Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

OCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 5/17

(Certification No.)

Prodotto: **VBrain EMS v. 1.0**
(Product)

Sviluppato da: **VITROCISET S.p.A.**
(Developed by)

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL1+

(ASE_SPD.1, ASE_REQ.2, ASE_OBJ.2, ALC_FLR.1)

Il Direttore
(Dott.ssa Rita Forsi)

Roma, 10 ottobre 2017

Common Criteria

SOGIS

This page is intentionally left blank

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Certification Report

VBrain EMS v. 1.0

OCSI/CERT/IMQ/12/2016/RC

Version 1.0

10 October 2017

Courtesy translation

Disclaimer: this translation in English language is provided for informational purposes only; it is not a substitute for the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Release	Authors	Changes/Remarks	Date
1.0	OCSI	First issue	10/10/2017

2 Table of contents

3 Acronyms

AES	Advanced Encryption Standard
BMS	Building Management System
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
COTS	Commercial Off-The-Shelf
DB	DataBase
DBMS	DB Management System
EAL	Evaluation Assurance Level
EMS	Enterprise Management System
HMI	Human Machine Interface
HTTPS	HyperText Transfer Protocol over Secure Socket Layer
HW	Hardware
IT	Information Technology
LGP	Linea Guida Provvisoria (*Provisional Guideline*)
LVS	Laboratorio per la Valutazione della Sicurezza (*Information Technology Security Evaluation Facility*)
NIS	Nota Informativa dello Schema (*Scheme Information Note*)
OCSI	Organismo di Certificazione della Sicurezza Informatica *(Information Security Certification Body*)
OPC	OLE for Process Control
OPC-UA	OPC Unified Architecture
OS	Operating System
PP	Protection Profile
PSIM	Physical Security Information Management
RFV	Rapporto Finale di Valutazione (*Evaluation Technical Report*)

RSA	Rivest-Shamir-Adleman
SAR	Security Assurance Requirement
SCADA	Supervisory Control And Data Acquisition
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SOGIS	Senior Officials Group Information Systems Security
SOGIS-MRA	SOGIS – Mutual Recognition Arrangement
ST	Security Target
SW	Software
TOE	Target of Evaluation
VBrain EMS	VBrain Enterprise Management System

4 References

[CC1] CCMB-2012-09-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 4, September 2012.

[CC2] CCMB-2012-09-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 4, September 2012.

[CC3] CCMB-2012-09-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 4, September 2012.

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014.

[CEM] CCMB-2012-09-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 4, September 2012.

[CONF] VBrain EMS Life-Cycle Support, Doc. n. VC_UGI_I00155_01_REL_0005, ver. 1.0, 28th June 2017, Vitrociset.

[GUI1] “VBrain EMS Guidance Documents”, version 1.1, 1st August 2017, Document ID: VC_UGI_I00155_01_REL_0004.

[GUI2] “VBRAIN EMS CONFIGURATION MANUAL - VBrain Administrators Guide” - version 1.1, 1st August 2017, Document ID: VC_UGI_I00155_01_MAN_0003.

[GUI3] “VBRAIN EMS HOSTS PREPARATION MANUAL - Server and Client Hosts”, version 1.1, 1st August 2017, Document ID: VC_UGI_I00155_01_MAN_0005.

[GUI4] “VBRAIN EMS INSTALLATION/RECOVERY MANUAL”, version 1.11st August 2017, Document ID: VC_UGI_I00155_01_MAN_0004.

[IEC 62451] OPC Unified Architecture (OPC UA) standard series: IEC TR 62541-1:2016, IEC TR 62541-2:2016, IEC 62541-3:2015, IEC 62541-4:2015, IEC 62541-5:2015, IEC 62541-6:2015, IEC 62541-7:2015, IEC 62541-9:2015, IEC 62541-10:2015, IEC 62541-11:2015, IEC 62541-13:2015, IEC 62541-100:2015.

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004.

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004.

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004.

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013.

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013.

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013.

[RFV] "Rapporto Finale di Valutazione – VBRAIN EMS", versione 1.1, 2 agosto 2017, Doc. N.: VCVTR1601Q_02.

[SOGIS] "Mutual Recognition Agreement of Information Technology Security Evaluation Certificates", Version 3, January 2010.

[TDS] "VBrain EMS Security Target V. 1.1", 1st August 2017, Document ID: VC_UGI_I00155_01_REL_0001.

5 Recognition of the Certificate

5.1 European Recognition of CC Certificates (SOGIS-MRA)

The European mutual recognition arrangement (SOGIS-MRA, version 3, [SOGIS]) was signed in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) for the assurance levels up to and including EAL4 for all IT products. The recognition of assurance levels higher than EAL4 is provided exclusively for products belonging to specific technical domains.

The current list of signatory nations and the technical domains for which the recognition of higher levels applies and further details are available in the SOGIS portal at http://www.sogisportal.eu.

The SOGIS-MRA logo is printed on the certificate to indicate that this certificate is recognized by the signatory nations in accordance with the arrangement.

This certificate is recognised under SOGIS-MRA for all indicated assurance components.

5.2 International Recognition of CC Certificates (CCRA)

The current version of the international mutual recognition agreement of the certificates issued according to CC (Common Criteria Recognition Arrangement, [CCRA]) was ratified the 8th September 2014. It applies to CC certificates compliant with the “collaborative” Protection Profiles (cPP), provided for levels up to and including EAL4, or to certificates based on assurance levels up to and including EAL2, with the possible augmentation with Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of the “collaborative” Protection Profiles (cPP) and further details are available in the CCRA portal at http://www.commoncriteriaportal.org.

The CCRA logo is printed on the certificate to indicate that this certificate is recognized by the signatory nations in accordance with the arrangement.

This certificate is recognised under CCRA for all specified assurance components.

6 Statement of Certification

The target of evaluation (TOE) is the software product “VBrain EMS v.1.0”, developed by VITROCISET S.p.A..

The TOE is a basic software component for the creation of SCADA systems that allows the supervision and control of technological systems, as well as management of security systems. Specifically, the TOE provides a framework for the integration of other software components, with the aim of managing different control systems operating in specific technological areas, such as energy, water distribution, buildings monitoring and control.

The evaluation has been conducted according to the requirements established by the Italian Scheme for the evaluation and security certification of systems and products in the information technology sector. The mentioned requirements are described in the Provisional Guidelines [LGP1, LGP2, LGP3] and in the Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body “Organismo di Certificazione della Sicurezza Informatica (OCSI)”, established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [TDS]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC v 3.1 for the assurance level EAL1 augmented with ASE_SPD.1, ASE_REQ.2, ASE_OBJ.2 and ALC_FLR.1, according to the information provided in the Security Target [TDS] and in the configuration in Appendix B – of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report documents the results of the security evaluation of the product "VBrain EMS v.1.0" according to the Common Criteria, and aims at providing information for potential buyers and/or users to assess the compliance of the security functionalities of the TOE with respect to the users' specific requirements.

This Certification Report has to be examined in conjunction with the Security Target [TDS], that specifies the functional requirements of the product, the level of assurance provided and the environment where the product is expected to run.

7.2 Executive summary

TOE Name	VBrain EMS v.1.0
Security Target	Security Target of "VBrain EMS v.1.0", v.1.1, 1st August 2017
Assurance Level	EAL1 augmented with ASE_SPD.1, ASE_REQ.2, ASE_OBJ.2, ALC_FLR.1
Developer	Vitrociset S.p.A.
Sponsor	Vitrociset S.p.A.
LVS	IMQ/LPS
CC Version	3.1 Rev. 4
Compliance to PP	No compliance declared
Evaluation start date	22nd November 2016
Evaluation end date	2nd August 2017

The evaluation results apply exclusively to the product version indicated in this Certification Report and only if all assumptions related to the operational environment are met as described in the Security Target [TDS].

7.3 Evaluated product

This section summarises some of the main functional and security functionalities of the TOE; for a detailed description, refer to the Security Target [TDS].

VBrain EMS is a software product of the VBrain Suite® that allows the creation of monitoring and control systems for small, medium and large infrastructures. VBrain EMS is able to manage heterogeneous data, also interoperating with third-party software. The

VBrain EMS component covers the functionalities of SCADA, PSIM, BMS, Energy management systems, and it represents the framework for the integration of other software components for the management of specific applicative environments.

The scheme in Figure 1 depicts the VBrain Suite architecture where the TOE operates. More specifically, the TOE is able to acquire and elaborate data from sensors, devices, plants and third-party systems that provide an OPC Unified Architecture (OPC-UA) ([IEC 62451]) interface.

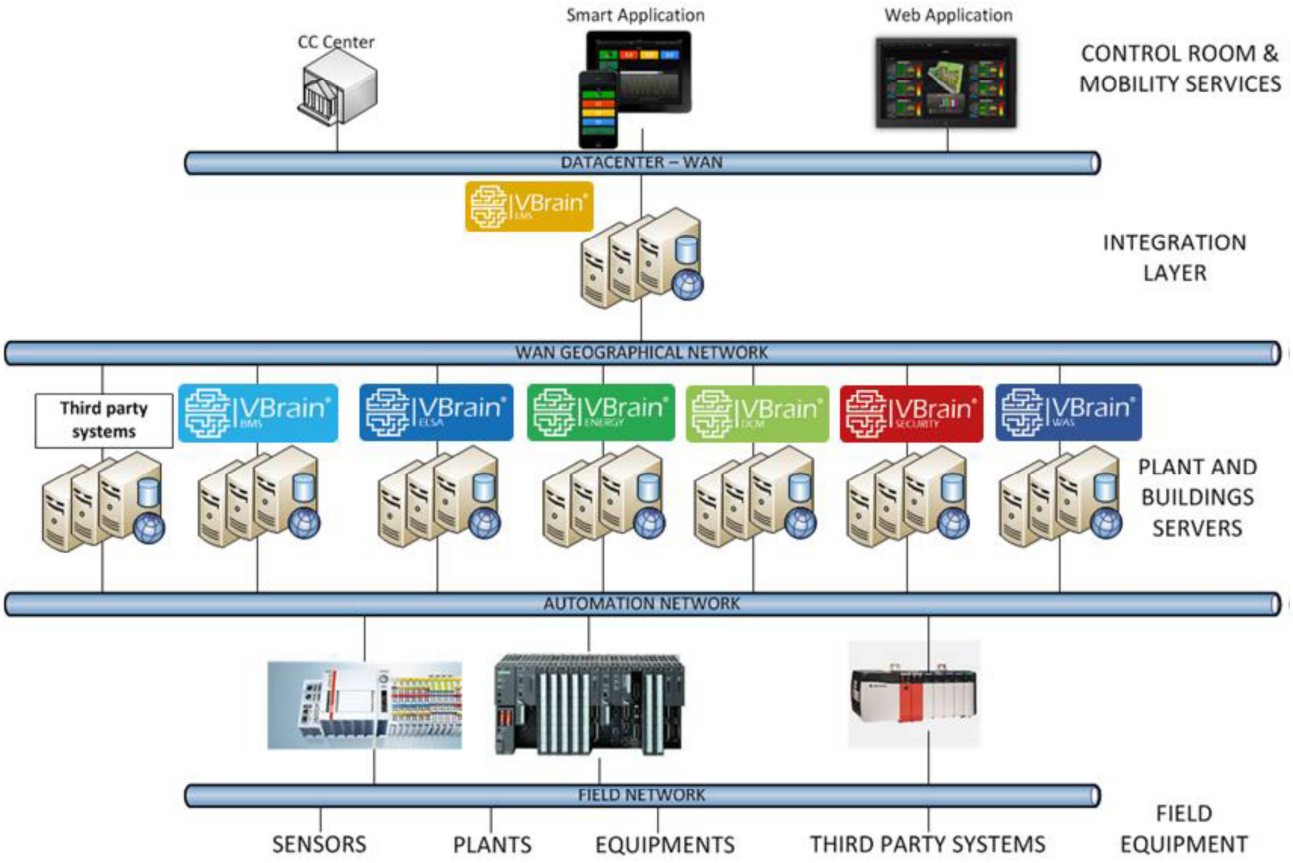

Figure 1 –VBrain Suite architecture

The application environments in which the TOE can operate include residential and public buildings, private offices, hospitals, technological systems for building management, industrial plants for power and energy supply, electrosmog analysis, automatic hydric systems, data centres, systems for physical security, and different kinds of critical infrastructures.

The TOE allows a trained operator of a control centre to manage the system using an interface that is available in three different configurations. More specifically, VBrain EMS v1.0 can be installed in the following three configurations:

1) “Desktop Client HMI” configuration, that employs an ad-hoc application on the client-side, adapted to the specific processes/plants/sites to be monitored and controlled;

2) "Web Client HMI" configuration, that employs a standard web application on the client-side and requires the use of an Internet browser;

3) "Complete" configuration, in which both the Desktop Client HMI and Web Client HMI interfaces are available in the client host.

In the reminder, further details about the TOE architecture are provided.

7.3.1 TOE architecture

7.3.1.1 Hardware

The TOE does not include HW components. The [TDS] provides recommendations about the HW to be employed in the operational environment in both the server and client sides for the three possible configurations, "Desktop Client HMI", "Web Client HMI" and "Complete".

7.3.1.2 Software

The SW modules that make up the TOE identified in [TDS], sec. 1.5.5, for the three possible configurations "Desktop Client HMI", "Web Client HMI" and "Complete" are depicted in Figures 2-4.

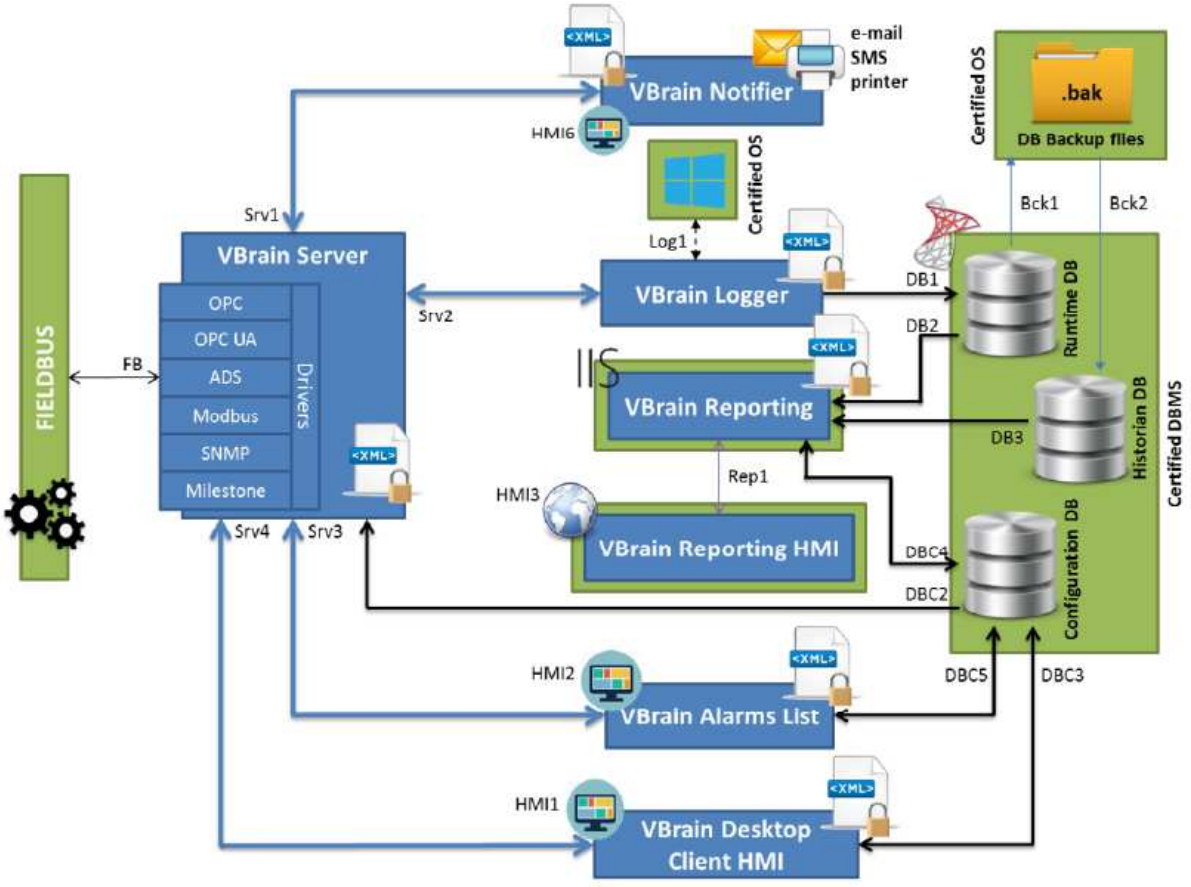

Figure 2 – "Desktop Client HMI" configuration

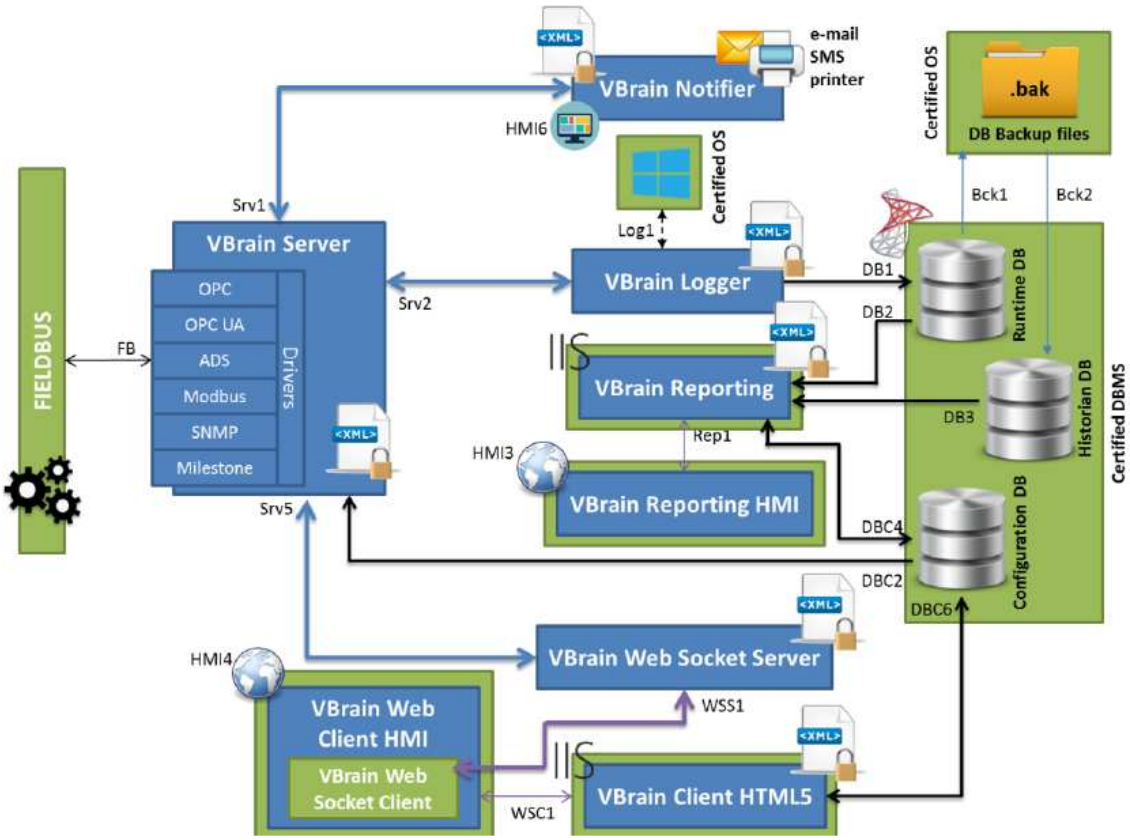

Figure 3 – “Web Client HMI” configuration

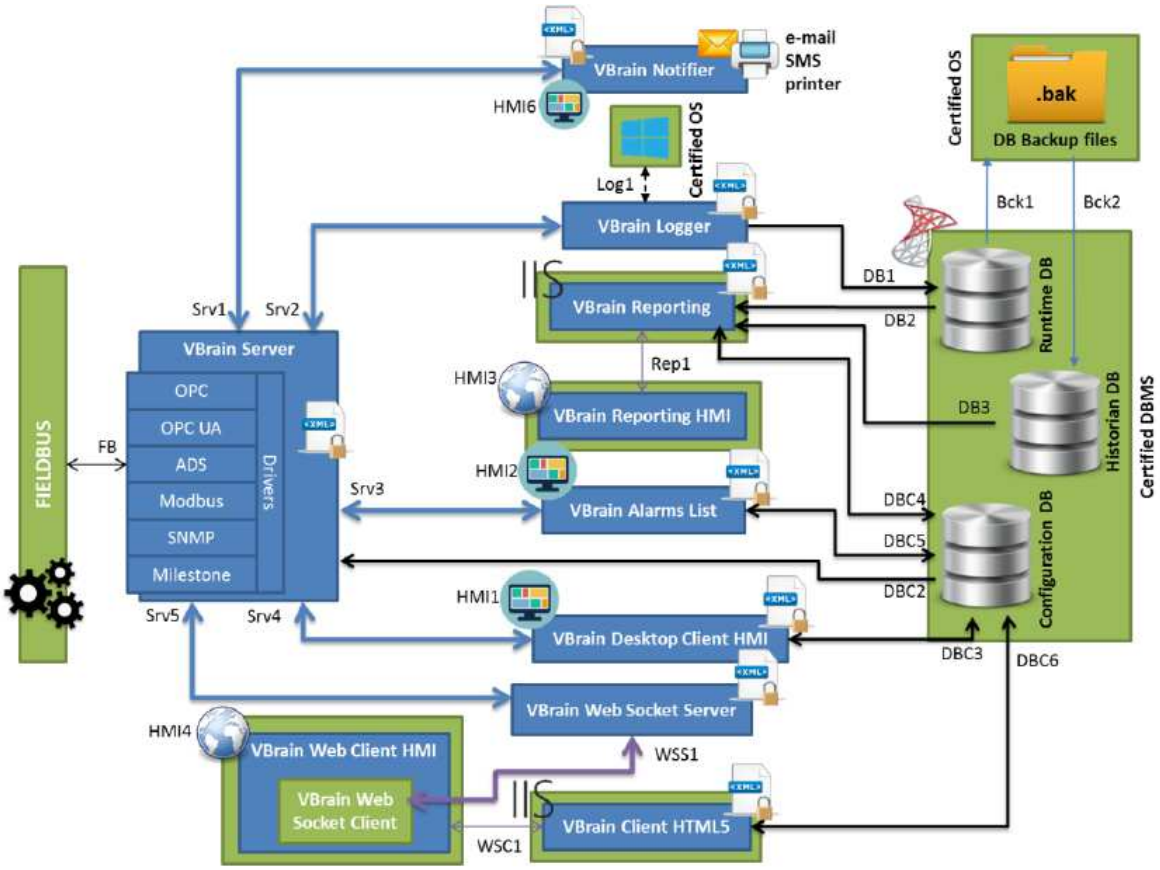

Figure 4 – “Complete” configuration

The software components depicted in Figures 2-4 are described in [TDS] at sec. 1.7.

7.3.1.3 Operational environment components

The TOE's operational environment includes the following certified COTS (for the certification references see [TDS] at sec. 1.5.4), necessary for the TOE operation:

- **DBMS**: Microsoft SQL Server 2012 Database Engine Enterprise Edition x64 (English), Version 11.0.3000.0 (with Service Pack 1), certified CC EAL4+ ALC_FLR.2, to manage the configuration DB, the runtime DB and the historian DB.

- **Operating System**: Windows Server 2012 R2 and Windows 10, Windows 8 and Windows Server 2012, Windows 7 and Windows Server 2008 R2, Windows 8.1.

In addition, some software pre-requirements are necessary on both server and client sides, depending on the HMI configuration of the client. These include the availability of the .NET Framework V 4.6.1 and of the .NET Framework V 3.5, of an Internet browser supporting HTML5, CCS3 and SVG, of the LabVIEW Run-Time Engine 2015 and of digital certificates necessary for the authentication and data exchange processes.

For further details related to the TOE's operational environment refer to [TDS], sec. 1.6, where the operational environment components are described, according to the HMI configuration employed in the TOE.

7.3.1.4 TOE users

One or more VBrain Servers are assigned to each TOE user, together with a role defining the allowed operations on each server, and one or more groups with the associated access permissions for the interfaces.

For the TOE management and use, the following user profiles are defined, with different roles and permissions:

- Administrators: System Administrator and Configuration Administrator.

- Operators: Commander, Acknowledger, Full Reader, Reader.

Specifically, the System Administrator manages the users and all other configuration functionalities of the TOE that are assigned to the Configuration Administrator.

The permissions for each user are detailed in Table 21 of [TDS]. The allowed operations for each user according to the role assigned are detailed in Table 17 of [TDS].

7.3.2 TOE security features

For the detailed description of the Security Functional Requirements (SFRs) refer to [TDS], sec. 6.1. The security objectives for the TOE's operational environment and the security functionalities of the TOE are summarised in the remainder.

7.3.2.1 TOE security objectives

TOE security objectives are here summarised:

- The TOE has to allow only the authorised administrator users to configure the TOE and to modify the TOE configuration (O.CONFIG).
- The TOE has to protect the integrity and confidentiality of data exchanged between different parts of the TOE (O.SECCOM).
- The TOE has to allow only the System Administrator to modify the users' roles and permissions (O.USER), has to identify the users before granting access to data and functions (O.IDENTIFY), has to allow the users to accede to functions and data depending on their role and relative authorisations assigned (O.ACCESS), and to the data acquired from the field through the FieldBus (such as sensor measurements, devices and actuators states, other notification from devices), to alarms, and to execute commands (O.AVAIL) depending on the role and relative assigned authorisations.
- The TOE has to store audit records, correlating them to the TOE users, and has to send events and alarms to the operators through different communication channels (as SMS, emails, printers, etc.) (O.AUDIT), has to ensure an effective management of the system functionalities and the security related data of the TOE, preventing its misuse (O.MANAGE).
- The TOE has to counter brute force or dictionary attacks (O.ANTI_BRUTE) and replay attacks (O.REPLAY), has to prevent users from creating a number of sessions with the VBrain Servers higher than the maximum number that is set for each user (O.SESSION).
- The TOE has to guarantee the availability of security related data, preventing the exhaustion of the DBs' storing capacity, as well as the backups storing capacity (O.EXHAUST), has to recover previous configurations and installations in case of malfunctioning or critical events (O.CRASH).

For a complete description of the TOE's security objectives refer to the Security Target [TDS], sec. 4.1.

7.3.2.2 Operational environment's security objectives

The security objectives for the TOE's operational environment are here summarised:

- manage the roles' sharing between administrators of the TOE, of the OS and of the DBMS; specifically, an OS administrator or DBMS administrator has to be also a TOE authorised administrator (OE.SO, OE.DB);

- guarantee that the physical access to the TOE server-side location is allowed only to the TOE authorised administrators (OE.PHYSICAL_ACCESS);

- select trusted, skilled and trained personnel to be appointed as TOE authorised administrator, so as not to compromise the TOE, OS and DBMS installation and configuration (OE.USER);

- guarantee the meeting of the various requirements during the installation, particularly that the TOE is installed and managed according to an evaluated configuration and based on the preparing procedures (OE.TOE_EVALUATED), that VBrain Server and VBrain Supervisor are installed on the same host (OE.INSTALL);

- provide an interface for the OS administrator identification which is able to activate and deactivate the server-side TOE components, and to configure VBrain Notifier (OE.IDENTIFY);

- guarantee TOE operation continuity in case of power outage (OE.CONTINUITY);

- support TOE operation through specific OS functionalities such as:

    - cryptographic functionalities (based on different algorithms such as RSA 2048, SHA256, AES 128/256) and HTTPS for the secure communication between client and server, and the creation of random first-use passwords for the users (OE.CRYPTO);

    - creation of audit records (OE.AUDIT);

    - access control to configuration files and DB data (OE.RESTRICT);

    - support during the TOE components activation and deactivation (OE.STATE);

    - provide a reliable time reference (OE.TIME).

For a complete description of the security objectives for the TOE operational environment refer to the Security Target [TDS], sec. 4.2.

7.3.2.3 Security functions

The TOE's security functions are the following:

- **SF_1: Configuration Management** – this functionality allows configuration and setting of all system parameters and creation of the users that are authorised to operate on it, including the security policies for the communication channels.

- **SF_2: Centralized Access Control** – this functionality assigns one or more servers to each user on which they can operate and the related permissions, as well as the maximum number of OPC-UA sessions that can be simultaneously created with each server.

- **SF_3: Identification and Authentication** – this functionality requires the user authentication for opening a VBrain Client HMI and before acceding to specific features or data, such as to VBrain Alarms List.

- **SF_4: Session handling** – this functionality manages the sessions activated simultaneously by the same user, that cannot be more that the maximum number which is configured for that user.

- **SF_5: Audit** – through the interaction with the OS, this functionality allows the creation of audit records for a predefined set of events and controls access to the audit records.

- **SF_6: Encryption** – this functionality performs the encryption of the configuration files and of the messages for secure communication, employing the encryption features provided by the OS.

- **SF_7: Security related data availability and service continuity** – this functionality guarantees the availability of security related data and service continuity, verifying that the core processes are active, responding, and did not reach the memory limit. If necessary, new instances of the involved process are automatically restarted. In addition, it manages the automatic backups creation.

For further details about the TOE security functions refer to the Security Target [TDS], sec. 7.1.

7.3.3 TOE configuration

The evaluated TOE is identified in [TDS] as version 1.0. All tests (functional and of vulnerability) have been conducted on this version of the TOE.

The TOE has been evaluated in its “Complete” configuration, as it includes all modules available in the other two configurations “Desktop Client HMI” and “Web Client HMI”. More specifically, Figures 5-7 show the SW components of the TOE which are employed in the chosen configuration.

SERVER-SIDE TOE COMPONENTS	OPERATORS-SIDE TOE COMPONENT
VBrain Server	VBrain Web Client HMI
VBrain Notifier	VBrain Desktop Client HMI
VBrain Logger	VBrain Reporting HMI
VBrain Reporting	VBrain Alarms List
VBrain Web Socket Server	
VBrain Client HTML5	
VBrain Configurator	
VBrain Supervisor	

Figure 5 – SW components in the “Complete” configuration

For further details about the evaluated configuration refer to Appendix B – .

7.4 Documentation

For the proper use of the TOE, aside the necessary expertise and training of the users, the Developer has prepared four guidance documents as reference documentation in addition to [TDS], which are listed in Appendix A – Guidelines for the secure use of the product. These consist of a general guidance document, a configuration manual, a server and client hosts preparation manual and a manual for the installation and recovery in case of failure.

For secure use of the TOE refer to what specified in the Security Target [TDS]. In addition, all additional commitments and recommendations described in sec. 8.2 of this report have to be followed.

7.5 Functional and assurance requirements

All Security Functional Requirements (SFRs) have been selected from CC Part 2 [CC2] and all Assurance Requirements (SARs) from CC Part 3 [CC3].

As this evaluation entails an assurance level EAL1 augmented with ASE_SPD.1, ASE_REQ.2, ASE_OBJ.2, ALC_FLR.1, the security problem is described in detail in the Security Target [TDS]. The Security Target [TDS], to which one may refer for a complete description and the application notes, specifies all security objectives for the TOE, the threats that these objectives have to counter, as well as the SFRs and the security functions that realise these objectives.

7.6 Product evaluation

The evaluation hast been performed according to the requirements of the Italian Scheme for the security evaluation and certification of IT systems and products, as described in the Provisional Guideline [LGP3] and in the Scheme Information Note [NIS3], and has been performed also according to the requirements of the Common Criteria Recognition Arrangement (CCRA).

The goal of the evaluation is to guarantee that the TOE satisfies what stated in the related Security Target [TDS]. Its review is highly recommended for the potential buyers and/or users. Initially, the Security Target was evaluated so as to guarantee that it represents a solid basis to test the requirements set by the CC standard. Successively, the TOE was tested according to what declared in the related Security Target [TDS]. Both parts of the test were conducted according to CC Part 3 [CC3] and CEM [CEM].

The Certification Body supervised the execution of the evaluation performed by the Evaluation Facility (LVS) IMQ/LPS.

The evaluation activities ended on the 2nd August 2017 with the release, by the LVS, of the Evaluation Technical Report [RFV] that was approved by the Certification Body on the 1st of September 2017. Finally, the Certification Body released this Certification Report.

7.7 General considerations about the certification validity

The evaluation targeted the security functionalities declared in the Security Target [TDS], in the operational environment described in the document. The evaluation has been conducted on the TOE configured as described in Appendix B – . It is suggested that the potential buyers and/or users verify that such a configuration meets their specific requirements and take into account the recommendations mentioned in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; it remains a probability (the lower, the higher the assurance level) that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to check regularly the arising of any new vulnerability after the issuance of this Certification Report and, if the vulnerability can be exploited in the operational environment of the TOE, check with the developer if security updates have been developed and if such updates have been evaluated and certified.

8 Evaluation outcome

8.1 Results of the evaluation

Following the analysis of the Evaluation Technical Report [RFV] released by the LVS and of the documents required for the certification, and considering the evaluation activities conducted, OCSI concluded that the TOE "VBrain EMS v.1.0" satisfies the requirements in Common Criteria Part 3 [CC3] which are expected for the assurance level EAL1 augmented with ASE_SPD.1, ASE_REQ.2, ASE_OBJ.2, ALC_FLR.1, related to the security functions described in the Security Target [TDS] and in the evaluated configuration described in Appendix B – . Table 1 summarises the final verdicts for each activity conducted by the LVS according to the assurance requirements provided in [CC3], for the reached assurance level.

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Positive
Conformance claims	ASE_CCL.1	Positive
Extended components definition	ASE_ECD.1	Positive
ST introduction	ASE_INT.1	Positive
Security objectives	ASE_OBJ.2	Positive
Derived security requirements	ASE_REQ.2	Positive
Security Problem Definition	ASE_SPD.1	Positive
TOE summary specification	ASE_TSS.1	Positive
Development	**Class ADV**	Positive
Basic functional specification	ADV_FSP.1	Positive
Guidance documents	**Class AGD**	Positive
Operational user guidance	AGD_OPE.1	Positive
Preparative procedures	AGD_PRE.1	Positive
Life cycle support	**Class ALC**	Positive
Labelling of the TOE	ALC_CMC.1	Positive
TOE CM coverage	ALC_CMS.1	Positive
Basic Flow Remediation	ALC_FLR.1	Positive
Tests	**Class ATE**	Positive
Independent testing - conformance	ATE_IND.1	Positive
Vulnerability assessment	**Class AVA**	Positive
Vulnerability survey	AVA_VAN.1	Positive

Table 1 – Final verdicts for the assurance requirements

8.2 Recommendations

The conclusions of the Certification Body are summarised in section Statement of Certification.

The potential buyers and/or users of the product “VBrain EMS v. 1.0” are encouraged to accurately understand the specific aim of the certification by reading this Report referred to the Security Target [TDS].

The TOE has to be employed according to the operational environment specified in sec. 1.6 of the Security Target [TDS]. It is suggested that the potential buyers and/or users verify that the requirements are met and take into account the recommendations made in this Report.

This Certification Report is valid only for the TOE in the evaluated configuration as described in Appendix B – .

9 Appendix A – Guidelines for the secure use of the product

The guidance documents relevant for the evaluation or referred inside the released document and available to the potential users of the TOE are the following:

- "VBrain EMS Security Target V. 1.1", 1st August 2017, Document ID: VC_UGI_I00155_01_REL_0001, [TDS];
- "VBrain EMS Guidance Documents", version 1.1, 1st August 2017, Document ID: VC_UGI_I00155_01_REL_0004, [GUI1];
- "VBRAIN EMS CONFIGURATION MANUAL - VBrain Administrators Guide" - version 1.1, 1st August 2017, Document ID: VC_UGI_I00155_01_MAN_0003, [GUI2];
- "VBRAIN EMS HOSTS PREPARATION MANUAL - Server and Client Hosts", version 1.1, 1st August 2017, Document ID: VC_UGI_I00155_01_MAN_0005, [GUI3];
- "VBRAIN EMS INSTALLATION/RECOVERY MANUAL", version 1.1, 1st August 2017, Document ID: VC_UGI_I00155_01_MAN_0004, [GUI4].

10 Appendix B – Evaluated configuration

The TOE has been evaluated in the “Complete” configuration briefly described in sec. 7.3.3 and detailed in [TDS] in sec. 1.5.5.

The TOE is identified in the Security Target [TDS] with version 1.0. The name and the version identify univocally the TOE and its set of components, making up the evaluated configuration of the TOE, verified by the Evaluators at the moment when the tests were conducted and to which the results of the evaluation itself apply.

Table 2 lists the components employed in the evaluated configuration:

Type	List of components
HW	No HW component is included in the TOE
SW	VBrain Server v1.0, VBrain Supervisor v1.0 VBrain Configurator v1.0 VBrain Logger v1.0 VBrain Notifier v1.0 VBrain Reporting v1.0 VBrain Reporting HMI v1.0 VBrain Desktop Client HMI v1.0 VBrain Web Socket Server v1.0 VBrain Alarms List v1.0 VBrain Web Client HMI v1.0 VBrain Client HTML5 v1.0
COTS	No COTS is included in the TOE

Table 2 – Evaluated TOE components

The HW and SW elements present in the evaluated TOE operational environment are identified in Tables 5-7 in sec. 1.6 of [TDS].

The components of the evaluated configurations are further detailed in the configuration list, provided by the Developer to the Evaluators in the document [CONF].

11 Appendix C – Test Activities

This appendix describes the Evaluators' and Developer's efforts during the test activities. For the assurance level EAL1 augmented with ASE_SPD.1, ASE_REQ.2, ASE_OBJ.2, ALC_FLR.1 such activities do not foresee the execution of functional tests by the Developer, but only of independent functional tests carried out by the Evaluators.

11.1 Test Configuration

The security functional tests, the vulnerability assessment activities and the penetration tests were conducted in the headquarters of Vitrociset S.p.A. and remotely through an Internet connection from the IMQ/LPS headquarters.

In conjunction with the execution of the tests, the preparing procedures were also verified, as well as the launching of the TOE, in accordance to the requirements of the assurance families AGD_PRE and AGD_OPE.

To verify the setting up, the Evaluators considered what described in the Security Target [TDS] and in the guides provided by the Developer [GUI1], [GUI2], [GUI3] and [GUI4], according to the configuration described in Appendix C of [RFV] based on the document [CONF] delivered by the Developer to the Evaluators and containing the configuration list.

During the test plan preparation phase, the Developers examined the TOE description in [TDS] and verified that the test configuration proposed by the Developer was coherent with what specified in the ST and in the functional specifications.

Moreover, before carrying out the single test sessions, the Evaluators verified that the TOE, together with the different components of its operational environment, was installed and configured as declared by the Developer and described in Appendix B – Evaluated configuration, guaranteeing the test repeatability and reproducibility.

11.2 Independent functional tests performed by the Evaluators

During the design of the independent TOE testing programme, the Evaluators took into account the Security Target [TDS] and the functional specifications.

The Evaluators examined the security functionalities of the TOE, as represented in the [TDS] and, based on their experience, programmed a set of tests to verify the suitability of the security functions of the TOE with respect to what established by CEM.

The functionality tests planned and conducted by the LVS aimed at verifying the following main features:

1. CONFIGURATION – the main security functionalities offered by VBrain Configuration are satisfied, especially the correct implementation of SF_1 for the configuration management;

2. OPC-UA COMMUNICATION – the use of OPC-UA for the communication between VBrain Server and the other TOE components to protect the integrity and confidentiality of the data exchanged;

3. EVENT LOG – the correct event log in the configuration DB and in log files, as well as the creation and correct encryption of the configuration files;

4. USER MANAGEMENT – unlike the Configuration Administrator, the System Administrator can manage the TOE users; a TOE user has to re-authenticate before acceding to VBrain Alarms List; after acceding for the first time to the TOE, the user has to change the password and set it according to the minimum security criteria; a TOE user cannot establish a number of contemporary OPC-UA sessions higher than the imposed limit; the correct implementation of SF_3 for the users authentication and identification;

5. OTHER MANAGEMENT FUNCTIONS – the management functions defined in [TDS] have to be implemented correctly and the alarms management functionality has to be enabled.

The functionality tests conducted by the Evaluators made it possible to verify that the TOE implements the security functions declared, extending the assessment to the overall system, including all components including both the TOE and the operational environment.

The test results proved the complete compliance with what expected according to the [TDS] and to the functional specifications.

Thereby, the TOE passed the independent testing phase with a positive verdict.

11.3 Vulnerability assessment and penetration tests

The vulnerability assessment was conducted on the same *test bed* employed for the functional tests. Its configuration resulted to be compliant with what declared in [TDS], the TOE was appropriately installed and it was in a known state, as previously observed in the activity AGD_PRE.1.

For the planning of the vulnerability assessment activities, considering the assurance level required for the evaluation and the type of TOE, the evaluation team took into account the potential vulnerabilities known for the servers and clients present in the operational environment, in addition to the communication protocols employed for the data exchange, that may be exploited to bypass or interfere with the security functionalities of the TOE.

Specifically, an IMQ's personal computer, equipped with a Kali-Linux release (oriented to penetration testing with an updated database of known vulnerabilities), was employed to conduct the test activities.

The vulnerability research focused on the VBrain Web Client HMI component, as it represents the TOE's component that may be potentially exposed on the Internet, using the *owasp-zap* and *Sqlmap* tools, and on the VBrain Server, for which *OpenVas* was employed, with the known vulnerabilities database updated to the 16th May 2017 (the evaluation activities for the ATE and AVA classes were carried out from 26/04/2017 to 21/06/2017). The preliminary tests conducted with such tools highlighted the presence of

potential vulnerabilities. More specifically, in the VBrain Server and in the VBrain Web Client HMI.

Thereby, the Evaluators examined the identified vulnerabilities and determined a set of penetration tests as appropriate for the evaluation level EAL1+. Specifically, it was assumed that the TOE had to resist to a hypothetical attacker with a Basic attack potential, according to what established by CEM (cfr. [CEM], Appendix B.4).

The penetration tests conducted by the Evaluators have observed the actual presence of vulnerabilities in the TOE operational environment, exploitable with a low attack potential. Specifically, the Evaluators verified that:

1. due to a vulnerability in the operating system Windows Server 2012 R2 installed on the server host and part of the operational environment, it was possible to provoke a reboot of the Server machine, with the resulting restart of VBrain Server and of all server-side components installed; the vulnerability required the installation of a proper patch on the operating system;

2. by sending groups of 500 packets of increasing length using the *owasp-zap* suite it was possible to totally disable the web application WebSocket Server, exposed on the Web Client HMI interface; the vulnerability required the Developer to modify how the OPC-UA sessions were created by the Web Client HMI.

Following the TOE and operational environment update with the aforementioned patches, the vulnerability tests were positively concluded.

For what concerns the vulnerability 2., it is worth highlighting that the TOE evaluation activity was conducted during the development activities. Thereby, the related modifications to the Web Client HMI are included in the version v1.0.