Control Systems and Components

Saia NT Technical Document

Step7 Extended Know-How Protection

Version:	Pre-1
Date:	October 31th, 2007
Status:	Preliminary
Classification:	For OEM customers only
File name:	Step7 Extended Know How Protection.doc

Revision History:

Version	Description of Version	Issue Date
Pre-1	Initial version	2007.10.31

Table of Contents

1 Step7 extended know-how protection

1.1 General

The S7 Know How Protection Flag in S7-Blocks does not Protect Blocks from copying from one PLC to other PLC, and with some knowledge it is possible to read a Know How Protected block.

This document is intended to describe how to configure a know-how protection for S7 Blocks, which solve the above described problems. The Idea is similar as on the M487 with FW-Extension. If the know-how protection Flag on a PLC block is set, and the PLC block is not stored in the SRAM (e.g. in a Flash), the MPI read routine of PLC blocks, sends only the block header back. With this mechanism it is not possible to copy PLC blocks from one PLC to other PLC with the Simatic Tool.

[REF 1] describes how to store S7 Blocks in Flash.

1.1.1 References

[REF 1]: Step7 Memory Extension Step7 Memory Extension_V2.pdf

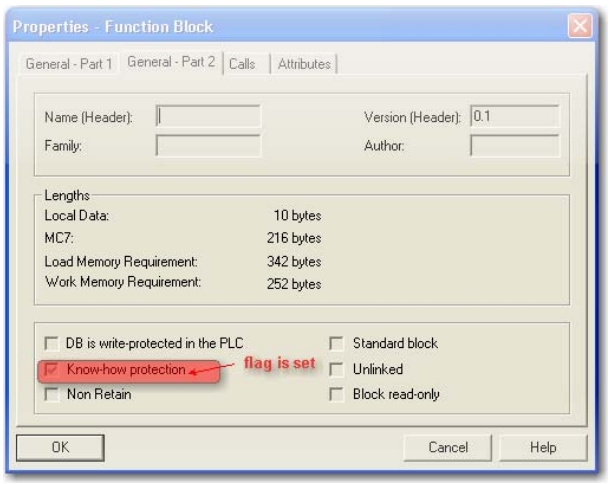
[REF 2]: FTP Configuration User Documentation for HTTP-Direct, FTP and FLASH_V1.5.pdf

1.2 Rules

The extended know-how protection works only if:

- The plc block is stored in the extended Step7 memory, **and**

- The know-how protection flag is set.



1.2.1 Restriction

- If a block already exists in the PLC file system, the block from the flash will not overwrite it and the extended know-how protection is not active.
- After downloading PLC blocks with the SIMATIC Software to the PLC, the blocks are copied into the PLC file system. The block in flash is not valid anymore and the extended know-how protection is not active.
- DB’s are never know-how protected.

2 Configuration FTP-Server

2.1 General

At startup, the FTP-Server can be configured with modified parameters. For downloading the PLC blocks, and to protect the PLC blocks there are two different FTP-Server configuration Files necessary.

2.2 Configuration for creating extended know-how protected blocks

To create the S7PROG directory and to copy your know-how protected blocks from the PLC directory to the S7PROG directory you have to login as PLC user.

After coping the plc block, you should change the configuration File to protect the PLC blocks for reading with FTP. The following configuration creates a PLC user and a configuration user.

```
# ****************************************
# FTP Configuration file
#
# ****************************************
#
FTPPLCBlocks=on                          # PLC blocks are visible
FTPRemoveDefaultUser=1                   # default user is removed
UserName=PLC,plcgroup,0x01,0xFF          # User = PLC
                                         # password = plcgroup
                                         # Belong to PLC Group.
                                         # Have access to all files / directories
                                         # By default read/write access
UserName=config,configgroup,0x02,0xFF    # User = config
                                         # password = configgroup
                                         # Belong to config Group.
                                         # Have access to all files / directories
                                         # By default read/write access
```

2.3 FTP Configuration for runtime

To protect the PLC files for reading over FTP, there exist two possibility:

- Switch of the FTP – Server

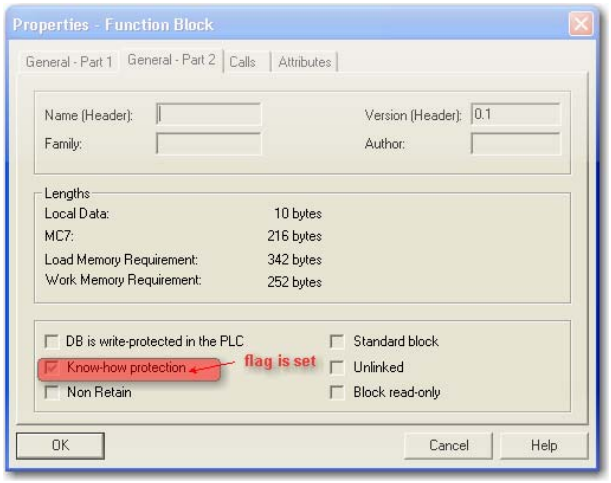
```
# ****************************************
# FTP Configuration file
#
# ****************************************
#
FTPStart=off    # FTP Server is not starting
```

- Switch of the visibility of PLC Blocks

```
# ****************************************
# FTP Configuration file
#
# ****************************************
#
FTPPLCBlocks=off                         # PLC blocks are not visible
FTPRemoveDefaultUser=1                   # default user is removed
UserName=admin,useadmin,0x00,0xFF        # User = admin
                                         # password = useadmin
                                         # Belong to no Group.
                                         # Have access to all files / directories
                                         # By default read/write access
UserName=user1,1234,0x10,0x10,rd_only    # User = user1
                                         # password = 1234
                                         # Belong to user1 Group.
                                         # Have access to all files / directories belonging to user1 group
                                         # defined with read only access
```

3 Example to create a extended know-how protected block

1. Create a know-how protected block with Simatic software. Download the block into the plc.



2. Download the Config file from chapter 2.2 with FTP into the Config directory

3. Close FTP connection and Power off and on the PLC.
4. Start a FTP connection as PLC user.
5. Create the S7PROG directory in the INTFLASH device.
6. Upload the plc block from the PLC to a temporary directory on the PC.
7. Delete the block in the plc.
8. Download the plc block from the temporary directory into the INTFLASH/S7PROG directory.

9. Close the FTP-Connection
10. Start a FTP connection as CONFIG user. (Second user definition in Chapter 2.2)
11. Delete the FTP configuration File on the Flash Device, and download the “Run Time” FTP configuration File. (Chapter 2.3)
12. Close the FTP-Connection, and Power off the PLC.
13. Power on the PLC and open a Defined FTP connection: The plc blocks are not visible anymore.