Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

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

Certificato n. 5/21

(Certification No.)

Prodotto: Zeta Server v1.1.1

(Product)

Sviluppato da: Prolan Power Zrt.

(Developed by)

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

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

Conforme a: Protection Profile for Application Software v1.3

(Conformant to)

(ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.1, ASE_REQ.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ALC_TSU_EXT.1, ATE_IND.1, AVA_VAN.1)

Il Direttore
(Dott.ssa Eva Spina)

[ORIGINAL DIGITALLY SIGNED]

Roma, 7 settembre 2021

Common Criteria

SOGIS IT SECURITY CERTIFIED

This page is intentionally left blank

Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Certification Report

Zeta Server v1.1.1

OCSI/CERT/CCL/01/2021/RC

Version 1.0

7 September 2021

Courtesy translation

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

1 Document revisions

Release	Authors	Information	Date
1.0	OCSI	First issue	07/09/2021

2 Table of contents

1 Document revisions 5
2 Table of contents 6
3 Acronyms 8
4 References 10
4.1 Criteria and regulations 10
4.2 Technical documents 11
5 Recognition of the certificate 12
5.1 CC Certificates recognition in Europe (SOGIS-MRA) 12
5.2 International CC Certificates recognition (CCRA) 12
6 Statement of certification 13
7 Summary of the evaluation 14
7.1 Introduction 14
7.2 Executive summary 14
7.3 Evaluated product 14
7.3.1 TOE architecture 15
7.3.2 TOE security features 15
7.4 Documentation 16
7.5 Protection profile conformance claims 16
7.6 Functional and assurance requirements 17
7.7 Evaluation conduct 18
7.8 General considerations about the certification validity 18
8 Evaluation outcome 19
8.1 Evaluation results 19
8.2 Additional assurance activities 20
8.3 Recommendations 20
9 Annex A – Guidelines for the secure use of the product 21
9.1 TOE Delivery 21
9.2 Installation, initialization and secure usage of the TOE 21
10 Annex B – Evaluated configuration 22
10.1 TOE operational environment 22

11 Annex C – Test Activities 23
11.1 Test configuration 23
11.2 Functional and independent tests performed by the Evaluators 23
11.3 Vulnerability assessment and penetration tests 23

3 Acronyms

API	Application Programming Interface
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GB	Gigabyte
GHz	Gigahertz
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIAP	National Information Assurance Partnership
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica
OS	Operating System
PII	Personally Identifiable Information
PP	Protection Profile
RAM	Random Access Memory
RPM	Red Hat Package Manager
SAR	Security Assurance Requirement
SCADA	Supervisory Control And Data Acquisition
SFP	Security Function Policy
SFR	Security Functional Requirement

SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Arrangement
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
ZSC	Zeta Substation Controller
ZCM	Zeta Client Manager

4 References

4.1 Criteria and regulations

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

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

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

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

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

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

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

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

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

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

4.2 Technical documents

[AGD] "Guidance Documentation - Zeta Server v1.1.1", v0.4, Prolan Power, 18 June 2021

[ETR] "Zeta Server 1.1.1" Evaluation Technical Report, v1, CCLab Software Laboratory, 30 June 2021

[PP-APP] Protection Profile for Application Software, Version 1.3, NIAP, 1st March 2019

[ST] "Security Target - Zeta Server v1.1.1", v1.3, Prolan Power, 18 June 2021

5 Recognition of the certificate

5.1 CC Certificates recognition in Europe (SOGIS-MRA)

The European mutual recognition arrangement (SOGIS-MRA, version 3, [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) for the assurance levels up to and including EAL4 for all IT products. A higher recognition level for evaluations beyond EAL4 is provided for IT Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on https://www.sogis.eu/.

The SOGIS-MRA logo printed on the certificate indicates that it is recognized under the terms of this agreement by signatory nations.

This certificate is recognised under SOGIS-MRA for all declared assurance components included in EAL1.

5.2 International CC Certificates recognition (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] was ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on https://www.commoncriteriaportal.org/.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA for all declared assurance components included in EAL1.

6 Statement of certification

The Target of Evaluation (TOE) is the software product “Zeta Server v1.1.1”, also referred to in the following as “Zeta Server”, developed by Prolan Power Zrt.

The TOE is an enterprise monitoring and supervisory control solution used to collect analogue and binary measurements of electrical equipment from a substation gateway and provides the possibility of issuing commands to those pieces of equipment if needed through a Web GUI that facilitates the visualization of the substation.

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

The objective of the evaluation is to provide assurance that the TOE complies with the requirements specified in the Security Target [ST]; the potential consumers and/or users of the product should review also the Security Target, in addition to the present Certification Report. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC v 3.1 for the assurance components included in the PP [PP-APP], according to the information provided in the Security Target [ST] and in the configuration shown in Annex B – Evaluated configuration of this Certification Report.

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

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product “Zeta Server v1.1.1” to provide assurance to the potential consumers and/or users that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should review also the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	Zeta Server v1.1.1
Security Target	“Security Target - Zeta Server v1.1.1”, v1.3 [ST]
Evaluation Assurance Level	Conformant to PP including the following assurance components: ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.1, ASE_REQ.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ALC_TSU_EXT.1, ATE_IND.1, and AVA_VAN.1
Developer	Prolan Power Zrt.
Sponsor	Prolan Power Zrt.
LVS	CCLab Software Laboratory
CC version	3.1 Rev. 5
PP conformance claim	Protection Profile for Application Software, Version 1.3 [PP-APP]
Evaluation starting date	19 March 2021
Evaluation ending date	30 June 2021

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are fulfilled.

7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE; for a detailed description, please refer to the Security Target [ST].

The TOE “Zeta Server v1.1.1” is an enterprise monitoring and supervisory control (SCADA) solution used to collect analogue and binary measurements of electrical

equipment from a substation gateway and provides the possibility of issuing commands to that equipment if needed through a Web GUI that facilitates the visualization of the substation.

The whole Zeta Solution consists of the Zeta Server application (the TOE) and the Substation Automation Gateway (SAGateway).

SAGateway interfaces with Zeta Server and relays collected data from the substation via various standard communication protocols, and also provides the possibility to issue commands to technology devices. Without this connection being established, Zeta Server's functionality is very limited. SAGateway is not part of the TOE.

7.3.1 TOE architecture

Zeta Server (the TOE) consists of the following subsystems:

- **Zeta Substation Controller (ZSC)**: it heavily relies on data collected from Substation Automation Gateway and is responsible for additional application calculations that supply necessary information for the Web GUI visualization relayed through the Zeta Client Manager.

- **Zeta Client Manager (ZCM)**: it is a web server application that supplies the necessary data to clients for substation visualization – according to user role – via secure SSL connection. It also interfaces Zeta Substation Controller to relay substation-related messages to clients, and also authorizes messages from clients and forwards them to Zeta Substation Controller. This software component is responsible for the majority of security functions on the server-side.

The **Web GUI** is the most important module of ZCM. In their web browser authorized users can see the current state of the substation in a visualized form and leverage the features provided by the software such as getting detailed information about technology devices, being informed about important changes, and immediately alarmed on unexpected behaviour. This interface usually consists of many views depending on the Substation Model, with various contents helping the operators to focus on different subsets of technology devices or the whole substation. Many of the security related settings can be changed through the security administration page. Users can also manage Substation Models on the corresponding management page.

The **Substation Model** describes the settings of Zeta Server and the displayed content of the Web GUI. It includes numerous types of containers and elements each serving as objects of realized functions, such as substation topology, views, data point types, event types, data lists, control-feedback relations, voltage levels, user group's authority, etc.

7.3.2 TOE security features

The Security Problem of the TOE, including security objectives, assumptions, threats and organizational security policies, is defined in sect. 3 of the Security Target [ST].

For a detailed description of the TOE Security Functions, consult sect. 6 of the Security Target [ST]. The most significant aspects are summarized below:

- **Cryptographic support**: the TOE protects its data using the platform's built in random number generator. It generates session identifiers, password encryption keys and other random values to defend against potential attacks.

- **User data protection**: the TOE protects sensitive data stored in non-volatile memory. The TOE restricts its access to network connectivity provided by the platform's hardware resources and does not access any of the platform's sensitive information repositories.

- **Security Management**: the TOE comes with default credentials and provides a Web GUI for user administration. The Security Administrator user can log in to the Web GUI using default credentials and has to change its password immediately. The Security Administrator can add or modify users and set user roles using the Web GUI.
  User accounts and their passwords are stored in a PostgreSQL database in a hashed form.

- **Privacy**: the TOE does not handle personally identifiable information (PII).

- **TSF Protection**: the TOE is compatible with its host OS platform when that is configured in a secured manner, using SELinux.
  The TOE uses a well-defined set of platform APIs and third-party libraries.
  The TOE provides the ability for the Installer to check its version and if an update is available. Internet connection needed for the latter.
  Updates are delivered in formats appropriate for the platform on which the TOE is hosted. They are digitally signed, and the signature is validated prior to installation. Installing an update of the application removes all previously installed files except configuration and audit/log files.

- **Trusted Channel/Path**: the TOE encrypts data in transit between itself and clients as well as the Substation Automation Gateway using HTTPS. The TOE relies on the platform to implement HTTPS encryption.

7.4 Documentation

The guidance documentation specified in Annex A – Guidelines for the secure use of the product is delivered to the customer together with the product.

The guidance documentation contains all information for secure initialization, configuration and secure usage the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in sect. 8.3 of this report.

7.5 Protection profile conformance claims

The Security Target [ST] claims exact conformance to the following Protection Profile:

- Protection Profile for Application Software, Version 1.3 [PP-APP]

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected or derived by extension from CC Part 3 [CC3].

All Security Functional Requirements (SFR) have been selected or derived by extension from CC Part 2 [CC2].

Considering that the Security Target claims exact conformance to the Protection Profile [PP-APP], it includes the following extended assurance component from this PP:

- ALC_TSU_EXT.1 (Timely Security Updates)

The ST also includes the following extended functional components from [PP-APP]:

- FCS_RBG_EXT.1 (Random Bit Generation Services)
- FCS_CKM_EXT.1 (Cryptographic Key Generation Services)
- FCS_STO_EXT.1 (Storage of Credentials)
- FDP_DEC_EXT.1 (Access to Platform Resources)
- FDP_NET_EXT.1 (Network Communications)
- FDP_DAR_EXT.1 (Encryption of Sensitive Application Data)
- FMT_MEC_EXT.1 (Supported Configuration Mechanism)
- FMT_CFG_EXT.1 (Secure by Default Configuration)
- FPR_ANO_EXT.1 (User Consent for Transmission of Personally Identifiable Information)
- FPT_API_EXT.1 (Use of Supported Services and APIs)
- FPT_AEX_EXT.1 (Anti-Exploitation Capabilities)
- FPT_TUD_EXT.1 and FPT_TUD_EXT.2 (Integrity for Installation and Update)
- FPT_LIB_EXT.1 (Use of Third Party Libraries)
- FPT_IDV_EXT.1 (Software Identification and Versions)
- FTP_DIT_EXT.1 (Protection of Data in Transit)

Please refer to the Security Target [ST] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST], whose review is recommended to potential consumers. Initially, the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM]. Furthermore, all specific assurance activities required by the Protection Profile for Application Software [PP-APP] have been carried out.

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) CCLab Software Laboratory.

The evaluation was completed on 30 June 2021 with the issuance by the LVS of the Evaluation Technical Report [ETR] that has been approved by the Certification Body on 26 July 2021. Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in Annex B – Evaluated configuration. Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

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

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETR] released by the LVS and documents required for the certification, and considering the evaluation activities carried out, on the basis of the evidence examined by the Certification group, OCSI concluded that the TOE "Zeta Server v1.1.1" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level defined by the SARs included in the PP [PP-APP], with respect to the security functions described in the Security Target [ST] and the evaluated configuration, shown in Annex B – Evaluated configuration.

Table 1 summarises the final verdicts for each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level defined by the SARs included in the PP [PP-APP].

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives for the operational environment	ASE_OBJ.1	Pass
Stated security requirements	ASE_REQ.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Basic functional specification	ADV_FSP.1	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Labelling of the TOE	ALC_CMC.1	Pass
TOE CM coverage	ALC_CMS.1	Pass
Timely Security Updates	*ALC_TSU_EXT.1*	Pass
Tests	**Class ATE**	Pass
Independent testing – conformance	ATE_IND.1	Pass
Vulnerability assessment	**Class AVA**	Pass
Vulnerability survey	AVA_VAN.1	Pass

Table 1 - Final verdicts for the assurance requirements

8.2 Additional assurance activities

The Protection Profile for Application Software [PP-APP] includes additional assurance activities that are specific to the TOE type, and are required for exact conformance to the PP.

The Evaluators performed the assurance activities required for all SFRs defined in the PP [PP-APP] and included in the Security Target [ST]. The objective of these sub-activities is to determine whether the requirements of the assurance activities defined in the PP are met.

All the PP assurance activities received a “Pass” verdict from the Evaluators.

8.3 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in sect. 6 - Statement of Certification.

Potential customers of the product “Zeta Server v1.1.1” are suggested to properly understand the specific purpose of this certification reading this Report with reference to the Security Target [ST].

The TOE must be used according to the Security Objectives for the operational environment specified in sect. 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all the assumptions and the Organizational security policies described, respectively, in sect. 3.2 and 3.3 of the Security Target [ST] are respected.

This Certification Report is valid for the TOE in its evaluated configuration; in particular, Annex A – Guidelines for the secure use of the product includes a number of recommendations relating to delivery, initialization and secure usage of the product, according to the guidance documentation provided together with the TOE ([AGD]).

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

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE Delivery

The TOE is software-only and is delivered by direct download from the Developer's website. The user receives the required login information as part of the purchase process.

Upon entering the credentials, the user should search for category "ZETA binary package", choose the version corresponding to the TOE and click on the download button. The TOE installer is provided as a ZIP archive.

Before installing/updating the TOE the installer must verify that the RPM package is the complete instance, it is provided by the Developer and it's intact from any modification. Therefore, all provided packages are digitally signed by the Developer and the user should check the digital signature before the install/update process takes place.

Precise instructions on how to verify the package's digital signature are given in chapter 7 (Acceptance of the TOE) of the guidance documentation [AGD].

9.2 Installation, initialization and secure usage of the TOE

Users should refer to the following document for instructions on how to install and configure the TOE components and setting up the operational environment:

- "Guidance Documentation - Zeta Server v1.1.1", v0.4, 18 June 2021 [AGD]

The guidance documentation [AGD] also describes the interfaces and functions of the TOE and provides information on their secure usage in accordance with the security objectives specified in the Security Target [ST].

10 Annex B – Evaluated configuration

The TOE is the software-only product “Zeta Server v1.1.1”, developed by Prolan Power Zrt.

The evaluated configuration consists of the TOE software and guidance documentation.

The physical parts of the TOE are as follows:

- “Zeta_Server_1.1.1.zip”, which includes the install package of the Zeta Server and a setup directory containing additional script files and environmental configuration files supporting the installation process.
- Guidance Documentation – Zeta Server v1.1.1 [AGD].

For more details, please refer to sect. 1.3 of the Security Target [ST].

10.1 TOE operational environment

The TOE’s operational environment includes the following:

- Platform on which the TOE is hosted. The TOE is capable of running on a general-purpose Linux operating system on a consumer-grade hardware.
- Other product components. Substation Automation Gateway is not mandatory but expected to be present. Without it the functionality of the TOE is very limited.
- A PostgreSQL Database containing user and application data, logs and history of measurement values of the substation devices.

The TOE is designed to run on a CentOS 7 Linux platform and was evaluated and tested on this specific Linux distribution.

The TOE has the following system requirements for its host platform:

- 4x 2GHz cores;
- 8 GB RAM;
- minimum of 1 GB disk storage.

The TOE can be installed on 1 GB of free space but the Developer recommends at least 30 GB disk storage for storing logs and data history.

For more details, please refer to chapter 8 (TOE Installation) of the guidance documentation [AGD].

11 Annex C – Test Activities

This annex describes the task of both the Evaluators and the Developer in testing activities. For the assurance level defined by the SARs included in the PP [PP-APP], such activities do not require the execution of functional tests by the Developer, but only independent functional tests and penetration tests by the Evaluators.

11.1 Test configuration

The Developer provided a virtual machine and a complete Zeta Solution for testing purposes. Its main components are Zeta Substation Controller (ZSC), Zeta Client Manager (ZCM), Web GUI, Substation Automation Gateway (SAGateway) and a Substation Model. The SAGateway and the Substation Model are not part of the TOE.

As a first step, the Evaluators downloaded the virtual machine from the Developer's website. The Evaluators logged in with credentials that had been provided before by the Developer. All evaluation relevant files are separated on the site.

After successful download, the virtual machine – that serves as an OS – was imported in the virtualization platform used for testing (VMware). Access to the virtual machine required login credentials which also had been given by the Developer. Then, digital signature was checked, database was created, certificates were generated, webserver was configured and finally SAGateway was installed to get a proper operational environment for the TOE.

Next, the TOE's RPM package was installed. The Evaluators followed the preparation steps described in chapter 8 of the guidance document [AGD] to create a secure configuration of the TOE.

11.2 Functional and independent tests performed by the Evaluators

The Security Target [ST] claims exact conformance to the PP [PP-APP], which defines test cases mapped to SFRs. The Evaluators performed all required test cases, thereby also fulfilling the requirements for ATE_IND.1.

Before initiating the testing activity, the Evaluators verified that the test environment was properly set up and the TOE was configured correctly.

The Evaluators executed all required tests described in the PP [PP-APP] and in the applicable NIAP Technical Decisions listed in sect. 2.1 of the Security Target [ST].

All the actual test results were consistent to the expected test results.

11.3 Vulnerability assessment and penetration tests

In a first phase, the Evaluators used Google dork techniques to look for publicly available information and known TOE vulnerabilities. To check what information was accessible for a potential attacker, the Evaluator searched with the keywords "prolan power" and "zeta". These results have not provided any meaningful information concerning the TOE or about any exploitable vulnerability.

The company's webpage was also examined; no information was available there about the TOE, only the SAGateway component is documented there (which is part of the operational environment).

Then, the Evaluators conducted an extended search to find known vulnerabilities affecting the third-party libraries used by the TOE, listed in chapter 9 of the Security Target [ST]. The Evaluators performed a Google search and also checked publicly available exploit databases for exploits against the third-party libraries.

As a result, all of the publicly accessible vulnerabilities and exploits for the TOE and the third-party libraries were collected. The identified vulnerabilities were examined one by one. Based on this analysis, just one candidate was selected for penetration tests: Denial of Service via ZIP bomb.

The Evaluators tried to exploit this potential vulnerability, but the TOE showed to be resistant against it. The results of the tests were documented and detailed enough for the repeatability.

The Evaluators could then conclude that the TOE is resistant to an attack potential of Basic in its intended operating environment. No exploitable or residual vulnerabilities have been identified.