参考情報

Pilz GmbH& Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern,
Germany
Deutschland/Germany
www.pilz.com

2024年5月16日

企業、機械、製品の保護

安全と産業サイバーセキュリティ -
ワンストップショップ

オフトフィルダン、2024年5月16日 -
セキュリティインシデントの影響は今やITシステムだけでなく、製造環境(OT)にも拡がりつつあります。産業サイバーセキュリティのインシデントには目標を定めた攻撃のほかに、意図せぬ不正操作もあります。生産における産業サイバーセキュリティの使命は、機械のデータや処理の完全性・機密性はもちろんのこと、設備と機械の可用性をも保証することです。企業がデータをコントロールできない場合、最終的には企業と従業員の安全に脅威が及びます。セキュリティなくして安全はなく、安全なくして人を保護することはできません！

EUの立法府は増大する脅威への対抗策を打ち出しています。**ネットワークおよび情報セキュリティに関するNIS 2指令**は、企業レベルでの総合的な情報セキュリティ管理システムの導入を義務付けています。

新しい機械規則2023/1230では、設備と機械の改ざんからの保護についての規定を設け、機械の機能安全に影響する部分に対するセキュリティ対策を求めています。

サイバーレジリエンス法(CRA)は、デジタル要素を伴う製品のセキュリティ対策を要求するもので、コントローラ、IOシステムやその他の、機械類に使用されるコンポーネントが対象です。

企業、機械、製品 –
すべてのレベルで、機械のメーカとオペレータはさまざまな課題と法的枠組みに対処しなくてはなりません。

たとえ法律で産業サイバーセキュリティが義務付けられていなくても、この問題に早期に取り組み、アドバイスを受けるべき十分な理由はいくつもあります。機械類の操作に用いる手順や要素の多くは不正操作されやすいため、詳細な調査と修正を緊急に行う必要があるのです。例として、耐用期間の長い機械では対応システムが旧式化して、やがて最新のセキュリティ基準を満たせなくなるという状況がしばしば起こり、システムには埋めることのできないセキュリティギャップが生じます。サプライヤはセキュリティの更新の提供をやめてしまっているからです。多くの場合、末端の機器にはマルウェアに対する保護を実装できなくなります。機器が古すぎ、無理に実装すれば、性能が低下して生産のダウンタイムの原因となるおそれがあります。

ピルツの包括的なサービスパッケージ

究極の目標は企業活動を守ることですが、そのためには、企業は適用される法的要件の特定、システムの弱点の検出と修正、従業員の意識向上とトレーニング、さらに、それらを踏まえた管理体制の施行を含む、さまざまな課題を克服する必要があります。セキュリティの目標は絶えず変化を続けることから、機械の産業サイバーセキュリティを定期的にチェックすることも欠かせません。

オートメーション企業ピルツは、そうした要求に対応するべく準備を整え、世界中の機械メーカとユーザのために、人と機械の保護に役立つあらゆる要素を統合したサービスパッケージを開発しました

。基本情報、入門ガイドおよびトレーニングから、実際のプロジェクトの実装を含めた産業サイバーセキュリティ・コンサルティングサービス(ISCS)までを、幅広くご提供しています。

オートメーションのエキスパートであるピルツは、最新の規格に合わせた簡明なセキュリティ知識を提供する2日間のエキスパート認定コース「CESA – Certified Expert for Security in Automation」を昨年から提供してます。さらに、このトレーニングでは、セキュリティリスクを防止するためのアクセス管理や技術的手段と組織的対策によるネットワークセキュリティの向上など、実践的なリスク低減対策も網羅しています。代表者が試験に合格すると、TÜV NORDから「CESA - Certified Expert for Security in Automation」認定証を授与され、この資格は世界中で認められます。

ピルツは新しい産業サイバーセキュリティ・コンサルティングサービス(ISCS)により、機械の安全関連検査を拡大し、安全とセキュリティに対する総合的なアプローチを創出しています。そして、機械の機能安全に関するサービスの実証済みの手法に基づき、IEC 62443シリーズのセキュリティ規格に準拠したサービスパッケージを開発しました。企業はこのサービスを利用して、産業サイバーセキュリティに十分な備えをし、最新の法的要件への適合を達成することができます。

産業サイバーセキュリティ強化のための4つのモジュール

ISCSは次の4つのモジュールで構成されています:
「保護要件分析」、「産業サイバーセキュリティのリスクアセスメ

ント」、「産業サイバーセキュリティのコンセプト」、「産業サイバーセキュリティシステムの検証」。

「保護要件分析」では、ピルツのエキスパートが企業を訪問して設備や機械の個々の「資産」の保護要件を特定し、それらの保護目標を決定します。第2のステップの「リスクアセスメント」では、システムのライフサイクル全体を通じての各サブセクションのすべてのリスクを、発生確率も含めて考慮します。その後、ピルツのエキスパートはお客様と、特定されたリスクや潜在的なハザードを軽減する解決策について話し合います。

第3のステップでは、ピルツのエキスパートが攻撃や不正操作、誤操作などによって生じるリスクを防御・軽減するための戦略と対策をまとめた「産業サイバーセキュリティのコンセプト」を作成します。さらに、システムのセキュアな動作や構造を継続的に保証するための方策や規則、ガイドラインも作成します。最後のステップ、「産業サイバーセキュリティのシステム検証」では、実装された対策の有効性を確認します。

セキュアな機械の可用性

産業サイバーセキュリティ・コンサルティングサービスは、サイバー攻撃の低減または防止に役立つとともに、意図せずして起こるセキュリティインシデントも減らすことができます。その結果として機械の可用性が向上し、最終的にはコストの削減と経済効率の維持につながります。

そして何より、ISCSは適切なセキュリティ対策を通して機械に関わる人員の保護を実現します。なぜなら、セキュリティインシデントは安全対策の妨げにもなるからです。たとえば、機械の前にライト

カーテンを設置し、オペレータが危険ゾーンに立ち入らないようにしていても、攻撃者が関連のコントローラやメカニズムを侵害することで、ライトカーテンの保護機能が無効化されないとも限らないのです。セキュリティは安全を守ります！

機械のメーカとユーザは、人と機械の保護に役立つあらゆる側面を考慮したピルツのサービスパッケージを入手できます。

上記のような理由から、機械に実装する際には、安全とセキュリティを合わせて検討するのが理にかなっています。セキュリティなくして安全はなく、安全なくして人を保護することはできないからです！

明確な制御: 誰が機械に何をできるか？

機械とオペレータの安全はひとえにアクセス制御にかかっています。対象が人であろうとネットワークであろうと、たとえば、機械の運転中には誰も危険ゾーンに入れないようにするために、入口を不正なアクセスから保護しなくてはなりません。権限を有する機械のオペレータがメンテナンスの目的で危険ゾーンに入る場合は、その間、他の人物が設備にアクセス可能であってはなりません。たとえ善意でも、誰かが同時に現場で、あるいはネットワークを介して操作やメンテナンスを行えば、重大な結果を招きかねません。

「Identification and Access Management」(I.A.M.)はそのための重要な要素の1つで、企業における設備や機械への権限やアクセスを明確に管理するものです。その中には、組織的な対策および仕様に加えて、適切な安全機能とセキュリティ機能が含まれます。ピルツのPITreaderのようなアクセス許可システムは、これらの機能を備えた最適な製品コンポーネントで

す。ユーザは従業員の保護、賠償責任保護、最大生産性、データ保護の観点から、各種の要件を達成できます。

ピルツのオペレーティングモード選択およびアクセス許可システムPITmode
fusionがあれば、機能安全に対応するオペレーティングモードの選択が可能になり、設備と機械へのアクセス許可を管理できます。オペレータはRFID技術でコード化されたトランスポンダを受け取ることで各自の責任と資格に応じて機械を有効化できる仕組みで、権限のある人員だけが、定められたオペレーティングモードで設備の操作や制御が可能になります。意図せぬ動作や不正操作に対する高度な保護が実現します。

このオペレーティングモード選択およびアクセス許可システムに、モジュラ式安全扉システムのコンポーネントを追加すると、安全とセキュリティに配慮した、機械へのアクセスの一貫したコンセプトが完成します。

データ、ノウハウ、オペレーションが不正アクセスや改ざんから十分に保護されておらず、外部の攻撃者が制御システムに侵入できれば、最高の安全扉保護も意味をなしません。

産業用ファイアウォールによる外部からのアクセス防止

ピルツのSecurityBridge産業用ファイアウォールの使命は、オートメーションネットワークを外部からのアクセスから保護することです。パソコンとコントローラ間のデータトラフィックを監視し、ハッカーの攻撃や不正操作の目標となりうる経路(アタックサーフェス)を減らします。SecurityBridgeはピルツのコントローラだけでなく、サードパーティーのコントローラも不正な操作から守ります。

ピルツは、安全とセキュリティに対する総合的なアプローチだけが、人と機械全体の保護を保証できると信じています。今後、企業はセキュリティへの取り組みの要否や範囲を自ら決定することはできません。今日ではセキュリティは法的要件の1つなのです。エンジニアリングにおける産業サイバーセキュリティとしてのセキュリティはIT部門だけの仕事ではなく、設計・製造の切り離せない一部です。あとからセキュリティを実装するのは複雑な手間であり、たいていの場合、使いやすさ、機能、生産性の面でマイナスになります。

((文字数：10,173))

((囲み記事:))

EUの産業サイバーセキュリティ法の概要

特にヨーロッパでは、立法府が脅威レベルに対応する一連の法律を制定しており、その結果、ヨーロッパでは世界のどこより厳格な要件が適用されます。しかし他の国々でもすでに合意は成立していて、いずれ法律として導入される見通しです。産業サイバーセキュリティのグローバルな整合化が進むものと予想されます。

NIS 2: 企業の義務の拡大

NIS (Network and Information Security)はサイバーセキュリティの強化を目的とする欧州連合指令です。2016年に制定され、これまではエネルギー、交通、銀行・金融、健康、飲用水の供給・販売、デジタルインフラといった重要インフラの提供者に適用されていました。そうした分野のサービス提

供者は「適切なセキュリティ対策」を導入し、サイバーセキュリティに関わる重大インシデントを報告する義務がありました。将来は、新しいNetwork and Information Security 2 EU 2022/2555 (NIS 2)指令により、サイバーセキュリティのためのリスクマネジメント対策が現在よりはるかに多数の企業に義務付けられます。NIS 2では対象セクタが拡大され、製造/生産業者、たとえば電気機器のエンジニアリングや製造を行う企業も含むことになります。

情報システムのリスク分析および安全コンセプト、サプライチェーンの保護、人員の安全などに関する要求事項が定められ、アクセス制御や設備管理のコンセプト、さらには管理のためのトレーニングも要求事項に含まれています。

NIS 2指令は2022年の終わりに欧州議会およびEU理事会で採択されました。すべてのEU指令と同様、直ちにEU加盟諸国で発効して拘束力を持つわけではなく、各国の国内法に統合される必要があります。EU加盟国はこの指令を2024年10月18日までに、国内法に組み込むことになっています。企業にとって賢明なのは、できるだけ早くNIS 2に対応し、自社の包括的なセキュリティ評価を実施することでしょう。情報セキュリティ管理システム（ISMS）の開発はその一例です。この観点から、情報セキュリティ規格であるISO 27001の認証を取得することは有用です。

風力タービンに関するNIS 2の例: NIS 2は将来、発電設備(例：風力タービン)メーカなどの機械製造業者も要件への適合を求められます。そして風力タービンの製造者には、オートメーション用ソリューション、コントローラ、センサなどが必要です。一定規模以上の電気部品メーカにもNIS

2が適用されます。また、NIS
2の規定ではサプライヤーも考慮されるため、ピルツのような企業は安全なサプライチェーンを心がけ、サプライヤーに遵守を求めなければなりません。このようにNIS
2はサプライチェーン全体に影響します。

新しい機械規則: セキュリティなしでCEマークは付けられない

機械指令2006/42/ECは、機械の機能安全に関して特別に重要な意義を果たしています。

機械類をヨーロッパに輸入する場合、機械製造者はこれまで必ず適切な適合性評価の手順を経て、CEマークを表示する必要がありました。

2023年6月に機械規則として再発行されたことを機に、仕様が最新技術に更新されました。法的規則なので、国内法への変換は不要です。機械製造業者は新たな要求事項に対応するための猶予期間を与えられ、2027年1月20日からはそれらを遵守しなくてはなりません。

この機械規則は現行の機械指令に代わるもので、サイバーセキュリティを必須の義務としている点が機械指令との大きな違いです。機械指令は純粋に安全性を評価するものであるのに対し、新規則はセキュリティ保護の目標を「破壊からの保護」(Protection against corruption)の章の「必須健康安全要求事項」(Essential health and safety requirements:
EHSR)に定めています。機械の安全機能は意図的/非意図的な破壊によって損なわれてはなりません。

このCEマーキングへの新たな道のりは機械のメーカとオペレータに新たな課題を課すものであり、これまでの安全とセキュリティの概念の見直しを迫るものといえます。

サイバーレジリエンス法: 製品のライフサイクル全体のセキュリティ

企業と機械類の総点検をすることに加えて、セキュリティ対策を装置(制御システムなど)に直接実装することも絶対に必要です。2022年9月、欧州委員会は製品のサイバーセキュリティ強化を目的とする規則のドラフトを提出しました。サイバーレジリエンス法(CRA)の対象は、他製品との通信が可能なデジタル要素(ハードウェアとソフトウェア)を伴う製品の製造業者です。スマートフォンやロボット掃除機のようなB2Cセグメントの製品も、コントローラやセンサ、オペレーティングシステムなどの純粋なソフトウェア製品、機械本体といったB2Bセグメントの製品と同様に、この影響を受けます。

実際にCRAの影響がどれほどあるかは、製品を分類するために最終的に設けられる基準によります。CRAの規定によると、適切なレベルのサイバーセキュリティが保証された製品以外は市場に出すことができません。これは製品のライフサイクル全体にわたって適用されます。つまり、セキュリティは製品開発時から始まるのです。これが、ピルツが数年かけて、開発プロセスをIEC 62443-4-1「産業用オートメーションおよび制御システムのセキュリティ - 第4-1部:
安全な製品開発ライフサイクル要求事項」に適合させ、セキュリティが実証されたSecurityBridgeなどを開発してきた理由です。

((文字数: 5,826))

図

図1

Grafik_aus_Prospekt_Schulungen_mit_Pilz_3c_en_ppt

ワンストップの安全とセキュリティ:
ピルツは機械の産業サイバーセキュリティのため、サービスと製品の包括的なソリューションパッケージを提供しています。(写真: © Pilz GmbH & Co. KG)

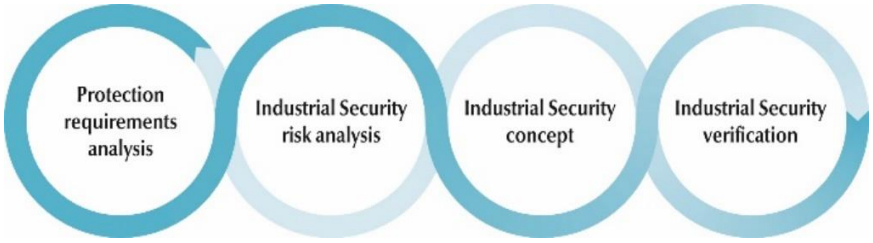
図2:

F_Services_ISCS_two_men_tablet_in_discussion_get1150297892_cold1

ピルツは、産業サイバーセキュリティ・コンサルティングサービスの開始により、設備と機械のセキュリティ対策を支援しています。(写真: © Westend61/[westend61] via Getty Images, © Pilz GmbH & Co. KG)

図3:

G_Cycle_Industrial_Security_en



ピルツの産業サイバーセキュリティ・コンサルティングサービスは4つのモジュールで構成されます:
「保護要件分析」、「産業サイバーセキュリティのリスクアセスメント」、「産業サイバーセキュリティのコンセプト」、「産業サイバーセキュリティシステムの検証」。(写真: © Pilz GmbH & Co. KG)

図4:

F_Press_IAM_Man_using_PITreader_Key_Get1169337234_Get1169337153_cold1

包括的な「Identification and Access Management」はアプリケーションへのアクセス権を管理し、安全性と産業サイバーセキュリティの両面から安全機能と安全対策の完全性を保証します。(写真: © Westend61/[Westend61] via Getty Images, © Pilz GmbH & Co. KG)

図5:

F_security_robot_man_virtual_world_Fot208731449_cold1_2019_06

産業サイバーセキュリティは、生産および産業設備を意図的な、または意図しない不具合から守る方法を説明しています。産業サイバーセキュリティの目的は、設備や機械の可用性、機械のデータや処理の完全性および機密性を保証することです。(写真: © ipopba/Fotolia.com; © Pilz GmbH & Co. KG)

Pilz – The Spirit of Safety

ピルツは、オートメーション技術分野の製品、システム、サービスを提供するグローバルサプライヤです。安全オートメーションの先駆者として、人、機械、環境の

安全を創造し続けています。同族企業ピルツの設立は1948年に遡り、現在ではオストフィルダンの本社を拠点として世界各国に42の現地法人・支店、2,500名の従業員を擁しています。

業界の技術リーダーであるピルツは、機械の安全と産業サイバーセキュリティを実現するためのトータルなオートメーションソリューションを提供しています。そのポートフォリオには、センサ、コントローラ、ドライブ技術に加え、産業用通信、診断、視覚化を目的としたシステムが含まれます。また、コンサルティング、エンジニアリング、トレーニングを含む各種サービスも国際的に提供しています。ピルツのソリューションは、機械エンジニアリングの業界にとどまらず、社内物流、包装、鉄道技術、ロボティクスなど、多くの業界で採用されています。

www.pilz.com

ピルツのソーシャルメディア:

ピルツのソーシャルメディアチャネルでは、当社に関する情報やピルツの社員、オートメーション技術の最新ニュースをお知らせし

プレス向け連絡先：

Martin Kurth

企業および技術プレス
電話：+49 711 3409-158
m.kurth@pilz.de

Sabine Karrer

技術および企業プレス
電話：+49 711 3409-7009
s.skaletz-karrer@pilz.de