IBM
PowerVM 3.1.3 with VIOS 3.1.3.10
for
POWER9 and Power10
Security Target

Version: 1.0

Date: 2022-06-23

Prepared by:

International Business Machines Corporation

Rochester, MN 55901

LIST OF TABLES

1. Security Target Introduction

1.1 Security Target and TOE Identification

ST Title: IBM PowerVM 3.1.3 with VIOS 3.1.3.10 for POWER9 and Power10 Security Target

ST Version: 1.0

ST Date: 2022-06-23

TOE Identification: IBM PowerVM FW950.30 and FW1010.10 with VIOS 3.1.3.10 operating on IBM Power Systems POWER9 and Power10 hardware

TOE Developer: IBM Corporation

Evaluation Sponsor: IBM Corporation

TOE Type: The TOE is a hypervisor with a virtual input/output system.

1.2 TOE Overview

The TOE is the IBM POWER Virtual Machine (PowerVM) FW950.30 and FW1010.10 with Virtual Input/Output System (VIOS) 3.1.3.10 for POWER9 and Power10 provided by International Business Machines (IBM) Corporation. (This version of PowerVM is also known as IBM PowerVM 3.1.3.) The TOE facilitates the sharing of hardware resources by disparate applications (e.g., AIX, Linux). The TOE includes the guidance documentation.

The product is based on the concept of a 'hypervisor' that is designed to instantiate 'partitions', each with its own distinct resources, that each appear to their hosted applications as a completely functional underlying platform. These partitions, known as logical partitions (LPARs), are implemented to prevent interference among partitions and to prevent simultaneous sharing of storage and other device resources. VIOS allows partitions access-controlled sharing of individual storage and network devices. The TOE is agnostic to the application running in an LPAR.

1.2.1 TOE usage

While PowerVM performs virtualization of the CPUs and memory space, VIOS performs virtualization of storage and network devices. PowerVM supports assigning individual physical storage or network devices to a partition, but it does not support sharing of physical storage and network devices between partitions. Thus, in a PowerVM-only model, a hardware platform running 100 partitions that all desire access to the Internet would need 100 network devices. By running VIOS in a partition, PowerVM can, for example, assign a small number of physical network devices to the VIOS partition and VIOS can provide virtualized networking to the 100 partitions through controlled sharing of the physical network devices; thus, significantly reducing the number of physical network devices required. A similar VIOS analogy applies to storage devices.

While not included as part of the TOE, the TOE is configured using a connected Management Console (MC) that provides access to the functions necessary to enable administrative personnel to effectively manage the allocation of resources (i.e., processors, memory, and I/O devices) to the configured partitions.

1.2.2 TOE security features

The TOE supports the following major security features.

- User data protection

- Identification
- Security management
- Protection of the TOE security function (TSF)

1.2.3 Non-TOE hardware and software

The TOE was evaluated on the following non-TOE hardware.

- IBM Power System E980 (POWER9)
- IBM Power System E1080 (Power10)

To configure and manage the TOE, one of the following non-TOE management consoles (MCs) is required.

- Hardware Management Console (HMC)—Hardware Console used for configuration and management of PowerVM and VIOS.
- Novalink—Software interface used for virtualization management and configuration for PowerVM.
- Power Virtualization Control (PowerVC)—Advanced virtualization and cloud management offering used for the management and configuration of PowerVM.
- Virtual Hardware Management Console (vHMC)—Software console used for the configuration and management of PowerVM and VIOS.

The following non-TOE software abstraction is required for VIOS.

- Open Firmware/Run-Time Abstraction (OF/RTA)—Support for the AIX (including VIOS) and Linux operating systems

1.3 Terminology and Acronyms

Term	Description
AIX	The IBM AIX operating system
EAL	Evaluation Assurance Level
ECD	Extended Components Definition
FSP	Flexible Service Processor
HMC	Hardware Management Console
HTTPS	Hypertext Transfer Protocol Secure
IBM i	The IBM i operating system
Linux	An IBM Linux operating system
LPAR	Logical Partition
MC	Management Console
OF/RTA	Open Firmware/Run-Time Abstraction
Operator Panel	Front panel controls on the physical server
PHYP	PowerVM Hypervisor
PowerVC	POWER Virtual Control
PowerVM	POWER Virtual Machine
SCSI	Small Computer System Interface
SLIC	System Licensed Internal Code
TOE	Target of Evaluation
TSF	TOE Security Function
vENT	Virtual Ethernet
vHMC	Virtual HMC
VIOS	Virtual Input/Output System

Term	Description
vSCSI	Virtual SCSI

1.4 TOE Description

The Target of Evaluation (TOE) is the IBM PowerVM FW950.30 and FW1010.10 with VIOS 3.1.3.10 firmware running on POWER9 and Power10 hardware. While the TOE is designed to generally support the entire line of IBM Power Systems products, it has been evaluated and tested on the models shown in section 1.2.3.

Similarly, while the TOE is designed to support multiple storage device types, only virtual Ethernet (vENT) and virtual Small Computer System Interface (vSCSI) devices have been evaluated and tested.

1.4.1 TOE architecture

The TOE consists of the PowerVM Hypervisor (PHYP) and VIOS both of which are highlighted in yellow in Figure 1.

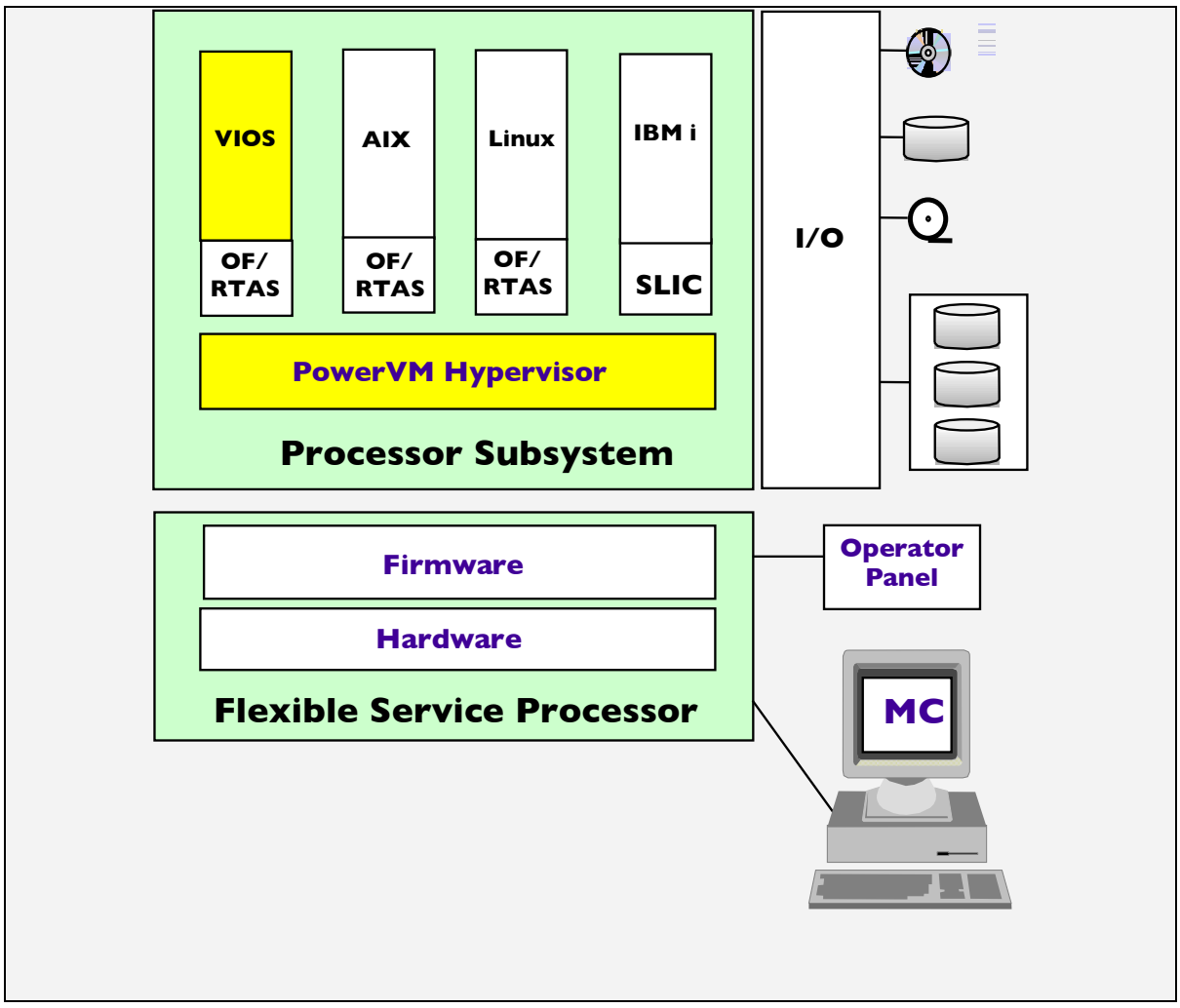

Figure 1: Product architecture

Note that Figure 1 identifies the TOE components in the yellow-filled boxes. The other components (e.g., MC, FSP, and operation systems) are outside the scope of the TOE.

1.4.1.1 Physical boundaries

The TOE images are downloadable from the developer's website over an HTTPS connection. The TOE software is comprised of the following images.

- PowerVM:
  - POWER9: 01VH950_092_045 (a.k.a. FW950.30)
  - Power10: 01MH1010_094_094 (a.k.a. FW1010.10)
- VIOS:
  - Virtual_IO_Server_Base_Install_3.1.3.10_Flash_092021_LCD8250308.iso
- The TOE guidance is contained in the document: IBM Power 3.1.3 User Guidance v1.1.pdf

As indicated earlier, the TOE consists of multiple architectural components. The components expose several interfaces both externally and internally.

The external interfaces include the interfaces to the subject operating in a partition. These include the Hypervisor interfaces as well as the hardware instructions available to applications. There is also an operator panel where basic, non-security related operator functions can be performed by a user with direct physical access to the TOE.

The internal interfaces, specifically those not also available externally, include the FSP interface to the Hypervisor.

I/O represents the physical I/O slots either integrated into the hardware drawers or I/O drawers external to the server. The I/O adapters allow for the connection of disk, network, SAN, tape, and other individual I/O devices.

Note that connections to a broad or public network are supported, but they would be treated as resources that can be granted to partitions for operating system use but would not be used by the TOE for its own purposes. Along these lines, while the TOE controls which devices a given partition can access, it does not control or otherwise constrain the nature of those devices. Any functions or connections of those devices are outside the scope of control of the TOE.

1.4.1.2 Logical boundaries

The physical boundaries can then be broken down into individual logical components. For example, a physical drawer may contain 8 different I/O devices and these individual devices are assigned by the Management Console (MC) to the configured virtual machines (partitions). When assigned to a partition, the logical I/O devices are available to be used by the partition (e.g., disk, network, tape).

This section summarizes the security functions provided by the TOE.

- User data protection
- Identification
- Security management
- Protection of the TSF

1.4.1.2.1 User data protection

Hypervisor

The Hypervisor manages the association of CPUs, memory, and I/O devices, in a relatively static environment, with partitions containing operating system instances. Memory and I/O devices can be assigned to single partitions and when assigned are accessible only by the partition (including OF/RTAS and the OS running in the partition). CPUs can also be assigned a single partition, and only that partition (and occasionally the TOE) can use that CPU. CPUs can also be configured to be shared among a collection of partition (shared processor partition or also called micro-partitions) and the Hypervisor will save/restore the hardware register state when switching between partitions.

Partitions have no control over the resources they are assigned. The Hypervisor receives the partition management information from the MC when it is being configured. Once configured, the configured values are continuously enforced.

VIOS

VIOS manages the association of partitions to virtualized storage and network devices and the association of virtualized storage and network devices to physical storage and network devices. Through the MC, an administrator assigns a set of physical storage and network devices to the VIOS partition. The administrator then creates virtual storage and network devices in VIOS, maps the physical devices to the virtualized devices, and maps the vSCSI and vENT to other partitions on the system. These other partitions access the virtualized storage and virtual networking controlled by VIOS. VIOS provides the separation protection between the virtualized storage and virtual network devices so that one partition cannot access another partitions information.

1.4.1.2.2 Identification

Partitions are implicitly identified by internal numerical identifiers associated with partitions (using internal data structures) as they are defined. Being implicitly identified by the TOE, partitions have no need, nor means, to identify themselves. Furthermore, the identification of a partition is guaranteed by the Hypervisor.

The Hypervisor identifies administrators for configuring and managing partitions and VIOS devices. Administrators use the MC to configure and manage the TOE.

1.4.1.2.3 Security management

All of the TOE configuration and management occurs via the interface to the MC. Administrators can configure and manage the security function policies (SFPs) used by the TOE.

1.4.1.2.4 Protection of the TSF

The components of the TOE protect themselves using the domains provided by the Power processors. The Hypervisor operates in the privileged domain and the partitions, like VIOS, operate in the unprivileged domain. This allows the Hypervisor to protect itself as well as the resources it makes selectively available to the applicable partitions.

Beyond protecting itself and its resources, the TOE is also designed such that when the hardware that supports a partition fails, the other partitions will continue uninterrupted.

2. Conformance Claims

Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017 is the basis for these conformance claims.

This Security Target claims the following conformances to the CC specifications.

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017
    - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017
    - Part 3 Conformant
    - Assurance Level: Evaluation Assurance Level (EAL) 2 augmented with ALC_FLR.2

There are no Protection Profile claims in this Security Target.

3. Security Problem Definition

The Security Problem Definition describes the security aspects of the intended environment in which the TOE is to be used and the way it is expected to be employed. The statement of the Security Problem Definition defines the following.

- Threats that the TOE counters
- Assumptions made about the operational environment and the intended method of use for the TOE

Furthermore, the TOE is intended to be used in environments where the relative assurance that its security functions are enforced is commensurate with EAL2 augmented with ALC_FLR.2 as defined in the CC.

3.1 Threats

T.ACCESS	An entity operating within a partition may be able to gain access to resources that belong to another partition as configured by an authorized user.
T.COMMUNICATE	An entity operating within a partition may be able to establish a communication channel with another partition.
T.INTERFERE	An entity operating within a partition may be able to disrupt the operation of another partition.

3.2 Assumptions

A.CONNECT	The TOE is assumed to be appropriately installed, including connections to device resources.
A.LOCATE	The TOE and its connections, including the HMC and its LAN, are assumed to be physically protected from unauthorized access or modification.
A.MANAGE	The TOE is assumed to be managed by users who are capable and trustworthy and will follow the applicable guidance correctly.

4. Security Objectives

This section defines the security objectives for the TOE and its supporting environment. The security objectives are intended to counter identified threats and address applicable assumptions.

4.1 Security Objectives for the TOE

O.AUTHORIZATION The TOE must ensure that resources can be assigned to partitions only by an authorized user and that those resources will not be accessible to other partitions.

O.COMMUNICATION The TOE must prevent a direct means of communication between partitions.

O.NONINTERFERE The TOE must ensure that each partition cannot access resources or communicate with other partitions.

4.2 Security Objectives for the Environment

OE.ADMIN A suitable management console must be configured for use by a capable and trustworthy user assigned to follow the applicable guidance in order to install and operate the TOE in a secure manner.

OE.INSTALL The TOE must be installed and configured in accordance with its guidance documents, including connecting appropriate device resources.

OE.PHYSICAL The TOE must be established in a physical environment suitable to protect itself and its external connections from inappropriate access and modification.

4.3 Security Objectives Rationale

This section shows that all secure usage assumptions and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption or threat.

	T.ACCESS	T.COMMUNICATE	T.INTERFERE	A.CONNECT	A.LOCATE	A.MANAGE
O.AUTHORIZATION	X					
O.COMMUNICATION		X				
O.NONINTERFERE			X			
OE.ADMIN						X
OE.INSTALL				X		
OE.PHYSICAL					X	

Table 1 Environment to Objective Correspondence

4.3.1 T.ACCESS

An entity operating within a partition may be able to gain access to resources that belong to another partition as configured by an authorized user.

This Threat is satisfied by ensuring that:

- O.AUTHORIZATION: By ensuring that resources can be accessed only by the partition assigned by an authorized user, the TOE mitigates the threat of partitions gaining access to resources of other partitions.

4.3.2 T.COMMUNICATE

An entity operating within a partition may be able to establish a communication channel with another partition.

This Threat is satisfied by ensuring that:

- O.COMMUNICATION: By ensuring that partitions cannot communicate with one another using any direct means provided by the TOE, the TOE limits the potential for inter-partition communication.

4.3.3 T.INTERFERE

An entity operating within a partition may be able to disrupt the operation of another partition.

This Threat is satisfied by ensuring that:

- O.NONINTERFERE: By ensuring that partitions are limited to access their assigned resources, the TOE mitigates the threat of interference among partitions.

4.3.4 A.CONNECT

The TOE is assumed to be appropriately installed, including connections to device.

This Assumption is satisfied by ensuring that:

- OE.INSTALL: This objective is intended to directly address the need to ensure that the TOE is appropriately installed and connected to other devices.

4.3.5 A.LOCATE

The TOE and its connections are assumed to be physically protected from unauthorized access or modification.

This Assumption is satisfied by ensuring that:

- OE.PHYSICAL: This objective is intended to directly address the need of physical protection for the TOE and its physical connections.

4.3.6 A.MANAGE

The TOE is assumed to be managed by users who are capable and trustworthy and will follow the applicable guidance correctly.

This Assumption is satisfied by ensuring that:

- OE.ADMIN: This objective is intended to directly address the need to assign capable and trustworthy administrators who will adhere to the applicable guidance.

5. Extended Components Definition

This Security Target does not contain extended components definitions (ECDs).

6. Security Requirements

The security requirements for the TOE have all been drawn from Parts 2 and 3 of the Common Criteria. The security functional requirements have been selected to correspond to the actual security functions implemented by the TOE while the assurance requirements have been selected to offer a reasonable degree of assurance that those security functions are properly realized by users of the TOE.

6.1 Conventions

The following conventions have been applied in this document.

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a slash character and the component acronym (e.g., /PHYP, /VIOS) placed at the end of the component. For example, FDP_ACC.2/PHYP and FDP_ACC.2/VIOS indicate that the ST includes two iterations of the FDP_ACC.1 requirement.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").

6.2 TOE Security Functional Requirements

The following table describes the SFRs satisfied by the TOE.

Requirement Class	Requirement Component
FDP: User data protection	FDP_ACC.2/PHYP: Complete access control
	FDP_ACC.2/VIOS: Complete access control
	FDP_ACF.1/PHYP: Security attribute based access control
	FDP_ACF.1/VIOS: Security attribute based access control
	FDP_IFC.2: Complete information flow control
	FDP_IFF.1: Simple security attributes
	FDP_RIP.1: Subset residual information protection
FIA: Identification and authentication	FIA_ATD.1/ADMIN: User attribute definition
	FIA_ATD.1/LPAR: User attribute definition
	FIA_UID.2: User identification before any action
	FIA_USB.1/ADMIN: User-subject binding
	FIA_USB.1/LPAR: User-subject binding
FMT: Security management	FMT_MSA.1/PHYP: Management of security attributes
	FMT_MSA.1/VIOS: Management of security attributes
	FMT_MSA.3: Static attribute initialization
	FMT_SMF.1: Specification of management functions
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_FLS.1: Failure with preservation of secure state

Table 2 TOE Security Functional Components

6.2.1 User data protection (FDP)

6.2.1.1 Complete access control (FDP_ACC.2/PHYP)

FDP_ACC.2.1 The TSF shall enforce the [**Resource Access Control Policy**] on [**subjects: partitions and objects: logical and physical CPUs, logical and physical memory, and logical and physical I/O devices**] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

6.2.1.2 Complete access control (FDP_ACC.2/VIOS)

FDP_ACC.2.1 The TSF shall enforce the [**VIOS Access Control Policy**] on [

a) **Network: VIOS virtual Ethernet device drivers acting on behalf of a group of LPAR partitions sharing a virtual network and VIOS Ethernet adapter device drivers (where either one can be the subject or object).**

b) **Volumes: VIOS vSCSI device drivers acting on behalf of LPAR partitions as subjects with Logical Volumes and Physical Volumes as objects.**

] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

6.2.1.3 Security attribute based access control (FDP_ACF.1/PHYP)

FDP_ACF.1.1 The TSF shall enforce the [**Resource Access Control Policy**] to objects based on the following: [**partition, logical and physical CPU, logical and physical memory, and logical and physical I/O device identities**].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**a given partition can access only logical and physical CPUs, logical and physical memory, and logical and physical I/O devices explicitly assigned to it**].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**no explicit authorization rules**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**no explicit denial rules**].

6.2.1.4 Security attribute based access control (FDP_ACF.1/VIOS)

FDP_ACF.1.1 The TSF shall enforce the [**VIOS Access Control Policy**] to objects based on the following: [

a) **Network: If a VIOS virtual Ethernet device driver acting on behalf of a group of LPAR partitions sharing a virtual network is mapped via an inter-LPAR communication channel to a VIOS Ethernet adapter device driver, then the device drivers can exchange untagged packets; otherwise, access is denied.**

b) **Volumes: If the logical volume or physical volume is mapped to a VIOS vSCSI device driver acting on behalf of an LPAR partition, then the device driver can access the logical volume or physical volume, respectively; otherwise, access is denied.**

].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**a given partition can access only logical and physical CPUs, logical and physical memory, and logical and physical I/O devices explicitly assigned to it**].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**no explicit authorization rules**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**no explicit denial rules**].

6.2.1.5 Complete information flow control (FDP_IFC.2)

FDP_IFC.2.1 The TSF shall enforce the [**Partition Separation Policy**] on [**partitions and attached resource contents**] and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

6.2.1.6 Simple security attributes (FDP_IFF.1)

FDP_IFF.1.1 The TSF shall enforce the [**Partition Separation Policy**] based on the following types of subject and information security attributes: [**partition identities and no attached resource content 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: [**I/O devices have been associated with partitions such that those devices enable some means of communication via their contents outside the scope of the TOE**].

FDP_IFF.1.3 The TSF shall enforce the [

a) Partitions cannot communicate with one another using physical CPU or memory resource contents.

b) **When a CPU is designated as shared, it can be assigned to partitions in successive time slots.**

].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [**no explicit authorization rules**].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [**no explicit denial rules**].

6.2.1.7 Subset residual information protection (FDP_RIP.1)

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [***allocation of the resource to***] the following objects: [**physical CPUs**].

6.2.2 Identification and authentication (FIA)

6.2.2.1 User attribute definition for administrators (FIA_ATD.1/ADMIN)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**user name, user ID, user role**].

6.2.2.2 User attribute definition for LPARs (FIA_ATD.1/LPAR)

FIA_ATD.1.1 Refinement: The TSF shall maintain the following list of security attributes belonging to individual **partitions** ~~users~~: [**unique partition id**].

6.2.2.3 User identification before any action for administrators (FIA_UID.2)

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.

6.2.2.4 User-subject binding for administrators (FIA_USB.1/ADMIN)

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [**user ID, user role**].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [**the TOE maps user names to a user role and a unique user ID**].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [**user IDs do not change once assigned**].

6.2.2.5 User-subject binding for LPARs (FIA_USB.1/LPAR)

FIA_USB.1.1 Refinement: The TSF shall associate the following user security attributes with subjects acting on the behalf of that **partition** ~~user~~: [**unique partition id**].

FIA_USB.1.2 Refinement: The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of **partitions** ~~users~~: [**partitions are identified internally when defined**].

FIA_USB.1.3 Refinement: The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of **partitions** ~~users~~: [**partition security attributes do not change once assigned**].

6.2.3 Security management (FMT)

6.2.3.1 Management of security attributes (FMT_MSA.1/PHYP)

FMT_MSA.1.1 The TSF shall enforce the [**Resource Access Control Policy and Partition Separation Policy**] to restrict the ability to [***modify***] the security attributes [**partition and resource identities (and association of resources to partitions)**] to [**administrator**].

6.2.3.2 Management of security attributes (FMT_MSA.1/VIOS)

FMT_MSA.1.1 The TSF shall enforce the [**VIOS Access Control Policy**] to restrict the ability to [***modify***] the security attributes [

a) For Network: mapping of virtual Ethernet device drivers acting on behalf of a group of LPAR partitions sharing a virtual network to Ethernet adapter device drivers

b) For Volumes: mapping vSCSI device drivers acting on behalf of LPAR partitions to logical volumes and physical volumes

] to [**administrator**].

6.2.3.3 Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the [**Resource Access Control Policy, Partition Separation Policy, and VIOS Access Control Policy**] to provide [***restrictive***[1]] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**no user**] to specify alternative initial values to override the default values when an object or information is created.

[1] The policy is restrictive in that resources can be accessed only after being explicitly assigned to a partition and that a given resource can be assigned only to a single partition.

6.2.3.4 Specification of management functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

a) Management of the Resource Access Control Policy and Partition Separation Policy

b) Management of the VIOS Access Control Policy

].

6.2.3.5 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles [**administrator**].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.2.4 Protection of the TSF (FPT)

6.2.4.1 Failure with preservation of secure state (FPT_FLS.1)

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [**memory and processor failures**].

6.3 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that **Table 3** indicates the requirements that effectively satisfy the individual objectives.

6.3.1 Security functional requirements rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

	O.AUTHORIZATION	O.COMMUNICATION	O.NONINTERFERE
FDP_ACC.2 /PHYP	X		X
FDP_ACC.2/VIOS	X		X
FDP_ACF.1/PHYP	X		X
FDP_ACF.1/VIOS	X		X
FDP_IFC.2		X	X
FDP_IFF.1		X	X
FDP_RIP.1	X		
FIA_ATD.1/ADMIN	X		
FIA_ATD.1/LPAR	X		
FIA_UID.2	X		
FIA_USB.1/ADMIN	X		
FIA_USB.1/LPAR	X		
FMT_MSA.1/PHYP	X		X
FMT_MSA.1/VIOS	X		X
FMT_MSA.3	X		X

FMT_SMF.1	X		
FMT_SMR.1	X		
FPT_FLS.1	X		

Table 3 Objective to Requirement Correspondence

6.3.1.1 O.AUTHORIZATION

The TOE must ensure that resources can be assigned to partitions only by an authorized user and that those resources will not be accessible to other partitions.

This TOE Security Objective is satisfied by ensuring that:

- FDP_ACC.2/PHYP & FDP_ACC.2/VIOS: In order to ensure that resources are restricted to partitions appropriately, an access control policy is defined which covers all resources as well as all operations.
- FDP_ACF.1/PHYP & FDP_ACF.1/VIOS: In order to ensure that resources are restricted to partitions appropriately, the access control rules ensure that partitions gain access to resources only when they are appropriately configured for that purpose.
- FDP_RIP.1: In order to ensure that resources (including information they contain) are restricted to partitions appropriately, the TOE must ensure that processor resources are cleared when allocated to partitions.
- FIA_ATD.1/ADMIN: In order to fully identify a user, the TOE maintains attributes associated with each user.
- FIA_ATD.1/LPAR: In order to limit resource access to specific partitions, the TOE must define identities associated with partitions.
- FIA_UID.2: In order to ensure that users are known to the TOE, the TOE identifies each user before allowing any other TSF-mediated action.
- FIA_USB.1/ADMIN: In order to map users to subjects for managing the SFPs, the TOE employs a mapping mechanism mapping each user name to a subject.
- FIA_USB.1/LPAR: In order to limit resource access to specific partitions, the TOE must ensure that partitions are continuously identified and that identification cannot change.
- FMT_MSA.1/PHYP & FMT_MSA.1/VIOS: In order to ensure that resources are managed properly, the TOE must ensure that assignment of resources to partitions cannot be accomplished by unauthorized users.
- FMT_MSA.3: In order to ensure that resources are managed properly, the TOE must ensure that they are not accessible by partitions until they are explicitly assigned.
- FMT_SMF.1: In order to manage the SFPs, the TOE provides SFP management functions.
- FMT_SMR.1: In order to support roles for management functions, the TOE provides user roles for managing the SFPs.
- FPT_FLS.1: In order to protect against inappropriate resource access, the TOE must protect itself against memory and processor failures.

6.3.1.2 O.COMMUNICATION

The TOE must prevent a direct means of communication between partitions.

This TOE Security Objective is satisfied by ensuring that:

- FDP_IFC.2: In order to limit potential means of communication between partitions, an information flow policy is defined which covers any means of communication between partitions.
- FDP_IFF.1: In order to limit potential means of communication between partitions, the information flow policy rules ensure that inter-process communication is not allowed using any mean provided by the TOE.

6.3.1.3 O.NONINTERFERE

The TOE must ensure that each partition cannot access resources or communicate with other partitions.

This TOE Security Objective is satisfied by ensuring that:

- FDP_ACC.2/PHYP & FDP_ACC.2/VIOS: In order to ensure that resources cannot be used for interference among partitions, an access control policy is defined which covers all resources as well as all operations.
- FDP_ACF.1/PHYP & FDP_ACF.1/VIOS: In order to ensure that resources cannot be used for interference among partitions, the access control rules ensure that partitions gain access to resources only when they are appropriately configured for that purpose.
- FDP_IFC.2: In order to ensure that communication mechanisms cannot be used for interference among partitions, an information flow policy is defined which covers any means of communication between partitions.
- FDP_IFF.1: In order to ensure that communication mechanisms cannot be used for interference among partitions, the information flow policy rules ensure that inter-process communication is allowed only using devices which may be subject to object reuse or other means of communication not controllable by the TOE.
- FMT_MSA.1/PHYP & FMT_MSA.1/VIOS: In order to protect against configuration-related interference attempts, the TOE must ensure that resource assignments cannot be established by unauthorized users.
- FMT_MSA.3: In order to protect against configuration-related interference attempts, the TOE must ensure that resource access is not allowed until it is explicitly configured.

6.4 Requirement Dependency Rationale

The following table identifies the dependencies of the requirements in this ST, including the requirements explicitly defined in this ST. As indicated in the table, all of the dependencies are satisfied.

ST Requirement	CC Dependencies	ST Dependencies
FDP_ACC.2/PHYP	FDP_ACF.1	FDP_ACF.1/PHYP
FDP_ACC.2/VIOS	FDP_ACF.1	FDP_ACF.1/VIOS
FDP_ACF.1/PHYP	FDP_ACC.1 and FMT_MSA.3	FDP_ACC.2/PHYP and FMT_MSA.3
FDP_ACF.1/VIOS	FDP_ACC.1 and FMT_MSA.3	FDP_ACC.2/VIOS and FMT_MSA.3
FDP_IFC.2	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 and FMT_MSA.3	FDP_IFC.2 and FMT_MSA.3
FDP_RIP.1	none	none
FIA_ATD.1/ADMIN	none	none
FIA_ATD.1/LPAR	none	none
FIA_UID.2	none	none
FIA_USB.1/ADMIN	FIA_ATD.1	FIA_ATD.1/ADMIN
FIA_USB.1/LPAR	FIA_ATD.1	FIA_ATD.1/LPAR
FMT_MSA.1/PHYP	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1 and FMT_SMF.1 and FDP_ACC.2/PHYP and FDP_IFC.2
FMT_MSA.1/VIOS	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1 and FMT_SMF.1 and FDP_ACC.2/VIOS
FMT_MSA.3	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1/PHYP, FMT_MSA.1/VIOS, and FMT_SMR.1
FMT_SMF.1	none	none
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_FLS.1	none	none

Table 4: Requirement Dependencies

6.5 Security Assurance Requirements

The security assurance requirements (SARs) for the TOE are the EAL2 SARs augmented with ALC_FLR.2 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

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

Table 5 EAL2 augmented with ALC_FLR.2 Assurance Components

6.6 Security Assurance Requirements Rationale

The TOE is intended for an environment requiring a basic level of assurance in the security functionality of conventional commodity TOEs, as presented in the statement of security environment (Section 3). The target assurance level of EAL2 augmented with ALC_FLR.2 is appropriate for such an environment.

7. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

7.1 TOE Security Functions

7.1.1 User data protection

The Hypervisor is designed to instantiate partitions for the purpose of supporting multiple simultaneous operating systems. As such, it implements a policy whereby partitions can access only those resources explicitly assigned to it.

In terms of access control, CPU, memory, and I/O devices can be assigned to a given partition and a partition can access those resources only when they are assigned to it. This is accomplished using hardware features supporting the mapping of these resources to established partitions. Hence, even when using hardware instructions directly, a partition cannot directly perceive that those other resources may exist. During operation of the TOE, CPU, memory, and I/O device resources can be assigned to only a single partition at any given point in time and cannot be simultaneously shared among partitions.

Normally, CPU, memory, and I/O resources are permanently assigned to a partition at configuration time. A CPU can be configured to be shared among partitions and subsequently partitions can utilize that CPU, one at a time, based on available time slots.

In terms of communication, a user can optionally choose to configure a virtual communication path between partitions via the Hypervisor. Also, partitions can be assigned to devices (NICs for example) and those devices might be capable of enabling some means of communication outside the scope of control of the TOE.

VIOS allows for sharing access to network devices (Ethernet) and storage volumes. NICs and storage devices are assigned to the VIOS partition by the Hypervisor. VIOS then presents vENT devices and vSCSI logical volumes to other partitions on the system. VIOS controls the mapping of partitions to logical volumes and the mapping of logical volumes to the physical drives. VIOS enforces access controls to provide separation between partitions of these shared virtual devices.

The User data protection function is designed to satisfy the following security functional requirements.

- FDP_ACC.2/PHYP & FDP_ACC.2/VIOS: The TOE controls all operations that a partition may perform on CPU, memory, and I/O device resources by allowing partitions to access (in any manner) only the resources explicitly assigned to it.
- FDP_ACF.1/PHYP & FDP_ACF.1/VIOS: As indicated above, partitions can access only those resources that have been assigned to it.
- FDP_IFC.2: The TOE offers no means of direct communication among partitions, so all means of inter-partition communication within the scope of the TOE are controlled.
- FDP_IFF.1: CPU, memory, and I/O device resources can be assigned to only one partition at a time. CPUs, memory, and I/O devices cannot be dynamically re-allocated, though they could be reallocated when the TOE is reconfigured while not in an operational state.
- FDP_RIP.1: When a partition initially starts and when it is assigned a new CPU, the corresponding CPU context is initialized to a known state appropriate to the partition (either a new starting state when initially assigned or restoration of the previous partition state when reassigned). *Note that I/O devices cannot be addressed with this claim since essentially any I/O device could be used and the TOE does not have the ability to clear the contents of all applicable I/O devices. Hence, it is left to the partitions themselves to address any associated issues related to reuse of information in devices when the TOE is reconfigured such that a device may be reassigned to a different partition.*

7.1.2 Identification

7.1.2.1 Administrators

The TOE allows TOE administrators to manage the access control and information control SFPs defined in this document. Administrators manage the policies using the MC (which is part of the operational environment) as the interface. The TOE identifies individual administrators by user name and translates that into a user ID each time an administrator identifies them self. In addition, individual administrators have a user role of "administrator."

This identification function is designed to satisfy the following security functional requirements.

- FIA_ATD.1/ADMIN: Each administrator is identified by a user name and user ID. Each administrator has a user role of "administrator" assigned to them.
- FIA_UID.2: Each administrator is uniquely identified prior to any other TSF-mediated action.
- FIA_USB.1/ADMIN: Unique, identifying partition numbers are assigned when partitions are created and cannot change except by deleting and recreating a partition.
- FMT_SMR.1: The TOE supports the role of "administrator." Each user is assigned a user role.

7.1.2.2 Partitions

When partitions are defined, they are assigned unique numbers in TOE-internal data structures which are subsequently used to identify the partition and to associate resources with the partition. Once a partition is created, its number will not change except when it is deleted and recreated. Given that each partition is uniquely identified by the TOE using TOE-internal data structures, the TOE effectively ensures that each partition is authentic on a continuous basis.

This identification function is designed to satisfy the following security functional requirements.

- FIA_ATD.1/LPAR: Each partition is identified by a unique partition number by the TOE and there is only one MC identified by virtue of its dedicated physical connection to the TOE.
- FIA_USB.1/LPAR: Unique identifying partition numbers are assigned when partitions are created and cannot change except by deleting and recreating a partition.

7.1.3 Security management

All functions to configure the TOE are available only through the dedicated physical MC interface. The MC allows an administrator of the TOE to create partitions and to assign CPU, memory, and I/O device resources to those partitions. Furthermore, each given resource can be assigned only to a single partition. The resulting configuration data is pushed to the TOE prior to it being placed in an operational, evaluated configuration.

The Security management function is designed to satisfy the following security functional requirements.

- FMT_MSA.1/PHYP & FMT_MSA.1/VIOS: The only interface available to manipulate the assignment of resources to partitions are offered through the dedicated MC connection.
- FMT_MSA.3: Partitions cannot access resources until they are defined and explicitly assigned resources via the MC and VIOS. The only interfaces available to create partitions and manipulate the assignment of resources to partitions are offered through the dedicated MC connection.
- FMT_SMF.1: The TOE allows for the management of the defined SFPs.
- FMT_SMR.1: The TOE supports the role of administrator, where each user has a user role attribute associated with each account.

7.1.4 Protection of the TSF

The FSP firmware depends on the FSP hardware (i.e., POWER9 and Power10) to provide a separate domain for its execution.

The hardware provides a privileged mode of execution specifically for the Hypervisor firmware. Only the Hypervisor firmware executes in that mode and it is only from this privileged execution mode that full, unconstrained access to the available resources (CPUs, memory, and I/O devices) is available. Even though the Hypervisor shares the available CPUs with its instantiated partitions, the contexts of the CPUs are saved and restored appropriately during every context switch to ensure uninterrupted operation of the Hypervisor and the partitions.

The Hypervisor firmware instantiates partitions that execute in other execution modes offered by the POWER9 and Power10 processors. Additionally, those partitions can access only those resources that have been specifically allocated for use by the associated partitions. While a partition can freely access the resources it has been assigned, there are no interfaces that might allow access to (or even the perception of) other unassigned or otherwise assigned resources.

The Hypervisor ensures that its security mechanisms cannot be bypassed by encapsulating partitions with their assigned resources and offering only limited interfaces that are designed to ensure that partitions cannot interfere with other partitions or the Hypervisor's own operation.

When the Hypervisor detects a memory failure in its own memory space, it terminates the entire system. When the Hypervisor detects a memory failure in partition memory, it passes the error to that partition for the partition to handle. When VIOS receives a partition memory failure from the Hypervisor, it terminates the partition and reboots. In both cases, the failed memory is removed from service before the software is reloaded.

When the Hypervisor detects a processor failure during its own execution, it terminates the entire system. When the system restarts, the processor is removed from service. When the Hypervisor detects a processor failure in a partition, it terminates the partition, removes the processor from service, creates a new partition, and reboots the partition's software (e.g., VIOS). In both cases, the failed processor is removed from service before the software is reloaded.

The Protection of the TSF function is designed to satisfy the following security functional requirement.

- FPT_FLS.1: When memory or processor failures are detected by the TOE, it shuts down and, when restarted, reverts to its previously secure configuration.

7.2 TOE Summary Specification Rationale

Each subsection in Section 7, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all security functions and assurance requirements. Furthermore, all the security functions are necessary for the TSF to provide the required security functionality.

This Section provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 6** demonstrates the relationship between security requirements and security functions.

	User data protection	**Identification**	**Security management**	**Protection of the TSF**
FDP_ACC.2/PHYP	X			
FDP_ACC.2/VIOS	X			
FDP_ACF.1/PHYP	X			
FDP_ACF.1/VIOS	X			

FDP_IFC.2	X			
FDP_IFF.1	X			
FDP_RIP.1	X			
FIA_ATD.1/ADMIN		X		
FIA_ATD.1/LPAR		X		
FIA_UID.2		X		
FIA_USB.1/ADMIN		X		
FIA_USB.1/LPAR		X		
FMT_MSA.1/PHYP			X	
FMT_MSA.1/VIOS			X	
FMT_MSA.3			X	
FMT_SMF.1			X	
FMT_SMR.1			X	
FPT_FLS.1				X

Table 6 Security Functions vs. Requirements Mapping