Protection profile of an industrial programmable logic controller

Version 1.1 mid-term

GTCSI

July 13, 2015

Preface

In the whole document, the acronym ToE (Target of Evaluation) designates the component being evaluated.

Text in red differs from the short-term version of the protection profile.

1 Product description

1.1 General description

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

In addition to standard references, there are two types of PLCs:

- redundant PLCs, used for higher availability of ICS;
- safety PLCs, used for ensuring safety of people and assets.

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.

1.2 Features

The ToE includes the following features:

- **User program execution:** The ToE runs a user program. This program processes the inputs and updates the outputs.
- **Input/output management:** The ToE is able to read local or remote inputs and to write local or remote outputs. These I/O can be digital or analog. These I/O allows the ToE controlling and commanding the industrial process.
- **Communication with the supervision:** The ToE can communicate with the SCADA for receiving commands and transmitting process data.
- **Administration functions:** The ToE includes administration functions in order to configure, or program the other functionalities of the ToE. Several administration interfaces are possible:
  - thick-clients (sometimes also called, depending on the context, administration console, programming workstation. . .);

  - web-clients;
  - removable devices (USB drives, SD memory cards, etc.).

- **Local logging:** The ToE supports the configuration of a local logging policy. It is possible, in particular, to log security and administration events.
- **Remote logging:** The ToE supports the definition of a remote logging policy. In particular, it is possible to log security and administration events.

1.3 Product usage

A PLC can be used in diverse architectures but a general framework can be characterized. The PLC 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 on 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 a serial bus or a removable device (SD memory cards, USB keys for instance).

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.

This basic architecture is depicted on figure 1.

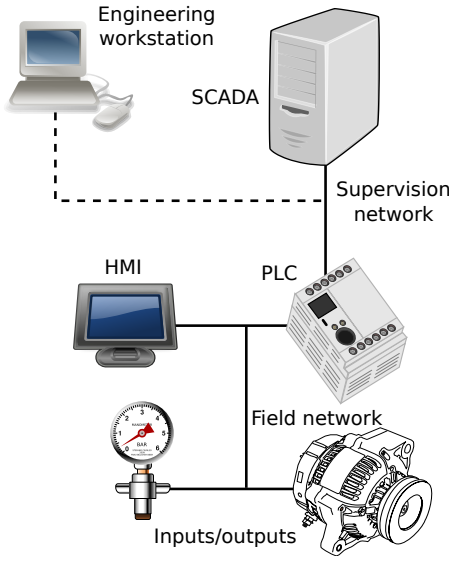

Figure 1: Typical network architecture for a PLC

1.4 Users

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

- **Operator:** This user can access the ToE data with read-only privileges.
- **Technician:** This user has the same privileges as the previous one and he can also modify some variables in the ToE.
- **Automation Engineer/administrator:** This 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. Moreover, the same person may own several user accounts corresponding to different profiles.

1.5 Assumptions

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

- **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 not necessarily in secured premises and the attacker can have access to all physical interfaces of the ToE. Similarly, the attacker can plug a trapped device (for instance, a USB drive or a SD card) on any physical port of the ToE. Conversely, the attacker cannot disassemble the ToE or perform physical attacks on it.

  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 by default:** Services of the ToE which are not covered by the security target are disabled in the default configuration (also named factory default configuration).
- **Security documentation:** The ToE is provided with a complete documentation for a secure usage. In particular, all secrets are listed in order to allow their customization.

  All recommendations included in this documentation are applied prior to the evaluation.

2 Critical assets

2.1 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 and integrity of these actions must be protected.
- **Data exchanges between the ToE and the supervision:** The integrity and authenticity of the exchanges between the supervision and the ToE must be protected.
- **Engineering workstation flows:** The flows between the ToE and the engineering workstation must be protected in integrity, confidentiality and authenticity.
- **Data exchanges between the ToE and another PLC:** For the communication between the ToE and another PLC, the use of dedicated I/O should be prefered. In the case where these exchanges should transit on a mutualized infrastructure, they must be protected in integrity and authenticity.

The security requirements for the critical assets are the following:

Asset	Availability	Confidentiality	Integrity	Authenticity
Control-command of the industrial process	X		X	
Data exchanges between the ToE and the supervision			X	X
Engineering workstation flows		(X)	X	X
Data exchanges between the ToE and another PLC			X	X
X: mandatory (X): optional				

2.2 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.
- **User program:** The ToE runs a program written and loaded by the users. Its integrity, confidentiality[1] and authenticity must be protected.
- **Configuration:** The configuration of the ToE must be protected in confidentiality and integrity. The attacker must not be able to discover the configuration of the ToE by other means than the ToE activity.
- **Excecution mode:** The integrity and authenticity of the execution mode of the ToE must be protected.
- **User authentication mechanism:** This mechanism can be based on a local database or on a remote authentication server. In both cases, the ToE must ensure the integrity and authenticity of the mechanism[2].
- **User secrets:** The user secrets can be passwords, certificates... They can be stored in the ToE or stored in a remote authentication server. In all cases, the ToE must ensure the integrity and confidentiality of these credentials.
- **Access control policy:** The policy can be stored locally or remotely on a authentication server. In both cases, the ToE must ensure the integrity of the access control policy.
- **Local logging:** Once configured, the local logging must remain operational.
- **Remote logging:** The ToE is capable of remote logging. Once configured, the logging must remain operational.
- **Local logs:** The integrity of the local logs must be ensured by the ToE.
- **Remote logs:** The remote logs generated by the ToE must be protected in integrity and authenticity. A mechanism must be present to detect the absence of a message in a sequence of properly received messages.

The security requirements for the critical assets are the following:

[1] Confidentiality is not a primary measure for protecting industrial control systems, it is a defense-in-depth measure. This security property can also be required for industrial secrecy purposes.

[2] All authentication mechanisms offered by the ToE may not necessarily be part of the security target. However, those which are not included in the security target must be disabled by default.

Asset	Availability	Confidentiality	Integrity	Authenticity
Firmware			X	X
User program		(X)	X	X
Configuration		(X)	X	
Excecution mode			X	
User authentication mechanism			X	X
User secrets		X	X	
Access control policy			X	
Local logging	X			
Remote logging	X			
Local logs			X	X
Remote logs			X	X
X: mandatory (X): optional				

3 Threat Model

3.1 Attackers

The following attackers are considered:

- **Attacker on the supervision network:** The attacker controls a device plugged on the supervision network of the ToE.
- **Attacker on the process network:** The attacker control a device plugged on the field network.
- **Evil user:** The attacker has compromised an unprivileged accound and tries to bypass the access control policy of the ToE.

3.2 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 compromise:** The attacker manages to obtain some parts of the configuration of the ToE by other means than the observation of the activity of the ToE[3].
- **User program alteration:** The attacker manages to modify, temporarily or permanently, the user program.

[3] This threat is considered only when the confidentiality of the user program has been identified as critical.

- **Configuation alteration:** The attacker manages to modify, temporary or permanently, the ToE configuration.
- **Configuration compromise:** The attacker manages to illegally obtain some parts of 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.
- **Local logs alteration:** The attacker manages to delete or modify a local log entry without being authorized by the access control policy of the ToE.
- **Remote logs alteration:** The attacker manages to modify a remote log entry without the receiver being able to notice it. The attacker manages to delete a remote log message without the receiver being able to notice it.
- **Parameters or command injection:** The attacker manages to modify parameters in the ToE or to transmitt commands without being authorized.
- **Flows alteration:** The attacker manages to corrupt exchanges between the ToE and an external component without being detected.
- **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.

4 Security objectives

The following security objectives are considered:

- **Malformed input management:** The ToE has been developped 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 is not sufficient for retrieving them.
- **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.
- **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.
- **Firmware signature:** At each update of the firmware, the integrity and authenticity of the new firmware are checked before updating. The integrity and authenticity of the firmware are also checked at boot time.
- **Configuration confidentiality and integrity:** The access control prevents any unauthorized person to read or modify the configuration of the ToE.
- **Integrity and authenticity of the user program:** The ToE ensure the integrity of the user program. Only authorized users can modify it.
- **Confidentiality of the user program:** The ToE protects the confidentiality of the user program. Only authorized users can access it.

- **Integrity and authenticity of commands and PLC 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.
- **Secure communication:** The ToE supports secured communication, protected in integrity and authenticity. If required, confidentiality is enforced with external components.
- **Logs integrity:** The integrity of the generated local logs is ensured and only the super-administrator is permitted to modify them.
- **Alarms integrity:** The ToE supports secure remote logging where authenticity and integrity are ensured. The transmission is also protected against replay and a mechanism is implemented for detecting missing logs.

A Critical assets vs threats

	Control-command of the industrial process	Data exchanges between the ToE and the supervision	Engineering workstation flows	Data exchanges between the ToE and another PLC	Firmware	User program	Configuration	Excecution mode	User authentication mechanism	User secrets	Access control policy	Local logging	Remote logging	Local logs	Remote logs
Denial of service	Av											Av	Av		
Firmware alteration					I Au										
Execution mode alteration								I							
User program compromise						(C)									
User program alteration	I					I Au									
Configuation alteration							I								
Configuration compromise							(C)								
Credentials theft										C I C					
Authentication violation									I Au						
Access control violation											I				
Local logs alteration														I Au	
Av: Availability, I: Integrity, C: Confidentiality, Au: Authenticity															

	Control-command of the industrial process	Data exchanges between the ToE and the supervision	Engineering workstation flows	Data exchanges between the ToE and another PLC	Firmware	User program	Configuration	Excecution mode	User authentication mechanism	User secrets	Access control policy	Local logging	Remote logging	Local logs	Remote logs
Remote logs alteration															I Au
Parameters or command injection	Av I	I Au													
Flows alteration	Av I	I Au	I Au	I Au											
Flows compromise			(C)												
Av: Availability, I: Integrity, C: Confidentiality, Au: Authenticity															

B Threats vs security objectives

	Denial of service	Firmware alteration	Execution mode alteration	User program compromise	User program alteration	Configuation alteration	Configuration compromise	Credentials theft	Authentication violation	Access control violation	Local logs alteration	Remote logs alteration	Parameters or command injection	Flows alteration	Flows compromise
Malformed input management	X														
Secure storage of secrets								X							
Secure authentication on administration interface						X	X	X	X						
Access control policy										X					
Firmware signature		X													
Configuration confidentiality and integrity						X	X								
Integrity and authenticity of the user program					X										
Confidentiality of the user program				X											
Integrity and authenticity of commands and PLC mode			X												

	Denial of service	Firmware alteration	Execution mode alteration	User program compromise	User program alteration	Configuation alteration	Configuration compromise	Credentials theft	Authentication violation	Access control violation	Local logs alteration	Remote logs alteration	Parameters or command injection	Flows alteration	Flows compromise
Secure communication													X	X	X
Logs integrity											X				
Alarms integrity												X			

C Contributors

This protection profile has been produced by the working group on cybersecurity for industrial systems, supervised by the French Network and Information Security Agency (ANSSI).

The following compagnies and organisms contributed to this document:

- Amossys
- ARC Informatique
- Belden
- DGA/MI
- Gimelec
- Oppida
- Phoenix Contact
- RATP
- Schneider Electric
- Siemens
- Sogeti
- Stormshield
- Thales