参考情報

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

自動化ネットワークにおける「ゾーンとコンデュイット」：セキュリティが安全を守ります

安全を最優先します

Ostfildern、2026年7月 –
機械規則により義務付けられているように、産業サイバーセキュリティは安全機能を不正操作から保護することを目的としています。つまり、セキュリティは安全機能が正常に動作するための前提条件なのです。しかし、自動化ネットワークに対して包括的な保護をどのように実現すればよいのでしょうか？IEC 62443-3-2や今後策定されるEN 50742といった標準は、システムをゾーンに分割し、接続を監視するという明確な指針を示しています。これは、業界団体や専門家による現在の推奨事項にも一貫して見られる原則です。ピルツは確信しています。安全と、いわゆる標準的な自動化を厳格に分離することが、効果的な機械安全の鍵であるということです。これは多重防護の原則に基づいており、ゾーンとコンデュイット方式を通じて実現されます。

家は、頑丈で安全に建てることができます。つまり、堅固な壁、耐火性のある建材、信頼性の高い電気設備、そして正常に作動する警報器を備えることで実現できます。この構造上の安全は、設計上の対策、センサ技術、および保護機構によって予期せぬ危険を未然に防ぐことを目的とした「機械安全」の典型的な例です。しかし、そのような家は、意図的な干渉を受けない場合にのみ安全が保たれます。暖房装置の操作、電気回路への妨害、あるいは警報システムの

無効化は、安全性を考慮して設計された建物を危険な場所へと変えてしまう可能性があります。機械の世界において、安全に関連する部品が不正に操作されたり、認証なく無効化されたりすれば、どんなに優れた安全設計もその効果を発揮できなくなります。

こうした状況において、セキュリティは外部からの保護という役割を果たします。具体的には、頑丈なドア、厳重な接続点、監視された接続、そして不正な侵入を防ぐための防護策などが挙げられます。つまり、セキュリティは事故そのものを防ぐものではなく、例えば不正な操作モードの選択や操作によってアクセス権を得た者による、保護メカニズムの無効化を防ぐ役割を果たすのです。安全を確実に維持する唯一の方法は、「安全のためのセキュリティ」です。

規制要件から提案された解決策まで

機械規則（EU）2023/1230では、設備と機械の安全機能の稼働において、セキュリティが初めて必須要件とされました。すなわち、意図的か否かを問わず、いかなる操作によっても安全機能が損なわれてはなりません。まさにここで、新たに策定された標準EN 50742が重要な役割を果たします。この標準は、機械規則におけるセキュリティに関する必須要件を明確にするのに役立つでしょう。本標準は、データの破損に対する保護に関する技術データを規定するとともに、安全機能に影響を及ぼす可能性のあるハードウェア、ソフトウェア、およびデータについて明確な要件を定めています。この標準は、開発から運用、そして廃棄に至るまでのライフサイクル全体をカバーしています。産業用自動化システムおよび制御システムのサイバーセキュリティに対する体系的なアプローチを定めた既存のIEC

62443シリーズ標準も、重要な役割を果たしています。本規格は、リスク分析、多重防護、およびセグメンテーションの原則（「ゾーンとコンデュイット」）のための体系的な枠組みを提供しており、EN 50742において、セキュリティ保護のための代替的または補完的なアプローチとして明示的に認められています。これらの標準は総じて、「安全のためのセキュリティ」の規範的な中核を成しています。これらは、機械のデジタル完全性が機能安全の前提条件として認識され、それに応じて保護されることを求めています。

「 ゾーンとコンデュイット」が機械の安全性を高める理由

家のイメージに戻ると、ボイラー室はあるゾーンを表し、スマートホームゲートウェイへの接続は、それに関連する配管を表しています。この接続が不正に操作された場合、たとえその部屋が完全に安全であっても、システム全体に影響が及ぶ可能性があります。したがって、個々のゾーンのセキュリティを確保するだけでなく、それらを接続する経路のセキュリティを確保することも極めて重要です。まさにここで、「ゾーンとコンデュイット」の原則が発揮されるのです。各ゾーンは明確に区切られており、ゾーン間の移行部分は監視されるよう設計されています。家において、ドアや割り当てられた鍵によって誰がどこへ入れるかが決まるのと同様に、産業プラントの内部においても、内部からの保護（安全）と外部からの不正操作に対する保護（セキュリティ）は、構造的に密接に結びついています。

その結果、多重防護の原則に基づいた保護コンセプトが生まれました。安全性は単一の防御策によって達成されるのではなく、次々と連なる複数の保護層によって実現されるのです。一つの壁を乗り越

えても、次の壁は依然として立ちはだかります。ゾーンはこうした階層化された空間を構成し、コンデュイットはゾーン間の監視対象となる通路です。こうすることで、単一の脆弱性によってシステム全体が危険にさらされることはありません。特に、安全が関わり、ひいては人々の命を守るという観点からはなおさらです。

ピルツは、このアプローチを「安全のためのセキュリティ」として一貫して追求しており、ここでいう「安全」とは、セキュリティの第一の保護目標です。重点は安全の確保にあり、それがひいては人々を守ることに繋がります。そのため、ピルツは安全機能を一般的な機械制御、すなわち標準的なオートメーションから分離し、それによって安全関連機能への影響を低減しています。これらの「アセット」の機能的な分離が明確であればあるほど、確実な保護を実現するために必要な追加の安全対策は少なくて済みます。

このアプローチのメリットは、機械のライフサイクル全体を通じて明らかです。安全機能と標準機能が分離されている場合、標準機能が更新されても、安全機能について並行して再認証や適合を行う必要はありません。これにより、保守や点検の作業が大幅に軽減されます。従来の安全コントローラは、標準的なコントローラに比べて安全上重要な更新の頻度も大幅に少ないため、この分離により、多くの不必要な介入が不要になります。分離構成には技術的な利点もあります。例えば、安全小型コントローラ「PNOZmulti

2」のような独立型安全システムは、さまざまなメーカーの制御システムと自由に組み合わせることができますが、一方、統合型システムは特定の技術に縛られることが多いためです。一方で、個別の安全対策を導入することで、攻撃者にとってのハードルは高まります。なぜなら、個別のシステムをそれぞれ個別に侵害しなければならないため、操作がはるかに困難になるからです。さらに、標準システムは必要に応じてオンラインにできる一方で、実際の安全機能は隔離された状態を維持できるため、攻撃対象領域を大幅に縮小することができます。

安全とセキュリティの自動化をこのように分離し、それぞれのセキュリティレベルを完全に調整することで、安全対策、メンテナンス、拡張計画の策定が容易になり、効率も向上します。したがって、標準プログラムの変更点を行う際、安全関連のセクションに手を加える必要がないため、必要なプログラミングや調整作業の負担が大幅に軽減されます。同時に、この分離はソフトウェアおよびサポートコストにも好影響をもたらします。なぜなら、システムを分離することで、ライセンス料やサービス料が抑えられることが多いからです。

分離による保護 — 訓練による能力向上

安全機能と標準的な自動化機能を明確に分離することで、技術的な堅牢性が確保されるだけでなく、オペレーターのミスも減り、必要なトレーニングも軽減されます。安全機能は専用のハードウェア上で動作し、組織的にも明確に分離されているため、標準プログラムに変更点が加えられた場合でも、その安全性は確保されます。その

結果、日常業務におけるミスが安全性を損なうことはなく、責任の所在もより明確になります。

ピルツは、企業がこのアーキテクチャを導入できるよう、包括的なトレーニングおよびサービスプログラムを提供しています。これには、「産業サイバーセキュリティの基礎」および「CESA – Certified Expert for Security in Automation」の研修コースのほか、産業サイバーセキュリティサービスが含まれます。これらでは、個々のブロックから堅牢な「安全のためのセキュリティ」の概念を構築する方法について解説するだけでなく、さらに踏み込んだ内容も扱っています。セキュリティリスクを体系的に管理し、包括的な安全コンセプトを構築する方法、IEC 62443の要件を組み込む方法、安全な機械ネットワークのアーキテクチャを構築する方法、そして実施された対策の効果を評価し、継続的に改善する方法を実証しています。

このアプローチの大きな利点の一つは、安全機能の保護がアーキテクチャ設計によってすでに保証されているため、ユーザの現場のオペレーターがセキュリティの問題に深く関与する必要がないという点です。このため、本研修コースは主に、セキュリティに関する意思決定を行う方やシステム設計者を対象としています。一方、現場のオペレーターについては、産業サイバーセキュリティに関する追加の研修を受けなくても、安全に業務を継続することができます。その結果、実用的な役割分担が実現し、プラントの運用が簡素化されると同時に、安全性が持続的に向上します。

明確な体制と適切な専門知識による安全性の向上

効果的な「安全のためのセキュリティ」戦略は、個別の対策によって実現されるものではなく、綿密に練られたアーキテクチャ、明確な責任分担、そして的を絞ったスキル開発を通じて実現されるものです。まさにここで、ピルツの出番となります。ピルツは多重防護を徹底し、安全システムと標準的な自動化システムを明確に分離することで、耐障害性の高い機械の基盤を築きます。さらに、実践的なトレーニングやコンサルティングを通じて、企業が自信を持ってこの道を進めるよう支援します。その結果、標準の要件を満たすだけでなく、日々の業務において具体的な付加価値をもたらすレベルの安全性が実現されます。それは、よりシンプルで堅牢、そして長期的に見てより効果的なものです。

((文字数: 9,640))

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ーです。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ています。

www.pilz.com/facebook
www.pilz.com/xing
www.pilz.com/youtube
www.pilz.com/linkedin

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

Jenny Skarman

技術プレス

電話：+49 711 3409-1067
j.skarman@pilz.de

Eva Gellner-Rößle

技術プレス

電話：+49 711 3409-7147
e.roessle@pilz.de