Security Target for PR/SM for IBM z14 and IBM LinuxONE Systems

Version:	**16.12**
Revision:	**1**
Status:	**RELEASE**
Last Update:	**2018-06-20**

Trademarks

The following terms are trademarks or registered trademarks of the International Business Machines Corporation in the United States, other countries, or both:

- ESCON®
- FICON®
- HiperSockets
- IBM®
- IBM® zEnterprise System
- OS/390®
- Processor Resource/Systems Manager
- PR/SM
- ResourceLink®
- RETAIN®
- S/360®
- S/370®
- S/390®
- System z®
- VM/ESA®
- VSE/ESA
- zEnterprise®
- z/Architecture®
- z/OS®
- z/VM®
- zSeries®
- z System
- Linux on z Systems
- IBM LinuxONE(tm)
- LinuxONE
- IBM z14
- z/TPF

Those trademarks followed by ® are registered trademarks of IBM in the United States; all others are trademarks or common law marks of IBM in the United States.

More details on IBM UNIX hardware, software and solutions may be found at ibm.com/servers/unix/.

InfiniBand is a registered trademark of the InfiniBand Trade Association.

Linux is a registered trademark of Linus Torvalds.

UNIX is a registered trademark of The Open Group in the United States and other countries.

IBM, the IBM logo, the e-business logo, LinuxONE, AIX, DB2, DB2 Universal Database, pSeries, RS/6000, SP and WebSphere are registered trademarks or trademarks of the International Business Machines Corporation in the United States and/or other countries.

Other company, product and service names may be trademarks or service marks of others. IBM may not offer the products, programs, services or features discussed herein in other countries, and the information may be subject to change without notice.

Legal Notice

General availability may vary by geography.

IBM hardware products are manufactured from new parts, or new and used parts. Regardless, our warranty terms apply.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. Any reliance on these statements is at the relying party's sole risk and will not create any liability or obligation for IBM.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Revision History

Revision	Date	Author(s)	Changes to Previous Revision
16.12	2018-06-20	Clemens Wittinger, atsec	Final Release.

Table of Contents

List of Tables

1 Introduction

1.1 Security Target Identification

Title:	Security Target for PR/SM for IBM z14 and IBM LinuxONE Systems
Version:	16.12
Revision:	1
Status:	RELEASE
Date:	2018-06-20
Sponsor:	IBM Corporation
Developer:	IBM Corporation
Certification Body:	BSI
Certification ID:	BSI-DSZ-CC-1048
Keywords:	access control, identification, authentication, audit, object reuse, z, LPAR, logical partitioning, isolation, PR/SM, LIC, cross-partition, HMC, SE

1.2 TOE Identification

The TOE is PR/SM, Driver Level D32L with Bundle Level S29 for IBM z14 and IBM LinuxONE Systems.

1.3 TOE Type

The TOE type is Hypervisor.

1.4 TOE Overview

The IBM z14 and IBM LinuxONE systems are world class enterprise servers designed to meet your business needs. The z14 and IBM LinuxONE systems are built on the inherent strengths of the IBM z platform and is designed to deliver new technologies and virtualization that provide improvements in price/performance for key new workloads. The z14 and IBM LinuxONE systems further extend z Systems leadership in key capabilities with the delivery of expanded scalability for growth and large scale consolidation, improved security and availability to reduce risk, and just-in-time capacity deployment, helping to respond to changing business requirements.

PR/SM is a hardware facility that enables the resources of a single physical machine to be divided between distinct, predefined logical machines called "logical partitions". Each logical partition is a domain of execution, and is considered to be a subject capable of running a conventional system control program (SCP) such as z/OS™, z/VM™, z/VSE, z/TPF™ or Linux on z System. These operating systems run unmodified in a PR/SM partition.

For detailed information on the PR/SM security features, please refer to section 1.5.2.

For the remainder of this document, IBM z14 and IBM LinuxONE Systems will be referred to as **z System**.

1.5 TOE Description

1.5.1 TOE Introduction and Logical Boundary

The TOE is the PR/SM Licensed Internal Code (LIC) kernel running on the z System. The kernel provides the capability to initialize the z System in LPAR mode, which is the only mode of operation covered in this evaluation. The TOE is implemented in LIC. The use of LIC prevents untrusted code from masquerading as part of the TOE and abusing TOE privileges. The TOE is composed of:

a) the LPAR LIC running on the Central Processing Complex (CPC) as hypervisor responsible for maintaining the isolation of logical partitions maintained and controlled by the TOE.

b) HMC LIC running on the Hardware Management Console (HMC) providing remote system administration functions to maintain the current configuration. The HMC is connected over internal network with one or more Support Elements.

c) SE LIC running on the Support Element (SE) physically located in the CPC cabinet and connected to the CPC. The SE also provides system administration functions to maintain the current configuration and can be used independently from an HMC connected to it.

PR/SM LIC provides the security administrator the ability to define a completely secure system configuration. When the system is defined in such a manner, total separation of the logical partitions is achieved thereby preventing a partition from gaining any knowledge of another partition's operation.

Only functions related to logical partition isolation, physical resource allocation, access control and audit are the subject of this Security Target. Additional functions of PR/SM related to normal operations and maintenance of the system are not considered as security enforcing functions because the TOE will be configured to provide a configuration consistent with secure isolation such that these operations cannot be in conflict with the security policy of PR/SM.

The other functions are therefore not evaluated for correctness and no vulnerability analysis for those functions is performed.

1.5.2 Summary of Security Features

1.5.2.1 Identification and Authentication

The TOE supports identification and authentication of users by means of:

- Unique identification via zone numbers assigned to each logical partition
- Unique user IDs assigned to each user of the HMC/SE

For the logical partitions, there is no specific password. The logical partition is authenticated by its existence in the I/O Configuration Dataset (IOCDS) definition when activation occurs. The zone number is used to mediate access between the logical partition and the physical resources of the processor assigned to that logical partition.

For the HMC/SE user, the required passwords are assigned by the security administrator. The use of the user ID and password allows the user of the HMC/SE to invoke the various functions that are defined as being allowed for that user ID.

1.5.2.2 Access Control and Information Flow Control

The TOE supports access control between users and resources by means of:

- The TOE implements LPAR Security Controls which define a partition's access to IOCDSs, performance data, cryptographic hardware, the channel reconfiguration process, and the authority to reset or shutdown other partitions.

- The TOE implements LPAR Security Controls which specify the partition's permissions to send BCPii commands to the SE part of the TOE and to specify which partition's configuration on the SE part of the TOE can receive and process BCPii commands. It should be noted that in the evaluated configuration no partition has either the send or receive BCPii permission.
- The TOE allows access to specific control units and devices on non-dedicated channels to be restricted.
- The TOE insures that dedicated channels, storage and physical CPs are **never** shared.
- The TOE will prevent the transfer of any message between a logical partition and **any** resource not explicitly allocated to it.
- The TOE implements management access controls to define configurable role based authorized administrator access to the TOE's management functions.

1.5.2.3 Auditing

The TOE supports auditing of relevant events by means of a security log with the following characteristics:

- All security relevant events are recorded in the security log. This auditing mechanism cannot be bypassed.
- The security log is protected from unauthorized deletions or modifications.
- Applications in logical partitions cannot read the security log.
- The security log can be offloaded for archival purposes.

1.5.2.4 Authorized Administration and Operation

PR/SM is a hardware facility that enables the resources of a single physical machine to be divided between distinct, predefined logical machines, called “logical partitions”. The HMC/SE workplace is the window from where users start tasks for monitoring and operating the CPC (central processor complex). A user profile determines which tasks and controls users can use on the workplace. Not all tasks are available for each user.

The following predefined default user IDs are established as part of base HMCs/SEs.

Operator - A person with operator authority typically performs basic system startup and shutdown operations using predefine procedures.

Advanced Operator - A person with advanced operator authority possesses operator authority plus the ability to perform some additional recovery and maintenance tasks.

Programmer - A person with programmer authority has the ability to customize the system in order to determine its operation.

Access Administrator - A person with access administrator authority has the ability to create, modify, or delete user profiles on the HMC or for service mode on the support element. A user profile consists of user identification, a password, managed resource roles and task roles

Service Representative - A person with service representative authority has access to tasks related to the repair and maintenance of the system.

In addition to the predefined user roles supplied with the console the ability to define customized user roles is also provided. A user role is a collection of authorizations. A user role can be created to define the set of tasks allowed for a given class of user (task roles) or it can be created to define the set of managed objects that are manageable for a user (managed resource roles). A customized user role is based on one of the predefined user roles from which objects or tasks are removed.

Once user roles are defined or customized they can be used to create new users with their own permissions. A user can be created with one or more user roles.

The following general definitions can be established:

Administrator
The Administrator is defined to be any user(s) with access to the HMC/SE workplace.

Security Administrator
Any administrator authorized to perform all of the following tasks:

- Archive Security Logs
- Change LPAR Controls
- Change LPAR Group Controls
- Change LPAR I/O Priority Queuing
- Change LPAR Security
- Customize/Delete Activation Profiles
- Input/Output (I/O) Configuration
- Logical Processor Add
- Manage Users Wizard
- Reassign Channel Path
- System Details
- User Management
- View Security Logs

A detailed list of the console actions authorized for each predefined role is contained in a respective section *Tasks and default user IDs* of [HMCOPG], which is integral part of the HMC online help.

1.5.2.5 Object Reuse

The TOE supports object reuse by means of:

- Clearing of all storage prior to allocation or re-allocation.
- Resetting all information in physical processors before dispatching the processor to a new logical partition.
- Resetting non-shared channel paths and attached I/O devices prior to allocation to a logical partition.

1.5.2.6 Reliability of Service

The TOE supports the control of the processor running time and wait completion processor parameters. These parameters provide the ability to share physical processor resources on either an event-driven basis or a time-driven basis. Disabling event driven dispatching causes shared physical processor resources to be distributed on the basis of time intervals according to the weights specified to effectively prevent unauthorized denial of service

1.5.2.7 TSF Protection

The TOE supports TSF protection by means of:

- Self test whenever the TOE is loaded and started and periodically during the TOE's operation.
- The PR/SM kernel is loaded into a protected area of central storage where it is inaccessible by any users, operating systems or applications.
- An alternate (backup) SE operates to provide real time mirroring of relevant system data: IOCDSs, audit log, image profiles.

1.5.3 Configuration

The target of the evaluation is the PR/SM LIC kernel running on the IBM z System hardware platforms which includes the following models with any number of supported CPs, any supported memory configuration and any supported capacity:

IBM z14, models

- M01
- M02
- M03
- M04
- M05

IBM LinuxONE, models

- LM1
- LM2
- LM3
- LM4
- LM5

System Name	IBM z14	IBM LinuxONE Emperor II
Machine Type (MT)	3906	
Machine Models (MM)	M01 M02 M03 M04 M05	LM1 LM2 LM3 LM4 LM5

Table 1: Supported Models

Note: *The IBM z System hardware platforms are not part of the TOE.*

Documentation related to the TOE and its evaluated configuration is provided in [TFM].

The TOE subject of this Security Target is LIC Driver Level D32L with Bundle Level S29, which includes the HMC/SE firmware version 2.14.0. For the remainder of this document, this LIC will be referred to as LPAR.

Please refer to the IBM publication(s) [SO], chapter 1 for more information on the capabilities of the IBM z System hardware platform.

The address space of the TSF is isolated from the address space of the partitions by hardware protection mechanisms (the "start interpretive execution" (SIE) instruction provided by the underlying processor as described below), and by the provision of separate hardware for the SE and I/O (SAP) processors. The TSF LIC and data is therefore protected from modification or tampering.

The security administrator uses an I/O configuration utility (IOCP) to define an IOCDS of the I/O resources and their allocation to specific logical partitions. The IOCDS should be verified by the security administrator prior to activating the partitions. PR/SM allows I/O resources to be dedicated to a single partition, relocatable among a defined set of partitions, or shared by a defined set of partitions. When a administrator wishes to activate a partition, the activation request is initiated

from the HMC. LPAR will receive an external interrupt and issue an instruction to obtain the description of the partition the administrator wishes to activate. LPAR will attempt to construct the partition and will inform the HMC of the success or failure of the command.

Several IOCDSs, defining different configurations, may be stored but only one is in effect at any time. The configuration becomes effective as part of the activation sequence.

Standard hardware resources such as a central processor, including computation and control registers, timers, clocks and storage; and I/O resources are objects allocated to logical partitions. These objects are subject to a non-discretionary access control policy under which each logical partition is only permitted access to resources allocated to it. Logical partitions are logical objects that are built from existing physical objects. These logical objects fall into one of three classes:

a) Logical processor facilities, which are supported by similar physical objects. Each such logical object is represented by an internal control block that contains current state information each time context is switched to a different logical partition.

b) Logical storage, central and storage class memory, is represented by the same amount of contiguous physical storage. PR/SM does not perform paging or move logical partitions once they have been placed in real storage. Physical storage can be de-allocated from one logical partition and reallocated to another. This feature can be disabled, and is subject to full object reuse control.

c) Logical I/O resources (channels) are implemented by physical resources of the same type. Such resources can be configured so that they are not shared by partitions. A channel can be de-allocated from one logical partition and reallocated to another, under the control of the security administrator.

The z/Architecture® and ESA/390® architecture support two instruction states: problem and supervisor. Problem state instructions can be executed in either problem or supervisor state. Semi-privileged instructions can be executed in supervisor state, or in problem state subject to one or more additional authorizations. Privileged instructions can be executed only in supervisor state. PR/SM exports a virtual machine including all architected instructions, and initiates the execution in supervisor state, so that all three classes of instruction can be executed within the logical partition. Thus each logical partition has both execution states available. PR/SM does not interfere with the logical partition's use of those states. A system control program (SCP) running in a logical partition can support z and ESA/390 architectural mode. The SCP can define whether it is running in z/Architecture mode or ESA/390 mode by a use of a SIGP instruction. Typically if the SCP understands z/Architecture mode it gets into z/Architecture mode immediately and remains in that mode. But z/OS will switch back to ESA/390 if it needs to load the standalone dump program.

PR/SM supports and uses the "start interpretive execution" (SIE) instruction to create an interpretative execution environment in which the logical partitions execute. PR/SM begins execution in non-SIE mode. When a logical partition is to be activated PR/SM establishes the parameters for each logical processor allocated to the partition in a control block called a "state description". PR/SM executes a SIE instruction, which dispatches the logical processor in SIE mode. The PR/SM hardware executes instructions in the logical processor in SIE mode until an exception condition occurs, which causes control to return to PR/SM in non- SIE mode. The exception conditions are events that cannot be handled in interpretative mode. PR/SM receives control in non-SIE mode. PR/SM maintains a state description for each logical processor of each logical partition so that each time a logical processor is dispatched, it is in the same context as when it last had control. Since this state description is updated by the hardware, it is impossible for one logical partition to acquire control with the wrong context (i.e. the context of another logical partition). The non-SIE/SIE distinction is a powerful privilege differentiation between PR/SM and the logical partitions.

The z System provides support for several features that are very helpful in many customer environments. However, these features are not recommended in a secure environment. As a result, the TOE provides security related controls to disable such features assuring separation of the logical partition(s). The security related controls are outlined below:

Logical Partition Isolation
This control reserves reconfigurable unshared channel paths for the exclusive use of a logical partition. Channel paths assigned to an isolated logical partition are not available to other logical partitions and remain reserved for that LP when they are configured offline.

I/O Configuration Control Authority
This control can limit the ability of the logical partition to read or write any IOCDS in the configuration locally or remotely. Logical partitions with control authority for the I/O configuration data can read and write any non-write protected IOCDS in the configuration, and can change the I/O configuration dynamically.

BCPii Permissions
This control can limit the ability of the logical partition to send BCPii commands to other partition's configuration on the SE part of the TOE and whether a logical partition's configuration can receive and process BCPii commands from other partitions. This control can also limit from which specific logical partitions a partition can receive BCPii commands on the SE part of the TOE. It should be noted that in the evaluated configuration no partition has either the send or receive BCPii permission.

Global Performance Data Control Authority
This control limits the ability of a logical partition to view central processor activity data for other logical partitions. Logical partitions with control authority for global performance data can view CP utilization data and Input/Output (IOP) busy data for all of the logical partitions in the configuration. A logical partition without control authority for the performance data can view only the CP utilization data for itself.

Cross-Partition Authority
This control can limit the capability of the logical partition to issue certain control program instructions that affect other logical partitions. Logical partitions with cross-partition authority can issue instructions to perform a system reset of another logical partition, deactivate any other logical partition, and provide support for the automatic reconfiguration facility.

In addition to the security controls mentioned above, the TOE also insures that central storage and storage class memory for each logical partition is isolated and cannot be shared with other logical partitions. The TOE rigidly enforces this “no sharing” rule during logical partition definition, logical partition activation, logical partition reconfiguration and during logical partition execution.

The TOE also “removes” central processors (CPs) from logical partitions by virtualizing physical CPs. Virtualized physical CPs are referred to as logical processors. Within the TOE, each logical CP is represented as a data structure that is associated with its specific logical partitions preventing the transfer of data between partitions.

Thus, when PR/SM is initialized for secure operation, one partition cannot gain access to the data within another partition nor modify any aspect of another partition.

With z/Architecture or ESA/390 architecture (which includes the functions of ESA/370 Architecture), these models have problem-program compatibility with S/360™, S/370™, and 4300 processors. They can access virtual storage in multiple address spaces and data spaces. This extends addressability for system, sub-system, and application functions that use z/Architecture or ESA/390 architecture.

2 CC Conformance Claim

This Security Target is CC Part 2 conformant and CC Part 3 conformant, with a claimed Evaluation Assurance Level of EAL5, augmented by ALC_FLR.3, ALC_TAT.3, ATE_FUN.2 and AVA_VAN.5.

This Security Target does not claim conformance to any Protection Profile.

Common Criteria [CC] version 3.1 revision 5 is the basis for this conformance claim.

3 Security Problem Definition

PR/SM is intended for use in environments where separation of workloads is a requirement, but where the use of a single hardware platform is desirable for reasons of economy, flexibility, security or management.

The acquisition and management of computer systems is subject to economies of scale in many areas. Leasing or purchase costs may be lower for a single large machine than for a number of smaller machines of equivalent total processing capacity. There may also be savings in operational costs resulting from lower machine room capacity and fewer operations staff.

PR/SM provides flexibility by allowing the single machine to be set up to provide a wide range of virtual machine configurations. As one workload grows, more resources can be allocated to it, providing significant advantages where the required configuration is subject to frequent change. PR/SM provides the facility to partition a single platform to run any combination of z/OS, z/VM, z/VSE, z/TPF or Linux on z Systems allowing requirements for different operating system environments to be met.

Where confidentiality is a concern, PR/SM provides separation of workloads, and prevents the flow of information between partitions. This trusted separation may be used where the separation is based on need to know, or where data at differing national security classifications must be isolated.

3.1 Threat Environment

PR/SM may be used in a variety of threat environments, and for each intended use of the product an analysis should be performed which compares the specific threats within that environment against the claimed functionality.

The TOE is confronted with two different types of users:

1. Administrators (and security administrators) manage and review the TOE's configuration
2. Partitions consume the TOE's core functionality to run the desired workloads

The possible threats can be classified into the following two cases:

- Partitions and administrators may gain unauthorized access to data.

  Partitions may gain access to data belonging to another partition, for which they do not have clearance, specific authorization, or a need-to-know. This may be achieved either directly (for example, by reading storage allocated to another partition, or by failure to clear a resource before reallocation), or indirectly (for example, through a covert channel).

  Unauthorized access to audit data may lead to a false record of administrator actions.

- Partitions may gain unauthorized access to system resources (i.e. channel path, control unit, I/O device, physical or logical processor): such actions being contrary to the security or resource policy of an Organization.

3.1.1 Threats countered by the TOE

T.Access_Data

Illegal access to data

access by a partition to data that is not owned by that partition (i.e. data in the storage and I/O resources allocated to another partition and not including system data);

T.Access_CPU

Illegal access or control of processors and storage

access by a partition to allocate or deallocate storage, or logical processors outside the limits of the configuration;

T.Access_IOCA

Illegal access of the I/O Configuration

access by a partition without *I/O configuration control authority* to any IOCDS;

T.Access_BCPii

Illegal use of BCPii

access by a partition without appropriate *BCPii Permissions* to send/or and receive BCPii commands;

T.Access_Perf

Illegal access to performance data

access by a partition without *global performance data control authority* to CPU and Input/Output processor data for all partitions;

T.LPAR_XCTL

Illegal control of another logical partition

access by a partition without *cross-partition control authority* to current configuration data (to reset or deactivate a partition only);

T.Obj_Reuse

Illegal transfer of data during resource reallocation

access by a partition to data transferred with resources (object reuse) when those objects are reallocated to that partition from another partition;

T.Audit_Data

Illegal modification of the content of the security log

access to the security log by an administrator to modify its contents;

Note: *By design, the contents of the security log cannot be modified while it is contained in the TOE. An (unauthorized) administrator might want to attempt to modify the security log to remove any evidence that he setup the system in a manner inconsistent with the directions in the PR/SM Planning Guide Appendix: Developing, building and delivering a certified system (which will be referred in the remainder of this document as the Trusted Facility Manual (*[TFM]*). Any administrator attempting to modify the security log would need intimate designer level knowledge of the system, and have access to development tools.*

3.2 Assumptions

The specific conditions listed below are assumed to exist in a secure LPAR environment and are outside the security functionality of the TOE.

3.2.1 Environment of use of the TOE

3.2.1.1 Physical assumptions

It is assumed that the following physical conditions are met:

A.Data_Secure

Backup of and physical controlled access to the TOE security log is required

The TOE records security-relevant actions performed by the administrator in a security log. The TOE will prune the security log to 67% of its maximum capacity when the security log has been filled. It is the customer's responsibility to archive the security log prior to the log reaching capacity. Physical access of archived security log data is also the responsibility of the customer.

A.Phys_Secure

Physical protection of processor, I/O and HMC is required

The environment of the hardware is physically secured against unauthorized access. Access to I/O devices is restricted to authorized personnel. In particular the HMC and the Local Area Network (LAN) connecting it to the SEs must be physically protected from access other than by authorized system administrators.

3.2.1.2 Configuration assumptions

It is assumed that the following configuration is met:

A.Sep_Strength

The configuration of the TOE with regard to partition separation will be carried out according to the instructions provided in [TFM].

3.2.1.3 Personnel assumptions

It is assumed that the following personnel conditions will exist:

A.Admin_Secure

Administrative Personnel Security

Logical partitions within the z System can be operated from the HMC and the SE. The administrator/operators of the system must be cleared for the highest security classification of work being performed on the system.

3.3 Organizational Security Policies

The TOE complies with the following organizational security policy:

3.3.1 Hardware Support

P.SEP

Hardware support for partitions and separation

Those responsible for the TOE must ensure that the hardware of a Central Processing Complex is partitionable into several independent partitions.

3.3.2 Connectivity

P.HMC_Network

Networking capabilities HMC.

Those responsible for the TOE must ensure that the networking capabilities of the HMC are configured according to the [TFM].

4 Security Objectives

4.1 Objectives for the TOE

This section defines the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any organizational security policies identified. Each objective is stated in bold type font. An application note, in normal font, which supplies additional information and interpretation, follows it.

O.Identity

Identity

The TOE must ensure that each logical partition has a unique identity.

A zone number uniquely identifies each logical partition.

O.Auth_Admin

Authorized Administration

The TOE provides facilities to enable an authorized administrator to effectively manage the TOE and its security functions.

The security functions provided by the TOE enable secure administration of:

- IOCDSs
- BCPii permissions
- logical processors and storage
- I/O channel paths, control units and devices
- cross-partition functions
- performance data access

O.Auth_Ops

Authorized Operations

The TOE provides facilities to enable authorized users to effectively operate the TOE in a secure manner.

The security functions provided by the TOE enable secure operation in the following areas:

- partition activation
- processor and storage allocation
- processor execution
- message transfers

O.Audit

Audit and Accountability

The TOE will provide the means of recording any security relevant events, so as to assist an administrator in the detection of potential attacks or misconfiguration of the TOE security features that would leave the TOE susceptible to attack, and also to hold users accountable for any actions that they perform that are relevant to security.

The TOE will record the security-relevant actions of the administrator in a security log. Deletions, modifications and reading of the security log are controlled in a secure manner.

O.Reuse

Object Reuse

The TOE will provide the means of allowing a partition to use a resource or service without the user identity or contents of the resource being disclosed to other entities.

The TOE will help to ensure no information is disclosed via storage, channels, physical processors.

O.Resource

Reliability of Service

The TOE will provide the means of controlling the use of resources by its users (partitions) so as to prevent unauthorized denial of service.

The TOE will provide functions that enable control of the physical processor running time and cross partition functions.

4.2 Objectives for the Operational Environment

The following are the security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they do not require the implementation of functions in the TOE hardware and/or software. These security objectives are assumed to be in place in the TOE environment. They are included as necessary to support the TOE security objectives in addressing the security problem defined in the TOE security environment.

OE.Data_Store

Off-TOE Data Storage

Security log data stored off of the TOE must be controlled for confidentiality and integrity according to the owner's needs.

The security log information from the TOE may be stored separately from the TOE for archival purposes. The personnel and systems, if any, in charge of this information are responsible for the maintenance of its required security.

OE.Perss

Personnel

Personnel working as administrators or other privileged positions must be carefully selected and trained.

Since the administrator has full access to system data, careful selection and training of administrators and others in privileged positions works to detect, prevent, or counter other attacks, and deters compromise of system data.

OE.Sec_Setup

Secure Setup

The TOE must be protected during the setup phase.

The TOE shall be protected during the setup phase to ensure that the operations that have to be performed in this phase to set up the TOE for normal operation within the intended environment and for the intended operation is done in accordance with the guidelines within this Security Target. Verification shall include inspection of the IOCDS definition, verification of the partition security controls, and verification of the profiles.

OE.Phys_Prot

Restricted physical and remote access

Physical access and remote access to the HMC and z System must be restricted only to authorized and approved users.

The HMC and z System must be installed in restricted areas for the purposes of limiting accessibility by company personnel and avoiding physical destruction or alteration of the hardware. In particular the HMC and the LAN connecting it to the SEs must be physically protected from access other than by authorized system administrators.

Additionally, this restricted access applies to the remote support facility, which must be completely disabled, as this is outside the scope of the evaluations.

OE.SIE

Memory access control

The underlying hardware must provide separation mechanism that can be used by the TOE to protect the TSF and TSF data from unauthorized access and modification.

The underlying processors must support the enforcement of memory access control defined by a caller of a specific processor instruction.

OE.IO_Resource

I/O resource access control

The underlying physical I/O LIC must provide separation mechanisms that can be used by the TOE to restrict access of one partition to authorized I/O resources as well as to restrict the I/O resource access to partition memory.

The physical I/O resources LIC must support the enforcement to restrict access requests from one partition to the partition's associated I/O resources. The LIC must also restrict the I/O resource access to partition memory so that only the partition can be accessed by the I/O resource, which has this resource assigned in the IOCDS.

4.3 Security Objectives Rationale

4.3.1 Security Objectives Coverage

The following table provides a mapping of TOE objectives to threats and policies, showing that each objective counters or enforces at least one threat or policy, respectively.

Objective	Threats / OSPs
O.Identity	T.Access_Data T.Access_CPU T.Access_IOCA T.Access_BCPii T.Access_Perf T.LPAR_XCTL
O.Auth_Admin	T.Access_IOCA T.Access_BCPii T.Access_Perf T.LPAR_XCTL

Objective	Threats / OSPs
O.Auth_Ops	T.Access_Data T.Access_CPU
O.Audit	T.Audit_Data
O.Reuse	T.Obj_Reuse
O.Resource	T.LPAR_XCTL

Table 2: Mapping of security objectives to threats and policies

The following table provides a mapping of the objectives for the Operational Environment to assumptions, threats and policies, showing that each objective holds, counters or enforces at least one assumption, threat or policy, respectively.

Objective	Assumptions / Threats / OSPs
OE.Data_Store	A.Data_Secure
OE.Perss	A.Admin_Secure
OE.Sec_Setup	A.Sep_Strength
OE.Phys_Prot	A.Phys_Secure P.HMC_Network
OE.SIE	P.SEP
OE.IO_Resource	P.SEP

Table 3: Mapping of security objectives for the Operational Environment to assumptions, threats and policies

4.3.2 Security Objectives Sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat, when achieved, actually contributes to the removal, diminishing or mitigation of that threat.

Threat	Rationale for security objectives
T.Access_Data	**O.Identity** helps to remove the threat of illegal access to data by a partition by assigning a zone number to each logical partition which provides it with a unique identity. **O.Identity** is additionally supported by **O.Auth_Ops** which then uses the unique zone number to establish ownership of processor and storage resources during partition activation and then prevents any illegal access to data or storage or message transfers during normal processor execution.
T.Access_CPU	**O.Identity** helps to remove the threat of illegal access or control of processors and storage by a partition by assigning a zone number to each logical partition which provides it with a unique identity. **O.Identity** is additionally supported by **O.Auth_Ops** which then uses

Threat	Rationale for security objectives
	the unique zone number to ensure that the limits established at partition activation for storage and logical processors are not exceeded during normal processor execution.
T.Access_IOCA	**O.Identity** helps to remove the threat of illegal access to the I/O configuration by a partition by assigning a zone number to each logical partition which provides it with a unique identity. **O.Identity** is additionally supported by **O.Auth_Admin** which then uses the unique zone number to restrict access to the IOCDS to only those logical partitions which have *I/O configuration control authority*.
T.Access_BCPii	**O.Identity** helps to remove the threat of illegal access to BCPii by a partition by assigning a zone number to each logical partition which provides it with a unique identity within the BCPii command. **O.Identity** is additionally supported by **O.Auth_Admin** which then uses the unique zone number to restrict access to BCPii to only those logical partitions which have the appropriate *BCPii Permissions*.
T.Access_Perf	**O.Identity** helps to remove the threat of illegal access to performance data by a partition by assigning a zone number to each logical partition which provides it with a unique identity. **O.Identity** is additionally supported by **O.Auth_Admin** which then uses the unique zone number to restrict access to global CPU and I/O processor performance data to only those logical partitions which have *global performance data control authority*.
T.LPAR_XCTL	**O.Identity** helps to remove the threat of illegal access to partition controls by a partition by assigning a zone number to each logical partition that provides it with a unique identity. **O.Identity** is additionally supported by **O.Auth_Admin**. Only when the Cross Partition functions are enabled due to **O.Auth_Admin** can one authorized partition take over control of an authorized target partition. **O.Resource** provides functions that enable control of the physical processor running time and cross-partition functions.
T.Obj_Reuse	**O.Reuse** provides the means to allow the partition to use a resource or service without the partition's identity or contents of the resource being disclosed to other entities. When resources are reallocated from one partition to another, the resources are either reset (cleared) or are dedicated to one partition and therefore cannot be reallocated.
T.Audit_Data	**O.Audit** helps to eliminate this threat by insuring that all security relevant events occurring on the system are recorded in a non-volatile security log. All events are guaranteed to be recorded and no modifications can be made to the security log except those consistent with the policy enforced by the TOE.

Table 4: Sufficiency of objectives countering threats

The following rationale provides justification that the security objectives for the environment are suitable to cover each individual assumption, that each security objective for the environment that traces back to an assumption about the environment of use of the TOE, when achieved, actually contributes to the environment achieving consistency with the assumption, and that if all security objectives for the environment that trace back to an assumption are achieved, the intended usage is supported.

Assumption	Rationale for security objectives
A.Data_Secure	**OE.Data_Store** defines that the security and integrity of the security log is predicated on the assumption that the security administrator will archive and backup the security log prior to reaching its capacity and thus automatic pruning and physically protect archived data off-TOE. Because there is no functionality within the TOE to prevent the Security Log from over-writing itself, such an environment is key to the security of the Security Log.
A.Phys_Secure	As specified in **OE.Phys_Prot**, the method for providing physical security of the hardware is assumed to be restricted access. Restricted access will help to insure that assets used by the TOE, which are outside the domain of the TOE, remain secure.
A.Sep_Strength	Protection of the TOE for establishment of the required strict separation mode, as specified by **OE.Sec_Setup** helps to guarantee that all of the defined requirements to establish secure separation will be completed to provide the operational environment consistent with the scope of the evaluation.
A.Admin_Secure	**OE.Perss** requires administrators and personnel working in other privileged positions (e.g. TOE operators) to be carefully selected and trained. This includes authorization with the required need to know for all levels of the TOE and satisfies the assumption of secure administration.

Table 5: Sufficiency of objectives holding assumptions

The following rationale provides justification that the security objectives are suitable to cover each individual organizational security policy (OSP), that each security objective that traces back to an OSP, when achieved, actually contributes to the implementation of the OSP, and that if all security objectives that trace back to an OSP are achieved, the OSP is implemented.

OSP	Rationale for security objectives
P.SEP	This policy requires that those responsible for the TOE ensure that the hardware running the TOE provides independent partitions. These partitions are separated from each other by the environment with the objective **OE.SIE** that provides a special execution environment for a software component enforcing that objective. In addition, **OE.IO_Resource** provides the capability of associating I/O resources to logical partitions to restrict access to arbitrary I/O resources. In addition **OE.IO_Resource** provides the capability of associating I/O resources with partitions, so that only assigned resources may have access to partition memory.
P.HMC_Network	In addition to restricting physical access to the HMC, **OE.Phys_Prot** requires that access via the remote support facility must also be prevented since this facility is not necessarily secure and outside of the TOE.

Table 6: Sufficiency of objectives enforcing Organizational Security Policies

5 Extended Components Definition

This Security Target does not contain any extended component definitions.

6 Security Requirements for the Operational Environment

Although CC Version 3.1 does not mandate the use of security requirements for the operational environment of the TOE, it allows to define the security objectives for the environment to the level of detail useful for the understanding and evaluation of a TOE. In the case of PR/SM the security functionality defined in chapter 7 of this Security Target depends on the supporting functionality defined in this section. The authors of this Security Target decided (also for compatibility with Security Targets used for previous versions of the TOE that have been evaluated against previous versions of CC) to define this functionality using the structure of Security Functional Requirements.

The operational environment of the TOE implements several policies that are mentioned in the security functional requirements for the operational environment. Those policies are:

Memory Access Control Policy

The TOE underlying processor implements a memory access control policy enforced for instructions provided by the processor (subjects), limiting access to memory locations of the hardware (objects). Using a particular processor instruction, i.e. the SIE instruction, the processor can be loaded with memory ranges applicable for subsequent instructions. In case privileged (supervisor mode) instructions are invoked, the processor remains bound by the storage limitations imposed by the SIE instruction. The processor implements a second SIE instruction that can be stacked on the first SIE, but this has no effect on the TOE, because the second SIE can only be set within the scope of memory restrictions defined by the first SIE instruction, managed by the TOE.

I/O Resource Access Control Policies

1. The TOE underlying hardware implements an I/O resource access control policy enforced on I/O resource instructions (subjects), limiting access to I/O resources (objects).
2. The TOE underlying hardware implements an I/O resource access control policy enforced on I/O resource operations (subjects), limiting access to partition memory (objects).

The TOE will be conformant to the assurance requirements required for level EAL5, as well as the augmentation identified in Section 2, "CC Conformance Claim" . The assumptions stated for the environment need to be satisfied by the IT environment. It is expected that any system integrating the TOE will provide documentation and procedures as well as technical measures (e. g. within the host system) to demonstrate that the assumptions are fulfilled and the policies are implemented. A separate system audit or system accreditation process has to check this.

The only operational environment for which security functional requirements are stated is the underlying hardware, i.e. Central Processors (CP), Assist Processors (SAP) used by the Channel Subsystem, and the zHost Bridge (zHB) used by PCI devices. That environment has to provide the mechanism to protect the TSF and TSF data from unauthorized access and tampering. This is expressed with the following security functional requirements for the hardware used to execute TOE software:

6.1 User data protection (FDP)

6.1.1 Subset access control (CP) (FDP_ACC.1-CP)

FDP_ACC.1.1 The operational environment shall enforce the **Memory Access Control Policy** on **instructions as subjects and memory locations as objects**.

6.1.2 Security attribute based access control (CP) (FDP_ACF.1-CP)

FDP_ACF.1.1 The operational environment shall enforce the **Memory Access Control Policy** to objects based on the **memory configuration defined**.

FDP_ACF.1.2 The operational environment shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

Access to memory locations is based on the memory configuration defined by the invocation of the SIE instruction. When in SIE mode access to memory is restricted by the environment defined when the SIE instruction was invoked.

Application note: *: The SIE (Start Interpretive Execution) instruction causes the central processor (CP) to adhere to memory definitions supplied with the invocation of SIE. The CP only allows access to the defined memory. The "SIE mode" sets special purpose registers in the CP, which are not visible to any application running on the CP.*

FDP_ACF.1.3 The operational environment shall explicitly authorise access of subjects to objects based on the following additional rules: **[none]**.

FDP_ACF.1.4 The operational environment shall explicitly deny access of subjects to objects based on the following additional rules: **[none]**.

6.1.3 Subset access control (IO) (FDP_ACC.1-IO)

FDP_ACC.1.1 The operational environment shall enforce the **I/O Resource Access Control Policy** on

- **I/O resource instructions as subjects and logical I/O resources as objects**
- **I/O resource operations as subjects and partition memory as the object**

.

6.1.4 Security attribute based access control (IO) (FDP_ACF.1-IO)

FDP_ACF.1.1 The operational environment shall enforce the **I/O Resource Access Control Policy** to objects based on the **logical I/O resource association with a partition**.

FDP_ACF.1.2 The operational environment shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. **Access to logical I/O resources is based on the partition ID of the requesting logical partition; the partition ID of the requesting partition must match the partition ID of the I/O resource as defined in the IOCDS.**
2. **Access to partition memory is based on the ID of the requesting I/O resource; the resource ID requesting access must be assigned to the partition as defined in the IOCDS.**

FDP_ACF.1.3 The operational environment shall explicitly authorise access of subjects to objects based on the following additional rules: **[none]**.

FDP_ACF.1.4 The operational environment shall explicitly deny access of subjects to objects based on the following additional rules: **[none]**.

6.2 Security management (FMT)

6.2.1 Static attribute initialisation (CP) (FMT_MSA.3-CP)

FMT_MSA.3.1 The operational environment shall enforce the **Memory Access Control Policy** to provide **permissive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The operational environment shall allow **no role** to specify alternative initial values to override the default values when an object or information is created.

Application note: *: The "default" values in this case are seen as the values the Central Processor (CP) has after start-up. They have to be "permissive", since the initialization routine needs to set up the memory and must have the ability to perform privileged instructions.*

6.2.2 Static attribute initialisation (IO.SAP) (FMT_MSA.3-IO.SAP)

FMT_MSA.3.1 The operational environment shall enforce the **I/O Resource Access Control Policy** to provide **permissive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The operational environment shall allow **no role** to specify alternative initial values to override the default values when an object or information is created.

Application note: *: The "default" values in this case are seen as the values the System Assist Processor (SAP) has after start-up. They have to be "permissive", since the initialization routine needs to set up the channel subsystem memory in protected hardware system area and must have the ability to perform privileged instructions.*

6.2.3 Static attribute initialisation (IO.PCI) (FMT_MSA.3-IO.PCI)

FMT_MSA.3.1 The operational environment shall enforce the **I/O Resource Access Control Policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The operational environment shall allow **no role** to specify alternative initial values to override the default values when an object or information is created.

Application note: *: A partition can only take control of those PCI devices that have been assigned to it. Taking control of PCI devices happens after the system has started and the TOE has been initialized.*

7 Security Requirements

7.1 TOE Security Functional Requirements

The TOE implements several policies that are mentioned in the security functional requirements. Those policies are:

Access Control Security Function Policy (SFP)
The TOE implements an access control policy between subjects and objects. The subjects or users are the logical partitions (LPARs) defined in the IOCDS and the administrator. The objects are the physical resources of the processor (CPs, storage, CHPIDS, IOCDSs, profiles, ...) as well as the logical partitions themselves. Access to objects by subjects will be mediated by this policy to insure that subjects are only able to gain access to authorized objects.

Information Flow Control Security Function Policy (SFP)
The TOE implements an information flow control policy between subjects and objects, and between objects and objects. The subjects or users are the logical partitions (LPARs) defined in the IOCDS and the administrator. The objects are the physical resources of the processor (CPs, storage, CHPIDS, audit data, performance data, IOCDSs, profiles, ...) and the logical processors instantiated on a physical processor on behalf of a logical partition. Flow of information between objects and subjects, and between objects and objects will be mediated by this policy to insure that information flow is only possible when subjects and objects are associated with the same logical partition.

Note: *The terms **subject** and **object** as used in the following sections are defined in section 9.2 as well as section 7.1.2.1.*

The following table shows the SFRs for the TOE, and the operations performed on the components according to CC part 1: iteration (Iter.), refinement (Ref.), assignment (Ass.) and selection (Sel.).

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
FAU - Security audit	FAU_GEN.1 Audit data generation		CC Part 2	No	No	Yes	Yes
	FAU_GEN.2 User identity association		CC Part 2	No	No	No	No
	FAU_SAR.1 Audit review		CC Part 2	No	No	Yes	No
	FAU_SAR.2 Restricted audit review		CC Part 2	No	No	No	No
	FAU_SAR.3 Selectable audit review		CC Part 2	No	No	Yes	No
	FAU_STG.1 Protected audit trail storage		CC Part 2	No	No	No	Yes
	FAU_STG.4 Prevention of audit data loss		CC Part 2	No	No	Yes	Yes
FDP - User data protection	FDP_ACC.2 Complete access control		CC Part 2	No	No	Yes	No

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
	FDP_ACF.1A Security attribute based access control (activation)	FDP_ACF.1	CC Part 2	Yes	No	Yes	No
	FDP_ACF.1B Security attribute based access control (allocation)	FDP_ACF.1	CC Part 2	Yes	No	Yes	No
	FDP_ACF.1C Security attribute based access control (channel path)	FDP_ACF.1	CC Part 2	Yes	No	Yes	No
	FDP_ACF.1D Security attribute based access control (control unit/devices)	FDP_ACF.1	CC Part 2	Yes	No	Yes	No
	FDP_IFC.1 Subset information flow control		CC Part 2	No	No	Yes	No
	FDP_IFF.1 Simple security attributes		CC Part 2	No	No	Yes	No
	FDP_RIP.2 Full residual information protection		CC Part 2	No	No	No	Yes
FIA - Identification and authentication	FIA_ATD.1 User attribute definition		CC Part 2	No	No	Yes	No
	FIA_UID.2 User identification before any action		CC Part 2	No	No	No	No
FMT - Security management	FMT_MSA.1A Management of security attributes (authorities)	FMT_MSA.1	CC Part 2	Yes	No	Yes	Yes
	FMT_MSA.1B Management of security attributes (resource limits)	FMT_MSA.1	CC Part 2	Yes	No	Yes	Yes
	FMT_MSA.1C Management of security attributes (candidate access)	FMT_MSA.1	CC Part 2	Yes	No	Yes	Yes
	FMT_MSA.3 Static attribute initialisation		CC Part 2	No	No	Yes	Yes
	FMT_MTD.1 Management of TSF data		CC Part 2	No	Yes	Yes	Yes
	FMT_SMF.1 Specification of Management Functions		CC Part 2	No	No	Yes	No
	FMT_SMR.1 Security roles		CC Part 2	No	No	Yes	No
FPR - Privacy	FPR_UNO.1 Unobservability		CC Part 2	No	Yes	Yes	No
FPT - Protection of the TSF	FPT_ITT.1 Basic internal TSF data transfer protection		CC Part 2	No	Yes	No	Yes
	FPT_STM.1 Reliable time stamps		CC Part 2	No	No	No	No

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
	FPT_TRC.1 Internal TSF consistency		CC Part 2	No	No	Yes	No
	FPT_TST.1 TSF testing		CC Part 2	No	Yes	Yes	Yes
FRU - Resource utilisation	FRU_RSA.1 Maximum quotas		CC Part 2	No	No	Yes	Yes
FTA - TOE access	FTA_TSE.1 TOE session establishment		CC Part 2	No	No	Yes	No

Table 7: SFRs for the TOE

7.1.1 Security audit (FAU)

7.1.1.1 Audit data generation (FAU_GEN.1)

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 **basic** level of audit; and

c) **the following auditable events:**

1. **creating or modifying the IOCDS part of a configuration;**
2. **modifying the reconfigurable part of a configuration;**
3. **selecting a configuration;**
4. **performing a power-on reset;**
5. **activating or deactivating logical partitions;**
6. **logging on or off the console.**

Application Note:

Changes to the BCPii configuration of a partition are covered by item 2.

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,

- **profile contents**
- **power-on reset options**

Application note: *The audit subsystem is always active and can be neither shut down nor be activated. Therefore, FAU_GEN.1.1 a) does not apply.*

7.1.1.2 User identity association (FAU_GEN.2)

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

7.1.1.3 Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide **the security administrator and the access administrator** with the capability to read **all audit information** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

7.1.1.4 Restricted audit review (FAU_SAR.2)

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

Application Note:

Apart from any user impersonating the generic role security administrator as defined in section 1.5.2.4 also users assigned the role Access Administrator (ACSADMIN) are granted explicit read- access to the audit records.

7.1.1.5 Selectable audit review (FAU_SAR.3)

FAU_SAR.3.1 The TSF shall provide the ability to apply **searches and sorting** of audit data based on **date or event criteria**.

7.1.1.6 Protected audit trail storage (FAU_STG.1)

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to **prevent** unauthorised modifications to the stored audit records in the audit trail.

7.1.1.7 Prevention of audit data loss (FAU_STG.4)

FAU_STG.4.1 The TSF shall **overwrite the oldest stored audit records** and **take no other actions** if the audit trail is full.

7.1.2 User data protection (FDP)

7.1.2.1 Complete access control (FDP_ACC.2)

FDP_ACC.2.1 The TSF shall enforce the **access control SFP** on

- **the subjects**
  - **defined logical partitions**
  - **processes acting on behalf of the administrator**
- **and the objects**
  - **physical CPs**
  - **physical CP timeslices**

- **logical processors**
- **physical storage**
- **CHPIDs**
- **control units/devices**
- **defined logical partitions**

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.

7.1.2.2 Security attribute based access control (activation) (FDP_ACF.1A)

FDP_ACF.1A.1 The TSF shall enforce the **access control SFP** to objects based on the following:

- **the subjects**
  - **defined logical partitions**
  - **processes acting on behalf of the administrator**
- **the objects**
  - **defined logical partitions**
- **the security attributes:**
  - **the cross-partition authority of a logical partition**

FDP_ACF.1A.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **a logical partition with cross-partition authority or a process acting on behalf of the administrator can deactivate or reset a logical partition.**

FDP_ACF.1A.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[none]**.

FDP_ACF.1A.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[none]**.

7.1.2.3 Security attribute based access control (allocation) (FDP_ACF.1B)

FDP_ACF.1B.1 The TSF shall enforce the **access control SFP** to objects based on the following:

- **the subjects**
  - **defined logical partitions**
- **the objects**
  - **defined logical partitions**
- **the security attributes:**
  - **resource limits (number of logical processors, physical processor time slices, amount of storage) attributed to logical partitions.**

FDP_ACF.1B.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **a logical partition can allocate the resources**
  - **logical processor**

- **physical processor time slices**
- **storage**

only within the resource limits as defined in the image profile.

FDP_ACF.1B.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[none]**.

FDP_ACF.1B.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[none]**.

7.1.2.4 Security attribute based access control (channel path) (FDP_ACF.1C)

FDP_ACF.1C.1 The TSF shall enforce the **access control SFP** to objects based on the following:

- **the subjects**
  - **subjects acting on behalf of authorized administrators**
- **the objects**
  - **defined logical partitions**
  - **CHPIDs**
- **the security attributes:**
  - **a logical partition's candidate access for the channel path**
  - **the logical partition isolation control for a logical partition.**

FDP_ACF.1C.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **subjects acting on behalf of authorized administrators may allocate CHPIDs to logical partitions according to the following rules:**
  - **a channel path may only be allocated to a logical partition with candidate access to it;**
  - **if a channel path is dedicated to a logical partition, it cannot be de-allocated from that partition;**
  - **if a channel path is reconfigurable and allocated to a logical partition with the logical partition isolation attribute, it cannot be de-allocated from that partition;**
  - **if a channel path is reconfigurable and allocated to a logical partition without the logical partition isolation attribute, it can be de-allocated from that partition;**
  - **a logical partition with the logical partition isolation attribute can deconfigure a channel path. To make it available for use by another logical partition, a process acting on behalf of an authorized administrator needs to release that channel path before the channel path becomes available to another logical partition.**

FDP_ACF.1C.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[none]**.

FDP_ACF.1C.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[none]**.

7.1.2.5 Security attribute based access control (control unit/devices) (FDP_ACF.1D)

FDP_ACF.1D.1 The TSF shall enforce the **access control SFP** to objects based on the following:

- **the subjects**
  - **defined logical partitions**
- **the objects**
  - **control unit/device**
- **the security attributes:**
  - **a logical partition's candidate access for the control unit/device**

FDP_ACF.1D.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **a logical partition has access to a control unit if the control unit is on a channel path allocated to the logical partition;**
- **a logical partition has access to a device if the device is attached to a control unit on a channel path allocated to the logical partition, and the logical partition has candidate access to the device.**

FDP_ACF.1D.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[none]**.

FDP_ACF.1D.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[none]**.

7.1.2.6 Subset information flow control (FDP_IFC.1)

FDP_IFC.1.1 The TSF shall enforce the **information flow control SFP** on

- **the subjects**
  - **activated logical partitions**
- **and the objects**
  - **resources**
  - **storage**
  - **processors**
  - **CHPIDs**
  - **I/O control units and devices**
  - **global performance data**

which controls the transfer of:

- **any information**

between subjects and objects. The following operations are mediated:

- **read central storage**
- **write central storage**
- **read storage class memory**
- **write storage class memory**
- **read I/O**
- **write I/O**

- **read central processor**
- **write central processor**

7.1.2.7 Simple security attributes (FDP_IFF.1)

FDP_IFF.1.1 The TSF shall enforce the **information flow control SFP** based on the following types of subject and information security attributes:

- **subjects**
  - **activated logical partitions**
- **with security attributes**
  - **logical partition identifier**
  - **cross-partition authority**
  - **global performance data authority.**
- **any information with security attributes**
  - **none**

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:

- **subjects**
  - **activated logical partitions**
- **with security attribute**
  - **logical partition identifier**
- **and rules**
  - ***Describable effect:* When an operation is executed on behalf of a logical partition, the effects that partition perceives must be capable of complete description only in terms of objects known to that partition.**
  - ***Isolation of effect:* When an operation is executed on behalf of an isolated partition, other partitions should perceive no effects at all. Neither shall an isolated partition perceive effects from an operation executed on behalf of non-isolated, co-operating partitions.**
  - ***I/O isolation:* I/O devices associated with an isolated partition affect the state perceived by only that partition. I/O devices associated with non-isolated, co-operating partitions will not affect the state perceived by any isolated partition.**
  - ***I/O-State effect:* I/O devices must not be able to cause dissimilar behavior to be exhibited by states that a partition perceives as identical.**
  - ***State-I/O effect:* A partition's I/O devices must not be able to perceive differences between states that the partition perceives as identical.**
  - ***Isolation determinacy:* The selection of the next operation to be executed on behalf of an isolated partition must depend only on the state of that partition and is independent of the state of any non-isolated, co-operating partitions.**

Application Note: "*Operations*" *as used in this SFR are those described in Subset information flow control (FDP_IFC.1)* .

FDP_IFF.1.3 The TSF shall enforce the **following additional information flow control SFP rules:[none]**.

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules:

- **the logical partition has cross-partition authority and the access is to reset or deactivate a logical partition;**
- **transfer of a message between a logical partition and a resource can occur if the partition has cross-partition authority and one of the following is true:**
  - **the message is a request to reset a partition,**
  - **the message is a response to a request to reset a partition,**
  - **the message is a request to deactivate a partition,**
  - **the message is a response to a request to deactivate a partition**
  - **the message is a request to send SNMP commands to an SE**
- **a logical partition with global performance data control authority can view the performance data of all other logical partitions.**

Application Note: "*Operations*" *as used in this SFR (reset or deactivate, message transfer, view performance data) are constructed out of the primitive operations specified in Subset information flow control (FDP_IFC.1)* .

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

7.1.2.8 Full residual information protection (FDP_RIP.2)

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **allocation of the resource to** all objects.

7.1.3 Identification and authentication (FIA)

7.1.3.1 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

- **logical partition identifier**
- **I/O configuration control authority**
- **cross-partition authority**
- ***send* BCPii command permission**
- ***receive* BCPii command permission**
- **logical partition isolation**
- **global performance data control authority**
- **resource limits**
- **partition scheduling parameters.**
- **candidate access**

Application Note: *Within the scope of the TOE, an individual user is a logical partition unless explicitly stated otherwise.*

7.1.3.2 User identification before any action (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.

Application Note: *This identification requirement applies to logical partitions as well as to the administrative users working on the HMC/SE.*

7.1.4 Security management (FMT)

7.1.4.1 Management of security attributes (authorities) (FMT_MSA.1A)

FMT_MSA.1A.1 The TSF shall enforce the **access control SFP** to restrict the ability to **assign** the security attributes

- **I/O configuration control authority**
- **cross-partition authority**
- ***send* BCPii command permission**
- ***receive* BCPii command permission**
- **logical partition isolation**
- **global performance data control authority**

to **the security administrator**.

7.1.4.2 Management of security attributes (resource limits) (FMT_MSA.1B)

FMT_MSA.1B.1 The TSF shall enforce the **access control SFP** to restrict the ability to **modify** the security attributes

- **resource limits (number of logical processors, amount of storage)**
- **partition scheduling parameters**

to **the security administrator**.

7.1.4.3 Management of security attributes (candidate access) (FMT_MSA.1C)

FMT_MSA.1C.1 The TSF shall enforce the **access control SFP** to restrict the ability to **assign** the security attributes

- **candidate access**

to **the security administrator**.

7.1.4.4 Static attribute initialisation (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the **access 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 **security administrator** to specify alternative initial values to override the default values when an object or information is created.

7.1.4.5 Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to **modify** the

- **IOCDS part of the configuration**
- **reconfigurable part of the configuration**

- **image profile**
- **reset profile**

to **the security administrator *or logical partitions with I/O configuration control authority*.**

Application Note: *A refinement was performed on this SFR since a logical partition is not a role maintained by the TOE but an authorized subject allowed to modify the configuration, if granted I/O configuration control authority.*

7.1.4.6 Specification of Management Functions (FMT_SMF.1)

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

- **object security attributes management.**

7.1.4.7 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles

- **security administrator**
- **administrator**
- **operator**
- **advanced operator**
- **programmer**
- **service representative**
- **access administrator**

and customized user roles defined based on the predefined default roles listed above.

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

Application Note:

The role security administrator listed above is not a predefined default role but a generic role with access to specific security related tasks as defined in section 1.5. Any predefined default role or customized role derived from such that has been granted access to at least all of those specific tasks is considered to be security administrator.

7.1.5 Privacy (FPR)

7.1.5.1 Unobservability (FPR_UNO.1)

FPR_UNO.1.1 The TSF shall ensure that **any subjects** are unable to observe ~~the operation~~ **any operation** on **any object/resource** by **any partition/subject**.

Application Note: *Subjects are defined as the logical partitions and the software running in these partitions which is a consistent view with FIA_ATD.1.*

Application Note: *An editorial refinement was performed for better readability.*

7.1.6 Protection of the TSF (FPT)

7.1.6.1 Basic internal TSF data transfer protection (FPT_ITT.1)

FPT_ITT.1.1 The TSF shall protect TSF data from **disclosure *and* modification** when it is transmitted between separate parts of the TOE.

Application Note: *Internal TSF data, specifically the security (audit) log, is protected when synchronized between dual SEs.*

Application Note: *An editorial refinement was performed for better readability.*

7.1.6.2 Reliable time stamps (FPT_STM.1)

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Application Note: *The TOE uses a hardware timer to maintain its own time stamp. This hardware timer is protected from tampering by untrusted subjects. The start value for this timer may be set by the system administrator, but the system administrator may also start a program that uses an external trusted time source to set this initial value.*

7.1.6.3 Internal TSF consistency (FPT_TRC.1)

FPT_TRC.1.1 The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.

FPT_TRC.1.2 When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for **recording of auditable events**.

7.1.6.4 TSF testing (FPT_TST.1)

FPT_TST.1.1 The TSF shall run a suite of self tests **during initial start-up, periodically during normal operation, at the request of the authorised user *and* at the conditions**

- **performing a reset or recovery**

to demonstrate the correct operation of **TSF implemented by the LPAR LIC**.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of **TSF data within the LPAR LIC**.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of **the LPAR LIC**.

Application Note: *An editorial refinement to FPT_TST.1.1 was performed for better readability.*

7.1.7 Resource utilisation (FRU)

7.1.7.1 Maximum quotas (FRU_RSA.1)

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources:

- **physical processor time slices**

that **subjects** can use **over a specified period of time**.

Application Note: *The term "subject" is equivalent to "logical processors" in the context of this SFR, since no other subjects may use processor time slices.*

7.1.8 TOE access (FTA)

7.1.8.1 TOE session establishment (FTA_TSE.1)

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on

- **the unavailability of necessary physical resources (CPs, storage, channels)**
- **exceeding the scheduling parameters for the logical partitions**

.

7.2 Security Functional Requirements Rationale

The following sections analyse the security requirements with regard to coverage and sufficiency as well as dependencies.

7.2.1 Security Requirements Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

Security functional requirements	Objectives
FAU_GEN.1	O.Audit
FAU_GEN.2	O.Audit
FAU_SAR.1	O.Audit
FAU_SAR.2	O.Audit
FAU_SAR.3	O.Audit
FAU_STG.1	O.Audit
FAU_STG.4	O.Audit
FDP_ACC.2	O.Auth_Ops, O.Resource
FDP_ACF.1A	O.Auth_Admin, O.Auth_Ops, O.Identity
FDP_ACF.1B	O.Auth_Admin, O.Auth_Ops, O.Identity
FDP_ACF.1C	O.Auth_Admin, O.Auth_Ops, O.Identity
FDP_ACF.1D	O.Auth_Admin, O.Auth_Ops, O.Identity

Security functional requirements	Objectives
FDP_IFC.1	O.Auth_Ops
FDP_IFF.1	O.Auth_Ops
FDP_RIP.2	O.Reuse
FIA_ATD.1	O.Identity
FIA_UID.2	O.Identity
FMT_MSA.1A	O.Auth_Admin, O.Auth_Ops, O.Resource
FMT_MSA.1B	O.Auth_Admin, O.Auth_Ops, O.Resource
FMT_MSA.1C	O.Auth_Admin, O.Auth_Ops, O.Resource
FMT_MSA.3	O.Auth_Admin, O.Auth_Ops, O.Resource
FMT_MTD.1	O.Audit, O.Auth_Admin, O.Auth_Ops
FMT_SMF.1	O.Auth_Admin
FMT_SMR.1	O.Auth_Admin
FPR_UNO.1	O.Reuse
FPT_ITT.1	O.Audit
FPT_STM.1	O.Audit
FPT_TRC.1	O.Audit
FPT_TST.1	O.Auth_Ops
FRU_RSA.1	O.Resource
FTA_TSE.1	O.Resource

Table 8: Mapping of security functional requirements to security objectives

7.2.2 Security Requirements Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives.

Security objectives	Rationale
O.Identity	The objective demands that each logical partition have a unique identity. The objective is covered by **FIA_ATD.1** that defines the security attributes belonging to an individual logical partition. **FIA_UID.2** requires that each logical partition is identified before any TSF-mediated action is performed on behalf of that logical partition. Finally **FDP_ACF.1*** enforces access control SFP to objects based on the list of security attributes.
O.Auth_Admin	O.Auth_admin requires security functions provided by the TOE to help to enable secure administration of the following: IOCDS, BCPii permissions, logical processors and storage, I/O channel paths and control units, cross-partition functions and performance data access. The TOE provides restrictive default values for security attributes governing these security functions as specified in **FMT_MSA.3**. The TSF ensures that only the security administrator can alter these security attributes as per **FMT_SMR.1** and **FMT_SMF.1**. **FDP_ACF.1*** specifies the TSF shall enforce the access control SFP to objects based on security attributes including partition scheduling parameters (logical processors and storage), and global performance data (performance data access). I/O channel paths and control units are covered by the security functions enforced in **FMT_MSA.1*** (*I/O configuration control authority* and *logical partition isolation*). The TSF restricts the ability to change the IOCDS to the security administrator as covered in **FMT_MTD.1**.
O.Auth_Ops	O.Auth_Ops requires that the TOE provide an authorized administrator an effective means to manage the TOE and its security functions. **FDP_ACC.2** provides authorized allocation of subjects to objects. **FDP_ACF.1*** provides for the establishment of security attributes and rules governing operations and access by subjects to objects based on these attributes. **FMT_MSA.1*** and **FMT_MSA.3** insure that once the authorization (or lack of authorization) is set, these attributes cannot be changed. **FMT_MTD.1** allows only the security administrator the ability to modify these settings. **FPT_TST.1** provides for periodic validation of the correct operation of the TOE to insure that there can be no compromise in the execution of authorized operations. **FDP_IFF.1** and **FDP_IFC.1** specify that the TSF shall enforce the information flow control SFP on logical partitions based on security attributes including: *global performance data access*, *I/O configuration control*, cross-partition reset/deactivate capability, and *logical partition isolation*.
O.Audit	The objective demands that the TOE provide the means of recording any security relevant events, so as to assist an administrator in the detection of potential attacks or misconfiguration of the TOE security features that would leave the TOE susceptible to attack, and also to hold users accountable for any actions that they perform that are relevant to security. The objective is covered by **FAU_GEN.1**, **FAU_GEN.2** and **FPT_STM.1** that define which events are recorded in the security log and associates an identity and timestamp with each event. **FAU_SAR.1**, **FAU_SAR.2** and **FAU_SAR.3** cover the ability of an authorized security administrator to read, search and sort the security log data. **FAU_STG.1**, **FMT_MTD.1** and **FAU_STG.4** cover the prevention of any unauthorized deletions or modification to the audit records as well as specify the actions that occur when the security log is full. Finally **FPT_ITT.1** and **FPT_TRC.1** cover the integrity and consistency of the security log when transmitted between dual support elements (SE).

Security objectives	Rationale
O.Reuse	O.Obj_Reuse requires that data is not transferred with resources when those resources are reallocated from one partition to another. FDP_RIP2. And **FPR_UNO.1** sufficiently satisfies this requirement. **FDP_RIP.2** ensures than any previous content of a resource is made unavailable when that resource is de-allocated from any and all objects. **FPR_UNO.1** ensures that partitions/subjects are unable to observe any operation on any object/resource by any other partition/subject.
O.Resource	The objectives states that the TOE will help to prevent unauthorized access to physical processor running time and cross-partition functions. **FDP_ACC.2** insures that the access control SFP is enforced to control all operations between subjects and objects. Therefore no subject (partition) can gain unauthorized access to the running time and partition control functions. **FMT_MSA.1*** and **FMT_MSA.3** insure that once the authorization (or lack of authorization) is set, these attributes cannot be changed. **FRU_RSA.1** enforces the running time slices that have been previously defined. Finally, **FTA_TSE.1** guarantees adherence to physical resource definitions and scheduling parameters.

Table 9: Security objectives for the TOE rationale

7.2.3 Security Requirements Dependency Analysis

The following table demonstrates the dependencies of the SFRs modeled in CC Part 2, and how the SFRs for the TOE resolve those dependencies.

Security functional requirement	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1	FAU_GEN.1
	FIA_UID.1	FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.1	FAU_STG.1
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1A FDP_ACF.1B FDP_ACF.1C FDP_ACF.1D
FDP_ACF.1A	FDP_ACC.1	FDP_ACC.2
	FMT_MSA.3	FMT_MSA.3

Security functional requirement	Dependencies	Resolution
FDP_ACF.1B	FDP_ACC.1	FDP_ACC.2
	FMT_MSA.3	FMT_MSA.3
FDP_ACF.1C	FDP_ACC.1	FDP_ACC.2
	FMT_MSA.3	FMT_MSA.3
FDP_ACF.1D	FDP_ACC.1	FDP_ACC.2
	FMT_MSA.3	FMT_MSA.3
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1	FDP_IFC.1
	FMT_MSA.3	FMT_MSA.3
FDP_RIP.2	No dependencies	
FIA_ATD.1	No dependencies	
FIA_UID.2	No dependencies	
FMT_MSA.1A	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.2 FDP_IFC.1
	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.1B	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.2 FDP_IFC.1
	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.1C	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.2 FDP_IFC.1
	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.3	FMT_MSA.1	FMT_MSA.1A FMT_MSA.1B FMT_MSA.1C
	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_SMF.1	No dependencies	
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPR_UNO.1	No dependencies	

Security functional requirement	Dependencies	Resolution
FPT_ITT.1	No dependencies	
FPT_STM.1	No dependencies	
FPT_TRC.1	FPT_ITT.1	FPT_ITT.1
FPT_TST.1	No dependencies	
FRU_RSA.1	No dependencies	
FTA_TSE.1	No dependencies	

Table 10: TOE SFR dependency analysis

7.3 Security Assurance Requirements

The security assurance requirements (SARs) for the TOE are the Evaluation Assurance Level 5 components as specified in [CC] part 3, augmented by ALC_FLR.3, ALC_TAT.3, ATE_FUN.2 and AVA_VAN.5.

The following table shows the SARs, and the operations performed on the components according to CC part 3: iteration (Iter.), refinement (Ref.), assignment (Ass.) and selection (Sel.).

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
ADV Development	ADV_ARC.1 Security architecture description	CC Part 3	No	No	No	No
	ADV_FSP.5 Complete semi-formal functional specification with additional error information	CC Part 3	No	No	No	No
	ADV_IMP.1 Implementation representation of the TSF	CC Part 3	No	No	No	No
	ADV_INT.2 Well-structured internals	CC Part 3	No	No	No	No
	ADV_TDS.4 Semiformal modular design	CC Part 3	No	No	No	No
AGD Guidance documents	AGD_OPE.1 Operational user guidance	CC Part 3	No	No	No	No
	AGD_PRE.1 Preparative procedures	CC Part 3	No	No	No	No
ALC Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation	CC Part 3	No	No	No	No
	ALC_CMS.5 Development tools CM coverage	CC Part 3	No	No	No	No
	ALC_DEL.1 Delivery procedures	CC Part 3	No	No	No	No
	ALC_DVS.1 Identification of security measures	CC Part 3	No	No	No	No
	ALC_FLR.3 Systematic flaw remediation	CC Part 3	No	No	No	No
	ALC_LCD.1 Developer defined life-cycle model	CC Part 3	No	No	No	No

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
	ALC_TAT.3 Compliance with implementation standards - all parts	CC Part 3	No	No	No	No
ASE Security Target evaluation	ASE_INT.1 ST introduction	CC Part 3	No	No	No	No
	ASE_CCL.1 Conformance claims	CC Part 3	No	No	No	No
	ASE_SPD.1 Security problem definition	CC Part 3	No	No	No	No
	ASE_OBJ.2 Security objectives	CC Part 3	No	No	No	No
	ASE_ECD.1 Extended components definition	CC Part 3	No	No	No	No
	ASE_REQ.2 Derived security requirements	CC Part 3	No	No	No	No
	ASE_TSS.1 TOE summary specification	CC Part 3	No	No	No	No
ATE Tests	ATE_COV.2 Analysis of coverage	CC Part 3	No	No	No	No
	ATE_DPT.3 Testing: modular design	CC Part 3	No	No	No	No
	ATE_FUN.2 Ordered functional testing	CC Part 3	No	No	No	No
	ATE_IND.2 Independent testing - sample	CC Part 3	No	No	No	No
AVA Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis	CC Part 3	No	No	No	No

Table 11: SARs

7.4 Security Assurance Requirements Rationale

This Security Target claims EAL5. The business requirements for customers of the z System identify EAL5 together with the augmentation identified in Section 2, "CC Conformance Claim" as the necessary assurance level for evaluation. This is due to the strong need to have logical partitions provide the same isolation as air-gapped systems. A high assurance level is needed to satisfy this need.

8 TOE Summary Specification

8.1 TOE Security Functionality

As defined earlier in this document, the TOE consist of the PR/SM LIC kernel running on the z System Hardware. This LIC implements the security functions specified in chapter 7. This chapter provides a more detailed description of the TOE interfaces and internals and how the TOE implements the security functional requirements.

The first section describes how LPAR is initialized as well as where LPAR resides in storage. This information is provided to provide a better understanding of the secure nature of LPAR code.

The second section provides a general overview of the flow of information between LPAR and the HMC. The last section describes the security functions of the TOE and relates them to the security functional requirements listed in chapter 7.1.

8.1.1 LPAR Kernel

The LPAR core image is loaded into the Hardware Area (HSA) by the SE. The SE then sets the prefix register of one processor to the beginning of the image and restarts this processor thereby turning control to LPAR initialization LIC. After LPAR initialization completes, partitions may be automatically activated based on image profiles, or a security administrator may allocate system resources via partition definition panels.

The amount of storage used by LPAR in HSA depends on the number of physical processors installed, the number of partitions defined, and the number of I/O devices defined in the IOCDS. All storage between X'0' and 4 MB is reserved for LPAR's core image. LPAR will allocate the rest of its storage from the range of 4 MB to 1.5 GB. All storage used by LPAR must fit below 1.5 GB in HSA. Since 0 to 1.5 GB is reserved exclusively for LPAR use, "real" HSA is allocated starting at 1.5 GB in 256 MB increments.

HSA is an area of central storage that is inaccessible to programs resident in logical partitions and is therefore secure.

8.1.2 Information Flow to/from HMC

Information flow between LPAR and the HMC is accomplished through a proprietary mechanism. When an administrator wishes to activate a partition, the activation request is initiated from the HMC. LPAR will receive an external interrupt and issue an instruction to obtain the description of the partition the administrator wishes to activate. LPAR will attempt to construct the partition and will inform the HMC of the success or failure of the command.

8.1.3 TOE Security Functions

The following section describes the security functions of the TOE and how they relate to the security functional requirements listed in section 7.1. This provides a better understanding of the TOE security functions and the mapping to the [CC].

8.1.3.1 Identification and Authentication

The TOE implements an Image profile to define the initial operational characteristics of a logical partition. In a given configuration each logical partition is uniquely named and has a corresponding Image profile. One of the parameters in the Image profile is the logical partition identifier (i.e. zone number). If a logical partition is in the current configuration, then the zone number uniquely identifies that partition. [Satisfies SFRs: FIA_UID.2]

Contributing is that unique user IDs assigned to each administrative user of the HMC/SE.

8.1.3.2 Access Control and Information Flow Control

The following describes the access control and information flow control functions implemented by the TOE:

a) TOE can be configured so that no logical partition has *I/O configuration control authority*. When it is necessary to change an IOCDS, PR/SM can be configured so that only one logical partition has *I/O configuration control authority*. [Satisfies SFRs: FMT_MSA.1 (authorities)]

b) The TOE can be configured so that no logical partition has *cross-partition control authority*. [Satisfies SFRs: FMT_MSA.1 (authorities)]

c) The TOE will permit the set of logical partitions with candidate access to a channel path to be restricted. A channel path can only be allocated to a logical partition if that partition has candidate access to the path. [Satisfies SFRs: FTA_TSE.1, FDP_ACC.2, FDP_ACF.1 (channel path), FMT_MSA.1(candidate access)]

d) The TOE will permit the set of logical partitions with candidate access to an I/O device on a shared channel path to be restricted. An I/O device will not be allocated to a partition without candidate access to it, even if the shared channel path to which the device is attached is allocated to the partition. [Satisfies SFRs: FDP_ACC.2, FDP_ACF.1 (control unit/devices)]

e) The TOE can be configured to prevent the shared use of any channel path, control unit or I/O device between logical partitions. [Satisfies SFRs: FDP_ACC.2, FDP_ACF.1 (channel path, control unit/devices)]

f) The TOE will permit a channel path to be allocated exclusively to one logical partition either by identifying the channel path as dedicated, or by designating the owning partition as isolated (isolation only applies to the partition's reconfigurable channel paths). The TOE will help to prevent the de-allocation of such a channel path from the partition, even when the channel path is off-line. [Satisfies SFRs: FDP_ACC.2, FDP_ACF.1 (channel path), FDP_IFC.1]

g) The TOE will help to ensure that a reconfigurable or dedicated channel path is never shared. [Satisfies SFRs: FDP_ACC.2, FDP_ACF.1 (channel path), FDP_IFC.1]

h) The TOE will help to ensure that control units and I/O devices cannot be allocated independently of the channel path to which they are attached. A control unit is allocated to a partition if a channel path to which it is attached is allocated to the partition. An I/O device is allocated to a partition if a control unit to which it is attached is allocated to the partition, and the partition has candidate access to the device. [Satisfies SFRs: FDP_ACC.2, FDP_ACF.1 (channel path, control unit/devices)]

i) The TOE can be configured so that a logical partition has dedicated use of the physical processors allocated to it. The TOE will help to ensure that a dedicated physical processor is allocated to only one logical partition, and will help to prevent the de-allocation of the physical processor while the logical processor using it is online and not check- stopped. [Satisfies SFRs: FDP_ACC.2, FPR_UNO.1, FDP_IFC.1]

j) The TOE can be configured so that no logical partitions have *global performance data control authority*. In this case, a logical partition will only be able to gather performance data about the resources allocated to it. [Satisfies SFRs: FMT_MSA.1 (authorities), FPR_UNO.1, FDP_ACC.2]

k) The TOE can be configured that no BCPii commands can be sent or received by logical partition's configuration on the SE part of the TOE, if no BCPii permissions are granted. When it is necessary that the SE and logical partitions exchange BCPii messages, PR/SM can be configured that logical partitions can send BCPii messages to the SE or receive and process BCPii messages on the SE part of the TOE either from all logical partitions with the BCPii send permission or from a defined set of logical partitions. [Satisfies SFRs: FMT_MSA.1 (authorities), FDP_IFF.1, FIA_ATD.1]. It should be noted that in the evaluated configuration no partition has either the send or receive BCPii permission.

8.1.3.3 Audit and Accountability

The TOE implements a Security Log that is designed to always be enabled and contains a record of security relevant events. The View Security Log task allows an administrator to view the log recorded while the Archive Security Log task allows an administrator to create an archival copy of the security log. [satisfies SFRs : FAU_SAR.1]. The View Security Log task also allows an administrator to search or sort the security relevant events based on date or event criteria. [satisfies SFRs : FAU_SAR.3]. The log data assists an administrator in detection of potential attack or misconfiguration of the TOE security features.

The TOE will record in a security log the security-relevant actions of the administrator. [satisfies SFRs: FAU_GEN.1] These actions are:

i) Creating or modifying the IOCDS part of a configuration;
ii) Modifying the reconfigurable part of a configuration[1];
iii) Selecting a configuration to become the next current configuration;
iv) Installing a selected configuration by a power-on reset, or activation;
v) Activating or deactivating logical partitions.
vi) Logging on or off the console.

Further audit and accountability related properties are:

a) Each security log entry will be able to be associated with the identity of the administrator that caused the event. [satisfies SFRs: FAU_GEN.2].
b) Each security log entry contains a reliable timestamp. [satisfies SFRs: FPT_STM.1].
c) The TOE will help to prevent the deletion or modification of these audit records by any user, except when the allocated audit space has been filled. In this case, the system will prune the log to 67% of its maximum capacity. [satisfies SFRs: FAU_STG.1 and FAU_STG.4]. Note: When archiving security logs to removable media, the security log will be pruned to 20% of its capacity if the security log exceeds 20% of the audit storage capacity.
d) The TOE will help to prevent the reading of the security log by logical partitions. [satisfies SFRs : FAU_SAR.2]

8.1.3.4 Authorized Administration

The authority level specified when defining a new user determines the tasks made available to that user. The TOE supports five default administrative roles (see also section 1.5.2.4):

- Operator
- Advanced Operator
- Programmer
- Access Administrator
- Service Representative.

In addition to the predefined user roles supplied with the console the ability to define customized user roles is also provided. A user role is a collection of authorizations. A user role can be created to define the set of tasks allowed for a given class of user (task roles) or it can be created to define the set of managed objects that are manageable for a user (managed resource roles). A customized user role is based on one of the predefined user roles from which objects or tasks are removed.

An *administrator* is defined to be any user(s) with access to the HMC/SE workplace.

A *security administrator* is defined to be any *administrator* authorized to perform all of the following tasks:

[1] Note that modifying BCPii permissions is covered by this.

- Archive Security Logs
- Change LPAR Controls
- Change LPAR Group Controls
- Change LPAR I/O Priority Queuing
- Change LPAR Security
- Customize/Delete Activation Profiles
- Input/Output (I/O) Configuration
- Logical Processor Add
- Manage Users Wizard
- Reassign Channel Path
- System Details
- User Management
- View Security Logs

These capabilities allow an authorized administrator to effectively manage the TOE and its security functions in the following way:

a) The TOE will help to prevent access to the IOCDS part of a configuration by a user, unless IOCDS Write Protection is disabled AND the user is a security administrator AND, in the case of Standalone IOCP I/O Configuration Control is enabled. [Satisfies SFRs: FDP_ACC.2, FMT_MSA.1 (authorities, resource limits, candidate access), FMT_MTD.1, FMT_SMF.1, FMT_SMR.1]

b) The TOE will help to prevent access to the reconfigurable part of a configuration by a user unless
   i) the user is the security administrator, or
   ii) the user is a logical partition and:
      a) The logical partition has *cross-partition control authority* and the access is to deactivate or reset a logical partition; or
      b) The access is to deallocate storage or logical processor resources allocated to the partition itself; or
      c) The access is to allocate storage or logical processor resources to the partition itself.

   [Satisfies SFRs: FDP_ACF.1 (activation, allocation), FDP_ACC.2, FMT_SMF.1, FMT_MSA.1 (authorities, resource limits, candidate access), FMT_SMR.1]

8.1.3.5 Authorized Operations

The authority level specified when defining a new user determines the tasks made available to that user. This capability allows an authorized administrator to effectively operate the TOE and its security functions in the following way:

a) The TOE will help to ensure that only logical partitions in the current configuration are activated. Only activated partitions and the administrator will be permitted access to objects. [Satisfies SFRs: FDP_ACC.2, FIA_UID.2, FMT_MSA.1 (resource limits), FMT_SMR.1]

b) The TOE will help to ensure that logical processor is allocated exclusively to a single partition, and that the number of logical processors allocated to a partition does not exceed the limit specified in the current configuration. Once deallocated, a logical processor cannot be reallocated to another partition. [Satisfies SFRs: FDP_ACF.1 (allocation), FIA_ATD.1, FTA_TSE.1, FMT_MSA.1 (resource limits)]

c) The TOE will help to ensure that a storage resource is never shared, and that the amount of storage allocated to a logical partition does not exceed the limit specified in the current configuration. [Satisfies SFRs: FDP_ACC.2, FDP_ACF.1 (allocation), FDP_IFC.1, FIA_ATD.1, FPR_UNO.1, FTA_TSE.1, FMT_MSA.1 (resource limits)]

d) The TOE will help to ensure that at most one logical processor can execute on a physical processor at any given time. Processors from different partitions may be dispatched on the same processor at different times. [Satisfies SFR: FPR_UNO.1]

e) The TOE will help to prevent the transfer of a message between a logical partition and resources that are not allocated to it, except where the logical partition is explicitly authorized to do so. For example, PR/SM will intercept I/O interrupts that are not for the currently executing logical processor and will present them to the appropriate logical processor. [Satisfies SFRs: FDP_IFC.1, FPR_UNO.1, FDP_IFF.1]

8.1.3.6 Object Reuse

The TOE ensures that the contents of physical processors, storage or I/O utilized by different logical partitions will be cleared of any residual information before being utilized by the receiving logical partition.

a) The TOE will help to ensure the clearing of information from a storage resource before that resource is allocated to a logical partition. [Satisfies SFR: FDP_RIP.2]

b) The TOE will help to ensure that the information in a physical processor that is available to the currently executing logical processor is unaffected by any previously executing logical processor from another logical partition. For example, on a context switch, the control registers, general registers and program status word in the physical processor will be restored to their previously saved values. [Satisfies SFR: FPR_UNO.1, FDP_IFF.1]

c) The TOE will send a reset signal to a non-shared channel path and its attached I/O devices before that channel is allocated to a logical partition. [Satisfies SFR: FDP_RIP.2]

8.1.3.7 Reliability of Service

The TOE implements a Reset profile to define the initial operational characteristics of the physical processors. [Satisfies SFR: FMT_MSA.3] Two of the parameters in the Reset profile are the processor running time and wait completion. These parameters provide the ability to share physical processor resources on either an event-driven basis or a time-driven basis. Disabling event driven dispatching causes shared physical processor resources to be distributed on the basis of time intervals according to the weights specified to effectively prevent unauthorized denial of service.

a) The TOE will enable the utilization of a physical processor resource by a logical partition to be restricted. [Satisfies SFR: FRU_RSA.1]

b) The logical partition can be prevented from releasing allocated processor time, or from receiving more than a configurable proportion of processor time. [Satisfies SFR: FTA_TSE.1]

8.1.3.8 Self Test

The TOE implements a set of self-test functions that are executed when the TOE is started or reset [Satisfies SFR: FPT_TST.1], and periodically during normal execution. These functions help to ensure that critical hardware functions work properly [Satisfies SFR: FPT_STM.1] and that the TOE has not been tampered with when it was powered off. [Satisfies SFR: FPT_TST.1]

8.1.3.9 Alternate Support Element

The TOE implements functions that permit a quick switch to another Support Element when the primary Support Element has a hardware problem. Mirroring functions are performed on a regular basis to communicate any hard disk changes from the primary SE to the alternate SE [Satisfies SFR: FPT_TRC.1]. The Support Elements communicate using TCP/IP over a private Ethernet network. [Satisfies SFR: FPT_ITT.1]

8.2 TOE Assurance Measures

The assurance measures provided by the developer to meet the security assurance requirements for the TOE are based on the developer action elements and the requirements on content and presentation of evidence elements defined for the individual assurance requirements in CC Part 3:

SAR	Assurance Measures
ADV_ARC.1	The HLD and LLD documents provide a detailed description of the architecture of the TOE. Implementation at the source code level is provided to the evaluators on a need to know basis under a nondisclosure agreement. A companion document, the Correspondence document provides the path from the SFRs to the actual implementation for all components of the TOE. The *Trusted Facility Manual* ([TFM]) document provides guidance on initialization and startup procedures.
ADV_FSP.5	The specifications for the security functions of the TOE are documented in the [PRSMPG] Chapter 3 - Security Related Controls section. A detailed outline for complete exploitation of the TOE's security functions is found in the [PRSMPG]. Additional specifications and user information are provided in the *IOCP User's Guide* and the *HMC Operators Guide*. A companion document, the Correspondence document provides additional guidance showing how the various pieces of the implementation provide the necessary mutual support.
ADV_IMP.1	As a companion to the source code and HLD/LLD, the Correspondence Document associates each component of the Security Target with the corresponding functional specification, high-level design, and low-level design documentation. Modules noted in the section "LLD" are either in bold text or plain text. Bold text modules enforce the security aspects of the component. Plain text modules are required to support, but not enforce the component.
ADV_INT.2	The TOE internals are documented in proprietary internal documents. These documents provide a descriptive representation of the major structural elements of LPAR and the functions they provide. The documents further refine the structural elements into subsystems. The interrelationships of the subsystems are represented by flow diagrams.
ADV_TDS.4	PR/SM's modular design and component interactions are discussed in proprietary internal documents. An architectural description of each component is also provided.
AGD_OPE.1	The [TFM] provides the guidance required to insure a secure environment. All security parameters are described along with warnings about security settings that should be controlled in a secure processing environment. Additionally, full operational guidance is included in [HMCOPG].
AGD_PRE.1	The required guidance documentation is provided in the [TFM] which provides the necessary information regarding establishing the correct physical environment, how to prepare the system for secure operation, procedures on how to correctly initialize

SAR	Assurance Measures
	the TOE, and operational considerations to insure continued operation in conjunction with the security polity. Additional preparatory information is included in the [IMPP] and [IM] manuals.
ALC_CMC.4	Development of the z System is complex and performed by multiple developers. In this environment changes are controlled with the support of automated tools that handle numerous changes and only allow them to be performed by authorized developers. PR/SM development is performed according to an ISO certified process.
ALC_CMS.5	An internal document discusses the processes by which design documentation, test documentation and development tools are tracked. Change control as well as authorization control is also discussed.
ALC_DEL.1	The required documentation for initial TOE delivery is provided in the *Installation Manual – Physical Planning* and the *Install Guide* documents. Updates to the TOE once installed are provided through the release of new Engineering Change (EC) levels or via the Microcode Fix (MCF) process. The required guidance for the installation, generation and start-up procedures is provided in the [TFM] which provides the necessary information regarding establishing the correct physical environment, how to prepare the system for secure operation, procedures on how to correctly initialize the TOE, and operational considerations to insure continued operation in conjunction with the security polity.
ALC_DVS.1	The security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation are described in the *Site Security Manual*. Several sites of IBM (including for example the site in Poughkeepsie) have been subject to an analysis of the developer security measures in other evaluations. Where possible this evaluation will re-use the results of those evaluations.
ALC_FLR.3	Development within IBM has a well-defined system for reporting flaws and tracing the status of the corrective actions for those flaws. In addition, well-defined procedures exist for IBM's clients to report security problems via the IBM Support Center, and for IBM to distribute security fixes to clients, and clients can register with IBM to receive special notification of security flaws and fixes.
ALC_LCD.1	An internal proprietary document describes the process used to develop the TOE. This process represents the Incremental Model life cycle in which the product is designed, implemented, integrated and tested as a series of incremental builds.
ALC_TAT.3	Well-defined development tools are in place for the implementation of the TOE.
ATE_COV.2	The test suite used to verify the correct implementation of the TOE has been constructed to provide a one-to-one correspondence between individual tests and the specific security relevant functions of the TOE. In some cases, a test will cover more than one security function. This is due to the nature of some of these functions. (For example, many functions will also leave an audit trail and the test therefore includes the audit capability as well) Additionally, the execution and verification of the test suite will include validation of the correctness of the external interfaces of the TOE as they are necessary for the invocation, execution and completion of the individual tests.
ATE_DPT.3	Developers perform low-level testing whenever a new requirement is added into LPAR code.

SAR	Assurance Measures
ATE_FUN.2	An internal document contains test plans, procedural descriptions and the goal of the test. Test results from the execution of the tests demonstrate that each and every security function has been tested and the results show that they behaved as specified.
ATE_IND.2	By independent testing and repeating a subset of developer tests, the evaluator will gain confidence in the developer's testing effort and in the test results. All the required resources to perform their own independent tests will be provided to the evaluation facility. The evaluation facility will perform and document the tests they have created and performed as part of the evaluation technical report for testing.
AVA_VAN.5	All the required testing resources to perform thorough and complete testing will be provided. Independent test teams verify the integrity of various subsystems prior to inclusion in an overall driver. The drivers undergo an acceptance test to insure suitability for widespread system test and verification. An independent system test organization is responsible to insure that the TOE faithfully implements the stated design and functionality. A thorough and systematic analysis of the implementation of the TOE was conducted to identify potential vulnerabilities in each subsystem of the TOE. Each vulnerability was subsequently examined by the appropriate designers to determine: ● Existence of the theoretical vulnerability ● Method and feasibility of exploitation ● Estimate of the bandwidth. Additionally, testcases/handloops will be created to attempt to measure the bandwidths. The results of this work are documented in an internal document. The required guidance documentation is provided in the [TFM] which provides the necessary information regarding establishing the correct physical environment, how to prepare the system for secure operation, procedures on how to correctly initialize the TOE, and operational considerations to insure continued operation in conjunction with the security policy.

Table 12: Assurance measures meeting the TOE security assurance requirements

9 Abbreviations, Terminology and References

9.1 Abbreviations

BCPii
Base Control Program internal interface

CC
Common Criteria

CFCC
Coupling Facility Control Code

CHPID
Channel Path Identifier

CP
Central Processor

CPC
Central Processing Complex

CSS
Channel Subsystem

HMC
Hardware Management Console

ICF
Internal Coupling Facility

IFL
Integrated Facility for Linux

IOCDS
I/O Configuration Data Set

LIC
Licensed Internal Code

MCM
Multichip Module

PR/SM
Processor Resource/Systems Manager™

PU
Processor Unit

SAP
Assist Processor

SAR
Security Assurance Requirement

SE
Support Element

SFR
Security Functional Requirement

ST
Security Target

STP
Server Time Protocol

SVMM
Separation Virtual Machine Monitor

TKE
Trusted Key Entry

TOE
Target of Evaluation

zIIP
IBM zEnterprise Integrated Information Processor

9.2 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

activated
In this state, a logical partition can access system resources via SIE mode.

allocated
A partition may only use a resource that is allocated to it.

Assets
Information or resources to be protected by the countermeasures of a TOE.

attached
I/O devices are attached to control units, and control units are attached to channel paths. This connectivity is described in the IOCDS part of the configuration. I/O devices are considered to be attached to the channel paths to which their control units are attached.

Attack potential
The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.

audit log
See security log

audit record
An entry in the audit log.

Authentication data
Information used to verify the claimed identity of a user.

authorized
A logical partition may be authorized to perform certain tasks with security implications. The possible authorizations are:

- *I/O configuration control authority* - the partition can update any IOCDS which is not write protected
- *Global performance data control authority* - the partition can view CPU and Input/Output Processor busy data for all logical partitions
- *Cross-partition control authority* - the partition can issue system control instructions that affect other partitions, i.e. to reset or deactivate another partition.

Authorized user
A user who may, in accordance with the TSP, perform an operation.

BCPii
IBM provides Base Control Program internal interface (BCPii) support within z/OS that allows authorized applications to query, change, and perform operational procedures against the installed System z hardware base through a set of application program interfaces. These applications can access the System z hardware that the application is running on and extend their reach to other System z processors within the attached process control (Hardware Management Console) network.

candidate access
A channel path or I/0 device may only be allocated to a logical partition which has candidate access to it. The security administrator defines which partitions have access to which paths as part of the IOCDS. The IOCP User's Guide describes how the IOCDS is set up using the IOCP utility. In the IOCDS, the access list for each device defines which partitions have candidate access to the device. The initial access list and candidate access list for each channel path together define which partitions have candidate access to the channel path.

channel path
A channel resource which can be allocated to a logical partition. The static attributes of a channel include its type, which partitions have candidate access to it, and whether it is shared, reconfigurable or dedicated. The dynamic attributes of a channel include its current allocation to a partition, and whether it is online.

check-stopped
This state indicates that a physical or logical processor has been subject to an unrecoverable failure.

component
The smallest selectable set of elements that may be included in a PP, an ST, or a package.

configuration
A set of objects (logical partitions and resources) and the relationships between them. This consists of two exclusive parts: the static configuration held in the IOCDS, and the reconfigurable data. The IOCDS part of a configuration identifies the logical partitions, channel paths, control units, and IO devices in the system; their connectivity and characteristics; the candidate access restrictions and initial allocations for channel paths and IO devices; and whether channel paths are shared, reconfigurable or dedicated.
The reconfigurable part of a configuration identifies the number of logical processors, and storage resources that may be allocated to a logical partition; the actual allocation of resources; scheduling parameters; status information such as whether logical processors and channel paths are online or off-line; and whether logical partitions are authorized, isolated, activated or deactivated.
Note that a single object in a configuration may contain both static data from the IOCDS and reconfigurable data.

control unit
A physical unit which may be attached to one or more channel paths (in one or more partitions) and manages a number of I/O devices. A control unit is allocated to a partition if a channel path to which it is attached is allocated to the partition.

current configuration
The configuration that is currently being enforced by PR/SM.

deactivate
In this state, a logical partition is prevented from running, i.e. it is denied access to all objects.

dedicated
A dedicated channel path is ever allocated to only a single partition. A dedicated physical processor is used exclusively by a single partition while the logical processor executing on the dedicated processor is online and not check-stopped. (Note that the exclusivity is only between partitions: a dedicated processor is still shared with the PR/SM controlling code).

global performance partition
The logical partition that is given the authority to view the activity data for other logical partitions.

human user
Any person who interacts with the TOE.

I/O Configuration Data Set
This is a system file that defines the available logical partitions, and the allocation of the available the I/O devices to the defined logical partitions.

I/O device
A physical device that may be attached to one or more control units (on one or more channel paths). An I/O device is allocated to a partition if a control unit to which it is attached is allocated to the partition, and the partition has candidate access to the IO device.

identity
A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym

internal communication channel
A communication channel between separated parts of TOE.

internal TOE transfer object
Communicating data between separated parts of the TOE. An entity within the TSC that contains or receives information and upon which subjects perform operations.

isolated
When a partition is isolated, its non-shared channel paths remain allocated to the partition even when the channel path is off-line.

logical partition
A virtual machine which runs on the host system. It has a unique identifier (the zone number) and name. A logical partition can be both an object and a user of the system. A logical partition has attributes determining whether the logical partition is authorized for various actions. Other attributes define the amount of logical processor and storage resources to be allocated to the partition, and the scheduling parameters for the partition's processors. The possible logical partitions are defined in the current configuration object. Only activated logical partitions may use the system.

logical processor
A logical interface to a physical processor, which allows the physical resource to be shared. Each activated partition has at least one logical processor Logical processors are never shared. Allocation of logical processors occurs only at logical configuration activation. The number of logical processors can be altered. When the number of logical processors is decreased, an increment of dispatchability/parallelism is deleted from the partition in a manner that corresponds to varying a physical processor off-line in basic mode.

message
A flow of information, including requests, responses and indications. If a partition has the *cross-partition control authority* attribute, it can send out a message to reset/deactivate another partition. If a partition as Global Performance Data enabled, it can request performance data (CP utilization data and IOP busy data) for all logical partitions in the configuration.

object
An object is a passive entity in a computing system. Objects are subject to access control. In this document the term "object" can be used synonymously to "resource".

online/off-line
A logical processor or channel path may be configured online or off-line. A resource cannot be used while it is off-line.

partition scheduling parameters
These parameters consist of two values: Processor Running Time and Wait Completion. The processor running time is the length of continuous time allowed for the dispatch of a logical CP. The wait completion setting determines if shared CP resources are divided on either an event- driven basis or a time-driven basis.

physical processor
A processor resource which may be dedicated to a single partition or shared between partitions.

processor unit
This is the generic term for the z/Architecture processor on the Multichip Module (MCM) that can be characterized as a:

- Central Processor (CP) to be used by an operating system
- Internal Coupling Facility (ICF) to be used by the Coupling Facility Control Code (CFCC)
- Integrated Facility for Linux (IFL)
- Additional Assist Processors (SAPs) to be used by the Channel Subsystem (CSS)
- IBM zEnterprise Integrated Information Processor (zIIP)

profiles
Image profiles and reset profiles are utilized. Reset profiles are used to: Select LPAR mode of operation; Select an LPAR mode IOCDS; Optionally specify an LP activation sequence; Enable I/O Priority Queuing. Image Profiles are used to Define LP characteristics and optionally specify automatic load settings.

reconfigurable
Reconfigurable resource may be moved between partitions, but is allocated to at most one partition at any one time.

resource
An object that can be allocated to a logical partition, i.e. channel path, control unit, I/O device, storage, physical processor, logical processor.

role
A predefined set of rules establishing the allowed interactions between a user and the TOE

security log
security-relevant actions are recorded in a security log. The security log file is 30 megabytes in size and can hold records of varying sizes (100 bytes - 1 kilobytes). In a typical installation this would represent many weeks worth of activity. This is also referred to as the audit log.

shared
the resource may be allocated to more than one logical partition at once.

storage
Each activated partition has an initial allocation of central storage. It may also have an initial allocation of storage class memory. Both types of storage are individually contiguous. In some circumstances, further areas of storage, known as reserved central storage and reserved storage class memory, may also be identified. This storage is reserved for future allocation to, and use by, the partition.

subject
A subject is an active entity in a computing system. Subjects can access objects. Subjects act on behalf of users.

users
A user is the system's notion of a logical or physical (human) entity accessing and using the system. The users are the administrator and logical partitions.

write protected
The IOCDS part of a configuration cannot be modified by any partition if it is write protected.

9.3 References

CC **Common Criteria for Information Technology Security Evaluation**
Version 3.1R5
Date April 2017
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf

HMCOPG **Hardware Management Console Operations Guide**
Version HMC Online Documentation
Date 2017

IM **IBM 3906 Installation Manual All Models**
Version GC28-6964-00a
Date 2017

IMPP **IBM 3906 Installation Manual for Physical Planning**
Version GC28-6965-00b
Date 2017

PRSMPG **z Systems System Processor Resource/Systems Manager Planning Guide**
Version SB10-7169-00c
Date 2017

SO **IBM z14 Technical Guide**
Version SG24-8451-00
Date August 2017

TFM **Developing, building, and delivering a certified system - Appendix B of [PRSMPG]**
Version SB10-7169-00c
Date 2017