G&D

KVM-over-IP matrix system with: ControlCenter-IP series with firmware 1.7, ControlCenter-IP-XS series with firmware 1.1, RemoteAccess-IP series with firmware 1.3, Vision-IP series with firmware 2.4, Vision XS-IP series with firmware 1.5

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 1.12

Prepared for:

Guntermann & Drunck GmbH
Obere Leimbach 9
57074 Siegen
Deutschland

Phone: +49 271 238720
www.gdsys.com

Prepared by:

Corsec Security, Inc.
12600 Fair Lakes Circle
Suite 210
Fairfax, VA 22003
United States of America

Phone: +1 703 267 6050
www.corsec.com

Table of Contents

List of Figures

List of Tables

1. Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is the Guntermann & Drunck GmbH (G&D) KVM-over-IP matrix system with: ControlCenter-IP series with firmware 1.7, ControlCenter-IP-XS series with firmware 1.1, RemoteAccess-IP series with firmware 1.3, Vision-IP series with firmware 2.4, Vision XS-IP series with firmware 1.5 and will hereafter be referred to as the TOE throughout this document. The TOE connects two sets of peripheral devices (audio, keyboard/mouse, user authentication, and one display) and one connected computer.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functionality and describes the physical and logical scope for the TOE as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile (PP), and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs to which the TOE adheres.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the SFRs and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms and Terms (Section 0) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 shows the ST and TOE references.

Table 1 – ST and TOE References

ST Title	*G&D KVM-over-IP matrix system with: ControlCenter-IP series with firmware 1.7, ControlCenter-IP-XS series with firmware 1.1, RemoteAccess-IP series with firmware 1.3, Vision-IP series with firmware 2.4, Vision XS-IP series with firmware 1.5 Security Target*
ST Version	Version 1.12
ST Author	Corsec Security, Inc.
ST Publication Date	February 6, 2026

TOE Reference	*G&D KVM-over-IP matrix system with: ControlCenter-IP series with firmware 1.7, ControlCenter-IP-XS series with firmware 1.1, RemoteAccess-IP series with firmware 1.3, Vision-IP series with firmware 2.4, Vision XS-IP series with firmware 1.5*

1.3 Product Overview

The KVM-over-IP matrix system with: ControlCenter-IP series with firmware 1.7, ControlCenter-IP-XS series with firmware 1.1, RemoteAccess-IP series with firmware 1.3, Vision-IP series with firmware 2.4, Vision XS-IP series with firmware 1.5 provides video, audio, USB and serial switching over an IP network. The system consists of:

- At least one ControlCenter-IP(-XS) matrix switch
- Multiple VisionXS-IP series console and computer modules
- Multiple Vision-IP series console and computer modules
- Multiple RemoteAccess-IP series computer modules

The KVM-over-IP modules are either computer modules with the extension “CPU” that connect to a workstation or server or virtual machine, or a console module with the extension “CON” that connects to a monitor, serial devices, keyboard/mouse, and other USB devices. The CPU and CON modules can be used as direct KVM extenders over IP-based network. Transmission is possible via CAT cable or fiber optics. In conjunction with a KVM-over-IP matrix switch as the central switching unit, this becomes a KVM-over-IP matrix system that lets a user operate many computers via many workstations, but this specific evaluation will focus on one connected computer.

1.4 TOE Overview

The TOE provides a secure medium to connect one or more input peripherals to one or more computers. The TOE models support connectivity between two sets of peripheral devices (audio, keyboard/mouse, userauthentication, USB devices, and one display) and one connected computer.

The TOE consists of a family of devices that support different computers, different monitors, and different types of display protocols depending on the model.

The TOE is made up of the following components:

- Vision-IP or VisionXS-IP as a KVM Extender Console
- Vision-IP or VisionXS-IP or RemoteAccess-IP as a KVM Extender CPU[1]
- ControlCenter-IP(-XS) as a KVM matrix switch

The TOE provides a capability to dynamically change the switching configuration to connect a particular computer to a particular peripheral set. The TOE enforces secure separation of information flows corresponding to what actions a logged-in user is permitted to perform. The corresponding Information Flow Control Security Policy is the main security feature of the TOE. Users have no rights initially, but are assigned the following individual rights:

- user rights,
- global device rights,
- individual device rights, and
- script rights.

[1] CPU – Computer Module

Users log in with either a simple password or two-factor authentication (which can include a certificate).

The TOE utilizes a UID[2] locking function that permits specific end devices only. Devices that connect to TOE components must have a proprietary G&D certificate installed to authenticate the device. An additional 'user' certificate can be installed on the devices by an administrator to further authenticate device to device to device prior to establishing communications. In addition, for a device to be used by users logged into the matrix switch, the device must be configured with UID locking.

By combining user rights with UID locking, a user must be logged into the TOE before the TOE will permit them to perform any actions on a specific device the user wishes to connect to, and only if the user is permitted to perform those actions on that device.

1.4.1 TOE Components

1.4.1.1 Vision-IP and VisionXS-IP (CON) and (CPU)

The Vision-IP series and VisionXS-IP series includes both console modules (CON) and computer modules (CPU). Multiple variations of the modules are detailed on the G&D website. Depending on the variant, the devices support up to 4K video compressed at 60 Hz, full keyboard/mouse emulation, serial communication, analog audio, embedded audio signals and up to 10Gbit/s ethernet data rate. Video interfaces include DisplayPort, DVI-I, DVI-D and USB-C. The devices also include a management network interface for access to a web-based Config Panel for management. Each management activity creates an audit log that is sent to an internal syslog server via the syslog protocol. Typically, one CON device is required for each monitor and one CPU device for each computer. For the evaluated environment the VisionXS-IP-DP-UHR-CON and VisionXS-IP-DPI-UHR-CPU-UG, which are both apart of the VisionXS-IP series, with VisionXS-IP firmware v1.5 is used. A CorSSL self-test routine is ran every time the Vision-IP and VisionXS-IP console and computer modules are powered on or reset to verify the integrity of the TOE and its firmware.

1.4.1.2 RemoteAccess-IP-CPU

The RemoteAccess-IP series includes only computer modules (CPU). Multiple variations of the modules are detailed on the G&D website. Depending on the variant, the devices let the user integrate virtual machines into an IP matrix switch ControlCenter-IP(-XS). The virtual machines can be accessed via network. To establish a network connection to virtual machines, use the SSH protocol. In addition, streams can also be received via RTP/TCP, RTSP/TCP and MMSH transport protocols. The H.264, VP8 and VP9 codecs for decoding video data and MPGA, MP3 and AC3 for decoding audio data are supported. The device also includes a management network interface for access to a web-based Config Panel for management. Each management activity creates an audit log that is sent to an internal syslog server via the syslog protocol. For the evaluated environment the Remote-IP-CPU-UG RemoteAccess-IP firmware v1.3 is used. A CorSSL self-test routine is ran every time the RemoteAccess-IP-CPU is powered on or reset to verify the integrity of the TOE and its firmware.

1.4.1.3 ControlCenter-IP(-XS)

ControlCenter-IP(-XS) provides IP-based matrix functions for the TOE alongside of at least a layer 2 managed switch that has additional control and monitoring features in addition to basic switch functions. The following settings in the network switch must be configured to ensure smooth operation of the IP matrix:

- Gigabit Ethernet capabilities
- Multicast
- IGMP[3]

[2] UID – Unique Identifier

[3] IGMP – Internet Group Management Protocol

- IGMP snooping
- IGMP Snooping Querier
- Ports 18244, 18245, and 18246 are open

ControlCenter-IP(-XS) handles the network logic to ensure all devices are accessible to each other and provides central administration for more than 2,000 devices. All communication and data transmissions are encrypted. Devices can be auto recognized. ControlCenter-IP(-XS) provides a web-based interface for management. Each management activity creates an audit log that is sent to an internal syslog server via the syslog protocol. The ControlCenter-IP 2.0 provides two data ethernet ports with a 10Mbit/s, 100Mbit/s or 1Gbit/s data rate.

ControlCenter-IP with firmware v1.7 is the tested device and ControlCenter-IP-XS with firmware v1.1 is a smaller form factor of the same device that in turn supports fewer devices. A CorSSL self-test routine is ran every time the ControlCenter-IP(-XS) is powered on or reset to verify the integrity of the TOE and its firmware.

The TOE provides central administration of registered and connected devices. The TOE has an integrated DHCP[4] server that is deactivated by default.

1.5 TOE Environment

The SecureCert feature is required when ordering the components of the TOE to ensure that the TOE is CC compliant. The TOE allows each component to connect to an NTP[5] server to provide NTP-synchronized date and time for reliable time stamps.

Network switches are required non-TOE components used alongside the ControlCenter-IP(-XS) to ensure the TOE works properly. The following must be configured on the network switches:

1. At least layer 2 managed switch that has additional control and monitoring features in addition to basic switch functions
2. Gigabit Ethernet capabilities
3. Multicast
4. IGMP
5. IGMP snooping
6. IGMP Snooping Querier
7. Ports 18244, 18245, and 18246 are open

[4] DHCP - Dynamic Host Configuration Protocol
[5] NTP – Network Time Protocol

1.6 TOE Description

This section primarily addresses the physical and logical components of the TOE that are included in the evaluation.

1.6.1 Physical Scope

Figure 1 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE.

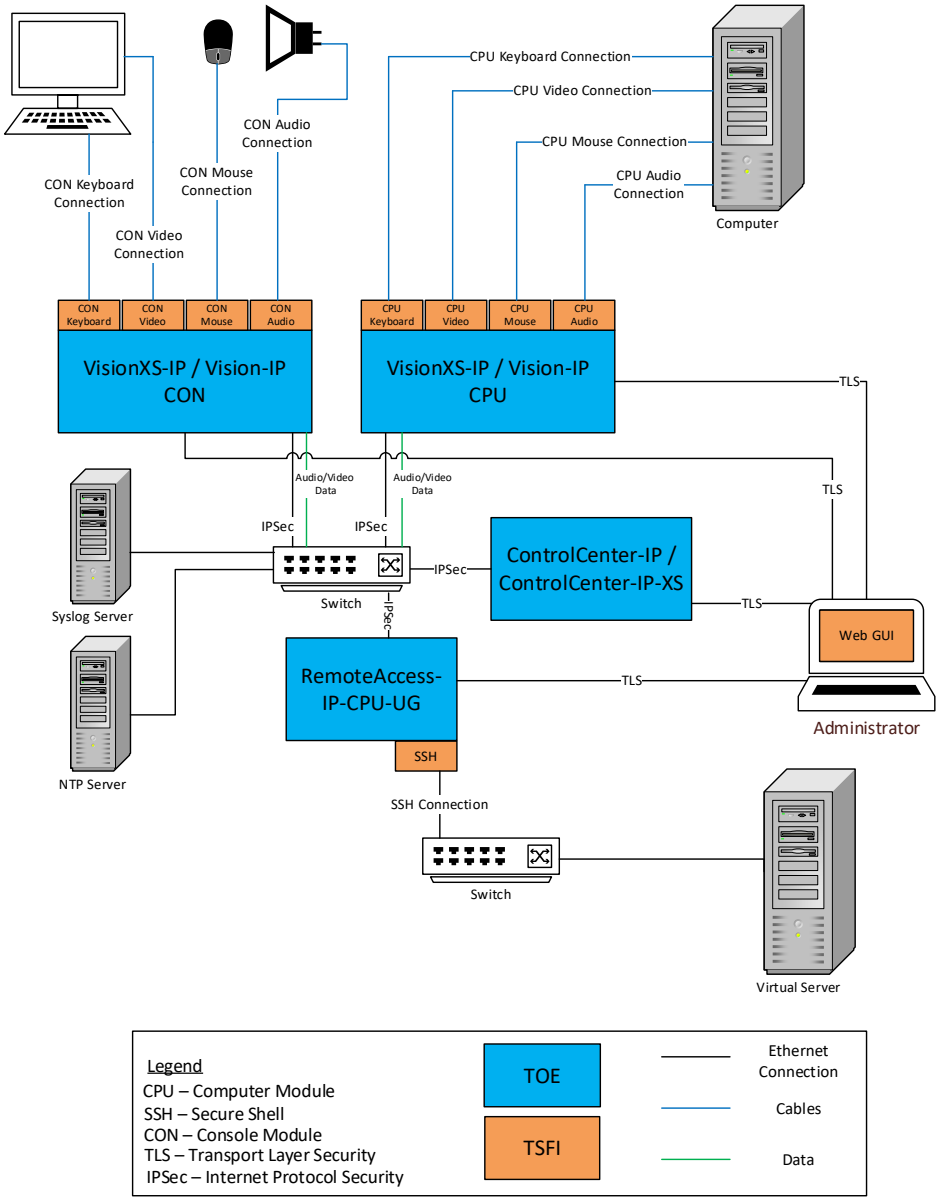

Figure 1 – Physical TOE Boundary

Note: The customer has the option to choose the XS or regular version of each available device, but any type can be used interchangeably within the TOE environment. For example, if VisionXS-IP CPU is used, VisionXS-IP CON or Vision-IP CON and ControlCenter-IP-XS or ControlCenter-IP can be used.

1.6.1.1 TOE Hardware and Firmware

The TOE is a hardware and firmware TOE, specifically KVM-over-IP, and is comprised of the components detailed in the following table.

Table 2 – TOE Components

Component	Firmware Version
ControlCenter-IP series	ControlCenter-IP firmware v1.7
ControlCenter-IP-XS series	ControlCenter-IP-XS firmware v1.1
Vision-IP series	Vision-IP firmware v2.4
VisionXS-IP series	VisionXS-IP firmware v1.5
RemoteAccess-IP series	RemoteAccess-IP firmware v1.3

1.6.1.2 Guidance Documentation

The guidance documents relevant to the installation and configuration of the TOE can be downloaded through the G&D website at https://www.gdsys.com/en/securecert or may be provided to the customer by email. The following PDF formatted guides (and corresponding SHA-256 hashes) are required reading and part of the TOE:

Table 3 – TOE Guidance Documentation Hashes

TOE Guidance Documentation	SHA-256 Hash
Configuring the matrix switch ControLCenter-IP with the web application >>Config Panel<< (English – version 1.70) July 24, 2025	554F1E4EC09C55E1F416DA90A502EE3C63B3F56EC77A6521B54B0261103B0570
Configuration and Operation of ControlCenter-IP (English - version 1.70) July 24, 2025	44BD856976C67D7E9957FEFFA8BAC7AF7809BB9D9D447487897AE3143735D563
Configuring the matrix switch ControLCenter-IP-XS with the web application >>Config Panel<< (English – version 1.10) July 29, 2025	0DE55FE6EB01BA1BF82269FDA12458A2CB31305291DD8048B3755C56A27FA96E
Configuration and Operation of ControlCenter-IP-XS (English - version 1.10) July 29, 2025	2703E12F0BF28BF4E6E1CBA6A502270703E16C60D77BC5BC623CAF3061BB2A29
»Config Panel« web application for the Vision-IP series (English – version 2.40) August 8, 2025	618F250DFF30BA5176569F0F763C811A7BA66B368C6EBDF3DEC418DD2D4AECE1
»Config Panel« web application for the VisionXS-IP series (English - version 1.40) July 29, 2025	B0558E4F8CFC45AFC2143061308544C477924AC0D861953E64E0AF8CA072483D
Configuring the RemoteAccess-IP-CPU with the web application >>Config Panel<< (English – version 1.20) September 5, 2025	310D6994A0590947E3C95761AB7AAAC3CCCC62AFE4258D1AC26532F1F46471CF
Installation Guide for ControlCenter-IP (German/English - version 1.70) July 24, 2025	01139D6B930BC7437B968EAC0E7026BC10B527A2E14652D60B109A01F9F9F76E
Installation Guide for ControlCenter-IP-XS (German/English - version 1.10) July 29, 2025	065004A9F4CA98C5C754B75DA2BE6C02481BBA58B099097D618DED5038D2D9E3
Installation and Operating of DP1.2-Vision-IP (German/English - version 1.40) August 8, 2025	387D62E9FFA0936176AE32EAE2421F79CE649989716E96B5C7E01A85DFBBF653
Installation and Operating Guide for VisionXS-IP-C-DP-UHR (German/English – version 1.40) July 29, 2025	A277B5D790392526674B848B3B511999929B9B8C83760E67DEAEAD567E238070
Installation Guide for RemoteAccess-IP-CPU (German/English - version 1.30) September 5, 2025	552D0E354FD4A51C2591C684AEC9B4C513ADC7431B5B54BF47B102FE3E95AAC7

The Guidance Documentation Supplement document is labelled as the following:

- G&D KVM-over-IP matrix system with: ControlCenter-IP series with firmware 1.7, ControlCenter-IP-XS series with firmware 1.1, RemoteAccess-IP series with firmware 1.3, Vision-IP series with firmware 2.4, Vision XS-IP series with firmware 1.5 Guidance Documentation Supplement Evaluation Assurance Level (EAL): EAL2+ Document Version: v0.17

The Guidance Documentation Supplement has the following hash value:

- SHA-256 Hash: 30A7B64C43184D501C1B570977A1AF4EC236FD66E1817CF54E2A88389C84262C

1.6.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The SFRs implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- Security Management
- Identification and Authentication
- User Data Protection
- Protection of the TSF

1.6.2.1 Security Audit

The TOE's components log administrative actions and send audit log messages to an internal syslog server via the syslog protocol.

1.6.2.2 User Data Protection

The TOE ensures that only connections with authorized devices are permitted. Video and analog audio signals as well as serial (RS232) signals flow unidirectionally from one peripheral interface to another while being protected from unauthorized users. USB signals (keyboard, mouse, HID and mass storage devices) flows bidirectionally.

1.6.2.3 Identification and Authentication

Administrators authenticate to the TOE using a username and password. In addition, 2-factor authentication can be used.

1.6.2.4 Security Management

The TOE's Web GUI lets administrators configure and manage specific TOE settings, view audit messages, and manage users.

1.6.2.5 Protection of the TSF

The TOE automatically runs a set of self-tests every time it is powered on or reset. This includes verifying the integrity of the firmware running on a TOE component. The TOE allows each component to connect to an NTP[5] server to provide NTP-synchronized date and time for reliable time stamps.

1.6.3 Product Physical/Logical Features and Functionality not included in the TOE

Features and/or Functionality that are not part of the evaluated configuration of the TOE include:

[5] NTP – Network Time Protocol

- SNMPv3
- RDP
- VNC

2. Conformance Claims

This section and Table 4 provide the identification for any CC, PP, and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 4 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017; CC Part 2 conformant; CC Part 3 conformant; no PP claim; EAL 2 with augmentation of ALC_FLR.2.
PP Identification	None
Evaluation Assurance Level	EAL2 augmented with Flaw Remediation (ALC_FLR.2)

3. Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies to which the TOE must comply
- Assumptions about the TOE, including physical, personnel, and connectivity aspects

3.1 Threats to Security

The threats for the TOE are listed in the following table. The description of each threat is followed by a rationale describing how it is addressed by the SFRs in the following chapters.

Table 5 – Threats

Name	Description
T.DATA_LEAK	A connection through the TOE between one or more computers may allow unauthorized data flow through the TOE.
T.SIGNAL_LEAK	A connection through the TOE between one or more computers may allow unauthorized data flow through bit-by-bit signaling.
T.RESIDUAL_LEAK	The TOE may leak (partial, residual, or echo) user data between the intended connected computer and another unintended connected computer.
T. UNINTENDED_USE	The TOE may connect the user to a computer other than the one to which the user intended to connect.
T.UNAUTHORIZED_DEVICES	The use of an unauthorized peripheral device with a specific TOE port may allow unauthorized data flows between connected devices or enable an attack on the TOE or its connected computers.
T.FAILED	Detectable failure of the TOE may cause an unauthorized information flow or weakening of TOE security functions.

3.2 Organizational Security Policies

The TOE does not require any organizational security policies.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. Table 6 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 6 – Assumptions

Name	Description
A.PHYSICAL	The TOE is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the device's physical interconnections and correct operation.
A.NO_WIRELESS_DEVICES	The environment includes no wireless peripheral devices.
A.TRUSTED_ADMIN	Administrators are trusted to follow and apply all guidance in a trusted manner.
A.NETWORK	Access to the TOE's ConfigPanel can be restricted to individual IP networks and individual devices.

Name	Description
A.TIMESTAMP	The IT environment provides the TOE with the necessary reliable timestamps.

4. Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 7.

Table 7 – Security Objectives for the TOE

Name	Description
O.COMPUTER_INTERFACE_ISOLATION	The TOE shall prevent unauthorized data flow to ensure that its connected peripheral devices cannot be exploited in an attempt to leak data. The TOE-computer interface shall be isolated from all other Computer interfaces while the TOE is powered.
O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED	The TOE shall not allow data to transit a Computer interface while the TOE is unpowered.
O.USER_DATA_ISOLATION	The TOE shall route user data, such as keyboard entries, only to the computer selected by the user. The TOE shall provide isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer.
O.NO_USER_DATA_RETENTION	The TOE shall not retain user data in non-volatile memory after power up or, if supported, factory reset.
O.NO_OTHER_EXTERNAL_INTERFACES	The TOE shall not have any external interfaces other than those implemented by the TSF.
O.LEAK_PREVENTION_SWITCHING	The TOE shall ensure that there are no switching mechanisms that allow signal data leakage between connected computers.
O.AUTHORIZED_USAGE	The TOE shall explicitly prohibit or ignore unauthorized switching mechanisms, either because it supports only one connected computer or because it allows only authorized mechanisms to switch between connected computers. Authorized switching mechanisms shall require express user action restricted to console buttons, console switches, console touch screen, wired remote control, and peripheral devices using a guard. Unauthorized switching mechanisms include keyboard shortcuts, also known as "hotkeys," automatic port scanning, control through a connected computer, and control through keyboard shortcuts. Where applicable, the results of the switching activity shall be indicated by the TSF so that it is clear to the user that the switching mechanism was engaged as intended. The TOE provides a management function to configure some aspects of the TSF, ensuring that whatever management functions it provides can only be performed by authorized administrators. The NTP server provides synchronized date and time for reliable time stamps.
O.PERIPHERAL_PORTS_ISOLATION	The TOE shall ensure that data does not flow between peripheral devices connected to different interfaces.
O.REJECT_UNAUTHORIZED_PERIPHERAL	The TOE shall reject unauthorized peripheral device types and protocols.
O.SELF_TEST	The TOE shall perform self-tests following power up or powered reset.

Name	Description
O.SELF_TEST_FAIL_INDICATION	The TOE shall provide clear and visible user indications in the case of a self-test failure.
O.SELF_TEST_FAIL_TOE_DISABLE	The TOE shall enter a secure state upon detection of a critical failure.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 Non-IT Security Objectives

Table 8 lists the non-IT environment security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 8 – Non-IT Security Objectives

Name	Description
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_WIRELESS_DEVICES	The operational environment will not include wireless keyboards, mice, audio, user authentication, or video devices.
OE.TRUSTED_ADMIN	The operational environment will ensure that trusted TOE Administrators are appropriately trained.
OE.NETWORK	The operational environment will ensure that trusted Administrators will be able to configure network restrictions.
OE.TIMESTAMP	The operational environment will ensure that the NTP servers providing time information to the TOE shall be on the local network and inaccessible to non-administrators.

5. Extended Components

This section details the extended SFRs and extended SARs met by the TOE.

5.1 Extended TOE Security Functional Components

This ST does not contain any extended security functional components.

5.2 Extended TOE Security Assurance Components

This ST does not contain any extended security assurance components.

6. Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignmentand selection operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Completed assignment statements within a selection statement are identified using [*underlined and italicized text within brackets*].

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 9 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 9 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	✓	✓		
FAU_STG.1	Protected audit trail storage	✓			
FDP_ETC.1	Export of User Data Without Security Attributes		✓		
FDP_IFC.1	Subset information flow control		✓		
FDP_IFF.1	Simple security attributes		✓		
FDP_ITC.1	Import of User Data Without Security Attributes		✓		
FIA_UAU.2	User authentication before any action				
FIA_UID.2	User Identification before any action				
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialization	✓	✓		
FMT_SMF.1	Specification of Management Functions		✓		
FMT_SMR.1	Security Roles		✓		
FPT_TST.1	TSF testing	✓	✓		

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

a. Start-up and shutdown of the audit functions;
b. All auditable events, for the [not specified] level of audit; and
c. [*user authentication*
changes to configurations].

FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

a. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other events*].

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1

The TSF shall be protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2

The TSF shall be able to [detect] unauthorized modifications to the stored audit records in the audit trail.

6.2.2 Class FDP: User Data Protection

FDP_ETC.1 Export of User Data Without Security Attributes

Hierarchical to: No other components

Dependencies: FDP_IFC.1 Subset information flow control
FDP_ACC.1 Subset access control

FDP_ETC.1.1

The TSF shall enforce the [*information flow control SFP*[6]] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2

The TSF shall export the user data without the user data's associated security attributes.

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components

Dependencies: FDP_IFF.1 Simple security attributes

The TSF shall enforce the [*information flow control SFP*] on [

- *Subject: devices, users*
- *Information: USB data, keyboard data, mouse data, video data, audio data*
- *Operations: bidirectional, unidirectional data flow between UID-locked peripheral device connections and the TOE*

].

[6] SFP – Security Function Policy

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1

The TSF shall enforce the [*information flow control SFP*] based on the following types of subject and information security attributes: [

- *subject: devices,*
  - *attribute: IP address, UID*
- *subject: users,*
  - *attribute: user permissions*
- *information controlled: USB, video, audio, keyboard, mouse data*

].

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: [*device IP is identified by UID locking and user has permissions for operation*].

FDP_IFF.1.3

The TSF shall enforce the [*data is purged prior to switching connections*].

FDP_IFF.1.4

The TSF shall explicitly authorise an information flow based on the following rules: [*data flow between UID-locked peripheral device connections and the TOE components' interfaces, unidirectional flow for video and audio data, bi-directional flow for USB, keyboard, and mouse data*].

FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules: [*the peripheral device IP address is not UID-locked*].

FDP_ITC.1 Import of User Data Without Security Attributes

Hierarchical to: No other components

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_ITC.1.1

The TSF shall enforce the [*information flow control SFP*] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2

The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE..

FDP_ITC.1.3

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [*no additional rules*].

6.2.3 Class FIA: Identification and Authentication

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication
Dependencies: FIA_UID.1 Timing of identification
FIA_UAU.2.1

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No dependencies
FIA_UID.2.1

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.4 Class FMT: Security Management

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components
Dependencies: FDP_IFC.1 Subset information flow control
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1

The TSF shall enforce the [*information flow control SFP*] to restrict the ability to [modify, delete, create] the security attributes [*user rights*] to [*administrators*].

FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles
FMT_MSA.3.1

The TSF shall enforce the [*information flow control 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 [*authorized administrators*] to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components
Dependencies: No dependencies
FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [

- *View the behavior of and configure KVM System Components*
- *Disable, enable, and modify Netfilter rules*
- *Creation and deletion of administrators*
- *Create, modify, and delete user permissions*

].

FMT_SMR.1 Security roles

Hierarchical to: No other components
Dependencies: FIA_UID.1 Timing of identification
FMT_SMR.1.1

The TSF shall maintain the roles [*administrators*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.2.5 Class FPT: Protection of the TSF

FPT_TST.1 TSF testing

Hierarchical to: No other components
Dependencies: No dependencies
FPT_TST.1.1

The TSF shall run a suite of self-tests [during initial start-up] to demonstrate the correct operation of [*the firmware image*].

FPT_TST.1.2

The TSF shall provide authorized users with the capability to verify the integrity of [TSF data].

FPT_TST.1.3

The TSF shall provide authorized users with the capability to verify the integrity of [*the firmware image*].

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3. Table 10 summarizes these requirements.

Table 10 – Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ALC: Life Cycle Support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM Coverage
	ALC_DEL.1 Delivery Procedures
	ALC_FLR.2 Flaw reporting procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – Sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

7. TOE Summary Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functionality

Each of the security requirements and the associated descriptions correspond to a security functionality. Hence, each security functionality is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functionality and rationalize that the security functionality satisfies the necessary requirements. Table 11 lists the security functionality and their associated SFRs.

Table 11 – Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_STG.1	Protected Audit Trail Storage
User Data Protection	FDP_ETC.1	Export of User Data Without Security Attributes
	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
	FDP_ITC.1	Import of User Data Without Security Attributes
Identification and Authentication	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_TST.1	TSF testing

7.1.1 Security Audit

The TOE's components generate audit messages for startup and shutdown of the audit function, user authentication, changes to configurations and send these to the internal syslog server via the syslog protocol. These audit messages are protected from unauthorized deletion and the TOE will detect when unauthorized modifications to the stored audit records have occurred.

The TOE audit records contain the following information:

Table 12 – Audit Record Contents

Field	Content
Timestamp	YYYY-MM-DDTHH:MM:SS±HHMM
Log name	Possible logs are:syslog
Syslog Severity Levels	Level 0 'emerg', 1 'alert', 2 'crit', 3 'err', 4 'warning', 5 'notice', 6 'info', 7 'debug'
Device name and Unique ID	Device name and UID of the device that generated the log message
Event type	Type of event, such as configuration change, authentication

Field	Content
Outcome	If applicable, success or failure

```
2024-06-17T08:00:51+02:00 syslog@CCIP000004EC info: ControlCenter-IP 'CCIP 000004EC'
(0x000004EC): User 'Admin' modified syslog parameters of device 'CCIP 000004EC'
(000004EC:00000102) via IP '172.17.30.48'
```

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_STG.1

7.1.2 User Data Protection

The TOE uses device UIDs and user permissions to determine what connections are allowed. Video and audio data flows unidirectionally from one peripheral interface to another while being protected from unauthorized users. USB data and keyboard and mouse data flow bidirectionally between peripheral devices based on UID locking and user permissions. If a console device is not permitted network access via UID locking, or if a user does not have sufficient access rights to a device, the device will not be accessible, and no video, audio, USB, keyboard, or mouse data will be transmitted to the device connected to the computer module. The TOE supports USB connections for keyboard and mouse. Non-volatile memory or storage is not used in any way for user data, with keyboard data purged upon switching computers. User data is not imported or exported with the user permissions or device UID.

TOE Security Functional Requirements Satisfied: FDP_ETC.1, FDP_IFC.1, FDP_IFF.1, FDP_ITC.1.

7.1.3 Identification and Authentication

Administrators authenticate to the TOE using a username and password prior to any access to the systems. The username and password is verified by the TOE itself in the TOE environment. Two-factor authentication can also be configured.

TOE Security Functional Requirements Satisfied: FIA_UAU.2, FIA_UID.2

7.1.4 Security Management

The TOE's Web GUI is used by administrators to configure and manage specific TOE settings, view the behavior of and configure KVM System Components, disable, enable, and modify Netfilter rules, and manage users. User management includes creating and deleting administrators and managing, modifying, and deleting user's permissions. User rights can be modified, deleted, or created by an administrator. Administrators are given permission to change default values for security attributes and specify the alternative initial values when an object or information is created. The only role supported by the TOE is the administrator role.

TOE Security Functional Requirements Satisfied: FMT_MSA.1, FMT_MSA.3, FTM_SMF.1, FMT_SMR.1

7.1.5 Protection of the TSF

The TOE's components automatically run a set of self-tests every time they are powered on or reset. This includes verifying the integrity of the firmware running on a TOE component. The firmware images are ControlCenter-IP series with firmware 1.7.000 (00745), ControlCenter-IP-XS series with firmware 1.1.000 (00287), RemoteAccess-IP series with firmware 1.3.000 (00296), Vision-IP series with firmware 2.4.000 (00970), and Vision XS-IP series with firmware 1.5.000 (00916). The TOE allows each component to connect to an NTP server to provide NTP-synchronized date and time for reliable time stamps. An NTP Server's trusted key is imported with the G&D ConfigPanel. This allows for authentication of the NTP server. Administrators must configure the hashing

algorithm for the trusted key to be SHA-1. A trusted administrator must configure the time synchronization with the NTP server based on their time zone.

TOE Security Functional Requirements Satisfied: FPT_TST.1

8. Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 5.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat and assumption that compose the Security Target. Sections 8.2.1 and 8.2.2 demonstrate the mappings between the threats and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 13 provides a mapping of the objectives to the threats they counter.

Table 13 – Threats: Objectives Mapping

Threats	Objectives	Rationale
T.DATA_LEAK A connection through the TOE between one or more computers may allow unauthorized data flow through the TOE.	O.COMPUTER_INTERFACE_ISOLATION The TOE shall prevent unauthorized data flow to ensure that its connected peripheral devices cannot be exploited in an attempt to leak data. The TOE-computer interface shall be isolated from all other Computer interfaces while the TOE is powered.	Isolation of computer interfaces prevents data from leaking between them without authorization.
	O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED The TOE shall not allow data to transit a Computer interface while the TOE is unpowered.	Maintaining interface isolation while the TOE is in an unpowered state ensures that data cannot leak between computer interfaces.
	O.USER_DATA_ISOLATION The TOE shall route user data, such as keyboard entries, only to the computer selected by the user. The TOE shall provide isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer.	The TOE's routing of data only to the selected computer ensures that it will not leak to any others.
	O.NO_OTHER_EXTERNAL_INTERFACES The TOE shall not have any external interfaces other than those implemented by the TSF.	The absence of additional external interfaces ensures that there is no unexpected method by which data can be leaked.
	O.PERIPHERAL_PORTS_ISOLATION The TOE shall ensure that data does not flow between peripheral devices connected to different interfaces.	Isolation of peripheral ports prevents data from leaking between them without authorization.
T.SIGNAL_LEAK A connection through the TOE between one or more computers may allow unauthorized data flow through bit-by-bit signaling.	O.COMPUTER_INTERFACE_ISOLATION The TOE shall prevent unauthorized data flow to ensure that its connected peripheral devices cannot be exploited in an attempt to leak data. The TOE-computer interface shall be isolated from all other Computer interfaces while the TOE is powered.	Isolation of computer interfaces prevents data leakage through bit-wise signaling because there is no mechanism by which the signal data can be communicated.
	O.NO_OTHER_EXTERNAL_INTERFACES The TOE shall not have any external interfaces other than those implemented by the TSF.	The absence of additional external interfaces ensures that there is no unexpected method by which data can be leaked through bit-wise signaling
	O.LEAK_PREVENTION_SWITCHING The TOE shall ensure that there are no switching mechanisms that allow signal data leakage between connected computers.	The TOE's use of switching methods that are not susceptible to signal leakage helps mitigate the signal leak threat.

Threats	Objectives	Rationale
T.RESIDUAL_LEAK The TOE may leak (partial, residual, or echo) user data between the intended connected computer and another unintended connected computer.	O.NO_USER_DATA_RETENTION The TOE shall not retain user data in non-volatile memory after power up or, if supported, factory reset.	The TOE's lack of data retention ensures that a residual data leak is not possible
T. UNINTENDED_USE The TOE may connect the user to a computer other than the one to which the user intended to connect.	O.AUTHORIZED_USAGE The TOE shall explicitly prohibit or ignore unauthorized switching mechanisms, either because it supports only one connected computer or because it allows only authorized mechanisms to switch between connected computers. Authorized switching mechanisms shall require express user action restricted to console buttons, console switches, console touch screen, wired remote control, and peripheral devices using a guard. Unauthorized switching mechanisms include keyboard shortcuts, also known as "hotkeys," automatic port scanning, control through a connected computer, and control through keyboard shortcuts. Where applicable, the results of the switching activity shall be indicated by the TSF so that it is clear to the user that the switching mechanism was engaged as intended. The TOE provides a management function to configure some aspects of the TSF, ensuring that whatever management functions it provides can only be performed by authorized administrators. The NTP server provides synchronized date and time for reliable time stamps.	The TOE's support for only switching mechanisms that require explicit user action to engage ensures that a user has sufficient information to avoid interacting with an unintended computer.
T.UNAUTHORIZED_DEVICES The use of an unauthorized peripheral device with a specific TOE port may allow unauthorized data flow between connected devices or enable an attack on the TOE or its connected computers.	O.REJECT_UNAUTHORIZED_PERIPHERAL The TOE shall reject unauthorized peripheral device types and protocols.	The TOE's ability to reject unauthorized peripherals mitigates the threat of unauthorized devices being used to communicate with connected computers.
T.FAILED Detectable failure of the TOE may cause an unauthorized information flow or weakening of TOE security functions.	O.SELF_TEST The TOE shall perform self-tests following power up or powered reset.	The TOE mitigates the threat of failures leading to compromise of security functions through self-tests of its own functionality
	O.SELF_TEST_FAIL_TOE_DISABLE The TOE shall enter a secure state upon detection of a critical failure.	The TOE mitigates the threat of failures leading to compromise of security functions by disabling all data flows in the event a failure is detected.
	O.SELF_TEST_FAIL_INDICATION The TOE shall enter a secure state upon detection of a critical failure.	The TOE mitigates the threat of failures leading to compromise of security functions by providing users with a clear indication when it is in a failure state and should not be trusted.

This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Assumptions

Table 14 provides a mapping of assumptions and the environmental objectives that uphold them.

Table 14 – Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.PHYSICAL The TOE is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the device's physical interconnections and correct operation.	OE.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	If the TOE's operational environment provides physical security, then the assumption is satisfied.
A.NO_WIRELESS_DEVICES The environment includes no wireless peripheral devices.	OE.NO_WIRELESS_DEVICES The operational environment will not include wireless keyboards, mice, audio, user authentication, or video devices.	If the TOE's operational environment does not include wireless peripherals, then the assumption is satisfied.
A.TRUSTED_ADMIN Administrators are trusted to follow and apply all guidance in a trusted manner.	OE.TRUSTED_ADMIN The operational environment will ensure that trusted TOE Administrators are appropriately trained.	If the TOE's operational environment ensures that only trusted administrators will manage the TSF, then the assumption is satisfied.
A.NETWORK Access to the TOE's ConfigPanel can be restricted to individual IP networks and individual devices.	OE.NETWORK The operational environment will ensure that trusted Administrators will be able to configure network restrictions.	If the TOE's operational environment ensures that trusted Administrators will be able to configure network restrictions, then the assumption is satisfied.
A.TIMESTAMP The IT environment provides the TOE with the necessary reliable timestamps.	OE.TIMESTAMP The operational environment will ensure that the NTP servers providing time information to the TOE shall be on the local network and inaccessible to non-administrators.	If the TOE's operational environment ensures that the NTP servers providing time information to the TOE shall be on the local network and inaccessible to non-administrators, then the assumption is satisfied.

This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.2.3 Security Objectives Rationale Relating to Organizational Security Policies

There are no Organizational Security Policies defined for this ST.

8.3 Rationale for Extended Security Functional Requirements

There are no extended SFRs defined for this ST.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended SARs defined for this ST.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 15 – Mapping of SFRs to Security Objectives

Objective	SFR												
	FAU_GEN.1	FAU_STG.1	FDP_ETC.1	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1	FIA_UAU.2	FIA_UID.2	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FMT_SMR.1	FPT_TST.1
O.COMPUTER_INTERFACE_ISOLATION			X	X	X	X							
O.USER_DATA_ISOLATION			X	X	X	X							
O.NO_OTHER_EXTERNAL_INTERFACES			X	X	X	X							
O.LEAK_PREVENTION_SWITCHING			X	X	X	X							
O.AUTHORIZED_USAGE	X	X	X	X	X	X	X	X	X	X	X	X	
O.PERIPHERAL_PORTS_ISOLATION			X	X	X	X							
O.REJECT_UNAUTHORIZED_PERIPHERAL			X	X	X	X							
O.SELF_TEST													X

Table 16 provides a mapping of the objectives and the SFRs that support them.

Table 16 – Objectives: SFRs Mapping

Objective	SFR	Rationale
O.COMPUTER_INTERFACE_ISOLATION The TOE shall prevent unauthorized data flow to ensure that its connected peripheral devices cannot be exploited in an attempt to leak data. The TOE-computer interface shall be isolated from all other Computer interfaces while the TOE is powered.	FDP_ETC.1 FDP_IFC.1 FDP_IFF.1 FDP_ITC.1	These information flow policies prevent unauthorized data flows between the different computer interfaces in the TOE.
O.USER_DATA_ISOLATION The TOE shall route user data, such as keyboard entries, only to the computer selected by the user. The TOE shall provide isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer.	FDP_ETC.1 FDP_IFC.1 FDP_IFF.1 FDP_ITC.1	These information flow policies ensure that user data will only transit the TOE to the computer that the user has explicitly selected it to go to and provides isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer.
O.NO_OTHER_EXTERNAL_INTERFACES The TOE shall not have any external interfaces other than those implemented by the TSF.	FDP_ETC.1 FDP_IFC.1 FDP_IFF.1 FDP_ITC.1	These information flow policies ensure all unauthorized devices and external interfaces are rejected, thus ensuring no signal data can be injected into the user data.
O.LEAK_PREVENTION_SWITCHING The TOE shall ensure that there are no switching mechanisms that allow signal data leakage between connected computers.	FDP_ETC.1 FDP_IFC.1 FDP_IFF.1 FDP_ITC.1	By preventing the use of unauthorized switching methods, signaling data leakage between connected computers is also prevented.

Objective	SFR	Rationale
O.AUTHORIZED_USAGE The TOE shall explicitly prohibit or ignore unauthorized switching mechanisms, either because it supports only one connected computer or because it allows only authorized mechanisms to switch between connected computers. Authorized switching mechanisms shall require express user action restricted to console buttons, console switches, console touch screen, wired remote control, and peripheral devices using a guard. Unauthorized switching mechanisms include keyboard shortcuts, also known as "hotkeys," automatic port scanning, control through a connected computer, and control through keyboard shortcuts. Where applicable, the results of the switching activity shall be indicated by the TSF so that it is clear to the user that the switching mechanism was engaged as intended. The TOE provides a management function to configure some aspects of the TSF, ensuring that whatever management functions it provides can only be performed by authorized administrators. The NTP server provides synchronized date and time for reliable time stamps.	FAU_GEN FAU_STG.1 FDP_ETC.1 FDP_IFC.1 FDP_IFF.1 FDP_ITC.1 FIA_UAU.2 FIA_UID.2 FMT_MSA.1 FMT_MSA.3 FMT_SMF.1 FMT_SMR.1	The SFRs mapped to this objective enforce authorized usage of the TOE through ensuring that the TOE either supports only one connected computer or by ensuring users can only control the behavior of peripheral and computer interfaces using authorized mechanisms, and through ensuring that administrators can only perform management functions with proper authorization. They also ensure that unauthorized usage is detected through the use of an auditing function and that a user does not inadvertently perform an action against an unintended computer through continuous indications of the selected port(s). The TOE relies on the NTP server for reliable time stamps.
O.PERIPHERAL_PORTS_ISOLATION The TOE shall ensure that data does not flow between peripheral devices connected to different interfaces.	FDP_ETC.1 FDP_IFC.1 FDP_IFF.1 FDP_ITC.1	These information flow policies ensure that there is no method by which unauthorized data flow can occur between peripheral ports.
O.REJECT_UNAUTHORIZED_PERIPHERAL The TOE shall reject unauthorized peripheral device types and protocols.	FDP_ETC.1 FDP_IFC.1 FDP_IFF.1 FDP_ITC.1	These information flow policies ensure the TOE rejects or otherwise prevents operation of unauthorized peripheral devices or protocols to work with the TOE.
O.SELF_TEST The TOE shall perform self-tests following power up or powered reset.	FPT_TST.1	The TOE performs self-tests following power up or powered reset to increase the likelihood that a malfunction in the TSF is detected.

8.5.2 Security Assurance Requirements Rationale

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. At EAL2, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria. The following table lists each SFR to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 17 – SFR Dependencies and Rationales

SFR	Dependency	Rationale
FAU_GEN.1 Audit Data Generation	FPT_STM.1 Reliable time stamps	Although FPT_STM.1 is not included, OE.TIMESTAMP ensures that the IT environment provides an accurate time.
FAU_STG.1 Protected audit trail storage	FAU_GEN.1 Audit Data Generation	Included

SFR	Dependency	Rationale
FDP_ETC.1 Export of User Data Without Security Attributes	FDP_IFC.1 Subset information flow control FDP_ACC.1 Subset access control	Included FDP_ACC.1 is optional and therefore not included
FDP_IFC.1 Subset information flow control	FDP_IFF.1 Simple security attributes	Included
FDP_IFF.1 Simple security attributes	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization	Included
FDP_ITC.1 Import of User Data Without Security Attributes	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization FDP_ACC.1 Subset access control	Included FDP_ACC.1 is optional and therefore not included
FIA_UAU.2 User authentication before any action	FIA_UID.1 Timing of identification	FIA_UID.2 is hierarchical to FIA_UID.1
FIA_UID.2 User identification before any action	None	N/A
FMT_MSA.1 Management of security attributes	FDP_IFC.1 Subset information flow control FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions FDP_ACC.1 Subset access control	Included FDP_ACC.1 is optional and therefore not included
FMT_MSA.3 Static attribute initialization	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	Included
FMT_SMF.1 Specification of Management Functions	None	N/A
FMT_SMR.1 Security roles	FIA_UID.1 Timing of identification	FIA_UID.2 is hierarchical to FIA_UID.1
FPT_TST.1 TSF testing	None	N/A

Acronyms and Terms

Table 18 defines the acronyms and terms used throughout this document.

Table 18 – Acronyms and Terms

Acronym	Definition
AD	Active Directory
CAT	Category
CC	Common Criteria
CON	Console Module
CPU	Computer Module
DHCP	Dynamic Host Configuration Protocol
DL	Dual-Link
DVI	Digital Visual Interface
EAL	Evaluation Assurance Level
G&D	Guntermann & Drunck
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
KVM	Keyboard Video Mouse
NTP	Network Time Protocol
OS	Operating System
PP	Protection Profile
RDP	Remote Desktop Protocol
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
UID	Unique Identifier
USB	Universal Serial Bus
VNC	Virtual Network Computing

Prepared by:

Corsec Security, Inc.

12600 Fair Lakes Circle, Suite 210
Fairfax, VA 22003
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com