RSPE

CSPN Security Target

Version

V1.3

1. History

Version	Date	Status	Author	Changes
1.0	13/02/2017		Oppida	Document created
1.1	20/03/2017		Oppida	Change of the security functions
1.2	04/03/2020		Belden	Update according to re certification
1.3	28/05/2020		Belden	Final update

Summary

Introduction

1.1 Document objects

A CSPN security target is a document specifying the scope of a CSPN evaluation [**CSPN**]. This Security Target serves as a basis for agreement between Hirschmann (manufacturer of the product) and its potential customers. 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

The present evaluated product is an industrial managed and modular switch RSPE. It has been specifically designed for industrial networks and harsh environment where IT switches cannot properly operate due to heat, humidity or dust.

This security target claims conformance with the requirements from the Protection profile of an industrial switch – short-term [**PP-Switch**] edited by ANSSI.

1.2 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-Switch	Protection profile of an industrial switch, version 1.° short-term, GTCSI, ANSSI, July 13, 2015

1.3 Target of Evaluation identification

The Target of the Evaluation (thereinafter "TOE") is composed of:

- The Modular Managed Industrial Switch RSPE embedding the HiOS 07.0 firmware

Manufacturer	Hirschmann
Organization URL	http://www.hirschmann.com/
Product's commercial name	RSPE
Firmware version	HiOS 07.0.07
Product's category	Industrial Switch

The manufacturer of the Switch RSPE is the company Hirschmann that acquired the previous product's manufacturer (Hirschman).

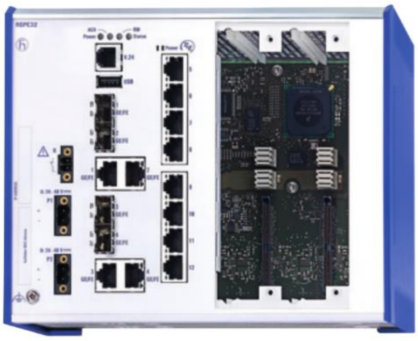

Figure 1 - The RSPE Switch

1.4 Glossary and terms

ANSSI	National agency of security of information systems (Agence Nationale de la Sécurité des Systèmes d'Information)
CSPN	First Level Security Certification (Certification de Sécurité de Premier Niveau)
TOE	Target of Evaluation. It is the product under evaluation.

2 Product description

2.1 General description

The RSPE is a managed industrial Ethernet switch developed by Hirschmann. It has been specifically designed for industrial networks and harsh environment where IT switches cannot properly operate due to heat, humidity or dust. It provides interconnection for different devices or network segments by using Ethernet. It supports logical network segregation with VLAN, several network oriented security features (denial of service prevention, MAC filtering, ARP Spoofing detection …).

2.2 Typical Users

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

- **Guest:** user having the permission to read-only the configuration of the TOE;
- **Operator:** User having the permission to read and write the configuration of the TOE, except for the security parameters;
- **Administrator:** User having a full read and write access to the configuration of the TOE;
- **End-device:** Unauthenticated machine of process that has a direct or indirect access to the TOE.

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.

2.3 Features

The TOE includes the following features:

- **Administration functions:** The TOE includes administration functions in order to configure, or program the other functionalities of the TOE. Several administration interfaces are possible:
  - serial link;
  - web-clients;
  - SSH.
- **User Management**
  - Provide individual logins, password and role for each users;
  - Define a password policy;
  - Login credentials can be stored locally or remotely on a RADIUS server (802.1 X or MAC based).
- **Local event logging:** The TOE supports the configuration of a local logging policy. It is possible, in particular, to log security and administration events (CLI and SNMP requests) with 8 severity levels. A time server (SNTP) can be used to provide a unified time for all the logs.
- **Port Security**
  - Enable/Disable physical port;
  - IP address Conflict Detection;
  - DHCP-based attack prevention (server spoofing, address exhaustion, IP hijacking, …);
  - Denial of Service prevention based on several protocols known vulnerabilities:
    - ICMP (fragmented packets, broadcast pings, maximum size);
    - TCP/UDP (null scan, Xmas Tree, SYN/FIN, SYN flood,);
    - IP (land attack).
  - Dynamic ARP Inspection.
- **Access Control Lists**: IPv4 packets can be filtered based on :

  - Source/destination IP address;
  - Source/destination TCP/UDP port;
  - Source/destination Mac address ;
  - Protocol, Ethertype;
  - Quality of service (type of service, differentiated services code point, class of service);
  - VLAN ID.
- **Network segregation:** The device includes network segregation (thanks to VLANs for instance) and the associated configuration interfaces
- **Network troubleshooting**: Thanks to the sFlow technology, the TOE provides a set of data that helps to identify malicious network traffic.

The following feature of the product are not within the TOE scope and will not be considered in the evaluation process:

- *Redundancy functions*: The TOE includes redundancy functions in order to ensure high availability for one or several functions.
- *Distant event logging* **:** The TOE offers the functionality to send event logs to a remote server using the syslog protocol.

2.4 Environment of use

1.1.1. Product usage

Industrial switches can be used in many different contexts. Nevertheless, we can distinguish two great categories with field networks connecting remote I/O with PLCs and supervision networks connecting PLCs with the SCADA system.
In low criticality systems, it is possible to use VLAN for segregating administration functions. Such an example of a topology is given on figure 1. On this figure, the segregation ensures that each PLC can only communicate with a given remote sensor and a given actuator (VLAN 2 and 3) It also prevents the communication between PLCs (VLAN 2 and 3 for the field network and 4 and 5 for supervision network). Finally, a VLAN is dedicated to the administration of the switches and the SCADA workstation.

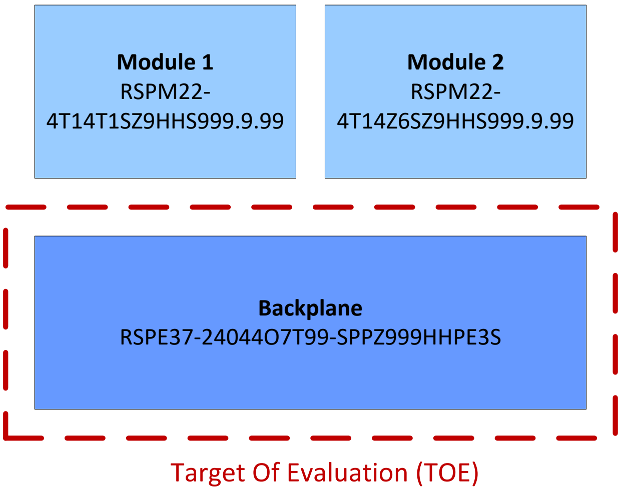
Module 1
RSPM22-4T14T1SZ9HHS999.9.99
Module 2
RSPM22-4T14Z6SZ9HHS999.9.99
Backplane
RSPE37-24044O7T99-SPPZ999HHPE3S
Target Of Evaluation (TOE)

Figure 2 - TOE boundaries

All the modules that can be plugged on the RSPE backplane provide more physical interfaces that can be used for plugging more users. They does not interfere with the security functions that are provided by the RSPE. The CSPN certificate is applied to the RSPE backplane independently of the modules that are plugged in.

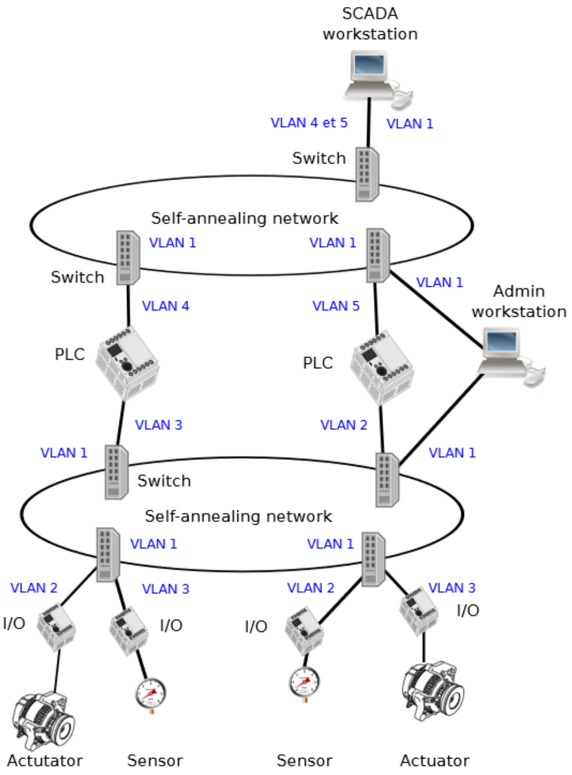

Figure 3 - Networks with VLAN segregation

1.1.2. Dependences of the product in materials, software and/or the firmware's of the system

The TOE is a dedicated appliance that does not require any dependences. It is delivered as a preconfigured state including all the component that are required.

1.1.3. Evaluation Scope

The remote audit logging is activated and uses syslog server.
All of the other administration actions are performed remotely through SSH or by using the web interface (protected with SSL/TLS).
The following protocols are used to protect communications:

- Administration VLAN: TLS or SSH Protocols are used.
- Syslog VLAN: TLS Protocol is used.

All the users are authenticated by using a password.
The administration action can be performed through a serial link for the users that have a physical access to the TOE.

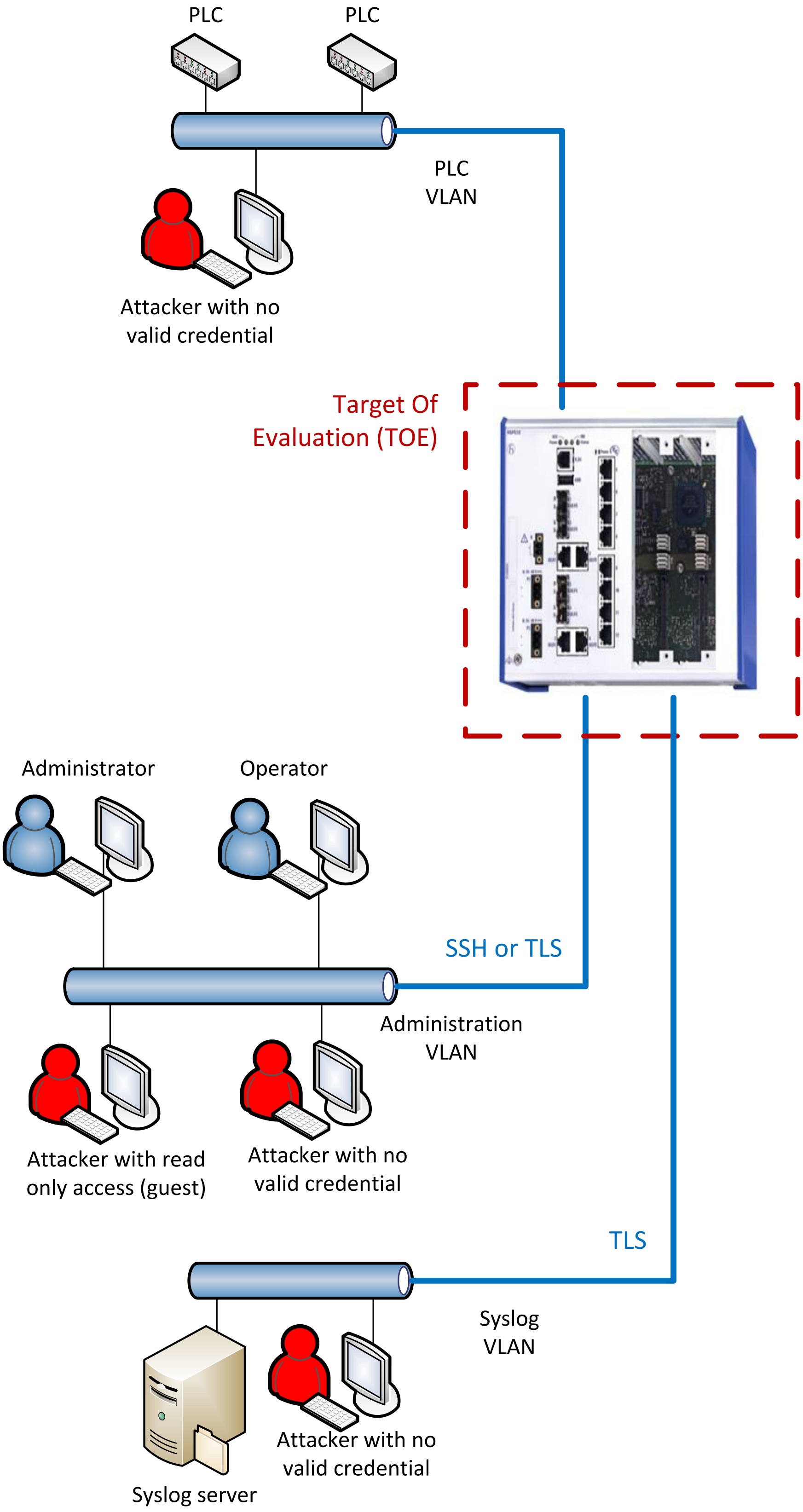
PLC
PLC
PLC VLAN
Attacker with no valid credential
Target Of Evaluation (TOE)
Administrator
Operator
SSH or TLS
Administration VLAN
Attacker with read only access (guest)
Attacker with no valid credential
TLS
Syslog VLAN
Attacker with no valid credential
Syslog server

Figure 4 - Evaluation Platform

2.5 Assumptions

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

- **Trusted administrators:** Administrators are trained for performing the tasks they are responsible for. They follow instructions and administration manuals of the TOE and they are not hostile.
- **Secure storage of the TOE:** 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.
- **Segregation policy:** We assume that the network segregation policy set up on the TOE is adapted to the use case.
- **Dimensioning:** We assume the TOE is properly dimensioned for its tasks.
- **Redundancy link:** There is a network link used in order to provide a redundancy function. It is supposed to be next to the TOE and not accessible by an attacker.
- **Firmware integrity:** The firmware integrity is assumed.
- **TLS Servers certificates :** These certificates are generated by the administrator and installed in accordance to the used guide.
- **Trusted users :** Guest users and Operator users are supposed to be trusted users.

3 Critical Assets

3.1 Critical assets of the environment

The critical assets of the environment are the following:

- **Frames:** The TOE ensures the filtering and the switching of frames between end devices.
- **Logical segregation:** The TOE ensures the network logical segregation between sub-networks.
- **End devices authentication:** The TOE authenticates directly connected end-devices

Asset	Availability	Confidentiality	Integrity	Authenticity
Frames	X			
Logical segregation	X		X	
End devices authentication	X		X	X

3.2 TOE critical assets

The critical assets of the TOE are the following:

- **Configuration:** The configuration of the TOE must be protected in confidentiality and integrity. It defines all the security features of the TOE. The attacker must not be able to discover the configuration of the TOE by other means than the TOE activity. He must not be able to change it either.
- **User secrets:** The user password fingerprints are stored locally in the TOE.
- **Logs:** All administration actions performed by on the TOE are logged in the syslog server.

The security requirements for the critical assets are the following:

Asset	Availability	Confidentiality	Integrity	Authenticity
Configuration		X	X	
User secrets		X		
Logs		X	X	

4 Threat model

4.1 Attackers

The following attackers are considered:

- **Evil end-device:** A device connected to the TOE is controlled by the attacker.
- **Evil administration device:** A device plugged on the administration network is controlled by the attacker but the attacker may not have valid credentials on the TOE.
- **Evil Guests:** An authenticated read-only user manages to modify the configuration of the TOE.

4.2 Threats

The following threats are considered:

- **Persistent denial of service:** The attacker manages to generate a persistent 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.
- **Network segregation violation:** The attacker manages to violate the logical network segregation.
- **Configuration alteration:** The attacker manages to modify, temporary or permanently, the TOE configuration.
- **Configuration compromise:** The attacker manages to illegally read some parts of the TOE configuration.
- **Credentials theft:** The attacker manages to steal user credentials.
- **Authentication bypass:** The attacker succeeds in authenticating himself without credentials.
- **Access control violation:** The attacker manages to obtain permissions that he does not normally have.

4.3 Critical assets vs threats

	Frames	Logical Segregation	End devices authentication	Configuration	User authentication mechanism	User secrets	Access control policy
Persistent denial of service	Av	Av	Av				
Network segregation violation		I, C					
Configuration alteration		Av		I	Av	Au	Au
Configuration compromise				C			
Credentials theft						C, I	
Authentication bypass					I, Au		
Access control violation							I

Table 1 - How threats impact assets

Av: Availibility
I: Integrity
C: Confidentiality
Au:Authenticity

5 Security functions

The TOE enforces the following security functions.

- **Secure communication**:
  - The TOE supports to secured communication (SSH, SSL/TLS), protected in integrity, confidentiality, authenticity and prevents from replay attacks.
  - Sessions tokens are protected against hijacking and replay. They have a short lifespan. The identity and the permissions of the user account are systematically checked before any privileged action.
- **Restriction Access Management:** The access control 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 switch administration interface.
- **Malformed input management:** The TOE has been developed in order to handle correctly malformed input, in particular malformed network traffic and user input inside the web interface.
- **Network segregation policy:** The TOE supports logical network segregation (with VLANs or PVLANs).
- **Secure storage of secrets:** User secrets are securely stored in the TOE. In particular, the compromise of a file system is not sufficient for retrieving or modifying them.

  Those secrets can belong to the following categories:
  - Authentication passwords for all users;
  - The configuration that is installed on the TOE.

  This configuration includes several security services provided by the TOE such as:
  - Enable/Disable physical port;
  - IP address Conflict Detection;
  - DHCP-based attack prevention (server spoofing, address exhaution, IP hijacking, …);
  - Denial of Service prevention based on several protocols known vulnerabilities:
    - ICMP (fragmented packets, broadcast pings, maximum size);
    - TCP/UDP (null scan, Xmas Tree, SYN/FIN, SYN flood,);
    - IP (land attack).
  - Dynamic ARP Inspection.

  It also includes the definition of the access control policy for all the end-devices plugged on the TOE:
  - Source/destination IP address;
  - Source/destination TCP/UDP port;
  - Source/destination Mac address ;
  - Protocol, Ethertype;
  - Quality of service (type of service, differentiated services code point, class of service);

  VLAN ID.

	Persistent denial of service	Network segregation violation	Configuration alteration	Configuration compromise	Credentials theft	Authentication bypass	Access control violation
Secure communication			X	X	X	X	X
Access control policy		X					X
Malformed input management	X		X				X
Network segregation policy		X					
Secure storage			X	X	X		

Table 2 - Threats covered by security functions