AXC F 3152 – CHANGE NOTES

Change notes for the AXC F 3152 controller

Application note
109651_en_10

1 General information

This document contains all changes made between firmware version 2020.3.1 and the current firmware version of the AXC F 3152 controller (Order No. 1069208).

Current firmware version: 2023.3.0

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.

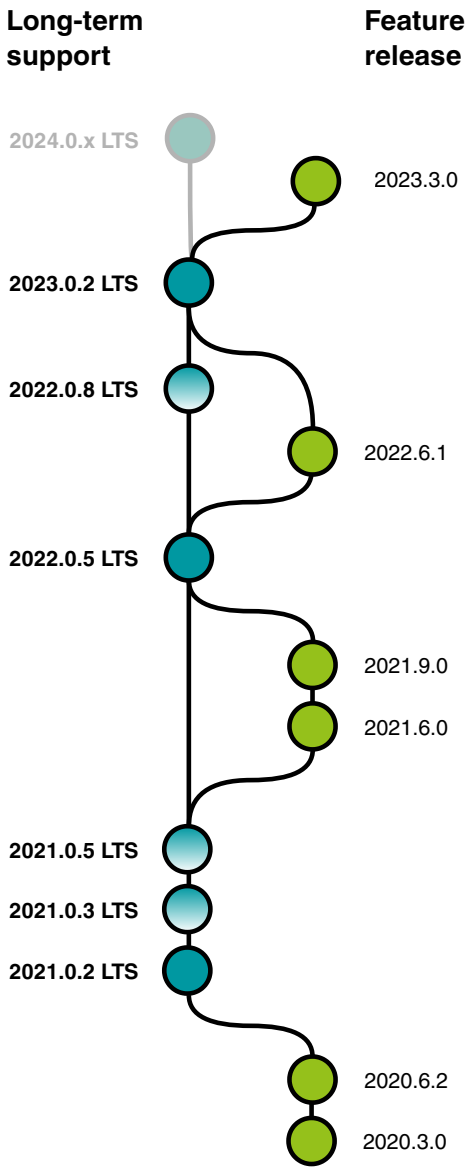
Firmware releases

Feature releases or hotfixes of an LTS version are based on the previous versions of the respective branch. Therefore they only contain the features, changes, error corrections, and security updates of the previous version. Refer to “Firmware releases AXC F 3152” on page 2 to see on which release branch your firmware version is located and which features, changes, error corrections, and security updates your firmware version contains.

2 Table of contents

Make sure you always use the latest documentation.
It can be downloaded at phoenixcontact.net/product/1069208.

3 Firmware releases AXC F 3152



4 Changes in firmware version 2023.3.0

- To be able to use all new functions of the firmware, you need PLCnext Engineer version 2023.0.1 LTS or newer.
  Select the latest template for firmware version 2023.0 LTS in the PLCnext Engineer project.
  Note: The PLCnext Engineer version 2023.3 is not recommended in combination with safety-related projects and local safety-related Axioline modules.
- In order to update to firmware version 2023.3.0 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 2023.0.2 LTS and firmware version 2023.3.0.

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

4.1 New functions

OPC UA

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.

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.

4.2 Error corrections

Axioline

After an unexpected termination of the PLCnext Runtime process it could happen that parameterized output substitute values for the local Axioline bus were not output but set to zero.

ESM

The ESM sporadically detected a task watchdog in combination with temporary high system load at lower priority and usage of IEC function blocks that internally initiate RSC services. This issue has been fixed.

OPC UA Client

Several memory leaks in case of read or write subscriptions were fixed.

Proficloud

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

PROFINET

- When the PROFINET controller established a connection to a PROFINET device, the order of parameters during DCP Connect Request was changed in some cases with firmware 2022.6.3. This change has been reverted because at least one PROFINET device type (equipped with an old firmware) did not connect with this changed order.
- 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.
- PROFINET controller: Due to an internal timer overflow a connection to some PROFINET devices could not be re-established after the controller operated longer than ~21 days.

SPLC

In combination with the left-alignable extension module “AXC F XT SPLC 3000” (item no. 1160157), a cycle time of 20 ms becomes effective although a “Safety PLC cycle time” greater than 20 ms is configured.

System

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.

WBM

The “Change Password” dialog did not handle special characters correctly.

4.3 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.

4.4 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

GIT

- CVE 2022-41903
- CVE-2022-23521

OpenSSL

- CVE-2023-0286
- CVE-2022-4304
- CVE-2023-0215
- CVE-2022-4450
- CVE-2023-0216

SQLite

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

Strongswan

- CVE-2023-26463

5 Changes in firmware version 2023.0.2 LTS

- 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.
- In order to update to firmware version 2023.0.2 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 2022.6.1 and firmware version 2023.0.2 LTS.

All parts of the previously released version and changes made in 2022.0.8 LTS are included in the current version.

5.1 New functions

Axioline

- Diagnostic information sent from an Axioline module to the Axioline master are now logged to the “Output.log” file and sent as a new notification “Arp.Io.Axioline.Device.*”. Thus, the history can be inspected in the notification log via WBM or PLCnext Engineer. Errors reported during start-up of the Axioline bus by an Axioline module have been logged to the “Output.log” file. Now these errors are logged additionally as new notification “Arp.Io.Axioline.Parameterization.Error”, respectively “Arp.Io.Axioline.Configuration.Error”. Such errors were difficult to find before, especially with IO-Link modules.
- The Axioline master firmware has received a maintenance update.

Cyber Security

- The “Security Profile” can now be activated without license.
- 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 “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

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.
- The PROFINET controller is recertified according to PROFINET specification version 2.42 and Net Load Class II.
- The PROFINET device is recertified according to PROFINET specification version 2.42 and Net Load Class II.

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. Note that Proficloud will support this feature in a future version.

– 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.

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.

SPLC

The left-alignable extension module AXC F XT SPLC 3000 (item no. 1160157) is supported.

WBM

– 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.

5.2 Changes

ESM

The maximum task latency in multi core applications (by using C++ or IEC 61131-3 programs in different tasks on different ESM) has been reduced significantly.

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.

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

5.3 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

– Sporadically it could happen that the ESM event task “Interbus cycle end” influenced the running INTERBUS by a runtime difference, if the system time of the controller was changed during operation. This could lead to a stop of the INTERBUS master.
– 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.

Fan module

When the PLC is switched on at high temperature a connected fan did not start.

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).

IEC 61131-3

- In case no task was configured to update the Axioline output data, Axioline outputs could cause standing outputs for a short time in the context of a task with linked Axioline ports if the task was stopped by a breakpoint set in PLCnext Engineer.
- When debugging IEC code using breakpoints in PLCnext Engineer, the PLC stopped with an exception.
- “Download Change” was not working if the PLC was used in combination with a AXC F XT PB left-alignable extension module.
- Using the C# method “DateTime.Now” in a static class could in some cases cause an error when downloading the project.
- If both SRL controllers (system redundancy) were in “backup” state (both with “force primary = false”), the system variables of the PLC's PROFINET device were reset.

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.

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.

PROFINET

- 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.
- 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.

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.

SD card

The detection whether the SD card is plugged in was corrected. This previously caused problems in combination with the left-alignable extension module AXC F XT SPLC 1000.

Status LEDs

The “SF” LED was not disabled after the last diagnosis disappears with the specifier “All subsequent disappears”.

System

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

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”.
- Errors occurred in the WBM Axioline diagnostics when displaying different Axioline base profiles (e.g. module 2.0 or 3.0 profile).
- When updating an older firmware version to version “2022.6.0” or “2022.6.1”, WBM access was not possible after the reboot. The only remedy was to restart the controller again.

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

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

Gnutls

– CVE-2022-2509

HMI

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

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

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

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

6 Changes in firmware version 2022.6.1

To be able to use all new functions of the firmware, you need PLCnext Engineer version 2022.6 or newer.
Select the latest template for firmware version 2022.6 in the PLCnext Engineer project.

6.1 New functions

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.
Note: With hardware revision 01 only the charge level is evaluated, the health state cannot be evaluated (WARN and FAIL have always the value FALSE).

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/”.

PROFINET

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 displayed on the PROFINET page in the “Diagnostics” area of the WBM.

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 notification 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”.

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.
  Note: With hardware revision 01 only the charge level is evaluated. The health state cannot be evaluated.

6.2 Changes

ESM

- 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.

Linux/SDK

- 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;”

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.
- When the “Security Profile” is enabled the “User Authentication” cannot be disabled.
- 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.

6.3 Error corrections

ESM

If an ESM task has a fatal error and exits immediately, an unhandled follow-up exception leads to a deadlock of the application.

HMI

With firmware versions 2022.0 LTS and earlier, the HMI server stopped when the password of a user who was not (or no longer) assigned any “EHmiLevel*” role has been changed in the HMI. To recover from this situation the PLC needed to be rebooted. This bug has been fixed.

PROFINET

- When cyclic tasks at all ESM (cores) were used and these tasks had an execution duration (ESM_DATA.ESM_INFOS[..].TASK_INFOS[..].MAX_EXEC_DURATION) longer than the configured Monitor time of a PROFINET device (in PLCnext Engineer: Profinet device in the PLANT area → interface node → Settings tab → Monitor time), this PROFINET device connection could be terminated and re-established. This bug has been fixed.
- 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).

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.

6.4 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.

6.5 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 DHE KEX algorithm(s) of the openSSH server will be removed in a future firmware release:
  - diffie-hellman-group14-sha256
  - diffie-hellman-group16-sha512
  - diffie-hellman-group18-sha512
  - diffie-hellman-group-exchange-sha256

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

C-ares

- CVE-2021-3672

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

Cyrus SASL

- CVE-2019-19906
- CVE-2022-24407

GLIBC

- CVE-2022-23218
- CVE-2022-23219

Kernel

- CVE-2018-12207

LIBEXPAT

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

Libxml

- CVE-2022-29824
- CVE-2022-23308

Ncurses

- CVE-2022-29458

Nginx

- CVE-2021-3618

OpenSSL

- CVE-2022-0778

OpenVPN

- CVE-2022-0547

Podman

- CVE-2022-1227
- CVE-2022-27649

Protobuf

- CVE-2021-22570

Python

- CVE-2021-29921

Rsync

- CVE-2020-14387

SSH

- CVE 2002-20001 (fixed, if Security Profile is enabled)

SSL

- CVE-2011-1473
- CVE-2011-5094

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

Zlib

– CVE-2018-25032

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.

HMI

– 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.

IPv6

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

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.

System

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

WBM

– Hardening the input validation of user names in “User Authentication”.
– Hardening of Cross-Site-Request-Forgery (CSRF) attack in user based web management.

7 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.

7.1 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.

7.2 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.
– 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-2022-28391

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

8 Changes in firmware version 2022.0.5 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.

8.1 New functions

Article

Support of the left-alignable extension module (machine learning module) AXC F XT ML 1000 (item no. 1259849).

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.
- A “Security Profile” can be activated via WBM. This requires a license as described in the topic “Security Profiles” in the “Security” section of https://www.plcnext.help. 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.

8.2 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 8222. 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”.

8.3 Error corrections

The following errors have been rectified:

Fan module

When the PLC was switched on at high temperature, a connected fan did not start.

Axioline

Sporadically and in rare cases the Axioline local bus did not start. This has been observed mainly when a firmware 2021.6 or 2021.9 has been used and an Axioline Smart Element module was used as first Axioline module. Restarting Axioline did resolve the situation. This workaround is no longer necessary.

SPLC

AXC F 3152 with AXC F XT SPLC 1000:

– 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.

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.

PROFIBUS

AXC F 3152 with AXC F XT PB:

– When a configured PROFIBUS device could not be found during the system start, it was not indicated by the related PROFIBUS system variable. This could only be detected by a blinking LED of the AXC F XT PB.
– Connecting PROFIBUS system variables with GDS ports or global variables in PLCnext Engineer prevented the project from starting after download (connecting I/O process data with GDS ports or global variables worked). The error message “Failed to get buffer pointer from frame ...” was emitted to the “Output.log”.

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 occured 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.

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.

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

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 “AWqK” 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.

9 Changes in firmware version 2021.9.0

– 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.

9.1 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.

PROFIBUS

Support of the left-alignable PROFIBUS master extension module AXC F XT PB (item no. 1091657).

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.

9.2 Error corrections

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.

OPC UA

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

Network

The Ethernet network ports “X1” and “X2” were not completely independent in terms of gateway handling. Now the system supports multiple network interfaces on the same subnet mask without mutual influence.

9.3 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.
– 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;”).
– Reset to default setting type 2 can only be performed with a running Linux system. If a user makes changes in the overlayFS that leads to problems booting the system, resetting the device via the reset button is not possible.

Only known workaround: You can boot the controller with an external SD card, copy the overlayFS to this external SD card and delete the overlayFS on the controller after that.

- 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.

9.4 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?Set HttpsCertificateIdentityStore” 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.

10 Changes in firmware version 2021.6.0

- To be able to use all new functions of the firmware, you need PLCnext Engineer version 2021.6.0 or newer.
  Select the latest template for firmware version 2021.6.0 in the PLCnext Engineer project.
- The versions “TLS v1.0/v1.1” in the context of the web server are supported in this firmware version, but will be disabled in one of the future firmware versions. The deactivation may cause connection problems with old browsers. There are no effects on the TLS function block functionality.

10.1 New functions

WBM

- The WBM has been extended by a page to activate and deactivate “System Services”.
- It is now possible to edit the IP configuration via WBM. Therefore the former display page “Network Configuration” has been renamed to “Network” and was moved from the “Information” to the “Configuration” area. It depends on the user role whether the IP settings can be edited or only viewed.

SPNS

- Support of the left-alignable safety-related extension AXC F XT SPLC 1000 (order no. 1159811).

IEC 61131

- The data type WSTRING has been added for IEC 61131-3 applications programmed with PLCnext Engineer version 2021.3 (or newer). Correspondingly the data type StaticWString<> has been added in C++ as template class. This data type is supported by IEC Runtime, GDS, Data Logger, OPC UA Server and HMI.
- The new function block family UDP_SOCKET_2, UDP_SEND_2 and UDP_RECEIVE_2 supports sending of UDP broadcast datagrams.
  The new function block family TLS_SOCKET_2, TLS_SEND_2 and TLS_RECEIVE_2 supports programming a TCP/TLS server which can communicate with more than one TCP/TLS client at the same time. These function blocks can be used in combination with PLCnext Engineer versions newer than 2021.6.0.

GDS

The link ability between process data (Octet String) and variables of the user application was extended.

HMI

The PLC state “Force Mode” is now displayed by the “DBG” LED (debug LED) or a display flag. Besides debug states (e.g. triggered by breakpoints), the DBG LED (respectively its corresponding element on the touch screen display) now also shows when the variables are forced.

DataLogger

- The DataLogger has been extended: By specifying the name of an ESM task, the values of all configured variables will be sampled within this task. This concerns resource-global variables and component ports as well as variables instantiated within a program associated to any ESM task.
- The DataLogger supports the configuration for triggered data logging.

System

The binding of licences 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 (order no. 1151112)
- SD FLASH 32GB PLCNEXT MEMORY LIC (order no. 1151111)

PLCnext Store

PLCnext Store and app installation improvements:

- The installation of apps without reboot is supported.
- Apps can be downloaded with improved speed.

10.2 Changes

System

- Linux kernel was updated to version 5.4 LTS.
- “Paho” libraries were updated to the following versions:
  - paho-mqtt-c: 1.3.8
  - paho-mqtt-cpp: 1.2.0
- The PLC project download performance was improved.
- When setting the IP address, subnet mask or gateway, the value “255.255.255.255” is now rejected as invalid. Previously the firmware did not boot (a reset to default setting type 1 was required.)

10.3 Error corrections

The following errors have been rectified:

GDS/RSC

During the implementation of WSTRING, the behavior of the IGdsDataAccess service has been changed with regards to writing a value to a variable or port of data type STRING or StaticString<>. If in previous firmware versions the value was longer than the capacity of the variable/port, only as much bytes as provided by the variable have been copied. Additionally a warning message has been written to the Output.log file.
With firmware 2021.6 in this case the service method returns DataAccessError::StringLengthExceeds, no bytes are copied, and no warning message is emitted. The same handling has been implemented for data type WSTRING.

WBM

- A difference in the network configuration was not detected and displayed in the WBM if, for example, a change was made by a “DCP” configuration via network.
- The representation of hex values in the WBM was partially inconsistent.
- After an update from firmware versions 2020.6.x and older to firmware versions 2021.0.x, it was possible that the adopted WBM certificate could not be changed afterwards. A reset to default setting type 1 was necessary to be able to change the certificate.
- When setting a new user password in WBM, an erroneous error message occurred if the new password was entered first in the field “Confirm Password” and then in “New Password”.
- In the text field “Tip of the day” inconsistent use of punctuation marks occurred.
- In the text field “Edit System Use Notification” there was an inconsistent display of previously saved characters when editing again.

IEC 61131

- If an application was stopped by a breakpoint, the fieldbus process data could queue for one cycle when stepping on.
- The IEC 61131 runtime system could enter an undefined error state when downloading a PLC project that happened to use the same type names that were already used internally. This caused ambiguities. This applied, for example, to program/task/instance or function block names.
- In firmware versions 2021.0.x it could happen that after an update of older firmware versions the error message “Task 'Globals' already defined.” could occur when restarting the existing boot project. As a result, the project could not start properly due to an incompatible ESM configuration.
- The controller went into the FAIL state after frequent cold starts of the PLC project. Before each call of the OPC UA server, a warning from the root is displayed: “Enumerator: Too many open files”. After that a “CRITICAL” log from the OPC UA server is displayed.

PROFINET

- An issue that led to limited operation with certain PROFINET controller quantity structures was fixed.
- An incompatibility of Engineer apps with the possibility to switch off PROFINET controller/device was fixed. Inconsistency errors occurred when trying to switch off the PROFINET device only.
- When shutting down the system, internal thread exceptions could sporadically occur when terminating the process. This could cause the system to stop responding.

Network

In case the “dhcp” option was configured in the “interfaces” configuration file, it could happen that the manual “DHCP Gateway” setting was overwritten.

SDK/C++

It was not possible for the “StaticString” class to completely empty the contained pre-initialized “CHAR” array. With firmware 2021.6 the methods Clear() and IsEmpty() have been added.

System

- Starting with firmware versions 2020.9.x, numerous unhelpful logging outputs of the “rngd daemon” could occur in the log file “/var/log/debug”. This led to very large logging files.
- During the system startup, the PLCManager loads the projects and checks whether a system watchdog has occurred before the controller is started. If C++ programs or components are part of the project, their constructors are executed during the loading process of the PLC project. If the project was reloaded after a system watchdog has occurred, this could lead to repeated crashes and restarts that result in an endless loop.
- After setting PROFINET device diagnosis (SF LED on) the SF LED remained on, even if the diagnostic event was already completed and no longer pending.

– When restarting the controller, some informative messages were erroneously written to the log as type “ERROR”.

PROFICLOUD

– In case the PLC lost the connection to the internet, the link to Proficloud.io was not being re-established automatically. To return to online mode with proficloud.io, the PLC required a reboot or a restart of the ProficloudV3 services via WBM.
– If the connection to the Internet was lost, the WBM page of ProficloudV3 could not be accessed as long as the Internet connection remains lost.
– When writing log messages too quickly one after the other, it could happen that not all log messages were displayed in the cloud or some had the same timestamp.
– When a large number of data points could not be sent due to a network link failure, stopping of the TSD service was severely delayed.
– Sending significantly more than 50 configured data points could take an unexpectedly long time. With firmware 2021.6 the performance has been improved so that one PLC can send the values of up to 300 variables to the Proficloud.

OPC UA

– When an OPC UA client tried to call a function without required arguments, the PLC crashed.
– If an OPC UA client tried to browse an array of struct with children of kind array of primitive types where the index is out of range, the PLC could crash.
– Certain changes to security policies were applied only after a restart.

DataLogger

– During data logging in connection with the display of HMI data trend it could happen that memory was not released again.
– A “Download changes” command of the PLC project did not work if a “Rocks DB” session (HMI trending) of the DataLogger was active at the same time.

ESM

– Sporadically it could happen that a higher priority task together with a lower priority task on the same ESM core had a startup delay that should not have happened according to the priority.
– Sporadically, it could happen that when starting the PLC project, the task runtime was extended during the first cycle.

10.4 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.
– 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. The user does not receive a message that not all data can be saved.
- 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.
- 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.
- Reset to default setting type 2 can only be performed with a running Linux system. If a user makes changes in the overlayFS that leads to problems booting the system, resetting the device via the reset button is not possible.
  Only known workaround: You can boot the controller with an external SD card, copy the overlayFS to this external SD card and delete the overlayFS on the controller after that.

10.5 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

SSL

– CVE-2020-1971
– CVE-2021-3449
– CVE-2021-3450
– When updating the OpenSSL version from 1.1.1i to 1.1.1k in firmware version 2021.0.5, the “scrypt” function for generating hash values was no longer supported.

RAUC

– CVE-2020-25860

HTTP

– A DoS attack on port 80 using HTTP frames could lead to a real-time impact on the PLC runtime.
– CVE-2021-23017

WBM

– A XSS attack was reflected in a JSON response. This might leave content consumers vulnerable to attacks if they do not appropriately handle the data (response).
– A string entered in “Edit System Use Notification” could be executed on the login page of the controller.
– Cross-site scripting (XSS) exploitation could occur when setting the certificate for the Identity Store.

SNMP

– When reading out the “OID .1.3.6.1.2.1.2.1.6.0” via a MIB browser, the controller crashed.

System

– The “execute bit” of the PLCnext log files (and database files) was mistakenly set.
– When adding certificate lists via the WBM (create new trust store, upload certificate as file), it could happen that the controller crashed afterwards.
– When starting the operating system (or the “rngd“-service), the CPU usage consistently spiked to 100% for several seconds.
– CVE-2021-3156
– CVE-2020-8492

11 Changes in firmware version 2021.0.5 LTS

To be able to use all new functions of the firmware, you need PLCnext Engineer version 2021.0.2 LTS or newer.

Select the latest template for firmware version 2021.0.0 LTS in the PLCnext Engineer project.

11.1 Changes

System

"Paho" libraries were updated to the following versions:

– paho-mqtt-c: 1.3.8
– paho-mqtt-cpp: 1.2.0

11.2 Error corrections

The following errors have been rectified:

System

An unusually high amount of logging entries in the log file /var/volatile/log/auth.log could cause the system to crash after some time.

GDS

Firmware version 2021.0 LTS rejected a GDS connection between a port variable of a C++ component and a port variable of a program instance. As a consequence the program did not start.

PLCnext Store

If a controller has been updated from a firmware version older than 2020.3 to a firmware version 2020.3 or newer, the folder /opt/plcnext/config in the overlay partition sporadically got wrong access rights. As a consequence it was not possible to install licenses. In the past a reset to "Default setting type 1" had to be performed as workaround. Firmware version 2021.0.5 LTS corrects the access rights.

ESM

With firmware version 2021.0 LTS the execution of tasks sporadically did not obey the task priorities, when a code worksheet was displayed in the online mode of PLCnext Engineer.

11.3 Known limitations and errors

– The app "MQTT_Client_Library" version 2 (Build 20210205), which is available in the PLCnext Store, is not compatible with firmware version 2021.0.5 and will cause a system watchdog which reboots the controller. Please contact the contributor of the app (PLCnext Store) for any questions and potential fixes.
– In addition, the known errors and limitations from firmware version 2021.0.3 LTS also exist in this firmware version.
See section 13.3 "Known limitations and errors" on page 36.

11.4 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

SSL

– CVE-2021-3449
– CVE-2021-3450

RAUC

– CVE-2020-25860

12 Changes in firmware version 2021.0.3 LTS

All changes described in section 13 “Changes in firmware version 2021.0.2 LTS” on page 32 are also valid for this firmware version.

12.1 Error corrections

The following errors have been rectified:

System

The bug fixing of firmware version 2021.0.2 LTS concerning the logging of information into files located at “tmpFS” has been reworked. As of firmware version 2021.0.3 LTS the following applies:

Logging information into files located at “tmpFS” occupied too much RAM. Consequently the System Watchdog re-started the controller. Now the following files are regularly checked:

- /var/log/debug
- /var/log/error
- /var/log/messages
- /var/log/syslog
- /var/log/auth.log
- /var/log/kern.log
- /var/log/user.log
- /var/log/cron.log
- /var/log/btmp
- /var/log/wtmp

If one of the files is too large, it will be moved to the backup. The backups are located in the same folder and ”.1” is appended to the backup file name. This will overwrite existing backups.

13 Changes in firmware version 2021.0.2 LTS

To be able to use all new functions of the firmware, you need PLCnext Engineer version 2021.0.2 LTS or newer.

Select the latest template for firmware version 2021.0.0 LTS in the PLCnext Engineer project.

13.1 New functions

Articles

With this firmware version the following articles are supported for the first time:

– AXC F XT EXP (Order No. 1139999)

IEC 61131

– Backup and restore of GDS retain variables is supported.
– The priority of the Linux thread representing an ESM task of type “IDLE” has been increased. It is now just below the lowest ESM priority (15). This results in less jitter and faster execution of the associated program instances due to less interruptions.
As a consequence the IDLE task can now interrupt the “Globals” task which updates system variables and IEC 61131-3 resource global variables that are connected with I/O. To prevent this Phoenix Contact recommends to select appropriate “update tasks” in the PLCnext Engineer project.

WBM

– Security related product information is available via links in the “Help” menu in the header of the WBM and in the “Tip of the day” section on the start page.
– IO-Link diagnostic information is available in the Axioline tree view on the “Local Bus” page.
– The “System Use Notification” can be edited on the “User Authentication” page in the “Security” area.
– The “System Use Notification” is displayed when logging in to WBM or PLCnext Engineer.
– The HTTPS certificate can be configured on the “Web Services” page to avoid browser security warnings.

PROFINET

– The PROFINET controller and device can be enabled and disabled separately via configuration file.
– PROFINET controller certification according to PROFINET specification version 2.4.1 and Net Load Class II.
– PROFINET device certification according to PROFINET specification version 2.4.1 and Net Load Class II.

Proficloud

– Basic support of Proficloud V3 (firmware update from the cloud).
– “Proficloud V3 TSD service” is supported and replaces the “Proficloud TSD service”. Hereby the change from “www.proficloud.net“ to “www.proficloud.io” is necessary.

OPC UA

The following topics apply to projects created with PLCnext Engineer 2021.0 LTS for a controller of firmware 2021.0 LTS:

– The new security policies “AES 128 SHA256 RSA OAEP” and “AES 256 SHA256 RSA PSS” are supported. These policies can be selected in the OPC UA configuration.
– When the UA server checks the certificate of the connecting client, the “ApplicationURI” from the client's “ApplicationDescription” has to match to the “SubjectAlternateURI” in the client's certificate. This check is performed by default for new projects as well as when an older controller is replaced by a controller of firmware 2021.0 LTS in the PLCnext Engineer project. If necessary the check can be suppressed by deactivating the “Check application URI against client certificate” checkbox in the OPC UA configuration in PLCnext Engineer.
– When the UA server is configured to use a “self-signed” certificate, the trust store “OpcUA-configurable” is used. The client certificate is checked against the Trust List and the Certificate Revocation List is applied. This applies to new projects as well as when an older controller is replaced by a controller of firmware 2021.0 LTS in the PLCnext Engineer project. Previous versions used the trust store “Empty” as default and no client authentication was applied. If necessary the former default can be applied by deactivating the “Use the truststore for client authentication” checkbox in the OPC UA configuration in PLCnext Engineer.
– The “SubscriptionKind” can now be selected in the OPC UA configuration in PLCnext Engineer. The options “Direct Read”, “High Performance” and “Real Time” are available. “Direct Read” is set as default for new projects as well as when an older controller is re-

placed by a controller of firmware 2021.0 LTS in the PLCnext Engineer project.
The previous default “Real Time” can be selected if required.

PLCnext Store

Multiple controller types are supported in the app extension (“app_info.json”).
During the installation of the app, the extension checks if the version of the app is suitable for the controller used.

HMI

- Trending data services in interaction with the PLCnext Engineer HMI trending functionality are supported.
- Multiple project languages in interaction with PLCnext Engineer HMI language settings are supported.

Docker

For Docker support a possible co-existence of “iptables” and “nftables” is useful. Therefore the default firewall configuration has been adjusted.
The names of the following tables and chains have been changed:

Old name	New name
FILTER	**plcnext_filter**
input	**plcnext_input**
output	**plcnext_output**
basic_filter	**plcnext_basic_filter**
user_input	**plcnext_user_input**
user_output	**plcnext_user_output**

For compatibility with existing firewall configurations, the new settings also contain the old names as “deprecatedName”.

IO-Link

The IO-Link system integration refers to all types of IO-Link master modules from Phoenix Contact which can be driven by the PLCnext controllers via PROFINET or Axioline:

- AXL F IOL8 2H (Order No. 1027843)
- AXL SE IOL4 (Order No. 1088132)
- AXL F IOL8 2H (Order No. 1027843)
- AXL SE IOL4 (Order No. 1088132)
- AXL E PN IOL8 DI4 M12 6M (Order No. 2701519)
- AXL E PN IOL8 DI4 M12 6P (Order No. 2701513)
- IOL MA8 PN DI8 (Order No. 1072838)

Note: A support by PLCnext Engineer is planned for version 2021.3.

13.2 Error corrections

The following errors have been rectified:

WBM

- When displaying the network settings, an empty page could be displayed if a parameter could not be read. Now the page is displayed completely and affected parameters are shown as “N/A”.
- When adding a new user in the user administration, the entered password was not deleted if the process was cancelled with “Cancel”.
- When using the Internet Explorer for LDAP configuration, a new LDAP server entry could not be created successfully.
- Spelling mistakes in various messages of the WBM have been corrected.
- If an INTERBUS peripheral error occurred that was resolved and acknowledged by the application, the “Local Bus (Interbus)” page was not reset and the error was still displayed.
- After downloading a PLC project, the name of the project was not immediately displayed in the WBM. The page had to be refreshed in the browser by the user.
- After removing a previously detected fan module and displaying the current state on the “Fan Control” page, the WBM service failed.
- Conflicting error messages occurred when entering invalid characters on the “Certificate Authentication” page.

IEC 61131

- The system could sporadically crash during the “Write and Start Project Changes” process if the PLCnext Engineer HMI component was reading variables at the same time. This fix has the following effects on the “Write and Start Project Changes” process:
  - GDS: Services respond with status “CurrentlyUnavailable“
  - OPC UA: It is not possible to update values and browse variables
  - PLCnext Engineer HMI: Use replacement value “0“
- Exceptions in connection with managed C# code used in the PLC project were not handled correctly. This could cause the IEC 61131 runtime to stop responding.
  Now the exception is shown/listed including the call stack.

- An unexpected PLC task watchdog could occur in a low-priority task with a very long cycle time in connection with cold, warm and hot restart.
- When reading the eCLR error catalog with PLCnext Engineer, the firmware of the standard controller (SIGSEGV) could sporadically crash. This subsequently raised a software watchdog.
- After starting the PLC project, the system variables for the system time were only maintained with a delay. As a result, the value “0” was displayed for several cycles.
- PROFINET plug alarms could not be reported via the function block “RECV_ALARM”.
- The cyclical call of the function block “AR_STATISTIC” led to a very high system load up to the sporadic reduction of the PROFINET communication.
- When executing the function blocks “RDREC” and “WRREC” in fast succession, it could happen that the corresponding PROFINET AR was removed and the function blocks could not process any further services. Corresponding error messages were issued.

PROFINET

- Under various project conditions, PROFINET performance could deteriorate or unexpected connection failures could occur.
  Extensive PROFINET performance optimizations have been made to eliminate this behavior.
- When reading the PROFINET device of the controller via PLCnext Engineer, it could happen that the matching module “I/O 512” could not be determined.
- The system variable “PNIO_CONFIG_STATUS” did not match the documented behavior. The corrected behavior now shows the value 3 after a successful connection setup. Bit 0 (Ready) and Bit 1 (Active) are set.
- No more DCP or DCERPC frames were sent after changing the local date or time of the controller. As a result, PROFINET could not function properly.
- After a restart of the device by voltage reset it could happen that the PROFINET controller could not establish a connection to all PROFINET devices. This occurred when connecting with large numbers of PROFINET devices.
- Minor problems in the representation of device specific information via LLDP were solved.
- If autonegotiation of remote devices is deactivated, the default speed option of the interface is 100 Mbit half-duplex. In that case an existing PROFINET connection has not been aborted.

RSC

The RSC service “Write DeviceSettings” with the parameter “Rtc.Date” had not considered leap years and had rejected corresponding settings with “OutOfRange”.

Fan

- If a defective fan module was detected there was an inconsistent diagnostic state in the system variables and the information displayed in the WBM. The “FAN_MAINTENANCE” flag was not activated.
- During the fan diagnosis the state could be reached that no errors or warnings were generated although a detected fan was not rotating.
- In case of a blocked FAN (no rotation) a calibration with zero speed was still performed.

System

- When restarting the PLCnext firmware after a software reset, an exception could occur very sporadically. This meant that the firmware could not be started properly.
- Sporadically it could happen that a remoting based communication (such as that of PLCnext Engineer) could not be established if connection requests were already sent to the controller during the boot phase.
- During the reboot of the controller a system watchdog could occur very sporadically. Especially when triggering the reboot via SSH terminal the current retain data of the PLC project could be lost.
- An SD card that was removed during operation triggered a stop of the PLC project, although the support of an external SD card was deactivated in the WBM configuration.
- The status LED on the device was blinking with the wrong frequency in case of a removed external SD card. It has been corrected according to the description.
- If the SD card was removed during operation and then the supply voltage was disconnected, the device was operated with the internal voltage buffer until it was empty. This could take up to 30 seconds.
- Reading “Status.Memory.Usage.Percent” via RSC interface was only possible with the user role “Admin”.
- If an app with temporary data was installed but not started and then the controller was restarted, the folder previously created for the app was deleted. As a result, the app could not access the folder after starting.
- The cold start event task was no longer executed during a cold start of the PLC project if a change was previously made that caused a cold start (e.g. change of project name).

- The basic CPU usage of the system was improved.
- The default text of the “System Use Notification” was improved. The “System Use Notification” is displayed when logging in to the controller (e.g. WBM or PLCnext Engineer).
- The file name of the firmware update container was changed.
  Now the complete firmware version is considered.
- Under rare conditions a power failure could result in retain values not being saved. When the voltage returned, older retain values were used. Now in these cases a cold restart is performed.
- Logging information into files located at “tempFS” occupied too much RAM. Consequently the System Watchdog restarted the controller.
  Now the following files are regularly checked:
  - /var/log/debug
  - /var/log/error
  - /var/log/messages
  - /var/log/syslog
  - /var/log/auth.log
  - /var/log/kern.log
  - /var/log/user.log

  If one of the files is too large it will be moved to the backup. This will overwrite existing backups.
- With firmware version 2021.0 LTS a reset to “Default setting type 1” was not possible when executed by pressing the reset button of the controller.

OPC UA

- With certain method calls the status “Bad” of the OPC UA server could occur during download changes of the PLC project.
- Due to an unfavorable startup sequence of the OPC UA component it could happen that certain alarms could not be detected in time.
- Browsing from a node to a child node and back did not work.
- When a value which shall be written to a STRING variable exceeds the maximum length of this variable, then writing is rejected with the error code “Bad_OutOfRange”.
  In previous versions the UA server truncated the value to the maximum length of the variable.

Docker

Firewall support for NAT (Network Address Translation) was not available. Options like "CONFIG_NFT_MASQ_IPV4" were not supported by this.

Axioline

If an Axioline bus contained a power terminal and a Smart Elements module with empty slots, the bus did not re-start after a power failure.

SDK/C++

The SDK related to firmware version 2021.0 LTS redefines the “std::make_unique” function, thus creating a conflict when compiling existing code.
Use the SDK related to firmware version 2021.0.2 LTS instead.

Network

- In case the "dhcp" option was configured in the "interfaces" configuration file, it could happen that the manual "DHCP Gateway" setting was overwritten.
- The Ethernet connection froze after a few minutes when the controller is connected to another port that is configured to 100 Mbit full-duplex without autonegotiation.

13.3 Known limitations and errors

- 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 a dedicated state of the retain values can be restored from a backup.
- Retain handling
  With extended retain handling in the context of this firmware, the retain variables are reinitialized by a cold start when downgrading to firmware 2020.3 or older. A previous saving of the retain variables by the user is not supported with firmware 2020.6 and older.
- Retain variable behavior in case of firmware downgrade
  If firmware 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.
- PLCnext CLI version
  The PLCnext CLI version used must match the current SDK for this version. Downward compatibility cannot be guaranteed.
- 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**
- Firmware downgrade
  After downgrading the firmware, it is recommended to reset to “Default setting type 1”. This is not necessary when updating the firmware.
- Firmware startup
  If the PLCnext system firmware has not started up properly, the WBM displays the error message “Bad Gateway 502”.
- Task name
  If “Event”, “EventTask” or “Globals” is used as the name of a task, an error condition of the controller occurs when the project is downloaded.
  This is because “Event”, “EventTask” and “Globals” 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.
- HMI pages during program downloads
  During a PLCnext Engineer program download (both total and changes), the web server returns an error 503 (busy) for requests to the HMI pages.
- Multiple DataLogger Sessions
  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. The user does not receive a message that not all data can be saved.
- 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.
- Crash during startup phase
  The system watchdog is not yet active during the startup phase if you start C++ extensions very early. If the user code causes a crash during this phase, this can lead to an endless boot loop.
  You can solve the problem by removing the SD card before rebooting.
- 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.
- “Download Changes“
  Sporadically a PLCnext Engineer project may reject “Download changes” without giving a reason.
- Uninstalling Solution Apps
  When a Solution App is uninstalled by the PLCnext Store, it can happen that the controller then no longer reacts to any actions by the PLCnext Store, although it reports the status “online”. A system watchdog was also sporadically observed. This behavior has not been observed when using the offline deactivation in the WBM for uninstalling a solution app.

- LAN gateway settings
  If there are several “Default Gateway” settings, only the setting of the first network interface is applied. The settings of other LAN adapters are ignored. Only one “standard gateway” is supported internally.
- Local time zone setting
  Setting local time zones is not fully supported.
- “DBG” LED
  The “DBG” LED should signal if a variable has been set via forcing in debug mode in the PLC project.
  This behavior is currently not supported. Despite forcing the variable, the “DBG” LED remains off.
- Firmware update
  The firmware update removes the following files so that the contents are lost:
  - /opt/plcnext/projects/Default/Plc/Eclr/Default.eclr.config
  - /opt/plcnext/projects/Default/Plc/Gds/Default.gds.config
  - /opt/plcnext/projects/Default/Plc/Meta/Default.meta.config
  - /opt/plcnext/projects/Default/Plc/Plm/Plm.config
  - /opt/plcnext/projects/Default/Plc/Esm/Default.esm.config
  - /opt/plcnext/projects/Default/Plc/Esm/ServiceTask.esm.config
  - /opt/plcnext/projects/Default/Plc/Esm/Globals.esm.config

  These files are not edited by PLCnext Engineer nor are they intended to be modified by the user.

13.4 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/
- https://cert.vde.com/de-de.

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

WBM

- CVE-2020-12517

System

- CVE-2020-12518

Shell

- CVE-2020-12519

LLDP

- CVE-2020-12521

SSL

- CVE-2020-1971

SNMP

- The SNMP “Get” call of “OID .1.3.6.1.2.1.2.2.1.6.0” for network interface used as PROFINET controller or device caused the firmware to crash.

14 Changes in firmware version 2020.6.2

To be able to use all new functions of the firmware, you need PLCnext Engineer version 2020.6.

Select the latest template for firmware version 2020.6.2 in the PLCnext Engineer project.

14.1 New functions

WBM

The connection to existing LDAP(S) servers can be configured in WBM.

GDS

Enhanced Retain Handling:

When changes to retain variables are transferred to the controller via “Download All”, no implicit cold start is performed. As many retain values as possible are retained. This behavior of the retain variables corresponds to the “Download Changes” behavior, where all variables are retained even if the project is changed at runtime.

To avoid data inconsistencies with retain variables, the retain variables are always initialized by an implicit cold start after a project change (project name). In the previous firmware versions a warm start was only carried out if the retain variables were exactly the same.

IEC 61131

- Improvement of jitter and latency for programs with IEC 61131 or C# context..
- New system variable “USER_PARTITION” to display the load of the user partition with the following elements:
  - MEM_TOTAL
  - MEM_FREE
  - MEM_USED
  - MEM_USAGE

PROFINET

Support of Fast Startup (FSU) by the PROFINET controller (up to 24 FSU devices).

OPC UA

- User comments on the confirmation and acknowledgement of alarms via OPC UA are supported. The comments are also entered in the “Notification Logger”.
- Basic support for loading new user-specific information models into the OPC UA server.

DataLogger

New RSC-API “IDataLoggerService2” for application of the DataLogger. The triggered logic analysis in PLCnext Engineer is based on this API.

Network

- Support of the “NetLoadLimiter” functionality.
- Support of a DHCP basic functionality for IP address allocation.

SDK/C++

The GCC compiler has been updated from version 8.3 to version 9.3. All newly created applications are now compiled on this basis.

14.2 Error corrections

The following errors have been rectified:

WBM

- The call of WBM pages could sporadically lead to a PROFINET connection termination.
- When configuring new firewall rules in WBM, not all available network interfaces were displayed.
- There was no character limitation when entering user or password. After 64 or 128 bytes the input string was cut off without error message.
- A notification field of a message was displaced in the “Notifications” menu when switching languages.
- Certain UTF-8 special characters could not be entered in the “Username” input field in the “User Authentication” menu.
  An empty error message was displayed.
- In the “Certificate Authentication” menu, the key type “RSA TPM 2048” was displayed in the “Add Identity Store” entry by mistake.

IEC 61131

- A “Fatal Exception” could occur if the project was to be restarted after debugging the project while following a certain procedure.
- If a PLCnext Extension component (ACF or PLM) or a PLCnext Engineer Shared Native Library was to be linked against a non-existent “shared object library”, a crash could occur.
- From this version on, the block “RTC_S” returns the local time, provided a time zone with root rights has been set before.
  In previous versions, the UTC time was always returned.

DataLogger

- The project could not be loaded if an exception was thrown due to too many configured variables in a DataLogger session.
  In this case the notification “Arp.Services.DataLogger.Error” is now displayed. The project is loaded without starting the incorrectly configured DataLogger session.
- The firmware could not be accessed if the parameter “maxFileSize” was too large during a DataLogger session that writes to a volatile sink.

PROFINET

- When loading projects that were created with PLCnext Engineer 2020.3, a notification “Arp.Io.PnC.ConfigurationWarning” with the severity “Warning” can be triggered. The PayLoadString is “Parsed FSParameterUUID '{}' has invalid format. Parameter will be ignored. Please check engineering and/or device description”.
  This problem has been fixed in PLCnext Engineer 2020.6 or later.
- The PROFINET connection setup could take a relatively long time if many nodes were used.
- The PROFINET controller could only process 10 RPC requests at a time. So far “nca_server_too_busy” was reported back to the PROFINET devices. Some devices did not repeat their RPC request.
  The PROFINET controller can now accept up to 45 RPC requests simultaneously.
- The controller sporadically had incorrect IP settings after a DCP factory reset was requested by the higher-level PROFINET controller.

GDS

- In case of fatal error (e.g. SIGSEGV) in a C++ program, a system watchdog could be triggered cyclically. Under certain circumstances this could also be caused by a faulty GDS configuration.
- When using the Write functions of the “IDataAccessService” RSC service, the variable could not be overwritten correctly if the data type of the overwrite value did not match the data type of the variable to be overwritten.

RSC

When using certain RSC services simultaneously, an exception in “CommonRemoting” or a “Protocol violation” ERROR could occur.

Fan module

- A connected fan module was not detected if the rotor was stationary or blocked.
- The timestamp of the fan calibration in the WBM and in the Output.log now shows the minutes with leading zeros (the minutes 0 to 9 after the full hour). This increases the readability and clarity of the time stamp.

ESM

In rare cases the detected watchdog of an ESM task was not handled correctly. Thereupon the firmware was terminated.

System

- During system startup, a system watchdog could be triggered if, for example, a higher-level PROFINET controller changed the IP settings via DCP protocol.
- With the C++ function “Directory::Clear(path)” from the namespace “Arp.System.Commons.Io” a directory could not be cleared as long as it was viewed with WinSCP.
- Names of NTP servers could not be set if they contained more than 2 dots.
- Under certain operating conditions cyclic error messages were entered in conjunction with LLDP. These messages are not errors and were therefore reclassified as debug information.
- When setting the IP address via DCP, an error message was erroneously entered in the “Output.log”, although the setting was successful.

Docker

An issue related to calling the Docker “exec” command to install or configure a Docker Container was fixed. So far only the Docker “run” command could be used.

14.3 Known limitations and errors

- 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.
- PLCnext CLI version
  The PLCnext CLI version used must match the current SDK for this version. Downward compatibility cannot be guaranteed.
- 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**
- 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. In general, when DHCP is switched on, the current IP settings are not yet displayed in the WBM and on the display, but the static settings last set are displayed.
- Retain handling
  With extended retain handling in the context of this firmware, the retain variables are reinitialized by a cold start when downgrading to firmware 2020.3 or older. A previous saving of the retain variables by the user is currently not supported.
- 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.
- HMI pages during program downloads
  During a PLCnext Engineer program download (both total and changes), the WebServer returns an error 503 (busy) for requests to the HMI pages.
- Multiple DataLogger Sessions
  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. The user does not receive a message that not all data can be saved.
- 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.
- SDK
  The SDK only works with PLCnext CLI 2020.0 or later, not with older versions (both PLCnext CLI 2019.x and PC WORX Target for Simulink 2019.x).
- If the controller is rebooted using the Linux command “sudo reboot” or the RSC service “IDeviceControlService::RestartDevice()” (also used by the “Reboot” button in the PLCnext Engineer cockpit), a system watchdog may occur in rare cases. This means that only a cold start is possible when the controller is subsequently booted, i.e. all retain variables are reinitialized.
  This behavior does not occur when the operating voltage is switched off and then booted.
- Voltage buffer
  If the SD card is removed during operation and then the supply voltage is disconnected, the device will operate with the internal voltage buffer until it is discharged. This can take up to 30 seconds.
- Crash during startup phase
  The system watchdog is not yet active during the startup phase if you start C++ extensions very early. If the user code causes a crash during this phase, this can lead to an endless boot loop.
  You can solve the problem by removing the SD card before rebooting.
- PROFINET name
  If firmware 2020.6 is downgraded to an older version, the PROFINET name is lost.
- Debugging of IEC 61131 code
  When debugging IEC 61131 code with activated breakpoints, display errors may occur in the call sequence function and variable contents.
- “Download Changes“
  Sporadically a PLCnext Engineer project may reject “Download changes” without giving a reason.
- RTC setting
  After setting a local time zone, unexpected results may occur when reading out times from different contexts (RTC-S FB, OPC UA, SPNS LOG).
- Restriction for Device Info service
  The “DI - Device Info - Status.Memory.Usage.Percent”

service no longer returns a value with the following roles:
  - “Engineer“
  - “Commissioner“
  - “Service“
  - “DataViewer“
  - “DataChanger“
  - “Viewer“
  - “UserManager”
- Controller in error state
  When using “Event” as name of a program, an error condition of the controller occurs when downloading the project. “Event” is already used internally as class name.
- Firmware downgrade
  After downgrading the firmware, it is recommended to reset to “Default setting type 1”. This is not necessary when updating the firmware.
- Bus behavior after power failure
  If an Axioline bus contains a power terminal and a Smart Elements module with empty slots, the bus will not restart after a power failure.
- Uninstalling Solution Apps
  When a Solution App is uninstalled by the PLCnext Store, it can happen that the controller then no longer reacts to any actions by the PLCnext Store, although it reports the status “online”. A system watchdog was also sporadically observed. This behavior has not been observed when using the offline deactivation in the WBM for uninstalling a solution app.
- Task watchdog
  A task watchdog may sporadically occur with a low-priority PLC task with a cycle time in the range of seconds if the running PLC project was stopped and immediately restarted with a cold/warm/hot start.
- Gateway settings LAN2 and LAN3
  If there are several “Default Gateway” ” settings, only the setting of LAN1 is used. The settings of other LAN adapters are ignored.

14.4 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/
- https://cert.vde.com/de-de.

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

OpenSSL

- CVE-2020-1967

Python

- CVE-2020-8492

System

- Activation of security-relevant compiler flags (e.g. to prevent unauthorized introduction of executable code).
- Correction of a problem that RSC-Services of fieldbus components could be used without authentication.

OpenSSL

- The outdated OpenSSL version 1.0.2 is no longer supported. Instead, the current OpenSSL version 1.1.1 is used.