Modicon M580 PAC

CSPN Security Target

Version 1.90

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 document is used to extend the existing CSPN certification of the M580 product passed in 2017, to the whole M580 product range following the ANSSI methodology ANSSI-CC-NOTE21/1.0 concerning the evaluation of a product range. The commonalities and the differences between the different products of the M580 range are detailed in the 'Impact Analysis Report' document V1.1 and V1.2 **[IMPACT ANALYSIS]**

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

[CYBERSEC]	Modicon Controllers Platform - Cyber Security Reference Manual, Schneider, July 2017
[M580HARD]	Modicon M580 - Hardware Reference Manual, Schneider, December 2015
[BMENOC]	Modicon M580 - BMENOC03.1 Ethernet Communication Module Installation and Configuration Guide, Schneider, December 2015
[CE_INSTALL]	Control Expert - Installation Manual, Schneider, December 2015
[CE_START]	Start Up Guide for Control Expert Installing an Application, ref UNY USE 40010V20E, Schneider, September 2004
[CE_LANG]	Control Expert - Program Languages and Structure Reference Manual, Schneider, December 2015
[CE_MODES]	Control Expert - Operating Modes, Schneider, December 2015
[TOE_M580_V1.7]	Modicon M580 PAC - CSPN Security Target - Version 1.7
[IMPACT ANALYSIS]	Modicon M580 PAC – Impact Analysis Report – Version 1.2 & Versions 1.1

Target of Evaluation identification

Manufacturer	Schneider Electric
Organization URL	http://www.schneider-eletric.fr
Product's commercial name	Modicon M580 : - CPU (*) - Communication module : BMENOC0301

Firmware version	CPU V3.10 & BMENOC V2.17
Product's category	Programmable Logical Controller (PLC)

(*) CPU list : BMEP581020, BMEP581020H, BMEP582020, BMEP582020H, BMEP582040, BMEP582040H, BMEP583020, BMEP583040, BMEP584020, BMEP584040, BMEP584040S, BMEP582040S, BMEP585040, BMEP585040C, BMEP586040, BMEP586040C, BMEH582040, BMEH582040C, BMEH584040, BMEH584040C, BMEH586040, BMEH586040C, BMEP58CPROS3

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

- The CPU module embedding the V3.10 firmware following the security rules described in the security documents (see assumptions).
  ThIS CPU module can be any module from the Modicon M580 range, with the P/N BMEa58x0y0z, where a can be P or H, x can be 1 to 6, y can be 2, 4 and z can be NULL, H, C or S. See Impact analysis document for common features and detailed differences.
  - **Note that, in case of safety configurations, safety rules require that the execution of the PLC application program must be executed by 2 different processors in parallel. In case of safety configurations, to ensure compliance with these safety rules, the CPU of the TOE must so be completed by an additional coprocessor module, referenced BMEP58CPROS3, hosted in the rack of the configuration.**.

- All the CPU firmware of the M580 range get the same version (V3.10 for this certification)
- Two BMENOC0301 Ethernet modules embedding the V2.17 firmware. These modules are collocated with the CPU to manage secured communications with upper layer (supervision and engineering software Control Expert).
- Note also that redundant configurations will require 2 redundant CPUs and 4 redundant communication modules.

Figure 1 - The M580 CPU

The redundancy and safety features are not in the scope of this evaluation

The engineering workstation, also called ‘Control Expert’ 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.

We assume that attackers do not have any physical access to the TOE, nor to the field network. The digital input or output module and the backplane components which are necessary in any PLC configuration, are so out of the scope of the evaluation.

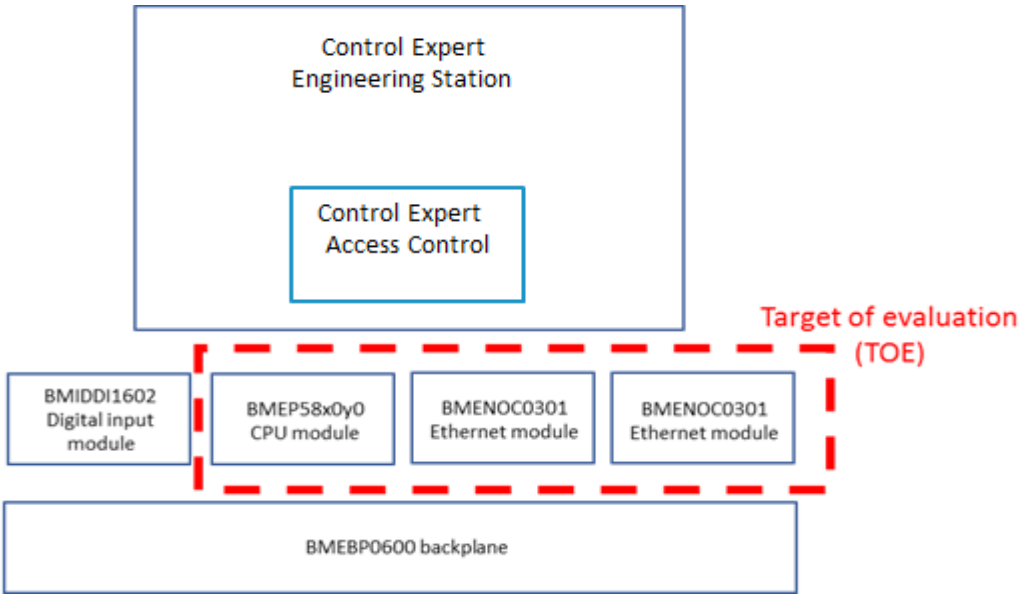


Figure 2 - TOE boundaries

Important: The M580 PLC is a modular system including a Power supply, a rack, a CPU communication modules, and Input / Output modules. Customers build their configurations according to their needs by adding modules in a rack (CPU, I/Os, Communication modules, …..). The CSPN configuration requires 2 BMENOC0301 communication modules in the rack, configured as described in this document. Customer can eventually add local input or outputs modules in this rack according to their needs, but adding additional communication modules providing a non authorized access from the outside to the TOE is prohibited

The architectures described in this document must be considered as reference when cyber security is required.

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 cycle, the PLC CPU processes the data received from its inputs, the sensors and sends commands to its outputs, the actuators.

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

The Modicon M580 range includes also products for specific use such as safety and redundancy features. The redundancy and safety features are not covered by this certification, only the cybersecurity features are part of this certification.

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 can read local inputs and to write local outputs. These I/O can be digital or analog. They can be also located in local racks, or in a remote rack, connected to the CPU via the device network, isolated from other networks 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/maintenance/management functions: The M580 includes administration, maintenance or management functions for configuration and programming. These functions are provided within Control Expert engineering software suite. By convention, in this document, we will adopt 'maintenance' to design any administration, maintenance and management function.
- Remote logging: The M580 supports the definition of a remote logging policy. In particular, it is possible to log security and administration events.
- Secure communication between BMENOC and HMI/SCADA and Control Expert is using 2 different IPSEC tunnels.

Product usage

The Modicon M580 can be used in diverse architectures but a general framework can be characterized.

Exchanges with the supervision (HMI, SCADA) are performed through a dedicated interface (via a separate Ethernet Module – BMENOC0301) on the supervision network.

Exchanges with the Engineering station (Control Expert) are performed through another dedicated interface (via a second Ethernet Module – BMENOC0301) on the maintenance network.

Firmware updates and user programs are loaded on the TOE through the maintenance network.

Communications on Supervision network and management network are protected by IPSEC.

During commissioning phase, initial configuration of TOE must be done with the Control Expert engineering workstation to the local USB port.

In normal operating conditions (PLC in running mode, SCADA connected on Ethernet supervision network), it is recommended that Control Expert engineering workstation should be disconnected from maintenance network.

The M580 can also be connected to inputs and outputs and to local HMI via a dedicated network called 'field network'. It is assumed that attackers do not have any access to this field network, not included in the TOE

Users

The users that may interact with the ToE are the following :

- **Technician/Operators :** They can access in R/W to the variables of the ToE.
- **Automation Engineer/administrator:** These user has maximal privileges. He can, in particular modify the user program and update the firmware of the ToE. In some cases, this type of user is called "developer".

Remark: A user is not necessary a human being, it may be a device or a third-party software. The same person may own several user accounts corresponding to different profiles.

In the particular case of a M580 PLC, these users' profiles are the following :

- **Operate**: Read/Write parameters and data only – No access on program/configuration allowed.
- **Program**: All functions are enabled

The correspondence between users defined in this security target and Predefined Control Expert security profiles is presented in the following table:

		Operator / Technician	Automation Engineer/administrator
Operate		X	
Program			X

Assumptions

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

- **Basic premises :** We assume that attackers do not have physical access to the PLC, nor to the field network. Field network is totally isolated from supervision network and from maintenance network.
- **Logs checking:** We assume that administrators check regularly the local and remote logs produced by the ToE.

- **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.
- **Active logging:** We assume that logging is operational and that logs are not corrupted inside the ToE.
- **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.
- **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]**.
- **User application verification:** Control Expert and the target do not feature an internal integrity check mechanism of the user application. We assume that PLC programs are realized by competent and trustworthy people, trained to do it in a secure way according to the cybersecurity reference guide [CYBERSEC]. We assume also that the transfer of the program in the target is realized by a trustworthy and competent administrator, and according to an organizational process who guaranty the integrity of the program. The configuration must be conformed to the requirements specified in the section **[**Evaluation platform**].**
- **First configuration:** We assume that the first configuration is uploaded to the ToE through the USB interface. The ToE m ust be unplugged from the network.
- **Firmware upgrade:** We assume that the firmware upgrade is performed either through the USB interface or through the maintenance network.
- **Strong passwords:** The administrators use strong passwords with a combination of uppercase, lowercase, numbers and special characters.

Operating modes in CSPN conditions

To be compliant with CSPN requirements, users must follow the following:

- Initial configuration of TOE must be done with a Control Expert engineering station connected in point to point to the local USB port of the PLC.
- In commissioning phase or in normal operating conditions, (running mode, SCADA connected on Ethernet Control network), Control Expert can be connected via Ethernet on the management network.

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.
- **SCADA flows:** The flows between the ToE and the SCADA 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
SCADA flows		X	X	X

ToE critical assets

The critical assets of the ToE are the following:

- **Firmware:** To work properly, the firmware must be protected both in integrity and authenticity.
- **PLC Memory :** The ToE memory contains the **PLC configuration** and the **user application program** loaded by the user. 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;
  - 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.
- **Physical user authentication mechanism:** This mechanism is based on a local database included in Control Expert. The integrity and authenticity of the mechanism is protected by a IPSEC tunnel between Control Expert and the BMENOC.
- **Scada user authentication mechanisms:** this mechanism is based on an IPSEC tunnel between SCADA and the BMENOC.
- **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 Control Expert 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.
- **User Access control policy:** This policy is stored in Control Expert for users. This policy is based on rights owned by users (read/write/update)
- **Scada Access control policy:** This policy is stored in the BMENOC for SCADA accessing it. This policy is based on rights granted by the PSK used in the IPSEC tunnel between SCADA and BMENOC. The access control policy is based on rights granted by the PSK and used in the IPSEC tunnels. The 2 PSKs must be different, following so a previous ANSSI recommendation.

The security requirements for the critical assets are the following:

Asset	Location	Availability	Confidentiality	Integrity	Authenticity
Firmware	CPU/NOC			X	X
PLC Memory (1)	CPU			X	X
Execution mode	CPU			X	X
User secrets	CPU		X	X	
Physical user authentication mechanism	CPU/NOC			X	x
Scada user authentication mechanism	NOC			X	X
User access control policy	CPU			X	
Scada access control policy	NOC			X	

Threat Model

Attackers

The following attackers are considered:

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

There is no attacker on the device or the HotStandby network defined in the [Evaluation platforms] architectures

Threats

The following threats are considered:

- **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).

- **_ User program alteration: The attacker manages to modify, temporarily or permanently, the user program.**
- **_ Configuration alteration: The attacker manages to modify, temporary or permanently, the ToE configuration.**
- **Credentials theft: The attacker manages to steal user credentials.**
- **Authentication violation: The attacker succeeds in authenticating himself without credentials.**
- **Access control violation: The attacker manages to obtain permissions that he does not normally have.**
- **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.

- **Flows compromise: In case of data flows requiring confidentiality, the attacker manages to fetch data by intercepting exchanges between the ToE and an external component**

Note : user program and configuration compromission threats are not considered in this security target.

Critical assets vs threats

	Control command of the industrial	Engineering workstation flows	Scada Flows	Firmware	PLC Memory	isms Physical user authentication	Execution mode	echanisms Scada authentication	User secrets	User access control policy	Scada access control policy
Denial of service	Av										
Firmware alteration				I, Au							
Execution mode alteration							I	I			
User program alteration	Av				I, Au						
Configuration alteration	Av	Au,I			I,Au						
Credential theft									C, I		
Authentication violation						I, Au		I, Au			
Acces control violation										I	I
Flows alteration		I, Au	I, Au								
Flows compromise		C	C								

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 Control Expert and then to connect it to the PLC;
- other services passwords (such as FTP).

Secure authentication on maintenance 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.

The access control policy is realized by the 2 BMENOC modules. The CPU does not manage any access control nor authorizations.

Firmware signature

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

Configuration integrity

The access control prevents any unauthorized person to read or modify the configuration of the ToE. The memory protection ensures the configuration protection. This configuration includes several security parameters that are provided by the TOE (see **[**Evaluation platform**]**) such as:

- Access control Policy;
- Enabled/Disabled Services (FTP, TFTP, HTTP, DHCP, SNMP, EIP, NTP);
- IPSEC parameters; - Syslog parameters;
- ...

Moreover, internal mechanisms between CPU and the modules provide the control of consistency of the configuration of all modules plugged in the rack. The communications between the CPU and the different modules is realized via the backplane. As we assumed that the backplane is not accessible to attackers, these internal mechanism are not in the scope of this certifications.

Integrity and authenticity of the ToE memory (user program and configuration)

The ToE ensure the integrity of the user program and of the configuration. Only authorized users can modify it.

The integrity and authenticity of the ToE user program and configuration is ensured by an authentication mechanism (application password) protected by the IPSEC tunnel between Control Expert and the BMENOC.

Integrity of the PLC execution mode.

The integrity of the PLC execution mode is ensured by the IPSEC tunnel between Control Expert and the BMENOC.

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

	LOCATION	e Persistent denial	Firware alteration	n Execution mode	tion User program	on Configuration	Credential Theft	h Authentication	n Access control	Flow alteration	ompromise Flow
Malformed input management	CPU NOC	X									
Secure storage of secrets	CPU NOC						X				
Secure authentication on maintenance interface	CPU					X	X	X			
Access control policy	NOC								X		
Firmware signature	CPU NOC		X								
Configuration integrity	CPU NOC					X					
Integrity and authenticity of the ToE memory	CPU NOC				X						
Integrity of the PLC execution mode	NOC			X							
Secure communication	NOC									X	X

Evaluation platforms

We intend to certify the whole M580 range, which include 22 products. As mentioned in the the Impact analysis report, the M580 range includes 3 types of platforms: the standard, highly available and safety platforms.

Please refer to the 'impact analysis M580 range' document to identify commonalities and differences between the different product of the range .

System Requirement for standard architecture

System required to evaluate the ToE is the following:

- Control Expert V14.1 software
- A backplane to mount CPU – ref BMEXBP0600
- A power supply – ref BMXCPS2000
- An digital input Module – ref BMXDDI1602
- A CPU ref BMEP582040 – taken as a reference
- 2 Ethernet communication modules BMENOC0301

System Requirement for Hot standby architecture

System required to evaluate the ToE is the following:

- Control Expert V14.1 software
- 3 backplanes to mount CPU – ref BMEXBP0600
- 3 power supply – ref BMXCPS2000
- 1 digital input Module – ref BMXDDI1602
- 2 CPU ref BMEH582040 – taken as a reference
- 4 Ethernet communication modules BMENOC0301
- 1 Communication drop for Remote IO

System Requirement for safety architecture

System required to evaluate the ToE is the following:

- Control Expert V14.1 software
- 1 backplane to mount CPU – ref BMEXBP0600
- 1 power supply – ref BMXCPS4002S
- 1 digital input Module – ref BMXDDI1602
- 1 CPU ref BMEP582040 – taken as a reference
- 2 Ethernet communication modules BMENOC0301
- 1 safety CPU ref BMEP584040S – taken as a reference
- 1 safety coprocessor BMEP58CPROS3
- 2 Ethernet communication modules BMENOC0301

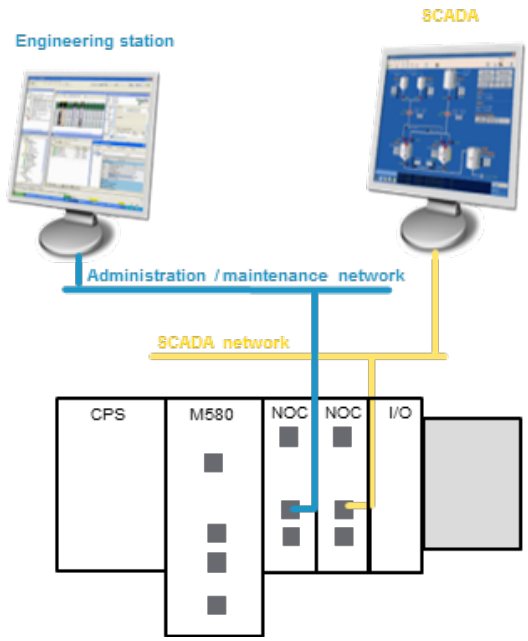
Evaluated configuration

All platforms must be evaluated in the following configuration:

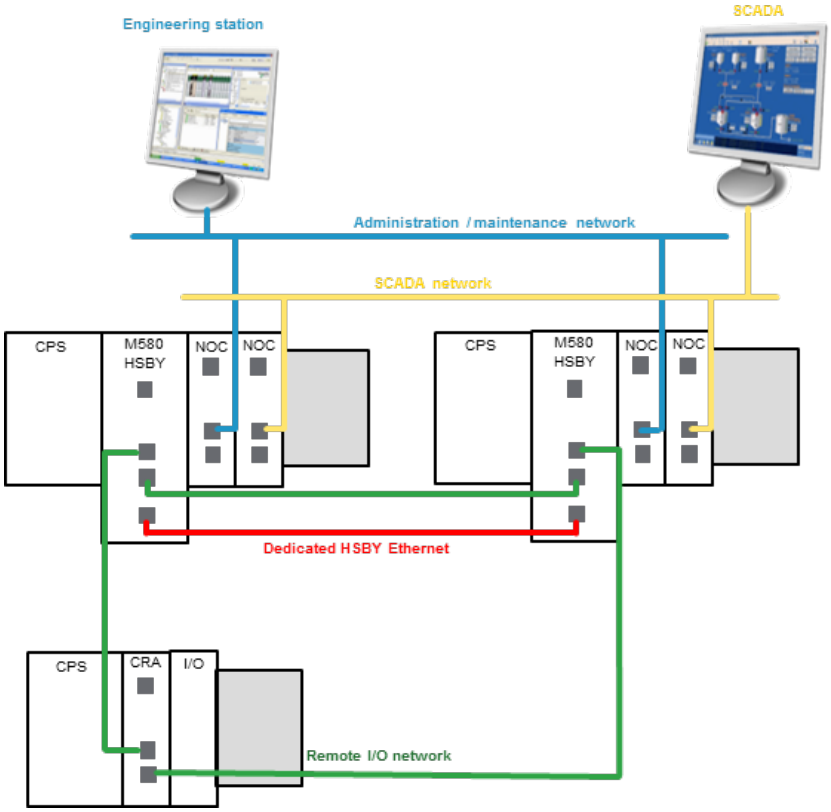
Parameter	Documentation	Section
ACL activated	**[BMENOC]**	Configuring Security Services
Enforce security selected (FTP, TFTP, HTTP, DHCP/BOOTP, SNMP, EIP, NTP protocols deactivated)	**[BMENOC]**	Configuring Security Services
IPSEC activated on BME NOC	**[BMENOC]**	Configuring Security Services
Log activated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

Platforms description

Each type of platform will be tested in an evaluation architecture, according the below diagrams

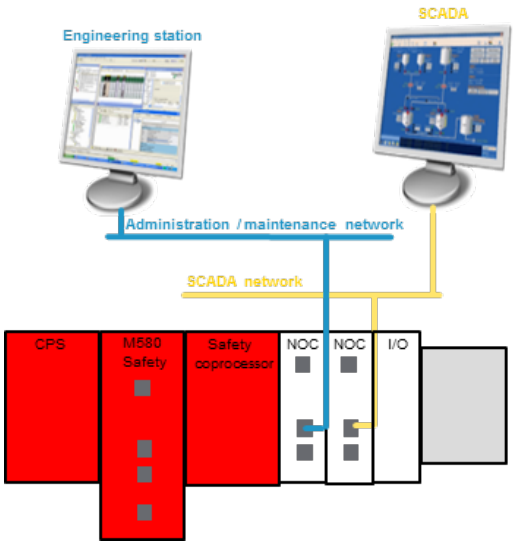


Evaluation platform of standard products



Evaluation platform of Hotstandby products

Note that we assume that no attacker can be on Remote IO or dedicated HSBY network.



Evaluation architecture of safety products