PREMIER MINISTRE

Secretariat General for National

Central Directorate for Information Systems Security

Certification Report ANSSI-CSPN-2019/14

Panorama E^2
Version 7.0

Paris, November 7, 2019

Director of the French National Agency for
Information Systems Security - ANSSI

Guillaume POUPARD

Courtesy Translation

Warning

This report is intended to provide sponsors with a document certifying the security level provided by the product under the operating or usage conditions set out in this report, for the version evaluated. It is also intended to inform potential buyers of the conditions in which they may use or operate the product, in order to ensure that the product is used under the conditions for which it has been evaluated and certified. Consequently, this certification report must be read in conjunction with the evaluated user and administration guides and the product's security target, which contains a list of threats and a set of assumptions about the usage environment and conditions, so that users can make an informed decision as to whether the product meets their security requirements.

Certification does not, however, constitute a product recommendation from ANSSI (French Network and Information Security Agency), and does not guarantee that the certified product is totally free of all exploitable vulnerabilities.

Any correspondence about this report has to be addressed to:

Secrétariat général de la défense et de la sécurité nationale Agence nationale de la sécurité des systèmes d'information Centre de certification
51, boulevard de la Tour Maubourg 75700 PARIS cedex 07 SP
France   certification@ssi.gouv.fr

Certification report reference **ANSSI-CSPN-2019/14**
Product name **Panorama E^2**
Product reference/version **Panorama E^2** **Version 7.00 integrated into Panorama Suite 2017 (build 17.00.011) with 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**
Product category **Other (SCADA)**
Evaluation criteria and version **FIRST LEVEL SECURITY CERTIFICATION *(CSPN)***
Sponsor **Codra ingénierie informatique** **Immeuble Hélios – 2 rue Christophe Colomb - CS 0851, 91300 Massy, France**
Developer **Codra ingénierie informatique** **Immeuble Hélios – 2 rue Christophe Colomb - CS 0851, 91300 Massy, France**
Evaluation facility **Oppida** **4-6 avenue du vieil étang, Bâtiment B - 78180 Montigny le Bretonneux, France**
Security functions evaluated **Malformed input management** **Secure communication** **Non-disclosure of login secrets of users managed by the *Active Directory*** **Integrity of the certificates of users of OPC-UA interfaces** **Integrity of connection secrets to OPC-UA Data Servers** **Access to data bases authenticated by the *Active Directory*** **Secure authentication** **Access permissions policy** **Software signature** **Configuration confidentiality and integrity** **Log integrity**
Security function(s) not evaluated **Not applicable**
Restriction(s) on use **Yes (see §3.2)**

Preface

Certification

The security certification of information technology products and systems is governed by amended decree No. 2002-535 of 18 April 2002. This decree states that:

- The central information system security department establishes **certification reports**. These reports specify the characteristics of the proposed security objectives. They may contain any warnings that the authors deem useful for security purposes. They may be disclosed to third parties or the general public at the sponsor's discretion (article 7).
- The **certificates** issued by the Prime Minister attest that the copy of the product or system evaluated complies with the specified security objectives. They also attest that the evaluations have been performed in accordance with current rules and standards, with the requisite competence and impartiality (article 8).

The CSPN (first level security certification) procedures are available at www.ssi.gouv.fr.

Contents

1 The product

1.1 Product presentation

The product evaluated is the “Panorama E^{2}, version 7.00” developed by *CODRA INGENIERIE INFORMATIQUE.*

Designed for deployment in industrial networks, Panorama E2 includes a SCADA server that can be connected to level 1 field equipment as defined by the CIM (Computer-Integrated Manufacturing) classification. This server enables the acquisition of field data and the sending of commands, as well as the management of alarms.
Panorama E2 also includes a SCADA client, which, among other things, allows a human-machine interface (HMI) to be presented to the user.
Panorama E2 can also be connected to other level 2 and 3 equipment, in particular via an OPC-UA server with HTTPS type links.

The figure below details the product's deployment architecture. The target of evaluation corresponds to the shaded area.

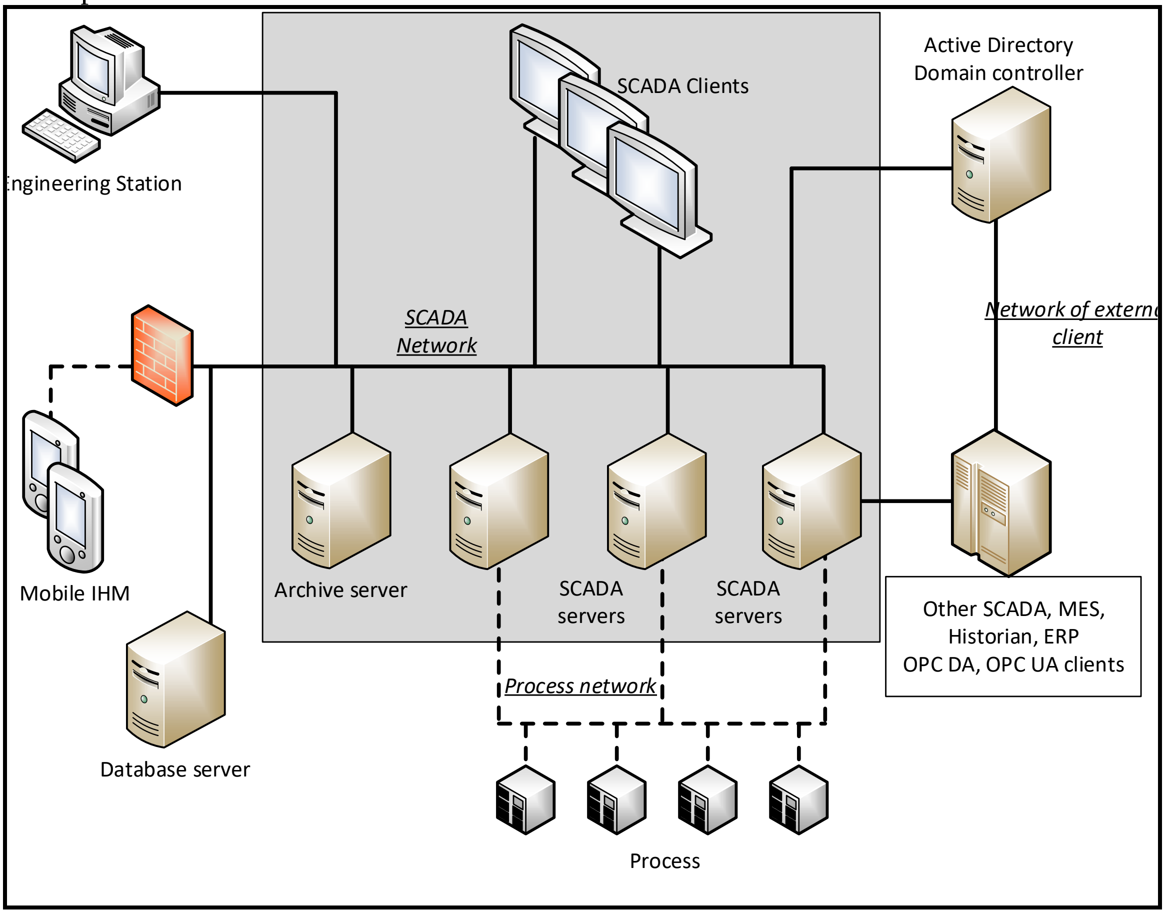


Figure 1 - The product's deployment architecture.

1.2 Description of the product evaluated

The security target [ST] describes the product evaluated, its security functionalities and its operating environment.

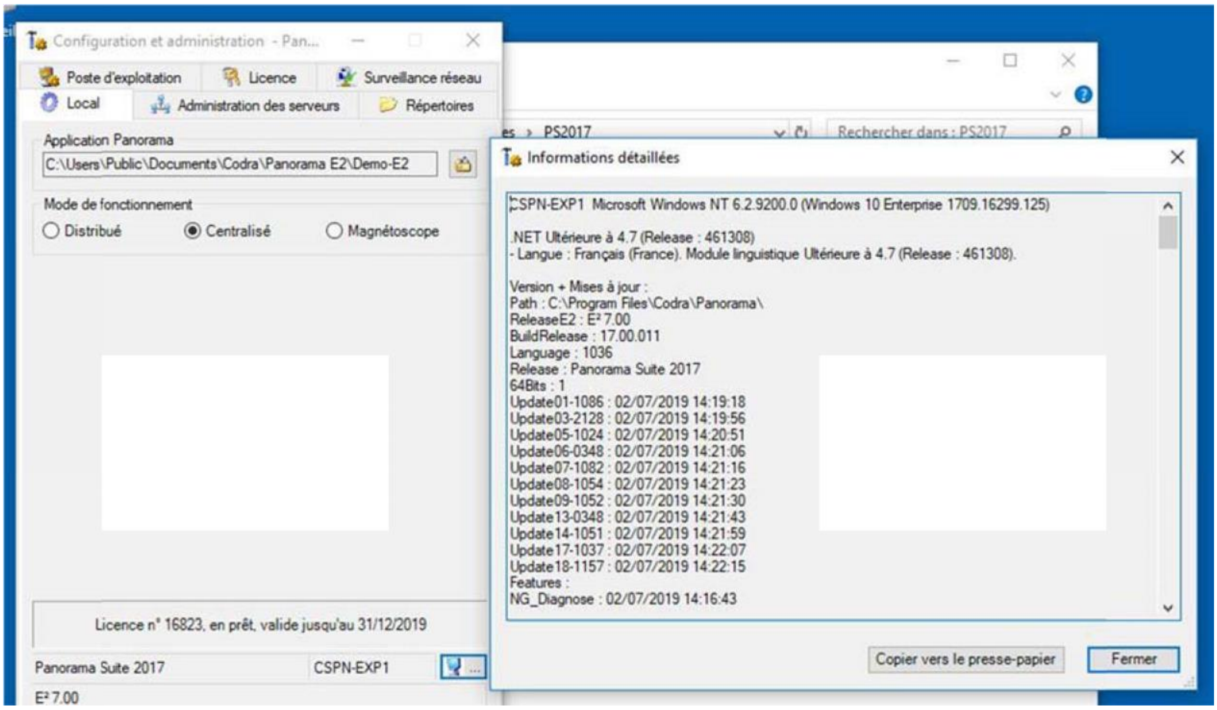
1.2.1 Product category

☐ 1 – intrusion prevention
☐ 2 – virus/malicious code protection
☐ 3 – firewall
☐ 4 – data erasure
☐ 5 – security administration and supervision
☐ 6 – identification, authentication and access control
☐ 7 – secure communication
☐ 8 – secure messaging
☐ 9 – secure storage
☐ 10 – secure operating environment
☐ 11 – set top box (STB)
☐ 12 – embedded hardware and software
☐ 13 – industrial programmable logic controller
☒ **99 – other (SCADA)**

1.2.2 Product identification

Product name	Panorama E^2
Number of evaluated version	7.00 (full version: Version 7 integrated into Panorama Suite 2017 (build 17.00.011) with updates PS2-1700-01-1086, 03-2128, 05-1024, 06-0348, 07-1082, 08-1054, 091052, 13-0348, 14-1051, 17-1037)

To check the version of Panorama E2, connect to one of the machines on which Panorama E2 is installed and run the "configuration & administration" program. In the "Local" tab, click on "Display details" as shown in the figure below.



Application Panorama: C:\Users\Public\Documents\Codra\Panorama E2\Demo-E2

Mode de fonctionnement: ○ Distribué ● Centralisé ○ Magnétoscope

Licence n° 16823, en prêt, valide jusqu'au 31/12/2019

Panorama Suite 2017 | CSPN-EXP1

E² 7.00

```
CSPN-EXP1  Microsoft Windows NT 6.2.9200.0 (Windows 10 Enterprise 1709.16299.125)

.NET Ultérieure à 4.7 (Release : 461308)
- Langue : Français (France). Module linguistique Ultérieure à 4.7 (Release : 461308).

Version + Mises à jour :
Path : C:\Program Files\Codra\Panorama\
ReleaseE2 : E² 7.00
BuildRelease : 17.00.011
Language : 1036
Release : Panorama Suite 2017
64Bits : 1
Update01-1086 : 02/07/2019 14:19:18
Update03-2128 : 02/07/2019 14:19:56
Update05-1024 : 02/07/2019 14:20:51
Update06-0348 : 02/07/2019 14:21:06
Update07-1082 : 02/07/2019 14:21:16
Update08-1054 : 02/07/2019 14:21:23
Update09-1052 : 02/07/2019 14:21:30
Update13-0348 : 02/07/2019 14:21:43
Update14-1051 : 02/07/2019 14:21:59
Update17-1037 : 02/07/2019 14:22:07
Update18-1157 : 02/07/2019 14:22:15
Features :
NG_Diagnose : 02/07/2019 14:16:43
```

Figure 2: Displaying the Panorama E^2 version and updates

1.2.3 Security functions

The security functions evaluated are:

- malformed input management;
- protection of the integrity and authenticity of the data streams on the SCADA networks and the network of external clients;
- protection of the confidentiality of user connection secrets;
- integrity of the certificates of users of OPC-UA interfaces;
- integrity of connection secrets to OPC-UA Data Servers;
- authentication of database accesses *via the Active Directory*;
- secure authentication;
- access control management;
- software signature;
- configuration confidentiality and integrity;
- log integrity.

1.2.4 Configuration evaluated

The test platform consists of the following elements:

- two functional servers, on which the Panorama E2 product is deployed on a set of virtual machines installed in an ESXi
  - one under Windows Server 2016 version 10.0.14393
  - the other under Windows 10 Enterprise version 10.0.16299

an *Active Directory* domain controller under Windows Server 2016 10.0.14393;

- a database under Windows Server 2016 10.0.14393;
- an operating workstation under Windows 10 Enterprise 10.0.16299;
- an engineering workstation under Windows 10 Enterprise version 10.0.16299;
- an external client under Windows 10 Enterprise version 10.0.16299;
- a process network device under Windows 10 Enterprise version 10.0.16299.

ESXi version: to check the ESXi version, log on to the web GUI. The version used for the evaluation was version 6.0.0 / 3073146, as shown in the figure below.

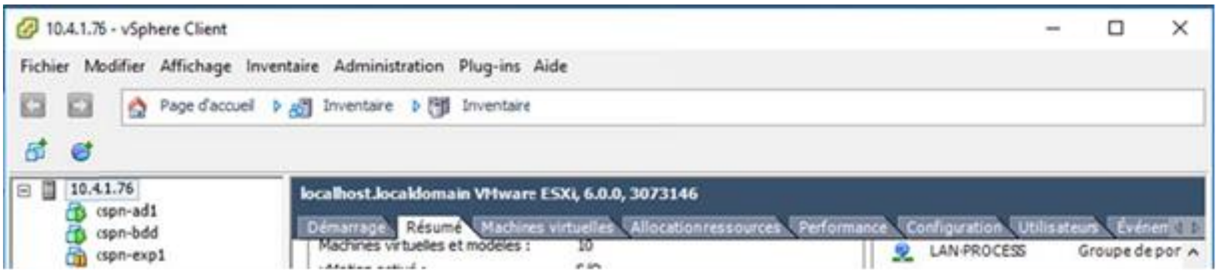


Figure 3: ESXi Version Display

OS versions: to check OS versions, connect to the Windows machines and launch "Get-WmiObject Win32_OperatingSystem | Select Caption, Version" in PowerShell. The OS versions used for evaluation are listed in chapter 1.2.4.

2 The evaluation

2.1 Evaluation benchmarks

The evaluation was performed in accordance with First Level Security Certification [CSPN]. The document references can be found in Annex2.

2.2 Anticipated workload and duration of the evaluation

The length of the evaluation was in line with the workload anticipated in the evaluation file.

2.3 The evaluation process

The evaluation process was conducted on the basis of the security requirements, sensitive assets, threats, users and security functions described in the security target [ST].

2.3.1 Product installation

2.3.1.1 Specific environment configuration features and installation options

The product was evaluated using the configuration specified in paragraph 1.2.4. The installations were carried out by the developer according to the recommendations given in chapter 3.2

2.3.1.2 Description of the installation process and of any non-conformities

Not applicable.

2.3.1.3 Installation time

Not applicable.

2.3.1.4 Notes and remarks

None.

2.3.2 Document analysis

The [GUIDES] and the [ANNEXE_PTF] document were made available to the evaluator for the purposes of this evaluation.
The product guides enable the product to be used without causing inadvertent degradation in security. Although the product was installed by the developer, the evaluator was able to review the [ANNEXE_PTF] document which was used during the installation, and found it to be adequate for the safe installation of the product.

2.3.3 Source code review (optional)

The evaluator reviewed the source code of the entire product using automated tools. The evaluator also performed a manual review of OPC-UA functions. This analysis contributed to the compliance and robustness analysis of the product's security functions.

2.3.4 Security function compliance analysis

All the security functions tested complied with the security target [ST].

2.3.5 Security function strength analysis

All the security functions underwent penetration tests and none of them displayed any exploitable vulnerability to the specified level of attack, in the product’s context of use.

2.3.6 Vulnerability analysis (conception, design, etc.)

2.3.6.1 List of known vulnerabilities

No known and exploitable vulnerabilities have been identified in the evaluated version of the product.

2.3.6.2 List of vulnerabilities discovered during the evaluation and expert opinion

Potential vulnerabilities were identified, however these proved to be unexploitable for the level of attacker considered.

2.3.7 Developer access

Not applicable.

2.3.8 Ease of use analysis

2.3.8.1 Cases where security is undermined

The risks identified during the evaluation lead to recommendations and restrictions of use for the user (see chapter 3.2).

2.3.8.2 Expert opinion on ease of use

No expert opinion was formulated by CESTI regarding the ease of use of the product.

2.3.8.3 Notes and remarks

None.

2.4 Cryptographic mechanism strength analysis

The product uses cryptographic functions to protect the confidentiality, integrity and authenticity of the data streams. For this purpose it relies on functions of the underlying Windows OS, whose source code is not available, which does not allow a cryptographic analysis in the sense of the CSPN methodology.
For this reason, the product has not been subject to an analysis of cryptographic mechanisms as part of this evaluation.

2.5 Random number generator analysis

The product does not implement a randomiser.

3 Certification

3.1. Conclusion

The evaluation was performed in accordance with current rules and standards, with the competence and impartiality required of an approved evaluation facility.

This certificate attests that the product evaluated “Panorama E^2, version 7.00” meets the security requirements set out in its security target [ST] based on the level of evaluation expected for first level security certification.

3.2. Recommendations and restrictions of use

This certificate relates to the product specified in chapter 1.2 of this certification report. Users of the certified product must comply with the environment security requirements specified in the security target [ST], and, where relevant in relation to the context of use of the product, must observe the following restrictions and recommendations.

In order to guarantee the secure use of the product, it is imperative that the user should observe the following measures:

- the SCADA network, the external client network and the process network must be separate networks;
- the deployment conditions stipulated in the security target [ST] must be respected and users must comply with the [GUIDES] provided;
- the user must consult the security bulletins [BDS] issued by the developer. 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.
- the user should follow the recommendations in [ANNEXE_PTF] when performing the installation, and not simply follow the installation program, as the installation program does not explicitly show how to perform a secure installation.

Annex 1. Documentary references for the product evaluated

[ST]	*PANORAMA Server and Client Short-Term CSPN Security Target* Reference: PANO/CSPN Target Short-term; Version: 3.5 Date: *8 October 2019.*
[RTE]	*CSPN Technical Evaluation Report – PANORAMA* Reference: OPPIDA/CESTI/PANORAMA/RTE; Version: 1.1 Date: 26 September 2019.
[GUIDES]	*Programmer's technical guide, integrated as online help in the product.*
[ANNEXE_PTF]	*PANORAMA Server and Client Short-Term CSPN Security Target* – Platform Annex Reference: PANO_CSPN Panorama Platform; Version: 1.2 Date: *26 June 2019.*
[BDS]	*Security bulletins, published under* https://codra.net/service/bulletin-securite-informatique

4 Annex 2. Certification references

<table>
<tr><td colspan="2">Amended decree No. 2002-535 of 18 April 2002 relating to the evaluation and certification of the security provided by information technology products and systems.</td></tr>
<tr><td>[CSPN]</td><td>First level security certification of information technology products, reference ANSSI-CSPN-CER-P-01/2.0 dated 6 September 2018.
Evaluation criteria for first level security certification, reference ANSSI-CSPN-CER-P-02/3.0 dated 18 March 2019.
Evaluation methodology for first level security certification, reference ANSSI-CSPN-NOTE-01/3 dated 6 September 2018.
Documents available at www.ssi.gouv.fr.</td></tr>
<tr><td>[RGS]</td><td>Cryptographic mechanisms – Rules and recommendations concerning the choice and dimensioning of cryptographic mechanisms, version 2.03 of 21 February 2014, appended to the general security reference base (RGS_B1), see www.ssi.gouv.fr.</td></tr>
</table>