



安全セキュアなRISC-VシステムのためのGreen Hills Softwareツール

Ryan Kojima
Embedded Software Consultant
Green Hills Software

 **RISC-V Day**
Tokyo2023 Summer



© 2023 Green Hills Software Do not Distribute Without Permission from Green Hills Software

スライド1

Green Hills Software

1982年以来、組み込みソフトウェアの安全性、セキュリティ、開発者の効率性において世界をリードしてきました。

テクノロジー・イノベーター

- 安心・安全な高性能オペレーティングシステム
- 安心・安全なハイパーバイザーと仮想化サービス
- クラス最高の統合開発環境
- セキュアなデバイスライフサイクルマネジメント

クリティカルシステム向けソフトのエキスパート



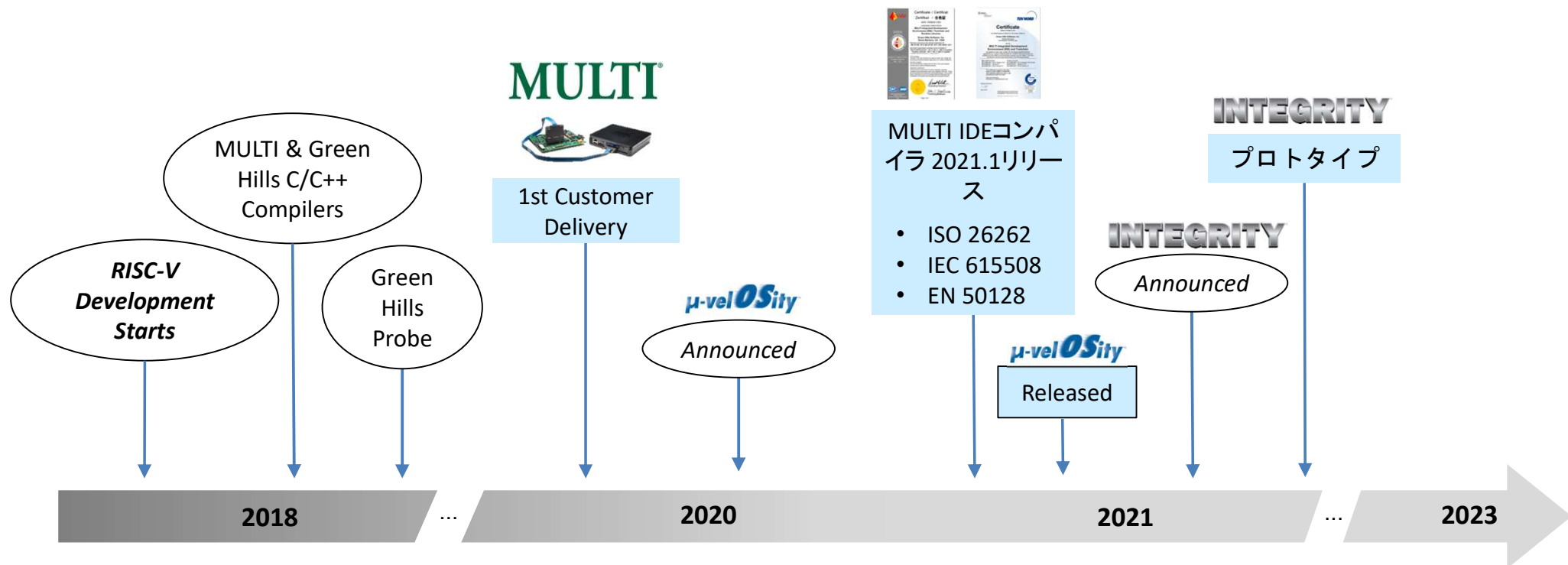
自動車、航空、Consumer、産業、
医療、ミリタリー、ネットワーク機器、ストレージ

機能安全・セキュリティ認証

- Common Criteria EAL 6+ (INTEGRITY-178)
- ISO 26262 ASIL D; IEC 61508 SIL 3;
- EN 50128 SIL 4, EN 50657; DO-178C DAL A
- Automotive Cybersecurity – ISO/SAE 21434
- CMMI Level 3 certified development teams
- ASPICE development process



Green Hills RISC-V Support Since 2018



Green Hills Software's 40 Years of Experience With CPUs

CISC

Intel x86, Pentium
 68xxx
 CPU32
 Fujitsu/Hitachi
 Mitsubishi TRON
 TRON uVPU*
 National Semi 32000
 DEC VAX
 Confidential

CISC / RISC

PowerPC 64-bit*
PowerPC 32-bit
Renesas V850
 VLE
 ColdFire
 MCore
 Intel i960
 Intel i860
 Hitachi SH-1/2/3/4
 Fujitsu FR
 Denso NDR
 Fairchild Clipper
 Confidential

RISC

ARM 64-bit*
ARM 32-bit*
Thumb / Thumb2
Infineon TriCore
RISC-V
 MIPS-16/32/64/X
 Xscale
 microMIPS
 Sun SPARC
 Fujitsu SPARClite
 Sony nCPU
 TRW RH32
 DEC Alpha
 Motorola 88000
 Denso NDRx
 Toshiba CORE1
 Renesas M32R

DSP

Starcore*
 PPC Altivec*
 ADI Blackfin
 Renesas SH-DSP
 BCM Firepath*
 LSI ZSP
 STM ST100
 Sony pDSP2
 Sony VectorEngine*
 Lexra Radiax
 Intrinsity Fastmath

Legend

Bold Currently popular or trending

* Includes vector support from Green Hills

Green Hills Softwareが提供するRISC-V向けソリューション

MULTI	MULTI® IDEとTimeMachine™ ▪ C/C++コンパイラとランタイムリブの最適化 ▪ マルチコアデバッグとトレース ▪ アドバンスドデバッグング	ヘテロジニアス・マルチ コアIDE C/C++コンパイラ
	ハードウェアデバッグ - JTAG/Trace ▪ マルチユーザー、高速、JTAG、トレースボードのブリングアップとデバッグング	Debug 1.0 UltraSoC Trace N-Trace
INTEGRITY	INTEGRITY Real-Time Operating System	分離カーネル RTOS
μ-velOSity	μ-velOSity Real-Time Operating System	スモールマイクロカー ネル RTOS
	エンジニアリング・コンサルティング	トレーニング、コンサル ティング



ISO 26262
ISO/SAE 21434



EN 50128
EN 50657



RISC-VのGreen Hillsツールチェーンサポート

RISC-V ISA(ベース+エクステンション)をサポート。

- 32 and 64-bit: rv32i, rv64i
- “A” Atomic instructions
- “B” Bit manipulation. Also “Zb...”
- “C” Compressed instruction set
- “F, D,” Single and double precision floating point
- “G” IMAFD Zicsr Zifencei
- “H” Hardware hypervisor (*planned*)
- “I” Base integer unit
- “M” Multiple and divide unit
- “OS” privileged instruction set
- “P” Packed SIMD instructions (*planned*)
- “Q” Quad precision floating point in assembler
- “V” Vector instructions, Also “Zv...” and “Zve...” in assembler
- “Zfhmin” Minimal half-precision floating point
- “Zfh” Half-precision floating point
- “Zfinx” Single-precision FP in integer registers
- “Zdinx” Double-precision FP in integer registers
- “Zc” Extended compress instructions (*planning*)
- “Zi” Control & Status Register; Instruction Fence

2種類の カスタムRISC-Vアセンブリ命令オプション

- 1) ユーザーがコンフィグファイルで新しいアセンブリ命令を定義する
 - 高速プロトタイピングに最適だが既存のRISC-V ISA シンタックスに制限される
 - コンパイラからIntrinsic functionとしてアクセス可能
 - Green Hills社製アセンブラ、デバッガ、シミュレータに対応
- 2) Green Hills、ツールチェーンにカスタムインストラクションを追加
 - 最も高度に最適化され、RISC-V以外の構文も扱える。
 - Green Hills、デバッガ、シミュレータに対応。
 - コンパイラは、可能な限り新しいアセンブリ命令を利用
 - グリーンヒルズのNightly Build ・ Validation Systemに組み込み

Debug and Trace

DM 1.0, RISC-V External Debug, Coresight Debug
N-Trace – waiting for hardware to test
UltraSoC Trace – engineering release

2023年3月28日

Production Software Tools and Design

INTEGRITY

RTOS – SEooC

- Green Hills Safety Layer – SEooC
- Common Architecture BSP – SEooC
- Production BSP
- Safety Qualified BSP

SEooC: “Safety Element out of Context”

μ-velOSity

RTOS – SEooC

μ-visor

Hypervisor – SEooC

MULTI

IDE Qualified for FuSa Development

- C/C++ compilers and toolchain
- Run-time libraries

**Safety
&
Security
Services**

Design, Develop & Deliver:

- Certification Support Package
 - Safety manuals, TARA, confidence-in-use reports
- Safety architectures, technical safety workshops

Production Deployments



ISO 26262 (ASIL D)
IEC 61508 (SIL 3)
DO-178B/C (DAL A)
EN 50128 (SIL 4)
ISO/SAE 21434



INTEGRITY® RTOS 安全でセキュアな分離カーネル

• 高度なRTOSアーキテクチャ

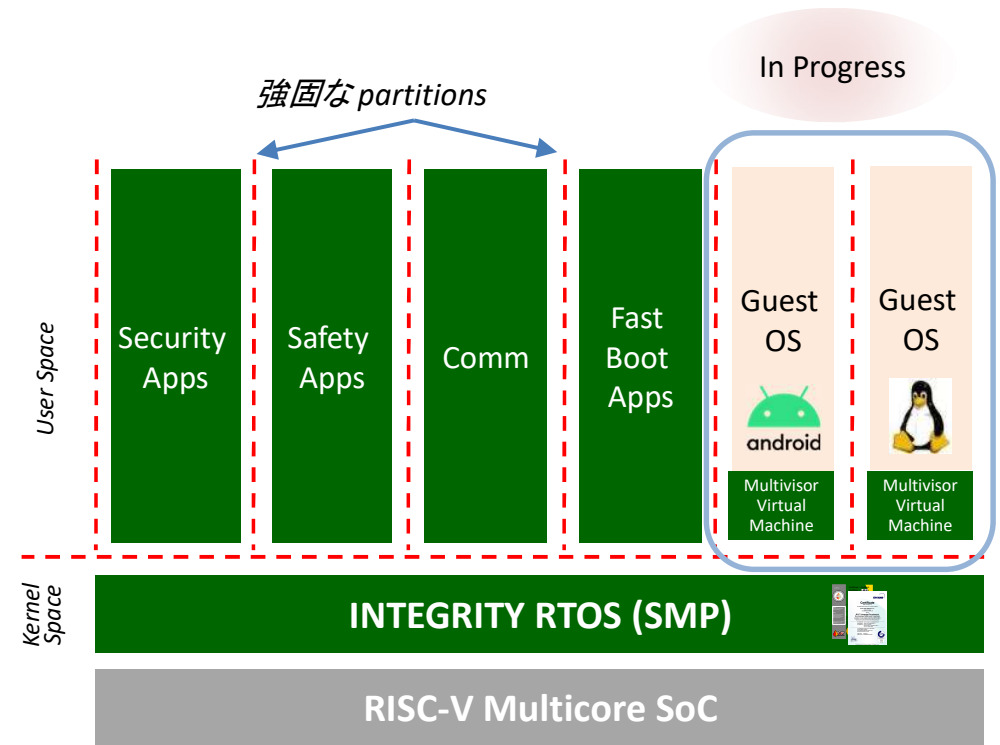
- 分離カーネルアーキテクチャ
- リソース保証のリアルタイムスケジューラ
- 高度なマルチコア SMP サポート
- Capabilities-based セキュリティモデル (最低限の権限)
- マイクロカーネルのサービスとして動作するセキュアハイパーバイザ
- リアルタイムデターミニズム
- 少ないシステムメモリ要求

• 証明された、認証済みの分離設計

- Common Criteria EAL 6+, 世界最上位のセキュリティ認証に対応 (INTEGRITY-178)
- ISO 26262 ASIL D; IEC 61508 SIL 3; EN 50128 SIL 4
- Highest FAA certifications
- Automotive Cybersecurity – ISO 21434 CAL4 (2021)

• 拡張性に優れたミドルウェアとエコシステム

- Full Ethernet Host/Router Stack, AVB/TSN, DoIP, SOME/IP
- File systems, Graphics, Wired/Wireless Connectivity, Stateful Firewall, SSL/TLS, IPsec IKE v2, SSH
- AUTOSAR Adaptive + AUTOSAR Classic
- ROS2 Clean Room Support, Data Distribution Service (DDS)



Contact Green Hills for Availability

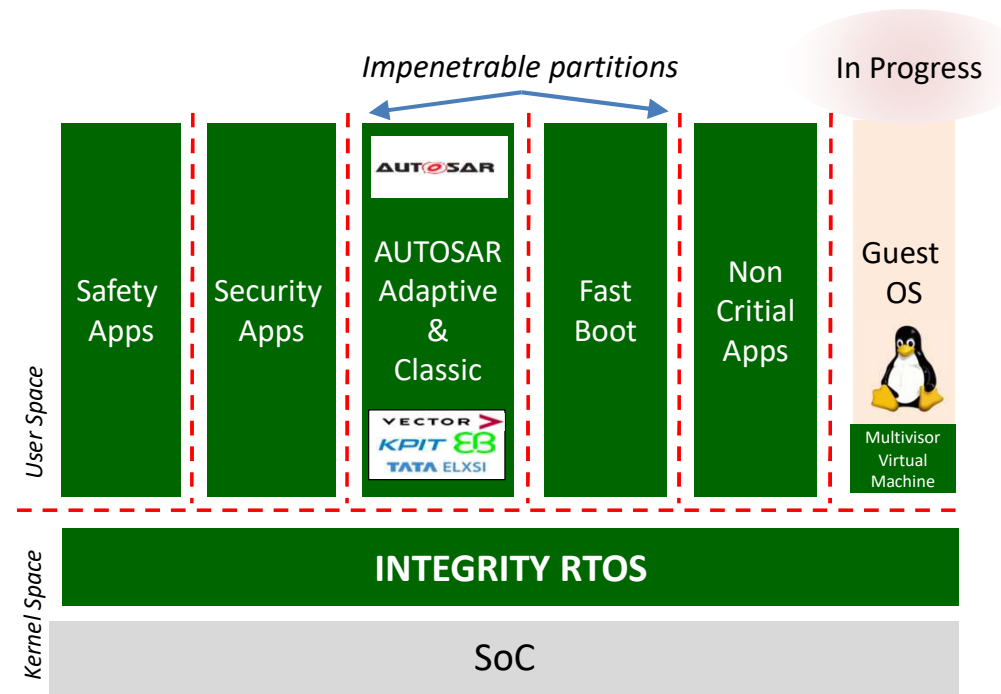
INTEGRITY RTOS機能概要

設計上の特徴

- ハードリアルタイムデターミニズム
- 時間・メモリ空間のパーティショニング
- スタックとアプリケーションの分離
- 許可ベースのセキュリティモデル(Least-Privilege)
- 重要なソフトウェアへのプロセッサリソース保証
- パーティションとデバイス間のアクセス制御は必須
- 情報フロー制御

メリット

- 異なるクリティカルレベルを持つ機能を同一コアで容易に実行可能
- Linuxや他のOSの安全な仮想化
- エラーや攻撃をパーティション内に留める
- フォールトリカバリーの提供
- 最小限のカーネルサイズと高速ブート
- 安全に分離されたミドルウェア
- POSIX、C++、AUTOSAR準拠



ISO 26262 ASIL D (Automotive)
ISO/SAE 21434 (Automotive Cybersecurity)
IEC 61508 SIL 3; EN 50657 (Industrial)
EN 50128 SIL 4 (Railway)
DO-178C DAL A (INTEGRITY-178 airborne)

μ-velOSity リアルタイムオペレーティングシステム

Cortex-M33、Cortex-M7、RISC-VなどのMCU向けRTOS

最速の実行速度と起動時間、最小のメモリフットプリント

- 設定可能な優先順位ベースのタスクスケジューリング
- IPCのための効率的なメッセージキュー
- 浮動小数点演算とMPU (Memory Protection Unit) をサポート
- No-OS (ベアメタル) からのコード移行が容易

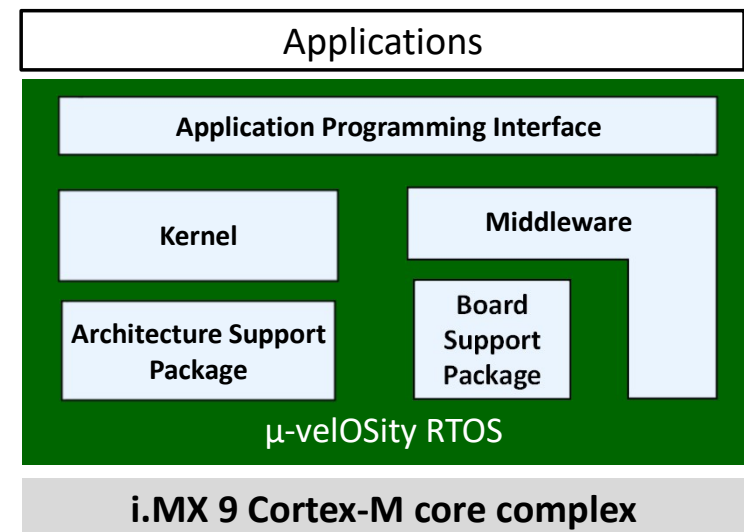
安全・セキュア

- SEooCとしてSIL/ASIL FuSa認証取得(2023年予定)
 - IEC 61508 SIL 3/4
 - EN 50128 / EN 50657 SIL 4
 - ISO 26262 ASIL D
- 自動車・産業用サイバーセキュリティ(2023年予定)
 - ISO/SAE 21434 CAL4, IEC 62434-4.1
- ISO 9001、Automotive SPICE PAM v3.1 (VDA Scope)のプロセス。



統合されたミドルウェア対応

クラス最高のMULTI IDEとC/C++コンパイラを統合。



μ-velOSity 採用例

- オートモーティブエアコン、スマートe-Fuse
- 輸液ポンプ、ワイヤレスバイタルサインモニター
- 民間航空機の客室管理システム
- エンタープライズクラスのSSDとRAIDコントローラ
- ワイヤレスセンサモジュールプラットフォーム
- GPS衛星通信リンクモジュール
- 非常用発電機

MULTI® 統合開発環境

シリコン、シミュレーター、エミュレーター用

難しいバグを素早く見つける

- 複数のヘテロジニアスコアにまたがるシングルデバッガーセッション
- 過去にさかのぼって最難関の問題を探す
- システムイベントの可視化と高度なイベントロギング - "How did I get here?"
- INTEGRITY、μ-ve/OSity、Linux、AUTOSAR、その他に対応したOS-Agnostic。

高品質で最適化されたコードをデプロイする

- MISRA Cアドヒアランスチェッカー
- ランタイムエラー検出とメモリリーク検出
- DoubleCheck® ソースコードアナライザ、コードカバレッジとパフォーマンスプロファイラ
- コントロールフローインテグリティ(CFI)およびSEI CERT-Cルールの実施



システム内で統合して制御する

- 命令セットシミュレータ内蔵
- フラッシュプログラミング
- プロジェクトビルダーとmakefileのインターフェース
- 外部プログラムによる制御のためのPython API
- MathWorks MATLAB/Simulinkのモデルを組み込みターゲットで実行する

最高のFuSaレベル

- C/C++コンパイラとライブラリの最適化
- 安全システム開発の認定を取得

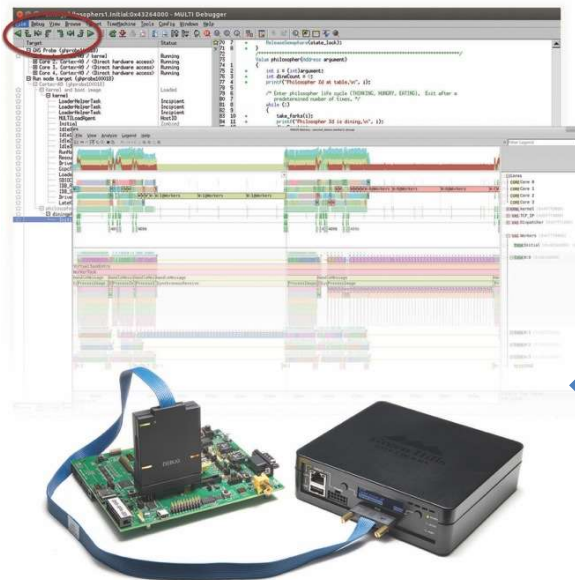


機能安全認証

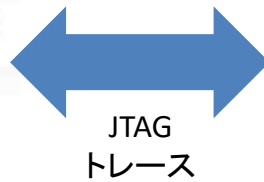
ISO 26262 ASIL D (自動車用)
ISO/SAE 21434 (自動車用サイバーセキュリティ)
IEC 61508 SIL 3; EN 50657 (工業用)
EN 50128 SIL 4 (鉄道)

ヘテロジニアスマルチコアでの統一デバッグを実現

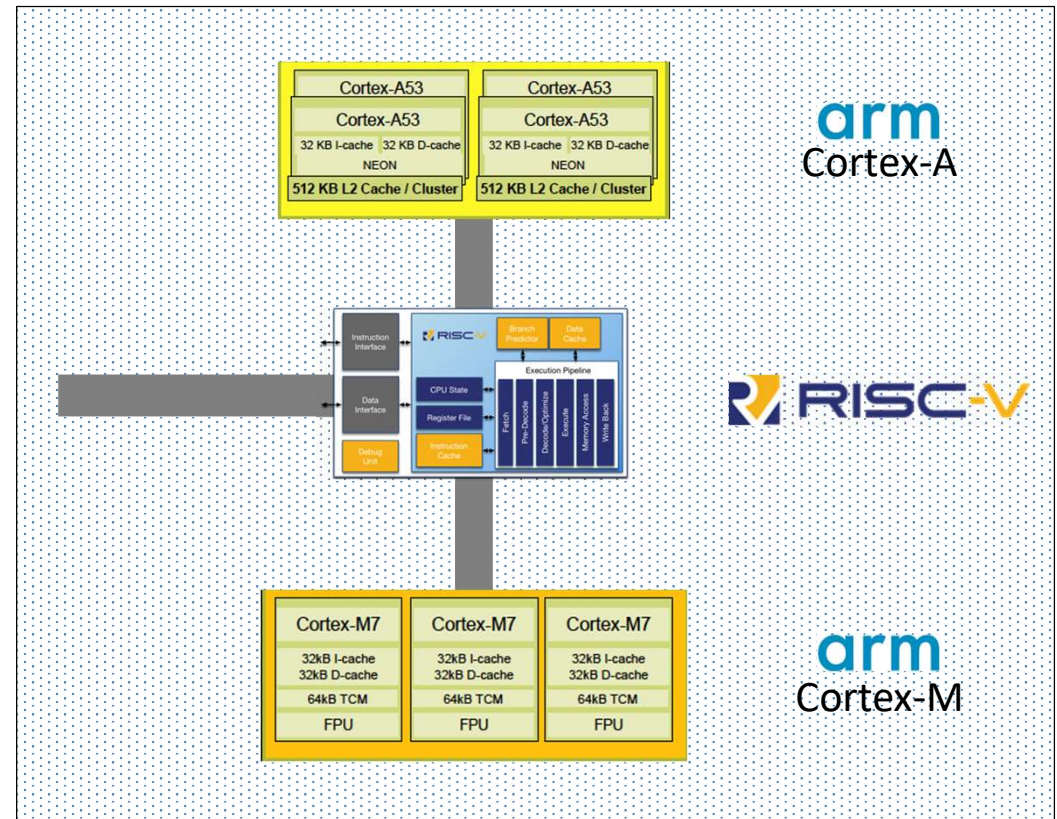
MULTI Debugger + History + TimeMachine



JTAG/Trace用Green Hillsプローブ



異種コアの同時統合デバッグ＋
システム可視化

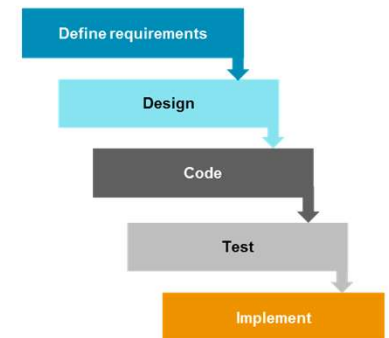


MULTIは、DEBUGとOPTIMIZATIONのための3つの強力な機能を装備

1. **TimeMachine**は、トレースデータを使って、時間の前と後ろの両方でデバッグを行うので、難しいバグも素早く見つけることが可能
2. **History View** を用いて、プログラムがどのようにしてここまで来たのか、そのためにシステムは何をしたのか把握
3. **Debug Snapshot** で、デバッグとヒストリーのセッションを保存し、同僚と簡単に共有



Waterfall



グローバルな規模での
コレボレーションに最適なツール
アジャイルまたはウォーターフォールで

その他の情報

プレス

- アンデス・テクノロジーとグリーンヒルズ・ソフトウェアが提携し、RISC-V向けの先進的な自動車用安全プラットフォームを実現
 - 2022年9月、[リンク](#)
- NSITEXEとGreen Hills Software、RISC-Vソリューションで提携
 - 2022年12月、[リンク](#)
- グリーンヒルズ・ソフトウェア、INTEGRITYをRISC-Vアーキテクチャ向けに拡張。
 - 2021年10月、[リンク](#)
- Green Hills Software、RISC-VベースSoC向けの豊富な製品ポートフォリオにRTOSサポートを追加
 - 2020年12月、[リンク](#)
- Green Hills Software、業界をリードする高度なソフトウェア開発ツールのRISC-Vへの対応を追加
 - 2020年6月、[リンク](#)



ウェブ

- RISC-V組込み[ソフトウェアソリューションリンク](#)

Green Hills Solutions Summary for RISC-V

- 40 年に及び組み込み業界での経験とテクノロジー
- 30年に及ぶグラフィカルなデバッグと非対称マルチコアSoCのサポート
- 25年に及ぶ安全セキュア、高信頼のRTOS
- 20年に及ぶ最高レベル機能安全認証済みのソフトウェアソリューション
- コードの状態を高度に把握し過去に戻ることができるデバッグ
- 生産性を最大限に高める包括的IDE
- RTOS、ハイパーバイザと高度に統合された開発ツール群
- グローバル・プロフェッショナルなサポートサービス

