Web ベースのプロセス制御を実現

プロセス産業の運用環境は複雑で、制御技術に対する要求は厳しい。オブジェクト指向のデータ管理を備えた web ベースのプロセス制御システムは、これに対する賢明な回答の一つである。

デジタルトランスフォーメーションの取り組みを始めていないプロセス産業の企業は、時代に取り残されるかもしれない。プロセス制御の歴史は、手動制御から空気圧、そして最終的には分散制御システム(DCS)へと進歩してきた。Web ブラウザ、ネットワーキング、インターネット、携帯電話通信、産業用モノのインターネット(IIoT)などの技術的進歩により、Web ベースのプロセス制御の環境が整った。その結果、ISA/IEC 62443 産業用サイバーセキュリティ規格に基づくセキュリティが組み込まれた、より柔軟で管理しやすい制御システムが実現された。

HTML5 で web ベースのプロセス制御

HTML5 は、追加のソフトウェアやプラグインの必要なしに Web アプリを作成できる言語だ。他の Web アプリケーションとの一貫性を維持し、タブレット、ラップトップ、スマートフォン、スマートテレビなどの多くのプラットフォームで動作するオープンな標準規格だ。そのねらいは、マルチメディアやその他の新しい機能をサポートしながら改善することだ。人間が読みやすく、web ブラウザ、パーサーなどのコンピュータやデバイスによって一貫して解釈でき、過去のソフトウェアとの下位互換性を維持できる。

HTML5 は、相互運用可能な実装を推奨するための詳細な処理モデルが含まれている。ドキュメントで使用可能なマークアップは拡張、派生、合理化することができる。また、複雑な Web アプリケーション用のマークアップおよびアプリケーション プログラミング インターフェイス (API) を提供する。

同じ理由で、HTML5 には低電力のデバイスを念頭に置いて設計された機能が含まれているため、クロスプラットフォームのモバイルアプリケーションの候補にもなっている。

これをプロセス制御に適用すれば、制御システムエンジニアリングおよび運用環境へのアクセスは、Google Chrome や Microsoft Edge などの HTML5 準拠の Web ブラウザが使用できる。HTML5 はオープンスタンダードであり、制御システム固有の規格ではない。

HTML5 Web ベースのプロセス制御では、インターネット接続は必要ない。これは、制御システムがクラウドで実行されているという意味ではなく、インターネットに接続されていないローカルネットワーク上でも動作できる。サーバーと Web クライアント間の通信

に HTML5 に基づく Web テクノロジが使用されている。
シーメンスは、オブジェクト指向のデータ管理機能をもつ SIMATIC PCS neo プロセス制御システムを発売し、Web ベースのプロセス制御を実現した。
PCS neo プラットフォームは、オープンテクノロジーを組み込んで、組織内の協業を加速しビジネスパフォーマンスを向上できる。PCS neo は、モジュールタイプパッケージ(MTP)や OPC UA を含む現在と発展中の将来の標準を取り込んだプラットフォームである。

Web ベースの プロセス制御の利点

HTML5 は、初めて完全に Web ベースの DCS を実現した SIMATIC PCS neo の強みだが、それだけにとどまらない。例えば、シーメンスのゼロインストールクライアントアプローチにより、PCS neo を実行するためのデバイスへのインストール作業は不要だ。
非 Web ベースの制御システムとは異なり、プロジェクト情報はサーバーに格納されるため、クライアントには多くのリソースは必要ない。これにより、システム全体のコストを削減できる。大規模なプラントの場合、通常必要な高価なサーバーは数台だけだ。ユーザーは、クライアントには低消費電力のマシンを用いてコストを削減できる。PCS neo クライアントの要件には、Windows 10 Enterprise と Google Chrome が含まれているだけである。
ゼロ・インストール・クライアント・アプローチでは、クライアントにソフトウェアやライセンスのインストールは必要ない。すべてのライセンスはサーバーレベルで集中管理されるため、システムのアップグレードが容易である。このことは迅速なシステム立ち上げと、必要に応じて拡張できるスケーラビリティを意味する。プロジェクトの規模が拡大したときには、プロジェクトのタイムラインを短縮するためにリソースを割り当て、より多くのエンジニアを追加できる。オペレータの端末は必要に応じて簡単に追加できる。
さらに、ゼロ・インストール・クライアント・アプローチは、ワークステーションの要件が少ないことを意味する。ユーザーは、コントロールルーム

の 4 面モニタを備えた PC、自宅やオフィスのラップトップ、現場のタブレットなど、最適なデバイスを柔軟に使用できる。
エンジニアリング、運用、保守用にライセンスをインストールした専用ワークステーションを用意する必要性は減る。ユーザーが必要なアクセス権を持っていれば、エンジニアリングと運用に同じワークステーションを使用できる。
PCS neo は、発売された DCS として初めて、エンジニアリングから監視および制御まで、完全に Web ベースになった。Web ベースはインターネットベースを意味しないことを再度強調する必要がある。プラントへのリモートアクセスは PCS neo の特徴であるが、閉じたネットワークであっても設計どおりに実行できる。
リモートアクセスにより、ユーザーは世界中どこにいても適切なエンジニアリングリソースを取り込むことができます。これにより、オペレータはどこからでもプラントを操作でき、自宅からプラントにアクセスすることも可能だ。リモートアクセスにより、クライアントへのインストールが不要となり、情報機器や出張コストが削減できる。HTML5 の Web 技術を使用することにより、エンジニアリングと運用における柔軟な分散コラボレーションや、セキュリティ標準に対応した非武装地帯(DMZ)のターミナルサーバーを介したリモートアクセスを提供することができる。
PCS neo Web ベースのプロセス制御システムは、すべてのタスクに対応する一貫したエンドツーエンドのワークベンチと、固定およびポータブルデバイスを問わず、直感的なグラフィカルユーザーインターフェイス(GUI)操作を提供する。これにより、運用者はプロセス情報を迅速に分析し、エンジニアとの連携により生産上の問題を速やかに診断し解決を図ることができる。日常業務でリアルタイムに意思決定を行うための情報が提供される。
直感的な GUI 画面は、使用するモニターサイズに自動的に調整され、単一のモニタでも 4 分割表示を設定できるため、機器費用が少なくて済む。さらに、ユーザーは画面表示をズームインまたはズームアウトしてプロセスディスプレイとフェースプレートをはっきりと表示することができ、Web ベースではないプロセス制御システムよりも優れた可視性を実現する。直感的な GUI は、タッチスクリーンが必要な場合には、より適したボタンサイズに変更できる。ユーザーは、他の HTML5 アプリケーションで使い慣れたショートカットが使えることに気が付くだろう。

ウェブベースプロセス制御でも安全にセキュリティを確保

シーメンスは、組み込みセキュリティを PCS neo の優先事項と考えている。統合されたセキュリティメカニズムを使用し、ユーザーがプロジェクト独自の構成に適応できるようにしている。安全で高速なデータアクセスは、最新のサイバーセキュリティ技術と、現場での役割に基づくアクセス権限管理を組み合わせることで可能となる。Web ベースのプロセス制御システムは、業界標準に準拠した以下の項目の多層防衛を組み込み、生産プラントを保護している。

•物理的および組織的なセキュリティ対策
•不正アクセスからユーザーの知的財産とノウハウを保護
•ネットワークセグメンテーション、アクセスポイントの保護、HTTPS、VPN、および証明書を用いた通信セキュリティ
•ユーザー管理と役割に応じた権限付与
•パッチ管理
•マルウェア検出
•IEC 62443-4-1 に基づきテュフ(TÜV)認証された安全な製品ライフサイクルプロセス
•IEC 62443-3-3 に基づき TÜV 認証されたネットワークおよびシステムセキュリティ
•IEC 62443-2-4 に基づき TÜV 認証された産業用制御システム(IACS)サービスプロバイダ
•現在の IACS セキュリティ標準に準拠
•安全なウェブ接続

物理アクセスの防御と監視は、ハードウェアに保存されている重要なデータを、物理的に隔離して保護することを意味する。Web ベースシステムに Web クライアントを通して接続する構成により、ユーザーは重要コンポーネントを高度にアクセス保護されたキャビネットルームで守ることができる。アクセス保護とは、次のものを指す。

•施設と建物
•制御と機器の部屋
•キャビネット
•DCS デバイス(コントローラ、入出力[I/O]システム、電源など)および PC
•ネットワークコンポーネント(スイッチ、ルーター、ワイヤレス、Wi-Fi)、およびローカルエリアネットワーク(LAN)ポート
•ケーブルと配線

PCS neo は、複数のファイアウォール層を介して分離されたネットワークセルで動作するように設計されている。フロントファイアウォールは、オフィスネットワークとのデータ交換を制御および制限する。非武装地帯(DMZ)では、制御制限されたデータ交換により、プラントへのサービスとサポートが可能となる。

すべてのホストで、PCS neo により Windows ファイアウォールが自動的に構成される。

PCS neo の強化されたシステムは、潜在的な脆弱性を排除することでセキュリティリスクを軽減することに役立つ。Web ベースのプロセス制御のパッチ管理では、プラントに適用されていないパッチを一覧できる。管理コンソールと統合された中央パッチ管理により、セキュリティ脆弱性を解消できる。Windows Server Update Services (WSUS) では、SIMATIC PCS neo で互換性を検証済みのマイクロソフト更新プログラムのインストールおよび管理をすることができる。

サイバー攻撃を早期に発見することで、システムに対策を講じ、潜在的な損害を軽減することができる。PCS neo はウイルス対策ソフトウェアと互換性があり、オプションシステムのセキュリティ情報およびイベント監視(SIEM)、侵入防御システム (IDS)、侵入防御システム (IPS) などのサポートにより、追加の保護を提供する。

認証とアクセス制御により、システムへのアクセスの制御、一覧、および簡単な管理が可能になる。ユーザーとアプリケーションには、タスクに必要な権限のみ付与される(最小限の特権)。

PCS neo は、Microsoft Windows ドメインをシステム環境および認証局として使用する。これは、DCS 専用のスタンドアロンドメインにすることも、社内ドメインに統合して、オペレーターが会社の電子メールと同じ資格情報で DCS にログオンすることもできる。ドメインと証明書を使用する時に、シーメンスはシステムにアクセスするユーザーを検証するだけでなく、末端のデバイスも検証している。これは、PCS neo が初期設定状態から採用している多層防衛戦略に沿ったものだ。

ソフトウェアはサーバーにのみインストールされ、ライセンスは管理コンソールによって一元管理される。DCS ソフトウェアやライセンスはクライアント ステーションでは必要ない。ユーザーがラップトップまたはモバイルデバイスからプラントにリモートアクセスした後に、そのデバイスを紛失した場合でも、デバイス上にはプラントデータは無い。プラントデータは、サイトにあるサーバー上のみにあり、制御キャビネット内で保護されているため 安全安心である。

アクセス制御は非常に重要だ。ユーザーは、システムのすべてのユーザーに適切なアクセス権限を付与する必要がある。それ以上でもそれ以下でもない。エンジニアまたはオペレータが PCS neo を開くと、使用しているステーションに認証局から発行された PCS neo 証明書がある場合にのみ、ユーザー名とパスワードの入力を求めるプロンプトが表示される。次に、ユーザーはドメイン固有のユーザー名とパスワードを入力し、PCS neo のアカウントとして有効ならば、必要なアクセス権限のみが与えられる。

PCS neo セキュリティ管理は、「ボルトで後付け」されているのではなく、「組み込まれている」のである。ユーザーは最低限の管理工数で組み込みセキュリティを実現できる—これは将来にわたって通用するコンセプトだ。

シーメンスは、パートナー向けにトレーニングを提供し、安全なインストールとセキュリティを推奨できるようにしている。そしてセキュリティ設定とベストプラクティスについてのドキュメントメントを提供している。

Web ベースのプロセス制御は、プロセス産業のユーザーが、デジタルトランスフォーメーションの潮流に取り残されずに、先を行くための方法である。

ウェブベース制御システムのサイバーセキュリティ

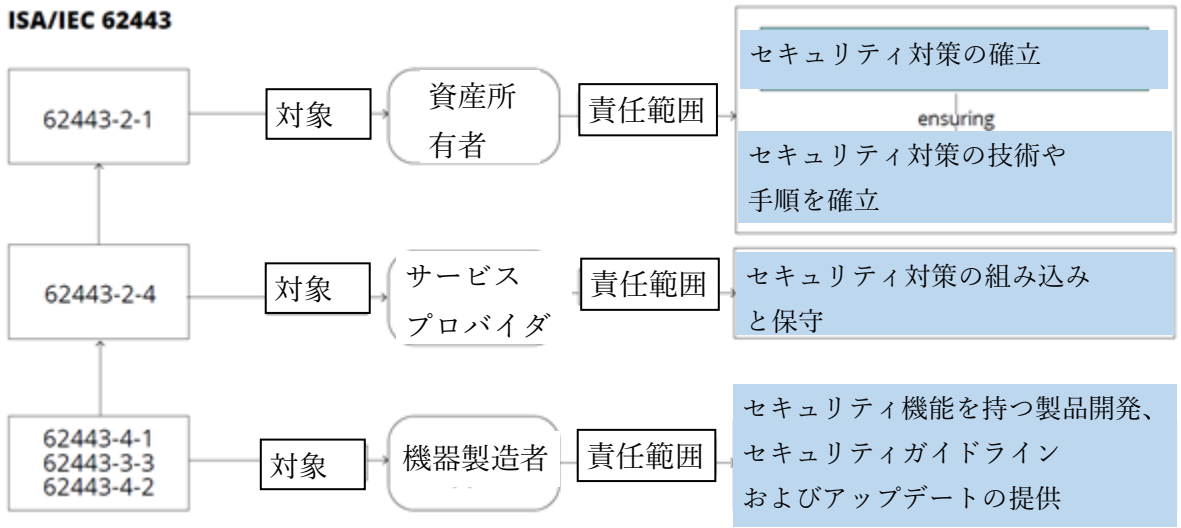
SIMATICS PCS neo はウェブベースの制御システムだが、ウェブベースはインターネットベースを意味するものではない。クローズドネットワーク上でも設計どおりに動作でき、ISA/IEC 62443 シリーズの規格を含む現在の産業用自動制御システム(IACS)セキュリティ規格に最初から適合するように設計されている

多くの組織では、ISO/IEC 27001/2 に基づく企業の IT システムのサイバーセキュリティを管理するポリシーと手順を確立している。

しかし、産業用運用技術 (OT) システムを保護するためには、別の アプローチが必要となる。ISA/IEC 62443 シリーズは、OT システムのセキュリティを確保するための規格である。ISO/IEC 27001/2 と組み合わせると、組織は共通のアプローチを通じて可能な限り ISO/IEC 27001/2 と整合させながら、必要に応じて IT と OT で異なるアプローチを適用することができる。

OT インフラストラクチャのセキュリティのために ISO/IEC 27001/2 と ISA/IEC 62443 のどちらを使用するべきかという議論をする人もいるが、正しいアプローチは両方を使用することである。SIEMENS AG で 40 年以上にわたり、規格、規制、認証の責任者を務めてきた Pierre Kobes は、ISA/IEC 62443 のほとんどの文書の作成に参加した。さらに、シーメンスで規格を実装するための複数のプロジェクトに関わって、変革を推進してきた。

彼は、ISA グローバルサイバーセキュリティ連盟のためのホワイトペーパーを執筆し、これら 2 つの世界的に受け入れられている標準を一緒に使用して、どのように統合された全社的サイバーセキュリティ計画を確立すれば良いかを説明した。



ISA/IEC 62443 は、産業運用設備の保護に関係するすべての事業者を対象としている。注意: 上図はパート 62443-2-1 の最新バージョンを参照しており、最終的に国際標準として承認されておらず、変更される可能性がある。
出典:ISAGCA

「資産所有者は、統合されたセキュリティ対策を備えた適切な技術ソリューションの設計と、これらのソリューションで使用される製品のセキュリティ機能に依存しています」と Kobes 氏は言う。「ISA/IEC 62443 シリーズは、サイバー脅威から運用設備を保護するため、資産所有者をサポートするすべての事業者に多層防衛アプローチを適用することを求めており、大きな付加価値を提供する。」

ISO/IEC 27001/2 には、特に機器製造者に対して 5 つの管理策 (クラス A.15) を規定し、他の管理策についても多くのガイダンスが多数含まれている。ISA/IEC 62443 シリーズは、OT 機器製造事業者が果たすべき役割を規定することにより、これらの管理策の実装をサポートしている。これらは、資産所有者が OT 機器製造事業者に課すサイバーセキュリティ要件の基礎となり、製品購入にあたっては機器製造者に対して ISA/IEC 62443 規格の第三者認証を要求する可能性がある。

Kobes 氏によると、例えば ISA/IEC 62443-4-1 では、機器製造者に対して、脅威モデリングや安全な設計原則の適用などにより、脆弱性を削減し管理することを求めている。コーディングガイドラインに従うことによるコードの脆弱性の排除や、ファジーテスト、侵入テスト、バイナリ分析などのテストによる脆弱性の発見と排除、ユーザー向けのセキュリティガイドラインの提供、現場で発見された脆弱性への対処や、セキュリティアップデートの提供方法なども機器製造者に求められている。

さらに、ISA/IEC 62443 シリーズには、OT インフラストラクチャで使用される製品の技術的セキュリティ機能の要件が含まれており、セキュリティレベル(SL)を定義して、資産所有者の許容可能なサイバーセキュリティリスクに見合った実現可能な保護レベルを区分している。

PCS neo は、ISA/IEC 62443 の関連項目について以下の認証を取得している。

- ISA/IEC 62443-4-1 に基づく安全な製品ライフサイクルプロセスの TÜV 認証
- ISA/IEC 62443-3-3 に基づくネットワークおよびシステムセキュリティの TÜV 認証
- ISA/IEC 62443-2-4 に基づく IACS サービスプロバイダ向けの TÜV 認証

シーメンス株式会社
東京都品川区大崎 1 丁目 11 番 1 号
http: //www.siemens.com/jp/