MOXA®

産業用ネットワーク構築に関するガイドブック

未来を見据えた
産業用ネットワーク構築のための
重要なヒント

Contents

MOXA®

デジタルトランスフォーメーションが加速しています

サプライチェーンの混乱、パンデミック、カーボンニュートラルに向けた推進など、世界中であらゆる業界がその影響を受けています。このような状況下において世界中の企業が市場シェアを維持し、混乱を回避し、イノベーションを取り入れるために現在、いかに柔軟にビジネスを回復および継続するためのオペレーショナルレジリエンスを必須と考え始めています。

“レジリエンス”は、過去に今日ほど重要になったことはありません。

多くの企業は、オペレーショナルレジリエンスを実現するために、**デジタルトランスフォーメーション**とテクノロジーに多額な投資をしています。例えば、リモートオペレーションに移行している企業もあれば、予測機能の追加に重点を置いている企業も多くあります。 マニファクチュアラーは、複雑で急速に変化する新しい状況に対応するために、自動化への投資が急増しています。デジタルテクノロジーを使用することで企業は、ネットワーク環境の変化に迅速に対応することができます。

34% の企業が、限られたサイトスタッフで、ほぼすべてのデバイス、機器、資産、施設、プロセスをリモートで監視および診断をしています。

— IDC 2021 年 オペレーションの将来に関する調査

シームレスコネクティビティ
がもたらす未来

産業組織のデジタル化を完全に実現するには、高度なデジタルテクノロジーを導入するだけでは十分ではありません。その成功は、これらの新しいソリューションを既存のレガシーネットワーク、インフラストラクチャ、プロセスにシームレスに統合し、統一されたデジタルエコシステムを構築できるかどうかにかかっています。データのシームレスかつリアルタイムの伝送が鍵となります。ITとOTシステムを統合することにより企業は、ローカル、リモート、クラウドベースのオペレーションを強化する技術的機能を最大限に活用することができます。IDCのIT/OTコンバージェンス調査*によると、30%以上の企業が、データヒストリアンソフトウェア、産業用制御システム、資産管理などのシステムからの運用データをエンタープライズデータガバナンスモデルに統合することを計画しています。2018年と比較するとOTとITシステムのコンバージェンスは、10%近く上昇しました。

従来は、別々に存在していたこれらのシステムを統合することは、独自の課題が生じます。これらのシステムのシームレスな統合は、不可逆的な傾向ですが、OTシステムは、コネクテッドアプリケーションの増加に対応するために、よりオープンなアーキテクチャを採用する必要があります。それを念頭に置いて強化された堅牢な産業用ネットワークの重要性はさらに高まっています。

* 2020 年 IT/OT コンバージェンスに関する世界的な調査結果

“IT/OT コンバージェンス”
は、オペレーショナルレジリエンスを実現するための未来への道筋です。

将来を見据えた産業用ネットワーク通信は、
このコンバージドされたデジタルの未来が成功する鍵となります。

MOXA®

産業用ネットワークは、進化しています
その準備は、できています

産業用ネットワークに無数のセンサーやマシンを導入するIT/OTコンバージドアプリケーションの急速な拡大に直面するに伴い、もはやデバイスが接続されているか、どうかの問題ではなく、必要なデータを必要な時に必要な場所に、必要な信頼性で転送し、継続的なオペレーションを実現することが重要になっています。

将来を見据えた
産業用ネットワークの 再定義：
ネットワークコネクティビティ + データコネクティビティ

堅牢なネットワークコネクティビティが重要であることは疑いありません。しかしながら、そればかりに気を取られていては、競合他社に差をつけられるばかりでイノベーションの機会を逃してしまう恐れがあります。

“機能信頼性”は、未来志向の産業用ネットワークを構築する際に念頭に置くべき重要な概念です。これは、安定したシームレスなネットワークコネクティビティに焦点を当てるだけでなく、シームレスなデータコネクティビティをサポートしてネットワーク設計をする必要があるという考え方です。この2つを組み合わせることで、リモートコントロールコマンドやインシデント対応メカニズムなどのインテリジェントな機能をオペレーションに組み込むことができます。

今後、ビジネスの成長を引き出す鍵となるのは、デジタルトランスフォーメーションです。産業用ネットワークは、この新しい方向性に適応するように進化していくでしょう。しかしながら、多くの企業にとって馴染みのない分野であるため新世代のネットワークに移行するには、いくつかのハードルが存在します。このガイドブックでは、産業用ネットワークの未来を見据える必要があるいくつかのヒントを提供します。

将来を見据えた産業用ネットワークで課題を克服する

[Challenge 1]:

より多くのデバイスが接続され、同じネットワークを介して通信が実行されることでシステムの複雑さは、指数関数的に増加します。また、システムダウンタイムを招きます。しかしながら、現在および将来の変革のニーズをサポートできる安定したネットワークとデータコネクティビティを開発することは、ほとんどの自動化ビジネスにとって課題です。

カスタマの声：

“PEAは、電気のエキスパートですが、重要なネットワーク通信については、専門的な知識がありません。そのためデジタル変電所通信システムの実装と維持には、信頼できるエキスパートの協力が必要です“。

Pongsakorn Yuthagovit,

Assistant governor,
PEA (Electricity Authority)

エキスパートのヒント:

産業オートメーションの未来は、シームレスなデータ伝送とデータ統合に大きく依存しています。堅牢なネットワーク基盤は、将来のユーザビリティと安定性を実現するための重要なビルディングブロックです。すなわち、**信頼性**こそが、将来にわたって通信を保護するネットワークソリューションを選択する際の最初の重要な考慮事項です。

堅牢なデバイスは、過酷な環境で安定した通信を行うための基盤です。産業用認証は、特定の厳しいアプリケーションでのネットワークのパフォーマンスと耐久性のベンチマークとなります。例えば、NEMA TS2認証は、デバイスが危険なITS（高度道路交通システム）環境で確実に動作することを証明します。統合をより容易にするために、**複数のインターフェースと高いポート密度**を備えた製品は、異なるコネクティビティシナリオに対応し、ネットワーク構造を簡素化することができます。さらに、リング拡張をサポートしていれば、既存のネットワークにデバイスを追加する際に、リスクが高くエラーが発生しやすいネットワークトポロジーを変更する必要がありません。また、ネットワークデバイスには、予期せぬ問題に対処し、ダウンタイムを回避するための**冗長化メカニズム**が備わっていることが重要です。例えば、冗長デュアル電源入力は、電源障害によるダウンタイムをなくし、その他のネットワークの冗長化機能は、ネットワークのリカバリーを早め、システムを迅速に再稼働させることが可能です。

ネットワークソリューションは、容易に統合できるものを選択することが大切

デジタルトランスフォーメーションは、ゆっくりとした段階的なプロセスであり、耐久性と適応性に優れた産業用ネットワークデバイスが必要です。従って、現在と将来の両方の機能をサポートするために必要な柔軟性を組み込むことが重要です。その1つが帯域幅です。帯域幅の広い製品を選択すると、時間の経過と共に需要が高まるにつれて、より多くのデバイスをサポートし、より多くのデータを伝送できます。もう1つの重要な側面は、物理的な設計です。キャビネットのスペースは、通常非常に限られています。しかしながら、製品サイズは、ポートの数によって異なることが多く、フィールドエンジニアが今後多くのデバイスのためにキャビネットスペースを計画することは頭の痛い問題です。コンパクトで統一感のある設計のネットワークデバイスなら将来の拡張を計画する上で、潜在的な課題をチャンスに変えることができます。

カスタマの声：

“Moxaハードウェアソリューションは、エッジまで完全なギガビットスピードを実現し、ファイバーインフラストラクチャに接続されているすべてのキャビネットに接続され、ネットワークを将来にわたって保証し、現在および将来のデータとビデオのニーズをサポートするために必要な帯域幅を提供します”。

Traffic engineer,
City government

今後は、IEEE802.1に基づく新しい規格であるTime-Sensitive Networking (TSN)がネットワークトラフィックに優先順位を付け、リアルタイム通信を保証します。つまり、タイムセンシティブデータが適切なタイミングで適切な場所に配信されることを意味します。TSNは、標準のイーサネットインフラストラクチャを活用して、産業オートメーションアプリケーションを単一の統合ネットワークに統合することができます。TSNは、すでに世界中のいくつかのミッションクリティカルなアプリケーションに採用されており、将来のデジタル化されたネットワーク環境でさらに多くの可能性を提供することが期待されています。TSNは、マシン内、マシン対マシン、マシン対監視など、様々なアプリケーションで確定的な通信を実現できます。

デジタルトランスフォーメーションを加速し、Industrial Internet of ThingsとIndustry 4.0が提供する可能性を最大限に活用するためにTSNテクノロジーでビジネスを未来に繋げましょう

[Challenge 2]:

ITとOTのコンバージェンスが加速する中、閉じられた環境OTシステムは、よりオープンなアーキテクチャへと徐々に移行しています。しかしながら、このことは、OTインフラストラクチャを潜在的なサイバー脅威にさらすことに繋がり、ハッカーの標的となります。重要なアプリケーションの生産情報のほとんどが機密情報でありまた、公共の安全に関連するためOTエンジニアは、システムのインテリジェント化と安全性を同時に維持するというプレッシャを受けます。サイバーセキュリティは、多くの企業がデジタル化の推進を躊躇したり、場合によってはプロセスを完全に停止させたりする主な障害の 1つです。

エキスパートのヒント:

オートメーション環境にデジタルテクノロジーを導入することは、サイバーセキュリティのリスクが発生する可能性があり、その結果、オペレーションが深刻な中断に繋がる可能性があります。OTエンジニアのために設計された**セキュアなネットワーキング**は、ネットワークセキュリティの導入を簡素化し、コンバージドインフラストラクチャへの移行の際にネットワークの保護と可用性の両方を維持することができます。

カスタマの声:

“食用油精製のカスタマは、製造プロセスの詳細が企業独自の秘密のレシピであるため、サイバーセキュリティについて非常に慎重です。そのような貴重な情報を公共のネットワークにさらす危険を冒す人は誰もいません。”

Jeffery Wong,

Senior business unit manager,
YNY Technology (Manuf

可用性は、OTネットワークにとって重要な目標であり、重要なインフラストラクチャは、24時間/365日休まず利用可能である必要があります。しかしながら、毎年、何百もの企業が何らかのセキュリティ侵害を経験しています。多くの場合、これらの侵害は、費用の損失と共に、オペレーションや評判に影響を与える可能性があります。多くのOTエンジニアにとって、サイバーセキュリティは、複雑かつ馴染みのない分野といえます。デジタルトランスフォーメーションに向けたサイバーセキュリティのリスクを軽減するために、特定の目的に設計されOTネットワークとサイバーセキュリティ対策を組み合わせることで、オペレーションに対する潜在的な脅威を最小限に抑えることができます。

深層防護を備えたセキュアなネットワークが解決策となります

深層防護は、OTエンジニアに適した解決策を提供します。優れた防御は、セキュアなネットワークインフラストラクチャを構築するための強固なビルディングブロックから始まります。まず、国際的なセキュリティ認証に合格し、国際的に認知された規格に基づくセキュリティ機能を備えた**セキュリティ強化デバイス**を選定する必要があります。IEC62443規格は、世界中で採用されている最も普及しているサイバーセキュリティ規格の1つです。この規格は、深層防護のアプローチを概説し概要し、コンポーネントレベルでの基本的要件を定め、資産所有者、システムインテグレータ、コンポーネントプロバイダ共通言語を提供します。標準化された基準により、ネットワーク機器の調達と統合が非常に容易になります。ワイヤレスネットワークでは、ミッションクリティカルなネットワーク環境において機密データを保護するための強固な認証と暗号化アルゴリズムを確立するWPAセキュリティ規格を採用しています。

次に、セグメンテーションと脅威防止を通じてアタックから**ネットワークを保護**するために第2の保護層が必要になります。一般的なセキュリティ制御テクノロジーには、Deep Packet Inspection(DPI) やファイアウォールなどがあります。これらのテクノロジーにより、悪意のある活動からネットワークの保護または侵入を隔離されたゾーンへ封じ込め損害を最小限に抑えることができます。

カスタマの声:

“発電所のコントローラとPCSおよびBMSコンテナ間の通信を保護するためにMoxaの産業用セキュアルータがセキュリティ境界を構築し、Modbus DPI機能は、システム間のModbus通信を保護します。”

Designer and manufacturer of energy storage systems, France

最後に、**ネットワークのステータスを常に最新の状態に保つ**ことが重要です。優れた可視性により、ハイレベルのシステムからエンドデバイスに至るまで、ネットワークのステータスをより理解することができます。専用のセキュリティマネージメントツールは、OTエンジニアがネットワークのセキュリティステータスを追跡することができます。リモートオペレーションに関しては、強力な安全対策に裏打ちされたセキュアな通信チャネルを備えることで、デジタルテクノロジーのすべての利点を余すことなく享受することができます。

[Challenge 3]:

コネクテッドデバイスの数が数十から数百以上に増加する。このような複雑なネットワークを手動で最小限のダウンタイムで管理することは、ますます困難になります。また、一部のアプリケーションによっては、ファクトリ内の移動ロボットのWi-Fiコネクションが見えないなど特別な特性をもつものもあり問題をさらに複雑にします。このような進化するネットワークを管理しながら、稼働時間を最大化しようとすることは、大変なタスクです。

カスタマの声：

“製鉄所内の環境は非常に厳しく、大型クレーンのワイヤレス信号に影響を及ぼしかねません。そのためオペレーションをスムーズに進めるためには、ワイヤレスネットワークをリアルタイムで綿密に監視および管理できる信頼性の高いソフトウェアが必要となります。”

Automation engineer,
Steel plant

エキスパートのヒント：

ネットワークとデバイスの相互接続が進み、ネットワークの規模は、拡大し続けています。このような大規模なネットワークにおいて、デバイスの設定やシステムのメンテナンスを効率的に行うためには、ネットワークを明確に可視化することが重要です。OTユーザーに合わせた**簡素化されたマネージメント**により特に特殊な要件をもつアプリケーションのネットワークコンフィギュレーションとマネージメントを容易にします。

デジタルユニファイドネットワークへの移行は、OTネットワークインフラストラクチャが必然的に規模を拡大し、ますます複雑で相互接続されます。単一障害点は、OTインフラストラクチャ全体、さらにはITネットワークシステムに大きく影響する可能性があります。従って、最大限の稼働時間を確保することは、ビジネスをスムーズに運営し続けるために不可欠です。異なるネットワークデバイスを単一のユニファイドオペレーティングシステム上で動作させることで、ネットワークのコンフィギュレーションとマネージメントを大幅に簡素化することができます。一方、全体的な監視アプローチは、問題に迅速に対応し、ネットワークの稼働時間を最大化することができます。

可視性は、OTネットワークマネージメントを簡素化するための基本です

ネットワークマネージメントは、非常に複雑です。そのためOTエンジニアの視点でネットワークを可視化する手段が重要です。プログラミング言語に慣れたITエンジニアとは異なり、より合理的で可視化されたインターフェースを好むかもしれません。**OTフレンドリーなネットワークマネージメントツール**は、リアルタイムなネットワークトポロジ、チャート、デバイスのセキュリティステータスを備えたユーザインターフェースによりオペレータがいつでもネットワークやデバイスのステータスをリモートから確認することができます。さらに、アプリケーションによっては、交通信号機ネットワークなどのように物理的に広範囲のエリアにまたがる分散型ネットワークもあります。セントラルロケーションからデバイスをリモートで管理することができればリソースと時間を削減でき、より効率的な運用が可能となります。

カスタマの声：

“Moxaの産業用ネットワークマネージメントソフトウェアを使用することで問題発生した箇所を容易に特定することができ、問題の解決に要する時間を大幅に短縮することができます。この合理化されたシステムは、シャットダウンの防止と発生時の復旧時間を大幅に短縮できます。”

Engineer,
Electricity Authority

アプリケーションによっては特殊な要件があることを考慮し、**特定のネットワーク環境に合わせたカスタマイズされた専用のマネージメントモジュール**を使用することで、機能の信頼性を強化することができます。例えば、自動化されたファクトリでは、Wi-Fiデバイス間のワイヤレスコネクションの品質が、自律移動ロボット（AMR）の効率を決定します。Wi-Fiリンクは、目に見えず動的であるため、ワイヤレスネットワークのリアルタイムスナップショットを作成してロボットの位置を特定し、潜在的な問題を発見することで、自動化の効率を大幅に向上させることができます。

デジタルトランスフォーメーションを産業アプリケーションに適用する

— 高度道路交通システム（ITS）への取り組み

都市化の拡大、それに伴う交通渋滞や二酸化炭素排出量の増加により、ITSの重要性が高まっています。言うまでもなく、ITSは、スマートシティやスマートトランスポーテーションを発展させるための重要な要素です。最近の調査*によると、グローバルのITS市場規模は、2028年までに428億米ドルに達し、2021年から2028年の間にCAGR 9.34%で拡大すると予想されています。より多くの交通インフラシステムが相互接続されるようになるにつれ、信頼性の高いデータ通信が不可欠となります。

ネットワークの完全デジタル化に伴い、予期せぬ障害を回避するために、以下の3点を考慮に入れる必要があります。

信頼性:

多くの交通ネットワークデバイスは、過酷な屋外環境に設置されるため信頼性が重要な要素となります。ネットワークバックボーンは、道路状況、信号機、ビデオ監視データなどを含むロードサイドの機器と交通管制センタとの間の大量のデータ伝送をサポートできる必要があります。高帯域幅、ハイパフォーマンス、拡張性を中心にネットワークを構築することで将来的なデバイスの追加に対応することができます。スムーズな交通輸送は、一貫したトラフィックデータの一貫したストリームに依存するため、ネットワーク全体に回復力があり、データが継続的に伝送されるように十分な冗長性が必要です。

セキュリティ:

Cybertalk.org によると、2020年6月から2021年6月の間に、輸送業界では毎週のランサムウェアアタックが186%増加しました*。これらのアタックが成功すると都市交通は、大混乱を起こし、生命にかかわる障害などが発生する可能性が生じます。そこでネットワークとOTのセキュリティの規律と機能を組み合わせることで、信頼性とリスクをより効率的に管理することができます。多くのトラフィックネットワークデバイスが屋外に設置され、改ざんに対して脆弱となっているため、セキュリティで保護されたハードウェアによってエッジでのネットワークの安全性を確保することができます。さらに、脅威を未然に防ぐメカニズム、ITとOTのネットワークのセグメント化、セキュアなネットワークマネージメント機能なども重要です。これらの安全対策を講じることで、悪意のあるトラフィックをブロックし、侵害時の被害の軽減、ネットワーク監視時に異常を発見したときに必要なアクションをプロアクティブに実行することができます。

簡素化されたマネージメント:

これらの相互接続された分散ネットワークデバイスを効率的に管理するために、セントラルロケーションからトラフィックネットワークを設定、監視、および診断することで時間とリソースを大幅に削減することができます。フィールドエンジニアが新しいネットワークデバイスをインストールする際、オペレーショナルエンジニアは、オンサイトでデバイスを構成するために遠くのサイトに行く必要がなくなりデバイスをリモートコントロールセンタから簡単にセットアップできます。リモートサイトで問題が発生した場合、灼熱の太陽の下や嵐の夜にエンジニアを派遣してキャビネットのデバイスをチェックする必要がなくなりました。ユーザフレンドリーで直感的なネットワークマネージメントシステムを使用することでエンジニアは、ネットワークのステータスをリモートで理解し、必要なアクションを実行することができます。

* インテリジェント交通システムの市場調査レポート (2021-2028), Fortune Business Insights

MOXA

Case Study

安全で効率的な街づくりために未来に繋がる交通インフラストラクチャを構築

先進的な都市である米国Lancasterは、高度なネットワークテクノロジーを使用して相互接続性を強化し、新しいAdvanced Traffic Management System(ATMS)ソリューションを構築することの重要性を認識しています。140を超えるトラフィックキャビネットは、ファイバーネットワークとATMSに接続されているため、すべてのトラフィックキャビネットとリモート資産を1つのセントラルロケーションから管理することができます。これにより、都市にリアルタイムのデータと予測インテリジェンスが提供され、交通事故や渋滞に適応できるようになりオペレーションが改善されました。

Moxaのスイッチを多数使用してギガビットのフルスピードをエッジまで広げるネットワークインフラストラクチャを構築し、ネットワークを将来にわたって保証し、現在および将来のデータとビデオのニーズをサポートしています。市政府は、その信頼性と堅牢さに非常に満足しています。Mitch Megas/Lancaster Cityの交通エンジニアは、キャビネットの1つが高圧線からの高電圧の通電事故後にキャビネット内で、まだ機能していた唯一のコンポーネントは、Moxaスイッチだけであったことを鮮明に覚えています。

さらに、Moxaのネットワークマネージメントソフトウェアの使用により、都市全体のネットワークのオペレーションステータスの監視、必要に応じてネットワークセキュリティ監査の実施をインシデントに迅速に対応できます。従来、エンジニアリングチームは、交通信号の不具合の報告を受身で待つしかありませんでした。しかし、今、彼らは何かが誤動作していると直ぐに反応することができます。これにより作業が簡単になるだけでなく、メンテナンスと運用の効率も向上しました。

SMART CITYとは?

Lancaster市は、先進的な技術データと予測的なインテリジェンスを用いてオペレーションの改善を行っています。

カスタマの声:

"デジタルネットワークインフラストラクチャのサポートにより市政府は、人的介入の必要性を67%削減し、個人のワークロードを軽減しました。"

City of Lancaster, USA

未来の道を開く交通輸送

Moxaの未来志向のネットワークソリューションで輸送システムのアップグレード、アイデアおよび機会を真のアドバンテージと利点に変えるための信頼性の高い基盤を提供します

ITSアプリケーションは、通常、大量のビデオデータをサポートするためにマルチギガビットアップリンクの、より高い帯域幅を必要とします。一方、自動運転車の増加傾向は、データ需要をさらに高めると予想されます。Moxaの**EDS-4000シリーズ**は、IEC62443-4-2規格に準拠したセキュリティ強化のマネージドイーサネットスイッチで、今後10年間にわたる将来性のある機能を提供する設計がされています。これらのスイッチは、4ギガビットSFPアップリンクポートのオプションを備えたファストイーサネットスイッチで、屋外　PTZカメラなどのデバイスに電力を供給する90 W IEEE 802.3bt PoE ポートをサポートしています。Turbo RingおよびTurbo Chainテクノロジーは、高速ネットワークの冗長性を提供し、常にオペレーションが中断しないことを保証します。一方、オペレーティングシステムの定期的なアップグレードと明確に定義された脆弱性対応とマネージメントにより、動的な輸送市場の可用性とセキュリティを向上します。

さらに、EDS-4000シリーズは、Moxaの産業用ネットワークマネージメントソフトウェアMXviewを介してネットワークデバイスのコンフィギュレーションとマネージメントの一元化をサポートし、コンフィギュレーションを合理化し、トラフィックオペレータのワークロードを軽減します。 最後に、EDR-G9010シリーズセキュアルータと組み合わせることで、重要なネットワークへのサイバーアタックを心配する必要がなくなることでスマートトランスポーテーションの開発により集中することができるようになります。

— 電力変電所への取り組み

変電所は、分散型電力網にとって不可欠な構成要素です。その制御および調整機能は、電力系統全体の安定性に極めて重要です。しかしながら、電力業界は、現在、より多くの再生可能エネルギーの統合や電力需要の増加などの新しいトレンドと課題の出現に直面しています。この中で変電所のデジタル化は、このような新しい動きに対応し、バランスを保ちながらオペレーショナルレジエンスを実現するために必要不可欠なものとなってきています。変電所の改革を成功させるには、基盤となる重要なネットワーク通信の柔軟性と可用性を最適化することが最も重要です。

変電所は、重要なインフラストラクチャであるため、デジタル化にあたっては、以下の3つの点に留意する必要があります。

信頼性:

変電所通信に関しては、可用性と信頼性が非常に重要です。あらゆる種類のパケット損失は、許容することができません。変電所のネットワークデバイスは、非常に過酷な動作環境にインストールされることが多いため、極端な温度や高い電磁干渉に耐えるために十分な耐久性が必要です。同様にネットワークの可用性を確保するために重要なことは、中断を回避し、リカバリータイムを最小限に抑えるための堅牢な冗長性メカニズムが必要です。また、IEEE 1588 Precision Time Protocol (PTP) をサポートするネットワークデバイスは、変電所ネットワークの信頼性にとって非常に貴重な構成要素です。正確な時刻同期により、電圧および電流情報のA/D変換までの機能を統合したマージングユニット内の変電所デバイスに正確なクロックを提供することでオペレータがピンポイントで制御し、問題があれば即座に対応することができます。

セキュリティ:

サイバーセキュリティは、変電所にとって重要な問題として認識されています。ITとOTの間の境界線が急速に薄れていく中で、適切にセグメント化されたネットワークは、重要なネットワーク通信を保護することができます。これには、適切なルータとスイッチ構成の設定、およびファイアウォールルール、アクセス制御、認可および認証ポリシーなどのセーフティメカニズムの管理が含まれます。

変電所ネットワークへのリモートアクセスは、オペレータが広く分散した電力網を監視および維持するための一般的方法ですが脆弱性が指摘されています。公共事業をサイバー脅威や侵害から保護するために、IEC61850認定のVPNソリューションの安全な形式のリモートアクセスによりオペレータは、各リモート変電所のIEDを安全に監視できます。セキュアに強化されたデバイスとセキュアなネットワーク管理機能を組み合わせることで、総合的な多層防御ネットワーク保護を構築し、重要な産業用ネットワークを安全に保つことができます。

簡素化されたマネージメント:

デジタル変電所システムは、24時間365日稼働する必要があります。不要な停止を回避しながらネットワークのマネージメントとオペレーションを向上させるには、リアルタイム監視が最も重要となります。物理的ネットワークトポロジを画面上で可視化する機能は、特に問題が発生した際に大きな利点を提供します。これにより、オペレータは問題の原因を迅速に特定し、すぐに対応できるため、リカバリータイムが大幅に短縮できます。

MOXA®

Case Study

タイのPattaya市がスマートシティの実現に向けて経済成長をパワーアップ

タイのPattaya市は、タイ全土の都市をスマートシティに変えるためのProvincial Electricity Authority (PEA)プログラムのパイロットテストに選定されました。PEAの支援を受けたこのプロジェクトは、電力供給の問題を特定するための手動プロセスからスマートグリッドテクノロジーを使用して停電の発生とその期間を最小限に抑える自動化されたプロセスに移行することで、市の電力網を変革することを目的としています。PEAは、タイの大手エンジニアリングコントラクタであるItalthai EngineeringとMoxaと提携して、このプロジェクトを実施しました。

スマートグリッドの重要な要素は、スマート変電所です。スマート電力インフラストラクチャへのスムーズな移行を実現するためにMoxaは、PEAに対し専門知識とトポロジー設計の提供を行い、様々な30年前の時代遅れの機器ブランド、モデル、タイプのシステムからシンプルで規格化された設計のシステムへの移行を支援しました。

自動運転とリアルタイム通信を実行する新しいスマートインフラストラクチャの変電所が実現しました。さらに、Moxaのネットワークマネージメントソフトウェアによりオペレータは、問題を容易に特定し、迅速に対応することができ、問題発生に対処するために必要な時間を大幅に短縮することができました。アップグレードされた新しいシステムは、シャットダウンを防ぎ、問題が発生した場合のリカバリータイムを短縮することができました。このパイロットプロジェクトで開発されたベストプラクティスは、PEAが他のパイロット都市で同様のアップグレードを展開する際に同じレベルの成功を実現するために使用できるようになりました。

デジタルネットワークで変電所を活性化

Moxaの将来を見据えたネットワークソリューションは、新しいデジタル変電所システムの改修や新規構築に信頼性の高い基盤の提供、運用効率の最大化、そして停止を最小限に抑えます。

デジタル変電所は、変電所の自動化を実現するためにデバイス間のシームレスな通信に大きく依存しています。Moxaの**RKS-G4000シリーズ**産業用ラックマウントスイッチは、多数のリンクを処理し、過酷な条件下で確実に動作できます。これらのIEC61850-3およびIEEE1613認定スイッチは、電磁干渉(EMI)などの様々な環境ハザードに対する堅牢な保護を提供し、重要なパケットを確実に伝送します。高精度の時刻同期を提供するハードウェアベースのIEEE1588PTP機能は、通信の精度を保証します。一方、直感的なユーザインターフェースとMoxaの産業用ネットワークマネージメントソフトウェアとの統合によりオペレータは、ネットワークを完全に可視化し、マネージメントを簡素化することができます。

セキュリティの脅威に対する懸念の高まりに直面している中でRKS-G4000シリーズは、IEC62443-4-2国際セキュリティ規格に合格し、重要なイーサネットネットワークをデバイスレベルから保護します。Moxaの**EDR-G9010シリーズ**産業用セキュアルータを重要なネットワークに統合することで、セキュリティ境界がさらに強化され、最前線のネットワーク防御を実現します。これらのセキュアルータは、電力に特化した様々なプロトコルを検出するネットワークパケットのデータ部分を検査するDeep Packet Inspection (DPI)をサポートしています。また、IEC 61850認定のVPNファイアウォールとしても機能し、複数のギガビットコネクションの多層防御を構築します。これらの機能を組み合わせることでオペレータは、イーサネットネットワークの長期的な機能の信頼性を実現し、デジタル変電所テクノロジーを最大限に活用することができます。

結論:
ネットワークの未来に備える

デジタルトランスフォーメーションは、オペレーショナルレジリエンスを実現しようとするあらゆる業界にとって、努力すべき目標です。シームレスでリアルタイムのデータ通信は、IT/OTコンバージェンスの基盤であり、オンサイトのエンドデバイスとコントロールセンタ間でデータフローをスムーズに実行し、中断のないオペレーションを保証します。Moxaは、産業ネットワークがこの新しい方向に向かって進化していることを目の当たりにしています。これを受けてMoxaは、ネットワークの将来性を再定義しています。このガイドブックに記載されている様々なヒントが、皆様のネットワークオペレーションを円滑にし、**ビジネスを将来にわたって保証**できることを願っています。

Your Trusted Partner in Automation

Moxa は産業オートメーション構築のための信頼できるパートナーです

Moxaは、産業分野における、モノのインターネット（IIoT）の接続を可能にするエッジコネクティビティ、産業用コンピューティング、ネットワークインフラストラクチャソリューション、オートメーションソリューションを提供する世界的なリーディングプロバイダです。産業界で30年以上の経験を誇るMoxaは、世界中で5千万台以上のデバイス接続を提供し、70か国以上に販売代理店およびサービスネットワークを展開しています。Moxaは、産業用通信インフラストラクチャに必要な信頼性の高いネットワークと真摯なサービスを常に提供し続け、永続的なビジネス価値を創造し続けています。

■ アイ・ビー・エス・ジャパン株式会社はMoxaの日本正規代理店です。
■ カタログ・資料請求・お問い合わせは info@ibsjapan.co.jp まで。

IBS Japan
アイ・ビー・エス・ジャパン株式会社

https://www.ibsjapan.co.jp/
E-mail：info@ibsjapan.co.jp
営業時間（土日・祝日を除く）9:00～17:30

■ 本社・厚木センター
〒243-0438　神奈川県海老名市めぐみ町2-2
ViNA GARDENS OFFICE13F
TEL 046-234-9200　FAX 046-234-7861

■ 東京システムセンター
〒151-0053　東京都渋谷区代々木2-4-9
NMF新宿南口ビル2F
TEL 03-5308-1177　FAX 03-5308-1188

■ 大阪営業所
〒532-0003 大阪府大阪市淀川区宮原1-2-6
新大阪橋本ビル4F
TEL 06-7176-9191　FAX 06-7176-9192

IBS-202208Moxa