ANALOG DEVICES
想像を超える可能性を
AHEAD OF WHAT'S POSSIBLE™

IEC 62443シリーズの規格：サイバー攻撃からインフラストラクチャを保護する方法

Christophe Tremlet、業務管理担当ディレクタ

概要

IEC 62443シリーズの規格は、サイバーセキュリティ上のレジリエンスを確立し、重要なインフラストラクチャとデジタル・ファクトリを保護するために設計された一連のプロトコルで構成されていますが、この記事では、この規格の基本的な根拠と利点について解説します。この先進的な規格は広範なセキュリティ層を提供しますが、証明取得にあたっての課題もいくつか生じています。ここでは、産業用自動制御システム（IACS）コンポーネントの証明取得という目標の実現に不可欠な支援を、セキュリティICがどのようにして提供するのかを説明します。

はじめに

ますます巧妙化するサイバー攻撃の可能性が増大しているにもかかわらず、これまでのIACSへのセキュリティ対策の導入は遅々たるものでした。その原因の1つは、これらのシステムの設計者や運用者が依拠すべき共通の基準がなかったことです。IEC 62443シリーズの規格は、より安全な産業インフラストラクチャへの道を開くものですが、これをうまく利用するには企業がその複雑な内容を整理して把握し、これらの規格に伴う新たな課題を理解する必要があります。

リスクにさらされる産業システム

水道、廃水処理、電力網などの重要インフラストラクチャのデジタル化によって、それらのシステムへのアクセスが中断されないことが毎日の生活にとって不可欠になりました。しかし、サイバー攻撃は依然としてこれらのシステムを混乱させる要因の1つとなっており、しかもその数は今後も増えると予想されています[1]。

インダストリ4.0は、高度なネットワークに接続された多数のセンサー、アクチュエータ、ゲートウェイ、アグリゲータを必要とします。ネットワークへの接続が増えればサイバーアタックによるリスクの可能性も増し、これまで以上にセキュリティ対策が重要になってきます。米国サイバーセキュリティ・社会基盤安全保障庁（CISA）のような組織の設置は、サイバー攻撃から重要インフラストラクチャを保護し、そのレジリエンスを確立することの重要性を示すものであると共に、それらの活動への実際の取り組みを示すものでもあります[2]。

なぜIEC 62443なのか

2010年にStuxnetが出現したことによって産業用インフラストラクチャの脆弱性が露呈しました[3]。Stuxnetは、遠方からIACSへの攻撃を成功させられることを示した世界初のサイバー攻撃でした。その後に続いた攻撃により、特定タイプの機器を標的にできるリモート攻撃を通じて、産業用インフラストラクチャに害を及ぼすことができるという認識が確立されました。

政府機関、公共サービス、IACSのユーザと装置メーカーは、IACSを保護する必要があることをすぐに理解しました。結果として、政府機関やユーザは組織的な対策やセキュリティの方針を自然に学び、装置メーカーはハードウェアやソフトウェアによる対応策を研究しました。しかし、以下のような理由からセキュリティ対策は遅れていました。

- インフラストラクチャが複雑であること
- 関係者の興味と関心がそれぞれ異なっていたこと
- 実装と使用可能なオプションが多岐にわたっていたこと
- 測定可能な目標がなかったこと

要するに関係者は、目標とすべき適切なレベルのセキュリティ、言い換えると保護機能とコストが慎重にバランスされたセキュリティというものが曖昧な状態に直面していたのです。

国際計測制御学会（International Society for Automation: ISA）は、ISA99イニシアチブの下で共通の基準を定めるために、ワーキング・グループを発足させました。最終的には、これがIEC 62443シリーズの規格の発表につながります。現在、この一連の規格は、図1に示すように4つのレベルとカテゴリにまと

められています。IEC 62443規格の範囲は非常に多岐にわたっており、組織としての方針、手順、リスク・アセスメント、ハードウェアおよびソフトウェア・コンポーネントのセキュリティなどの項目を包含しています。この広範な規格の範囲によって、その内容を実際の現状に合わせたり、現状を内容に反映させたりすることが可能になっています。加えてISAは、IACSに関わるすべての関係者の様々な興味に対処する際に、包括的なアプローチを採用しました。一般に、セキュリティ上の関心は関係者ごとに異なります。例えば、IPの盗用について考える場合、IACS運用者が興味を寄せるのは製造工程の保護だと思いますが、機器メーカーの興味の対象は人工知能（AI）アルゴリズムをリバース・エンジニアリングから保護することかもしれません。

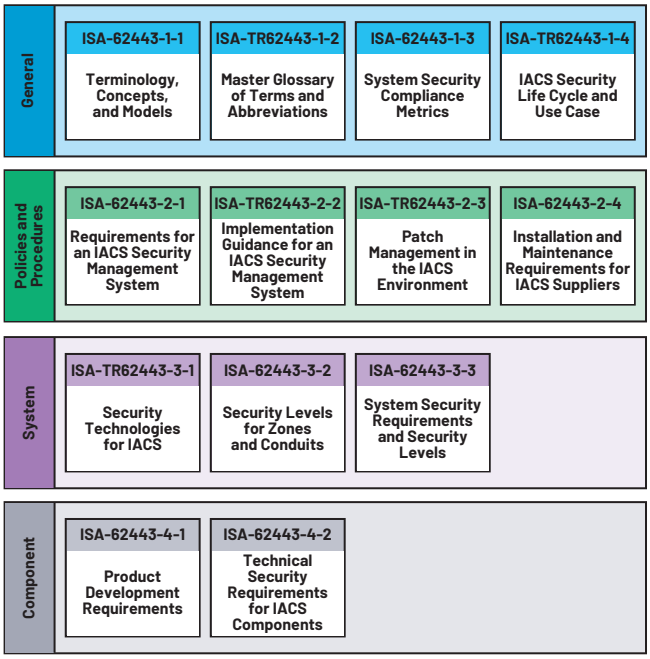

図1　IEC 62443は包括的なセキュリティ規格

また、IACSは本来複雑なものなので、セキュリティに関わるあらゆる要素を考慮することが不可欠です。セキュリティ機器が手順や方針に対応していない場合は、手順や方針だけあっても不十分ですし、高いセキュリティ機能を備えたコンポーネントであっても、その安全な使用法が手順によって適切に定められていなければ無駄になってしまいます。

図2のグラフは、ISAの証明を通じてIEC 62443規格採用の変化を示したものです。予想通り、産業界の主要関係者によって定められた規格は、セキュリティ対策の実装を加速しました。

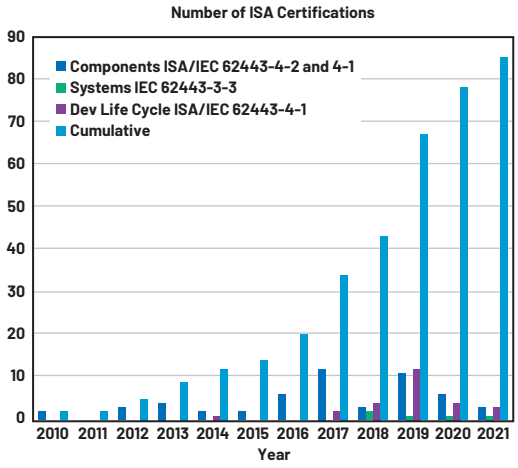

図2　ISA証明数の変化[4]

IEC 62443適合証明の取得：複雑な課題

IEC 62443は非常に範囲の広い効果的な規格ですが、同時にその複雑さに圧倒されてしまうおそれもあります。その量はほぼ1000ページに及びます。サイバーセキュリティ・プロトコルを明確に理解するのは学習曲線が関係してくるような作業で、専門用語を身に着ける以上のことが求められます。IEC 62443内の各セクションに示す概念は相互に依存し合うものなので（図3を参照）、これらのセクションは全体の中の一部として捉える必要があります。

例えば、IEC 62443-4-2に従ってIACS全体を対象としたリスク・アセスメントを行う必要があり、その結果は機器の目標セキュリティ・レベルを決定する条件となります[5]。

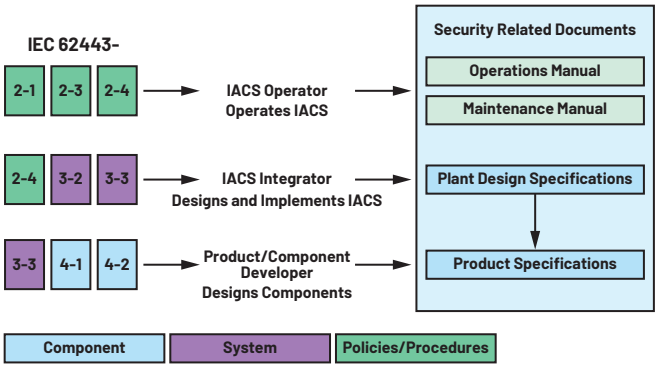

図3　証明プロセスの概要

IEC 62443に準拠した機器の設計

最も高いセキュリティ・レベルにはハードウェア実装が必要

IEC 62443は、図4に示すように分かりやすい言葉でセキュリティ・レベルを定義しています。

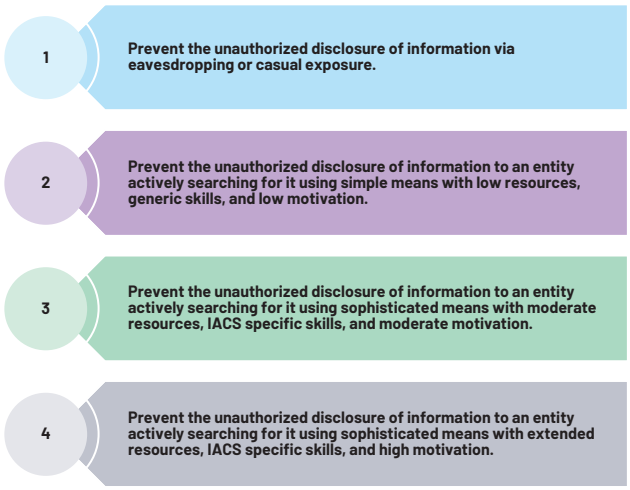

図4　IEC 62443のセキュリティ・レベル

IEC 62443-2-1は、セキュリティ・リスク・アセスメントを義務付けています。このプロセスの結果として、各コンポーネントには目標セキュリティ・レベル（SL-T）が割り当てられます。

図1と図3に示すように、規格のいくつかの部分がプロセスと手順について定めている一方で、IEC 62443-4-1とIEC 62443-4-2はコンポーネントのセキュリティについて定めています。IEC 62443-4-2によるコンポーネント・タイプは、ソフトウェア・アプリケーション、ホスト・デバイス、組込みデバイス、およびネットワーク・デバイスです。IEC 62443-4-2は、それぞれのコンポーネント・タイプに対し、該当するコンポーネント要求事項（CR）と強化要求事項（RE）に基づいて機能セキュリティ・レベル（SL-C）を定めています。表1に、SL-A、SL-C、SL-Tの概要と相互の関係を示します。

表1　セキュリティ・レベルの概要

	目標セキュリティ・レベル	機能セキュリティ・レベル	達成セキュリティ・レベル
略号	(SL-T)	(SL-C)	(SL-A)
定義	システム・レベルのリスク・アセスメントに従って機器が達成すべきセキュリティ・レベル	IEC 62443-4-2に基づいて機器がサポートするCRに従って機器が達成し得るセキュリティ・レベル	機器が達成したセキュリティ・レベル
目標	SL-T ≥ リスク・アセスメントにより決定されたレベル	SL-C ≥ SL-T	SL-A ≥ SL-T

ネットワークに接続されたプログラマブル・ロジック・コントローラ（PLC）の例を見てみましょう。ネットワーク・セキュリティを確保するには、PLCが攻撃の入口とならないようにPLCを認証する必要があります。よく知られているのは公開鍵ベースの認証です。IEC 62443-4-2には次のように規定されています。

- レベル1は公開鍵暗号を考慮していません。
- レベル2には、証明書の署名による確認などの一般的に採用されているプロセスが必要です。
- レベル3と4では、認証プロセスに使用するプライベート鍵のハードウェア保護が必要です。

セキュリティ・レベル2からは、秘密鍵またはプライベート鍵を使用する暗号に基づくメカニズムを含む多くのセキュリティ機能が必要です。セキュリティ・レベル3と4では、多くの場合、セキュリティ機能または暗号機能をハードウェアベースで保護する必要があります。この場合、産業用コンポーネント設計者は、ターンキー型セキュリティICを利用して、以下のような必須メカニズムを埋め込むことができます。

- 安全な鍵保管
- サイド・チャンネル攻撃からの保護
- 以下のような機能を処理するコマンド
  - メッセージの暗号化
  - デジタル署名の計算
  - デジタル署名の確認

これらのターンキー型セキュリティICは、IACSコンポーネントの開発者が複雑なセキュリティ・プリミティブ設計にリソースを費やさなくても済むようにします。セキュリティICを使用するもう1つの利点は、汎用の機能と専用のセキュリティ機能を自然に分離できるという本質的な長所があることです。セキュリティがシステム全体に分散しているのではなく、1つの要素に集中している場合は、セキュリティ機能の強みを評価しやすくなります。更にこの機能の分離には、コンポーネントのソフトウェアまたはハードウェアを変更した後もセキュリティ機能の確認を維持できるという利点もあります。アップグレードを行っても、すべてのセキュリティ機能を評価し直す必要はありません。

更に、セキュリティICベンダーは、PCBレベルやシステム・レベルではアクセスできない、極めて強力な保護手法を実装することができます。これは、極めて巧妙な攻撃に対しても最高レベルの耐性を実現できる強化型のEEPROMやフラッシュ・メモリ、あるいは物理複製困難関数（PUF）などのケースです。総合的に見ると、セキュリティICはシステム・セキュリティを確立するための強力な基礎となります。

エッジのセキュリティ確保

インダストリ4.0を実現するということは、あらゆる場所であらゆる時に検出を行うことを意味します。したがって、より多くのエッジ・デバイスを展開する必要があります。IACSエッジ・デバイスには、センサー、アクチュエータ、ロボット・アーム、PLCとそのI/Oモジュールなどが含まれます。各エッジ・デバイスは高度にネットワーク化されたインフラストラクチャに接続されるので、攻撃の潜在的な入口となります。攻撃表面はデバイス数に比例して広がりますが、それだけに止まらず、多様なデバイスの組み合わせは本質的に攻撃ベクトルの種類を拡大します。アプリのセキュリティおよび侵入テスト・ベンダーであるSEWORKSのCTOを務めるYaniv Karta氏は、「既存のプラットフォームには利用可能な攻撃ベクトルが多数存在し、エンドポイントもエッジ・デバイスも脅威にさらされることが多くなる」と語っています。一例として、複雑なIACSでは、すべてのセンサーが同じベンダーのものとは限らず、マイクロコントローラ、オペレーティング・システム、あるいは通信スタックに関するアーキテクチャが共通しているわけでもありません。また、それぞれのアーキテクチャが固有の弱点を抱えている可能性があります。MITRE ATT&CKデータベース[6]やICS-CERTアドバイザリ[7]が示すように、結果としてIACSには脆弱性が蓄積され、それによって脅威にさらされることになります。

更に、より多くのインテリジェンス機能をエッジに組み込むという産業用モノのインターネット（IIoT）のトレンド[8]によって、システム的な決定を自律的に下せるようなデバイスが開発されるように

なっています。したがって、これらの決定が安全、システムの動作、その他にとって非常に重要であるということを踏まえると、デバイスのハードウェアとソフトウェアを信頼できるものにすることが更に重要になります。加えて、デバイス開発者のR&D IP投資を盗用から保護すること（例えばAIアルゴリズムに関するものなど）は例外なく考慮すべき事項であり、これは、ターンキー型セキュリティICがサポートできる保護手段を導入するという決定の主要な動機となり得ます。

もう1つの重要なポイントは、不十分なサイバーセキュリティは機能安全に悪影響を及ぼすということです。機能安全とサイバーセキュリティの関係は複雑であり、これについて論じようとすると別途記事を書かなければならないくらいですが、とりあえず以下の点を強調しておくことができます。

- IEC 61508：電気式／電子式／プログラマブル電子式の安全関連システムの機能安全には、IEC 62443に基づくサイバーセキュリティ・リスクの分析が不可欠です。
- IEC 61508は主としてハザードとリスクの分析に焦点を当てており、サイバーセキュリティに関わる事象が深刻なものであった場合は、その都度セキュリティに対する脅威の分析と脆弱性の分析を事後に行うよう義務付けています。

上に挙げたIACSエッジ・デバイスは組込みシステムです。IEC 62443-4-2は、悪意あるコードからの保護メカニズム、安全なファームウェア・アップデート、物理的タンパリングの防止と検出、信頼の基点のプロビジョニング、ブート・プロセスの完全性などのシステムについて、具体的な要求事項を定めています。

ADIのセキュア・オーセンティケータによりIEC 62443の目標を達成

アナログ・デバイセズのセキュア・オーセンティケータはセキュア・エレメントとも呼ばれ、実装の容易さと良好なコスト効率を念頭に、これらの要求を満たせるように設計されています。ホスト・プロセッサに必要なすべてのソフトウェア・スタックを備えた固定機能ICが、ターンキー・ソリューションです。

結果としてセキュリティの実装はアナログ・デバイセズに委託する形となり、コンポーネントの設計者は本来の業務に集中することができます。セキュア・オーセンティケータは本質的に信頼の基点であり、ルート鍵や秘密情報、そしてファームウェア・ハッシュなどの装置状態を示す要注意データを、安全かつ改ざんできない形で保存します。これらのオーセンティケータは、認証、暗号、セキュア・データ・ストレージ、ライフサイクル管理、セキュア・ブート／アップデートを含め、広範な暗号機能のセットを備えています。

ChipDNA™の物理複製困難関数（PUF）技術は、従来のようにフラッシュやEEPROMに暗号鍵を保存するのではなく、ウェーハの製造過程で自然に発生する無作為の変動を利用して暗号鍵を作成します。利用されるこの変動はごくわずかなものなので、チップのリバース・エンジニアリングに使われる極めて高価かつ高度な侵入技術（走査型電子顕微鏡、収束イオン・ビーム、マイクロプロービングなど）でも、鍵を取り出すことはできません。集積回路以外でこのレベルの抵抗を実現できる技術はありません。

セキュア・オーセンティケータは、証明書および証明書チェーンを管理することもできます[9]。

加えて、アナログ・デバイセズは非常に安全性の高い鍵と証明書の事前プログラミング・サービスを工場で提供しているので、受託メーカー（OEM）はプロビジョニング済みのデバイスを受け取って、それを自社の公開鍵インフラストラクチャ（PKI）にシームレスに組み込んだり、オフラインPKIをイネーブルしたりすることができます。高い信頼性を備えたその暗号機能は、安全なファームウェア・アップデートとブートを可能にします。

セキュア・オーセンティケータは既存の設計に高度なセキュリティを追加するのに最適のオプションです。BOMコストを低く抑えながら、セキュリティ確保を目的とするデバイスのアーキテクチャ変更に必要なR&Dの負担を軽減します。例えば、メインのマイクロコントローラを変更する必要はありません。一例を挙げると、DS28S60およびMAXQ1065セキュア・オーセンティケータは、図5に示すように、IEC 62443-4-2のすべてのレベルの要求に対応しています。

DS28S60とMAXQ1065は3mm × 3mmのTDFNパッケージを使用しているので、スペースの制約が厳しい設計に適しています。また、消費電力が少ないので、消費電力が厳しく制限されるエッジ・デバイスにも最適です。

表2　DS28S60とMAXQ1065の主要パラメータの概要

デバイス機能	DS28S60/MAXQ1065
動作温度	–40°C～+105°C
ホスト・インターフェース	SPI (I^2Cは開発中)
電源電圧	1.62V～3.63V
最大アクティブ電流	3mA
アイドル電流（代表値、25°C）	0.4mA
パワーダウン電流（25°C）	100nA

IEC 62443-4-2の要求に対応するセキュリティ機能を備えたマイクロコントローラが、IACSコンポーネント・アーキテクチャに既に組み込まれている場合でも、鍵や証明書を配布するためにセキュア・オーセンティケータの利点を生かすことができます。秘密IC認証情報を扱うためには高価な製造施設が必要ですが、これによってOEMやその契約メーカーによる投資の負担が軽減されます。このアプローチは、マイクロコントローラに保存された鍵を保護し、JTAGなどのデバッギング・ツールを通じて抜き出されるのを防ぐことにもなります。

ポートフォリオの製品構成と製品の詳細はanalog.com/en/product-category/secure-authenticators.htmlで参照できます。

Secure Authenticator Features	IEC 62443 High Level Requirements	SL1	SL2	SL3	SL4
ECDSA/HMAC/AES MAC	Communication Integrity	X	X	X	X
Secure Boot	System Integrity: Boot Firmware, Configuration Data Integrity	X	X	X	X
AES Encryption	Data Confidentiality (at Rest, in Transit)	X	X	X	X
ECDSA Verification	User Authentication	X	X	X	X
ECDSA Signature/Verification	Device Authentication		X	X	X
Dedicated ECDSA/SHA/AES Engines	Hardware Security for Authentication			X	X
x.509 Certificate Verification	Certificate-Based Authentication, Standard PKI		X	X	X
ECDSA Signature	Protection of Audit Information		X	X	X
ECDSA Signature	Multifactor User Authentication			X	X
External Tamper Input	Tamper Resistance and Detection, Notification of Attempts			X	X
Security IC Firmware Update + System	Secure Updates (Security Module and System)		X	X	X
ChipDNA-Based Secure Storage	Hardware Secure Storage for Private Keys			X	X

図5　セキュア・オーセンティケータの機能とIEC 62443の要求事項の対応

まとめ

IEC 62443規格の要求事項をまとめ、それを採用することによって、IACSの関係者は信頼できる安全なインフラストラクチャへの道を開きました。セキュア・オーセンティケータは、ハードウェア・ベースのセキュリティを必要とするIEC 62443規格準拠コンポーネントの未来を支える基盤です。OEMは、セキュア・オーセンティケータが自社の求める証明を実現する助けとなることを理解し、自信を持って設計を行うことができます。

参考資料

1　Lorenzo Franceschi-Bicchierai. “Ransomware Gang Accessed Water Supplier’s Control System.” Vice, August 2022.

2　“Protecting Critical Infrastructure.” Cybersecurity and Infrastructure Security Agency.

3　Bruce Schneier. “The Story Behind The Stuxnet Virus.” Forbes, October 2010.

4　“ISASecure CSA Certified Components.” ISASecure.

5　Patrick O’Brien. “Cybersecurity Risk Assessment According to ISA/IEC 62443-3-2.” Global Cybersecurity Alliance.

6　“ATT&CK Matrix for Enterprise.” MITRE ATT&CK®.

7　“Cybersecurity Alerts & Advisories.” Cybersecurity and Infrastructure Security Agency.

8　Ian Beavers. “インダストリアルIOTのセンシングと計測：エッジ・ノード” Analog Devices, Inc., August 2017.

9　“Trust Your Digital Certificates—Even When Offline.” Design Solutions, No.56, May 2017.

著者について

Christophe Tremletは、EMEA地域におけるセキュア・オーセンティケータ製品ラインの業務管理担当ディレクタです。セキュリティICに関係して25年以上の経験を持ち、製品エンジニアリングとアプリケーションの管理を行ってきました。Christopheは、セキュア・マイクロコントローラに特化した新興企業であるInnova Cardで最高技術責任者を務めた経験があり、マキシム・インテグレーテッドではエンジニアリングと営業を担当していました。Thales社でマーケティングおよびセールス担当ディレクタとして3年間を過ごした後に、アナログ・デバイセズへ入社しました。

＊英語版技術記事はこちらよりご覧いただけます。

TA24493-4/23