aunav.NEXT
Security Target

v 1.2

PROYTECSA SECURITY S.L.
Ctra. Nacional 240, km 134,5
22500 Binéfar – Spain
Tel: +34-974 431 510
Fax: +34-974430627
URL: http://www.proytecsa.net
E-mail: info@proytecsa.net

LEGAL INFORMATION

Contents

1 ST INTRODUCTION

1.1 ST Reference

Title: aunav.NEXT Security Target

Version: v 1.2

Author: Javier Tallón (http://www.jtsec.es)

Date of publication (dd/mm/yyyy): 16/04/2015

1.2 TOE Reference

TOE Name: aunav.NEXT

TOE Version: v 1.0

TOE Feveloper: PROYTECSA SECURITY S.L.

Abbreviations of the TOE used in this ST: ROBOT. The terms “ROBOT” and “TOE” are used indistinctively in this declaration of Security, with the same meaning.

1.3 TOE Overview

The TOE is an articulated and extensible robot fitted with controls and intelligent handling that allows performing functions of reconnaissance, identification, and removal of any type of device or threat detected, especially the ones that are explosives. Its control system is remote so system operators are kept at a totally safe work distance.

1.3.1 Principal Security functionality

The TOE provides Security mechanisms to guarantee that only personnel duly authorized can use the TOE. The security characteristics are:

- *Authentication:* It is not possible to take any action with the TOE thru the communication RF and BT channels without previous authentication.
- *Encrypted RF communication channel with secure protocols:* The Security of the communications of the management console of the TOE (*Remote Case Controller*), is ensured with the implementation of the encrypted secure protocol AES-128 ECB.

- *Service priority in the access with RF:* data and orders sent thru the remote case controller have preference in the communication with the TOE.

1.3.2 Non-TOE Hardware/Software/Firmware

To handle the TOE the following components are necessary (see Fig):

- *Remote Case Controller:* case that allows the control of the movements of the TOE.

Type	**Name and version**
Hardware	Embedded Computer VBOX-3600-i7 SILVUS SC3800 dual-band MIMO radio Unit
Software	Aunav.NEXT Controller Suitcase v1.0 Windows Embedded 7 Standard or later

- *Bluetooth PS3 Gamepad:* to control the TOE movements without the necesity to use the *Remote Case Controller.*

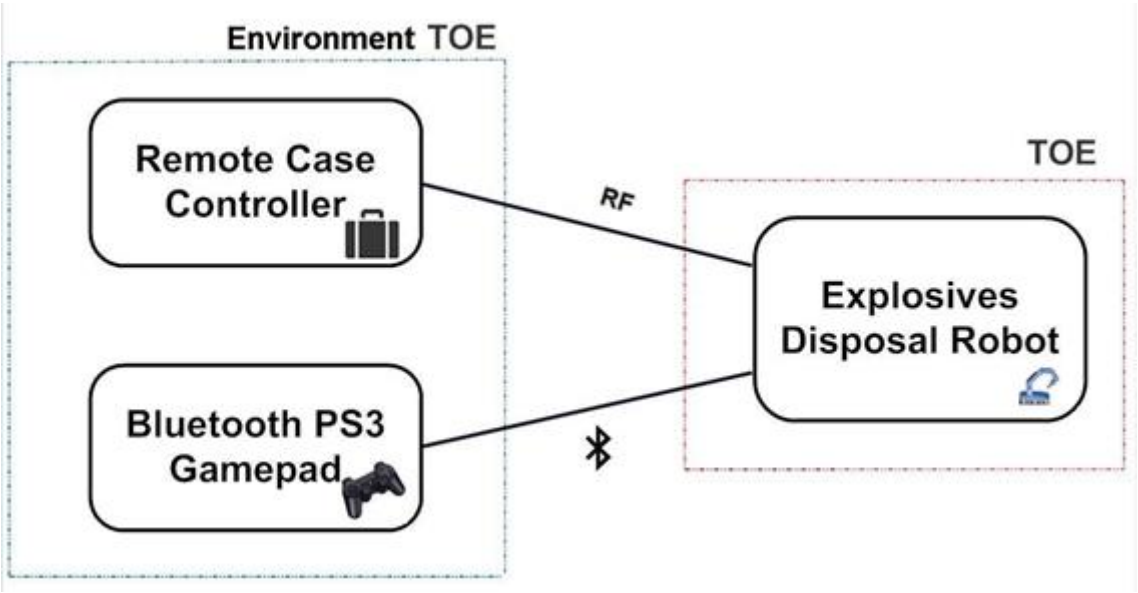

Fig.

1.3.3 Non-TOE Security Features

The TOE is delivered with the “Bluetooth PS3 Gamepad” and the “Remote Case Controller”. This last one could include extra security features no subjected to evaluation, so no guarantees are established over the former in this ST.

1.4 TOE Description

1.4.1 Logical scope

The TOE logical scope is defined grouping functionalities in the following functional classes that will be detailed afterwards in this Security Target.

1.4.1.1 Authentication of the communication channels

The authentication of the Bluetooth channel is given by the knowledge of the authentication key established in the pairing between PS3 Gamepad and the TOE according to the Bluetooth protocol, being impossible to perform any action on the TOE without knowing that key.

The authentication in the RF channel is given by the knowledge of the encryption key used to communicate, being impossible to perform any action on the TOE without knowing that key.

1.4.1.2 Protection of communication channels

The ROBOT encrypts the RF communication channel. The security of the communications with the TOE from the control case, are ensured with the implementation of the encrypted secure protocol AES-128 ECB. The encryption password is configured during the manufacture process and is not changed nor destructed during the operation.

1.4.1.3 Service Priority in RF access

In the communications with the TOE preference is given to data and commands sent thru the control suitcase over the ones sent by Bluetooth.

1.4.2 Physical scope

The Physical scope of the TOE is summarized in the following table:

Name	Type	Description
aunav.NEXT Hardware The robot is distributed with the software pre-installed.	Hardware	Robot hardware
aunav.NEXT Software Pre-installed in hardware.	Software	Software that is executed on robot hardware
Preparation manual	Documento	Manual used to install TOE and

Distributed on CD.		prepare the operational environment in a secure way.
Operation Manual Distributed on CD.	Document	Manual used to operate TOE in a secure way.

1.4.3 TOE Evaluated configuration

The TOE is distributed in one unique version submitted to evaluation.

2 CONFORMANCE CLAIMS

This Security Target and the TOE described are in accordance with the requirements of Common Criteria 3.1R4.

This Security Target claims conformance with the following parts of Common Criteria:

Conformance with [CC31p2].

Conformance with [CC31p3].

The methodology to be used for the evaluation is described in the “Common Evaluation Methodology” of the Common Criteria standard of September 2012, Version 3.1 revision 4 [CEM31] defining a level of evaluation assurance EAL2 + ALC_FLR.1.

This Security Target does not claims conformance with any Protection Profile.

3 SECURITY PROBLEM DEFINITION

This section describes the security aspects of the ROBOT operational environment and its expected use in said environment. It includes the declaration of the TOE operational environment that identifies and describes:

- the alleged known threats that will be countered by the TOE;
- The organizational security policies that the TOE has to adhere to;
- The TOE usage assumptions in the suggested operational environment.

We will begin defining Assets, Subjects and Agents of threats.

Assets

A.Control The authenticity of the control data that allow to control the ROBOT when in transit from the suitcase or from the Bluetooth controller.

A.Content The content of the communication between suitcase and ROBOT

Subjects

S.Trustworthy Trustworthy users: TOE users, authorized operators and administrators, persons in charge of installation and system maintenance as well as environment security.

Threat agents

S.Attackers A human being or process that acts in its name, outside the TOE and whose objective is to modify or corrupt the protected files of the TOE. The attacker, at best, has knowledge of obvious vulnerabilities, has a low ability level and limited resources. The attacker has no physical access to the TOE but has access to the environment of the former.

3.1 Assumptions

The assumptions when using the TOE are the following:

- ***AS.PERSONNEL***: it is supposed that the users of the TOE (S. Trustworthy) behave according to expectations and do no act maliciously.
- ***AS.PHYSICAL***: it is presumed that there is no physical access to the TOE, that it is protected by appropriate security measures to guarantee the access only to authorized personnel (S. Trustworthy). The same way, the gamepad and the ROBOT remote case controller are presumed protected. This makes the

attacks through them not possible as not being accessible by attackers (S. Attackers).

3.2 Threats to Security

This section identifies the threats to assets that require protection by the TOE. The threats are defined in terms of assets concerned, attackers and the adverse action that materializes the threat.

- ***T.COMM_RF***: one (S. Attacker) impersonate the control suitcase and takes over the control of the TOE (A. Control) or eavesdrop upon its communications (A. Content).
- ***T.COMM_BT***: one attacker (S. Attacker) impersonate the Bluetooth control and takes over the TOE control (A. Control).

Denial of Services attacks are considered out of the scope of this ST.

3.3 Organizational Security Policies (OSP)

The organizational Security policies are defined as follows.

- ***P.PRIORITY***: the data and commands sent thru the remote case controller have preference in communications with the TOE, over the ones sent thru the Bluetooth control.

4 SECURITY OBJECTIVES

The security objectives are high level declarations, concise and abstract of the solution to the problem exposed in the former section, which counteracts the threats and fulfills the security policies and the assumptions. These are divided in two types:

- the security objectives for the TOE and
- the security objectives for the operational environment.

4.1 Security objectives for the TOE

The security objectives for the TOE are listed as follows:

- ***O.AUTHENTICATION:*** the TOE will not allow the access to its interfaces prior to authentication.
- ***O.ENCRYPTION:*** Encryption of RF channel. The information transmitted thru the radio frequency channel will be encrypted.
- ***O.PRIORITY:*** the data and commands sent thru the remote case controller have preference in communications with the TOE, over the ones sent thru the Bluetooth control.

4.2 Security targets for the operational environment

The targets of the TOE security for the operational environment are listed as follows:

- ***OE.PERSONNEL:*** the environment of operation of the TOE has to guarantee that the TOE operators behave as expected and not maliciously.
- ***OE.PHYSICAL:*** the operation environment of the TOE has to warranty the impossibility of physical access to the TOE, the Bluetooth control and the robot remote case controller.

4.3 Reasoning of the Security targets

The following table maps the security targets of the TOE to the threats of the security problem established.

Security objectives for the TOE	**Threats**	**Justification**
O.AUTHENTICATION	T.COMM_BT T.COMM_RF	The security objective O.AUTHENTICATION mitigates the threats T.COMM_BT and

		T.COMM_RF as it doesn't allow any action prior to authentication with the ROBOT.
O.ENCRYPTION	T.COMM_RF	The security objective for the TOE O.ENCRYPTION mitigates the threat T.COMM_RF with the use of AES 128 ECB encryption, whose key is uploaded to the TOE during the manufacturing process.

The following table maps the security objectives of the TOE to the security policies established.

Security objectives for the TOE	**OSPs**	**Justification**
O.PRIORITY	P.PRIORITY	Security objective for the TOE O.PRIORITY enforces directly the policy P.PRIORITY

The following table maps the security objectives for the operational environment to the assumptions defined in the security problem.

Security objectives for the operational environment	**Assumptions**	**Justification**
OE.PERSONNEL	AS.PERSONNEL	The security objective for the operational environment OE.PERSONNEL upholds directly the compliance of the assumption AS.PERSONNEL
OE.PHYSICAL	AS.PHYSICAL	The security objective for the operational environment OE.PHYSICAL upholds directly the compliance of the assumption AS.PHYSICAL

5 SECURITY REQUIREMENTS

This section defines the Security functional requirements (SFRs) and the Security assurance requirements (SARs) that fulfill the TOE. Assignment, selection and iteration operations have been made, adhering to the following conventions:

1. Assignments. The word "***assignment***" is maintained and the resolution is presented in boldface, italic and blue color.
2. Selections .The word "***selection***" is maintained and the resolution is presented in boldface, italic and blue color.
3. Iterations. It includes "**/"** and an "**identifier**" following requirement identifier that allows to distinguish the iterations of the requirement. Example: **FCS_COP.1 / RF.**

No refinements exist.

5.1 Extended components definition

No extended security functional components have been defined in this security target.

No extended security assurance components have been defined in this security target.

5.2 Security Functional Requirements (SFRs)

5.2.1 Authentication

5.2.1.1 FIA_UAU.2/BT 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.

Application note: The requirements FIA_UAU.2/BT defines the necessity to authenticate to the TOE when the control is connected thru the Bluetooth channel. The said authentication is given implicitly by the knowledge of the communication key between both entities.

5.2.1.2 FIA_UAU.2/RF 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.

Application note: The requirement FIA_UAU.2/RF defines the necessity to authenticate to the TOE when the control suitcase connects thru RF channel .The said authentication is given implicitly by the knowledge of the communication key between both entities.

5.2.2 Communication channel protection

5.2.2.1 FCS_COP.1/RF Cryptographic operation

FCS_COP.1.1 The TSF shall perform [***assignment: encryption and decryption o the radio frequency channel between ROBOT and remote case controller using the key assigned during the manufacture of the TOE to the RF receiver/emitter. This key isn't changed nor destroyed.***] In accordance with a specified cryptographic algorithm [***assignment: AES (ECB)***] and cryptographic key sizes [***assignment: 128***] that meet the following: [***assignment: none***].

Application note: The RF channel encryption key is upload in the ROBOT during manufacture. The said key is neither changed nor destroyed during TOE operation. Any change requires the TOE to be put under maintenance, out of any operation.

5.2.3 Communication channel priority

5.2.3.1 FRU_PRS.1 Limited priority of service

FRU_PRS.1.1 The TSF shall assign a priority to each subject in the TSF.

FRU_PRS.1.2 The TSF shall ensure that each Access to [***assignment: the control of the ROBOT using BT/RF channels]*** shall be mediated on the basis of the subjects assigned priority.

Application note: This requirement models the priority access of the RF remote case controller over the BT gamepad over the robot.

5.3 Security Functional Requirements rationale

5.3.1 Necessity and sufficiency analysis

The following table provides the TOE security objectives mapping to the Security Functional Requirements. Included is the necessity and sufficiency analysis to fulfill the security objectives of the TOE.

Security objective	**Functional requirement**	**Justification**
O.AUTHENTICATION	FIA_UAU.2/RF	FIA_UAU.2/RF contributes to fulfill the objective as it forces the user to know the key before taking any action thru the RF channel. Together with FIA_UAU.2/BT it is sufficient to fulfill the security objective for the TOE T.AUTHENTICATION.
	FIA_UAU.2/BT	FIA_UAU.2/BT contributes to fulfill the objective as it forces the user to know the key before taking any action thru the BT channel. Together with FIA_UAU.2/RF it is sufficient to fulfill the security objective for the TOE T.AUTHENTICATION
O.ENCRYPTION	FCS_COP.1/RF	FCS_COP.1/RF contributes to fulfill this target as it uses the AES ECB algorithm to encrypt and decrypt the data that is sent from the TOE remote case controller thru the radio frequency channel. In the encryption/decryption of the data with the AES ECB algorithm a 128 bits key is used, which is uploaded during the manufacture of the TOE.

O.PRIORITY	FRU_PRS.1	FRU_PRS.1 enforces this objective directly when establishing a priority in the access to the robot control between the Bluetooth and RF channels.

5.3.2 Dependency analysis

FIA_UAU.2/RF	FIA_UID.1	See (1)
FIA_UAU.2/BT	FIA_UID.1	See (1)
FCS_COP.1/RF	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	See (2)
FRU_PRS.1	There are no dependencies	OK

1. The dependencies of FIA_UAU.2/RF nor FIA_UAU.2/BT have not been satisfied

The reason is that in both cases, the dependency with FIA_UID.1 is not relevant to the described TOE as there is no identification functionality that allows to distinguish the user in these contexts; the identification is implicit and is associated with the authentication functionality.

2. The dependencies of FCS_COP.1/RF have not been satisfied.

The reason is that the encryption key used in the RF channel is uploaded to the ROBOT during manufacture. The said key is not changed nor destroyed during TOE operation. Any change would require the TOE to be placed under maintenance outside real operation. Thereafter it is justified that the inclusion of the dependencies FCS_COP.1 is not necessary regarding the establishment, renewal and possible destruction of the password.

5.4 Security assurance requirements (SARs)

The security assurance requirements are the ones associated to the package EAL 2 incremented with the component ALC_FLR.1 (as specified in [CC31p3]). These are listed in the following table:

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.1 Basic Flaw remediantion
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components 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
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

5.5 Justification of the assurance requirements

The assurance requirements have been selected according to the evaluation assurance level EAL 2 increased with the component ALC_FLR.1. The selected assurance level is appropriate for the threats specified in the security problem in the operational environment described.

6 TOE SUMMARY SPECIFICATION

6.1 Authentication

6.1.1 RF channel

Before the delivery to the end user of the TOE an encryption key is configured in the emitter/receiver of the SILVUS radio frequency unit of the TOE and in the one belonging to the remote case controller that ensures the communications between them.

The TOE requires user authentication thru the RF channel before taking any other action. The said authentication is given implicitly by the knowledge of the channel encryption key.

The implementation of this requirement is direct as the ignorance of the key will preclude the use of the communication channel. Like this, users or attackers that ignore the encryption key will not be able to eavesdrop the channel nor introduce data in it.

Moreover the implementation of the TOE will only admit RF communication channels and Bluetooth, being the only way to send orders to the TOE in its evaluated state, enforcing the FIA_UAU.2/RF requirement.

Associated requirements: FIA_UAU.2/RF.

6.1.2 Bluetooth channel

The ROBOT pairs initially in a physical way when connecting the USB cable to the Bluetooth PS3 Gamepad. Like that a channel key is established. This operation is performed prior to the end user TOE delivery.

The TOE requires the authentication of the users thru the BT channel before taking any other action. The said authentication is given implicitly because it implies the knowledge of the channel encryption key.

The implementation of this requirement is direct as the ignorance of the key will preclude the use of the communication channel. Like this, users or attackers that ignore the encryption key will not be able to eavesdrop the channel nor introduce data in it.

Moreover the implementation of the TOE will only admit RF and Bluetooth communication channels, being the only way to send orders to the TOE in its evaluated state, enforcing the FIA_UAU.2/BT requirement.

Associated requirements: FIA_UAU.2/BT.

6.2 RF channel communication protection

The communication channel between TOE and remote case controller thru radio frequency is encrypted with AES 128 ECB. The key used to encrypt the data is already introduced in the TOE and the remote case controller when operating the TOE. This key cannot be changed nor eliminated without putting the TOE under maintenance, precluding real operations.

The implementation of the requirement is made thru a Freescale Crypto Engine cryptographic chip. This will process all the information transmitted thru the channel encrypting the information sent and decrypting the information received, using the key configured to that purpose when moving the TOE to its evaluated state.

Associated requirements: FCS_COP.1/RF.

6.3 Communication channel priority

The TOE implements a fixed and pre-established priority order in the access to the TOE control, like this there is always a priority of the RF channel over the BT channel.

To implement this requirement, prior to processing any petition from the Bluetooth channel, there is a checkup that no user is connected (logged in) to the RF channel, so petitions from the Bluetooth will be attended when the RF channel is not in use. Thus the requirement is implemented.

Associated requirements: FRU_PRS.1

7 REFERENCES

[CC31p2]	Common Criteria for Information Technology Security Evaluation. Versión 3.1 Revisión 4 Part 2. September 2012
[CC31p3]	Common Criteria for Information Technology Security Evaluation. Versión 3.1 Revisión 4 Part 3. September 2012
[CEM31]	Common Methodology for Information Technology Security Evaluation. Versión 3.1 Revisión 4. September 2012

8 ACRONYMS

All acronyms used in [CC31p2] and [CC31p3] can be applied

CCN	Centro Criptológico Nacional
CC	Common Criteria
EAL	Evaluation Assurance Level
I&A	Identification & Authentication
RF	Radio Frequency
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target Of Evaluation
TSF	TOE Security Functionality
BT	Bluetooth
PS	Play Station
AES	Advanced Encryption Standard
ECB	Electronic Codebook