Secure Analogue and Digital KVM Switches

Black Box models
SW2008A-USB-EAL, SW4008A-USB-EAL, SW2006A-USB-EAL, SW4006A-USB-EAL

Adder models
AVSD1002-XX, AVSD1004-XX, AVSV1002-XX, AVSV1004-XX

Security Target
(EAL2 augmented by ALC_FLR.2)

Version 1.1
Date: 17 September 2012

Prepared by: Logica UK Limited

Prepared for: Black Box Corporation
Adder Technology Limited

Black Box Corporation
1000 Park Drive
Lawrence PA 15055
US

Adder Technology Limited
Saxon Way, Bar Hill
Cambridge
CB23 8SL, UK

Contents

List of Tables

List of Figures

Revision History

Date	Version	Details
16 July 2012	0.1	First draft.
23 July 2012	0.2	Updated following CB comments.
24 Aug 2012	1.0	Issued at v1.0.
17 Sept 2012	1.1	Correction to version number of this document in section 2.1

1 Preamble

1.1 Document Purpose and Conventions

1 This document is the Security Target (ST) relating to eight Keyboard-Video-Mouse (KVM) switches supplied by Black Box Corporation and Adder Technology Limited. It is written to conform to the requirements of the Common Criteria (CC) for Information Technology Security Evaluation (see [CC]).

2 The eight KVM switches are identified in Section 2.2 below. Requirements placed on “the TOE” or “the TSF” in this ST apply to each one of these eight switches; for example, a security requirement that specifies “The TSF shall ...” applies to each and every switch. In other words, each and every switch is to be evaluated in accordance with the CC evaluation methodology (see [CEM]).

3 If it is necessary to refer to all eight switches collectively, the term “the set of TOEs” may be used as an alternative to “all eight switches”.

4 A specific switch is identified as such (using the identifiers stated in Section 2.2).

5 References (see Section 1.2) are given as mnemonics within square brackets.

6 The use of italics (for some terminology) is explained at the start of the Glossary (Section 1.3).

7 Note that, for convenience, and in common with the approach generally adopted for STs concerned with IT products, this document uses “switch” when, strictly speaking, “type of switch” or “model” would be more accurate.

1.2 References

[CC] Common Criteria for Information Technology Security Evaluation, Parts 1-3, CCMB-2009-07-001-3, Version 3.1 Revision 3 Final, July 2009

[CEM] Common Methodology for Information Technology Security Evaluation, CCMB-2009-07-004, Version 3.1 Revision 3 Final, July 2009

[GPG] CESG Good Practice Guide No. 11, KVM switches, Issue 1.2, March 2009

[PD166] Precedent Database PD-0166: Switching Additional Devices in a Peripheral Sharing Switch, 19 May 2011, see http://www.niap-ccevs.org/PD/0166.html

[PP] Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, IAD, Version 1.2, 21 August 2008
(see http://www.niap-ccevs.org/pp/archived/pp_psshid_v1.2/)

[PPv21] Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, IAD, Version 2.1, 7 September 2010 (see www.commoncriteriaportal.org)

[ST-PP] Secure Analogue and Digital KVM Switches
Black Box models SW2008A-USB-EAL, SW4008A-USB-EAL, SW2006A-USB-EAL, SW4006A-USB-EAL, SW2009A-USB-EAL, SW4009A-USB-EAL
Adder models AVSD1002-XX, AVSD1004-XX, AVSV1002-XX, AVSV1004-XX AVSC1102-XX, AVSC1104-XX
Security Target (EAL4 augmented by ALC_FLR.2 and ATE_DPT.2), Version 1.2, 26 November 2010.

1.3 Glossary

1.3.1 Terms

8 This ST is (demonstrably) conformant with the Peripheral Sharing Switch (PSS) Protection Profile (PP), see [PPv21], which defines a number of terms that are used throughout the PP. Such of those terms which are considered to be pertinent to this ST are included amongst the following collection of terms; the PP terms are italicised in this ST document whenever they are used in statements (e.g. SFRs) that originate from [PPv21]. (The PP uses SMALL CAPITALS rather than *italics* to identify specific terms.)

9 The definitions of italicised terms below are generally repeated verbatim from [PPv21], apart from some changes to make the definitions specific to this ST and the TOE, and some editorial changes (including additional or alternative words which are either taken from other parts of the PP or which are added in order to resolve, for example, a circular definition).

10 However, the [PPv21] term *Peripheral Port Group ("Group")/ Peripheral Port Group ID* is renamed *port group (id*) - to remove any potential confusion related to the PP's use of *Peripheral Port Group* to relate to both peripherals and computers - and its definition is reworded to align more closely with the TOE description given in Chapter 2 of the PP. (See Section 3.2 below for further comments about the PP.)

11 Note that in this ST, following the familiar KVM acronym, the term "mouse" generally means any *pointing device*; and "video" may be used as shorthand for a video *monitor* (or display).

attribute	Synonymous in this document with *port group id*, and equivalent to the [CC] Part 1 term "(information) security attribute".
authorised user	A *user* who has been granted permission to interact with the TOE and all of its attached *peripherals* and *computers*. This ST assumes that all *users* are *authorised users.*
computer	A programmable machine. The two principal characteristics of a *computer* are: It responds to a specific set of instructions in a well-defined manner, and It can execute a prerecorded list of instructions (a software program). For the purposes of this document, any programmable machine controlling a monitor and/or loudspeakers, and accepting signals from a keyboard and/or a mouse, will qualify as a *computer*.
channel change	A change (initiated by the *user*) of which *switched computer* is currently *connected* to the TOE.
connected	A state in which information can be intentionally transferred between *device(s)* and *computer(s)*.
connection	A path for information flow between two or more *device(s*) or between two or more *computer(s)* or between *device(s*) and *computer(s)*.
design constraint	In this ST, a design constraint is a contribution towards countering a threat by ruling out possible option(s) available to the TOE designers (e.g. to use re-programmable components), as opposed to specifying an explicit SFR to counter the threat.
device	A unit of hardware/firmware that is capable of providing input to a *computer* and/or of receiving output from a *computer*.

enumeration	The process by which a USB device is configured for use.
id	An identifier. See *port group (id)*.
object	Synonymous in this document with *peripheral data*.
peripheral	A *device* that may be attached to the TOE.
peripheral data	Information sent from or to a *peripheral*.
port group (id)	A subset of the TOE's *ports* that is treated as a single entity by the TOE. There is one *port group* for the set of *shared peripherals* and one *port group* for each *switched computer*. Each *switched computer port group* has a unique logical *id*. The *shared peripherals port group* also has an *id* which at any given time is the same as that of the *switched computer port group* that is currently *connected* to the TOE (as selected by the *authorised user*).
port	One of a number of external sockets on the TOE which are used for attaching *peripherals* and *computers* to the TOE.
residual data	Any *peripheral data* stored in a *switch*.
shared peripheral	A *peripheral* attached to the TOE. (See also *port group*.)
subject	Synonymous in this document with *port group*.
switch	A *device* permitting a single set of *peripherals* to be shared among two or more *computers*. Synonymous with "the TOE" in this document.
switched computer	A *computer* attached to the TOE. (See also *port group*.)
TEMPEST	A synonym for Radiation Security.
TOE	See Paragraph 2.
user	The human operator of the TOE. (See also *authorised user*.)
user data	Data for the user, that does not affect the operation of the TSF. (This is taken from the [CC] Part 1 glossary.) Note that, in this ST, "user data" is equivalent to the term "*user* information", which appears without definition in [PPv21].

1.3.2 Abbreviations

12 Some of the following abbreviations are taken from the [CC] Part 1 glossary.

ARC	(security) Architecture
CAC	Common Access Card
CAD	Computer Aided Design
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme (US)
CEM	Common Criteria Evaluation Methodology
CESG	UK Government's National Technical Authority for Information Assurance (originally an abbreviation of Communications-Electronics Security Group)
CM	Configuration Management
DDC	Display Data Channel - a communication protocol between a graphics card (part of a computer in the context of this ST) and a monitor
DVI	Digital Video Interface
DVI-I	Digital Video Interface - Integrated
EDID	Extended Display Identification Data - a data structure provided by a monitor to describe its capabilities to a graphics card (part of a computer in the context of this ST)

GPG	Good Practice Guide
IAD	Information Assurance Directorate (part of the NSA)
IT	Information Technology
KVM	Keyboard-Video-Mouse
KVMA	Keyboard-Video-Mouse-Audio
LED	Light Emitting Diode
NIAP	National Information Assurance Partnership (US)
NSA	National Security Agency (US)
PCB	Printed Circuit Board
PD	Precedent Database
PP	Protection Profile
PS/2	Personal System/2
PSS	Peripheral Sharing Switch
RAM	Random Access Memory
ROM	Read Only Memory
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
UK	United Kingdom
US	United States
USB	Universal Serial Bus
VGA	Video Graphics Array
VIR	Visual Indication Rule

2 Introduction

2.1 ST Reference

13 This ST document is identified as:

Secure Analogue and Digital KVM Switches
Black Box models SW2008A-USB-EAL, SW4008A-USB-EAL, SW2006A-USB-EAL, SW4006A-USB-EAL
Adder models AVSD1002-XX, AVSD1004-XX, AVSV1002-XX, AVSV1004-XX
Security Target (EAL2 augmented by ALC_FLR.2),
Version 1.1 of 17 September 2012,
prepared by Logica UK Limited for Black Box Corporation and Adder Technology Limited.

2.2 TOE Reference

14 The set of TOEs is identified in the following table. “XX” in the Part No. indicates the mains lead country code, as follows:

a) UK = United Kingdom

b) US = United States

c) EURO = Europe

d) AUS = Australia.

Table 1 The set of TOEs

Model, i.e. switch (type)	Part No.	Identifier (in this ST)
Black Box ServSwitch Secure USB DVI 2 port switch	SW2008A-USB-EAL	BServD-2
Black Box ServSwitch Secure USB DVI 4 port switch	SW4008A-USB-EAL	BServD-4
Black Box ServSwitch Secure USB VGA 2 port switch	SW2006A-USB-EAL	BServV-2
Black Box ServSwitch Secure USB VGA 4 port switch	SW4006A-USB-EAL	BServV-4
AdderView Secure DVI 2 port switch	AVSD1002-XX	AViewD-2
AdderView Secure DVI 4 port switch	AVSD1004-XX	AViewD-4
AdderView Secure VGA 2 port switch	AVSV1002-XX	AViewV-2
AdderView Secure VGA 4 port switch	AVSV1004-XX	AViewV-4

2.3 TOE Overview

15 Each of the TOEs is a KVM switch (also known as a PSS). This is a set of hardware and firmware within a metal case, to which may be attached, via cables, two or four computers (depending on whether the TOE is a 2 port or 4 port switch) and a single set of peripherals (USB keyboard, video monitor and USB mouse). Each of the TOEs requires an external power supply.

16 The BServD-2/-4 and AViewD-2/-4 switches handle dual link DVI-I video traffic, i.e. both digital and analogue traffic; the other switches handle analogue video traffic only. The BServD-2/-4 and AViewD-2/-4 switches also handle computer audio output signals, i.e. they are actually KVMA switches to which loudspeaker(s) may be attached; the other switches are not KVMA switches.

17 Note that PD-0166, see [PD166], states that analogue audio devices (e.g. speakers) that incorporate no digital signals whatsoever may be attached to a PSS that conforms to [PPv21].

18 A legacy computer which handles PS/2 (as opposed to USB) keyboard and mouse signals may be attached to a BServV-2/4 or AViewV-2/4 switch (i.e. a switch that supports analogue video traffic only). The attachment is via a different type of cable from that normally supplied to connect computers to these switches; the conversion between the computer's PS/2 signals and the peripherals' USB signals is done automatically by the switch.

19 A representative 4 port KVM switch in its operational environment is depicted in Figure 1.

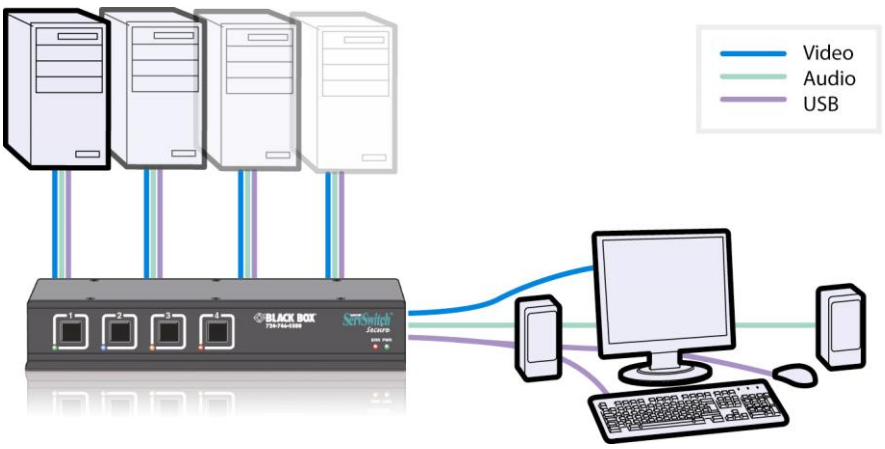

Figure 1 A typical 4 port KVM switch

20 At any one time, the peripherals are connected, through the TOE, to just one of the computers, as indicated by which light (out of 2 or 4) is illuminated on the TOE's front panel. A user can change the connection, i.e. switch the peripherals to connect to another computer attached to the TOE, by means of push buttons on the front panel.

21 The user interacts with the currently connected computer, via the peripherals, exactly as if the peripherals were connected directly to that computer. Hence, the purpose of the TOE is, in essence, to enable the user(s) to economise on peripheral equipment acquisition costs and operating space requirements.

22 Apart from requiring an external power supply, the TOE is entirely self-contained, i.e. it does not require any other hardware, firmware or software in order to function. (However, obviously, it can perform no useful function until a set of peripherals and more than one computer are attached to it.)

23 From a security viewpoint, the primary function of the TOE is to ensure that user data cannot be shared or transferred between computers via the TOE. This is particularly important where user data processed on one computer is more highly classified (i.e. protectively marked) than data processed on another computer.

24 The TOE includes various design features to meet this security requirement, in particular:

a) Unidirectional flow of keyboard and mouse data;

b) Dedicated Display Data Channel (DDC) bus and Extended Display Identification Data (EDID) memory emulation;

c) Active erasing of USB host controller circuit RAM at each channel change;

d) Unambiguous channel selection.

25 In addition, the TOE incorporates features to ensure that:

a) Any USB device used with it is valid (i.e. is only a keyboard or mouse device);

b) Firmware within the TOE, e.g. TSF ROM, is protected from modification.

26 Each of the above security features is described further in Subsection 2.4.3.

27 The CESG Good Practice Guide (GPG) to KVM switches (see [GPG]), discourages the use of “USB-enabled switches” (i.e. switches, such as the TOE, to which USB peripherals may be attached); but many of the TOE’s security features mitigate against the GPG’s concerns (as explained in Subsection 2.4.5). Note also that most modern KVM switches are USB-enabled.

2.4 TOE Description

2.4.1 Taxonomy of the Set of TOEs

28 Apart from the livery on the cases, the four Black Box switches (BServD-2 through to BServV-4) listed in Table 1 are identical to the corresponding Adder switches (AViewD-2 through AViewV-4), and will not be described further in this ST.

29 The security features of the two Adder 2 port switches are identical to those of the corresponding Adder 4 port switches; in fact, the only difference between each pair of switches is that the circuitry and ports in the latter that deal with two of the four ports (to which computers may be attached) are not present in the former. Hence, the two Adder 2 port switches will also not be described further in this ST.

30 Thus, the set of TOEs may be adequately described in this ST by considering:

a) The AdderView Secure DVI 4 port switch (AViewD-4), which is capable of handling dual link DVI-I digital and analogue video traffic; and

b) The AdderView Secure VGA 4 port switch (AViewV-4), which can handle analogue video traffic only.

31 The main security features of these two switches are described in Subsection 2.4.3. These features are, in essence, common to all eight switches, and they are the primary means of satisfying the security functional requirements (SFRs) specified in Chapter 7 of this ST.

32 Some other features of the eight switches are outlined in Subsection 2.4.4. These features are security-related, but in general they do not play as direct a role as the main security features in satisfying the security requirements specified in this ST.

33 A summary of the TOE's design constraints is given in Section 8.4. This includes an outline of how the design of the TOE is constrained (i.e. influenced by) a detailed consideration of how best to counter the threat of information being transferred between computers attached to the TOE.

2.4.2 Scope of the TOE

34 The physical (and logical) scope of the TOE is the whole KVM switch, i.e. the metal case and all the hardware and firmware contained within it.

35 Chapter 9 provides, for each of the set of TOEs, further details of the TOE's components and guidance documentation, and of the peripherals and computers that may be attached to the TOE.

36 Note that this definition of the scope of the TOE does not conflict with the statements above regarding the extent to which the TOE's "Main Security Features" and "Other Features" will be examined during the evaluation of the TOE. In other words, following a successful evaluation of the TOE, potential consumers may have an EAL2 (augmented) level of confidence that the TOE solves the security problem defined in Chapter 4, plus an additional (but unspecified) level of confidence engendered by the presence of the TOE's "Other Features".

2.4.3 Main Security Features

37 This subsection describes the four main security features of the TOE introduced earlier, which collectively ensure that user data cannot be shared or transferred between computers via the TOE. Further details of how these features are implemented are given in Chapter 8.

38 **Unidirectional flow of keyboard and mouse data**: Data can flow only from the attached keyboard and mouse devices to the TOE's computer ports. Data cannot flow from a computer port to the keyboard and mouse devices. This characteristic is enforced by the hardware design. This ensures that it is not possible for one computer to transfer data to another by means of the keyboard and mouse signalling channels.

39 **Dedicated DDC bus and EDID memory emulation**: The EDID memory device contained within a shared monitor and the DDC bus used to link this to computers can form a potential covert attack channel. To counter this, the TOE has dedicated DDC bus and EDID memory emulation circuitry per computer port. The EDID data is collected once from the monitor when the TOE is powered on and transferred to each of the TOE's computer port circuitry in a unidirectional manner. Since each computer port circuitry has its own copy of the EDID (which cannot be altered by the computer) it is not possible for one computer to transfer information to another via the DDC bus and EDID memory.

40 **Active erasing of USB host controller circuit RAM at each channel change**: At each channel change the TOE's USB host controller circuit (which controls the shared peripherals) erases its entire RAM. This helps guard against any possibility of residual data remaining after a channel change and being transferred to another computer.

41 **Unambiguous channel selection**: The TOE has a selection button per channel (i.e. per switched computer). This allows direct and unambiguous channel selection. In addition, each channel has colour coded visual feedback to confirm the selected channel. The selection buttons provide the only method for changing channel. Common KVM features such as hot key or mouse switching are excluded, preventing remote control of the switch. This policy also reduces the possibility of accidental channel change during normal use.

42 **Dedicated keyboard and mouse peripheral ports**: The TOE's USB host controller circuit will allow only keyboard and mouse devices to function at the keyboard and mouse ports. Other types of device (such as USB flash memory drives) attached to the keyboard or mouse ports will not be permitted to function, i.e. once they have been enumerated and configured (and hence identified as not a keyboard or mouse device) they will be un-configured and prevented from functioning.

43 **Non-upgradeable firmware**: Firmware within the TOE is protected from modification and contained in components that are permanently soldered to a PCB. Any changes to the firmware would therefore require intrusive hardware modification.

2.4.4 Other Features of the Switches

44 This subsection describes the "other" security-related features of the eight switches introduced earlier.

45 **Power down of shared USB peripheral devices during a channel change**: Every time the channel is changed the shared USB peripherals are powered down, reset and re-enumerated. This minimizes the possibility of residual data persisting within buffers of the shared peripherals.

46 **Power down of USB host controller circuit during a channel change**: Every time the channel is changed the TOE's USB host controller circuit is powered down and reset. This - together with the active erasure of its RAM (see Paragraph 40) - minimizes the possibility of residual data persisting in buffers within the host controller circuit.

47 **Keyboard and mouse device emulation**: The TOE emulates a fixed keyboard and mouse device on its keyboard and mouse connections to the computer ports. Regardless of the actual device, or type of device connected to the keyboard or mouse peripheral ports, the computer will see only the emulated keyboard and mouse device. This logically isolates the computer from the attached peripheral devices. For instance, if a memory device was connected into the keyboard or mouse port, the computer would have no knowledge of it and no way to communicate with it.

48 **No common power supply**: To minimise the potential of signaling via the power supply, the TOE does not have a common power supply. Instead, the circuitry associated with each computer port is powered via that computer's USB port, and the shared keyboard, mouse and monitor circuitry is powered by the TOE's power supply.

49 **High port to port electrical isolation**: The TOE exhibits high levels of port to port isolation to facilitate data separation (e.g. RED/BLACK data separation).

50 **Low radiated emissions profile**: The TOE meets the appropriate national requirements (in the country where used) for conducted/radiated electromagnetic emissions. Furthermore, the TOE has a low radiated emissions profile to mitigate against TEMPEST style attacks.

51 **No microphone connection**: Microphone circuitry within a computer enables sensitive recording of small analogue signals. Making a connection to a computer's microphone port therefore poses a potential security threat as very low crosstalk levels potentially could be "recorded" and act as a means by which a non-selected computer could read the data being sent to another computer. Therefore the TOE has no microphone connections to minimize the risk of the user connecting the switch to a sensitive analogue input.

52 **Active erasing of USB host controller circuit data buffers once used**: Once a piece of data has passed through the TOE's USB host controller circuit data buffer, it is erased from the buffer. This helps guard against RAM data remenance.

53 **Tamper-evident seals**: The switch is fitted with external tamper-evident seals to give a rapid visual indication of a potential tamper attempt.

2.4.5 CESG GPG Concerns

54 This subsection explains how various features of the TOE mitigate against the concerns expressed in the CESG GPG regarding the use of USB-enabled switches.

55 [GPG] Paragraph 30 raises concern over shared memory (in the switch or in an attached device) that could be used to transfer data from one computer to another; this is mitigated by actively powering down not only the TOE's USB host controller at each channel change, but also the attached peripherals (and also erasing data buffers and memory).

56 [GPG] Paragraph 32 raises concerns of covert channels existing within a switch, whereby data could be written from one computer, to an attached device, and then read by another computer after the channel has been changed. This is a valid concern because it is easy for a typical computer to write into a typical keyboard's memory using standard commands such as "update keyboard LEDs". The TOE prevents this from happening by preventing the computer from writing to the attached keyboard and mouse. Data can only flow from the keyboard and mouse to the computers.

57 The policy of actively powering down (at every channel change) not only the USB host controller but also the attached peripherals and re-enumerating them further helps to reinforce the TOE's security features that counter the threat of covert channels, since any embedded processor in an attached peripheral will be reset and reconfigured.

58 [GPG] Paragraph 33 considers DDC connections as possible covert attack paths. As highlighted in Section 2.4.3 this is a very real threat that is mitigated by the TOE's dedicated DDC bus and EDID memory emulation.

59 [GPG] Paragraph 33 also considers a microphone connection to be a possible covert attack path. There are no microphone connections on the TOE as they would connect to a sensitive analogue input where very low crosstalk levels could potentially be "recorded" by a computer.

60 [GPG] Paragraph 29 warns of the dangers of upgradeable firmware; the TOE has no re-programmable memory, which protects against modification of the firmware.

61 [GPG] Paragraphs 45 and 46 caution against USB devices that have built-in mass storage, or extra connections for devices such as webcams. The TOE will not enumerate such devices. Only keyboard or mouse devices will be enumerated at the keyboard and mouse ports, and only keyboard and mouse data will be passed across the switch.

62 [GPG] Paragraph 51 recommends the use of tamper-evident seals. All models in the set of TOEs are fitted with tamper-evident seals during manufacture.

3 Conformance Claims

3.1 Common Criteria Conformance

63 This ST is conformant to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3 Final of July 2009, as follows:

a) Part 2 extended with the EXT_VIR.1, EXT_IUC.1 and EXT_ROM.1 components;

b) Part 3 conformant (EAL2 augmented by ALC_FLR.2).

3.2 Protection Profile Conformance and Rationale

64 This ST is demonstrably conformant to the Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, Version 2.1 of 7 September 2010.

65 This PP conformance claim is based on the following rationale:

a) Subject to the comments given below, and at the start of Section 1.3 above regarding the definition of terms, the assumptions, security objectives and security requirements specified in this ST are, collectively, identical to or equivalent to or more restrictive than those in [PPv21] which are applicable to the TOE, and address the same threats as are defined in [PPv21].

66 In other words, the solution specified in this ST to the generic security problem defined in [PPv21] is equivalent to, or more restrictive than, that described in [PPv21], and hence this ST is demonstrably conformant to [PPv21] (as permitted by [CC], Part 1, Paragraph 484).

67 [PPv21] Paragraph 5.1.1.3, FDP_IFF.1, includes the following element, which is not contained within [CC] Part 2, FDP_IFF.1:

a) “4. The TSF shall provide the following: [No additional SFP capabilities.]”.

68 It is not clear why this element has been included (with no reference in [PPv21] to an extension of [CC] Part 2), and since it imposes no additional requirements on the TOE it has not been included in this ST.

69 [PPv21] has also removed the SFR FMT_SMF.1 (which is a dependency of FMT_MSA.1) that was present in [PP], an earlier version of [PPv21]; however, [PPv21] Section 6.4 (Dependencies Not Met) gives no justification for why FMT_SMF.1 is omitted. Hence, this ST includes the FMT_SMF.1 SFR, for consistency with [CC] Part 2.

70 Note also that [PPv21] appears to contain some inaccuracies, e.g. references to functional requirements FDP_ETC.1, FDP_ITC.1 in Section 6.3, Security Requirements Rationale. (These SFRs were present in [PP] but are not included in the security requirements specified in [PPv21]; hence, these SFRs are not referred to again in this ST.)

4 Security Problem Definition

4.1 Threats

71 The asset to be protected by the TOE is the information transiting the TOE (i.e. the user data). The threat agent is considered to be a person with physical access to the TOE (who is expected to possess “average” expertise, few resources, and moderate motivation).

72 [PPv21] also identifies “failure of the TOE or *peripherals*” as a possible threat agent, but does not elaborate on that statement. In this ST, failure of the TOE or of peripherals attached to the TOE is considered to be a topic for the evaluation’s vulnerability analysis, rather than a threat agent.

73 The identified threats to the asset are listed below; they are from [PPv21], with clarifications and editorial changes.

74 **T.INVALIDUSB** The *authorised user* will connect unauthorised USB devices to the peripheral switch (i.e. to the TOE).

75 **T.RESIDUAL** *Residual data* may be transferred between *port groups* with different *ids*.

76 **T.ROM_PROG** The TSF may be modified by an attacker such that code embedded in reprogrammable ROMs is overwritten, thus leading to a compromise of the separation enforcing components of the code and subsequent compromise of the data flowing through the TOE.

77 **T.SPOOF** Via intentional or unintentional actions, a *user* may think the set of *shared peripherals* is *connected* to one *computer* when in fact they are connected to a different one. (This does not mean that the TOE has to counter this threat by being able to determine what is connected to it; neither does it mean that this threat is to be addressed by the operational environment.)

78 **T.TRANSFER** A *connection*, via the TOE, between *computers* may allow information transfer. (In other words, information may flow, via the TOE, between *switched computers*.)

4.2 Organisational Security Policies

79 No Organisational Security Policies are specified for the TOE.

4.3 Assumptions

80 Assumptions made on the operational environment are listed below; they are from [PPv21], with clarifications and editorial changes.

81 **A.ACCESS** An *authorised user* possesses the necessary privileges to access the information transferred via the TOE. (All) *users* are *authorised users*.

82 **A.MANAGE** The TOE is received, installed and managed in accordance with the manufacturer’s directions.

83 **A.NOEVIL** Each *authorised user* is non-hostile and follows all TOE usage guidance.

84 **A.PHYSICAL** The TOE is physically secure.

5 Security Objectives

5.1 Security Objectives for the TOE

85 The TOE's security objectives are listed below; they are from [PPv21], with clarifications and editorial changes.

86 **O.CONF** The TOE shall not violate the confidentiality of information which it processes. Information generated within any given *connection* between *shared peripherals* and a *switched computer* shall not be accessible within any other *shared peripherals - switched computer connection* (i.e. one with a different *port group id*).

87 **O.INDICATE** The *authorised user* shall receive an unambiguous indication of which *switched computer* has been selected.

88 **O.ROM** TOE software/firmware shall be protected against unauthorised modification. Embedded software must be contained in mask-programmed or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly.

89 (See Section 6.4 for comments related to this objective.)

90 **O.SELECT** An explicit action by the *authorised user* shall be used to select the *switched computer* to which the set of *shared peripherals* is *connected*. Single push button, multiple push button or rotary selection methods are used by most (if not all) current market products. Automatic switching based on scanning shall not be used as a selection mechanism.

91 **O.SWITCH** All *devices* in a *shared peripherals port group* shall be *connected* to at most one *switched computer* at any given time.

92 **O.USBDETECT** The TOE shall detect any USB connection that is not a pointing device, keyboard or display and will perform no interaction with that device after the initial identification.

5.2 Security Objectives for the Operational Environment

93 The security objectives for the operational environment are listed below; they are from [PPv21], with clarifications and editorial changes.

94 **OE.ACCESS** Each *authorised user* shall possess the necessary privileges to access the information transferred by the TOE. All *users* are *authorised users.*

95 **OE.MANAGE** The TOE shall be received, installed and managed in accordance with the manufacturer's directions.

96 **OE.NOEVIL** Each *authorised user* shall be non-hostile and follow all usage guidance.

97 **OE.PHYSICAL** The TOE shall be physically secure.

5.3 Rationale

98 The following table (overleaf) traces objectives to threats and assumptions. It is an abbreviated version of the [PPv21] Tables 6.1 and 6.2, with the addition of O.SWITCH to assist in countering T.RESIDUAL. The entries in the "Notes" column justify why the objectives counter the threats.

Table 2 Tracing of objectives to threats and assumptions

Threat/Assumption	Objective(s)	Notes
T.INVALIDUSB	O.USBDETECT	This objective directly counters the threat.
T.RESIDUAL	O.CONF, O.SWITCH	O.CONF directly counters the threat (because *residual data* is encompassed by the term "information" used in its definition); O.SWITCH diminishes the threat because the risk of information being transferred between *port groups* with different *ids* is increased if a *shared peripheral* is connected to more than one *switched computer* at any given time.
T.ROM_PROG	O.ROM	This objective directly counters the threat.
T.SPOOF	O.INDICATE, O.SELECT	These objectives directly counter the threat.
T.TRANSFER	O.CONF, O.SWITCH	O.CONF directly counters the threat; O.SWITCH diminishes the threat because the risk of information being transferred between *switched computers*, via the TOE, is increased if a *shared peripheral* is connected to more than one *switched computer* at any given time.
A.ACCESS	OE.ACCESS	This objective directly upholds the assumption.
A.MANAGE	OE.MANAGE	This objective directly upholds the assumption.
A.NOEVIL	OE.NOEVIL	This objective directly upholds the assumption.
A.PHYSICAL	OE.PHYSICAL	This objective directly upholds the assumption.

99 By inspection of Table 2, it can be seen that:

a) Each security objective identified earlier traces to at least one threat or assumption;

b) Each threat or assumption identified earlier has at least one security objective tracing to it;

c) No objective for the TOE traces back to an assumption;

d) All threats will be adequately countered (i.e. removed, diminished or mitigated), and all assumptions upheld, if all the objectives are achieved.

6 Extended Components Definition

6.1 Introduction

100 [PPv21] specifies an EXT (EXTended requirements) class containing three families, each of which contains a single component, identified as EXT_VIR.1, EXT_IUC.1 and EXT_ROM.1. This ST defines these components below; the definitions are from [PPv21], with clarifications and editorial changes.

6.2 The EXT_VIR.1 Component

101 There are no management activities or auditable actions foreseen for this component.

102 **EXT_VIR.1 Visual Indication Rule**

Hierarchical to: No other components.

Dependencies: No dependencies.

EXT_VIR.1.1 A visual method of indicating which *computer* is *connected* to the set of *shared peripherals* shall be provided (by the TSF) that is persistent for the duration of the *connection*.

Application note: This does not require tactile indicators, but does not preclude their presence.

6.3 The EXT_IUC.1 Component

103 There are no management activities or auditable actions foreseen for this component.

104 **EXT_IUC.1 Invalid USB Connection**

Hierarchical to: No other components.

Dependencies: No dependencies.

EXT_IUC.1.1 All USB *devices* attached to the TOE shall be interrogated (by the TSF) to ensure that they are valid (i.e. are a pointing device, keyboard or display). No further interaction with non-valid *devices* shall be performed (by the TOE).

Application note: The TOE does not support USB display devices, which are actively disallowed.

6.4 The EXT_ROM.1 Component

105 There are no management activities or auditable actions foreseen for this component.

106 **EXT_ROM.1 Read-Only ROMs**

Hierarchical to: No other components.

Dependencies: No dependencies.

EXT_ROM.1.1 TSF software embedded in ROMs must be contained in mask-programmed or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly.

Application note: It is debatable whether this component specifies required “security functionality” as opposed to a “design constraint”; however, it is stated in [PPv21] Table 6.3 that this component provides an easily-verifiable means of satisfying the O.ROM objective (“TOE software/firmware shall be protected against unauthorised modification. ….”).

7 Security Requirements

7.1 Security Functional Requirements

7.1.1 Introduction and the Data Separation SFP

107 The SFRs for the TOE are specified in the following subsections; the SFRs are from [PPv21], with changes and additions noted where necessary, plus clarifications and editorial changes. The components are drawn from the CC Part 2 families FDP_IFC, FDP_IFF, FMT_MSA and FMT_SMF; and from the EXT_VIR, EXT_IUC and EXT_ROM families introduced in the preceding section.

108 Words which appear in square brackets are the result of permitted operations on components.

109 The information flow control SFP (Security Function Policy) that is assigned to some components is named in [PPv21] as the **Data Separation SFP**, and is defined as follows:

The TOE shall allow *peripheral data* to be transferred only between *port groups* with the same *id*.

110 Note that it follows from Section 1.3 above that “the user data’s associated security attributes” equates to “*attributes*”, and “the information controlled under the (Data Separation) SFP” equates to “*objects*”.

7.1.2 User data protection (FDP)

111 **FDP_IFC.1** (Subset information flow control)

Dependencies: FDP_IFF.1 (Simple security attributes).

FDP_IFC.1.1 The TSF shall enforce the [Data Separation SFP] on [the set of *port groups*, and the bi-directional flow of *peripheral data* between the *shared peripherals* and the *switched computers*].

112 **FDP_IFF.1** (Simple security attributes)

Dependencies: FDP_IFC.1 (Subset information flow control) and FMT_MSA.3 (Static attribute initialisation).

FDP_IFF.1.1 The TSF shall enforce the [Data Separation SFP] based on the following types of subject and information security attributes: [*port groups* (*subjects*) and *peripheral data* (*objects*); and *port group ids* (*attributes*)].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [Switching rule: *peripheral data* can flow to a *port group* with a given *id* only if it was received from a *port group* with the same *id*].

FDP_IFF.1.3 The TSF shall enforce the [none, i.e. no additional information flow control SFP rules].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [none].

(Section 3.2 above explains why an element of FDP_IFF.1 in [PPv21] has been omitted from this ST.)

7.1.3 Security management (FMT)

113 **FMT_MSA.1** (Management of security attributes)

Dependencies: (FDP_ACC.1 or FDP_IFC.1]), FMT_SMR.1 (Security roles) and FMT_SMF.1 (Specification of management functions).

FMT_MSA.1.1 The TSF shall enforce the [Data Separation SFP] to restrict the ability to [modify] the security attributes [*port group ids*] to [the *user*].

114 [PPv21] includes the following application note:

An *authorised user* shall perform an explicit action to select the *computer* to which the shared set of *peripherals* is *connected*, thus effectively modifying the *port group id* associated with the *peripherals*.

115 **FMT_MSA.3** (Static attribute initialisation)

Dependencies: FDP_MSA.1 and FMT_SMR.1.

FMT_MSA.3.1 The TSF shall enforce the [Data Separation SFP] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [none, i.e. no identified role] to specify alternative initial values to override the default values when an object or information is created.

116 [PPv21] includes the following application note re FMT_MSA.3.1:

On start-up, one and only one attached *computer* shall be selected.

117 Application note re FMT_MSA.3.2:

This ST (following [PPv21]) does not include the FMT_SMR.1 component (see Subsection 7.1.5). Hence, the *user* is not a role in the CC sense; however, the *user* is not exempt from the FMT_MSA.3.2 prohibition (on specifying initial values).

118 **FMT_SMF.1** (Specification of management functions)

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [selection via an explicit action by an *authorised user* of the *computer* to which the shared set of *peripherals* is *connected*].

119 Note that [PPv21] does not include FMT_SMF.1; Section 3.2 above explains why it is included in this ST.

7.1.4 Extended requirements (EXT)

120 **EXT_VIR.1** (Visual Indication Rule)

Dependencies: No dependencies

EXT_VIR.1.1 A visual method of indicating which *computer* is *connected* to the set of *shared peripherals* shall be provided (by the TSF) that is persistent for the duration of the *connection*.

Application note:

This does not require tactile indicators, but does not preclude their presence.

121 **EXT_IUC.1** (Invalid USB Connection)

Dependencies: No dependencies

EXT_IUC.1.1 All USB *devices* attached to the TOE shall be interrogated (by the TSF) to ensure that they are valid (i.e. are a pointing device, keyboard or display). No further interaction with non-valid *devices* shall be performed (by the TOE).

Application note: The TOE does not support USB display devices, which are actively disallowed.

122 **EXT_ROM.1** (Read-Only ROMs)

Dependencies: No dependencies

EXT_ROM.1.1 TSF software embedded in ROMs must be contained in mask-programmed or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly.

Application note: See Section 6.4 for comments about this component.

7.1.5 Dependencies, management and audit

123 It can be seen by inspection that, with one exception, the dependencies of the above SFRs are satisfied. The exception is the absence of FMT_SMR.1 (Security roles), which is a dependency of FMT_MSA.1 (Management of security attributes) and FMT_MSA.3 (Static attribute initialisation).

124 The justification for this absence, as stated in [PPv21], is as follows:

The TOE is not required to associate *users* with roles; hence, there is only one “role”, that of *user*. This deleted requirement [i.e. omitted SFR] ... allows the TOE to operate normally in the absence of any formal roles.

125 After due consideration, and in the absence of any FAU_GEN (Security audit data generation) components for the TOE, there are (apart from MSA.1.1) no management activities or auditable actions specified in connection with the above SFRs.

7.2 Security Functional Requirements Rationale

126 Table 3 (overleaf) traces the above SFRs to the security objectives for the TOE. It is an abbreviated version of the [PPv21] Table 6.3, with some changes (for the reasons outlined in Section 3.2 above), and the addition of three SFRs that are considered to also contribute to implementing O.SWITCH. The entries in the “Notes” column justify why the SFRs meet the objectives.

Table 3 Tracing of SFRs to objectives for the TOE

Objective	SFR(s)	Notes
O.CONF	FDP_IFC.1, FDP_IFF.1	These SFRs directly implement the objective, because they both enforce the Data Separation SFP.
O.INDICATE	EXT_VIR.1	This SFR directly implements the objective.
O.ROM	EXT_ROM.1	See the application note in Section 6.4.
O.SELECT	FMT_MSA.1, FMT_SMF.1	These SFRs directly implement the objective (see also the application note for FMT_MSA.1).
O.SWITCH	FDP_IFC.1, FDP_IFF.1, FMT_MSA.3, FMT_SMF.1	These SFRs implement the objective, because each one either enforces the Data Separation SFP, or supports a robust implementation of the objective. (See the definition of *port group (id)*; the crucial points are that: Each *switched computer port group* has a **unique** logical *id*; The *shared peripherals port group* also has an *id* which at any given time **is the same as** that of the *switched computer port group* that is currently *connected* to the TOE. In other words, if the SFP is enforced correctly, then by definition the *shared peripherals* can be *connected* to only one *switched computer* at any given time.)
O.USBDETECT	EXT_IUC.1	This SFR directly implements the objective.

127 By inspection of Table 3, it can be seen that:

a) Each SFR specified earlier traces to at least one objective for the TOE;

b) Each objective for the TOE identified earlier has at least one SFR tracing to it;

c) All objectives for the TOE will be achieved (to the level of assurance specified by the following SARs) if all the SFRs are satisfied (to the specified assurance level).

7.3 Security Assurance Requirements

128 The SARs for the TOE are those specified in [PPv21], i.e. the TOE is to be assured to an EAL2 (augmented) level.

129 The assurance components that are relevant to the TOE itself are listed in Table 4 (overleaf), together with a summary of the “developer actions”, i.e. a summary of what the TOE’s developer (Adder Technology Ltd) has to provide to the evaluators. The component(s) that augment EAL2 are indicated in bold.

130 In addition, the ST (this document) is to be evaluated against the “ASE_” components for EAL2 as listed in [CC], Part 3, Table 3.

131 Further details of the assurance components are given in [CC] Part 3. The “evaluator actions” for each component are elaborated in [CEM], which details, for example, how the evaluators should process what the developer provides to them.

Table 4 Assurance requirements

[CC] assurance component	Developer to provide	Notes
Development		
ADV_ARC.1	Security architecture description of the TSF (TOE Security Functionality)	The TOE design shall prevent the TSF being bypassed or tampered with by untrusted active entities. (In practice the ARC description will probably be a separate section or annex in the design description - see ADV_TDS.1).
ADV_FSP.2	Security-enforcing functional specification of the TSF	Include a tracing to the SFRs specified in the ST.
ADV_TDS.1	Basic design of the TOE (describe the design in terms of subsystems)	Include a mapping from the TSFIs (TSF Interfaces, which are described in the functional specification, see ADV_FSP.2) to the subsystems.
Guidance Documents		
AGD_OPE.1	Operational user guidance	Describes how to use the TOE in a secure manner, both for normal (unprivileged) users and for administrators (who are privileged to configure the TOE's security functions - but this may not be applicable for this evaluation).
AGD_PRE.1	The TOE (i.e. an actual switch), including its preparative procedures	Procedures describe how to accept (i.e. receive), install and set-up the TOE in a secure manner. (Evaluators' applying these procedures to the TOE can be done at the same time as penetration testing - see below, AVA_VAN.2).
Life Cycle Support		
ALC_CMC.2	The TOE (i.e. an actual switch) and a reference for it; CM (configuration management) documentation and evidence that a CM system is being used	The CM system needs to uniquely identify all configuration items that constitute the TOE.
ALC_CMS.2	Configuration list for the TOE	List to include the parts that constitute the TOE.
ALC_DEL.1	Delivery procedures	Include evidence that the developer follows the documented procedures.
ALC_FLR.2	Flaw (remediation) reporting procedures	Include guidance addressed to TOE users.
Tests		
ATE_COV.1	Evidence of test coverage	Evidence to show that developer's tests cover some of the TSFIs (which are described in the functional specification,see ADV_FSP.2).
ATE_FUN.1	Functional testing (of the TSF)	Developer's test results (test plans and specifications, expected and actual results).

[CC] assurance component	Developer to provide	Notes
ATE_IND.2	The TOE (i.e. an actual switch) for independent testing, plus technical support and resources during the testing that are equivalent to those used in the developer's functional testing of the TSF	Independent testing - sample, i.e. evaluators repeat a sample of the developer's tests; the evaluators also conduct their own additional functional tests. Can be done at the same time as penetration testing - see AVA_VAN.2.
Vulnerability Assessment		
AVA_VAN.2	The TOE (i.e. an actual switch) for penetration testing, plus technical support and resources during the testing (see ATE_IND.2)	Evaluators carry out a vulnerability analysis (based on the ADV and AGD evidence), then undertake penetration testing of the TOE.

7.4 Security Assurance Requirements Rationale

132 The combination of required assurance components (i.e. EAL2 augmented by ALC_FLR.2) is that specified in [PPv21].

133 The CC characterises an EAL2-assured IT product as one that has been structurally tested.

7.5 Conclusion

134 The preceding rationales in this ST demonstrate that, if all the security requirements are satisfied, and all security objectives for the operational environment are achieved, then there exists assurance (to the EAL2 augmented level) that the TOE solves the security problem defined in Chapter 4.

135 Note also that the TOE was previously certified, to the EAL4 augmented level of assurance, against Security Target [ST-PP] (which was based on [PP], i.e. it specified essentially the same SFRs as this ST).

8 TOE Summary Specification

8.1 Introduction

136 The next two sections summarise how each of the two switches identified in Subsection 2.4.1 (as being representative of the set of TOEs) satisfies all the SFRs specified in this ST.

137 General constraints on the design of the TOE (resulting from security considerations) are discussed in Section 8.4.

138 For each of the eight switches in the set of TOEs, further details of its components and guidance documentation, and of the peripherals and computers that may be attached to it, are given in Chapter 9.

8.2 AdderView Secure DVI 4 port Switch (AViewD-4)

8.2.1 Switch Architecture Outline

139 Figure 2 (overleaf) depicts the switch's internal security architecture in terms of "controller" components (each constructed from hardware/firmware sub-components and circuitry). To avoid cluttering the diagram, just one computer controller is shown, but the other three computer controllers are identical to it, both in terms of their constituent sub-components and connections to other controllers.

140 The solid arrows indicate the flow of peripheral data (including peripheral control signals), and the dotted arrows indicate the flow of switch control signals. "W, X, Y, Z" are explained in the following paragraphs; note that in reality these sub-components are not inter-connected.

141 When the user powers up the switch the switch controller ensures that one computer only is connected to the shared peripherals, and the USB host controller circuit ensures that only keyboard and mouse devices are attached (enumerated) at the keyboard and mouse ports. (The latter check is also done whenever a device is attached to one of these USB ports, and at every channel change.) When the user presses a selection button the switch controller signals the USB host controller, the audio controller and the video controller to instigate a channel change (to the selected computer port); the switch controller also toggles the relevant LEDs on the switch's front panel. The USB host controller erases its entire RAM at every channel change.

142 The USB host controller and the computer controller implement a unidirectional flow of keyboard and mouse data as follows. When a USB peripheral sends a peripheral control signal to the USB host controller (e.g. when the keyboard's caps lock key is pressed) the controller responds as if it was a computer (e.g. it signals the keyboard to illuminate the caps light) before passing the peripheral's signal on to the computer via circuitry "Z" in the computer controller. The actual computer's response is also handled by "Z", which does not pass it back to the USB host controller.

143 The computer controller also has a dedicated DDC bus connecting it to the video controller. This bus carries EDID data from the video controller to the computer controller's EDID memory emulation circuitry "X" (when the switch is powered up). Video output from the computer is sent to the video peripheral via the computer controller's "Y" circuitry and the video controller.

144 Audio output from the computer is sent to the audio peripheral (i.e. to powered analogue audio speakers) via the computer controller's "W" circuitry and the audio controller.

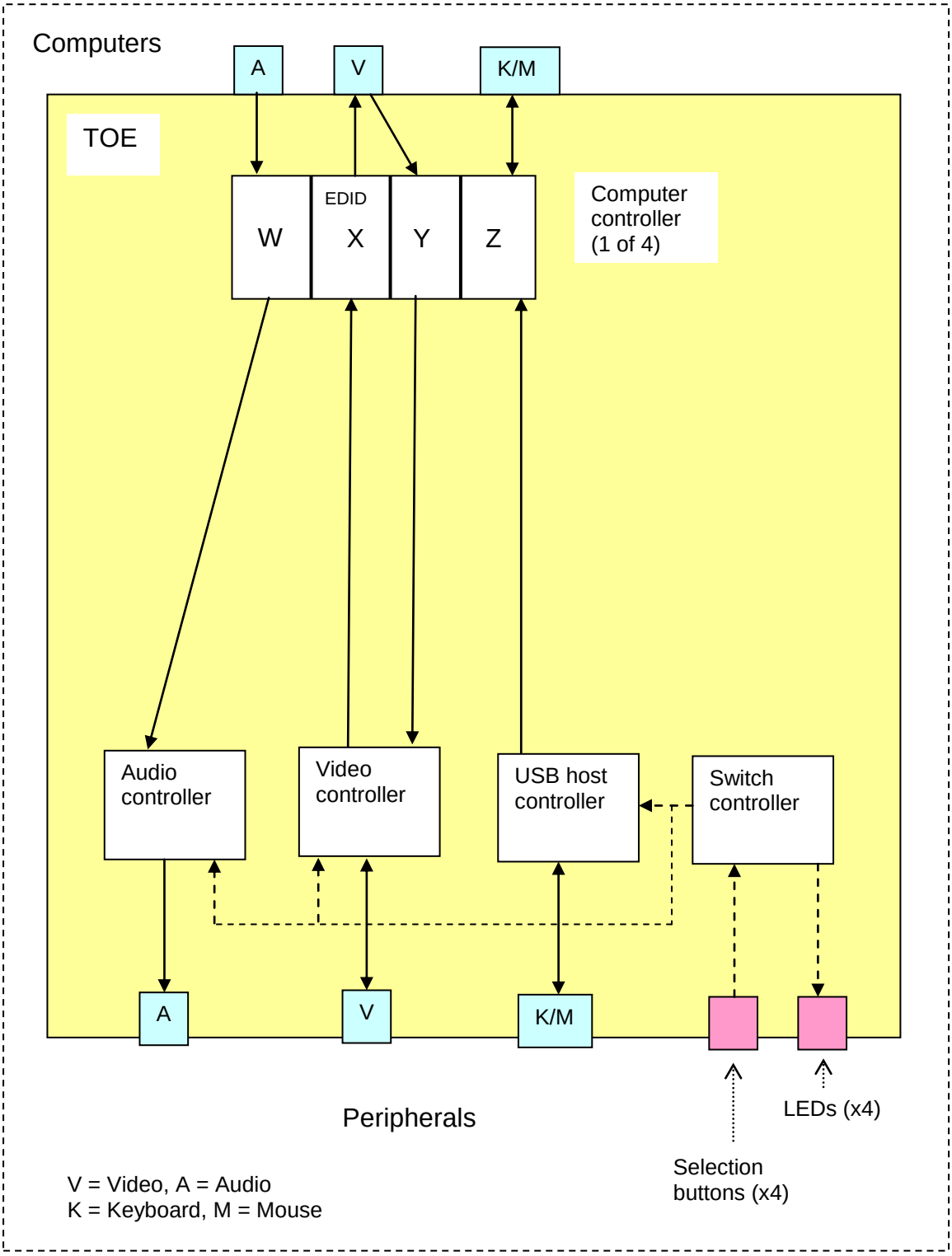

Figure 2 AViewD-4 architecture outline

145 The above description covers the switch's main security features that were introduced in Subsection 2.4.3 (apart from the "non-upgradeable firmware feature", which is discussed in Section 8.4), and also underpins Table 5 below.

8.2.2 Implementation of Security Functional Requirements

146 The following table indicates how - in terms of the preceding subsection's outline architecture description - the switch meets each of the SFRs specified in Section 7.1.

Table 5 AViewD-4 implementation of SFRs

SFR(s)	Component(s)	Additional Notes
FDP_IFC.1, FDP_IFF.1	Switch controller, USB host controller, Audio controller, Video controller	There is one computer controller per computer port; the switch controller ensures that none is linked (via the audio, USB or video controller) to another computer controller.
FMT_MSA.1, FMT_SMF.1	Switch controller	
FMT_MSA.3	Switch controller	
EXT_VIR.1	Switch controller	For each computer port, there is exactly one LED associated with it; each LED is illuminated only when its associated computer port is selected; each LED is colour-coded, i.e. is coloured differently from each of the other LEDs.
EXT_IUC.1	USB host controller	
EXT_ROM.1	All components with embedded TSF software/firmware	See Section 8.4 (and the application note in Section 6.4).

8.3 AdderView Secure VGA 4 port Switch (AViewV-4)

8.3.1 Switch Architecture Outline

147 Figure 3 (overleaf) depicts the switch's internal security architecture in terms of "controller" components (following the same approach and conventions used for Figure 2). In essence, the AViewV-4 switch architecture is the same as the AViewD-4 switch architecture, with the removal of the audio-handling capability.

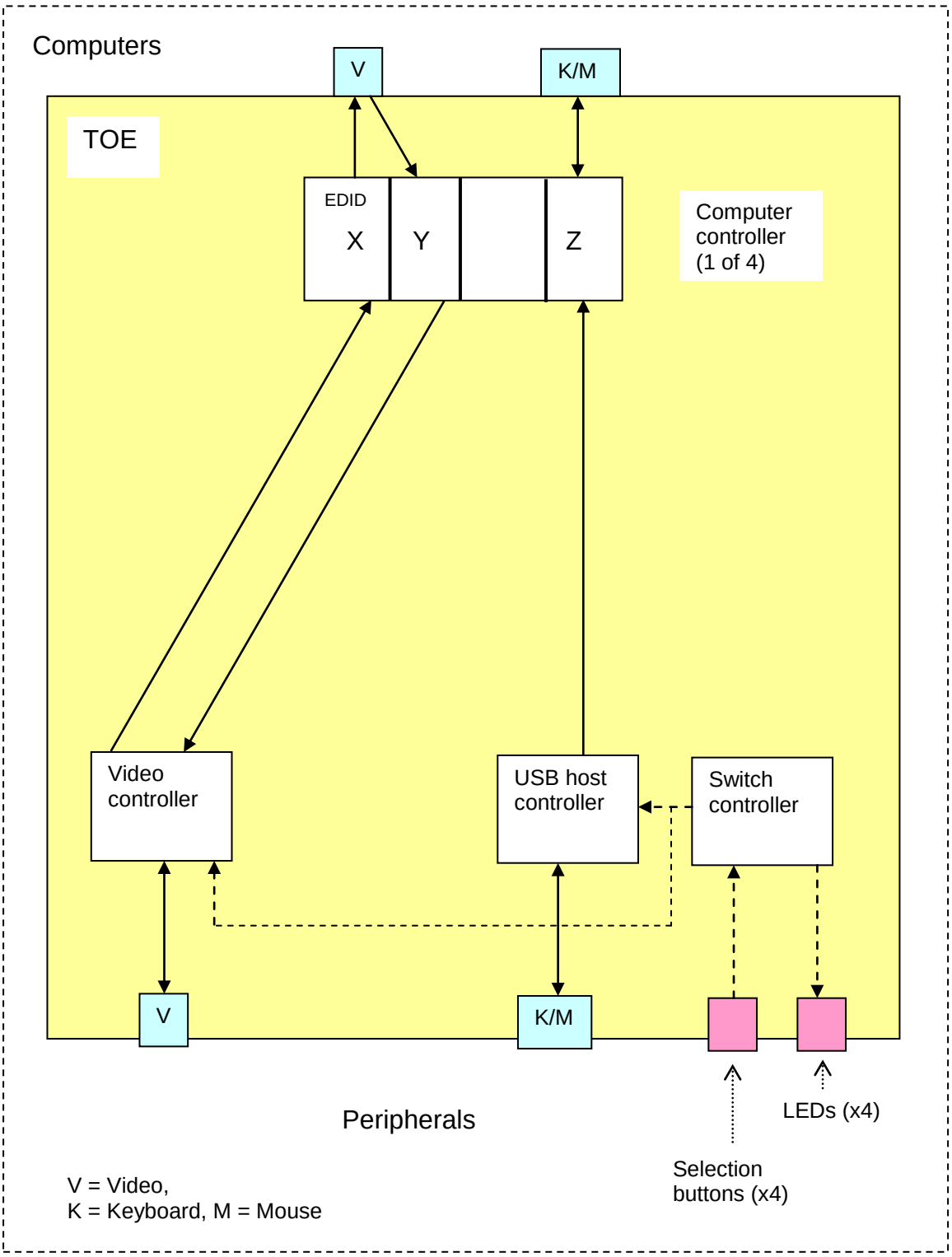

Figure 3 AViewV-4 architecture outline

148 The above description covers the switch's main security features that were introduced in Subsection 2.4.3 (apart from the "non-upgradeable firmware feature", which is discussed in Section 8.4), and also underpins Table 6 below.

8.3.2 Implementation of Security Functional Requirements

149 The following table indicates how - in terms of the preceding subsection's outline architecture description - the switch meets each of the SFRs specified in Section 7.1.

Table 6 AViewV-4 implementation of SFRs

SFR(s)	Component(s)	Additional Notes
FDP_IFC.1, FDP_IFF.1	Switch controller, USB host controller, Video controller	There is one computer controller per computer port; the switch controller ensures that none is linked (via the USB controller or video controller) to another computer controller.
FMT_MSA.1, FMT_SMF.1	Switch controller	
FMT_MSA.3	Switch controller	
EXT_VIR.1	Switch controller	For each computer port, there is exactly one LED associated with it; each LED is illuminated only when its associated computer port is selected; each LED is colour-coded, i.e. is coloured differently from each of the other LEDs.
EXT_IUC.1	USB host controller	
EXT_ROM.1	All components with embedded TSF software/firmware	See Section 8.4 (and the application note in Section 6.4).

8.4 Design Constraints and Further Threat Considerations

150 As stated in Section 6.4, [PPv21] includes the SFR EXT_ROM.1 as an easily-verifiable means of satisfying the O.ROM objective, which states that:

"TOE software/firmware shall be protected against unauthorized modification. Embedded software must be contained in mask-programmed or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly".

151 The TOE's electronic components are either hardware or firmware components. The hardware components are standard items (e.g. resistors) that are incapable of being programmed; the firmware components are standard items (e.g. microprocessors) that include no programmable memory capability apart from one-time-programmable read-only memory which is permanently attached (non-socketed) to a PCB. The TOE does not contain any programmable logic arrays, nor does it contain any software apart from the code which is one-time-programmed into its firmware as the last stage of its manufacturing process (prior to final testing and packaging).

152 As stated in Section 6.4, it is debatable whether the EXT_ROM.1 component specifies required "security functionality" as opposed to a "design constraint"; however, the key point is that [PPv21] accepts the component as an adequate means of meeting the O.ROM objective.

153 Further design constraints have been identified by the TOE designers during their consideration of how best to counter T.TRANSFER (the threat of information being transferred between computers attached to the TOE).

154 Describing these constraints is beyond the scope of this ST (which is not intended to be a detailed design specification), but as an indication of their extent the following list gives what may be called "some of the variations on the T.TRANSFER theme" that the TOE designers have taken into account:

a) Firmware "holes" or malfunction;
b) Common storage;
c) Timing analysis;
d) Electrical crosstalk;
e) Forced malfunction;
f) User error;
g) Faulty installation;
h) Faulty electronics;
i) Shorting or loading the power supply;
j) Faulty or subverted cabling;
k) Subverted switch;
l) Electromagnetic emissions snooping;
m) Light emissions snooping;
n) Power surges (e.g. lightning strikes).

155 See also Subsection 2.4.4 above.

9 TOE Component Details

156 For each of the eight switches in the set of TOEs, further details of its components and guidance documentation, and of the peripherals and computers that may be attached to it, are given on the Black Box and Adder web sites, see http://www.blackbox.com/ and http://www.adder.com/.