Certification Report

IAI/MLM Autonomous Air Combat Maneuvering Instrumentation (AACMI) Trusted Data Guard (TDG) v1.0

Sponsor and developer: ***IAI/MLM***
P.O. Box 45, Beer-Yaakov
70350
Israel

Evaluation facility: ***Brightsight***
Delftechpark 1
2628 XJ Delft
The Netherlands

Report number: **NSCIB-CC-12-36874-CR**

Report version: **1**

Project number: **NSCIB-CC-12-36874**

Authors(s): **Denise Cater**

Date: **August 13, 2014**

Number of pages: **14**

Number of appendices: **0**

Head office Apeldoorn:
Boogschutterstraat 11A
P.O. Box 541
7300 AM Apeldoorn
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

Location Apeldoorn:
Vissenstraat 6
P.O. Box 541
7300 AM Apeldoorn
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

Location Enschede:
Josink Esweg 10
P.O. Box 337
7500 AH Enschede
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 859

TÜV Rheinland Nederland B.V. is a registered company with the Amsterdam Chamber of Commerce under number 27288788
info@nl.tuv.com
www.tuv.com/nl

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 4 (ISO/IEC 15408)
Certificate number	**C12-36874**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	***IAI/MLM*** **Located in Beer-Yaakov, 70350 Israel**
Product and assurance level	**IAI/MLM Autonomous Air Combat Maneuvering Instrumentation (AACMI) Trusted Data Guard (TDG) v1.0,** Assurance Package: ▪ EAL4 augmented with ASE_TSS.2
Project number	**NSCIB-CC-12-36874-CR**
Evaluation facility	**Brightsight BV located in Delft, the Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 4 (ISO/IEC 18045)

Common Criteria Recognition Arrangement for components up to EAL4

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 4 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 4. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Validity

Date of issue : **13-08-2014**

Certificate expiry : **13-08-2019**

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

TÜV Rheinland Nederland B.V.
P.O. Box 541
7300 AM Apeldoorn
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

CONTENTS:

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products.

A part of the procedure is the technical examination (evaluation) of the product according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025, General requirements for the accreditation of calibration and testing laboratories.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

Recognition of the certificate

The Common Criteria Recognition Arrangement and SOG-IS logos are printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the IAI/MLM Autonomous Air Combat Maneuvering Instrumentation (AACMI) Trusted Data Guard (TDG) v1.0 (hereinafter referred to as "TDG v1.0"). The developer of the TDG v1.0 is IAI/MLM located in Beer-Yaakov, Israel and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The IAI/MLM AACMI system is used for training fighter pilots. The IAI/MLM AACMI system consists of a pod (referred to as 'EHUD') that is attached to a fighter aircraft to continuously record and broadcast relevant training information such as position, speed, angle-of-attack, amount of weapons left, the firing of simulated weapons, etc. The combination of the training information is then used to build and maintain a coherent and realistic view of the current situation during the training flight.

The training information is recorded on a Removable Storage Media (RSM) or Simulation Platform PCMCIA (SiPP) flash memory card and broadcast, via an unclassified AACMI RF Data Link network, to other IAI/MLM AACMI-systems participants.

All the EHUD activities are managed and controlled by an on-board Data Processor (referred to as 'IMM MK5')

The information to be broadcasted via the AACMI RF Data Link can contain unauthorized information, which would allow attackers to derive detailed weapons performance information. Also, residual information left in the IMM MK5 memories after completing the exercise and shutdown pod power might facilitate attackers to get said restricted information as well.

The TDG consists of two components in EHUD pod: the SDW (Security Double Wall) and IMM MK5 (Integrated Main Module).

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands and was completed on 30 July 2014 with the delivery of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*. The certification was completed on 13 August 2014 with the preparation of this Certification Report. It should be noted that the certification results only apply to the specific version of the product as evaluated.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the TDG v1.0, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the TDG v1.0 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]*[1] for this product provide sufficient evidence that it meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ASE_TSS.2 (TOE summary specification with architectural design summary).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 4 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the TDG v1.0 evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the TDG v1.0 from IAI/MLM located in Beer-Yaakov, Israel.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Part Number[2]	Version[3]
Hardware	Security Double Wall	B-18600-***-300000	N/A
	IMM MK5	B-18500-+++-300000	N/A
Software	FTG software	B-00707-500000	A
	FTG firmware	B-610-00197	#
	HTG firmware	B-610-00198	#

To ensure secure usage a set of guidance documents is provided together with the TDG v1.0. Details can be found in section 2.5 of this report.

2.2 Security Policy

The major security features provided by the TOE are:

- The TOE filters: the TOE ensures that the end user filtering policy, as depicted in a CAT table, is followed: no unauthorized information is passed to the Transmitter;
- The TOE filters under failure: the TOE tests itself upon start-up and, when a failure is detected, ensures that no unauthorized information is passed to the Transceiver. In addition, when the TOE undergoes a single failure during operation, it ensures that still no unauthorized information is passed to the Transmitter;
- The TOE is tamper-evident: if it has been physically tampered with, this will be detectable;
- The TOE clears residual information in its non-volatile memory upon power down.
- The SDW protects against writing to its non-volatile memory.
- The IMM MK5 protects against accidental writing to its volatile memory.

2.3 Assumptions and Clarification of Scope

As far as security is concerned, the TOE exists in four distinct security environments:

- The Flight Environment: the TOE is connected to an Aircraft;
- The O-Level Environment: the TOE is stored at an Airbase;
- The I-Level Environment: the TOE is at an Intermediate Repair Facility;
- The D-Level Environment: the TOE is at the Developer.

[2] "***" means any 3 digits. This value reflects the embedded CAT table and non-security-relevant hardware changes. "+++" means any 3 digits. This value reflects non-security-relevant hardware changes

[3] "#" means any digit. This value reflects the embedded CAT table (which itself is out of scope of the evaluation)

The normal transitions between these environments are provided in Figure 1. Each environment contains its own threats, assumptions and organisational security policies (OSP). When transitioning between the D-Level and I-Level environments (so the TOE is not contained within the Pod), the TOE is transported in a tamper evident box.

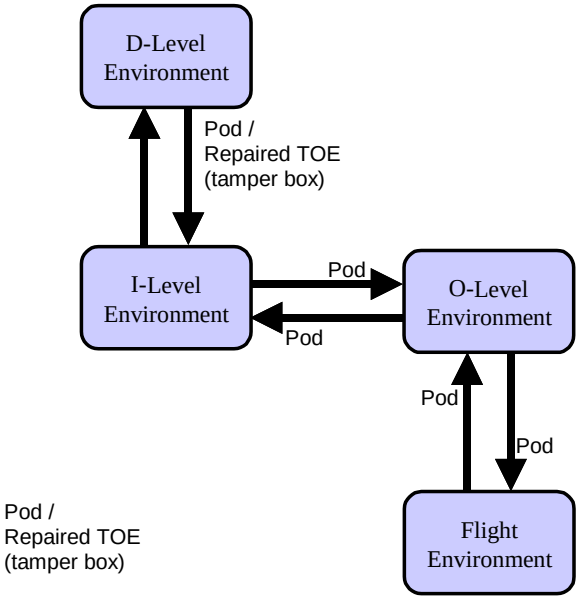


Figure 1 Possible transitions between environments

2.3.1 Usage assumptions

The TOE is contained within the EHUD pod, which is a closed system requiring no user or administrator interaction when installed in the Flight Environment.

For the other environments the following assumptions apply:

- The TOE assumes that in the O-Level environment, the Pod is never opened.
- The O-Level Staff will inspect (monitor) the Pod for failures, and if a failure is found the Pod is transferred to the I-Level Environment.
- All TOEs brought into the I-Level Environment from the D-Level Environment will be inspected by the I-Level Staff to determine whether physical tampering has occurred. If this has occurred, the TOE will be handled according to the appropriate procedures.
- The TOE is normally never physically opened in the I-Level Environment. If TOEs are found to be malfunctioning, the I-Level Staff will send the TOE to the D-Level Environment.

2.3.2 Environmental assumptions

The Flight Environment is the environment in which the TOE is operational. In this environment the TOE is contained in a Pod, and the Pod is attached to the wing of an operational aircraft.

The O-Level Environment is typically an Airbase. In this environment the TOE is contained in a Pod, and this Pod is stored on the Airbase.

The I-Level Environment is an Intermediate Repair Facility, which may be on the same location as the O-Level environment (i.e. an Airbase).

When the TOE is broken, the I-level Environment can only replace the TOE in the Pod with a new identical TOE: the TOE is never repaired in this environment. The I-Level Environment receives broken-down Pods (containing the TOE) from the O-Level Environment. It then disassembles the Pod, diagnoses the Pod, repairs/replaces faulty non-TOE parts or replaces the TOE and sends the Pod back to the O-Level Environment. Any parts that were replaced are sent to the D-level Environment for further repair or disposal.

The D-Level Environment is the environment of the Developer. It produces Pods (containing the TOE) and sends these to the I-Level Environment. It also receives faulty parts (including TOEs) from the I-Level Environment. It sends back repaired or new parts (including TOEs) to the I-Level Environment.

Furthermore, the following organisational security policies relate to the environment in which the TOE shall be operated (for the detailed and precise definition of the organisational security policy refer to the *[ST]*, chapter 3):

- P.F.CORRECT_OUT detailing the TOE must not transmit data objects containing unauthorised information to the transmitter while in the Flight environment, as defined in [ST] section 3.2.2;
- P.O.INSPECT detailing the inspection of the POD for failures in the O-Level environment, as defined in [ST] section 3.3.2;
- P.I.INSPECT, P.I.NO_OPEN and P.I.SEALED detailing the inspection of the POD for failures, receiving the sealed POD and the policy to never open the POD in the I-Level environment, as defined in [ST] section 3.2.2;
- There are no Organisation Security Policies for the D-Level environment.

2.3.3 Clarification of scope

The software and firmware of the IMM MK5 and the CAT table (embedded within the SDW firmware) are not included in the scope of the TOE, as detailed in Section 2.4 of this report.

As detailed in section 2.3.2 of this report, there are a number of environmental assumptions and OSPs that counter threats to the TOE. These items must be addressed in the operational environment in order to ensure all threats to the TOE are countered, as the TOE does not provide complete defence against physical attack. The two measurement layers that prevent modification of the TOE and/or POD to bypass the filter are:

- Tamper seals on the casing of the TOE (FPT_PHP.1)
- Delivery to the I-Level Environment in a tamper evident box

Both measurement layers have been subject of penetration tests, as detailed in section 2.6.2 of this report.

2.4 Architectural Information

The target of evaluation (TOE) Trusted Data Guard (TDG) consists of the following components:

- The SDW which receives ‘data objects’ from the IMM MK5 and ‘data objects’ from the Receiver. The SDW contains two filters:
  - Firmware Trusted Guard - removes unauthorized information according to the rules defined in the CAT table.
  - Hardware Trusted Guard - verifies whether the data received from FTG indeed does not contain unauthorized information (according to the rules defined in the CAT table), and if so forwards it as authorized data to the transmitter.
- The IMM MK5, the main Data Processor in EHUD pod: It contains Firmware (not part of the TOE), Software (not part of the TOE) and an RWD:
  - The RWD, a Residual (non-volatile) memory Write Disable mechanism in IMM MK5 prevents write access (unless a SUC is inserted) to the non-volatile storage of the IMM MK5.

The exact rules to determine which information is unauthorized are defined in a classified customized CAT table. The CAT is a Certified Allocation Table embedded in the firmware of the SDW and holds patterns which identify certified data objects allowed to pass through to the transmitter. While the SDW firmware is included in the TOE, the embedded CAT table is not part of the TOE. The CAT is prepared together with the final user and provides a fast and modular way to configure the SDW security filter and match it to the specific security requirements of the end user. Non-volatile memory components in the IMM MK5 are protected against accidental writing by the Software. RWD is an

electrical circuit that is intended to enable writing to some of the non-volatile memory of the IMM MK5 with the intention of software updates.

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Part Number	Version
[UG] User Guide	B-00119-100000	Issue B
[TLTL] Tamper Label Track Log	B-720-00125	Issue E
[HWDD] HW Design documentation for SDW FPGAs	B-18617-300000	Issue C

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer has performed testing at a TSFI and subsystem level. The developer has performed manual testing of the IMM MK5 and extensive automated testing of the SDW.

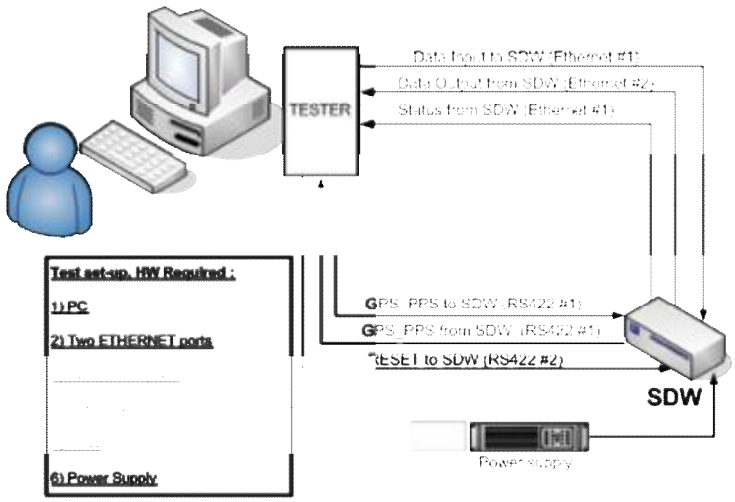
The evaluators repeated all developer tests of the SDW. The evaluators performed 4 additional functional tests of the SDW, tested the tamper seal on the TOE, and performed an analysis of the IMM MK5 RWD circuitry against the schematics during a visit to the development site in Beer-Yaakov, Israel.

2.6.2 Independent Penetration Testing

The evaluators performed penetration testing of the tamper seals on the TOE casings and penetration testing of the tamper evident box in which the TOE is to be delivered.

2.6.3 Test Configuration

For functional testing, the TOE was installed according to the guidance and connected to the SDW test tool (Tester) as shown below:



The SDW Tester Application runs on Windows XP SP3 and utilises a set of scripts for execution of the test cases.

In addition to the test configuration above, a Quartus II (Altera) tool is used to update the CAT table prior to execution of the test cases.

All SDW test cases were executed on the above test configuration.

To perform penetration testing of the tamper seals the evaluators received the seals glued on the TOE, as if they were delivered to a customer. For penetration testing of the tamper evident box the actual box and lock was used, as will be used in delivery of the TOE to the customer.

2.6.4 Testing Results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its ST and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Evaluated Configuration

The TOE is defined uniquely by its name and version number TDG v1.0. This can be verified by the customer as detailed in *[UG]* section 8.5.

It should be noted that the part numbers for the hardware implicitly identify the versions of software/firmware installed on the hardware.

2.8 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[4] which references several Intermediate Reports and other evaluator documents. The verdict of each claimed assurance requirement is given in the following tables:

Development		**Pass**
Security architecture	ADV_ARC.1	Pass
Functional specification	ADV_FSP.4	Pass
Implementation representation	ADV_IMP.1	Pass
TOE design	ADV_TDS.3	Pass

Guidance documents		**Pass**
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass

Life-cycle support		**Pass**
Configuration Management capabilities	ALC_CMC.4	Pass
Configuration Management scope	ALC_CMS.4	Pass
Delivery	ALC_DEL.1	Pass
Development security	ALC_DVS.1	Pass
Life-cycle definition	ALC_LCD.1	Pass
Tools and techniques	ALC_TAT.1	Pass

[4] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

Security Target		Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.2	Pass

Tests		Pass
Coverage	ATE_COV.2	Pass
Depth	ATE_DPT.1	Pass
Functional tests	ATE_FUN.1	Pass
Independent testing	ATE_IND.2	Pass

Vulnerability assessment		Pass
Vulnerability analysis	AVA_VAN.3	Pass

Based on the above evaluation results the evaluation lab concluded the TDG v1.0, to be **CC Part 2 conformant, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented by ASE_TSS.2**. This implies that the product satisfies the security technical requirements specified in Security Target for IAI/MLM Autonomous Air Combat Maneuvering Instrumentation (AACMI) Trusted Data Guard (TDG) v1.0, Issue E.

2.9 Evaluator Comments/Recommendations

2.9.1 Obligations and hints for the developer

To remain within the scope of the certificate the developer must only apply the changes as described in *[SSR]* and *[FLASH]*. This policy and procedure detail the limited (non-security-relevant) changes that can be made to the hardware.

The CAT table is outside the scope of the evaluation and so can be updated as necessary. However, no other firmware change is permissible in the evaluated version. No FTG software change is permissible within the evaluated version.

2.9.2 Recommendations and hints for the customer

The User Guidance (as outlined in Section 2.5 of this report) contains necessary information about the usage of the TOE. In particular the customer must ensure the environmental constraints, which provide countermeasures against physical attacks, are implemented in the operational environments to ensure the TOE is physically protected at all times. This guidance is documented in User Guide (*[UG]*) and Tamper Label Track Log (*[TLTL]*).

Customer must check the received TOE with tamper seals according to the user guidance, *[UG]*.

The developer of the IMM MK5 software (assumed to be IAI/MLM) must apply the guidance provided in HW Design documentation for SDW FPGAs (*[HWDD]*)

3 Security Target

The Security Target for IAI/MLM Autonomous Air Combat Maneuvering Instrumentation (AACMI) Trusted Data Guard (TDG) v1.0, Issue E, 17 July 2014 *[ST]* is included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

AACMI	Autonomous Air Combat Maneuvering Instrumentation
CAT	Certified Allocation table
FTG	Firmware Trusted Guard
HTG	Hardware Trusted Guard
IAI	Israel Aerospace Industries
IMM	Integrated Main Module
IT	Information Technology
ITSEF	IT Security Evaluation Facility
MK5	Mark 5
MLM	Subsidary company of IAI
NSCIB	Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging
PCMCIA	Personal Computer Memory Card International Association
PP	Protection Profile
RWD	Residual (non volatile) memory Write Disable
RSM	Removable Storage Media
SDW	Security Double Wall
SiPP	Simulation Platform PCMCIA
TDG	Trusted Data Guard
TOE	Target of Evaluation
TSFI	TOE Security Functionality Interface

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, version 3.1, Revision 4, September 2012.
[CEM]	Common Methodology for Information Technology Security Evaluation, version 3.1, Revision 4, September 2012.
[ETR]	Brightight, Evaluation Technical Report IAI/MLM Autonomous Air Combat Maneuvering Instrumentation (AACMI) Trusted Data Guard (TDG) v1.0, EAL4+, version 3.0, 30 July 2014.
[FLASH]	Flash Management for TDG System, Rev. C
[HWDD]	HW Design documentation for SDW FPGAs, B-18617-300000, Issue C
[NSCIB]	Nederlands Schema for Certification in the Area of IT Security, Version 2.0, 1 July 2011.
[SSR]	System Security Requirements for the SDW, Issue E
[ST]	Security Target for IAI/MLM Autonomous Air Combat Maneuvering Instrumentation (AACMI) Trusted Data Guard (TDG) v1.0, Issue E, 17 July 2014.
[TLTL]	Tamper Label Track Log, B-720-00125, Issue E
[UG]	User Guide, B-00119-100000, Issue B

(This is the end of this report).