Modicon M580 PAC

CSPN Security Target

Version 1.5

Introduction

A CSPN security target is a document specifying the scope of a CSPN evaluation [CSPN]. The Security Target serves as a basis for agreement between the manufacturer of the product and the potential consumer of the product. The Security Target describes the exact security properties of the product in an abstract manner, and the potential consumer can rely on this description because the product has been evaluated to meet this security target.

This security target claims conformance with the requirements from the Protection profile of an industrial programmable logic controller – short-term [PP-PLC] edited by ANSSI.

References

[CSPN]	Certification de Premier Niveau des produits des technologies de l'Information (*First level assessment of IT products*), ref. ANSSI-CSPN-CER/P/01 version 1, ANSSI, 30/05/2011
[PP-PLC]	Protection profile of an industrial programmable logic controller, version 1.1 short-term, GTCSI, ANSSI, July 13, 2015

[CYBERSEC]	Modicon Controllers Platform - Cyber Security Reference Manual, Schneider, May 2015
[M580HARD]	Modicon M580 - Hardware Reference Manual, Schneider, December 2015
[BMENOC]	Modicon M580 - BMENOC03.1 Ethernet Communication Module Installation and Configuration Guide, Schneider, December 2015
[UNITY_INSTALL]	Unity Pro - Installation Manual, Schneider, December 2015
[UNITY_START]	Start Up Guide for Unity Pro Installing an Application, ref UNY USE 40010V20E, Schneider, September 2004
[UNITY_LANG]	Unity Pro - Program Languages and Structure Reference Manual, Schneider, December 2015
[UNITY_MODES]	Unity Pro - Operating Modes, Schneider, December 2015

Target of Evaluation identification

Manufacturer	Schneider
Organization URL	http://www.schneider-eletric.fr
Product's commercial name	Modicon M580
Firmware version	V2.20 & V2.11
Product's category	Programmable Logical Controller (PLC)

The Target of the Evaluation (thereinafter “ToE”) is composed of:

- The BMEP582040 CPU module embedding the V2.20 firmware following the security rules described in the security documents (see assumptions),
- The BMENOC0301 Ethernet module embedding the V2.11 firmware. This module is collocated with the CPU to manage secured communication with upper layer (supervision and engineering software Unity Pro).

The manufacturer of the Modicon M580 CPU is Schneider Electric.

Figure 1 - The M580 CPU

Unity Pro software suite is not included in the scope of the evaluation. It is assumed to be reliable and secure for this evaluation.

PCs are not included in the scope of the evaluation. PCs are assumed to be reliable and secure for this evaluation. The way to harden them is outside the scope of the evaluation but to establish secure communications with the PLC, Windows is supposed to be configured as mentioned in the Cyber Security reference Manual.

The digital input module and the backplane components necessary to use the CPU module and the Ethernet module are out of the scope of the evaluation.

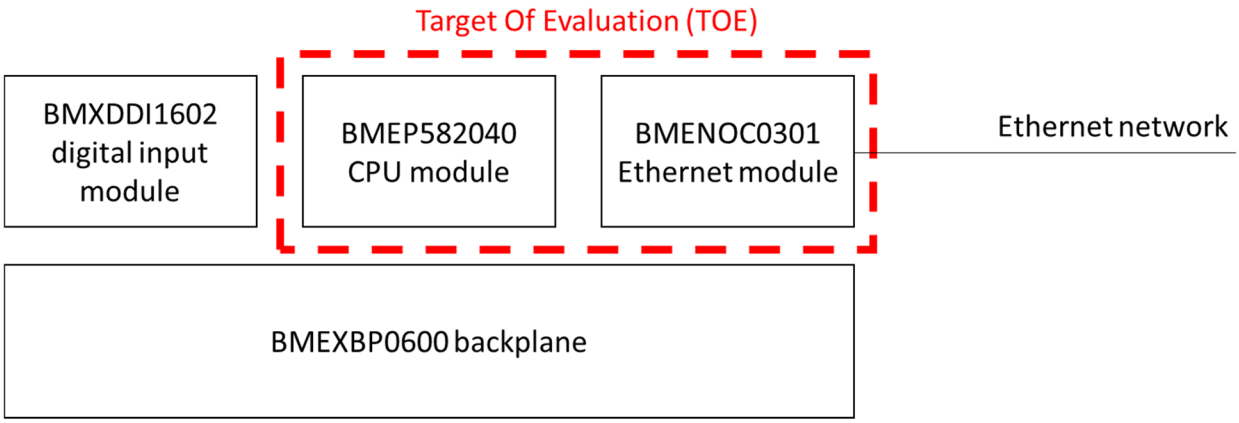


Figure 2 - TOE boundaries

Product description

General description

The Modicon M580 is a programmable logic controller (PLC) designed for controlling and commanding an industrial process, in a continuous way, without human intervention. At each step, the PLC processes the data received from its inputs, the sensors and sends commands to its outputs, the actuators.

The PLC must be able to run in a hostile environment. In particular, it must run despite humidity, dust or unusual temperatures for IT systems, and strong EMC or mechanical constraints.

Features

The Modicon M580 offers the following features:

- User program execution: The M580 runs a user program that processes the inputs and updates the outputs.
- Input/output management: The M580 is able to read local inputs and to write local outputs. These I/O can be digital or analog. These I/O allows the M580 controlling and commanding the industrial process.
- Communication with the supervision: The M580 can communicate with the SCADA for receiving commands and transmitting process data using the Modbus protocol
- Administration functions: The M580 includes administration functions for configuration and programming these administration functions are provided within Unity Pro engineering software suite.
- Remote logging: The M580 supports the definition of a remote logging policy. In particular, it is possible to log security and administration events.

Product usage

The Modicon M580 can be used in diverse architectures but a general framework can be characterized. The M580 is connected to inputs and outputs and to its local HMI through the same communication interface on the field network. Exchanges with the supervision (HMI,

SCADA) are performed through a dedicated interface (via a separate Ethernet Module – BMENOC0301) on the supervision network. In the secured architecture the field network is not directly connected to the supervision network. The PLC is managed with an engineering workstation. Firmware updates and user programs can, in general, be loaded on the PLC through the network, thanks to Ethernet interface.

In the case of a network maintenance, the use of a dedicated network is recommended.

This network should be physically isolated from other networks or, at least, logically isolated.

In practice, an engineering workstation is often plugged on the supervision network. This engineering workstation should not be permanently plugged but only when it is necessary.

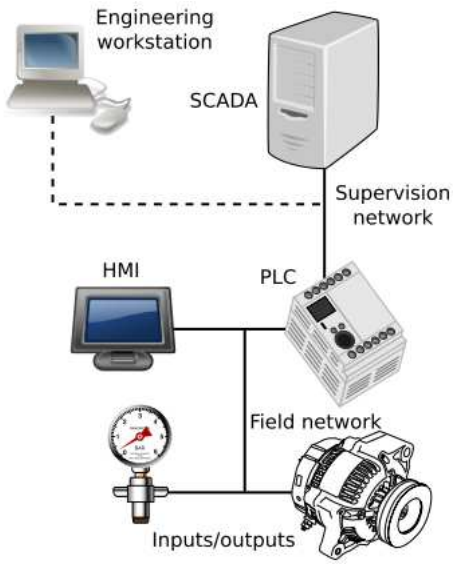


Figure 3 - PLC usage

Users

The users that may interact with the ToE have the following predefined Unity Security Editor's profiles:

- ReadOnly: no application modification is authorized
- Operate: application execution and parameters modification enabled
- Program: all functions are enabled

The same person may own several user accounts corresponding to different profiles.

The administrator role described in the **[Assumptions]** part correspond to the Program role discribed above.

Assumptions

Assumptions on the environment and the use case of the ToE are the following:

- **Security documentation:** The ToE is provided with a complete set of documents for a secure usage: user guides, white paper. All recommendations included in this

documentation are applied prior to the evaluation. At the time of the evaluation, the applicable reference document is: **[CYBERSEC]**.

- **Administrators:** ToE administrators are competent, trained and trustworthy.
- **Premises:** The ToE is located in secure premises with a restricted access limited to trustworthy people. In particular, the attacker does not have access to the physical ports of the ToE. Since identical products to the ToE may be purchased freely, the attacker may purchase one in order to research vulnerabilities by any possible mean.
- **Unevaluated services disabled:** Services of the ToE which are not covered by the security target are disabled in the configuration. Some other services are disabled by user program following security documentation.
- **User application verification:** We assume that the integrity of the user application containing the configuration and the user program (.STU file) is controlled by the administrator before it is uploaded to the ToE and matches his expectation. The configuration must be conform to the requirements specified in the section **[**

- **Threats** covered by security functions

	Persistent denial of service	Firmware alteration	Execution mode alteration	Memory alteration	Flows alteration
Malformed input management	X				
Secure storage of secrets				X	
Secure authentication on administration interface					X
Access control policy					X
Firmware signature		X			
Integrity and authenticity of the ToE memory				X	
Integrity of the PLC execution mode			X		
Secure communication					X

- Evaluation platform**].**
- **Active logging:** We assume that logging are operational and that logs are not corrupted inside the ToE.
- **Logs checking:** We assume that administrators check regularly the local and remote logs produced by the ToE.
- **First configuration:** We assume that the first configuration is uploaded to the ToE through the USB interface. The ToE must be unplugged from the network.
- **Firmware upgrade:** We assume that the firmware upgrade is performed through the USB interface. The ToE must be unplugged from the network.
- **Strong passwords:** The administrators use strong passwords with a combination of upcase, lowcase, numbers and special characters.

Critical assets

Critical assets of the environment

The critical assets of the environment are the following:

- **Control-command of the industrial process:** The ToE controls and commands an industrial process by reading inputs and sending commands to actuators. The availability of these actions must be protected.

- **Engineering workstation flows:** The flows between the ToE and the engineering workstation must be protected in integrity, confidentiality and authenticity.

The security requirements for the critical assets are the following:

Asset	Availability	Confidentiality	Integrity	Authenticity
Control-command of the industrial process	X			
Engineering workstation flows		X	X	X

ToE critical assets

The critical assets of the ToE are the following:

- **Firmware:** In order to work properly, the firmware must be protected both in integrity and authenticity.
- **PLC Memory:** The ToE memory contains the PLC configuration and a program loaded by the users. Its integrity and authenticity must be protected while it's running. Users must be authenticated to change the running configuration on the ToE.
  The configuration contains parameters such as the followings:
  - Access control Policy;
  - RUN/STOP by input only activated;
  - Memory protection activated;
  - Enabled/Disabled Services (FTP, TFTP, HTTP, DHCP, SNMP, EIP, NTP);
  - IPSEC parameters;
  - Syslog parameters;
  - ...
- **Execution mode:** The integrity and authenticity of the execution mode of the ToE must be protected.
- **User secrets:** The user secrets are the passwords used in order to perform the user authentication. There are several kinds of password:
  - the PSK used to mount the IPSEC tunnel;
  - the application password used to read the .STU file with unity and then to connect to the ToE;
  - other services passwords (such as FTP).

  They are stored in the ToE. The user secrets are never transmitted “in clear” through the network. The FTP service is only used to upgrade the firmware of the ToE. This action must be perform through the USB interface avoiding man-in-the-middle attacks. The ToE must ensure the integrity and confidentiality of these credentials.

The security requirements for the critical assets are the following:

Asset	Availability	Confidentiality	Integrity	Authenticity
Firmware			X	X
PLC Memory			X	X
Execution mode			X	
User secrets		X	X	

Threat Model

Attackers

The following attackers are considered:

- Attackers on the supervision network: The attackers control a device plugged on the supervision network of the ToE.

There is no attacker on the field network defined on the **Figure 3 - PLC usage**.

Threats

The following threats are considered:

- **Persistant denial of service:** The attacker manages to generate a denial of service on the ToE by performing an unexpected action or by exploiting a vulnerability (sending a malformed request, using a corrupted configuration file...). This denial of service can affect the whole ToE or only some of its functions.
- **Firmware alteration:** The attacker manages to inject and run a corrupted firmware on the ToE. The code injection may be temporary or permanent and this does include any unexpected or unauthorized code execution. A user may attempt to install that update on the ToE by legitimate means. Finally, the attacker manages to modify the version of the firmware installed on the ToE without having the privilege to do so.
- **Execution mode alteration:** The attacker manages to modify the execution mode of the ToE without being authorized (a stop command for instance).
- **Memory alteration:** The attacker manages to modify, temporarily or permanently, the user program or the configuration that are ran inside the PLC memory.
- **Flows alteration:** The attacker manages to corrupt exchanges between the ToE and an external component without being detected. He can perform attacks such as credential theft, access control violation or control-command of the industrial process mitigation.

Critical assets vs threats

	Control-command of the industrial process	Engineering workstation flows	Firmware	PLC Memory	Execution mode	User secrets
Denial of service	Av					
Firmware alteration			I, Au			
Execution mode alteration					I	
Memory program alteration	I			I, Au		
Flows alteration	Av	Au,C,I				C, I

Av: Availability, I: Integrity, C: Confidentiality, Au: Authenticity

Security functions

The ToE enforces the following security functions.

Malformed input management

The ToE has been developed in order to handle correctly malformed input, in particular malformed network traffic.

Secure storage of secrets

User secrets are securely stored in the TOE. In particular, the compromise of a file system or of only a file is not sufficient for retrieving or modifying them.

Those secrets can belong to the following categories:

- the PSK used to mount the IPSEC tunnel;
- the application password used to read the .STU file with unity and then to connect it to the PLC;
- other services passwords (such as FTP).

Secure authentication on administration interface

Session tokens are protected against hijack and replay. They have a short lifespan. The identity and the permissions of the user account are systematically checked before any privileged action.

In the evaluated configuration, an *application password* is set. This password is used to prevent any modification on the PLC from a non-authenticate user.

Access control policy

The access control policy is strictly applied. In particular, the implementation guarantees the authenticity of privileged operations, i.e. operations that can alter identified critical assets.

The *Access Control List (ACL)* is activated in the evaluated configuration. Only identified IP addresses can connect to the PLC.

Firmware signature

At each update of the firmware, integrity and authenticity of the new firmware are checked before updating.

Integrity and authenticity of the ToE memory

The *Memory protection* feature is activated in the evaluated configuration. It prevents the modification of the running program without an action in specific I/O. if no I/O module is installed (like it is the case in the evaluated configuration), the programming interface is blocked.

The ToE ensures the integrity and authenticity of the user program. Only authorized users can modify it.

The memory protection ensures also the configuration protection. This configuration includes several security parameters that are provided by the TOE (see **[**

Threats covered by security functions

	Persistent denial of service	Firmware alteration	Execution mode alteration	Memory alteration	Flows alteration
Malformed input management	X				
Secure storage of secrets				X	
Secure authentication on administration interface					X
Access control policy					X
Firmware signature		X			
Integrity and authenticity of the ToE memory				X	
Integrity of the PLC execution mode			X		
Secure communication					X

Evaluation platform**]**) such as:

- Access control Policy;
- RUN/STOP by input only activated;
- Memory protection activated;
- Enabled/Disabled Services (FTP, TFTP, HTTP, DHCP, SNMP, EIP, NTP);
- IPSEC parameters;
- Syslog parameters;
- ...

Integrity of the PLC execution mode

The ToE must ensure that the execution mode of the ToE can only be modified by authorized users. This implies, in particular, that they are authenticated.

The *RUN/STOP by input only* feature is activated in the evaluated configuration. This feature deactivates the possibility to change the RUN/STOP status through the Ethernet interface.

Secure communication

The ToE supports secured communication, protected in integrity, confidentiality and authenticity (IPSEC encrypted with ESP).

The FTP protocol is disabled in the evaluated configuration. IPSEC ensures Modbus secured communication through BME NOC.

Threats covered by security functions

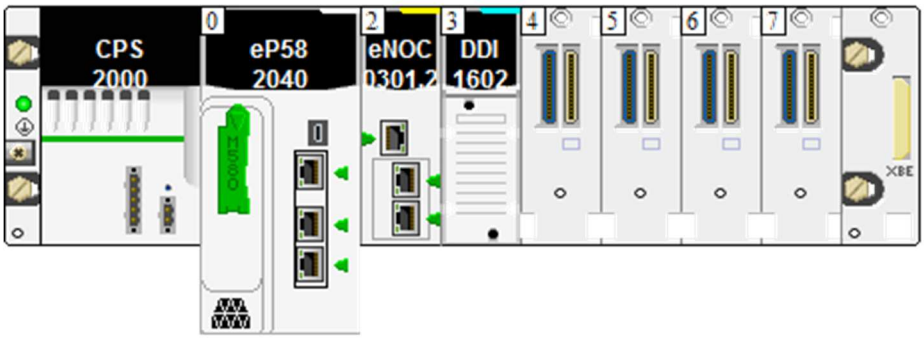
	Persistent denial of service	Firmware alteration	Execution mode alteration	Memory alteration	Flows alteration
Malformed input management	X				
Secure storage of secrets				X	
Secure authentication on administration interface					X
Access control policy					X
Firmware signature		X			
Integrity and authenticity of the ToE memory				X	
Integrity of the PLC execution mode			X		
Secure communication					X

Evaluation platform

System Requirement

System required to evaluate the ToE is the following:

- Unity Pro v11 software
- A backplane to mount CPU – ref BMEXBP0600
- A power supply – ref BMXXBP2000
- An digital input Module – ref BMXDDI1602



Evaluated configuration

The ToE is evaluated in the following configuration:

Parameter	Documentation	Section
ACL activated	**[BMENOC]**	Configuring Security Services
RUN/STOP by input only activated	**[M580HARD]**	Managing Run/Stop Input
Memory protection activated	**[M580HARD]**	Memory Protect
Enforce security selected (FTP, TFTP, HTTP, DHCP/BOOTP, SNMP, EIP, NTP protocols deactivated)	**[BMENOC]**	Configuring Security Services
IPSEC activated on BME NOC	**[BMENOC]**	Configuring Security Services
Log activated	**[BMENOC]**	Logging DTM and Module Events to the Syslog Server
No upload information stored inside CPU	**[UNITY_MODES]**	PLC embedded data
Project fully secured : o Application secured with login & password o Section protection activated	**[M580HARD]**	Helping a Project in Unity Pro
Default password for FTP service changed	**[UNITY_MODES]**	Firmware Protection
Application sections are set with no read / write access	**[UNITY_MODES]**	Section and Subroutine Protection

Platform description

For the evaluation of the Modicon M580 CPU, the following platform has been deployed:

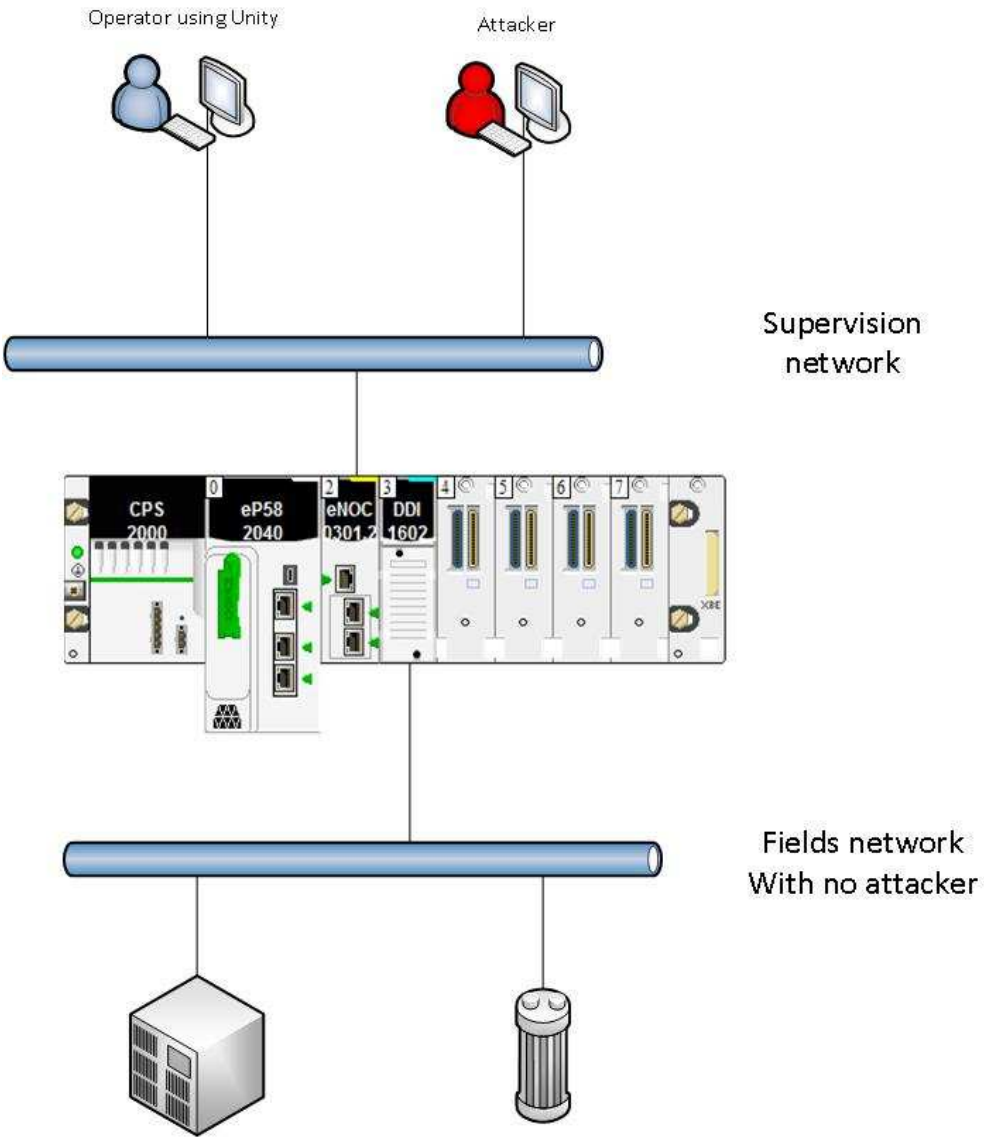


Figure 4 - Evaluation platform architecture