

SFW RFC 4072S, BPC 9102S and AXC F XT SPLC 3000 - CHANGE NOTES

Change notes for the safety-related firmware of RFC 4072S,
BPC 9102S and AXC F XT SPLC 3000

Application note
111044_en_02

© Phoenix Contact 2023-11-27

1 General notes


This document describes all changes to the safety-related firmware of the iSPNS 3000 in the RFC 4072S Remote Field Controller as well as of the SPLC 3000 in the BPC 9102S industrial box PC and in the left alignable safety-related AXC F XT SPLC 3000 controller as of the following firmware versions:


- RFC 4072S, Order No. 1051328, 02.00.0010
BPC 9102S, Order No. 1246285:
- AXC F XT SPLC 3000, Order No. 1160157: 02.10.0006

Current version of the safety-related firmware: 02.10.0006

Table of contents

1	General notes	1
2	Changes in firmware version 02.10.0006	2
2.1	Error corrections	2
3	Changes in firmware version 02.10.0005	3
3.1	New funktions	3
3.2	Error corrections	3
4	Changes in iSPNS firmware version 02.00.0010	4
4.1	New funktions	4
4.2	Error corrections	4

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


 This document is valid for all products listed in the “General notes” on page 1.

2 Changes in firmware version 02.10.0006


NOTE: Unsuccessful update process possible

From 27.11.2023, use the file "SPLC_02.10.0006_Bundle_UPD_2.2.0.0.zip" to avoid an unsuccessful update process of the safety-related firmware (see section 2.1 "Error corrections").

AXC F XT SPLC 3000:

 If you operate the AXC F XT SPLC 3000 on an AXC F 2152, the PLCnext firmware version 2023.6 or later must be installed on the AXC F 2152. We recommend setting the cycle time of the SPLC 3000 to $T_{ZSPLC} \geq 10$ ms.

RFC 4072S and BPC 9102S:

 In order to update to safety-related firmware version 02.10.0006, PLCnext firmware version 2023.0.4 LTS or later must be installed on your controller.

To update the safety-related firmware to version 02.10.0006, proceed as described in application note AH XX RFC 4072S SFW UPD (109812). The update method described in the application note is currently approved for the RFC 4072S and the BPC 9102S.

- Check the integrity of firmware update file "SPLCFirmware2.10.0006Update.exe" using the following SHA-256 checksum:

SHA-256 checksum before 27.11.2023:

**E1CE8411433E8114A5105D09AAE17CD3
03450F063C1326C01E9003BD9D558DF9**

SHA-256 checksum from 27.11.2023 when using the file "SPLC_02.10.0006_Bundle_UPD_2.2.0.0.zip":

**08C619D565BCA2F47CD33EFC4A2D0A13
73C7DDECA68CA67428E2766E98135FF6**

After a successful update, the following version of the safety-related firmware is displayed after entering the correspondig command in the Windows prompt:

SK1 SLL: 2.1.7
SK1 TLL0: 1.20.21
SK1 TLL1: 1.20.21
SK1 APP: 2.10.6
SK1 FPGA: 2.34.1
SK1 IWD: 1.2.7
SK2 SLL: 1.6.6
SK2 TLL0: 1.20.21
SK2 TLL1: 1.20.21
SK2 APP: 2.10.6

2.1 Error corrections

- The management/diagnostic variables parameterized in the application project could not be used properly if the application project was created with a PLCnext Engineer project template version 2022.X or older.
This error has been rectified.
- Update from 27.11.2023:
The use of the firmware update file previously provided by Phoenix Contact could lead to an unsuccessful update process if an ACF component (*.acf.config files) was instantiated at the same time.
This error has been rectified when using the file "SPLC_02.10.0006_Bundle_UPD_2.2.0.0.zip".

3 Changes in firmware version 02.10.0005

RFC 4072S and BPC 9102S:



In order to update to safety-related firmware version 02.10.0005, PLCnext firmware version 2023.0.4 LTS or later must be installed on your controller.

To update the safety-related firmware to version 02.10.0005, proceed as described in application note AH XX RFC 4072S SFW UPD (109812). The update method described in the application note is currently approved for the RFC 4072S and the BPC 9102S.

- Check the integrity of firmware update file “SPLCFirmware2.10.0005Update.exe” using the following SHA-256 checksum:

**AE111E7505B0C8451954349BDFD1BC0062400157C9
F85DD9D3F4BF5C5F26B8F4**

After a successful update, the following version of the safety-related firmware is displayed after entering the correspondig command in the Windows prompt:

```
SK1 SLL: 2.1.7
SK1 TLL0: 1.20.21
SK1 TLL1: 1.20.21
SK1 APP: 2.10.5
SK1 FPGA: 2.34.1
SK1 IWD: 1.2.7
SK2 SLL: 1.6.6
SK2 TLL0: 1.20.21
SK2 TLL1: 1.20.21
SK2 APP: 2.10.5
```

3.1 New funktions

- Support of recipes in the safety-related application
The following function blocks are available in PLCnext Engineer after inserting the “RecipeFile_SF” library:
 - SF_RecipeDeleteDataSet
 - SF_RecipeDeleteFile
 - SF_RecipeRead
 - SF_RecipeWrite
 With these function blocks, it is possible to store variable values in the application program beyond restarting the safety-related controller in order to restore or reload them afterwards on request.
- Safety-related log file (safety protocol/log)
The following information is stored in the safety-related log file:
 - Version and build date of the safety-related firmware
 - Changes to the controller password of the safety-related controller
Each change is logged only once.
- Support of the F-Device of the safety-related controller
The safety-related controller (SPLC 3000 and iSPNS 3000) can be operated as a lower-level F-Device on a higher-level PROFIsafe F-Host. The PROFIsafe profile version 2.4 and version 2.6MU1 are supported.
- SAFE OS version 3.6
The number of function block instances (see “Characteristic data of the safety-related controller” in the device-specific user manual) has been increased from 8192 to 16384, maximum.

3.2 Error corrections

- In the event of a voltage failure, it was possible to delete non-safety-related log files on the inserted SD card and to recreate the log file system.
This error has been rectified by optimizing synchronization of the standard controller and the safety-related controller.
- When using the fan module on the RFC 4072S, the safety-related controller sporadically switched to the safe state and issued an error with error code 0x924E at the same time.
This error has been rectified.

4 Changes in iSPNS firmware version 02.00.0010

RFC 4072S:



In order to update the safety-related firmware version 02.00.0010, PLCnext firmware version 2022.0.5 or later must be installed on your controller.

To update the safety-related firmware to version 02.00.0010, proceed as described in application note AH XX RFC 4072S SFW UPD (109812). The update method described in the application note is currently only approved for the RFC 4072S.

- Check the integrity of firmware update file "SPLCFirmware2.00.0010Update.exe" using the following MD5 checksum:

AFB95625CAC0D9176DEA09376E0839CC

After successful update, the following version of the safety-related firmware is displayed after entering the corresponding command in the Windows prompt:

```
Sk1 SLL: 2.1.7
Sk1 TLL0: 1.20.10
Sk1 TLL1: 1.20.10
Sk1 APP: 2.0.10
Sk1 FPGA: 2.26.1
Sk1 IWD: 1.2.5
Sk2 SLL: 1.6.6
Sk2 TLL0: 1.20.10
Sk2 TLL1: 1.20.10
Sk2 APP 2.0.10
```

4.1 New funktions

With every restart of the RFC, the following data is saved to the log file of the safety-related controller:

- iSPNS firmware version
- Version creation date

4.2 Error corrections

- Channel synchronization error
Due to the tolerance setting of the channel synchronization monitoring between channel 1 and channel 2 of the safety-related controller being too low, the safety-related controller sporadically switched to the safe state in large safety-related application projects. Error codes 0x8013 and 0x9013 were displayed.
This error has been rectified.
- Synchronization error between standard controller and safety-related controller
Due to the synchronization of the standard controller and the safety-related controller being carried out too early after a restart, the safety-related controller was able to switch to the safe state.
Now, the first synchronization is implemented once the energy storage for undervoltage buffering (UPS) has been fully charged.
This error has been rectified.
- Sporadic change to the safe state
In rare cases, the safety-related controller switched to the safe state after 49 days while displaying error code 0x80A8.
This error has been rectified.
- Optimization of the startup behavior regarding robustness.