

ホワイトペーパー エグゼクティブサマリー

組み込みシステムの整合性（インテグリティ）保護

インダストリー 4.0 のメリットとセキュリティのバランス

インダストリー 4.0 の出現により、制御システムはますます相互接続され、パブリックネットワークを介して通信するようになっています。IoTおよび産業用 IoT で連携して動作するこれらのシステムによってもたらされる付加価値は、近年、疑いの余地なく証明されています。ただし、パブリックネットワークの利用は、悪用の可能性がある多くの脆弱性により、サイバー犯罪者の攻撃対象領域を大幅に拡大します。

制御システムのコントローラーの中心には、組み込みソフトウェアがあり、知的財産の損失だけでなく、悪質なコードの改ざんによるマルウェアの侵入を防ぐために保護しなければなりません。つまり、システムの整合性を保証です。

整合性保護には、システムリソースやプログラムおよびデータを不正な操作から保護するセキュリティ対策が含まれます。主な課題は、データの整合性を保証し、システムをセーフモードにし、攻撃が検出されればすぐに全ての機能の実行を停止することです。組み込みシステムの整合性は、明確に定義されたプロセスで暗号化方式を使用し、キー管理と状態ストレージを安全なハードウェアデバイスに依存することで保証できます。

このホワイトペーパーでは、整合性保護の基本的な目的を説明し、ネットワークにつながる物理システムに対する主な攻撃ポイントを特定し、暗号化メカニズムの背後で機能する基本的な対策を定義し、組み込みシステムの保護に伴う多くの課題に対処します。また、組み込みシステムの基本構成と、CodeMeter のスマートカードベースのテクノロジーによる保護について説明します。さらに、以下の CodeMeter による整合性チェックの実装に関連する手順についても説明しています。

- OEM ソフトウェアバージョンの作成
- 静的コード分析とリバースエンジニアリングを防ぐためのプログラムコードの暗号化
- アプリケーションとオペレーティングシステムイメージの両方のプログラムコードに署名
- 復号プロセスに必要なパブリック要素の保存
- ベンダーのサイトに秘密の署名キーを保存
- ロードおよび実行時の操作中に署名とハッシュの検証を実装

またここでは、バックワードチェック、ブートローダー、証明書のチェーンなど、追加の保護対策についても説明しています。

CodeMeter は、Windows、macOS、Linux などの一般的な全てのオペレーティングシステムと、Windows Embedded、Real-Time Linux、VxWorks、および CODESYS 等の PLC をサポートしています。これには、対称および非対称暗号化方式(AES、RSA、ECC)の安全な実装、ハッシュ関数(SHA-256) 、署名検証用関数 (ECDSA) 、および乱数ジェネレーターが含まれています。CodeMeter には、市場で最も厳しい整合性とソフトウェア保護、およびコード改ざんに対する保護を実装するために必要なすべての利用可能なツールが付属しています。

ホワイトペーパーをダウンロード

sales-jp@wibu.com | www.wibu.jp

WIBU SYSTEMS

2026-03-03