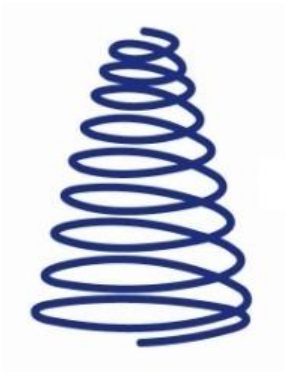

ORNET Neuron Security Target

Common Criteria: EAL1

Version 1.1

16-FEB-12

Document management

Document identification

Document ID	ORN_ST_EAL1
Document title	ORNET Neuron Security Target
Product version	v1.2.2

Document history

Version	Date	Description
0.1	11-SEP-10	Release for internal review.
0.2	9-SEP-11	Addressing EORs
1.0	21-NOV-11	Final
1.1	16-FEB-12	Update Software and Hardware requirement.

Table of Contents

1 Security Target introduction (ASE_INT)

1.1 ST and TOE identification

ST Title	ORNET Neuron Security Target
ST Version	1.1, 16-FEB-12
TOE Title	ORNET Neuron
TOE Version	Version 1.2.2
Assurance Level	EAL1
CC Identification	Common Criteria for Information Technology (IT) Security Evaluation, Version 3.1, July 2009, incorporating: • Part One – Introduction and General Model, Revision Three, July 2009; • Part Two – Security Functional Components, Revision Three, July 2009; and • Part Three – Security Assurance Components, Revision Three, July 2009. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, July 2009, Version 3.1, Revision 3, CCMB-2009-07-004

1.2 Document organization

This document is organized into the following sections:

- Section 1 provides the introductory material for the ST as well as the TOE description including the physical and logical scope of the TOE.
- Section 2 provides the conformance claims for the evaluation.
- Section 3 defines the security objectives for the environment.
- Section 4 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and 3, respectively that must be satisfied by the TOE.

- Section 5 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE

1.3 TOE description

1.3.1 TOE type and usage

The Target of Evaluation (TOE) is the ORNET Neuron and is referred to as the TOE or ORNET Neuron in this document. ORNET Neuron is a web-based application that that allows users to monitor the performance of machines used in semiconductor and electronic manufacturing factories through a set of software modules that is served through the TOE. The set of software modules are:

- Failure Mode and Effect Analysis (FMEA) is a new module designed to send and receive failure mode immediately and screened in the spreadsheet. User can create new FMEA and generate reports. The software can create various types of reports for the FMEA.

- Machine Perfomance Analyzer (MPA) is a module where user used to view reports according to the search selection using the MPA interface.

- Statistical Process Control (SPC) is intended to help user to do data entry and generate report based on their entry.

- Tool Life Scheduling (TLS) comes with various maintenance tasks such as preventive maintenance, tasks scheduling, tasks reminder, shutdown planning, etc. There are also other tasks included such as inspection, lubrication, parts change, servicing and etc.

- Reject Analysis (RA) Module is a new module designed to track and monitor rejects in the production area. User can do data entry and generate reports. The software can create various types of reports for the RA and can be grouped by machine number, lot number, location, etc.

1.3.2 TOE security functions

The following table highlights the range of security functions and features implemented by the TOE.

Security function	Description
Access control	The TOE manages access control based on user IDs, user roles and access control lists. The TOE maintains access control lists for each object. Each ACL maps users and roles to the modules and functions that they are permitted to perform.

Security function	Description
Identification and authentication	The TOE requires that each user is successfully identified (user ID) and authenticated (password) before any interaction with the functionality of the TOE is permitted.
Security Management	The TOE provides functions that allow management of the TOE and its security functions. The TOE restricts access to the management functions based on the role of the user.

1.3.3 Physical scope of the TOE

The TOE comprises the ORNET Neuron web application hosted on a web server. A typical installation of the TOE can be found in Figure 1 below and identifies the various components of the ORNET Neuron architecture.

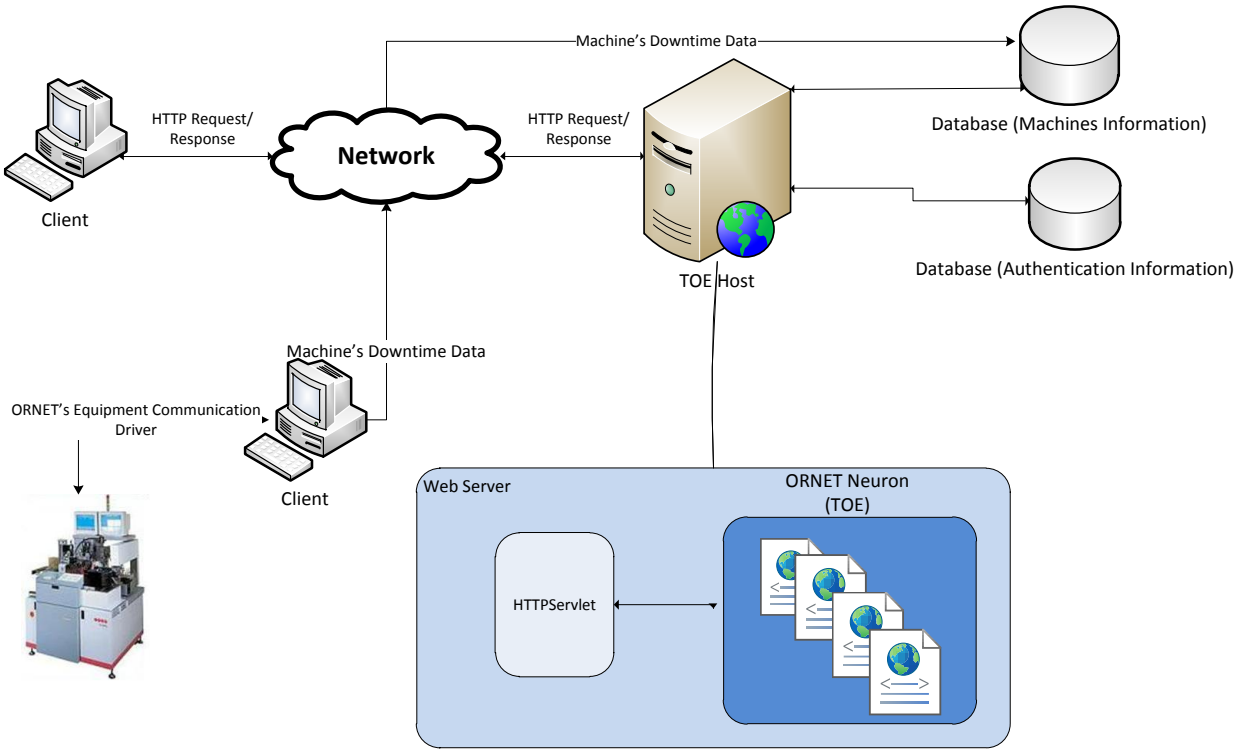

Figure 1 – ORNET Neuron Deployment

To collect data from the equipment or machine, ORNET's proprietary Equipment Communication Driver (SCES) will be installed in a PC and connected to the equipment or machine. The data will be sent direct to the database. This is not part of the TOE.

1.3.4 Supporting hardware, software and/or firmware

The TOE operates in a web server environment. In addition to requiring services from the environment to achieve its primary aim, the TOE also relies on the environment to maintain a secure posture so that the application cannot be compromised by factors out of the TSF Scope of Control.

The TOE requires the following of from the environment to function:

Minimum Software Requirements	Details
Operating System	Windows XP Service Pack 3 Windows Server 2003 Standard Edition Windows Server 2008 Standard Edition
Web Server	IIS version 5.1
Browser	Internet Explorer version 7.0 (recommended) Google Chrome version 15.0 Mozilla version 3.6.20 Safari version 5.0 Avant version 2012 Lite build 7 Orca version 1.2 build 6
Database	SQL Server 2008/2005/2000 Standard Edition Oracle 10g R2 x64/x86 Edition
Web installer package	Microsoft .Net Framework 2.0 Microsoft .Net Framework 3.5

Minimum Hardware Requirements	Details
Processor	Intel Dual Core 3.0GHz (for SQL Server) Intel Xeon Processor 2.0GHz (for Oracle)
RAM	4GB
Supported Architectures	X86 X64

The TOE requires, specifically, that the underlying environment provide appropriate authentication and authorisation controls for all users and administrators in the underlying environment (including the Operating System, RDBMS, and Web Server). The TOE also requires that the underlying environment, primarily the Client browser and Web Server, provide protection for authentication details traversing the network.

1.4 Logical scope of the TOE

The logical boundary consists of the security functionality of TOE is summarized below.

1.4.1 Access Control

The access control function permits a user to access the machines information only if a userID or role of the user has permission to perform the requested action on the resource. Access rules are stored in Access Control Lists associated with each object in the TSF Scope of Control.

1.4.2 Identification and Authentication

When a user issues a request to the TOE to access the modules as defined in section 1.3.1, the TOE requires that the user (being a User or Administrator) identify and authenticate themselves before performing any TSF mediated action on behalf of the user. The TOE checks the credentials presented by the user upon the login page against the authentication information in the database. Each users account only exists in the database that relates to the user organisation.

1.4.3 Security Management

The TOE contains various management functions to ensure efficient and secure management of the TOE:

- User management;
- Machine management

The TOE maintains seven roles within the TOE to ensure that the functions are restricted to only those users that need to have access to privileged functions. The roles maintained by the TOE are: Administrator, User Admin, Machine Admin, Reset Password, Data Entry, View Reports and Standard Control Limit roles. The functions above, and indeed, aspects of these functions, are restricted based on these roles.

2 Conformance Claim (ASE_CCL)

The ST and TOE are conformant to version 3.1 (Revision 3) of the Common Criteria for Information Technology Security Evaluation.

The following conformance claims are made for the TOE and ST:

- Part 2 conformant. Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1, Revision 3, July 2009.

- Part 3 conformant, EAL1. Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1, Revision 3, July 2009. Evaluation is EAL1.

3 Security objectives (ASE_OBJ)

3.1 Overview

The security objectives at an EAL1 level of assurance include concise statements of the objectives to be achieved by the supporting environment.

3.2 Security objectives for the environment

Identifier	Objective statements
OE.ENVIRONMENT	Those responsible for the TOE must ensure that appropriate authentication and authorisation controls for all users and administrators in the underlying environment (including the Operating System, RDBMS, and Web Server)
OE.COMMS	Those responsible for the TOE must ensure that the TOE environment, primarily the Client browser and Web Server, provides protection for authentication and user data traversing the network.
OE.ADMIN	The owners of the TOE must ensure that the administrator who manages the TOE is not hostile and is competent.
OE.PHYSICAL	Those responsible for the TOE must ensure that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.
OE.DATABASE	Those responsible for the TOE must ensure that the databases in the TOE environment have been correctly configured according to the principle of least privilege.
OE.MANAGEMENT	Those responsible for the TOE must ensure that all management of the TOE is performed through the management interfaces of the TOE and not through the underlying environment.

4 Security requirements (ASE_REQ)

4.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

4.2 SFR conventions

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions that are used within this ST to depict their application:

- **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].

- **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].

- **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.

- **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_IFF.1a and FDP_IFF.1b.

4.3 Security functional requirements

4.3.1 Overview

The security functional requirements are expressed using the notation stated in Section 4.2 and summarized in the table below.

Identifier	Title
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1a	Management of TSF data
FMT_MTD.1b	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles

4.3.2 FDP_ACC.1 Subset access control

Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the [**Access Control SFP**] on [**Subjects:** **a) HTTP request on behalf of users** **Objects:** **a) Protected resources (machine information)** **Operations:** **a) Viewing, modification of machine information**]
Dependencies:	FDP_ACF.1 - Security attribute based access control
Notes:	None.

4.3.3 FDP_ACF.1 Security attribute based access control

Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the [**Access Control SFP**] to objects based on the following: [**Subject attribute:** **a) ID of the user** **b) corresponding user role** **Object attributes:** **a) Access Control List**]
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**The operation is allowed, if:** **a) The Access Control List for an object permits the user ID to access that object; OR** **b) The Access Control List for an object permits the User Role to access that**

	Object.]
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**the Administrator role can access all records and functions**].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**None**].
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
Notes:	None.

4.3.4 FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
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.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

4.3.5 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
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.
Dependencies:	No dependencies.
Notes:	None.

4.3.6 FMT_MSA.1 Management of security attributes

Hierarchical to:	No other components.

FMT_MSA.1.1	The TSF shall enforce the [**Access Control SFP**] to restrict the ability to [***write or delete***] the security attributes [**that map user IDs to roles to only the users that are mapped**] to [**the Administrator role, User Admin Role**].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

4.3.7 FMT_MSA.3 Static attribute initialisation

Hierarchical to:	No other components.
FMT_MSA.3.1	The TSF shall enforce the [**Access Control SFP**] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [**Administrator, User Admin**] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Notes:	None.

4.3.8 FMT_MTD.1a - Management of TSF Data

Hierarchical to:	No other components
FMT_MTD.1a.1	The TSF shall restrict the ability to [***query, modify, delete, clear,*** [**Create**]] the [**Access Control Lists, Mapping of users to Roles, User accounts**] to [**Administrator and User Admin Role**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

Notes:	None.

4.3.9 FMT_MTD.1b - Management of TSF Data

Hierarchical to:	No other components
FMT_MTD.1b.1	The TSF shall restrict the ability to [***modify***] the [**User Password**] to [**the Administrator role, User Admin Role and the Reset Password Role**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

4.3.10 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [**a) mapping user IDs to roles** **b) creation of users with default passwords** **c) deletion of users** **d) changing of passwords** **e) management of Access Control lists** **f) manage machine information** **g) reset password**]
Dependencies:	No dependencies.
Notes:	None.

4.3.11 FMT_SMR.1 Security Roles

Hierarchical to:	No other components.

FMT_SMR.1.1	The TSF shall maintain the roles [**Administrator, User Admin, Machine Admin, Reset Password, Data Entry, View Reports and Standard Control Limit roles**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

4.4 Dependency analysis

SFR	Dependency	Inclusion
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1 FMT_MSA.3
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UID.2	No dependencies	N/A
FMT_MSA.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1 FDP_ACF.1 FMT_SMF.1 FMT_SMR.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1
FMT_MTD.1a - Management TSF Data	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 FMT_SMR.1
FMT_MTD.1b - Management of TSF Data	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 FMT_SMR.1

SFR	Dependency	Inclusion
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2

4.5 TOE security assurance requirements

The assurance package for the evaluation of the TOE is Evaluation Assurance Level 1 (EAL1).

EAL1 provides a basic level of assurance by a limited security target and an analysis of the SFRs in that ST using a functional and interface specification and guidance documentation, to understand the security behavior.

The analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TSF.

EAL1 also provides assurance through unique identification of the TOE and of the relevant evaluation documents.

This EAL provides a meaningful increase in assurance over unevaluated IT.

Assurance class	Assurance components
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMS.1 TOE CM coverage
	ALC_CMC.1 Labelling of the TOE
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing - conformance

Assurance class	Assurance components
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

4.6 Assurance measures

Assurance requirement	Assurance measures	Demonstration
ADV_FSP.1 Basic functional specification	Development	The development assurance measure provides all the necessary design documentation to support the analysis of the TOE for an evaluation at EAL1. The functional specification provides a detailed description of the security functions of the TOE.
AGD_OPE.1 Operational user guidance	Guidance documents	The operational user guidance documentation provides the guidance for end users, administrators and other parties who will utilise the TOE. These documents provide all the necessary instructions and direction for ensuring that the TOE is installed, configured, used and administered in a secure manner.
AGD_PRE.1 Preparative procedures		
ALC_CMC.1 Labelling of the TOE	Life cycle support	Configuration management measures provide the assurance that the TOE and supporting evidence can be uniquely identified.
ALC_CMS.1 TOE CM coverage		
ASE_CCL.1 Conformance claims	Security Target evaluation	Security Target evaluation assurance measures ensure that the claim to EAL1 can be accurately appraised.
ASE_ECD.1 Extended components definition		
ASE_INT.1 ST Introduction		
ASE_OBJ.1 Security objectives for the operational environment		

Assurance requirement	Assurance measures	Demonstration
ASE_REQ.1 Stated security requirements		
ASE_TSS.1 TOE summary specification		
ATE_IND.1 Independent testing - conformance	Tests	The tests assurance measure ensures that the TOE has been appropriately tested for the claimed set of security functions. The test plans for the TOE identifies the set of security functions that are to be tested, the procedures for establishing the test environment and also for conducting the test cases. The results of the tests are also recorded to provide evidence of test results.
AVA_VAN.1 Vulnerability survey	Vulnerability assessment	The TOE will be made available for vulnerability analysis and penetration testing.

5 TOE summary specification (ASE_TSS)

5.1 Overview

This section provides the TOE summary specification, a high-level definition of the security functions claimed to meet the functional and assurance requirements.

The TOE security functions include the following:

- **Access Control**
- **Identification and Authentication**
- **Security Management**

5.1.1 Access Control

The TOE enforces an access control policy on protected resource (machine information). After a user identifies and authenticates to the TOE, the TOE will check all HTTP request to the protected resource from the user. The TOE will permit a user to access a protected resource only if a userID or role of the user has permission to perform the requested action on the resource (**FDP_ACC.1, FDP_ACF.1**). The TOE maintains access control lists for each object within an organisation. Each ACL maps users and roles to the operations that they are permitted to perform on the object.

There are seven users maintained by the TOE. They are Administrator, User Admin, Machine Admin, Reset Password, Data Entry, View Reports and Standard Control Limit roles (**FMT_SMR.1**). Each type of user will have different access rights to a protected resource. All users will have a unique user ID.

5.1.2 Identification and Authentication

When a user issues a request to the TOE to access a protected resource (machine information), the TOE requires that the user (being a Administrator, User Admin, Machine Admin, Reset Password, Data Entry, View Reports and Standard Control Limit) identify and authenticate themselves before performing any TSF mediated action on behalf of the user (**FIA_UID.2, FIA_UAU.2**). The TOE checks the credentials presented by the user upon the login page against the authentication information in the database. Each users account only exists in the database that relates to the user organisation.

5.1.3 Security Management

The TOE contains various management functions to ensure efficient and secure management of the TOE (**FMT_SMF.1**):

- User management;
- Machine management;

User Management

The TOE only allows Administrator, User admin to query, create, delete, and modify users into the respective in the database.

They can also modify the access control list, mapping of users to roles as well as modifying the user accounts (**FMT_MTD.1a, FMT_MSA.1**).

Machine Management

The TOE only allows Administrator, User admin and Reset Password to modify passwords in the database (**FMT_MTD.1b**).

The TOE allows no one to change the default values of the TSF data and security attributes of the TOE (**FMT_MSA.3**).