

Green Hills Software



INTEGRITY

最も先進的なRTOSテクノロジー


Green Hills[®]
SOFTWARE

最もセキュアで信頼できるリアルタイムOS

Green Hills Softwareの主力OSであるINTEGRITY®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、総合的な信頼性、完全なセキュリティ、最大限のリアルタイム応答性を組み込みシステムに提供します。様々な業界から認定され、リーダーシップの実績が際立っているINTEGRITYは、リアルタイムOSの基準を設けています。

最大のパフォーマンス、セキュリティ、信頼性

INTEGRITYは、組み込み開発者のアプリケーションが、セキュリティ、信頼性、およびパフォーマンスに関する要件を可能な限り最大限に満たせるよう、設計段階から考慮されています。

これを実現するためにINTEGRITYは、ハードウェアメモリ保護機能を使用して、組み込みアプリケーションを隔離・保護するセキュアなパーティションを作成しています。セキュアなパーティションは、各タスクを適切に実行するのに必要なリソースを確保し、サービス拒否攻撃、ワーム、トロイの木馬といった悪意のあるコードから、OSとユーザタスクを保護します。他のメモリ保護型のOSとは異なり、セキュリティや保護のためにリアルタイムパフォーマンスを犠牲にすることはありません。

統合されたミドルウェアとプラットフォーム

開発者が、すぐに製品開発に取掛かれるようにGreen Hills Softwareは、INTEGRITY向けに、統合・検証されたミドルウェアを幅広く提供しています。

- ▲ FFS、FAT、NFS、ジャーナリングファイルシステム
- ▲ IPv4/IPv6ホスト、およびルーティングネットワークスタック
- ▲ FIPS 140-2認証のネットワークセキュリティプロトコル
- ▲ 高度なLayer 3ルーティングプロトコル
- ▲ Webサービス: HTTPS、SOAP、AJAX、JSON、XML
- ▲ 完全なWi-Fiサポート
- ▲ USBホストスタック、デバイススタック、クラスドライバ
- ▲ 2D、3D、OpenGLグラフィックス

これらのミドルウェアパッケージは、それぞれINTEGRITYの先進的なリアルタイムOS機能とシームレスに連携して、十分に活用できるように事前に統合し、テストされています。

Green Hills Softwareは、特定の業界向けに、完全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。それぞれのプラットフォームには、INTEGRITY、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、およびマニュアルが含まれており、以下の分野向けが用意されています。

- ▲ 自動車
- ▲ セキュアなモバイル機器
- ▲ アビオニクス
- ▲ セキュアなネットワークング
- ▲ 産業安全
- ▲ ソフトウェア無線
- ▲ 医療機器
- ▲ ワイヤレス機器

中心となるソフトウェア、およびマニュアルすべてが、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
- ▲ 開発リスクの軽減
- ▲ 品質とイノベーションをさらに重視

安全性とセキュリティの認定

15年以上前に発表されて以来、INTEGRITYは数多くの認定、および認証評価を取得し、リーダーシップの実績が証明されています。開発者は、設計において最高水準の安全性、セキュリティ、信頼性を達成できます。

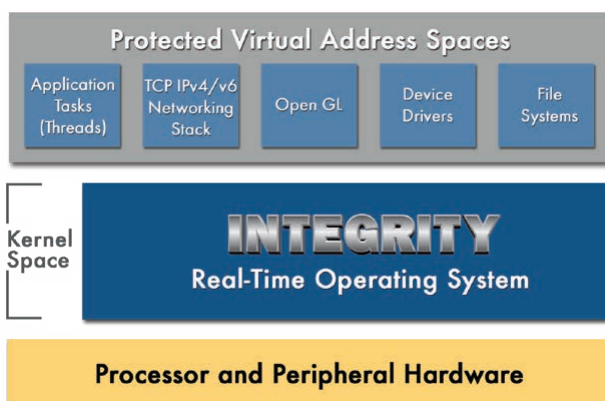
- ▲ FAA: DO-178B、Level A (INTEGRITY-178)
- ▲ NSA: EAL 6+ High Robustness Common Criteria SKPP. OSに関して、これまでに達成された最高のセキュリティ水準 (INTEGRITY-178)
- ▲ FDA: Class II、およびClass IIIの医療機器の認可
- ▲ EN 50128 SWSIL 4、IEC 61508 SIL 3: 機能安全

保証されたセキュリティ

INTEGRITYは、分離、損害の制限、情報フロー制御のポリシーを、組み込み設計者が実施するのに必要なすべての機能を提供するとともに、複雑化、および常時接続化が進む現在のアプリケーションに、セキュアなネットワークングを提供します。

INTEGRITYのMILS (Multiple Independent Levels of Security) 分離カーネルアーキテクチャは、セキュリティ機能を分離する非常にロバスタなメカニズムを提供します。真のMILSカーネルであるINTEGRITY-178Bは、商用OSでこれまで達成された最も厳格なコモンクライテリアのセキュリティ評価、EAL 6+ High Robustnessの認証を取得しています。

INTEGRITYの分離カーネルは、割当てられたメモリ領域を超えたプロセスの書き込みを防ぐことで、誤ったコードや悪意のあるコードによる損害から保護します。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外からの意図されていないアクセスを防ぎます。



INTEGRITYアーキテクチャは、保護された複数の仮想アドレス空間をサポートしており、それぞれに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。INTEGRITYカーネルは、カーネルモードのタスクとともに、自身のアドレス空間で自身を保護します。

信頼性のための設計

従来のOSでは、クラッシュ、ロックアップ、コントロール不能などが原因で、人工衛星の喪失、車のエンスト、医療モニタの故障など、大きな損害を引起す恐れがありました。しかしINTEGRITYは、こうした不具合を招く故障から、重要なアプリケーションや自身を保護します。

これを実現するためINTEGRITYは、他のどのプロセスが利用しようとしても、CPUの時間、およびメモリリソースが個々のプロセスで常に利用できるように、保証されたシステムリソースを提供します。

悪意のあるイベントや意図しないイベントがあると、システムリソースへのアクセスが拒否され、システムプロセスを思い通りに実行できなくなる可能性があります。こうしたサービス拒否攻撃を防ぐためにINTEGRITYでは、CPUの時間とメモリの固定資源を各プロセスに割当てることができます。特定のプロセスに対して時間帯を確保することで、こうした固定資源は、実行中のタスクが自身の時間帯以外に実行されないようにし、他のプロセスの整合性も維持します。

厳格な真のリアルタイムパフォーマンス

ハードウェアのメモリ管理ユニット (MMU) を活用する初のリアルタイムOSのひとつとして、INTEGRITYは、セキュリティと保護のためにリアルタイムパフォーマンスを犠牲にすることのない、厳格な真のリアルタイムOSです。INTEGRITYは、ナノ秒単位でイベントに応答可能であることが保証されています。

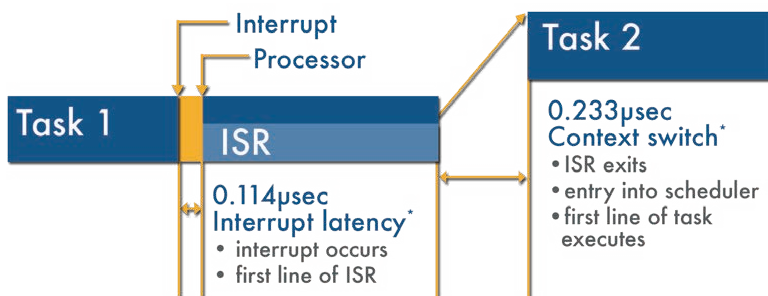
INTEGRITYカーネルサービスはすべて、システムコールのオーバーヘッドが最小限になるよう最適化されています。複雑なシステムコールは、他のシステムコールを実行できるよう保留にすることができます。INTEGRITYは、複数の優先レベルをサポートしてCPUのパーセンテージ割当てを完全に制御する、本当のリアルタイムのスケジューラを使用しています。

INTEGRITYは、絶対最小待ち時間を、最も優先順位の高い割込みに常に提供します。これを確実に実施するため、カーネルは割込みのマスクまたはブロックを実行しません。また、一部のシステムで割込みを一時的にブロックする可能性のあるような、長い待ち時間を伴う命令を回避します。

重要なデッドラインを守る

INTEGRITYでは、リクエスト中のプロセスが提供するCPUの時間リソースをカーネルのみが使用して、リクエストされたサービスを実行します。いずれの処理の動作にも関係なく、測定可能な最大カーネルサービス時間によってカーネルサービス時間が制限されるため、表に出ない実行時間も回避されます。

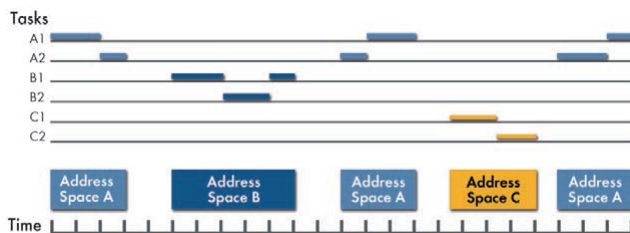
また、INTEGRITYは、優先順位の逆転を防ぐために、独自の最高値固定セマフォ機能を用います。優先順位の逆転は、優先順位の低いタスクが優先順位の高いタスクを不確定の時間拒否した時に、デッドライン違反、および実行エラーを引起す可能性があります。



割込み待ち時間を最低限にするため、INTEGRITYカーネルは、重要なデータ構造の操作中でもマスク、または割込みをブロックすることはありません。

パーティションスケジューリング

安全性の制約が厳しいINTEGRITYファミリのINTEGRITY-178Bは、複数レベルで最適化された拡張パーティションスケジューラ (EPS) を統合でき (オプションのARINC 653-1が必要)、他のシステム、またはプロセスのイベントに関係なく、指定したアドレス空間に特定の割合のCPU時間を割当てることができます。各パーティションでは、CPUの特定の時間帯をこのアドレス空間内のタスクで常に利用できるようEPSが指定します。また、EPSは、CPUの時間帯の限界を適用して、他のパーティションのタスクに悪影響を与えないように、悪意のあるコード、ウイルス、ハッカーの侵入を防止します。



INTEGRITY-178Bには、オプションでARINC-653の2段階のパーティションスケジューラを組み込むことができます。これにより、指定したアドレス空間に特定の割合のCPUの時間をサポートできます。

保証されるメモリリソース

INTEGRITYは、様々な状況からメモリを保護します。

- ▲ メモリの枯渇
- ▲ メモリの破壊
- ▲ メモリへの許可されていないアクセス

INTEGRITY独自のメモリ割当てシステムは、あるアドレス空間が他のアドレス空間のメモリを使い果たさないようにします。

十分なカーネルメモリを確保できるようにINTEGRITYは、プロセスの要求に対し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。これが無ければ、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、および組込み仮想化のサポート

ハイパーバイザモードや、マルチコアといった組込みマイクロプロセッサのトレンドによって、新たなタイプのシステムソフトウェアアーキテクチャへの道が開かれています。AMP、True SMP、統合されたMultivisor仮想化テクノロジーといったINTEGRITYの柔軟な展開方式によって、このような説得力のある新たな機能を実現されています。

先進的なマルチコアのサポート

INTEGRITYのモダンなアーキテクチャは、組込みシステムをターゲットとするマルチコアプロセッサに最適です。INTEGRITYは、組込み、およびリアルタイムの使用に最適化した非対称型マルチプロセッシング(AMP)、および対称型マルチプロセッシング(SMP)を完全にサポートしています。組込みシステムの設計者は、タスクに適したマルチプロセッシングアーキテクチャを選択できます。GHSの統合開発環境 MULTI®に含まれている先進的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、システムのパフォーマンスと信頼性を高めることができます。



INTEGRITYによるマルチコアプロセッサの柔軟なサポートによって、幅広いアーキテクチャ機能がユーザにもたらされ、さらにはセキュアで信頼性のある分離ポリシーにより、リアルタイムのデータミニスティックなパフォーマンスが提供されます。

AMPのサポート

AMPのサポートにより、各プロセッサのコアでINTEGRITYカーネルの1つのインスタンスが実行されます。ユーザアプリケーションは、指定したコアに隔離、および固定されるため、各コアが自身のメモリ領域を所有します。AMPは異機種環境のCPUに適しており、他のマルチコアアーキテクチャよりも、パフォーマンスと効率が高くなる可能性があります。また、データミニスティックな動作を提供しつつ、プロセスが実行される場所を設計者が制御できるようにします。

SMPのサポート

SMPは、シンプルなマイクロカーネル設計、高速かつデータミニスティックな割り込み応答時間、カーネル内の割り込みを禁止にしないポリシーを持つため、既存のINTEGRITYアーキテクチャに適した拡張機能です。INTEGRITYでSMPをサポートしても、リアルタイムの保証を妨げることはありません。それに加えて

INTEGRITYのミドルウェアは、ユーザ空間にプロセスとして実装されているため、コアへの配布が容易です。

INTEGRITYのSMP機能:

- ▲ セキュリティと安全性が認定された実績がある、先進的な分離カーネルアーキテクチャ
- ▲ よりデータミニスティックになるように、コア上で最も優先順位の高いタスクを自動的に実行
- ▲ 実行中のタスクが、すべて同じ優先順位になるよう求めるオプションモードにより、シングルコアからの移植を支援
- ▲ 他のSMPのOSよりも、カーネルロックがはるかに少ない「スマートSMPロック」

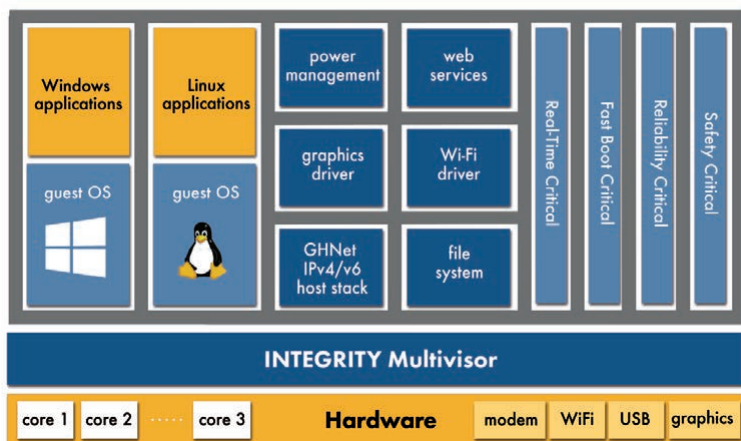
INTEGRITYのセキュアな仮想化

INTEGRITY Multivisor™は、現在のマイクロプロセッサで利用可能で、様々なハードウェア機能を処理するのに十分な柔軟性をもつアーキテクチャを備えた、ロバストで移植可能な仮想化インフラです。ゲストOSに対して最小限の変更、または変更なしで利用可能な、ハードウェア仮想化設備を最大限に利用します。

Intel VT、Freescale QorIQ、ARM-VE、ARM TrustZoneといった、ハイパーバイザアクセラレーション対応のプロセッサにおいて、INTEGRITY Multivisorは、ゲストOSに変更を加えなくても、高パフォーマンスの「完全仮想化」をサポートします。

ハイパーバイザモードのアシスタントがないプロセッサでは、INTEGRITY Multivisorは、慎重に計画された最小限の変更のみをゲストOSに加えて、移行、および移植の容易さを犠牲にすることなくパフォーマンスを最大化します。

INTEGRITY Multivisorは、コアを管理するために、柔軟かつ強力なメカニズムを提供します。システムの要件に応じて、AMPモデル、またはSMPモデルの動的なスケジューリングワークロードで、コアとゲストOSを静的に結び付けます。



INTEGRITY Multivisorは、リアルタイムアプリケーション、ミドルウェア、ドライバの包括的なエコシステムと汎用のゲストOSを組合せています。

統合されたプラットフォームとミドルウェア

INTEGRITY分離カーネル上に構築されたプラットフォームは、必要となるツールとミドルウェアすべてを一つにまとめ、事前に統合された完全なソリューションを提供するものです。メーカーは、開発コストと市場投入時間のどちらも削減することができます。

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、カーエレクトロニクス関連のあらゆるサブシステムに対応しており、開発コストの軽減、および市場投入時間の短縮に向けたセキュアなパーティション、マルチコア仮想化、

高速ブート、先進的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ます。自動車向けプラットフォームの製品は、ISO 26262 (ASIL D)、IEC 61508 (SIL 4)、EN 50128 (SWSIL 4)をはじめとする最高水準の安全性認定を達成しています。

航空機向けプラットフォーム



INTEGRITYは多数の商用、および軍用航空機の配備において、成功を収めてきた長年の実績があります。航空機向けプラットフォームは、INTEGRITY-178B、アビオニクスの業界標準ARINC 653-1アプリケーションソフトウェアインタフェースのサポート、およびFAA安全性認定に必要な文書を組合せています。INTEGRITY-178Bは、フライトに不可欠なアビオニクスシステム向けのFAAで最も厳格な基準、RTCA/DO-178B Level Aの認定を取得しています。

産業安全向けプラットフォーム



産業安全向けプラットフォームは、要求が厳しいIEC 61508 Safety Integrity Level 4 (SIL 4) までの認定が求められる、安全かつセキュアで信頼性の高い制御システムのソフトウェアコンポーネント構築向けに、完全なソリューションを提供します。このプラットフォームは、自動車、鉄道、原子力など、安全性、およびセキュリティの制約が厳しいその他の分野にも適用できます。

医療機器向けプラットフォーム



医療機器向けプラットフォームは、比類のない使用実績によって証明されている認定済みテクノロジーをベースとしています。このプラットフォームを用いて、医療機器メーカーは最新の規制、およびテクノロジーの要件にも対応しながら、より早く低コストで、さらに高性能な製品を製造することができます。

セキュアなIoTプラットフォーム



モノのインターネット (IoT) に秘められた莫大な潜在能力は、情報搾取や攻撃に対しても同じように莫大な機会を新たにもたらします。これに対抗すべく、Green Hillsはセキュリティサービスとそれに関連した製品群を提供します。それによってデバイスの開発者は、単なる構成要素のレベルから企業全体のインフラに至るまでの保護システムを構築することができます。また、そこには、FIPS140-2向け暗号ツールキット、鍵の生成、デバイスのオーセンティケーション (識別検証)、電子署名、認証への支援、そしてセキュリティのコンサルタントが含まれています。

セキュアなネットワーク向けプラットフォーム



セキュアなネットワークプラットフォームにより、ネットワーク開発者は、システム設計の中心となるデバイスセキュリティをINTEGRITYのOSテクノロジーから構築することができます。このプラットフォームは、先進的なGHNet™ ネットワーキングスタック、およびGateD® Layer 3ルーティング機能と、INTEGRITYの分離アーキテクチャを組合せることで、システムのスループットを損なうことなく、最大限のセキュリティ、および信頼性を実現します。

ソフトウェア無線向けプラットフォーム



ソフトウェア無線向けプラットフォームは、Software Define Radio (SDR) システムの開発、および配備向けに標準ベースの完全なリファレンスプラットフォームを提供します。米軍の総合戦術無線システム (JTRS) から、SDRのメリットが受けられる公共安全無線システム、および商用通信システムまで対応します。

ワイヤレス機器向けプラットフォーム



ワイヤレス機器向けプラットフォームは、完全に統合されたテストパッケージで、主要なソフトウェアテクノロジーを提供することでWi-Fi対応製品の開発を促進します。セキュリティ、および無線テクノロジーの業界リーダーとの協力、および共同開発により完成しました。

IPv4/IPv6ネットワークング

INTEGRITYは、包括的なIPv4/IPv6ネットワークング機能をサポートしており、最終製品の要求を満たすように作られた先進的なソリューションを選択できます。組込みアプリケーション向けに構築されているスタックは、最適化されたパフォーマンスとスケーラビリティに対する先進的アルゴリズムを利用しており、広範囲におよぶプロトコルの適合性、および相互運用性試験を受けています。

このネットワークングスイートは、組込みシステム固有のニーズを満たし、無線、自動車、コンシューマ、住居、ゲートウェイ、企業ルータ、携帯電話インフラ、携帯電話機といった様々なアプリケーションに対応できるよう基礎から開発されました。

USBソリューション

INTEGRITYでは、USB 1.1 (フルスピード)とUSB 2.0 (ハイスピード)のホストスタック、およびデバイススタックに加えて、これらスタックを使用するための様々なクラスドライバ、およびサンプルアプリケーションが利用できます。こうした製品によって、アプリケーションにUSB接続を迅速かつ容易に追加できます。

USBホスト、およびデバイスコントローラライブラリ

USBデバイスコントローラライブラリは、USBデバイスドライバのコーディング作業を簡易化します。一般的なUSBや様々なI/O機器の多くに対応するので、ユーザは製品固有の要件に専念することができます。USB 2.0ホストスタックは、標準的なUHCI、OHCI、EHCIコントローラを使用します。

サポートされているクラスドライバ:

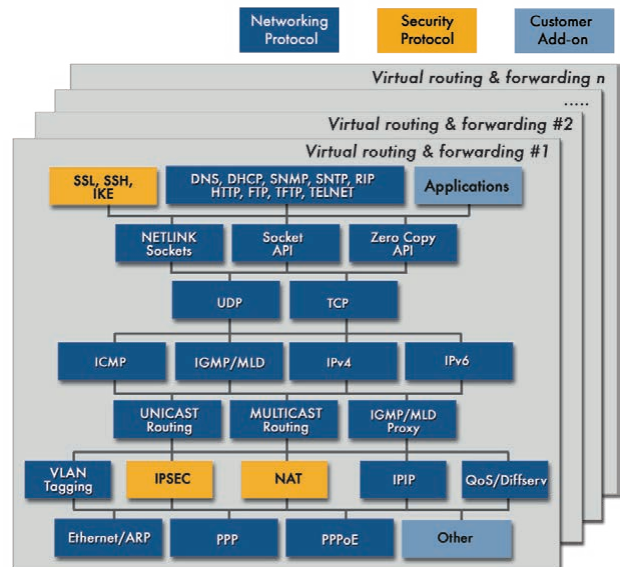
- ▲ マウス、キーボード、ハブ
- ▲ 出力デバイスのオーディオクラス
- ▲ マスストレージクラス
- ▲ 通信クラス

メディアソリューション

Portable Embedded GUI (PEG) は、最小限のメモリフットプリントのみで、タッチスクリーン、およびLCDディスプレイ向けの2Dグラフィカルユーザインタフェースを作成できる、包括的なライブラリを提供します。さらには、OpenGLといった3Dグラフィックス、および高度に調整された次世代ディスプレイ向けのグラフィックスアクセラレータドライバもINTEGRITYに統合されています。



画像提供: Altia社



INTEGRITYのTCP/IPスタックは、高性能でスケーラブルなスタックの業界標準プロトコルを幅広く提供します。

ファイルシステム

INTEGRITYは、UNIXライクのファイルシステム、DOS/FAT 12/16/32、ISO9660、Wear Leveling NOR/NAND Flash File Systems、Network File Systemsなど、様々なファイルシステムをサポートしています。一般に仮想ファイルシステム (VFS) と呼ばれるINTEGRITYのファイルシステムのフレームワークモデルでは、こうした様々なファイルシステムのサポートを簡単に追加・削除したり、独自のファイルシステムを追加することができます。INTEGRITYでは、以下の先進的なファイルシステム機能も提供しています。

Partitioning Journaling File System (PJFS) Libraryは、停電からの安全な復帰、およびクイックブート向けの高信頼性を備えたファイルサーバです。トランザクションのジャーナリング、およびクライアントのパーティショニングによって、データの整合性を維持します。

エンド・ツー・エンドのセキュリティソリューション

モノのインターネット (IoT: Internet of Things) が急増する中、何十億台もの組み込みデバイスが2020年までにインターネットに接続されると予想されています。こうしたデバイスは、それぞれ一意のIPアドレスを持つため、攻撃の標的となります。このため組み込み開発者は、コンポーネント、デバイス、ソフトウェア、ネットワーク、データのライフサイクルを通じた保護に重点的に取組まなくてはなりません。

INTEGRITY SECURITY SERVICES™

A Green Hills Software Company

こうしたニーズに対応するために、INTEGRITY Security Services (ISS) が GHSの組織として設立さ

れました。ISSは、デバイスと企業セキュリティインフラ、両方に対処するエンド・ツー・エンドのソリューションを、組み込みシステムの開発者に提供します。

▲ **組み込み暗号化ツールキット**: 高保証のデータ保護開発向けのFIPS 140-2に準拠した暗号化ツールキットの包括的なスイートです。

▲ **Device Lifecycle Management (DLM) システム**: 暗号デバイス開発のプロセスを保護して簡易化できるように特別に設計された企業向けの柔軟なキー管理インフラです。DLMは、電子署名サービスやサプライチェーンのキー管理といったメーカーのセキュアなデバイスに対し、重要インフラのサポートを提供します。

組み込み暗号化ツールキット

ISSの組み込み暗号化ツールキットは、エンド・ツー・エンドのセキュリティ開発向け暗号化ライブラリの完全なスイートをシステム開発者に提供します。個別、またはバンドルで利用可能なコンポーネントには、以下のものがあります。

- ▲ FIPS 140-2準拠の暗号化アルゴリズムライブラリ
- ▲ TLS/SSLスタック
- ▲ SSH 2.0スタック

- ▲ IPSec/IKEスタック
- ▲ セキュアなブートソリューション
- ▲ Device Lifecycle Management (DLM) エージェント

ISS暗号化ツールキットはすべて、ソフトウェア改ざんの検出、メモリ内の重要データの保護、ベストプラクティスの相互認証を用いたセキュアな通信を行えるように設計されています。

高保証の企業向けキー管理インフラ

Device Lifecycle Management (DLM) システムは、組み込みセキュリティの開発に不可欠な、あらゆるインフラのキー管理サービスを提供します。

DLMは、複数の製品ライン、および分散生産環境で、高保証のキー管理と業務管理を実現するために、業界で認められた標準を使用しています。エンジニアリング、製造、IT部門は、DLMを使用してソフトウェア署名、証明書、一意のデバイスキーをセキュアに生成できます。アプライアンス、またはホストクラウドサービスとして利用可能なDLMは、企業の製品セキュリティ向けの最も包括的なソリューションで、以下のことを実現します。

- ▲ 認可されていない利用、過剰生産、グレーマーケットから重要な資産、および知的財産を保護
- ▲ 重要なデータをサードパーティのサーバ、および信頼できないネットワークから隔離することで、セキュアなキーやソフトウェアの配布を実現
- ▲ セキュアな製品の設計、および製造を通じて信頼性の高いIoTを作成

使用可能なボードサポートパッケージ



INTEGRITYは、すぐに開発に着手できるように、様々なボードサポートパッケージ (BSP) を提供しています。INTEGRITYのBSPは、ボード上のメモリを初期化するほか、シリアルやEthernetデバイスといった多くの周辺機器に対応します。INTEGRITYは、ROMまたはフラッシュメモリに格納可能で、大半のBSPには、フラッシュプログラミングを容易に行うためのサポートが含まれています。INTEGRITYは、フラッシュメモリに容易にアクセスできるように、シンプルなAPIを提供します。

リファレンスBSP、および関連するハードウェアサポートは、以下のベンダーのボードで利用可能です。

- | | | |
|-------------------------------------|--|----------------------------|
| ▲ Advantech | ▲ Eurotech Group | ▲ Neat SRL |
| ▲ Aitech Defense Systems | ▲ Extreme Engineering Solutions (X-ES) | ▲ NVIDIA |
| ▲ Altera/Cyclone | ▲ Freescale Semiconductor | ▲ Pico Computing |
| ▲ BAE Systems | ▲ GE Intelligent Platforms | ▲ Renesas Electronics Corp |
| ▲ Creative Electronic Systems (CES) | ▲ Kontron | ▲ Spectrum Digital |
| ▲ Concurrent Technologies | ▲ Logic PD | ▲ Thales Computers |
| ▲ Curtiss Wright Controls | ▲ Momentum Computers | ▲ Texas Instruments |
| ▲ EMAC, Inc. | ▲ MEN Mikroelectronick | ▲ Xilinx/Zynq |
| ▲ Emerson Network Power | | |

作成、デバッグ、最適化を容易に実行

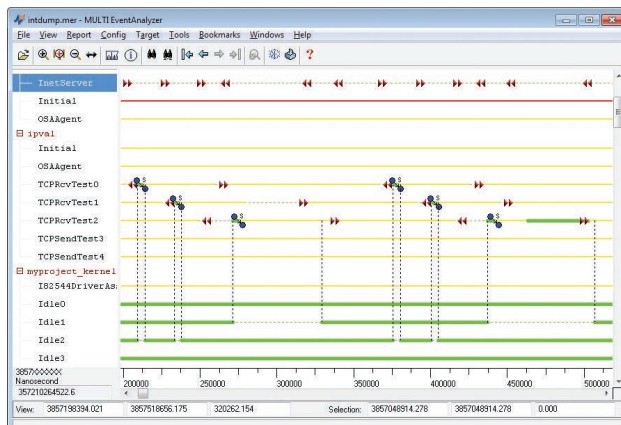
マルチコア対応で、OS別のグラフィカルな開発・解析ツールが含まれる強力なスイートによって、INTEGRITYアプリケーションの設定、デバッグ、最適化が簡単に行えます。これらのツールを通して、複雑なINTEGRITYアプリケーションの作成、システム全体のリソースのグラフィカルな設定、様々なシステムイベントの視覚化を支援します。

INTEGRITYプロジェクトウィザード

プロジェクトウィザードでは、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フェースで作業を行うことで、必要なBSP、必要なアドレス空間数、画像の動的なロードと静的な定義のどちらを実行するかどうかなど、様々なプロジェクト属性から選択することができます。また、共有ライブラリ、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を選択できます。

EventAnalyzerによるイベントのロギング

強力なEventAnalyzer™によって、システムの複雑なリアルタイム処理を一目で把握できます。セマフォコール、タスクのコンテキストスイッチ、割込みといった重要なOSイベントが、リアルタイムでターゲット上に記録されます。イベント情報は、ホストに転送され、EventAnalyzer GUIでグラフィカルに表示されます。イベントロギングは、完全に制御、および設定可能で、独自のユーザー定義イベントを作成することもできます。



EventAnalyzerのビューウィンドウに表示されるイベントをシングルクリックで選択すると、イベントのソースコードを表示するデバッグウィンドウが開き、デバッグを実行できます。

INTEGRITYでは、事後分析モード、またはライブモードでシステムイベントを記録できます。事後分析モードでは、データが最小限のオーバーヘッドでターゲットに収集されます。エラーの後など、リクエストに応じてイベントをアップロードし、エラーの根本原因を判断する情報を解析することができます。ライブモードでは、TCP/IP、またはシリアル経由でデータがホストに継続的に送信されるため、システムの稼働中は、データの履歴を実質無制限に収集、および分析可能になります。

INTEGRITYシミュレータ

INTEGRITYシミュレータ (ISIM™) では、ターゲットとなるハードウェアがなくても、INTEGRITYベースの組込みアプリケーションの開発とテストを行えます。ISIMは、ターゲットプロセッサ上で実行する同じバイナリコードをシミュレートして、従来のネイティブシミュレータよりも現実的な結果を算出します。仮想メモリ、周辺機器、TCP/IPをはじめとして、INTEGRITY API全体をシミュレート可能です。

ResourceAnalyzerによるシステム情報の視覚化

INTEGRITY用にカスタマイズされたResourceAnalyzer™は、システム全体のCPU、およびメモリの使用率の統計を追跡・視覚化できる先進的なランタイム解析ツールです。この情報を使用することで、タスク、およびアドレス空間の効率を最大限に引出し、システム全体のパフォーマンスを改善できます。

Integrateユーティリティ

Integrate™ユーティリティは、複数のアドレス空間をまたぐタスク、接続、その他のカーネルオブジェクトの初期状態を構築し、システムセキュリティを検証してリソースの可用性を確保します。使い勝手が良く強力なIntegrateのインタフェースを通じて、アドレス空間、クロック、タスク、セマフォ、通信など、INTEGRITYシステム全体のリソースすべてを設定することができます。

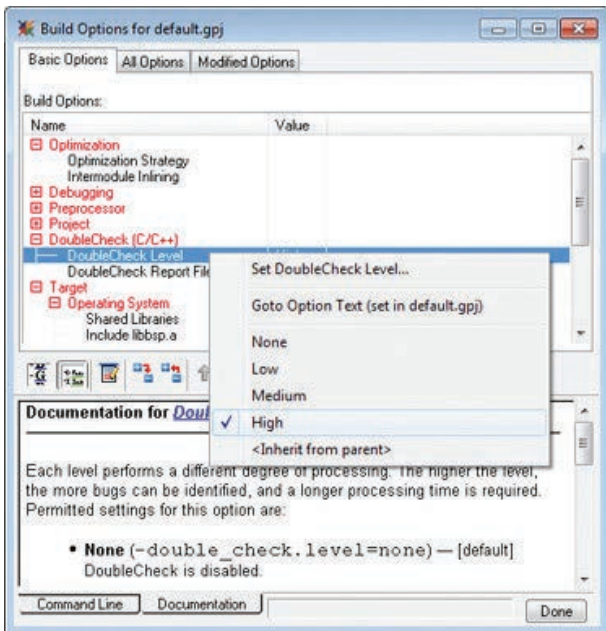
Integrateでは、INTEGRITYアプリケーションの構築に使用される所定の形式の設定ファイルが生成されます。この設定ファイルが読取られ、アドレス空間、およびOSのオブジェクトを確認し易くなるようにコンテンツがグラフィカルに表示されます。

統合開発環境 MULTI

MULTIには、C、C++、EC++、MISRA Cの組込みソフトウェアの開発、デバッグ、および最適化を行うために、業界で最も強力な実績のあるツールが搭載されています。MULTIは、Windows、Unix、Linux、HP-UXホスト上で稼働し、あらゆるGreen Hills Softwareのコンパイラに直観的なグラフィカルインタフェースを提供しており、INTEGRITYターゲットへのリモートデバッグをサポートしています。この洗練された多様なツールによって、MULTIは開発・製造コストを軽減し、デバイスのパフォーマンスと信頼性を高められるように支援します。

静的ソースコード解析ツール DoubleCheck

DoubleCheck™は、バグをより簡単に修正できる開発の初期段階で発見するために用いる、強力な静的解析ツールです。多数のソースファイルにおよぶ大量のコードを迅速に解析し、複雑な処理によって発生するバグを特定します。コンパイラに組込まれているDoubleCheckによって、プロジェクト構築に伴うデバッグの自動化を簡単に行えるようになるため、外部ツールや複雑なスケジューリングが不要になります。



動的実行解析ツール TimeMachine

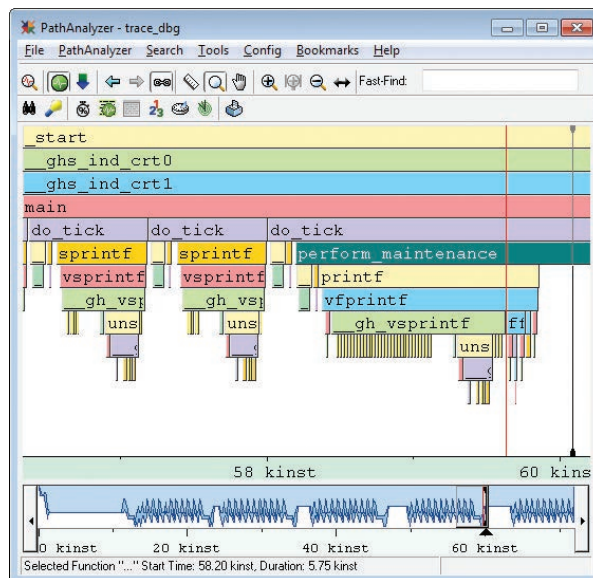
TimeMachine™は、様々なトレース解析ツールを提供しており、組込みソフトウェアの開発者がバグを迅速に検出、および修正し、容易に最適化を行って、自信を持ってテストを受けることができます。TimeMachineでは、開発者がコード内を前後にステップ、および実行できる革新的な機能が、一般的なデバッグインタフェースに統合されています。

MULTIプロファイラ

MULTIプロファイラは、実行されていないブロック、およびソース行を容易に判断できるコードカバレッジレポートを提供します。この情報を使用すると、プログラム実行のより詳細な把握、テストスイートの完了、パフォーマンスのボトルネックの迅速な特定が可能になります。

PathAnalyzer

アプリケーションのコールスタックを時系列にグラフィック表示するTimeMachineのPathAnalyzer™は、予期しない割り込みや、ランダムな不具合といったイベントによって引きこされる不正な実行パス、コード内の非効率な箇所、特異なバグを特定できるように支援します。



TimeMachineには、コールスタックを時系列で表示するPathAnalyzerツールが搭載されています。

最適化コンパイラ

Green Hills Softwareの世界クラスのC、C++、Embedded C++、MISRA C、Adaコンパイラは、INTEGRITYをサポートしています。これらの最適化コンパイラは、言語固有のフロントエンド、グローバル最適化、ターゲット固有の最適化とコードジェネレータで構成されています。

主要な業界標準に適合することで、様々なプロジェクト、およびソースコードファイル間での互換性を高めています。Green Hills SoftwareのCコンパイラは、ANSI X3.159-1989 Standard C (ISO/IEC 9899、およびFIPS PUB 160) に完全に適合しており、Strict ANSI、Permissive ANSI、Transition Mode、MISRA C、K+R、GNU Cといったプログラミング言語の方言をサポートしています。Green Hills SoftwareのC++ライブラリは、スケラブルでC++サポートが要求される特別な水準に対応するよう調整されています。Green Hills Softwareの最適化C++コンパイラは、Standard (ANSI/ISO) C++、Annotated C++ Reference Manual (ARM、Ellis & Stroustrup作成) で定義されているC++、Embedded C++ (EC++)、Embedded C++ with Templatesといった方言をサポートしています。豊富なC++方言のサポートには、名前空間、およびテンプレートへの適合、Linuxカーネル全体の構築に使用されるGNU C/C++拡張互換性などが含まれています。

簡易化された移行

レガシーコード、およびサードパーティコードの再利用や統合をサポートするため、INTEGRITYは、様々な環境向けに記述されたアプリケーションをホスト可能です。開発者は、Linux、VxWorks、その他のOSを使用するアプリケーションなどのレガシーアプリケーションを、非常に少ない再コーディングで統合することができます。また、他のOSに対するAPIサポートも提供可能です。

INTEGRITYの規格に合致したPOSIX APIコールや、INTEGRITY Multivisorテクノロジーによって、最小限の手間、または変更だけで、INTEGRITY上でLinuxアプリケーションを実行可能です。基本的なVxWorks APIレイヤは、メッセージキュー、およびセマフォ、タスク、ウォッチドッグ、およびカーネル空間割込みサービスに対するコアVxWorksサービスコールをサポートしています。

幅広いカーネルの可視化

MULTI、およびINTEGRITY間の密接な統合によって、カーネルイベントを幅広く可視化できるようになりました。カーネルデータ構造、タスク実行リスト、リソースに関して、これまでにない可視性がもたらされたことで、組込み開発者はバグを特定し易くなり、アプリケーションの要件を満たせるようシステムパフォーマンスを細かく調整できます。

マルチタスクデバッグ

MULTIでは、INTEGRITYを実行する様々な設定に対して、マルチタスクデバッグを実行できます。異なるプロセッサ、同一プロセッサ、ISIMシミュレータ、あるいはこれらの環境の組合せによる真の異機種マルチプロセッサデバッグで、各タスクを実行することができます。

先進的なマルチタスクデバッグ機能には、以下のものが含まれています。

- ▲ 同時に複数プロセッサの複数アドレス空間で、複数のタスクをデバッグする機能。それぞれのタスクは、色分けされた独自のデバッグウィンドウに表示されます。
- ▲ システムのタスクを追跡して、デバッグするタスクを選択する、タスク実行リストウィンドウ。タスクの名前、実行ステータス、優先順位、スタックサイズ、スタック用途(高水位線)といった、タスクごとに有用な情報が示されます。
- ▲ タスク作成時に新たなデバッグウィンドウを自動的に開く機能。
- ▲ タスク固有、および(「AnyTask」と呼ばれる)アドレス空間の広いブレイクポイントを設定する機能。
- ▲ 大半のボードに対応するシリアル、およびEthernetの両方で同時発生するマルチタスクデバッグのサポート。
- ▲ ファイル、および端末の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」タスクも含む)の相対実行時間を表示する機能。

カーネルアウェアネス

MULTIでは、INTEGRITYのカーネルオブジェクト、タスクとリソース、およびそれらのステータスを包括的に表示することができます。ソースがなくても、INTEGRITYの状態の完全なスナップショットを確認できるため、仮想アドレス空間のデバッグ、および閲覧を行えます。

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搭載されており、単独のハードウェアネットワーク接続(TCP/IP Ethernet、またはシリアル)からホスト、およびMULTIの単独インスタンスまで、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を実現します。

INTEGRITYシェル

INTEGRITYは、ターゲットシェルを提供しており、telnetまたはrlogin経由でアクセスすることができます。アプリケーションコードの実行前でも、ターゲットと直接通信することができます。このシェルは、MULTIとは関係のないモジュールのロード、およびアンロード、FTP、タスク、およびモジュールのリスト作成、ネットワーク構成の設定、ターゲットメモリの読み取り/書出し、ファイルシステムサービスの実行を行うことができます。

パートナーのエコシステム

INTEGRITYは、様々なサードパーティの組込み製品と統合されています。

- | | | |
|---|------------------------------------|---|
| ▲ SNMP Research: SNMP | ▲ aicas: Java | ▲ McObject: インメモリデータベース |
| ▲ Visuality Systems: CIFS | ▲ Intellegraphics: Wi-Fi/OpenGL | ▲ Swell Software: Portable Embedded GUI |
| ▲ Data Connection: ATM | ▲ Raima: RDBM | ▲ Vector Software: ユニットレベルテスト |
| ▲ SAP: Bluetooth | ▲ RTI: NDDS | ▲ Objective Interface: CORBA |
| ▲ Stollmann: Bluetooth | ▲ KW Software: SoftPLC | ▲ Elektrobot: グラフィックス構築ツール |
| ▲ LogicPD: SOM | ▲ Presagis: OpenGL/X11 | ▲ Rightware: グラフィックス構築ツール |
| ▲ RadVision: VOIP, SIP, RTP/RTCP | ▲ Ansys/Esterel: SCADE ソフトウェアモデリング | ▲ Altia: グラフィックス構築ツール |
| ▲ TeamF1: Kerberos, K509, TACACS+ | ▲ Virtutech: システム仮想化 | ▲ CriticalBlue: マルチコア解析ツール |
| ▲ HCC Embedded: ファイルシステムソリューション | ▲ Ixxat: データ通信プロトコル | ▲ Obigo: HTML5ブラウザ |
| ▲ Digia QT: グラフィックス構築ツール | ▲ LieberLieber: モデルエンジニアリング | ▲ LDRA: ユニットレベルテスト |
| ▲ Clarinox Technologies: Wi-Fi/Bluetooth | ▲ 3S CoDeSys: IEC 61131-3開発システム | ▲ Crank: グラフィックス構築ツール |
| ▲ Socionext: グラフィックス構築ツール | ▲ 3D Inc: グラフィックス構築ツール | ▲ TTEch Computertechnik:
タイムトリガ方式プロトコル |
| ▲ IBM Rational Rhapsody: UML 2.0アプリケーションモデリング | | |

トレーニング、およびコンサルティングサービス

GHSのコンサルタントによる専門的なトレーニングによって、INTEGRITYを使用する開発者は、生産性を高め、INTEGRITYの機能や統合された製品を最大限に活用する方法を習得できます。

トレーニングセッション

Green Hills Softwareは、世界各地で年間を通して定期的にトレーニングセッションを開催しています。講義と実践演習を通じて、出席者は以下の方法を習得できます。

- ▲ リアルタイムOSのコンセプトを自社の設計に適用する
- ▲ 自社のアプリケーションで主要なINTEGRITYの機能を活用する
- ▲ INTEGRITYを用いて特定の目的を達成するのに最適なメカニズムを決定する
- ▲ その他



INTEGRITYの精度度や開発者の多忙なスケジュールに対応するため、トレーニングセッションには、Expressコース、およびIntensiveコースが用意されています。Expressコースでは、INTEGRITYの簡単な概要を紹介し、Intensiveコースでは、先進的なコンセプトを出席者に提示して、出席者の個々の関心分野に重点的に取り組む機会を提供します。

クイックスタートプログラム

リアルタイムOSに慣れるには時間がかかります。可能な限り早くソフトウェアの開発に精通していただけるよう、Green Hills Softwareでは、クイックスタートプログラムを開発しました。

新規顧客がGreen Hills Softwareのソフトウェアにどのように慣れるのかを把握してから、新規プロジェクトの立上げのあらゆる段階に対応するクイックスタートプログラムのコンポーネントを開発しました。コンポーネントには、オンサイトでのINTEGRITYのインストール、および設定、カスタムのボードサポートパッケージ開発、アプリケーションの移植、製品のカスタマイズ、ツールインタフェースの開発、一般的なトレーニングが含まれます。

オンサイトでのサポート、およびコンサルティング

いくつかの課題は、オンサイトでやりとりすることで早く解決できることが分かっています。また、INTEGRITYや関連製品のメリットを十分に把握して享受するには、実演によるコーチングが有益な手段であると認識しています。この目的を達成するためにGreen Hills Softwareは、エキスパートエンジニアによるオンサイトでのサポート、およびコンサルティングを提供しています。

カスタムエンジニアリングサービス

Green Hills Softwareは、組込みソフトウェアテクノロジーのリーダーとして世界的に有名です。しかし、アプリケーションの中には、予測が困難で非常に特殊な要件が必要となる場合があります。こうした状況に対応するため、Green Hills Softwareでは、カスタムソフトウェア開発を専門的に扱うグループとして、カスタムエンジニアリングサービス部門を設立しました。このグループに所属するエンジニアは、特別な機能の追加、既存製品のカスタマイズ、新たなテクノロジーの考案を行うことができます。ニーズを教えていただければ、そのニーズが必要な時に必要なだけ提供します。

サポートされているプロセッサ

INTEGRITY Architecture Support Package (ASP) は、CPUの初期化、例外処理、迅速なコンテキストスイッチを、以下のプロセッサファミリに提供しています。

- | | | |
|------------------------------------|---------------------------------|------------------------------|
| ▲ Altera Cyclone | ▲ NXP I.MX (ARM) | ▲ Renesas RZ |
| ▲ Applied Micro (APM) Powerアーキテクチャ | ▲ NXP Vybrid (ARM) | ▲ Socionext ARM |
| ▲ AMD x86 | ▲ IBM Power Architecture | ▲ Texas Instruments OMAP |
| ▲ ARM Ltd. | ▲ Imagination Technologies MIPS | ▲ Texas Instruments DaVinci |
| ▲ Cavium OCTEON III | ▲ Intel Powerアーキテクチャ | ▲ Texas Instruments Jacinto |
| ▲ NXP Qorivva (Powerアーキテクチャ) | ▲ Marvell ARM and PXA | ▲ Texas Instruments Sitara |
| ▲ NXP QorIQ (Powerアーキテクチャ) | ▲ NVIDIA Tegra | ▲ Texas Instruments Hercules |
| ▲ NXP ColdFire | ▲ Renesas R-CAR | ▲ Xilinx Zynq |

本社

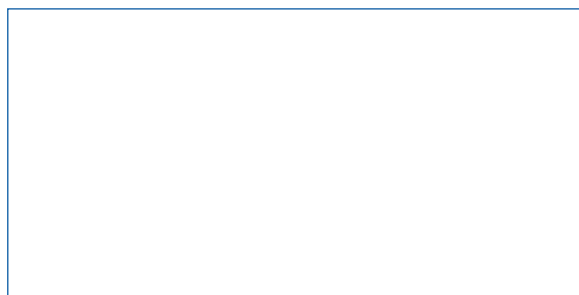
〒101-0045 東京都千代田区神田鍛冶町3-4 oak神田鍛冶町
TEL: 03(3251)3170 FAX: 03(3251)3167

名古屋テクニカルセンター

〒460-0003 愛知県名古屋市中区錦1-11-11 名古屋インターシティ
TEL: 052(231)9980 FAX: 052(231)0035

大阪テクニカルセンター

〒530-0003 大阪府大阪市北区堂島1-6-20 堂島アバンザ
TEL: 06(6347)7780 FAX: 06(6347)7712
URL: www.adac.co.jp ▲ e-mail: sales@adac.co.jp



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