BPC 9102S – CHANGE NOTES

Change notes for the BPC 9102S Remote Field Controller

Application note
1246285_en_5

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: 2023.0.4 LTS

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.

Note:

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

2 Table of contents

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

3 Changes in firmware version 2023.0.4 LTS

- 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.

3.1 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 supported. 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 permanently in the PLC and sent after reconnection. The feature 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, local 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 default, “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.manifest.config' does not exist.”.
– During startup a notification is emitted which lists all installed 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 Linux
syslog client can be configured to forward its log messages 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 interface.
– The “General Data” page now provides additional article information on the safety PLC.
– The generation of the new private key “RSA 2048 Hardware 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.

3.2 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 renamed 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 namespace “Arp::System::Commons::Threading” by accident. 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::Commons::Threading::”.
- LDAP (libldap) has been updated to version 2.5.12. This version does no longer depend on “libgcrypt20.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 error).
- 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”. Before 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 “VariableInfo” 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.

3.3 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.

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.

- CVE-2023-26463

3.5 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

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”.

4 Changes in firmware version 2022.0.8 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.
  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

4.1 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.

4.2 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.
- 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

5 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

5.1 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”.

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.

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.

5.2 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.

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.

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.

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”.

5.3 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.

5.4 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.

5.5 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.

6 Changes in firmware version 2021.9

– 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.

6.1 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.

6.2 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.

6.3 Known limitations and errors

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_INFOS[*].ESM_TICK_COUNT” and “ESM_DATA.ESM_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.

6.4 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.