IEC62443

ISA-62443-2-1	IEC 62443-2-1	Requirements for an IACS Security Management System	WG2	TG1	Published, Under Revision
ISA-TR62443-2-2	IEC/TR 62443-2-2	Implementation Guidance for an IACS Security Management System	WG2	TG2	Proposed
ISA-TR62443-2-3	IEC/TR 62443-2-3	Patch Management in the IACS Environment	WG6	N/A	Approved
ISA-62443-2-4	IEC 62443-2-4	Requirements for IACS Solution Suppliers	IEC TC65/WG10	N/A	Draft for Comment
ISA-TR62443-3-1	IEC/TR 62443-3-1]	Security Technologies for IACS	WG1	N/A	Published, Under Revision
ISA-62443-3-2	IEC 62443-3-2	Security Risk Assessment and System Design	WG4	WG4TG3	Draft for Comment
ISA-62443-3-3	IEC 62443-3-3	System Security Requirements and Security Levels	WG4	WG4TG2	Published
ISA-62443-4-1	IEC 62443-4-1	Product Development Requirements	WG4	WG4TG6	Draft for Comment
ISA-62443-4-2	IEC 62443-4-2	Technical Security Requirements for IACS Components	WG4	WG4TG4	Under Development

現場管理

システム

制御製品

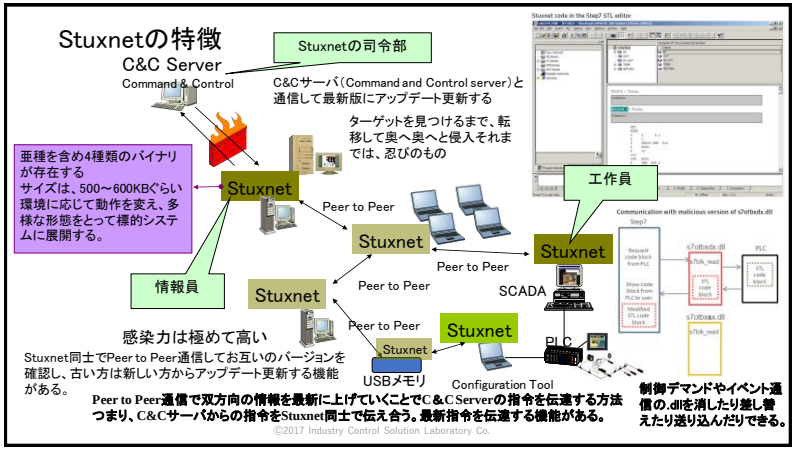
http://isa99.isa.org/ISA99%20Wiki/WP_List.aspx

制御システムを標的にしたサイバー攻撃事例

- 攻撃手法も高度技術を使用しており、組織的サイバー攻撃兵器としても開発し、取引されている。
- 対策を考えるには、攻撃対象、攻撃武器、侵入経路、攻撃内容、被害状況などの具体的情報が必要となる。

	2008	2010	2014	2014	2015	2016.8～
発生場所	トルコ	イラン	ドイツ	韓国	ウクライナ	イラン
攻撃対象	石油パイプライン	核燃料施設	製鉄所	原子力発電所	電力変電所	製油所 天然ガス基地など
攻撃武器	不明	Stuxnet	トロイの木馬	外部操作を可能にしたマルウェア	スピアフィッシングメールで感染	不明 サイバー攻撃ではないかと疑われている
侵入経路	監視カメラの通信ソフト	USBメモリ	電子メールの添付ファイル	インターネットからの侵入	インターネットからの侵入	不明
攻撃内容	パイプ管圧への過剰な負荷	遠心分離機への過剰な負荷	溶鉱炉の異常停止	マルウェアを使った遠隔操作	UPSを攻撃	不明
被害状況	パイプライン爆発	遠心分離機を破壊	生産設備の損傷	実被害なし	広いエリアで6時間停電	石油貯蔵タンク爆発火災（10月）

Stuxnetの特徴



PLC Blaster Worm：コントローラに仕込まれるマルウェア

- PLCのコンフィギュレーションツールやPLCにつながるポータルツールからWormをPLCに送り込み、PLCからPLCに感染させることもできる。PLCをネット上のC&Cサーバーの支配下におくこともできる。

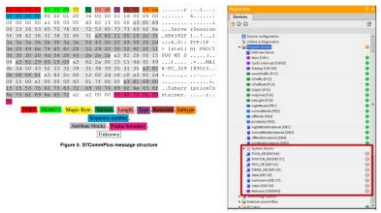


Figure 14. TIA portal exposes the worm

資料は、Asia Black Hat 2016の発表PDFより引用

対策は、IEC62443-4-1の更新版でも対策あり

Vendor	Product	Ethernet	Transfer TCP/UDP	TCP/IP Functions
Siemens	S7-300	Ja	Ja	Ja
Siemens	S7-400	Ja	Ja	Ja
Siemens	S7-1200	Ja	Ja	Ja
Siemens	S7-1500	Ja	Ja	Ja
Mitsubishi Electric	MELSEC iQ-R	Ja	Ja	Ja
Mitsubishi Electric	MELSEC iQ-F	Ja	Ja	Ja
Mitsubishi Electric	MELSEC-Q	Ja	Ja	Ja
Mitsubishi Electric	MELSEC-L	Ja	Ja	Ja
Mitsubishi Electric	MELSEC-F	Ja	Ja	Nein
Mitsubishi Electric	MELSEC-QS/WS	Ja	Ja	Nein
Schneider Electric	Modicon Easy M	Nein	Nein	Nein
Schneider Electric	Modicon M	Ja	Ja	Nein
Schneider Electric	Modicon LM	Ja	Ja	Nein
Schneider Electric	Modicon Premium	Ja	Ja	Nein
Schneider Electric	Modicon Quantum	Ja	Ja	Nein
Schneider Electric	Preventa XPS Quantum	Ja	Ja	Nein
Rockwell Automation	ControlLogix	Ja	Ja	Ja
Rockwell Automation	CompactLogix	Ja	Ja	Ja
Rockwell Automation	MicroLogix	Ja	Ja	Ja
Rockwell Automation	SmartGuard 600	Ja	Ja	Nein
Rockwell Automation	SLC 500	Ja	Ja	Ja
Rockwell Automation	PLC-5	Ja	Ja	Ja
Rockwell Automation	GuardPLC	Ja	Ja	Nein
Rockwell Automation	Micro800	Ja	Ja	Nein

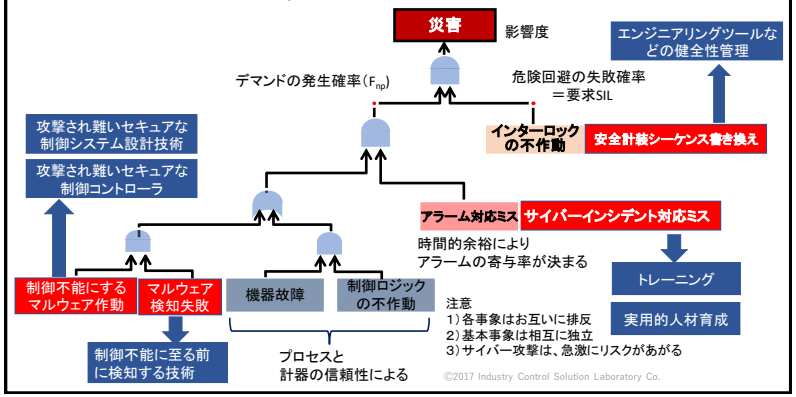
制御システムの攻撃方法

- 定常時／非定常時の操作ミス（誤判断・誤操作）を誘発する
  - 制御ネットワークを使えなくする
    - ネットワークのServerかPCからＤＯＳ攻撃を加えて通信エラーを起こす
  - 現場で発生していないアラームを発報させる
    - ＤＣＳやＳＣＡＤＡの監視制御のアラームデータに新しい警報を追加
    - 過去起きたアラームを再度表示
  - 現場で発生しているアラームを監視画面に表示させない
    - アラームデータが上がってきてもデータベースに書き込まない
    - アラームデータを消去
- 直接攻撃
  - SCADAの制御動作をスローダウンもしくは機能停止させる
    - SCADA ServerにWormを送り込みフル稼働させる：Worm
    - 使用しているファイルを暗号化する：Ransomware
    - 制御データがSCADAに上がってこなくする：通信ドライバを消去、データベースを消去
  - 制御コントローラを機能停止する
    - コントローラの正常レジスタをOFFにする：PLC Blaster Worm
    - コントローラの停止レジスタをONにする：PLC Blaster Worm
  - 実際にメカニックストレスを与える
    - 制御コントローラにストレスデマンドを送り込む：Stuxnet

要因

- □ 業務系ネットワークと生産系ネットワークを分けていない
- □ セグメント／ゾーン設計ができていない
- □ 冗長化システムは、ハードウェア故障対策しか考慮されていない（サイバー攻撃についての冗長化になっていない）
- □ エンジニアリングツールのセキュリティ管理をしていない
- □ インシデント検知機能が無い
- □ インシデント対応トレーニングをしていない
- □ 回復作業のトレーニングが実施されていない（すべてベンダ任せ）
- □ 脆弱性情報が管理されていない
- □ パッチバージョン管理をしていない

安全のFTA（Fault Tree Analysis）に制御システムセキュリティ・リスクを加える



制御セキュリティを施したシステム設計プロセス

1. 事業要求仕様の確認　制御セキュリティ対策要求仕様
2. 基本システム構成設計　制御システムネットワーク設計
3. リスクアセスメントの第一段階
   - サイバーリスクアセスメント
     - サイバーリスク特定・分析・評価
4. 対策を考慮した基本システム構成設計
   - サイバーリスクアセスメント
     - サイバーリスク低減
5. リスクアセスメントの第二段階
   - サイバーリスクアセスメント
     - サイバーリスク再評価
6. 製造手配　発注仕様書、セキュリティ性能試験要求
7. エンジニアリング　制御セキュリティシステム設計、脆弱性対策、インシデント検知・対応・回復
8. システム評価試験　試験方案、試験結果評価
9. 現場調整・チューニング・試運転　セキュリティ設定・チューニング、インシデント対応確認

ここで実施する作業を取り上げてリモートサービスシステムを分析の一部を紹介

制御セキュリティを施したシステム設計プロセスの内容は、eICSの講座で受講

実践的制御セキュイリティ講座eICSカリキュラム