AUSTRALASIAN INFORMATION SECURITY EVALUATION PROGRAM

Certification Report

Certificate Number: 2003/29

Compucat

Serial Data Regulator Version 1.0

Issue 1.2
October 2003

Issued by:

Defence Signals Directorate - Australasian Certification Authority

Executive Summary

This report describes the findings of the evaluation of Compucat's Serial Data Regulator Version 1.0, developed by Compucat Research Pty Ltd, to the Information Technology Security Evaluation Criteria evaluation level E6. The report concludes that the product has met the target assurance level of ITSEC E6, and includes recommendations by the Australasian Certification Authority that are specific to the secure use of the product. The evaluation was performed by CSC Australia and was completed in September 2003.

The Compucat Serial Data Regulator is a hardware device that provides unidirectional data flow. It is designed to allow for the passage of data from a lower classified system to a higher classified system, while ensuring that information cannot pass through the device in the opposite (high to low) direction.

The Serial Data Regulator consists of a send unit, receive unit and an interconnecting fibre optic cable. The Serial Data Regulator is installed as a null modem between two serial (RS232) communications ports. The receive unit is assumed to connect to the higher classified system, and the send unit to the lower classified system.

The Serial Data Regulator has been found to uphold the claims made in the Security Target. Potential customers are urged to consult the public version of the Security Target before planning to implement the product. While the Serial Data Regulator is relatively simple in nature, potential customers should ensure that the product is deployed within its intended operational environment (as stated by the Security Target), in conjunction with the recommendations raised in Chapter 9 of this report.

Ultimately, it is the responsibility of the user to ensure that the Serial Data Regulator meets their requirements. For this reason, it is ***strongly*** recommended that prospective users of the product obtain the public version of the Security Target, and read this Certification Report thoroughly prior to deciding whether to implement the product.

Table of Contents

Chapter 1 Introduction

Intended Audience

This certification report states the outcome of the IT security evaluation of Compucat's Serial Data Regulator (SDR). It is intended to assist potential users when judging the suitability of the product for their particular requirements.

This report should be read in conjunction with the public version of the Security Target for the SDR (Ref [9]), which provides a description of the security requirements and specifications that were used as the basis of the evaluation. The public version of the Security Target (Ref [9]) is available for download at http://www.dsd.gov.au. A copy of the full Security Target (Ref [8]) may be requested from Compucat.

Identification

Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to Chapter 7: Evaluated Configuration.

Table 1: Identification Information

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	Compucat Serial Data Regulator Version 1.0
Software Version	N/A
Security Target	Serial Data Regulator SDR-01 Security Target, P/N 2066-0009-09, October 2003
Evaluation Level	ITSEC E6
Evaluation Technical Report	Evaluation Technical Report for the Compucat Serial Data Regulator 1.0, Version 4.0, October 2003
Version of ITSEC	ITSEC Version 1.2, June 1991
Methodology Used	Information Technology Security Evaluation Manual (ITSEM) Version 1.0, 10 September 1993
	ITSEC Joint Interpretations Library (JIL) Version 2.0, November 1998
	Manual of Computer Security Evaluation Part I - Evaluation Procedures (EM4), Issue 1.0, April 1995
	Manual of Computer Security Evaluation Part II - Evaluation Techniques and Tools (EM5), Issue 1.0, April 1995
Sponsor	Compucat Research Pty Limited
Developer	Compucat Research Pty Limited
Evaluation Facility	CSC Australia
Certifiers	Chris Pennisi, Lachlan Turner

Description of the TOE

The Target of Evaluation (TOE) is called the Serial Data Regulator, developed and manufactured by Compucat Research Pty Limited.

The SDR is a hardware only device that provides unidirectional data flow. It is designed to allow for the passage of data from a lower classified system to a higher classified system, while ensuring that information cannot pass through the device in the opposite (high to low) direction.

The security of the unidirectional transfer is implemented in hardware, at the physical layer of the OSI model. Thus, any network protocol that does not require handshaking across the SDR can be used to provide data transfer (e.g. UDP).

The SDR consists of a send unit, receive unit and an interconnecting fibre optic cable. The SDR is installed as a null modem between two serial (RS232) communications ports. The receive unit is assumed to connect to the higher classified system, and the send unit to the lower classified system.

The SDR provides a single security objective to allow transfer of information from the lower classified system without compromising the confidentiality of information on the higher classified system. In doing so, the SDR implements two Security Enforcing Functions (SEFs).

For further information on the specific hardware components included in the evaluated configuration refer to Chapter 7: Evaluated Configuration, or the *Product Rationale* section of the Security Target (Ref [9]).

Chapter 2 Security Policy

The underlying security policy for the TOE defines the set of laws, rules and practices regulating the processing of sensitive information and the use of resources by the SDR.

At the E6 level of assurance, the sponsor is required to provide a formal model of the security policy to define the underlying security policy to be enforced by the TOE. A summary of the informal representation of the security policy has been provided below.

Informal Security Policy

The informal security policy for the SDR can be stated as follows:

> *"The SDR will maintain the confidentiality of the intended receiving system by ensuring that data can only be passed to the receiving system from the sending system and that no data can be passed from the receiving system to the sending system."*

Formal Security Policy

A formal model of the underlying security policy was assessed as part of the evaluation process. This formal model is included in the Annexure of the full Security Target (Ref [8]).

Chapter 3 Intended Environment for the TOE

This chapter outlines the intended method of use for the product and the intended environment in which the TOE is designed to operate, and for which the TOE has been evaluated. This chapter also clarifies the scope of the evaluation. Organisations wishing to implement the TOE in its evaluated configuration should review the evaluation scope to confirm that all the required functionality has been included in the evaluation, and must ensure that any assumed conditions are met in their operational environment.

Method of Use

The Security Target (Ref [9]) outlines the following intended methods of use for the SDR:

- The SDR connects to the sending system through a serial interface (RS232) to provide a single path connection that can be verifiably configured to ensure data can only be sent from the sending system.

- The SDR is connected to the receiving system through a serial interface (RS232) to provide a single path connection that can be verifiably configured to ensure data can only be received by the receiving system.

- Protocols used to transfer data through the SDR must be able to operate without acknowledgement from the receiving system to prevent the possible use of return signals as covert data paths.

Intended Operating Environment

The evaluation of the SDR took into account the following assumptions about the intended operating environment of the TOE:

- The SDR should be installed by a technician who is competent in installing IT terminal equipment.

- No physical interaction is required to operate the SDR once installed.

- Physical security of the SDR receive unit should be the same as that required for the computing or communication system to which the SDR receive unit is attached.

- The SDR receive unit is tamper-evidently sealed at the time of manufacture by chemically welding the unit cover to its base. The nature of the seal is such that it will provide a clearly visible indication if the SDR receive unit is opened. Evidence of unauthorised opening could indicate that the security mechanism of the SDR might have been tampered with.

- The integrity of the tamper evident sealing of the SDR receive unit case should be checked on a regular basis. The frequency of such checks should be determined by risk assessment based on the location in which the SDR receive unit is installed.

Clarification of Scope

The scope of the evaluation is limited to those claims made in the Security Target (Ref [9]). All security related claims in the Security Target were evaluated by CSC Australia as a component of the evaluation. A summary of the Security Target is provided in Appendix A of this Certification Report. The evaluated configuration for the TOE is provided in Chapter 7: Evaluated Configuration.

The TOE provides the following evaluated security functionality:

- **Confidentiality:** The SDR provides a single security objective to allow the transfer of information from a lower classified system (connected to the send unit) without compromising the confidentiality of information on a higher classified system (connected to the receive unit).

Potential users of the TOE are advised that the following **have not been evaluated** as part of the evaluation of the SDR:

- Systems (including their associated data and applications) connected to the send and receive units.

- File transfer software supplied with the SDR.

Chapter 4 TOE Architecture

The SDR consists of the following major architectural components:

- Send Unit:
    - RS-232 interface: a serial data cable interface from the lower classified system to the send unit.
    - Power Supply: provides individual power to the send unit.
    - Indicator LEDs: used to indicate the presence of power (PWR) and data passing through the unit (Tx).
    - Fibre optic transmit module: hardware required to transmit the lower classified data to the receive unit.
- Receive Unit:
    - RS-232 interface: a serial data cable interface from the higher classified system to the receive unit.
    - Power supply: provides individual power to the receive unit.
    - Indicator LEDs: used to indicate the presence of power (PWR), data passing through the unit (Rx) and an operational connection to another fibre optic interface (LNK).
    - Fibre optic receive module: hardware required to receive the lower classified data from the send unit.
- Fibre Optic Cable: a single cable providing the connection between the send and receive units.

All communication between the two units of the SDR is constrained to pass via the optical diode formed by the fibre optic transmitter/receiver pair. The one-way nature of the link is dependent upon the physical inability of the receive unit fibre optical receiver to transmit – the fibre optic cable does not contribute to the enforcement of security functionality.

Chapter 5 Documentation

It is important that the SDR is used in accordance with the guidance documentation in order to ensure the secure usage of the TOE. Compucat provides the following document with the product:

- Compucat Serial Data Regulator User Manual (SDR-01), P/N 2010-0138-03, August 2003 (Ref [11])

The Compucat SDR User Manual (Ref [11]) is intended to provide the administrator with the guidance and information required to install and configure the TOE in a secure manner. It also provides guidance for operating the TOE in a secure manner.

Administrators should ensure that the recommendations listed in Chapter 9 of this document are also read in conjunction with the SDR User Manual (Ref [11]).

Chapter 6 IT Product Testing

The objectives associated with the testing phase of evaluation can be placed into the following categories:

- **Functional testing:** Tests performed to ensure that the TOE operates according to its specification and is able to meet the requirements stated in the Security Target (Ref[9]).
- **Penetration testing:** Tests performed by the evaluators on the TOE to confirm whether or not known vulnerabilities are actually exploitable in practice.

Functional Testing

As part of the implementation work package the evaluators checked the developer's test documentation to ensure that it contains adequate plans, purpose, procedures and results for each developer test. This enabled the evaluators to gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE. In addition, the evaluators repeated all of the developer tests, in order to verify that the test results matched those recorded by the developers, and used this information to create further tests on the TOE.

The test documentation explained how the developer's tests covered the implementation of the two security enforcing functions, and was assessed to be of a standard that allowed for the tests to be repeatable and reproducible.

Penetration Testing

The developers performed a construction and operational vulnerability analysis of the SDR, in order to identify any vulnerabilities in the construction or operation of the TOE. These analyses included a search for possible vulnerability sources in the evaluation deliverables, the intended TOE environment, public domain sources and internal Compucat sources. No construction vulnerabilities were identified by the developers. Only one operational vulnerability was identified by the developer. The developers were able to demonstrate that this vulnerability was not exploitable when the TOE was deployed in its evaluated configuration.

Based on the information given in the developer's vulnerability analyses, the evaluators were able to devise a penetration test plan that would confirm whether or not identified vulnerabilities are exploitable in practice. In addition, the evaluators performed independent construction and operational vulnerability analyses to identify any additional vulnerabilities that had not been addressed by the developers. Based on this information, the evaluators identified further independent penetration tests. Upon completion of the penetration testing activity, the evaluators concluded that the TOE did not display any susceptibility to vulnerabilities obtained from the developer or those from the evaluators' independent vulnerability analyses.

Chapter 7 Evaluated Configuration

The TOE is comprised of the following components:

- User Manual (Part Number 2010-0138-03) (Ref [11])
- Send Unit (Part Number 1105-0050-01)
- Receive Unit (Part Number 1105-0051-01)
- Two 240V AC to 9V DC 400mA plug pack power supplies
- Two serial data cables 25 pin D-Type male to 9 pin D-Type female
- One 5 metre fibre optic cable (optional longer cable is available up to 50 metres)

Please note that the security enforcing functions of the TOE are hardware based, The software provided with the delivered product **does not** implement the security functionality of the TOE and was not included in the scope of the evaluation.

Procedures for Determining the Evaluated Version of the TOE

Purchasers of the TOE should use the following procedures to ensure that the delivered product is the evaluated product.

Once an SDR has been received, the following actions should be performed by the administrator:

1. Open the packaging for the SDR and retrieve the User Manual (Ref [11]) that provides instructions for examining the integrity of the tamper evident casing for both the receive and send units;
2. Recover the Dispatch Docket that has been sent by the vendor. This checklist provides the Part Numbers and Serial Numbers for the delivered SDR(s);
3. Verify that the integrity of the tamper evident casing of both units is not compromised in accordance with section 2.4.4 of the User Manual (Ref [11]);
4. Verify that the SDR serial numbers listed on the Dispatch Docket correspond to the SDR serial numbers located on the back of the SDR casing for both the send and receive units;
5. Check that the part number for each SDR unit identified on the checklist corresponds to the part number on the back of the respective SDR units:

   ✓ The part number for the send unit should read **1105-0050-01**. **This is the evaluated version.**

   ✓ The part number for the receive unit should read **1105-0051-01**. **This is the evaluated version**;

6. Initial against the row with the SDR details;
7. Repeat steps 3 - 6 for all received SDR units on the Dispatch Docket; and
8. Complete the details at the bottom of the checklist and return the list to the vendor's fax number provided on the checklist.

Secure Delivery of the TOE

The TOE should only be delivered by one of the following delivery options:

1. Delivery and installation on site by a suitably cleared Compucat technician.
2. Delivery to site by a suitably cleared Compucat staff member.
3. Delivery via the Commonwealth "safe hand" system.
4. Delivery by a "safe hand" courier.

Purchasers of the TOE should confirm the Serial Data Regulator delivery procedures once an order has been placed with Compucat. These procedures should be understood to ensure that the integrity of the TOE is not compromised during its delivery from the manufacturer to the customer site.

Chapter 8 Results of the Evaluation

Evaluation Procedures

The criteria against which the TOE is judged are expressed in the ITSEC (Ref [6]). The methodology used is described in the Joint Interpretations Library (JIL), Information Technology Security Evaluation Manual (ITSEM) and Evaluation Memoranda (EM) 4 and 5 (Refs [5], [7], [3], [4]). The evaluation was also carried out in accordance with the operational procedures of the AISEP (Refs [1], [2]).

Certification Result

After due consideration of the Evaluation Technical Report (Ref [10]) produced by the evaluators and the conduct of the evaluation as witnessed by the certifiers, the Australasian Certification Authority has determined that the Serial Data Regulator upholds the claims made in the Security Target (Ref [8]) and has met the requirements of the ITSEC E6 assurance level.

Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability that exploitable vulnerabilities remain undiscovered.

ITSEC Assurance Levels

The requirements for each of the ITSEC assurance levels have been summarised in Table 2. Please note that the Serial Data Regulator has met the requirements for assurance level E6.

Table 2 – ITSEC Assurance Levels

Assurance Level	Description
E1	At this level there shall be a security target and an informal description of the architectural design of the evaluated Target Of Evaluation (TOE). Functionality testing shall indicate that the TOE satisfies its security target.
E2	In addition to the requirements for level E1, there shall be an informal description of the detailed design. Evidence of functional testing shall be evaluated. There shall be a configuration control system and an approved distribution procedure.
E3	In addition to the requirements for level E2, the source code and/or hardware drawings corresponding to the security mechanisms shall be evaluated. Evidence of testing of those mechanisms shall be evaluated.
E4	In addition to the requirements for level E3, there shall be an underlying formal model of security policy supporting the security target. The security enforcing functions, the architectural design and the detailed design shall be specified in a semiformal style.

E5	In addition to the requirements for level E4, there shall be a close correspondence between the detailed design and the source code and/or hardware drawings.
E6	In addition to the requirements for level E5, the security enforcing functions and the architectural design shall be specified in a formal style, consistent with the specified underlying formal model of security policy.

A detailed explanation of the assurance requirements for E6 can be found in the ITSEC (Ref [6]).

General Observations

The certifiers would like to acknowledge the invaluable assistance provided by CSC Australia and Compucat Research Pty Limited staff during the evaluation. The successful completion of this evaluation was made possible by their cooperation, technical assistance and attention to issues raised during the process.

Chapter 9 Recommendations

The following recommendations include information highlighted by the evaluators during their analysis of the developer's deliverables, during the conduct of the evaluation, and during the additional activities performed by the certifiers.

Scope of the Certificate

This certificate applies only to version 1.0 of the product. This certificate is only valid when the SDR correctly comprises the designated components. These components are identified in Chapter 7: Evaluated Configuration and there is an accompanying description explaining how the administrator can verify this version information on delivery.

This certificate is only valid when the SDR is installed and configured in its evaluated configuration as described in Chapter 7 and in accordance with the SDR User Manual (Ref [11]).

Intended Environment

The SDR should only be used in accordance with the intended environment described in the *Product Rationale* section of the Security Target (Ref [9]), including consideration of all physical, personnel and IT security measures. Further, it is recommended that the SDR installation be accredited by an appropriate security authority to ensure that the intended environment described in the Security Target (Ref [9]), together with the recommendations provided in this chapter, exists or has been implemented.

Physical Security of SDR Units

The send unit requires connection to a lower classified system (i.e. the sending system) and the receive unit to a higher classified system (i.e. the receiving system). **The SDR does not counter the threat that it could be bypassed by directly connecting the receiving and sending systems together.** Therefore, it is recommended that the receive unit and the attached receiving system are placed in a physically secure environment to which only authorised personnel have access. Administrators should also check the cabling connections from both units to their attached systems to ensure that the SDR is correctly connected and that there are no unauthorised connections.

Users of the TOE should ensure that the physical security of the SDR units, both send and receive, is commensurate with that required for the computing or communication system to which the unit is attached.

Administrators should locate the send and receive units such that any sign of tampering with the casings is clearly visible. Further, the integrity of the tamper evident casing on both units should be regularly inspected for any sign of damage as explained in the User Manual (Ref [11]). A regular inspection procedure should be incorporated into the site or system security plan (the frequency of which should be based on the outcomes of a risk assessment). **The Administrator should**

immediately report any discovery of damage or tamper to their appropriate security authority and the data transfer path should be disabled.

Protocol Considerations

Administrators should be aware that the protocol required for the transfer of data across the SDR cannot implement hand-shaking. **Under no circumstances should an Administrator connect a return path from the receiving system to the sending system in order to implement data transfer using a network protocol that uses handshaking (e.g. TCP).** This will invalidate the security policy of the SDR, and could result in the transmission of information from the higher classified system to the lower classified system.

Integrity and Confidentiality of Transferred Data

Administrators should be aware that the SDR does not provide mechanisms to ensure the integrity or confidentiality of data transferred from the send unit to the receive unit. It is recommended that the users of the TOE assess their own environment for requirements to protect the confidentiality and integrity of transferred data.

Integrity and Availability of Higher Classified System

Administrators should note that the SDR does not counter any threats to the integrity or availability of the higher classified system due to an attack from the lower classified system. It is recommended that transferred data be checked for malicious content with an appropriate product.

Guidance for Purchasers - Delivery Procedures

Upon delivery of the Serial Data Regulator, TOE. Purchasers will receive a Dispatch Docket that confirms serial and part number details that should be completed and faxed back to the point of dispatch. A procedure for determining the version of the TOE is provided in Chapter 7 of this report.

If an SDR is not to be installed immediately, purchasers should ensure that the product is stored in a physically secure environment to which only authorised personnel have access. Further, the integrity of the tamper evident casing should be regularly inspected for any sign of damage or tamper, as explained in the User Manual (Ref [11]). **The purchaser should immediately report any discovery of damage or tamper to their appropriate security authority.**

Appendix A Security Target Information

A brief summary of the Security Target (Ref [8]) is given below. Potential purchasers should obtain a copy of the Security Target to ensure that the security enforcing functions meet the requirements of their security policy. A copy of the Security Target can be obtained from Compucat.

Security Objectives

The SDR has the following IT security objective:

O1 Maintain the confidentiality of data on the receiving system by preventing data passing from the receiving system to the sending system. This prevents compromise of data on the receiving system where the:

a) Receiving system has data that is classified at a higher level than the sending system is authorised to access;

b) Receiving system has data with 'need-to-know' categories that the sending system is not authorised to access.

Intended Method of Use

The Intended Method of Use for the SDR is:

U1 The SDR connects to the sending system through a serial interface (RS232) to provide a single path connection that can be verifiably configured to ensure data can only be sent from the sending system.

U2 The SDR is connected to the receiving system through a serial interface (RS232) to provide a single path connection that can be verifiably configured to ensure data can only be received by the receiving system.

U3 Protocols used to transfer data through the SDR must be able to operate without acknowledgement from the receiving system to prevent the possible use of return signals as covert data paths.

Intended Operating Environment

The Intended Operating Environment for the SDR is:

E1 The SDR should be installed by a technician who is competent in installing IT terminal equipment.

E2 No physical interaction is required to operate the SDR once installed.

E3 Physical security of the SDR receive unit should be the same as that required for the computing or communication system to which the SDR receive unit is attached.

E4 The SDR receive unit is tamper-evidently sealed at the time of manufacture by chemically welding the unit cover to its base. The nature of the seal is such that it will provide a clearly visible indication if the SDR receive unit is opened. Evidence of unauthorised opening could indicate that the security mechanism of the SDR might have been tampered with.

E5 The integrity of the tamper evident sealing of the SDR receive unit case should be checked on a regular basis. The frequency of such checks should be determined by risk assessment based on the location in which the SDR receive unit is installed.

Summary of Security Features of the TOE

The following security enforcing functions are provided by the SDR:

SEF 1 The TOE shall prevent the direct flow of data from the receiving system to the sending system. This is achieved by isolating the receiving system from the sending system with an optical diode. This function prevents the compromise of data by preventing the direct transfer of data from the receiving system to the sending system.

SEF 2 The TOE shall prevent the covert flow of data from the receiving system passing to the sending system through control circuits. This is achieved by not providing control circuits from the SDR receiver unit to the SDR sender unit. This function prevents the compromise of data by eliminating the control circuits as a possible covert transfer path.

Appendix B Acronyms

ACA	Australasian Certification Authority
ACE	AISEP Certificate Extension
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
DSD	Defence Signals Directorate
ETR	Evaluation Technical Report
ISO	International Standards Organisation
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEM	Information Technology Security Evaluation Manual
JIL	Joint Interpretations Library
LED	Light Emitting Diode
OSI	Open Systems Interconnection
SDR	Serial Data Regulator
SEF	Security Enforcing Function
SOM	Strength of Mechanism
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
UDP	User Datagram Protocol

Appendix C References

[1] AISEP Publication No.1- Description of the AISEP
AP 1, Version 2.0, February 2001
Defence Signals Directorate

[2] AISEP Publication No.2 - The Licensing of the AISEFs
AP 2, Version 2.1, February 2001
Defence Signals Directorate

[3] Manual of Computer Security Evaluation Part I - Evaluation Procedures
EM 4, Issue 1.0, April 1995
Defence Signals Directorate
(EVALUATION-IN-CONFIDENCE)

[4] Manual of Computer Security Evaluations Part II - Evaluation Tools and Techniques
EM 5, Issue 1.0, April 1995
Defence Signals Directorate
(EVALUATION-IN-CONFIDENCE)

[5] Information Technology Security Evaluation Criteria
Joint Interpretations Library (JIL)
Version 2.0, November 1998

[6] Information Technology Security Evaluation Criteria (ITSEC)
Commission of the European Communities
CD-71-91-502-EN-C, Version 1.2, June 1991

[7] Information Technology Security Evaluation Methodology (ITSEM)
Commission of the European Communities
Version 1.0, 10 September 1993

[8] Serial Data Regulator SDR-01 Security Target
P/N 2066-0009-09
October 2003
Compucat Research Pty Limited

[9] Serial Data Regulator SDR-01 Security Target (Abridged)
P/N 2066-0010-02
September 2003
Compucat Research Pty Limited

[10] Compucat Serial Data Regulator Evaluation Technical Report (ETR)
Version 4.0, October 2003
CSC Australia
(EVALUATION-IN-CONFIDENCE)

[11] Compucat Serial Data Regulator SDR-01
User Manual
P/N 2010-0138-03
August 2003

[12] Compucat Serial Data Regulator SDR-01
Delivery Process
P/N 2058-0075-03
May 2003