



# VBRAIN EMS Security Target V. 1.1

1<sup>st</sup> August 2017

**DOCUMENT STATUS**

1. DOCUMENT TITLE:			
<b>VBRAIN EMS SECURITY TARGET</b>			
2. DOCUMENT CLASSIFICATION ID:			
<b>VC_UGI_I00155_01_REL_0001</b>			
3. EDIT.	4. UPDATE	5. DATE	6. REASON FOR UPDATING
<b>1</b>	<b>1</b>	<b>01/08/2017</b>	<b>Final issue</b>

7. PAGE UPDATING			
FROM PAGE	FROM PAGE	FROM PAGE	FROM PAGE

8. TOTAL NUMBER OF PAGES: 77
------------------------------

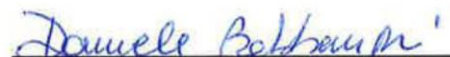
**AUTHORS:**

Etchevés Miciolino Estefanía

Morabito Luigi


**APPROVAL:**

Babbanini Daniele



## TABLE OF CONTENTS

<b>DOCUMENT STATUS.....</b>	<b>2</b>
<b>REFERENCES.....</b>	<b>6</b>
<b>DOCUMENT TERMINOLOGY .....</b>	<b>7</b>
<b>1 ST INTRODUCTION .....</b>	<b>9</b>
1.1. ST REFERENCE.....	9
1.2. TOE REFERENCE.....	9
1.3. DOCUMENT ORGANIZATION.....	9
1.4. DOCUMENT CONVENTIONS .....	10
1.5. TOE OVERVIEW.....	11
1.5.1. USAGE OF THE TOE .....	12
1.5.2. OPERATIVE MODES OF THE TOE .....	13
1.5.3. MAJOR SECURITY FEATURES OF THE TOE.....	15
1.5.4. TOE TYPE .....	19
1.5.5. TOE CONFIGURATION .....	20
1.6. REQUIRED NON-TOE COMPONENTS .....	22
1.7. TOE DESCRIPTION.....	24
1.7.1. TOE Architecture.....	28
1.7.2. TOE USERS PROFILES.....	30
1.7.3. PHYSICAL SCOPE OF THE TOE .....	30
1.7.4. LOGICAL SCOPE OF THE TOE .....	30
1.7.5. TOE GUIDANCE DOCUMENTATION.....	30
1.7.6. USER DATA AND TSF DATA (SECURITY RELATED DATA) HANDLED BY THE TOE .....	30
<b>2 CONFORMANCE CLAIM .....</b>	<b>32</b>
2.1. CC CONFORMANCE CLAIM .....	32
2.2. PP CONFORMANCE CLAIM .....	32
<b>3 SECURITY PROBLEM DEFINITION.....</b>	<b>32</b>
3.1. THREATS .....	32
3.2. ORGANISATIONAL SECURITY POLICIES.....	33
3.3. ASSUMPTIONS.....	34
<b>4 SECURITY OBJECTIVE .....</b>	<b>35</b>
4.1. SECURITY OBJECTIVES FOR THE TOE .....	35
4.2. SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT.....	36
4.3. SECURITY OBJECTIVES RATIONALE .....	38
<b>5 EXTENDED COMPONENTS DEFINITION .....</b>	<b>44</b>
<b>6 SECURITY REQUIREMENTS.....</b>	<b>44</b>
6.1. SECURITY FUNCTIONAL REQUIREMENTS .....	44
6.1.1. SECURITY AUDIT (FAU).....	45
6.1.2. IDENTIFICATION AND AUTHENTICATION (FIA) .....	47
6.1.3. TOE ACCESS (FTA) .....	49
6.1.4. USER DATA PROTECTION (FDP).....	50

---

6.1.5.	PROTECTION OF THE TSF (FPT) .....	58
6.1.6.	SECURITY MANAGEMENT (FMT).....	59
6.2.	SECURITY ASSURANCE REQUIREMENTS .....	62
6.3.	SECURITY FUNCTIONAL REQUIREMENTS RATIONALE.....	63
6.3.1.	CC Component Dependencies .....	63
6.3.2.	Tracing between SFRs and the security objectives for the TOE.....	64
<b>7</b>	<b>TOE SUMMARY SPECIFICATION .....</b>	<b>67</b>
7.1.	SECURITY FUNCTION .....	67
7.1.1.	SF_1: Configuration Management .....	67
7.1.2.	SF_2: Centralized Access Control .....	68
7.1.3.	SF_3: Identification and Authentication .....	68
7.1.4.	SF_4: Session handling.....	70
7.1.5.	SF_5: Audit.....	71
7.1.6.	SF_6: Encryption .....	73
7.1.7.	SF_7: User data availability and service continuity.....	73
7.2.	TOE SUMMARY SPECIFICATION RATIONALE .....	75

## LIST OF TABLES

Table 1: Terms and Acronyms used in the Security Target .....	8
Table 2: ST Reference .....	9
Table 3: ST Organization and Section Descriptions .....	9
Table 4: SW/HW prerequisites of Server components .....	22
Table 5: SW/HW prerequisites of Client components in TOE - Web Client HMI configuration .....	22
Table 6: SW/HW prerequisites of Client components in TOE - Desktop Client HMI configuration .....	23
Table 7: SW/HW prerequisites of Client components in TOE - Complete configuration .....	23
Table 8: Threats .....	33
Table 9: Organizational Security Policies.....	34
Table 10: Assumptions.....	34
Table 11: Security Objectives for the TOE .....	35
Table 12: Security objectives for the Operational Environment .....	37
Table 13: Tracing between security objectives for the TOE and security objectives for the Operational Environment vs. Threat, OSP and Assumption. ....	39
Table 14: Rationale for Mapping of Threats, Policies, and Assumptions to Objectives.....	43
Table 15: List of SFR and related operations .....	45
Table 16: List of Auditable events managed by the TOE.....	45
Table 17: VBrain EMS Access control policy .....	51
Table 18: OPC-UA information flow control policy.....	52
Table 19: USER DATA Information Flow Control Policy Specification .....	56
Table 20: VBrain EMS Management functions .....	60
Table 21: Permissions granted to each user role.....	60
Table 21: Security Assurance Requirements .....	62
Table 22: TOE SFR dependency rationale .....	63
Table 23: Mapping of TOE SFRs to Security Objectives .....	64
Table 24: Rationale for TOE Security Objectives coverage by SFRs.....	66
Table 25: TOE components accessible to TOE user roles .....	68
Table 27: TOE Security Functions/SFRs mapping.....	75
Table 28: SFR to TSF rationale.....	77

## LIST OF FIGURES

Figure 1: VBrain Suite architecture .....	11
Figure 2: Organization of VBrain Suite products .....	12
Figure 3: VBrain EMS operational contexts.....	13
Figure 4: VBrain EMS operative modes .....	14
Figure 5: Client/Server architecture .....	19
Figure 6: Multi-nodal architecture .....	20
Figure 7: VBrain Notifier schema .....	24
Figure 8: Treeview example .....	27
Figure 9: TOE software Architecture legend.....	28
Figure 10: TOE software Architecture in “Desktop Client HMI” configuration.....	28
Figure 11: TOE software Architecture in “Web Client HMI” configuration .....	29
Figure 12: TOE software Architecture in “Complete” configuration .....	29
Figure 13: Example of stored data visualization .....	72
Figure 14: VBrain Alarms List example .....	72

**REFERENCES**

- [CCP1] CCMB-2012-09-001 – Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, ver. 3.1 Revision 4, September 2012.
- [CCP2] CCMB-2012-09-002 – Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, ver. 3.1 Revision 4, September 2012.
- [CCP3] CCMB-2012-09-003 – Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, ver. 3.1 Revision 4, September 2012.
- [CEM] CCMB-2012-09-004 – Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, ver. 3.1 Revision 4, September 2012.

**DOCUMENT TERMINOLOGY**

TERM	DEFINITION
ADO.NET	ActiveX Data Objects for .NET
BMS	Building Management System
CC	Common Criteria (ISO/IEC 15408) Version 3.1 Rev. 4
DCM	Data Center Management
EAL	Evaluation Assurance Level
ELSA	ElectroSmog Analysis
EMS	Enterprise Management System
EVENT/ALARM/WARNING	An event is defined as a measure state change. Alarms and warning are set when a measure exceed a predefined threshold
FIELDBUS	Terms used to indicate the devices that are used in field from which the TOE acquires signals
FIFO	First In – First Out
HMI	Human-Machine Interface: a graphical interface that allows a person to interact with a control system. It may contain trends, alarm summaries, pictures, or animation.
IIS	Internet Information Services
ISP	Internet Service Provider
IT	Information Technology
JSON/XML	Javascript Object Notation: it is another text notation that has all of the advantages of XML, but is much better suited to data-interchange
NODE	monitored device/site in the FIELDBUS
OPC	OLE (Object Linking and Embedding) for Process Control
OE	OPERATIONAL ENVIRONMENT - environment in which the TOE is operated
OS	Operating System
OSP	Organizational Security Policy
PLC	Programmable Logic Controller: a small industrial computer that controls one or more hardware devices.
REST	REpresentational StateTransfer
SCADA	Supervisory Control and Data Acquisition
SECURITY RELATED DATA	USER DATA AND TSF DATA as defined in § 1.7.6
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOA	Service-Oriented Architecture
SOAP	Simple Object Access Protocol
SOC	Security Operation Center
ST	Security Target

TERM	DEFINITION
<b>TOE</b>	Target of Evaluation
<b>TOE AUTHORIZED ADMINISTRATORS</b>	Both System Administrator and Configuration Administrator user roles as defined in Table 17 of § 6.1.4.
<b>TSC</b>	TOE Scope of Control
<b>TSF</b>	TOE Security Functions
<b>TSFI</b>	TOE Security Functionality Interfaces
<b>VBRAIN “CLIENT- TYPE” COMPONENT</b>	<p>The following TOE components installed at Server-side: VBrain Server (that is an OPC-UA Client-type application with reference to FieldBus from which it acquires data), VBrain Web Socket Server, VBrain Logger, VBrain Notifier (that are OPC-UA Client-type applications with reference to VBrain Server).</p> <p>The following TOE components installed at TOE Operator-side: VBrain Desktop Client HMI, VBrain Alarms List (that are OPC-UA Client-type applications with reference to VBrain Server), and the following TOE components that aren’t OPC-UA Clients: VBrain Web Client HMI, VBrain Reporting HMI.</p>
<b>VBRAIN “SERVER-TYPE” COMPONENT</b>	The following TOE component installed at Server-side: VBrain Server (that is an OPC-UA Server application with reference to all other OPC-UA TOE Components, except for the “standalone” ones) and the following TOE components that aren’t OPC-UA Servers: VBrain Web Socket Server, VBrain Notifier, VBrain Reporting, VBrain Client HTML5.
<b>VBRAIN “STANDALONE” COMPONENTS</b>	The following TOE components installed at Server-side: VBrain Configurator and VBrain Supervisor (that don’t directly interface with any other TOE component).
<b>VBrain EMS</b>	VBrain Enterprise Management System, the TOE
<b>WSC</b>	Web Socket Client
<b>WSS</b>	Web Services Security
<b>XML</b>	<p>Extensible Markup Language. It is a text format that provides two enormous advantages as a data representation language:</p> <ul style="list-style-type: none"> <li>It is text-based.</li> <li>It is position-independent.</li> </ul>
<b>TOE CORE APPLICATIONS</b>	The default TOE core applications monitored by VBrain Supervisor are: VBrain Server, VBrain Logger and VBrain Web Socket Server

**Table 1: Terms and Acronyms used in the Security Target**



## 1 ST INTRODUCTION

### 1.1. ST REFERENCE

[1]

<b>Title:</b>	<i>VBrain EMS Security Target</i>
<b>Version:</b>	<i>1.1</i>
<b>Date:</b>	<i>1<sup>st</sup> August 2017</i>
<b>Assurance Level:</b>	<i>EAL 1 augmented with ASE_SPD.1, ASE_REQ.2, ASE_OBJ.2, ALC_FLR.1</i>
<b>CC Version:</b>	<i>Common Criteria v.3.1 Revision 4</i>
<b>Author:</b>	<i>VITROCISSET S.p.A</i>

**Table 2: ST Reference**

### 1.2. TOE REFERENCE

[2] The TOE unique reference is VBrain EMS version 1.0

### 1.3. DOCUMENT ORGANIZATION

[3] This Security Target follows the following format:

Section	Title	Description
1	<b>Introduction</b>	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE.
2	<b>Conformance Claims</b>	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable.
3	<b>Security Problem Definition</b>	Specifies the threats, assumptions and organizational security policies that affect the TOE.
4	<b>Security Objectives</b>	Defines the security objectives for the TOE/Operational Environment and provides a rationale to demonstrate that the security objectives counter the threats.
5	<b>Extended Components Definition</b>	Describes extended components of the evaluation (if any).
6	<b>Security Requirements</b>	Contains the functional and assurance requirements for this TOE.
7	<b>TOE Summary Specification</b>	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

**Table 3: ST Organization and Section Descriptions**

#### 1.4. DOCUMENT CONVENTIONS

[4] The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 rev. 4 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in Part 2 of the Common Criteria are refinement, selection, assignment and iteration.

- The *assignment* operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in *italics blue text*, i.e. *assignment\_value(s)*.
- The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold blue text**. Any text removed is indicated with a **bold blue strikethrough** format (Example: ~~TSE~~).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by underlined blue text.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FIA\_XXX.1.1 (1) and FIA\_XXX.1.1 (2) refer to separate instances of the FIA\_XXX.1 security functional requirement component.

### 1.5. TOE OVERVIEW

- [5] Vitrociset is a system integrator with many years of experience in the field of remote control systems. Over the years, Vitrociset has developed many products and a large body of knowledge that allows it today to tackle even the most difficult challenges.
- [6] Vitrociset remote control systems are able to integrate a lot of different brands, technologies and third party systems, because the goal is to provide customers with turnkey products.
- [7] VBrain EMS has been designed and developed internally by Vitrociset, created with the intention of providing secure and integrated solutions for the realization of complex systems composed by its own products and third party products. VBrain EMS is able to perform specific functionalities, integration services and Security Operation Center (SOC) processes.
- [8] The TOE - VBrain Enterprise Management System - **VBrain EMS<sup>®</sup>** - is the application layer on which its six verticalizations, i.e. the others products of the VBrain Suite<sup>®</sup>, are originated.
- [9] VBrain EMS represents a scalable and configurable platform which allows to realize remote command and control system of small, medium and large technological plants, as well as integrated security systems, implementing internationally recognized standards both for signal acquisition and for interoperability with similar third party systems.
- [10] Here it is sketched a typical VBrain Suite architecture, that may include one or more TOEs. As better explained in § 1.5.4, VBrain EMS's architecture allows to create different hierarchical levels of nodes.

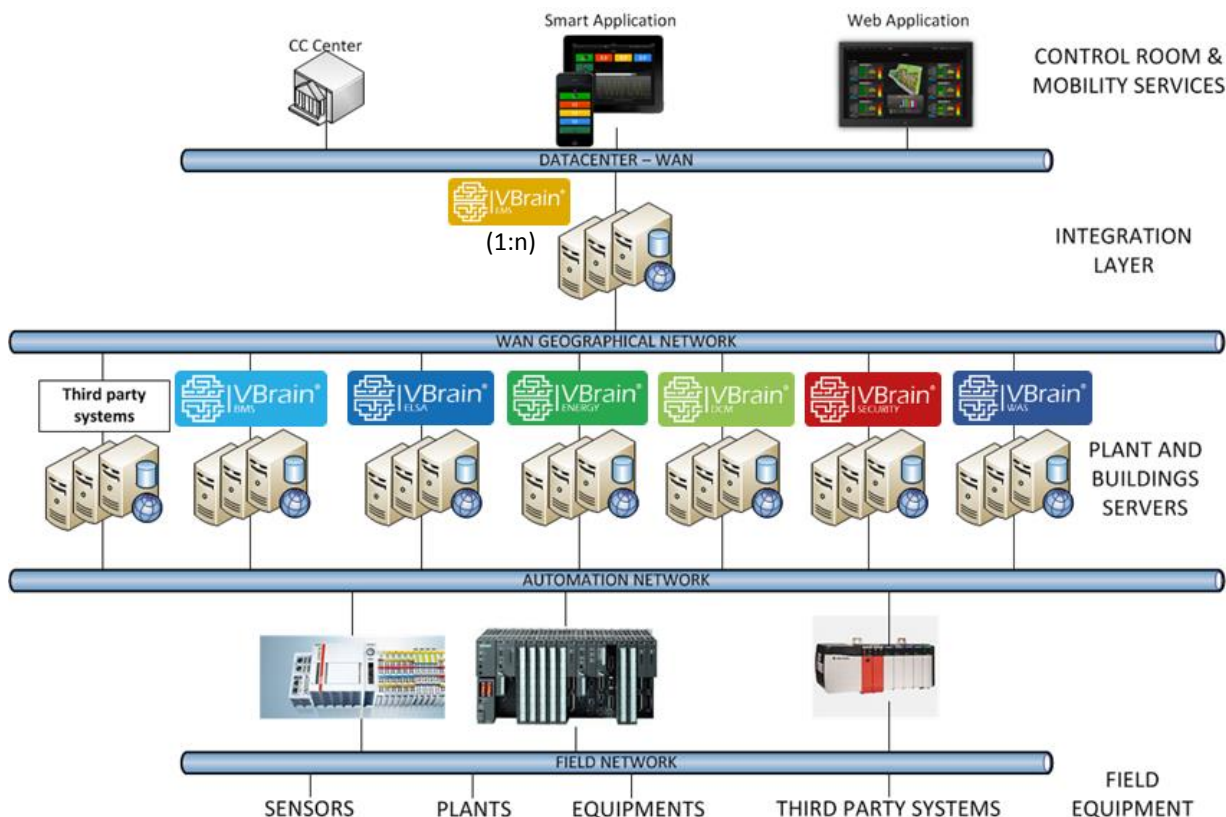


Figure 1: VBrain Suite architecture

- [11] VBrain EMS is a SCADA technology, completely compliant with the latest software technology developments and, thanks to *OPC Unified Architecture* interoperability, it is an evolved instrument

that allows interfacing with a multiplicity of field objects and ease of communication with other systems of the same type.

- [12] Due to its features, the TOE is able to collect process data and standardize heterogeneous data from sensors, devices, systems and third-party systems, so as to visualize them on understandable and intuitive interfaces with different detail levels. Thanks to its high flexibility degree, VBrain EMS is employable in several and different application contexts.
- [13] The product guarantees reliability and high efficiency for main functions:
- field equipment control with graphical representation of components;
  - data acquisition from any equipment;
  - detailed graphical visualization of interfaces and analysis tools;
  - alarms and fault signals management;
  - immediate commands transmission by supervisor;
  - integration between process and electrical distribution system;
  - record/optimization of consumption and failure analysis.

### 1.5.1. USAGE OF THE TOE

- [14] The VBrain Suite is a family of Vitrociset products, which main scope is to provide integrated solutions for the realization of complex remote control systems for distributed systems and equipment. VBrain EMS, one of the VBrain Suite components, is the here addressed TOE.
- [15] All the products constituting the VBrain Suite are based on VBrain EMS, and allow to perform remote control of decentralized or geographically distributed technological systems in order to cover several needs.
- [16] Application opportunities are the most various: individual housing, public housing and private office buildings, hospitals, technological systems. Everything to control in real-time operation, ensuring constantly to the user, the service, timeliness and efficiency in maintenance, in order to reduce, or in some cases prevent, anomalies or interruptions of business continuity.
- [17] VBrain EMS can integrate third party systems as well as the other Vitrociset VBrain Suite products, that represent a typical usage of the TOE. Specifically, every VBrain Suite product is based on VBrain EMS, that implements all the security aspects and represents the cross-domain product.
- [18] Aside to VBrain EMS, the VBrain Suite contains 6 vertical products that allow to implement specific functionalities, which are depicted in the following picture.
- [19] **The TOE, VBrain EMS, is an independent product that represents the “cross-domain” from which all VBrain Suite products are originated.**

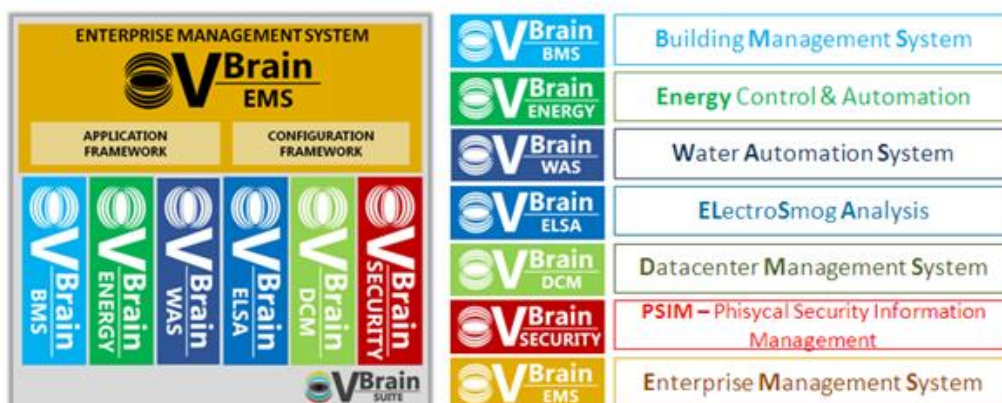


Figure 2: Organization of VBrain Suite products

- [20] **VBrain BMS** is aimed to the realization of systems for the integrated management of all the technological systems of a building, as systems for access control, video surveillance, fire detection, lighting control, smart elevators, air conditioning.
- [21] **VBrain ENERGY** is aimed to the realization of monitoring systems for electrical installations, optimization of energy savings by identifying waste, consumption analysis, historicizing, consumption statistics in real time and automated procedures. **VBrain WAS (Water Automation system)** is aimed to the realization of systems for water management.
- [22] **VBrain SECURITY** is a PSIM (Physical Security Information Management System) aimed to the realization of systems for the integrated management of only safety equipment, such as access control, fire protection, intrusion detection and video surveillance.
- [23] **VBrain DCM** is aimed to the creation of systems for the integrated management of all facilities and technological equipment in a data center, which includes systems for access control, fire detection, lighting control, climate control and networking equipment.
- [24] **VBrain ELSA** is aimed to the realization of systems for the monitoring and analysis of electromagnetic emissions.
- [25] Each product of VBrain Suite originated from VBrain EMS is applicable in a specific technological context and application scope, summarized in the following picture:



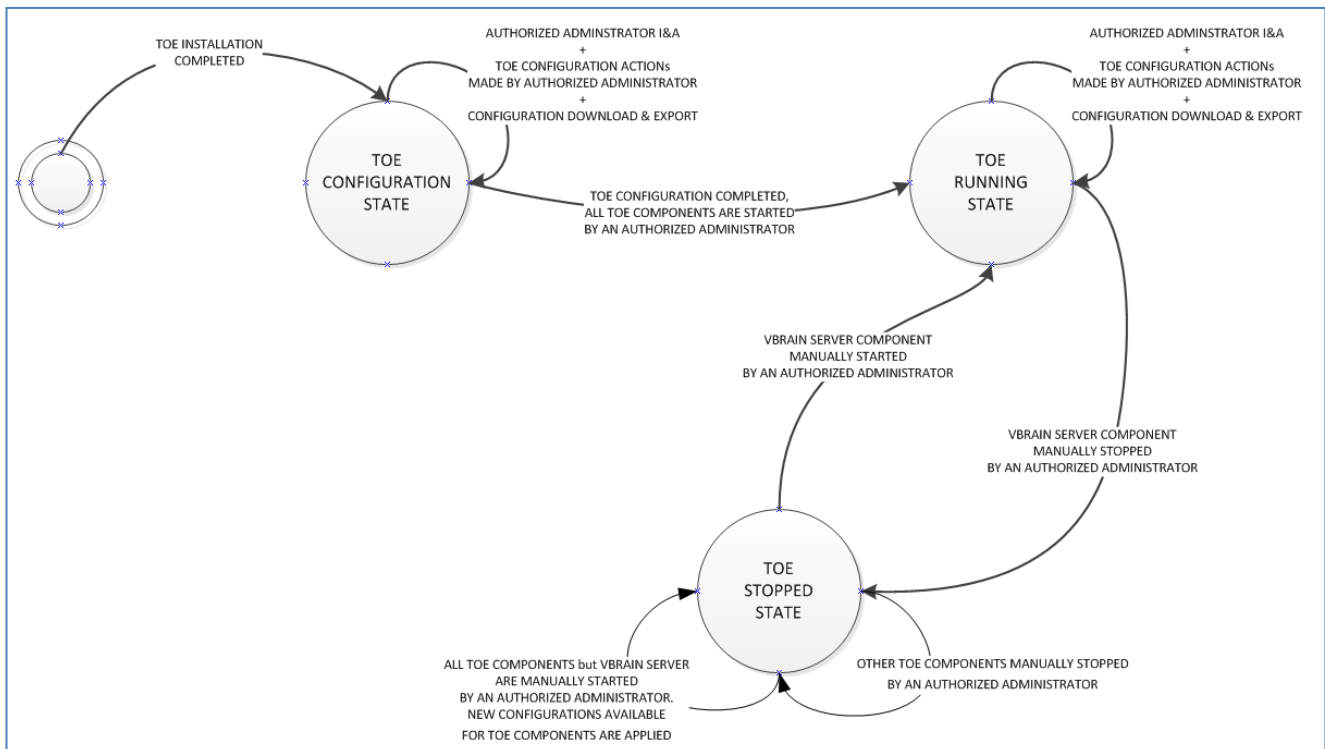
**Figure 3: VBrain EMS operational contexts**

### 1.5.2. OPERATIVE MODES OF THE TOE

- [26] After the installation of each component of the TOE in its Operational Environment, the TOE will be available for configuration, but security features will not be yet available, as well as TOE users are not defined, yet. That is, the TOE components are installed, but are not functioning nor configured. TOE components, but VBrain Configurator, cannot be activated before their configuration.
- [27] The TOE authorized administrators are responsible for the TOE configuration through the interfaces offered by the VBrain Configurator component. This operation is handled in the CONFIGURATION

STATE. The CONFIGURATION STATE is entered by the TOE only the first time each TOE component needs to be configured.

- [28] In addition, through VBrain Configurator, the System Administrator is able to create and delete TOE users.
- [29] An authorized administrator in CONFIGURATION STATE can manually export the configuration files from the host where VBrain Configurator is installed to the host/s where the other TOE components are installed, using a removable memory device (USB key, USB HDD, SD card, CD/DVD, etc.).
- [30] When each TOE component configuration is completed, the TOE components can be executed by an OS system administrator: note that TOE authorized administrators are the only “system administrators” configured at OS level. When all TOE components are active and running, the TOE enters in RUNNING STATE and all the security functionalities offered by the TOE are available for the different user roles authorized to access VBrain EMS.
- [31] When the TOE is in RUNNING STATE, a TOE authorized administrator can change a TOE component’s configuration of through the interfaces offered by VBrain Configurator (standalone TOE component), but new configurations are made effective only after a “stop-and-restart” operation on each TOE component is performed by an OS System Administrator.
- [32] When VBrain Server is manually stopped by an authorized OS System Administrator, the TOE enters the STOPPED STATE: TOE operators will see from a Client HMI that VBrain Server is unreachable. In this case, a Client HMI will start polling for VBrain Server to check when VBrain Server is reachable again, so that the TOE can exit the STOPPED STATE and return back in the RUNNING STATE.
- [33] In the STOPPED STATE, an OS System Administrator can proceed stopping all the other TOE components and restarting them so that, if the TOE components configuration has been modified or a new configuration has been created, it will be updated by TOE components at the moment of their launch.



**Figure 4: VBrain EMS operative modes**

### 1.5.3. MAJOR SECURITY FEATURES OF THE TOE

- [34] In the following section, the main VBrain EMS features are listed; the major security features offered by the TOE are highlighted in **bold**.
- [35] **The TOE grants the TOE System Administrator the rights to create and configure new TOE users with different access levels, assigning them a list of VBrain Servers that can be accessed and the user role/group for each Server. In addition, for each assigned Server, the TOE System Administrator sets the maximum number of OPC-UA sessions that can be opened by each TOE user.**
- [36] **TOE users are uniquely identified and authenticated before any other interaction can take place on behalf of that user.**
- [37] **After a positive login of a TOE user, the TOE grants a proper session handling on behalf of that user.**
- [38] **The TOE allows protected communication with data import/export between different TOE components and external IT system/devices (e.g., FieldBus OPC-UA devices, or third party systems interfacing the TOE via OPC-UA, or another TOE instance) through the standard industrial protocol OPC-UA (Unified Architecture):** the Operational Environment supports the TOE granting both RSA 2048 cryptographic support for communication channel protection and cryptographic protection of messages exchanged over the communication channel with AES 128. For each VBrain Client-type application, a dedicated session is opened for communication and the encrypted messages exchanged during a session may contain sensors measurements, actuators and devices states, commands, alarms, and other device notifications.
- [39] **The TOE asks a confirmation to the user in case a manual closing of a Server-side TOE component has been requested.** The Operational environment supports the TOE preventing Server-side TOE components manual closing, either accidental or intentional, requested by unauthorized users. Only authorized OS System Administrators may close those applications. Upon user closing request, a window will be displayed asking to confirm the operation.
- [40] The TOE allows “*user-friendly*” configuration through a dedicated application – VBrain Configurator – which does not require programmer skills since it uses intuitive insertion pages and different configuration levels depending on user expertise: **all TOE components and TOE users configurations, included OPC-UA Server/Client configurations, are backed up on a relational database (configuration DB).**
- [41] **The TOE grants configuration coherence, data integrity, and limits human errors. Controls are performed by the VBrain Configurator.**  
The confidentiality of TOE components and TOE users configuration is granted also with the support of the Operational environment.
- [42] **Raw and calculated measures, alarms and commands are periodically** (periodicity is configurable according to monitored devices’ characteristics) **stored by the TOE on a relational database (runtime DB). The TOE offers also the functionality of archiving, visualizing and reporting of historical data in tabular and graphical formats (historian DB). The TOE grants data availability for runtime and post-processing.**
- [43] An important VBrain EMS feature is the possibility to send commands to the monitored plant/device through the HMI, when allowed according to user role (each user is associated with a list of VBrain Servers that he can access and a role and group for each Server). The command sending operation is a critical action because it requires the determination of a control procedure to adopt, the implementation of a conditioning action on the controlled process and the monitoring of its effects. All these phases are important to obtain a positive result, so it is fundamental to pay attention to all

the involved processes so to avoid damaging effects on the system and monitored devices in FieldBus controlled by the TOE.

- [44] Command sending is made possible through graphical objects on VBrain Client HMI, as buttons, switches and knobs similar to the real ones, that make the operator feel as the action is performed directly on the controlled device.
- [45] Control sequences can be performed in three different modes:
- Automatic – the operator can visualize the steps sequence, that are independently performed by the system, which is responsible of checking at each step the pre- and post-conditions that guarantee the process goes from a stable state to another stable one.
  - Semiautomatic – VBrain Server does not act independently, but suggests the operator the necessary steps to be performed, asking for authorization.
  - Manual – VBrain Server is completely excluded from the device management, and the operator executes manually all the steps of the procedure, checking the pre- and post-conditions that guarantee the process's stability.
- [46] **Commands are correlated to the user who requested their execution and are executed by VBrain Server only after having positively checked that the user has proper rights for their execution, according to the VBrain Server to which is associated, and the assigned role and groups.**
- [47] **Commands executed by VBrain Server are logged by VBrain Logger in the *runtime DB*, together with the indication of the user who requested their execution and other related information.**
- [48] The TOE offers the possibility to trigger alarms, making the operators aware of critical states of the system.
- [49] Measurements can be snoozed to avoid operators are overloaded with information in case of frequent alarms' triggering for the same measurement.
- [50] **TOE grants that alarms are acknowledged and measurements are snoozed only by authorized users and that acknowledged alarms and snoozed measurements are logged in *runtime DB*, together with the indication of the user who performed this operation and other related information.**
- [51] The DBMS supports the TOE in:
- protecting the confidentiality and integrity of TOE configuration (*configuration DB*);
  - protecting the confidentiality and integrity of measures, alarms and commands (*runtime DB*);
  - protecting the confidentiality and integrity of historical logs (*historian DB*).
- [52] The TOE can execute automatic procedures and sequences on the basis of the actual state of the underlying/controlled/monitored process or specific measured values. **The monitored and controlled system's resilience and responsiveness is enhanced by the TOE, guaranteeing availability and business continuity.** From the monitoring and control point of view, the correct operation of the underlying process is guaranteed by the proper SCADA operation. To such end, SCADA reliability and continuity is of paramount importance. Automation is related to commands and sequences, the VBrain Supervisor operation, and backups management.
- [53] To this end, **VBrain Supervisor** is installed, **which continuously monitors the operating state of the VBrain Server-side core applications**, and re-runs the related process in case it becomes unresponsive, so to guarantee data availability for the VBrain Client-type applications.
- [54] The TOE offers trend and mean runtime graphical representation of measurements.
- [55] Data representation is offered by the TOE on customizable interfaces which guarantee:



- multi-Client HMI: several HMI Clients may be active at a certain time, each of which establishes a dedicated OPC-UA session with VBrain Server;
- **access to applications and interfaces is granted to a user according to its role and group for a specific VBrain Server;**
- 2D, 3D and GIS plant/site visualization;
- **alarms management to authorized users;**
- **events management to authorized users;**
- measures and alarms lists, which are presented through a Web Client HMI compliant with mobile devices.

[56] The TOE performs **self-diagnostic through the event-based automatic application restoring, a runtime DB backup procedure and the runtime DB backup folder management on the basis of a FIFO policy.**

[57] The TOE offers the possibility to acquire FieldBus data through one or more of the implemented drivers: it is out of the scope of the TOE CC evaluation and certification process to verify the correct implementation of the different protocols, recognized by the TOE through the drivers, implemented according to the standards referenced below:

- **OPC** (OLE for Process Control) is a software interface standard that allows Windows programs to communicate with industrial hardware devices, i.e., which helps specifying the communication of real-time plant data between control devices from different manufacturers, defining a standard set of objects, interfaces and methods for use in process control and manufacturing automation applications to facilitate interoperability.

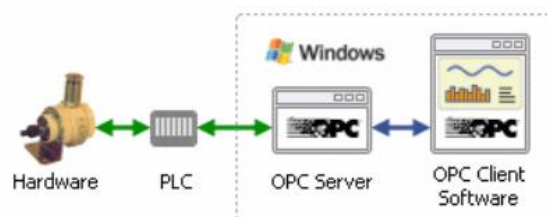
<https://opcfoundation.org/about/opc-technologies/opc-classic/>  
<http://www.opcdatahub.com/WhatIsOPC.html>

OPC is implemented in Server/Client pairs. The OPC Server is a software program that converts the hardware communication protocol used by a device into the OPC protocol. The OPC Client software is any program that needs to connect to the hardware, such as an HMI. The OPC Client uses the OPC Server to get data from or send commands to the hardware.

OPC is a Client/Server architecture that allows any process (Client) based on OPC to access any data source (Server) with OPC interfaces. The use of OPC standard grants the independence of VBrain EMS's SW from the hardware/software features of the data source and a homogeneous view of different data formats.

VBrain Server plays the role of OPC Client with respect to the field devices.

Communication between OPC Client and OPC Server is not protected.



- **OPC-UA** (OPC Unified Architecture): in 2008, the OPC Foundation released OPC Unified Architecture (OPC-UA), a platform independent service-oriented architecture that integrates all the functionalities of the existing OPC Classic specifications into one extensible framework, and is backward compatible with OPC Classic. It was developed to provide a path forward from the

original COM-based communications model to a cross-platform service-oriented architecture for process control, while enhancing security and providing an information model.

<https://opcfoundation.org/about/opc-technologies/opc-ua/>

- **ADS** (Automation Device Specification) is a native Beckhoff TwinCAT system transport layer protocol, developed for data exchange between the different software modules, that runs on top of the TCP/IP or UDP/IP protocols. It allows the user within the Beckhoff system to use almost any connecting route to communicate with all the connected devices and to parameterize them. Beckhoff offers an OPC Server for the purpose of having a standardized interface for communication used in automation engineering.  
[http://infosys.beckhoff.com/english.php?content=../content/1033/cx8010/html/bt\\_ethernet%20ads%20potocols.htm&id=](http://infosys.beckhoff.com/english.php?content=../content/1033/cx8010/html/bt_ethernet%20ads%20potocols.htm&id=)
- **MODBUS** is a serial communications protocol, commonly available for connecting industrial electronic devices, as it enables communication among many devices connected to the same network.  
[http://www.modbus.org/docs/Modbus\\_Application\\_Protocol\\_V1\\_1b3.pdf](http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf)
- **SNMP** (Simple Network Management Protocol) is an Internet-standard protocol, component of the Internet Protocol Suite, developed to monitor network-attached devices for conditions that warrant administrative attention. It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects. SNMP allows Servers to share information about their current state, and provides also a channel through which an administrator can modify predefined values. SNMP is a protocol implemented on the application layer of the networking stack.
- **MILESTONE** is the driver used for the integration of the most common video surveillance and IP video management system.  
<https://www.milestonesys.com/>

#### 1.5.4. TOE TYPE

- [58] The TOE is a software TOE, used for implementing a SCADA, that has been developed using the following programming languages: C#, Microsoft .Net Framework 4.6, Visual Studio 2015 and LabVIEW 2015 (National Instruments).
- [59] The TOE implementation and operation is supported by the following certified COTS that are part of the Operational environment (also indicated respectively as Certified DBMS and Certified OS in the figures representing TOE configurations):
- **DBMS:**  
 Microsoft SQL Server 2012 Database Engine Enterprise Edition x64 (English), Version 11.0.3000.0 (including Service Pack 1), certified CC EAL4+ ALC\_FLR.2, to manage *configuration DB*, *runtime DB* and *historian DB* databases.  
 Certification report is available at the following address:  
[https://www.commoncriteriaportal.org/files/epfiles/0811a\\_pdf.pdf](https://www.commoncriteriaportal.org/files/epfiles/0811a_pdf.pdf);
  - **Operating System (see <https://msdn.microsoft.com/en-us/library/dd229319.aspx>):**  
 Windows Server 2012 R2 and Windows 10 ([https://www.commoncriteriaportal.org/files/epfiles/cr\\_windows10.pdf](https://www.commoncriteriaportal.org/files/epfiles/cr_windows10.pdf))  
 Windows 8 and Windows Server 2012 ([http://www.commoncriteriaportal.org/files/epfiles/st\\_vid10520-vr.pdf](http://www.commoncriteriaportal.org/files/epfiles/st_vid10520-vr.pdf))  
 Windows 7 and Windows Server 2008 R2 ([http://www.commoncriteriaportal.org/files/epfiles/st\\_vid10390-vr.pdf](http://www.commoncriteriaportal.org/files/epfiles/st_vid10390-vr.pdf))  
 Windows 8.1 ([https://www.niap-ccevs.org/st/st\\_vid10592-vr.pdf](https://www.niap-ccevs.org/st/st_vid10592-vr.pdf))
- [60] The communication framework has been entirely developed according to the OPC-UA standard specification (IEC 62541 - [https://opcfoundation.org/wp-content/uploads/2014/05/OPC-UA\\_Security\\_EN.pdf](https://opcfoundation.org/wp-content/uploads/2014/05/OPC-UA_Security_EN.pdf)), which allows complete interoperability between software applications and automation components.
- [61] Taking advantage of the Microsoft .Net functionalities, the implementation of the OPC Foundation standard allowed the creation of a common environment for communication and data management between different devices and system modules. The OPC-UA technology standardizes data exchange between automation and software components based on the Client/Server principle and allows the realization of “global” interoperability. For all these reasons, a standard data exchange is possible between different devices and/or software applications, regardless of the manufacturer, the programming language and the Operating System.
- [62] The system has been developed according to the standard defined in the documents available after user registration at <https://opcfoundation.org/developer-tools/specifications-unified-architecture>.
- [63] VBrain EMS’s architecture allows to create different hierarchical levels of nodes, namely a multi-nodal distribution, where each node can be a Server, a Client or a Server-Client node.

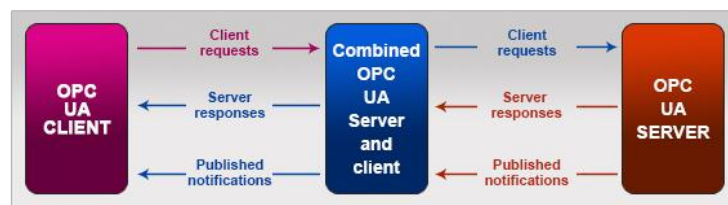
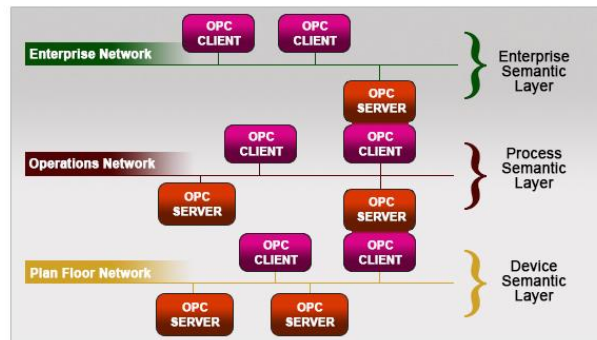


Figure 5: Client/Server architecture



**Figure 6: Multi-nodal architecture**

- [64] TOE “Client-type” components set includes both OPC-UA Clients and non-OPC-UA Clients. As well, TOE “Server-type” components set includes both OPC-UA Servers and non-OPC-UA Servers.
- [65] VBrain Server behaves as an OPC-UA Server with respect to the other TOE “Client-type” components, while is a OPC-UA Client with respect to external OPC-UA Servers (e.g., FieldBus devices, OLCs,...) from which the TOE acquires data.
- [66] Only the VBrain Server TOE component may assume both the role of OPC-UA Server and OPC-UA Client.

### 1.5.5. TOE CONFIGURATION

- [67] Server-type TOE Components, described at §1.7, may be installed on the same host or in several different hosts.
- [68] The TOE can be installed in three different configurations:

**1) “Desktop Client HMI” Configuration:**

SERVER-SIDE TOE COMPONENTS	OPERATOR-SIDE TOE COMPONENT
VBrain Server	VBrain Desktop Client HMI
VBrain Notifier	VBrain Reporting HMI
VBrain Logger	VBrain Alarms List
VBrain Reporting	
VBrain Configurator	
VBrain Supervisor	

- [69] In this configuration, the main operator HMI – VBrain Desktop Client HMI – is constituted by an ad-hoc application developed in LabVIEW, designed and customized for the specific process/plant/site to be monitored and controlled.
- [70] The installation of LabVIEW Run-Time Engine 2015 on the Client HMI host is required for its operation.
- [71] VBrain Alarms List represents an additional application that can be independently opened, but which provides a complete overview about the state of the monitored system only if flanked to VBrain Client Desktop HMI.

## 2) “Web Client HMI” Configuration:

SERVER-SIDE TOE COMPONENTS	OPERATOR-SIDE TOE COMPONENT
VBrain Server	VBrain Web Client HMI
VBrain Notifier	VBrain Reporting HMI
VBrain Logger	
VBrain Reporting	
VBrain Web Socket Server	
VBrain Client HTML5	
VBrain Configurator	
VBrain Supervisor	

- [72] In this configuration, the operator HMI is represented by a Web application – VBrain Web Client HMI – hence a browser is required for its operation, where one or more pages with different panels can be opened.
- [73] To its functioning, VBrain Web Socket Server needs to be installed and properly configured on the Server-side of VBrain EMS.

## 3) “Complete” Configuration (Desktop Client HMI + Web Client HMI):

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	

In such configuration, both VBrain Client HMIs are available in the Client host. Thereby, the information related to the state of the monitored system (measurements, events, alarms) and its control can be performed both through the Web Client HMI and/or the Desktop Client HMI.

- [74] It should be noted that when “n” TOEs are installed in the same Operational Environment so that “n” VBrain Servers can be monitored by the same Client HMI (multi-nodal architecture), nothing changes about TOE components installed / TOE configurations: using the interfaces offered by VBrain Configurator, the VBrain Server component belonging to TOE<sub>A</sub> could be configured either as OPC-UA Server or OPC-UA Client for the VBrain Server component belonging to TOE<sub>B</sub>.
- [75] The data to be published will be configured for each OPC-UA Server, as well as the data to be subscribed for each OPC-UA Client, but this will be transparent for a TOE operator to which one or more Servers will be associated. The TOE operator will be allowed to visualize data from the Server/s associated to him.

## 1.6. REQUIRED NON-TOE COMPONENTS

[76] The operational environment is represented by the following components.

### SERVER-SIDE

<b>Operating System</b>	<b>Microsoft Windows Server OS</b> certified CC compliant (See [59]), with the associated Product Key (also indicated as certified OS in the figures representing TOE configurations): <ul style="list-style-type: none"> <li>- Windows Server 2012 R2</li> <li>- Windows Server 2012</li> <li>- Windows Server 2008 R2</li> </ul>
<b>DBMS</b>	<b>Microsoft SQL Server 2012 Database Engine Enterprise Edition x64 (English), Version 11.0.3000.0 (including Service Pack 1)</b> certified CC EAL4+ ALC_FLR.2 (also indicated as certified DBMS in the figures representing TOE configurations). See also [59].
<b>Other required software</b>	.NET Framework V 4.6.1 .NET Framework V 3.5 IIS (Internet Information Services) 8
<b>Recommended hardware</b>	<b>HDD:</b> at least 50GB of free disk space (36GB for Windows Server 2012 R2 with GUI installation, 6GB for SQL Server 2012 Enterprise SP1 installation), to be increased according to the databases and Client HMI panels dimension. <b>RAM:</b> at least 8GB, to be increased according to the databases' dimension. <b>CPU:</b> at least 2,0 GHz. <b>x86 Processor:</b> Pentium III-compatible processor or faster. <b>x64 Processor:</b> AMD Opteron, AMD Athlon 64, Intel Xeon with Intel EM64T support, Intel Pentium IV with EM64T support, or faster. <b>NIC:</b> Gigabit (10/100/1000baseT) Ethernet adapter.

Table 4: SW/HW prerequisites of Server components

### OPERATOR-SIDE

#### TOE in "Web Client HMI" configuration:

<b>Software prerequisites</b>	.NET Framework V 4.6.1 .NET Framework V 3.5 Internet browser compliant with HTML5 and CSS3 and SVG management. Despite not being mandatory, the VBrain Server certificate can be downloaded and installed by the TOE user in order to let the Web Client HMI trust the VBrain Server. The Web Socket Client component is automatically downloaded and installed by the browser when accessing VBrain Web Client HMI URL.
<b>Recommended hardware</b>	According to the OS and other applications installed on the Host Client. <b>NIC:</b> Gigabit (10/100/1000baseT) Ethernet adapter.

Table 5: SW/HW prerequisites of Client components in TOE - Web Client HMI configuration

**TOE in “Desktop Client HMI” configuration:**

<b>Operating System</b>	<b>Microsoft Windows OS</b> certified CC, with the associated Product Key: <ul style="list-style-type: none"> <li>- Windows 10/8.1/8/7</li> <li>- Windows Server 2012 and Windows Server 2012 R2</li> <li>- Windows Server 2008 R2</li> </ul>
<b>Software prerequisites</b>	.NET Framework V 4.6.1
	.NET Framework V 3.5
	LabVIEW Run-Time Engine 2015
	VBrain Server certificate has to be manually installed by the TOE user in the the local machine “personal” certificate store (see <a href="https://docs.microsoft.com/en-us/windows-hardware/drivers/install/local-machine-and-current-user-certificate-stores">https://docs.microsoft.com/en-us/windows-hardware/drivers/install/local-machine-and-current-user-certificate-stores</a> ) in order to let VBrain Desktop Client HMI trust VBrain Server.
<b>Recommended hardware</b>	<b>HDD:</b> at least 10GB of free disk space (620MB for LabVIEW Run-Time Engine 2015 installation), to be increased according to the OS, other applications installed on the Host Client and to the Client HMI panels’ dimension. <b>RAM:</b> at least 4GB. <b>CPU:</b> at least 2 GHz <b>x86 Processor:</b> Pentium III/Celeron-compatible or faster. <b>X64 Processor:</b> Pentium 4-compatible or faster. <b>NIC:</b> Gigabit (10/100/1000baseT) Ethernet adapter.

Table 6: SW/HW prerequisites of Client components in TOE - Desktop Client HMI configuration

**TOE in “Complete” configuration:**

<b>Operating System</b>	<b>Microsoft Windows OS</b> certified CC , with the associated Product Key: <ul style="list-style-type: none"> <li>- Windows 10/8.1/8/7</li> <li>- Windows Server 2012 and Windows Server 2012 R2</li> <li>- Windows Server 2008 R2</li> </ul>
<b>Software Prerequisites</b>	.NET Framework V 4.6.1
	.NET Framework V 3.5
	One among the major Internet browsers compliant with HTML5 & CSS3 and SVG management, in their most updated version.
	LabVIEW Run-Time Engine 2015
	VBrain Server certificate has to be manually installed by the TOE user in the the local machine “personal” certificate store (see <a href="https://docs.microsoft.com/en-us/windows-hardware/drivers/install/local-machine-and-current-user-certificate-stores">https://docs.microsoft.com/en-us/windows-hardware/drivers/install/local-machine-and-current-user-certificate-stores</a> ) in order to let VBrain Desktop Client HMI trust VBrain Server.
<b>Recommended hardware</b>	<b>HDD:</b> at least 10GB of free disk space (620MB for LabVIEW Run-Time Engine 2015 installation), to be increased according to the OS, other applications installed on the Host Client and to the Client HMI panels’ dimension. <b>RAM:</b> at least 4GB. <b>CPU:</b> at least 2 GHz <b>x86 Processor:</b> Pentium III/Celeron-compatible or faster. <b>X64 Processor:</b> Pentium 4-compatible or faster. <b>NIC:</b> Gigabit (10/100/1000baseT) Ethernet adapter.

Table 7: SW/HW prerequisites of Client components in TOE - Complete configuration

## 1.7. TOE DESCRIPTION

[77] The TOE (VBrain monitoring system or VBrain EMS) is composed of the software implementing the components listed below:

- **VBRAIN SERVER:** the core application, responsible for data acquisition from FieldBus devices (outside the TOE boundary), data elaboration and normalization, commands actuation, alarms generation and publication of all measurements variations. It includes several drivers to interface FieldBus devices.
- **VBRAIN SUPERVISOR:** responsible for granting service continuity.
- **VBRAIN LOGGER:** responsible for logging in the *runtime DB* all acquired and elaborated data. It also performs self-diagnostic through an event-based automatic *runtime DB* backup procedure and the runtime DB backup folder management on the basis of a FIFO policy.
- **VBRAIN CONFIGURATOR:** used by TOE authorized administrators to configure the TOE and the TOE users.
- **VBRAIN REPORTING and VBRAIN REPORTING HMI:** allow TOE users, according to their role and access rights, to access and consult stored data (both in *runtime* and *historian DB*) in order to perform analysis of the information related to the systems' evolution.
- **VBRAIN NOTIFIER:** in charge of forwarding information related to measures towards the operators through different communication services or peripheral devices, as e-mail, SMS, printers, among others, according to its configuration. Its modularity allows the configuration of new means to notify information about selected measures. By means of its ad-hoc configurator, accessible only by OS System Administrator, it is possible to set the notice receivers, the default message to be sent, and the specific measurements or alarms that are to be monitored. Hence, an encrypted JSON/XML configuration file is created (by VBrain Notifier), which is loaded by the VBrain Notifier application at its startup.

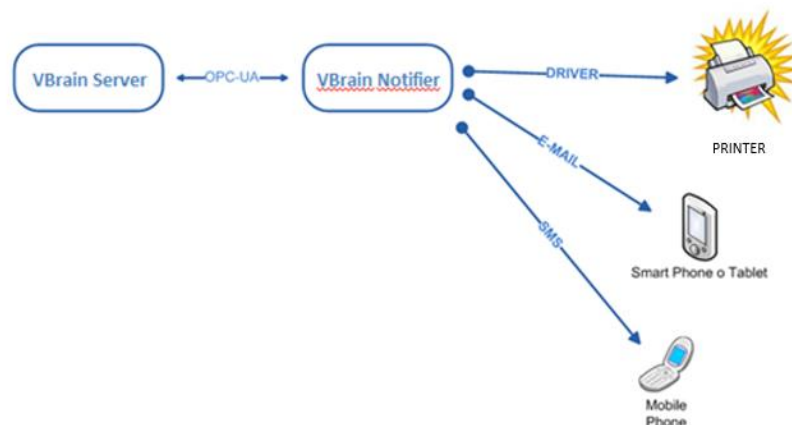


Figure 7: VBrain Notifier scheme

- **VBRAIN CLIENT HMI:** VBrain EMS provides field data visualization through two applications:
  - **VBRAIN DESKTOP CLIENT HMI**
  - **VBRAIN WEB CLIENT HMI and VBRAIN CLIENT HTML5**
- **VBRAIN ALARMS LIST:** in the “Desktop Client HMI” configuration of the TOE, it presents to the operator a table containing only the measurements with condition different from “NORMAL” and/or communication status different from “GOOD”.



- **VBRAIN WEB SOCKET SERVER:** provides the TOE in the “Web Client HMI” configuration with all Server functionalities through Web Socket technologies.

[78] The interfaces have a fundamental role in systems’ monitoring and supervision, as they represent the means through which the operators authenticate themselves, manage and control a process. The Human Machine Interface (HMI) components’ design takes particular care of communication with human, intuitiveness, self-explaining, ease of use and optimization.

## VBRAIN CLIENT HTML5 and VBRAIN WEB CLIENT HMI

- [79] The VBrain Web Client HMI application has a last generation web interface developed using HTML5 and CSS3. It is composed of a main dashboard, a dynamic tree view and a central container, and all the VBrain Desktop Client HMI functionalities described in the next paragraph are maintained.
- [80] The application is characterized by a "responsive design", in which the layout automatically adapts according to the environment in which the application is used (smartphone, tablet or PC) allowing for optimal displaying.



- [81] VBrain Client HTML5 is the web application containing the code executed by IIS and the HMI panels repository, and guarantees the required visualization and operation of VBrain Web Client HMI through an Internet browser. VBrain Web Client HMI allows immediate access to alarms notification, charts management, commands execution and graphical synoptic visualization, on the basis of the role and groups and VBrain Servers assigned to the logged user.
- [82] The responsive design paradigm used to develop the application guarantees a layout that automatically adapts to mobile devices as tablets and smartphones, allowing optimal visualization of the overall plant/site state.
- [83] The interfaces, realized through vector graphic in an SVG editor, are completely customizable to the specific requirements.

## VBRAIN DESKTOP CLIENT HMI

- [84] The VBrain Desktop Client HMI provides several features to provide simple data consultation, alarms management, command and sequence execution.
- [85] The VBrain Desktop Client HMI's graphical interface allows the visualization of instantaneous values, aggregated information and alarms on customizable synoptics.
- [86] The graphic engine is LabVIEW, a graphic programming environment developed by National Instruments (NI) based on data flow and block diagrams. The NI graphic language allows the easy development of highly defined and completely customizable HMIs. For these reasons, VBrain Desktop Client HMI represents an efficient tool for process supervision, management and control. It is designed as transparent as possible for the operator and the controlled process, which are the real system actors. The interface provides a real-time view of all monitored measurements and states on all workstations where this VBrain Desktop Client application is installed.
- [87] Through VBrain Desktop Client HMI, the operator has a complete and efficient view of the operating state of all the monitored process/plant/site components. Each graphical interface is defined accordingly to exact specifications, depending on the monitored plants/sites and needs.
- [88] The fundamental elements that constitute the VBrain Desktop Client HMIs are:
- graphical interfaces;
  - visualization of the operating state of each device/plant/site;
  - treeview;

- operator commands management;
- services nodes.

### TREEVIEW

[89] Treeview is a component of the main screen, composed of nodes that allow the access to the different monitored devices/sites interfaces. Each node assumes a different color based on the status/condition of all the measurements present in the related interface (child nodes). The predefined colors (which can be also configured) are:

- **red**, in case of alarm (ALARM);
- **orange**, in case of warning (WARNING);
- **grey**, in case of communication loss (NOT\_ACQUIRED and BAD\_ACQUISITION);
- **green**, if there are no problems (NORMAL).



Figure 8: Treeview example

[90] A logic measurement is associated to each parent node. This logic measurement represents a correlation of all logical/physical measurements associated to all its child nodes. The parent node always reports the most serious condition between all of the related child nodes.

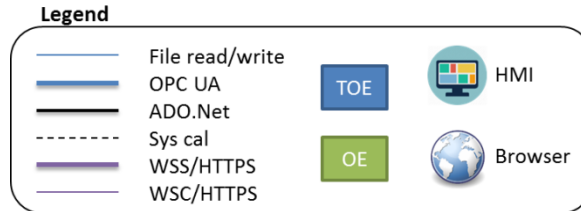
[91] Examples of correlation between measures conditions are the following:



[92] An exception is represented by the NOT\_ACQUIRED and BAD\_ACQUISITION (grey) cases, which are not related to a measured value, but to the communication loss with the acquisition device. In such a case, it is considered as the most serious condition, and the condition is automatically reported by the parent node, which is displayed in grey.

### 1.7.1. TOE Architecture

[93] In the following figures the TOE components are represented for each allowed TOE configuration.

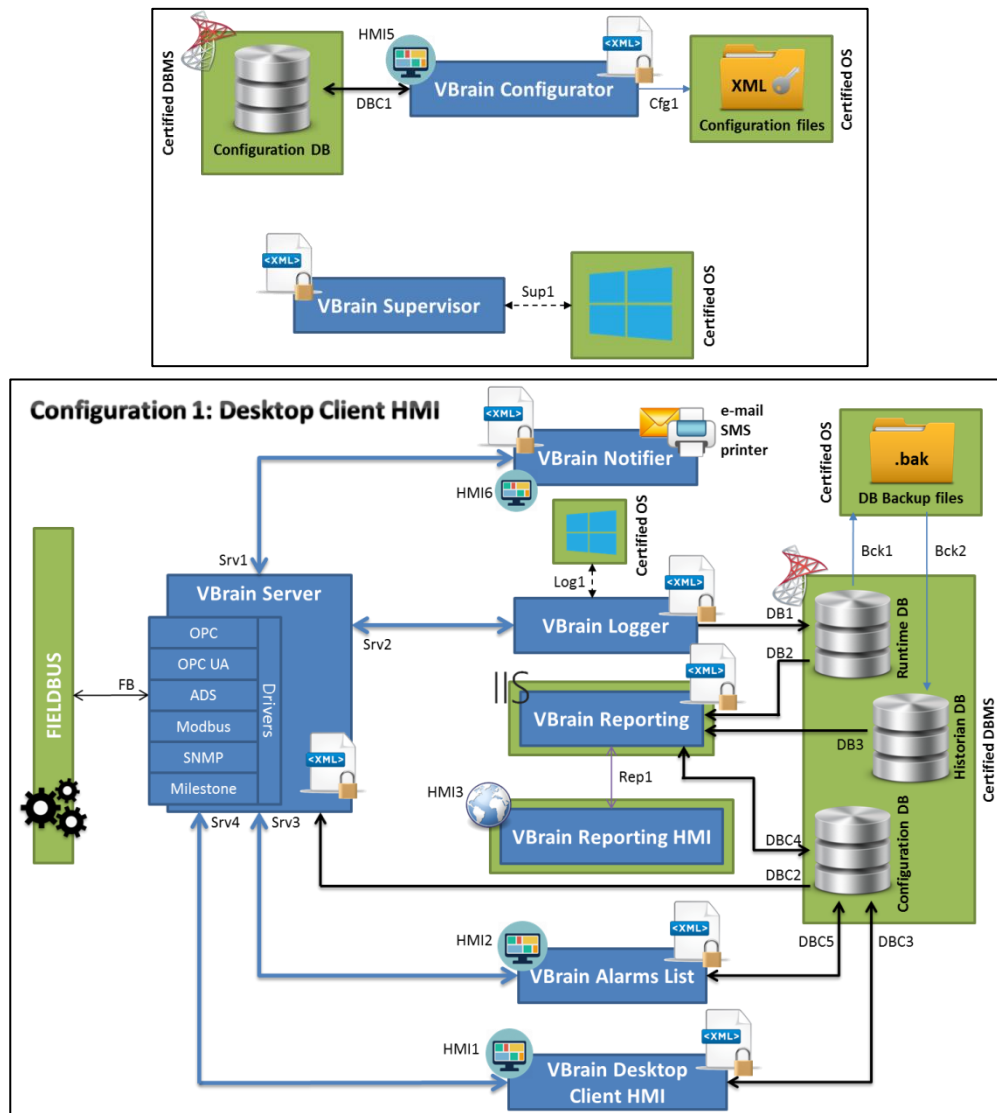


**Figure 9: TOE software Architecture legend**

[94] The TOE components are highlighted in blue, while the components belonging to the Operational environment are represented in green.

[95] **The HMI TOE components offer interfaces to TOE users.**

[96] In each configuration, the following TOE components are installed: VBrain Configurator (with its own HMI accessed only by TOE administrators) and VBrain Supervisor.



**Figure 10: TOE software Architecture in “Desktop Client HMI” configuration**

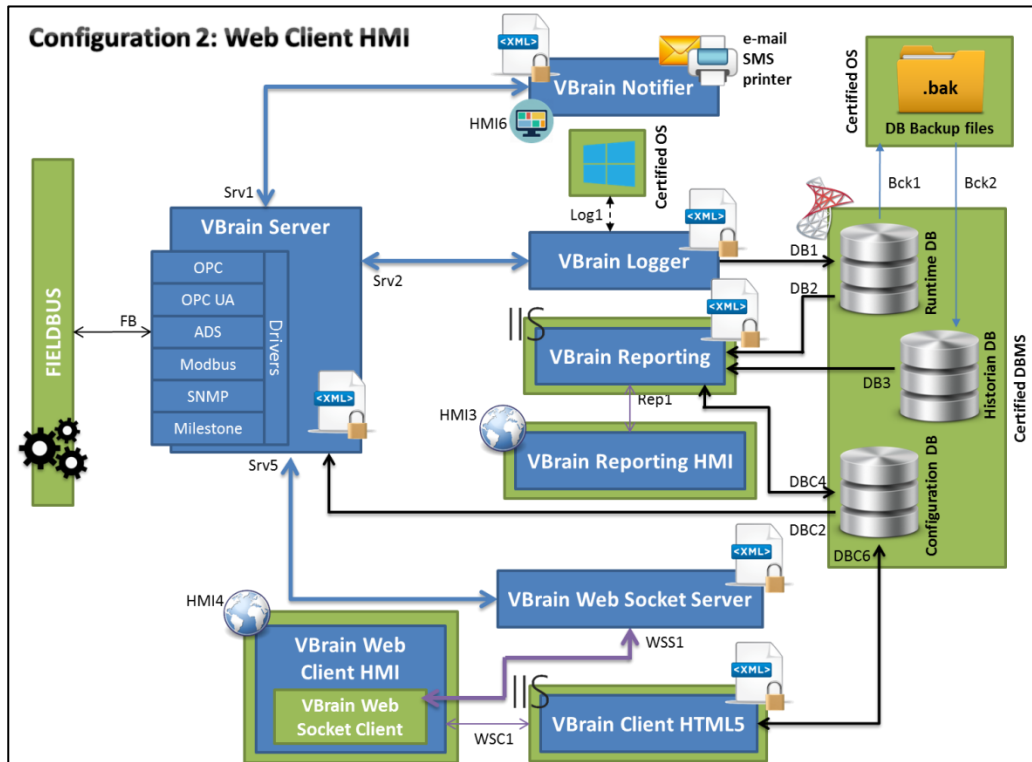


Figure 11: TOE software Architecture in "Web Client HMI" configuration

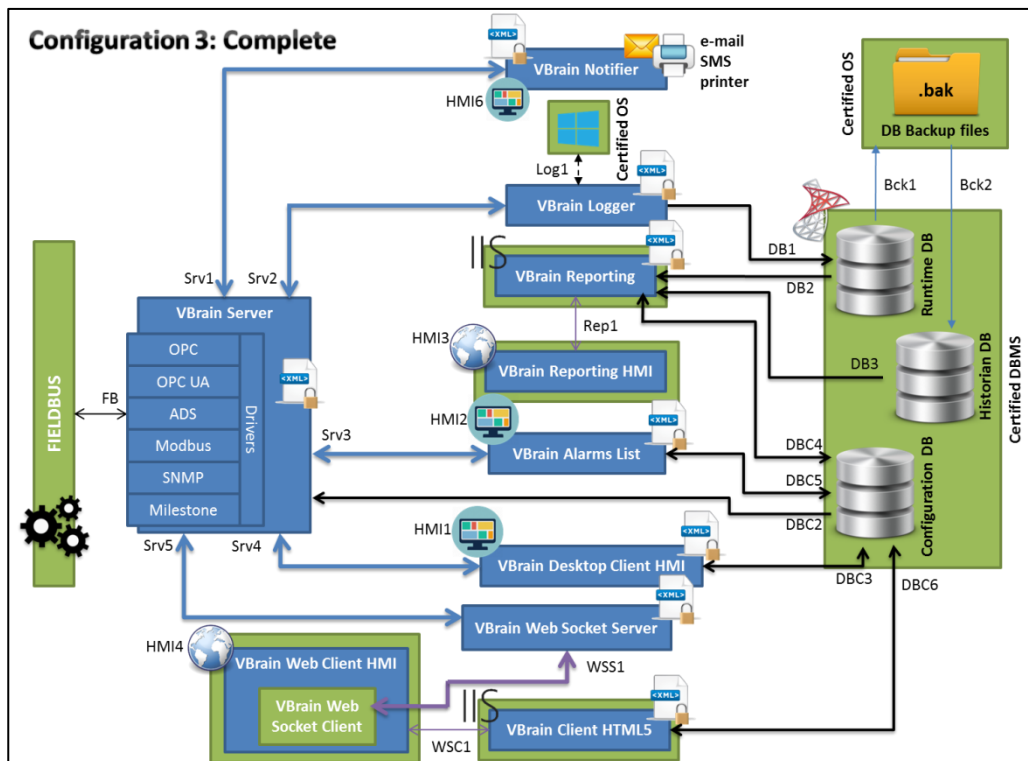


Figure 12: TOE software Architecture in "Complete" configuration

### 1.7.2. TOE USERS PROFILES

- [97] Each configured TOE user is assigned to:
- one or more specific VBrain Servers;
  - an opportune role, for each VBrain Server associated to the user, based on the type of operations the user is allowed to perform;
  - one or more groups, defining the access policy to the different interfaces offered.
- [98] The available roles to be associated during the TOE installation and user creation are:
- Two types of **Administrator** roles: **System Administrator** and **Configuration Administrator**.
  - Four kinds of **Operator** roles: **Commander**, which is hierarchical to **Acknowledger**, which is hierarchical to **Full Reader**, which is hierarchical to **Reader**. Permissions granted to each user role are detailed in table 21, while the operations allowed to each user role and the rules governing access among controlled subjects and controlled objects are detailed in table 17.

### 1.7.3. PHYSICAL SCOPE OF THE TOE

- [99] The Physical scope of the TOE consists of the software implementing the TOE components listed below:
- **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.**

### 1.7.4. LOGICAL SCOPE OF THE TOE

- [100] According to the description provided in § 1.5.3, the logical boundary of the TOE includes the following type of security functionalities, which will be described in the following sections:
- Security Audit;
  - Identification and authentication;
  - TOE access;
  - User data protection;
  - Protection of the TSF;
  - Security Management.

### 1.7.5. TOE GUIDANCE DOCUMENTATION

- [101] The following guidance documentation is provided as part of the TOE:
- VBrain EMS User Guide.
  - VBrain EMS Configuration Manual.
  - VBrain EMS Installation/Recovery Manual V. 1.0.
  - VBrain EMS Hosts Preparation Manual - Server and Client Hosts.

### 1.7.6. USER DATA AND TSF DATA HANDLED BY THE TOE

[102] The TOE handles the following TSF DATA:

- **TOE CONFIGURATIONS:** {USERS CONFIGURATION, TOE COMPONENTS CONFIGURATION including both OPC-UA communication configuration and applicative configuration};
- **USERS' CREDENTIALS:** {username, password};
- **AUDIT LOGS;**
- **RUNTIME DB BACKUP FILE.**

[103] The TOE handles the following **USER DATA:**

- **MEASURES** - for each measure the TOE can acquire from a monitored child node in the FieldBus, the following information are handled by the TOE:
  - **Name** – measure name.
  - **Description** – short measurement description.
  - **Value** – measure value.
  - **Status** – indicates the status of the connection/acquisition with the child node from which the measure is acquired. Possible values are the following: GOOD, NOT\_ACQUIRED (measure has never been acquired), BAD\_ACQUISITION (connection loss), BAD\_CALIBRATION (calibration expression error), BAD\_ALARM (threshold expression error), BAD\_DEADBAND (deadband expression error).
  - **Condition** – indicates if an alarm is active and its criticality level. Possible values are the following: NORMAL, WARNING (Low/High threshold overcome), ALARM (Low Low/High High threshold overcome).
  - **Alarm Time** – date and time of alarm triggering.
  - **Alarm\_Ack** – indicates if an operator has acknowledged the anomaly.
  - **Acknowledge user** – indicates the username associated to the operator who acknowledged the alarm.
  - **Acknowledge Time** – date and time when an operator has acknowledged the anomaly.
  - **Returned** – indicates if an anomalous measurement condition has returned.
  - **Returned Time** – date and time when an anomalous measurement condition has returned.
  - **Snoozed** – indicates if an operator has snoozed the anomalies on the measure.
  - **Snooze Time** – date and time when an operator has snoozed the anomalies on the measure
  - **Snooze user** – indicates the username associated to the operator who snoozed the anomalies on the measure.
  - **To\_Log** – indicates whether the measure is to be logged on *runtime DB*.
  - **To\_Notify** – indicates whether the measure is to be notified internally and/or externally according to VBrain Notifier configuration.
  - **ON/OFF** – indicates if the measure is to be acquired from the FieldBus device.
  - **Calibration enable** – indicates if a calibration is to be made to the acquired raw measurement.
  - **Threshold enable** – indicates if a threshold is to be set to the raw or calculated value, so to trigger an alarm in case the specified threshold is overcome.
- **COMMANDS:**
  - **Name** – command name.
  - **Description** – short command description.
  - **Execution time** – time when the command has been executed by the device.
  - **Request time** – time when the command execution has been requested by the TOE user.
  - **Response time** – time when the device has sent the result for the requested command.
  - **Input arguments** – arguments provided in input at command request.
  - **Output arguments** – arguments provided as output by the device at command response.
  - **Result** – result provided by the device for the requested command.

## 2 CONFORMANCE CLAIM

### 2.1. CC CONFORMANCE CLAIM

[104] This Security Target and this TOE conform to Common Criteria version 3.1 rev. 4.

[105] In particular, this Security Target is compliant with:

- Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, conformant, ver. 3.1 Revision 4, September 2012, CCMB-2012-09-002.
- Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, conformant, ver. 3.1 Revision 4, September 2012, cod. CCMB-2012-09-003 at Evaluation Assurance Level 1 augmented with ASE\_SPD.1, ASE\_REQ.2, ASE\_OBJ.2, ALC\_FLR.1.

### 2.2. PP CONFORMANCE CLAIM

[106] This Security Target does not claim conformance to a Protection Profile.

## 3 SECURITY PROBLEM DEFINITION

[107] This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed.

[108] In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required.
- Any organizational security policy statements or rules with which the TOE must comply.
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

[109] This chapter identifies assumptions as A.assumption, threats as T.threat and policies as P.policy.

### 3.1. THREATS

[110] The following table lists the threats. See [120] for evidence of coverage for each threat.

[111] The assumed attack potential of the attacker for all the threats is **BASIC**.

<i>Threat</i>	<i>Description</i>
<b>T.MASQUERADE</b>	A malicious external IT or human entity may obtain valid identification and authentication (I&A) data (i.e. users' credentials), in order to masquerade as a legitimate user of the TOE, using a brute force or dictionary attacks or sniffing users' credential transferred between Operator-side and Server-side and between separate Server-side parts of the TOE.
<b>T.INTERCEPT</b>	A malicious external IT or human entity may intercept the data exchanged between TOE "Operator-side" and "Server-side" or between separate "Server-side" parts of the TOE, to compromise their confidentiality or integrity.
<b>T.CONFIG</b>	An unauthorized user may change the configuration of the TOE, intentionally or not, causing potential intrusions and security events to go undetected.
<b>T.PRIVIL</b>	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
<b>T.INTEGRITY</b>	An unauthorized user may compromise the integrity of the configuration data and other data generated or stored by the TOE.



<b>T.CONFIDENTIALITY</b>	An unauthorized user may compromise the confidentiality of the configuration data and other data generated or stored by the TOE.
<b>T.NOTRACE</b>	An unauthorized user may perform operations or changes to TSF settings without being accountable for it.
<b>T.LOSSOF</b>	An unauthorized user may change or delete data or alarms collected or generated by the TOE.
<b>T.INTERR</b>	Unexpected interruptions to the operation of the TOE may cause security related data to be lost. Such interruptions may arise from human error or from failures of software or power supplies.
<b>T.EXHAUST</b>	A malicious external IT or human entity may cause security related data to be lost or prevent their future recording by taking actions to exhaust <i>runtime DB</i> storage capacity or <i>runtime DB</i> backup folder capacity.
<b>T.INSTALL</b>	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
<b>T.IMPROPERUSE</b>	An authorized user may improperly send commands, acknowledge alarms or snooze measurements, interrupt TOE components execution, launch from a VBrain Client HMI other applications for remote management without having the rights to do so, or may make a contemporary access to the TOE from more than the configured number of Client host (same username) or launch more than the configured number of Client-type applications, opening separate sessions with VBrain Server.
<b>T.REPLAY</b>	A malicious external IT or human entity may access the TOE by replaying the authentication data of an authorized user.

**Table 8: Threats**

[112] The Threats reported in Table 8 may represent a risk for the following TOE and non-TOE assets:

- both TOE administrators' and TOE users' credentials;
- data exchanged between TOE "Operator-side" and "Server-side";
- data exchanged between separate "Server-side" parts of the TOE;
- stored TOE user data;
- stored TOE configuration data;
- stored TOE security functions and data;
- TSF settings;
- TOE applications normal (or expected) operation;
- VBrain databases (*runtime DB*, *configuration DB*, *historian DB*).

### 3.2. ORGANISATIONAL SECURITY POLICIES

[113] An organizational security policy is a set of rules, practices, and procedures intended to be imposed by an organization using VBrain EMS to address its security needs. This section of the security problem definition shows the OSPs that are to be enforced by the TOE, its Operational Environment, or a combination of the two.

<i>Policy</i>	<i>Description</i>
<b>P.ACCOUNT</b>	TOE users shall be accountable for their security related activities.
<b>P.PROTECT</b>	The TOE shall be protected from unauthorized access to its functions.
<b>P.MANAGE</b>	The TOE shall be managed only by authorized users.
<b>P.ACCESS</b>	Security related data collected and produced by the TOE shall only be accessed for authorized purposes by authorized users.
<b>P.INTEGRITY</b>	Security related data collected and produced by the TOE shall be protected from unauthorized modification.

<b>P.PHYSICAL_ACCESS</b>	The physical access to the area where Server-side TOE components are hosted shall be protected from unauthorized access.
<b>P.CONFIGURATION</b>	TOE authorized administrators are responsible for the correct configuration of both the TOE and its Operational Environment.
<b>P.FAILURE</b>	procedures are in place in the operational environment to ensure that, after failures or other discontinuities affecting TOE operation, recovery without security compromise is obtained.
<b>P.AUDITLOG</b>	TOE authorized administrators must ensure that audit functions are used and managed effectively. Such use and management procedures shall apply to the TOE's audit trail and the audit trail for the underlying Operating System and the database Servers. In particular the system clocks must be protected from unauthorized modification (so that the integrity of audit timestamps is not compromised).

**Table 9: Organizational Security Policies**

### 3.3. ASSUMPTIONS

[114] This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

<i>Assumption</i>	<i>Description</i>
<b>A.TRAINING</b>	It is assumed that users of the TOE will be trained sufficiently in order to properly configure, administrate, manage and operate the TOE, and exercising proper control over user data and TSF data according to their responsibilities.
<b>A.DBMS_ACCESS</b>	It is assumed that access to VBrain databases, used by the TOE via mechanisms outside the TOE boundary, is allowed only to authorized administrative users.
<b>A.OS_ACCESS</b>	It is assumed that access to the Operating System, used by the TOE via mechanisms outside the TOE boundary, is allowed only to authorized administrative users.
<b>A.TRUST</b>	It is assumed that the TOE authorized administrators are not hostile, careless or willfully negligent observing the instructions provided by the TOE documentation.
<b>A.TIME</b>	It is assumed that the Operational Environment provides a reliable time reference.
<b>A.SECCOM</b>	It is assumed that the Operational environment supports the TOE providing a secure line of communication between the Server-side TOE components and operator-side TOE components.
<b>A.TOE_EVALUATED</b>	It is assumed that the TOE is installed, configured, and managed in accordance with its evaluated configuration.
<b>A.USERS</b>	It is assumed that authorized users do not actively or negligently compromise the security of the computer on which the TOE is installed and/or used. Examples for such compromising actions would be: <ul style="list-style-type: none"> <li>- Placing malicious software (like programs containing viruses or Trojan horses) on the computer,</li> <li>- modifying the TOE program or data files.</li> </ul>
<b>A.RESTRICT</b>	It is assumed that the OS upon which TOE components reside will be configured to restrict modification to TOE executable files, the OS itself, configuration files and databases to only the TOE authorized administrators.

**Table 10: Assumptions**

## 4 SECURITY OBJECTIVE

[115] Security objectives are concise, abstract statements of the intended solution to the security problem definition (see § 3). The set of security objectives for the TOE and the Operational Environment form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the Operational environment. This section identifies the security objectives for the TOE and its operational environment, as well as providing a mapping of the objectives to the threats, OSPs, and assumptions included in the security problem definition. This mapping also provides rationale for how the threats, OSPs, and assumptions are effectively and fully addressed by the security objectives.

### 4.1. SECURITY OBJECTIVES FOR THE TOE

[116] The IT security objectives for the TOE are addressed below. See in § 6.3.2 which SFRs covers the TOE objectives and in § 7 which security functions fulfill the SFRs selected.

<i>Objective</i>	<i>Description</i>
<b>O.CONFIG</b>	The TOE grants that only TOE authorized administrators are allowed to configure the TOE, to change its configuration when TOE is operational and to make effective those changes.
<b>O.USER</b>	The TOE grants that only the System Administrator is allowed to create and delete users, to assign them the list of (one or more) Servers he is allowed to access and a specific user role for each VBrain Server, and to set the number of OPC-UA sessions the TOE user is authorized to handle. The TOE grants that only a TOE administrator is able to assign the users to one or more groups, limiting their access to the HMI panels.
<b>O.IDENTIFY</b>	The TOE shall identify users prior to allowing access to its functions and data.
<b>O.ANTI_BRUTE</b>	The TOE shall take specified actions or disable the account of the user that attempts to guess a password with brute force or dictionary attack.
<b>O.ACCESS</b>	The TOE shall allow authorized users to access only to authorized TOE functions and data according to their access rights.
<b>O.SECCOM</b>	The TOE protects integrity and confidentiality during security related data exchanges between separate parts of the TOE.
<b>O.REPLAY</b>	The TOE shall counter the exposure to message replay attacks using a message sequencing mechanism between its separate parts.
<b>O.CRASH</b>	The TOE shall permit to recover its configuration in event of disaster or to restore its previous installation.
<b>O.AVAIL</b>	The TOE grants the availability to authorized users of acquired data from the FieldBus (sensors measurements, actuators and device states, other device notifications) as well as alarms and executed commands, according to their access rights.
<b>O.AUDIT</b>	The TOE must record audit records, correlating them to the proper user when applicable, as a result of specific TOE activities and operations performed by TOE users. When applicable, according to the TOE configuration, events and alarms are forwarded to TOE operators through different communications services.
<b>O.MANAGE</b>	The TOE shall include a set of functions that allows the efficacious management of its functionalities and data by TOE authorized administrators
<b>O.EXHAUST</b>	The TOE grants availability of security related data preventing exhaustion of DB storage capacity and DB backup folder capacity
<b>O.SESSION</b>	The TOE prevents that a TOE user opens more than the configured number of separate sessions with VBrain Server.

**Table 11: Security Objectives for the TOE**

## 4.2. SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

[117] The Operational Environment of the TOE implements technical and procedural measures to assist the TOE in correctly providing its security functionality.

[118] In the following table are described a set of statements describing the goals that the Operational Environment shall achieve.

<i>Objective</i>	<i>Description</i>
<b>OE.IDENTIFY</b>	The Operational Environment supports the TOE in identifying and authenticating the authorized Operating System Administrators allowed to close and restart TOE components installed in Server-side and to configure the VBrain Notifier component through a dedicated HMI.
<b>OE.PHYSICAL_ACCESS</b>	The physical access to the area where Server-side TOE components are hosted will be granted to TOE authorized administrators only.
<b>OE.DB</b>	The operational environment must ensure that access to the databases via mechanisms outside the TOE boundary is restricted to TOE authorized administrators only, that will be configured in the CC certified DBMS as databases administrators, and that TOE users and applicative users are properly configured in the DBMS for the following TOE components: VBrain Logger, VBrain Reporting, VBrain Alarms List, VBrain Server, VBrain Desktop Client HMI, VBrain Client HTML5, VBrain Web Socket Server, VBrain Configurator.
<b>OE.SO</b>	The operational environment must ensure that access to the CC certified Operating System via mechanisms outside the TOE boundary is restricted to TOE authorized administrators only, that will be configured in the Operating System as OS System Administrators. Only TOE authorized administrators, after their logging as OS System Administrator, can launch and execute Server-side TOE components and review the log files stored by the OS.
<b>OE.ADMIN</b>	TOE authorized administrators shall be faithfully selected, skilled and trained for proper operation without compromising: <ul style="list-style-type: none"> <li>- the TOE functionalities during its installation, configuration, administration and management;</li> <li>- the security of the Server hosts on which the TOE, the Operating System and the DBMS are installed according to their CC certified configuration;</li> <li>- the security of removable memory devices used to export configuration files;</li> <li>- the security of log files stored by the OS.</li> <li>- the security of TOE Configuration folder name and of <i>ConfigurationVersion.txt</i> file</li> </ul>
<b>OE.OPER</b>	TOE operators shall be skilled and trained for proper operation without compromising the security of the Client hosts on which the TOE is installed and/or used.
<b>OE.INSTALL</b>	The operational environment must ensure that VBrain Server and VBrain Supervisor TOE components are installed on the same Server host, while the other TOE components may be installed on different Server hosts. During TOE installation a "default TOE user" with "System Administrator" role must be defined in the <i>Configuration DB</i> . It will be provided with a default "first access valid password", that must be changed at its first login to the TOE.

<i>Objective</i>	<i>Description</i>
<b>OE.TOE_EVALUATED</b>	The operational environment must ensure that the TOE is installed, configured and managed in its Operational Environment, in accordance with one of its evaluated configurations and according to preparative procedures. In case the TOE is installed as part of a multi-nodal architecture, it could interface other VBrain EMS products that are assumed to be installed, configured and managed in accordance with one of its evaluated configurations and according to preparative procedures. They will be considered by the TOE as a trusted IT product.
<b>OE.CRYPTO</b>	The Operational Environment shall provide cryptographic functionalities (RSA 2048 bit key generation, AES 128 bit key generation for OPC UA implementation, Random Number Generation, RSA encryption/decryption, SHA256 hashing, AES 256 encryption/decryption of configuration files using .NET 4.6.1 libraries) and protocols (HTTPS based on AES 128/256) to properly support the TOE for secure transfer of data between operator-side and Server-side, separate Server-side parts of the TOE and for random password generation to be used for the TOE users first access.
<b>OE.RESTRICT</b>	The operational environment must ensure that: <ul style="list-style-type: none"> <li>- the OS is configured to prevent modification to TOE executable files, to the OS itself and to allow authorized users (TOE administrators or authorized applicative users associated to TOE components) to access only TOE components and data, grant access to the configuration files and to <i>runtime DB</i> backup folder only to authorized applicative users;</li> <li>- the DBMS is configured to prevent modification to itself and to restrict to authorized applicative users the access to the security related data stored in the DBs managed (Runtime DB, Historian, DB and Configuration DB).</li> </ul>
<b>OE.CONTINUITY</b>	The Operational Environment shall ensure operational continuity in case of failures of power supplies.
<b>OE.TIME</b>	The Operational Environment shall provide the TOE with a reliable time reference.
<b>OE.STATE</b>	OS System Administrators (the only System Administrators configured at OS level are TOE authorized administrators), after being identified and authenticated as, are allowed and responsible for stopping/restarting TOE components in order to implement a new configuration, i.e., properly handling the TOE operational mode transition from "TOE RUNNING" to "TOE STOPPED", and vice versa, when a TOE component configuration change is needed.
<b>OE.AUDIT</b>	The Operational Environment shall support the TOE in the generation of audit records, correlating them to the proper user when applicable, as a result of specific TOE activities, operations performed by TOE users, and errors related to the TOE applications' and/or OPC-UA Client/Server operation. In addition, the Operational Environment shall guarantee that only OS System Administrators can accede and visualize the aforementioned audit information.

**Table 12: Security objectives for the Operational Environment**

### 4.3. SECURITY OBJECTIVES RATIONALE

[119] This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies (if applicable). The following table provides a high level mapping of coverage for each threat, assumption, and policy:

OBJECTIVE \ THREAT/POLICIES /ASSUMPTION/	O.CONFIG	O.USER	O.IDENTIFY	O.ANTI_BRUTE	O.ACCESS	O.SECCOM	O.REPLAY	O.CRASH	O.AVAIL	O.AUDIT	O.MANAGE	O.EXHAUST	O.SESSION	OE.IDENTIFY	OE.PHYSICAL_ACCESS	OE.DB	OE.SO	OE.ADMIN	OE.OPER	OE.INSTALL	OE.TOE_EVALUATED	OE.CRYPTO	OE.RESTRICT	OE.CONTINUITY	OE.TIME	OE.STATE	OE.AUDIT		
T.MASQUERADE																													
T.INTERCEPT																													
T.CONFIG																													
T.PRIVIL																													
T.INTEGRITY																													
T.CONFIDENTIALITY																													
T.NOTRACE																													
T.LOSSOF																													
T.INTERR																													
T.EXHAUST																													
T.INSTALL																													
T.IMPROPERUSE																													
T.REPLAY																													
P.ACCOUNT																													
P.PROTECT																													
P.MANAGE																													
P.ACCESS																													
P.INTEGRITY																													
P.PHYSICAL_ACCESS																													
P.CONFIGURATION																													
P.FAILURE																													
P.AUDITLOG																													
A.TRAINING																													
A.DBMS_ACCESS																													
A.OS_ACCESS																													
A.TRUST																													

OBJECTIVE THREAT/POLICIES /ASSUMPTION/	O.CONFIG	O.USER	O.IDENTIFY	O.ANTI_BRUTE	O.ACCESS	O.SECCOM	O.REPLAY	O.CRASH	O.AVAIL	O.AUDIT	O.MANAGE	O.EXHAUST	O.SESSION	OE.IDENTIFY	OE.PHYSICAL_ACCESS	OE.DB	OE.SO	OE.ADMIN	OE.OPER	OE.INSTALL	OE.TOE_EVALUATED	OE.CRYPTO	OE.RESTRICT	OE.CONTINUITY	OE.TIME	OE.STATE	OE.AUDIT	
A.TIME																												
A.SECCOM																												
A.TOE_EVALUATED																												
A.USERS																												
A.RESTRICT																												

Table 13: Tracing between security objectives for the TOE and security objectives for the Operational Environment vs. Threat, OSP and Assumption.

[120] The following table provides detailed evidence of coverage for each threat, policy, and assumption:

<b>THREATS, POLICIES, ASSUMPTIONS</b>	
T.MASQUERADE	O.ANTI_BRUTE grants the disabling of the account if a malicious user attempts to obtain the login credentials using a brute force or dictionary attacks. OE.CRYPTO grants that cryptographic functionalities properly support the TOE for secure transfer of data, among which identification and authentication data, between Operator-side and Server-side and between separate Server-side parts of the TOE.
T.INTERCEPT	O.SECOM grants protection of integrity and confidentiality during user, TOE and security related data exchanges between separate parts of the TOE. OE.CRYPTO grants that cryptographic functionalities properly support the TOE for secure transfer of data between Operator-side and Server-side and between separate Server-side parts of the TOE. Encryption of configuration files is done with the AES 256 protocol, with the Operational Environment support, using .NET 4.6.1 libraries. The Operating System, via .NET Framework 4.6.1, provides cryptographic support to the TOE for RSA/AES key generation and messages encryption.
T.CONFIG	O.CONFIG grants that only TOE authorized administrators are allowed to change the configuration of the TOE when it is in RUNNING state and to make those changes effective.
T. PRIVIL	O.ACCESS grants that the authorized users can access only to authorized TOE functions and data according to their role, groups and VBrain Servers to which are associated. O.IDENTIFY grants identification of users prior to allowing them the access to its functions and data. OE.IDENTIFY grants that the Operational Environment supports the TOE in identifying and authenticating the authorized Operating System Administrators allowed to close and restart TOE components installed on the Server-side and to configure the VBrain Notifier component through a dedicated HMI.
T.INTEGRITY	OE.PHYSICAL_ACCESS guarantees the access to the area where Server-side TOE components are hosted is allowed to TOE authorized administrators only. OE.RESTRICT grants that: <ul style="list-style-type: none"> <li>- the OS is configured to prevent modification to TOE executable files, to prevent modification to the OS itself;</li> <li>- the DBMS is configured to prevent modification to itself.</li> </ul>
T.CONFIDENTIALITY	O.SECOM grants protection of confidentiality during user, TOE and security related data exchanges between separate parts of the TOE. OE.CRYPTO grants that cryptographic functionalities properly support the TOE for secure transfer of data between Operator-side and Server-side and between separate Server-side parts of the TOE.
T.NOTRACE	O.AUDIT and OE.AUDIT grant logging of audit records, correlating them to the proper user when applicable, as a result of specific TOE activities, operations performed by TOE users, and errors related to the TOE applications' and/or OPC-UA Client/Server operation.
T.LOSSOF	O.ACCESS grants that the authorized users can access only to authorized TOE functions and data according to their role, groups and VBrain Servers to which are associated. O.AVAIL grants the availability to authorized users according to their role, groups and VBrain Servers to which are associated, of acquired data from the FieldBus (sensors measurements, actuators and device states, other device notifications) as well as alarms and executed commands. O.EXHAUST grants availability of security related data to prevent exhaustion of DB storage capacity and DB backup folder capacity OE.RESTRICT grants that: <ul style="list-style-type: none"> <li>- the OS is configured to allow authorized users (TOE administrators or authorized applicative users associated to TOE components) to access only TOE components and data;</li> <li>- the OS is configured so that the access to TOE configuration files and to <i>runtime DB</i> backup folder is permitted only to authorized applicative users (associated to the following TOE components: VBrain Configuration, VBrain Logger, VBrain Reporting) and to allow only to OS System Administrators to execute and stop TOE components;</li> <li>- the DBMS is configured to restrict to authorized applicative users (associated to the following TOE components: VBrain Configuration, VBrain Logger, VBrain Reporting) the access to the security related data stored in the DBs managed.</li> </ul>
T.INTERR	O.CRASH grants that the TOE recovers its configuration or restores its previous installation in case of disaster. OE.CONTINUITY grants that the Operational Environment ensures operational continuity in case of failures of power supplies.
T.EXHAUST	With O.EXHAUST the TOE grants availability of security related data to prevent exhaustion of DB storage capacity and DB backup folder capacity
T.INSTALL	OE.INSTALL grants that those responsible for the TOE installation ensures that VBrain Server and VBrain



<b>THREATS, POLICIES, ASSUMPTIONS</b>	
	<p>Supervisor TOE components are installed on the same Server host. During TOE installation a “default TOE user” with “System Administrator” role must be defined in the Configuration DB. It will be provided with a default “first access valid password”, that must be changed at its first login to the TOE.</p> <p>OE.ADMIN grants that TOE authorized administrator shall be faithfully selected, skilled and trained for proper operation without compromising:</p> <ul style="list-style-type: none"> <li>- the TOE functionality during its installation, configuration, administration and management;</li> <li>- the TOE functionality when stopping/restarting TOE components in order to implement a new configuration;</li> <li>- the security of the Server hosts on which the TOE, the Operating System and the DBMS are installed;</li> <li>- the security of removable memory devices used to export configuration files.</li> </ul>
T.IMPROPERUSE	<p>With O.MANAGE, the TOE shall include a set of functions that allow the efficacious management of its functionality and data.</p> <p>With O.SESSION, the TOE prevents a TOE user from locking the username in use from another PC (by inserting a wrong password for three times) when the configured limit for opened sessions has been reached, an improper use of a username from different users and any incoherence in the association between a username and a command, an alarm Ack or a measurement snooze request.</p> <p>O.IDENTIFY grants identification of users prior to allowing them the access to its functions and data.</p> <p>OE.OPER grants that the TOE operators are skilled and trained for proper operation without compromising the security of the Client hosts on which the TOE is installed and/or used.</p>
T.REPLAY	<p>With O.REPLAY, the TOE shall counter the exposure to message replay attacks using a message sequencing mechanism between its separate parts.</p>
P.ACCOUNT	<p>O.AUDIT grants logging of audit records, correlating them to the proper user when applicable, as a result of specific TOE activities and operations performed by TOE users.</p>
P.PROTECT	<p>O.IDENTIFY grants identification of users prior to allowing them the access to its functions and data.</p>
P.MANAGE	<p>O.ACCESS grants that the authorized users can access only to authorized TOE functions and data according to their role, groups and VBrain Servers to which are associated.</p> <p>O.USER grants that only the System Administrator is allowed to create and delete users, to assign them a list of (one or more) VBrain Servers he is allowed to access to and the related roles for each VBrain Server, and to set the number of OPC-UA sessions the TOE user is authorized to handle. In addition, only a TOE administrator can associate the users to one or more groups, limiting their access to the HMI panels.</p>
P.ACCESS	<p>O.ACCESS grants that the authorized users can access only to authorized TOE functions and data according to their role, groups and VBrain Servers to which are associated.</p>
P.INTEGRITY	<p>O.SECCOM grants protection of integrity during security related data exchanges between separate parts of the TOE.</p>
P.PHYSICAL_ACCESS	<p>With OE.PHYSICAL_ACCESS, the physical access to the area where Server-side TOE components are hosted is granted to TOE authorized administrators only.</p>
P.CONFIGURATION	<p>O.CONFIG grants that only TOE authorized administrators are allowed to change the configuration of the TOE when it is in RUNNING state and to make those changes effective.</p> <p>OE.ADMIN grants that TOE authorized administrator shall be faithfully selected, skilled and trained for proper operation without compromising:</p> <ul style="list-style-type: none"> <li>- the TOE functionality during its installation, configuration, administration and management;</li> <li>- the TOE functionality when stopping/restarting TOE components in order to implement a new configuration;</li> <li>- the security of the Server hosts on which the TOE, the Operating System and the DBMS are installed;</li> <li>- the security of removable memory devices used to export configuration files.</li> </ul>
P.FAILURE	<p>O.CRASH grants that the TOE recovers its configuration or restores its previous installation in case of disaster.</p> <p>OE.CONTINUITY grants that the Operational Environment ensures operational continuity in case of failures of power supplies.</p>
P.AUDITLOG	<p>With O.MANAGE, the TOE shall include a set of functions that allows the efficacious management of its functionality and data.</p> <p>O.CONFIG grants that only TOE authorized administrators are allowed to change the configuration of the TOE when it is in RUNNING state and to make effective those changes.</p> <p>OE.RESTRICT grants that:</p> <ul style="list-style-type: none"> <li>- the OS is configured to prevent modification to TOE executable files, to prevent modification to the OS itself and to allow authorized users (TOE administrators or authorized applicative users associated to TOE components) to access only TOE components and data;</li> <li>- the OS is configured so that the access to TOE configuration files and to <i>runtime DB</i> backup folder is permitted only to authorized applicative users (associated to the following TOE components: VBrain Configuration, VBrain Logger, VBrain Reporting) and to allow only to OS System Administrator to</li> </ul>

<b>THREATS, POLICIES, ASSUMPTIONS</b>	
	<p>execute and stop TOE components;</p> <ul style="list-style-type: none"> <li>- the DBMS is configured to prevent modification to itself and to restrict to authorized applicative users (associated to the following TOE components: VBrain Configuration, VBrain Logger, VBrain Reporting) the access to the security related data stored in the DBs managed.</li> </ul>
A.TRAINING	<p>OE.ADMIN grants that TOE authorized administrator shall be faithfully selected, skilled and trained for proper operation without compromising:</p> <ul style="list-style-type: none"> <li>- the TOE functionality during its installation, configuration, administration and management;</li> <li>- the TOE functionality when stopping/restarting TOE components in order to implement a new configuration;</li> <li>- the security of the Server hosts on which the TOE, the Operating System and the DBMS are installed;</li> <li>- the security of removable memory devices used to export configuration files.</li> </ul> <p>OE.OPER grants that the TOE operators shall be skilled and trained for proper operation without compromising the security of the Client hosts on which the TOE is installed and/or used.</p>
A.DBMS_ACCESS	<p>OE.DB grants that those responsible for the TOE configuration and administration must ensure that access to the database via mechanisms outside the TOE boundary is restricted to TOE authorized administrators only, that will be configured in the DBMS as database administrators, and that TOE users and applicative users are properly configured in the DBMS for the following TOE components: VBrain Logger, VBrain Reporting, VBrain Alarms List, VBrain Server, VBrain Desktop Client HMI, VBrain Client HTML5, VBrain Web Socket Server, VBrain Configurator. In particular:</p> <ul style="list-style-type: none"> <li>• VBrain Logger is authorized to write on <i>runtime DB</i>;</li> <li>• VBrain Reporting is authorized to read from <i>runtime DB</i> and from <i>historian DB</i> and to read from/write on <i>configuration DB</i>;</li> <li>• VBrain Alarms List is authorized to read from/write on <i>configuration DB</i>;</li> <li>• VBrain Server is authorized to read from <i>configuration DB</i>;</li> <li>• VBrain Desktop Client HMI is authorized to read from/write on <i>configuration DB</i>;</li> <li>• VBrain Client HTML5 is authorized to read from/write on <i>configuration DB</i>.</li> </ul>
A.OS_ACCESS	<p>OE.SO grants that those responsible for the TOE configuration and administration must ensure that access to the Operating System via mechanisms outside the TOE boundary is restricted to TOE authorized administrators only, that will be configured in the Operating System as System Administrators. Only TOE authorized administrators, after their logging as OS System Administrator, can launch and execute Server-side TOE components.</p>
A.TRUST	<p>OE.ADMIN grants that TOE authorized administrator shall be faithfully selected, skilled and trained for proper operation without compromising:</p> <ul style="list-style-type: none"> <li>- the TOE functionality during its installation, configuration, administration and management;</li> <li>- the TOE functionality when stopping/restarting TOE components in order to implement a new configuration;</li> <li>- the security of the Server hosts on which the TOE, the Operating System and the DBMS are installed;</li> <li>- the security of removable memory devices used to export configuration files.</li> </ul> <p>OE.STATE ensures that TOE authorized administrators are responsible for properly handling the TOE operational mode transition from "TOE RUNNING" to "TOE STOPPED" , and vice versa, when a TOE configuration change is needed.</p>
A.TIME	<p>OE.TIME grants that the Operational Environment provides the TOE with a reliable time reference.</p>
A.SECCOM	<p>OE.CRYPTO grants that cryptographic functionalities properly support the TOE for secure transfer of data between Operator-side and Server-side and between separate Server-side parts of the TOE.</p>
A.TOE_EVALUATED	<p>With OE.TOE_EVALUATED, those responsible for the TOE configuration and administration must ensure that the TOE is installed, configured and managed in its Operational Environment, in accordance with one of its evaluated configurations and according to preparative procedures.</p> <p>In case the TOE is installed as part of a multi-nodal architecture, it could interface other VBrain EMS products that are assumed to be installed, configured and managed in accordance with one of its evaluated configurations and according to preparative procedures. These will be considered by the TOE as trusted IT products.</p>
A.USERS	<p>OE.OPER grants that the TOE operators shall be skilled and trained for proper operation without compromising the security of the Client hosts on which the TOE is installed or from which the TOE is used.</p>
A.RESTRICT	<p>OE.RESTRICT grants that:</p> <ul style="list-style-type: none"> <li>- the OS is configured to prevent modification to TOE executable files, to prevent modification to the OS itself and to allow authorized users (TOE administrators or authorized applicative users associated to TOE components) to access only TOE components and data;</li> <li>- the OS is configured so that the access to TOE configuration files and to runtime DB backup folder is permitted only to authorized applicative users (associated to the following TOE components: VBrain Configuration, VBrain Logger, VBrain Reporting) and to allow only to OS System Administrator to</li> </ul>

THREATS, POLICIES, ASSUMPTIONS	
	<ul style="list-style-type: none"><li>- execute and stop TOE components;</li><li>- the DBMS is configured to prevent modification to itself and to restrict to authorized applicative users (associated to the following TOE components: VBrain Configuration, VBrain Logger, VBrain Reporting) the access to the security related data stored in the DBs managed.</li></ul>

**Table 14: Rationale for Mapping of Threats, Policies, and Assumptions to Objectives**

## 5 EXTENDED COMPONENTS DEFINITION

[121] This Security Target does not include any extended components.

## 6 SECURITY REQUIREMENTS

[122] In this section the TOE security requirements are defined in terms of Security Functional Requirements (SFRs), specified according to conventions explained in section 1.4, and Security Assurance Requirement (SARs).

### 6.1. SECURITY FUNCTIONAL REQUIREMENTS

[123] The functional security requirements for this Security Target consist of the following components from Part 2 of the CC [CCP2], all of which are summarized in the following table detailing the operations that have been performed on the SFRs (A=Assignment, S=Selection, R=Refinement, I=Iteration).

		A	S	R	I
<b>FAU - Security Audit</b>					
FAU_GEN.1	Audit data generation	x	x		
FAU_GEN.2	User identity association				
FAU_SAR.1	Audit review	x			x
FAU_SAR.2	Restricted audit review				
FAU_SAR.3	Selectable audit review	x			
<b>FIA - Identification and authentication</b>					
FIA_UID.2	User identification before any action				
FIA_UAU.2	User authentication before any action				
FIA_UAU.6	Re-authenticating	x			
FIA_AFL.1	Authentication failure handling	x	x		x
FIA_ATD.1	User attribute definition	x			
FIA_SOS.1	Verification of secrets	x			
FIA_SOS.2	Generation of secrets	x			
<b>FTA – TOE Access</b>					
FTA_TSE.1	TOE session establishment	x			
FTA_SSL.4	User-initiated termination				
FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions	x			
<b>FDP – User Data Protection</b>					
FDP_ACC.1	Subset access control	x			
FDP_ACF.1	Security attribute based access control	x			
FDP_IFC.1	Subset information flow control	x			x
FDP_IFF.1	Simple security attributes	x			x
FDP_ITT.1	Basic internal transfer protection	x	x		
FDP_ETC.1	Export of user data without security attributes	x			
FDP_ITC.1	Import of user data without security attributes	x			
<b>FPT – Protection of the TSF</b>					
FPT_ITC.1	Confidentiality of exported TSF data				
FPT_TEE.1	Testing of external entities	x	x		x
FPT_ITT.1	Internal TOE TSF data transfer		x		
<b>FMT – Security management</b>					
FMT_SMR.1	Security Roles	x			
FMT_MOF.1	Management of security functions behavior	x	x		
FMT_SMF.1	Specification of Management Functions	x			
FMT_MSA.1	Management of security attributes	x	x		

		A	S	R	I
FMT_MSA.3	Static attribute initialization	x	x		

**Table 15: List of SFR and related operations**

[124] The rest of this section details the functional requirements taken from the catalog [CCP2], organized by functional families, and adapts them for this Security Target.

**6.1.1. SECURITY AUDIT (FAU)**

**SECURITY AUDIT DATA GENERATION (FAU\_GEN)**

**FAU\_GEN.1 Audit data generation**

**FAU\_GEN.1.1**

The TSF shall be able to generate an audit record of the following auditable events:

- a) start-up and shutdown of the audit functions;
- b) all auditable events for the not specified level of audit; and
- c) *auditable events defined in following table:*

<b>Auditable events managed by the TSF</b>	<b>Audit data stored in addition to:</b> <ul style="list-style-type: none"> <li>• <i>date and time of the event,</i></li> <li>• <i>type of event,</i></li> <li>• <i>subject identity (if applicable),</i></li> <li>• <i>outcome (success or failure) of the event</i></li> </ul>	<b>where the audit data are stored</b>
Command execution	Command information (§1.7.6, [103])	<i>runtime DB</i>
Acquired measures	Measure name, raw value, calculated value, alarm, condition	<i>runtime DB</i>
Warnings and alarms	Alarm information (§1.7.6, [103])	<i>runtime DB</i>
Alarm acknowledge	/	<i>runtime DB</i>
Measurement snooze	/	<i>runtime DB</i>
TOE user authentication	TOE component involved	<i>configuration DB log file Microsoft Windows Event Viewer</i>
TOE user locked	TOE component involved	<i>configuration DB log file</i>
TOE user password changed	TOE component involved	<i>configuration DB</i>
TOE new configuration download	/	<i>configuration DB log file</i>
TOE configuration version in use	/	<i>TOE Configuration folder name ConfigurationVersion.txt file</i>
User data management (creation, modification, deletion)	Data fields involved	<i>configuration DB log file</i>
Communication session (OPC-UA & HTTPS) opening/closure	/	<i>log file</i>
runtime DB backup restore on historian DB request (by VBrain Reporting)	/	<i>log file</i>

**Table 16: List of Auditable events managed by the TOE**

**Application Note:**

*Log file* consists of a number of files containing diagnostic information and errors related to the applications' operation and OPC-UA Client/Server communication.

More specifically, a log file is created for each VBrain application, which is managed by Vitrociset proprietary libraries, and a log file generated by the OPC-UA libraries. All log files are located in a specific folder of the VBrain applications' hosts, and are accessible only by OS System Administrators. Thereby, the folders' access control is managed by the OS.

#### **FAU\_GEN.1.2**

The TSF shall record within each audit record at least the following information:

- a) date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- b) for each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *none*.

#### **FAU\_GEN.2 User identity association**

##### **FAU\_GEN.2.1**

For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

#### **SECURITY AUDIT REVIEW (FAU\_SAR)**

##### **FAU\_SAR.1 Audit review**

###### **FAU\_SAR.1.1 (1) FR**

The TSF shall provide *users with role "Full Reader", "Acknowledger", "Commander" and "Configuration Administrator"* with the capability to read *all the stored data, excluding the TOE users' data*, from the audit records.

###### **FAU\_SAR.1.2**

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

##### **FAU\_SAR.1 Audit review**

###### **FAU\_SAR.1.1 (2) SA**

The TSF shall provide *users with role "System Administrator"* with the capability to read *all the stored data, including the TOE users' data*, from the audit records.

###### **FAU\_SAR.1.2**

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

##### **FAU\_SAR.2 Restricted audit review**

###### **FAU\_SAR.2.1**

The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

##### **FAU\_SAR.3 Selectable audit review**

###### **FAU\_SAR.3.1**

The TSF shall provide the ability to apply *searches* of audit data based on *time frame and/or date of the event and/or type of event and/or state of event and/or name of event*.

## 6.1.2. IDENTIFICATION AND AUTHENTICATION (FIA)

### USER IDENTIFICATION (FIA\_UID)

#### **FIA\_UID.2 User identification before any action**

##### **FIA\_UID.2.1**

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

### USER AUTHENTICATION (FIA\_UAU)

#### **FIA\_UAU.2 User authentication before any action**

##### **FIA\_UAU.2.1**

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

#### **FIA\_UAU.6 Re-authenticating**

##### **FIA\_UAU.6.1**

The TSF shall re-authenticate the user under the conditions *attempt to change the current password through VBrain Desktop Client HMI, VBrain Web Client HMI or VBrain Reporting HMI*.

#### **Application note:**

Re-authentication of a user that tries to access other applications through the links available on the VBrain Web Client HMI is not needed because VBrain Server is able to re-identify the user reusing the username provided for logging into the VBrain Web Client HMI. This is possible since the same HTTPS session is maintained.

### AUTHENTICATION FAILURE (FIA\_AFL)

#### **FIA\_AFL.1 Authentication failure handling**

##### **FIA\_AFL.1.1 (1) user with role different from System Administrator**

The TSF shall detect when three unsuccessful authentication attempts occur related to *consecutive instance of a TOE operator attempting to authenticate themselves on one of the following TOE components: VBrain Web Client HMI, VBrain Desktop Client HMI, VBrain Alarms List or VBrain Reporting HMI or consecutive instance of a TOE Configuration Administrator attempting to authenticate themselves on VBrain Configurator*.

##### **FIA\_AFL.1.2 (1) user with role different from System Administrator**

When the defined number of unsuccessful authentication attempts has been met, the TSF shall *lock the user account if the user role is different from System Administrator, otherwise log the authentication attempt*.

##### **FIA\_AFL.1.1 (2) user with System Administrator role**

The TSF shall detect when one unsuccessful authentication attempts occur related to *a TOE System Administrator attempting to authenticate themselves on one of the following TOE components: VBrain Web Client HMI, VBrain Desktop Client HMI, VBrain Alarms List or VBrain Reporting HMI or VBrain Configurator*.

##### **FIA\_AFL.1.2 (2) user with System Administrator role**

When the defined number of unsuccessful authentication attempts has been met, the TSF shall *log the unsuccessful authentication attempt*.

## **USER ATTRIBUTE DEFINITION (FIA\_ATD)**

### **FIA\_ATD.1 User attribute definition**

#### **FIA\_ATD.1.1**

The TSF shall maintain the following list of security attributes belonging to individual users:

- *user identity;*
- *password;*
- *list of Server IDs (IP addresses) on which a user is allowed to authenticate;*
- *role for each VBrain Server;*
- *groups;*
- *number of OPC-UA sessions opened for the specific user;*
- *attempts to login counter.*

## **SPECIFICATION OF SECRET (FIA\_SOS)**

### **FIA\_SOS.1 Verification of secrets**

#### **FIA\_SOS.1.1**

The TSF shall provide a mechanism to verify that secrets meet:

- *passwords minimal length: 10 characters;*
- *passwords contains at least 1 uppercase letter and at least 1 lowercase letter and at least 1 number and at least one of the following special characters: @ ? ! # \$ % & - = \_ + \*;*
- *new passwords must differ from previous password.*

### **FIA\_SOS.2 Generation of secrets**

#### **FIA\_SOS.2.1**

The TSF shall provide a mechanism to generate secrets that meet

- *passwords minimal length: 10 characters;*
- *passwords contains at least 7 integer numbers, 1 uppercase letter and at least 1 lowercase letter and one of the following special characters: @ ? ! # \$ % & - = \_ + \*;*
- *new passwords must differ from previous password.*

#### **FIA\_SOS.2.2**

The TSF shall be able to enforce the use of TSF generated secrets for *Identification and Authentication Security Function implemented by the following TOE components for first access of TOE users: VBrain Configurator, VBrain Desktop Client HMI, VBrain Alarms List, VBrain Reporting HMI, VBrain Web Client HMI.*



### **6.1.3. TOE ACCESS (FTA)**

#### **TOE SESSION ESTABLISHMENT (FTA\_TSE)**

##### **FTA\_TSE.1 TOE session establishment**

###### **FTA\_TSE.1.1**

The TSF shall be able to deny session establishment based on *number of OPC-UA sessions opened by the specific user*.

#### **SESSION LOCKING AND TERMINATION (FTA\_SSL)**

##### **FTA\_SSL.4 User-initiated termination**

###### **FTA\_SSL.4.1**

The TSF shall allow user-initiated termination of the user's own interactive session.

#### **LIMITATION ON MULTIPLE CONCURRENT SESSIONS (FTA\_MCS)**

##### **FTA\_MCS.2 Per user attribute limitation on multiple concurrent sessions**

###### **FTA\_MCS.2.1**

The TSF shall restrict the maximum number of concurrent **OPC-UA** sessions that belong to the same user according to the rule: *configurable maximum of concurrent OPC-UA sessions per user*.

###### **FTA\_MCS.2.2**

The TSF shall enforce, by default, a limit of *configurable number of OPC-UA* sessions per user.

**6.1.4. USER DATA PROTECTION (FDP)**

**ACCESS CONTROL POLICY (FDP\_ACC)**

**FDP\_ACC.1 Subset access control**

**FDP\_ACC.1.1**

The TSF shall enforce the *VBrain EMS access control SFP* on:

Subjects: *TOE users*;

Objects: *the following TOE components: VBrain Configurator, VBrain Desktop Client HMI, VBrain Web Client HMI, VBrain Alarms List, VBrain Reporting HMI*;

Operations among subjects and objects covered by the SFP: *as described in the third column of Table 17.*

SUBJECTS	SUBJECTS' ATTRIBUTES	RULES GOVERNING ACCESS AMONG CONTROLLED SUBJECTS AND CONTROLLED OBJECTS	OBJECTS	OBJECTS' ATTRIBUTES	ALLOWED OPERATIONS <i>The user shall access the functions offered by the OBJECT after providing a valid username and password. User privileges define operations the user can perform on the OBJECT.</i>
TOE users	User's role	User's role is <b>System Administrator</b>	VBrain Configurator	User privileges	operations allowed to Configuration Administrator + management of TOE Users & applicative users associated to TOE components which need to authenticate on DBMS and to open OPC-UA sessions + visualization of TOE user state (active/first access to be done/locked/number of failed login attempt)
	User's role	User's role is <b>Configuration Administrator</b>	VBrain Configurator (restricted access to VBrain Configurator functionalities)	User privileges	operations allowed to Commander + Creation and management of: Server/Client, acquisition drivers, measurements, commands, warnings, alarms, subscriptions and nodes, nodes treeview HMI panels configuration + DB parameters management and maintenance + Server certificates creation + TOE Configuration download and export to Hosts
	User's role + User's groups + List of VBrain Servers associated to the user + Number of OPC-UA session opened for the user	User's role is <b>Commander</b> + User is allowed to connect, after positive login, to the Server hosting VBrain Server configured to communicate with the specified OBJECTS + The same user is not already logged on another Server host + Less than configured OPC-UA sessions are opened for the user	VBrain Desktop Client HMI VBrain Web Client HMI VBrain Alarms List VBrain Reporting HMI	User privileges	operations allowed to Acknowledger + Commands operation, through the accessible HMI panels according to restrictions defined by System Administrator for the groups to which the user belongs
		User's role is <b>Acknowledger</b> + All other rules stated above		User privileges	operations allowed to Full Reader + Acknowledge operation on alarms and Snooze operation on measurements, according to restrictions defined by System Administrator for the groups to which the user belongs
		User's role is <b>Full Reader</b> + All other rules stated above		User privileges	operations allowed to Reader + Visualization of all historical measurements and alarms states, through the accessible HMI panels according to restrictions defined by System Administrator for the groups to which the user belongs.

SUBJECTS	SUBJECTS' ATTRIBUTES	RULES GOVERNING ACCESS AMONG CONTROLLED SUBJECTS AND CONTROLLED OBJECTS	OBJECTS	OBJECTS' ATTRIBUTES	ALLOWED OPERATIONS <i>The user shall access the functions offered by the OBJECT after providing a valid username and password. User privileges define operations the user can perform on the OBJECT.</i>
		User's role is <b>Reader</b> + All other rules stated above	VBrain Desktop Client HMI VBrain Web Client HMI VBrain Alarms List	User privileges	Visualization of all runtime measurements and alarms states, through the accessible HMI panels according to restrictions defined by System Administrator for the groups to which the user belongs

Table 17: VBrain EMS Access control policy

**ACCESS CONTROL FUNCTIONS (FDP\_ACF)**

**FDP\_ACF.1 Security attribute based access control**

**FDP\_ACF.1.1**

The TSF shall enforce the *VBrain EMS access control SFP* to objects based on the following: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes as specified in Table 17.*

**FDP\_ACF.1.2**

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects as specified in Table 17.*

**FDP\_ACF.1.3**

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none.*

**FDP\_ACF.1.4**

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *none.*

**INFORMATION FLOW CONTROL POLICY (FDP\_IFC)**

**FDP\_IFC.1 Subset information flow control**

**FDP\_IFC.1.1 (1) OPC-UA**

The TSF shall enforce the *OPC-UA information flow control SFP* on *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP as in the following table.*

**Application Note:**

All internal communications between VBrain Server component and other Client-type TOE components installed at Server-side (VBrain Server, VBrain Logger, VBrain Notifier, VBrain Alarms List, VBrain Desktop Client HMI, VBrain Web Socket Server) are based on OPC-UA protocol.

As well, the TOE may use the OPC-UA protocol also to communicate with some nodes in the FieldBus. This is also the case when the TOE interfaces another instance of the TOE itself in a multi-nodal architecture, as described in § 1.5.4.

Before an USER DATA exchange is possible via OPC-UA protocol, an OPC-UA session should be properly setup between sender and receiver that will exchange, in this case, specific session handling messages in order to setup, with the support of the environment, an encrypted communication between OPC-UA senders and receivers.

SUBJECT	SECURITY ATTRIBUTE	POSSIBLE VALUES
OPC-UA message	SUBJECT_TYPE	FIELDBUS NODE, TOE COMPONENT
	NODE_ID	NULL, VALID_NODE_ID in the list of NODEs monitored by the TOE (VBrain

<b>sender,</b>		Server)
<b>OPC-UA message receiver</b>	NODE_CONNECTED_PROTOCOL	OPC-UA, OPC, ADS, Modbus, SNMP, Milestone
	TOE_COMPONENT_ID	VBrain Server, VBrain Logger, VBrain Notifier, VBrain Desktop Client HMI, VBrain Alarms List, VBrain Web Socket Server
	OPC-UA type	Server-type, Client-type
<b>INFORMATION</b>	<b>SECURITY ATTRIBUTE</b>	<b>POSSIBLE VALUES</b>
<b>OPC-UA messages</b>	OPC-UA session ID	NULL/NOT NULL
<b>OPERATION</b>	<b>SECURITY ATTRIBUTE-BASED RELATIONSHIP BETWEEN SUBJECT SECURITY ATTRIBUTES AND INFORMATION SECURITY ATTRIBUTES</b>	
<b>OPC-UA message exchange between TOE COMPONENTS</b>	<p><b>The operation takes place if:</b></p> <p><b>OPC-UA session ID is NOT NULL AND {</b>                      OPC-UA message sender.SUBJECT_TYPE = TOE COMPONENT AND                      OPC-UA message sender.OPC-UA type = Server-type AND                      OPC-UA message sender.TOE_COMPONENT_ID = VBrain Server AND                      OPC-UA message receiver.SUBJECT_TYPE = TOE COMPONENT AND                      OPC-UA message receiver.OPC-UA type = Client-type AND                      OPC-UA message receiver.TOE_COMPONENT_ID = (VBrain Logger OR VBrain Notifier OR VBrain Desktop Client HMI OR VBrain Alarms List OR VBrain Web Socket Server) AND                      }  <b>OR</b>                      {                      OPC-UA message sender.SUBJECT_TYPE = TOE COMPONENT AND                      OPC-UA message sender.OPC-UA type = Client-type AND                      OPC-UA message sender.TOE_COMPONENT_ID = (VBrain Logger OR VBrain Notifier OR VBrain Desktop Client HMI OR VBrain Alarms List OR VBrain Web Socket Server) AND                      OPC-UA message receiver.SUBJECT_TYPE = TOE COMPONENT AND                      OPC-UA message receiver.OPC-UA type = Server-type AND                      OPC-UA message receiver.TOE_COMPONENT_ID = VBrain Server                      }</p>	
	<p>{                      OPC-UA message sender.SUBJECT_TYPE = FIELDBUS NODE AND                      OPC-UA message sender.OPC-UA type = Server-type AND                      OPC-UA message sender.NODE_ID = VALID_NODE_ID AND                      OPC-UA message sender.NODE_CONNECTED_PROTOCOL= OPC-UA AND                      OPC-UA message receiver.SUBJECT_TYPE = TOE COMPONENT AND                      OPC-UA message receiver.OPC-UA type = Client-type AND                      OPC-UA message receiver.TOE_COMPONENT_ID = VBrain Server                      }  <b>OR</b>                      {                      OPC-UA message sender.SUBJECT_TYPE = TOE COMPONENT AND                      OPC-UA message sender.OPC-UA type = Client-type AND                      OPC-UA message sender.TOE_COMPONENT_ID = VBrain Server AND                      OPC-UA message receiver.SUBJECT_TYPE = FIELDBUS NODE AND                      OPC-UA message receiver.OPC-UA type = Server-type AND                      OPC-UA message receiver.NODE_ID = VALID_NODE_ID AND                      OPC-UA message receiver.NODE_CONNECTED_PROTOCOL= OPC-UA                      }</p>	
<b>OPC-UA message exchange between TOE COMPONENT (VBrain Server) And FIELDBUS NODE</b>	<p>{                      OPC-UA message sender.SUBJECT_TYPE = FIELDBUS NODE AND                      OPC-UA message sender.OPC-UA type = Server-type AND                      OPC-UA message sender.NODE_ID = VALID_NODE_ID AND                      OPC-UA message sender.NODE_CONNECTED_PROTOCOL= OPC-UA AND                      OPC-UA message receiver.SUBJECT_TYPE = TOE COMPONENT AND                      OPC-UA message receiver.OPC-UA type = Client-type AND                      OPC-UA message receiver.TOE_COMPONENT_ID = VBrain Server                      }  <b>OR</b>                      {                      OPC-UA message sender.SUBJECT_TYPE = TOE COMPONENT AND                      OPC-UA message sender.OPC-UA type = Client-type AND                      OPC-UA message sender.TOE_COMPONENT_ID = VBrain Server AND                      OPC-UA message receiver.SUBJECT_TYPE = FIELDBUS NODE AND                      OPC-UA message receiver.OPC-UA type = Server-type AND                      OPC-UA message receiver.NODE_ID = VALID_NODE_ID AND                      OPC-UA message receiver.NODE_CONNECTED_PROTOCOL= OPC-UA                      }</p>	

**Table 18: OPC-UA information flow control policy**

**FDP\_IFC.1.1 (2) USER DATA**

The TSF shall enforce the *USER DATA information flow control SFP* on *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP as in the following table.*

**Application Note:**

The TOE (VBrain Server component) will receive updates form monitored devices/sites (i.e. nodes) in the FieldBus, through specific drivers, in terms of measures/warnings/alarms and it will send them commands (or sequence of commands).

If the TOE (VBrain Server component) does not acquire any data from a FieldBus child node for a (configurable) time it deduces that the child node status and the parent node master status is BAD\_ACQUISITION (connection loss). In this case, the proper DRIVER component will start trying to re-establish the connection with the child node.

When the connection is recovered, the child node will send its last acquired measure to the TOE.

The TOE (VBrain Server component) will also receive warning/alarm Acknowledges and/or measurement Snoozes upon TOE authorized users actions on VBrain Alarms list or a VBrain Client HMI.

Furthermore, the TOE (VBrain Server component) will receive Commands results from FieldBus nodes.

Each node is seen by the TOE (VBrain Server component) as a logical aggregation of each measure acquired by its child nodes that compose it.

Each child node acquired measure [stored by VBrain in (LIST OF) CHILD NODE'S CURRENT\_MEASURE] is updated upon a variation received from the FieldBus (i.e., when a CHILD NODE'S ACQUIRED\_MEASURE differs from CHILD NODE'S CURRENT\_MEASURE stored in VBrain Server and VBrain Server (LIST OF) CHILD NODE'S CHANGED\_MEASURE is updated).

In the following table, the security attributes relevant for the USER DATA INFORMATION FLOW CONTROL POLICIES enforced by the TOE are represented.

In the following:

- the notation **NODE<sub>n</sub>** indicates the n-nth NODE monitored by the TOE;
- the notation **NODE<sub>n,m</sub>** indicates the m-nth CHILD-NODE of **NODE<sub>n</sub>** monitored by the TOE;
- the notation **VBrain Client HMI** indicates either VBrain Desktop Client HMI or VBrain Web Client HMI.

SUBJECT	SECURITY ATTRIBUTE	POSSIBLE VALUES
<b>FIELDBUS NODE</b>	MASTER_STATUS (OR logical function of each measure status associated to each child node related to each device/site monitored by the TOE). If one of the CHILD NODEs is unreachable, the master status of the parent NODE is set to BAD_ACQUISITION ) (LIST OF) CHILD NODE'S ACQUIRED_MEASURE	GOOD NOT_ACQUIRED BAD_ACQUISITION (i.e., connection loss)
	COMMAND_RESULT	NULL, NOT NULL (valid result code is retrieved)
	(LIST OF) NODE'S CHANGED_MASTER_STATUS	TRUE/FALSE
<b>VBrain Server</b> (For each monitored NODE)	(LIST OF) CHILD NODE'S CHANGED_VALUE	TRUE/FALSE
	(LIST OF) CHILD NODE'S CURRENT_MEASURE	See details for measures
	(LIST OF) CHILD NODE'S PROTOCOL	NULL, OPC-UA, OPC, ADS, Modbus, SNMP, Milestone
	(LIST OF) CHILD NODE'S COMMAND_RESULT_RECEIVED	TRUE/FALSE
	(LIST OF) CHILD NODE'S COMMAND_USERNAME	VALID/NOT VALID
	CONNECTED_USER_CREDENTIALS	VALID/NOT VALID
<b>VBrain Client HMI</b>	AUTHORIZED_USER	TRUE/FALSE according to access control policy
	COMMAND_TO_BE_SENT	TRUE/FALSE
	ACK_TO_BE_SENT	TRUE/FALSE
	SNZ_TO_BE_SENT	TRUE/FALSE
	CONNECTED_USER_CREDENTIALS	VALID/NOT VALID
<b>VBrain Reporting HMI</b>	AUTHORIZED_USER	TRUE/FALSE according to access control policy
	RUNTIMEDB_CHOSEN	TRUE/FALSE
	HISTORIADB_CHOSEN	TRUE/FALSE
	RUNTIMEDB_BKPFIL CHOSEN	TRUE/FALSE
	CONNECTED_USER_CREDENTIALS	VALID/NOT VALID
<b>VBrain Alarms List</b>	AUTHORIZED_USER	TRUE/FALSE according to access control policy

	ACK_TO_BE_SENT	TRUE/FALSE
	SNZ_TO_BE_SENT	TRUE/FALSE
<b>VBrain Notifier</b>	CONFIGURED_NOTIFICATION_RECEIVER	TRUE/FALSE
<i>runtime DB</i>	/	/
<i>historian DB</i>	/	/
<i>configuration DB</i>	/	/
<b>INFORMATION</b> Related to CHILD NODEs	<b>SECURITY ATTRIBUTE</b>	<b>POSSIBLE VALUES</b>
<b>MEASURE</b>	CONDITION	NORMAL WARNING ALARM
	ON	TRUE/FALSE
	ALARM_ACK	ACK/NACK
	SNOOZED	TRUE/FALSE
	TO_LOG	TRUE/FALSE
	TO_NOTIFY	TRUE/FALSE
<b>COMMAND</b>	NAME	ONE OF THE CONFIGURED COMMAND IDENTIFIERS
	USERNAME	USER's CREDENTIALs
	RESULT	NO_RESULT/RESULT CODEs
<b>OPERATION</b>	<b>SECURITY ATTRIBUTE-BASED RELATIONSHIP BETWEEN SUBJECT SECURITY ATTRIBUTES AND INFORMATION SECURITY ATTRIBUTES</b>	<b>NOTES</b>
<b>MEASURE shown on VBrain Client HMI</b>	<p><b>The operation takes place if:</b>                      (FIELD BUS NODE [NODE<sub>n</sub>]. MASTER STATUS = GOOD AND VBrain Server[NODE<sub>n:m</sub>].CHANGED_VALUE = TRUE)  <b>OR</b>                      (VBrain Server[NODE<sub>n</sub>].CHANGED_MASTER STATUS = TRUE) <b>AND</b>                      VBrain Server[NODE<sub>n:m</sub>].CURRENT_MEASURE.ON = TRUE  <b>AND</b>                      VBrain Alarms List.CONNECTED_USER's CREDENTIALs = VALID <b>AND</b>                      VBrain Alarms List.AUTHORIZED_USER = TRUE</p>	A CHILD NODE measure variation acquired from FIELD BUS is shown on VBrain Client HMI if it has been configured to be acquired and the user has the rights to see it according to access control policy.
<b>MEASURE logged on runtime DB (by VBrain Logger)</b>	<p><b>The operation takes place if:</b>                      (FIELD BUS NODE [NODE<sub>n</sub>]. MASTER STATUS = GOOD AND VBrain Server[NODE<sub>n:m</sub>].CHANGED_VALUE = TRUE)  <b>OR</b>                      (VBrain Server[NODE<sub>n</sub>].CHANGED_MASTER STATUS = TRUE) <b>AND</b>                      VBrain Server[NODE<sub>n:m</sub>].CURRENT_MEASURE.ON = TRUE                      VBrain Server[NODE<sub>n:m</sub>].CURRENT_MEASURE.TO_LOG = TRUE</p>	A CHILD NODE measure variation acquired from FIELD BUS is logged on runtime DB if it has been configured to be logged.
<b>ALARM/WARNING updated on VBrain Alarms List and/or VBrain Client HMI for the connected user</b>	<p><b>The operation takes place if:</b>                      FIELD BUS NODE [NODE<sub>n</sub>]. MASTER STATUS = GOOD <b>AND</b>                      VBrain Server[NODE<sub>n:m</sub>].CHANGED_VALUE = TRUE <b>AND</b>                      VBrain Server[NODE<sub>n:m</sub>].CURRENT_MEASURE.ON = TRUE <b>AND</b>                      VBrain Server[NODE<sub>n:m</sub>].CURRENT_MEASURE.ON = TRUE <b>AND</b>                      VBrain Server[NODE<sub>n:m</sub>].CONDITION = (WARNING OR ALARM) <b>AND</b>{                      VBrain Alarms List.CONNECTED_USER's CREDENTIALs = VALID <b>AND</b>                      VBrain Alarms List.AUTHORIZED_USER = TRUE                      }  <b>AND</b>                      {                      VBrain Client HMI.CONNECTED_USER's CREDENTIALs = VALID <b>AND</b>                      VBrain Client HMI.AUTHORIZED_USER = TRUE <b>AND</b>                      }                      }</p>	A CHILD NODE measure variation acquired from FIELD BUS triggers an alarm/warning that is displayed in VBrain Alarm List and/or VBrain Client HMI for the connected user, if he has the rights to see it according to access control policy.
<b>MEASURE notified externally to configured i-nth receiver (print/mobile phone/email service)</b>	<p><b>The operation takes place if:</b>                      (FIELD BUS NODE [NODE<sub>n</sub>]. MASTER STATUS = GOOD AND VBrain Server[NODE<sub>n:m</sub>].CHANGED_VALUE = TRUE)  <b>OR</b>                      (VBrain Server[NODE<sub>n</sub>].CHANGED_MASTER STATUS = TRUE) <b>AND</b>                      VBrain Server[NODE<sub>n:m</sub>].CURRENT_MEASURE.ON = TRUE  <b>AND</b></p>	A CHILD NODE measure variation acquired from FIELD BUS is notified externally to the i-nth device configured as a "notification_receiver" for that measure.

	<p>VBrain Server[NODE<sub>n:m</sub>].CURRENT_MEASURE.TO_NOTIFY = TRUE  <b>AND</b>  VBrain Notifier.CONFIGURED_NOTIFICATION_RECEIVER[i] is TRUE</p>	
<p><b>ALARM/WARNING notified internally on VBrain Client HMI</b></p>	<p><b>The operation takes place if:</b>  FIELD BUS NODE [NODE<sub>n</sub>]. MASTER STATUS = GOOD <b>AND</b>  VBrain Server[NODE<sub>n:m</sub>].CHANGED_VALUE = TRUE <b>AND</b>  VBrain Server[NODE<sub>n:m</sub>].CURRENT_MEASURE.ON = TRUE <b>AND</b>  VBrain Server[NODE<sub>n:m</sub>].CONDITION = (WARNING OR ALARM) <b>AND</b>  VBrain Client HMI.CONNECTED_USER's CREDENTIALS = VALID <b>AND</b>  VBrain Client HMI.AUTHORIZED_USER = TRUE</p>	<p>A CHILD NODE measure variation acquired from FIELD BUS triggers an alarm/warning that is notified internally in the VBrain Client HMI (for the connected authorized user)</p>
<p><b>ALARM/WARNING notified externally to configured i-nth receiver (print/mobile phone/email service)</b></p>	<p><b>The operation takes place if:</b>  FIELD BUS NODE [NODE<sub>n</sub>]. MASTER STATUS = GOOD <b>AND</b>  VBrain Server[NODE<sub>n:m</sub>].CURRENT_MEASURE.ON = TRUE <b>AND</b>  VBrain Server[NODE<sub>n:m</sub>].CURRENT_MEASURE.SNOOZED = FALSE <b>AND</b>  VBrain Server[NODE<sub>n:m</sub>].CONDITION = (WARNING OR ALARM) <b>AND</b>  VBrain Server[NODE<sub>n:m</sub>].CHANGED_VALUE = TRUE <b>AND</b>  VBrain Server[NODE<sub>n:m</sub>].CURRENT_MEASURE.TO_NOTIFY = TRUE <b>AND</b>  VBrain Notifier.CONFIGURED_NOTIFICATION_RECEIVER[i] is TRUE</p>	<p>A CHILD NODE measure variation acquired from FIELD BUS triggers an alarm/warning that is notified externally to the i-nth device configured as a "notification_receiver" for that alarm/warning.</p>
<p><b>ALARM ACK logged on runtime DB (by VBrain Logger)</b></p>	<p><b>The operation takes place if:</b>  FIELD BUS NODE [NODE<sub>n</sub>]. MASTER STATUS = GOOD <b>AND</b>  VBrain Server[NODE<sub>n:m</sub>].CHANGED_VALUE = TRUE <b>AND</b>  VBrain Server[NODE<sub>n:m</sub>].CURRENT_MEASURE.TO_LOG = TRUE <b>AND</b>  VBrain Server[NODE<sub>n:m</sub>].CURRENT_MEASURE.CONDITION = (ALARM OR WARNING)  <b>AND</b>  VBrain Server[NODE<sub>n:m</sub>].CURRENT_MEASURE.ALARM_ACK = NACK  <b>AND</b>  {  VBrain Alarms List.CONNECTED_USER's CREDENTIALS = VALID <b>AND</b>  VBrain Alarms List.AUTHORIZED_USER = TRUE <b>AND</b>  VBrain Alarms List.ACK_TO_BE_SENT = TRUE  }  <b>OR</b>  {  VBrain Client HMI.CONNECTED_USER's CREDENTIALS = VALID <b>AND</b>  VBrain Client HMI.AUTHORIZED_USER = TRUE <b>AND</b>  VBrain Client HMI.ACK_TO_BE_SENT = TRUE  }</p>	<p>When A CHILD NODE measure variation acquired from FIELD BUS triggers an alarm/warning that should be acknowledged, if VBrain Server receives an acknowledge from an authorized user operating through VBrain Client HMI or VBrain Alarm List, the alarm ACK is accepted and it is logged on <i>runtime DB</i> by VBrain Logger, upon a request from VBrain Server.</p>
<p><b>SNOOZE logged on runtime DB (by VBrain Logger)</b></p>	<p><b>The operation takes place if:</b>  FIELD BUS NODE [NODE<sub>n</sub>]. MASTER STATUS = GOOD <b>AND</b>  VBrain Server[NODE<sub>n:m</sub>].CURRENT_MEASURE.TO_LOG = TRUE <b>AND</b>  <b>AND</b>  {  VBrain Alarms List.CONNECTED_USER's CREDENTIALS = VALID <b>AND</b>  VBrain Alarms List.AUTHORIZED_USER = TRUE <b>AND</b>  VBrain Alarms List.SNZ_TO_BE_SENT = TRUE  }  <b>OR</b>  {  VBrain Client HMI.CONNECTED_USER's CREDENTIALS = VALID <b>AND</b>  VBrain Client HMI.AUTHORIZED_USER = TRUE <b>AND</b>  VBrain Client HMI.SNZ_TO_BE_SENT = TRUE  }</p>	<p>If VBrain Server receives a measurement snooze request from an authorized user operating through VBrain Client HMI or VBrain Alarm List, the measurement SNOOZE is accepted and it is logged on <i>runtime DB</i> by VBrain Logger, upon a request from VBrain Server.</p>
<p><b>COMMAND EXECUTION REQUEST to FIELD BUS CHILD NODES</b></p>	<p><b>The operation takes place if:</b>  VBrain Client HMI.CONNECTED_USER's CREDENTIALS = VALID <b>AND</b>  VBrain Client HMI.AUTHORIZED_USER = TRUE <b>AND</b>  VBrain Client HMI.COMMAND_TO_BE_SENT = TRUE <b>AND</b>  VBrain Server[NODE<sub>n:m</sub>].COMMAND_USERNAME[COMMAND.NAME] = VALID <b>AND</b>  VBrain Server[NODE<sub>n</sub>].CHANGED_MASTER_STATUS = FALSE <b>AND</b>  FIELD BUS NODE<sub>n</sub>.MASTER_STATUS IS NOT (BAD_ACQUISITION OR NOT_ACQUIRED)</p>	<p>VBrain Server sends a command execution request to a FIELD BUS CHILD NODE if it receives a valid command request from an authorized user and the status of the connection with the CHILD NODE is available.</p>
<p><b>EXECUTED COMMAND logged on runtime DB</b></p>	<p><b>The operation takes place if:</b>  VBrain Server.COMMAND_RESULT_RECEIVED[NODE<sub>n:m</sub>] = TRUE <b>AND</b></p>	<p>When VBrain Server receives a valid command result from</p>

(by VBrain Logger)	FIELD BUS NODE <sub>n,m</sub> .COMMAND_RESULT IS NOT NULL (VALID RESULT CODE is retrieved to VBrain Server)	a CHILD NODE, it asks VBrain Logger to log on <i>runtime DB</i> the data related to the executed command .
<b>DATA</b> (ACQUIRED MEASURES/WARNINGS/ALARMS/EXECUTED COMMANDS) <b>RETRIEVAL FROM runtime DB</b> (by VBrain Reporting)	<b>The operation takes place if:</b> VBrain Reporting HMI.CONNECTED_USER's CREDENTIALS = VALID <b>AND</b> VBrain Reporting HMI.AUTHORIZED_USER = TRUE AND VBrain Reporting HMI.RUNTIMEDB_CHOSEN = TRUE	DATA (acquired measures/warnings/alarms/ executed commands) are retrieved from <i>runtime DB</i> by VBrain Reporting when requested by an authorized user who chooses the <i>runtime DB</i> as the source for data retrieval.
<b>DATA</b> (ACQUIRED MEASURES/WARNINGS/ALARMS/EXECUTED COMMANDS) <b>RETRIEVAL FROM historian DB</b> (by VBrain Reporting)	<b>The operation takes place if:</b> VBrain Reporting HMI.CONNECTED_USER's CREDENTIALS = VALID <b>AND</b> VBrain Reporting HMI.AUTHORIZED_USER = TRUE AND VBrain Reporting HMI.HISTORIANDB_CHOSEN = TRUE AND VBrain Reporting HMI. RUNTIMEDB_BKPFILFILE_CHOSEN = TRUE	DATA (acquired measures/warnings/alarms/executed commands) are retrieved from <i>historian DB</i> by VBrain Reporting when requested by an authorized user who chooses a previous <i>runtime DB</i> backup as the source for data retrieval among those available in VBrain Reporting HMI.

**Table 19: USER DATA Information Flow Control Policy Specification**

**INFORMATION FLOW CONTROL FUNCTIONS (FDP\_ IFF)**

**FDP\_ IFF.1 Simple security attributes (1) OPC\_UA**

**FDP\_ IFF.1.1 (1) OPC\_UA**

The TSF shall enforce the *OPC-UA information flow control SFP* based on the following types of subject and information security attributes: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes as listed in Table 18.*

**FDP\_ IFF.1.2 (1) OPC\_UA**

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes as described in Table 18.*

**FDP\_ IFF.1.3 (1) OPC\_UA**

The TSF shall enforce the *none (no additional information flow control SFP rules).*

**FDP\_ IFF.1.4 (1) OPC\_UA**

The TSF shall explicitly authorize an information flow based on the following rules: *none.*

**FDP\_ IFF.1.5 (1) OPC\_UA**

The TSF shall explicitly deny an information flow based on the following rules: *none.*

**FDP\_ IFF.1 Simple security attributes (2) USER DATA**

**FDP\_ IFF.1.1 (2) USER DATA**

The TSF shall enforce the *USER DATA information flow control SFP* based on the following types of subject and information security attributes: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes as listed in Table 19.*



### **FDP\_IFF.1.2 (2) USER DATA**

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes as described in Table 19.*

### **FDP\_IFF.1.3 (2) USER DATA**

The TSF shall enforce the *none (no additional information flow control SFP rules).*

### **FDP\_IFF.1.4 (2) USER DATA**

The TSF shall explicitly authorize an information flow based on the following rules: *none.*

### **FDP\_IFF.1.5 (2) USER DATA**

The TSF shall explicitly deny an information flow based on the following rules: *none.*

## **INTERNAL TOE TRANSFER (FDP\_ITT)**

### **FDP\_ITT.1 Basic internal transfer protection**

#### **FDP\_ITT.1.1**

The TSF shall enforce the *OPC-UA information flow control SFP* to prevent the [disclosure, modification, loss of use](#) of user data when it is transmitted between physically-separated parts of the TOE.

#### **Application Note:**

All internal communications between VBrain Server component and other OPC-UA Client-type TOE components (VBrain Server, VBrain Logger, VBrain Notifier, VBrain Alarms List, VBrain Desktop Client HMI, VBrain Web Socket Server) are based on OPC-UA protocol with:

- *SecurityLevel = 3;*
- *SecurityMode = Sign&Encrypt* i.e., each message exchanged between above mentioned TOE components is signed and encrypted. The Operational environment (OE.CRYPTO) provides the TOE with AES 128 bit encryption and cryptographic key generation;
- *SecurityPolicyUri = Basic128Rsa15;*
- *TransportProfileUri = WsHttpXmlOrBinaryTransport.*

## **EXPORT FROM THE TOE (FDP\_ETC)**

### **FDP\_ETC.1 Export of user data without security attributes**

#### **FDP\_ETC.1.1**

The TSF shall enforce the *USER DATA information flow control SFP* when exporting user data, controlled under the SFP(s), outside of the TOE.

#### **FDP\_ETC.1.2**

The TSF shall export the user data without the user data's associated security attributes.

#### **Application Note:**

User data exported outside the TOE (i.e., logged on *runtime DB* and an *historian DB*) are:

- measures/warnings/alarms acquired from FieldBus monitored NODES and;
- command executed on FieldBus monitored NODES and;
- acknowledged alarms;
- snoozed measurements.

**IMPORT FROM OUTSIDE OF THE TOE (FDP\_ITC)****FDP\_ITC.1 Import of user data without security attributes****FDP\_ITC.1.1**

The TSF shall enforce the *VBrain EMS information flow control SFP* when importing user data, controlled under the SFP, from outside of the TOE.

**FDP\_ITC.1.2**

The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

**FDP\_ITC.1.3**

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: *none*.

**Application Note:**

User data imported from outside the TOE are:

- measures/warnings/alarms acquired from FieldBus monitored NODES and;
- user data retrieved from *runtime DB* and from *historian DB* onto VBrain Reporting HMI (through VBrain Reporting).

**6.1.5. PROTECTION OF THE TSF (FPT)****CONFIDENTIALITY OF EXPORTED TSF DATA (FPT\_ITC)****FPT\_ITC.1 Inter-TSF confidentiality during transmission****FPT\_ITC.1.1**

The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorized disclosure during transmission.

**Application Note:**

The SFR refers to TOE user credentials and TOE configurations protection:

- The hash of a TOE user's password (the hash is generated with the support of the Operational environment) is exported to the *configuration DB* (from VBrain Reporting HMI or VBrain Alarms List or VBrain Client HMI or VBrain Configurator upon a password change requested by a TOE user);
- An encrypted JSON/XML file (encrypted with the support of the Operational environment) is exported to a specific directory of the Operating System (from VBrain Configurator) when the download of a new configuration for a TOE component is requested by an authorized TOE administrator.

**INTERNAL TOE TSF DATA TRANSFER (FPT\_ITT)****FPT\_ITT.1 Basic internal TSF data transfer protection****FPT\_ITT.1.1**

The TSF shall protect TSF data from disclosure, modification when it is transmitted between separate parts of the TOE.

**TESTING OF EXTERNAL ENTITIES (FPT\_TEE)****FPT\_TEE.1 Testing of external entities (1) DBMS****FPT\_TEE.1.1 (1) DBMS**

The TSF shall run a suite of tests at the first launch of VBrain Logger and periodically during normal operation to check the fulfillment of *the following condition: the runtime DB has not reached the maximum configured size or the last backup of the runtime DB is not older than a configurable number of days*.

**FPT\_TEE.1.2 (1) DBMS**

If the test fails, the TSF shall (*VBrain Logger*) ask the DBMS to:

- *save data stored in the runtime DB in a backup file in the runtime DB backup folder;*
- *delete the oldest half of the records inside the runtime DB.*

**FPT\_TEE.1 Testing of external entities (2) OS**

**FPT\_TEE.1.1 (2) OS**

The TSF shall run a suite of tests periodically during normal operation to check the fulfillment of *the following condition: the runtime DB backup folder managed by the Operating System has not reached the maximum configured size.*

**FPT\_TEE.1.2 (2) OS**

If the test fails, the TSF shall (*VBrain Logger*) ask the OS to delete the oldest runtime DB backup file.

**6.1.6. SECURITY MANAGEMENT (FMT)**

**SECURITY MANAGEMENT ROLES (FMT\_SMR)**

**FMT\_SMR.1 Security roles**

**FMT\_SMR.1.1**

The TSF shall maintain the roles *System Administrator, Configuration Administrator, Commander, Acknowledger, Full Reader, Reader.*

**FMT\_SMR.1.2**

The TSF shall be able to associate users with roles.

**MANAGEMENT OF FUNCTIONS IN TSF (FMT\_MOF)**

**FMT\_MOF.1 Management of security functions behavior**

**FMT\_MOF.1.1**

The TSF shall restrict the ability to determine the behavior of, disable, enable, modify the behavior of the functions *defined in Table 20* to *TOE authorized administrators.*

**SPECIFICATION OF MANAGEMENT FUNCTIONS (FMT\_SMF)**

**FMT\_SMF.1 Specification of Management Functions**

**FMT\_SMF.1.1**

The TSF shall be capable of performing the following management functions: *list of management functions defined in the following table:*

MANAGEMENT FUNCTIONS
Maintenance (deletion, modification, addition) of the group of users with read access right to the audit records
Management of the user identities
Management of the number of allowed OPC-UA sessions for user
Management of the authentication data by an administrator
Management of the authentication data by the user associated with this data
Managing the group of roles that can interact with the functions in the TSF
Managing the group of roles that can interact with the security attributes
Management of the <i>runtime DB</i> backup time

MANAGEMENT FUNCTIONS
Management of the <i>runtime DB</i> backup frequency
Management of the maximum size that could be reached by <i>runtime DB</i>
Management of the maximum size that could be reached by <i>runtime DB</i> backup folder
Create and set up one or more Servers and Clients configurations
Configure the drivers and threads for communication with the field devices
Create and configure the acquired measures, generated commands and alarms
Publish the measures, commands and alarms made available through the Client HMIs
Configure the OPC-UA Client/Server communication channels
Save, delete and export the configurations
Create and manage Server certificates

**Table 20: VBrain EMS Management functions**

**MANAGEMENT OF SECURITY ATTRIBUTES (FMT\_MSA)**

**FMT\_MSA.1 Management of security attributes**

**FMT\_MSA.1.1**

The TSF shall enforce the *VBrain access control SFP to restrict the ability to [change default, query, modify, delete, \[Monitor, Manage, Perform\]](#) the security attributes [defined in the following table](#) to the authorized roles identified in the following table.*

AUTHORISED ROLES	ABILITY TO	SECURITY ATTRIBUTE
System Administrator	Change default, modify, delete	Users (TOE Administrators and Operators) credentials
	Change default, query, modify, delete	Operator Servers assignment, operators roles, allowed OPC-UA sessions
Configuration Administrator	Change default, modify, delete	Measurements, alarms and commands configuration, Server/Client configuration, data acquisition channel configuration, HMI panels configuration, operators groups
Commander	Manage/Perform	Commands, alarms acknowledge and measurements snooze
Acknowledger	Manage/Perform	Alarms acknowledge and measurements snooze
Full Reader	Monitor	All runtime and historical data
Reader	Monitor	All runtime data

**Table 21: Permissions granted to each user role**

**FMT\_MSA.3 Static attribute initialization**

**FMT\_MSA.3.1**

The TSF shall enforce the *VBrain EMS access control SFP* to provide permissive default values for security attributes that are used to enforce the SFP.

**FMT\_MSA.3.1**

The TSF shall allow the *TOE authorized administrators* to specify alternative initial values to override the default values when an object or information is created.

## 6.2. SECURITY ASSURANCE REQUIREMENTS

[125] The assurance security requirements for this Security Target are taken from Part 3 of the CC according to [CCP3] Table 3. These assurance requirements compose an Evaluation Assurance Level 1 (EAL1) augmented by ASE\_SPD.1, ASE\_REQ.2, ASE\_OBJ.2, ALC\_FLR.1 (EAL1+). SAR dependencies are satisfied since, according to table 20 of [CCP3] and according to ALC\_FLR.1 description at page 143 of [CCP3]:

SAR	DEPENDENCY	RATIONALE
ASE_SPD.1	none	none
ASE_REQ.2	ASE_ECD.1 ASE_OBJ.2	Satisfied since ASE_ECD.1 is included in EAL1 package while ASE_OBJ.2 has been included among the augmentations considered vs EAL1
ASE_OBJ.2	ASE_REQ.2	Satisfied including ASE_REQ.2 among the augmentations considered vs EAL1
ALC_FLR.1	none	none

[126] EAL1+ is chosen because the TOE is supposed to be used in an Operational Environment in which the attack potential of an attacker is BASIC.

[127] The following table describes the security assurance requirements:

CLASS HEADING	CLASS FAMILY	DESCRIPTION
<b>ADV: Development</b>	ADV_FSP.1	Basic functional specification
<b>AGD: Guidance documentation</b>	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
<b>ALC: Life-cycle support</b>	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
	ALC_FLR.1	Basic flaw remediation
<b>ASE: Security Target Evaluation</b>	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended component definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE summary specification
<b>ATE: Tests</b>	ATE_IND.1	Independent testing - conformance
<b>AVA: Vulnerability assessment</b>	AVA_VAN.1	Vulnerability survey

Table 22: Security Assurance Requirements

### 6.3. SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

#### 6.3.1. CC Component Dependencies

[128] This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies.

[129] The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

SFR	DEPENDENCY	RATIONALE
FAU_GEN.1	FPT_STM.1	Satisfied by OE.TIME in the environment
FAU_GEN.2	FAU_GEN.1	Satisfied
	FIA_UID.1	Satisfied by FIA_UID.2, hierarchical to FIA_UID.1
FAU_SAR.1	FAU_GEN.1	Satisfied
FAU_SAR.2	FAU_SAR.1	Satisfied
FAU_SAR.3	FAU_SAR.1	Satisfied
FIA_UID.2	-	-
FIA_UAU.2	FIA_UID.1	Satisfied by FIA_UID.2, hierarchical to FIA_UID.1
FIA_UAU.6	-	-
FIA_AFL.1	FIA_UAU.1	Satisfied by FIA_UAU.2, hierarchical to FIA_UAU.1
FIA_ATD.1	-	-
FIA_SOS.1	-	-
FIA_SOS.2	-	-
FTA_TSE.1	-	-
FTA_SSL.4	-	-
FTA_MCS.2	FIA_UID.1	Satisfied by FIA_UID.2, hierarchical to FIA_UID.1
FDP_ACC.1	FDP_ACF.1	Satisfied
FDP_ACF.1	FDP_ACC.1	Satisfied
	FMT_MSA.3	Satisfied
FDP_IFC.1	FDP_IFF.1	Satisfied
FDP_IFF.1	FDP_IFC.1	Satisfied
	FMT_MSA.3	Satisfied
FDP_ITT.1	FDP_ACC1.1 or FDP_IFC.1	Satisfied by FDP_IFC.1
FDP_ETC.1	FDP_ACC1.1 or FDP_IFC.1	Satisfied by FDP_IFC.1
FDP_ITC.1	FDP_ACC1.1 or FDP_IFC.1	Satisfied by FDP_IFC.1
	FMT_MSA.3	Satisfied
FPT_ITC.1	-	-
FPT_TEE.1	-	-
FPT_ITT.1	-	-
FMT_SMR.1	FIA_UID.1	Satisfied by FIA_UID.2, hierarchical to FIA_UID.1
FMT_MOF.1	FMT_SMR.1	Satisfied
	FMT_SMF.1	Satisfied
FMT_SMF.1	-	-
FMT_MSA.1	FMT_SMF.1	Satisfied
	FMT_SMR.1	Satisfied
	FDP_ACC.1	Satisfied
FMT_MSA.3	FMT_MSA.1	Satisfied
	FMT_SMR.1	Satisfied

**Table 23: TOE SFR dependency rationale**

6.3.2. Tracing between SFRs and the security objectives for the TOE

SFR/O	O.CONFIG	O.USER	O.IDENTIFY	O.ANTI_BRUTE	O.ACCESS	O.SECOM	O.REPLAY	O.CRASH	O.AVAIL	O.AUDIT	O.MANAGE	O.EXHAUST	O.SESSION
FAU_GEN.1										x			
FAU_GEN.2										x			
FAU_SAR.1										x			
FAU_SAR.2										x			
FAU_SAR.3										x			
FIA_UID.2			x										
FIA_UAU.2			x										
FIA_UAU.6			x										
FIA_AFL.1				x									
FIA_ATD.1			x										
FIA_SOS.1			x										
FIA_SOS.2			x										
FTA_TSE.1													x
FTA_SSL.4													x
FTA_MCS.2													x
FDP_ACC.1		x			x								
FDP_ACF.1		x			x								
FDP_IFC.1						x	x		x				
FDP_IFF.1						x			x				
FDP_ITT.1						x							
FDP_ETC.1								x					
FDP_ITC.1								x					
FPT_ITC.1								x					
FPT_TEE.1												x	
FPT_ITT.1						x							
FMT_SMR.1											x		
FMT_MOF.1											x		
FMT_SMF.1	x										x		
FMT_MSA.1	x				x								
FMT_MSA.3	x				x								

Table 24: Mapping of TOE SFRs to Security Objectives

[130] The following table provides detailed evidence of coverage for each security objective.



OBJECTIVE	RATIONALE
<b>O.CONFIG</b>	<p>The TSF is capable of performing a set of management functions, including those to configure the TOE, to change and make effective the configuration of the TOE when it is in RUNNING state [FMT_SMF.1].</p> <p>The TSF enforces the VBrain access control SFP to restrict the ability to change the configuration of the TOE only to the System Administrator and Configuration Administrator [FMT_MSA.1], [FMT_MSA.3].</p>
<b>O.USER</b>	<p>The TSF enforces a VBrain EMS access control SFP on TOE users allowing only the System Administrator to create and delete users, and to assign them the list of (one or more) Servers he is allowed to access, a specific user role for the specific Server, and the limit number of OPC-UA sessions the TOE user is allowed to open. In addition, only a TOE administrator is allowed to assign to the users one or more groups, limiting their access to the HMI panels [FDP_ACC.1], [FDP_ACF.1].</p>
<b>O.IDENTIFY</b>	<p>The TSF requires each user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that user [FIA_UID.2], [FIA_UAU.2].</p> <p>The TSF shall re-authenticate the user under the following condition: attempt to change the current password through VBrain Desktop Client HMI, VBrain Web Client HMI or VBrain Reporting HMI [FIA_UAU.6].</p> <p>The TSF shall maintain a set of security attributes belonging to individual users, among which the User identity and Password required for identification [FIA_ATD.1].</p> <p>The TSF shall provide a mechanism to verify that secrets meet certain levels of complexity. The TSF shall be able to enforce the use of TSF generated secrets for Identification and Authentication Security Function [FIA_SOS.1], [FIA_SOS.2].</p>
<b>O.ANTI_BRUTE</b>	<p>The TSF detects when three unsuccessful authentication attempts occur related to consecutive instances of a TOE operator attempting to authenticate itself on a TOE component. When three unsuccessful authentication attempts have been met, the TSF locks the user account if the user role is different from System Administrator, otherwise logs the authentication attempt [FIA_AFL.1].</p>
<b>O.ACCESS</b>	<p>The TSF enforces a VBrain access control SFP on TOE users allowing only authorized users to access only to authorized TOE functions and data according to their role [FDP_ACC.1], [FDP_ACF.1], [FMT_MSA.1], [FMT_MSA.3].</p>
<b>O.SECOM</b>	<p>The TSF enforces the OPC-UA and User Data information flow control SFPs to prevent the disclosure, modification, loss of use of user, TOE and security related data when it is transmitted between physically-separated parts of the TOE [FDP_ITT.1], [FDP_IFC.1], [FDP_IFT.1].</p> <p>The TSF protects TSF data from disclosure and modification when it is transmitted between separate parts of the TOE [FPT_ITT.1].</p>
<b>O.REPLAY</b>	<p>The TSF enforces the OPC-UA information flow control SFP, using a message sequencing mechanism, to prevent message replay attacks between separate parts of the TOE [FDP_IFC.1].</p>
<b>O.CRASH</b>	<p>The TSF enforces information flow control SFPs when imports and exports user data, controlled under the SFP, from and to outside of the TOE [FDP_ETC.1], [FDP_ITC.1].</p> <p>The TSF protects TSF data transmitted from the TSF to another trusted IT product from unauthorized disclosure during transmission [FPT_ITC.1].</p> <p>When the TOE (VBrain Logger) needs to create a new <i>runtime DB</i> backup file, if the <i>runtime DB</i> backup folder managed by the Operating System reaches the maximum configured size, the oldest file is deleted.</p>

<p><b>O.AVAIL</b></p>	<p>The TSF enforces the User Data information flow control SFP which states that:</p> <ul style="list-style-type: none"> <li>- a child node measure variation acquired from FieldBus is displayed in the VBrain Client HMI for the connected user if he has the rights to see it according to his role/groups;</li> <li>- a child node measure variation acquired from FieldBus indicating that an alarm/warning has been triggered is notified internally in the VBrain Client HMI (for the connected authorized user);</li> <li>- when VBrain Server receives a valid command result from a child node, it asks VBrain Logger to log on the <i>runtime DB</i> the data related to the executed command [FDP_IFC.1], [FDP_IFF.1].</li> </ul>
<p><b>O.AUDIT</b></p>	<p>Security-relevant events must be defined and auditable for the TOE and the user associated with the events must be recorded [FAU_GEN.1, FAU_GEN.2]. The TOE provides TOE authorized administrators with the capability to read a specific set of audit information and the ability to apply searches of audit based on time frame and/or date of the event and/or type of event and/or state of event and/or name of event [FAU_SAR.1], [FAU_SAR.2], [FAU_SAR.3].</p>
<p><b>O.MANAGE</b></p>	<p>The TSF shall maintain the roles System Administrator, Configuration Administrator, Commander, Acknowledger, Full Reader, Reader [FMT_SMR.1]. The TSF restricts the ability to disable, enable, determine and modify the behavior of the security functions to TOE authorized administrators [FMT_MOF.1]. The TSF is capable of performing a set of management functions that allows the efficacious management of security functionality of the TOE and its data [FMT_SMF.1].</p>
<p><b>O.EXHAUST</b></p>	<p>The TSF shall run a suite of tests at the first launch of VBrain Logger and periodically during normal operation to check that the <i>runtime DB</i> has not reached the maximum configured size, to check that the last backup of the runtime DB is not older that a configurable number of days and to check that the <i>runtime DB</i> backup folder, managed by the Operating System, has not reached the maximum configured size. If the first test fails, the VBrain Logger asks the DBMS to save data stored in the <i>runtime DB</i> in a backup file in the <i>runtime DB</i> backup folder and to delete the oldest half of the records inside the runtime DB. If the second test fails, the VBrain Logger asks the OS to delete the oldest <i>runtime DB</i> backup file [FPT_TEE.1].</p>
<p><b>O.SESSION</b></p>	<p>The TSF denies session establishment based on a number of OPC-UA sessions opened for the specific user [FTA_TSE.1]. The TSF allows only a limited number of concurrent OPC-UA sessions that belong to the same user [FTA_MCS.2].  OPC-UA sessions between OPC-UA Client and OPC-UA Server are automatically closed if a closure request is sent by an OPC-UA Server/Client to its counterpart [FTA_SSL.4].</p>

**Table 25: Rationale for TOE Security Objectives coverage by SFRs**

---

## 7 TOE SUMMARY SPECIFICATION

### 7.1. SECURITY FUNCTION

[131] The security functions described in the following subsections fulfill the security requirements that are defined in Section 6.1 – Security Functional Requirements. The security functions performed by the TOE are as follows:

SF_1:	Configuration Management
SF_2:	Centralized Access Control
SF_3:	Identification and Authentication
SF_4:	Session handling
SF_5:	Audit
SF_6:	Encryption
SF_7:	Security related data availability and service continuity

[132] The following paragraphs describe the security features implemented by the TOE and how they are implemented.

#### 7.1.1. SF\_1: Configuration Management

[133] VBrain Configurator is used by TOE authorized administrators, through its HMI, prior successful user login, to configure and setup all parameters of the system and the users allowed to operate on it. This application allows the configuration of all other TOE components and of all the security policies related to the communication channels and profiling. VBrain Configurator works independently from all other TOE components, which have to be restarted so as to implement any configuration modifications.

[134] The TOE allows an authorized administrator to perform the following operations:

- TOE users management;
- management of Applicative users associated to TOE components which need to authenticate on DBMS;
- creation and configuration of physical measures;
- creation and configuration of virtual measures;
- alarms and warnings configuration;
- measures calibration;
- measure-to-log configuration;
- configuration of treeview and graphical interfaces;
- configuration of operations associated to buttons and nodes;
- acquisition driver configuration;
- creation of new Client-type and Server-type applications;
- Server certificate creation (with the support of the Operational environment);
- maximum *runtime DB* dimension ;
- *runtime DB* backup time;
- *runtime DB* backup frequency;
- maximum dimension of the *runtime DB* backup folder;
- period of inactivity of a FieldBus CHILD NODE after which the status of the child node and the master status of the parent node is declared equal to BAD\_ACQUISITION (i.e., connection loss) by VBrain Server.

[135] These features allow an easy management of the configuration concerning alarms and warnings triggered upon undesired changes of the monitored systems.

[136] A configuration is downloaded locally as an encrypted folder, containing the JSON/XML files related to the single TOE components, including OPC-UA Client/Server configuration. The files encryption is performed by VBrain Configurator itself, prior their download, using the AES 256 algorithm implemented by the Operating System (.NET Framework V 4.6.1). In case VBrain

Configurator is not installed on the Server/Client host where the files are required, these are manually exported by the System Administrator or Configuration Administrator into the required hosts using removable memory devices.

[137] The Operating System will support the TOE in granting that only authorized System Administrators (i.e., TOE authorized administrators) can access the encrypted folder above mentioned.

**7.1.2. SF\_2: Centralized Access Control**

[138] Through VBrain Configurator, the TOE System Administrator creates users, associates them to one or more specific Servers, assigning a role for each Server, and set the maximum number of OPC-UA sessions a TOE user is allowed to open.

[139] Each role defined in the TOE is statically associated to specific access rights and operations that can be performed by the users assigned to the specific role in the associated Server.

[140] In addition, through VBrain Configurator, a TOE administrator can define groups of TOE operators, which will be allowed to accede only to specific panels of the VBrain Client HMIs, depending on the configuration. The objective is to limit users access to the process’ critical areas through the HMI, and particularly to prevent the critical alarms’ acknowledge or snooze carried out by not specialized personnel with user role “Acknowledger”.

[141] In addition, it is possible to use VBrain Configurator to create Server certificates. This feature is available to a TOE administrator, and exploits the OPC-UA libraries.

[142] In the following table, the TOE components accessible to specific TOE user roles are represented, while Table 17 describes the TOE access control policy.

	VBrain Configurator	VBrain Server	VBrain Logger	VBrain Notifier	VBrain Supervisor	VBrain Web Socket Server	VBrain Reporting HMI	VBrain Desktop Client HMI	VBrain Web Client HMI	VBrain Alarms List
System Administrator	✓						✓	✓	✓	✓
Configuration Administrator	✓*						✓	✓	✓	✓
Commander							✓	✓	✓	✓
Acknowledger							✓	✓	✓	✓
Full Reader							✓	✓	✓	✓
Reader								✓	✓	✓

✓\* : restricted access to VBrain Configurator functionalities

**Table 26: TOE components accessible to TOE user roles**

**7.1.3. SF\_3: Identification and Authentication**

[143] During TOE installation a “default TOE user” with “System Administrator” role will be defined in the *configuration DB* with a default “first access valid password” associated, which is provided by the TOE Developer. At his first access to VBrain Configurator, he will be asked to change his password, inserting a new valid one that will substitute the default one. “Valid” means here “respecting the complexity criteria defined for TOE users’ password”.

[144] Note that the same procedure shall be followed by all other users (created through VBrain Configurator by TOE System Administrator) to whom a “first access password”, randomly

generated by VBrain Configurator, will be associated. This password must be changed at the first access to the TOE using one of the VBrain Client HMIs available on TOE Client hosts (Operator-side).

- [145] The default System Administrator “first access password”, the passwords randomly generated by VBrain Configurator with the support of Operational environment as “first access password” for the created/reset TOE users, and the passwords chosen by TOE users, must satisfy specific complexity rules (use of both lowercase and uppercase letters, numbers and symbols) and must be made at least of 10 characters. These will be stored in the *configuration DB* after being hashed SHA 256 with the support of the Operational environment.
- [146] VBrain EMS provides field data visualization to TOE users positively identified and authenticated through two applications (Client HMIs): **VBrain Desktop Client HMI** and **VBrain Web Client HMI**. (Note that for VBrain Web Client HMI, when the browser page is reloaded, user authentication and identification is to be redone.)
- [147] To work correctly in the “Web Client HMI” configuration, the TOE needs the installation of another application, namely VBrain Web Socket Server. It is a VBrain Client-type application installed on the Server-side that gathers data from VBrain Server and provides all Server functionalities through web socket technologies.
- [148] When a TOE user launches a VBrain Client HMI, whether Desktop or Web, or when a TOE user tries to access to VBrain Alarms List from VBrain Desktop Client HMI, or when an authorized administrator launches VBrain Configurator, a login screen appears for user authentication. The inserted password is then hashed SHA 256 and compared by the TOE component trying to be accessed with the credentials entered by the user (username + hashed password) to those corresponding to the indicated user, if existing, stored in the *configuration DB*. If these match, user authentication proceeds with a second check on user credentials performed by VBrain Server (and by VBrain Web Socket Server when the TOE is in “Web Client HMI” configuration), otherwise a pop-up window highlights the authentication error.
- [149] If VBrain Server is able to correctly open an OPC-UA session for the user requesting to be identified and authenticated by the TOE, the identification and authentication procedure positively ends, otherwise an error message is retrieved.
- [150] To access other applications via links provided by VBrain Web Client HMI according to user role, VBrain Server performs an additional check on the credentials used on the initial login. This is possible because it keeps the same HTTPS session. Conversely, if the links are accessed through VBrain Desktop Client HMI, the user is prompted to log in again as stated above.
- [151] Each user trying to access the TOE functionalities through an HMI can perform no more than three consecutive unsuccessful login attempts with the same existing username. After the third, the username will be locked and an error message is retrieved, impeding the user to make further attempts. As a consequence, the user should contact the System Administrator, who will reset the password in the *configuration DB* with a default one, randomly generated by VBrain Configurator with the support of Operational environment, and unlock the username. Then, the user will be able to login with the default password provided by the System Administrator, and the system will automatically ask the user to create a new password, which will be hashed and saved in the *configuration DB*, replacing the default one.
- [152] When a TOE user’s password change is needed (at first use or after a password reset performed by System Administrator, or upon user request), Client HMI applications interface *configuration DB* to complete the password change operation. An error message is retrieved in case the inserted password does not satisfy the complexity criteria defined and implemented by the TOE.
- [153] After login, the operator is able to perform only the operations that are allowed for its specific role.
- [154] Commands and sequences can be executed only by logged-in operators with “Commander” role or by users belonging to the specific command authorization list (group), which is defined during the system’s configuration through VBrain Configurator and is employed for particularly critical commands.

- [155] For security reasons, the user credentials and role are re-verified by VBrain Server after the request for a command execution is carried out by the logged-in user. If it has been attempted by an unauthorized user, the command will not be performed, and an error message will be displayed to the operator. Conversely, if successful, a message communicates the command has been carried out.
- [156] Commands on the HMI that are not allowed for the logged-in operator are not executed.
- [157] When the condition of a measurement changes to WARNING or ALARM, i.e., the acquired value overcomes the configured thresholds, the related indicator blinks to indicate the anomaly.
- [158] A measurement can be snoozed to prevent the operators' information overload due to frequent alarm triggering. In case the acquired value for the snoozed measure overcomes the configured thresholds, the related indicator will not blink but will be highlighted.
- [159] The alarm acknowledge and/or measurement snooze can be performed only by TOE user with "Acknowledger" (or higher) role through a pop-up window, which is opened by right-clicking on the highlighted device on the Client HMI.
- [160] The user's role is verified again by VBrain Server after the alarm acknowledge or measurement snooze request is carried out by the logged-in user. If it has been attempted by an unauthorized user, the alarm acknowledge or measurement snooze will not take place, and an error message will be displayed to the operator. Conversely, if successful, a message communicates the alarm acknowledge or measurement snooze has been accomplished.
- [161] If a measurement condition returns to NORMAL before the acknowledge operation, it continues to be not acknowledged, the related indicator continues to blink, and the alarm status will be set as RETURNED. In this way, information about the anomaly is not lost and the operator can be aware of the previous anomalous condition despite its return. An exception is made for the snoozed measurements, for which the condition is set back to NORMAL.
- [162] The TOE prevents Server-side TOE components manual application accidental closing by presenting to the user a pop-up window asking for confirmation of the closure operation.
- [163] In case the operation is confirmed, the TOE is supported by the Operating System that checks whether or not the request came from a logged OS System Administrator (i.e., TOE authorized administrator): in negative case, the operation is forbidden.

#### **7.1.4. SF\_4: Session handling**

- [164] Each user accessing the TOE through a VBrain Client HMI, whether Desktop or Web, is allowed to open a maximum configured number of working sessions (OPC-UA sessions) with VBrain Server associated with the same TOE user.
- [165] In case of TOE Web Client HMI configuration, the number of opened sessions for the same user will be checked also by VBrain Web Socket Server before being checked by VBrain Server.
- [166] In this way, a TOE user is allowed to use on the same Client host both VBrain Desktop Client HMI and VBrain Alarms List, each of which opens its own OPC UA session with VBrain Server.
- [167] There is also the constraint that prevents a TOE user logging at the same time with the same username from an unauthorized number of Client hosts. This attempt will cause an error message to be prompted where the TOE user is attempting to log in, leaving intact the current opened sessions.
- [168] The communication session is unique for all data transmissions, hence it is shared by measures and commands.
- [169] OPC-UA sessions between OPC-UA Client and OPC-UA Server are automatically closed if a closure request is sent by an OPC-UA Server/Client to its counterpart.

**7.1.5. SF\_5: Audit**

**SECURITY AUDIT DATA GENERATION**

[170] The auditable events upon which security audit data are created and managed by the TOE are listed in the Table 16, while in the following table all the events that TOE Administrators can review with the support of the Operating System, after being positively authenticated as OS System Administrator, are listed.

<b>Auditable events managed by Operational Environment</b>	<b>where the audit data are stored by Operational Environment</b>
TOE components start and stop	Log file, consisting of a number of files containing diagnostic information and errors related to the applications' operation and OPC-UA Client/Server communication. More specifically, a log file is created for each VBrain application, which is managed by Vitrociset proprietary libraries, and a log file generated by the OPC-UA libraries. All log files are located in a specific folder of the VBrain applications' hosts, and are accessible only by OS System Administrators. Thereby, the folders' access control is managed by the OS.
OS user login	
<i>runtime DB</i> backup file restored to <i>historian DB</i> after request by TOE user through VBrain Reporting HMI	<i>historian DB</i> (backup restore data)

**SECURITY AUDIT REVIEW**

- [171] **VBrain Reporting** and **VBrain Reporting HMI** allow TOE users, according to their role and access rights, to accede and consult stored data (both in *runtime* and *historian DB*) in order to perform post-analysis on the historical data (i.e., information related to the TOE's evolution) and to create customized reports for specific needs.
- [172] VBrain Reporting is the web application containing the code executed by IIS and the HMI panels repository, and guarantees the required visualization and operation of VBrain Reporting HMI through an Internet browser. Hence, an Internet browser HTML5 & CSS3 compliant makes it possible to run the VBrain Reporting application, which is installed on a Server host.
- [173] VBrain Reporting HMI can be accessed from VBrain Desktop Client HMI or from VBrain Web Client HMI. In the latter case, no further login is required, as it maintains the same HTTPS session. Nevertheless, the user's credentials are re-verified by VBrain Server. In case VBrain Reporting HMI is accessed directly through the specific URL or from VBrain Desktop Client HMI, user login will be required. All type of users can launch VBrain Reporting HMI, but historic backedup data is displayed only to users with role "Full reader" or superior.
- [174] VBrain Reporting allows users with role "Full reader" or superior to select which *runtime DB* backup file is to be restored in the *historian DB* in order to visualize, in VBrain Reporting HMI, measurements, alarms and commands previously stored by the VBrain Logger application. User identification and authentication through VBrain Reporting HMI is performed as described in § 7.1.3, comparing the entered user's credentials with those stored in the *configuration DB*.
- [175] To such end, the selected backup is restored to the *historian DB*, and data is displayed in the proper panel according to the type (measurements, alarms or commands). If backup restoring is attempted by an unauthorized user, an error message is displayed to the operator and data restoring to the *historian DB* is not carried out.
- [176] In particular, the visualization of data stored in two different databases is possible:
  - *runtime DB*, the database on which the VBrain Logger achieves runtime data acquired from VBrain Server;
  - *historian DB*, a database where it is possible restore backup files previously created, so to have access to older information stored by the VBrain Logger application.

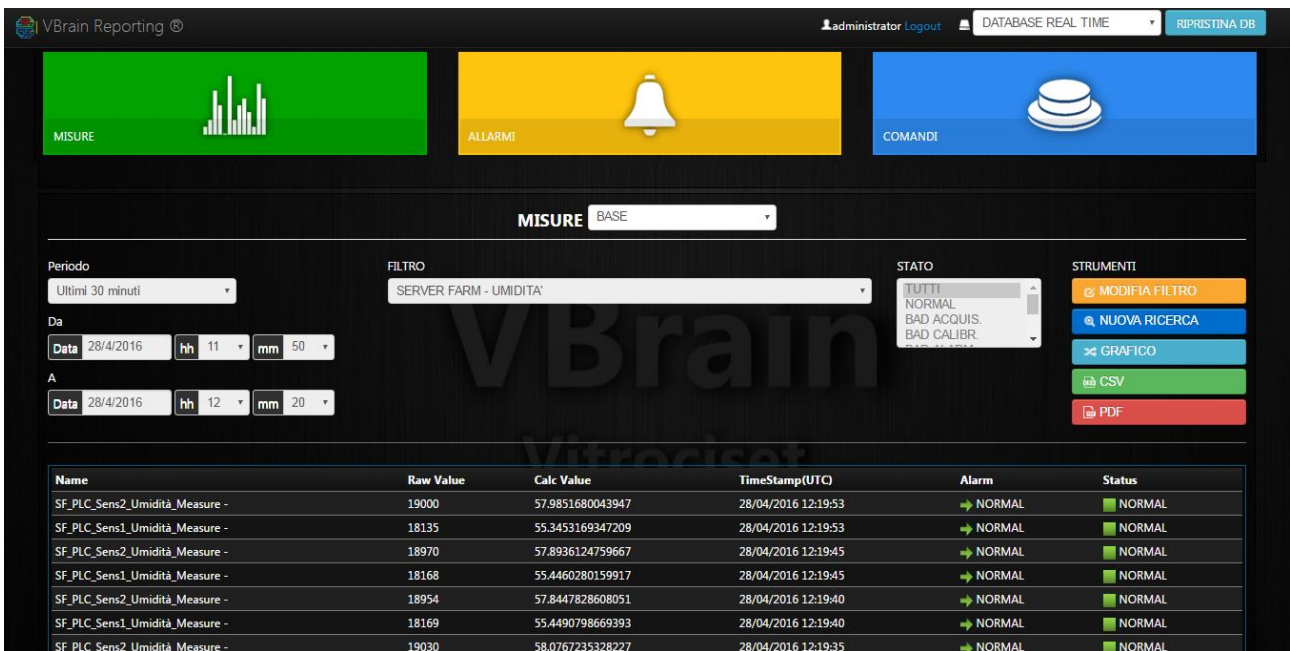


Figure 13: Example of stored data visualization

- [177] In the “Desktop Client HMI” configuration of the TOE, the **VBrain Alarms List** component is installed on the Client host, which presents to the operator a table containing only the measurements with condition different from “NORMAL” and/or communication status different from “GOOD”.
- [178] Despite it can be accessed through a link in VBrain Desktop Client HMI, user login is required (user identification and authentication is performed as described in § 7.1.3, comparing the entered user’s credentials with those stored in the *configuration DB*). Only the users with role “Reader” or superior can launch VBrain Alarms List. If access is attempted by an unauthorized user, an error message is displayed to the operator and the application is not opened.
- [179] Nevertheless, the alarm acknowledge and/or measurement snooze operations will be performed by VBrain Server only if requested by an user with role “Acknowledger” or superior. Users with a role lower than “Acknowledger” can only visualize the alarms’ state.
- [180] As all other TOE components, VBrain Alarms List has its own configuration file.
- [181] Figure 14 provides an example of information reported by VBrain Alarms List.

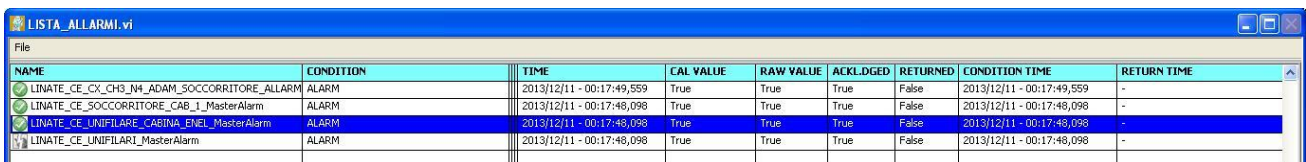


Figure 14: VBrain Alarms List example

- [182] On the left side, there is a symbol representing the alarm state. Alarms are correlated to one or more measurements provided by a specific device.
- [183] Such list allows to acknowledge one or more alarms that have not been acknowledged, yet. In addition, one or more displayed measurements can be snoozed. Moreover, an acoustic alarm can easily enabled/disabled from the interface.
- [184] Through **VBrain Configurator**, a TOE user with System Administrator role can visualize TOE user state (active/first access to be done/locked/number of failed login attempt).



### 7.1.6. SF\_6: Encryption

#### **CONFIGURATION FILE ENCRYPTION**

- [185] Upon request of a TOE authorized administrator, a new TOE configuration is downloaded locally by VBrain Configurator in a specific folder, containing the encrypted JSON/XML files related to the single applications. For distributed systems, such files are manually exported by the System Administrator or Configuration Administrator into the required hosts by means of removable memory devices. Encryption of the configuration files is done with the AES 256 algorithm, with the Operational Environment support, using the .NET Framework V 4.6.1 libraries.
- [186] The key employed for encryption consists of two parts:
- A fixed part, hardwired in the VBrain EMS modules source code, known only by the Developer;
  - A variable part, unknown to the Developer, consisting in the SHA 256 hash value of the System Administrator's password.
- [187] Such a key is automatically composed by VBrain Configuration prior the TOE configuration download, and cannot be modified by the TOE administrator logged in to VBrain Configurator. This key is never destroyed.
- [188] In order to protect JSON/XML configuration files' integrity, as required by FPT\_ITT.1, a SHA 256 hash value is associated to it before encryption so that, after decryption, the file integrity could be checked.

#### **SECURE COMMUNICATION**

- [189] All internal communications, according to the policy detailed in the INFORMATION FLOW CONTROL POLICY SECTION in § 6, between VBrain Server component (OPC-UA Server) and other OPC-UCA Client-type TOE components are based on OPC-UA protocol.
- [190] As well, the TOE may use the OPC-UA protocol also to communicate with some nodes in the FieldBus. This is also the case when the TOE interfaces another instance of the TOE itself in a multi-nodal architecture, as described in § 1.5.4.
- [191] OPC-UA protocol is used in the TOE configuring *SecurityLevel* parameter equal to 3, the *SecurityMode* to Sign&Encrypt, i.e., each message exchanged between the above mentioned TOE components is signed and encrypted.
- [192] The Operational environment (OE.CRYPTO) supports the TOE for AES 128 bit encryption and cryptographic key generation for OPC UA implementation.
- [193] Before an USER DATA exchange or a TSF DATA (users' credentials) exchange is possible via OPC-UA protocol, an OPC-UA session should be properly setup between sender and receiver that will exchange, in this case, specific session handling messages in order to setup, with the support of the Operational Environment, an encrypted communication between OPC-UA senders and receivers.
- [194] The Operational environment (OE.CRYPTO), i.e. Operating System via .NET Framework V 4.6.1, supports the TOE granting both RSA 2048 cryptographic encryption and cryptographic key generation for OPC UA implementation for communication channel protection and cryptographic protection of messages and commands exchanged over the communication channel with AES 128.

### 7.1.7. SF\_7: Security Related data availability and service continuity

- [195] The activity of a SCADA involves the handling of data representative of the process status and the operating conditions of the infrastructure that constitutes the control system as sensors, actuators, data acquisition equipment, communication systems, processing system.
- [196] **VBrain Server** is the core application, responsible for data acquisition and elaboration from FieldBus devices (outside the TOE boundary), like monitoring sensors, actuators, smart automation units, PLCs or third-party systems, data normalization and elaboration, commands actuation,

alarms generation on the basis of the configured thresholds, and it publishes all measurements variations on the network, so to be used from all Client applications. It includes several drivers to interface FieldBus devices.

[197] Moreover, VBrain Server has the following functionalities:

- FieldBus data concentrator;
- communication manager between FieldBus devices and Client applications;
- communication manager with Logger application.

[198] **VBrain Supervisor** is installed on the same Server host where VBrain Server is installed, and it periodically checks through the Windows APIs if the configured Server-side core processes are running, automatically starts the predefined applications if closed and, in case the application becomes unresponsive or if the configured limit of memory is reached, it launches a new instance of the monitored process, so as to guarantee service continuity.

[199] Data storage in the database takes a central role in the process of implementing a supervision system. **VBrain Logger** is responsible for the logging in the *runtime DB* of all data acquired and elaborated by the TOE, that are configured to be logged.

[200] Supervision and monitoring activities use the *runtime DB* for storing data related to the instant in which these are observed.

[201] VBrain Logger is also responsible of the *runtime DB* periodical backup (the periodicity is configurable) to a dedicated folder.

[202] Hence, two relational databases managed by the certified DBMS and related to the process can be distinguished:

- *runtime VBrain database (runtime DB)*, where data acquired by VBrain Server is stored in an event-driven basis;
- *historian VBrain database (historian DB)*, where data previously backedup are restored under user request for analysis purposes using VBrain Reporting HMI.

[203] Both *runtime* and *historian DBs* contain the following logged data:

- acquired measures;
- warning and alarms;
- executed commands.

[204] In addition, VBrain Logger performs self-diagnostic through an event-based automatic backup procedure and the *runtime DB* backup folder management on the basis of a FIFO policy. The application manages the data backup in the following ways:

- **Periodic data archiving:** according to a temporal base OR a maximum size reached criterion, the oldest half of the records inside the runtime DB is deleted and data are saved in a backup file in the *runtime DB* backup folder. Hence, such database is kept lightweight and its performance is improved. In this way, the TOE grants availability and integrity of runtime data.
- **Oldest backup file deletion:** in case the DB backup folder reaches the maximum configured size, when a new backup file is to be created, the oldest is deleted. In this way, the TOE grants monitored system's integrity and availability. In order to check the DB backup folder dimension and to delete the oldest runtime DB backup file when needed, VBrain Logger interfaces the OS.

**7.2. TOE SUMMARY SPECIFICATION RATIONALE**

[205] This section demonstrates that the TOE’s Security Functions completely and accurately meet the TOE SFRs. The following table provides a mapping between the TOE’s Security Functions and the SFRs.

SFR / SF	SF_1	SF_2	SF_3	SF_4	SF_5	SF_6	SF_7
FAU_GEN.1					x		
FAU_GEN.2					x		
FAU_SAR.1					x		
FAU_SAR.2					x		
FAU_SAR.3					x		
FIA_UID.2			x				
FIA_UAU.2			x				
FIA_UAU.6			x				
FIA_AFL.1			x				
FIA_ATD.1			x				
FIA_SOS.1			x				
FIA_SOS.2			x				
FTA_TSE.1				x			
FTA_SSL.4				x			
FTA_MCS.2				x			
FDP_ACC.1		x					
FDP_ACF.1		x					
FDP_IFC.1						x	
FDP_IFF.1						x	
FDP_ITT.1						x	
FDP_ETC.1							x
FDP_ITC.1							x
FPT_ITC.1						x	
FPT_TEE.1							x
FPT_ITT.1						x	
FMT_SMR.1	x						
FMT_MOF.1	x						
FMT_SMF.1	x						
FMT_MSA.1	x						
FMT_MSA.3	x						

**Table 27: TOE Security Functions/SFRs mapping**

The following table provides a rationale for the mapping between the TOE’s SFRs and the Security Functions.

SFR	SF and rationale
FAU_GEN.1	<p><b>SF_5 – Audit:</b> the TSF generates the log of the operations specified in Table 16, while the table at § 7.1.5 lists all the events that the TOE administrators can review with the support of the Operating System, after being positively authenticated as OS System Administrator.</p>
FAU_GEN.2	<p><b>SF_5 – Audit:</b> the TOE associates the identity of the user that caused the event for each event logged.</p>
<p>FAU_SAR.1 FAU_SAR.2 FAU_SAR.3</p>	<p><b>SF_5 – Audit:</b> Alarms are correlated to one or more measurements provided by a specific device and these are displayed in VBrain Alarms List HMI. On the left side of VBrain Alarms List interface, there is a symbol representing the alarm state. Such list allows to acknowledge one or more alarms that have not been acknowledged, yet. In addition, one or more measurements can be snoozed. Moreover, an acoustic alarm can easily enabled/disabled from the interface. VBrain Reporting and VBrain Reporting HMI allow TOE users, according to their access rights, to access and consult stored data (both in <i>runtime</i> and <i>historian DB</i>) in order to perform post-analysis on the historical data (i.e., information related to the TOE’s evolution) and to create customized reports for specific needs.</p>
<p>FIA_UID.2 FIA_UAU.2 FIA_UAU.6</p>	<p><b>SF_3 – Identification and Authentication:</b> the TSF requires users to identify and authenticate themselves before invoking any other TSF function or before viewing any TSF data. No action can be initiated before proper identification and authentication. Server-side applications can be closed only by an authorized logged OS System Administrator (i.e., TOE authorized administrator).</p>
<p>FIA_AFL.1 FIA_ATD.1</p>	<p><b>SF_3 – Identification and Authentication:</b> each user trying to access the TOE functionalities through an HMI can perform no more than three consecutive unsuccessful login attempts with the same existing username. After the third, the username will be locked and an error message is retrieved, impeding the user to make further attempts. As a consequence, the user should contact the System Administrator, who will replace the password in the <i>configuration DB</i> with a default one, randomly generated by VBrain Configurator with the support of the Operational environment, and unlock the username. Then, the user will be able to login with the default password provided by the System Administrator, and the system will automatically ask the user to create a new password, which will be hashed and saved in the <i>configuration DB</i>, replacing the default one.</p>
<p>FIA_SOS.1 FIA_SOS.2</p>	<p><b>SF_3 – Identification and Authentication:</b> the default System Administrator “first access password”, the passwords randomly generated by VBrain Configurator with the support of Operational environment as “first access password” for the created/reset TOE users, and the passwords chosen by TOE users, must satisfy specific complexity rules (use of both lowercase and uppercase letters, numbers and symbols) and must be made at least of 10 characters. When a TOE user’s password change is needed (at first use or after a password reset performed by System Administrator, or upon user request), Client HMI applications interface the <i>configuration DB</i> to complete the password change operation. An error message is retrieved in case the inserted password does not satisfy the complexity criteria defined and implemented by the TOE.</p>
<p>FTA_TSE.1 FTA_SSL.4 FTA_MCS.2</p>	<p><b>SF_4 – Session handling:</b> each user accessing the TOE through a VBrain Client HMI, whether Desktop or Web, is allowed to open a maximum configured number of working sessions (OPC-UA sessions) with VBrain Server associated with the same TOE user. The TSF prevents a TOE user logging at the same time with the same username from an unauthorized number of Client hosts. This attempt will cause an error message to be prompted where the TOE user is attempting to log in, leaving intact the current opened sessions. OPC-UA sessions between OPC-UA Client and OPC-UA Server are automatically closed if a closure request is sent by an OPC-UA Server/Client to its counterpart. The communication session is unique for all data transmissions, hence it is shared by measures and commands.</p>

SFR	SF and rationale
FDP_ACC.1 FDP_ACF.1	<b>SF_2 – Centralized Access Control:</b> through VBrain Configurator, a TOE administrator can define groups of TOE operators, which will be allowed to accede only to specific panels of the VBrain Client HMIs, depending on the configuration. The objective is to limit users' access to the process' critical areas through the HMI, particularly to prevent the critical alarms' acknowledge and/or measurement snooze carried out by not specialized personnel with user role "Acknowledger". Table 26 represents the TOE components accessible to specific TOE user roles. In the Table 17 the TOE access control policy is described.
FDP_ITT.1 FPT_ITC.1 FDP_IFC.1 FDP_IFF.1 FPT_ITT.1	<b>SF_6 – Encryption:</b> the TOE enforces the OPC-UA information flow control SFP to prevent disclosure, modification and loss of use of user data and TSF data when are transmitted between physical-separated parts of the TOE. The TSF shall enforce the user data information flow control SFP when exporting user data, controlled under the SFP(s), outside of the TOE. The TSF protects all TSF data transmitted from the TSF to another trusted IT product from unauthorized disclosure during transmission.
FDP_ETC.1	<b>SF_7 – Security related data availability and service continuity:</b> according to a temporal base or a maximum size reached criterion, the oldest half of the records inside the runtime DB is deleted and data are saved in a backup file in the <i>runtime DB</i> backup folder. Hence, such database is kept lightweight and its performance is improved. In this way, the TOE grants availability and integrity of runtime data. The TSF enforces the user data information flow control SFP when exports user data outside the TOE. User data exported are: <ul style="list-style-type: none"> <li>- measures/warnings/alarms acquired from FieldBus monitored NODES and;</li> <li>- command executed on FieldBus monitored NODES and;</li> <li>- acknowledged alarms</li> <li>- snoozed measurements.</li> </ul>
FDP_ITC.1	<b>SF_7 – Security related data availability and service continuity:</b> the TSF enforces the VBrain EMS information flow control SFP when imports user data from outside the TOE. User data imported are: <ul style="list-style-type: none"> <li>- measures/warnings/alarms acquired from FieldBus monitored NODES and;</li> <li>- user data retrieved from <i>runtime DB</i> and from <i>historian DB</i> onto VBrain Reporting HMI (through VBrain Reporting).</li> </ul>
FPT_TEE.1	<b>SF_7 – Security related data availability and service continuity:</b> VBrain Logger performs self-diagnostic through an event-based automatic backup procedure and the <i>runtime DB</i> backup folder management on the basis of a FIFO policy. The application manages the data backup in two different ways: event-based and periodic data archiving, and oldest backup file deletion. In the first method, according to a temporal base or a maximum size reached criterion, the oldest half of the records inside the runtime DB is deleted and data are saved in a backup file in the <i>runtime DB</i> backup folder. In the second method, when a new backup file needs to be created and the backup folder reaches the maximum configured size, the oldest file is deleted.
FMT_SMF.1 FMT_MOF.1	<b>SF_1 – Configuration Management:</b> the management functions that must be provided for effective management of the TOE are defined and described in Table 20. The TSF restricts the ability of performing changes in the management functions only to TOE authorized administrators.
FMT_SMR.1	<b>SF_1 – Configuration Management:</b> the TOE maintains the roles specified in the SFR.
FMT_MSA.1	<b>SF_1 – Configuration Management:</b> the TOE ensures the access to the security attributes are restricted, so to enforce the access control policy for the TOE.
FMT_MSA.3	<b>SF_1 – Configuration Management:</b> the TOE ensures the default values of security attributes are restrictive in nature, so to enforce the access control policy for the TOE.

Table 28: SFR to TSF rationale