HITACHI
Inspire the Next

日立超LSIシステムズが提供する TRONリアルタイムOSソリューション

2017/12/14

株式会社 日立超LSIシステムズ

トロンフォーラム TRON Safe Kernel WG 座長
豊山　祐一

自己紹介

HITACHI
Inspire the Next

豊山 祐一 （とよやま ゆういち）

株式会社 日立超LSIシステムズ
IoTソリューション事業部　主管技師

1986年入社　以来、組込みシステムのソフト開発に従事
2002~2008年　YRPユビキタス・ネットワーク研究所に出向
坂村教授のもとT-Kernelの開発などに取り組む

2009年~　日立超LSIにてT-Kernelを中心とした組込みソフトの開発に取組む。
主な製品： OpenTK、リアルタイム・オーガナイザ

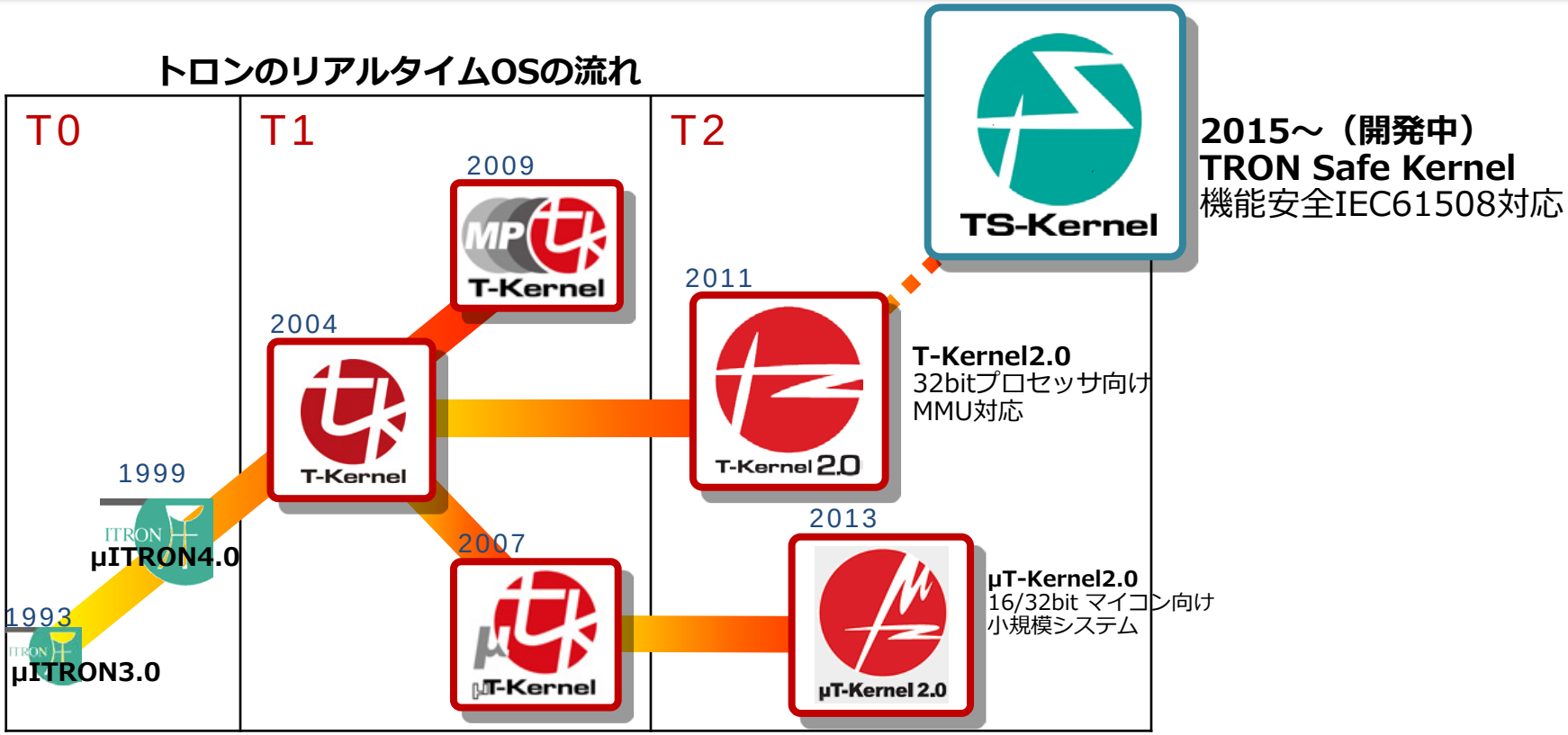
2015年~　トロンフォーラム　TRON Safe Kernel WG 幹事を務め、機能安全OSの開発に取り組む（2016/10~ WG座長）

日立超LSIのリアルタイムOSへの取組み

HITACHI
Inspire the Next

- 日立超LSIは、90年代より**μITRON**を使用した組込みシステムの開発に従事
- 2002年より次世代のTRON OSである**T-Kernel**の開発に参画
- 現在も**トロンフォーラム**の幹事会員として**トロンプロジェクト**に携わる

2015年10月　TRON Safe Kernel WGに幹事として参加（2016年10月より座長）
TRON Safe Kernelの仕様策定、開発に取り組む



機能安全対応OS ”TRON Safe Kernel”

HITACHI
Inspire the Next

TRON Safe KernelはTRONフォーラムで新たに開発された機能安全に対応したリアルタイムOSです。

■ **組込システムの様々な分野で機能安全認証の必要性が増大**
- 組込システム向けRTOSの機能安全対応が必要
- トロン仕様RTOSが機能安全規格に対応することが強く求められる

■ **2015年10月 トロンフォーラム内に**TRON Safe Kernel WG**を設立 仕様策定、開発を開始**

<TRON Safe Kernelの開発目標>
- μITRON/T-Kernelを継承するリアルタイムOS　＋　**機能安全対応機能**
- 機能安全規格**IEC61508 SIL３**の第三者認証取得可能なOS

■ **2017年12月 TRON Safe Kernel仕様書 公開**
TRONフォーラムHPから入手可能
- ソースコード公開は2018年春を予定

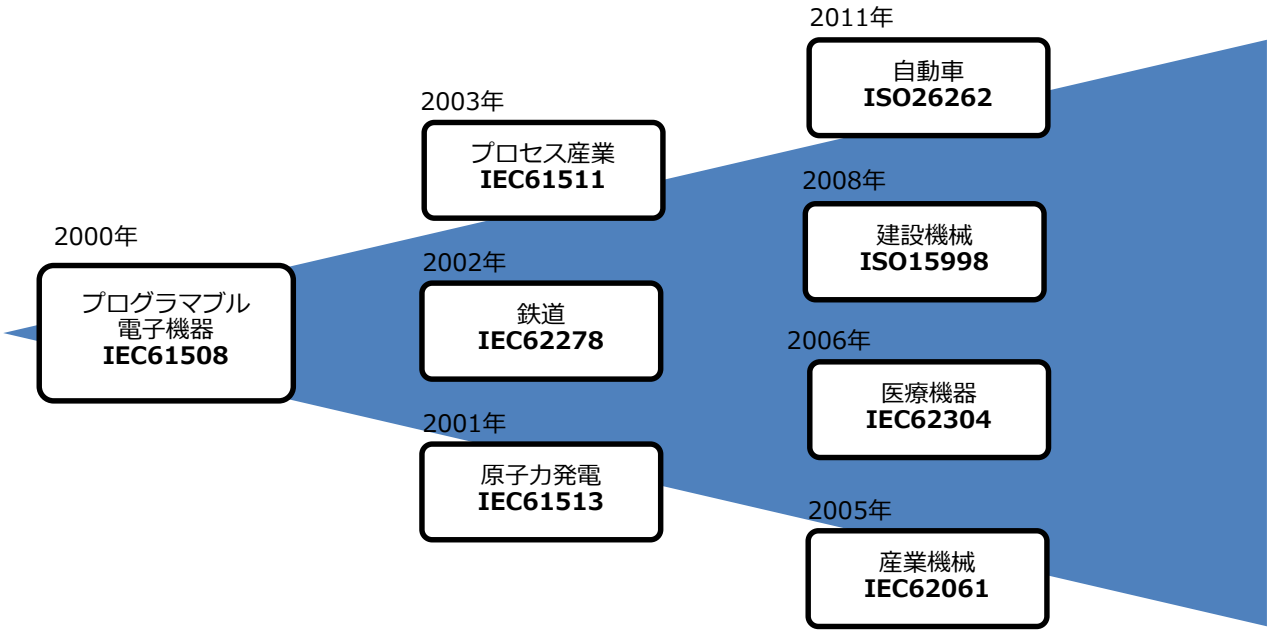
TS-Kernel

機能安全の必要性

HITACHI
Inspire the Next

機能安全とは：
- 人の安全を確保するための方策の一つ
- 機能的な工夫により危険を許容可能な範囲に低減させる

90年代、欧州を中心に検討が進み、2000年以降、各分野で安全規格が制定。今後も広がっていくと考えられる
⇒　組込みソフトウェアも機能安全の対象となる



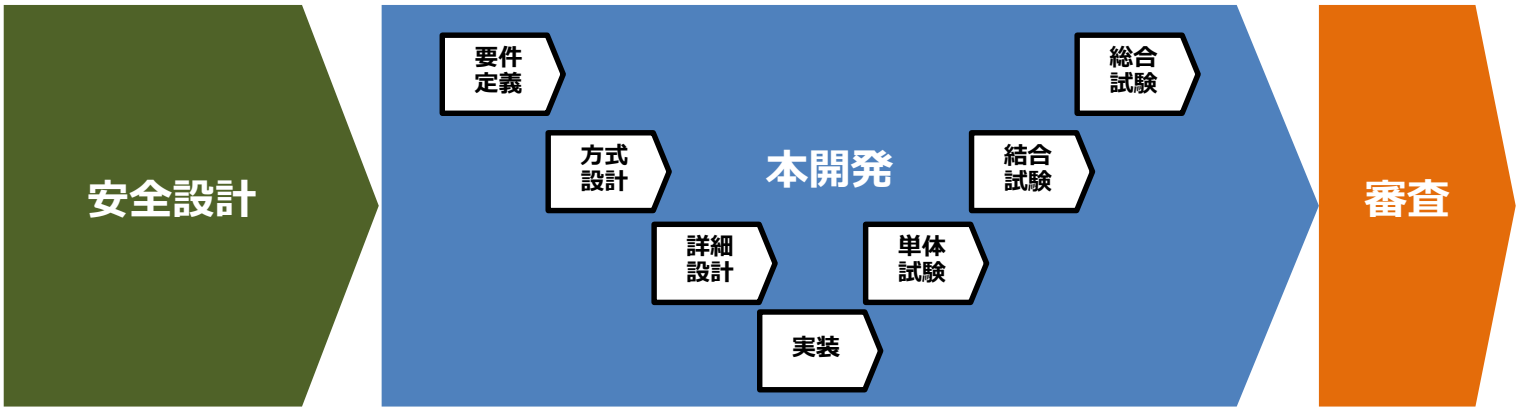
<主な機能安全規格>

機能安全に対応したソフトウェア開発の課題

HITACHI
Inspire the Next

機能安全に対応したソフトウェアの開発はコストがかかる

- 安全設計（故障のリスク分析、安全要求仕様の作成など）
- V&V(Verification and Validation:検証と妥当性確認）に基づく開発プロセス
- 認証機関による審査



機能安全に対応したソフトウェア開発の工数削減のためには
機能安全に対応したOSが必要

⇒ **TRON Safe Kernel**

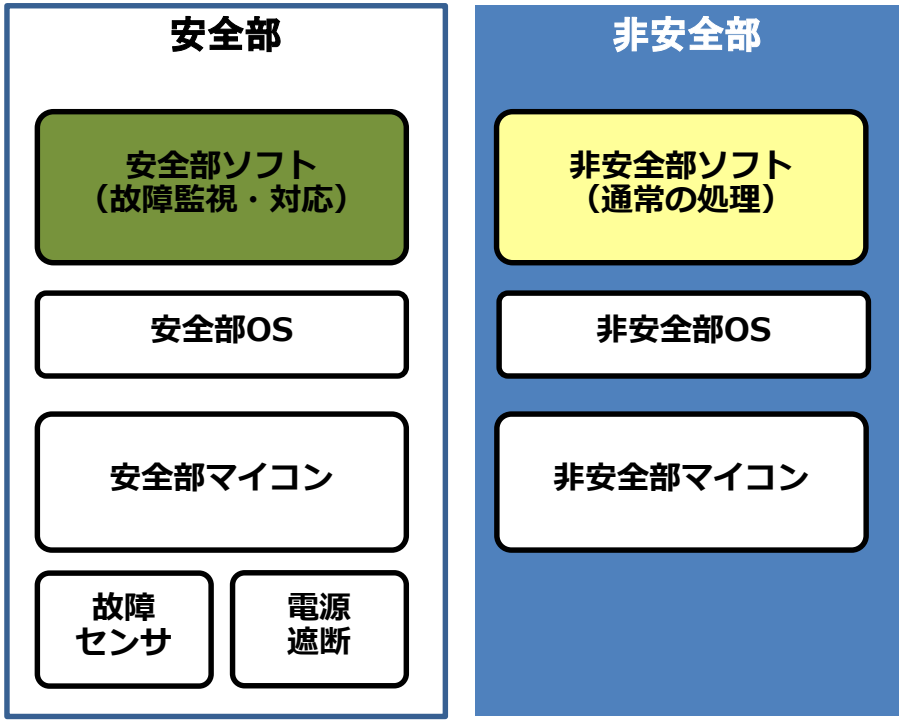
安全・非安全の分離による開発工数の低減

HITACHI
Inspire the Next

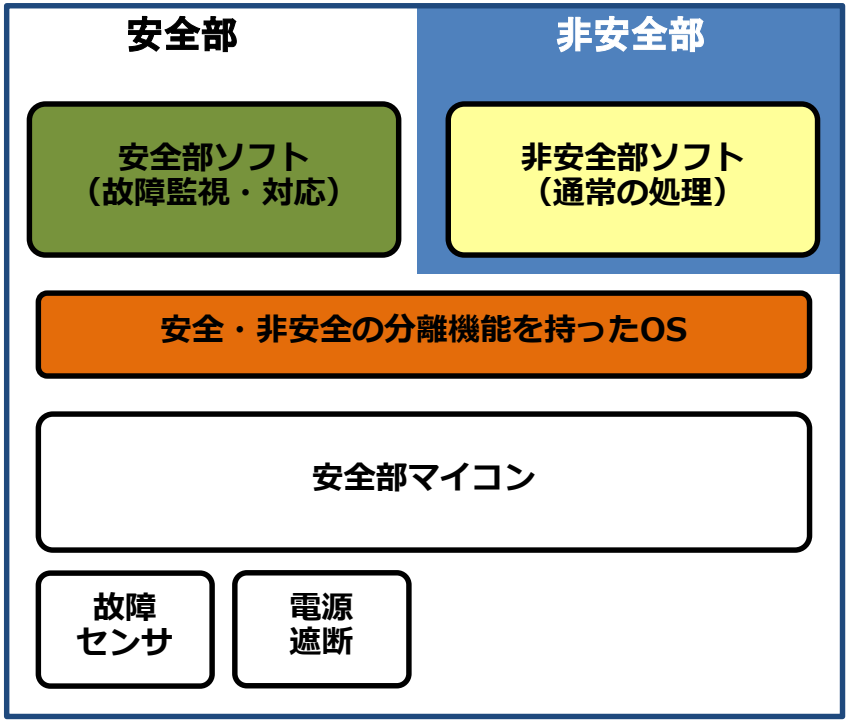
ソフトウェアを安全・非安全に分離

- 安全ソフトのみを機能安全規格に従って開発
- 非安全ソフトは、従来の開発、またはソフト資産を活用

ソフトウェアの安全･非安全分離の例



(a). ハードウェアレベルの分離



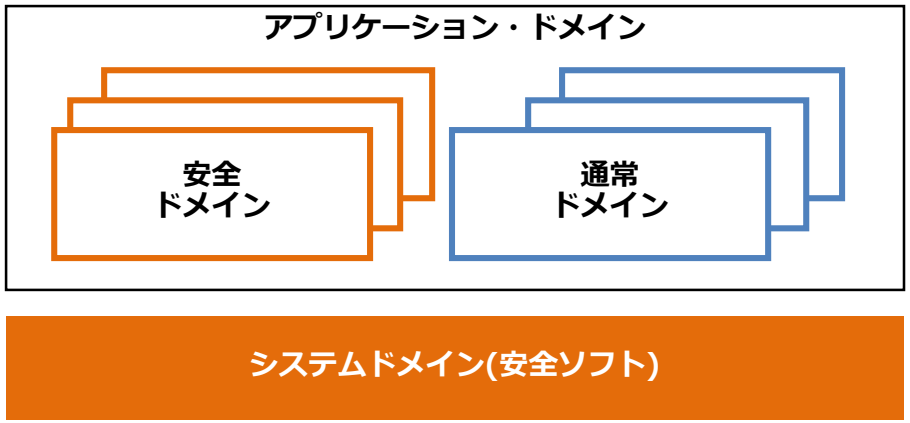
(b). ソフトウェアレベルの分離

TRON Safe Kernelによるソフトウェアの分離

HITACHI
Inspire the Next

TRON Safe Kernelは、安全水準の異なるソフトウェアを分離実行するための**ドメイン管理機能**を備える
ソフトの分離は機能安全認証を取得したOSが保証

ドメイン：　空間的、時間的に独立したソフトウェア領域 ソフトウェアはいずれかのドメインに属する	
安全ドメイン	安全アプリ(安全水準の高いアプリ、安全ソフト)が実行される
通常ドメイン	通常アプリ(安全水準の低いアプリ、非安全ソフト)が実行される
システムドメイン	システムソフトが実行される (システムソフトは、システム最高水準の安全ソフト)



TRON Safe Kernelの主な特徴

HITACHI
Inspire the Next

T-Kernel/μITRONを継承する組込システム向けRTOS
＋　**機能安全対応機能**

ソフトウェアのドメイン分離

安全水準の異なるソフト（安全・非安全）を時間的・空間的に分離

OS自体の機能安全対応

機能安全規格IEC61508 SIL３に準拠した開発プロセスと内部設計

故障検出・異常処理の対応

●**故障診断ハンドラ**、
故障診断ソフトを定期的、または任意のタイミングで実行
●**異常例外ハンドラ**
検出した故障(異常例外)に対応するを処理を実行

日立超LSIシステムズのTRON RTOSソリューション

HITACHI
Inspire the Next

- TRONフォーラムの幹事会員として、T-Kernelの様々な開発に参画
- オープンソースのT-Kernelを中心とした組込システム向けの様々なソリューションを提供しています。

[製品]
T-Kernel2.0オープンソース・パッケージ
OpenTK®

[製品]
マルチコア・マルチOSソリューション
リアルタイム・オーガナイザ
マルチコア・プロセッサで、T-KernelとLinuxを同時実行

実績

自動車分野：　カーナビ、車載メータなど各種車載機器
FA・産業分野：　製造ライン監視装置、RAIDシステム、MRI制御、電子顕微鏡など
民生分野：　携帯端末など

“OpenTK for ARM Cortex-A”

HITACHI
Inspire the Next

- オープンソースのT-Kernel 2.0のパッケージ製品を発売
- ライセンスはオープンソースのまま（商利用自由・ロイヤリティ無し）

T-Kernel 2.0オープンソースパッケージ

OpenTK® for ARM Cortex-A

- **ARM Cortex-A7,A8,A9,A15などARMv7-Aコアに対応**
- **オープンソースのリファレンスに対して機能強化**
  - メモリ保護、システムタイマのティックレス化、多重割込み管理、FPU対応など
- **オープンソースのTCP/IPプロトコルスタックを提供**
- **サンプルのデバイスドライバ等の提供**
  - 日立超LSIシステムズ製 Solution Engine G1 （RZ/G1M, Cortex-A15コア）
  - **ルネサス エレクトロニクス製 RZ/G1Eスターターキット (Cortex-A7コア)**

開発環境の展開

IARシステムズ製 ARM用統合開発環境
IAR Embedded Workbench® for ARM(EWARM) 対応

対応プロセッサの展開

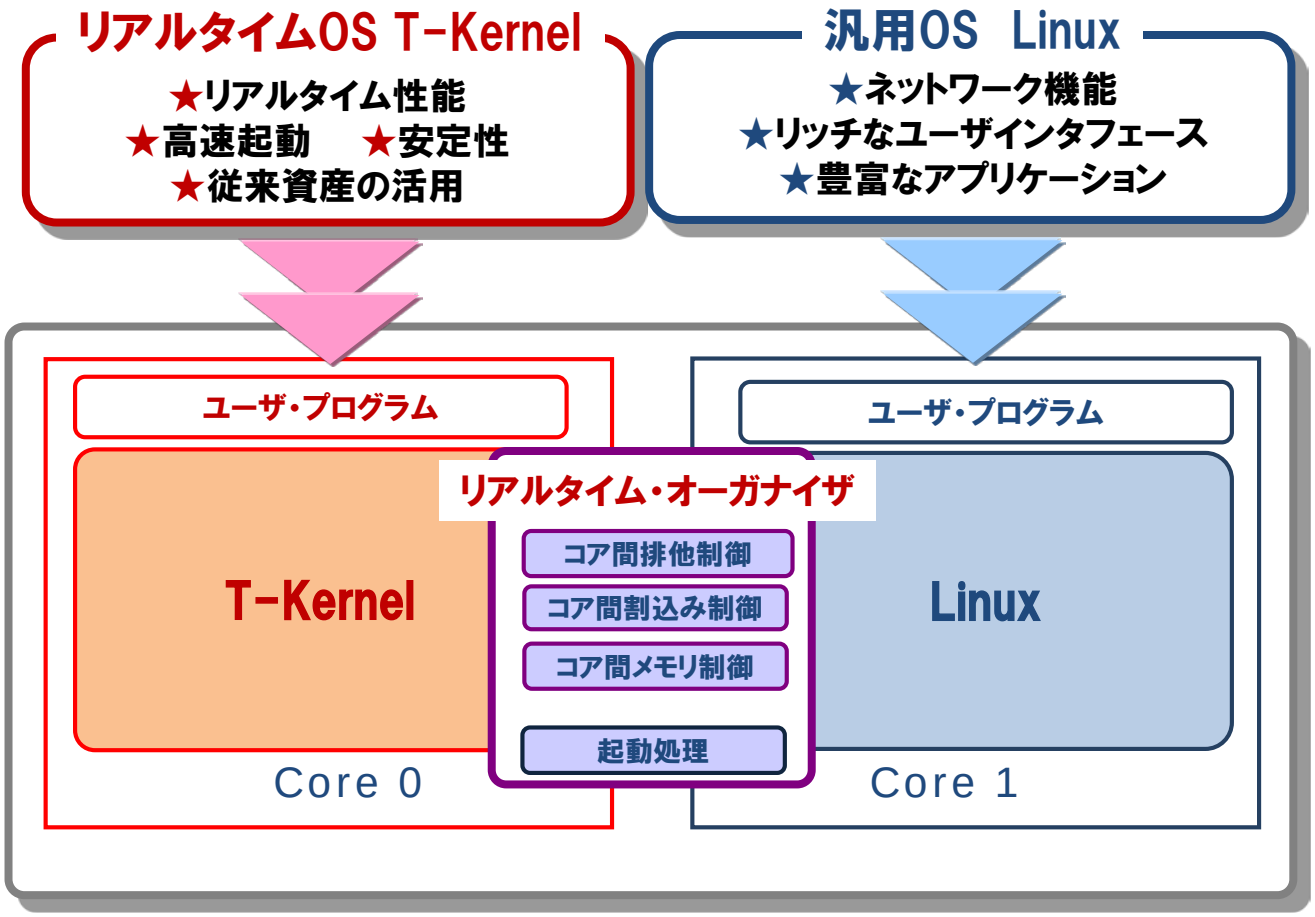
各種プロセッサへの対応を進めていきます

ARM Cortex-M、Cortex-R
64bit ARMv8-A、他

※対応プロセッサ、提供時期などはお問い合わせください

マルチコアを利用したマルチOS実行環境

- リアルタイムOSと汎用OSをそれぞれのコアで同時に実行
  - コア間の同期・通信通信のための機能を提供



リアルタイム・オーガナイザ V

HITACHI
Inspire the Next

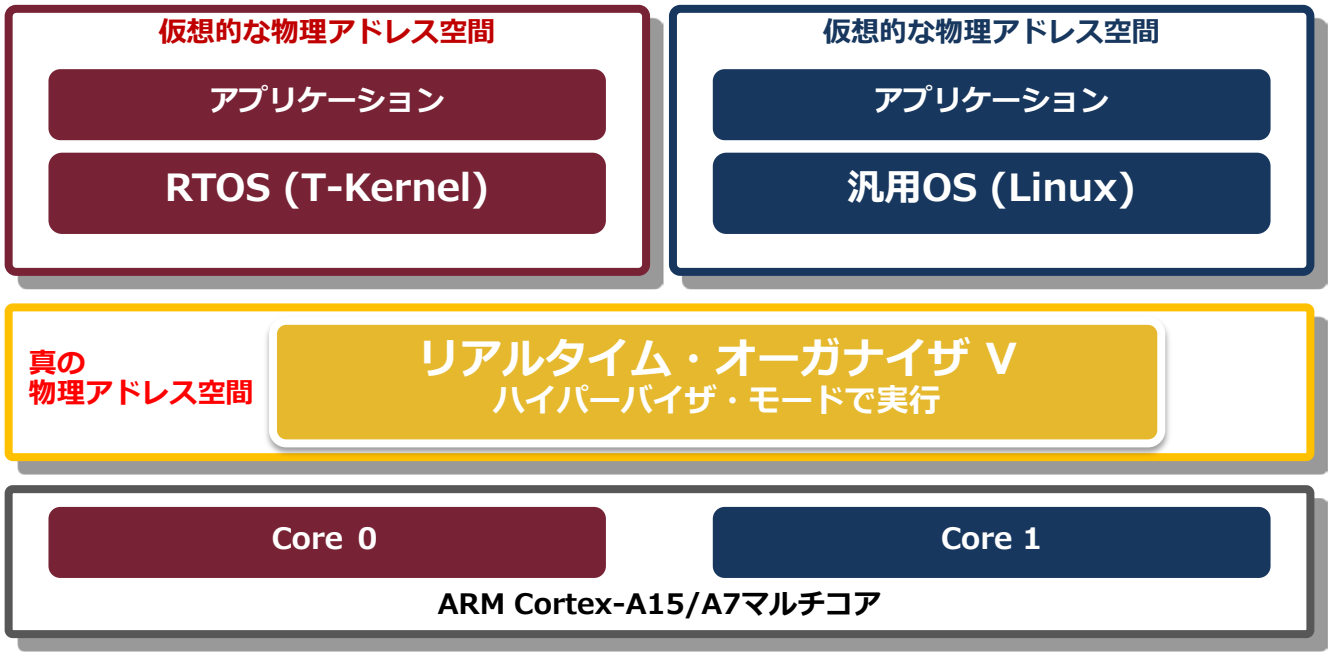
ARM Cortex-A15/A7からハードウェアによる仮想化拡張機能がサポート

- 物理アドレス空間を仮想化可能(中間物理アドレス空間)
- 従来の特権モードより優先的なハイパーバイザ・モードを提供

仮想化機能対応マルチコア・マルチOS実行環境

リアルタイム・オーガナイザ V

LinuxとT-Kernelを別々の中間物理アドレス空間で実行
⇒　OSのシステムレベルでも干渉は不可



HITACHI
Inspire the Next

END

株式会社 日立超LSIシステムズ