1 Introduction

This document contains three modules for CPU usage time.

These are:

- period-based scheduling, see page 5,
- priority-based scheduling, see page 17,
- CPU-affinity-based allocation (also referred to as CPU pinning), see page 28.

In a single-core system, CPU usage time is wall-clock time.

In a multicore system, CPU usage time *T* is two-dimensional, it is the product of the number *n* of CPU cores and the wall-clock time *t*, i.e. $T = t * n$. In these systems *T* can be allocated according to the three different techniques listed above.

Each of these is described by a separate PP module. An ST-author must choose at least one of these PP modules, but can also choose any combination (that is any two or three modules) if the system uses a combination of the scheduling techniques.

Application note: If applicable, the ST author shall mention that time is needed for CPU reallocation itself (“jitter”) in the ST. If applicable, the ST author shall mention that also the sharing of other resources between different partitions may lead to jitter and/or blocking effects.

The following subsections describe these different techniques in terms of examples and how they may be combined.

1.1 Period-Based Scheduling

In the period based scheduling technique a period consisting of windows is repeated invariably.

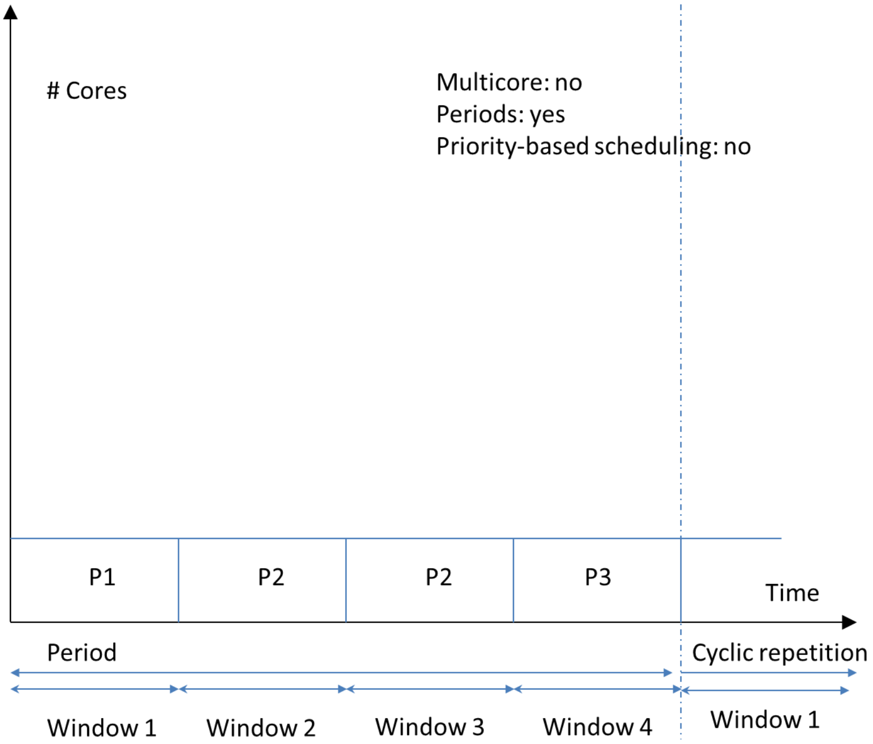

Figure 1: Period-based scheduling. P1 to P3 denote the three different partitions running on the SK in this example.

Figure 1 shows the example of a system with just one core, where the period (major time frame) is repeated with cyclic periodicity. This means that after the first time period has passed the scheduling starts again as from the beginning with Window 1. In each period, the first time window is assigned to partition P1, two subsequent periods are assigned to partition P2, and the last period is assigned to partition P3.

1.2 Priority-Based Scheduling

This kind of scheduling technique is based on priorities assigned to partitions or application processes within partitions. In the latter case, the partitions inherit the priority of their application processes and the partitions are scheduled according to that priority.

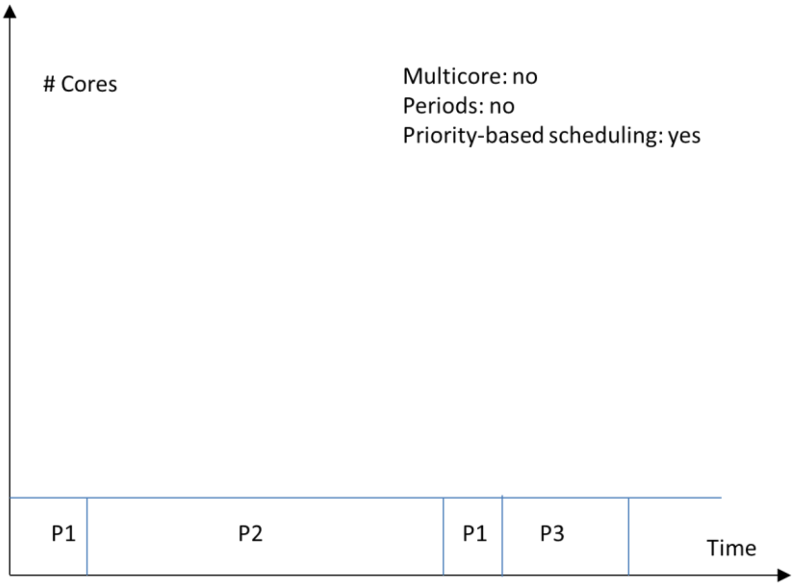

Figure 2: Priority-based scheduling.

Figure 2 shows a system with one core on which CPU time is assigned via priority-based scheduling. In the example partitions P1, P2, and P3 are scheduled according to their priority. This kind of scheduling only can be used in a security context in configurations where untrusted partitions have a lower priority than trusted partitions.

1.3 CPU-affinity Based Allocation

This kind of CPU allocation uses fixed CPU affinities, which do not vary over time.

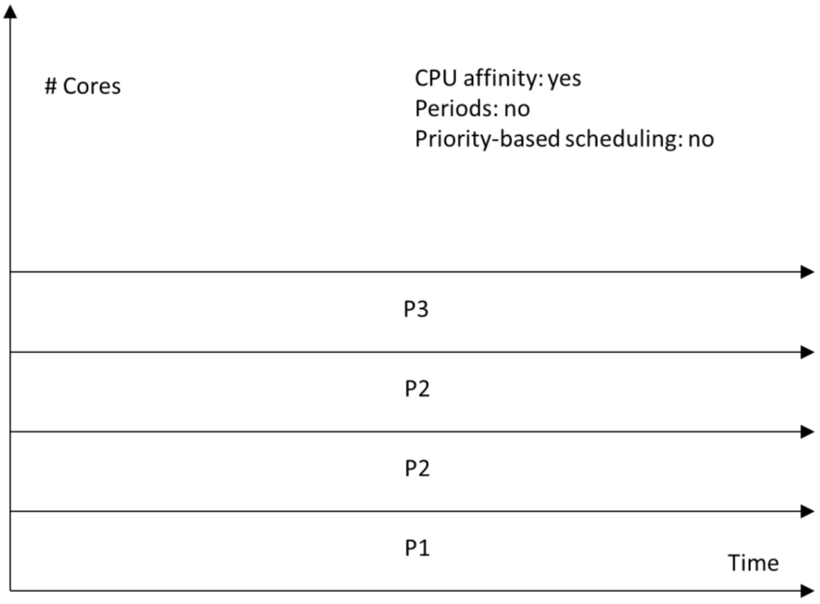

Figure 3: CPU-affinity-based allocation.

Figure 3 shows a system with four cores on which CPU time is assigned by CPU-affinity allocation. In the example partition P1 is assigned to core #1, P2 is assigned to cores #2 and #3, P3 is assigned to core #4.

1.4 Combinations of Different Scheduling Mechanisms

Any combination of period-based, priority-based scheduling and CPU-affinity-based allocations is possible.

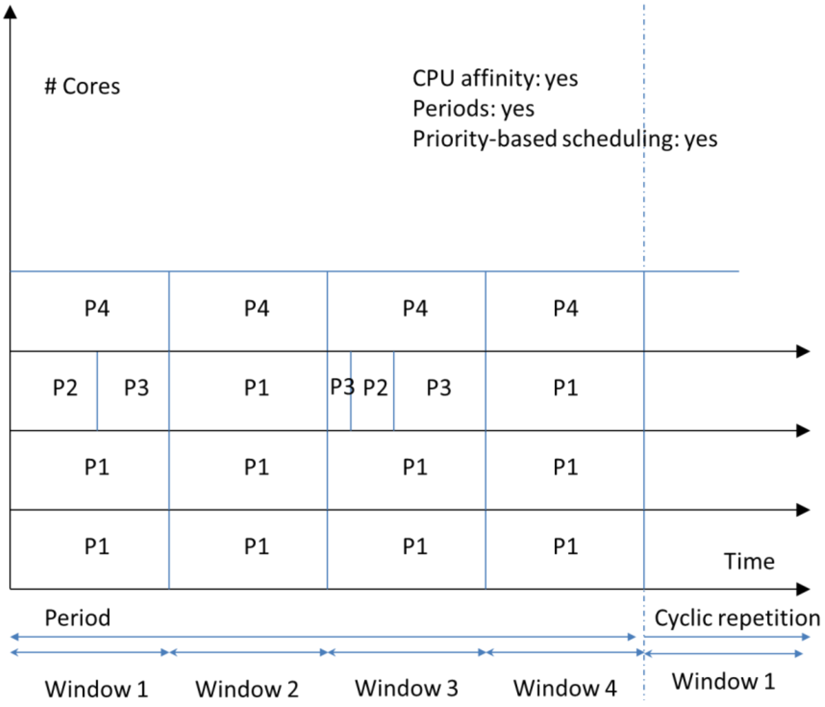

Figure 4: Possible combination of CPU-affinity allocation, period-based and priority-based scheduling.

Figure 4 shows an example for a system with four cores, which are assigned by CPU-affinity allocation. In the example configuration partition P1 is assigned exclusively to cores #1 and #2, Partition P4 is assigned to core #4. Core 3 periodically switches between two regimes: P2 and P3 share the same windows (Window 1 and Window 3), within these windows, priority-based scheduling is applied to decide whether P2 or P3 is scheduled. Core 3 has also Window 2 and Window 4 assigned to P1. As P1 is exclusively assigned this window on core 3, there is no priority-based scheduling in this case.

Period-based scheduling module

Chapter 1 Introduction

This section identifies the PP module as well as the base PP and provides a Module overview for potential users.

1.1 PP Module Reference

Title: MILS Platform Protection Profile Period-based scheduling module
Sponsor: certMILS Consortium
CC Version: 3.1 (Revision 5)
Assurance Level: see the base PP.
Version: draft
Keywords: Base PP, PP Module, Operating System, Separation Kernel, MILS

1.2 Base PP Identification

Base MILS Platform Protection Profile, Version: 1.0.

1.3 PP Module Overview

This PP module supplements the base PP by specifying functions associated with the time separation implemented by Separation Kernels using period-based scheduling.

Chapter 2 Consistency Rationale

This section states the correspondence between the PP module and its base PP.

2.1 TOE Type Consistency

The TOE type for which both the base PP and this PP module are designed is “a special kind of operating system, namely a Separation Kernel (SK).”

An SK is a special kind of operating system that allows to effectively separate different containers called “partitions” from each other. Applications themselves are hosted in those partitions. They can also be entire operating systems. The SK is installed and runs on a hardware platform (e.g. embedded systems, desktop class hardware).

The PP module extends the base PP by specifying one of several different alternatives for covering the CPU time allocation. All PP configurations, consisting of the base PP and any individual CPU time module or any of the combinations thereof maintain that the role integrating the TOE in a product has a means to control the assignment of CPU time to partitions.

Application Note: This module can be combined with the priority-based scheduling module, e.g. in order to describe a two-level scheduler that first assigns periods and then allows priority-based scheduling within those periods. This module can be combined with the CPU affinity module in order to assign CPUs to partitions, e.g. globally by a CPU affinity attribute of each partition or each application. It can be combined with both modules e.g. to describe a two-level scheduler in a system that also implements CPU affinity.

2.2 Security Problem Definition Consistency

The security problem definition as defined in the CPU time PP modules brings no modifications to the SPD defined in the base PP. Then, all assets, threats, organisational security policies and assumptions remain with no changes.

2.3 Security Objectives Consistency

The security objectives as defined in the CPU time PP modules brings no modifications to the security objectives defined in the base PP.

2.4 Security Functional Requirements Consistency

In addition to the set of SFRs included in the base PP, this PP module defines:

- FRU_RSA.1/TIME Maximum quotas - This SFR is compatible with the set of SFRs defined in the base PP as it adds independent functionality regarding maximum quotas of CPU time that a partition can use.

Chapter 3 Conformance Claim

This protection profile module claims conformance to

- Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1, Revision 5. April 2017. CCMB-2017-04-001 [1]
- Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components. Version 3.1, Revision 5. April 2017. CCMB-2017-04-002 [2]
- Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components. Version 3.1, Revision 5. April 2017. CCMB-2017-04-003 [3]

as follows

- Part 2 conformant.

The "Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 5, April 2017. CCMB-2017-04-004, [4]" has to be taken into account.

This PP module is associated with the Base MILS Platform Protection Profile Version 1.0.

3.1 Conformance Rationale

Since a PP module cannot claim conformance to any PP, this section is not applicable.

3.2 Conformance Statement

This PP module requires strict conformance of any ST or PP claiming conformance to this PP module.

Note: claiming conformance to this PP module also requires claiming conformance to the Base MILS Platform Protection Profile.

Chapter 4 Security Problem Definition

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

- Known and presumed threats countered by either the TOE or by the security environment.
- Organizational security policies with which the TOE must comply.
- Assumptions about the secure usage of the TOE.

4.1 Assets

The asset relevant to this module is CPU time (AS.TIME) defined in the base PP.

4.2 Threats

A threat agent is an active subject within an untrusted partition.

T.DEPLETION

By consuming CPU time, an attacker makes these resources unavailable to the TOE itself and/or to trusted subjects and/or to other untrusted subjects.

4.3 Organizational Security Policies

This module defines no organizational security policies.

4.4 Assumptions

The assumptions are the same as in the base PP.

Chapter 5 Security Objectives

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

This section presents the solution to the security problem in terms of objectives for the TOE and its operational environment.

5.1 Security Objectives for the TOE

OT.AVAILABILITY

The TOE shall preserve the availability of CPU time.

5.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are the same as for the base TOE.

5.3 Security Objectives Rationale

	OT.AVAILABILITY
T.DEPLETION	X

Table 1: Security Objectives Rationale

T.DEPLETION is countered directly by **OT.AVAILABILITY** as the TOE will actively keep the resources operation alive and available for partitions using them.

Chapter 6 Extended Components Definition

This module does not define any extended component.

Chapter 7 Security Requirements

This section defines the Security Functional Requirements (SFRs) in relationship with the set of TOE security objectives in the PP module and with the security functional requirements of the base PP. This PP module does not introduce specific assurance requirements. The assurance requirements are defined by the Base MILS Platform Protection Profile.

FRU_RSA.1/TIME Maximum Quotas

FRU_RSA.1.1/TIME The TSF shall enforce maximum quotas of the following resources [CPU time] that [selection: individual user, defined group of users, subjects] can use [selection: simultaneously, over a specified period of time].

7.1 Security Requirements Rationale

Table 2 shows the coverage of the security objectives by the SFRs.

	OT.AVAILABILITY
FRU_RSA.1/TIME Maximum quotas	X

Table 2: SFR Rationale

OT.AVAILABILITY

The SFR FRU_RSA.1 maximum quotas service meets OT.AVAILABILITY by ensuring that CPU time is assigned to partitions as configured.

7.2 Security Functional Requirements Dependencies Analysis

The following dependencies are defined for the SFRs used in this PP module:

SFR	Dependencies	Satisfied?
FRU_RSA.1/TIME	None	N/A

Chapter 8 Application Notes

The functionality shall be implemented in a manner that the operative system executes the periods within the defined time constraints. Otherwise the TOE could fail. These time constraints depend of the application type. For example, regarding industrial control systems (ICS) of electrical networks, the response time shall be in the order of millisecond. This module defines reactivity that is based on period-based scheduling.

Note that the chosen SFR FRU_RSA.1 is only to ensure maximum quotas, not minimum quotas. This is because fixed minimum quotas are not feasible if period-based scheduling is combined with priority-based scheduling. Yet, an ST author can also choose to use FRU_RSA.2 for minimum quotas if applicable.

Chapter 9 List of Abbreviations

Abbreviation	Translation
CC	Common Criteria
HW	Hardware
OS	Operating System
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SK	Separation Kernel
SW	Software

Chapter 10 Bibliography

[1] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1, Revision 5. April 2017. CCMB-2017-04-001

[2] Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components. Version 3.1, Revision 5. April 2017. CCMB-2017-04-002

[3] Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components. Version 3.1, Revision 5. April 2017. CCMB-2017-04-003

[4] Common Criteria for Information Technology Security Evaluation. Evaluation Methodology. Version 3.1, Revision 5. April 2017. CCMB-2017-04-004

Priority-based scheduling module

Chapter 1 Introduction

This section identifies the PP module as well as the base PP and provides a Module overview for potential users.

1.1 PP Module Reference

Title: MILS Platform Protection Profile Priority-based scheduling module
Sponsor: certMILS Consortium
CC Version: 3.1 (Revision 5)
Assurance Level: see the base PP.
Version: draft
Keywords: Base PP, PP Module, Operating System, Separation Kernel, MILS

1.2 Base PP Identification

Base MILS Platform Protection Profile, Version: 1.0.

1.3 PP Module Overview

This PP module supplements the base PP by specifying functions associated with the time separation implemented by Separation Kernels using priority-based scheduling.

Chapter 2 Consistency Rationale

This section states the correspondence between the PP module and its base PP.

2.1 TOE Type Consistency

The TOE type for which both the base PP and this PP module are designed is “a special kind of operating system, namely a Separation Kernel (SK).”

An SK is a special kind of operating system that allows to effectively separate different containers called “partitions” from each other. Applications themselves are hosted in those partitions. They can also be entire operating systems. The SK is installed and runs on a hardware platform (e.g. embedded systems, desktop class hardware).

The PP module extends the base PP by specifying one of several different alternatives for covering CPU time allocation. All PP configurations, consisting of the base PP and any individual CPU time module or any of the combinations thereof maintain that the role integrating the TOE in a product has a means to control the assignment of CPU time to partitions.

Application Note: This module can be combined with the period-based scheduling module, e.g. in order to describe a two-level scheduler that first assigns periods and then allows priority-based scheduling within those periods. This module can be combined with the CPU affinity module in order to assign CPUs to partitions, e.g. globally by a CPU affinity attribute of each partition or each application. It can be combined with both modules e.g. to describe a two-level scheduler in a system that also implements CPU affinity.

2.2 Security Problem Definition Consistency

The security problem definition as defined in the real time PP modules brings no modifications to the SPD defined in the base PP. Then, all assets, threats, organisational security policies and assumptions remain with no changes.

2.3 Security Objectives Consistency

The security objectives as defined in the real time PP modules brings no modifications to the security objectives defined in the base PP.

2.4 Security Functional Requirements Consistency

In addition to the set of SFRs included in section 6.1 of the base PP, this PP module defines:

- FRU_PRS.1 Limited Priority of Service – This SFR is compatible with the set of SFRs defined in the base PP as it adds independent functionality regarding priority of service access to CPU time by partitions.

Chapter 3 Conformance Claim

This protection profile module claims conformance to

- Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1, Revision 5. April 2017. CCMB-2017-04-001 [1]
- Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components. Version 3.1, Revision 5. April 2017. CCMB-2017-04-002 [2]
- Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components. Version 3.1, Revision 5. April 2017. CCMB-2017-04-003 [3]

as follows

- Part 2 conformant.

The "Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 5, April 2017. CCMB-2017-04-004, [4]" has to be taken into account.

This PP module is associated with the Base MILS Platform Protection Profile Version 1.0.

3.1 Conformance Rationale

Since a PP module cannot claim conformance to any PP, this section is not applicable.

3.2 Conformance Statement

This PP module requires strict conformance of any ST or PP claiming conformance to this PP module.

Note: claiming conformance to this PP module also requires claiming conformance to the Base MILS Platform Protection Profile.

Chapter 4 Security Problem Definition

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

- Known and presumed threats countered by either the TOE or by the security environment.
- Organizational security policies with which the TOE must comply.
- Assumptions about the secure usage of the TOE.

4.1 Assets

The asset relevant to this module is CPU time (AS.TIME) defined in the base PP.

4.2 Threats

A threat agent is an active subject within an untrusted partition.

T.DEPLETION

By consuming CPU time, an attacker makes these resources unavailable to the TOE itself and/or to trusted subjects and/or to other untrusted subjects.

4.3 Organizational Security Policies

This module defines no organizational security policies.

4.4 Assumptions

The assumptions are the same as in the base PP.

Chapter 5 Security Objectives

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

This section presents the solution to the security problem in terms of objectives for the TOE and its operational environment.

5.1 Security Objectives for the TOE

OT.AVAILABILITY

The TOE shall preserve the availability of CPU time.

5.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are the same as for the base TOE.

5.3 Security Objectives Rationale

	OT.AVAILABILITY
T.DEPLETION	X

Table 3: Security Objectives Rationale

T.DEPLETION is countered directly by **OT.AVAILABILITY** as the TOE will actively keep the resources operation alive and available for partitions using them.

Chapter 6 Extended Components Definition

This module does not define any extended component.

Chapter 7 Security Requirements

This section defines the Security Functional Requirements (SFRs) in relationship with the set of TOE security objectives in the PP module and with the security functional requirements of the base PP. This PP module does not introduce specific assurance requirements. The assurance requirements are defined by the Base MILS Platform Protection Profile.

7.1 Security Functional Requirements

FRU_PRS.1 Limited Priority of Service

FRU_PRS.1.1 The TSF shall assign a priority to each subject in the TSF.

FRU_PRS.1.2 The TSF shall ensure that each access to CPU time shall be mediated on the basis of the subjects assigned priority.

7.2 Security Requirements Rationale

Table 2 shows the coverage of the security objectives by the SFRs.

	OT.AVAILABILITY
FRU_PRS.1 Limited priority of service	X

Table 4: SFR Rationale

OT.AVAILABILITY

The SFR FRU_PRS.1 limited priority of service meets OT.AVAILABILITY by ensuring that the CPU time is made available to partitions based on priorities.

7.3 Security Functional Requirements Dependencies Analysis

The following dependencies are defined for the SFRs used in this PP module:

SFR	**Dependencies**	**Satisfied?**
FRU_PRS.1	None	Yes

Chapter 8 Application Notes

The functionality shall be implemented in a manner that the operative system executes the highest priority tasks within the defined time constraints. Otherwise the TOE could fail. These time constraints depend of the application type. For example, regarding industrial control systems (ICS) of electrical networks, the response time shall be in the order of millisecond. This module defines reactivity that is based on priority-based scheduling.

Chapter 9 List of Abbreviations

Abbreviation	Translation
CC	Common Criteria
HW	Hardware
OS	Operating System
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SK	Separation Kernel
SW	Software

Chapter 10 Bibliography

[1] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1, Revision 5. April 2017. CCMB-2017-04-001

[2] Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components. Version 3.1, Revision 5. April 2017. CCMB-2017-04-002

[3] Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components. Version 3.1, Revision 5. April 2017. CCMB-2017-04-003

[4] Common Criteria for Information Technology Security Evaluation. Evaluation Methodology. Version 3.1, Revision 5. April 2017. CCMB-2017-04-004

CPU affinity module

Chapter 1 Introduction

This section identifies the PP module as well as the base PP and provides a Module overview for potential users.

1.1 PP Module Reference

Title: MILS Platform Protection Profile CPU affinity module
Sponsor: certMILS Consortium
CC Version: 3.1 (Revision 5)
Assurance Level: see the base PP.
Version: draft
Keywords: Base PP, PP Module, Operating System, Separation Kernel, MILS

1.2 Base PP Identification

Base MILS Platform Protection Profile, Version: 1.0.

1.3 PP Module Overview

This PP module supplements the base PP by specifying functions associated with the time separation implemented by Separation Kernels using CPU-affinity-based allocation.

Chapter 2 Consistency Rationale

This section states the correspondence between the PP module and its base PP.

2.1 TOE Type Consistency

The TOE type for which both the base PP and this PP module are designed is “a special kind of operating system, namely a Separation Kernel (SK).”

An SK is a special kind of operating system that allows to effectively separate different containers called “partitions” from each other. Applications themselves are hosted in those partitions. They can also be entire operating systems. The SK is installed and runs on a hardware platform (e.g. embedded systems, desktop class hardware).

The PP module extends the base PP by specifying one of several different alternatives for covering CPU time allocation. All PP configurations, consisting of the base PP and any individual CPU time module or any of the combinations thereof maintain that the role integrating the TOE in a product has a means to control the assignment of CPU time to partitions.

Application Note: This module can be combined with the period-based scheduling module to indicate that the CPU affinity mechanism is combined with period-based scheduling. This module can be combined with the priority-based scheduling module to indicate that the CPU affinity mechanism is combined with priority-based scheduling. It can be combined with both modules e.g. to describe a two-level scheduler using both period-based and priority-based scheduling in a system that also implements CPU affinity.

2.2 Security Problem Definition Consistency

The security problem definition as defined in the real time PP modules brings no modifications to the SPD defined in the base PP. Then, all assets, threats, organisational security policies and assumptions remain with no changes.

2.3 Security Objectives Consistency

The security objectives as defined in the real time PP modules brings no modifications to the security objectives defined in the base PP.

2.4 Security Functional Requirements Consistency

In addition to the set of SFRs included in section 6.1 of the base PP, this PP module defines:

- FDP_ACC.2/AFFIN Complete Access Control – Access to Virtual Network Interfaces – This SFR is compatible with the set of SFRs defined in the base PP as it adds an independent access control policy to CPU cores.
- FDP_ACF.1/AFFIN Security Attribute Based Access Control – Access to Virtual Network Interfaces – This SFR is compatible with the set of SFRs defined in the base PP as it adds an independent access control policy to CPU cores.
- FMT_MSA.1/AFFIN Management of Security Attributes – This SFR is compatible with the set of SFRs defined in the base PP as it adds independent and specific functionality for managing the security attributes of the new access control policy. This SFR must be iterated when used with the base PP.

- FMT_MSA.3/AFFIN Static attribute initialisation This SFR is compatible with the set of SFRs defined in the base PP as it adds independent and specific functionality for initialising the security attributes of the new access control policy. This SFR must be iterated when used with the base PP.

Chapter 3 Conformance Claim

This protection profile module claims conformance to

- Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1, Revision 5. April 2017. CCMB-2017-04-001 [1]
- Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components. Version 3.1, Revision 5. April 2017. CCMB-2017-04-002 [2]
- Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components. Version 3.1, Revision 5. April 2017. CCMB-2017-04-003 [3]

as follows

- Part 2 conformant.

The "Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 5, April 2017. CCMB-2017-04-004, [4]" has to be taken into account.

This PP module is associated with the Base MILS Platform Protection Profile Version 1.0.

3.1 Conformance Rationale

Since a PP module cannot claim conformance to any PP, this section is not applicable.

3.2 Conformance Statement

This PP module requires strict conformance of any ST or PP claiming conformance to this PP module.

Note: claiming conformance to this PP module also requires claiming conformance to the Base MILS Platform Protection Profile.

Chapter 4 Security Problem Definition

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

- Known and presumed threats countered by either the TOE or by the security environment.
- Organizational security policies with which the TOE must comply.
- Assumptions about the secure usage of the TOE.

4.1 Assets

The asset relevant to this module is CPU time (AS.TIME) defined in the base PP.

4.2 Threats

A threat agent is an active subject within an untrusted partition.

T.DEPLETION

By consuming CPU time, an attacker makes these resources unavailable to the TOE itself and/or to trusted subjects and/or to other untrusted subjects.

4.3 Organizational Security Policies

This module defines no organizational security policies.

4.4 Assumptions

The assumptions are the same as in the base PP.

Chapter 5 Security Objectives

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

This section presents the solution to the security problem in terms of objectives for the TOE and its operational environment.

5.1 Security Objectives for the TOE

OT.AVAILABILITY

The TOE shall preserve the availability of CPU time.

5.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are the same as for the base TOE.

5.3 Security Objectives Rationale

	OT.AVAILABILITY
T.DEPLETION	X

Table 5: Security Objectives Rationale

T.DEPLETION is countered directly by **OT.AVAILABILITY** as the TOE will actively keep the resources operation alive and available for partitions using them.

Chapter 6 Extended Components Definition

This module does not define any extended component.

Chapter 7 Security Requirements

This section defines the Security Functional Requirements (SFRs) in relationship with the set of TOE security objectives in the PP module and with the security functional requirements of the base PP. This PP module does not introduce specific assurance requirements. The assurance requirements are defined by the Base MILS Platform Protection Profile.

7.1 Security Functional Requirements

FDP_ACC.2/AFFIN Complete Access Control –CPU Core Access Control

FDP_ACC.2.1/AFFIN: The TSF shall enforce the [**CPU core access control policy**] on [**subjects: partitions, objects: CPU cores**] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2/AFFIN: 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.

FDP_ACF.1/AFFIN Security Attribute Based Access Control – CPU Core Access Control

FDP_ACF.1.1/AFFIN: The TSF shall enforce the [**CPU core access control policy**] to objects based on the following: [**subjects: partitions, objects: CPU cores, security attributes: partition ID, CPU cores of the partition in the configuration**].

FDP_ACF.1.2/AFFIN: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- **The partition PA can run a thread on CPU core C if [describe how the policy to do this is defined**].

FDP_ACF.1.3/AFFIN: The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [list of additional rules, if any].

FDP_ACF.1.4/AFFIN: The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [list of additional rules, if any].

FMT_MSA.1/AFFIN Management of Security Attributes

FMT_MSA.1.1/AFFIN The TSF shall enforce the [**CPU core access control policy**] to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorised entity].

FMT_MSA.3/AFFIN Static attribute initialisation

FMT_MSA.3.1/AFFIN The TSF shall enforce the [**CPU core access control policy**] to provide [selection: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/AFFIN The TSF shall allow the [**no-one**] to specify alternative initial values to override the default values.

7.2 Security Requirements Rationale

Table 2 shows the coverage of the security objectives by the SFRs.

	OT.AVAILABILITY
FDP_ACC.2/AFFIN	X
FDP_ACF.1/AFFIN	X
FMT_MSA.1/AFFIN	X
FMT_MSA.3/AFFIN	X

Table 6: SFR Rationale

OT.AVAILABILITY

The SFR FDP_ACF.1/AFFIN ensures that partitions are pinned to CPU cores.

7.3 Security Functional Requirements Dependencies Analysis

The following dependencies are defined for the SFRs used in this PP module:

SFR	Dependencies	Satisfied?
FDP_ACC.2/AFFIN	FDP_ACF.1	yes (FDP_ACF.1/AFFIN)
FDP_ACF.1/AFFIN	FDP_ACC.1	yes (FDP_ACC.2/AFFIN)
FMT_MSA.3/AFFIN	[FDP_ACC.1 or FDP_IFC1] FMT_MSA.1 FMT_SMR.1	yes (FDP_ACC.2/AFFIN) yes N – The TOE does not implement roles. The entities accessing the resources are trusted partitions that do not play different roles in the access to such resources.
FMT_MSA.1/AFFIN	FMT_SMR.1 FMT_SMF.1	N – The TOE does not implement roles. The entities accessing the resources are trusted partitions that do not play different roles in the access to such resources. base PP

Chapter 8 Application Notes

The functionality shall be implemented in a manner that the operative system executes the highest priority tasks within the defined time constraints. Otherwise the TOE could fail. These time constraints depend of the application type. For example, regarding industrial control systems (ICS) of electrical networks, the response time shall be in the order of millisecond. This module defines reactivity that is based on exclusively assigning partitions to CPU cores. This module only can be meaningfully used in a system with more than one CPU core (“multicore” system).

Chapter 9 List of Abbreviations

Abbreviation	Translation
CC	Common Criteria
HW	Hardware
OS	Operating System
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SK	Separation Kernel
SW	Software

Chapter 10 Bibliography

[1] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1, Revision 5. April 2017. CCMB-2017-04-001

[2] Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components. Version 3.1, Revision 5. April 2017. CCMB-2017-04-002

[3] Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components. Version 3.1, Revision 5. April 2017. CCMB-2017-04-003

[4] Common Criteria for Information Technology Security Evaluation. Evaluation Methodology. Version 3.1, Revision 5. April 2017. CCMB-2017-04-004