HITACHI
Inspire the Next

日立超LSIシステムズが提供する
機能安全OSソリューション

TRON Safe Kernel の紹介

2016/12/15

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）

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
- 機能仕様書、ソースコードがトロンフォーラムから**オープンソース**として公開（2017年予定）

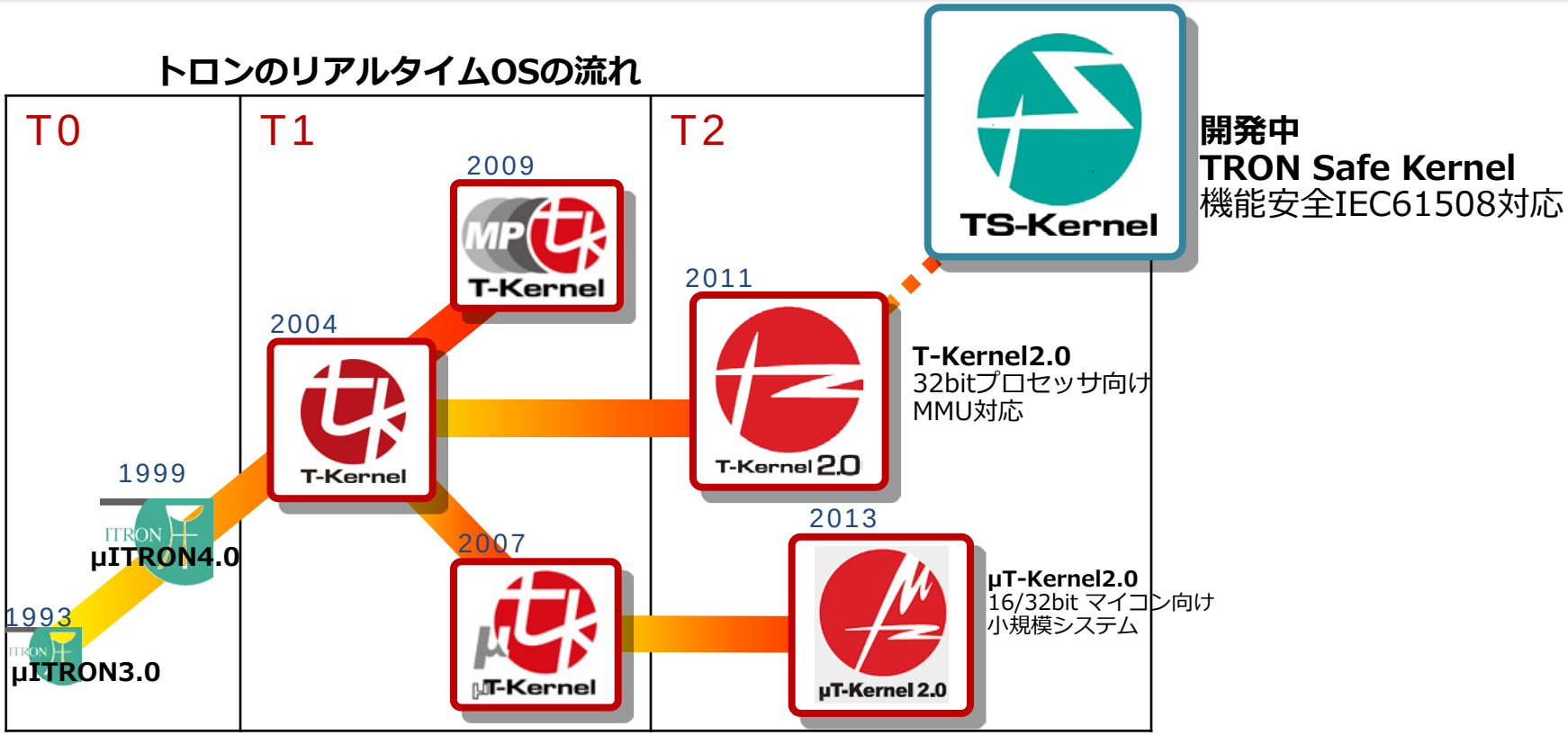
TS-Kernel

日立超LSIのTRON Safe Kernel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



TRON Safe Kernelの機能安全対応

HITACHI
Inspire the Next

TRON Safe Kernenlは、単にOSが機能安全認証に対応するだけではありません

TRON Safe Kernelの機能安全対応機能
機能安全に対応したソフトウェア開発において役に立つ機能
⇒ 機能安全対応の開発工数の低減

安全ソフト（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

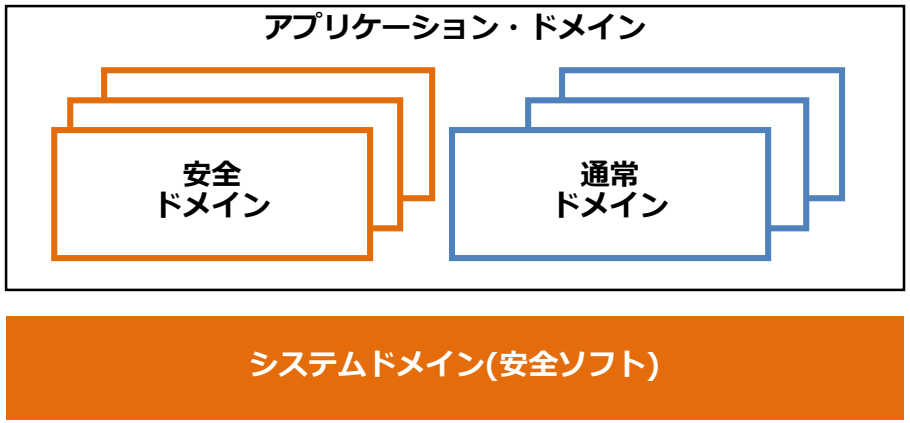
ソフトウェアを安全・非安全に分離
- 安全ソフトのみを機能安全規格に従って開発
- 非安全ソフトは、従来の開発、またはソフト資産を活用

TRON Safe Kernelのドメイン管理機能

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)



さらに様々な機能安全対応

HITACHI
Inspire the Next

■ **その他、安全ソフトをつくるために必要な機能をサポート**

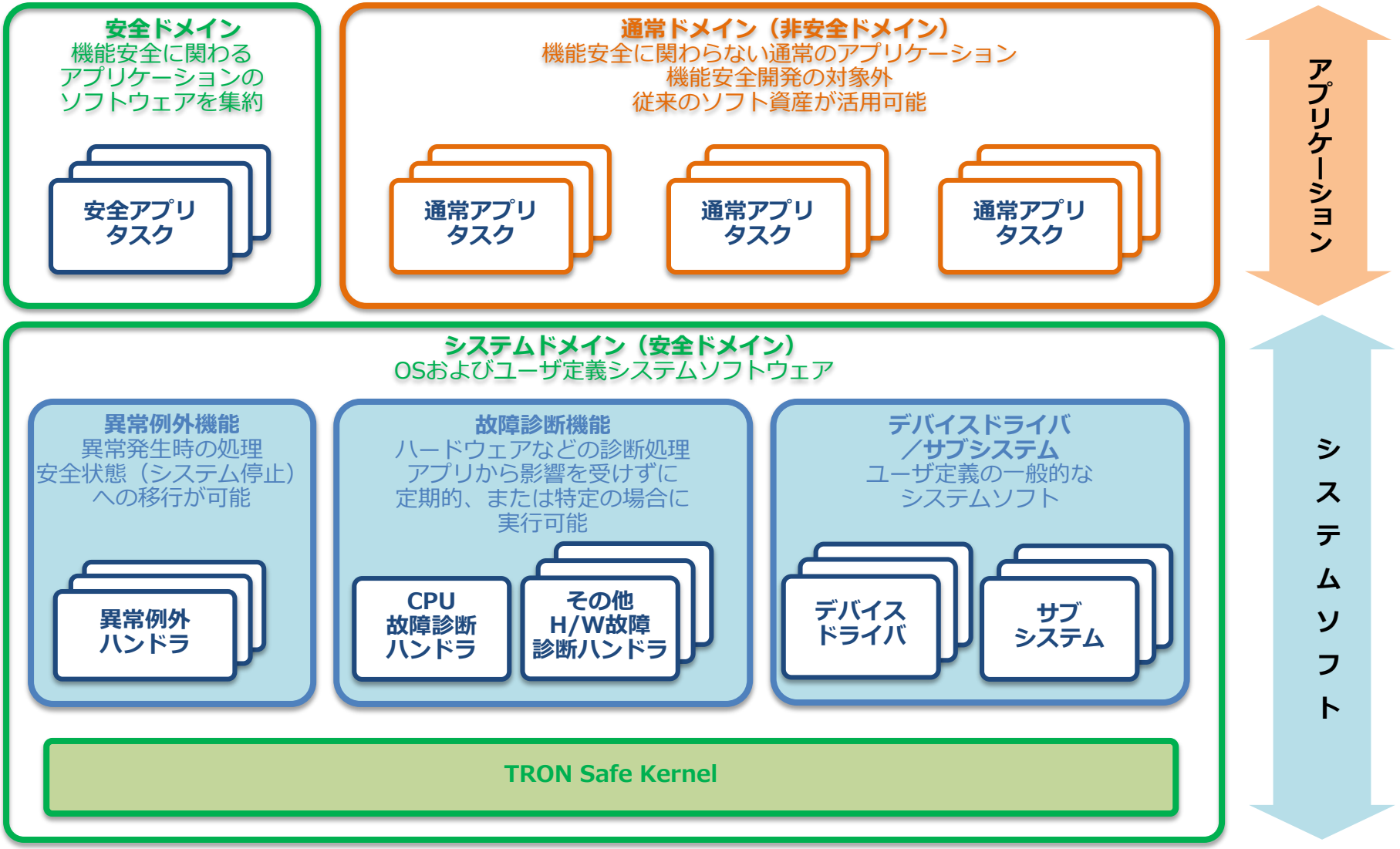
- **故障診断機能**：　システムの故障診断
- **異常例外機能**：　異常検出時の安全動作

安全ソフトをつくための枠組みはTRON Safe Kernelが提供
ユーザは実際の処理だけを作ればよい

■ **TRONのOSとしてリアルタイム性能も重視**

- リアルタイム性能に優れるリアルタイムOSとして、機能安全を実現するための様々な機能拡張

TRON Safe Kernelによるソフトウェア構成



日立超LSI製品　“OpenTK Safety”

HITACHI
Inspire the Next

TRON Safe Kernelは2017年オープンソースとして公開を目標に
トロンフォーラム　WGにて現在開発中

日立超LSIシステムズから製品化予定

TRON Safe Kernel仕様準拠　機能安全OS
“OpenTK Safety”　2017年２Q発売予定

- **機能安全規格 IEC61508 SIL3 認証取得予定**
  第三者認証機関（TuVラインランド）による認証取得

対象ハードウェア（1stターゲット）

- ルネサス エレクトロニクス製 RX631/RX63Nマイコン
  IEC61508認証取得CPUとして選択

会場、日立ブースにてデモ展示中（A-11）

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、IoTソリューション事業の一環として、
TRONプロジェクトのリアルタイムOS **T-Kernel2.0**をベースとした
製品 “**OpenTK**”を開発、販売しています。

組込システム向け
リアルタイムOS

T-Kernel2.0
オープンソースパッケージ
OpenTK
for ARM Cortex-A

T-Kernel 2.0

さらに

最新の各種プロセッサへの対応
ARM Cortex-Mマイコン
ARMv8-A 64ビット・プロセッサ

機能安全対応OS
TRON Safe Kernel

マルチコア・マルチOS対応

マルチコア・マルチOSソリューション

HITACHI
Inspire the Next

“リアルタイム・オーガナイザ”は、マルチコア・プロセッサ上で
リアルタイムOS T-Kernelと、汎用OS Linuxのマルチ OS環境を実現

新製品“リアルタイム・オーガナイザV”は、ARM Cortex-A15/A7の
仮想化機能に対応し、より信頼性の高いマルチOS環境を実現します。

会場、日立ブースにてデモ展示中（A-11）

END

株式会社 日立超LSIシステムズ