MISH TECH JOURNAL（ミッシュ・テックジャーナル）は、最新の情報をいち早くお届けする技術情報誌です。

Powered by MISH

MISH TECH JOURNAL

2024 Summer

Vol.17

https://www.mish.co.jp

CONTENTS

コンピュータのセキュリティと改ざん防止技術 - P.2-6
- はじめに
- Information Assurance（情報保証）
- 連邦情報処理規格（FIPS）
- グローバル化：Common Criteria
- COTS 製品の改ざん防止
- 防止・検出・応答：改ざん防止の 3 原則
- AT をゼロから構築
- ルートオブトラスト
- Intel のトラストエクスキューション
- Freescale（NXP）トラストアーキテクチャ
- COTS セキュア FPGA テクノロジー
- まとめ

データの暗号化とセキュアイレース ——— P.7-14
- はじめに
- ケーススタディ：NATO AGS
- 重要な用語
- 暗号化
- 暗号化メカニズムの比較
- 暗号化キーの処理
- ユーザー名 / パスワードのスキーム
- 事前共有キー
- 電力の損失
- 暗号消去
- 自己暗号化ドライブ（SED）
- ハードウェアフルディスク暗号化（HWFDE）
- ハードウェア暗号化による認証
- 自己暗号化ドライブとの比較
- ソフトウェア暗号化
- 二重暗号化と CSfC
- セキュアイレース
- 物理的消去 / 破壊オプション
- まとめ

マルチチャンネル多機能計測システムの構築 - P.15-19
- はじめに
- 産業用モーター制御
- ソースレスポンステスト
- シミュレーション
- まとめ

複数のデジタイザを同期するための手法 - P.20-25
- はじめに
- 同期における重要な要素
- クロックリファレンス
- トリガーの重要な要素
- 外部トリガーの分配
- マルチボード用のソフトウェア
- 8CH システムのセットアップ
- 96CH システムのセットアップ
- まとめ

新製品ピックアップ ——— P.26-27
- SPECTRUM 社製　M5i.3367-x16 10GSPS 高速 A/D ボード
- Extreme Engineering 社製　XPedite7871 CPU ボード
- CP North America 社製　MTP-24 マルチディスプレイポータブル PC
- CP North America 社製　TFX1-173 3 画面耐環境液晶ディスプレイ
- CP North America 社製　CPX1-241 24 インチパネルマウントディスプレイ

‘24夏号特集

ANTI-TAMPER TECHNOLOGY

コンピュータのセキュリティと改ざん防止技術

企画・編集・発行/株式会社ミッシュインターナショナル
〒190-0004 東京都立川市柏町4-56-1 グローバルビル
TEL：042-538-7650 Email：sales@mish.co.jp

SPECIAL FEATURE

コンピュータのセキュリティと改ざん防止技術

現代社会は、全ての情報機器がネットワークに接続され、いつでも世界中の情報にアクセスすることができる世の中です。しかし、そのネットワーク網を悪用したサイバー攻撃で特定のシステムを機能不可にすることが可能で、特に軍事分野ではそれが致命的になります。ここではサイバー攻撃に対するセキュリティ機能のひとつである改ざん防止（Anti-Tamper）技術を説明します。

はじめに

サイバー脅威が増大する今日の環境において、ミッションを成功させるために安全な組込みコンピュータと通信システムは不可欠です。データの処理・保存・送信の際にはデータの整合性を保護する必要があります。これらのシステムの戦略的リスク管理はInformation Assurance (IA) として知られており、物理的・技術的および管理的制御の組み合わせが必要になります。

安全保証されたシステムの中核となるのは、ハードウェア、ファームウェアおよびソフトウェアレベルで階層化されたセキュリティ機能を使用した改ざん防止 (Anti-Tamper) 保護機能に基づく、正真正銘の信頼できる基盤です。

Abaco Systems社は、改ざん防止と保護を可能にする機能を組み込むことで保証されたシステムのニーズに応えています。この記事では、安全なプラットフォームをサポートし情報保証 (Information Assurance) を提供するためのCOTS改ざん防止フレームワークの使用に焦点を当てます。

Information Assurance（情報保証）

Information Assuranceの概念は、防御ベースの情報システムの設計・取得・設置・運用・アップグレードおよび交換の各段階に浸透しています。目標は、情報の機密性・完全性・認証・否認防止および可用性の適切なレベルを維持することです。

情報保証と改ざん防止を確保するための基準は、国内および国際的なさまざまなチャネルを通じて維持されています。

連邦情報処理規格（FIPS）

米国政府は、政府請負業者によるコンピュータシステムでの使用を目的として公表された連邦情報処理規格（FIPS）を提供し、国立標準技術研究所（NIST）はハードウェアとソフトウェアを含む暗号化モジュールの要件を調整するためにFIPS 140情報処理規格を発行しています。FIPS 140-2は、カナダ政府の通信保安局（CSE）との共同の取り組みとして暗号モジュール検証プログラム（CMVP）を確立しています。NISTのテストでは、モジュールが４つのセキュリティレベルのいずれかに該当することが確認されます。FIPS 140-3は、追加の概念を組み込み、４つのセキュリティレベル内で変更された要件と制限を提供することを目的としたドラフト規格です。

グローバル化：Common Criteria

情報技術セキュリティ評価の共通基準（Common Criteria）、つまりISO/IEC 15408はコンピューターセキュリティ認証の国際規格です。これは、ヨーロッパ、カナダ、および米国の国防総省規格を統合したものです。プロファイルと機能要件によって設計が推進され、ラボテストの結果によりセキュリティソリューションの堅牢性を示す評価保証レベル（EAL）が決まります。 国際承認アレンジメント（CCRA）は、加盟国が評価済みシステムを相互に承認することを規定しています。Common Criteriaは通常、ファイアウォールとオペレーティングシステムに使用され、暗号化の実装を指定しません。

COTS製品の改ざん防止

社内設計の専門知識と主要パートナーやサプライヤーとの関係により、オプションのセキュリティ機能を備えた標準COTS製品を提供することが可能になります。ただし、COTS機能とカスタムコンテンツ（機密扱いの顧客固有の方法）を区別することが必要になります。図１を参照してください。黄色で強調表示されたAT機能がこの記事の焦点です。

COTS/カスタムの二分法では、低コストで信頼性の高いCOTSソフトウェア、パーティショニング、暗号化、半導体機能、および物理マテリアルを活用しながら、顧客は高度に専門化された独自のテクノロジー、ポリシー、および手順を利用できるようになります。たとえば、改ざん検出センサーからの入力などのハードウェア相互接続設計はCOTSにすることができますが、改ざん対応のためのプログラム動作（FPGAなど）はカスタム化することができます。カスタム機能の動作はCOTS設計プロセスの一部ではないため公開されることはありませんが、アンチタンパーフレームワークはアーキテクチャと密接に結合されています。

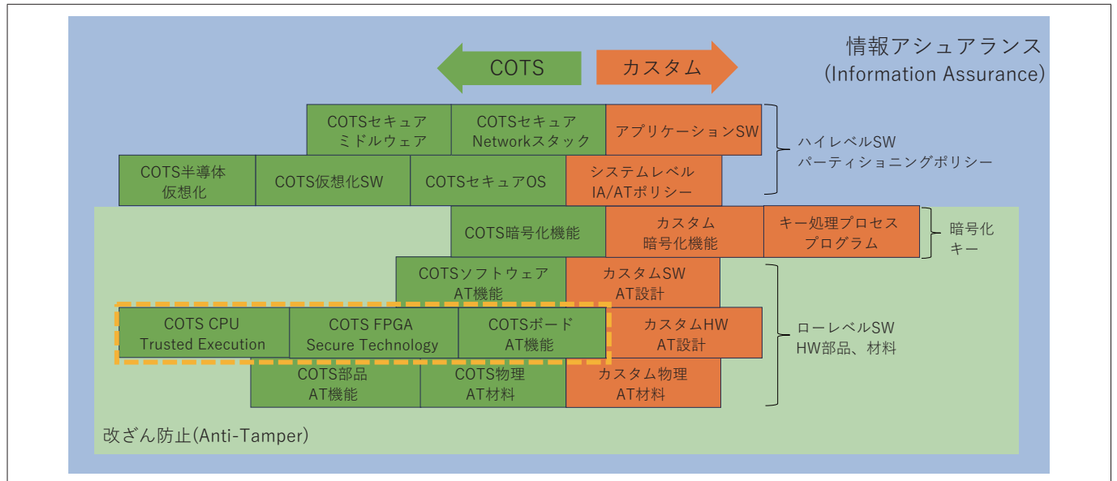


図１．情報アシュアランスの COTS 品とカスタム品の関係

防止・検出・応答：改ざん防止の３原則

攻撃者は安全なシステムから情報を取得しようとします。攻撃は本質的に受動的である場合もあれば、能動的である場合もあります。受動的な攻撃には、タイミング、動的な電力消費、または電磁漏洩から秘密を確認するためのサイドチャネル分析が含まれます。プローブ回路や画像コンポーネントも同様です。積極的な攻撃には、物理的侵入やハードウェアの変更が含まれます。信号破損、プロトコル攻撃、悪意のあるソフトウェアによる障害の誘発も含まれます。

● 防止

理想的には、安全なシステム内のATは攻撃によるセキュリティ侵害を防ぎますが、脅威がセキュリティ戦略よりも高度な場合には、十分に長い時間遅延が発生することを期待して、少なくとも重要な情報の取得を遅らせるように機能します。その結果、情報は役に立たなくなります。

予防的保護手段の例としては、シールド、カプセル化、暗号化などがあります。

● 検出

ATセーフガードは脅威を検出し、能動的または受動的に脅威を阻止することもできます。保護メッシュと低電力または無電力改ざんセンサーは違反を通知することができ、半導体の物理的複製不可能機能（PUF）は検証のためにデバイスを一意に識別する手段を提供します。

● 応答

脅威が検出されると、システムは多くの場合それ自体の重要な要素を破壊することによって積極的に対応できます。メモリリソースのゼロ化、通信インターフェースの無効化、暗号化キーの消去、発火や高電流による損傷の誘発などは改ざんイベントへの対応の例です。

図２は、システム例の４つの層（筐体、列線交換可能ユニット（LRU）またはプラグ可能回路基板、プリント配線基板（PWB）、および半導体）の基本的なAT機能の一部を示しています。 図３は２つのAbaco製品を示しています。１つは6U OpenVPX堅牢シングルボードコンピュータ、もう１つは耐環境コンピュータです。

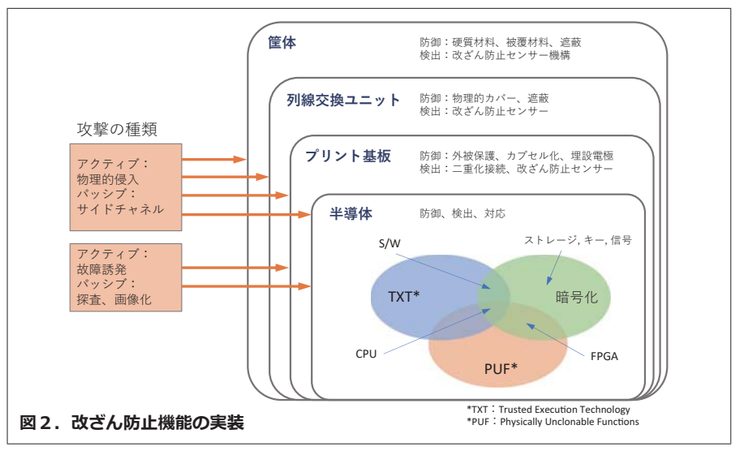


図２．改ざん防止機能の実装

図 3．Abaco 社の 6U OpenVPX SBC と耐環境システム

ATをゼロから構築

特定のシステムの脅威モデルは、そのシステムの展開方法、攻撃者の能力、重要なテクノロジーやプログラム情報の種類、

MISH Tech Journal 2024 SUMMER

その他の要因によって異なります。したがって、目標は有用なCOTSベースの改ざん防止オプションを提供し、特定の脅威に最適に対処するためにカスタムの側面を含めることを可能にすることです。これを達成するために、ATの原則がハードウェア設計の初期段階に組み込まれます。

ルートオブトラスト

最も低いレベルでは、堅牢なAT設計には、ルートオブトラストつまりセキュアブートプロセスの基盤を提供する認定されたCPUベースのハードウェア/ファームウェア要素が必要です。ルートオブトラストは次のステージを検証し、各ステージが検証されるたびに信頼できるシステムを構築する一連のプロセスを開始します。これにより、信頼できないコードの実行が防止され、変更されたセキュリティ値の使用を検出することでソフトウェア攻撃が防止されます。IntelおよびFreescaleプロセッサは、暗号キーと認定された変更不可能なBIOSまたはboot ROMを使用しその方法を提供します。これらの機能については次のセクションで説明します。

もう1つの重要なコンポーネントは、FPGAベースのセキュリティハブです。これは改ざんイベントを検出し、カスタマイズされた応答を提供する中央システムモニターです。セキュリティハブは信頼できる処理システムと連携し、ATポリシーを管理するための独立した制御を提供します。

最後に、暗号化ストレージはデータとアプリケーションソフトウェアを保護するために使用されます。アーキテクチャの例を図4に示します。

Intelのトラストエクスキューション

IntelのTrusted Execution Technology (TXT) は、不正なソフトウェアによる監視や変更が不可能な、安全で隔離されたソフトウェア実行スペースを定義します。実行スペースには、プロセッサ、チップセット、およびオペレーティングシステムカーネルによって管理される専用のリソースがあります。CPUは、メモリへのアクセスを強化するために保護されたパーティションを提供します。プラットフォームコントローラーハブ(PCH) はメモリ保護ポリシーを適用し、グラフィックスハードウェアおよび入出力デバイスへの保護されたデータ転送を提供します。また、PCHは暗号キーを生成および保存しセキュアブートプロセス中にプラットフォームの状態を保存し、システムのセキュア状態のレポートまたは証明をサポートするハードウェアデバイスであるトラステッドプラットフォームモジュール(TPM)にもインターフェースします。

図5は、安全なインテルTXTブートプロセスの手順を示しています。

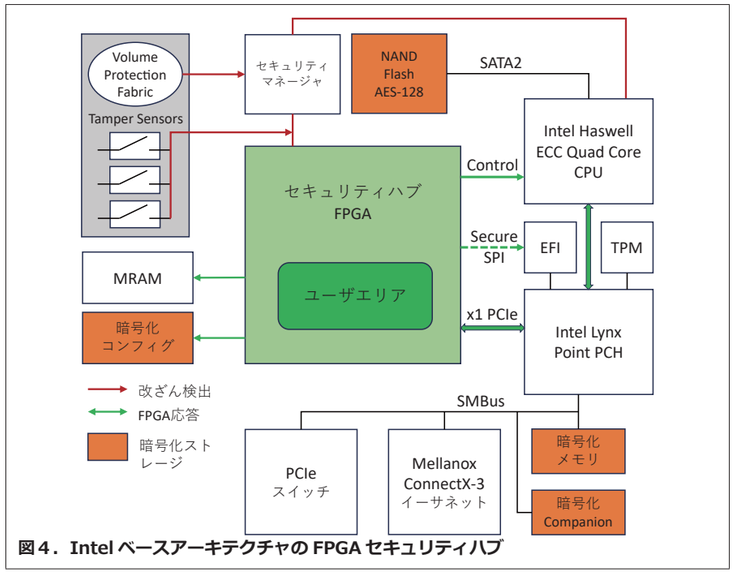


図4．Intel ベースアーキテクチャの FPGA セキュリティハブ

測定と拡張：

1. システムのリセット後、BIOSブートブロックは測定のための信頼ルート(CRTM)のコアとして機能し、最初に信頼されていないコンポーネントであるシステムBIOSを測定します。 測定値はBIOSコードのハッシュ値であり、TPMのプラットフォーム構成レジスタ(PCR)の1つに保存されます。保存操作は実際には、既存のPCRコンテンツと新しい測定情報を連結したものです。つまり、保存された値には最後の起動以降にシステムに加えられた変更が反映されます。このプロセスは「Extension(拡張)」と呼ばれます。
2. BIOSはハードウェアとマスターブートレコードを測定しPCRを拡張します。
3. マスターブートレコードは、Intel TXTのプリローダー、Loader 1を測定しPCRを拡張します。プリローダーは、信頼できる実行を開始する命令用にメモリを準備します。

検証：

4. Loader 1は、認証されたコードモジュール(ACM)を検証します。ACMはIntelによってデジタル署名されたチップセット固有のコードで、次に実行できるアプリケーションのリストを検証します。
5. ACMはLoader 2を検証します。Loader 2はプラットフォーム設定レジスタ、システム管理モードコード、およびオペレーティングシステムローダーを検証します。

実行：

6. オペレーティングシステムローダーがオペレーティングシステムを準備し起動します。

TPMの動作：

7. その後、セキュアオペレーティングシステムがTPMの所有権を取得できるようになり、現在のPCR値を使用してデータをシール(暗号化)する機能が提供されます。PCR値がデータが封印されたときと同じである場合にのみ、データの封印を解除(復号化)できます。TPMの所有権はTPMがクリアされた場合にのみ変更でき、前のキー所有者によって封印されたデータを封印解除しようとすると失敗します。ネットワーク化されたシステムでは、TPMは現在のPCRセットの引用に署名することによって、レポートの信頼ルート(RTR)として機能することもできます。

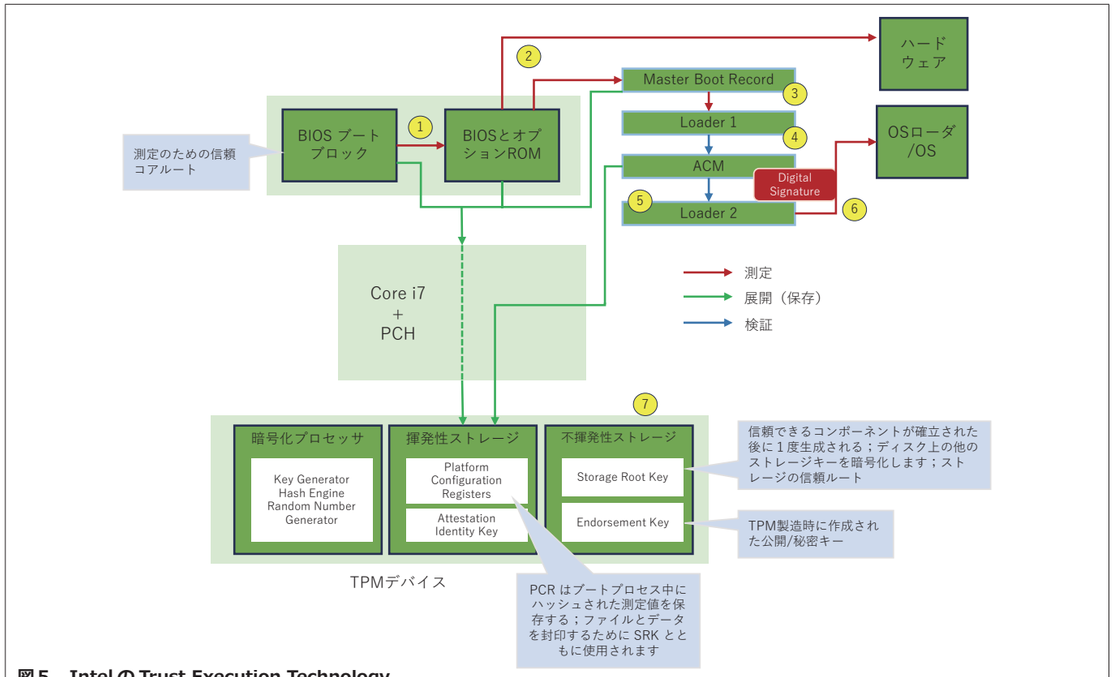


図5．Intel の Trust Execution Technology

Freescale(NXP)トラストアーキテクチャ

Freescale (NXP) の QorIQ Trust Architectureは、セキュアブート、セキュアランタイム、セキュアデバッグ、改ざん検出、およびデバイス固有の秘密キーの使用を提供します。これによりCPUによる信頼できないコードの実行が防止され、変更されたセキュリティキーの使用が防止されます。

セキュリティ機能はQorIQシステムオンチップに内蔵されており、外部の信頼できるデバイスは必要ありません。図6は、Freescaleセキュアブートプロセスの手順を示しています。

コード署名とプロビジョニング：

1. トラストアーキテクチャは、ユーザーによるPublicキーとPrivateキーのペアの生成に依存しており、これはFreescaleコード署名ツールを使用して実現できます。Privateキーは、QorIQプロセッサ上で実行されるすべてのコードにデジタル署名するために使用されます。Privateキーは保護する必要があります。署名付きコードへの変更はセキュアブートプロセス中に検出できます。
2. Publicキーは、デバイスのプロビジョニング中にハッシュ化され、CPUにプログラムされます。これは外部セキュアブートコード(ESBC)のデジタル署名を検証するための基礎を提供します。

ブート前フェーズ：

3. リセット後、すべてのデバイスのアクティビティがブロックされます。ヒューズの値はセキュリティヒューズプロセッサ(SFP)によって感知され、インターフェースとメモリをロックダウンし、起動前にセキュリティポリシーを適用します。次に、プリブートローダー (PBL) が外部不揮発性メモリからリセットコンフィギュレーションワードをロードして、システムコンフィグレーションを開始します。

内部セキュアブートコード(ISBC)フェーズ:

4. CPUはブートを許可され、内部ブートROM内の配線された場所から内部ブートコードの実行を開始します。ISBCは本質的に信頼されています。デバイスへのPublicキーのバインドを確認し、ESBCのデジタル署名を検証し、ESBCイメージを検証し最初の命令が検証された範囲内にあり実行されることを確認します。

外部セキュアブートコード(ESBC)フェーズ:

5. ESBCは、モノリシックイメージまたはマルチステージブートイメージにすることができ、オペレーティングシステムまたはアプリケーションのデジタル署名とイメージを検証し、それによって信頼の連鎖を拡張します。

COTSセキュアFPGAテクノロジー

FPGAセキュリティハブは、システム全体の改ざん検出センサーから入力を受け取り、プロセッサとインターフェースする機能を備えています。保存されているデータ、設定、およびキーを消去し、適切な改ざん応答を提供するためにインターフェースを無効にします。FPGAは、標準COTSまたはカスタムされた構成のいずれかを使用してその応答動作を定義できます。

FPGAコンフィグレーションは、コンテンツを保護するためにさまざまな保護手段を使用して暗号化されます。 AMD(Xilinx) Artixデバイスと Lattice MACHXO2デバイスは両方ともセキュリティハブとして機能するために使用されます。

- **AMD（Xilinx）**

AMD Artix FPGAは、さまざまなAT機能を提供します。パッシブ機能(COTS機能)はチップに組み込まれており設計開発

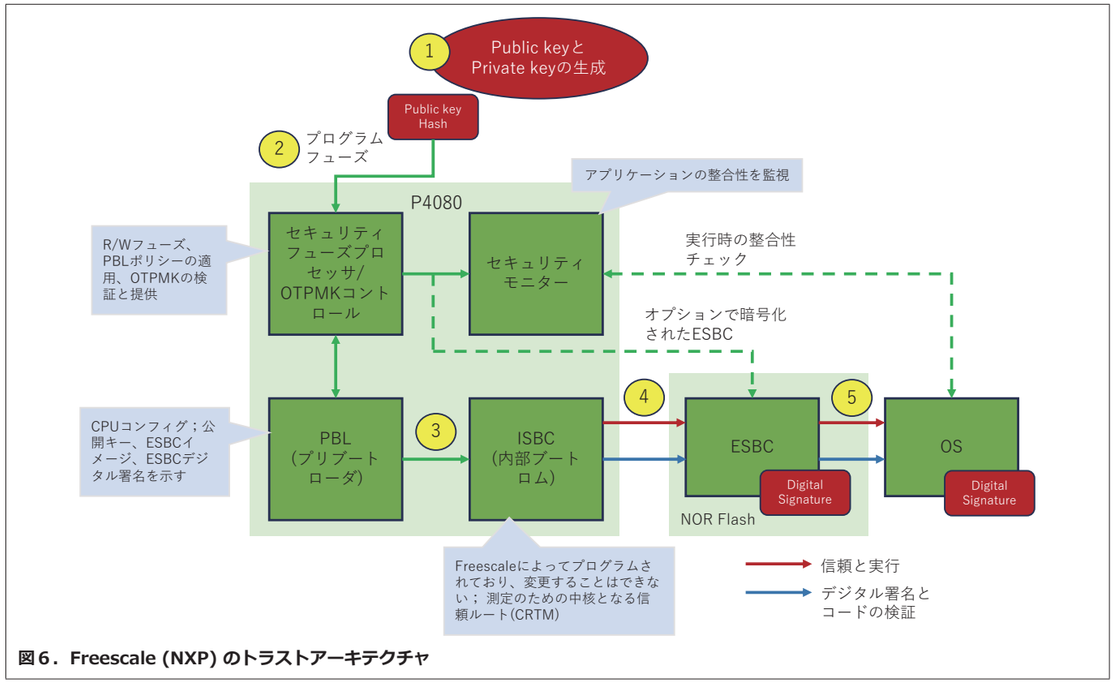


図６．Freescale (NXP) のトラストアーキテクチャ

は必要ありませんが、アクティブ機能はカスタム FPGA設計作業の一部として必要に応じて組み込むことができます。

表１は、利用可能な AT機能の完全なリストを示しています。

- **Lattice**

Lattice MACHXO2 FPGAには、オンチップの組み込みフラッシュメモリが組み込まれており、コンフィグレーションビットストリームの脆弱性を排除します。デバイスセキュリティビットは、デバイスからの設定のリードバックを防ぎワンタイムプログラム可能モードにより、設定の消去や再プログラミングを防ぎます。

Anti-Tamper機能	タイプ	カテゴリー
揮発性AES-256 BBRAM キーストレージ	パッシブ	防御
不揮発性AES-256 eFUSE キーストレージ	パッシブ	防御
256bit AESビットストリームの復号化	パッシブ	防御
HMAC SHA-256ビットストリームの認証	パッシブ	防御
ハード化したリードバック無効化回路	パッシブ	防御
堅牢なキーロード有限ステートマシン	パッシブ	防御
JTAG無効化	アクティブ	防御
JTAG監視	アクティブ	検出
内部コンフィグメモリの整合	アクティブ	検出
オンチップ温度・電圧監視／警告	アクティブ	検出
傍受プログラム	アクティブ	検出
固有識別子（デバイスDNAとユーザeFUSE）	アクティブ	検出
内部コンフィグメモリクリア	アクティブ	応答
内部AES-256 BBRAMキー消去	アクティブ	応答
グローバル トライステート（GTS）	アクティブ	応答
グローバル セットリセット（GSR）	アクティブ	応答

表１．AMD Artix の Anti-Tamper 機能

まとめ

アンチタンパーは、組み込みシステムの情報保証スキーム全体において重要な役割を果たします。アンチタンパーを導入することで、予防・検出・対応のための多層的な保護手段が提供されます。慎重に検討されたCOTS/カスタムの組み合わせでは、低コストで信頼性の高いCOTS要素を活用しながら、お客様は機密性の高いテクノロジー、ポリシー、および手順を組み込むことができます。Abaco社はパートナーとの連携を利用してハードウェア、ミドルウェア、スタック、パーティション化されたオペレーティングシステム、ハイパーバイザー間の相乗効果を提供します。IntelのTrusted Execution Technology とFreescale (NXP) の Trust Architecture の使用により、業界標準の信頼メカニズムが提供されAMD (Xilinx) またはLatticeベースのFPGAセキュリティハブが堅牢な改ざん応答を強化します。ハードウェア構築オプションを利用して、顧客の要件を満たす柔軟性を提供します。

リファレンスドキュメント：

Abaco Systems: Anti-Tamper Technology: Safeguarding Today's COTS Platforms

Abaco SYSTEMS
AMETEK

DATA SECURITY

データの暗号化とセキュアイレース

貴重なデータを保護する方法として暗号化は重要な機能です。ここでは、ハードウェア暗号化、ソフトウェア暗号化、自己暗号化ドライブ（SED）、およびデータを永久に削除するためのセキュアイレースなど、組み込みシステムのデータセキュリティ技術について説明します。

はじめに

データは非常に貴重なリソースであり、多くのアプリケーションにとってデータは保護される必要があります。一般的に、システムには次の３種類のデータがあります。

「Data in Use」：コンピュータシステム内で頻繁に処理されます。DRAM、キャッシュまたはプロセッサエンジンに存在する場合があります。

「Data in Transit」：通常、ネットワークやデータリンク接続を介して、異なるコンピュータシステム間で送信されます。

「Data at Rest」：不揮発性ディスクドライブに保存されます。多くの場合、ドライブはコンピュータシステムから物理的に取り外すことができます。

ここでは、保存データ「Data at Rest」についてのみ説明します。

システムインテグレータとエンドユーザが保存データの保護を検討する理由は複数あります。データ保護のプログラム要件または業界標準によって、保存データ保護のどのレベルが必要か、または必要になるかが決まります。多くの場合、データセキュリティではデータとデータにアクセスするためのキーの両方を保護するために、複数のシステムの統合と運用の変更が必要になります。

航空宇宙および防衛システムで使用される最新の堅牢な組込みコンピュータおよびサーバーは、過酷な環境で動作する必要があります。これらのシステムは、無人で動作するプラットフォーム上にある場合があり、そのためにデータセキュリティの必要性が高まりますが、ローカルオペレータが存在しないためシステムの複雑さも増大します。基地でうまく機能していたとしても、戦場ではデータセキュリティが機能するとは限りません。

ここでは、堅牢な組込みシステムで保存データを保護するためのさまざまなオプションを詳しく見ていきます。また、保存データを暗号化するためのさまざまな方法と、そのデータを消去するためのオプションの詳細について検討しています。暗号化とセキュアイレースは、アプリケーションやプログラムのニーズに応じて、個別に使用することも一緒に使用することもできます。

Galleon Embedded Computing社製品には、最高機密に至るまでの幅広いデータセキュリティオプションが用意されています。この記事は１つの解決策を推進するものではなく、さまざまなアプローチの長所と短所に関する情報を提供することを目的としています。アプリケーションに最適なソリューションは、データセキュリティ要件、運用要件、機器の場所、データレート、その他の要件に依存する可能性があります。

ケーススタディ：NATO AGS (Alliance Ground Surveillance)

無人航空機システム（UAS）では、ミッション中に機体が紛失したりコントロールできない場所に運ばれたりした場合にデータがどうなるかという懸念が常にあります。これは、このプログラムのデータ記録および管理要件におけるセキュリティ側面の１つにすぎません。

Galleon Embedded Computing社は、これらの要件を満たすCOTSソリューションを提供することができます。ハードウェアフルディスク暗号化機能を備えたGalleon製 XSR Network Attached Storage (NAS)が、使いやすさ、小型サイズ、セキュリティ機能、および利用可能な大容量ストレージの理由により選択されました。ソリューション全体を小型の伝導冷却パッケージで提供するCOTSソリューションにより、航空機への設置と統合が容易になりました。XSR Secure NASは、NATO AGS UASなどのプラットフォーム上で複数の機能を提供できます。

複数のデータストレージオプションとキーイングオプションを備えたこのシステムは、安全なデータレコーダおよびストレー

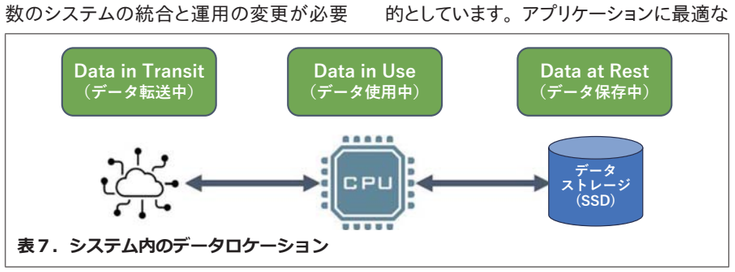


表７．システム内のデータロケーション

MISH Tech Journal 2024 SUMMER

ジシステムとしてだけでなく、その他重要なシステムに接続されたネットワークブートデバイスとしても使用できます。

XSR Secure NASは、複数のGigabitイーサネットポートと、他のシステムに接続するための幅広い共通インターフェイス用の10GbEオプションを提供します。NATO AGSプログラムは、イーサネットなどの一般的なインターフェイスを使用して、コンピュータ間の接続を標準化します。標準化には、より優れた長期サポートとライフサイクル管理が可能になるという利点があります。

大容量のXSRリムーバブルデータモジュール(XSR RDM)は、ハードウェアフルディスク暗号化ソリューションで保護されています。XSR RDMを使用すると、最大80TBの高速/大容量ストレージを工具不要で取り外し交換できます。データ分析やミッションの準備のためにXSR RDMとの間でデータを移動するには、互換性のあるハードウェアフルディスク暗号化モジュールを備えたオフロードサーバーが使用されます。

Galleon社は、NATO AGSプログラムに完全なソリューションを提供しました。

重要な用語

ここでは、記事全体で使用される一般的な用語を説明します。

AES (Advanced Encryption Standard): アメリカが標準暗号として定めた共通鍵暗号アルゴリズム

Authentication: 暗号化されたデータにアクセスできるように、暗号化エンジンを有効化/ロック解除する

Brute force attack: 256bitキーを推測して暗号化されたデータにアクセスしようとする試み

CSfC (Commercial Solutions for Classified): 国家安全保障システム(NSS)データを保護するソリューションで使用される商用製品を承認するための米国政府のプログラム

CC (Common Criteria for Information Technology Security Evaluation): コンピュータセキュリティのための国際規格であり、Common Criteria Recognition Arrangement (CCRA) の技術的規格

DAR (Data at Rest): デジタル形式で保存されている非アクティブなデータのこと

DEK (Data Encryption Key): ドライブとの間でデータを暗号化/復号化するために使用される鍵

EDEK (Encrypted DEK): DEKの暗号化されたキーのこと

FIPS 140-2 (Federal Information Processing Standard 140-2): 暗号化デバイスおよびモジュールを承認するために使用される米国政府の規格

HWFDE (Hardware Full Disk Encryption): ハードウェアによるフルディスク暗号化

KEK (Key Encryption Key): EDEKの暗号化/復号化に使用される鍵のこと、通常はPBKDF2を使用してユーザー名/パスコード認証データから生成される

NAS (Network Attached Storage): ネットワーク接続ストレージ

PSK (Pre-shared Key): 安全なデータモジュールの移植性を実現する既知の暗号化キー

PBKDF2 (Password Based Key Derivation Function 2): 256bitキーと比較して、ユーザー名とパスワードの組み合わせにおけるエントロピーの不足を軽減するように設計されたキー導出関数

RDM (Removable Data Module): リムーバブルデータモジュール

SSD (Solid State Drive): フラッシュメモリアレイを使用したストレージドライブ

SWFDE (Software Full Disk Encryption): ソフトウェアによるフルディスク暗号化

Symmetric Encryption: 対称暗号化：暗号化と復号化に同じ暗号化キーを使用する

Asymmetric Encryption: 非対称暗号化：キーの組み合わせ(秘密キーと公開キーなど)を使用してデータを暗号化する。通常は安全なリンクで使用される

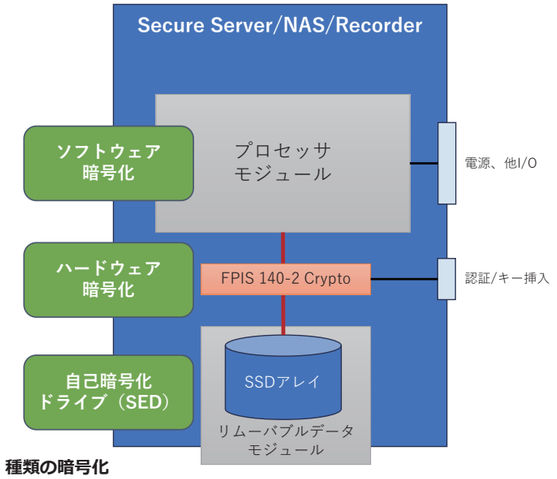


図８．３種類の暗号化

暗号化

暗号化により、データは消去することなく保護されます。例えば、搭載されたレコーダ/NASからリムーバブルデータモジュール(RDM)を基地に移動する場合、データは保護された状態です。

保存データの暗号化にはいくつかの種類があります。ここでは、自己暗号化ドライブ(SED)、ハードウェアフルディスク暗号化(HWFDE)、およびソフトウェアフルディスク暗号化(SWFDE)を含むソフトウェア暗号化について説明します。SEDはハードウェア暗号化の一種ですが、ここでは「ハードウェア暗号化」という用語は、SSDへのパス内のインラインハードウェア暗号化ソリューションとして使用されていることに注意してください。

3つの方法はすべて標準の暗号化アルゴリズム(AES-256)を使用します。

AESはブロック暗号であり、データのブロックを暗号化することを意味していることに注意してください。暗号化されていないデータ内の繰り返しパターンが同一の暗号化されたデータパターンでエンコードされないように、保存データには追加の保護が必要です。このリスクから保護するために広く使用されているスキームの1つがAES-XTS (XTS-AESとも呼ばれます)です。

暗号化メカニズムの比較

このセクションでは、保存データに通常使用される3つの異なる暗号化メカニズムの概要を説明します。

● 自己暗号化ドライブ(SED)

暗号化はSSD (Solid State Drive)の機能の一部として利用されます。

SEDには、認定/承認されたバージョンやOpalのような商業規格に準拠したバージョンなどさまざまなバージョンがあります。Opalベースの SEDでは通常、暗号化キーはSSD内に作成および保存(暗号化)され、エクスポートできません。Opalベースのドライブのロック解除は比較的簡単で、通常はパスワードを入力するだけでロックを解除できます。認定/承認されたSEDでは、キー処理のオプションが異なるため暗号化デバイスがSSD内にあることを除けば、以下で説明するインライン暗号化装置に似ています。

● ハードウェア暗号化(HWFDE)

コンピュータシステムとドライブ間のパスで暗号化デバイスが使用されます。さまざまな暗号化キーの処理とロック解除スキームが利用可能です。ハードウェア暗号化は、リムーバブルドライブと同じ製品に組み込まれている場合があります。外部暗号化装置もいくつかあり、その一部は高いセキュリティレベルで認定されています。これらは同じように機能しキー処理に関して同様のオプションがあります。違いは、これらが個別のエンクロージャであることと認証/承認のレベルが異なる場合があることです。

● ソフトウェア暗号化(SWFDE)

ドライブに送信されるデータは、コンピュータ上で実行されているソフトウェアによって暗号化されます。通常、キーはソフトウェアで作成され、各ドライブのパーティションに保存(暗号化)されますが、他のオプションも利用できます。

暗号化メカニズム	利点	欠点
自己暗号化ドライブ(SED)	✓ 利用が簡単 ✓ 価格が安い	✓ キーと暗号化デバイスがSSD内にある ✓ AESアルゴリズム以外は通常は認定されていない ✓ 通常パスワードは1つだけ
ハードウェア暗号化 (HWFDE)	✓ 認定された暗号を使用 ✓ 認証可能 (共通基準) ✓ 専用プロセッサを備えた専用キー交換ポートによりキーや認証がメインプロセッサドメインに公開されることがない	✓ 複雑なシステム統合とユーザー対話 ✓ 単一のストレージトポロジ(現時点ではSATA)に関連付けられている
ソフトウェア暗号化 (SWFDE)	✓ 認証可能 (共通基準) ✓ パーティションの個別暗号化	✓ キーはSSD内に保存される ✓ キーイングと認証管理のための慎重な統合が必要

表２．暗号化メカニズムの比較表

ソフトウェア暗号化にはある程度のプロセッササイクルが必要ですが、通常パフォーマンスへの影響は最小限であることに注意してください。ほとんどのプロセッサには暗号化/復号化オフロードエンジンが含まれているため、メインプロセッサエンジンにはそれほど負荷がかかりません。したがって、プロセッサのパフォーマンスについては表2の欠点として挙げられていません。

暗号化キーの処理

保存データの暗号化には、ディスクへの書き込みおよびディスクからの読み取り時にデータを暗号化および復号化するある種の暗号化プログラムが含まれます。図9はデータ暗号化キー(DEK)の概念を示しています。

AES-256はブルートフォース攻撃からデータを保護するのに非常に効果的であるため、データにアクセスできる唯一の方法は、攻撃者がデータ暗号化キー(DEK)にアクセスした場合です。したがって、キー処理メカニズムの選択はデータ全体のセキュリティにとって重要です。ほとんどの場合、メカニズムが安全であればあるほどシステムはさらに複雑になります。根本的に異なる2つのアプローチがあります。キー自体を転送するか、キーを暗号化して保存し認証を使用してキーを復号化します。

一部のシステムでは電源投入時にキー(DEK)がシステムに提供されます。ただし、キーの保護は複雑になる可能性があるため、多くのシステムではデータ暗号化キー(DEK)をプラットフォームまたはディスクに保存する代替方法が使用されています。単純な攻撃からキーを保護するために、キーは暗号化された形式で保存されます。図10は暗号化データ暗号化キー(Encrypted Data Encryption Key)の概念を示しています。また、EDEKをDEKに変換する暗

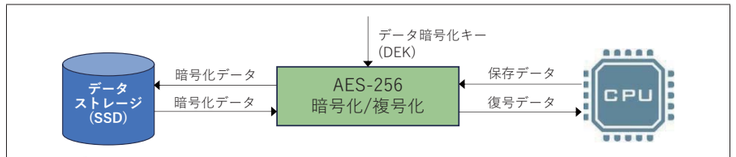


図９．データ暗号化キー (DEK)

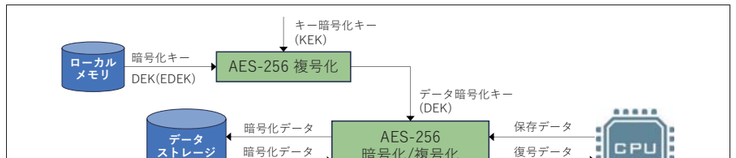


図１０．暗号化データ暗号化キー (EDEK)

	暗号化キーハンドリング方法	利点	欠点
暗号化キーを直接転送 (ローカルには何も保存されず、ユーザ名/パスワードも存在しないため潜在的な弱点が生じる)			
1	物理的トークン	✓ 利用が簡単	✓ トークンの管理とロギング ✓ 無人システムは仮想トークンを必要とするか、機体・車両が紛失した場合に公開される可能性がある ✓ すべてが一意のトークンを持つ複数の安全なシステムをプラットフォーム上に統合するのが複雑
2	安全なリンク経由で送信	✓ 集中キー管理：キーはいかなる形式でもローカルの不揮発性メモリに保存されない	✓ キーは安全なリンクの終端で暗号化されていない形式で利用できる必要がある ✓ リンクは安全でなければならない
暗号化キーを事前共有 (暗号化されたキー (EDEK) はローカルに保存され、キーを復号化するには認証が必要)			
3	手動で入力された認証データ(キーボードまたはローカル接続)	✓ 単独で使用可能：プラットフォームの外部からのリンクは必要ない	✓ 無人車両 (UAVなど) での使用には不便 ✓ ユーザ名/パスワードの記憶：ランダム性/不規則性の低減
4	安全なリンク経由で認証データを送信	✓ ユーザー名/パスワードは複雑にできることで不規則性が増す	✓ リンクは安全でなければならない
5	認証データはローカルサーバーに保存、EDEKはリムーバブルデータモジュール (RDM) に保存：起動時に自動ロック解除	✓ 最も単純な方法：システムレベルの複雑さを解消する ✓ RDMデータのセキュリティが確保されている (*サーバーから分離されている場合) ✓ キーは自動生成されSSDに保存される	✓ 輸送時にのみデータが保護される ✓ 暗号化キーを消去するとバックアップや復元ができなくなる

表３．キーハンドリングの認証オプションの比較

号化に使用されるキーである、Key Encryption Key (KEK)も導入されています。Key Encryption Key (KEK) は、(DEKを暗号化することにより) EDEK を生成するためにも使用されます。KEKの生成と処理については、次のセクションで説明します。

表3は、起動時のキー処理や認証に使用できる代替方法の利点と欠点を示しています。

ユーザー名/パスワードのスキーム

データ暗号化キーをローカルに保存することは常識に反しているように思えるかもしれませんが、AES-256暗号化を使用すればそれ自体はセキュリティリスクではありません。ただし、ユーザー名/パスワードを使用してキーのロックを解除する認証にはある程度のリスクが伴います。問題は、ユーザー名/パスワードの不規則性 (ランダム性) が低い、または 256bitのキーよりも長さが短い可能性があることです。したがって、攻撃者は256bitキー自体ではなく、ユーザー名とパスワードの組み合わせを推測することを狙う可能性があります。このリスクを軽減するために、このような攻撃をより困難にするためにさまざまな技術が使用されています。

- ハッシュ (Hashing) – プロセッサを大量に消費する非可逆アルゴリズム。完了までに意図的に時間をかけて、一定期間内に試行できるユーザー名とパスワードの組み合わせの数を減らします。ハッシュ関数は、強力な保護を提供しながら、通常の操作 (正しいパスワードが入力されたとき) の遅延が比較的短くなるよう所要時間に基づいて選択されます。
- ソルト(Salt) - ランダムに生成された値をアルゴリズムに追加することで不規則性が追加され、共通のユーザー名/パスワードが複数のユーザーまたはユニット間で同じハッシュ/キー暗号化キーを生成するのを防ぎます。
- レート制限 - 試行間の時間遅延を要求する前に、誤った推測の数を制限します。 注：これは、攻撃者が暗号化されたDEKにアクセスできない場合にのみ役立ちます(図11参照)。
- フォレンジック対策 – 暗号化/ハッシュされた暗号化キーをストレージ内で分割し、攻撃者が部分的に消去または損傷したストレージから暗号化キーを回復することをより困難にします。

ユーザー名/パスワードスキームを保護するために使用されるプロセスの例は、Hash関数とSaltを組み合わせてユーザー名/パスワード攻撃から保護するPBKDF2 (Passwordbased key derivation function 2)です。

このユーザー名とパスワードのスキームを使用すると、複数の異なるユーザーが同じ暗号化キーに対して独自のユーザー名とパスワードの組み合わせを持つことが可能になります。キー処理ソリューションは、有効なユーザー名ごとに個別の暗号化キー (EDEK)とSaltを保存するだけです。

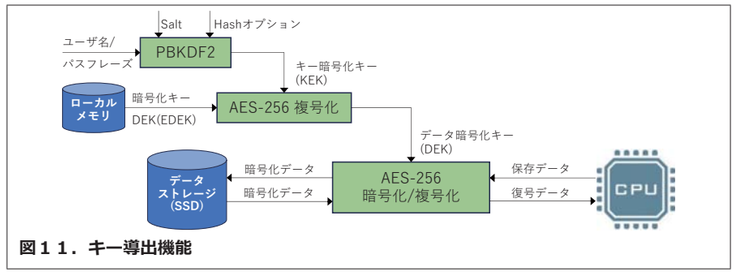


図１１．キー導出機能

データ暗号化キー (DEK)はまだ１つだけであるため、その256bitキーに対するブルートフォース攻撃によるセキュリティの低下はありません。

事前共有キー

事前共有キーは、システムの試運転中に(通常は安全な場所で)デバイスに(暗号化された形式で)書き込まれるキーです。その後、必要に応じてキーを再利用できるようになります。 別の方法は、キーをデバイス内で自動生成し同じデバイス内に保存(暗号化)することです。 これらのシステムでは通常、キーをエクスポートすることはできません。

事前共有キーを使用すると、脅威が存在し保存されたキー (EDEK)を消去することでデータが保護されている場合でも、データは永久に失われるわけではなく脅威が存在しなくなった後の段階で取得できます。対照的に、自動生成キーの場合EDEKが破壊されるとデータは永久に回復できなくなります。

電力の損失

電源が失われるか取り外されると、DEKは揮発性メモリに保存されているため失われます。要するに保存データは保護されます。EDEKは不揮発性メモリに保存されるため保存されたEDEKはそのまま残ります。電源が再投入されると、(どのキー処理メカニズムが使用されても)DEKが再度ロードされデータに再びアクセスできるようになります。

暗号消去

脅威が検出された場合、多くの暗号化システムでは電源をオフにすることなくDEKを削除/破棄できます。これによりデータが保護され、脅威が存在しなくなったとき次回のシステム起動時にDEKが再度ロードされます。

ただし、追加のセキュリティレベルとしてEDEKをローカルに保存するシステムの場合、オプションで暗号化消去を使用してこれを破棄することもできます。前述したように、事前共有キーを使用すると、脅威がアクティブでなくなったときにEDEKがリロードされデータが回復されます。

対照的に、一部の暗号化システム (例えば以下で説明するOpal SED) では、暗号消去により DEKとEDEKの両方が消去されます。EDEKは事前共有キーではないため、このような暗号化消去の後はデータを回復できなくなります。

自己暗号化ドライブ (SED)

このセクションでは、Opal3などの規格に基づいて暗号化および復号化アルゴリズムを実装するSEDについて説明します。最高機密の実装に必要な、より安全なキー処理アルゴリズムを実装するSEDの例がいくつかあります。これらについてこの後のセクションで個別に説明します。

多くのSSDベンダーが自己暗号化ドライブを提供しています。自己暗号化ドライブには、ドライブハードウェアの不可欠な部分として暗号化回路が組み込まれており、有効にするとエンドユーザに対して完全に透過的になります。使用される方法と用語はSSDベンダーによって異なりますが、基本的なプロセスにはSSDのロックとロック解除が含まれます。

多くの場合、高レベルのセキュリティと高度なキー管理に対する厳格な要件がない場合、SEDはシンプルでコスト効率の高いソリューションとなります。この目的で使用される SEDには、検証済みのAESアルゴリズム実装が必要であることに注意してください。検証は暗号アルゴリズム検証プログラム(CAVP)を使用して利用でき、米国政府のNISTグループが運営するコンピューターセキュリティリソースセンター(CSRC)で照合されます。

自己暗号化SSDは、標準操作の一部として暗号化/復号化を適用します(通常パフォーマンスへの影響はほとんどありません)。このような暗号化と復号化自体は、ユーザーには気付かれません。これは、SSDに書き込まれるすべてのデータが暗号化され、SSDから読み取られるすべてのデータが復号化されるためです。暗号化キーはSSDによって自動生成されます。

SEDのセキュリティ機能は、デバイスをロックおよびロック解除することによって有効になります。ロックは、特別なコマンドを使用して特別なコード(パスコード/パスフレーズを含む)をSSDに書き込むことで実施されます。次に、SSDは新しいキーを作成(暗号化)して保存し、そのキーを使用してデバイスに書き込まれるすべてのデータまたはデバイスから読み取られるすべてのデータの暗号化/復号化を行います。その後、(別の特別なコマンドを使用して同じコードをSSDに書き込むことによって)ロックが解除されるまでデバイスはアクセスできなくなります。

通常このパスコード/パスフレーズはSSD内には保存されません。 代わりに、前のセクションで説明したPBKDF2アルゴリズムなどの技術を使用してSSD内の暗号化キー (SSD内でランダムに作成される)を暗号化/復号化するために使用し、追加のデータセキュリティを提供しています。

注：すべてのドライブベンダーが、暗号化と消去機能の処理方法を定義する規格(OPALなど)に完全に準拠しているわけではありません。したがって、実装がドライブベンダー固有になることが多く、ドライブのアップグレード/変更により互換性の問題が発生する可能性があります。

- **SEDによる認証**

商用コンピュータ(ノートPCなど)では、ユーザーはSSDのブート初期化中にパスワードを入力する必要があります。多くのプログラム、特に組込みコンピューティング、NAS、またはレコーダアプリケーションでは、このローカル認証は適していません。

したがって、Galleon社は表３のオプション4および5で説明されている代替オプションを提供します。キーはSED内で作成され、暗号化された形式で保存されるため認証の唯一のオプションは、キーのロックを解除するためのパスワード認証に基づきます。ほとんどのSEDでは、ドライブのロックを解除するパスワードは１つだけです。複数のユーザーが個別の認証を行うオプションはありません。

- **SEDによるセキュアイレース**

多くのSEDはセキュアイレースアルゴリズムも実装しており、二重のデータセキュリティを提供していることに注意してください。通常、脅威がアクティブな場合暗号化キーはデータとともに消去されます。

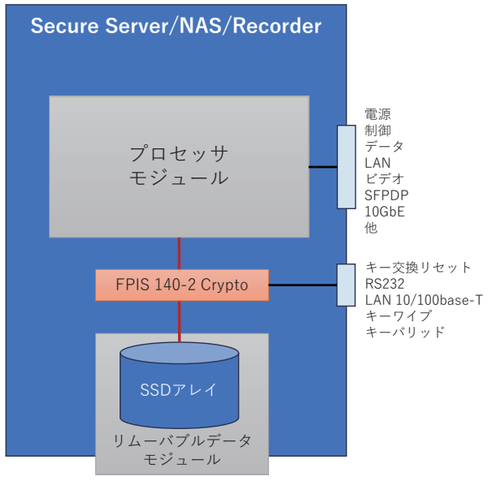


図１２．ハードウェアフルディスク暗号化 (HWFDE)

ハードウェアフルディスク暗号化(HWFDE)

最高レベルのセキュリティを実現するために、Galleon社は複数の暗号化デバイスを使用するSATAからSATAへのハードウェアフルディスク暗号化モジュールによって実装される高度なデータ暗号化(AES-256)を提供します。これらの暗号化デバイスは FIPS 140-2 に認定されており、データの暗号化および復号化機能を提供します。

暗号化モジュールは、図12に示すようにオペレーティングシステムおよびユーザーアプリケーションに対して完全に透過的にキー交換を処理する自己完結型ユニットです。

ハードウェア暗号化による認証

Galleon社は、ハードウェア暗号化ソリューションを使用して表３にリストされている認証のすべてのオプション(物理的トークンを除く)を提供します。いずれの場合も、RDM (リムーバブルデータモジュール) は取り外して基地に輸送でき、サーバー / NAS/ レコーダと同じキーを基地の機器で使用できます。

暗号キー (DEK) が暗号化モジュールに直接提供される場合 (表３のオプション2)、モジュールはメインプロセッサから完全に分離された専用のイーサネットリンクを介して安全なリンク通信を提供します。よって、暗号キー (DEK) が公開されない限りデータは安全です。

事前共有キーオプションが使用される場合、キーはPBKDF2と同様のキー導出関数を使用して暗号化モジュールに保存されます (上記のセクションで説明)。認証データ (ユーザー名 / パスフレーズ) が不明でない限りシステムは安全です。複数の(ほぼ無制限) 異なるユーザーが個別の認証データを持つことができ、各ユーザーの特定のRDMへのアクセスを制限するオプションも利用できます。

RDMがサーバーから取り外されると、暗号化ハードウェア (キーが保存されている場所) から物理的に分離されるため、最終目的地まで安全に輸送でき、そこで同じ暗号化ハードウェアとデータ取得用の事前共有キーを使用してサーバーまたはドッキングステーションに再インストールされます。

最後に、暗号化ハードウェアはコンピュータシステムの一部であるため、選択したディスクとは独立しておりシステムにインストールされているどのSSDでも動作します。これにより、特定のSSDに組み込まれた暗号化機能との互換性を維持する必要がなく、将来の最新の SSDテクノロジーと容量へのアップグレードが可能になります。さらに、用途に応じてカスタマイズされた記憶媒体を使用することができます。たとえば、研究室や開発で使用する低コストの商用グレードのSSDや、配備されたミッション用のハイエンドの軍用グレードの SSDはすべて同じ暗号化ハードウェアでサポートされています。

注：この記事の執筆時点では、暗号化用に認定されている暗号化デバイスはSATA接続に基づいています。

自己暗号化ドライブとの比較

Galleon社ハードウェア暗号化ソリューションは FIPS 140-2認定の暗号デバイスを使用しますが、Opalベースの自己暗号化SSDはアルゴリズムの正確さに関連する認定のみを実施しています。

また、ハードウェア暗号化モジュールは暗号化キーがディスク内に保存されず、暗号化エンジンがSSD内ではなくコンピュータシステム内にあるため、自己暗号化ドライブと比較して追加のデータセキュリティを提供します。自己暗号化ドライブでは、キーと暗号化エンジンの両方がSSD内に存在します。

パスコードが安全なリンクを介して送信される場合、認証は自己暗号化ドライブと非常に似ていますが、その場合でも使用されるイーサネットリンクはキー管理を処理するマイクロコントローラー専用であるため、一般的なプロセッサよりも暗号化モジュールの方が有利です。

最後に、ハードウェア暗号化によりシステムはリンクの終端で認定されたSSDを使用できるようになりますが、SEDに基づく暗号化は特定のSSDベンダーから提供されています。

ソフトウェア暗号化

保存データのソフトウェア暗号化は業界で広く使用されており、コンピュータの電源投入時に簡単なユーザー名 / パスワードまたは指紋ID認証を使用します。このタイプの機能は、より安全なアプリケーションでも利用できハードウェア暗号化と併用してデータのセキュリティを強化することもできます。この２つの暗号化は完全に独立しているため、セキュリティの強度がさらに高まります。その代償としてシステム起動時の認証要件がさらに複雑になります。

保存データに対するCSfC(Commercial Solutions for Classified)の承認には、独立したプロセッサと認証によるこの２層暗号化が必要です。２つの層を完全に分離しておくことにより、一方のソリューションで特定された潜在的な脆弱性がもう一方のソリューションに影響を与えないためソリューション全体のセキュリティが強化されます。

ソフトウェア暗号化は、LUKS (Linux Unified Key Setup) ディスク暗号化ソリューションなどさまざまな形式で利用できます。LUKSでは、暗号化キーはSSDに保存され、PBKDF2アルゴリズムを使用して保護されたパスフレーズで暗号化されます。データの暗号化と復号化はメインプロセッサ上で行われます。LUKSは、暗号化キーごとに最大８つのキースロット(８つの異なる認証ユーザー名 / パスワード) をサポートします。

ソフトウェア暗号化は、同じディスク上の異なるパーティションに個別の暗号化キーを簡単に使用できる唯一のオプションであることに注意してください。ハードウェア暗号化デバイスはセクターアドレスに基づくキーマップをサポートできますが、暗号化システムとOSのパーティションマップを同期させると非常に複雑になりリスクが高まります。

二重暗号化とCSfC

複数層の暗号化を使用すると、特に認証接続とメカニズムが完全に独立している場合、データのセキュリティが大幅に強化されます。これは、米国のCommercial Solutions for Classified (CSfC) プログラムのベースとなっています。

・ソフトウェアフルディスク暗号化 (SWFDE) は認証にメインプロセッサを使用します。
・ハードウェアフルディスク暗号化 (HWFDE) は認証と暗号化デバイスへのDEK のロードに別のプロセッサを使用します。

これら２つのメカニズムを組み合わせることで、優れたレベルのデータセキュリティが提供され、Common Criteria認証と組み合わせることでCSfCの承認が可能になります。

セキュアイレース

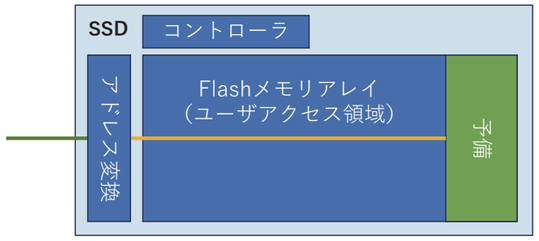


図１３．SSDの予備領域

ほとんどのアプリケーションでは、完全なデータセキュリティを実現するために関連する「crypt erase」(暗号化キーのみが消去される) を使用した暗号化で十分です。ただし、この章ではディスクに保存されているデータ全体の消去について説明します。

Secure Eraseは、実行すると復元することが不可能になる (または少なくとも非常に困難になる) 方法でストレージメディア上のデータを消去します。セキュアイレース機能はソリッドステートドライブ (SSD) メディアに実装されているため、この機能をサポートするモデルでのみ使用できます。これらのSSDには、ハイエンドのミリタリグレードのSLCとインダストリアルグレードのMLCデバイスがあります。

従来のソフトウェアベースのセキュアイレースアルゴリズム (ハードディスクドライブ用に開発された) では、これらのドライブでオーバープロビジョニングが使用されるため、SSDメディアを初期化できないことに注意してください。つまり、メモリセルの磨耗に関連する問題を軽減するために、SSDにはドライブに記載されている容量よりも多くのフラッシュメモリが搭載されています。通常、フラッシュメモリの５～15%がこの目的のために予約されています。FLASHコントローラは、この追加のフラッシュメモリを使用して、摩耗の兆候が見られるセルを交換します。これらのメモリセルはユーザーアプリケーションからアクセスできないため、セキュアイレースSWアルゴリズムはこれらのブロックを消去できず、機密データがドライブ上の予備セルに残される可能性があります。したがって、Secure EraseアルゴリズムをSSDコントローラのファームウェアに実装する必要があります。

注：不良フラッシュセル / ブロックがある場合、フラッシュコントローラでもそのデータを上書きできない場合があります。コントローラは通常、ベストエフォート方式を採用しますが、不良セルが上書きできるという保証はありません。同様に、フラッシュコントローラに障害が発生した場合どのセルも消去できなくなります。

使用可能なアルゴリズムは、選択したドライブモデルによって異なります。

● **コンテンツの消去と割り当てテーブル**

「fast erase」という用語は、フラッシュコントローラの割り当てテーブルのみが消去され、メモリセルの内容は消去されないプロセスとして使用されることがあります。この場合、フラッシュメモリセルの実際の内容はそのまま残されているため、メモリをデバイスから取り外して直接アクセスした場合に読み取られる可能性があります。「secure erase」アルゴリズムは、各メモリセルを物理的に消去または他の既知の状態にクリアするという点で完全に異なります。また、「military erase」という用語も、より高度なアルゴリズムを指す場合によく使用されます。各メモリセルは、ユーザーデータが読み取り可能な状態で残らないようにするために、多数の消去および上書きサイクルを実施します。

● **セキュアイレースアルゴリズムのオプション**

フラッシュメモリはブロックベースで動作するように設計されており、ブロック内のすべてのメモリセルは一括消去されます。個々のセルは個別に書き込むことができますが、単一のセルを消去することはできません。この制限により、メモリデバイスの寿命にある程度の影響を与えます。

ただし、ブロック消去は非常に高速で完全ディスク消去にも役立ちます。フラッシュメモリブロック消去コマンド(SSDコントローラが内部的に発行) に基づいてSSD消去を実行することは、「zeroise」、「fast erase」、または「quick erase」と呼ばれます。

SSDが異なれば、利用可能な他のアル

ゴリズムのオプションも異なります。消去アルゴリズムで利用可能なオプションの多くは磁気メディア (HDD) 用に開発されたものであり、単純なフラッシュ消去と比較してデータのセキュリティが実際に大幅に向上するかどうかは不明であることに注意してください。いずれの場合も、SSDコントローラはSSDホストとの対話を行わずにコマンドを発行したり、フラッシュメモリアレイにデータを書き込んだりします。

● 消去の実行と消去時間

Galleon社からは、消去機能を実行するための次のような複数の方法が提供されています。

・ディスクリート入力
・APIコマンド
・ディスクリート入力とAPIコマンドの組み合わせ

Galleon社製品 (XSR、G1、オフロードサーバーまたはドッキングステーション) 内では、これらのコマンドはSSD自体に正しいコマンドを発行するために使用されます。

残念ながら、セキュアイレース機能を実行する方法について定義された規格はありません。したがって、実行とアルゴリズムはベンダーの実装に依存します。一部の製品では、SSDのフロントパネルコネクタで利用できるディスクリート信号、またはデバイスに存在するメンテナンスインターフェイス接続の1つを通じて安全な消去をトリガーする方法を提供しています。ホストOSが発行するカスタムSATAコマンドによる実行もサポートしているものもあります。

セキュアイレースの実行にかかる時間は、選択したSSDのメーカーとタイプおよび必要なアルゴリズムによって大きく異なります。表4は、いくつかの代表的なドライブのアルゴリズムとその消去時間を示しています。

※表に記載されている時間は、消去シーケンス (該当する場合) のハードウェアとソフトウェアの両方のトリガーに適用される推定値として示されています。実際に完了するまでの時間は、F/Wの実装、SSDベンダー、フラッシュタイプ、ソフトウェアのオーバーヘッドなどによって異なります。

● 消去の完了

Galleon社が提供するすべてのアルゴリズムとSSDベースのソリューションでは、消去コマンドがSSDに発行されると、SSDコントローラは消去プロセスが完了するまで他のすべてのコマンドを無視します。これは電源が遮断された場合でも当てはまります。SSDへの電力が回復すると、コントローラは消去プロセスを完了するまで続行します。これが発生すると、ドライブはコマンドやアクセスに応答しなくなりエラーになるか見えなくなります。

消去方法	SSD容量に依存する消去時間			
	128GB	256GB	512GB	1TB
D0hクリア	7s	14s	17s	34s
クイック/高速消去	7s	14s	17s	34s
US Air Force AFSSI-5020	8ms	16ms	25ms	49ms
DOD 5220.22-M	8ms	16ms	25ms	50ms
US Navy NAVSO P-2539-26	8ms	16ms	25ms	50ms
NSA 130-2	22ms	48ms	74ms	168ms
US Army AR380-19	22ms	48ms	74ms	168ms
NSA 9-12	8ms	16ms	25ms	49ms
IRIG 106-07	22ms	48ms	74ms	168ms

表4．セキュアイレース消去時間の比較

物理的消去/破壊オプション

一部のSSDは、データセキュリティのための物理的破壊手法を実装しています。

使用されるメカニズムは、フラッシュメモリセルに非常に高い電圧と大電流を印加することです。理論的には、これによりデバイスからデータを回復することは不可能になります。

Galleon社は現在、レコーダ/NAS/サーバー内でこのオプションを提供していません。これには以下の理由があります。

※物理破壊SSDのメーカーは信頼できる検証方法を明示できませんでした。物理的な破壊方法の検証は、(ほとんどの場合) SSDにアクセスできなくなったこと、またはフラッシュメモリデバイスにアクセスできなくなったことを確認することで行われてきました。これらの手法はいずれも、フラッシュストレージセルが破壊されたこと (または例外なくすべてのデバイスで同じ結果が発生すること) を実際に検証するものではありません。使用されている破壊方法を検証する明確な証拠がないため、Galleon社はこれらの装置を推奨していません。

まとめ

データセキュリティは非常に複雑なテーマです。システム設計の段階全体で考慮する必要があり、既存のシステムに追加するのは困難です。

組込みシステムの保存データを保護するために利用できるさまざまなメカニズムが多数あります。通常、最良のセキュリティはデータを保護するために複数のメカニズムを使用する多層アプローチで実現されます。Galleon社の製品はこれらのメカニズムを個別にまたは複数の保護層として利用できます。

多くの暗号化メカニズムにより、システムの設計と運用が複雑になります。ただし、データが安全であることの利点は、複雑さが増すことによる欠点よりも重要です。

保存データのセキュリティにより、運用のセキュリティ要件が軽減されます。たとえば、装備した武装警備員を常時配置する必要がなくなります。同様に、正しいデータセキュリティ方法を採用することで、他の方法ではほぼ不可能だった古いデータモジュールの廃棄も簡単になります。

Galleon社は、システムインテグレータにデータセキュリティメカニズムの選択についてアドバイスおよびサポートしてきた豊富な経験を持っています。

リファレンスドキュメント：
Galleon Embedded Computing社：
Data Security : Encryption & Secure Erase

TEST&MEASUREMENT

マルチチャンネル多機能計測システムの構築

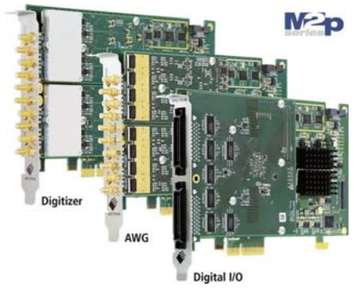
多チャンネルのアナログ信号を取得する場合、オシロスコープなどの測定器を複数台使用してシステムを構築することができますが、高速デジタイザ (A/Dボード) を使用することでより簡単にPC上で解析することが可能になり、システム全体をコンパクトにすることができます。ここではその手法と応用例をご紹介します。

はじめに

今日、エレクトロニクスのテストと計測はマルチチャンネル計測および多機能計測の方向に進み続けています。テスト対象の電子デバイスは、並列トポロジやアレイトポロジを使用することで複雑さが増し続けており、タイミングの一貫性を維持したままより多くの測定を高速で実行する必要があります。

PCベースの計測システムサプライヤーであるSpectrum Instrumentation社は、低コストでマルチチャネルテストシステムの構築を可能にするPCIeカード(M2pシリーズ)の多彩なラインナップを揃えています。

M2pシリーズは、3種類の異なる製品カテゴリで合計39種類の製品を提供しており、アナログ信号取得用のデジタイザ、アナログ信号生成用の任意波形発生器(AWG)、および高速デジタル信号の取得と生成の両方が可能なデジタルI/Oカードがあります。



ここでは、さまざまな用途に対応したマルチチャンネル/多機能テストシステムでM2pシリーズ製品をどのように使用できるかを紹介します。

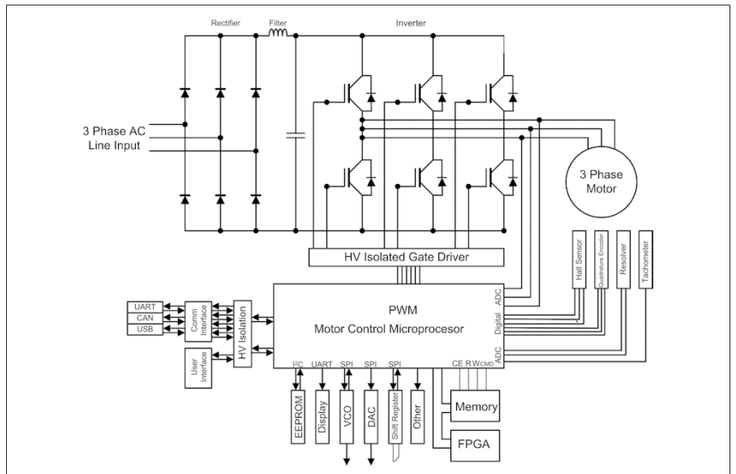


図14．一般的なモーター制御システムのブロック図

産業用モーター制御

電気モーターは、現代のエレクトロニクスがどのように変化したかを示す良い例です。 1990年代以降、モーター(特に産業用モーター) は電力線駆動から電子ベースのモーター駆動に移行してきました。現在使用されているモーターの90%を占める750ワット未満の小型モーターでも、電子モーター駆動が使用されています。一般的なモーター制御システムを見てみましょう(図14)。

モーターコントローラーはスイッチング電源のように動作します。主電源を整流およびフィルタリングして、主電源ACをDCバスに変換します。ポータブルデバイスのモーターはバッテリーを使用してDCバスに電力を供給します。このDCバスは、パルス幅変調(PWM) 信号を使用してモーターを駆動するスイッチングインバーターに電力を供給します。DCモーターの場合、インバーターはモーターの転流にも使用されます。次に、速度センサーと角度位置センサーがモーターの速度とトルクをフィードバックして、フィードバック制御ループを完成させます。制御用マイクロプロセッサは、アナログ信号とデジタル信号の両方を備えたミックスドシグナルデバイスです。シリアルインターフェイスは、マイクロプロセッサとコントローラディスプレイ、EEPROM、VCO、DACなどの補助デバイスとの間で通信します。

この環境は、M2pシリーズのモジュラー機器に最適です。デジタイザはアナログ信号を取得・表示・分析することができます。一方、デジタルI/Oモジュールはアドレスバスやデータバスで使用されるものなど、デジタル信号に対して同じことを行うこと

MISH Tech Journal 2024 SUMMER

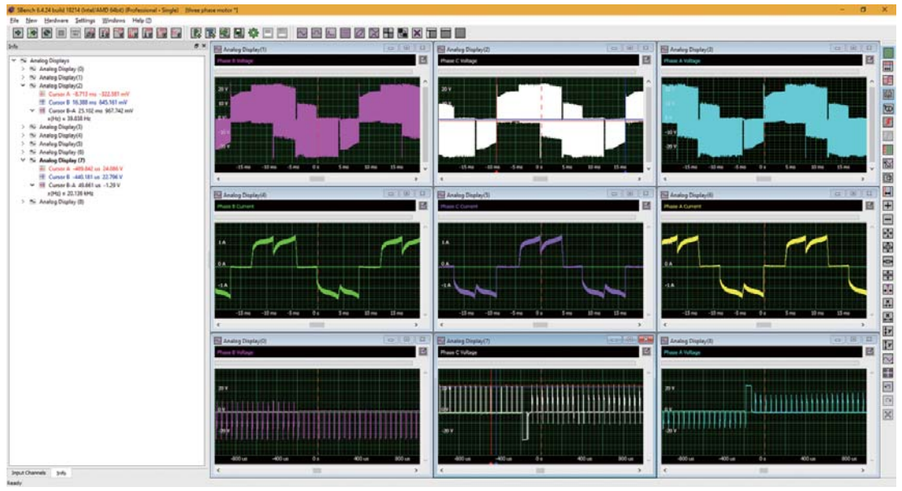


図１５．BLDC モーターからの三相電圧と電流。 電圧波形（上段）、電流波形（中段）、電圧波形の拡大（下段）

ができます。AWGは、取得した信号またはソフト的に作成された信号に基づいてセンサー信号をシミュレートできます。

実際の例として、携帯用ハンドツールで使用される三相ブラシレスDC(BLDC)モーターの電圧と電流の測定を考えてみます。相電圧と電流は、最大125MS/sでサンプリングする16bit, 8ch M2p.5968-x4デジタイザを使用して取得されました。デジタイザは、図15に示すように、Spectrum製SBench6ソフトウェアによって制御され、測定データの表示と分析にも使用されます。

サンプリングレート10MS/sでの40msの取得期間は、モーター回転の約1.6周期を捕捉します。Analog Display(2)（上部中央）のカーソルは、左側の情報パネルに表示されているように 25msの回転周期を測定します。これは、回転周波数40Hzまたは1分あたり2400回転に相当します。電圧波形は、台形制御とも呼ばれる6ステップ整流の特性を示しています。整流は、回転ごとに6つの「パルス状」波形セグメントとして電流波形にも観察されます。電圧波形は、PWM電圧波形のスイッチングされた性質を示しています。最下段の水平方向に拡大した図は個々のパルス波形を示しています。Analog Display(7)（中央下）のカーソルは、スイッチング周波数を20kHzとして測定します。インバーターセクションはフローティングでグランド（接地）基準ではなく、三相デルタ接続は6つの差動チャネルを使用します。つまり、システム内に2枚のデジタイザーカードを使用した12個のシングルエンドチャネルになります。

モーターコントローラーは、ホール効果センサーの出力を使用してモーター速度とシャフトの角度位置を決定します。このセンサーは、モーターハウジング内に120°間隔で配置された3つのホール効果トランスデューサーで構成されています。センサーには、各ホール効果トランスデューサーから1つずつ3つのデジタル出力があります。

図16に示すように、ホール効果センサーの三相出力はM2p.7515-x4 デジタルI/Oカードを使用して取得できます。M2p.7515-x4は、最大32個のデジタルチャネルを最大サンプルレート125MS/sで取得または出力できます。M2pシリーズには、最大16枚の異なるカード（デジタイザ、AWG、デジタルI/Oモジュール）を組み合わせ同期（共通のクロックおよびトリガ信号を共有）して、同じタイミングで使用できるM2p-Star-Hubというオプションもあります。

図１６．三相のホール効果センサー取得波形

3つのホール効果センサーのデジタル出力は、回転周期を6つのサブ周期に分割し、それぞれが60°の回転範囲に収まります。図の下部にある色付きのボックス表示は、モーターアーマチュアの1回転中に発生する6つのセンサー出力状態を示しています。ホール効果センサーにより、モーターコントローラーはモーターの速度と角度位置を決定できます。6つのセンサー状態を使用してモーター巻線を整流し回転を維持します。

32bit幅のデジタルI/Oモジュールは、図17に示すようにパラレルデジタルバスを調査することもできます。デジタル信号はビット単位またはバス単位で表示できます。ビューワーの注釈は、16進数、8進数、2進数、または符号付きまたは符号なし10進数形式で表示できます。

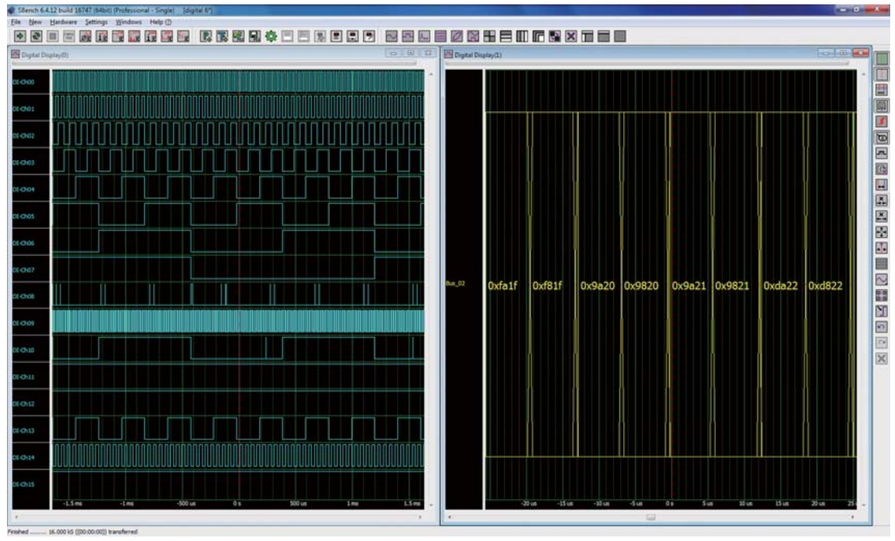


図１７．16bit パラレルバスのビット毎の表示（左）とバス表示（右）

ソースレスポンステスト

アンプ、フィルタ、受信機、デジタルインターフェイスなどの一部の電子デバイスは、テストのために外部から励起する必要があり、信号源と測定器が必要です。モジュール式デジタイザおよびモジュール式任意波形発生器(AWG)は、帯域幅、サンプルレート、およびメモリを構成できる複数のソースおよび測定チャンネルで利用できます。2つの製品を1つのシステムに組み合わせることで、広範なテスト要件を満たす非常にコスト効果が高く効率的な方法が提供されます。この例では、Spectrum製 M2p.5968-x4 16bitデジタイザと M2p.6568-x4 8ch 125MHz, 16bitの任意波形発生器で構成される刺激応答テストシステムを使用します。

位相マージンは重要な性能指数であり、閉ループ制御システムの安定性を示すのに役立ちます。これは、開発およびデバッグ中に電源で行われる最も一般的な設計検証測定の1つです。位相マージンの測定は、デジタイザと信号源の両方を必要とするソースレスポンス測定の例です。

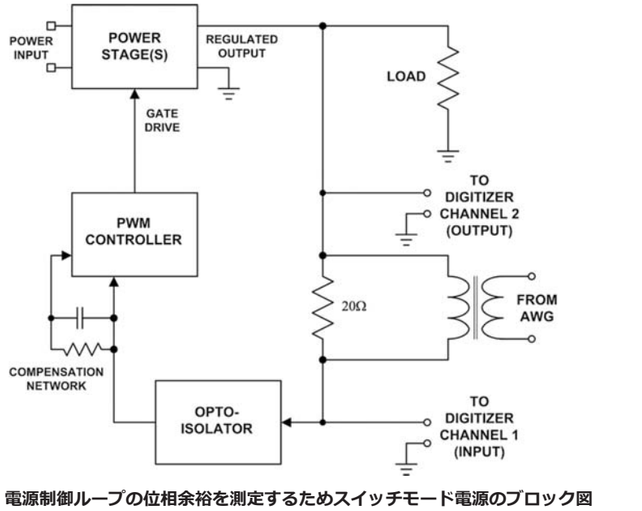


図１８．電源制御ループの位相余裕を測定するためスイッチモード電源のブロック図

位相マージンは、ループがユニティゲインを持つ周波数における開回路制御ループの入力と出力間の位相差です。360°位相シフトを伴うユニティゲインは不安定な振動状態です。この測定はフィードバック制御ループの開ループ特性を特徴づけますが、閉ループ構成で測定されることがほとんどです。図18のブロック図は、閉ループ構成を維持しながら位相マージンやゲインマージンなどの開ループ特性を測定するための一般的な接続図を示しています。

この例では20オームの小さな拡散抵抗が、回路の通常動作を妨げない点で制御ループに挿入されます。AWGからの小さな正弦波信号が変圧器を介して注入され、周波数が変化するとデジタイザで電圧を測定することによって、ループ周囲のゲインと位相差を決定できます。ループゲインは、チャンネル2で測定されたループ出力をチャンネル1で測定されたループ入力で割った比です。位相差もループの入力と出力の間で直接測定されます。正弦波の周波数は、入力波形と出力波形が等しくなるまで変化します（ユニティゲイン、0dB）。この周波数での位相差がループの位相マージンです。この測定で遭遇する最大の困難は、電源のスイッチングノイズの存在下で発生する小さな電圧を正確に測定することであることに注意してください。ノイズの影響は、平均化、正弦波励起との同期、または信号のフィルタリングによって

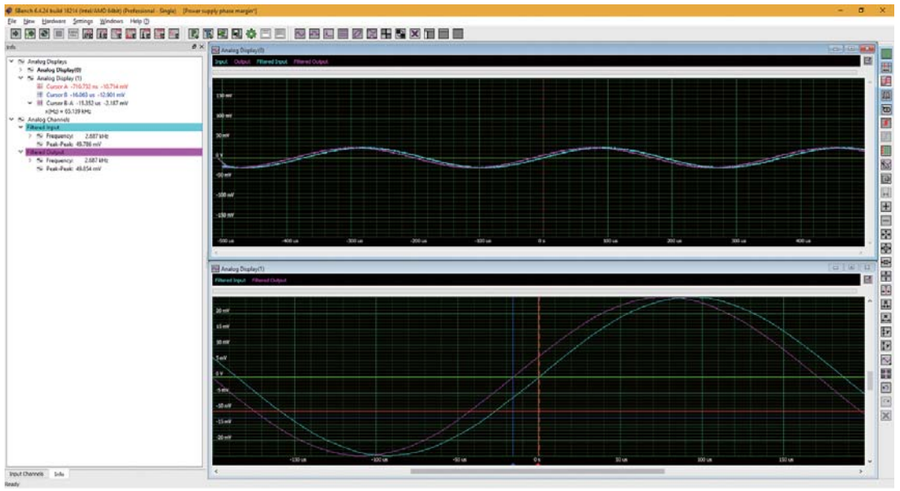


図１９．位相マージンを測定した結果。ユニティゲインが 2.687kHz の周波数で発生しました。波形間の時間差は -15.352us (-14.85°)

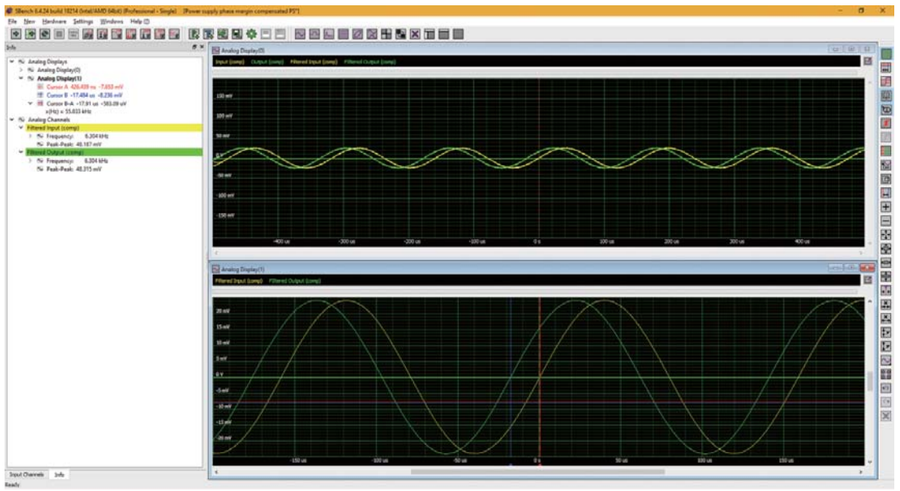


図２０．補償ネットワーク値の変更による位相マージンの改善結果。遅延は -17.91us、ユニティゲイン周波数は 6.304kHz にシフトし、位相余裕はより安定した -40.6°になりました。

大幅に軽減できます。この例(図19)では、Spectrum製 SBench6ソフトウェアは、測定前に両方の信号に20kHzローパスフィルターを適用します。

位相差は、遅延とユニティゲイン周波数の360°の積として計算されます。

入力波形と出力波形の形状は、ループが正弦波励起によってオーバードライブされていないことを示す良い指標であることにも注意してください。オーバードライブは非正弦波形として表示されます。

測定された位相マージン -14.85°は非常に低いです。位相マージンは、PWMコントローラーの補償ネットワークを調整することで増加しました。結果を図20に示します。位相マージンは -40.6°に増加しました。これによりシステムの安定性が大幅に向上します。

シミュレーション

開発状況によっては、現在手元にないシステム要素が必要になる場合があります。不足している部品が入手可能になるまで作業を停止することなく、AWGを使用して不足している要素をシミュレートすることができます。AWGは、ソフト的にまたはデジタイザやオシロスコープから波形をインポートすることによって、非常に多様な波形を生成できます。例として、図21に示す心電図(ECG)信号があります。

波形を取得したら、その振幅とオフセットを変更することで修正できます。他の波形を算術的に波形と組み合わせることができます。また、波形をフィルタリングすることもできます。これらの変更を行った後、結果の出力をAWGにインポートできます。

AWGは、出力される波形にリアルタイムの変化を生成することもできます。テスト手順に必要なすべての波形をすぐにロードし、AWGのシーケンスモードを使用して

図２１．デジタイザによってキャプチャされた30秒の長さのECG波形。波形はSBench6 関数トレースに転送され、そこでAWGにインポートできます。

必要に応じて選択できます。これにより、複数のジェネレータを切り替える必要がなくなり、新しい波形をロードするのにかかる時間が短縮されテスト速度が大幅に向上します。

波形セグメントのリアルタイム制御により、さまざまなテストのニーズに適応して応答することが容易になります。測定されたテスト結果によってシーケンスの順序が変更される可能性があり、これはテストプロセスを停止することなく発生する可能性があります。これは、測定されたパフォーマンスに基づいてテスト条件を変更できる適応テストを可能にするため、最も強力な利点です。

RFID、イーサネット、または自動車のアプリケーションで発生する可能性のある、マンチェスターエンコードされたシリアルデータストリームの出力を検討します。メッセージの内容は、図22に示すように、AWGシーケンスモードを使用してオンザフライで変更できます。

この例には、異なるデータ内容を持つ4つのパケットがあります。波形の数は、AWGで使用可能な波形メモリによってのみ制限されます。1つのパケットが出力されると、出力される次のパケットがコンピュータ制御によって選択されます。選択されたパケットはキューに入れられ、現在のパケットが終了した後シームレスに出力されます。したがって、この例では、テスト中に4つのパケットのいずれかをオンデマンドで出力できます。

まとめ

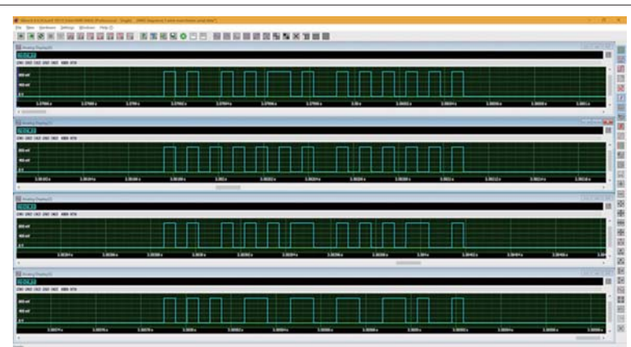


図２２．AWG 波形メモリに保存されているこれら 4 つの異なるマンチェスター符号化シリアルデータ

複数のM2pシリーズ、デジタイザ、AWG、またはデジタルI/Oカードをテストシステムで使用し、インタラクティブに動作してさまざまな信号の取得と供給を行うことができます。Star-Hubモジュールを使用して3種類のM2pシリーズカードすべてを相互にリンクし、位相安定した同期を実現できます。M2pカードはハーフサイズのPCI Express x4モジュールであるためPCシステムに直接実装することができます。PCIeバスにより、CPUおよびGPUとの間で最大700MB/sのデータ転送が可能になります。モジュラー設計、高速データ転送、高度な処理テクノロジーへのアクセスを組み合わせることで、非常に強力なマルチチャネル、多機能テストおよび測定システムを簡単に作成できます。M2pシリーズ製品は、Spectrum Instrumentation社の SBench 6ソフトウェアでサポートされており、さまざまなサードパーティソフトウェアパッケージやプログラミング言語を使用してプログラムすることもできます。

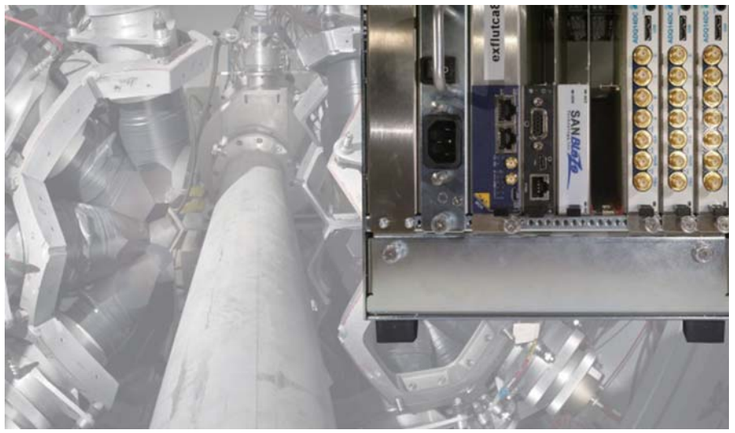
リファレンスドキュメント：
SPECTRUM社　Application Note：
Easy creation of customized multi-channel, multi-functional test and measurement systems

SPECTRUM INSTRUMENTATION

TECHNOLOGY

複数のデジタイザを同期するための手法

多チャンネルのアナログ信号を高速サンプリングで同時に取得する為には、クロック、トリガー、ケーブル接続など様々な要素について検討が必要です。ここではTeledyne SP Devices製のADQ14デジタイザを使用した同期手法とその応用例をご説明します。



はじめに

Teledyne SP Devices社製14bitデジタイザ「ADQ14」は、2GSPSで2チャンネルまたは1GSPSで4チャンネルとして利用できます。ここでは、システムを非常に多くのチャンネルに拡張する方法を説明します。同期の方法には、さまざまな状況に対応する非常に多くの解決策があります。ここではいくつかの事例を紹介しますので、実際のシステムに最適なものを選択してください。

この記事は、複数のADQ14を相互に同期することに重点を置いていることに注意してください。これは、1つのADQ14を外部機器に同期することとは異なります。

同期における重要な要素

トリガーとクロックはシステムのタイミングを構築する外部信号です。クロック信号はサンプリングの速度を設定し、トリガー信号はイベントがいつ始まるかを伝えます。複数のデジタイザの同期は次の3つの重要な要素に依存します。

1. クロック周波数はすべてのADQ14ユニットで調整され、同位相である必要があります。これには共通外部クロックリファレンスが必要です。
2. 各ADQ14にはデータの記録開始点を決定する信号が必要です。これはトリガー信号で行われ、すべてのユニットで調整する必要があります。
3. タイムスタンプは各ADQ14の取得時間をカウントします。このカウンターはすべてのユニットにおいて同相で動作する必要があります。

● **クロックリファレンス信号**

フロントパネルのクロックリファレンス信号入力により、10MHzの共通の外部クロックリファレンスが有効になります。

PXIeおよびMTCAユニットは、バックプレーン経由でのクロックリファレンスの配布もサポートしています。この共通のクロックリファレンスにより、同期の長期的な安定性が保証されます。図23(a)は、クロックが位相ロックされていない場合の2枚のデジタイザ間のドリフトを示しています。 図23(b)は、共通のクロックリファレンスを使用した位相ロック状態を示しています。

クロックの同期が重要となる状況は3つあります。

1. 各チャネルでのデータ駆動型収集。タイムスタンプを使用して個々のパルスの絶対時間を測定しチャネル間の比較を行います。(これはファームウェアオプション-FWPDを使用する場合の一般的な使用例です)
2. 非常に長い収集記録。(たとえばクロック周波数の1ppmの偏差は、長さ106サンプルのデータの最後にある1サンプルの偏差を意味します)。
3. 複数のボードを使用したPCへの連続ストリーミング。位相ロックされていない場合データレートが異なります。

尚、クロックリファレンスが重要ではない状況もあります。

1. 複数のボードが同じソースからの外部トリガーでトリガーされ取得時間が短い場合。
2. 取得データの絶対的なタイミングは重要でない場合。

● **トリガー**

トリガーは測定の開始点を表します。トリガーは、システム内のリアルタイム参照イベントでもあります。同期の観点からは2種類のトリガーがあります。

1. 同期トリガー：トリガー信号はクロックリファレンスに位相ロックされます。システムは完全に同期し完全に反復的になります。トリガーをクロックに位相ロックすると、トリガーのプロパティがデジタルシリアルリンクと同様に設定されます。重要なパラメータはセットアップ時間とホールド時間、つまりクロックエッジに対する到達時間です。
2. 非同期トリガー：トリガー信号はクロックリファレンスに位相ロックされません。非同期トリガーが利点となる状況があります。これは、トリガーとクロック間の相関が統計的特性を乱す可能性がある反復測定用です。

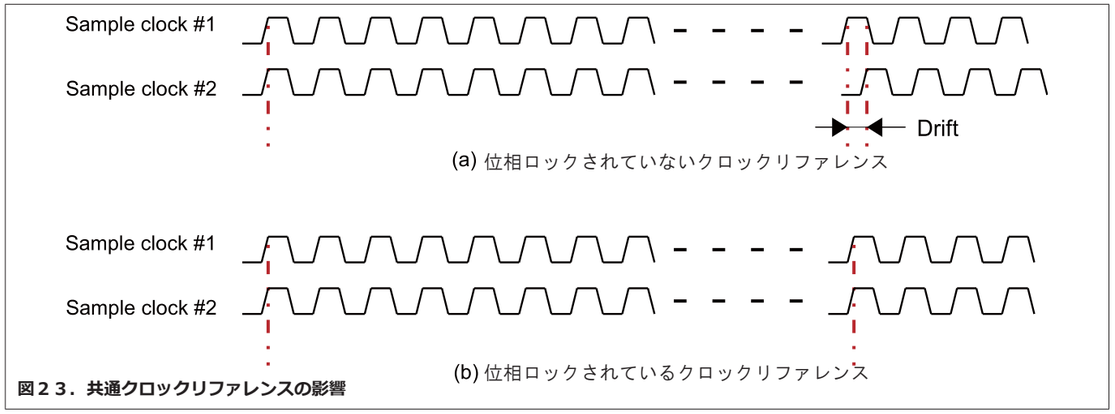


図２３．共通クロックリファレンスの影響

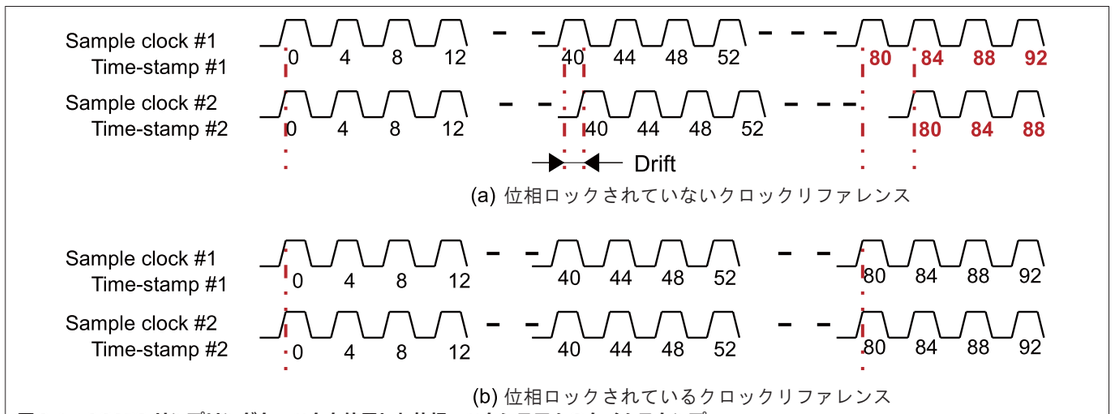


図２４．2GSPS サンプリングクロックを使用した位相ロックシステムのタイムスタンプ
(タイムスタンプのタイムベースは 125ps で、1 サンプル周期は 1/2GHz = 500ps であることに注意してください。タイムスタンプはサンプル周期ごとに 4 カウントします。)

● **タイムスタンプ**

タイムスタンプは、トリガーとクロックからの情報を伝えるリアルタイム測定です。タイムスタンプカウンタは、トリガイベント前のサンプル期間の数をカウントします。

タイムスタンプは、実際のクロックリファレンスに関連したペースで実行されます。外部クロックリファレンスが使用されている場合、タイムスタンプもそのクロックソースに関連付けられます。このように、これはリアルタイムクロックと考えることができます。

ADQ14がフリーランニングの場合、タイムスタンプのリアルタイム値は内部クロックの精度になります。

複数のデジタイザが共通のクロックリファレンスで位相ロックされている場合、タイムスタンプカウンタも同位相になります(図24)。

タイムスタンプは 64ビット整数で、LSBは理想的には125psを表します。サブサンプル精度には、外部トリガー入力に関する追加情報が含まれています。他のすべてのトリガーモードはサンプルごとにのみ解決されます。タイムスタンプの使用方法の詳細については、ADQ14マニュアルを参照してください。

クロックリファレンス

クロックの分配は同期の直接的な要素です。これは周波数と位相調整の2つのパートで構成されます。

● **クロック周波数**

共通のソースからのクロック信号を分岐し、すべてのボードにルーティング(配布)します。これにより、周波数つまりタイムベースがシステム内のすべてのデジタイザで共通であることが保証されます。

● **クロック位相**

サンプリングの瞬間(タイミング)は、アナログ入力信号に対するクロック信号の位相によって決まります。

同期の観点から見ると、クロック信号の時間遅延はアナログ信号の遅延と同等です。したがって、アナログ入力のケーブル長をクロック信号と一致させることも同様に重要です。システム全体の校正手順を行わなければ絶対精度は保証できません。ただし、ほとんどの状況では絶対的な精度は必要ありません。

潜在的な固定遅延に加えて、内部クロック生成にジッターが発生します。1つのデジタイザには約300fs RMSジッターがあります。これは、ADQ14デジタイザの任意のペア間のタイミングジッターが 300fs x SQRT(2) = 424fs であることを意味します(ガウス分布を仮定)。

● **クロック分配(フロントパネル)**

クロック分配は50オームシステムです。ボードが2枚の場合のみ、1つのデジタイザからのクロックリファレンス出力を使用し、それを別のデジタイザのクロックリファレンス入力に接続できます。これで、2つのデジタイザは同相になります。さらに多くのデジタイザを使用する場合は、クロック分配にファンアウトバッファが必要になります。

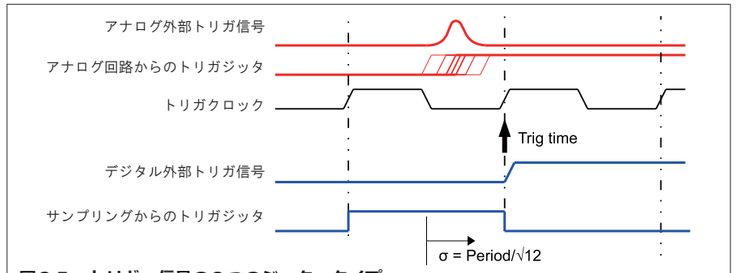


図25．トリガー信号の2つのジッタータイプ

● **クロック分配(バックプレーン)**

PXIeおよびMTCAフォームファクタは、バックプレーン経由のクロックリファレンスの配布をサポートしています。

トリガーの重要な要素

● **トリガーのジッター**

トリガージッターは2つの異なるタイプで発生します(図25)。

波形(赤):トリガー入力にはガウス分布ジッターがあり、入力トリガー信号エッジのタイミングに影響を与えます。これはトリガー入力段のアナログコンポーネントのノイズが原因で発生します。このジッターのRMS値は10psです。

波形(青):トリガーをサンプリングするプロセスです。受信する物理的なトリガー信号とトリガーのデジタル表現の差は、長方形の分布を持つ確率変数です。このようなプロセスのRMS値はPERIOD/SQRT(12)です。外部トリガーは8GSPSトリガークロックでサンプリングされ、36ps RMSのジッターが発生します。

● **トリガーのセットアップ及びホールド時間**

トリガーがクロックリファレンスに位相ロックされている場合、そのタイミングはセットアップ時間とホールド時間を持つデジタル信号に匹敵します。このセクションでは、同期トリガーのプロパティを分析します。同期トリガーを使用する場合、測定セットアップ全体が位相ロックされていると想定されます。

したがって、最も低い時間分解能はサンプルレートです。外部トリガーの追加のサブサンプル精度には追加情報は含まれません。ただし、サブサンプル精度を使用してトリガー信号の位相を決定し、測定セットアップの特性を分析することができます。

ADQ14の最大サンプリングクロックは2GHzです。これは、タイミングウィンドウが500psであることを意味します。前述のRMSジッターが10psの場合、セットアップ時間とホールド時間は6σつまり60psに設定できます。よってウィンドウは500-60-60=380psです。このタイミング精度は、正確なシステム設計によって実現できます。(380psは約76mm同軸ケーブルでの信号伝播時間であることに注意してください。)

同期システムを構築する場合、絶対的な安定性に対する要件が厳しくなります。設計を簡素化するために、タイムスタンプを使用してトリガー時間に関する不確実性を解決できます。

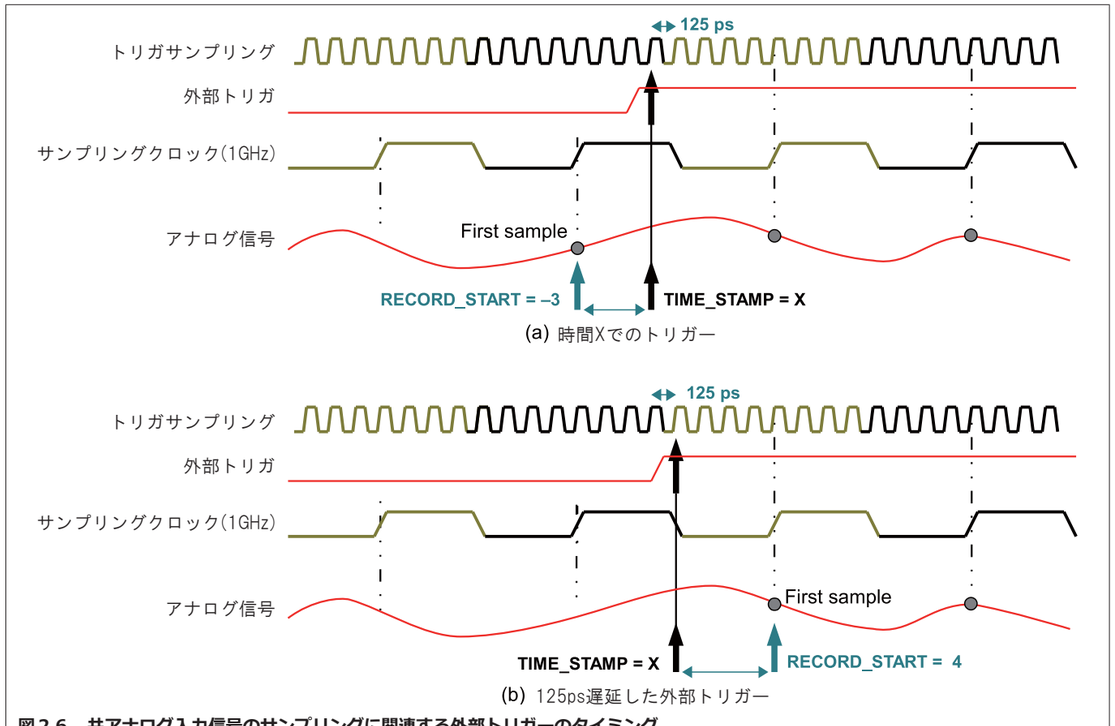


図26．共アナログ入力信号のサンプリングに関連する外部トリガーのタイミング

● **トリガーの位相ロック**

トリガー信号は、デジタイザのクロックリファレンスに位相ロックされます。これを実行するにはいくつかの重要な要件があります。

①トリガーソースはデジタイザの10MHzクロックリファレンスにアクセスする必要があります。ADQ14が内部クロックリファレンスを出力してトリガーソースに送信するか、トリガーソースにデジタイザに送信されるクロックリファレンスが含まれている必要があります。

②トリガーソースはデジタイザから出力することができます。内部トリガーをオンにし、トリガーコネクタを出力に設定します。これでトリガーはデジタイザに位相ロックされます。

● **トリガーケーブルの長さ**

トリガー信号のケーブル長は重要です。同軸ケーブルの一般的な伝播特性は光速の66%です。 これは、8GHz(125ps)のトリガー分解能が25mmのケーブル長に相当することを意味します。

● **タイムスタンプによる外部トリガーの解決**

トリガーの位相要件を緩和することで、セットアップが大幅に簡素化される場合があります。トリガー信号とクロック間の位相調整の絶対精度の代わりに、タイムスタンプを使用して個々のチャンネルのタイミングを解決できます。図26は、アナログ入力信号のサンプリングに関連する外部トリガーのタイミングを示しています。この例では、外部トリガーはトリガークロックの1周期(125ps)異なり、最初のサンプルはサンプリングクロックの1周期(1ns)異なります。TIME_STAMPおよびRECORD_STARTパラメータは、レコードがいつ開始されたか、および複数のデジタイザからのレコードをどのように配置するかを示します。

● **非同期トリガー**

トリガー信号がリファレンスクロックに位相ロックされていない場合、これは非同期トリガーと呼ばれます。このトリガーは、サンプリングクロックとの関係が明確に決められておらず、図25のような長方形の分布に従って時間内のさまざまな位置に現れます。トリガージッターは、トリガーがサンプリングされる分解能つまり8GSPSによって決まり、トリガージッターは36ps RMSとなります。

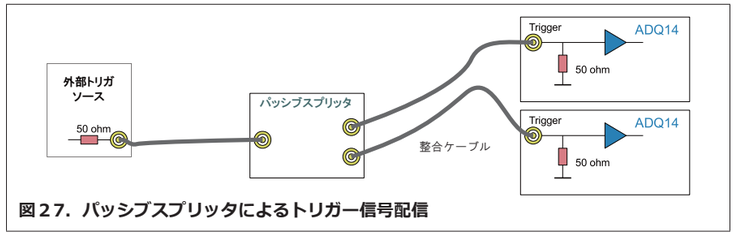


図27．パッシブスプリッタによるトリガー信号配信

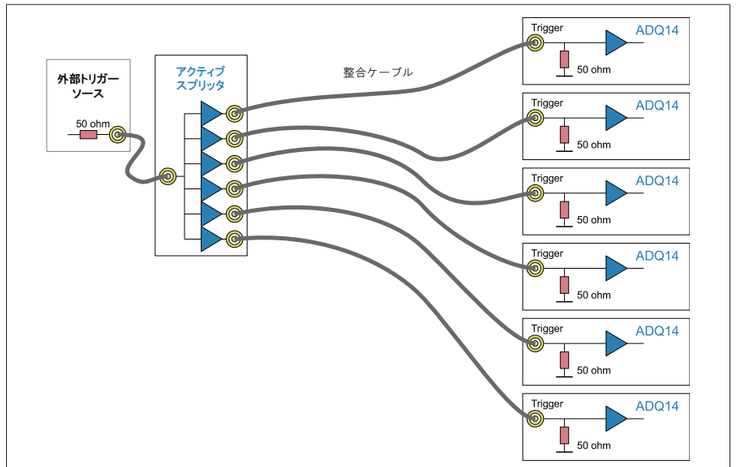


図28．アクティブスプリッタ（ADQTDU）によるトリガー信号配信

外部トリガーの分配

● **開始トリガーの分配**

トリガーは、さまざまな方法でスター接続により分配することができます。ここでは、いくつかの例を紹介します。また、システム内の反射を抑制するには、良好なインピーダンス整合が不可欠です。ADQ14は50オームのインピーダンス用に設計されており、50オームのシステムを構築するための標準コンポーネントは通常トリガーの分配に十分適しています。

● **パッシブスプリッタ**

パッシブスプリッタは、複数枚のデジタイザを使用する場合最もコスト効率の良いソリューションです(図27)。トリガー信号にはDC成分が含まれるため、パッシブスプリッタはDC結合する必要があります。これは、スプリッタが抵抗性であり、損失が各ステージで6dBとなることを意味します。6dBは振幅の半分が失われます。2枚のデジタイザをトリガーするのは簡単ですが、4枚のデジタイザをトリガーするには約3～4Vのソースドライブが必要です。

● **アクティブスプリッタ**

アクティブスプリッタには、各出力信号

MISH Tech Journal 2024 SUMMER

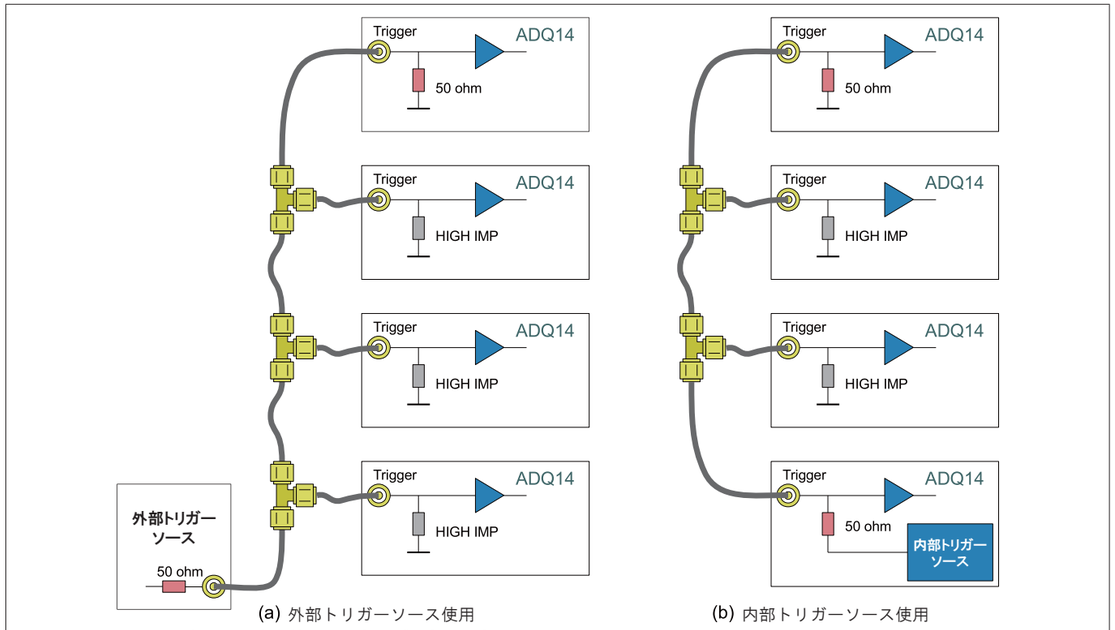


図29. ハイインピーダンス設定を使用したトリガー信号配信

にアンプが含まれています(図28)。よって、このソリューションでトリガーできるデジタイザの数に基本的に制限はありません。

ADQTDUは、トリガーの分配に使用できるトリガファンアウトバッファです。ADQTDUには6つの出力があるため、最大24チャネルを駆動できます。また、サードパーティのパワースプリッタを使用することも可能です。

- **バス接続**

トリガー入力を高インピーダンスに設定すると、バス接続が可能になります(図29)。これにより、1枚のボードで複数枚のカードをトリガーできます。但し、これは正しい50オームシステムではないため、反射が発生することに注意してください。ケーブルを短くすると反射を抑えることができます。最後のデジタイザでエンドポイントを50オームに終端することが重要です。この方法は、シャーシ内の隣接するカード間で使用できます。

図29(a)では、トリガーソースは外部機器です。

図29(b)では、デジタイザの1つがトリガーソースとして使用されています。これを内部トリガージェネレータと組み合わせて、自己完結型システムを構築できます。

- **PXIeバックプレーントリガー**

バックプレーン経由でトリガーを使用するには、シャーシにPXIe準拠のバックプレーンが必要であり、シャーシのトリガタイミングスロットにトリガタイミングモジュールも必要です。

マルチボード用のソフトウェア

APIはスレッドセーフではないことに注意することが重要です。いずれにしても、マルチスレッドアプリケーションを実装することをお勧めします。重要なのは、一度に1つのスレッドだけがデジタイザにアクセスするようにすることです。マルチスレッドシステムの起動手順は、ListDevicesを使用して利用可能なボードを検索することです。FindDevicesはメインスレッドからボードとの通信を開始するため、使用しないでください。ListDevicesは、使用可能な各ADQ14のIDを返します。IDごとに1つのスレッドを開始します。

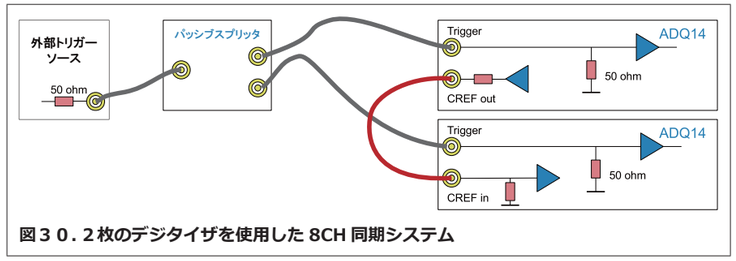


図30. 2枚のデジタイザを使用した8CH同期システム

8CHシステムのセットアップ

図30にADQ14を2枚使用した8CH同期システムの構成例を示します。

[システム構成]

- 8チャンネル
- 1GSPS
- PCIeフォームファクタ
- 外部非同期トリガー

[ハードウェアのセットアップ]

- ADQ14-4Cはボードごとに1GSPSで4チャンネルを備えています。ADQ14-4C-PCIeを2枚使用し8チャンネルを構成します。
- PCに2枚のデジタイザをセットアップします。
- パッシブスプリッタを使用してトリガーを2枚のカードに分配します。
- いずれかのカードのクロックリファレンス出力を使用し、もう一方のカードのクロックリファレンス入力に接続します。

[ソフトウェアのセットアップ]

- タイムスタンプリセットを使用してカード間のタイミングを同期します。
- トリガーブロッカーを使用してシステムを待機状態にし、すべてのカードを同時にスタートします。

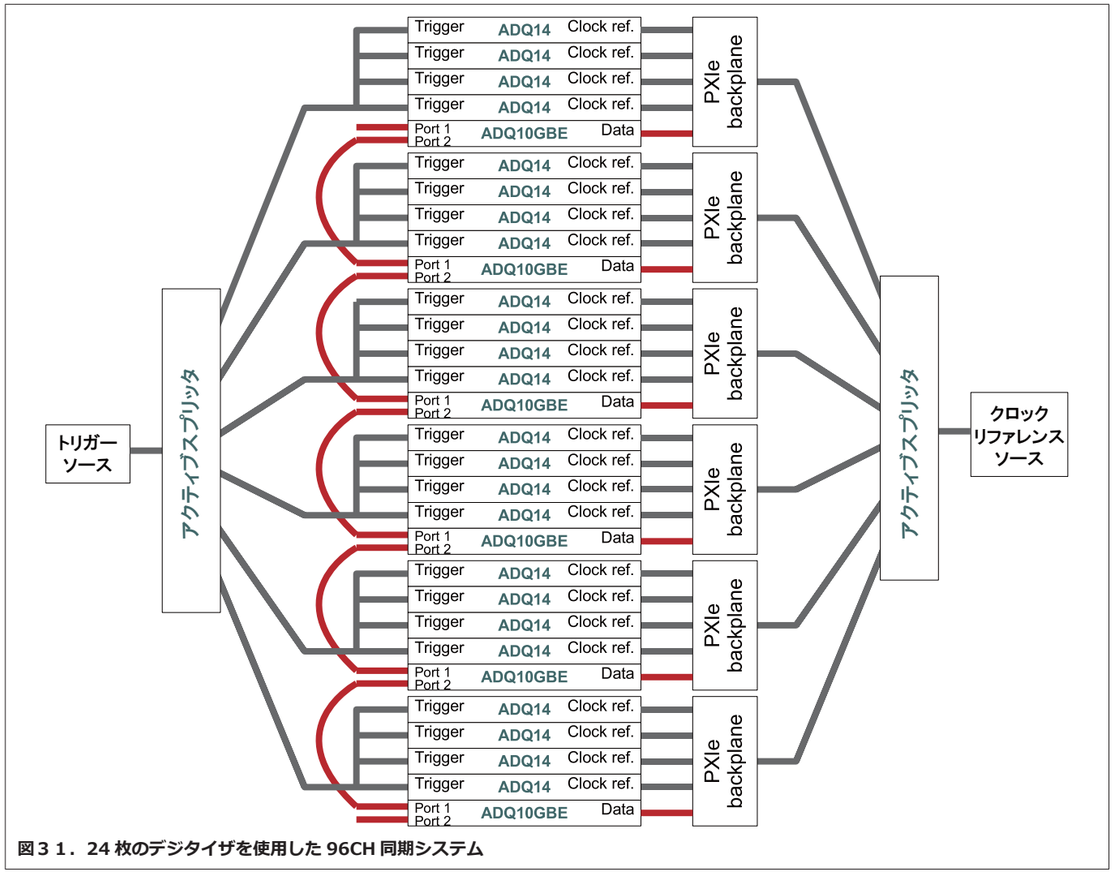


図31. 24枚のデジタイザを使用した96CH同期システム

96CHシステムのセットアップ

図31にADQ14を24枚使用した96CH同期システムの構成例を示します。

[システム構成]

- 96チャンネル
- 1GSPS
- PXIeフォームファクタ

[ハードウェアのセットアップ]

- ADQ14-4Cはボードごとに1GSPSで4チャンネルを備えています。ADQ14-4C-PXIeを24枚使用します。
- シャーシに4枚のデジタイザを配置します(合計6台のシャーシを使用)。
- 4枚のデジタイザをグループにしてバス経由でトリガーを接続します。つまり6グループということになります。
- アクティブスプリッタ (ADQTDU)を使用して、6つのグループすべてにトリガーを分配します。
- クロックリファレンスはバックプレーン配信を使用します。
- アクティブスプリッタ (ADQTDU)を使用して、クロックリファレンスをすべてのシャーシに分配します。
- ADQ10GBE (Option)を使用して、シャーシ間でデータを送信するためにイーサネット接続します。
  ADQ10GBEは図のように接続し、隣接するシャーシにデータを送信したりスイッチを介して他のシャーシにデータを送信することができます。

[ソフトウェアのセットアップ]

- タイムスタンプリセットを使用してカード間のタイミングを同期します。
- トリガーブロッカーを使用してシステムを準備状態にし、すべてのカードを同時にスタートします。

まとめ

ここで説明したように高速サンプリングで多チャンネルのアナログ信号を同期して取得するためにはさまざまな検討事項があります。この記事を参考にすることで、マルチチャンネルシステムの導入の助けになれば幸いです。

リファレンスドキュメント：
Teledyne SP Devices社： Application Note：Synchronizing several ADQ14

TELEDYNE SP DEVICES
Everywhereyoulook™

新製品ピックアップ

ここでは今年の新製品をピックアップして紹介します。
- SPECTRUM社製　M5i.3367-x16 10GSPS高速A/Dボード
- Extreme Engineering社製　XPedite7871 CPUボード
- CP North America社製　MTP-24 マルチディスプレイポータブルPC
- CP North America社製　TFX1-173耐環境3画面液晶ディスプレイ
- CP North America社製　CPX1-241 24インチパネルマウントディスプレイ

SPECTRUM社製　M5i.3367-x16 10GSPS高速A/Dボード

M5i.3367-x16 は、10GHz 12bit 1chの ADコンバータを搭載した PCI Expressタイプの高速A/Dボードです。 4.7GHzの広帯域幅をサポートしており、5GHz 12bit 2chとして利用することもできます。標準で4GBのオンボードメモリを搭載しており、広帯域信号を高精度に記録する事が可能です。ホストインタフェースは、PCI Express x16 Gen3インタフェースを備えています。最適化されたドライバにより、最大12.8 GB/sでのデータストリーミング速度が可能です。超音波、レーダ、LiDAR、無線通信、レーザ、加速器、非破壊検査などのアプリケーションに最適です。

M5i.3367-x16 仕様	
サンプリングレート	10GSPS/5GSPS
チャンネル数	1ch/2ch
分解能	12bit
帯域幅	4.7GHz
オンボードメモリ	2G サンプル（標準）, 8G サンプル（オプション）
ホストインタフェース	PCI Express Gen.3 x16
温度範囲	0 ～ +50℃
OS	Windows, Linux

Extreme Engineering社製 Xpedite7871　CPUボード

XPedite7871は、Intel Xeon D-2700（Ice Lake-D）ファミリのCPUを搭載し、SOSAに準拠した3U OpenVPXのCPUボードです。大量のデータ及び情報の保護を必要とする演算アプリケーションに最適です。Microsemi PolarFire FPGAと統合して、データの改ざんや監視から保護するカスタム機能を提供し、厳格なセキュリティ機能が必要な用途に理想的なソリューションを提供します。VxWorksとLinuxをサポートしています。

XPedite7871 仕様	
プロセッサ	Xeon D-2700 (Ice Lake-D)
メモリ	最大 64GB DDR4 ECC SDRAM 最大 32GB SLC NAND flash
セキュリティ	Microsemi PolarFire FPGA with 256MB SPI flash SecureCOTS テクノロジ Trusted Platform Module (TPM)
ネットワーク	40GBASE-KR4, 10GBASE-KR, 10/100/1000BASE-T
I/O ポート	USB2.0, PCIe, RS-232/422/485
フォームファクタ	3U VPX
温度範囲	-40 ～ +85℃ (Conduction Cool)
OS	VxWorks, Linux

CP North America社製　MTP-24 マルチディスプレイポータブルPC

MTP-24は、24インチのディスプレイを3画面搭載した耐環境ポータブルPCです。24インチのLCDディスプレイを3画面搭載していますので、広大な作業スペースにより作業を効率化します。ノートブックPCでは性能が充分でないが、デスクトップを持ち込むことができない場所での利用に効力を発揮します。MTP-24は 高い堅牢性基準に基づいて構築されており、要求の厳しい環境でも MILスペックレベル、またはそれを超える性能を発揮します。OSはWindows又はLinuxをサポート。

MTP-24 仕様	
プロセッサ	Xeon 又は Core シリーズサポート
ディスプレイ	21 インチ x3 画面
メモリ	構成オプション
ストレージ	構成オプション
動作温度	MIL-STD-810, Method 501.6
湿度	MIL-STD-810, Method 507.6
砂埃	MIL-STD-810, Method 510.6
OS	VxWorks, Linux

CP North America社製　TFX1-173 耐環境３画面液晶ディスプレイ

TFX1-173は、堅牢なミリタリグレードの 2U ラックマウントタイプの 3画面液晶ディスプレイです。液晶パネルの解像度は1280x1024で、17.3インチ TFT LCD パネルを 3画面備えています。優れた強度を備えたディスプレイにより広大な作業スペースを提供します。TFX1-173は、明るい場所でもさまざまな温度環境で動作できるため、極端な屋外環境に最適です。お客様固有のアプリケーション要件に合わせてカスタマイズもできます。空挺オペレーション、陸上オペレーション、海上オペレーション、テレメトリ、通信、画像処理、監視など過酷な環境で利用できます。

TFX1-173 仕様	
画面サイズ	17.3 インチ x3 画面
入力	VGA (D-sub 15pin), DVI-D, HDMI, コンポジット (*Option)
解像度	1920 × 1200
コントラスト	600:01:00
ブライトネス	400 cd/m2 (1000 cd/m2)
動作温度	0 ～ +70℃
高度	10,000 ft (3048m), MIL-STD-810, Method 507.6
サイズ	482.6 x 88.9 x 613.2 mm

CP North America社製　CPX1-241 24インチパネルマウントディスプレイ

CPX1-241は、24インチのミリタリグレードのパネルマウント液晶ディスプレイです。さまざまなラグド軍事用途、特に広い画面スペースを必要とする用途に最適です。ディスプレイには赤外線タッチ スクリーンが搭載されており、マルチタッチジェスチャーテクノロジー (Windows 7/10) をサポートしています。標準で接着された疎油性反射防止ガラスオーバーレイが装備されており、オプションのマイクロメッシュEMIフィルターも利用できます。空挺オペレーション、陸上オペレーション、海上オペレーション、テレメトリ、診断・シミュレーション、C4ISR、通信、画像処理などさまざまな用途にご利用いただけます。

CPX1-241 仕様	
画面サイズ	24 インチ
入力	VGA, DVI-D, HDMI
解像度	1920 × 1200
コントラスト	1000:01:00
バックライト	LED
動作温度	0 ～ +50℃
高度	MIL-STD-810, Method 507.6
サイズ	584.2 x 392.9 x 81.3 mm

地球温暖化を考える９

「2050年カーボンニュートラル」
カーボンニュートラルとは、温室効果ガスの排出量を差し引きゼロにした状態を言います。
世界の二酸化炭素排出量は約314億トンと言われています。その内の32%が中国なのですね。中国に次いでアメリカ、インドとなるわけですが、この時点で50%を超えています。つまり、この３か国に頑張っていただかないと2050年のカーボンニュートラル実現は難しくなりますよね。ただ、日本もロシアに次いで第5位となっていますので、国土面積を考えるとどう見ても排出量が多いと思われてもしかたないでしょう。
さて、カーボンニュートラルを実現するためにどうすれば良いかですが、CO2の排出量を減らすと同時に吸収量を増やす必要があります。この排出と吸収で差し引きゼロになれば良いわけです。また、現在は大気中のCO2を除去する取り組みも行われているようです。これだけ高度な文明を築いた人間なのだから、CO2を排出しない仕組みやCO2を除去することもできないことは無いはず！できる対策は地道に実行していきましょう。

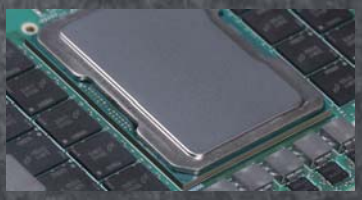
展示会のご案内
現在のところ今年の出展予定はありません。

受託開発
弊社ではソフトウェア・ハードウェア及びFPGAの受託開発も承っております。お困りの事がございましたらお気軽にご相談ください。
✉ sales@mish.co.jp

おわりに
テックジャーナルでは、これからも出来る限りお客様に有効となる情報を提供していきたいと思います。
今後ともどうぞよろしくお願いいたします。

『ミッシュ・テックジャーナル』次回発行をお楽しみに！

Intel® Xeon® D-2700



SECURED
TRUSTED
RUGGED
EMBEDDED COMPUTER

SECURECOTS™

MADE IN USA

X-ES
Extreme Engineering Solutions

Extreme Engineering Solutions (X-ES)社は、2002年にアメリカのウィスコンシン州で設立された組込みコンピュータボードのリーディングサプライヤです。シングルボードコンピュータ・耐環境システム・ネットワークI/Oモジュール・イーサネットスイッチ・SSDドライブなどのハードウェア及びソフトウェアの供給、また顧客アプリケーションの優れたサポート・サービスを提供しており、ミリタリの市場で高い評価を得ています。

MISH 株式会社ミッシュインターナショナル
〒190-0004 東京都立川市柏町 4-56-1 TEL：042-538-7650
e-mail：sales@mish.co.jp URL：https://www.mish.co.jp