AXC F 2152 – CHANGE NOTES

Change notes for the AXC F 2152 controller

Application note
108427_en_44

1 General information

This document contains all changes made between firmware version 1.0.0 and the current firmware version of the AXC F 2152 controller (item no. 2404267).

Current firmware version: **2024.6.0**

Observe the following general notes:

Toolchain

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.

Material damage due to a freezing of the outputs

With firmware versions 2019.6, 2019.3, or 2019.0 LTS, a high CPU load in conjunction with frequent PROFINET disconnections may cause the outputs of the Axioline local bus to freeze.

Make sure to perform an update to firmware version **2019.0.4 LTS**, **2019.6.3** or **2019.9** or higher.

Firmware update

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 2152” on page 3 to see on which release branch your firmware version is located and which features, changes, error corrections, and security updates your firmware version contains.

Documentation

- Make sure you always use the latest documentation. It can be downloaded at phoenixcontact.net/product/2404267.
- Further information on the PLCnext Runtime and programming can be found under plcnext.help
- Further information on security in the context of PLCnext Technology can be found under security.plcnext.help

Firmware version

Product revision VC 19 of the controller is delivered with firmware version 2024.0.8 LTS.

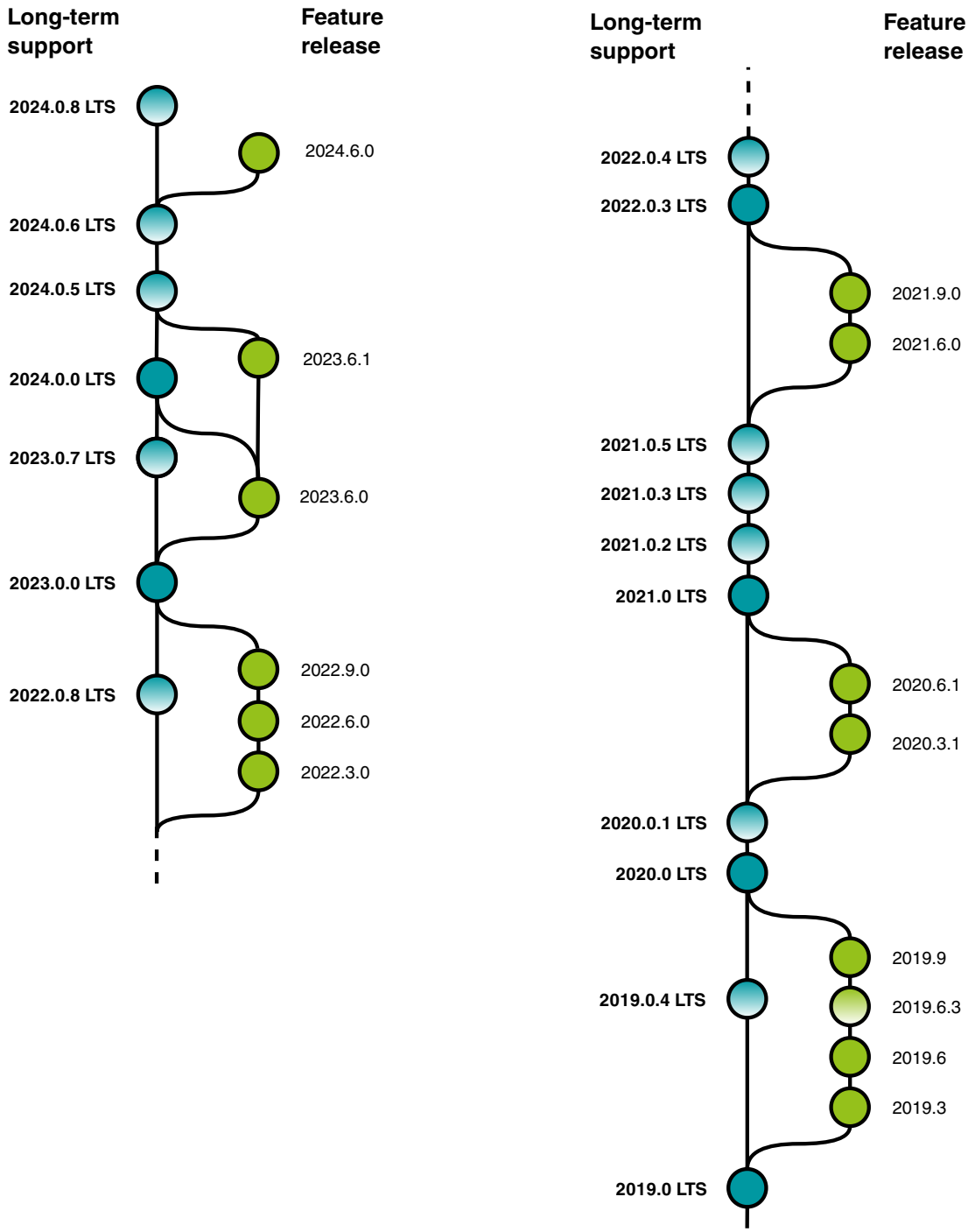
1.1 Maritime approvals

The following firmware versions are certified for use in maritime applications:

- 2024.0.0 LTS
- 2023.0.0 LTS
- 2022.0.4 LTS
- 2022.0.3 LTS
- 2021.0.3 LTS
- 2020.0.1 LTS
- 2020.0 LTS
- 2019.0.4 LTS
- 2019.0 LTS

2 Table of contents

3 Firmware releases AXC F 2152



4 Changes in firmware version 2024.6.0

To be able to use all new functions of the firmware, you need PLCnext Engineer version 2024.6 or newer.
Select the latest template for firmware version 2024.6 in the PLCnext Engineer project.

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

If you use a left-alignable functional safety extension module with your controller, the following safety-related firmware versions must be used:

- AXC F XT SPLC 1000: **01.01.0000**
- AXC F XT SPLC 3000: **02.10.0006**

This section describes changes made between firmware version 2024.0.6 LTS and firmware version 2024.6.0.

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

4.1 New functions

Configurable alarms

When configurable alarms (as defined in PLCnext Engineer) are confirmed or acknowledged via REST API a comment can be specified optionally. The alarm stores the latest comment. Specifying no comment keeps the previous comment, specifying an empty comment removes the previous comment.

Modbus TCP client

In combination with PLCnext Engineer 2024.6 (or newer) the firmware supports an Modbus TCP client. This client can be configured using PLCnext Engineer.

As factory default setting, the feature Modbus TCP client is deactivated. If necessary it can be activated via the WBM page “System Services”.

OPC UA

The OPC UA client delivers diagnostic information. This information can be retrieved from the OPC UA server:
For each client connection there is one node (with child nodes) under Root.Objects.DeviceSet.<PLC-type>.eUAClient.Connections, where <PLC-type> is the type name of the PLCnext Control device (e.g. “AXC F 2152” or ”RFC 4072S”). These nodes belong to the newly introduced namespace “urn:<node-name>:PhoenixContact:eUAServer/eUAClient/” where <node-name> is the name configured for the OPC UA server.

4.2 Changes

OPC UA client

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

OPC UA server

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

PROFINET

- In case of factory defaults behavior the PROFINET names of the PLC have been changed. In the past the name “pnc” indicated PROFINET controller and “pnd” indicated PROFINET device function. As this is ambiguous for ETH adapters which support both functions now the name of the ETH adapter became part of the PROFINET name. The names have been changed:
  - LAN1: From “axcf2152-pnd” to “axcf2152-lan1”
  - EXTLAN (AXC F XT ETH 1 TX): From “axcf2152-pnc” to “axcf2152-extlan1”
- The PROFINET controller stack had to be adapted to the increased requirements of the PROFINET certification test, resulting in an increased CPU load in ESM 1. In exceptional cases, this can lead to a task watchdog in PLC projects with many PROFINET connections and tightly set ESM task watchdog times.

4.3 Error corrections

Axioline

The following error occurred in combination with a connected Axioline bus that contained a power module (e.g. “AXL F PWR 1H”) and right-hand-side an Axioline SE module carrier with at least one empty slot. If in this case the bus power was lost, the Axioline bus was not set to operation entirely after power return.

Configurable alarms

When a “ConfirmAlarm” or “AcknowledgeAlarm” was processed and Authentication was used by the project, the

alarm server was not setting the user field to the user name of the currently logged in user if the call succeeds.

HMI

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

Network

If the PROFINET controller or the PROFINET device was deactivated via the system management for the purpose of IP address assignment via DHCP for the corresponding interface, the system crashed when the firmware was restarted.

OPC UA client

- The OPC UA client did not handle its subscriptions correctly when the OPC UA server was shut down (e.g. due to a “Write and start project” command in PLCnext Engineer). Therefore, the firmware was terminated due to a segmentation violation (SIGSEGV) or the configured local variables were no longer updated. Both effects occurred sporadically.
- The OPC UA client did not check whether certain write operations were successful. After a connection loss this sometimes led to longer periods of time in which the values of the variables in the OPC UA client did not match the values in the OPC UA server, even if the connection had been re-established for some time.

OPC UA server

During data access via OPC UA and the simultaneous execution of a PLC state transition, an unexpected exception could occur sporadically. The OPC UA server is now synchronized against these PLC state transitions.

Proficloud

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

PROFINET

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

PROFINET device

- If the PROFINET device was requested to reset its settings to factory defaults via DCP (e.g. using “NetNames+”), a connection to the PROFINET device was not possible. A reboot was necessary.
- PROFINET System Redundancy: When the primary PROFINET controller has already established an AR to the built-in PROFINET device of the PLCnext Control device and now the backup PROFINET controller established its AR, an unnecessary alarm has been sent to the primary controller indicating return of submodule.

SPLC

When using an “AXC F XT SPLC 1000” or “AXC F XT SPLC 3000” left-alignable safety-oriented extension module and the CPU load of the PLC was high, it could happen sporadically that running PROFINET connections could not be kept stable.

4.4 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.

4.5 Security updates

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

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

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

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

Git

– CVE-2024-32002

OpenSSH

– CVE-2024-6387
– CVE-2024-39894

OpenSSL

– CVE-2023-5678
– CVE-2024-0727
– CVE-2024-2511
– CVE-2024-4741
– CVE-2024-4603

LibSSH2

– CVE-2023-48795

Network

– A weakness in network robustness in case of a DoS attack has been fixed.
– A system watchdog in combination with TCP network load on two interfaces simultaneously with active NetloadLimiter has been fixed.

5 Changes in firmware version 2024.0.8 LTS

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

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

If you use a left-alignable functional safety extension module with your controller, the following safety-related firmware versions must be used:

- AXC F XT SPLC 1000: **01.01.0000**
- AXC F XT SPLC 3000: **02.10.0006**

This section describes changes made between firmware version 2024.0.6 LTS and firmware version 2024.0.8 LTS.

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

5.1 Error corrections

ANSI C

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

System watchdog

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

5.2 Known limitations and errors

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

5.3 Security updates

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

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

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

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

Nano

- CVE-2024-5742

OpenSSL

- CVE-2024-5535
- CVE-2024-6119

Python

- CVE-2024-6232
- CVE-2024-7592

SSH

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

6 Changes in firmware version 2024.0.6 LTS

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

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

If you use a left-alignable functional safety extension module with your controller, the following safety-related firmware versions must be used:

- AXC F XT SPLC 1000: **01.01.0000**
- AXC F XT SPLC 3000: **02.10.0006**

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

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

6.1 New functions

SDK

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

6.2 Error corrections

PLCnext Apps

The PLCnext App “CODESYS Control for PLCnext SL” could not access Axioline I/O with firmware versions 2024.0.0 to 2024.0.5. This bug has been fixed.

PROFINET

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

TLS2 FB

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

OPC UA client

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

OPC UA server

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

6.3 Known limitations and errors

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

6.4 Security updates

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

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

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

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

Git

– CVE-2024-32002

OpenSSH

– CVE-2024-6387
– CVE-2024-39894

OpenSSL

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

SD card

With firmware versions from 2024.0.0 LTS to 2024.0.5 LTS the notification “Security.Arp.Device.Interface.SdCardStatusSet” was not emitted when the support of the external SD card was activated or deactivated on the WBM page “SD Card”.

7 Changes in firmware version 2024.0.5 LTS

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

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

If you use a left-alignable functional safety extension module with your controller, the following safety-related firmware versions must be used:

- AXC F XT SPLC 1000: **01.01.0000**
- AXC F XT SPLC 3000: **02.10.0006**

This section describes changes made between firmware version 2024.0.0 LTS and firmware version 2024.0.5 LTS.

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

7.1 Changes

WBM

The WBM page “Security - SD Card” cannot be accessed and operated by the user role “Engineer”. It turned out that it is sufficient when roles “Admin” and “SecurityAdmin” can access and operate this WBM page.

7.2 Error corrections

ANSI C

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

Alarms

A memory leak has been fixed in the alarm server. This leak could occur when alarms were viewed in the eHMI and the browser was closed abruptly (without deleting the created alarm subscription).

HMI

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

Network

In combination with AXC F XT ETH 1TX:

When DHCP was enabled for an ETH port and there was no link when the PLC booted, the PLC did not send any DHCP requests. This has not been observed for ETH ports with an integrated switch.
Note: DHCP is only possible for ETH adapters without activated PROFINET function.

OPC UA client

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

OPC UA server

Very sporadically a SIGSEGV (segmentation fault) could occur which led to a system watchdog. The stack trace in the Output.log file indicated that one or more methods of the class “Arp::Services::OpcUAServer::Internal::InformationModel::Common::SampleGroup” was involved. In many cases this error occurred when variables have been removed from or added to the list of monitored items, where in parallel other clients created or freed OPC UA sessions. The longer the list of monitored items, the more likely it was that the error occurred.
This known issue has been fixed.

Safety

In combination with an AXC F XT SPLC 1000 or AXC F XT SPLC 3000, a safety-related process data output can be connected to both a safety-related variable and a standard variable. In this case the value of the safety-related variable is copied to the safety-related process data output as well as to the standard variable. With firmware version 2024.0.0 LTS the value was copied to the safety-related process data output but not to the standard variable. For this firmware version the following workaround can be used: Create an additional safety-related variable in the safety program and assign the value of the already existing safety-related variable. In PLCnext Engineer remove the connection to the standard variable and create a new connection from the added safety-related variable to the standard variable.
This known issue has been fixed.

7.3 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.

8 Changes in firmware version 2024.0.0 LTS

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

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

If you use a left-alignable functional safety extension module with your controller, the following safety-related firmware versions must be used:

- AXC F XT SPLC 1000: **01.01.0000**
- AXC F XT SPLC 3000: **02.10.0006**

This section describes changes made between firmware version 2023.6.0 and firmware version 2024.0.0 LTS.

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

8.1 New functions

DataLogger

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

GDS

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

IEC 61131

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

Licenses

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

Proficloud

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

SD card

“Reset to default settings” can be configured to set the (external) SD card as enabled. This can be configured at the WBM page “SD card”. In previous firmware versions “reset to default settings” did not change the enabled/disabled state of the (external) SD card.
Note: The activation of the “Security Profile” implicitly disables the (external) SD card and configures “reset to default settings” to keep the enabled/disabled state.

Security

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

System

- If a system watchdog (SWD) occurs due to a fatal error that has caused a PLCnext process to die, the following files are saved before the system is rebooted:
  - reason.log
  - kernel.log
  - sys.log

  If an LTTNG session is active, its trace is saved, too. These files are saved to the folder */opt/plcnext/watchdogDaemon/[timestamp]* where *[timestamp]* is created from the time at which the SWD occurred. If more than 3 SWD occur, the oldest folder will be removed. If the PLC is rebooted due to the

hardware watchdog reset, it is not possible to save these files. This can happen if the hardware watchdog is no longer triggered by the firmware, for example due to a heavy, high-priority load on the system.

– In combination with firmware 2024.0 LTS (or newer), PLCnext Engineer (2024.0.1 LTS or newer) supports configurable alarms.
– Changes of PLC states are serialized and dedicated state transitions can be monitored with a timeout. This prevents from scenarios in which a low-priority task requests to change the PLC state (which can also occur implicitly, for example by calling the "RestartDevice()" method of "IDeviceControlService") while the PLC Manager is performing another state transition (for example from "PlcState::Running to PlcState::Stop").

WBM

The WBM page "Security - SD Card" can be accessed and operated by the user role "Engineer", too. This became necessary by the optional encryption of the SD card.

8.2 Changes

Linux

– The OpenSSL library has been updated to version 3.0. The PLCnext firmware uses this version only. For compatibility reasons the previous OpenSSL library (version 1.1.1) still exists in the file system. As this version is outdated, it will be removed in one of the next firmware releases. For applications (including PLCnext Apps) which use the OpenSSL library, an update is recommended as soon as an application version is available, which uses OpenSSL 3.0.
– LTTng has been updated to version 2.13.9 and there has been a significant change in the "lttng-ust" (LTTng user space tracing). If an application/library is instrumented with LTTng user space tracing and has been compiled without using the "ArpTracing.cmake" support of the LTTng user space tracing in PLCnext SDK (available since FW 2022.6), the instrumented application/library cannot be loaded any longer by the firmware ("undefined symbol" is reported in Output.log). In that case the instrumentation of LTTng user space tracepoint in the application/library has to be changed to use the "ArpTracing.cmake" support of the PLCnext SDK and it needs to be recompiled. Matlab Simulink applications, which use the "PLCN_EnableLTTNG" compile option, have to be compiled with PLCnext Target for Simulink v2.3 or newer.
– Library "paho-mqtt-c" has been updated to version 1.3.13.

OPC UA

– The OPC UA client and server use the OpenSSL library to validate X.509 certificates using the OpenSSL flag X509_V_FLAG_X509_STRICT. As firmware 2024.0 LTS is updated to OpenSSL 3.0, the X.509 certificate validation became more strict, especially for non self-signed certificates. This may cause the server to return the error "BadSecurityChecksFailed" on client connection attempts. Make sure that, according to OPC UA Part 6, client issuer as well as client application X.509 certificates are conform to RFC 5280, especially to the sections listed below. This applies to self-signed certificates as well as user-managed certificates.
  – 4.1.1.2 signatureAlgorithm
  – 4.1.2.6 Subject
  – 4.2.1.1 Authority Key Identifier
  – 4.2.1.2 Subject Key Identifier
  – 4.2.1.3 Key Usage
  – 4.2.1.6 Subject Alternative Name
  – 4.2.1.9 Basic Constraints
– In the NamespaceArray of the OPC UA server the index of namespace http://phoenixcontact.com/OpcUa/PubSubConfiguration has changed from index 8 to index 2. This namespace is optional and it appears only if the feature "OPC UA PubSub" is activated on the WBM page "System Services". Currently the firmware does not provide anything in that namespace, it is only a preparation for future extensions.

8.3 Error corrections

Axioline

Some Axioline modules (for example analog outputs) provide status information in their process data. In case of a module error (for example loss of power supply) these process data inputs are filled with an error code. However, in certain situations these process data inputs returned "0" instead of the error code. This error has been corrected. Only process data inputs of modules connected to the controller's local bus have been affected. Not affected are retrieving module errors via PDI request as well as displaying these errors at the WBM page "Diagnostics - Local Bus".

ESM

- If two ESM tasks cause a task watchdog at (nearly) the same time, the event task “Arp.Plc.Esm.OnException” was executed twice. Additionally, the PLC was attempted to be stopped twice in parallel. This failed and the PLC had to be rebooted. This error has been corrected and the event task as well as the PLC stop is now executed only once.
- In some situations calling the function block “GET_EXCEPTION_INFOS” in the event task “Arp.Plc.Esm.OnException” caused an exception. This has been fixed. In additon to update to firmware 2024.0 LTS or newer, the PLC project has also to be re-compiled using PLCnext Engineer 2024.0.1 LTS or newer.
- In combination with PLC IDLE task and Axioline configured to use that IDLE task as “Trigger Task”, the PLC project stops after some time due to a task watchdog. After that the PLC had to be rebooted.

EtherNet/IP

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

GDS

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

IEC 61131

- When breakpoints are set in the IEC 61131-3 program, the “PlcState::Debugging” flag was reset in the transition from “PLC STOP” to “PLC HOT START” and then set again when changing from “PLC Running” to “Debugging”. The fieldbus output values could be switched on again for a short time period when the PLC was in the state “Running”.
- “Download Changes” (“Write and Start Project Changes” in PLCnext Engineer) implicitly creates a backup of the current project. If “Download Changes” is not possible (for any reason), the current project is restored from this backup. If “Download All” (“Write and Start Project” in PLCnext Engineer) is performed immediately after a rejected or failed “Download Changes” attempt, the PLC is reset. Resetting conflicted with restoring and ended in an I/O exception. The firmware now keeps the state flag “Running | DcgNotPossible” until the restoring process has been finished. Depending on the project size, the restoring process may take several seconds. Note that PLCnext Engineer 2023.9 (or newer) checks this state before it offers the “Download All” option.
- In case of large projects and an extensive use of certain firmware function blocks, an exception could occur after a “Download Changes” attempt (“Write and Start Project Changes” in PLCnext Engineer). The following is reported in the Output.log: “SetupPlc(changing) with out of memory error - GC heap of the application domain”. The firmware function blocks have been updated in PLCnext Engineer version 2023.0.6 LTS and in 2024.0 LTS (or newer).
- An exception after “Download Changes” (“Write and Start Project Changes” in PLCnext Engineer) has been triggered if the function block “AR_STATISTIC_ITERATE” was enabled and generated new values. To fix this bug, re-compile and download the project using PLCnext Engineer 2024.0 LTS (or newer).
- In the function “MOVE” that is used with the function “EN/ENO”, a value of a multi-element-variable was assigned to a wrong address. To fix this bug, re-compile and download the project using PLCnext Engineer 2024.0 LTS (or newer).
- In a C# eCLR Library the runtime created a vectored exception when calling “File.Exists(null)”.

OPC UA client

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

OPC UA server

- A fatal exception could occur if “IndexRange” is used when accessing a variable that is not of type array or of type string.
- After the OPC UA server started with a changed project the server might return “BadNodeIdUnknown” when a client tried to continue monitoring an existing subscription item.
- Subscriptions did not work after a warm or cold start with project changes.
- A sporadic fatal exception could occur in case of OPC UA session creation and login.
- If several elements of a string array are subscribed using “IndexRange”, a fatal error occurred and the PLC stopped.

PROFINET

- If a “write record” could not be processed immediately by the PROFINET stack, it was buffered. When a new transmission attempt was made, it was then incorrectly sent as a “read record” packet.
- The RSC service “IAcyclicCommunicationService::RecordWrite()” has a timeout in which the profinet device has to respond. In some cases this timeout was too short and has been increased to 15s. The IEC function block “WRREC” internally uses this service, too.
- A PROFINET device with a device access point (DAP) starting at “Slot 1” could not be accessed via the “AR_MGT” function block.
- An inconsistent “SF-LED” state could occur at the PROFINET controller, if in case of an activated network port monitoring of a connected PROFINET switch the controller was plugged to another port during runtime and then plugged back to the original port.
- The PROFINET controller sent a “Write Request” with wrong lengths calculated in the “NDR header” when establishing the connection. This led to a “Write Response” error for PROFINET stations with very large parameter records (for example “PN/PB Gateway”).
- After PROFINET alarms of a certain severity occurred, these were not reset again for going alarms and remained in the diagnostic memory. As a result they were displayed incorrectly in the WBM and it could also happen that the “SF-LED” remained active.

Proficloud

- A fatal exception occurred if the Proficloud component with “Remanent Buffering” was enabled and the DataLogger component was manually disabled on the WBM page “System Services”.
- If a Proficloud TSD connection was lost, the logging was flooded with an unnecessary number of messages.
- If a Proficloud connection was disconnected, the connection could not be deactivated in the WBM.
- When a physical connection to the Proficloud was interrupted for several hours and re-established afterwards, the component could not reconnect automatically to the Proficloud.

SPLC

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

System

- After starting the PLCnext Engineer logic analysis, which contained an element of an array of struct, a system watchdog could occur sporadically.
- A system watchdog with reboot could occur while reading software information of a PLCnext Engineer project. This issue could occur if the manifest file in the PCWE directory is deleted after the “File::Exists” call but before the file is accessed by other operations. This could be the case during a “Download Changes” process (“Write and Start Project Changes” in PLCnext Engineer).
- Sometimes an OPC UA client did not receive the last “UpdateStatus” message after a successful installation of a firmware update. The last message informs about the reboot of the device (100 %) but the client only saw the “copy rootfs” message (90 %).
- If the controller was in the standard PLC status “ready/blocked” after a system watchdog, a “FATAL - Exception” was triggered if the “General Data (SPLC)” page of the SPLC was opened in the WBM.

WBM

- The “User Partition” value that was displayed on the WBM page “Cockpit” did not match the value of the global IEC 61131 system variable “USER_PARTITION.MEM_USAGE”.
- The memory partition was displayed in the WBM in “MiB” but shown with the unit “MB”. Now it is calculated as MB.

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

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

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

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

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

Curl

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

DBus

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

File

– CVE-2022-48554

GDS

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

GLib

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

Glibc

– CVE-2023-5156
– CVE-2023-4911

GnuTLS

– CVE-2024-0553
– CVE-2024-0567

GRPC

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

Libcap

– CVE-2023-2603

Libssh

– CVE-2023-6004

Network

With firmware version 2023.0.7 LTS and 2023.6, booting with an active security profile and the network link “AXC F XT ETH 1TX” plugged in at the same time was not possible.

NTP

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

NVT

– CVE-2022-29900
– CVE-2022-29901

OPC UA

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

OpenSSH

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

OpenSSL

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

Perl

– CVE-2023-47100

Python

– CVE-2022-40897
– CVE-2023-40217

Procps

– CVE-2023-4016

SQLite

– CVE-2023-7104

SqashFS

– CVE-2021-41072

Sudo

– CVE-2023-42465

Tcpdump

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

UM

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

Vim

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

Zlib

– CVE-2023-45853

9 Changes in firmware version 2023.6.1

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

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

If you use a left-alignable functional safety extension module with your controller, the following safety-related firmware versions must be used:

- AXC F XT SPLC 1000: **01.01.0000**
- AXC F XT SPLC 3000: **02.10.0006**

This section describes changes made between firmware version 2023.6.0 and firmware version 2023.6.1.

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

9.1 Error corrections

C++ API

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

9.2 Known limitations and errors

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

10 Changes in firmware version 2023.6.0

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

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

If you use a left-alignable functional safety extension module with your controller, the following safety-related firmware versions must be used:

- AXC F XT SPLC 1000: **01.01.0000**
- AXC F XT SPLC 3000: **02.10.0006**

This section describes changes made between firmware version 2023.0.0 LTS and firmware version 2023.6.0.

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

10.1 New functions

C++ API

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

IEC 61131-3

- The IEC 61131-3 non-standard function “GET_MICROSECONDS” is supported. To use this feature PLCnext Engineer 2023.6 (or newer) with a project template for this firmware or newer is required.
- The IEC 61131-3 non-standard function block “NETLOAD_LIMITER_STATISTIC” supports the access to the statistics of the netload limiter. To use this feature PLCnext Engineer 2023.6 (or newer) with a project template for this firmware or newer is required.
- Namespaces in IEC 61131-3 POUs are supported. To use this feature PLCnext Engineer 2023.6 (or newer) with a project template for firmware 2023.6 or newer is required.

INTERBUS

Notifications for a basic diagnosis of INTERBUS in combination with “AXC F XT IB” or “AXC F IL ADAPT” were added.

Linux

- CURL supports TFTP protocol (TFTP client)
- Podman was updated to version 4.4.3. This includes the update of related packages and requires to shift the network stack to “netavark” and “aadvard-dns.”

OPC UA

- Any variable known by the GDS can be read or written by the OPC UA client. In previous firmware versions only variables indicated with the “OPC” flag could be used by the OPC UA client.
- A project update for standard (non-safety) PLCnext Engineer projects is supported according to “DI SU Software Update Base Server Facet” and “DI SU Cached Loading Server Facet”. For this purpose the user roles “Admin” and “SoftwareUpdate” now additionally allow the update of projects (besides firmware updates). In PLCnext Engineer 2022.9 (and newer) an export of an updated application can be generated (“Export PLCnext Engineer Software Package”/“Export PLCnext Engineer Software Package (with sources)”). The exported project files can be uploaded to the Device and Update Management App and from there assigned to further devices. Note that an appropriate version (newer than 23.0.1) of the Device and Update Management App is required.

PROFINET

PROFINET diagnostic messages, which are sent in the USI format (User Structure Identifier) are printed in plain text (in English language) as notification and are displayed as well on the PROFINET diagnostics WBM page.
PLCnext Engineer collects the required interpretation rules from the FDCML description of the used PROFINET devices and plain text messages that are related to the device's USI diagnosis. Both information are sent to the PLC as a part of the project. Additionally, an USI diagnosis can be converted to a plain text message via the new RSC service “ITextLookup2”. To use this feature PLCnext Engineer 2023.6 or newer with a project template for this firmware version is required. Furthermore the used FDCML files need to contain the necessary USI diagnosis information. Currently the FDCML files delivered

with PLCnext Engineer (2023.6) installation do not contain this information.

SD card

When using the “AXC F XT SPLC 3000” the SD card is no longer mandatory.

10.2 Changes

Alarms

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

Firewall

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

IEC 61131-3

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

Notifications

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

SDK installer

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

WBM

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

10.3 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.

C#

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

ESM

– A cyclic ESM task configured to trigger the Axioline bus did not trigger the Axioline bus. Instead the ESM used a calculated update interval. Now the Axioline bus is triggered by the configured ESM task.
– 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.

GDS

The update of GDS connectors is also performed when the PLC is started (cold, warm, or hot restart). This ensures that initial values or retained values of OUT ports are for-

warded to their connected IN ports before the task of the IN port is executed.

IEC 61131-3 and C#

- The handling of the heap memory has been optimized. This includes allocation of heap (new operator as well as implicitly, for example by using string or other reference data types) as well as the Garbage Collector. These optimizations result in less time blocked by mutexes. Blocking by mutexes can prevent high priority tasks from execution and in rare cases caused an ESM task watchdog. These effects occurred in a very stochastic manner.
- The firmware did not handle variables of array data types and the usage of VAR_IN_OUT correctly. When such variables were used in a DataLogger session or in the “Logic Analyzer” of PLCnext Engineer the PLC detected a software watchdog (SWD). The PLC was rebooted and a cold start had to be performed (hereby retentive variables were set to their initial values).

OPC UA

- The OPC UA server did not provide data when subscribing to multiple matrices within a subscription. However, if only one matrix was subscribed, it worked. If a 2D matrix of type string was subscribed, the variable update of a previously subscribed 2D int matrix froze. This condition could only be removed by resubscribing to the 2D int matrix. This bug (known issue) has been fixed.
- If a matrix for monitoring was used, various unexpected results occurred when using “IndexRange” and “String” as data type:
  - When initially reading out the matrix after logging in, a “DataChange” event with several changes was erroneously triggered.
  - If a “DataChange” event was performed after writing, the strings in the matrix were truncated.
  - Sporadically a “Segmentation Fault” occurred when reading out the matrix.

  This bug (known issue) has been fixed.
- Using the value “0” as NamespaceIndex in the configuration of OPC UA client could lead to a fatal error. This bug (known issue) has been fixed.
- In case of a warm start of the PLC, subscriptions from the “clientconfig.xml” had not been loaded and created.
- 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 starting the firmware, the PROFINET communication sporadically ran into a timeout. In combination with the left-alignable extension module “AXC F XT SPLC 1000” the Safety I/O modules were consequently passivated even though the PROFINET communication was re-established after the timeout.
- After resetting the PLC with attached left-alignable extension module “AXC F XT ETH 1TX” to factory defaults, both ETH adapters got the same PROFINET name. With firmware 2023.6 and newer “-pnc” is appended to the name of the PROFINET controller and “-pnd” is appended to the name of the PROFINET device. If no “AXC F XT ETH 1TX” is present, the PROFINET name is reset to “axcf2152-pnc”.
- 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.
- 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.
- 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.

RSC services

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

SDK

The class “SecurityNotificationPayload” was missing in the SDK. The following header files were added.

- “Arp/System/NmPayload/Security/SecurityNotificationPayload.hpp”
- “Arp/System/NmPayload/Security/SecurityNotificationInfo.hpp”

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

- When the NTP daemon is disabled, the hardware clock drifts significantly, and it is only resynchronized with the system clock at the start of the reboot sequence.
- The text messages of a loaded safety-relevant project in the notifications and “Output.log” showed incorrect CRC information.
- 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.
- The “paho” library was updated from version “v1.3.10” to “v1.3.12”. This update solves several incompatibilities with the IEC 61131-3 “IIoT_Library_V4.x”. In particular, it fixes a “system watchdog” in combination with “MQTT-Client FB” in case of a failed MQTT connection.

WBM

- If many PROFINET devices are used and the button to jump to the tree node is pressed in the “Device List” tab of the “Diagnostics - PROFINET” page, the “Tree View” tab was opened but often it was not automatically scrolled to the desired device.
- In the “Device List” tab of the “Diagnostics - PROFINET” page the link to the device‘s web page was only shown if the connection to the device could be established during project load. Now the PROFINET device is regularly checked if it offers a web page.
- In some cases the “Diagnostics - PROFINET” page of the WBM displayed a wrong IP address (e.g. “10.10.10.1”) for the PROFINET controller.
- The display of the used and free memory of the user partition was optimized at the “Cockpit” page of the WBM.
- At the “Password Policy” tab of the WBM page “User Authentication” the description of the “password reuse” settings could possibly be misinterpreted and has therefore been corrected.
- The “Change Password” dialog did not handle special characters correctly.

10.4 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.

10.5 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.

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

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

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

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

Curl

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

C-ares

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

Freetype

- CVE-2023-2004

Firewall

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

Git

- CVE-2023-22490
- CVE-2023-25652
- CVE-2023-29007
- CVE 2022-41903
- CVE-2022-23521

Kernel

- CVE-2022-1012

Libxml2

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

N-curses

- CVE-2023-29491

Network

In the case of an attack with a high network load, network communication could be permanently interrupted despite an activated firewall and activated Netload Limiter. This could only be remedied by a restart of the controller.

OpenSSL

- CVE-2023-2650
- CVE-2023-0464
- CVE-2023-0465
- CVE-2023-0466
- CVE-2023-0286
- CVE-2022-4304
- CVE-2023-0215
- CVE-2022-4450
- CVE-2023-0216

Podman

- CVE-2022-2989

Python

- CVE-2022-45061
- CVE-2023-24329

Rsync

- CVE-2022-29154

SNMP

- CVE-2022-44792
- CVE-2022-44793

Sqlite

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

Strongswan

- CVE-2023-26463

Sudo

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

Syslog

- CVE-2022-38725

Tar

- CVE-2022-48303

Vim

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

11 Changes in firmware version 2023.0.7 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 2023.0.0 LTS or newer at least a firmware version 2022.0 LTS or newer must be installed on the PLC. Older firmware versions will not accept the *.rauc firmware update file.

This section describes changes made between firmware version 2023.0.0 LTS and firmware version 2023.0.7 LTS.

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

11.1 Error corrections

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.
- If the PLC rejected a “Download changes” command (“Write and Start Project Changes” executed by PLCnext Engineer), for example because the change could be performed in real time, the PLC was rebooted due to a system watchdog.

Network

In case of an attack with high network load, network communication could be permanently interrupted despite an activated firewall and activated Netload Limiter. This could only be remedied by a restart of the controller.

OPC UA

- OPC UA client: Several memory leaks in case of read or write subscriptions were fixed.
- Using the value 0 as NamespaceIndex in the configuration of OPC UA client could lead to a fatal error.

Proficloud

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

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.
- 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.

System

- The file “/var/log/daemon.log” could become very large and in worst case causes an out of memory situation. This file is now considered by “logrotate” and therefore can no longer become that large.
- Update of “paho” library from version “v1.3.10” to “v1.3.12”.
  This update solves several incompatibilities with the IEC 61131-3 “IIoT_Library_V4.01”. In particular, it fixes a “system watchdog” in combination with “MQTT-Client FB” in case of a failed MQTT connection.

WBM

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

11.2 Known limitations and errors

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

11.3 Security updates

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

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

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

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

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

C-ares

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

Curl

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

Firewall

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

Freetype

– CVE-2023-2004

Git

– CVE 2022-41903
– CVE-2022-23521
– CVE-2023-22490
– CVE-2023-29007

Glibc

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

Libxml2

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

Ncurses

– CVE-2023-29491

OpenSSL

– CVE-2023-0286
– CVE-2022-4304
– CVE-2023-0215
– CVE-2022-4450
– CVE-2023-0216
– CVE-2023-2650
– CVE-2023-0464
– CVE-2023-0465
– CVE-2023-0466
– CVE-2023-3817

Rsync

– CVE-2022-29154

Strongswan

– CVE-2023-26463

Sqlite

– CVE-2022-46908

Syslog-NG

– CVE-2022-38725

Tar

– CVE-2022-48303

User Manager

With activated “Security Profile” the role “Engineer” erroneously also had the rights of the role “SafetyEngineer”.

12 Changes in firmware version 2023.0.0 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 2023.0.0 LTS or newer at least a firmware version 2022.0 LTS or newer must be installed on the PLC. Older firmware versions will not accept the *.rauc firmware update file.

This section describes changes made between firmware version 2022.9.0 and firmware version 2023.0.0 LTS.

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

12.1 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).

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.

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.

12.2 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.

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.

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

12.3 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.

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.
- 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.
- When using the AXC F 2152 as PROFINET device in SRL mode (system redundancy) the system variable “PND_S1_Data_Length” was set to 0 when the PLC was stopped. When the PLC was started again, the variable remained 0.

Network

AXC F 2152 with AXC F XT ETH 1TX:

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

Notifications

C# call stack after unhandled exception was doubled in “Notification.log”.

OPC UA

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

- Project update via OPC UA: If the controller was in the “PreparedForUpdate” state, no activation of a downloaded boot project was possible. This was also not indicated by an error message.
- Some file transfer issues were fixed, e.g. “Writable” attribute was always true and PLC crash when removing permissions.

PROFINET

- If the “MaintenanceItem: Demanded” and the “Property Flag” “Maintenance Demanded” both occurred in the same PROFINET alarm frame, the alarm was not displayed in the PROFINET bus diagnostics in the WBM.
- In connection with a set PROFINET cycle time of 1 ms, the PROFINET controller could experience increased latency. This behavior was caused by an unfavorable timing during the communication processing of the process data.
- During the startup parameterization of a subordinate IO-Link master at an “AXL F BK PN TPS” bus coupler, the error message “0xA002” (wrong module found) could occur.
- When reading the “ModuleDiffBlock” with the function block “GET_MODULE_DIFF_BLOCK” it could happen that the states “WRONG_MODULE” and “NO_MODULE” were not returned. The error occurred when there is a module difference but no submodule difference. With “WRONG_MODULE” and “NO_MODULE” there is no submodule difference and therefore the difference was incorrectly not saved.
- If a bus coupler was operated via the PROFINET controller as a subordinate device without connected I/O modules, the “SF” LED was not activated. The bus coupler reports an “SF” and the PROFINET diagnostics in the WBM also shows this state, but neither the status LED nor the system variable “PNIO_SYSTEM_SF” indicated this.
- 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.

RSC

When calling the “IDeviceInfoService” “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”.
- The LED flashing behavior related to PROFINET did not match the description in the manual when wire break and network error were triggered in quick succession.

System

- When installed apps requested a restart of the firmware, it could sporadically happen that this restart was not performed properly.
- 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.
– Errors occurred in the WBM Axioline diagnostics when displaying different Axioline base profiles (e.g. module 2.0 or 3.0 profile).

12.4 Known limitations and errors

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

12.5 Security updates

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

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

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

BusyBox
– CVE-2022-30065

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

13 Changes in firmware version 2022.9.0

To be able to use all new functions of the firmware, you need PLCnext Engineer version 2022.9 or newer.
Select the latest template for firmware version 2022.9 in the PLCnext Engineer project.

This section describes changes made between firmware version 2022.6.0 and firmware version 2022.9.0.

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

13.1 New functions

OPC UA

OPC UA supports ReverseConnect. PLCnext Engineer 2022.9 (or newer) and the related template are required for the configuration of this feature.

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.

13.2 Changes

OPC UA

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

13.3 Error corrections

PROFINET

- 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.

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).

WBM

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.

13.4 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.

13.5 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.

BusyBox 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

Curl

– CVE-2022-32207
– CVE-2022-32206
– CVE-2022-32208
– CVE-2022-32205

Vim

– CVE-2022-2522
– CVE-2022-2571
– CVE-2022-2580
– CVE-2022-2581
– CVE-2022-2598

14 Changes in firmware version 2022.6.0

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.

14.1 New functions

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.

14.2 Changes

ESM

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;"

PROFINET

The PROFINET PRL (Phoenix Redundancy Layer) is no longer supported with firmware version 2022.6.

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.

14.3 Error corrections

ESM

If an ESM task had a fatal error and exited immediately, an unhandled follow-up exception led to a deadlock of the application.

PLCnext Engineer

When setting date/time via PLCnext Engineer and immediately shutting off the power supply, the date/time setting did not become effective.

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”.
- with AXC F XT ETH 1TX:
  On the WBM page “Network” in the “Configuration” area, LAN interfaces and ports were displayed incorrectly.

14.4 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.

14.5 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.

BusyBox 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

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 re-configuration 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.

15 Changes in firmware version 2022.3.0

To be able to use all new functions of the firmware, you need PLCnext Engineer version 2022.3 or newer.
Select the latest template for firmware version 2022.3 in the PLCnext Engineer project.

15.1 New functions

Articles

Basic support of the left-alignable extension module for net measurement and protection AXC F XT PMP-1000VAC (item no. 1307473).

15.2 Changes

Notification

Performance optimization in the “CreateNonBlockingNotificationRegistration2” mechanism. Now the “SendNotification()” method call in the real-time context is faster and needs much less CPU time.

15.3 Error corrections

ESM/INTERBUS

With firmware version 2022.0.4 LTS or earlier, an ESM event task could be executed only up to 2,147,483,648 times ($1{,}024^3 \times 2$) after power on. This affected mainly the “Interbus cycle end” ESM event task. This task is available for the AXC F controllers in combination with the “AXC F IL ADAPT” or “AXC F XT IB” extension modules. With firmware version 2022.3, this issue is solved.

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.

15.4 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.

15.5 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.

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

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

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

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

LIBEXPAT

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

16 Changes in firmware version 2022.0.10 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.

This section describes changes made between firmware version 2022.0.8 LTS and firmware version 2022.0.10 LTS.

16.1 Error corrections

INTERBUS

If many INTERBUS devices were connected, it could happen that the asynchronous communication services (mailbox) stopped due to an internal buffer overflow. The PLC needed to be restarted. This bug has been fixed.

16.2 Known limitations and errors

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

17 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.

17.1 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.

17.2 Security updates

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

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

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

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

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

BusyBox

– CVE-2022-28391

Curl

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

Cyrus SASL

– CVE-2019-19906
– CVE-2022-24407

HMI

Hardening against DoS attacks.

IPv6

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

LIBEXPAT

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

LIBXML

– CVE-2022-29824
– CVE-2022-23308

OpenSSL

– CVE-2022-0778

OPC UA

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

OpenVPN

– CVE-2022-0547

Vim

- CVE-2022-1381
- CVE-2022-1420
- CVE-2022-1733
- CVE-2022-1796
- CVE-2022-1621
- CVE-2022-1616
- CVE-2022-1619
- CVE-2022-1629
- CVE-2022-1735
- CVE-2022-1769
- CVE-2022-1785
- CVE-2022-1620
- CVE-2022-1674
- CVE-2022-1771
- CVE-2022-1886
- CVE-2022-1851
- CVE-2022-1898
- CVE-2022-1720
- CVE-2022-1154
- CVE-2022-0943
- CVE-2022-1160
- CVE-2022-1381
- CVE-2022-0729
- CVE-2022-0572
- CVE-2022-1420
- CVE-2022-0696
- CVE-2022-0685
- CVE-2022-0714
- CVE-2022-0361
- CVE-2022-0368
- CVE-2021-3973
- CVE-2021-3796
- CVE-2021-4166
- CVE-2022-1733
- CVE-2022-1796
- CVE-2022-1621
- CVE-2022-1616
- CVE-2022-1619
- CVE-2022-1629
- CVE-2022-1735
- CVE-2022-1769
- CVE-2022-1785
- CVE-2022-1620
- CVE-2022-1674
- CVE-2022-1771
- CVE-2022-1886
- CVE-2022-1851
- CVE-2022-1898
- CVE-2022-1927
- CVE-2022-1942
- CVE-2022-1720
- CVE-2022-2129
- CVE-2022-2175
- CVE-2022-2182
- CVE-2022-2183
- CVE-2022-2343
- CVE-2022-2207
- CVE-2022-2210
- CVE-2022-2344
- CVE-2022-2304
- CVE-2022-2345
- CVE-2022-2208
- CVE-2022-2231
- CVE-2022-2287
- CVE-2022-2285
- CVE-2022-2284
- CVE-2022-2286
- CVE-2022-2289
- CVE-2022-2288
- CVE-2022-2264
- CVE-2022-2206
- CVE-2022-2257

ZLib

- CVE-2018-25032

18 Changes in firmware version 2022.0.4 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.

18.1 Error corrections

The following errors have been rectified:

eHMI

Depending on the history of firmware versions installed on a particular PLC, it could happen that a web browser could no longer connect to the PLCnext Engineer HMI on the PLC after updating to firmware 2022.0 LTS.

Network

After a reboot or power reset, a connection/link with the built-in Ethernet adapters could sporadically not be established due to autonegotiation problems. This behavior occured mainly in combination with some switches and when using short cables.

System

- If the PROFINET controller was deactivated, an unwanted notification was emitted (“A subscriber subscribed to not registered notification name: Arp.Io.PnC.Alarm”).
- After a power-up and subsequent cold start of the PLC project, a “fatal error” could occur very sporadically in the controller, followed by a restart triggered by the “system watchdog”. This only affected projects with Axioline local bus process data linked in the GDS.

WBM

The PROFINET diagnosis in the WBM did not recognize some dedicated module/submodule diagnosis (USI format). As a consequence the related modules/submodules were indicated as “Ok” although a diagnosis alarm was active.

18.2 Known limitations and errors

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

19 Changes in firmware version 2022.0.3 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.

19.1 New functions

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 licence (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 both, PROFINET standardized and vendor-specific error codes at 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. GSDML) 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.

19.2 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 used 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.

Netload Limiter

– The “Netload Limiter” function is supported. With the “Netload Limiter” function you can limit the network traffic to prevent the controller from stopping in case of network storms.
– The “Netload Limiter” is actived by default. For the built-in Ethernet interface (X1/X2), a limit of 32 packets per millisecond is configured initially.

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.

19.3 Error corrections

The following errors have been rectified:

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 2152 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

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

– After a power reset, the firmware could sporadically not be started properly and a System Watchdog occured.
– 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 2152 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.

Retain

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

Notifications

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

19.4 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.

19.5 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.

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

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

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

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

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
- CVE-2021-20305

GIT

- CVE-2021-40330
- CVE-2021-21300

GLIBC

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

GNUTLS

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

LIBSSH2

- CVE-2019-17498

LIBXML2

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

PERL

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

TAR

- CVE-2021-20193

NGINX

- CVE-2021-23017

NET-SNMP

- CVE-2019-20892

GMP

– CVE-2021-43618

Python

– CVE-2019-20907

LIBEXPAT

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

CURL

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

BusyBox

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

  The documented CVEs were not fixed via an update of BusyBox. Instead, the affected BusyBox components have been removed: The following config switches have been switched off (“not set”):
  CONFIG_FEATURE_SEAMLESS_LZMA=y
  CONFIG_ASH=y
  CONFIG_AWK=y

  In the case of “AWK” it makes no difference as this tool is also integrated from the core utils library. The shell “ASH” and the “LZMA” algorithms (i.e. for unzip) are no longer supported.
– CVE-2018-1000500

OPC UA

– CVE-2021-45117

BASH

– CVE-2019-18276

Network

DoS attacks over network could lead to a PLC project stop caused by the ESM Task Watchdog.

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.

20 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.

20.1 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.

OPC UA

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

20.2 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.

GDS

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

OPC UA

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

20.3 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.

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

EthernetIP is no longer possible.
This can be remedied by subsequently activating the ports:
  – Incoming connections: **port 44818**
  – Outgoing connection: **port 2222**

– PLCnext CLI version
The PLCnext CLI version used must match the current SDK for this version. Downward compatibility cannot be guaranteed.
– Configuration changes to safety nodes
With attached AXC F XT SPLC 1000:
Only a complete recompilation and redownload of the standard and safety project guarantees a consistent adoption of configuration changes to safety nodes in the bus structure of the standard project.
– Firmware downgrade
After downgrading the firmware, it is recommended to reset to “Default setting type 1”. This is not necessary when updating the firmware.
– WBM error message
If the PLCnext system firmware has not started up properly, the WBM displays the error message “Bad Gateway 502”.
– Task name
If “Event”, “EventTask”, “ServiceTask” or “Globals” is used as the name of a task, an error condition of the controller occurs when the project is downloaded. It occurs because these names are already used internally as class name.
– DHCP
DHCP can only be switched on for Ethernet adapters that are not assigned as PROFINET controllers or PROFINET devices. To make the settings effective in the network, the device must be restarted.
– Variables
The content of the variables “ESM_DATA.ESM_INFOS[*].ESM_TICK_COUNT” and “ESM_DATA.ESM_INFOS[*].ESM_TICK_INTERVAL” is permanently set to 0.
– Error during program download
During a PLCnext Engineer program download (both total and changes), the web server returns an error 503 (busy) for requests to the HMI pages.
– DataLogger
If two or more DataLogger sessions are configured to write to the same database, only the data of one session will be transferred to the database on the SD card at the end. As of firmware 2021.9 the user receives a notification indicating which session is recorded.
– Retain data
Using the maximum quantity structures of the retain data can increase the task duration of the using task. This can trigger a task watchdog for time-critical applications.
– STRING variables
Access to long STRING variables outside the application is limited to 511 bytes. This concerns reading and writing via the RSC services “IDataAccessService” and “ISubscriptionService”. These services are used by OPC UA, PLCnext Engineer HMI and the online functions of PLCnext Engineer, among others.
From firmware version 2021.6: The same applies for WSTRING variables. Please note that WSTRING variables are converted to UTF8 when accessed via RSC services.
– “Download Changes“
Sporadically a PLCnext Engineer project may reject “Download changes” without giving a reason.
– Restart after app installation
Sporadically it can happen that a restart of the firmware requested by an app installation does not work properly. If the firmware does not start up correctly, the controller can be restarted by one of the following 3 possible actions:
  – Restart of the firmware via SSH (/etc/init.d/plcnext restart)
  – Reboot of the controller via SSH
  – Power reset of the controller
– Local time zone setting
Setting local time zones is not fully supported.
– “Link” and “Active” LEDs
The “Link” and “Active” LEDs on the network interfaces “X1” and “X2” are not active when a “10BaseT” connection is used.
– PROFINET cycle time
The use of a PROFINET cycle time of 1 ms leads to a deviation of the jitter behavior required by the controller certification.
Operation in this state is possible, but not recommended.
– Language standard C++ 17
With the SDK version 2021.6 the language standard C++ 17 has been set in the compiler options ("-std=c++17"). The firmware itself is also compiled with this option set. Besides some general C++ issues related to this C++17 standard, the following issue is related to PLCnext:
C++ 17 introduces the data type “std::byte” which is unfortunately not compatible with “Arp::byte”. Therefore, if the namespaces “std” and “Arp” are both ac-

tive the compilation results in an error. In this case existing C++ sources have to be adjusted so that they explicitly use “Arp::byte” (e.g. by adding “using byte = Arp::byte;“).

– Communication errors
  Sporadic communication errors may occur between PLCnext Engineer and the controller. A reboot of the controller solves the problem.
– Unexpected behavior using the Select() method
  The Select() method of the classes Arp::System::Commons::Ipc::IpcSocket, Arp::System::Commons::Net::Socket
  and Arp::System::Commons::Net::TlsSocket returns true, when the socket is shut down. Compared to BSD sockets, this behavior is unexpected. As this is a legacy method it is now remarked as deprecated. In future, additionally a new method Poll() will be implemented.
– System crash caused by user components
  If a user component causes a crash before the system watchdog is activated, the firmware terminates and the controller is available via SSH only.
  Note: The system watchdog is activated just before the IControllerComponent::Start() method is invoked.
– License operations, such as adding or removing a license, include cryptographic operations and hence shall only be performed if the PLC is stopped. This may avoid side effects due to preempting the license operations by tasks running with higher priority.

20.4 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.

21 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.

21.1 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 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 (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.

21.2 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.)

21.3 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.
- In connection with a PLC project which uses almost the entire number of possible retain variables, a PLC task watchdog could sporadically occur after a restart of the controller.
- 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 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”.
- After activating the MRP function, it was not shown as activated when reading back the status. After restarting the controller it was deactivated again.

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.

21.4 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.

- 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.
- “Link” and “Active” LEDs
  The “Link” and “Active” LEDs on the network interfaces “X1” and “X2” are not active when a “10BaseT” connection is used.
- PROFINET cycle time
  The use of a PROFINET cycle time of 1 ms leads to a deviation of the jitter behavior required by the controller certification.
  Operation in this state is possible, but not recommended.
- Language standard C++ 17
  With the SDK version 2021.6 the language standard C++ 17 has been set in the compiler options ("-std=c++17"). The firmware itself is also compiled with this option set. Besides some general C++ issues related to this C++17 standard, the following issue is related to PLCnext:
  C++ 17 introduces the data type “std::byte” which is unfortunately not compatible with “Arp::byte”. Therefore, if the namespaces “std” and “Arp” are both active the compilation results in an error. In this case existing C++ sources have to be adjusted so that they explicitly use “Arp::byte” (e.g. by adding “using byte = Arp::byte;“).
- Communication errors
  Sporadic communication errors may occur between PLCnext Engineer and the controller. A reboot of the controller solves the problem.
- Unexpected behavior using the Select() method
  The Select() method of the classes Arp::System::Commons::Ipc::IpcSocket, Arp::System::Commons::Net::Socket
  and Arp::System::Commons::Net::TlsSocket returns true, when the socket is shut down. Compared to BSD sockets, this behavior is unexpected. As this is a legacy method it is now remarked as deprecated. In future, additionally a new method Poll() will be implemented.

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

21.5 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.

System

– The “execute bit” of the PLCnext log files (and database files) was mistakenly set.
– 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

22 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.

22.1 Changes

System

"Paho" libraries were updated to the following versions:

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

22.2 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

– During offline installation of licenses a reboot is recommended. If this reboot has been performed by switching off the power, the license files on the controller could be lost.
– 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.

DataLogger

During the writing of large databases and simultaneous unexpected system restart due to a voltage interruption or a system watchdog, an invalid state of the database could occur. As a result, the system could not restart properly afterwards.

22.3 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 2021.0.2 LTS also exist in this firmware version.
See section 24.3 "Known limitations and errors"on page 55.

22.4 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

23 Changes in firmware version 2021.0.3 LTS

All changes described in section 24 “Changes in firmware version 2021.0.2 LTS” on page 55 are also valid for this firmware version.

23.1 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 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
- /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.

24 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.

24.1 New functions

PROFINET

- 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.

24.2 Error corrections

The following errors have been rectified:

PROFINET

- 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 were solved, which occurred when a superseded PROFINET controller requested to check the MRP configuration of the PROFINET device.
- Minor problems in the representation of device specific information via LLDP were solved.
- Sporadic link problems were solved that occurred with a PROFINET device which only offers 100 Mbit full-duplex/half-duplex.
- In combination with AXC F XT ETH 1 TX:
  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.

System

- 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.

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.

24.3 Known limitations and errors

- 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.

– In addition, the known errors and limitations from firmware version 2021.0 LTS also exist in this firmware version.
See section 25.3 “Known limitations and errors” on page 60.

24.4 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-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.

25 Changes in firmware version 2021.0 LTS

To be able to use all new functions of the firmware, you need PLCnext Engineer version 2021.0 LTS. Select the latest template for firmware version 2021.0 LTS in the PLCnext Engineer project.

25.1 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.

Proficloud

“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 when an older controller is replaced 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.

25.2 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.
– 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.
- The PROFINET controller performance was improved.

RSC

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

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.
- 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.

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.

25.3 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.
- PROFINET PRL support
  Firmware version 2021.0.0 LTS is the last version which supports PROFINET PRL (Phoenix Redundancy Layer).
  Future versions will no longer support this feature.
- 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
  AXC F 2152 in combination with AXC F XT ETH 1TX extension module: 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.
- “Link” and “Active” LEDs
  The “Link” and “Active” LEDs on the network interfaces “X1” and “X2” are not active when a “10BaseT” connection is used.
- PROFINET cycle time
  The use of a PROFINET cycle time of 1 ms leads to a deviation of the jitter behavior required by the controller certification.
  Operation in this state is possible, but not recommended.

25.4 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

– CVE-2020-12517

System

– CVE-2020-12518

Shell

– CVE-2020-12519

LLDP

– CVE-2020-12521

26 Changes in firmware version 2020.6.1

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 2020.6.1 in the PLCnext Engineer project.

26.1 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 16 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 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.

PROFICLOUD

PROFICLOUD V3 basic support (firmware update from the cloud).

26.2 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.
– After switching off MRP, an AXC F 2152 was no longer accessible as a device.

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.

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.

INTERBUS

With the AXC F 2152 in conjunction with the AXC F IL ADAPT extension module, the error “SYSFAIL” could occur when working with breakpoints. If, after working with breakpoints in a project, the program continued running without entering a breakpoint again, the “SYSFAIL” signal was not reset. Although the fieldbus continued to run, process data exchange was no longer possible.

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.

26.3 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.
- Internal network interface
  Sporadically, frequent calls of PROFINET Read or Write REC may cause communication to the corresponding AR to be disturbed and a connection termination may occur.
- 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.
- 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.
- Retain variable behavior with firmware downgrade
  If firmware 2020.0 or later is downgraded to 2019.9 or older and then upgraded again to firmware version 2020.0 or later, a cold start is performed.
  The retain variables are set to their initialization value.
- 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.
- AXC F 2152 with extension module AXC F XT ETH 1TX
  If both network adapters are configured with the same "Subnet Mask", the PROFINET controller functionality will not work as desired. A proper connection setup is not possible.
- 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.
- After resetting the controller there is no TrustStore with the name "proficloudv3". The TrustStore is necessary for the update via ProficloudV3.
  Workaround: Re-create the TrustStore in the WBM of the controller.
- Gateway settings LAN2
  AXC F 2152 in combination with AXC F XT ETH 1TX extension module: If there are several "Default Gateway" settings, only the setting of LAN1 is used. The settings of other LAN adapters are ignored.

26.4 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

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.

27 Changes in firmware version 2020.3.1

To be able to use all new functions of the firmware, you need PLCnext Engineer version 2020.3. Select the latest template for firmware version 2020.3.1 in the PLCnext Engineer project.

27.1 New functions

System

You can now set the parameters for the NTP time server protocol in PLCnext Engineer.

DCP flashing

DCP flashing for PROFINET controllers/devices of the PLCnext Control family has been implemented.

PROFINET diagnostics

The PROFINET controller provides diagnostic information as function block “ARStatistik”.

New functions in WBM

- Display and download of the notification log
  The notifications are displayed in the WBM on a separate page.
- Extended Ethernet display
  The WBM provides an extended display of information about the Ethernet configuration of all available LAN interfaces.

Docker

“Docker” is supported for all articles of the PLCnext family. Additionally the “Balena Engine” is supported. (“nftables” configuration, “cgroups” are mounted at boot time).

OPC UA server

- Configurable “subscription type”
  The component can now be configured using the configuration file “PCWE.opcua.config”, e.g. using the PLCnext Engineer software.
- Support of “DateTime“
  The data type “DateTime” is supported via OPC UA in any nesting, e.g. Structs, ArraysOf ..., Simple Var, FBs etc.

Linux

The packages for “rsync” for file synchronization are supported.

27.2 Error corrections

The following errors have been rectified:

- System files
  System files modified with “root” access could prevent proper reboot after a firmware update.
- Axioline
  In conjunction with the AXC F XT IB module, the contents of the diagnostic parameter registers in the system variables were swapped.
- WBM
  - Some WBM diagnostic pages were not displayed correctly with Internet Explorer.
  - On the WBM page for network configuration, the name “Baud rate” was incorrect. This was changed to "Data rate".
  - A WBM session of a logged on user was never terminated if a page with cyclically updated data was open.
  - An eHMI user could never log out completely.
- IEC 61131
  An error could occur when restoring the retain data after a reboot.
  This behavior only occurred in the PLCnext Engineer project if program instances were moved to another ESM task.
- DataLogger
  After a firmware update, logging into the DataLogger database did not work anymore if the database design had changed.
- RSC
  Synchronous execution of RSC services without security context was not supported and could lead to an unexpected error message.

27.3 Known limitations and errors

- Retain variables
  - If a warm start is requested via PLCnext Engineer and this is not possible internally, 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 initialization values.
- Special characters
  When using UTF8 special characters (Unicode) for the user name and password, the length restriction (user name = 64 bytes, password = 128 bytes) can take effect, although the maximum character length was not used. This reason is that the number of bytes and not the number of characters is limited in the RSC service.
- OpenSSL
  For security reasons, applications should no longer be linked against the outdated OpenSSL version 1.0.2.
- PLCnCLI version
  The PLCnCLI version used must match the current SDK for this version. Backward compatibility cannot be guaranteed.
- GNU compiler
  With the GNU compiler types GCC (8.3.0, 9.2.1) used, a quadratic increase in compilation time and memory consumption on the desktop PC is observed when very large structures are used.
  Note this behavior if you use a large number of ports in PLCnext applications (e.g. connection of a very large number of Simulink signals).
- 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**
- System variables
  The system variables ESM_DATA.ESM_INFOS[*].ESM_TICK_COUNT and ESM_DATA.ESM_INFOS[*].ESM_TICK_INTERVAL are no longer supported.
  Now, the value of the variables is always 0.
- Error during program download
  During a program download (both complete and modifications) in PLCnext Engineer, the WebServer returns 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 from one session is transferred to the database on the SD card. You will **not** receive a message that not all data can be saved.
- Debugging
  After debugging a PLCnext Engineer project with breakpoints, the project may stop after restarting.
- PROFINET connection setup
  The PROFINET connection setup can take a long time in combination with a very large PROFINET structure.
- PROFINET Read/Write
  Frequent calls of PROFINET Read or Write REC may disturb the communication to the corresponding AR. A connection termination may occur.
- Increased task duration caused by retain data
  If the maximum retain data volume is used, the duration of the task may increase. A task watchdog could be triggered in 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 and PLCnCLI
  The SDK only works with PLCnCLI 2020.0 or later, not with older versions (both PLCnCLI 2019.x and PC Worx Target for Simulink 2019.x).
- Reboot via Linux shell
  After rebooting the controller via the Linux shell, a system watchdog may occur in rare cases. When the controller is subsequently booted, only a cold start is possible. This initializes all retain variables.
  This behavior only occurs when rebooting via the Linux shell. No system watchdog was observed when the controller lost power.
- OpenSSL update
  Updating the OpenSSL version 1.0.2 to version 1.1.1 can lead to problems with existing C++ applications that are based on this and run in the same process (e.g. function extensions). Phoenix Contact recom-

mends paying attention to possible updates in the PLCnext Store.
In the event of incompatibility, the firmware may not start up.

- Switching off MRP
  After switching off MRP, a restart of the AXC F 2152 is required in order for it to work properly.
- 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.
- 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 with a “factory reset”.
- PROFINET name
  If firmware 2020.3 is downgraded to an older version, the PROFINET name is lost.
- Debugging 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”
  Occasionally “Download Changes” may be rejected in a PLCnext Engineer project without stating a reason.

27.4 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

git

- CVE-2019-19604
- CVE-2019-1387
- CVE-2019-1348

vim

- CVE-2019-20079

sqlite3

- CVE-2019-19646
- CVE-2019-19645
- CVE-2019-16168
- CVE-2019-8457

28 Changes in firmware version 2020.0.1 LTS

In interaction with this firmware the following points are not necessary:

- Update of PLCnext Engineer
- Update of SDK files for high-level language applications

28.1 Error corrections

The following problems have been fixed:

- A problem that led to cyclical connection terminations of the PROFINET application relationships (AR). This behavior occurred depending on the cycle times of the ESM tasks.
- A problem that caused an incorrect recovery of the retain data after a reboot of the controller. This behavior only occurred if program instances in the PLC project were moved to another ESM task.
- A problem that caused the controller to stop booting after resetting the controller to factory default type 2 (factory default). In this state the BOOT LED flashes red (2 Hz). The LED D is permanently yellow.
- A problem that was possible in conjunction with OPC UA. Scalar data types could be written with the wrong data type. This could lead to incorrect data in the IEC project when overwriting with larger data types. The error code “StatusCodes.BadTypeMismatch” would be expected here.

29 Changes in firmware version 2020.0 LTS

If you changed system files via a “root” access, the controller might not start up correctly after a firmware update.

- In this case, reset the controller to default setting type 1.

29.1 New functions

Offline installation of apps from the PLCnext Store

You can install apps downloaded from the PLCnext Store via the WBM of the controller without Internet connection and activate the corresponding licenses.

DataLogger improvements

- When configuring the DataLogger, you can specify the percentage of data to be deleted when the database reaches its maximum size (attribute “deleteRatio”).
- You can configure the data format of time and date (attribute “tsfmt”).

For more detailed information on configuring the DataLogger, please refer to the “PLCnext Technology” user manual.
The user manual can be downloaded at phoenixcontact.net/product/2404267.

Axioline Smart Elements

The controller supports Axioline Smart Elements.

Implementation of the “SysV IPC” Linux extension

With this extension, you can use the three IPC techniques (semaphore, message queue, and shared memory) of “SysV”.

OpenSSL update to version 1.1.1

The OpenSSL library has been updated to version 1.1.1.

Recommended:
Use version 1.1.1 of the OpenSSL library.
The older version 1.0.2 of the OpenSSL library is still part of the firmware for reasons of downward compatibility.

Docker software support

Options for support of the Docker software have been enabled in the Linux kernel.

29.2 Error corrections

– Task execution
  Sporadically a task was not executed correctly in the given cycle.
  This error has been rectified.
– eHMI visualization after “Download Changes”
  After downloading program changes to the controller, the eHMI visualization could only be used after reloading the page in the browser.
  This error has been rectified.
– Data exchange with PROFICLOUD
  If variable values from an ESM1 task and from an ESM2 task were to be transferred to PROFICLOUD at the same time, the data exchange with PROFICLOUD was interrupted.
  This error has been rectified.
– Accessing an undefined element in the array
  When accessing an undefined element within a multi-dimensional array (“Array of Array” or “Array of Struct”) with OPC UA, the controller broke down.
  This error has been rectified.
– Length limitation of strings
  If strings with a length of more than 2993 bytes were created, access with OPC UA or RSC services of the GDS could cause the controller to break down.
  This error has been rectified. As part of the error correction, the length of a string was limited to a maximum of 511 bytes.

29.3 Known limitations and errors

– Mixed operation of different OpenSSL versions
  If the use of existing C++ applications (Function Extensions) results in mixed operation of the OpenSSL versions 1.0.2 and 1.1.1, the controller does not boot.
  Recommended: If you are using an app of the type "Function Extension" from the PLCnext Store, check whether an update is already available in the PLCnext Store.
– Automatic cold start
  If you initiate a warm start in PLCnext Engineer and this is not possible internally, a cold start is performed automatically, i.e., the retain variables are reinitialized.
– Cold start after system watchdog
  After a system watchdog, a cold start is performed.
– System watchdog after reboot via shell
  If you restart the controller via the shell, the system watchdog is triggered sporadically.
– Limitation of password and username
  The length of the password is limited to 64 bytes and the length of the user name is limited to 128 bytes. Note that the entered characters are UTF-8 encoded, i.e. one character can occupy up to four bytes (e.g. umlauts).
– PLCnCLI version and SDK version
  The PLCnCLI version must match the current SDK version (2020.0.0). Downward compatibility cannot be ensured.
– One database for several DataLogger sessions
  If you configure two or more DataLogger sessions to write to the same database, only the data from one session is transferred to the database on the SD card. There is no message that not all of the data can be stored.
– STOP of the controller after debugging
  After setting breakpoints in debug mode, the controller can switch to the STOP state when the project is restarted.
– PROFINET connection setup
  In the case of very large PROFINET quantity structures, the PROFINET connection setup can take several minutes.
– PROFINET connection interruptions
  Frequent calls of the “Read Record” and “Write Record” function blocks can occasionally interrupt the PROFINET connection.
– EtherNet/IP™
  If you enable the controller firewall in the WBM, EtherNet/IP™ is no longer available.
  To be able to use EtherNet/IP™ with enabled firewall, you have to activate the ports for incoming and outgoing connections subsequently (port 44818 and port 2222).
– C++ projects
  C++ projects that were created using “WorkerThread” in SDK version 2019.0 LTS have to be compiled again using an SDK version ≥ 2019.3.
  Otherwise, the “WorkerThread” is not loaded after restart of the application.
– Copying configuration files
  If you use the Linux command “scp” **without** the option “-p” to copy configuration files from a Linux PC to the directory /opt/plcnext/projects on the controller, the file permissions are partly set incorrectly.

Remedy:
After copying the configuration files, use the Linux command “chmod” to set the file permissions in such a way that the firmware can delete the configuration files in case of “Download Changes” (group: “plcnext” , owner: “plcnext_firmware”).

– Large amount of retain data

  In projects with a large amount of retain data, the PLC task watchdog infrequently triggers.

– Error message on HMI display

  While a program or program changes are being downloaded to the controller, the “503 (busy)” error message is displayed on a connected HMI display.

30 Changes in firmware version 2019.9

If you changed system files via a “root” access, the controller might not start up correctly after a firmware update.
In this case, reset the controller to default setting type 1.

30.1 New functions

New function in the WBM

A diagnosis for the local bus is available in the WBM.

PROFINET System Redundancy Layer (SRL)

In operation as PROFINET controller or PROFINET device the controller now supports PROFINET SRL.

Forcing GDS variables

You can now force GDS variables and thus the I/Os connected via PROFINET or Axioline F.

PROFINET controller: Behaviour of the BF-C LED

If you do not configure a PROFINET device or interrupt the connection using the "AR_MGT" function block, the BF-C LED remains switched off.

30.2 Error corrections

- Freezing of the outputs
  A high CPU load and frequent PROFINET disconnections could cause the outputs to freeze.
  This error has been rectified.
- Delay of a variable value during the start of the controller
  If 24 V voltage was applied to a digital input of the Axioline F local bus and the signal was transmitted with a global variable or a port link into the application, there could be a delay of several cycles. The error occurred during the start of the controller.
  This error has been rectified.
- Changing the IP address via DCP
  Changing the IP address via DCP could affect the real-time of the project and trigger the PLC task watchdog.
  This error has been rectified.
- CPU load after PROFINET connection setup
  After many PROFINET connections had been established, the controller could reach 100 % CPU load and the firmware could no longer react.
  This error has been rectified.
- Resetting the IP address via DCP
  If there was a connection to at least one configured PROFINET participant, the PLC task watchdog could be triggered when the IP address was reset via DCP.
  This error has been rectified.
- Setting breakpoints in debug mode
  If a breakpoint was set in debug mode, the PLC task watchdog could be triggered.
  This error has been rectified.
- Error of the Notification Logger
  If an error occurred during a restart of the controller, the Notification Logger was not automatically configured and notifications were not displayed in PLCnext Engineer.
  This error has been rectified.

30.3 Known limitations and errors

When using SafetyBridge Technology, note the following:
To ensure reliable operation in conjunction with SafetyBridge Technology, make the following settings in PLCnext Engineer.
“/ Profinet” editor group, “Interface List” editor:
Reduction ratio: 8 (or higher)
Monitor factor: 6 (or higher)

- System variables
  The system variables ESM_DATA.ESM_INFOS[*].ESM_TICK_COUNT and ESM_DATA.ESM_INFOS[*].ESM_TICK_INTERVAL are no longer supported.
  Now, the value of the variables is always 0.
- Copying configuration files
  If you use the Linux command “scp” **without** the option “-p” to copy configuration files from a Linux PC to the directory /opt/plcnext/projects on the controller, the file permissions are partly set incorrectly.
  Remedy:
  After copying the configuration files, use the Linux command “chmod” to set the file permissions in such a way that the firmware can delete the configuration files in case of “Download Changes” (group: “plcnext” , owner: “plcnext_firmware”).
- Deinstalling a licensed app from the PLCnext Store
  The deinstallation of a licensed app via the PLCnext Store is not possible if you manually deleted the license from the controller beforehand.
- Large amount of retain data
  In projects with a large amount of retain data, the PLC task watchdog infrequently triggers.

– Error message on HMI display

  While a program or program changes are being downloaded to the controller, the "503 (busy)" error message is displayed on a connected HMI display.

– C++ projects

  C++ projects that were created using “WorkerThread” in SDK version 2019.0 LTS have to be compiled again using an SDK version ≥ 2019.3.
  Otherwise, the “WorkerThread” is not loaded after restart of the application.

– EtherNet/IP™

  If you enable the controller firewall in the WBM, EtherNet/IP™ is no longer available.
  To be able to use EtherNet/IP™ with enabled firewall, you have to activate the ports for incoming and outgoing connections subsequently (port 44818 and port 2222).

31 Changes in firmware version 2019.0.4 LTS

When using SafetyBridge Technology, note the following:
To ensure reliable operation in conjunction with SafetyBridge Technology, make the following settings in PLCnext Engineer.
“/ Profinet” editor group, “Interface List” editor:
Reduction ratio: 8 (or higher)
Monitor factor: 6 (or higher)

Firmware version 2019.0.4 LTS offers the same features as firmware version 2019.0 LTS, but the error described below has been rectified.

31.1 Error corrections

– Freezing of the outputs
  A high CPU load and frequent PROFINET disconnections could cause the outputs to freeze.
  This error has been rectified.

32 Changes in firmware version 2019.6.3

When using SafetyBridge Technology, note the following:
To ensure reliable operation in conjunction with SafetyBridge Technology, make the following settings in PLCnext Engineer.
“/ Profinet” editor group, “Interface List” editor:
Reduction ratio: 8 (or higher)
Monitor factor: 6 (or higher)

Firmware version 2019.6.3 offers the same features as firmware version 2019.6, but the error described below has been rectified.

32.1 Error corrections

– Freezing of the outputs
  A high CPU load and frequent PROFINET disconnections could cause the outputs to freeze.
  This error has been rectified.

33 Changes in firmware version 2019.6

If you changed system files via a “root” access, the controller might not start up correctly after a firmware update.
In this case, reset the controller to default setting type 1.

33.1 New functions

PROFINET stack

The PROFINET controller/device stack was updated from version 6.2 to version 6.3:

– MRP Client function
– SRL S2 function

MRP (Media Redundancy Protocol)

You can use the controller as a Media Redundancy Client (MRC) in an MRP ring. The MRC is activated and configured via the higher-level controller and PDEV objects.
Only the default domain 0xFFFFFFFF is supported.

DataLogger

The DataLogger transfers real-time date from the GDS (Global Data Space) to an SQL based database for recording and storage.
The scope of functions of the DataLogger was extended:

– New recording modes:
  – Storage in case of changes
  – Continuous
– Historical data can be called within a defined period of time.

For more detailed information on the DataLogger, please refer to the “PLCnext Technology” user manual.

Updating Axioline F I/O data

The behavior for updates of Axioline F I/O data was changed:

If you do not select a trigger task, the firmware automatically calculates an interval for updating the Axioline F I/O data from the interval times of all available cyclic tasks. Event or idle tasks are not taken into account for the calculation. If no cyclic task is available, the data of the Axioline F modules is updated every 500 µs.

As an alternative to a cyclic task, you can select an idle task for updating Axioline F I/O data.

Interval times for cyclic tasks

The interval time of a cyclic task now has to be at least 1 ms.
For projects that were created using an earlier firmware version and contain cyclic tasks with interval times < 1 ms, the PLC task watchdog might trigger.

TON_R_LTIME, TP_R_LTIME and TOF_R_LTIME function blocks

The time accuracy of the TON_R_LTIME, TP_R_LTIME and TOF_R_LTIME function blocks was improved. Now, also times < 1 ms can be recorded.
To be able to use the improved time accuracy of the function blocks in existing projects, you have to compile the project again and transfer it to the controller.

New functions in the WBM

– On the “Profinet” page, the PROFINET topology is displayed in tree view.
– You can activate the support of an external SD card via the WBM.
  If you deactivate the support of an SD card, and the SD card is then inserted into the controller, the SD card is not recognized during the initialization phase of the controller. Therefore, the data from the internal parameterization memory is **not** automatically copied to the SD card.
– The name of the PLCnext Engineer project running on the controller is displayed.
– On the “License Management” page, you can view the licenses of the apps from the PLCnext Store that are installed on the controller.

OPC UA Historical Access (HA)

The integrated OPC UA server (eUA) supports access to historical data (OPC UA Historical Access Specification).

PROFINET controller/device function

– Now, you can select if an application relation (AR) is to be established while the boot project is being loaded.
– The DNS names of the PROFINET controller and the PROFINET devices can now be set via the “IConfigurationService” RSC service.
Via the RSC interface, the functions Read(), Write(), GetControllerName() und GetDeviceNames() are now available.

For more detailed information on RSC (Remote Service Calls), please refer to the “PLCnext Technology” user manual.

33.2 Error corrections

– HTTPS connection
After 20 minutes, the connection of an HTTPS client to the HTTPS server used to be disconnected automatically.
This error has been rectified.
– Static_String array in C++ programs
In an array of the type Static_String (C++), the array size was miscalculated.
This error has been rectified.
– Disconnection from the HMI web server
After the DISABLE system variable of the HMI_CONTROL data structure was set to TRUE, and this way, the connection to the HMI web server was set, the PLCnext Engineer HMI web server and the client were able to connect nevertheless.
This error has been rectified.
– Controller breakdown in the PROFINET network
If in a larger PROFINET network, the IP address of a PROFINET device was changed, the controller used to break down.
This error has been rectified.
– PROFINET diagnostic state in the WBM
If the application relation (AR) of a PROFINET device was disabled, a wrong diagnostic state was displayed on the “Profinet” page in the WBM.
This error has been rectified.
– AXC F 2152 as a PROFINET device
The AXC F 2152 could not be operated as a PROFINET device under PROFINET controllers from third-party manufacturers.
This error has been rectified.
– SINT type process data elements
Linking SINT type process data elements led to a runtime error in the application program (LED FAIL).
This error has been rectified.
– Reading out OPC UA subscriptions
Reading out OPC UA subscriptions via the “UA Expert” tool was not possible.
This error has been rectified.
– OPC UA: “IecTime” data type variables
“IecTime” data type variables were not displayed correctly.
This error has been rectified.
– OPC UA: Index based monitoring
Independent of the index set, all data of an array was output during index based monitoring.
This error has been rectified.
– OPC UA: Index calculation
Access to an array of the data type StaticString resulted in errors in index calculation.
This error has been rectified.
– Traces in the format YYYYMMDD
For traces in the format YYYYMMDD, sometimes the leading 0 was missing for the day.
This error has been rectified.
– Setting breakpoints
Setting breakpoints in extensive ST code worksheets resulted in controller freezing.
This error has been rectified.
– Event task “Cold Start”
In the following cases, the event task “Cold Start” was not executed:
  – After resetting the controller to default setting type 1 or 2
  – After SFTP transmission of the project and subsequent reboot of the controller

This error has been rectified.
– Installed apps from the PLCnext store
Resetting the controller to default setting type 1 or 2 resulted in licensing conflicts for apps from the PLCnext store that were installed on the controller.
This error has been rectified.

33.3 Known limitations and errors

– System variables

  The system variables ESM_DATA.ESM_INFOS[*].ESM_TICK_COUNT and ESM_DATA.ESM_INFOS[*].ESM_TICK_INTERVAL are no longer supported.
  Now, the value of the variables is always 0.

– C++ projects

  C++ projects that were created using “WorkerThread” in SDK version 2019.0 LTS have to be compiled again using an SDK version ≥ 2019.3.
  Otherwise, the “WorkerThread” is not loaded after restart of the application.

– EtherNet/IP™

  If you enable the controller firewall in the WBM, EtherNet/IP™ is no longer available.
  To be able to use EtherNet/IP™ with enabled firewall, you have to activate the ports for incoming and outgoing connections subsequently (port 44818 and port 2222).

– HMI applications

  You cannot access an HMI application while a PLCnext Engineer project is downloaded to the controller.
  In this case, an error message is displayed in the web browser.

– Copying configuration files

  If you use the Linux command “scp” **without** the option “-p” to copy configuration files from a Linux PC to the directory /opt/plcnext/projects on the controller, the file permissions are partly set incorrectly.
  Remedy:
  After copying the configuration files, use the Linux command “chmod” to set the file permissions in such a way that the firmware can delete the configuration files in case of “Download Changes” (group: “plcnext” , owner: “plcnext_firmware”).

– Deinstalling a licensed app from the PLCnext Store

  The deinstallation of a licensed app via the PLCnext Store is not possible if you manually deleted the license from the controller beforehand.

– Availability of network services

  In case of frequent and fast linkUp and linkDown in large PROFINET quantity structures, the controller can infrequently reach 100% CPU load. In this case, network services are no longer available.

– Restart of a project

  For projects with extremely long task cycle times (e.g., 15000 ms), the restart of the project after a project download can take several minutes.

– Setting network settings via DCP

  Setting network settings via DCP can affect the real-time of the project. For watchdog times < 10 ms, this can infrequently result in a triggering of the PLC task watchdog.

– SafetyBridge Technology

  Reliable operation in conjunction with SafetyBridge Technology is not ensured.
  If you want to use SafetyBridge Technology, use the controller with firmware version 2019.3.

34 Changes in firmware version 2019.3

34.1 New functions

PRL (Phoenix Redundancy Layer)

The PROFINET device functionality has been extended to include the PRL function (Phoenix Redundancy Layer).

EtherNet/IP™ device function

You can use the controller as an EtherNet/IP™ device.

Dynamic bus configuration

The controller supports the dynamic bus configuration of the Axioline F local bus.

Left-alignable INTERBUS master

The controller now supports left-alignment of the INTERBUS AXC F XT IB master (Order No. 2403018).

PLCnext Store: New app types

The controller supports the execution of the app types “function extension” , “runtime” , “library” , and “solution app” .

34.2 Known limitations and errors

- Static_String array in C++ programs
  The array sizes are incorrectly calculated in Static_String-type arrays (C++), meaning that access to the second element contained in the array and to those following is incorrect.
  String arrays in IEC 61131 programs are not affected by this.
- AXC F 2152 as a PROFINET device
  The AXC F 2152 cannot be operated as a PROFINET device under PROFINET controllers from third-party manufacturers.
- Monitor time of PROFINET data
  The PROFINET data monitor time must be at least 24 ms. The monitor time is the product of “Reduction ratio” and “Monitor factor” (in PLCnext Engineer: “Profinet” editor group, “Interface list” editor).

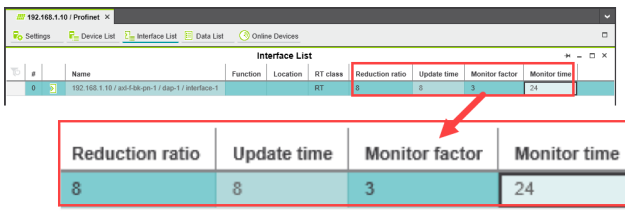


Figure 1 Monitor time

- Metrics that can be transferred to the PROFICLOUD
  You can transfer up to 194 variable values as metrics into the PROFICLOUD.
- Very high CPU utilization
  The online connection to PLCnext Engineer may be interrupted when the controller CPU utilization is very high.
  The connection interruption is indicated in PLCnext Engineer without any indication of the cause.
- Setting breakpoints is not supported
  Setting breakpoints in debug mode results in the controller becoming unreachable.

35 Changes in firmware version 2019.0 LTS

Please note:
Updating to firmware version 2019.0 LTS will reset the controller to factory default setting type 1. Any application-specific data and projects on the controller will be deleted.

35.1 New functions

Download changes

The controller now supports the “Download Changes” function. With the “Download Changes” function, program changes can be transferred to the controller during operation without interruption.

This is subject to the following conditions:

– You have not made any changes to the bus configuration.
– You have not changed the process data assignment.
– You have not changed the properties of the existing tasks (e.g., task type, interval, watchdog).
– You have not deleted any tasks or added any new tasks.

Left-alignment of Axioline F extension modules

The controller now supports left-alignment of the Axioline F AXC F XT ETH 1TX extension module (left-alignable Ethernet interface, Order No. 2403115).

New functions in the WBM

New functions are now available in the web-based management (WBM), e.g., PROFINET diagnostics and firewall configuration.

Declaring retentive data

You can now also declare variables from C++ programs as retentive data in PLCnext Engineer.

Updating Axioline F I/O data

You can now specify the refresh interval for Axioline F I/O data. This is done by selecting which task triggers the Axioline F I/O data update in the PLCnext Engineer project.

To do this, proceed as follows:

- Double-click on the “Axioline F (x)” node in the “PLANT” area.

The “/ Axioline F” controller editor group opens.

- Select the “Trigger task” view in the “Settings” editor.
- In the drop-down list, select the task that is to trigger the Axioline F I/O data update.

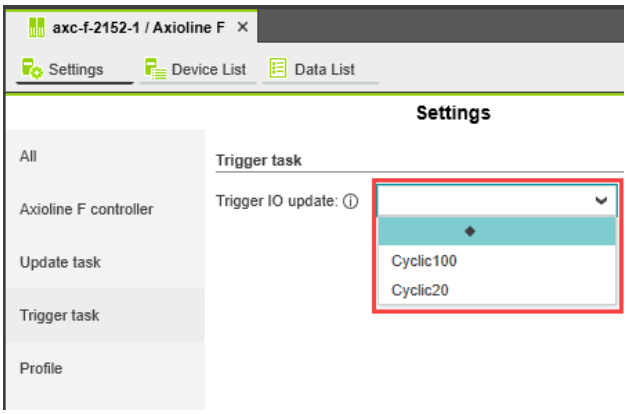


Figure 2 Select Trigger task

If you do not select a task, the update will occur by default every 50 ms.

35.2 Known limitations and errors

– AXC F 2152 as a PROFINET device

  The AXC F 2152 cannot be operated as a PROFINET device under PROFINET controllers from third-party manufacturers.

– Downloading PC Worx Engineer projects to the controller

  You can only download PLCnext Engineer projects to the controller with firmware version 2019.0 LTS that were created and compiled in PLCnext Engineer version 2019.0 LTS. Projects that you created in PC Worx Engineer must be re-created in PLCnext Engineer.

  If you download a PC Worx Engineer project to the controller with firmware version 2019.0 LTS, the project will not run on the controller. However, no error message is displayed in PLCnext Engineer.

Please note:
The PC Worx Engineer software has been renamed to PLCnext Engineer:
Name up to Version 7.2.3: PC Worx Engineer
Name starting from Version 2019.0 LTS:
PLCnext Engineer

– Monitor time of PROFINET data

  The PROFINET data monitor time must be at least 24 ms. The monitor time is the product of “Reduction ratio” and “Monitor factor” (in PLCnext Engineer: “Profinet” editor group, “Interface list” editor).

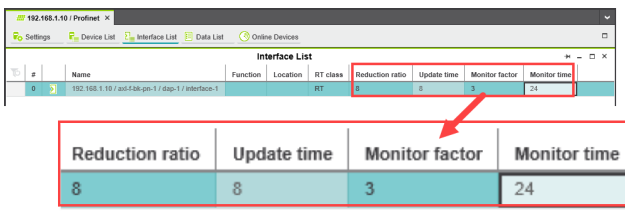


Figure 3 Monitor time

– Metrics that can be transferred to the PROFICLOUD

  You can transfer up to 194 variable values as metrics into the PROFICLOUD.

– Exceeding CPU system limits

  Exceeding the CPU system limits for the controller may result in an interruption of the online connection to PLCnext Engineer.
  The connection interruption is indicated in PLCnext Engineer without any indication of the cause.

– Setting breakpoints is not supported

  Setting breakpoints in debug mode results in the controller becoming unreachable.

36 Changes in firmware version 1.2.0

36.1 New functions

Design of a PLCnext Inline station

As an alternative to an Axioline F station, you can now set up a PLCnext Inline station using the controller. To do so, you need the AXC F IL ADAPT Inline adapter terminal (Order No. 1020304). You can directly install the Inline modules in series on the adapter terminal.

License verification

When an SD card is used, the controller now verifies if the SD card contains a Phoenix Contact license. You can only use the controller together with an appropriate Phoenix Contact SD card.

36.2 Notes on firmware downgrades and resetting the controller

For performing firmware downgrades, please note the following:

Downgrade to a firmware version ≤ 1.0.2

After downgrading to a firmware version ≤ 1.0.2, you can only use the controller with an SD card. Using it without an SD card is possible starting from firmware version 1.1.0.

- Ensure that the SD card has been inserted before switching the controller on, in order that the controller can use it.
- Only use an SD card provided by Phoenix Contact.

Downgrade to firmware version 1.0.0

After downgrading to firmware version 1.0.0, you can only use the reset button of the controller while an application is running.
Resetting the controller to default setting type 2 is not possible.

For resetting the controller to default setting type 2, please note the following:

When restoring to default setting type 2, the firmware of the controller is also reset to the delivery state. Controllers with a firmware version ≤ 1.0.2 can only be used **with** an SD card. Using them without an SD card is possible starting from firmware version 1.1.0.

- Ensure that the SD card has been inserted before switching the controller on, in order that the controller can use it.
- Only use an SD card provided by Phoenix Contact.

36.3 Known limitations and errors

- Time-outs during the communication with PCP devices

  If more than eight PCP devices are connected at the same time, time-outs can occur during the communication between the controller and the PCP devices.
- Maximum permissible number of Axioline F local bus devices

  Currently, a maximum of 30 Axioline F local bus devices is supported.
- Interrupting the PROFINET communication

  When transmitting files via SFTP to the controller, the PROFINET communication is interrupted.
- Function of the reset button

  When the controller is reset to default setting type 2, all LEDs light up after approx. 30 s.
  To actually restore the controller to default setting type 2, you need to press and hold the reset button for another 2 s after all LEDs have lit up.

37 Changes in firmware version 1.1.0

Please note:
After the update to firmware version 1.1.0, the controller has to be restarted.

37.1 New functions

Use of SD card now optional

The SD card is now optional and is no longer mandatory for operating the controller.

– Operation without SD card:
  All data is saved on the internal parameterization memory. If you make changes to files and directories on the internal parameterization memory, the Linux operating system generates an overlay filesystem from the changed files and directories.
– Operation with SD card:
  If you use an SD card, all application-specific data (e.g. network configuration, project bus configuration, etc.) is saved to the SD card.
  Two cases of SD card use can be distinguished:
  1) There is no overlay filesystem on the SD card:
     If there is an overlay filesystem on the internal parameterization memory, it is copied to the SD card.
  2) There already is an overlay filesystem on the SD card:
     If there is an overlay filesystem on the internal parameterization memory, it is **not** copied to the SD card.
     The controller accesses the overlay filesystem on the SD card. The overlay filesystem on the internal parameterization memory is deleted.

Please note:
The SD card is recognized during initialization of the controller. If you insert the SD card during operation, the SD card will not be detected.
Make sure that the SD card has been inserted before you switch on the controller.

Memory expanded

– The program memory of the controller has been expanded from 4 MB to 8 MB.
– The data memory of the controller has been expanded from 8 MB to 16 MB.

38 Changes in firmware version 1.0.2

Please note:

After an update from firmware version 1.0.0 to firmware version 1.0.2, high-level language programs created with the Phoenix Contact SDK version 1.0.0 will no longer be executable. In this case, proceed as follows:

- Download the latest version of the Phoenix Contact SDK from phoenixcontact.net/products and install it.
- Compile existing high-level language programs with the latest version of the Phoenix Contact SDK.

When updating from firmware version 1.0.1 to firmware version 1.0.2, this procedure is not necessary.

38.1 Error corrections

– PROFINET configuration

  The controller was stopped when transmitting a PC Worx Engineer project with a faulty PROFINET configuration to the controller.
  This error has been rectified.

38.2 Known limitations and errors

– Controller breakdown

  In some rare cases the controller may break down. In case of a controller breakdown, power is disconnected to the I/O modules contained in the bus configuration.

39 Changes in firmware version 1.0.1

Please note:

After an update from firmware version 1.0.0 to firmware version 1.0.1, high-level language programs created with the Phoenix Contact SDK version 1.0.0 will no longer be executable. In this case, proceed as follows:

- Download the latest version of the Phoenix Contact SDK from phoenixcontact.net/products and install it.

Compile existing high-level language programs with the latest version of the Phoenix Contact SDK.

39.1 Error corrections

– Task processing time

  The programmed maximum task processing time was exceeded by occasional task processing time outliers. The ESM watchdog was triggered.
  This error has been rectified.

– User authentication

  A user authentication security vulnerability was patched.

– Requested memory

  An error occurred when memory was requested from a C++ program. The requested memory was not released again.
  This error has been rectified.

– Data Access Service

  An error in the Data Access Service (online view in the “Data List” editor in PC Worx Engineer) has been rectified.

– Subscription service

  During data query via OPC UA, an error occasionally occurred in the subscription service.
  This error has been rectified.