name "pnc" indicated PROFINET controller and "pnd" indicated PROFINET device function. As this is ambiguous for ETH adapters which support both functions now the name of the ETH adapter became part of the PROFINET name. The names have been changed.

– The PROFINET controller stack had to be adapted to the increased requirements of the PROFINET certification test, resulting in an increased CPU load in ESM 1. In exceptional cases, this can lead to a task watchdog in PLC projects with many PROFINET connections and tightly set ESM task watchdog times.

GDS

Global variables connected to I/O and also system variables are no longer updated by the ESM task "GLOBALS" if no update task is configured. Instead the update is per-

formed by the task "GdsGlobals". This task has the same priority and the same interval time of 50 ms but is not controlled by the ESM. This means that the variables are updated even in PLC state "Stop".
Note: This is especially useful if the new system variable "PLC_STATE" shall be displayed via HMI.

Diagnostic log files

The diagnostic logging is split into several files, for example:
– Arp.log
– Arp.Init.log
– Arp.Io.ProfinetStack.log
– Arp.Services.Ehmi.log
– Arp.Services.SpnsProx.log
– Custom.log

Previously, all log message have been logged in the file "Output.log". In addition, the Linux command line tool "arp-merge-logs" has been developed and integrated in the PLCnext Linux. With this tool multiple log files can be merged into a single file.
At the same time the non-security-related Arp log messages are no longer forwarded to syslog. Security-related logs are forwarded to syslog as with previous firmware versions.

User manager

The name of the PLCnext user role "SecurityAdmin" has been changed to "SecurityEngineer". Only the name has been changed, the role's permissions remain the same.

Security Profile

– When activating the Security Profile, the PLCnext user "admin" remains (previous firmware versions did remove this user). Anyhow, this configuration must be adopted after the first installation to a minimum configuration feature set needed for the application. See PLCnext Security Info Center (2025.0) for further information on risk analysis and secure-by-default configuration.
– When the Security Profile is active, the system services "APP MANAGER", "DATALOGGER", "GRPC LOCAL SERVER", "LINUX SYSLOG", "MODBUS CLIENT TCP", "NETLOAD LIMITER", "OPCUA CLIENT", "PLCNEXT STORE", "PROFICLOUD" and "SOFTWARE UPDATE" can be activated or deactivated via WBM or by an app.

– When activating the Security Profile, the system services "APP MANAGER", "DATALOGGER", "GRPC LOCAL SERVER", and "NETLOAD LIMITER" are active additionally compared to firmware 2024.6.

– When activating the Security Profile, the firewall configuration allows incoming and outgoing ICMP requests (ping).

System watchdog/system monitor

A new firmware component "system monitor" has been implemented. It monitors RAM and CPU load and emits notifications if certain levels are exceeded. In case of further exceeding the component "system watchdog" is informed and becomes active. Therefore, this component has been refactored. Both components reside in the same library. The "system watchdog" also reacts when a firmware process died. In these cases the "system watchdog" collects diagnostic information and supervises an emergency exit procedure. For diagnostics purpose several logs and active LTTNG traces are collected into a folder named /opt/plcnext/logs/Arp.System.Monitoring/[timestamp]-Arp.system.Monitoring.Monitor.[reason] (Note that this path has been changed compared to FW 2024.0 and 2024.6.). Up to 10 logs can be stored, older folders are deleted if necessary.

Furthermore, by RSC service or using PLCnext Engineer the start behavior after a system watchdog can be configured (PLC remains in PlcState::Stop or performs a cold start). The above mentioned refactoring also changed the location where this configuration is stored. Consequently after updating to firmware 2025.0 or newer this configuration is reset to the default setting (PLC remains in PlcState::Stop). Similarly, if this setting is performed with firmware version 2025.0 or newer, it will be lost during a firmware downgrade.

PLC

– The PLC state is available as system variable "PLC_STATE" (global variable in PLCnext Engineer). This variable is updated by the "GdsGlobals" task.

– The PLC state has been extended by the flag "SystemError". This flag is set when an error is detected during the setup phase of the firmware. Often these are configuration errors and should be fixed before rebooting the PLC. A "SystemError" will also occur if a shared object (*.so) is configured for loading in an ACF project that is compiled for an older version of the firmware (≤ 2024.6).

RSC

– The RSC service "IDeviceControl::StartFirmwareUpdate()" has been refactored in order to use the update mechanism of the Software Update component including the "PreparedForUpdate" state. In this con-text the RSC service expects the firmware RAUC container in the folder /opt/plcnext/custom (previously /opt/plcnext).

WBM

– The integrated NTP server has been changed from "ntpd" to "chronyd". Configured NTP servers are not converted during firmware up- or downgrade. Therefore check the NTP configuration and correct it if necessary after a firmware up- or downgrade. Furthermore firmware ≤ 2024.6 was able to store a comment per each configured NTP server, which is no longer supported with firmware 2025.0.

Notes:

– "ntpd" is configured at /etc/ntp.conf. If necessary check here for the NTP server's IP addresses when updating the NTP configuration via WBM or PLCnext Engineer.

– With firmware 2025.0 the PLC may take several minutes to store date and time, for example if it is set via PLCnext Engineer. Do not power off the PLC during this period.

– With firmware 2025.0 the WBM has been refactored. In this context the former WBM page "Cockpit" was split into the pages "Overview" and "Device Maintenance". "Overview" is displayed as default page after login and contains all displays while "Device Maintenance" contains all operational buttons. The "Welcome page" has been removed in the context of this refactoring.

– The diagnosis of the Axioline local bus was improved. In particular with many Axioline modules and/or modules which need longer time to respond to the PDI requests of the PLC, some diagnostic information was not displayed in the past.

3.3   Error corrections

ANSI C LIB

The ANSI C function "getBufferPtrByPortname()" created unnecessary copies of the buffer. As a consequence buffers returned by a previous call to this function (to get the buffer of a different port) were not updated on the fieldbus.

Configurable alarms

When a "ConfirmAlarm" or "AcknowledgeAlarm" was processed and Authentication was used by the project, the alarm server was not setting the user field to the user name of the currently logged in user if the call succeeds.

DataLogger

The "IDataLoggerService2" "ReadVariablesData" method returned unexpected results like records for the NULL entries in the database, but these only contained the "consistency" flag and the record type and no value.

EHMI

An exception of the eHMI occurred when too long strings for "user" or "password" were used for authentication.

GDS

Sporadic flickering could occur at fieldbus outputs when global variables were forced.

HMI

When a configurable alarm (configured in PLCnext Engineer) was confirmed or acknowledged, this state could be seen in the HMI. If in this situation the browser has been refreshed (F5) or a new HMI session was started, the information about which user (IP address) confirmed/acknowledged was lost.
This information is now available.

IEC 61131-3

– A non-existent "AR_USER_ID" generated an exception in the PROFINET function block "GET_MODULE_-DIFF_BLOCK" and stopped the PLC project.
– The "IDLE Task" priority was displayed incorrectly as "0" in the "TASK_INFO" structure.
– The function blocks "PACK" and "UNPACK" do not process variables of data type "WSTRING".
– After "Download Changes" ("Write and Start Project Changes" in PLCnext Engineer) the error message "free node at xxx is too small during DC procedure" could occur.
– When loading a retain backup file, the text "Backup file generated" was displayed incorrectly in the notification "Security.Arp.Plc.Retain.BackupFilePrepared".
– In case the PLC is stopped due to an exception (within the code of an ESM task) the retain values are invalidated. As a consequence a cold restart is required. So far the invalidation was performed only in case of an ESM task watchdog (but not in case of other exceptions). Tipp: If you are regularly facing exceptions, consider to use the function save/restore retain values in the cockpit of the WBM or PLCnext Engineer.
– After "Download Changes" ("Write and Start Project Changes" in PLCnext Engineer) it was not possible to safe the retain data with the button from PLCnext Engineer cockpit.
– If the PLC was in "RUN" or "STOP" state and "Reset" was called in this state, the PLC was first stopped and then reset. The entire sequence had no timeout monitoring, which could lead to blocking in unfavorable project situations.
– The data type "IecWString80" was incorrectly not supported in Native Shared Library (C#/C++) projects.

Network

– When new network adapter settings were written by "DCP", two gateway entries were active by mistake.
– If the PROFINET controller or the PROFINET device was deactivated via the system management for the purpose of IP address assignment via DHCP for the corresponding interface, the system crashed when the firmware was restarted.

OPC UA server

– After downloading a new project, a system crash could occur sporadically if the OPC UA configuration was changed from "DNS name" to "IP address".
– During data access via OPC UA and the simultaneous execution of a PLC state transition, an unexpected exception could occur sporadically. The OPC UA server is now synchronized against these PLC state transitions.

OPC UA client

– After a running OPC UA server/client communication is disconnected, it could happen that the exchanged data to the client was not updated according to the PLC project status after the connection was re-established.
– If communication with the OPC UA server failed, for example due to a system crash, the communication of the OPC UA client never restarted correctly, even if the OPC UA server returned to normal status.
– Subscribing a huge amount of variables on the OPC UA server led to a "FATAL - Signal SIGSEGV" error when at the same target 32 clients were also subscribing a huge amount of variables.

– The OPC UA client has logged important information only with activated DEBUG level to the 'Output.log' file.

– The OPC UA client feature relies on changes in the source data to trigger the transfer of data between the client and the server. If the source data did not change for any period of time, there was no guarantee that the data values were synchronized between the client and the server, for example after an interruption in the client-server connection.

– The OPC UA client did not handle its subscriptions correctly when the OPC UA server was shut down (e.g. due to a "Write and start project" command in PLCnext Engineer). Therefore, the firmware was terminated due to a segmentation violation (SIGSEGV) or the configured local variables were no longer updated. Both effects occurred sporadically.

– The OPC UA client did not check whether certain write operations were successful. After a connection loss this sometimes led to longer periods of time in which the values of the variables in the OPC UA client did not match the values in the OPC UA server, even if the connection had been re-established for some time.

Proficloud

When remanent buffering was activated after the connection to the Proficloud was interrupted, the PLC prevented Proficloud from reestablishing the connection. Additionally, if in this situation the WBM page "Proficloud Services" was opened, the WBM got blocked and a new connection to the WBM could not be established. To recover from either of both problems the PLC needed to be restarted.

PROFINET

– After hot-swapping a connected "AXL-P" I/O module, all PROFINET channel alarms were incorrectly cleared.

– The root-cause of LLDP error messages in the log file "Output.log" in combination with several switch types was fixed.

– Sporadically, an "AR Device deactivated" was sent by the PROFINET controller during a PLC project change.

– In the case that a module is configured on a PROFINET device whose submodules are configured in different APIs and alarms were received by the PROFINET controller for one or more of these submodules, the diagnostic processing in the WBM en-

tered an endless loop, which led to the high CPU load by a WBM task. This effect has been observed with PROFINET devices which are connected via VXLAN tunnel to the PROFINET controller.

– PROFINET System Redundancy: When the primary PROFINET controller has already established an AR to the built-in PROFINET device of the PLCnext Control device and now the backup PROFINET controller established its AR, an unnecessary alarm has been sent to the primary controller indicating return of submodule.

RSC

It was not possible to use a string length of greater than 4096 bytes in the data type "RscString<int N>" of RSC services.

Safety

– The following known issue has been fixed:

   If the "Download Changes" mechanism ("Write and Start Project Changes" in PLCnext Engineer) is used along with the SPLC 1000/3000, please take into account a possible malfunction in case the following steps have been performed:

1 A safety-related project is downloaded to the safety-related controller.

2 A non-safety-related project is downloaded to the standard controller.

3 A modified safety-related project is downloaded to the safety-related controller.

4 An attempt is made to change the non-safety-related project using "Download Changes" ("Write and Start Project Changes" in PLCnext Engineer), which is rejected by the PLCnext firmware of the standard controller (for example, by changing the task configuration).

5 The device is restarted. (for example, voltage failure and recovery or request for restart in PLCnext Engineer)

Attention: After the restart, the safety-related controller executes the original safety-related project from step 1. In order to prevent the described behavior, please additionally carry out the following measures after every change of the safety project:

   – Perform a restart in the PLCnext Engineer software in the "Cockpit" editor of the standard controller or switch off the supply voltage of the device for at least 30 s and then switch it on again (power reset).

– Compare the CRC checksum of the safety-related project using the system variables of the safety-related controller or in the "Cockpit Safe PLC" in the PLCnext Engineer software with the original CRC checksum before the restart.

SDK

With the SDK version 2021.6 the language standard C++ 17 has been set in the compiler options (-std=c++17). The firmware itself is also compiled with this option set. Besides some general C++ issues related to this C++17 standard, the following issue is related to PLCnext Technology: C++ 17 introduced the data type std::byte which was unfortunately not compatible with Arp::byte. Therefore, if the namespaces std and Arp were both active in the compilation process, this resulted in an error.
This known issue has been fixed, Arp::byte is now mapped to std:.byte.

SD card

The log message from the ExternalSDCardComponent in the log file in "Output.log" was ambiguous: It was unclear whether the message "de-activation state: activated" meant that the state was "deactivated" or "activated".

SPNS

Reading "I&M0" data failed.

System

– A system watchdog could occur sporadically. A possible cause of these watchdogs could be found in the connector to the PLCnext Store, especially when the PLC was not connected to the store. The system watchdog was preceded by a SIGSEGV.

– In connection with the initialization of the "SFP" interface, there were sporadic startup problems during the booting process.

– A software update could not be performed if the PLC was in state "FatalError".

– If a user component caused a crash before the system watchdog was activated, the firmware terminated and the controller was available only via SSH.
Note: The system watchdog was activated just before the "IControllerComponent::Start()" method was invoked. This known issue has been fixed.

TLS 2 FB

– An exception occurred in the function block in case the Ethernet connection was interrupted.

– The error code "0xC212" occurred unexpectedly on the function block "TLS_SOCKET_2", although data could be exchanged.

– A high CPU load that was associated to the use of the "TLS_2" function blocks has been detected in the previous firmware version.

– The TLS_*_2 FB could not detect some passive socket closed when "a cable got pulled". The TLS_*_2 FB continued to show an active connection for quite some time, way beyond the PLC's KeepAlive settings. In combination with PLCnext Engineer version 2024.0.4 LTS or newer this issue has been solved. Note: This issue was erroneously reported as fixed with firmware 2024.0.6 LTS. Now it has definitely been fixed.

WBM

– It was impossible to select a "Identity Store for HTTPS certificate" if a bad certificate was installed beforehand.

– The texts and icons for the diagnostic pages in the WBM for PROFINET and local bus were previously different and have now been harmonized.

– The role "UserManager" did not have the permission for the LDAP configuration in the WBM as described in the documentation.

3.4 Known limitations and errors

The known limitations and errors can be found in the PLCnext Info Center at:
https://www.plcnext.help/te/Known_issues.htm
Here you will find a constantly updated overview of all known issues.

3.5 Security updates

The following security updates have been made in this release. For more information about the specified CVE numbers, see:

– https://nvd.nist.gov/vuln

– https://cert.vde.com

Information on the Phoenix Contact "PSIRT" can be found at: https://www.phoenixcontact.com/psirt

PLCnext Technology App

– The start script "initScriptTemplate" of PLCnext Technology Apps could be executed by the local user "root". If an attacker succeeded in installing a malicious app or have it installed, he was able to fully compromise the system.

– The "post_updatescript" within the "updateconfigs" part was executed with "root" privileges. This allowed a PLCnext Technology App to extend its privileges.

Bind

– CVE-2024-12705

Crun

– CVE-2025-24965

Curl

– CVE-2025-0665
– CVE-2025-0167
– CVE-2024-11053
– CVE-2024-9681

Coreutils

– CVE-2024-0684

Git

– CVE-2024-32002

Glib

– CVE-2024-52533

Kernel

– CVE-2020-16120

Libpcap

– CVE-2023-7256
– CVE-2024-8006

Libexpat

– CVE-2024-8176
– CVE-2024-50602

Libmodbus

– CVE-2024-10918

Libssh2

– CVE-2023-48795

Libtasn1

– CVE-2024-12133

Libxml2

– CVE-2025-27113
– CVE-2024-25062

Nano

– CVE-2024-5742

Openssh

– CVE-2025-26466
– CVE-2025-26465
– CVE-2024-6387
– CVE-2024-39894

Openssl

– CVE-2024-6119
– CVE-2024-9143
– CVE-2024-5535
– CVE-2023-5678
– CVE-2024-0727
– CVE-2024-2511
– CVE-2024-4741
– CVE-2024-4603

OpenVPN

– CVE-2024-28882
– CVE-2024-5594

Patch

– CVE-2019-20633
– CVE-2019-13638
– CVE-2019-13636
– CVE-2018-1000156
– CVE-2018-20969
– CVE-2018-6951
– CVE-2018-6952

Podman

– CVE-2024-9341

Python

– CVE-2023-27043
– CVE-2024-9287
– CVE-2024-6232
– CVE-2024-6345
– CVE-2024-7592

Rsync

– CVE-2024-12084
– CVE-2024-12085
– CVE-2024-12086
– CVE-2024-12087

– CVE-2024-12088
– CVE-2024-12747

SSH

A DoS (Deny of Service) attack using LOIC (Low Orbital Ion Canon) at port 22 resulted in high RAM usage.

System

– In addition to the standard file attributes, ACL (Access Control Lists) are implemented into the file system. ACL enable a more specific set of permissions to a file or directory.
– The user "plcnext_firmware" or "admin" could create ACF settings files in an unintended location that was evaluated during startup.
– An attacker who has local access to the system with the unprivileged user "plcnext_firmware" could gain root privileges by manipulating the network configuration.
– With the call "sudo date -f file_name" it was possible to read any file without permission.
– An attacker who has local access to the system with the unprivileged user "admin" or "plcnext_firmware" could manipulate any software libraries on the system. This allowed them to gain "root" privileges.
– An attacker who has local access to the system with the unprivileged user "admin" was able to replace the "CNI" plugins for the "Podman" container environment with malicious scripts. In this way, he was able to gain "root" privileges.
– Some "bash" scripts that are allowed to be executed by users of the "plcnext" group or the "plcnext_firmware" user were vulnerable to the injection of unsafe environment variables.
– The "admin" user was able to edit files in the "/etc/plcnext/" folder using the "sed -i" command.
– All users had "read/write" access in "/dev/shm". Shared memory should usually be only read/writeable by the group or user that created the memory. This was corrected.
– When the "Security Profile" was activated, the "Notification Manager" incorrectly displayed PROFINET entries, although PROFINET was deactivated.
– NN-2024-123 - The following vulnerability has been fixed: A "root" privileged "watchdog daemon" configuration file could be manipulated to restart the device. Due to a change in the system design, now this possibility of manipulation is no longer possible.

– NN-2024-124 - The following vulnerability has been fixed: The "watchdog daemon" executed an unsafe "chmod" command abusing symbolic links leading to a local privilege escalation. Due to a change in the system design, now this possibility of manipulation is no longer possible.
– NN-2024-145 - The following vulnerability has been fixed: The startup script arp-preinit running on the Linux operating system executes an unsafe chmod command with root privileges over multiple files that can be controlled by a low privileged user member of the plcnext Linux group. By abusing symbolic links, an attacker may force the startup process to set read/write permissions on arbitrary files inside the file system, potentially leading to a local privilege escalation on the system.
– NN-2024-146 - The following vulnerability has been fixed: The service security-profile running on the Linux operating system executes an unsafe chmod command with root privileges over multiple files that can be controlled by a low privileged user member of the plcnext Linux group. By abusing symbolic links, an attacker may force the startup process to set read/writes permissions on arbitrary files inside the file system, potentially leading to a local privilege escalation on the system.

Unzip

– CVE-2022-0530
– CVE-2022-0529
– CVE-2021-4217
– CVE-2018-1000035
– CVE-2018-18384
– CVE-2016-9844
– CVE-2019-13232
– CVE-2015-7696
– CVE-2015-7697

WBM

– Certain "cipher suites" that are no longer considered secure have been deactivated.
– In the "Cockpit" view, the connection was lost if it was also opened in another browser tab.
– It was possible to open an "Alert" window via script using the name of a "TrustStore".
– The "nginx" logging could under certain circumstances lead to flooding of the log files "auth.log", "syslog", "error" and "nginx/error.log".

– The cache-control and pragma HTTP header had not been set properly or are missing allowing the browser and proxies to cache content.

Wget

– CVE-2024-38428
– CVE-2024-10524

4 Changes in firmware version 2024.0.9 LTS

This section describes changes made between firmware version 2024.0.6 LTS and firmware version 2024.0.9 LTS. All parts of the previously released version are included in the current version.

> **ℹ** To be able to use all new functions of the firmware, you need PLCnext Engineer version 2024.0 LTS or newer.
> Select the latest template for firmware version 2024.0 LTS in the PLCnext Engineer project.

> **ℹ** In order to update to firmware version 2023.0.0 LTS or newer at least a firmware version 2022.0 LTS or newer must be installed on the PLC. Older firmware versions will not accept the *.rauc firmware update file.

> **ℹ** The following safety-related firmware versions must be used.
> Please contact the Competence Center Services as to the details on safety firmware update procedure:
> Phone: +49 5281 946 2777
> E-mail: safety-service@phoenixcontact.com
>
> 02.10.0006 ✔

> **ℹ** Attention! - If you updated the firmware from any previos firmware-version,
> you can no longer downgrade/upgrade to the origin firmware-version.
> The next available update from FW 2024.0.9 is FW 2025.0.2 and newer

4.1 Error corrections

ANSI C

The ANSI C function "getBufferPtrByPortname()" created unnecessary copies of the buffer. As a consequence buffers returned by a previous call to this function (to get the buffer of a different port) were not updated to the fieldbus. This bug has been fixed.

DataLogger

The "IDataLoggerService2" "ReadVariablesData" method returned unexpected results like records for the NULL entries in the database, but these only contained the "consistency" flag and the record type and no value.

RSC

It was not possible to use a string length of greater than 4096 bytes in the data type "RscString<int N>" of RSC services.

Safety

The following known issue has been fixed:

If the "Download Changes" mechanism ("Write and Start Project Changes" in PLCnext Engineer) is used along with the SPLC 1000/3000, please take into account a possible malfunction in case the following steps have been performed:

1. A safety-related project is downloaded to the safety-related controller.
2. A non-safety-related project is downloaded to the standard controller.
3. A modified safety-related project is downloaded to the safety-related controller.
4. An attempt is made to change the non-safety-related project using "Download Changes" ("Write and Start Project Changes" in PLCnext Engineer), which is rejected by the PLCnext firmware of the standard controller (for example, by changing the task configuration).
5. The device is restarted. (for example, voltage failure and recovery or request for restart in PLCnext Engineer)

Attention: After the restart, the safety-related controller executes the original safety-related project from step 1. In order to prevent the described behavior, please additionally carry out the following measures after every change of the safety project:

– Perform a restart in the PLCnext Engineer software in the "Cockpit" editor of the standard controller or switch off the supply voltage of the device for at least 30 s and then switch it on again (power reset).
– Compare the CRC checksum of the safety-related project using the system variables of the safety-related controller or in the "Cockpit Safe PLC" in the PLCnext Engineer software with the original CRC checksum before the restart.

System watchdog

Sporadically a system watchdog could occur. A possible cause of these watchdogs could be found in the connector to the PLCnext Store, especially when the PLC was not connected to the store. The system watchdog was preceded by a SIGSEGV.

TLS FB

– A high CPU load that was associated to the use of the "TLS_2" function blocks has been detected in the previous firmware version.

– The TLS_*_2 FB could not detect some passive socket closed when "a cable got pulled". The TLS_*_2 FB continued to show an active connection for quite some time, way beyond the PLC's KeepAlive settings. In combination with PLCnext Engineer version 2024.0.4 LTS or newer this issue has been solved. Note: This issue was erroneously reported as fixed with firmware 2024.0.6 LTS. Now it has definitely been fixed.

WBM

The role "UserManager" did not have the permission for the LDAP configuration in the WBM as described in the documentation.

4.2 Known limitations and errors

ℹ The known limitations and errors can be found in the PLCnext Info Center at: https://www.plcnext.help/te/Known_issues.htm Here you will find a constantly updated overview of all known issues.

4.3 Security updates

The following security updates have been made in this release. For more information about the specified CVE numbers, see:

– https://nvd.nist.gov/vuln
– https://cert.vde.com

Information on the Phoenix Contact "PSIRT" can be found at: https://www.phoenixcontact.com/psirt

Bash

PxC PSIRT Report: Some bash scripts that are allowed to be executed by users in the "plcnext" group or the "plcnext_firmware" user were vulnerable to unsafe environment variable injection.

Security profile

– Correction of parameter "AllowTcpForwarding" of ssh configuration in security profile from "yes" to "no".
– The sshd_config for the security profile missed the include mechanism from default configuration.

Curl

– CVE-2024-9681
– CVE-2024-11053
– CVE-2025-0167

FastCGI

– CVE-2025-23016

Glib

– CVE-2024-52533

Libxml2

– CVE-2025-27113

Libexpat

– CVE-2024-50602

Nano

– CVE-2024-5742

Openssh

– CVE-2025-26465
– CVE-2025-26466

Openssl

– CVE-2024-9143
– CVE-2024-5535
– CVE-2024-6119

Openvpn

– CVE-2024-5594

Python

– CVE-2024-6232
– CVE-2024-7592

SSH

A DoS (Deny of Service) attack using LOIC (Low Orbital Ion Canon) at port 22 resulted in high RAM usage.

Vim

– CVE-2024-41957
– CVE-2024-41965

5 Changes in firmware version 2023.6.4

i Attention! - Due to a hardware change in hardware-revision HW:04 a device with FW 2023.6.4 can not be downgraded/upgraded to any previsios firmware-version.
The next available update for a device with FW 2023.6.4 installed is:
FW 2024.0.9
FW 2025.x and newer.

i Attention! - If you updated the firmware from any previos firmware-version (2024.0.4 or 2023.x.x) to FW 2023.6.4, you can no longer downgrade/upgrade t
o the origin firmware-version
The next available update for a device with FW 2023.6.4 installed is:
FW 2024.0.9
FW 2025.x and newer.

i To be able to use all new functions of the firmware, you need PLCnext Engineer version 2025.0 LTS or newer.
Select the latest template for firmware version 2023.6 in the PLCnext Engineer project.

i The safety-related firmware version 02.10.0006 must be used.
Please contact the Competence Center Services as to the details on safety firmware update procedure:
Phone: +49 5281 946 2777
E-mail: safety-service@phoenixcontact.com

i In order to update to firmware version 2023.6.4 or newer at least a firmware version 2022.0 LTS or newer must be installed on the PLC. Older firmware versions will not accept the *.rauc firmware update file.

This section describes changes made between firmware version 2023.6.0 and firmware version 2023.6.4.
All parts of the previously released version are included in the current version.

5.1 Error corrections

– Due to a hardware change in hardware-revision HW:04, FW 2023.6.4 does support the changed hardware.
– Loading large safety projects resulted in error "ERR_HNF_PT_READ_TEMPERATURE_NOT_ POSSIBLE (0x924C)". This bug has been fixed.
- In case of synchronization error in combination with the SPLC hardware, synchronization timers could sporadically be created. This bug has been fixed.

C++ API

– The class "TlsSocket2" now reloads the Trust Store (including Certificate Revocation List) before a new handshake (renegotiation). This is required for the IEC 62351-3 certification.
– Developers that used the external/customer SDK version 2023.x LTS were unable to use the "PImpl pattern" due to the missing file "Arp/System/Core/PimplPtr.inl".

5.2 Known limitations and errors

The known limitations and errors can be found in the PLCnext Info Center at:
https://www.plcnext.help/te/Known_issues.htm
Here you will find a constantly updated overview of all known issues.

5.3 Security updates

i BusyBox will be disabled in a future firmware release and replaced by other packages if necessary.

The following security updates have been made in this release. For more information about the specified CVE numbers, see:
– https://nvd.nist.gov/vuln
– https://cert.vde.com

Information on the Phoenix Contact "PSIRT" can be found at: https://www.phoenixcontact.com/psirt

OpenSSH

– CVE-2024-6387

6 Changes in firmware version 2024.0.6 LTS

ℹ️ To be able to use all new functions of the firmware, you need PLCnext Engineer version 2024.0 LTS or newer.
Select the latest template for firmware version 2024.0 LTS in the PLCnext Engineer project.

ℹ️ The safety-related firmware version 02.10.0006 must be used.
Please contact the Competence Center Services as to the details on safety firmware update procedure:
Phone: +49 5281 946 2777
E-mail: safety-service@phoenixcontact.com

ℹ️ In order to update to firmware version 2023.0.0 LTS or newer at least a firmware version 2022.0 LTS or newer must be installed on the PLC. Older firmware versions will not accept the *.rauc firmware update file.

This section describes changes made between firmware version 2024.0.5 LTS and firmware version 2024.0.6 LTS.

All parts of the previously released version are included in the current version.

6.1 New functions

SDK

The (previously internal) class "Arp::System::Commons::Threading::ConditionVariable" has been made available in the SDK. This class can be used to synchronize between multiple threads. The class "std::condition_variable" should not be used for synchronization.

6.2 Error corrections

OPC UA client

When the OPC UA client configuration is loaded and "ns=0" is specified in the identifier of <LocalVariable> element or in the <NodeId> element of the <RemoteVariableDescriptor>, a SIGSEGV (segmentation fault) could occur which led to a system watchdog.

If the OPC UA client was connected to another OPC UA server and this server was restarted, the OPC UA client did no longer update its monitored items.

OPC UA server

– Very sporadically a SIGSEGV (segmentation fault) could occur which led to a system watchdog. The SIGSEGV could occur when a a new PLC project was downloaded while a connected OPC UA client performed a longer operation, e.g. writing a large array.
– With a large number of OPC UA variables, sporadically an unexpected segmentation fault could occur after some time of apparently normal operation.

PROFINET

In the case that a module is configured on a PROFINET device whose submodules are configured in different APIs and alarms were received by the PROFINET controller for one or more of these submodules, the diagnostic processing in the WBM entered an endless loop, which led to the high CPU load by a WBM task. This effect has been observed with PROFINET devices which are connected via VXLAN tunnel to the PROFINET controller.

TLS2 FB

– After adding an instance of the function block TLS_SOCKET_2 to the project via Download Changes ("Write and Start Project Changes" in PLCnext Engineer) the PLC stops with a "Arp::System::Commons::Plc::NullReferenceException". This problem occurs with PLCnext Engineer version 2024.0.3 LTS. In combination with PLCnext Engineer version 2024.0.4 LTS or newer this issue has been solved.
– The TLS_*_2 FB could not detect some passive socket closed when "a cable got pulled". The TLS_*_2 FB continued to show an active connection for quite some time, way beyond what the KeepAlive settings on the PLC. In combination with PLCnext Engineer version 2024.0.4 LTS or newer this issue has been solved.
– There has been a notable increase in CPU load when TLS_*_2 FB instances with PLCnext Engineer version 2024.0.3 LTS are active. In combination with PLCnext Engineer version 2024.0.4 LTS or newer this issue has been solved.
– The error code "0xC204" ("The datagram is too long") could sporadically occur on the TLS_SEND_2 function block, although there was no length overrun in the application. In combination with PLCnext Engineer version 2024.0.4 LTS or newer this issue has been solved.

ANSI C

Writing process data to a fieldbus via the "ANSI C" API did not work. This known issue has been fixed.

HMI

When retrieving variable values via the POST method of the REST API a memory leak may occur. To avoid this problem register and read the variables as a group or use the GET method of the REST API instead.
This known issue has been fixed.

6.3 Known limitations and errors

The known limitations and errors can be found in the PLCnext Info Center at:
https://www.plcnext.help/te/Known_issues.htm
Here you will find a constantly updated overview of all known issues.

6.4 Security updates

BusyBox will be disabled in a future firmware release and replaced by other packages if necessary.

The following security updates have been made in this release. For more information about the specified CVE numbers, see:

– https://nvd.nist.gov/vuln
– https://cert.vde.com

Information on the Phoenix Contact "PSIRT" can be found at: https://www.phoenixcontact.com/psirt

Git

– CVE-2024-32002

OpenSSH

– CVE-2024-6387
– CVE-2024-39894

OpenSSL

– CVE-2024-4603
– CVE-2024-2511
– CVE-2024-4741

7 Changes in firmware version 2024.0.3 LTS

ℹ️ To be able to use all new functions of the firmware, you need PLCnext Engineer version 2024.0 LTS or newer.
Select the latest template for firmware version 2024.0 LTS in the PLCnext Engineer project.

ℹ️ The safety-related firmware version 02.10.0006 must be used.
Please contact the Competence Center Services as to the details on safety firmware update procedure:
Phone: +49 5281 946 2777
E-mail: safety-service@phoenixcontact.com

ℹ️ In order to update to firmware version 2023.0.3 LTS or newer at least a firmware version 2022.0 LTS or newer must be installed on the PLC. Older firmware versions will not accept the *.rauc firmware update file.

This section describes changes made between firmware version 2023.6.0 and firmware version 2024.0.2 LTS.

7.1 New functions

DataLogger

The recording of variables in the context of an IDLE task has been improved. Instead of recording each task cycle the recording time stamp is used to approximate to the sample rate.

GDS

Concurrent data exchange from different CPU cores has been optimized. In particular 2 or more ESM tasks assigned to different ESM (CPU core) and exchanging data with the same I/O buffer could block each other. In worst case scenarios an ESM task watchdog could occur. The performance optimization of the I/O buffer minimizes the risk of an ESM task watchdog.

IEC 61131

Download Changes ("Write and Start Project Changes" in PLCnext Engineer) while variables are forced, is now supported. In combination with firmware 2024.0 LTS (or newer) PLCnext Engineer 2024.0 LTS (or newer) does no longer reset the force state implicitly before downloading changes. Now the forcing state is kept if variables, which are currently forced, do still exist as forcible variables in the changed project. Otherwise the firmware rejects the Download Changes command and emits a notification. In this case the user can check the list of forced variables

in PLCnext Engineer and unforce variables that prevent downloading changes.

Licenses

The PLCnext firmware is capable of using licenses, which are managed by a license server in the network. Currently this feature can only be used with the PLCnext Simulation products because only the license "PLCnext ENG SIM" can be hosted on a license server (PC). For other PLCnext controllers this capability is only a preparation for future features. The access to the license server can be configured via WBM. Currently if a license server is configured, no licenses can be accessed which are stored at the device or LIC SD card.

Proficloud

The Proficloud can be configured to send the values of the marked variables to an MQTT server instead of the Proficloud. This MQTT server can be in a local network or in the cloud. The MQTT server to be used, can be configured in the WBM.

Security

A LIC SD card can be encrypted to avoid unauthorized access. Encryption can be started via WBM page "Security - SD Card".

System

– If a system watchdog (SWD) occurs due to a fatal error that has caused a PLCnext process to die, the following files are saved before the system is rebooted:
  – reason.log
  – kernel.log
  – sys.log
  If an LTTNG session is active, its trace is saved, too. These files are saved to the folder */opt/plcnext/watchdogDaemon/[timestamp]* where *[timestamp]* is created from the time at which the SWD occurred. If more than 3 SWD occur, the oldest folder will be removed. If the PLC is rebooted due to the hardware watchdog reset, it is not possible to save these files. This can happen if the hardware watchdog is no longer triggered by the firmware, for example due to a heavy, high-priority load on the system.
– In combination with firmware 2024.0 LTS (or newer), PLCnext Engineer (2024.0.1 LTS or newer) supports configurable alarms.
– Changes of PLC states are serialized and dedicated state transitions can be monitored with a timeout. This prevents from scenarios in which a low-priority task requests to change the PLC state (which can also occur implicitly, for example by calling the

"RestartDevice()" method of "IDeviceControlService") while the PLC Manager is performing another state transition (for example from "PlcState::Running to PlcState::Stop").

7.2   Changes

Linux

–   The OpenSSL library has been updated to version 3.0. The PLCnext firmware uses this version only. For compatibility reasons the previous OpenSSL library (version 1.1.1) still exists in the file system. As this version is outdated, it will be removed in one of the next firmware releases. For applications (including PLCnext Apps) which use the OpenSSL library, an update is recommended as soon as an application version is available, which uses OpenSSL 3.0.

–   LTTng has been updated to version 2.13.9 and there has been a significant change in the "lttng-ust" (LTTng user space tracing). If an application/library is instrumented with LTTng user space tracing and has been compiled without using the "ArpTracing.cmake" support of the LTTng user space tracing in PLCnext SDK (available since FW 2022.6), the instrumented application/library cannot be loaded any longer by the firmware ("undefined symbol" is reported in Output.log). In that case the instrumentation of LTTng user space tracepoint in the application/library has to be changed to use the "ArpTracing.cmake" support of the PLCnext SDK and it needs to be recompiled. Matlab Simulink applications, which use the "PLCN_EnableLTTNG" compile option, have to be compiled with PLCnext Target for Simulink v2.3 or newer.

–   Library "paho-mqtt-c" has been updated to version 1.3.13.

OPC UA

–   The OPC UA client and server use the OpenSSL library to validate X.509 certificates using the OpenSSL flag X509_V_FLAG_X509_STRICT. As firmware 2024.0 LTS is updated to OpenSSL 3.0, the X.509 certificate validation became more strict, especially for non self-signed certificates. This may cause the server to return the error "BadSecurityChecksFailed" on client connection attempts. Make sure that, according to OPC UA Part 6, client issuer as well as client application X.509 certificates are conform to RFC 5280, especially to the sections listed below. This applies to self-signed certificates as well as user-managed certificates.

  –   4.1.1.2 signatureAlgorithm
  –   4.1.2.6 Subject

  –   4.2.1.1 Authority Key Identifier
  –   4.2.1.2 Subject Key Identifier
  –   4.2.1.3 Key Usage
  –   4.2.1.6 Subject Alternative Name
  –   4.2.1.9 Basic Constraints

–   In the NamespaceArray of the OPC UA server the index of namespace http://phoenixcontact.com/Opc-Ua/PubSubConfiguration has changed from index 8 to index 2. This namespace is optional and it appears only if the feature "OPC UA PubSub" is activated on the WBM page "System Services". Currently the firmware does not provide anything in that namespace, it is only a preparation for future extensions.

7.3   Error corrections

ESM

–   If two ESM tasks cause a task watchdog at (nearly) the same time, the event task "Arp.Plc.Esm.OnException" was executed twice. Additionally, the PLC was attempted to be stopped twice in parallel. This failed and the PLC had to be rebooted. This error has been corrected and the event task as well as the PLC stop is now executed only once.

–   In some situations calling the function block "GET_-EXCEPTION_INFOS" in the event task "Arp.Plc.Esm.OnException" caused an exception. This has been fixed. In addition to update to firmware 2024.0 LTS or newer, the PLC project has also to be re-compiled using PLCnext Engineer 2024.0.1 LTS or newer.

EtherNet/IP

Sporadically the activated "EtherNet/IP" component could block a PLC state change after project download.

GDS

–   It was possible to force a variable with a value of an inappropriate data type.

–   In case of a deactivated "Ethernet/IP" component in the PLCnext Engineer project, an error occurred after an update to firmware 2023.6.

IEC 61131

–   When breakpoints are set in the IEC 61131-3 program, the "PlcState::Debugging" flag was reset in the transition from "PLC STOP" to "PLC HOT START" and then set again when changing from "PLC Running" to "Debugging". The fieldbus output values could be switched on again for a short time period when the PLC was in the state "Running".

– "Download Changes" ("Write and Start Project Changes" in PLCnext Engineer) implicitly creates a backup of the current project. If "Download Changes" is not possible (for any reason), the current project is restored from this backup. If "Download All" ("Write and Start Project" in PLCnext Engineer) is performed immediately after a rejected or failed "Download Changes" attempt, the PLC is reset. Resetting conflicted with restoring and ended in an I/O exception. The firmware now keeps the state flag "Running | DcgNotPossible" until the restoring process has been finished. Depending on the project size, the restoring process may take several seconds. Note that PLCnext Engineer 2023.9 (or newer) checks this state before it offers the "Download All" option.

– In case of large projects and an extensive use of certain firmware function blocks, an exception could occur after a "Download Changes" attempt ("Write and Start Project Changes" in PLCnext Engineer). The following is reported in the Output.log: "SetupPlc(changing) with out of memory error - GC heap of the application domain". The firmware function blocks have been updated in PLCnext Engineer version 2023.0.6 LTS and in 2024.0 LTS (or newer).

– An exception after "Download Changes" ("Write and Start Project Changes" in PLCnext Engineer) has been triggered if the function block "AR_STATISTIC_ITERATE" was enabled and generated new values. To fix this bug, re-compile and download the project using PLCnext Engineer 2024.0 LTS (or newer).

– In the function "MOVE" that is used with the function "EN/ENO", a value of a multi-element-variable was assigned to a wrong address. To fix this bug, re-compile and download the project using PLCnext Engineer 2024.0 LTS (or newer).

– In a C# eCLR Library the runtime created a vectored exception when calling "File.Exists(null)".

OPC UA client

The GDS client could not access PLC variables (attribute "LocalVariable" in XML element "eUAClientNodeMapping") if "Visibility of variables" is set to "None" in the OPC UA configuration of PLCnext Engineer.

OPC UA server

– A fatal exception could occur if "IndexRange" is used when accessing a variable that is not of type array or of type string.

– After the OPC UA server started with a changed project the server might return "BadNodeIdUnknown" when a client tried to continue monitoring an existing subscription item.

– Subscriptions did not work after a warm or cold start with project changes.

– A sporadic fatal exception could occur in case of OPC UA session creation and login.

– If several elements of a string array are subscribed using "IndexRange", a fatal error occurred and the PLC stopped.

PROFINET

– If a "write record" could not be processed immediately by the PROFINET stack, it was buffered. When a new transmission attempt was made, it was then incorrectly sent as a "read record" packet.

– The RSC service "IAcyclicCommunicationService::RecordWrite()" has a timeout in which the PROFINET device has to respond. In some cases this timeout was too short and has been increased to 15 s. The IEC function block "WRREC" internally uses this service, too.

– A PROFINET device with a device access point (DAP) starting at "Slot 1" could not be accessed via the "AR_MGT" function block.

– An inconsistent "SF-LED" state could occur at the PROFINET controller, if in case of an activated network port monitoring of a connected PROFINET switch the controller was plugged to another port during runtime and then plugged back to the original port.

– The PROFINET controller sent a "Write Request" with wrong lengths calculated in the "NDR header" when establishing the connection. This led to a "Write Response" error for PROFINET stations with very large parameter records (for example "PN/PB Gateway").

– After PROFINET alarms of a certain severity occurred, these were not reset again for going alarms and remained in the diagnostic memory. As a result they were displayed incorrectly in the WBM and it could also happen that the "SF-LED" remained active.

Proficloud

– A fatal exception occurred if the Proficloud component with "Remanent Buffering" was enabled and the DataLogger component was manually disabled on the WBM page "System Services".

– If a Proficloud TSD connection was lost, the logging was flooded with an unnecessary number of messages.

– If a Proficloud connection was disconnected, the connection could not be deactivated in the WBM.

– When a physical connection to the Proficloud was interrupted for several hours and re-established afterwards, the component could not reconnect automatically to the Proficloud.

SPLC

In case of a synchronization error in combination with the SPLC hardware, numerous synchronization timers could sporadically be created. This could result in a PLC task watchdog.

System

– After starting the PLCnext Engineer logic analysis, which contained an element of an array of struct, a system watchdog could occur sporadically.

– A system watchdog with reboot could occur while reading software information of a PLCnext Engineer project. This issue could occur if the manifest file in the PCWE directory is deleted after the "File::Exists" call but before the file is accessed by other operations. This could be the case during a "Download Changes" process ("Write and Start Project Changes" in PLCnext Engineer).

– Sometimes an OPC UA client did not receive the last "UpdateStatus" message after a successful installation of a firmware update. The last message informs about the reboot of the device (100 %) but the client only saw the "copy rootfs" message (90 %).

– If the controller was in the standard PLC status "ready/blocked" after a system watchdog, a "FATAL - Exception" was triggered if the "General Data (SPLC)" page of the SPLC was opened in the WBM.

WBM

– The "User Partition" value that was displayed on the WBM page "Cockpit" did not match the value of the global IEC 61131 system variable "USER_PARTITION.MEM_USAGE".

– The memory partition was displayed in the WBM in "MiB" but shown with the unit "MB". Now it is calculated as MB.

7.4 Known limitations and errors

ℹ️ The known limitations and errors can be found in the PLCnext Info Center at:
https://www.plcnext.help/te/Known_issues.htm
Here you will find a constantly updated overview of all known issues.

7.5 Security updates

ℹ️ BusyBox will be disabled in a future firmware release and replaced by other packages if necessary.

The following security updates have been made in this release. For more information about the specified CVE numbers, see:

– https://nvd.nist.gov/vuln

– https://cert.vde.com

Information on the Phoenix Contact "PSIRT" can be found at: https://www.phoenixcontact.com/psirt

Curl

– CVE-2023-38039
– CVE-2023-46219
– CVE-2023-46218
– CVE-2023-38545
– CVE-2023-38546

DBus

– CVE-2023-34969
– CVE-2022-42010
– CVE-2022-42011
– CVE-2022-42012

File

– CVE-2022-48554

GDS

Security notifications for write access were not deactivated if a new PLC project was loaded without activation.

GLib

– CVE-2023-29499
– CVE-2023-32636
– CVE-2023-32643
– CVE-2023-32611
– CVE-2023-32665

Glibc

– CVE-2023-5156
– CVE-2023-4911

GnuTLS

– CVE-2024-0553
– CVE-2024-0567

GRPC

- CVE-2023-33953
- CVE-2023-32731
- CVE-2023-32732
- CVE-2023-4785
- CVE-2023-44487

Libcap

- CVE-2023-2603

Libssh

- CVE-2023-6004

NTP

- CVE-2023-26551
- CVE-2023-26552
- CVE-2023-26553
- CVE-2023-26554
- CVE-2023-26555
- Any content could be injected into the NTP configuration file via the WBM configuration of the NTP service if a line break was inserted in the comment field.

NVT

- CVE-2022-29900
- CVE-2022-29901

OPC UA

The manual firmware update procedure via an OPC UA server did not work as documented.

OpenSSH

- CVE-2023-48795
- CVE-2023-51384
- CVE-2023-51385

OpenSSL

- CVE-2023-5363
- CVE-2023-4807
- CVE-2023-3817

Perl

- CVE-2023-47100

Python

- CVE-2022-40897
- CVE-2023-40217

Procps

- CVE-2023-4016

SQLite

- CVE-2023-7104

SqashFS

- CVE-2021-41072

Sudo

- CVE-2023-42465

Tcpdump

With the call "sudo tcpdump" it was possible to read the contents of files without read rights.

UM

The "User Manager" accepted a newly created PLCnext user with the name "plcnext_firmware". The "UID" and the access rights were identical with the internal user "plcnext_firmware".

Vim

- CVE-2023-5441
- CVE-2023-5344
- CVE-2023-5535
- CVE-2023-4781
- CVE-2023-4734
- CVE-2023-4733
- CVE-2023-4736
- CVE-2023-4735
- CVE-2023-4750
- CVE-2023-4738
- CVE-2023-4752
- CVE-2023-4751
- CVE-2023-48231
- CVE-2023-48237
- CVE-2023-48706
- CVE-2023-46246

Zlib

- CVE-2023-45853

8   Changes in firmware version 2023.6.0

ℹ	–	To be able to use all new functions of the firmware, you need PLCnext Engineer version 2023.6 or newer. Select the latest template for firmware version 2023.6 in the PLCnext Engineer project. – The safety-related firmware version 02.00.0010 must be used. Please contact the Competence Center Services as to the details on safety firmware update procedure: Phone: +49 5281 946 2777 E-mail: safety-service@phoenixcontact.com – In order to update to firmware version 2023.0.3 LTS or newer at least a firmware version 2022.0 LTS or newer must be installed on the PLC. Older firmware versions will not accept the *.rauc firmware update file.

This section describes changes made between firmware version 2023.0.4 LTS and firmware version 2023.6.0.

8.1   New functions

C++ API

The new class TlsSocket2 was implemented. As a further development of the class TlsSocket, this new class offers additional methods to support security requirements of IEC 62351-3.

IEC 61131-3

– The IEC 61131-3 non-standard function "GET_MICROSECONDS" is supported. To use this feature PLCnext Engineer 2023.6 (or newer) with a project template for this firmware or newer is required.

– The IEC 61131-3 non-standard function block "NETLOAD_LIMITER_STATISTIC" supports the access to the statistics of the netload limiter. To use this feature PLCnext Engineer 2023.6 (or newer) with a project template for this firmware or newer is required.

– Namespaces in IEC 61131-3 POUs are supported. To use this feature PLCnext Engineer 2023.6 (or newer) with a project template for firmware 2023.6 or newer is required.

Linux

– CURL supports TFTP protocol (TFTP client)

– Podman was updated to version 4.4.3. This includes the update of related packages and requires to shift the network stack to "netavark" and "aadvard-dns."

OPC UA

– Any variable known by the GDS can be read or written by the OPC UA client. In previous firmware versions only variables indicated with the "OPC" flag could be used by the OPC UA client.

– A project update for standard (non-safety) PLCnext Engineer projects is supported according to "DI SU Software Update Base Server Facet" and "DI SU Cached Loading Server Facet". For this purpose the user roles "Admin" and "SoftwareUpdate" now additionally allow the update of projects (besides firmware updates). In PLCnext Engineer 2022.9 (and newer) an export of an updated application can be generated ("Export PLCnext Engineer Software Package"/"Export PLCnext Engineer Software Package (with sources)"). The exported project files can be uploaded to the Device and Update Management App and from there assigned to further devices. Note that an appropriate version (newer than 23.0.1) of the Device and Update Management App is required.

PROFINET

PROFINET diagnostic messages, which are sent in the USI format (User Structure Identifier) are printed in plain text (in English language) as notification and are displayed as well on the PROFINET diagnostics WBM page.
PLCnext Engineer collects the required interpretation rules from the FDCML description of the used PROFINET devices and plain text messages that are related to the device's USI diagnosis. Both information are sent to the PLC as a part of the project. Additionally, an USI diagnosis can be converted to a plain text message via the new RSC service "ITextLookup2". To use this feature PLCnext Engineer 2023.6 or newer with a project template for this firmware version is required. Furthermore the used FDCML files need to contain the necessary USI diagnosis information. Currently the FDCML files delivered with PLCnext Engineer (2023.6) installation do not contain this information.

8.2   Changes

Alarms

Alarm notifications (Arp.Services.Alarms.Log.*) are logged into a separate archive "alarms" (file: /opt/plcnext/projects/Default/Services/NotificationLogger/alarms.config).

ESM

As an alternative to the event task "Arp.Plc.Esm.OnStop" two further event tasks "Arp.Plc.Esm.OnPowerDown" and "Arp.Plc.Esm.OnStop2" are introduced. While "Arp.Plc.Esm.OnStop" is executed during power down as well as when the PLC is stopped, the two new tasks enable to program different behaviors in each case. When "Arp.Plc.Esm.OnStop" is configured, "Arp.Plc.Esm.OnPowerDown" and "Arp.Plc.Esm.OnStop2" cannot be configured. PLCnext Engineer (2023.6 or newer) maps these event tasks using the following names in the task editor:

–   "Arp.Plc.Esm.OnStop" → Stop and power down
–   "Arp.Plc.Esm.OnPowerDown" → Power down
–   "Arp.Plc.Esm.OnStop2" → Stop

Firewall

The firewall rules no. 8 ("SNMP") and no. 9 ("PROFINET Uni-/Multicast Ports") were removed from the default rules because PROFINET could almost not be used at all with an activated firewall using the default firewall rules of PLCnext. The rules could be misinterpreted that a PROFINET communication is possible even if the firewall is activated. At https://security.plcnext.help you can find information on how to configure the firewall to enable PROFINET communication.

IEC 61131-3

When "Download Changes" ("Write and Start Project Changes" in PLCnext Engineer) cannot be executed successfully a notification is emitted. The warning "Arp.Plc.Domain.DownloadChanges.Refused" indicates that "Download Changes" could not be performed (for example not possible in real-time operation) or is not supported due to improper preconditions (for example task configuration has changed). In these cases "Download All" ("Write and Start Project" in PLCnext Engineer) would work. The error "Arp.Plc.Domain.DownloadChanges.Failed" indicates that the project is erroneous. In this case also "Download All" won't work. This change also resolves the known issue "Sporadically a PLCnext Engineer project may reject "Download changes" without giving a reason.".

Notifications

–   The names of some notifications were changed, new notifications were added, and some less helpful notifications were removed. For more details refer to the notification topics at https://www.plcnext.help. Notifications of severity "Internal" are no longer logged by default.
–   If during power on no proper value can be read from the RTC clock (for example due to a long time without power) a notification is emitted.

SDK installer

The names of the SDK installer files were simplified. They consist, separated by "-" (minus), of the article name, "linux-sdk" or "mingw-sdk" and the version name. The file extension was not changed(.sh for Linux and .tar.gz for Windows/mingw). The file names of the firmware container were adapted, too. The file name consists, separated by "-" (minus), of the article name, the version name and version number (incl. build number). The file extension .rauc was not changed.

System

The startup time of the device has been optimized in case the capacitor of the integrated UPS is discharged.

WBM

On the PLCnext Store page, the display of the connection and registration status was improved, including a reconnect button.

6.3   Error corrections

C#

The C# method "System.IO.Path.Combine()" used "\" (backslash) instead of "/" (slash) as delimiter in paths. The code of this method is downloaded via PLCnext Engineer to the PLC. To fix this bug, the template has to be updated in the PLCnext Engineer project (replace controller) to a PLC with firmware 2023.6 (or newer).

GDS

The update of GDS connectors is also performed when the PLC is started (cold, warm, or hot restart). This ensures that initial values or retained values of OUT ports are forwarded to their connected IN ports before the task of the IN port is executed.

IEC 61131-3 and C#

– The handling of the heap memory has been optimized. This includes allocation of heap (new operator as well as implicitly, for example by using string or other reference data types) as well as the Garbage Collector. These optimizations result in less time blocked by mutexes. Blocking by mutexes can prevent high priority tasks from execution and in rare cases caused an ESM task watchdog. These effects occurred in a very stochastic manner.

– The firmware did not handle variables of array data types and the usage of VAR_IN_OUT correctly. When such variables were used in a DataLogger session or in the "Logic Analyzer" of PLCnext Engineer the PLC detected a software watchdog (SWD). The PLC was rebooted and a cold start had to be performed (hereby retentive variables were set to their initial values).

OPC UA

– The OPC UA server did not provide data when subscribing to multiple matrices within a subscription. However, if only one matrix was subscribed, it worked. If a 2D matrix of type string was subscribed, the variable update of a previously subscribed 2D int matrix froze. This condition could only be removed by resubscribing to the 2D int matrix. This bug (known issue) has been fixed.

– If a matrix for monitoring was used, various unexpected results occurred when using "IndexRange" and "String" as data type:
  – When initially reading out the matrix after logging in, a "DataChange" event with several changes was erroneously triggered.
  – If a "DataChange" event was performed after writing, the strings in the matrix were truncated.
  – Sporadically a "Segmentation Fault" occurred when reading out the matrix.
  This bug (known issue) has been fixed.

– In case of a warm start of the PLC, subscriptions from the "clientconfig.xml" had not been loaded and created.

PROFINET

– Projects with a lot of PROFINET I/O points (40,000 or more) could not be downloaded to the PLC.

– PROFINET device: A wrong answer to a PN-Read Request (Slot/Subslot/Index 0/0/0x8029) with too small

RecordDataLength (e.g. 1024) was generated for the Read Response.

Proficloud

Application update via Proficloud: If there was an empty directory inside the ZIP archive of a software package the extraction failed.

RSC services

The execution of the method "IDirectoryService::Create()" with an already existing path did not return the expected "FileSystemError::AlreadyExist" value.

Safety

– In case of a system watchdog of the standard firmware the safety board was not consistently reset.

– When changing the project from a profile with F-Device (23.0) to a profile without F-Device (<23.0) the SPLC runs into a FailSafe state ("invalid f-dest address" was reported). The PLC had to be rebooted.

SDK

The class "SecurityNotificationPayload" was missing in the SDK. The following header files were added.
  – "Arp/System/NmPayload/Security/SecurityNotificationPayload.hpp"
  – "Arp/System/NmPayload/Security/SecurityNotificationInfo.hpp"

System

– The text messages of a loaded safety-relevant project in the notifications and "Output.log" showed incorrect CRC information.

– When rebooting the PLC using the RSC service "IDeviceControlService::RestartDevice()" a system watchdog could occur. As a consequence a "cold start" was performed and the retain values were initialized. The same behavior could occur with the IEC function block "PBCL_SysRestart_1" of the library "PLCnextBase" available at the PLCnext Store. This bug could occur since firmware version 2022.6.

– The "paho" library was updated from version "v1.3.10" to "v1.3.12". This update solves several incompatibilities with the IEC 61131-3 "IIoT_Library_V4.x". In particular, it fixes a "system watchdog" in combination with "MQTT-Client FB" in case of a failed MQTT connection.

WBM

– If many PROFINET devices are used and the button to jump to the tree node is pressed in the "Device List" tab

of the "Diagnostics - PROFINET" page, the "Tree View" tab was opened but often it was not automatically scrolled to the desired device.

– In the "Device List" tab of the "Diagnostics - PROFINET" page the link to the device's web page was only shown if the connection to the device could be established during project load. Now the PROFINET device is regularly checked if it offers a web page.

– In some cases the "Diagnostics - PROFINET" page of the WBM displayed a wrong IP address (e.g. "10.10.10.1") for the PROFINET controller.

– The display of the used and free memory of the user partition was optimized at the "Cockpit" page of the WBM.

– At the "Password Policy" tab of the WBM page "User Authentication" the description of the "password reuse" settings could possibly be misinterpreted and has therefore been corrected.

8.4   Known limitations and errors

The known limitations and errors can be found in the PLCnext Info Center at:

https://www.plcnext.help/te/Known_issues.htm

Here you will find a constantly updated overview of all known issues.

– In rare cases, the BPC 9102S may not boot after a restart via the WBM, the PLCnext Engineer, a console comand or after a firmware update.
If the SD card cannot be read after a restart of the PLC, a manual restart must be done via the power supply.

8.5   Security updates

– As part of the OpenSSH update from "8.4p.1" to "8.8p1" (or newer), "SHA1" will be disabled in a future firmware release.
– Busy box will be disabled in a future firmware release and replaced by other packages if necessary.

The following security updates have been made in this release. For more information about the specified CVE numbers, see:

– https://nvd.nist.gov/vuln
– https://cert.vde.com

Information on the Phoenix Contact "PSIRT" can be found at: https://www.phoenixcontact.com/psirt

Curl

– CVE-2022-43551
– CVE-2022-43552
– CVE-2023-27533
– CVE-2023-27534
– CVE-2023-28320
– CVE-2023-28321
– CVE-2023-28322
– CVE-2023-28319
– CVE-2023-23914
– CVE-2023-23916
– CVE-2023-23915

C-ares

– CVE-2022-4904
– CVE-2023-32067
– CVE-2023-31147
– CVE-2023-31130
– CVE-2023-31124

Freetype

– CVE-2023-2004

Firewall

It was possible to establish an SSH connection at boot time of the PLC before the firewall is started. This connection remained active even when the firewall is activated and configured to block this connection.

Git

– CVE-2023-22490
– CVE-2023-25652
– CVE-2023-29007

Kernel

– CVE-2022-1012

Libxml2

– CVE-2022-40303
– CVE-2016-3709
– CVE-2023-28484
– CVE-2023-29469

N-curses

– CVE-2023-29491

OpenSSL

– CVE-2023-2650
– CVE-2023-0464
– CVE-2023-0465
– CVE-2023-0466

Podman

–   CVE-2022-2989

Python

–   CVE-2022-45061
–   CVE-2023-24329

Rsync

–   CVE-2022-29154

SNMP

–   CVE-2022-44792
–   CVE-2022-44793

Sqlite

–   CVE-2022-46908
–   CVE-2022-35737
–

Sudo

–   CVE-2023-22809
–   CVE-2023-27320
–   CVE-2023-28486
–   CVE-2023-28487

Syslog

–   CVE-2022-38725

Tar

–   CVE-2022-48303

Vim

–   CVE-2022-4141
–   CVE-2022-4292
–   CVE-2023-0049
–   CVE-2023-0054
–   CVE-2023-2426
–   CVE-2023-2609
–   CVE-2023-2610

9 Changes in firmware version 2023.0.7 LTS

ℹ️ – To be able to use all new functions of the firmware, you need PLCnext Engineer version 2023.0 LTS or newer.
Select the latest template for firmware version 2023.0 LTS in the PLCnext Engineer project.
– The safety-related firmware version 02.00.0010 must be used.
Please contact the Competence Center Services as to the details on safety firmware update procedure:
Phone: +49 5281 946 2777
E-mail: safety-service@phoenixcontact.com
– In order to update to firmware version 2023.0.3 LTS or newer at least a firmware version 2022.0 LTS or newer must be installed on the PLC. Older firmware versions will not accept the *.rauc firmware update file.

This section describes changes made between firmware version 2023.0.4 LTS and firmware version 2023.0.7 LTS.

9.1 Error corrections

Proficloud

When Proficloud was configured to cache values (WBM setting "Remanent Buffering Enabled") and the connection between PLC and Proficloud was broken, the consumed memory increased. If this situation continued for too long, this could even cause a "System Watchdog".

System

Update of "paho" library from version "v1.3.10" to "v1.3.12". This update solves several incompatibilities with the IEC 61131-3 "IIoT_Library_V4.01". In particular, it fixes a "system watchdog" in combination with "MQTT-Client FB" in case of a failed MQTT connection.

9.2 Known limitations and errors

ℹ️ The known limitations and errors can be found in the PLCnext Info Center at:
https://www.plcnext.help/te/Known_issues.htm
Here you will find a constantly updated overview of all known issues.

– In rare cases, the BPC 9102S may not boot after a restart via the WBM, the PLCnext Engineer, a console comand or after a firmware update. If the SD card cannot be read after a restart of the PLC, a manual restart must be done via the power supply.

9.3 Security updates

ℹ️ – As part of the OpenSSH update from "8.4p.1" to "8.8p1" (or newer), "SHA1" will be disabled in a future firmware release.
– BusyBox will be disabled in a future firmware release and replaced by other packages if necessary.

The following security updates have been made in this release. For more information about the specified CVE numbers, see:

– https://nvd.nist.gov/vuln
– https://cert.vde.com

Information on the Phoenix Contact "PSIRT" can be found at: https://www.phoenixcontact.com/psirt

C-ares

– CVE-2022-4904
– CVE-2023-32067
– CVE-2023-31147
– CVE-2023-31130
– CVE-2023-31124

Curl

– CVE-2022-43551
– CVE-2023-38545
– CVE-2023-38546
– CVE-2022-43552
– CVE-2023-23914
– CVE-2023-23916
– CVE-2023-23915
– CVE-2023-28320
– CVE-2023-28321
– CVE-2023-28322
– CVE-2023-28319
– CVE-2023-27533
– CVE-2023-27534

Firewall

It was possible to establish an SSH connection at boot time of the PLC before the firewall was started. This connection remained active even when the firewall was activated and configured to block this connection.

Freetype

– CVE-2023-2004

Git

– CVE-2023-22490
– CVE-2023-29007

Glibc

– CVE-2023-4813
– CVE-2023-5156
– CVE-2023-4911

Libxml2

– CVE-2022-40303
– CVE-2023-28484
– CVE-2023-29469

Ncurses

– CVE-2023-29491

OpenSSL

– CVE-2023-2650
– CVE-2023-0464
– CVE-2023-0465
– CVE-2023-0466
– CVE-2023-3817

Rsync

– CVE-2022-29154

Sqlite

– CVE-2022-46908

Syslog-NG

– CVE-2022-38725

Tar

– CVE-2022-48303

User Manager

With activated "Security Profile" the role "Engineer" erro-
neously also had the rights of the role "SafetyEngineer".

10 Changes in firmware version 2023.0.4 LTS

ℹ️ – In order to update to firmware version 2023.0.4 LTS or newer at least a firmware version 2022.0.8 or newer must be installed on the PLC. Older firmware versions will not accept the *.rauc firmware update file.
– The safety-related firmware version 02.00.0010 or 02.10.0000 (upon release) must be used.
Please contact the Competence Center Services as to the details on safety firmware update procedure:
Phone: +49 5281 946 2777
E-mail: safety-service@phoenixcontact.com
– To be able to use all new functions of the firmware, you need PLCnext Engineer version 2023.0 LTS or newer. Select the latest template for firmware version 2023.0 LTS in the PLCnext Engineer project.

This section describes changes made between firmware version 2022.0.8 and firmware version 2023.0.4 LTS.

All parts of the previously released version are included in the current version.

10.1 New functions

Cyber Security

– A "Security Profile" can be activated via WBM. When the "Security Profile" is activated, the PLC is rebooted and set into a secure state. This includes deleting the project, resetting nearly all configurations and deactivating potentially insecure system services. Possible use cases and security contexts are described in the Security Info Center (https://security.plcnext.help). If these conditions are met, the certification by "TÜV Süd" according to the security standard IEC 62443-4-2 can be applied.
– The TLS socket classes (C++) support CRLs, session renegotiation and session resumption (partially supports IEC 62351).
– The TLS socket classes (C++) support querying the certificate used by the peer during the TLS handshake (partially supports IEC 62351).
– Additional security notifications of the system status are logged during the start-up of the PLCnext firmware.
– The new user role "SafetyEngineer" is supported.

– The new user role "SafetyFirmwareUpdater" is supported.
– The project integrity check results are visualized to the user in the WBM (when "Security Profile" is activated).

HMI

The display of a "System Use Notification" when logging in to HMI applications is now supported.

IEC 61131-3

The "DEVICE_INFO" function block is now supported in user applications (PLCnext Engineer 2023.0 LTS or newer).

OPC UA

– The PubSub feature was extended with the following facets:
  – Subscriber UADP Dynamic Data or Events Facet
  – Publisher UADP Dynamic Data or Events Facet
  – Subscriber UADP Flexible Layout Facet
  – Publisher UADP Flexible Layout Facet
– The OPC UA server supports references to nodes in its own address space according to "https://reference.opcfoundation.org/Core/docs/Part17/A.2/".
– The "Minimum UA Client Profile" has been implemented. Currently only manual configuration is supported (configuration via PLCnext Engineer is in progress).
– OPC UA supports ReverseConnect. PLCnext Engineer 2022.9 or newer and the related template are required for the configuration of this feature.

PLCnext Store

– Extension of PLCnext Store support with the following sub-jects:
  – Specifying the ContainerID for license operations.
  – Report active ContainerIDs to the PLCnext Store.
  – Transfer SD card slot status to the PLCnext Store.
  – In addition to licences bound to the device, licences can now also be bound to the LIC SD cards.
– New file formats (*.PlcNextRaC, *.PlcNextRaU, *.PlcNextRaR) for offline licensing in combination with the PLCnext Store are supported.

PROFINET

- Adjustable process data widths for the built-in PROFINET device in combination with the GSDML configuration are now supported. Instead of the previous fixed value of 512 bytes, you can now select from a predefined set of values between 2 and 512 bytes.

– In case of module differences, the notification "Arp.Io.PnC.ArReady" contains information about the "ModuleDiffblock" which has been sent by the PROFINET device. The module difference is also dis -played on the PROFINET page in the "Diagnostics" area of the WBM.

Proficloud

– The update of the application via Proficloud is support-ed. In PLCnext Engineer 2022.9 and newer an export of an updated application can be generated ("Export PLCnext Engineer Software Package"/"Export PLCnext Engineer Software Package (with sources)"). The exported files can be uploaded to the Proficloud and from there assigned to further devices (for this the "DMS Basic Add-on" is required).

– In case the connection between the Proficloud and the PLC is interrupted, the data can now be cached perma-nently in the PLC and sent after reconnection. The fea-ture can be enabled and configured via the "Proficloud Services" page in the WBM.

DataLogger

The DataLogger has been improved to emit more notificati-ons.

IEC 61131-3

A new function block "UPS_DIAGNOSTICS" can be used by the application. For further details on this function block refer to the help of PLCnext Engineer 2022.6 or newer. Additionally, the new system variable "UPS_DIAGNOSTICS" was introduced.

Linux/OS/Docker

– The local gRPC server was integrated for the first time. With this first step gRPC offers a kind of standardized open source, programming language independent, lo-cal interface to most of the published RSC services.

– The Docker engine Podman was integrated for the first time. With this step Podman is exclusively available for use in context of PLCnext Store apps.

Security

– An integrity check for PLCnext Engineer projects was implemented. The action in case of an integrity breach can be configured ("Warning" mode is enabled by de-fault, "Error" mode can be configured).
Note: If the integrity check is active, any project is checked while loading. This means that an integrity breach is also detected for projects without the hash code, e.g. projects that are created with a PLCnext Engineer version prior to 2022.6. The notifica -tion payload will report: "Manifest file 'PCWE.mani-fest.config' does not exist.".

– During startup a notification is emitted which lists all in-stalled PLCnext apps.

– The syslog configuration has been extended to include events logged by "podman".

– Security-related notifications are logged to a dedicated notification archive. Additionally these notifications are forwarded to the Linux syslog. In the WBM the Li-nux syslog client can be configured to forward its log mes-sages to one or more syslog servers.

System

Restricted SFTP access can be configured to predefined folders.

WBM

– The TLS version and a cipher suite can be selected on the "Web Services" page.

– If a password expiration is configured, the WBM shows a warning after login indicating when the password will expire within the configured period.

– On the page "License Management" the UUID of the PLC is shown if a license is stored on the PLC.

– A WBM page "Integrated UPS" has been introduced for diagnostics of the Integrated Uninterruptible Power Supply.

– Password complexity rules and session properties can be configured on the WBM page "User Authentication".

– NTP servers can be configured on the new WBM page "Date and Time".

– The new "Netload Limiter" tab on the page "Network" now supports the display of "NetLoadLimiter" statistic values and the user configuration for each network in-terface.

– The "General Data" page now provides additional arti-cle information on the safety PLC.

– The generation of the new private key "RSA 2048 Hard-ware protected key" is now supported in "Add Identity Store", "Key Type" on the "Certificate Authentication" page.

– A new WBM page "Cockpit" is provided.

– WBM users can change their own password directly via the new "Cockpit" page.

RSC

The RSC service "IDeviceStatusService" is extended to read additional information. The items "Status.Memory.Usage.Percent.Actual", "Status.RunStopSwitch.Supported" and "Status.RunStopSwitch.Position" have been added.

10.2 Changes

ESM

– The maximum task latency in multi core applications (by using C++ or IEC 61131-3 programs in different tasks on dif-ferent ESM) has been reduced significantly.
– The power down sequence has been refactored for PLCs with an integrated UPS. The ESM event task "Arp.Plc.Esm.OnStop" is now terminated at latest after 500 ms (even in case of a configured watchdog beyond 500 ms). If this event task is terminated, the retentive data are regarded as invalid and do not persist. As a consequence, a cold restart is performed when the power returns.
– The handling of the "Idle" task by the ESM has been optimized. The resulting cycle time is shorter and the idle task is now executed more often.

GDS

The GDS has been optimized so that less time is required to execute the GDS connectors.

Firmware update/downgrade

When a firmware version 2023.0 or newer is installed and is then downgraded to firmware version 2023.0, the application is implicitly removed and all configurations except the network configuration (file /etc/network/interfaces) are reset to the factory default configuration.

IEC 61131-3

The function block "UPS_DIAGNOSTICS" has been re-named to "READ_UPS_DIAGNOSTICS" because the original name caused a conflict with the system variable of the same name.

Linux/SDK

– Some PLCnext SDK header files included the name-space "Arp::System::Commons::Threading" by acci-dent. This has now been corrected. In order to eliminate compiler errors, C++ projects created by the customer may need to include the namespace explicitly (e.g.

statement "using Arp::System::Commons::Threading;") or use the fully qualified name by preceding the name of the related types with "Arp::System::Com-mons::Threading::".
– LDAP (libldap) has been updated to version 2.5.12. This version does no longer depend on "libg-crypt20.so". Therefore, "libgcrypt" is no longer part of the PLCnext Linux.
– GCC compiler has been upgraded from version 9.3 to version 11.2. When executed on Microsoft Windows with MinGW, the feature "pre-compiled header" does not work due to this update (gcc reports an internal er-ror).
– By accident some PLCnext SDK header files included the namespace "std". This has now been corrected. In order to eliminate compiler errors, C++ projects created by the customer may need to include the namespace explicitly (i.e. statement "using std;") or use the fully qualified name by preceding the name of the related types with "std::".
– During refactoring of some PLCnext RSC services, type aliases were removed. This also happened inside the "IDataLoggerService2" which utilizes the "VariableInfo" class from namespace "Arp::Plc::Gds::Services". Be-fore the refactoring this class was introduced into the "Arp::Services::DataLogger::Services" namespace by the "VariableInfo.hpp" file, located in the same directory as the "IDataLoggerService2.hpp". By now, the "Vari-ableInfo" class is not directly included in the "Arp::Services::DataLogger::Services" namespace but used as a type alias inside the "IDataLoggerService2" interface. This means, applications that used the "VariableInfo.hpp" before the refactoring of the "IDataLoggerService2" now have to include the following statement in order to compile successfully: "using VariableInfo = Arp::Services::DataLogger:: Service::IDataLoggerService2::VariableInfo;"

OPC UA

The "ManufacturerUri" has been renamed again from http://www.phoenixcontact.com" to http://phoenixcontact.com.

System

The feature "reset to default setting" now considers OCI containers. The folders below will now be removed:
– /media/rfs/rw/var
– /media/rfs/rw/data

SD Card

The partitioning of "SD FLASH 8GB PLCNEXT MEMORY LIC (item no. 1151112)" and "SD FLASH 32GB PLCNEXT MEMORY LIC (item no. 1151111)" has been changed. The PLCnext firmware has been adopted to this partitioning.

WBM

– A security notification "Security.Arp.System.Um.SystemUseNotificationSet" is issued when the "System Use Notification" is changed via WBM.

– Details about the "ModuleDiffBlock" are displayed on the PROFINET page in the "Diagnostics" area of the WBM. In particular the Module ID of the module that is physically present at the device is displayed.

Retain

An unexpected cold restart of the PLC project could sporadically occur after a restart of the controller. This caused the retain variables to be set to their initial values. The reason was an internal task watchdog during system shutdown, which marked the last saved retain data as invalid.

10.3   Error corrections

C++

RSC services that return values as 'out' parameters of an array data type and are called from C++ code, now clear the array before writing any value.

ESM

– The LOGIC ANALYZER in PLCnext Engineer did not log any variable values if an ESM task of type "IDLE" has been selected. This occurred with firmware version 2022.6 and 2022.9 and has been fixed for firmware version 2023.0.0 LTS.

– If an ESM task has a fatal error and exits immediately, an un-handled follow-up exception leads to a deadlock of the ap-plication.

HMI

When changes made in the HMI project were applied with "Download Changes", a "SIGSEGV" exception could occur that resulted in a PLC system watchdog (SWD).

Network

– Parallel access of multiple instances to the network adapter port status could result in error messages or exceptions.

– When an Ethernet network storm occurs at an Ethernet interface that is used by PROFINET and the Ethernet link is cut off and reconnected again, an ESM task watchdog could occur.

WBM/Security

– The option "Exclude admin users from timeout" did not work, the admin cannot be excluded. This option can be set at the "Session Configuration" tab of the WBM page "User Authentication".

– On the WBM page "Network" in the "Configuration" area, LAN interfaces and ports were displayed incorrectly.

IEC 61131-3

– When debugging IEC code using breakpoints in PLCnext Engineer, the PLC stopped with an exception.

– Using the C# method "DateTime.Now" in a static class

PLCnext Store

If an app created a file with write permissions in the temporary files directory ("/var/tmp/appsdata/"), these write permissions were removed after a system reboot. As a result, the app could no longer write to the file.

Notifications

– C# call stack after unhandled exception was doubled in "Notification.log".

– The status change related to the control of an optional fan was not written correctly to the "Output.log" file.

OPC UA

– When an eCLR component variable (IEC 61131-3 resource global variable), e.g. Arp.Plc.Eclr/PLC_CRC_PRJ, was configured to be published via "PubSub", an exception occurred during start-up. The "PubSub" component and the "UA Server" could apparently not be reached afterwards.

– Some file transfer issues were fixed, e.g. "Writable" attribute was always true and PLC crash when removing permissions.

– When using a custom information model namespace the "BrowseName" was not returned to the OPC UA client.

PROFINET

– If the "MaintenanceItem: Demanded" and the "Property Flag" "Maintenance Demanded" both occurred in the same PROFINET alarm frame, the alarm was not displayed in the PROFINET bus diagnostics in the WBM.

– In connection with a set PROFINET cycle time of 1 ms, the PROFINET controller could experience increased latency. This behavior was caused by an unfavorable timing during the communication processing of the process data.

– During the startup parameterization of a subordinate IO-Link master at an "AXL F BK PN TPS" bus coupler, the error message "0xA002" (wrong module found) could occur.

– When reading the "ModuleDiffBlock" with the function block "GET_MODULE_DIFF_BLOCK" it could happen that the states "WRONG_MODULE" and "NO_MODULE" were not returned. The error occurred when there is a module difference but no submodule difference. With "WRONG_MODULE" and "NO_MODULE" there is no submodule difference and therefore the difference was incorrectly not saved.

– If a bus coupler was operated via the PROFINET controller as a subordinate device without connected I/O modules, the "SF" LED was not activated. The bus coupler reports an "SF" and the PROFINET diagnostics in the WBM also shows this state, but neither the status LED nor the system variable "PNIO_SYSTEM_SF" indicated this.

– When loading the project, an exception could occur if the following applied: A submodule with different input and output data width with corresponding data ports was registered to the controller's PROFINET device via the bus configuration of the superior PROFINET controller.

– Setting values of "maxSlots" or "maxSubslots" in the PROFINET settings files were not effectively adopted.

– The "MaxSupportedRecordSize" from the GSDML description of a PROFINET device will now be evaluated and interpreted accordingly by the PROFINET controller. Special cases that e.g. "MaxSupportedRecordSize" of a PROFINET device is greater than the maximum record size of the PROFINET controller will be handled correctly.

– When a superior PROFINET controller attempted to set an IP address of the PROFINET device of the PLCnext controller while the system was booting, the firmware could crash (SIGSEGV).

RSC

When calling the "IDeviceInfoService" with parameters "General.Hardware.VersionMajor" or "General.Hardware.VersionMinor", the device responded with "ident not found" in the "Output.log" file.

System

– When installed apps requested a restart of the firmware, it could sporadically happen that this restart was not performed properly.

– After updating from firmware version 2021.6.7 to 2022.6.1, the firewall returned error messages regarding IPv6.

– In connection with "Docker" support, the kernel flag "CONFIG_MACVLAN" was set incorrectly.

– It could sporadically happen that the PLC went into an error state during "Download changes". Even downloading the project did not solve the error state. The PLC had to be rebooted.

– The file "/var/log/daemon.log" could become very large and in worst case it could cause an out of memory situation. This file is now considered by "logrotate" and therefore can no longer become that large.

User Manager

– Deleting all entries in "Blocked Passwords" in the WBM under "Security", "User Authentication", "Password Policy" did not work. After "Apply and reboot", all default entries were still present.

– The security notification "ResetUserRolesFailed" could not be triggered.

WBM

– The "Additional value" in the PROFINET diagnostics of a device was displayed unformatted.

– The "Additional value" in the PROFINET diagnostics of a device was displayed with wrong error code.

– Incorrectly parameterized modules were not always displayed as faulty in the "Tree View" of the PROFINET diagnostics.

– A "Link down" error was shown in the PROFINET diagnostics for a device, although a "Disappear" alarm has already been received.

– Very long DNS names were displayed unclearly in the PROFINET diagnostics for a device.

– On the WBM page "Network" in the "Configuration" area, LAN interfaces and ports were displayed incorrectly.

– Different "escape" behavior on different WBM pages has now been unified.

– Some long diagnostic texts in the context of PROFINET device diagnostics were truncated.

– The "Integrated Uninterruptible Power Supply" WBM page displayed the "HFAIL" state as a "warning" instead as an "error".

– When updating an older firmware version to version "2022.6.1", WBM access was not possible after the reboot. The only remedy was to restart the controller again.

10.4 Known limitations and errors

ℹ The known limitations and errors can be found in the PLCnext Info Center at:

https://www.plcnext.help/te/Known_issues.htm

Here you will find a constantly updated overview of all known issues.

10.5 Security updates

ℹ – As part of the OpenSSH update from "8.4p.1" to "8.8p1" (or newer), "SHA1" will be disabled in a future firmware release.

– Busy box will be disabled in a future firmware release and replaced by other packages if necessary.

The following security updates have been made in this release. For more information about the specified CVE numbers, see:

– https://nvd.nist.gov/vuln

– https://cert.vde.com

Information on the Phoenix Contact "PSIRT" can be found at: https://www.phoenixcontact.com/psirt

Busybox

– CVE-2022-30065

Curl

– CVE-2022-32207
– CVE-2022-32206
– CVE-2022-32208
– CVE-2022-32205
– CVE-2022-35252
– CVE-2022-42915
– CVE-2022-42916

Dpkg

– CVE-2022-1664

E2fsprogs

– CVE-2022-1304

Git

– CVE-2022-29187
– CVE-2022-39260
– CVE-2022-39253
– CVE 2022-41903
– CVE-2022-23521

Gnutls

– CVE-2022-2509

HMI

– Hardening against DoS attacks.

– Hardening against memory leak problems in case of network attacks.

– In some cases requests via the "REST" interface to variables of data type "STRING" that are not marked as "HMI" could cause the PLC to crash.

– Hardening the input validation of user names in "User Authentication".
– Hardening of Cross-Site-Request-Forgery (CSRF) attack in user based web management.
– The post-payload of the "WebConfiguration.cgi?SetHttpsCertificateIdentityStore" function could be modified in a way that could potentially be exploited via reflected XSS (cross-site scripting).

Libtirpc

– CVE-2021-46828

Libxml2

– CVE-2022-40304

Libexpat

– CVE-2022-40674
– CVE-2022-43680

Linux

– CVE-2022-1015
– CVE-2022-1016

Logrotate

– CVE-2022-1348

OpenSSL

– CVE-2022-2097

Python
– CVE-2022-42919
– CVE-2021-29921

SSH

– CVE 2002-20001
  The following vulnerable DHE KEX algorithm(s) of the openSSH server have been completely removed:
  – diffie-hellman-group14-sha256
  – diffie-hellman-group16-sha512
  – diffie-hellman-group18-sha512
  – diffie-hellman-group-exchange-sha256

StrongSwan

– CVE-2022-40617

Sudo

– CVE-2022-43995

User Manager

– By mistake, the "SecurityToken" when creating and modifying users was always "0000000" in the security notifications.
– Hardening of Trust and Identity Stores.

Vim

– CVE-2022-1927
– CVE-2022-1942
– CVE-2022-2129
– CVE-2022-2175
– CVE-2022-2182
– CVE-2022-2183
– CVE-2022-2343
– CVE-2022-2207
– CVE-2022-2210
– CVE-2022-2344
– CVE-2022-2304
– CVE-2022-2345
– CVE-2022-2231
– CVE-2022-2287
– CVE-2022-2284
– CVE-2022-2289
– CVE-2022-2288
– CVE-2022-2264
– CVE-2022-2206
– CVE-2022-2257
– CVE-2022-2208
– CVE-2022-2285
– CVE-2022-2286
– CVE-2022-2257
– CVE-2022-2522
– CVE-2022-2571
– CVE-2022-2580
– CVE-2022-2581
– CVE-2022-2598
– CVE-2022-3234
– CVE-2022-3235
– CVE-2022-3256
– CVE-2022-3278
– CVE-2022-3296
– CVE-2022-3297
– CVE-2022-3324
– CVE-2022-3352
– CVE-2022-3705

C-ares

– CVE-2021-3672

WBM

– Umlauts in the password of the "User Manager" were not handled correctly. The password rule for upper and lower case was not followed. This could lead to unintentionally weaker passwords.
– Hardening of WBM against Cross-Site-Scripting.

Zlib

– CVE-2022-37434

Freetype

– CVE-2022-27404
– CVE-2022-27405
– CVE-2022-27406

GLIBC

– CVE-2022-23218
– CVE-2022-23219
– CVE-2021-35942
– CVE-2020-6096
– CVE-2020-29562

LDAP

– The LDAP "GroupMappings" were compared with "case sensitivity" on the controller, although the "case sensitivity" support was disabled on the LDAP server. No error message indicating this fact was thrown. Now when the firmware reads in its LDAP server configuration, the LDAP "GroupMappings" were converted to lower case.
– The cipher list setting for the LDAP TLS configuration for the server connection was not properly applied. As a result, the highest possible encryption method was not always selected for the communication.

Ncurses

– CVE-2022-29458

Nginx

– CVE-2021-3618

Podman

– CVE-2022-1227
– CVE-2022-27649

Protobuf

– CVE-2021-22570

Rsync

– CVE-2020-14387

SSL

– CVE-2011-1473
– CVE-2011-5094

CSV

– Sanitized the output (CSV file) of the notifications export in the WBM in order to prevent CSV injection software attack from CVE-2014-3524.

System

– It was possible to get admin rights partially via a reconfiguration of the user roles "Engineer" or "Commissioner".

11 Changes in firmware version 2022.0.8 LTS

ℹ – To be able to use all new functions of the firm-ware, you need PLCnext Engineer version 2022.0.1 LTS or newer.
Select the latest template for firmware version 2022.0.0 LTS in the PLCnext Engineer project.
– It is strongly recommended to use the safety firmware 02.00.0010.
Please contact the Competence Center Services as to the details on safety firmware update procedure:
Phone: +49 5281 946 2777
E-mail: safety-service@phoenixcontact.com

ℹ **Attention when Downgrading the firmware**
Any BPC 9102S with a hardware-revision >=03 cannot be downgraded to a firmware version
<= 2022.0.x ! This results in a defective hardware.
A BPC 9102S HW: >=3 cannot be downgraded to FW 2022.0.8!

11.1 Known limitations and errors

ℹ The known limitations and errors can be found in the PLCnext Info Center at:
https://www.plcnext.help/te/Known_issues.htm
Here you will find a constantly updated overview of all known issues.

11.2 Security updates

ℹ – As part of the OpenSSH update from "8.4p.1" to "8.8p1" (or newer), "SHA1" will be disabled in a future firmware release.
– BusyBox will be disabled in a future firmware release and replaced by other packages if necessary.

The following security updates have been made in this release. For more information about the specified CVE numbers, see:
– https://nvd.nist.gov/vuln
– https://cert.vde.com
Information on the Phoenix Contact "PSIRT" can be found at: https://www.phoenixcontact.com/psirt

BusyBox
– CVE-2022-28391

Curl
– CVE-2022-22576
– CVE-2022-27778
– CVE-2022-27779
– CVE-2022-27782
– CVE-2022-27774
– CVE-2022-27776
– CVE-2022-30115
– CVE-2022-27780
– CVE-2022-27781
– CVE-2022-27775
– CVE-2022-32207
– CVE-2022-32206
– CVE-2022-32208
– CVE-2022-32205

Cyrus SASL
– CVE-2019-19906
– CVE-2022-24407

HMI
Hardening against DoS attacks.

IPv6
Fixed IPv6 firewall rules despite IPv6 is not fully supported yet.

LIBEXPAT
– CVE-2022-25235
– CVE-2022-25236
– CVE-2022-25313
– CVE-2022-25314
– CVE-2022-25315

LIBXML
– CVE-2022-29824
– CVE-2022-23308

OpenSSL
– CVE-2022-0778

OPC UA
Unified Automation reported several security risks for the OPC UA SDK 1.7.6 and before. All reported issues are fixed with the update of OPC UA SDK version 1.7.7.

OpenVPN
– CVE-2022-0547

Vim

– CVE-2022-1381
– CVE-2022-1420
– CVE-2022-1733
– CVE-2022-1796
– CVE-2022-1621
– CVE-2022-1616
– CVE-2022-1619
– CVE-2022-1629
– CVE-2022-1735
– CVE-2022-1769
– CVE-2022-1785
– CVE-2022-1620
– CVE-2022-1674
– CVE-2022-1771
– CVE-2022-1886
– CVE-2022-1851
– CVE-2022-1898
– CVE-2022-1720
– CVE-2022-1154
– CVE-2022-0943
– CVE-2022-1160
– CVE-2022-1381
– CVE-2022-0729
– CVE-2022-0572
– CVE-2022-1420
– CVE-2022-0696
– CVE-2022-0685
– CVE-2022-0714
– CVE-2022-0361
– CVE-2022-0368
– CVE-2021-3973
– CVE-2021-3796
– CVE-2021-4166
– CVE-2022-1733
– CVE-2022-1796
– CVE-2022-1621
– CVE-2022-1616
– CVE-2022-1619
– CVE-2022-1629
– CVE-2022-1735
– CVE-2022-1769
– CVE-2022-1785
– CVE-2022-1620
– CVE-2022-1674
– CVE-2022-1771

– CVE-2022-1886
– CVE-2022-1851
– CVE-2022-1898
– CVE-2022-1927
– CVE-2022-1942
– CVE-2022-1720
– CVE-2022-2129
– CVE-2022-2175
– CVE-2022-2182
– CVE-2022-2183
– CVE-2022-2343
– CVE-2022-2207
– CVE-2022-2210
– CVE-2022-2344
– CVE-2022-2304
– CVE-2022-2345
– CVE-2022-2208
– CVE-2022-2231
– CVE-2022-2287
– CVE-2022-2285
– CVE-2022-2284
– CVE-2022-2286
– CVE-2022-2289
– CVE-2022-2288
– CVE-2022-2264
– CVE-2022-2206
– CVE-2022-2257

ZLib

– CVE-2018-25032

12 Changes in firmware version 2022.0.1 LTS

| | – To be able to use all new functions of the firmware, you need PLCnext Engineer version 2022.0.1 LTS or newer.
Select the latest template for firmware version 2022.0.0 LTS in the PLCnext Engineer project.
– It is strongly recommended to use the safety firmware 02.00.0010 at availability. This firmware will presumably be issued at the end of April 2022.
Please contact the Competence Center Services as to the details on safety firmware update procedure:
Phone: +49 5281 946 2777
E-mail: safety-service@phoenixcontact.com |

| | **Attention when Downgrading the firmware**
Any BPC 9102S with a hardware-revision >=03 cannot be downgraded to a firmware version <= 2022.0.x ! This results in a defective hardware.
A BPC 9102S HW: >=3 cannot be downgraded to FW 2021.0.1! |

12.1 New functions

System

The binding of licenses for certain extension functionalities is now also possible in connection with an inserted SD card with corresponding license. This works exclusively with the following SD cards:
– SD FLASH 8GB PLCNEXT MEMORY LIC (item no. 1151112)
– SD FLASH 32GB PLCNEXT MEMORY LIC (item no. 1151111)
– SD FLASH PLCNEXT MEMORY LIC CFG (item no. 1308064)

Linux/OS/Docker

The local gRPC server was integrated for the first time. With this first step gRPC offers a kind of standardized open source, programming language independent, local interface to most of the published RSC services.

OPC UA

– Controller to controller (C2C) data exchange via UDP protocol has been implemented according to the OPC UA Publish and Subscribe specification. "Publisher UDP UADP Periodic Fixed Profile" and "Subscriber UDP UADP Periodic Fixed Profile" are supported. Signing and encryption are not supported yet. The communication can be configured via PLCnext Engineer (from version 2022.0.1 LTS). The feature can be enabled via WBM. If enabled, it can be evaluated during a 4 hours trail-period. Otherwise a license (item no. 1392702) must be purchased from the PLCnext Store.
– A firmware update is supported according to "DI SU Software Update Base Server Facet" and "DI SU Cached Loading Server Facet". For this purpose the new user role "SoftwareUpdate" has been introduced. This is a preparation for managing and updating the standard (non-safety) firmware (*.rauc) by a Device and Update Management Service (DaUM), which will be released as an app for PLCnext in 2022.

WBM

– Password complexity rules and session properties can be configured on the WBM page "User Authentication".
– NTP servers can be configured on the new WBM page "Date and Time".

Cyber Security

Security-related notifications are logged to a dedicated notification archive. Additionally these notifications are forwarded to the Linux syslog. In the WBM the Linux syslog client can be configured to forward its log messages to one or more syslog servers.

PROFINET

– PROFINET diagnostic information for modules and submodules are logged as notifications (Notification Logger). Additionally this information is shown on the "Profinet" page in the "Diagnostics" area of the WBM. Furthermore, in case of a PROFINET error, the WBM page displays a plain text in English language along with the corresponding error code. The plain text is issued for the module or submodule level. PLCnext Engineer 2022.0.1 LTS or newer (a template for firmware 2022.0 LTS or newer has to be used as well) collects the corresponding texts from the device description file (FDCML resp. GSD) of the related PROFINET devices. The collected texts are part of the downloaded project.

– Support of PROFINET "ModuleDiffBlock" information with RSC service "IArConfigurationService" and IEC 61131-3 function block "GET_MODULE_DIFF_BLOCK" (PLCnext Engineer 2022.0.1 LTS and newer). The WBM already displays a module difference in the tree view and also shows the message "wrong module" in the device details of the PROFINET diagnosis.

12.2   Changes

GDS

In case of GDS configuration errors, all errors are collected into a single notification. The previous firmware versions only stated the first configuration error and stopped further reading of the configuration files.

C++/SDK

Due to a minor cleanup of the namespaces, some missing using statements may cause an error when compiled with an SDK version 2022.0 or newer. This may occur in following cases:

1. If the classes "Arp.System.Commons.Console" or "Arp.System.Commons.Environment" are used, insert a "using namespace Arp::System::Commons;" statement as a remedy.

2. If any class of the "Arp.System.Commons.Exceptions" namespace is used, there are two remedies:
   If the dedicated exception header file has been included, insert a "using namespace Arp::System::Commons::Exceptions;" statement as a remedy.
   If the general header file "Arp/System/Commons/Exceptions.h" has been included, insert a "using namespace Arp;" statement as a remedy.

Retain

In extremely rare cases not all retain variables can be set to their correct remanent value after a power loss. This situation is now improved. When the PLC is rebooted, incorrect values are detected and a cold restart is performed automatically. A corresponding warning is emitted to the log file "Output.log".

HMI

For projects compiled with PLCnext Engineer 2022.0.1 LTS (and newer) with a template for firmware 2022.0 LTS (and newer), the system variable HMI_STATUS was replaced by the system variable HMI_STATUS2. It was replaced because the member HMI_STATION_NUM has been added to the HMI_STATUS_STRUCT and as a consequence the new data type HMI_STATUS2 needed to be implemented in PLCnext Engineer.

PROFINET

Reduction of frequent and for end users unhelpful messages in the log file "Output.log". This mainly concerns messages in the PROFINET context.

EtherNet/IP™

The EtherNet/IP product code of the slave device has been changed from 8220 to 8228. This may affect the configuration of the corresponding Ethernet/IP master if it relies on the product code.

12.3   Error corrections

The following errors have been rectified:

SPLC

– In case the "SafetyProxyTask" was in an overload situation, it could happen that the real duration of this task could not be seen in the corresponding TASK_INFOS structure of the ESM_DATA variable.

– Under certain project conditions which led to an overload situation, the SPLC could switch to the failure state (FS) during operation and as a result the application was stopped. Additional logging messages have been added in case a comparable behavior occurs.

– When in PLCnext Engineer the interval time of the "SafetyTask" has been changed and the project is downloaded to the PLC, it could happen that the SPLC went into failure state (FS). Afterwards the PLC needed to be rebooted.

– The resolution of the safelog (visible in the "Safety PLC log messages" view of PLCnext Engineer) has been changed from seconds to milliseconds.

– During operation it could happen that the SPLC switched to failure state (FS) and the error code "0x80C9".

Network

– Although the "Netload Limiter" was enabled, the PLC project could be affected by special network packet storms.

– With heavy network load, CPU load problems could occur due to a great volume of logging messages.

IEC 61131-3

– When a function block programmed in SFC (Sequential Function Chart) was changed in PLCnext Engineer, these changes could not be sent to the PLC using "Download Changes" due to an exception. This error only occurred with firmware 2021.9

– In rare cases, the PLC could not be restarted after stopping when using PLCnext Engineer. The problem only occurred when a cold and warm start were performed and a PROFINET controller was used. The problem did not occur during a hot start. The PLC had to be rebooted.

– In rare cases, when the firmware rejected a "Download Changes" command, the project was damaged and had to be downloaded again.

System

In rare cases, the PLC could run immediately into an ESM task watchdog after a power reset.

PROFINET

A timer overflow in the PROFINET stack that occurred after 49 days was fixed. This mainly affected protocols like DCP during connection establishment or the cyclic LLDP neighbor discovery.

Retain

Retain variables inside a function block that have been added by a "Download Changes" command have been stored in the retentive memory with the value 0. As a consequence, the value was set to 0 after stop and warm start . This error occurred since firmware version 2021.0 LTS.

Notifications

After a connection loss when displaying notifications in the PLCnext Engineer cockpit, it could happen that the display of notifications in the WBM generally no longer worked. Only the error message "Lost connection to Controller! (timeout)" was displayed.

12.4   Known limitations and errors

	The known limitations and errors can be found in the PLCnext Info Center at: https://www.plcnext.help/te/Known_issues.htm Here you will find a constantly updated overview of all known issues.

12.5   Security updates

	– As part of the OpenSSH update from "8.4p.1" to "8.8p1" (or newer), "SHA1" will be disabled in a future firmware release. – Busy box will be disabled in a future firmware release and replaced by other packages if necessary.

The following security updates have been made in this release. For more information about the specified CVE numbers, see:

– https://nvd.nist.gov/vuln

– https://cert.vde.com

Information on the Phoenix Contact "PSIRT" can be found at: https://www.phoenixcontact.com/psirt

SSL

– CVE-2021-3712
– CVE-2021-3711
– Deprecated encryption versions "TLSv1.0" and "TLSv1.1" were allowed over certain ports.

Strongswan

– CVE-2021-41990
– CVE-2021-45079

Open SSH

– CVE-2016-20012

Open VPN

– CVE-2020-15078

Nettle

– CVE-2021-3580 (CVSS: 7.5)
– CVE-2021-20305 (CVSS: 8.1)

GIT

– CVE-2021-40330
– CVE-2021-21300

GLIBC

– CVE-2021-35942
– CVE-2020-6096
– CVE-2020-29562

GNUTLS

– CVE-2021-20231
– CVE-2021-20232
– CVE-2020-24659

LIBSSH2

– CVE-2019-17498

LIBXML2

– CVE-2021-3517
– CVE-2021-3518
– CVE-2021-3537

PERL

– CVE-2020-10878
– CVE-2020-10543
– CVE-2020-12723

TAR

– CVE-2021-20193

NGINX

– CVE-2021-23017

NET-SNMP

– CVE-2019-20892

GMP

– CVE-2021-43618

Python

– CVE-2019-20907

LIBEXPAT

– CVE-2021-45960
– CVE-2022-22824
– CVE-2022-22823
– CVE-2022-22822
– CVE-2022-22825
– CVE-2021-46143
– CVE-2022-22826
– CVE-2022-22827
– CVE-2022-23852
– CVE-2022-23990

CURL

– CVE-2021-22946
– CVE-2020-8169
– CVE-2021-22926
– CVE-2020-8177
– CVE-2021-22922
– CVE-2021-22947
– CVE-2021-22897
– CVE-2021-22925
– CVE-2021-22923
– CVE-2021-22898

Busybox

– CVE-2021-42374
– CVE-2021-42386
– CVE-2021-42380
– CVE-2021-42381
– CVE-2021-42379
– CVE-2021-42384
– CVE-2021-42378
– CVE-2021-42382
– CVE-2021-42385

   The documented CVEs were not fixed via an update of busybox. Instead, the affected busybox components have been removed: The following config switches have been switched off ("not set"):
   CONFIG_FEATURE_SEAMLESS_LZMA=y
   CONFIG_ASH=y
   CONFIG_AWK=y
   In the case of "AWK" it makes no difference as this tool is also integrated from the core utils library. The shell "ASH" and the "LZMA" algorithms (i.e. for unzip) are no longer supported.

– CVE-2018-1000500

OPC UA

– CVE-2021-45117

BASH

– CVE-2019-18276

LDAP

A change from the registered "Cipher Suite" to the default value in the LDAP configuration did not work.

PROFINET

– The public "IConfigurationService" could be used by mistake in the C++ SDK without authorization.
– The data length at the "IAcyclicCommunicationService::RecordWrite" was not checked properly. This could result in memory being read beyond the vector boundary and sent as record data.

WBM/HMI

Deprecated SSL/TLS protocols in nginx web server have been disabled. Only TLS v1.2 and v1.3 are now enabled.

13 Changes in firmware version 2021.9

ℹ️ — To be able to use all new functions of the firmware, you need PLCnext Engineer version 2021.9.0 or newer.

Select the latest template for firmware version 2021.9.0 in the PLCnext Engineer project.

ℹ️ **Attention when Downgrading the firmware**

Any BPC 9102S with a hardware-revision >=03 cannot be downgraded to a firmware version

<= 2022.0.x ! This results in a defective hardware.

13.1 New functions

System

The binding of licenses for certain extension functionalities is now also possible in connection with an inserted SD card with corresponding license.
This works exclusively with the following SD cards:
– SD FLASH 8GB PLCNEXT MEMORY LIC
  (item no. 1151112)
– SD FLASH 32GB PLCNEXT MEMORY LIC
  (item no. 1151111)
– SD FLASH PLCNEXT MEMORY LIC CFG
  (item no. 1308064)

Linux/OS/Docker

The Docker engine Podman was integrated for the first time. With this step Podman is exclusively available for use in context of PLCnext Store apps.

DataLogger

The DataLogger has been improved to emit more notifications.

PLCnext Store

Extension of PLCnext Store support with the following subjects:
– Specifying the ContainerID for license operations.
– Report active ContainerIDs to the PLCnext Store.
– Transfer SD card slot status to the PLCnext Store.
– In addition to licenses bound to the device, licenses can now also be bound to the LIC SD cards.

OPC UA

The OPC UA server of the controller has been certified according to OPC UA version 1.0.4.

13.2 Error corretions

The following errors have been rectified:

System

In rare cases, the controller did no longer recognize the SD card after an interruption of the power supply. All LEDs flashed and the controller could not be connected via Ethernet. Only some 2 GB SD cards were affected by this.

PLCnext Store

If an app created a file with write permissions in the temporary files directory ("/var/tmp/appsdata/"), these write permissions were removed after a system reboot. As a result, the app could no longer write to the file.

GDS

If with firmware 2021.6.0 a fieldbus I/O of data type Bitstring or OctetString was connected to a program port of data type ARRAY, only the value of the first ARRAY element was transferred. The remaining elements were not copied.

OPC UA

When using a custom information model namespace the "BrowseName" was not returned to the OPC UA client.

13.3 Known limitations and errors

ℹ️ The known limitations and errors can also be found in the PLCnext Info Center at:

https://www.plcnext.help/te/Known_issues.htm

Here you will find a constantly updated overview of all known issues.

– Retain variables
  – If a requested warm start is not possible to execute via PLCnext Engineer, an implicit cold start is automatically executed. The retain variables are set to their initialization value.
  – After a system watchdog, only a cold start can be performed when the controller is started. The retain variables are set to their respective initialization values.
    From firmware 2021.0 LTS and newer a dedicated state of the retain values can be restored from a backup.
  – If firmware version 2020.0 LTS or later is downgraded to 2019.9 or older and then upgraded again to firmware version 2020.0 LTS or later, a cold start is performed. The retain variables are set to their initialization value.
– EthernetIP
  If the firewall is activated via WBM, the operation of

EthernetIP is no longer possible.
This can be remedied by subsequently activating the ports:
- Incoming connections: **port 44818**
- Outgoing connection: **port 2222**
- PLCnext CLI version
The PLCnext CLI version used must match the current SDK for this version. Downward compatibility cannot be guaranteed.
- Configuration changes to safety nodes
With attached AXC F XT SPLC 1000:
Only a complete recompilation and redownload of the standard and safety project guarantees a consistent adoption of configuration changes to safety nodes in the bus structure of the standard project.
- Firmware downgrade
After downgrading the firmware, it is recommended to reset to "Default setting type 1". This is not necessary when updating the firmware.
- WBM error message
If the PLCnext system firmware has not started up properly, the WBM displays the error message "Bad Gateway 502".
- Task name
If "Event", "EventTask", "ServiceTask" or "Globals" is used as the name of a task, an error condition of the controller occurs when the project is downloaded. It occurs because these names are already used internally as class name.
- DHCP
DHCP can only be switched on for Ethernet adapters that are not assigned as PROFINET controllers or PROFINET devices. To make the settings effective in the network, the device must be restarted.
- Variables
The content of the variables "ESM_DATA.ESM_IN-FOS[*].ESM_TICK_COUNT" and "ESM_DATA.ES-M_INFOS[*].ESM_TICK_INTERVAL" is permanently set to 0.
- Error during program download
During a PLCnext Engineer program download (both total and changes), the web server returns an error 503 (busy) for requests to the HMI pages.
- DataLogger
If two or more DataLogger sessions are configured to write to the same database, only the data of one session will be transferred to the database on the SD card at the end. As of firmware 2021.9 the user receives a notification indicating which session is recorded.

- Retain data
Using the maximum quantity structures of the retain data can increase the task duration of the using task. This can trigger a task watchdog for time-critical applications.
- STRING variables
Access to long STRING variables outside the application is limited to 511 bytes. This concerns reading and writing via the RSC services "IDataAccessService" and "ISubscriptionService". These services are used by OPC UA, PLCnext Engineer HMI and the online functions of PLCnext Engineer, among others.
From firmware version 2021.6: The same applies for WSTRING variables. Please note that WSTRING variables are converted to UTF8 when accessed via RSC services.
- "Download Changes"
Sporadically a PLCnext Engineer project may reject "Download changes" without giving a reason.
- Restart after app installation
Sporadically it can happen that a restart of the firmware requested by an app installation does not work properly. If the firmware does not start up correctly, the controller can be restarted by one of the following 3 possible actions:
  - Restart of the firmware via SSH (/etc/init.d/plcnext restart)
  - Reboot of the controller via SSH
  - Power reset of the controller
- Local time zone setting
Setting local time zones is not fully supported.
- "Link" and "Active" LEDs
The "Link" and "Active" LEDs on the network interfaces "X1" and "X2" are not active when a "10BaseT" connection is used.
- PROFINET cycle time
The use of a PROFINET cycle time of 1 ms leads to a deviation of the jitter behavior required by the controller certification.
Operation in this state is possible, but not recommended.
- Language standard C++ 17
With the SDK version 2021.6 the language standard C++ 17 has been set in the compiler options ("-std=c++17"). The firmware itself is also compiled with this option set. Besides some general C++ issues related to this C++17 standard, the following issue is related to PLCnext:
C++ 17 introduces the data type "std::byte" which is unfortunately not compatible with "Arp::byte". Therefore, if

the namespaces "std" and "Arp" are both active the compilation results in an error. In this case existing C++ sources have to be adjusted so that they explicitly use "Arp::byte" (e.g. by adding "using byte = Arp::byte;").

– Communication errors
Sporadic communication errors may occur between PLCnext Engineer and the controller. A reboot of the controller solves the problem.

– Unexpected behavior using the Select() method
The Select() method of the classes Arp::System::Commons::Ipc::IpcSocket, Arp::System::Commons::Net::Socket and Arp::System::Commons::Net::TlsSocket returns true, when the socket is shut down. Compared to BSD sockets, this behavior is unexpected. As this is a legacy method it is now remarked as deprecated. In future, additionally a new method Poll() will be implemented.

– System crash caused by user components
If a user component causes a crash before the system watchdog is activated, the firmware terminates and the controller is available via SSH only.
Note: The system watchdog is activated just before the IControllerComponent::Start() method is invoked.

– License operations, such as adding or removing a license, include cryptographic operations and hence shall only be performed if the PLC is stopped. This may avoid side effects due to preempting the license operations by tasks running with higher priority.

12.4 Security updates

The following security updates have been made in this release. For more information about the specified CVE numbers, see:

– https://nvd.nist.gov/vuln
– https://cert.vde.com

Information on the Phoenix Contact "PSIRT" can be found at: https://www.phoenixcontact.com/psirt

WBM

– Deprecated SSL/TLS protocols in nginx web server have been disabled.
Only TLS v1.2 and v1.3 are now enabled.
– The post-payload of the "WebConfiguration.cgi?SetHttpsCertificateIdentityStore" function could be modified in a way that could potentially be exploited via reflected XSS (cross-site scripting).

LDAP

– The LDAP "GroupMappings" were compared with "case sensitivity" on the controller, although the "case sensitivity" support was disabled on the LDAP server. No error message indicating this fact was thrown. Now when the firmware reads in its LDAP server configuration, the LDAP "GroupMappings" were converted to lower case.
– The cipher list setting for the LDAP TLS configuration for the server connection was not properly applied. As a result, the highest possible encryption method was not always selected for the communication.