Security functions

Jump to bottom

Federico Barresi edited this page on Jan 12, 2019 · 3 revisions

With these functions is possible to know the current protection level, and to set/clear the current session password.

Especially because, if you look at the source code, there is an encoding function that translates the plain password before send it to the PLC.

PASSWORD HACKING IS VERY FAR FROM THE AIM OF THIS PROJECT

Detailed information about the protection level can be found in §33.19 of "System Software for S7-300/400 System and Standard Functions".

Function	Purpose
SetSessionPassword	Send the password to the PLC to meet its security level (login)
ClearSessionPassword	Clears the password set for the current session (logout)
GetProtection	Gets the CPU protection level info

SetSessionPassword

Description

Send the password to the PLC to meet its security level.

Declaration

```
public int SetSessionPassword(string Password);
```

Parameters

Name	Type	Note
Address	string	8 chars UTF-8 string

Return value

- 0 : The function was accomplished with no errors.
- Other values : see the Errors Code List.

Remarks

A password accepted by a PLC is an 8 chars string, a greater password will be truncated, and a smaller one will be "right space padded".

ClearSessionPassword

Description

Clears the password set for the current session (logout).

Declaration

```
public int ClearSessionPassword()
```

Return value

- 0 : The function was accomplished with no errors.
- Other values : see the Errors Code List.

GetProtection

Description

Gets the CPU protection level info.

Declaration

```
public int GetProtection(ref S7Protection Protection)
```

Parameters

Name	Type	Note
Protection	S7Protection	see definition below

Struct declaration

```
public struct S7Protection
{
```

```
        public ushort sch_schal;
        public ushort sch_par;
        public ushort sch_rel;
        public ushort bart_sch;
        public ushort anl_sch;
    };
```

Fields description

Name	Value	Meaning
sch_schal	1,2,3	Protection level set with the mode selector.
sch_par	0,1,2,3	Password level, 0 : no password
sch_rel	0,1,2,3	Valid protection level of the CPU
bart_sch	0,1,2,3,4	Mode selector setting (1:RUN, 2:RUN-P, 3:STOP, 4:MRES, 0:undefined or cannot be determined)
anl_sch	0,1,2	Startup switch setting (1:CRST, 2:WRST, 0:undefined, does not exist or cannot be determined)

See also §33.19 of "System Software for S7-300/400 System and Standard Functions"

Return value

- 0 : The function was accomplished with no errors.
- Other values : see the Errors Code List.

S7Helper

S7MultiVar

Clone this wiki locally

https://github.com/fbarresi/Sharp7.wiki.git