Partition OS Safety Concept

Version 1.00
Created on Dec 25, 2012

株式会社ヴィッツ
名古屋市中区栄 1-13-1 白川第 2 ビル
2F・7F

承認	審査	作成

EDITION	DATE OF CHANGE	REVISION REASON	CREATED BY	AFFILIATION
Version 0.01	2010/10/25	New document	Hara	Witz Inc.
Version 0.10	2011/02/14	modification on the basis of comment from TUV	Hara	Witz Inc.
Version 0.11	2011/04/20	modification on the basis of comment from TUV Review Report	Honda	Nagoya Univ.
Version.0.2	2011/09/13	modification on the basis of comment from TUV	Honda	Nagoya Univ.
Version.0.30	2011/09/24	modification on the basis of comment from TUV	Honda	Nagoya Univ.
Version 0.31	2012/01/20	Modification on the basis of meeting with TUV	Hara	Nagoya Univ.
Version 0.4	2012/06/12	Modification on the basis of TUV review report of the ParOS 2011 Add new profile BCC+.	Honda	Nagoya Univ.
Version 0.5	2012/09/13	Modification on the basis of TUV review report of the ParOS 2012/7	Honda	Nagoya Univ.
Version 0.6	2012/09/18	Modification on the basis of comment from TUV meeting at 2012/9/18	Honda	Nagoya Univ.
Version 0.61	2012/09/19	Modification on the basis of comment from TUV meeting at 2012/9/19	Honda	Nagoya Univ.
Version 0.62	2012/10/18	Add “Partition exception handler” to Table 5.4 conformance class	Hara	Witz Inc.
Version 1.00	2012/12/25	Release	Hara	Witz Inc.

目次

1 概要

本書は、パーティショニング機能を搭載したリアルタイムオペレーティングシステムである"Partitioning Operating System(ParOS)"の安全コンセプトについて記載する。

ParOS の適用システムから要求されるパーティショニング要求を 4 レベルに分類し、この要求に対する ParOS のパーティショニング機能について説明する。

1.1 ParOS目的

ParOS は、自動車、移動支援ロボット、介護ロボット、航空宇宙（飛行機、ロケット）等の高い信頼性が求められ、性質の異なる複数のアプリケーションを単一コンピュータシステム上で実行する必要のあるシステムを対象としている。

1.2 タグ

Safety Goal や機能要求に対して以下の様にタグを付加する。[module]には対象とする ParOS のモジュール名が入る。モジュール名は、 Exective、SafeOS、COM、HW がある。各モジュールについては後述する。

表 1.1 タグの一覧

タイプ	タグ
Safety Goal	【SG-xx】
Functional Requirement	【[module]:FR-xx】
Safety Requirement	【[module]:SR-xx】
Safety Integrity Requirement	【[module]:SIR-xx】

1.3 関連文書

Reference ID	Title	Revision	Data
[IEC]	IEC 61508:2010 Edition 2.0 Part1-7	2.0	2010/04
[ISO]	ISO 26262:2011 Part10	First	2011/11/15
[SafeOS_SC]	Safe OS Safety Concept	0.90	2009/12/09
[SafeOS_SRS]	Safe OS Software Safety Requirement Specification	0.90	2010/01/13
[SafeOS_SA]	Safe OS Safety Analysis	0.90	2009/12/10
	Safe OS Safety Analysis(detail)	0.90	2009/03/24
[SafeOS_SM]	Safe OS Safety Manual	1.00	2010/02/12
[ParOS_SRS]	Partition OS Safety Requirement Specification	1.00	2012/12/25
[ParOS_SA]	Partition OS Safety Requirements Analysis Plan And Results Report	1.00	2012/12/25
	Partition OS Safety Requirement Analysis Result Report(detail)	1.00	2012/12/25
[ParOS_SM]	Partition OS Safety Manual	1.00	2012/12/25
[WITZ_S]	Function Safety Management Standard	2.3.0	2012/01/16

2　ParOSの対象システムとParOSの一般機能

本章では以下の内容ついて述べる。

・ParOS の対象（想定）システム

・ParOS の基本機能（安全機能は含まない）

・ParOS の基本機能の故障モード

図 2.2に、”ParOSの対象（想定）システム(Assumption system(user) requiment)”、”ParOSの基本機能（安全機能は含まない）(Abstract Level ParOS function)”、”ParOSの基本機能の故障モード(Failure Mode for Abstract Level ParOS functions)”の関係を示す。

“Safety Goal”については、3 章で述べる。”安全要求（Top Level Safety Requirement）”は、5 章で述べる。

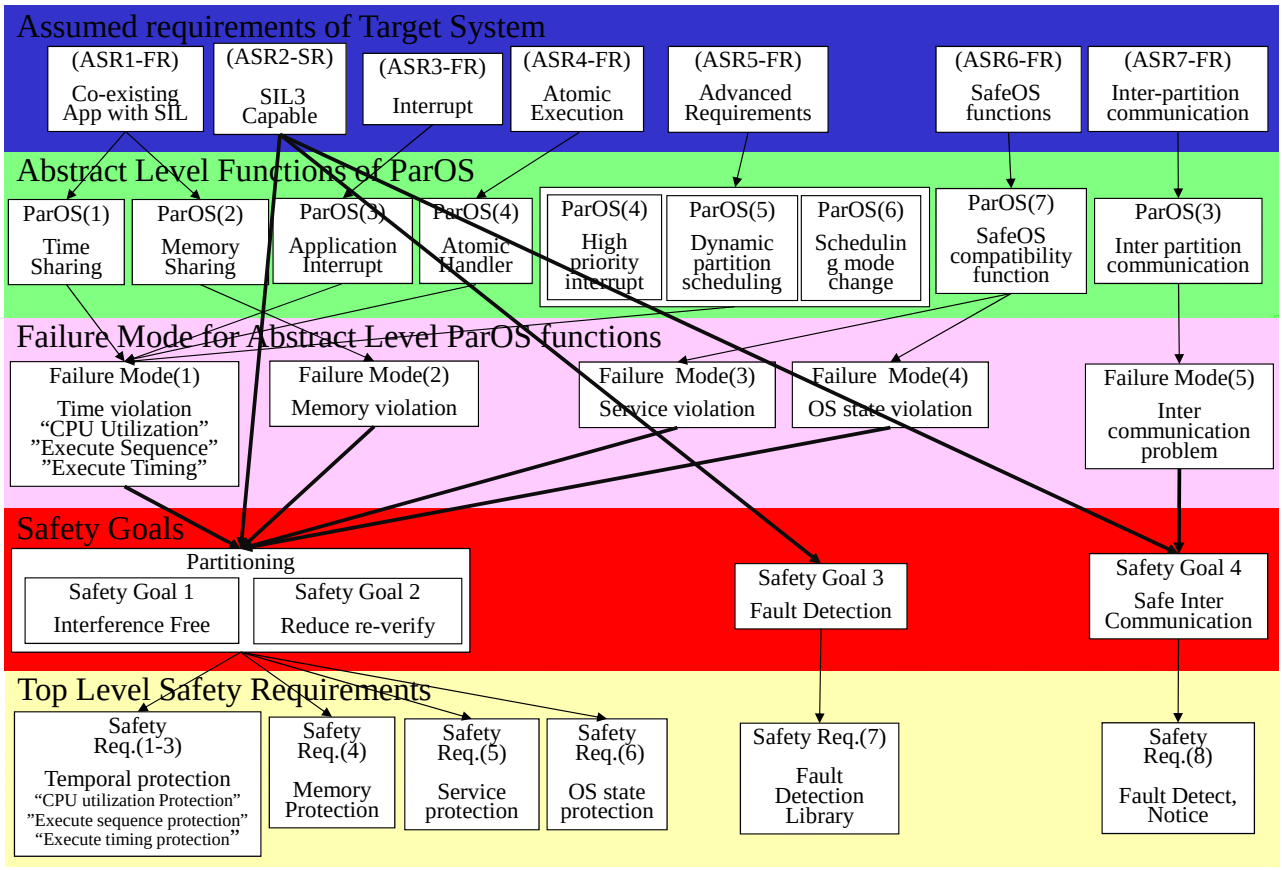


図 2.1 ParOS の対象システムの要求、ParOS の基本機能、ParOS の故障モード、ParOS の Safety Goal、安全要求の関係

2.1 ParOSの対象（想定）システム

ParOSの適用を想定しているシステムの構成図を図 2.2に示す。

(ASR1-FR) Co-existing App with SIL

- 2個以上のそれぞれ異なるSIL/ASILを持つ複数のアプリケーションが単一のコンピュータシステム上に存在する。
- それぞれのアプリケーションは、異なるベンダーにより開発される。
- あるアプリケーションが変更された場合、他のアプリケーションの再検証は可能な限り減らしたい。
- それぞれのアプリケーションには、メモリ領域やCPU利用率、実行順序、実行タイミングが割り付けられている。

(ASR2-SR) SIL3 Capable

- 幾つかのパーティションは高い 安全度水準（SIL） を要求する。
    - ハードウェアトレランスが1の場合は、 SIL3
    - ハードウェアトレランスが0の場合は、SIL2
- ParOSには、システム中の最高の安全度水準のアプリケーションと同じ安全度水準が要求される。

(ASR3-FR) Interrupt

- 各アプリケーションは、割込みを使用する。ただし要求される割込み応答性は高くない（他のアプリケーション実行中は禁止される）。

(ASR4-FR) Atomic Execution

- 一連の処理を中断することなく実行したい。
    - 例)デバイスの初期化

(ASR5-FR) Advanced Requirements

- アプリケーションによっては、以下の機能を要求する。
    - 高速応答割込み
    - CPU利用率の向上のための動的アプリケーションスケジューリング
        - あるアプリケーションがアイドル状態となった場合、他のアプリケーションを実行する。
    - アプリケーションスケジューリングの動的変更。

(ASR6-FR) SafeOS function

- アプリケーションは、SafeOS[SafeOS_SRS]の機能を使用。

(ASR7-FR) Inter-partition communication

- 異なるSILのアプリケーション間で通信を行う。

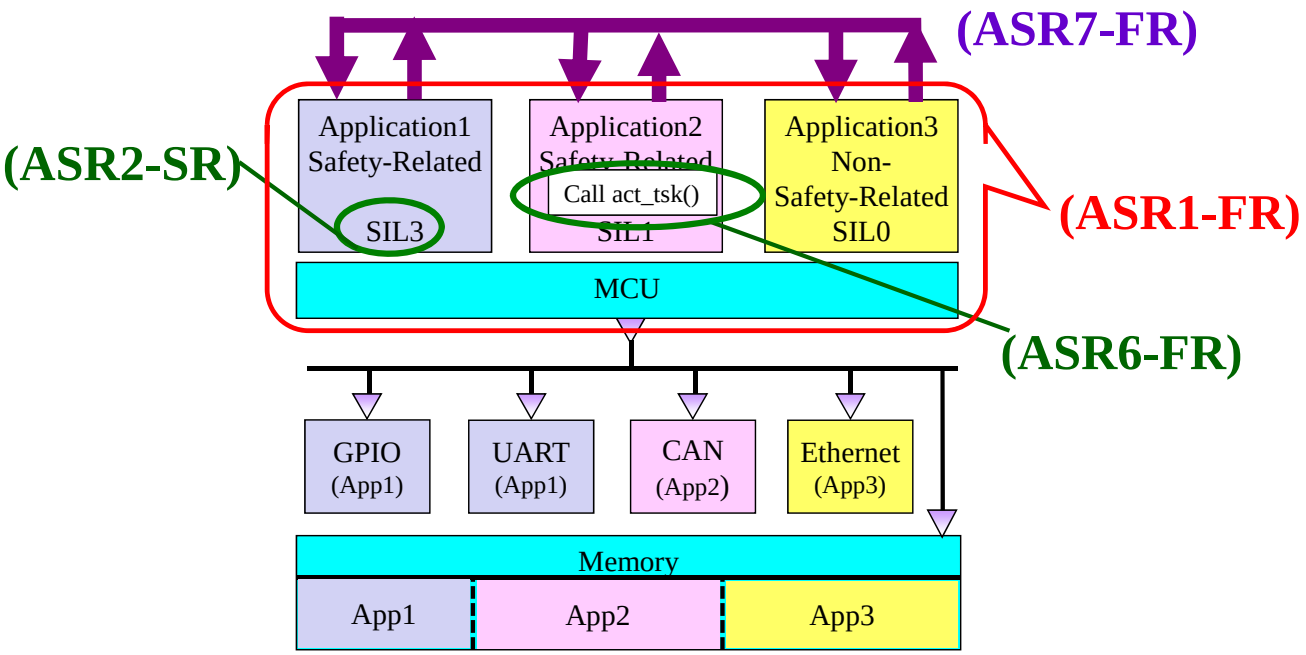


図 2.2 ParOS の対象システムの構成

2.2 ParOSの基本機能（安全機能は含まない）

2.1 で述べたシステムの要求を満たすため、ParOS は以下の機能を提供する。

ParOS(1) : Time Sharing

- CPU 時間をアプリケーション間でシェアする機能。

ParOS(2) : Memory Sharing

- メモリをアプリケーション間でシェアする機能。

ParOS(3) : Application Interrupt

- 対応するアプリケーションが実行中の時のみ受け付ける割込み機能。

ParOS(4) : Atomic Handler

- 一連の処理を中断することなく実行できる機能。

ParOS(5) : High priority interrupt

- 高速応答割込み機能。

ParOS(6) : Dynamic partition scheduling

- あるアプリケーションがアイドルになった場合、その時間で他のアプリケーションを実行する機能。

ParOS(7) : Scheduling mode change

- アプリケーションのスケジューリングを動的に変更する機能。

ParOS(8) : SafeOS compatibility function

- SafeOS の互換機能。

ParOS(9) : Inter partition communication

- アプリケーション間の通信機能。

2.3 ParOSの基本機能の故障モード

2.2 で述べた ParOS の基本機能における故障モードは次の通りである。

Failure Mode(1)：Time violation

- “CPU利用率”
  - ・アプリケーションが割り当てられた以上のCPU利用率を消費する。
- ”実行順序”
  - ・アプリケーションが割り当てられた実行順序ではない順序で実行される。
- ”実行タイミング”
  - ・アプリケーションが設計時に定めた実行タイミングではない実行タイミングで実行。

Failure Mode(2)：Memory violation

- アプリケーションが割り当て外のメモリにアクセス。

Failure Mode(3)：Service violation

- アプリケーションが他のアプリケーションに対してAPIを発行。

Failure Mode(4)：OS state violation

- アプリケーションがシステム（OS）状態を不正に変更。

Failure Mode(5)：Inter communication problem

- アプリケーション間通信に関する問題が発生。
  - 例)データ値が不正、送信タイミングが不正。

3　安全目標

ParOS の Safety Goal を以下に示す。【SG-1】と【SG-2】は、ISO26262 Part6 D.2 に記載される 2 個のパーティショニングの目的と同等である。なお、パーティショニングされているプログラムの単位をパーティションと呼ぶ。

Safety Goal 1【SG-1】

@@パーティションの故障が、他のパーティションに影響を及ぼさないこと。異なる安全度水準のパーティションを同一のシステム上で実行できること[ParOS-SW-01-SC-0001][]@@

Safety Goal 2【SG-2】

@@あるパーティションに変更があった場合、他のパーティションの再検証の必要がない、もしくは検証レベル（労力）を下げることが可能であること。パーティションを個別に検証可能（検証範囲や工数を減らせる）であること。[ParOS-SW-01-SC-0002][]@@

Safety Goal 3【SG-3】

@@故障診断率（Diagnosys Coverage）90%以上の診断方法を含む故障検出ライブラリを提供する。[ParOS-SW-01-SC-0004][]@@

故障検出ライブラリを含むParOS自身は、SIL3 を満たすために必要なプロセスで開発すること。同一のParOSモジュールを用い、デュアルチャンネル・ハードウェア構成としハードウェアのフォールトトレランスが1の場合はSIL 3を満たすことができ、シングルチャンネル・ハードウェア構成でフォールトトレランスが0の場合はSIL 2を満たすことができること。

Safety Goal 4【SG-4】

@@パーティション間通信で通信相手に問題が発生し停止した場合に、その停止を検知できること。[ParOS-SW-01-SC-0005][]@@

4　アーキテクチャ

@@全てのSGは、パーティショニング機能を持つParOSにより実現する。[ParOS-SW-01-SC-0006][]@@ParOSの各パーティションとParOSのインタフェースの図（論理図）を図 4.1に、コードとデータの構成を図 4.2に示す。

@@ParOS の機能は、Executive, SafeOS、COM から構成されている。これらのコンポーネントが使用するメモリはパーティションから保護されている。[ParOS-SW-01-SC-0007][]@@

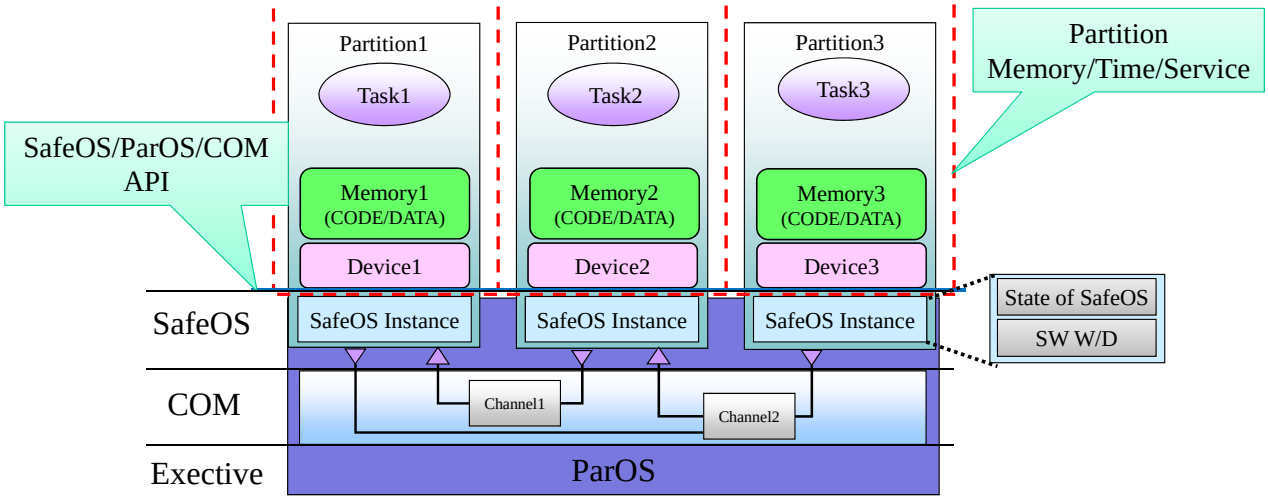
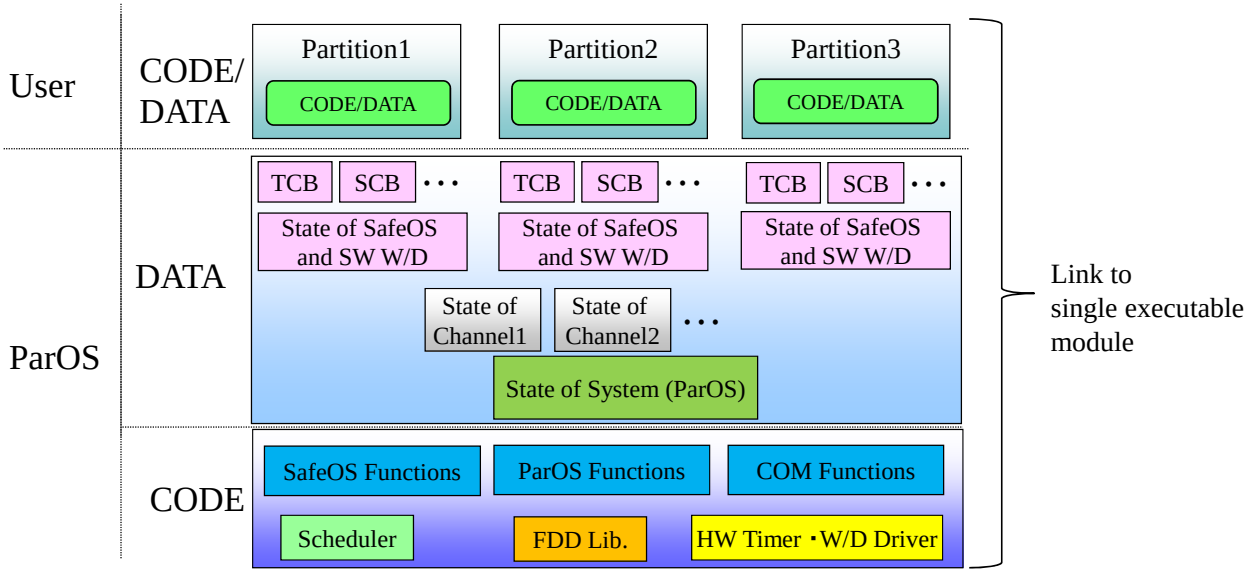


図 4.1ParOS の論理図



TCB : task control block
SCB : semaphore control block

図 4.2ParOS のコード・データ構成図

4.1 ParOS コンポーネント

Partition

各パーティションには、独立した SafeOS のインスタンスが割り付けられる。そのため、各パーティションの SafeOS の状態は独立である。また、パーティション毎にメモリやデバイスが割り付けられている。

Executive

@@Executive は、各パーティショニング機能を実現する。[ParOS-SW-01-SC-0009][ParOS-SW-01-SC-0007]@@また、@@ランダムハードウェア故障検出を行うための故障検出ライブラリ(

FDD)を持つ。故障検出ライブラリにより【SG3】を実現する。詳細については、6 章を参照のこと。[ParOS-SW-01-SC-0010][ParOS-SW-01-SC-0004]@@

@@各パーティションインスタンスの実行シーケンスモニタに対して仮想化されたタイマや W/D タイマを提供する。[ParOS-SW-01-SC-0011][]@@

SafeOS互換機能

@@ParOS は、パーティションに SafeOS[SafeOS_SRS]互換の機能を提供する。 [ParOS-SW-01-SC-0012][ParOS-SW-01-SC-0007]@@ただし、@@【SG1】【SG2】に反する以下の機能は使用することができない。

・タイムイベントハンドラ（周期ハンドラ・アラームハンドラ）
・割込みハンドラ・割込みサービスルーチン
・CPU 例外管理機能[ParOS-SW-01-SC-0013][ParOS-SW-01-SC-0001,ParOS-SW-01-SC-0002]@@

@@アプリの実行シーケンス監視を行う実行シーケンスモニタもパーティション毎に独立している。[ParOS-SW-01-SC-0014][]@@@@実行シーケンスモニタで用いるタイマや W/D タイマは、Executive により仮想化されたタイマや W/D タイマを用いる。すなわち、全てのパーティションで同じのタイマハードウェアや W/D タイマハードウェアを共有する。[ParOS-SW-01-SC-0015][ParOS-SW-01-SC-0011]@@

COM

@@COM はパーティション間の通信を実現する。[ParOS-SW-01-SC-0016][ParOS-SW-01-SC-0007]@@@@送受信データはチャネルと呼ばれるオブジェクトに格納される。[ParOS-SW-01-SC-0017][]@@@@各パーティションはインタフェースを介してチャネルに接続する。[ParOS-SW-01-SC-0018][]@@

4.2 実装モデル

図 4.2に示すように、ParOSは一般のVMのように、各SafeOSとParOSのコードやデータが独立しているのではなく、コードとデータが一体となっている。

各パーティションに割り付ける SafeOS のインスタンスの実現は、パーティション毎に独立した SafeOS の状態を持つことにより実現している。チャネルやシステム状態（ParOS の状態）は、全てのパーティションで共有する。また、各アプリケーションのコードやデータと共に１つの実行モジュールにリンクされて実行される。

4.3 メモリ保護

@@図 4.2に示すParOSのメモリ領域は、アプリケーション（パーティション）から保護されている。[ParOS-SW-01-SC-0008][]@@

図 4.2に示すように、各パーティションとParOSのコード領域とデータ領域は、一つの実行モジュールにリンクされるが、図 4.3に示す様に、各コードとデータはそれぞれまとめられ、メモリに配置される。

パーティションはメモリ保護が有効なモード（通常はユーザーモード）で、ParOS はメモリ保護が無効なモード（通常は特権モード）で実行される。

各パーティションにはコード領域とデータ領域とデバイスが割り付けられ、ParOS は、MPU ないし MMU により、各パーティションが割り付けられたリソースのみアクセス可能なように保護を行う。具体的には、実行するパーティションを変更するタイミングで MPU/MMU の設定を切り替えることで保護を実現する。

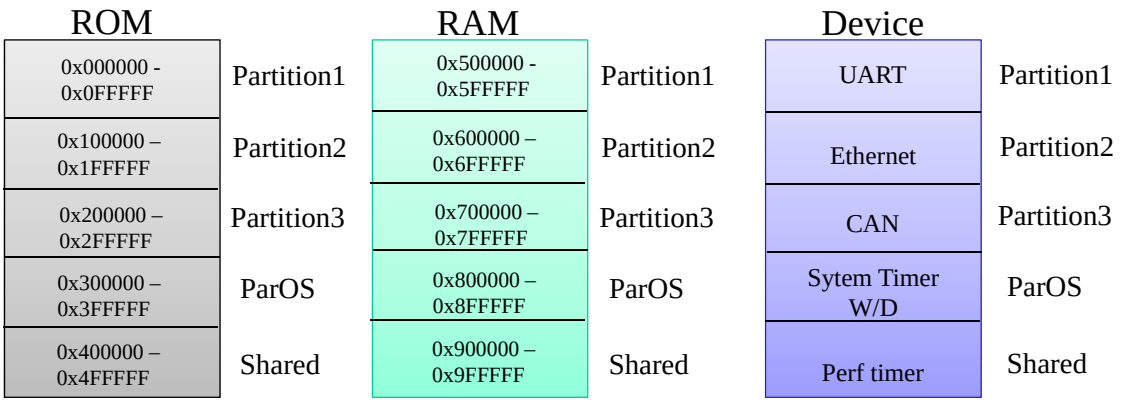


図 4.3ParOS のメモリ図

5 パーティショニング

5.1 パーティショニングレベル

【SG-1】【SG-2】を実現するために要求されるパーティショニングはシステム毎に異なるため、以下のようにパーティショニングレベル(ParLv1～4)を定める。パーティショニングレベルが高いほど、多くのパーティショニングを必要とする。

表 5.1@@パーティショニングレベル[ParOS-SW-01-SC-0019][ParOS-SW-01-SC-0001,ParOS-SW-01-SC-0002]@@

	ParLv1	ParLv2	ParLv3	ParLv4
サービス保護	○	○	○	○
メモリ保護	○	○	○	○
CPU 利用率保護	-	○	○	○
システム(OS)状態保護	-	-	○	○
実行順序保護	-	-	○	○
実行タイミング保護	-	-	-	○

各パーティショニングの詳細は次の通りである。

5.2 パーティショニングの種類

5.2.1 時間パーティショニング

CPU利用率保護: Safety Requirement (1)

@@設計時に各パーティションに CPU 利用率を割り当て、割り当てた CPU 利用率を満足するようにパーティションを実行すること。CPU 利用率が守られていれば、パーティションの実行順序の入れ替えや実行の中断は許容する。[ParOS-SW-01-SC-0022][ParOS-SW-01-SC-0001,ParOS-SW-01-SC-0002]@@

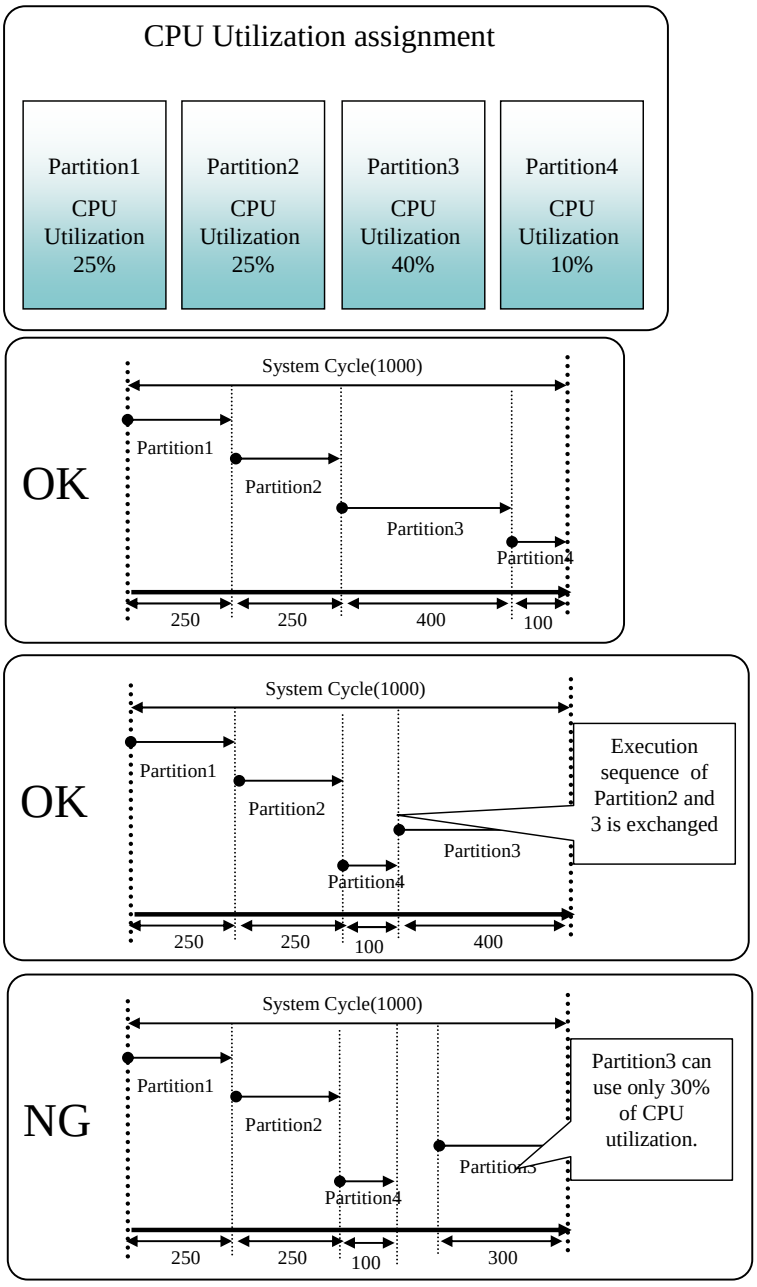


図 5.1CPU 利用率保護

実行順序保護: Safety Requirement (2)

@@設計時に設定したパーティションの実行順序を実行時に守ること。実行順序はシステム周期と呼ぶ任意の一定時間内の時間をパーティションに割り付ける。

実行順序が守られていれば、開始時間の遅れ（ジッター）や、実行の中断は許容するが、許容値をユーザーに明示させること。[ParOS-SW-01-SC-0024][ParOS-SW-01-SC-0001,ParOS-SW-01-SC-0002]@@

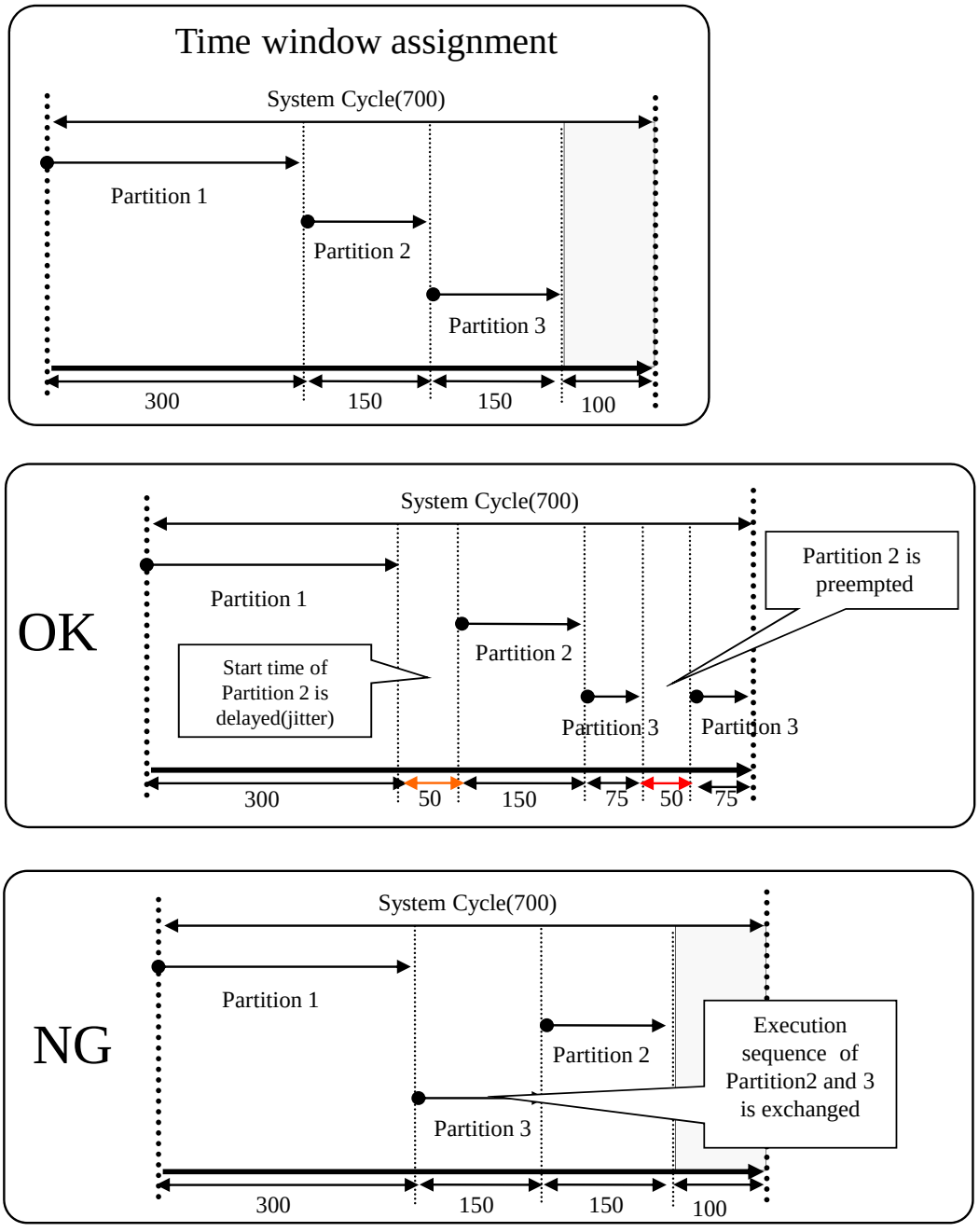


図 5.2 実行順序保護

実行タイミング保護: Safety Requirement (3)

@@設計時に設定したパーティションの実行順序を実行時に守ること。開始時間の遅れ（ジッター）や、実行の中断も許容しない。[ParOS-SW-01-SC-0025][ParOS-SW-01-SC-0001,ParOS-SW-01-SC-0002]@@

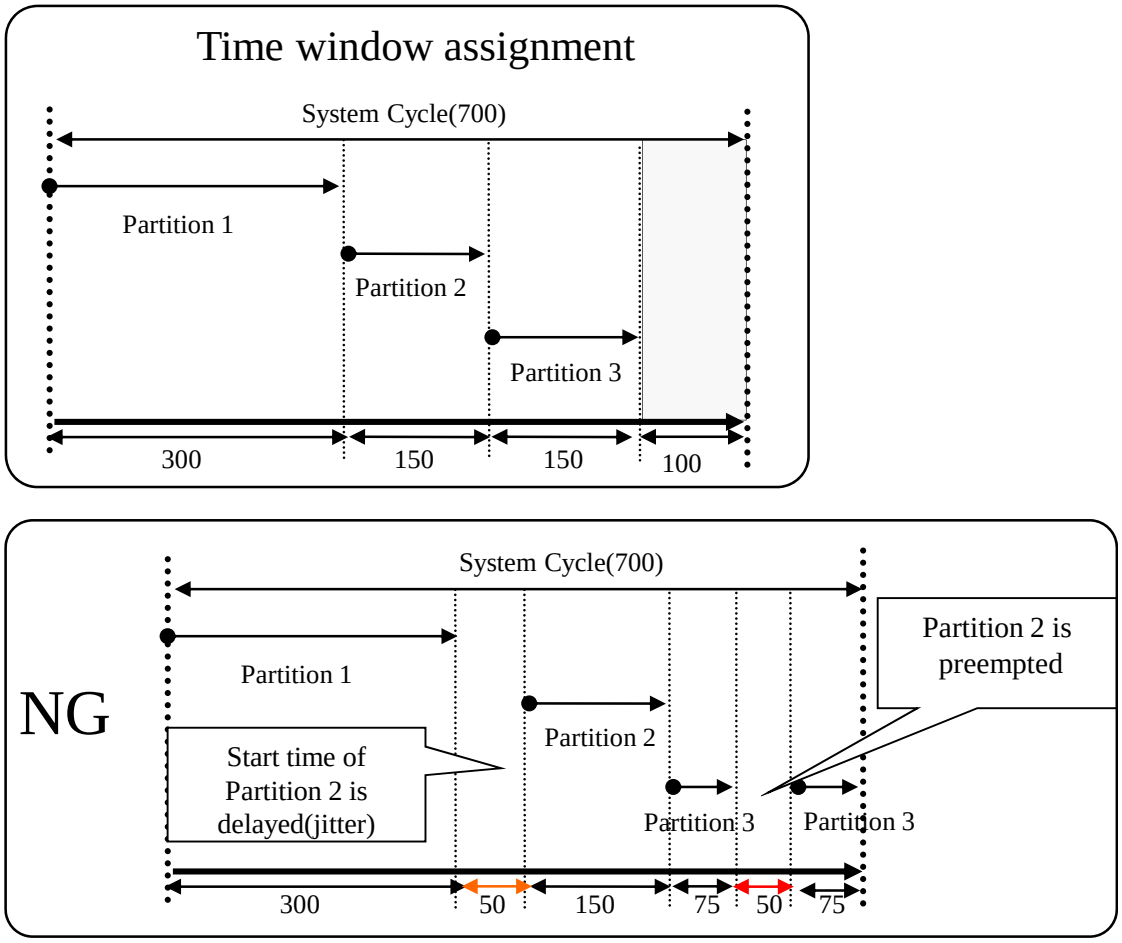


図 5.3 実行タイミング保護

5.2.2 メモリパーティショニング

メモリ保護: Safety Requirement（4）

@@設計時に各パーティションにメモリ領域を割り当て、実行時に割り当てたメモリ領域に対する他のパーティションからの書き込みを禁止すること。[ParOS-SW-01-SC-0021][ParOS-SW-01-SC-0001,ParOS-SW-01-SC-0002]@@

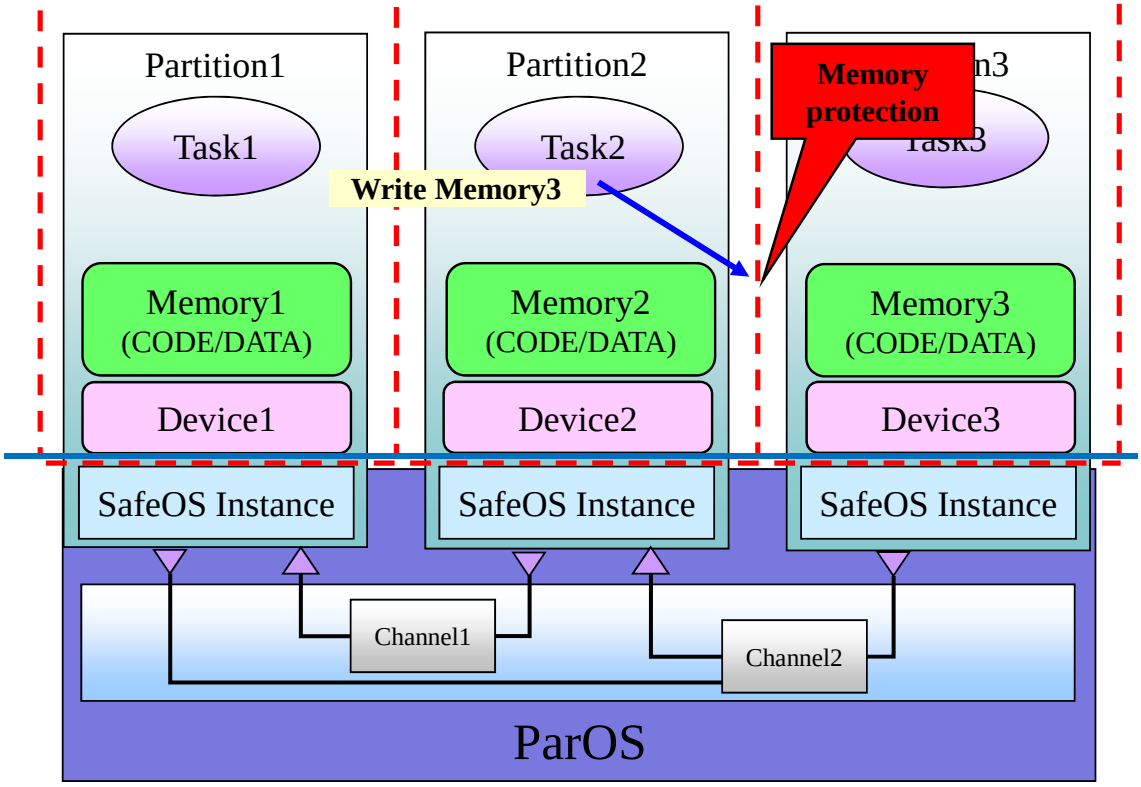


図 5.4 メモリ保護

5.2.3 システム(OS)パーティショニング

サービス保護: Safety Requirement (5)

@@あるパーティションから他のパーティションに影響を与えるシステムコールの発行や、OS を破壊するシステムコールの発行を禁止すること。[ParOS-SW-01-SC-0020][ParOS-SW-01-SC-0001,ParOS-SW-01-SC-0002]@@

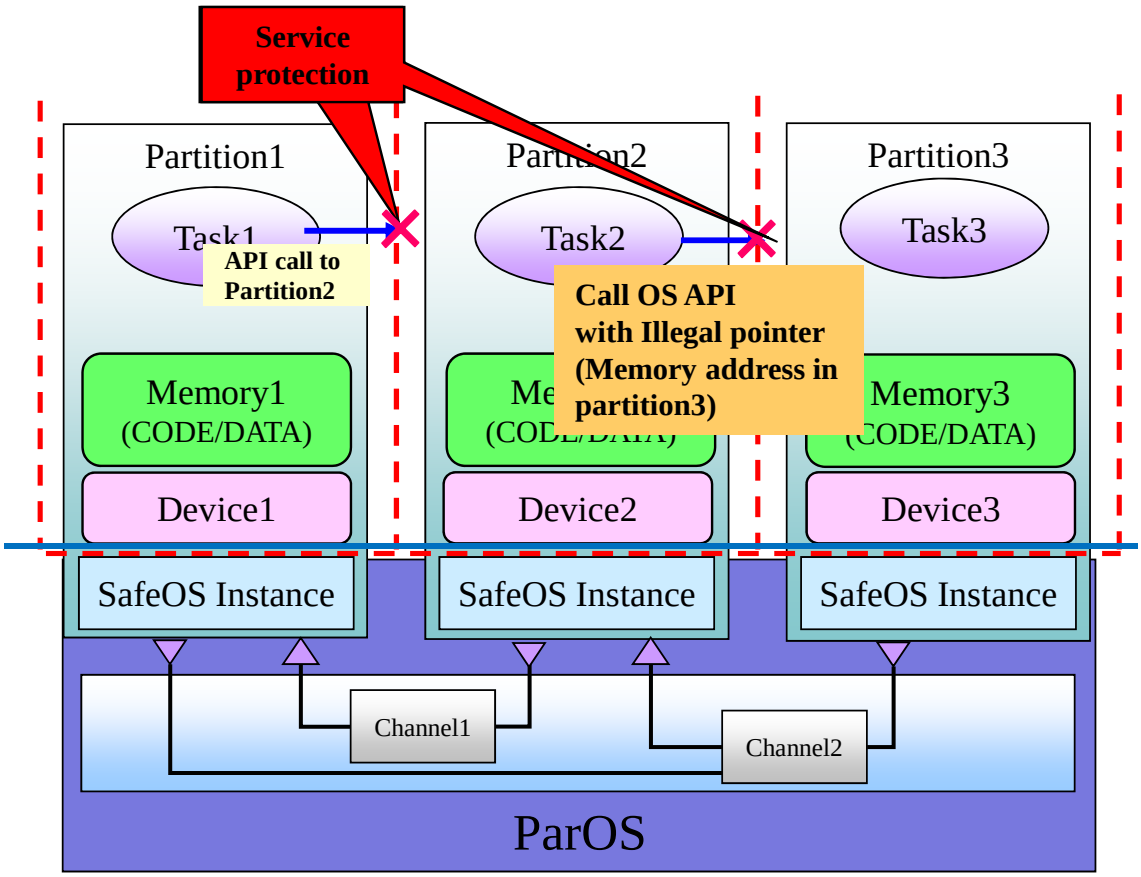


図 5.5 サービス保護

システム(OS)状態保護: Safety Requirement (6)

@@パーティション間のシステム(OS)状態が独立であること。パーティション切替時に、切替元パーティションのシステム状態を保存して、切替先パーティションのシステム状態を HW に反映する。[ParOS-SW-01-SC-0023][ParOS-SW-01-SC-0001,ParOS-SW-01-SC-0002]@@

例えば、あるパーティションが OS の状態をディスパッチ禁止状態としたとしても、他のパーティションはその影響をうけない。

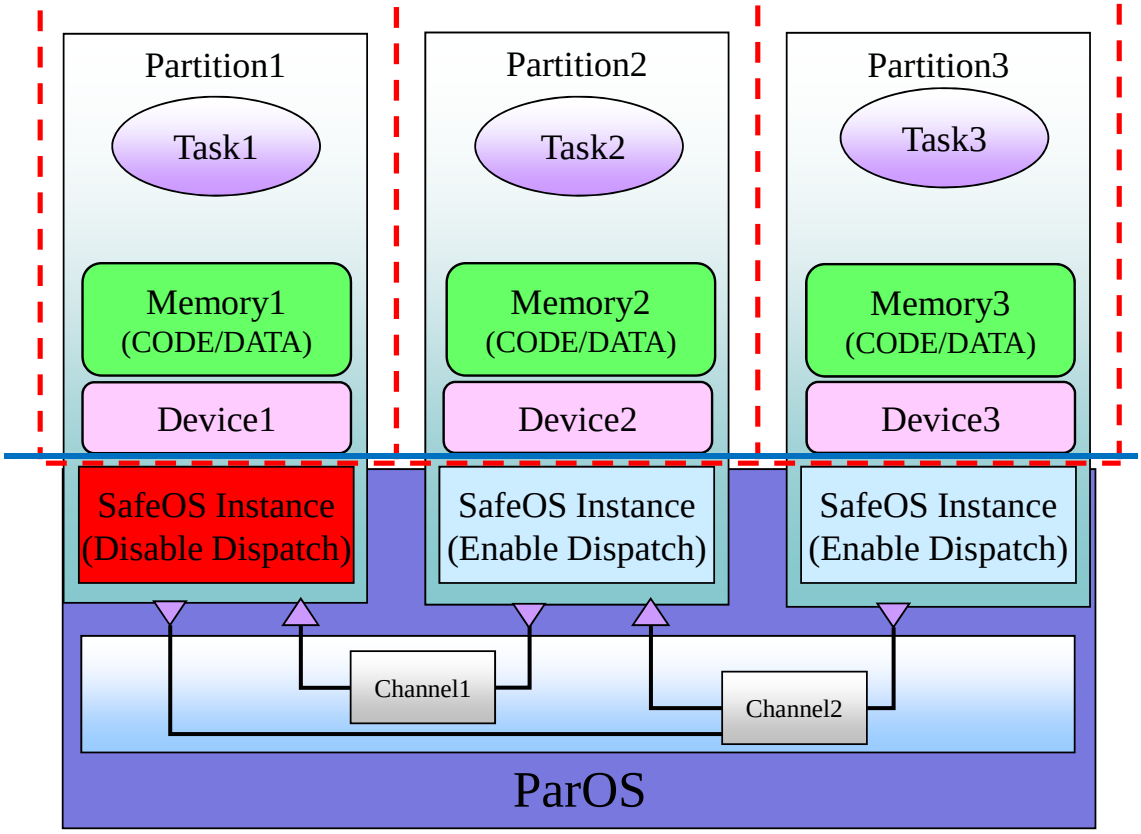


図 5.6 システム(OS)状態保護

5.3 アプリケーションレベル

パーティションレベルと関連して、アプリケーションが要求する性質や OS の機能をアプリケーションレベルとして定める。アプリケーションレベル毎に使用可能なパーティションレベルが異なる。

表 5.2@@アプリケーションレベル[ParOS-SW-01-SC-0026][ParOS-SW-01-SC-0019]@@

	APPReqLv0	APPReqLv1	APPReqLv2	APPReqLv3
Priority Base Scheduling	○	○	○	○
タスクと割込みハンドラ	○	○	○	○
スレーブデバイス使用	○	○	○	○
リアルタイム性	-	○	○	○
高速割込み応答	-	-	○	○
デバイス共有	-	-	-	○
マスタデバイス使用	-	-	-	○
適用可能なパーティションレベル	ParLv2～4	ParLv3～4	ParLv3	ParLv3

5.4 パーティショニング機能

【SG1】及び【SG2】を満たすため、Executive は以下のパーティショニング機能を要する。以下の表では安全維持機構と実現するパーティショニングとの関係も示す。

表 5.3@@パーティショニング機能と実現するパーティショニング[ParOS-SW-01-SC-0027][ParOS-SW-01-SC-0020,ParOS-SW-01-SC-0021,ParOS-SW-01-SC-0022,ParOS-SW-01-SC-0023,ParOS-SW-01-SC-0024,ParOS-SW-01-SC-0025]@@

安全維持機能	実現するパーティショニング
サービス保護機能【EXECTIVE:SIR-1】	サービス保護
メモリ保護機能【EXECTIVE:SIR-2】	メモリ保護
周期実行ポリシー【EXECTIVE:SR-1】 （パーティションスケジューラ）	CPU 利用率保護 実行順序保護 実行タイミング保護
システム(OS)情報保護機能【EXECTIVE:SIR-3】	システム(OS)状態保護

サービス保護機能

@@"サービス保護"を実現する機能。あるパーティションから他のパーティションのオブジェクトに対するシステムコールの発行を禁止する。

アプリケーションからの API 呼び出し時にパラメータチェックを行う。[ParOS-SW-01-SC-0028][ParOS-SW-01-SC-0027]@@

メモリ保護機能

@@"メモリ保護"を実現する機能。設計時に各パーティションにメモリ領域を割り当てる。割り当てたメモリに関して、他のパーティションからの書き込みを禁止する。具体的にはプロセッサの持つ MPU ないし MMU を制御して保護を実現する。[ParOS-SW-01-SC-0029][ParOS-SW-01-SC-0027]@@

周期実行ポリシー（パーティションスケジューラ）

@@"CPU 利用率保護","実行順序保護","実行タイミング保護"を実現する機能。システム周期を定め、各パーティションにシステム周期内を複数のタイムウィンドウに分割し、そのタイムウィンドウをパーティションに割り付ける。OS はこのタイムウィンドウの設定と割り付けに従って各パーティションを実行する。

パーティションを確実に切り替えるため、各パーティションから操作を禁止され、割り込み優先度が最高のタイマを用いて、パーティションの切り替えタイミングを生成する。[ParOS-SW-01-SC-0030][ParOS-SW-01-SC-0027]@@

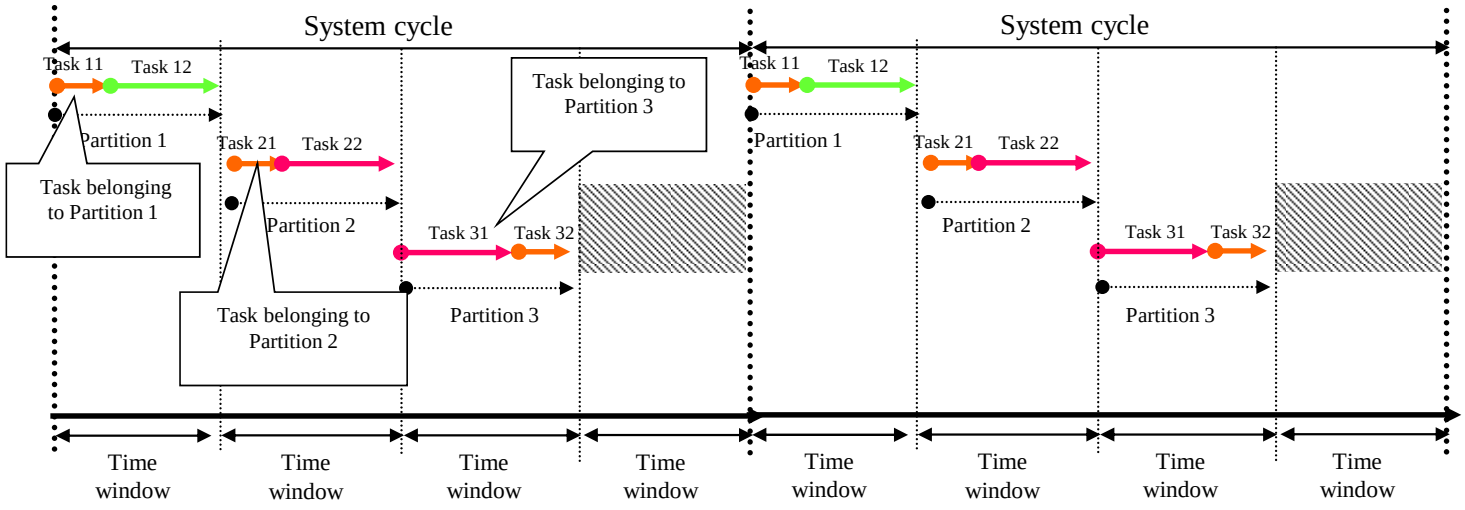


図 5.7 周期実行ポリシー

システム(OS)情報保護機能

@@"システム(OS)情報保護"を実現する機能。パーティション毎に独立したシステム(OS)状態を提供する。周期実行ポリシー（パーティションスケジューラ）の指示によりパーティションを切り替えた時、OS 状態や割込みコントローラの設定を切替先のパーティションの情報に切り替える。 [ParOS-SW-01-SC-0031][ParOS-SW-01-SC-0027]@@

5.5 コンフォーマンスクラス

【SG3】を満たすために、ParOS では、3 種類のコンフォーマンスクラスを定める。

- BCC(Basic Conformance Class)
- BCC+(Basic Conformance Class Plus)
- ECC(Extended Conformance Class)
- DCC(Development Conformance Class)

それぞれのコンフォーマンスクラスがサポートする機能は次の通りである。
ParOS の実装はいずれかのコンフォーマンスクラスに従う。

表 5.4@@コンフォーマンスクラス[ParOS-SW-01-SC-0032][ParOS-SW-01-SC-0028,ParOS-SW-01-SC-0029,ParOS-SW-01-SC-0030,ParOS-SW-01-SC-0031]@@

		BCC	BCC+	ECC	DCC
パーティショニング機能	サービス保護機能	○	○	○	○
	メモリ保護機能	○	○	○	○
	システム（OS）情報保護機能	○	○	○	○
	SafeOS 互換安全維持機能	○	○	○	○
	周期実行ポリシー	○	○	○	○
	SafeOS 互換機能	○	○	○	○
一般機能	アプリケーション割込み	○	○	○	○
	タイムウィンドウハンドラ	○	○	○	○
	アトミックハンドラ	○	○	○	○
	パーティション例外ハンドラ	○	○	○	○
	システム例外ハンドラ	○	○	○	○
	パーティション間通信	○	○	○	○
	アイドル属性			○	○
	スケジューリングモード変更			○	○
	システム割込み		*	○	○
	システムタスク				○
	システムタイムイベントハンドラ				○
Partition Level		ParLv4	ParLv3	ParLv3	

*機能制限付きシステム割り込み

BCC は最もパーティションの強度が高く、パーティショニングレベル 4 を満たす。

ECC は BCC に安全機能が幾つか追加されている。高速な割込みを実現する"システム割込み"をサポートすることにより、【実行タイミング保護】を実現出来なくなり、パーティションレベルは 3 となる。

DCC はパーティショニングが適用されないシステムパーティションをサポートするため、既存システムの ParOS を用いたパーティショニング環境への移行を容易にするため、開発時に用いることを想定している。

BCC+は BCC をベースとしたコンフォーマンスクラスである。BCC+は BCC でサポートとしている全ての機能に加えて、BCC に機能制限付きシステム割込みをサポートしている。

BCC+は ECC と同じパーティションレベル 3 であるが、ECC と比較して、機能が少ないため、実装が容易であり、ほぼ BCC と同様の実装となる。

BCC+を導入した理由は次の通りである。ECC は多くの機能をサポートするため、実装が複雑化して、オーバヘッドが大きい。BCC では、システム割込みが使えず、組込みシステムの高リアルタイム性を実現することが困難であるため定めた。

BCC+は割り込みの高速な応答を機能制限付きシステム割込みで実現すると共に、機能を制限することで、実装の簡素化と低オーバヘッドを実現している。

安全機能に対する要求に関しては、ParOS Software Safety Requirement Specification を参照のこと。

5.6 オペレーションモード

5.6.1 ParOSの状態と状態遷移

ParOS は 5 個の状態を持つ。各状態とその状態遷移は次の通りである。

- @@未定義状態[ParOS-SW-01-SC-0056][]@@
  - 電源投入時/リセット割込みルーチン実行時に遷移
- @@システム初期化中状態[ParOS-SW-01-SC-0057][]@@
  - 初期化処理を実行。
- @@システム通常状態[ParOS-SW-01-SC-0058][]@@
  - パーティションを実行
- @@システム終了処理中状態[ParOS-SW-01-SC-0059][]@@
  - 終了処理を実行。
- @@システム停止状態[ParOS-SW-01-SC-0060][]@@
  - システム終了処理終了後に遷移。実行を停止

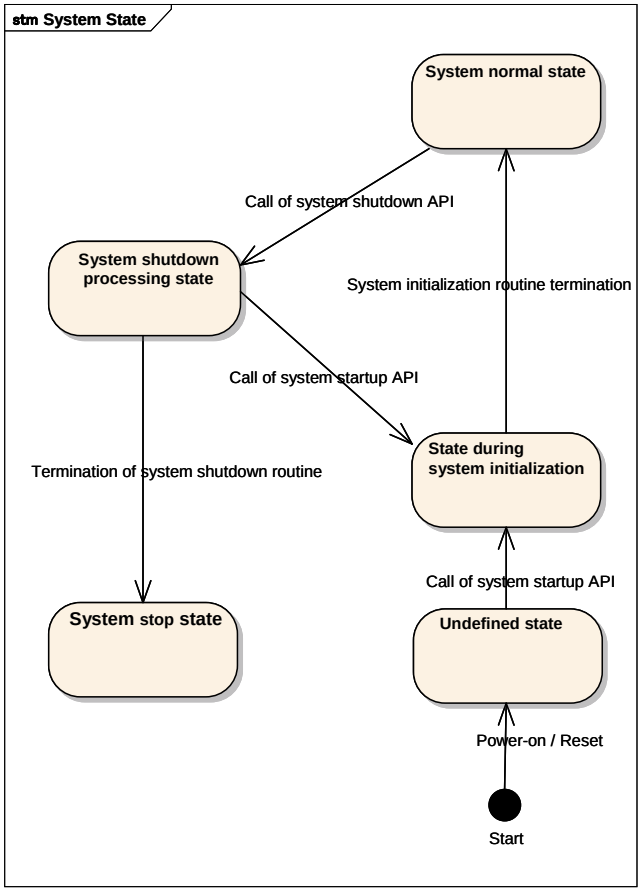


図 5.8 @@ParOS の状態遷移[ParOS-SW-01-SC-0069][ParOS-SW-01-SC-0056,ParOS-SW-01-SC-0057,ParOS-SW-01-SC-0058,ParOS-SW-01-SC-0059,ParOS-SW-01-SC-0060]@@

5.6.2 パーティションの状態と状態遷移

各パーティションは 7 個の状態を持つ。パーティションの各状態とその状態遷移は次の通りである。

- @@通常状態[ParOS-SW-01-SC-0061][]@@
  - パーティションに属するアプリケーション割込みが有効に。
  - パーティションに属するタイムウィンドウハンドラが有効に。

  - @@実行状態(TPS_NORMAL) [ParOS-SW-01-SC-0062][ParOS-SW-01-SC-0061]@@
    - 割り当てられたタイムウィンドウが実行され、かつ実行するべき処理単位が存在し実行されている状態。
  - @@休止状態(TPS_IDLE)[ParOS-SW-01-SC-0063][ParOS-SW-01-SC-0061]@@
    - 割り当てられたタイムウィンドウが実行され、かつ実行するべき処理単位が存在しない状態。
  - @@実行可能状態(TPS_RUNNABLE) [ParOS-SW-01-SC-0064][ParOS-SW-01-SC-0061]@@
    - システム周期内に未実行の割り当てられたタイムウィンドウが存在する状態。
  - @@満了状態(TPS_EXPIRE)[ParOS-SW-01-SC-0065][ParOS-SW-01-SC-0061]@@
    - システム周期内の割り当てられたタイムウィンドウが全て実行された状態。もしくはシステム周期内に割り当てられたタイムウィンドウが存在しない場合。

- @@初期化中状態(TPS_INIT)[ParOS-SW-01-SC-0066][]@@
  - パーティションの初期化を実行している状態。
  - パーティションに属する割込みが無効に。
  - パーティションに属するタイムイベントハンドラが無効に。

- @@終了処理中状態(TPS_TER)[ParOS-SW-01-SC-0067][]@@
  - パーティションの終了処理を実行している状態。
  - パーティションに属する割込みが無効に。
  - パーティションに属するタイムイベントハンドラが無効に。

- @@停止状態(TPS_STOP)[ParOS-SW-01-SC-0068][]@@
  - パーティションを終了した状態。
  - パーティションに属する割込みが無効に。
  - パーティションに属するタイムイベントハンドラが無効に。

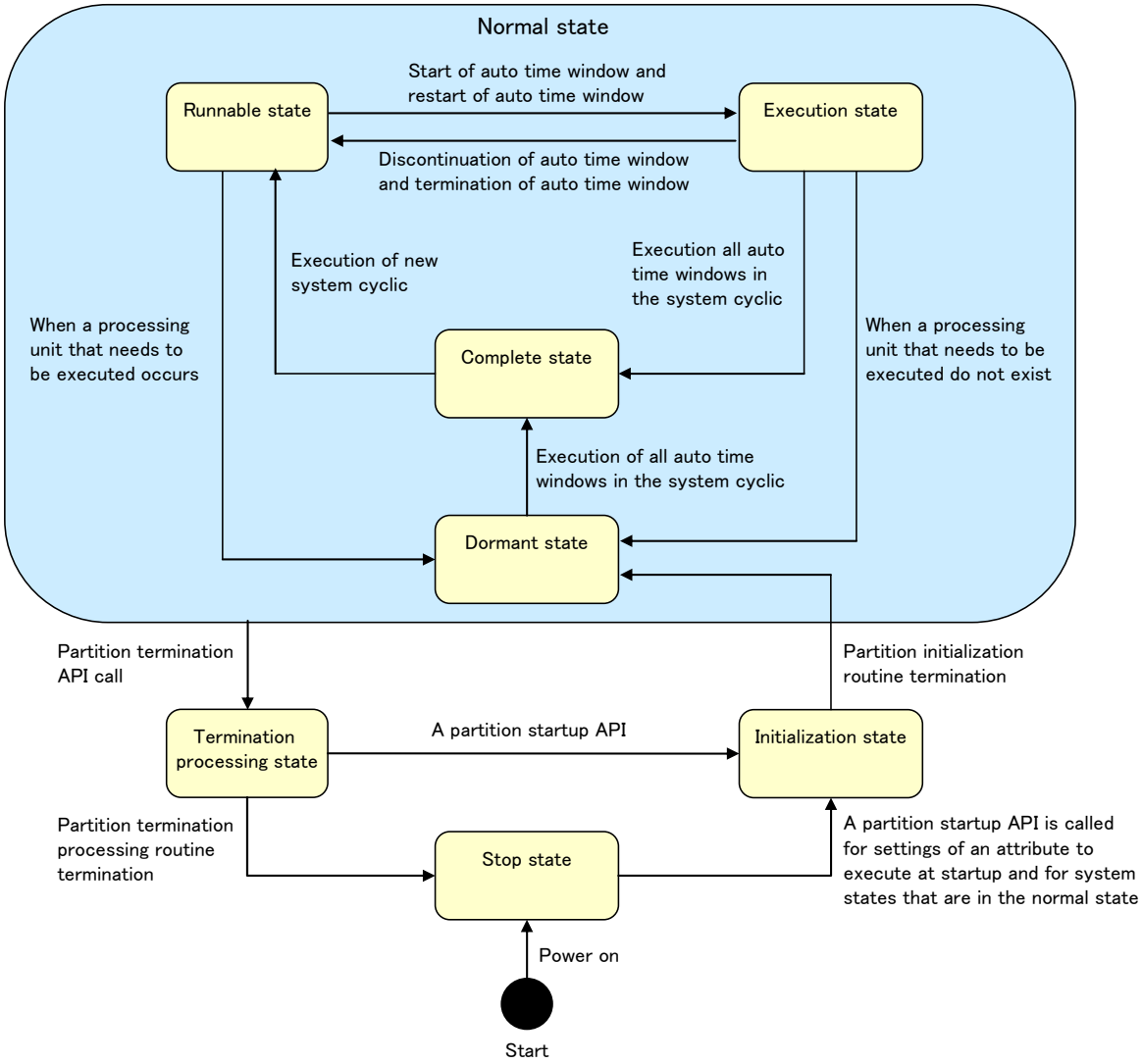


図 5.9 @@パーティションの状態遷移[ParOS-SW-01-SC-0070][ParOS-SW-01-SC-0061,ParOS-SW-01-SC-0062,ParOS-SW-01-SC-0063,ParOS-SW-01-SC-0064,ParOS-SW-01-SC-0065,ParOS-SW-01-SC-0066,ParOS-SW-01-SC-0067,ParOS-SW-01-SC-0068]@@

5.7 ParOS機能の依存関係

ParOS の機能は、次の示す依存関係がある。

(1) Cycle Execute Policy と Service, System state, Memory protection 間

- @@アクティブなパーティションが変更された場合、Cycle Execute Policy は、Service, System state, Memory protectionを呼び出す。[ParOS-SW-01-SC-0071][]@@

(2) System State Protection と INTC 間

- @@System State Protection は INTC を制御する。[ParOS-SW-01-SC-0072][]@@

(3) Between Memory Protection と MPU 間

- @@Memory Protection は、MPU を制御する。[ParOS-SW-01-SC-0073][]@@

(4) Timer と Cycle Execute Policy 間

- @@Timer は割込みを発生させ、Cycle Execute Policy を呼び出す。[ParOS-SW-01-SC-0074][]@@

(5) Idle Attribute と Cycle Execute Policy 間

- @@実行中のパーティションがアイドルになった場合、Idle Attribute は、 Cycle Execute Policy を呼び出し、パーティションを切り替える。[ParOS-SW-01-SC-0075][]@@

(6) System Interrupt と Timer 間

- @@System Interrupt が実行されると、タイマー割込みを禁止する。[ParOS-SW-01-SC-0076][]@@

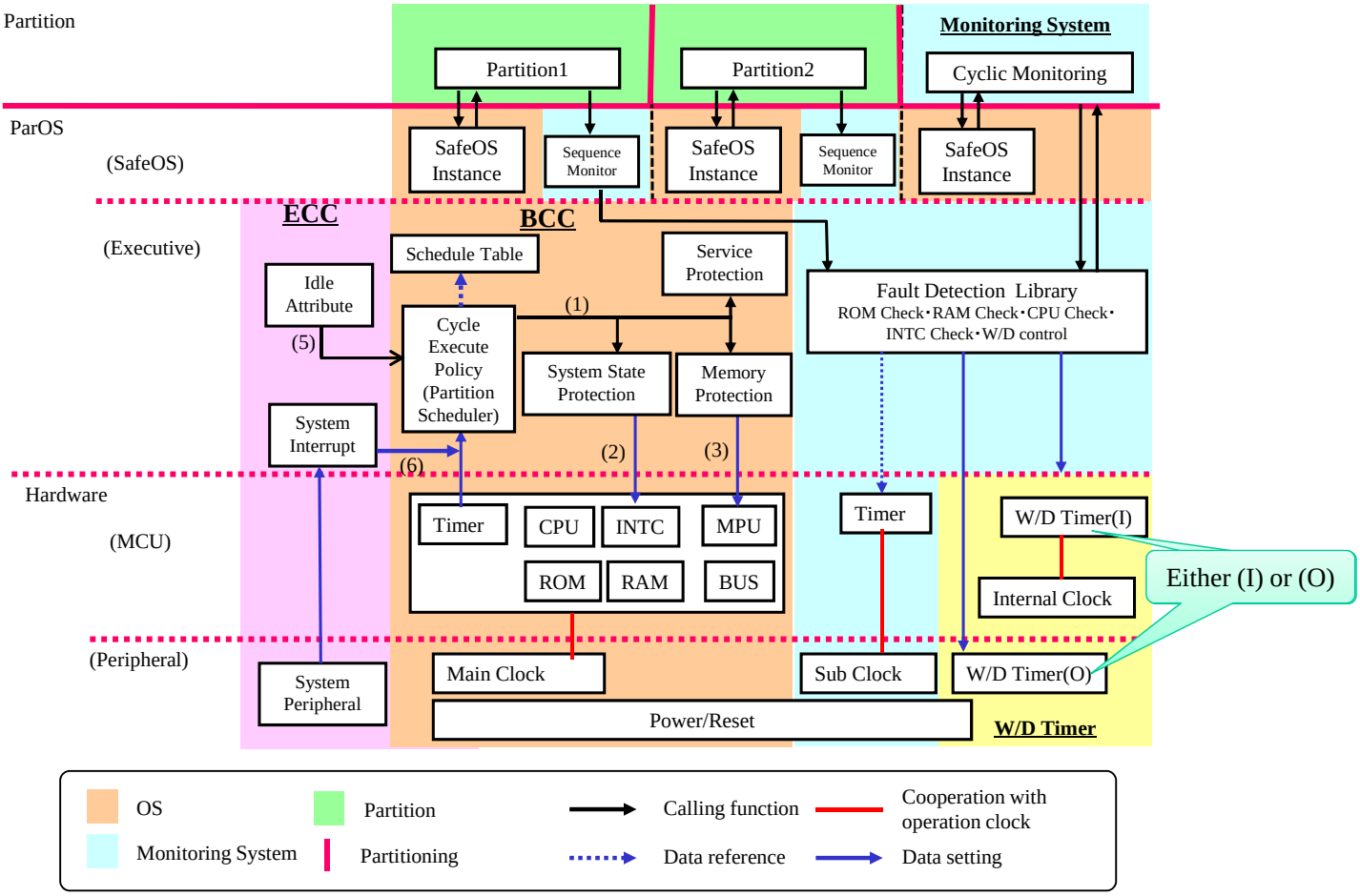


図 5.10ParOS 機能構成図

5.8 Safety Goalを脅かす可能性があるParOSの機能

以下の ParOS の機能は ParOS のパーティショニングに影響を与える可能性があるため、使用時には、

(1) ソフトウェア例外API

- システム例外ハンドラを実行する。システム例外ハンドラは、全ての処理単位より優先して実行される。
- システムインテグレータは、“システム例外ハンドラチェックフック” を用いて、ソフトウェア例外APIの不正な呼び出しを防ぐこと。

(2) パーティションのアイドル属性 [ECC]

- アイドル属性が付加されたパーティションは、”CPU利用率”、”実行順序”,”実行タイミング”が変化する。

(3) システム割込み [ECC]

- システム割込みが実行されると、その時点で実行中のパーティションの”実行タイミング”が変化する。
- システム割込みハンドラのオーバーランや、システム割込みの規定値以上の発生は、”CPU利用率”,”実行順序”,”実行タイミング”を変化させる。
- システム割込みの時間保護を使用すること。

(4) スケジューリングモード変更 [ECC]

- スケジューリングモードを変更すると、”CPU利用率”,”実行順序”,”実行タイミング”が変化する。
- システムインテグレータは、”スケジューリングモード変更フック”を用いて、スケジューリングモード変更APIの不正な呼び出しをチェックする必要がある。

5.9 一部機能に対する対策の必要性

ParOS の一部の機能は、使用方法を間違えると、SG1/SG2 を満たせなくなる可能性がある。これらの機能に対しては、対応する ParOS の対策機能を用いて対策を実施する必要がある。対策は、システム上で最も高い安全度水準で開発する必要がある。詳細については[4]Safe OS Software Safety Requirement Specification や [6]Safe OS Safety Manual を参照のこと。

6　故障検出: SafeOS互換安全維持機能

【SG3】を満たすため、ParOS は、SafeOS 互換の安全維持機能を持つ。
ParOS とアプリケーションの故障検出のためのシステム構成を以下に示す。
ParOS では以下の 2 種類の故障検出が必要となる。

6.1 パーティション内故障検出 : Safety Requirement(7)

パーティション内（アプリケーション）の故障検出機能。この機能は SafeOS の故障検出機能と互換の機能である。

6.1.1 システマティック故障検出

@@パーティションとして動作するアプリケーションや ParOS のシステマティック故障を検出するため、実行シーケンスモニタを持つ。[ParOS-SW-01-SC-0034][]@@@@実行シーケンスモニタ機能は、パーティション毎に管理される。[ParOS-SW-01-SC-0035][]@@アプリケーションは、実行シーケンスモニタを呼び出すことにより、システマティック故障検出を行う。

@@実行シーケンスモニタ機能が用いるタイマや W/D タイマは Executive が単一のタイマハードウェアと W/D タイマハードウェアをパーティション毎に多重化する。[ParOS-SW-01-SC-0036][]@@

6.1.2 ハードウェア故障検出

システム上でハードウェアの故障検出を行うための、周期監視アプリケーションを用意する。故障検出ライブラリは各種のハードウェアのチェック機能を持つ。

周期監視アプリケーションはタスクで構成され、故障検出ライブラリの機能を呼び出し、ランダムハードウェア故障検出を行う。異常を検出した場合は、全て周辺検出アプリケーションへ通知される。どのタイミングでどのような故障検出を実施するかはユーザ依存とする。W/D 制御に関しては各故障検出結果を基に周期的に実行する。

周期監視アプリケーションへのタイムウィンドウ割り当てや実行頻度はユーザー依存とする。

MCU 層の W/D タイマは内蔵 W/D、周辺回路層の W/D タイマは外部 W/D を示す。どちらか一方の W/D をユーザーが指定する。

@@システムタイマ、故障検出ライブラリが使用するタイマは独立したタイマである。[ParOS-SW-01-SC-0037][]@@@@システムタイマはタスクの周期起動やカーネルの時間管理に使用する。[ParOS-SW-01-SC-0038][]@@@@故障検出ライブラリのタイマは実行シーケンスモニタや W/D 制御での時間監視に使用する。[ParOS-SW-01-SC-0039][]@@

上記安全目標およびコンセプトを実現するために必要なハードウェアの条件を「ハードウェア要件」にて規定する。

故障検出ライブラリの詳細や、本構成で安全を保障できることは、関連文書[3,4,5,6]を参照のこと。

7　パーティション間通信（COM）

本章では、パーティション間通信（COM）の機能要求とパーティション間通信フォールト検出と通知について述べる。

7.1 機能要求

- 【SG1】【SG2】を満たすための要求であるサービス保護【SIR-1】より、パーティション間は SafeOS の API を用いて通信ができないため、@@パーティション間通信専用の機能を提供すること。[ParOS-SW-01-SC-0040][]@@【COM:SR-1】
- @@パーティション間通信はチャネルと呼ばれるオブジェクトにより実現する。[ParOS-SW-01-SC-0041][]@@【COM:SR-2】
- @@各アプリケーションは設計時にインタフェースによりチャネルに接続し、メッセージをやり取りする。[ParOS-SW-01-SC-0042][]@@【COM:SR-3】
- @@パーティション通信は、データがキューイングされるメッセージチャネルと、データがキューイングされない状態変数チャネルを持つ[ParOS-SW-01-SC-0043][]@@。【COM:SR-4】
- @@チャネルは実行状態と停止状態の 2 状態を持ち、停止状態のチャネルに読み書きするとエラーとなる。[ParOS-SW-01-SC-0044][]@@【COM:SR-5】

7.2 パーティション間通信フォールト検出と通知 : Safety Requirement(8) :

【SG4】を満たすために、それぞれのチャネルは、次の安全維持機能を持つ。なお、@@データの内容の正当性や送受信タイミングについてはユーザープログラムで保証する必要がある。[ParOS-SW-01-SC-0055][]@@詳細については [6]Safe OS Safety Manual を参照のこと。

7.2.1 メッセージチャネル

@@メッセージチャネルに読み込み待ち、書き込み待ちのパーティションが存在する場合に、チャネルの状態が停止状態になった場合には、それらのパーティションの待ち状態を解除して、エラーを返す[ParOS-SW-01-SC-0045][ParOS-SW-01-SC-0043]@@【COM:SIR-1】。

7.2.2 状態変数チャネル

@@状態変数チャネルは、データの更新周期を設定でき、更新周期を超えて更新されない場合は、チャネルの状態を停止状態とする。[ParOS-SW-01-SC-0046][ParOS-SW-01-SC-0043]@@【COM:SIR-2】

8　ハードウェア要求

ParOS を実行するために、システムは次のハードウェアを備える必要がある。

基本アーキテクチャ

@@MCU は中央処理演算処理装置(CPU)、割込みコントローラ(INTC)、アドレスバス(Bus)、内蔵 ROM(ROM)、内蔵 RAM(RAM)、タイマ、ウォッチドッグ機能(MCU 内蔵である場合)を有すること。[ParOS-SW-01-SC-0047][]@@【HW:SIR-1】

メモリ保護ハードウェア

@@MCU は実行しているプログラムに対して特定のメモリへのアクセスを制限する機構(MPU や MMU)を持つこと。[ParOS-SW-01-SC-0048][]@@【HW:SIR-2】

ユーザーモードデバイスアクセス

@@メモリアクセスの制限のために、非特権モードを持つ場合、非特権モードであっても、許可されたデバイスへは直接アクセス可能であること。[ParOS-SW-01-SC-0049][]@@【HW:SIR-3】

クロック

@@周辺回路としてはメインクロック、サブクロック、内蔵クロック、電源、ウォッチドッグ(MCU 内蔵でない場合)を有すること。[ParOS-SW-01-SC-0051][]@@【HW:SIR-5】

ウオッチドック

@@ウォッチドッグは、MCU 内蔵機能または外部部品のいずれかを用いる。フォールトトレランス 1 となるハードウェアを用いること。[ParOS-SW-01-SC-0052][]@@【HW:SIR-6】
※SIL2 を満たすことを目標とする場合、フォールトトレランス 0 のハードウェアを用いること。

パーティションスケジュール用タイマ

@@タイマは 1 つのカウンタに対してコンペア値を 2 個持ち、カウンタの値をクリアせずにコンペア値を変更可能であること。[ParOS-SW-01-SC-0053][]@@【HW:SIR-7】

さらに、性能のため以下の機能を持つことを推奨する。

低オーバヘッドの割込み禁止許可

@@割込みを低オーバヘッドで個別に許可・禁止することが可能であること。[ParOS-SW-01-SC-0050][]@@【HW:SIR-4】

9　開発プロセス

Safety Goal3 を満たすため、ParOS は、TUV ZUD によって IEC61508 SIL3 のプロセス認証された、WITZ の開発プロセスを用いて開発される。