WHITE PAPER



産業オートメーションと CodeMeter

機械と制御システムのメーカーが Win-Win になる機会を創出

Oliver Winzenried, CEO WIBU-SYSTEMS AG
www.wibu.com

WIBU SYSTEMS

目次

はじめに 3

保護することのメリット 4

安全の基盤 5

脅威とその対応 6

新しいビジネスモデル 9

まとめ 11

著者



Oliver Winzenried（オリバー・ウィンジェンリート）WIBU-SYSTEMS AG (Germany) 共同創設者 兼 CEO オリバー・ウィンジェンリートは、カールスルーエの大学で電気工学の学位を取得後すぐに起業家としてのキャリアを開始し、家電、自動車、産業工学向けの電子および ASIC 設計、ハードウェア、マイクロコントローラー、組込みアプリケーション開発に注力しました。1989 年にマルケルス・ブッフハイトと共に Wibu-Systems を設立し、引き続き会社の CEO を務めています。

彼のソフトウェア保護への情熱は、安全なライセンス管理や改ざん防止ソリューションからドングルの技術革新まで、多くの特許をもたらしました。 彼は個人的にも研究開発プロジェクトや SD カード アソシエーションのような標準化団体に注力しています。

彼は、バーデンヴュルテンベルク州にある VDMA 地域協会の理事でもあり、VDMA の医療技術ワーキンググループの理事、bitkom の理事、およびカールスルーエ工科大学（KIT）FZI リサーチセンター（FZI）の FZI フレンズ協会の委員会議長を務めています。

2017 年には、Embedded Computing Design 編集チームから Top Embedded Innovator of the Year 賞を受賞し、ドイツの電子出版物 Markt & Technik の読者からは 2015 年の Automation 部門と 2018 年 Pioneers and Innovators 部門で、Manager of the Year に二度選出されました。

はじめに

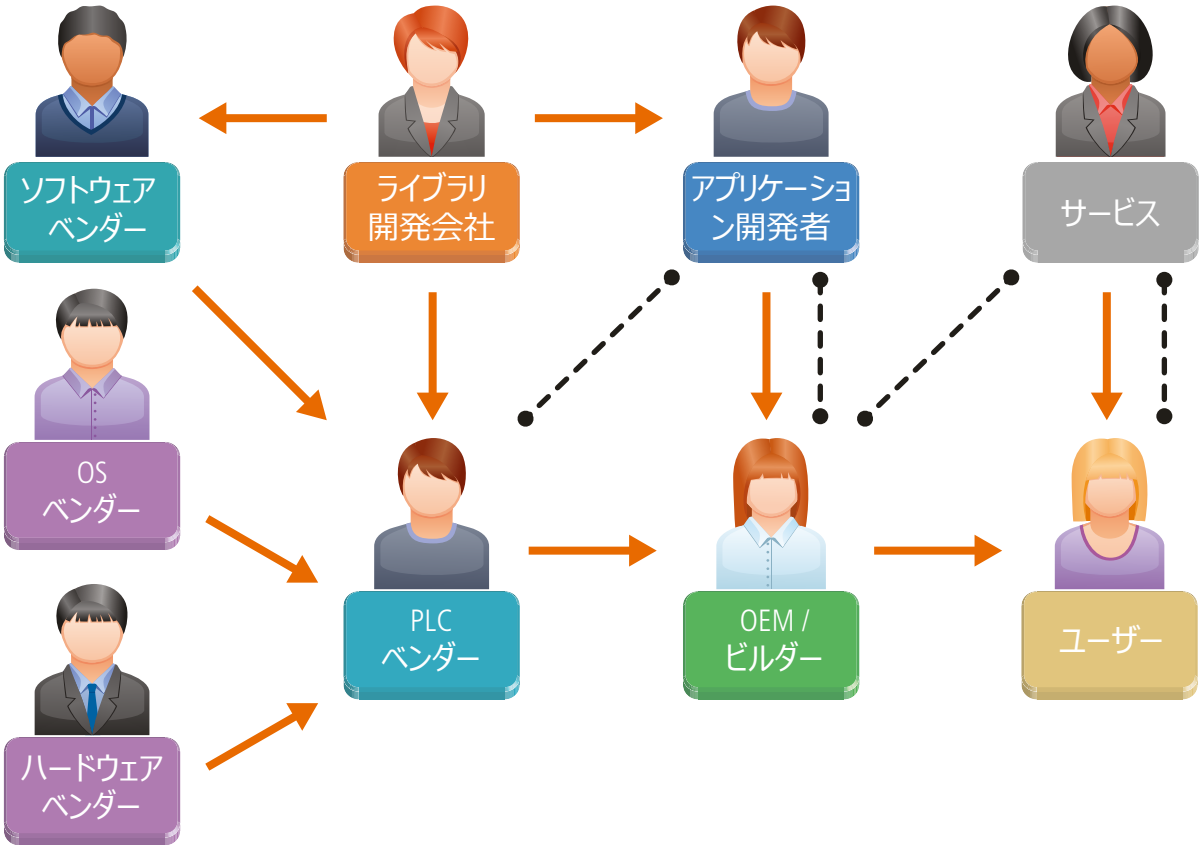
製造装置はプラント全体から個々の機械に至るまで、単独または複合の統合制御システムの使用に依存しています。それらのシステムはハードウェアとソフトウェアの組み合わせで構成され、プラントエンジニアが目的のアプリケーションをプログラムするために使用します。制御システムや製造機械のメーカーにとって、ソフトウェアは多くの機能やアプリケーションに不可欠なキーとして重要な USP（Unique Selling Point）になる可能性があります。このホワイトペーパーでは、機械と制御システムの製造会社およびユーザーが CodeMeter から得られる多くの競争上の利点について説明します。また、CodeMeter および AxProtector の暗号化技術の概念や使用法の概要についても説明します。コスト意識の高い機械エンジニアは、有用な制御システムの価格に注意を払わなければなりません。たとえ機械工学において高額な投資が必要な分野だとしても、制御システムの価格を無制限に上昇させることは受け入れられません。CodeMeter のような保護テクノロジーの統合には、事前のコストが必要です。追加投資に見合う収益は見込めますか？ 機械装置全体のコストの中で、制御システムの占める割合はどのくらいですか？ 制御を保護することや保護システムの導入は、エンジニアリングビジネスの長期的な見通しとパフォーマンスに影響を与える可能性がありますか？

次のページ以降では、これらの質問に回答していきます。

保護することのメリット

保護技術の統合することで、機械設計のコピーや競合他社への重要なノウハウが不正に転送されることを防ぎます。つまり、わずかな追加投資で、数百万ユーロに相当する企業への潜在的な損害と損失を防ぐことができるのです。制御システムや製造機械の開発会社は、CodeMeter を使用することで最小限の労力で新規のビジネスモデルを立ち上げ、ポートフォリオを拡大することができます。例えば、効果的なライセンス管理ソリューションは、特定の機能のアクセス権と使用権の制御や、アクセスの回数制限を可能にします。機能オンデマンドライセンスモデルは、顧客の要望に個別に応えることができると同時に、製造機械の開発会社が自身の基本的な機械の製品ポートフォリオを管理可能なモデルの範囲に抑えることができます。リバースエンジニアリングに対する保護は、設計の違法コピーを阻止し、市場シェアとブランドイメージの両方を保護することに役に立ちます。機械オペレーターとユーザーも、組込みシステム整合性保護により、ソフトウェアの破壊や不正操作の防止といった恩恵を受けることができます。このシステムは、生産工程を特定の注文に限定する必要のあるシナリオにも使用することができます。例えば、高級製品が違法に増産され横流しされることを防ぐために、この方法でバッチサイズを制限することをプラントオペレーターは顧客の追加サービスとして提案することが可能です。したがって、製造機械と制御装置のメーカーおよびユーザーは、CodeMeter の早期かつ完全な統合から恩恵を受けます。これは、制御システムの開発者が創造する力を持つというメリットをもたらします。CodeMeter という 単一の製品で脅威に対抗し、同時に新しいビジネスモデルを始めることができます。これは、制御装置の開発者が CodeMeter のシステムへの統合を検討し、製造機械メーカーと交渉するのに十分な動機となります。

オートメーション業界の関係者



安全の基盤

セキュリティは、機械またはプラントのエンジニアリングプロセスの開始時に始まります。 次の要素が関係します。

制御と開発環境

プラントエンジニアが制御システムを機械に統合すると、制御システムの開発者は、専用のソフトウェアコンポーネントの形で開発環境を提供します。プロジェクトの各エンジニアには、個々の開発環境が存在します。これらのエンジニアが開発プロセスの各部に適切なライセンスを持つことは、制御システムの生産者の利益のためとなります。完成した機械には複数の制御を含めることができるため、複数の開発環境と制御系をパッケージとして提供することが可能です。

ハードウェア、ランタイム環境、および OS

制御システムは基本的にハードウェアとランタイム環境の組み合わせであり、VxWorks 、Windows Embedded 、Embedded Linux などのリアルタイム OS (RTOS) を使用して動作しますが、OS がなくても動作するランタイム環境もあります。

ランタイム環境も、制御システム開発者が提供するソフトウェアコンポーネントです。独自のノウハウが含まれるため、開発者のビジネスモデルにとって不可欠な構成要素となり、保護に値します。

IEC 61131 プログラミング言語とアプリケーション

機械メーカーは、制御システム開発会社が提供する開発環境を使用して、目的のアプリケーションを IEC 61131 プログラミング言語でスクリプト化します。アプリケーションは、機械がその意図された目的をどのように実行するかを制御システムに伝えます。機械エンジニアの特殊なノウハウは、機械とその制御間の相互作用にあります。センサー、モーター、軸がどのように連携するかによって、機械の動作速度と精度が決まります。その能力は機械エンジニア独自のセールスポイントであり、研究開発への多額の投資に対する最終的な成果です。この目的のために研究開発に投資された資産は、エンジニアの競争上の優位性や非常に重要な機密資産を維持することを目的としています。

CodeMeter による段階的な保護

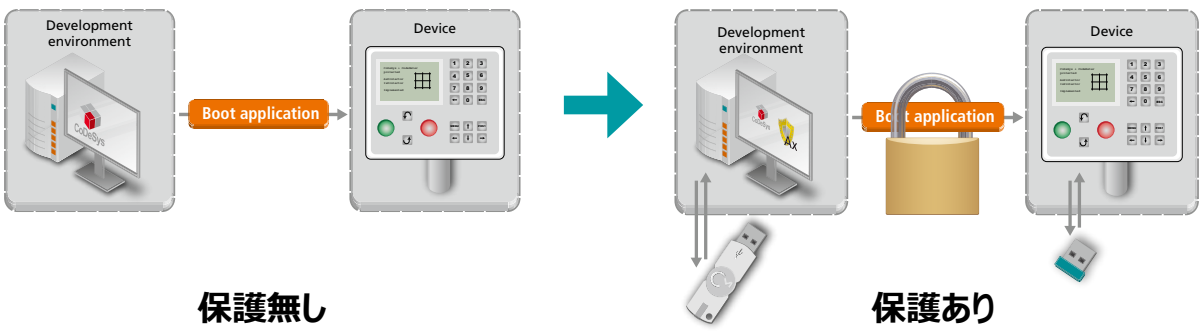
OS 、ランタイム環境、開発環境、およびアプリケーションは、セキュアな連携を形成します。

AxProtector テクノロジーで保護された開発環境上のアプリケーション

まず統合開発環境は、ランタイム環境に転送する前に AxProtector テクノロジーを使用してアプリケーションを暗号化します。このステップは、開発環境がアプリケーションをロックし、「署名」で封印するコンテナとして可視化することができます。

ランタイム環境で保護されたアプリケーション

制御システムのランタイム環境は、アプリケーションがクローズドのコンテナ内に保存されたことを認識します。そして、そのコンテナに適したキーの場所とロックの解除方法を知っています。コンテナのロックを解除する前に、署名（シール）をチェックします。署名が有効な場合は、コンテナを開きアプリケーションを取得します。このシールは、妨害行為に対する追加の保護を提供します。不正なソフトウェアを含む未承認のコンテナは開かれません。この保護されたルートは、ハッカーが送信を盗聴することを防ぎます。したがって、アプリケーションは可能な限り最も安全な方法で開発環境からランタイム環境に移行します。



AxProtector による保護機能により、ドングルライセンスと検証済みソフトウェアでのみ制御を実行可能

ランタイム環境の保護

高スキルのハッカーがランタイム環境を妨害しようとした場合、ハッカーは再び CodeMeter の保護に直面します。信頼性の高い保護の実現には、ランタイム環境を安全に起動する必要があります。CodeMeter は、多くの OS とランタイム環境で使用することが可能です。

基盤

OS 、ランタイム環境、開発環境、および実際のアプリケーションでは、CodeMeter と AxProtector テクノロジーを保護レイヤーとして使用して、このチェーンのすべての関係者が資産を効果的に保護できるようにする必要があります。CodeMeter の利点は明らかです。単一の安全なライセンスソリューションですべての人を保護することができます。また、すべてのライセンス（複数ベンダーの発行分を含む）を単一のドングルで保護することができます。

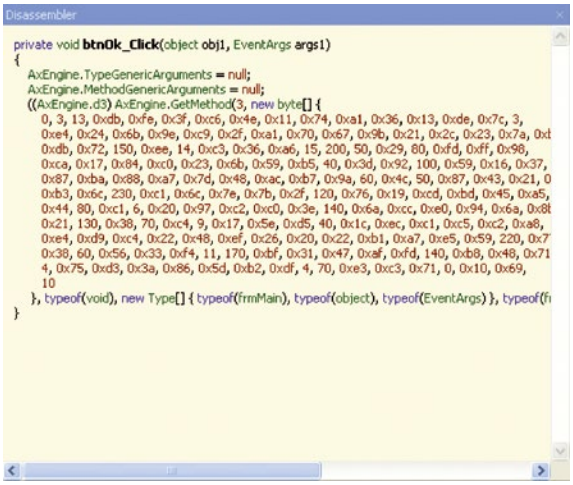
脅威とその対応

リバースエンジニアリングによる模倣

Copy Cat（CC ）は、最初のクローン猫でした。クローンには元の遺伝子が使用されますが、Copy Cat の毛皮はクローンの母親とは異なっていました。グローバル市場では、商用 Copy Cat の数が増加し、どの産業分野でも影響を受けています。産業機器の製造企業は、高級品やファッションブランドと同様の苦しみを受けています。偽造者は、研究開発の莫大なコストを節約し、より安価な材料を使用することで利益を得ます。偽造者は、はるかに低コストでビジネスを行うことが可能なため、確立された市場を弱体化させ、混乱させます。多くの模倣品は元のオリジナルブランドで製品を提供しており、低い品質によって被害企業のブランドイメージを損なわせることがよくあります。完璧な保護は不可能ですが、模倣品の増加を確認することは可能です。模倣者は、どのように活動するのでしょう？彼らはパブリックドメインにあるドキュメントを読み取り、製品のパンフレット、仕様、およびマニュアルをスキャンします。そして見本市や展示会を訪れ、獲物の写真を撮ります。また彼らは単に製品を購入して分解し、その設計を計測するかもしれません。これを防ぐことは不可能です。ソフトウェアをリバースエンジニアリングする場合、模倣者は CodeMeter および AxProtector の暗号技術という強敵に遭遇します。ソフトウェアの保護チェーンのすべてのフェーズで CodeMeter および AxProtector テクノロジーが使用されている限り、リバースエンジニアリングは失敗します。クローズドチェーンとしての保護は、ブートローダー、OS 、ランタイム環境、アプリケーション、そのパラメーター、設定、さらにはユーザーのデータにまで及びます。CodeMeter は、様々な OS とランタイム環境で使用することができます。

AxProtector で暗号化された関数、クラス、メソッドは、ハッカーから読み取り不可能





リバースエンジニアリングからの保護

機械の偽造品を作成できるのは、その OS にアクセスできる場合のみとなります。偽造者は、リバースエンジニアリングのために制御システムからアプリケーションコードを抽出しようとします。これらの試みは、AxProtector テクノロジーによってブロックされるか、ほとんど不可能なことです。

ライセンス保護と違法コピー

製品を 1 つ購入して複数利用。これはソフトウェアのよくある宿命です。
非倫理的な人々は、友人や知人にソフトウェアを提供したり、他人の所有物を盛んに取引したりすることで知られています。CD をコピーし、ライセンス番号を書き留めます。違法コピーよりも作成が簡単なものはありません。多くのソフトウェアパッケージを単一のライセンスからインストールするのに時間はかかりません。単純なライセンスのシリアル番号とパスワードは効果的な保護ではありません。CodeMeter のような統合されたライセンス保護システムは、犯罪者が乗り越えるのが不可能な程はるかに高い壁を作ります。CodeMeter のガードを破ったハッカーはいません。ソフトウェア開発者の ROI は、有効なライセンスが存在する場合にのみ機能するため、保護されています。CodeMeter を実装および統合することにより、自身のライセンスを管理しています。ライセンスプロセスを管理する必要があるため、実装は最初のステップにすぎず、その他に、ライセンスの作成、ライセンスの配布、ライセンスの更新、ライセンスのバックアップと復元、および豊富なレポートによるデータマイニングがあります。これらすべてのタスクについて、CodeMeter License Central は、ライセンスを作成および配布するための単一のソリューションとして利用可能です。これは、販売および流通プロセスと統合され、ライセンス発行者のビジネスプロセスを合理化します。このようなライセンス管理と保護は、以前は PC ソフトウェアに限定されていましたが、それだけでなく長期にわたり産業機械やプラント全体の重要な要素となっており、多くの機能を担っています。プラントオートメーションでは、違法コピーのリスクを無視できません。

輸出規制

制御システムは普遍的に適用可能であり、多目的な設計があります。それらはしばしば厳しい輸出規制の対象となります。そのような制御システムの製造企業は、製品が禁輸地域のユーザーに販売されないことを確実にすることを要求されます。この要件を満たすには、CodeMeter のライセンス保護と組み合わせて、信頼できるエンジニアリング会社への選択的かつ限定的な販売を行うことが必要となります。ライセンス権は、個々の機能レベルまで定義することが可能です。選択された重要な機能はライセンスで保護されており、適切なアクティベーションコードでのみ動作します。このレベルの保護は、制御システムの開発者が輸出管理に関して法的要件を満たしていることを意味しています。CodeMeter License Central に記録されたライセンスの改ざん防止の詳細は、開発者のデューデリジェンスの証拠となります。ライセンス保有者も同様です。すべてのライセンスは、ソフトライセンスファイル形式または工業基準のドングルとして、専用のコンテナに保存されます。

テロ、破壊行為

テロと破壊行為は、今日の世界では脅威となります。サイバー犯罪が増加し、昔からのテロリストや自爆テロ犯に、技術システムを操作して目的を追求する知識を持つ犯罪者が加わっています。彼らの使命は、伝統的な爆弾であれ、改ざんされた制御システムによって引き起こされた爆風であれ、実質的で目立つ被害を生み出すことです。強欲、復讐、およびイデオロギーは、人、機械、および製品を標的とし犯罪的注意を増大させています。制御システムは、都市の無人の地下鉄、化学工場、または郊外の風力発電所など、至る所に存在します。遠隔でのメンテナンスとパラメーター化は、これらの操作にアクセスすることを望んでいるサイバー犯罪者に開かれた窓となってしまっています。ほとんどの制御は、VPN とファイアウォールで保護された、閉じられたネットワークの中にあります。しかし、これらの手段は、制御自体を不正アクセスから保護しているのでしょうか？ VPN のアクセスデータは、脅し取られたり、盗まれたりする可能性があります。優れたファイアウォールでさえ、ハッカーの侵入を許してしまいます。ハッカーがネットワークにアクセスできるようになると、ほとんどの扉が開かれてしまいます。ファイアウォールの背後には、制御システムがむき出しになっています。CodeMeter は、制御システムへのこのような不正アクセスから保護することができます。すべての制御システムは、個別に保護されて存在しています。CodeMeter で保護された制御は、ハッキングに対して手ごわい障壁をもたらします。例えばハッカーは、マルウェアをシステムにロードしたり、犯罪目的で操作したりすることは不可能です。

デモデバイス

賢明なテロリストは、開発者ツールやプロトタイプデザインにアクセスしようと試みますが、CodeMeter によってそれは不可能となります。個別のキーでこれを防ぐことができるため、デモデバイスをリバースエンジニアリングしてライブシステムを操作することはできません。したがって、完全に機能するプロトタイプは、最終的な市場システムと互換性がありません。

OPC UA とセキュリティ

OPC UA は、インターネットにアクセスする接続デバイス用の ISO 標準プロトコルであり、一般的な使用例として遠隔でのメンテナンスがあります。OPC-UA 標準にはセキュリティ仕様が含まれていますが、ほとんどのインスタンスはセキュリティプロトコルなしで OPC UA を使用しています。日常のビジネスにおいて、この点における最大の障害は、キーおよび権限の管理と割り当てにあります。Wibu-Systems は、アクセスキー管理のこの問題を、証明書を管理できる CodeMeter License Central で解決します。CodeMeter は、標準に完全に準拠した OPC UA のプロトコルを使用して、OPC UA と統合するように構成することができます。これにより、OPC UA は認証と暗号化通信のセキュリティを確保することが可能です。

整合性保護

プラントの整合性を確実に保護することは、営業上の利点となります。これは、コンポーネントの適合性の保証にも当てはまります。業界独自の標準は、生産設備の正確な仕様を規定しています。レール認定、防爆性、食品安全、耐振動性、または水密性のあるコンポーネントであっても、意図した目的のために製造および装備されています。生産工場のオペレーターは、すべてのコンポーネントとソフトウェアが完全に適合していることの保証を求めています。CodeMeter では、署名されたプログラムコードを使用してこのレベルの整合性を保護し、信頼できる認証チェーンに含めることができます。

不正操作

すべてのテクニカルデバイスは特定の操作領域向けに作成されており、その製造者はその条件および仕様の下での効果的な作業を保証しています。顧客が機器を改ざんして、指定された範囲を超えて機器を変えてしまう場合、製造者にはどのような影響があるでしょうか？ 改造されたオートバイはより速く、よりうるさくなり、そしてすぐに交通警察によって道路から降ろされます。ライダーは保険を失い、多額の罰金を科されることとなります。改造された生産プラントはより速く稼働し、追加の利益を生み出すかもしれませんが、それらのコンポーネントも記録的な早さで消耗することになります。機械の製造者が元の仕様の範囲外で実行されていることを証明できない場合、定期的なメンテナンスと保証の対象となる必要があります。CodeMeter を使用することで、プラント機械のメーカーは、パラメーターの不正な変更から保護したり、改ざん防止ログに変更を記録したりすることができます。

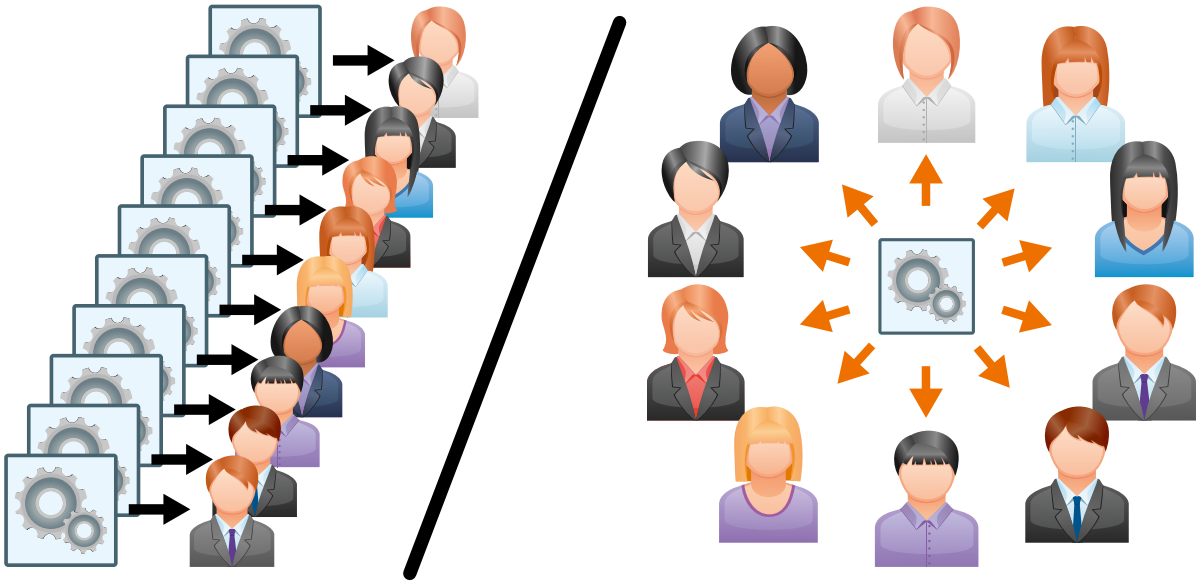
プラントエンジニアが有するソースコードのモジュール保護

プラントエンジニアは通常、アプリケーションのソースコードを読み取り可能な形式で所有しています。ソースコードにアクセスすることにより、顧客は機械の内部動作を妨害する可能性があるので、今では効果的な保護が不可欠となります。ソースコードが編集可能である機会が存在することは、確かに資格のある保守担当者にとって合理的な要件となります。例えば、関連性の低い不良センサーをオフラインにして、次のメンテナンス間隔でセンサーが修理されるまで生産プロセスを実行し続ける時などが考えられます。対照的に、セキュリティやプラントエンジニアの重要なノウハウを保護するための重要なコンポーネントは、そのような外部アクセスから保護する必要があります。顧客は、機能しているソースコードをコピーして、許可されていない第三者に渡すことはできません。繰り返しになりますが、CodeMeter が提供するライセンスメカニズムは効果的な障壁となります。プラントエンジニアの顧客だけでなく、その従業員もソースコードにアクセスすることができます。開発者は、機械アプリケーションを IEC 61131 言語で記述します。そのためには、読み取り可能なソースコードにアクセスする必要があります。メンテナンス技術者は、ルーチンでソースコードを操作する必要があります。強制的または誘惑によって、違法な偽造者はこれらの社員をコードへの開かれた扉として使用することができます。ソースコードは、不誠実な従業員や顧客から同様に保護する必要があります。CodeMeter はその保護を保証します。偽造者はソースコードを入手する可能性がありますが、実行可能なアプリケーションを作成することはできません。

新しいビジネスモデル

生産コストの削減

複数のバリエーションを 1 つの製品でカバーしている場合、生産コストを下げることが可能です。製品管理がより簡単になり、コスト効率が高くなります。開発者が利用可能なバリアントを不正使用から保護することができる限り、ソフトウェア製品はこのモデルの完璧な候補となります。機械制御システムは複数の軸を制御できる場合がありますが、2 つの軸のみを制御する必要がある機械メーカーは、これらの 2 つの軸に対してのみ支払いを行いたいと考えています。機械開発者にとって、ソフトウェアが追加の 6 つの軸を制御可能かどうかは関係のないことです。このシナリオでは、制御システムの開発者は 8 つの軸を管理する機能をソフトウェアに組み込みますが、クライアントが取得したライセンスは 2 つの軸の制御のみをアクティブにさせます。ライセンスは、CodeMeter License Central で管理および処理されます。CodeMeter によって利用可能となった多くのライセンスオプションは、制御システムメーカーに製品の一部として使用権の豊富な選択肢を与えます。 同時に開発者は、CodeMeter License Central で可能となった、きめ細かいライセンスオプションによってシンプルさが反映されたリーン生産プロセスといった、必要なときに提供されるパーソナライズされたライセンスを使用して、1つのマスター製品を管理するだけでよいのです。



物流の効率化：10 人のユーザーに対して 10 台のマシンを用意するのではなく、ライセンスによって構成された 1 台のオールインワン・マシンだけが存在

フィーチャーオンデマンド

生産プラントを開発する際、機械エンジニアは、追加の軸を操作するためには、さらなる制御が必要となることに気付くかもしれません。彼らは、これらの軸を制御するため、既存のソフトウェアで機能を有効化するための追加のライセンスを購入することでしょう。新しいソフトウェアをインストールする必要はありません。制御システムの開発者はこの新しい仕様に迅速に対応し、基本の標準製品に個別の拡張可能なソリューションを提供することができます。これにより、プラントエンジニアは顧客向けに追加機能を販売およびアクティベーションし、双方に新しいビジネスチャンスを生み出すことができるのです。

一時的なライセンス

機能を評価したりベンチマークテストを実行したりするために、ユーザーがソフトウェアのテストのみを行う場合があります。ユーザーがソフトウェアのフル機能バージョンへアクセスするのが理想となりますが、ソフトウェア開発者は、これらのデモバージョンが違法に永続的に利用されていないことを確認する必要があります。一時的に使用可能なライセンスがその確認方法となります。時間、数量、または機能制限は自由に組み合わせ可能です。

サービス技術者の監視

時間制限または数量制限のあるライセンスは、インストール、メンテナンス、および修理サービスにも関連しています。技術者は、職務を遂行する上で広範なアクセス権を必要とすることがよくあります。セキュリティは、アクセス権が顧客の現場での実作業期間のみに制限されることを要求します。ライセンスは、サービスの提供終了直後に期限切れとなるため、不正アクセスをすることはできません。

数量制限のあるライセンス

機能またはソフトウェアアプリケーションへのアクセス数を、制限するシステムもあります。この制限オプションにより、製品設計を定義した生産量やバッチサイズに制限することができるため、機械エンジニアにとって興味深い新たなビジネスチャンスを生まれることとなります。極秘の「時間外シフト」で生産され、闇市で取引される高価なデザイナーファッションのような違法な製品に対し、機械自体は第一の防御になります。

制御システムの改造

すべての制御システムに CodeMeter の機能が搭載されているわけではありませんが、既存の機械に後付けすることは技術的に問題ありません。Wibu-Systems のドングルは工業仕様に対応しており、複数のインターフェイスで利用することが可能で、USB ドングルとしての CmStick 、または SD カード、microSD カード、またはコンパクトフラッシュカード形式の CmCard が含まれています。頑丈なスティックとカードは、幅広い温度範囲で確実に機能し、コンフォーマルコーティングによって結露から保護されています。ターゲット制御システムのアクティベーションを含む CmDongle または CmActLicense ファイルのライセンスは、オンラインとオフラインの両方で転送可能なため、そのシステムはネットワークアクセスのない機械にとって魅力的なオプションとなります。

まとめ

産業用制御システムの開発者の検討次第で、CodeMeterとAxProtectorテクノロジーを使用して、自社とパートナー双方にメリットのある状況を実現できます。CodeMeterによる保護はすでに多くのOSで利用可能であり、CODESYSやBernecker＆Rainer's Automation Studioなどの開発システムに実装されているため、必要なものはすべて簡単にアクセスすることができます。

CodeMeterを選択することは、制御システムの開発者とそのパートナーに多くの恩恵をもたらします。

- リバースエンジニアリングに対する保護
- 違法コピーに対する保護
- 機能オンデマンドによる新しいビジネスチャンス
- 輸出管理の改善
- 整合性および不正操作からの保護
- 改ざん防止ログ
- 破壊行為に対する保護
- デモンストレーションユニットの制御
- 機械向けソフトウェアライセンスの簡素化されたロジスティクス
- 生産コストの削減
- 研究開発投資と技術的優位性の保護

簡単なソフトウェア更新で、既存の制御システムに保護を後付けすることが可能です。CodeMeterは、ここで説明するすべてのユースケースに対して、拡張可能なソリューションでアクセス権、証明書、キー、およびライセンスを管理するための単一の標準手法を提供します。CodeMeterライセンスは、ドングルまたはライセンスファイルのいずれかの専用ライセンスコンテナに保存されます。コンテナには、制御システムや生産機械のメーカー、評価を行う顧客など、複数の権利所有者のライセンスを保存することができます。Wibu-SystemsのCodeMeterドングルは、工業用に対応できるよう設計されています。

Wibu-Systems について

ドイツ本社



WIBU-SYSTEMS AG
Zimmerstrasse 5
76137 Karlsruhe, Germany
Telephone: +49 721 93172-0
sales@wibu.com | www.wibu.com

Wibu-Systems は 1989 年に Oliver Winzenried と Marcellus Buchheit の 2 名により創設された非公開企業で、ソフトウェアライセンシング市場における革新的なセキュリティテクノロジのグローバルリーダーです。

Wibu-Systems の包括的かつ様々な賞を受賞したソリューションはソフトウェアベンダや PC, PLC, 組込, モバイル,クラウド環境の形態でアプリケーションが提供されているインテリジェント機器メーカに対してデジタルアセットやノウハウの保護、ライセンシング、セキュリティのためのユニークかつ国際的に特許取得済みのプロセスを提供します。

Wibu-Systems はそのモットーである “Perfection in Protection, Licensing and Security”, を基に、ソフトウェアメーカやインテリジェントデバイスメーカの知的財産を非合法/不正利用、リバースエンジニアリング、タンパ攻撃、妨害/破壊工作から守り、ERP, CRM, 電子商取引プラットフォームに統合することで新しいデジタルビジネスモデルの創造に貢献します。

Wibu-Systems オフィス

WIBU-SYSTEMS 株式会社
日本
+81 45 565 9710
info-jp@wibu.jp

WIBU-SYSTEMS USA, Inc.
米国: +1 800 6 Go Wibu
+1 425 775 6900
sales@wibu.us

WIBU-SYSTEMS (Shanghai) Co., Ltd.
上海: +86 21 5566 1790
北京: +86 10 8296 1560/61
info@wibu.com.cn

WIBU-SYSTEMS BV/NV
オランダ: +31 74 750 14 95
ベルギー: +32 2 808 6739
sales@wibu.systems

WIBU-SYSTEMS LTD
英国 | アイルランド
+44 20 314 747 27
sales@wibu.systems

WIBU-SYSTEMS SARL
フランス
+33 1 86 26 61 29
sales@wibu.systems

WIBU-SYSTEMS
スペイン | ポルトガル
+34 91 123 0762
sales@wibu.systems

WIBU-SYSTEMS
北欧 | バルト諸国
+46 8 5250 7048
sales@wibu.systems

Wibu-Systems は、プログラムまたはこのドキュメントを事前の通知なしに変更する権利を明示的に留保します。
© 2022 WIBU-SYSTEMS AG – WIBU®, CodeMeter®, SmartShelter®, SmartBind® and Blurry Box® は、WIBU-SYSTEMS AG の登録票商標です。このドキュメントで使用されているその他すべてのブランド名および製品名は、それぞれの所有者の商号、サービスマーク、商標、または登録商標です。

5062-003-07 / 2022-04-05 © 2026 WIBU-SYSTEMS AG