INTEGRITY RTOS

最も安全・セキュアで、信頼性の高いRTOS

Green Hills® SOFTWARE

最も安全・セキュアで、信頼性の高いRTOS

Green HillsのRTOSファミリのフラッグシップであるINTEGRITY® リアルタイムOS（RTOS：Real-Time Operating System）は、マイクロカーネルアーキテクチャを中心に構築されており、組み込みシステムに対して完全な信頼性、絶対的なセキュリティ、認証済みの安全性を備えた唯一のソフトウェア基盤を提供します。INTEGRITYは、さまざまな産業分野において安全性、およびセキュリティのために世界で最も多く認証されたRTOSであり、RTOSの基準を確立しています。

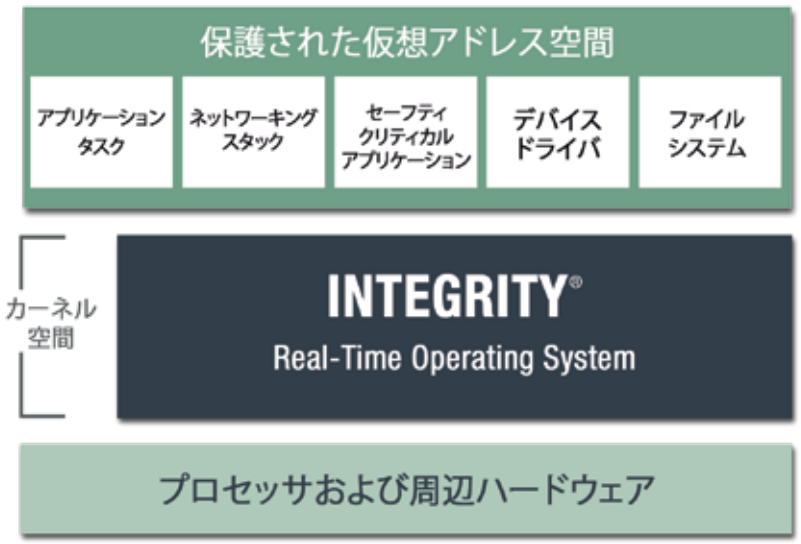
プロジェクトの開発フェーズにおいて、INTEGRITYはMULTI®統合開発環境（IDE: Integrated Development Environment）と密接に統合されており、開発者に対して高度なマルチコア開発ツールを提供します。これにより、困難なバグの発見と修正にかかる時間を短縮し、より高品質なコードを量産製品に展開することが可能になります。

最高レベルの要求事項を満たすために

INTEGRITYは、開発者がアプリケーションプロセッサ上でセキュリティ、安全性、性能、および信頼性に関する最高レベルの要求事項を満たせるように設計されています。これを実現するために、INTEGRITYは次の機能を提供します。

- メモリ保護による分離
- プロセッサリソースの保証
- ハードリアルタイムデターミニズム
- 高度なマルチコア活用とデターミニズム
- Linux、Androidなどをホストできるセキュアハイパーバイザ
- POSIX、およびAUTOSARに基づく標準サポート

この実現のために、INTEGRITYはハードウェアメモリ保護を利用し、組み込みアプリケーションを隔離・保護するセキュアパーティションを作成します。セキュアパーティションは、各タスクに正しく実行するために必要なリソースを保証し、オペレーティングシステム、およびユーザタスクを異常、または悪意あるコード（サービス拒否攻撃、ワーム、トロイの木馬など）から完全に保護します。他のメモリ保護型オペレーティングシステムとは異なり、INTEGRITYはセキュリティや保護のために、リアルタイム性能を犠牲にすることは決してありません。



INTEGRITYアーキテクチャは、複数の保護された仮想アドレス空間をサポートしており、それぞれの空間には、複数のアプリケーションタスクを含めることができます。

統合プラットフォーム

特定の産業分野向けに、Green Hillsは完全に統合されたエコシステムを提供するプラットフォームを用意しています。各プラットフォームには、INTEGRITYに加え、開発ツール、業界固有のミドルウェア、リファレンスハードウェア、およびドキュメントが含まれています。プラットフォームは、以下の分野向けに提供されています。

- 自動車
- セキュアIoT
- アビオニクス
- 産業用安全システム
- ソフトウェア無線
- 医療機器

中心となるソフトウェア、およびドキュメントすべてが、高度に統合されたプラットフォームに組み込まれていることで、開発者は次のことが実現できます。

- より迅速なターゲット機器の開発や出荷
- 市場投入時間の短縮
- 開発リスクの低減
- 品質とイノベーションをより重視

保証されたセキュリティ

INTEGRITYは、組み込み設計者が分離、ダメージ制限、情報フロー制御のポリシーを実施するために必要な、すべての機能を提供します。また、INTEGRITYは今日のコネクテッドアプリケーション向けに、ネットワーキング機能と最新のセキュリティプロトコルも提供します。

INTEGRITYのセパレーションカーネルアーキテクチャは、セキュリティクリティカルな機能を分離するための極めて堅牢なメカニズムを提供します。INTEGRITY-178 RTOSは、商用オペレーティングシステムとして達成された最も厳格なセキュリティ評価である、コモンクライテリア EAL6+ High Robustnessに認証されています。

INTEGRITYは、プロセスが割り当てられたメモリ領域を超えた書き込みを防止することにより、異常、または悪意あるコードによる損傷を防ぎます。さらに、INTEGRITYのパーティションは、データが存在するパーティションの外部からの意図しないアクセスを防止します。

信頼性のためのアーキテクチャ

従来型のオペレーティングシステムは、クラッシュ、ロックアップ、制御不能な動作を引き起こし、衛星の喪失、車両の停止、医療モニタの故障といった高額な損失をもたらす可能性があります。しかし、INTEGRITYはこれらの障害を引き起こす不具合から、クリティカルなアプリケーションとOS自身の両方を保護します。

これを実現するために、INTEGRITYはシステムリソースを保証しており、他のどのプロセスが利用しようとしても、CPU時間とメモリリソースが各プロセスに常に利用可能であることを確実にします。

悪意ある、または意図しないイベントは、システムリソースへのアクセスを拒否し、システムプロセスの正常な実行を妨げる可能性があります。これらのサービス拒否（DoS）攻撃を防ぐために、INTEGRITYは各プロセスに対してCPU時間とメモリの固定リソースを割り当てることができます。特定プロセスのために時間枠を保証することで、これらの固定リソースは、実行中のタスクが自身に割り当てられた時間枠を超えて動作することを防ぎ、他のプロセスの整合性を保護する役割も果たします。

抽象化レイヤとミドルウェア

製品開発を迅速に開始できるようにするため、Green HillsはINTEGRITYに統合・検証された幅広いミドルウェア、および抽象化レイヤを提供しています。提供されている抽象化レイヤ、およびミドルウェアには、次のようなものがあります。

ランタイム環境向け抽象化レイヤ

- Linux, Android
- POSIX
- AUTOSAR Adaptive, AUTOSAR Classic
- Java
- ROS 2

ミドルウェア

- Communication & connectivity
- Secure networking & data storage
- Embedded firewall
- File systems
- OTA software updates
- GUI development kits
- Data Distribution Service (DDS)
- Web services
- Databases

安全性、およびセキュリティ認証

INTEGRITYの技術は、25年以上前のリリース以来、その卓越した実績を裏付ける数々の認証、および認可を取得してきました。これにより、開発者は安全性、セキュリティ、信頼性において最高レベルの要件を満たすことが可能になります。

- **FAA:** DO-178B/C DAL A（INTEGRITY-178, INTEGRITY-178 tuMP）
- **NSA:** SKPP High Robustness and Common Criteria EAL 6+—the highest security level ever achieved for an operating system（INTEGRITY-178）– and Raise the Bar（RTB）for Cross Domain Solutions（CDS）
- **FDA:** Class II and Class III medical device approval
- **Industrial safety:** EN 50128/50657 SIL 4, IEC 61508 SIL 3
- **Automotive:** ISO 26262 ASIL D and automotive cybersecurity standards as defined by ISO/SAE 21434 CAL 4 and UNECE WP.29 CSMS

ハードリアルタイムデターミニズム

INTEGRITYは、真のハードRTOSであり、セキュリティや保護のためにリアルタイム性能を犠牲にすることは決してありません。INTEGRITYは、常に最優先の割り込みを絶対最小待ち時間で処理します。

INTEGRITYのカーネルサービスは、すべてシステムコールのオーバーヘッドを最小化するよう最適化されています。システムコールは、他のプロセスの実行を許可するために一時停止できる仕組みを持ちます。また、INTEGRITYは複数の優先度レベルをサポートするリアルタイムスケジューラを使用しており、CPUの使用割合を完全に制御できる設計になっています。

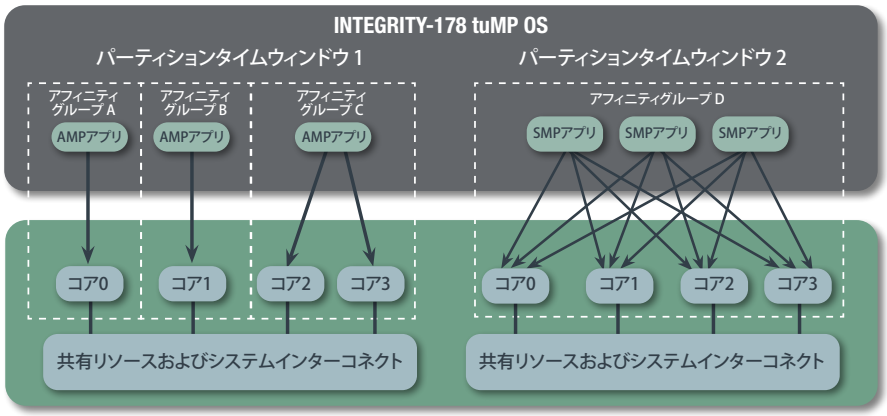
クリティカルなデッドラインを守るために

INTEGRITYでは、カーネルアプリケーションから要求されたサービスを実行するために、システム設計者が指定したCPU時間リソースのみを使用します。INTEGRITYが予期しない実行時間を防ぎ、デターミニズムを提供するもう一つの方法は、アプリケーションが行うあらゆる操作に関係なく、カーネルサービス時間を制限することです。

また、INTEGRITYはHighest Lockerセマフォを提供し、優先度逆転を防止します。優先順位の逆転は、優先順位の低いタスクが優先順位の高いタスクを不確定の時間拒否した時に、デッドライン違反、および実行エラーを引き起こす可能性があります。

パーティション単位のスケジューリング

INTEGRITY-178 tuMP™は、システムインテグレータに対して、シンプルな非対称型マルチプロセッシング（AMP: Asymmetric Multi-Processing）から、近代の対称型マルチプロセッシング（SMP: Symmetric Multi-Processing）、そして最大限のデターミニズムと効率性を兼ね備えた限定型マルチプロセッシング（BMP: Bound Multi-Processing）まで、幅広いソフトウェアマルチプロセッシングアーキテクチャを選択できる柔軟性を提供します。ARINC 653 Part 1 Required Services Supplements 4 & 5の最新版を満たすには、何らかの形式のBMPが必要です。INTEGRITY-178 tuMPは、DAL AレベルでARINC 653サポートの一環としてSMPおよびBMP機能を提供する唯一のRTOSです。



INTEGRITY-178 tuMPの時間変動機能により、異なるパーティション時間枠のコアに対してアプリケーションを割り当てることが可能になります。

保証されたメモリリソース

INTEGRITYは、次のような障害からメモリを保護します。

- メモリ枯渇
- メモリ破壊
- メモリへの不正アクセス

INTEGRITY独自のメモリ割り当てシステムにより、あるアドレス空間が他のアドレス空間のメモリを枯渇させることを防ぎます。

十分なカーネルメモリを確保できるように、INTEGRITYはプロセスの要求に応じて生成されるメッセージ、セマフォ、または他のカーネルオブジェクトにカーネルメモリが使用されないよう要求します。その代わりにカーネルは、要求元のプロセスが提供するメモリリソースを用いて、プロセスにより要求されたすべてのサービスを実行します。

ユーザスタックのオーバーフローを避けるために、INTEGRITYのカーネルは独自のメモリスタックを持ちます。これがなければ、カーネルがユーザプロセスのスタックにアクセスする必要が生じることになります。ただし、ユーザプロセスが未知のコード（つまりカーネル）による使用の影響を受ける場合、最大スタックサイズを予測することは不可能なため、これにより問題が発生する可能性があります。

マルチコアと組み込み仮想化

INTEGRITYは、ソフトウェアシステム設計者に対し、マルチコアプロセッサの最大性能と制御を引き出す魅力的な選択肢を提供します。INTEGRITYの柔軟な展開モデルは、AMP、SMP、BMPを含み、さらに仮想化技術であるINTEGRITY Multivisor®を統合することで、現代のマルチコアSoC向けに新たなソフトウェアアーキテクチャを実現します。

高度なマルチコアサポート

INTEGRITYのマイクロカーネルアーキテクチャは、組み込みシステム向けに設計されたマルチコアプロセッサに最適です。INTEGRITYは、完全な非対称型マルチプロセッシング（AMP）と対称型マルチプロセッシング（SMP）を提供し、INTEGRITY-178 tuMPは、さらにタスクを特定コアに割り当てて制御を強化する限定型マルチプロセッシング(BMP)も提供します。これらのオプションにより、組み込みシステム設計者は、マルチコアの利用とデターミニズムを最大限制御できます。

さらに、Green HillsのMULTIツールスイートに搭載された高度なマルチコアデバッグ機能と組み合わせることで、開発者は市場投入時間を短縮した上で、システム性能と信頼性を向上させることができます。

INTEGRITYのAMPサポート

AMPモードでは、INTEGRITYカーネルのインスタンスが各プロセッサコア上で個別に動作します。ユーザアプリケーションはコアごとに分離され、各コアは自身のメモリ領域を所有します。AMPはヘテロジニアスCPU環境に適しており、他のマルチコアアーキテクチャに比べて高い性能と効率を実現できる可能性を持っています。また、よりデターミニスティックな動作を提供し、プロセスが実行される箇所を設計者が制御できる利点もあります。

INTEGRITYのSMPサポート

SMPは、INTEGRITYのマイクロカーネル設計、高速かつデターミニスティックな割り込み応答時間、カーネル内で割り込みを無効化しないポリシーに適した拡張機能です。INTEGRITYのSMPサポートは、リアルタイム保証を損なうことがありません。さらにINTEGRITYのミドルウェアは、ユーザ空間内のプロセスとして実装されており、コア間で容易に分散処理可能です。INTEGRITY SMPの特長は以下のようになります。

- セキュリティ、および安全性が認証された実績がある高度なセパレーションカーネルアーキテクチャ
- N個の最高優先度タスクを、N個のコア上で自動的に実行
- オプションでコアバインディング機能を使用し、タスクやタスク群を特定のコア、またはコアグループに固定可能

INTEGRITY-178 tuMPのBMPサポート

BMPは、共有リソースの競合への対処を目的とした、マルチコアの航空機搭載ソフトウェア向け仕様であるAC-193（旧CAST-32A）に準拠するSMPの拡張・限定形式です。BMPでは、アプリケーションのタスクを特定のコアに静的に割り当てることで、システムアーキテクトが複数コアの並列実行を厳密に制御できるようにします。

プロセッササポート

INTEGRITYは、以下を含む主要メーカの幅広いプロセッサアーキテクチャをサポートしています。

- Intel Cyclone
- AMD x86
- AMD Zynq-7000 SoC, AMD UltraScale+ MPSoC, AMD Versal
- ARM Cortex-A
- BAE RAD750
- IBM 970
- Intel Architecture
- Marvell
- Microchip PolarFire SoC
- NVIDIA
- NXP i.MX
- NXP Layerscape
- NXP MPC5xxx
- NXP QorIQ
- NXP S32
- Qualcomm Snapdragon
- Renesas R-Car, RZ
- RISC-V
- ST Telemaco
- Texas Instruments DaVinci
- Texas Instruments Jacinto
- Texas Instruments Sitara

INTEGRITYにおけるセキュア仮想化

INTEGRITY Multivisorは、INTEGRITYのオプションの仮想化サービスであり、ゲストOSを実行しながら、最高レベルの安全性、セキュリティ、および性能を実現します。これにより、Linux、Android、Windows環境などを、INTEGRITYのネイティブタスクとして動作するクリティカルなタスクと共に、重要度が混在するシステムとして効率的に実行できるようになります。

INTEGRITY Multivisorは、INTEGRITYカーネルを利用してクリティカル機能と非クリティカル機能を安全に分離し、プロセッサ仮想化機能を活用して最大性能を引き出しながら、仮想マシンと共有ペリフェラルを効率的に管理します。

仮想化は、ユーザ空間で動作する仮想マシンモニタにより実装され、分離は特権モードで動作するINTEGRITYセパレーションマイクロカーネルによって提供されます。

INTEGRITY Multivisorは、ゲストOSとネイティブINTEGRITY機能間でのペリフェラル制御と共有に関する幅広いオプションをサポートしています。

またINTEGRITY Multivisorは、システム要件を満たすためにコア管理を柔軟かつ強力に制御するメカニズムを提供します。ゲストOSは、非対称型マルチプロセッシング(AMP)モードでコアに静的に割り当てることも、対称型マルチプロセッシング(SMP)モードでワークロードを動的にスケジュールすることも可能です。

INTEGRITY Multivisorは、INTEGRITYのパーティショニングマイクロカーネル技術によって、汎用ゲストOSとクリティカルなアプリケーションを安全かつセキュアに同時実行します。

アーキテクチャ、プロセッサ、およびボードサポート

INTEGRITYアーキテクチャサポートパッケージ(ASP: Architecture Support Package)は、CPU初期化、例外処理、迅速なコンテキストスイッチングを提供し、Arm、Intel、Power、MIPSを含むすべての主要な組み込みCPUアーキテクチャをサポートします。INTEGRITYボードサポートパッケージ(BSP: Board Support Package)は、ASPを基盤とし、ボードレベルでのメモリ、割り込み、アクセラレータ、ペリフェラル、およびミドルウェアのサポートを提供します。INTEGRITY BSPは頻繁に追加されており、最新のBSPサポート状況については、お問い合わせください。

Green Hillsは、業界をリードする商用オフザシェルフ(COTS: Commercial Off-The-Shelf)ボードメーカと広範に協力し、INTEGRITYが各種ボード上で動作できるよう支援しています。

INTEGRITYプラットフォームとミドルウェア

INTEGRITYセパレーションマイクロカーネルを基盤とするGreen Hillsプラットフォームは、必要なツールとミドルウェアをすべて統合した完全統合型ソリューションを提供し、メーカが開発コストと市場投入までの時間を削減できるよう支援します。

▲ 自動車向けプラットフォーム

自動車向けプラットフォームは、以下を含む幅広いアプリケーション領域をカバーします。ECU統合、パワートレインとボディ制御、自動運転、インスツルメントクラスタ、ゲートウェイ、コネクテッドカー、AUTOSAR対応システムなど、これらすべてのプラットフォームは、セキュアパーティション、マルチコア仮想化、迅速な起動、高度な開発ツールを備えたスケーラブルなランタイム環境を提供し、開発コスト削減と市場投入時間短縮を実現します。自動車プラットフォームでは、ISO 26262（ASIL D）、IEC 61508（SIL 3）、EN 50128（SIL 4）、ISO/SAE 21434 CAL 4、UNECE WP.29 CSMSなどの最高レベルの安全認証を取得済みです。

▲ 航空機向けプラットフォーム

INTEGRITYは、民間、および軍用航空機における多数の成功事例を持っています。アビオニクスプラットフォームは、INTEGRITY-178 tuMP、航空業界標準ARINC 653-1アプリケーションソフトウェアインターフェースサポート、FAA安全認証に必要なドキュメントを統合しています。INTEGRITY-178は、FAAの最も厳しい基準であるRTCA/DO-178C Level Aに認証されています。さらに、INTEGRITY-178 tuMPはマルチコアプロセッサで、RTCA/DO-178C、およびAC 20-193に基づく民間航空機適合性認証を達成した唯一のRTOSです。

▲ 産業安全向けプラットフォーム

このプラットフォームは、安全で信頼性の高い制御システムソフトウェアの構築（たとえIEC 61508 Safety Integrity Level 4（SIL 4）までの認証要求があったとしても）に最適です。本プラットフォームは、自動車、鉄道、原子力などのセーフティクリティカル領域への適用が可能です。また、事前認証済みのINTEGRITY、統合ミドルウェア、SIL 3/SWSIL 4認証レポート、および安全マニュアルも含まれています。

▲ 医療機器向けプラットフォーム

このプラットフォームは、豊富な実運用実績に裏打ちされた認証技術に基づいており、医療機器メーカが、より高度な製品を、より迅速かつ低コストで開発できるよう支援します。また、最新の規制要件、および技術要件にも対応しています。

▲ セキュアなIoTプラットフォーム

IoT（Internet of Things）の膨大な可能性は、同時に大規模な攻撃リスクももたらします。これに対抗するため、Green Hillsはコンポーネントレベルから、企業インフラ全体にわたる保護を組み込むためのセキュリティサービスと製品を提供しています。

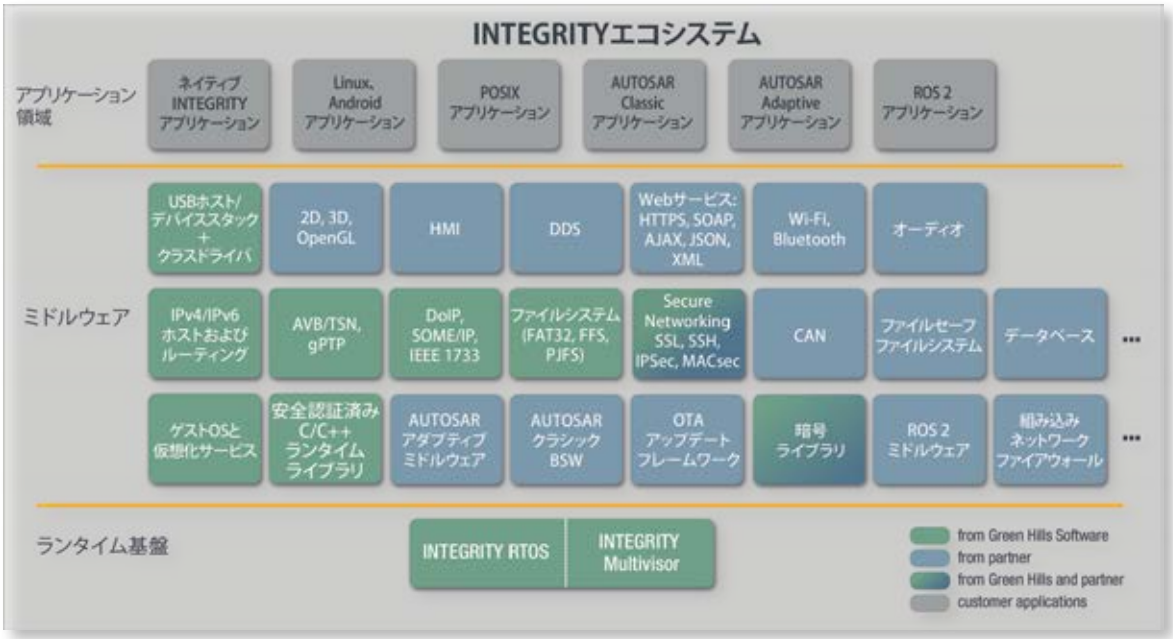
▲ ソフトウェア無線向けプラットフォーム

このプラットフォームは、標準に準拠した完全なリファレンスプラットフォームを提供し、ソフトウェア無線（SDR: Software-Defined Radio）システムの開発、および展開を可能にします。対応するシステムの範囲は広く、米国軍のJoint Tactical Radio System（JTRS）から、公共安全用無線システム、商用通信システムまで含まれます。このプラットフォームにより、SDRの利点を最大限に活用したシステム構築が実現できます。

IPv4/IPv6ネットワーキング

INTEGRITYは、最終製品の要求に合わせた高度なソリューションを選択できる、包括的なIPv4/IPv6ネットワーキング機能をサポートしています。このスタックは、組み込みアプリケーション向けに特別に設計されており、最適化されたパフォーマンスとスケーラビリティを実現するために高度なアルゴリズムを適用し、広範なプロトコル適合性、および相互運用性テストを受けています。

このネットワーキングスイートは、ワイヤレス、自動車、民生機器、住宅向け、ゲートウェイ、企業向けルーター、携帯電話のインフラ、携帯電話機など、組み込みシステムの特定ニーズに対応するために一から開発されました。



INTEGRITYエコシステムは、安全性、セキュリティ、信頼性、リアルタイム性能に重点を置き、幅広いミドルウェアおよび実行環境を網羅しています。

さらに、TSN（Time Sensitive Networking）は制御機能に対する保証されたレイテンシと、安全クリティカルな通信のための冗長ネットワークパスを構築する機能を追加します。

主要なAVB（Audio Video Bridging）プロトコルは、ネットワークトラフィックを整形し、ミッションクリティカルデータに優先順位を与え、安全クリティカル領域でのネットワーク冗長性を確保します。サポートされる主なプロトコルは、以下の通りです。

- トランスポートプロトコル：IEEE1722（AVTP）
- クレジットベースシェイパ：IEEE 802.1Qav/802.1Qat
- AVDECCサポート：IEEE1722.1
- アプリケーション固有コンフィグレーション：802.1BA

USBホスト、およびデバイスコントローラ ライブラリ

INTEGRITYでは、USB 3.0ホスト、デバイスタック、多数のクラスドライバ、およびサンプルアプリケーションが提供されています。これらの製品により、アプリケーションにUSB接続機能を迅速かつ容易に追加できます。サポートされているクラスドライバは、以下の通りです。

- マウス、キーボード、ハブ
- マスストレージクラス
- 出力デバイス用オーディオクラス
- 通信クラス

グラフィックソリューション

Green Hillsは、業界をリードするグラフィックス、およびHMIツールキットサプライヤと統合し、INTEGRITYベースシステムに近代のUI/UXを提供しています。統合パートナーは、以下の通りです。

- Altia
- Crank Software
- The Qt Company
- DiSTI
- Rightware

ファイルシステム

INTEGRITYは、さまざまなファイルシステム（UNIXライクファイルシステム、DOS/FAT 12/16/32、ISO9660、NOR/NANDフラッシュ向けウェアレベリングファイルシステム、ネットワークファイルシステム（NFS）など）をサポートしています。INTEGRITYのファイルシステムフレームワークモデル（VFS: Virtual File System）により、これらのファイルシステムのサポートを簡単に追加・削除できるほか、独自のファイルシステムも追加可能です。

さらに、INTEGRITYパーティショニングジャーナリングファイルシステム（PJFS:Partitioning Journaling File System）ライブラリにより、高度なファイルシステム機能が提供されます。PJFSは、電源障害からの安全な復旧と高速起動を実現する高信頼性ファイルサーバーであり、トランザクションジャーナリングとクライアントパーティション化によってデータ整合性を維持します。

簡単に作成、デバッグ、最適化

プロジェクトの開発フェーズにおいて、INTEGRITYはMULTIと密接に統合されています。MULTIは、業界で最も高度なツールスイートであり、複雑なマルチコアシステムの理解を容易にし、INTEGRITYアプリケーションの迅速な作成・最適化を支援します。

INTEGRITY プロジェクトウィザード

プロジェクトウィザードを使用すれば、数回のクリックでINTEGRITYアプリケーションや、プロジェクトを簡単に作成できます。グラフィカルインターフェースを通じて、使用するBSP、およびミドルウェアコンポーネント（ファイルシステム、TCP/IPスタック、リソース解析、デバッグエージェントなど）のようなプロジェクト属性を選択できます。

MULTI 統合開発環境

MULTIは、過去30年以上にわたり、何千人もの開発者に利用されてきた業界で他に類を見ない統合開発環境です。この環境は、組み込みプロセッサ向けのコード作成、デバッグ、最適化のために使用されており、開発者は難解なバグの発見と修正、パフォーマンスのボトルネックの特定、将来的な問題の予防を容易に行うことができます。MULTIを活用することで、ソフトウェアを予定通りに納品するためのコストが削減されるほか、ソフトウェア品質の問題による高額なリコールを回避しやすくなり、より効率的なコードによって必要なメモリとCPUサイズが削減されるため、ハードウェアコストも低減されます。

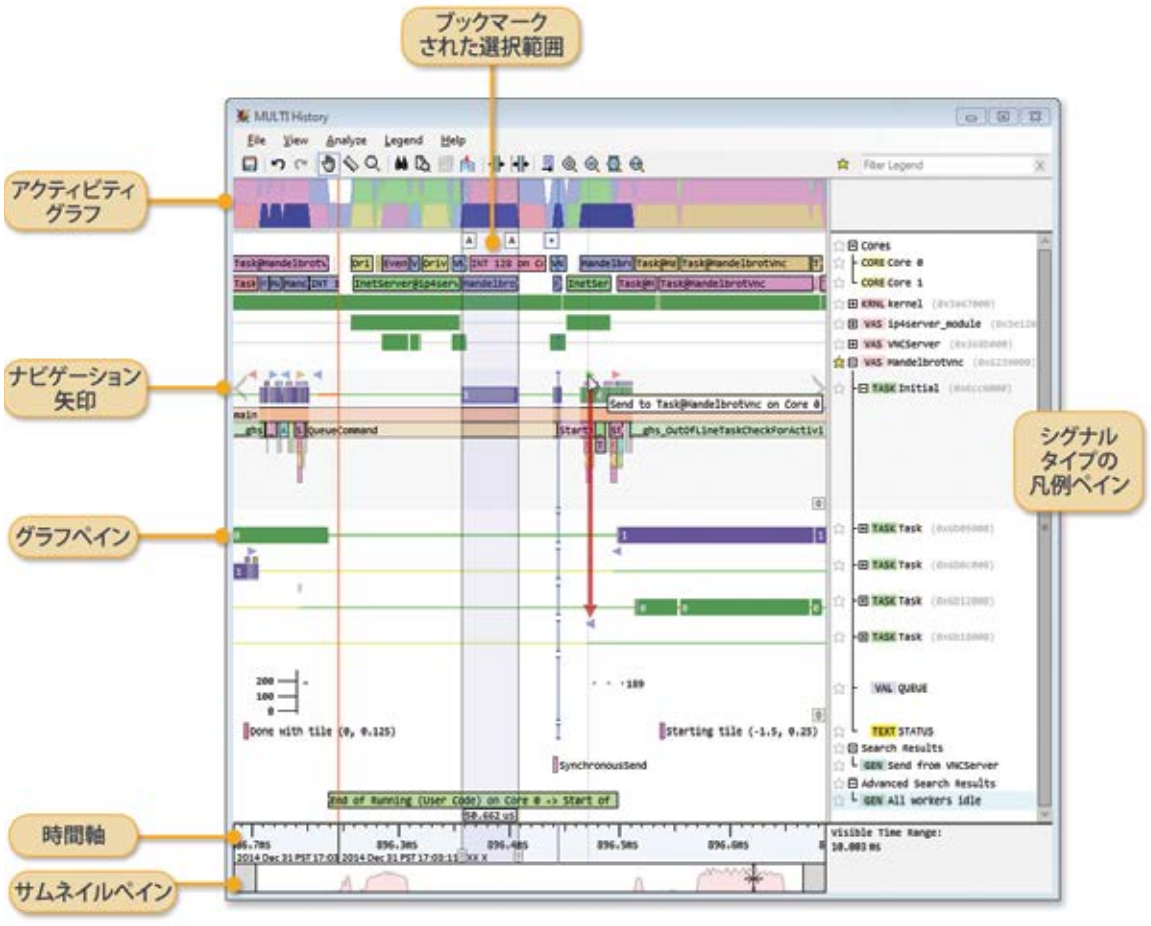
INTEGRITY シミュレータ

INTEGRITYシミュレータ（ISIM）を使用すれば、ターゲットハードウェアなしで、INTEGRITYベースの組み込みアプリケーションの開発・テストが可能になります。ISIMは、ターゲットプロセッサ上で実行されるのと同一のバイナリコードをシミュレートするため、従来型ネイティブシミュレータよりも現実的な結果が得られます。ISIMは、仮想メモリ、周辺機器、TCP/IPなど、INTEGRITY API全体をシミュレートできます。

MULTI ツールスイート

MULTIに含まれるツール群は、組み込みソフトウェア開発者のニーズに特化した完全な開発環境を構築するために、Green Hillsの開発者によって設計されました

- 安全認証済みC/C++コンパイラ、およびランタイムライブラリ
- マルチコアデバッグ
- History® viewer
- リバースプレイデバッグ TimeMachine®
- OSアウェアネス
- 静的コード解析 DoubleCheck™
- ランタイムエラー検出
- メモリリーク検出
- パフォーマンスプロファイラ
- エディタ
- 命令セットシミュレータ
- コードカバレッジ
- プロジェクトマネージャ
- バージョン管理
- フラッシュプログラマ
- Pythonインタフェース
- MATLAB/Simulinkとの統合



History viewerは、複雑なヘテロジニアス・マルチコア・システムにおけるプログラム実行の過去数秒、数分、あるいは数日間を表示することで、システムへの前例のない可視性を提供します。

Integrate ユーティリティ

Integrate™ユーティリティは、業界をリードする独自の革新的なツールであり、複数のアドレス空間にわたって、タスク、接続、その他のカーネルオブジェクトの初期状態を設定することでシステムのセキュリティを検証し、リソースの可用性を保証することを可能にします。Integrateは、使いやすく強力なインターフェースを備えており、アドレス空間、クロック、タスク、セマフォ、コネクションなど、INTEGRITYシステム全体のリソースを構成することができます。

また、Integrateは人間が読みやすいようにフォーマットされたコンフィグレーションファイルを生成し、そのファイルはINTEGRITYアプリケーションのビルド時に使用されます。このユーティリティは、コンフィグレーションファイルを読み取り、その内容をグラフィカルに表示するため、アドレス空間やオペレーティングシステムオブジェクトの状態を容易に把握することができます。

幅広いカーネルの可視化

MULTIとINTEGRITYとの密接な統合により、カーネルイベントを詳細に見ることができます。カーネルのデータ構造、タスクリスト、リソースに対するかつてない視点を得られるため、開発者はバグの特定やシステムパフォーマンスの微調整をより容易に行うことができます。

マルチタスクデバッグ

MULTIは、INTEGRITY上で稼働するさまざまな構成に対応したマルチタスクデバッグ機能を提供します。各タスクは、異なるプロセッサ上、同じプロセッサ上、ISIMシミュレータ上、またはそれらを組み合わせた環境で実行でき、真のヘテロジニアスマルチプロセッサデバッグが可能です。

高度なマルチタスクデバッグ機能には、次が含まれます。

- 複数プロセッサ、複数アドレス空間にわたる複数タスクの同時デバッグ（各タスクに色分けされたデバッガウィンドウ）
- システム内のタスクを追跡し、デバッグ対象タスクを選択できるタスクリストウィンドウ（タスク名、実行状態、優先度、スタックサイズ、スタック使用率（ハイウォーターマーク）を表示）
- タスク作成時に、自動的に新しいデバッガウィンドウを起動
- タスク個別、またはアドレス空間全体（AnyTask）単位でのブレークポイント設定
- シリアル、およびイーサネット経由での同時マルチタスクデバッグサポート
- ファイル、およびターミナルI/Oのホストエミュレーション
- すべてのタスク（「アイドル」タスクを含む）の相対実行時間の表示

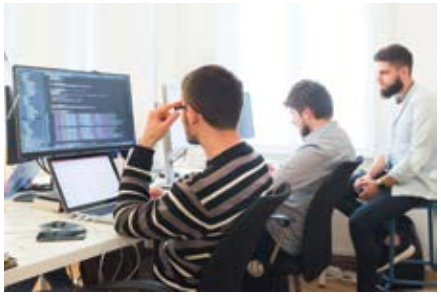
カーネルアウェアネス

MULTIは、INTEGRITYカーネルのオブジェクト、タスク、リソース、およびその状態を包括的に可視化します。ソースコードがなくても、開発者はINTEGRITYの状態を完全にスナップショット表示し、仮想アドレス空間のデバッグと表示を行うことができます。

INTEGRITYデバッグエージェント

INTEGRITYには強力なデバッグエージェントが含まれており、ボードやシャーシをはじめとする、マルチプロセッサシステムのリモートデバッグが可能です。ホストとは単一のネットワーク接続（TCP/IP、イーサネット、またはシリアル）で接続され、MULTIの単一インスタンスからシステム全体をデバッグできます。

トレーニング、およびコンサルティングサービス



Green Hillsのコンサルタントによる専門的なトレーニングにより、INTEGRITYを使用する開発者は、より迅速に生産性を高め、統合された製品の力を最大限に活用できるようになります。

トレーニングセッション

Green Hillsは、年間を通じて世界各地でトレーニングセッションを開催しています。講義とハンズオン演習を通じて、参加者は次の内容を学びます。

- RTOSの概念を設計に適用する方法
- INTEGRITYの主要機能をアプリケーションで活用する方法
- INTEGRITYを使用して、特定目的を達成するための最適な手段の選定

トレーニングセッションには、Express（短縮版）とIntensive（集中版）の2種類があり、INTEGRITYに対する習熟度や、開発者の多忙なスケジュールに対応できるようになっています。Expressトレーニングでは、INTEGRITYの概要を迅速に把握できるよう構成されており、Intensiveトレーニングでは、より高度な概念に焦点を当て、参加者が特に関心のある領域に集中できるような機会が提供されます。

クイックスタートプログラム

新しいRTOSでの開発を始めるには、時間がかかることがあります。Green Hillsは、できる限り早くソフトウェア開発を開始できるようにするため、クイックスタートプログラムを開発しました。

新規のお客様が当社ソフトウェアに慣れていく過程を研究した結果に基づき、クイックスタートプログラムは、新しいプロジェクトの立ち上げにおけるあらゆる段階をサポートできるように設計されています。このプログラムには、INTEGRITYのオンサイトでのインストールとコンフィグレーション、カスタムボードサポートパッケージの開発、アプリケーションのポーティング、製品カスタマイズ、ツールインターフェースの開発、そして一般的なトレーニングなどが含まれる場合があります。

オンサイトサポートとコンサルティング

課題によっては、オンサイトでの対応によって、より早く解決できる場合があります。また、ライブコーチングはINTEGRITY、および関連製品をより深く理解し、最大限活用するための重要な手段です。そのためにGreen Hillsは、専門エンジニアによるオンサイトサポートとコンサルティングを提供しています。

IoTセキュリティアドバイザー

Green Hillsの全ビジネスユニットから集められた専門家チームで構成されるIoTセキュリティアドバイザーは、デバイスがインターネットに接続することによって生じるプライバシーおよびセキュリティ課題への対応を必要とする組織に向け、次のようなコンサルティングサービスを提供します。

- システムセキュリティ設計コンサルティング
- 包括的な認証取得支援
- 脅威および脆弱性評価

Corporate Headquarters

30 West Sola Street ▲ Santa Barbara, CA 93101
ph: 805.965.6044 ▲ fax: 805.965.6343 ▲ email: info@ghs.com ▲ www.ghs.com

Green Hills Software GK

〒150-0001東京都渋谷区神宮前1-5-8神宮前タワービルディング 13階
電話番号: 03-6741-7168 ▲ お問い合わせ: jpsales@ghs.com

株式会社アドバンスドデータコントロールズ

〒101-0045東京都千代田区神田鍛冶町3-4oak神田鍛冶町
電話番号：03-3251-3170(代) ▲ www.adac.co.jp