PANORAMA Server and Client Short-Term CSPN Security Target

CSPN Target

Reference: PANO/CSPN Target Short-term-V3.5

Date: 08/10/2019

CHANGE RECORD

Version	Date	Comments
3.0	27/04/2018	Version refocused on Panorama E² Addition of the security bulletin concept SNMP Agent function excluded from the target HTTP, OPC.TCP and Net.TCP bindings of the OPC-UA server are excluded from the target LON acquisition excluded from the target
3.1	24/04/2019	Modification of profiles in operation is excluded from the target Partial reactivation of the sensitive asset bst5 "OPC-UA data server function certificate" and of the security function fs5 "Secure storage of data server function certificates"
3.2	06/06/2019	Update of target identification Updated definition of attackers Clarifications on bst4 and bst5 assets and fs4 and fs5 security functions
3.3	29/07/2019	Correction to the summary table of "ToE Sensitive Assets"
3.4	30/07/2019	Removal of the private key concept in bst5
3.5	08/10/2019	Addition to the product identification (§1.2) Details added to hs11

CONTENTS

1. INTRODUCTION

1.1 Purpose

This document describes the target for the First-Level Security Certification (CSPN certification) for the SCADA Server and Client component of Panorama E².

This document has taken for reference:

- The ANSSI short-term protection profile for a SCADA Server application (20151005_NP_ANSSI_SDE_4067_PJ3_serveur_scada_court_terme_PJ3).
- Some elements concerning users and local logs taken from the medium-term version for the server (20151005_NP_ANSSI_SDE_4067_PJ4_serveur_scada_moyen_terme_PJ4).
- The protection profile for a medium-term MES/SCADA Client application extrapolated to short-term to take it to the level of the server component (20151005_NP_ANSSI_SDE_4067_PJ9_client_scada_mes_moyen_terme_PJ9).

The target description follows the scheme of these profiles.

1.2 Product identification

Manufacturer	Codra Ingénierie Informatique Immeuble Hélios - 2 rue Christophe Colomb - CS 0851 91300 Massy, France
Link	https://codra.net/
Product	Panorama E²
Version	Panorama E² V7.00 integrated into Panorama Suite 2017 (build 17.00.011) + following updates: PS2-1700-01-1086 ; 03-2128 ; 05-1024 ; 06-0348 ; 07-1082; 08-1054 ; 09-1052 ; 13-0348 ; 14-1051 ; 17-1037 ; 18-1157
Category	SCADA

1.3 Reference documents

Reference	Title (translated)
ANSSI: securite_industrielle_GT_methode_classification-principales_mesures	Cybersecurity of Industrial Systems - Classification Method and Key Measures
ANSSI: 20151005_NP_ANSSI_SDE_4067_PJ3_serveur_scada_court_terme_PJ3	Protection profile for a short-term SCADA Server application
20151005_NP_ANSSI_SDE_4067_PJ4_serveur_scada_moyen_terme_PJ4	Protection profile for a medium-term SCADA Server application
20151005_NP_ANSSI_SDE_4067_PJ9_client_scada_mes_moyen_terme_PJ9	Protection profile for a medium-term MES/SCADA Client
ANSSI-CSPN-CER-P-01/1.1 5/12	First level security certification of information technology products
ANSSI-CSPN-CER-I-02.	Evaluation methodology for the CSPN and RTE required content, Instruction

Reference	Title (translated)
ANSSI-CC-NOTE-21/1.0	Application note: Methodology for the evaluation of a product range
V7.2 dated 6/11/17	Panorama manual

1.4 Terminology and abbreviations

1.4.1 Abbreviations

AD: Active Directory, directory service for Windows operating systems

API : Application Programming Interface

CIM: computer-integrated manufacturing, a concept denoting the complete automation of manufacturing processes

CSPN: [French] Certification de Sécurité de Premier Niveau, meaning First-Level Security Certification

DCOM: Distributed Component Object Model, Microsoft technology

MES: Manufacturing Execution System, an IT system whose primary objectives are to collect production data in real time from all or part of a factory or workshop

n.a: Not Applicable

OPC: OLE for Process Control, an initially OLE-based communication protocol based on COM/DCOM

OPC-DA: OPC based on DCOM for real-time Data Access

OPC-UA: OPC Unified Access, based on web services

SCADA: Supervisory Control And Data Acquisition

ToE: (Target of Evaluation)

1.4.2 Terminology

Authenticity: Property of any information or processing that guarantees its identity, origin and possibly its destination.
(source [FR only]: securite_industrielle_GT_methode_classification-principales_mesures)

Confidentiality: Private aspect of data or of a process, to which access is restricted solely to certain individuals or to authorised entities or processes in view of requirements of the service
(source [FR only]: securite_industrielle_GT_methode_classification-principales_mesures).

Cybersecurity: A desired condition for an information system, allowing it to withstand events of malicious origin that are likely to compromise the availability, integrity or confidentiality of data stored, processed or transferred or the services provided by the system.

(source [FR only]: securite_industrielle_GT_methode_classification-principales_mesures).

Note: For the purposes of this document, "security" shall be synonymous with "cybersecurity".

Availability: Property allowing the expected service to be performed in the desired time and in conformity with the expected conditions of use.
(source [FR only]: securite_industrielle_GT_methode_classification-principales_mesures).

Integrity: Property of protecting the accuracy and completeness of assets.
(source [FR only]: securite_industrielle_GT_methode_classification-principales_mesures).

SCADA client: (Panorama workstation) Software installed on a user workstation enabling the human operator to interact with the SCADA Server. The SCADA Client allows the operator to view the data processed or generated by the server and to send commands (see § 2.1 Product description). In the protection profile, referred to as the SCADA Client Application or Client Application.

SCADA Server: (Panorama functional server) Software installed on a machine that operates without operator intervention and which enables the acquisition of "process" data, generation of commands, management of alarms, storing of values (see § 2.1 Product description). In the protection profile, referred to as the SCADA Server Application or Server Application.

Definitions from other ANSSI SCADA protection profiles:

Engineering workstation: (Panorama development workstation) Software which enables the configuration, parameter setting, programming and testing of all or part of the industrial SCADA system.

Historian: A history server, which uses a remote database and is used to store the various alarms or values from the SCADA system or the industrial process. The history server can be local or centralized.

2. DESCRIPTION OF THE REFERENCE PRODUCT

2.1 Product description

2.1.1 General product description

Panorama E² is a SCADA system that is used in industrial networks. It is interconnected with CIM level 1 field equipment and can interface with other third party equipment and software at CIM level 2 or CIM level 3.

Panorama consists of various hardware and software components that use a variety of information to operate. The system can be modeled schematically as shown in Figure 1.

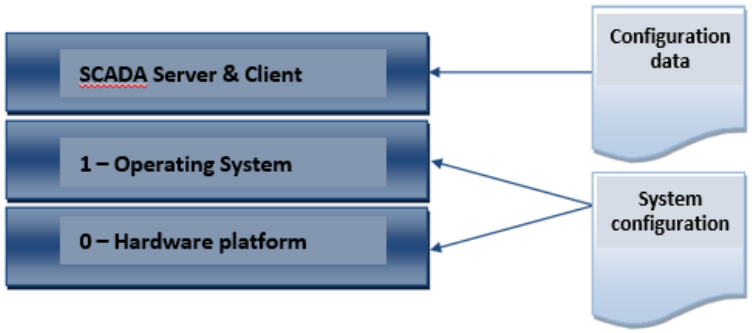

FIGURE 1 – Modeling an industrial SCADA system

Layer 0 - Hardware Platform and Layer 1 - Operating System These are the execution platform for the product: In the case of Panorama, these are machines running under Microsoft Windows.

In the remainder of this document, the bricks of the operating system necessary for the proper functioning of the product are considered to be part of this product execution platform. The same applies to applications such as a database manager, like SQL Server, which provide general purpose functionality and a certain level of integration with the operating system.

To operate, these system layers require a number of so-called "system configuration" elements.

Layer 2 - SCADA Server and SCADA Client: they constitute the ToE and provide the functionalities described in paragraph "2.1.2 Description of product functions".

In order to operate, a SCADA Server and the SCADA Client require configuration data. This data is made up of all the information required to configure the SCADA system so that its operation can be adapted to the context of a particular installation. Typical configuration data includes:

- For the Server: list of field I/O, communication with the devices, archiving characteristics, configuration of alarms, formulas, scripts, etc.
- For the client: drawing information, background information, information for animation, control of symbols to represent the status of the installations, standard HMI elements: texts, buttons, checkboxes, lists, trend configuration files, histograms, etc.

In addition to its configuration data, a SCADA Server handles data that can be described as "process" data. These are made up of all the information directly related to the installation. It includes:

- data from the field and handled by the SCADA Server. This data is important to allow the user to monitor the operation of the installation.

- data such as pre-configured commands or recipes which, if sent to the equipment, may affect the running of the installation.

The SCADA Client allows the operator to view the data processed or generated by the server and to send commands.

In addition to its configuration data, a SCADA Client handles data received from the servers. This is made up of all the information related to the status of the installation or generated internally by the server.

Panorama E² is part of the Panorama Suite which also includes Panorama COM (an acquisition front-end) and Panorama Historian. It shares the following with these products: the installation kit, the development environment and many technical elements for the server component. Note: an option in the installation kit allows you to install only Panorama E².

2.1.2 Description of product functions

The ToE comprises the following functions:

Server Component:

- **Field data acquisition and sending of commands:** ToE includes communication functions that support exchanges with field devices such as PLCs, controllers, IEDs[1]. (CIM level 1), with protocols such as OPC-DA, OPC-UA, SNMP V1/V2/V3, BACnet, IEC, Modbus. The LON protocol is excluded from the scope.

- **Data exchanges:** ToE can send and receive information streams using interfaces (OPC DA Server, OPC-UA Server, SNMP Agent) with systems such as a history server, MES, engineering station, SCADA servers, client workstations, etc. The SNMP Agent function is excluded from the target scope. Regarding the OPC-UA server, the following types of links are excluded: HTTP, Net.TCP and OPC.TCP (only HTTPS type links are included in the scope).

  These systems may be located on the same CIM 2 level, on the CIM 3 level, or even be remote on an external network.

  ToE also supports sending of e-mails, SMS, Fax, managing voice on-call, exchanging files as an FTP client and ping testing. These functions are outside the scope of the target.

- **Alarm management:** ToE detects alarm conditions from information received from field equipment or from internal data and handles the processing, transmission and logging of this information.

- **Archiving functions**: ToE provides functions for archiving and extracting values.

  This function can be rendered through:

  - On-stream or selective archiving which can store in a private format:
    - locally on the machine producing the data
    - on a remote machine using the "archive server".
  - A database export (public format)

[1] Intelligent Electronic Device, a term used in the field of electrical energy, which includes all automation equipment with protection or local control functions such as circuit breakers, transformers, etc.

- **Redundancy functions:** ToE enables redundant operation to ensure high availability of its functions.

- **Dynamic persistence function:**

This function consists of two sub-functions:

  - Value storage: ToE allows real-time data values to be stored between two start-ups, for example to avoid restarting counts or countdowns to zero (function available outside of redundancy). Internal use.

  - Traceability of changes: Log of changes to adjustable priorities, such as alarm threshold values. External use.

Client Component:

- **Human-Machine Interface:** ToE includes human machine interface functions**:**

  - Management of mimic diagrams that allow installation status to be represented graphically and local commands to be sent to ToE or transmitted to the process.

  - Alarms: Display of states, alarm history and commands such as acknowledgement, disabling, report entry, etc.

  - Display of trends, histograms, etc.

  - GeoScada and Web Browser functions. These functions are outside the scope of the target.

  - Operator identification. Only the external authentication of operators is within the scope of the target. Modification of profiles during operation is excluded.

- **Redundancy compatibility:** Automatic selection of active server

Commonalities:

- **Data processing, scripting and scheduling:** ToE provides processing, calculation and "scheduling" functions.

- **Generic access to a database table:** Database and recipe interface. ToE allows to access a database table in order to read, write or delete records.

- **Local backup storage:** ToE provides a mechanism to store entries locally for archiving functions which access databases when remote storage is inaccessible. When communication is restored there is an automatic transfer of the locally stored values.

- **Administration functions:** ToE comprises several interfaces to allow its administration: configuration management, user management. Note: these administration functions are used by different categories of users (see § 4 Description of the different users).

- **Configuration deployment functions:** ToE includes an interface allowing the deployment of configuration data that has been updated on the engineering workstation: general architecture of the application, I/O data, communication with field devices, alarm conditions, mimics, formulas, etc.

Note: some of these configuration data elements defined as adjustable can be adapted during operation, but under no circumstances can the structure of the application be modified.

Note: for reliability and cybersecurity reasons, the server control function associated with the copy function is disabled.

- **Diagnostics function:** ToE provides diagnostic functions to monitor its operation and internal status (e.g. Tracer, Application explorer)

- **Local logging of events:** ToE offers a policy for local logging of security and administration events. Logged events are described in the manual "*Application Security > Security and Network Operations > Using Logs*".

The following functions are outside the scope of the target

- Access to a database other than SQL Server.
- Mobile HMI Server and SmartBMS access.
- Panorama Historian Export and transfer of archives to Historian.
- Extension of the Panorama SCADA functions delivered as standard by the use of user objects developed by the configurators using the same integration methodology as the Panorama functions.
- Licenses provided by the Panorama License Server (SLP): Use of specialized Safenet key on USB port or license file.

These functions are natively disabled. To enable them, they must be added to the application configuration file.

2.2 Description of the product usage architecture

Legend to diagrams:

- the dashed flows are outside the scope of this CSPN
- grey blocks represent the modules covered by the CSPN

Panorama supports several types of physical network architecture: two are typical

- Client-Server, single network
- Client-Server, separate process network

Only the latter architecture is adopted to offer a suitable level of security.

In these types of architecture, the software components are deployed across multiple machines in order to distribute processing, to be closer to the field equipment, to ensure scalability, for redundancy of certain functions, and to offer several "thick" client workstations.

Note:

- A standalone architecture is also supported: It means putting all the ToE elements on a single machine, without the "archive server" function, which is not useful in this configuration.
- In Panorama terminology:
    - The SCADA Server is called the "Functional Server".
    - The SCADA Client is referred to as a "Workstation"
- The Mobile HMI server is considered as a functional server.
- For load balancing and redundancy all architectures are possible: for instance, it is not necessary to pair the servers.

For logical flows, please refer to the manual "*Application security > Security and network operation > Configuration for Panorama networking > Appendix: principle of network exchanges*".

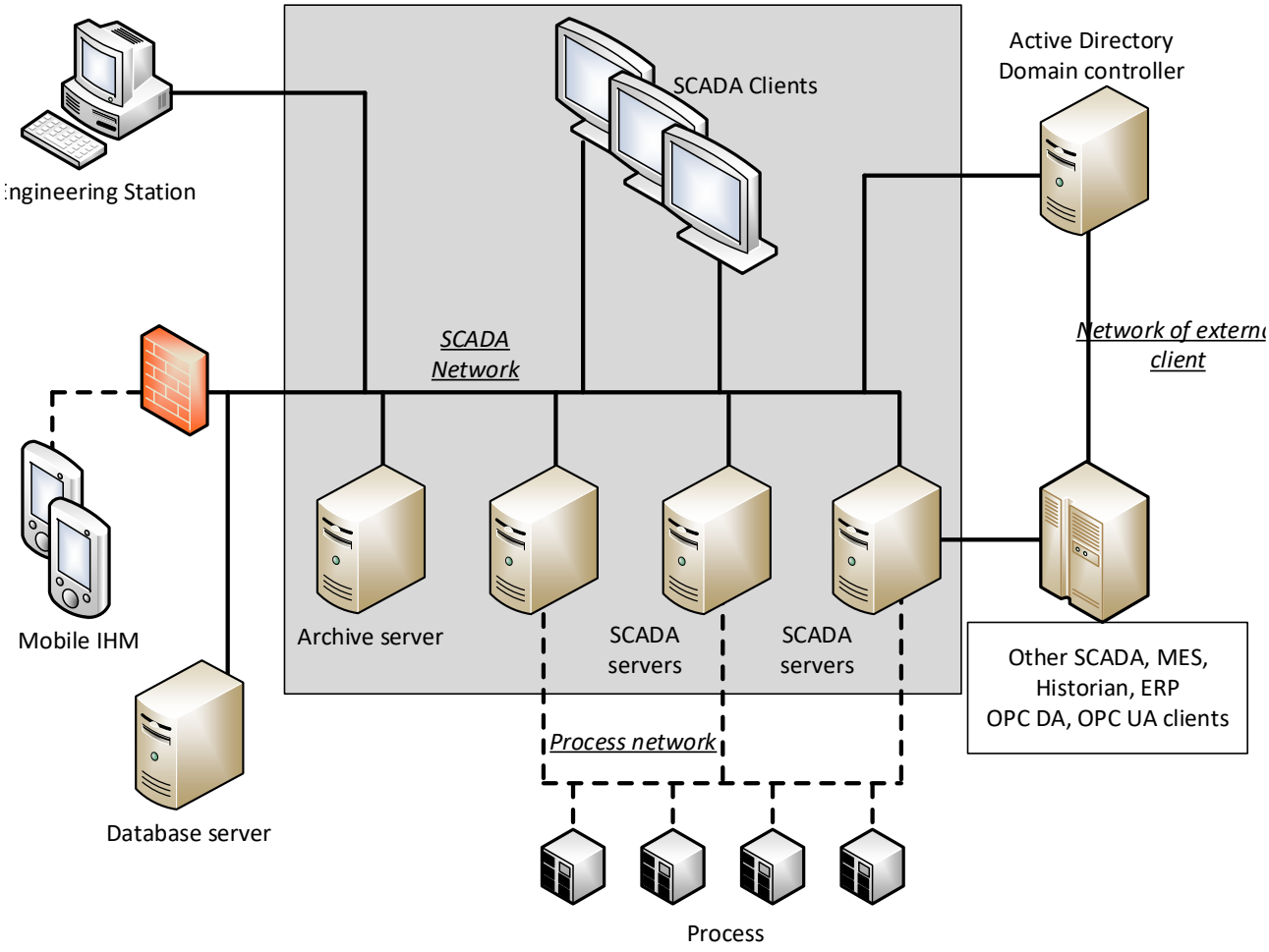

FIGURE 2 – Client-Server Architecture, separate process network

Three networks:

- SCADA network: an internal ToE network, connected to the dedicated database server and to the engineering workstation
- Process network
- Network of external clients (Other SCADA, MES, ERP, etc.)

3. SCOPE OF EVALUATION

3.1 Configuration and mode of operation

- Windows versions:
    - Windows 10 (1709)
    - Windows Server 2016 1607

  together with their security updates
- Windows in a domain.
- Advanced DCOM configuration with configuration of Panorama services in a dedicated account, see Panorama manual.
- The OPC-DA clients of the Panorama data server function are in the same domain as the ToE.
- Functions that are not useful for a machine are not installed on it.

3.2 Evaluation platform

The platform presented below is the minimum platform allowing all sensitive assets and security features to be brought into play.

The configuration of the Panorama application must involve:

- Internal data streams: application distributed over two logical servers with links between data distributed over the two servers and the client machine contains a mimic diagram with, for example, a trend curve and an alarm window.
- All functions that use a database.
- The interfaces for accessing operating and processed data (see below).
- The data streams with the engineering station

In terms of machines, the following is required:

- ToE
    - Two SCADA Servers, one under Windows 10 and the other under Windows Server 2016
    - A SCADA Client machine (Windows 10)
- Outside ToE
    - A domain Server (Windows server 2016)
    - An engineering workstation (Windows 10)
    - A machine with OPC-DA and OPC-UA Client (Windows 10)

- A machine that simulates the process (Windows 10)

- Outside and inside ToE
  - A machine that contains the database (outside ToE) and the archive server (ToE) (Windows 10). Hosting of the Archive Server and SQL Server on the same machine is a very common case for customers.

4. DESCRIPTION OF THE DIFFERENT USERS

Preamble: Unless otherwise specified, the users described below are managed by Active Directory. The others are managed by the ToE.

The list of user types that can interact with the ToE is as follows:

- **Operator:** Users whose main role is to operate the ToE from the SCADA Client.
  Via the HMIs, the operator can:
  - view the data, in particular by navigating between graphical views,
  - send commands (local to the ToE or else sent on to the process),
  - view events and histories,
  - view and acknowledge alarms,
  - adapt the dynamically modifiable part of the configuration (see § 6.2 bst 2)
  - diagnose,
  - stop and start the application.

- **Application Configurator/Developer:** Users in charge of the design, development and maintenance (upgrades or corrective maintenance) of the SCADA application, without the ability to modify the underlying software.
  In the case of ToE, the application developers perform the following functions:
  - distribution of configuration data updates,
  - changes of application on the ToE,
  - license management,
  - management of the dynamic persistence database,
  - definition of the user permissions policy for users managed by the ToE,
  - Note: in order to carry out their tasks, they also have the user permissions of operators.

- **System-Backup operator**: User tasked with backing up data generated by applications, such as databases or archive files. From time to time, may also be called upon to restore data backed up on the ToE. The permissions necessary for this latter task are assigned temporarily by the administrator.

- **Administrator**: Users responsible for administration of the ToE: installation, software updates and ability to enable or disable logs.

- **Auditor:** User with the right to view all or part of the event logs produced by the ToE.

- **Super-administrator:** User whose role is to define the user permissions policy for users managed in AD.

- **ToE services execution user:** User under which "Windows Service" type processes are executed within ToE. This may be different for each service.

- **Users of external interfaces:** Users of third-party applications which access the "Operating Data" and "Processed Data" through the "Data Server" stream using the "Collaborative data streams". They can perform the same actions as an operator with the exception of diagnostics. They can be limited in their actions depending on the interface used and the configuration of the application. There are two types of "External interface users":

  - **User of external OPC-DA interfaces:** This user type is managed by AD.

  - **User of external OPC-UA interfaces**: This user type is managed by the ToE (using certificates).

Notes:

A user does not have to be a physical person and can be a third-party device or program. In addition, the same physical person can be the holder of several accounts with different user profiles.

IMPORTANT: "Panorama users", as defined in the Panorama user manual, are an application over-layer that allows operators to be differentiated. This notion does not come into play with respect to the target, which relies on "Windows Users" to differentiate between users for the purposes of the protection profile.

5. ASSUMPTIONS ON THE ENVIRONMENT:

Following assumptions are made regarding the environment and the conditions of use of the ToE:

h 1) **Information system hygiene rules:** The recommendations set out in ANSSI publication "Guideline for IT Hygiene" are followed where they are applicable.

Accordingly, the Windows accounts and passwords required to use Panorama are only provided to users with the appropriate profile.

For all the machines in the domain, only the administrators have the account name and password of the local administration account for the machine. Only the super-administrator has the right to register a machine with the domain.

The system implementing the product must have an applicable security policy, ideally one based on the ANSSI Guideline for IT Hygiene. An Information System Security (ISS) officer is responsible for implementing and supervising the policy.

Note: In the chapter entitled "Application security", the manual quotes this document and details the majority of these points in the Panorama Windows framework, without systematically going as far as instructions for use. The customer must adapt the recommendations to their own specific case.

h 2) **Analyzing logs:** It is considered that the "auditors" regularly view the local logs generated by the equipment. They study them and react, where necessary, by applying a cybersecurity incident handling procedure.

h 3) **Users:** The users defined in chapter "4 Description of the different users" are all competent, trained and non-hostile.

h 4) **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.
On the other hand, since identical products to the ToE may be purchased freely, the attacker may purchase one in order to research vulnerabilities by any possible means.

h 5) **Dimensioning:** ToE is assumed to be properly sized for the processing it is to perform.

h 6) **Authentication servers:** Authentication servers used to authenticate users are considered to be healthy and correctly configured, as per the recommendations of the ANSSI security guide for Active Directory ("Recommandation de sécurité relatives à Active Directory" N°DAT-NT-17/ANSSI/SDE/NP dated 10/9/2014).

h 7) **Database servers:** The database servers are considered to be healthy and correctly configured.

h 8) **Healthy operating system:** The operating system of the system implementing the ToE is considered healthy at the beginning of the evaluation and throughout the evaluation except in the case of ToE failure.

h 9) **Hardened operating system:** The operating system is assumed to have been configured and "hardened" in accordance with the ToE manufacturer's recommendations.
In particular:

- The operating system is assumed to be up to date.
- The domain is configured so that only the domain administrator (super-administrator) can add a machine to the domain and the associated DNS servers.
- Only accounts that need to log on a ToE machine can do so (using a GPO at the domain server level for example).

h 10) **Unevaluated services absent:** All services provided by Panorama but outside the security target are not configured/added in the Panorama application by the developer.

h 11) **Security documentation:**

- The ToE is supplied with a detailed manual on how to use it securely, cf. "Security of the application" chapter. In particular, all the connection secrets present by default are listed to allow their customization.
- Security bulletins are published:
  - As soon as a security vulnerability is discovered, with the provision of a solution or instructions for use
  - As soon as an improvement in security is available, for example following changes in standards.

All the recommendations stemming from this documentation and from the security bulletins have been applied for evaluation, including to machines other than those hosting the ToE and which may or may not be on the network: The typical example is: "the Panorama application's protection rules are applied on all the machines where it is copied".
In particular, as stated in the Security Bulletin Pano/BS-010, a policy should be put in place to monitor the expiry status of certificates and to update the list so that the thumbprint of expired certificates for OPC-UA can be removed and replaced by those of renewed certificates.

h 12) **External module:** It is assumed that no external modules[2] are installed on the ToE. For example, user objects are clearly excluded from the target.

h 13) **Software non-adherence:** The ToE has been developed in such a way that it does not adhere to a given version of an external component[3] (operating system, software, library). In particular, the user must have the possibility to apply security updates of any external component.
Otherwise, this component must be integrated into the ToE.

h 14) **Activation of logs:** The local logging function based on Windows event logs is assumed to be activated, functional, intact and authentic.

[2] An external module is a software element that brings new functionalities to the ToE but is not essential for its operation. For example: "Panorama user object"

[3] An external component is a software element necessary for the operation of the ToE

6. DESCRIPTION OF SENSITIVE ASSETS TO BE PROTECTED

6.1 Sensitive assets of the environment

The sensitive assets of the environment are as follows:

bse 1) **Data stream towards the engineering station:** this is a file copy stream by SMBv3 and the use of a share accessible only to the configurators. When the copy is triggered from the engineering station, there are additional UDP and DCOM streams if server control is used. These streams do not exist if the copy is triggered from the ToE.

The data streams between the ToE and the engineering station must be protected in terms of integrity, confidentiality and authenticity.

Note: Confidentiality of the data stream from the engineering station is not based on encryption of the application by Panorama.

bse 2) **Data streams to a history server:** The data streams between the ToE and a history server must be protected in terms of integrity and authenticity, SQL Server streams.

bse 3) **Collaborative streams:** Collaborative streams must be protected in terms of integrity and authenticity. They consist of all streams between the ToE and other system components:

I) ToE status monitoring stream: this allows to know if a server is accessible, if an application is loaded and which one, and to know the status of the application's "logical servers". This stream is based on UDP and a proprietary protocol. Used in conjunction with the control stream, see below

II) Application control stream from the "Administration & Configuration" tool used from a machine outside ToE, DCOM stream.

III) Data stream with the on-stream archive server function, DCOM data stream, for transfer by API from a machine outside ToE.

IV) Data stream for remote diagnostic tools such as "Application Explorer" (DCOM stream) and the tracer (Pipe), from a machine outside ToE.

V) OPC-DA and OPC-UA "data server" streams which allow access to operating data and/or the sending of commands.

bse 4) **Operating data**: The operating data is made up of all the information useful for the correct operation of the SCADA system in the operational phase. This set includes instantaneous values, alarms and commands.

The data is made available to third party applications (Application extensions, other SCADA, Hypervision, MES, ERP) by ToE through standard interfaces described below.

The data must be protected in terms of integrity and authenticity.

Access to this data is governed by the permissions policy of the ToE or by the services offered by the operating system or the database server. It is useful to know how this data is accessed:

I) From internal streams (see § 6.2 Sensitive assets of the ToE bst10)

II) From collaborative streams bse3

III) Data archived by the archive server, DCOM stream
Accessible by DCOM via an extraction object either from the Client workstation or from a tool that uses this object's public API.

bse 5) **User authentication mechanism managed by AD:** The integrity and authenticity of the mechanism must be protected by the ToE.

bse 6) **User connection secrets managed by AD:** ToE must guarantee the integrity and confidentiality of these identifiers.

The security requirements for sensitive assets in the environment are as follows:

Asset	Availability	Confidentiality	Integrity	Authenticity
Data stream towards engineering station		X	X	X
Data streams to a history server			X	X
Collaborative streams			X	X
Operating data			X	X
User authentication mechanism managed by AD			X	X
User connection secrets managed by AD		X	X	

6.2 Sensitive assets of the ToE

The sensitive assets of the ToE are as follows:

bst 1) **Software:** In order to correctly fulfil its functions, for the software, the integrity must be protected under all circumstances and authenticated at the time of installation or update.

The software includes the items that are installed by the Panorama installation kit and are used when running the ToE: binaries, class descriptors and reference applications.

bst 2) **Configuration:** The configuration of the ToE must be confidential and compliant in terms of integrity. Within the framework of Panorama any user of the ToE can have read access to the application. The attacker must not be able to discover this configuration other than by observing ToE activity.

The configuration comes partly from the engineering station. Another part is done locally on each machine, such as the configuration of local backup storage, network monitoring, etc.

The part coming from the engineering station can be dynamically modified on the ToE by the operators. This concern only the values of "adjustable" properties. The adjustments are stored by the ToE with the same level of confidentiality and integrity as the rest of the configuration.

bst 3) **Authentication mechanism for users managed by ToE:** The integrity and authenticity of the mechanism must be protected.

bst 4) **Certificates of users of external OPC-UA interfaces of the ToE**: These are certificates presented by the users of external OPC-UA interfaces to enable their identification by the ToE. ToE must guarantee the integrity of these identifiers.

bst 5) **Certificates of the OPC-UA Data Servers of the ToE**: For this version of the target, this is a certificate used by the OPC-UA Data Server function. ToE must guarantee the integrity of these elements.

bst 6) **Database connection secrets:** ToE must guarantee the integrity and confidentiality of these identifiers.

bst 7) **Permissions management policy:** The integrity of this permissions management policy must be guaranteed.

bst 8) **Local logging function:** ToE has a local logging function that, once activated, must remain operational.

bst 9) **Local events logs:** The integrity of the local logs generated by the ToE must be guaranteed.

bst 10) **Internal streams:** They are made up of all the internal streams between the different machines within the ToE, and must be protected in terms of integrity and authenticity:

I) ToE status monitoring stream: this allows the following to be known: whether a server is accessible, or an application is loaded and which one, and to know the status of the application's "logical servers". This stream is based on UDP and a proprietary protocol.

II) Application control stream from the Panorama application or from the "Administration & Configuration" tool, DCOM stream.

III) Data exchange streams, including alarms, DCOM stream. This includes streams between servers as well as between servers and clients.

IV) Data stream with the on-stream archive server function, DCOM stream.

V) Data stream for remote diagnostic tools such as "Application Explorer" (DCOM stream) and the tracer (Pipe).

VI) Stream to access the operators' settings reference. This is a file copy stream by SMBv3

and the use of a share accessible to operators and to configurators.

bst 11) **Generated data**: The "generated data" is made up of all the information useful for the correct operation of the SCADA system in the operational phase and generated internally by the ToE, for instance from operating data. This set includes counter values, formula results, properties of Panorama objects, etc.

It is accessible and processed in the same way as operating data "§ 6.1 Sensitive assets of the environment bse 4".

bst 12) **Archived data:** The archived data is made up of the data stored by the "On-stream or selective archiving" function. Note: The function can store both "operating data" and "generated data".

It must be stored with integrity and authenticity, and at all times it must be protected and available.

The security requirements for sensitive assets of the ToE are as follows:

Asset	Availability	Confidentiality	Integrity	Authenticity
Software			X	X
Configuration		X	X	
Authentication mechanism for users managed by ToE			X	X
Certificates of users of external OPC-UA interfaces of the ToE			X	
Certificates of the OPC-UA Data Servers of the ToE			X	
Database connection secrets		X	X	
Permissions management policy			X	
Local logging function	X			
Local events logs			X	
Internal streams			X	X
Generated data			X	X
Archived data	X		X	X

7. DESCRIPTION OF THREATS

7.1 Description of threat-agents

The following threatening agents are considered:

am1) **Malicious user Level 1:** An attacker with a user account managed by AD but which is not a user account as defined in "4 Description of the different users". He is seeking to use the ToE.

am2) **Malicious user Level 2:** An attacker with a user account managed by AD and who has a user account as defined in "4 Description of the different users" without having administration privileges (administrator or super-administrator). He seeks to overstep the permissions of the account he has compromised.

am3) **Attacker in the industrial system:** Any attacker without an account seeking to attack the ToE.

None of these attackers are located on the "process" network.

7.2 Threats to be considered

The following threats are to be considered (§ 9 Assets /Threats/Security coverage table indicates to which assets these threats apply):

m 1) **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, etc.).

m 2) **Data stream alteration:** The attacker manages to modify exchanged data without being detected.

m 3) **Data streams compromise:** For data streams requiring confidentiality, the attacker manages to recover information by intercepting exchanges between the ToE and an external component.

m 4) **Software corruption:** The attacker manages to modify, temporarily or permanently, the ToE software. The attacker manages to execute illegitimate code on the ToE.

m 5) **Configuration corruption:** The attacker manages to modify, temporarily or permanently, the configuration of the ToE.

m 6) **Configuration compromise:** The attacker manages to illegally obtain all or part of the ToE configuration.

m 7) **Credentials theft:** The attacker manages to steal a user's connection secrets or database connection secrets.

m 8) **Authentication violation:** The attacker succeeds in authenticating himself without having the connection secrets.

m 9) **Access permissions violation:** The attacker manages to obtain permissions that he does not normally have.

m 10) **Local event logs compromise:** The attacker manages to delete or modify an entry in the local event logs without having been authorized to do so by the ToE permissions policy.

8. SECURITY FUNCTIONS

The security functions are as follows ($ 9 Assets /Threats/Security coverage table indicates to which threats these objectives apply):

fs 1) **Malformed input management:** The ToE has been developed in order to correctly handle malformed input, in particular malformed network traffic.

fs 2) **Secure communication:** The ToE supports secured communication, protected in integrity and authenticity. If required, confidentiality is enforced for data streams described in chapter "6.1 Sensitive assets of the environment".

fs 3) **Non-disclosure of user connection secrets managed by AD**: ToE does not allow the connection secrets of a user authenticated by AD to be retrieved.

fs 4) **Integrity of the certificates of users of external OPC-UA interfaces of the ToE**: ToE must be able to protect these certificates so that only authorized users can modify them.

fs 5) **Integrity of certificates of the OPC-UA Data Servers of the ToE**: ToE must be able to protect these certificates so that only authorized users can modify them.

fs 6) **Access to databases using Integrated Security:** ToE allows access to databases using "Integrated Security", thus avoiding the storage of database connection secrets.

fs 7) **Secure authentication:** Use of ToE requires user authentication to differentiate between users and thus protect assets such as the configuration and various connection secrets.

fs 8) **Access control policy:** The user permissions policy is managed in a very strict way. In particular, the implementation of this policy makes it possible to guarantee the authenticity of critical operations, i.e. those liable to damage the identified sensitive assets.

fs 9) **Software signature:** The installation kit and updates are all signed with a certificate in the name of Codra, provided by a recognized certification authority.

Note: this allows the administrator to verify the authenticity and integrity of the software components when installing or updating them.

fs 10) **Configuration confidentiality and integrity:** The user management policy does not allow an unauthorized person to read or modify all or part of the ToE configuration. It is based on the use of Windows accounts and the setting up of appropriate permissions on the directory containing the application.

fs 11) **Log integrity:** Panorama records its logs with such permissions that only the administrators and the super-administrator can disable Panorama logs, delete one of these logs or one of their events.

9. ASSETS /THREATS/SECURITY COVERAGE TABLE

It is of interest to associate the lines that have crosses in the same column, which makes it possible to see by **which security function(s) an asset is covered**, by moving from part A to part B).

Examples:

- Part A) Software is covered by "Software Signature" in part B) through the column "Software Corruption"
- "User Authentication Mechanism" is covered by "Secure Storage of Secrets" and "Secure Authentication with Authentication Server".

Legend:

A = Authenticity

C = Confidentiality

Av = Availability

I = Integrity

THREATS	Denial of service	Data stream alteration	Data streams	Software corruption	Configuration corruption	Configuration compromise	Credentials theft	Authentication violation	Access permissions policy violation	Local events logs compromise
A) ASSETS										
bse1) Data stream towards engineering station		I A	C			C				
bse2) Data streams to a history server		I A								
bse3) Collaborative streams		I A								
bse4) Operating data		I A							IA	
bse5) User authentication mechanism managed by AD								IA		
bse6) User connection secrets managed by AD							CI			
bst1) Software				IA						
bst2) Configuration					I	C				
bst3) Authentication mechanism for users managed by ToE								IA		
bst4) Certificates of users of external OPC-UA interfaces of the ToE								I		
bst5) Certificates of the OPC-UA Data Servers of the ToE					I					
bst6) Database connection secrets							CI			
bst7) Permissions management policy									I	
bst8) Local logging function	Av									
bst9) Local events logs										I
bst10) Internal streams		I A								
bst11) Generated data		I A							IA	
bst12) Archived data	Av	I A							IA	
B) Security features										
fs1: Malformed input management	X									
fs2: Secure communication		X	X							
fs3: Non-disclosure of user connection secrets managed by AD							(2)			
fs4: Integrity of the certificates of users of external OPC-UA interfaces of the ToE								(3)		
fs5: Integrity of certificates of the OPC-UA Data Servers of the ToE					(5)					
fs6: Access to databases using Integrated Security							(4)			
fs7: Secure authentication		(1)			X	X	X	X		
fs8: Access permissions policy									X	
fs9: Software signature				X						
fs10: Configuration confidentiality and integrity					I	C				
fs11: Log integrity										X

(1) Contributes to authenticity of data stream "to and from engineering station"
(2) For the asset "User connection secrets defined in AD"
(3) For the asset "Certificates of users of external OPC-UA interfaces of the ToE"
(4) For the asset "Database connection secrets"
(5) For the asset "Certificates of the OPC-UA Data Servers of the ToE"