制御ベンダ／装置ベンダ／Sierに求められるセキュリティ対策についての提言

制御システムセキュリティ検討タスクフォース
普及啓発WG座長
IAF/VEC事務局長　村上正志

自己紹介：村上正志

- **1977年～1991年：日本ﾍﾞｰﾚｰ株式会社のシステムエンジニア**
  - 火力発電所のボイラ自動制御装置、プラント監視制御装置のシステム設計：
    広野2号、苫小牧1号、渥美3/4号、知多第二火力1/2号、東扇島1号、秋田、東新潟、川内、仙台、西名古屋、海南、新小倉、阿南、御坊、姉ヶ崎、五井、袖ヶ浦、高砂、松島、下関、玉島、尼崎、伊達、勿来、港、海外プラントなどの建設、改修などを担当
  - 空気式制御装置⇒電子式アナログ制御装置⇒DDC（16bit⇒32bit⇒64bit）
  - 高速故障診断装置を企画、開発、37セット納入
- **1991年～1994年：画像処理VMEボードメーカーに従事**
  - 大型カラー印刷機の画像処理、大蔵省印刷局の検査装置などのシステムコンサルティング
- **1994年～現在：株式会社デジタル**
  - SCADA製品の事業戦略企画推進担当
  - SE部長
  - 1999年～現在VEC事務局長
- **現在担当している標準化団体**
  - **経済産業省商務情報政策局主催制御システムセキュリティ対策タスクフォース委員**
    - **普及啓発ワーキング座長**
  - 日本OPC協議会企画副部会長
  - PLCopen　Japanの幹事ﾒﾝﾊﾞｰ、OPC WG主査
  - IAF（Industrial Automation Forum）運営委員会幹事
  - NECA：ﾌﾟﾛｸﾞﾗﾏﾌﾞﾙ表示器専門技術委員会委員
  - グリーンIT推進協議会正会員
  - 日本能率協会主催計装制御技術会議企画委員会委員、など

サイバー攻撃の脅威が現実になる

- **大きな事故にはつながっていないが、現場の制御システムにまで脅威が来ている現実**

- サイバー攻撃により企業が抱えるリスクは高くなっている。
- 制御システムセキュリティ対策を施していく必要がある。

実被害金額の試算は、生産操業できなかったことで失った売り上げ金額と復旧工事費用とそれに関わった人件費の総額になる。
復旧に時間がかかればかかるほど大きくなる。

トータルリスク管理項目例

- **災害勃発**
  - **地震、津波、火山活動、洪水による直接／間接被害**
  - **災害によるインフラ機能停止・就業不可**
- **サプライチェーン支障**
  - **戦時・クーデター・政変による素材調達／流通不可**
  - **価格高騰**
  - **ストライキ**
- **爆発、火災勃発**
- **サイバー攻撃による被害　⇒　操業停止による損害**
- **感染症流行**

- 米国では、原子力発電所から化学工場、水道施設がサイバー攻撃されている。
- サイバーテロ集団組織が増えている。
- 日本国内でも、実被害が出ている。
  - 石油プラントの生産情報管理系サーバーがマルウェアに汚染され、10日間ほど生産停止。
  - 半導体工場で生産監視制御系ネットワークのPCがマルウェアに汚染され、復旧作業に1ヶ月間ほど要した。
  - 企業の生産機密情報が海外のサイトに出ていた。

サイバー攻撃の目的と手法

業界内シェアが高い制御システム製品ほど社会的影響が大きい。

2011年
・防衛産業の日本企業の約80台のサーバーやパソコンから50以上のウィルスに感染した。
・Stuxnetがサイバー兵器として応用されている。

2010年
・Stuxnet登場
イランのウラン濃縮施設の遠心分離機の制御装置8400台のうち、4600台ほどが、Stuxnetによって、故障停止させられた。
フィンランドのウラン濃縮施設も同じ制御システムであったことで、被害受ける。

2009年以前
・2003年1月、米国Davis Besse原子力発電所のシステムをSlammerが停止させた。

2003年3月ハッキングによって、100台以上の車が動かなくなる。

2003年8月、米国東部の鉄道の信号管理システムがW32/Blasterに感染し、列車を停止させる。

2005年8月、ダイムラークライスラーの13の自動車工場をZotobワームが操業停止に追い込む。

サイバーテロの目的
① 社会パンデミックを起こす。
✧ 市場混乱、社会混乱
✧ 競合攻撃、株価操作
② 競合情報を入手・売却
✧ 企業機密情報搾取してコピー製品を造る企業へ売却。
③ 企業乗っ取り工作
✧ 企業脅迫

分類
① 企業機密情報を搾取：Duqu
✧ 製造製品開発機密情報、制御製品機密情報
② 企業機密情報を書き換え：ワーム、マルウェア
③ 制御操作して制御施設を破壊：Stuxnet

現象
① 知らないうちに製造製品の機密情報が外部のWebに公開されている。
② 生産情報が書き換えられている。
✧ 生産数量、品質レシピ、品質検査基準値
③ 制御システムを操作
✧ 制御システムが暴走、停止
✧ 制御施設が破壊される。爆発、火災
④ リフレッシュ作業でのリスク
✧ 危険な作業を伴う
✧ その間、生産操業ができない⇒収入が無い

Stuxnet

Stuxnetの司令部

C&C Server
Command & Control

C&Cサーバ(Command and Control server)と通信して最新版にアップデート更新する

ターゲットを見つけるまで、転移して奥へ奥へと侵入
それまでは、忍びのもの

亜種を含め4種類のバイナリが存在するサイズは、500～600KBぐらい
環境に応じて動作を変え、多様な形態をとって標的システムに展開する。

Stuxnet

Peer to Peer

Stuxnet

工作員

Stuxnet

Peer to Peer

情報員

Peer to Peer

Stuxnet

SCADA

Peer to Peer

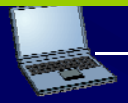
Stuxnet

感染力は極めて高い

Stuxnet同士でPeer to Peer通信してお互いのバージョンを確認し、古い方は新しい方からアップデート更新する機能がある。

Stuxnet

USBメモリ



Configuration Tool

PLC

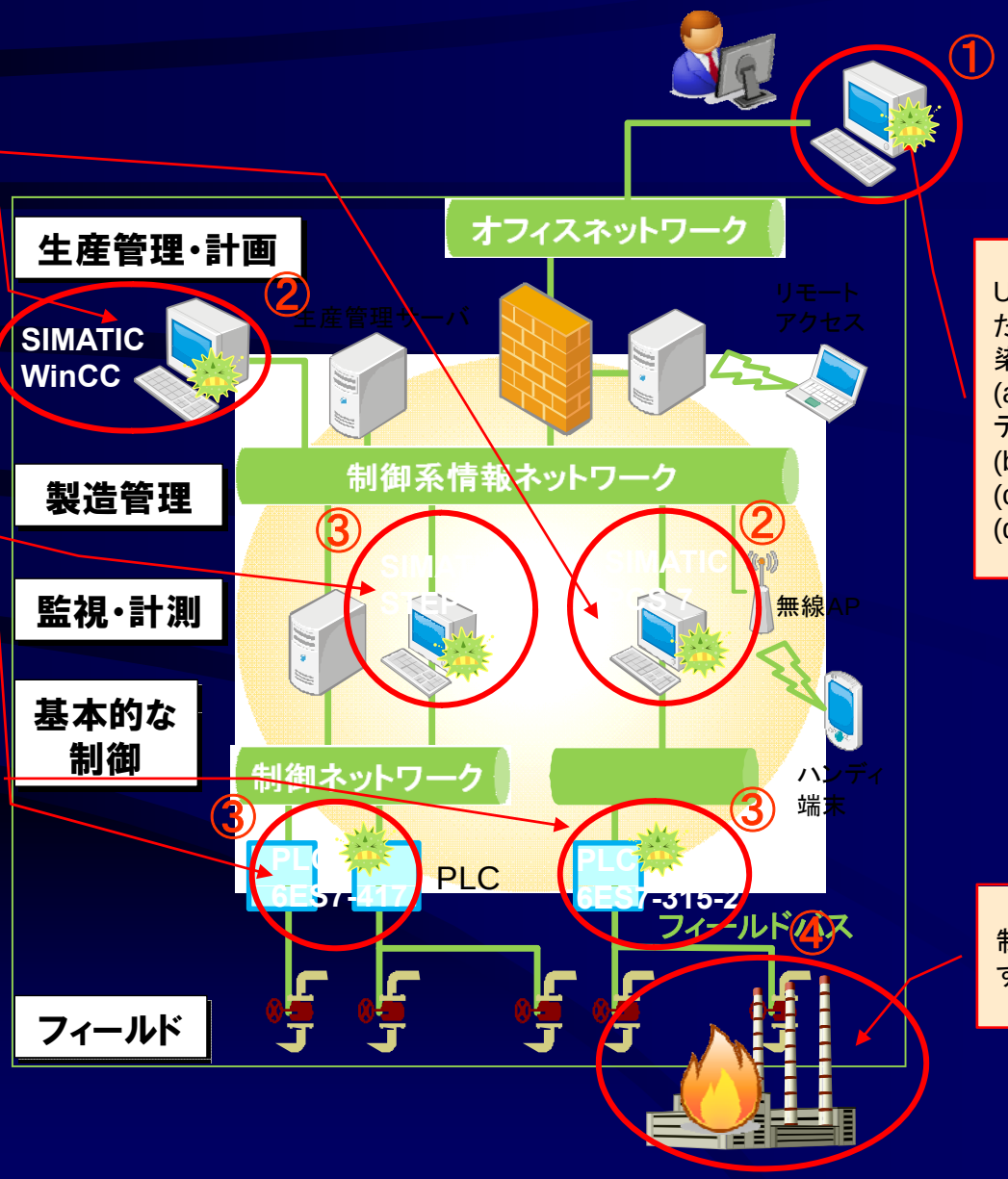
Peer to Peer通信で双方向の情報を最新に上げていくことでC＆C Serverの指令を伝達する方法
つまり、C&Cサーバからの指令をStuxnet同士で伝え合う。最新指令を伝達する機能がある。

Stuxnet攻撃例

独シーメンス社製遠隔監視ソフトウェア（SIMATIC WinCC or SIMATIC PCS 7）の脆弱性を悪用して、SQL コマンド経由で SIMATIC WinCC あるいは、SIMATIC PCS 7 の稼働する Windows システムに感染

独シーメンス社製ソフトウェア (SIMATIC STEP 7) を悪用して、PLC (プログラマブルロジックコントローラ) に悪質なコードの書き込み

独シーメンス社製エンジニアリングツール (SIMATIC STEP 7) を悪用して、PLC (プログラマブルロジックコントローラ) に悪質なコードの書き込み



ウィルスに感染したUSBメモリ

USBメモリやインターネットを通じた情報システムへのウイルス感染
(a)USB などのリムーバブルメディア経由
(b)ネットワーク経由
(c)ファイル共有経由
(d)感染 PC において権限昇格

制御システム上にある装置に対する攻撃の実行

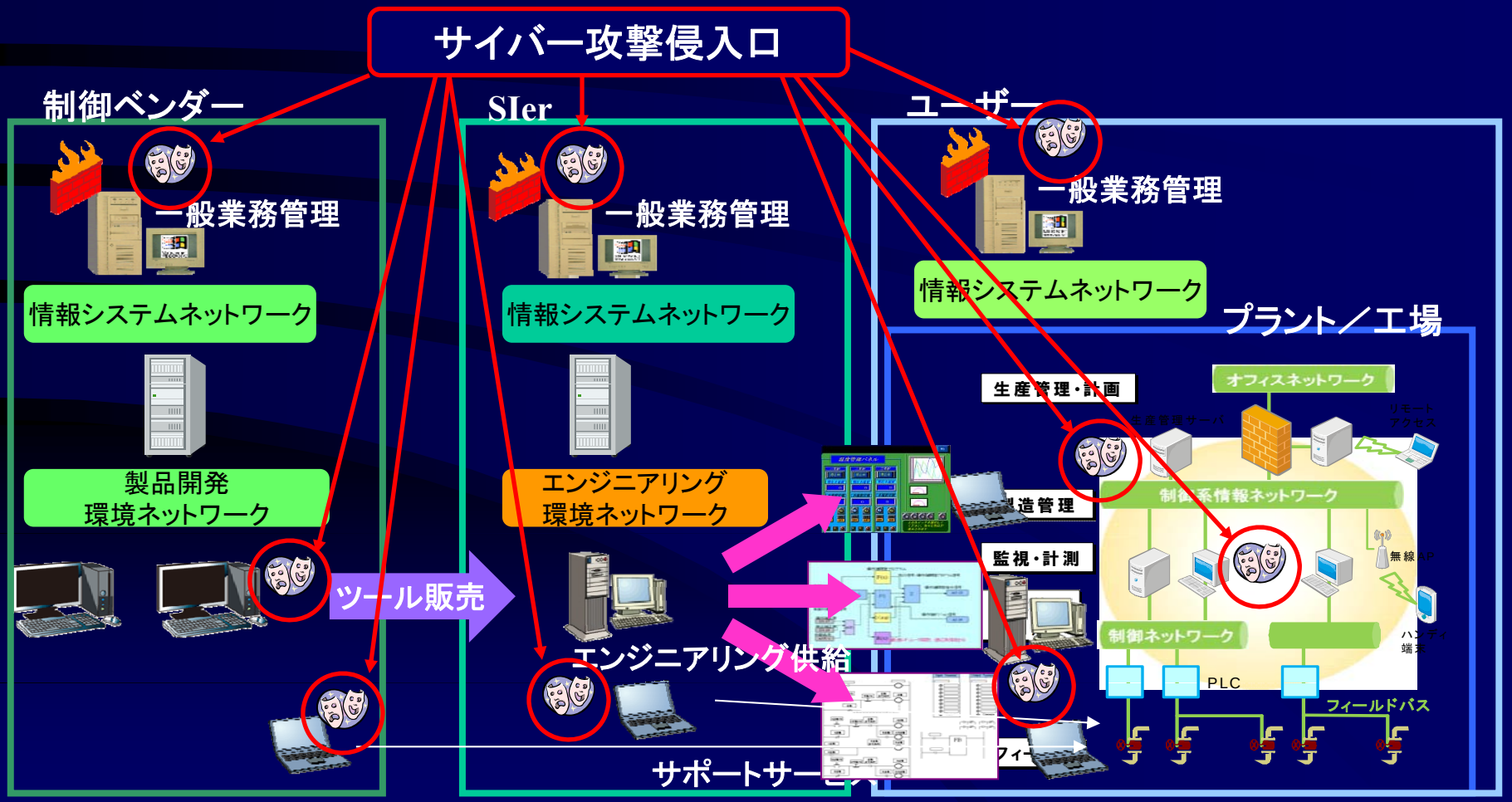
Agenda

1. 現場の防衛の支えとなるベンダの役割
2. 制御製品に求められるセキュリティ対応
3. 製品開発の品質保証に求められるセキュリティ対応
4. 制御製品開発環境の健全性
5. 現場へのサービス対応について
6. インシデント対応時のベンダへのお願い

7. 極めの制御システムセキュリティ対策とは、？

1. 現場の防衛の支えとなるベンダの役割

- 社会インフラ、ライフライン、基幹産業の安全を支えている供給ベンダの役割は、重い。
- その業界内でシェアが高いほど、重要制御製品対象となる。



ユーザー視点の課題／ニーズ

現場防衛力アップにつながるものが欲しい。

- SSATは、セキュリティ認識を持って対処できるかの評価ツール
- 現場で欲しいのは、現場の実践的防衛力アップにつながるツール：どのような取組みが必要かをまとめたものがあって、それを身につけさせてくれて、内容を理解したかどうかの確認ツール

- 事業リスクの理解
- 継続した管理をしているか
- 防御体制の質
- マルウェア対策認識
- 内部からの脅威認識
- セキュリティ管理レベル
- バックアップと回復のしなりお
- 物理的セキュリティ管理
- 対応能力の確立
- サードパーティ・リスク管理
- プロジェクトへの参画
- 調達関係

運用管理レベルを評価する

世界レベルとの比較が可能
レベルをあげるには、トレーニングセンターで受講

CSET
制御システム設計評価

SSAT
管理認識評価

IEC62443-1
概要・コンセプト

IEC62443-2
管理・運用・プロセス
製造組織要件
セキュリティ機能要件
受入テスト要件
メンテ／保守要件

人

- 経営者／工場長
- 計装エンジニア
- 現場責任者
- 現場作業者
  ボードマン／フィールドマン／メンテナンス作業者

啓発
情報
育成

日本ユーザが求めるもの

カイゼンできる人を育てる

サイバー攻撃リスクに対する投資が重要であること

IEC62443の知識と現場の応用力強化
制御製品の脆弱性情報
現場でのインシデント対応設計
セキュリティ対策した制御システム設計と管理の手法

作業上のセキュリティ認識アップ
作業上のビールス感染を防ぐことと不具合発見でセキュリティ問題の可能性を含むという認識

現場の実践的防衛力アップ
全員がトレーニングを受けるには、時間も経費もかかる。そんな余裕は無い。
ボードマン、フィールドマンやメンテナンス作業者に求めるセキュリティ問題認識は、作業上のビールス感染を防ぐことと不具合発見でセキュリティ問題の可能性を含むという認識

SIer（計装ｴﾝｼﾞﾆｱ）視点の課題／ニーズ

制御システムエンジニアリングの実践的防衛力アップにつながる技術を身につけたい

- 現場の制御システムの実践的防衛力アップ
- 健全なエンジニアリング環境の確保⇒整備⇒管理
- 実践的インシデント対応技術とその対応作業のための制御システム設計手法

制御システムを評価する

IEC62443-1
概要・コンセプト

IEC62443-2
管理・運用・プロセス

製造組織要件
セキュリティ機能要件
受入テスト要件
メンテ／保守要件

IEC62443-3
通信プロトコル
外部インターフェース
システム設計技術

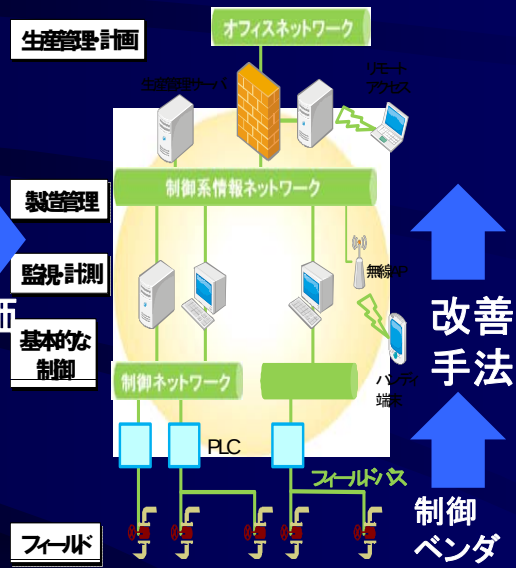
IEC62443-4
コンポーネント・デバイス

IEC62443

評価

評価ツール：Achilles

制御システム



改善手法

制御ベンダ情報

制御システムを改善する

日本のSIerが求めるもの

新たな課題への経営者の理解

IEC62443の知識と現場の改善手法
制御製品の脆弱性情報
制御製品のｾｷｭﾘﾃｨ対策情報
制御システムインシデント対応技術
安全操業を継続するためのｾｷｭﾘﾃｨ対策
強化した制御システムの設計方法と管理方法

エンジニアリング環境の健全化

世界レベルとの比較が可能
レベルをあげるには、トレーニングセンターで受講

制御システムセキュリティ技術にも、国際的競争力が求められる。

日本の計装エンジニアリングは、国際的にも評価が高い。そこに実践的ｾｷｭﾘﾃｨ対策を施した制御システム設計エンジニアリング力を身につけて優位にビジネスを継続したい。

制御ベンダ視点の課題／ニーズ

- **サイバー攻撃に対処できる制御製品開発**
  - クリーンな制御製品開発環境の整備
  - サイバー攻撃を想定した品質検査
  - 高度セキュア化技術の制御製品応用
- **インシデント対応の情報公開対応**

制御製品を評価する

IEC62443-1
概要・コンセプト

IEC62443-2
管理・運用・プロセス

製造組織要件
セキュリティ機能要件
受入テスト要件
メンテ／保守要件

IEC62443-3
通信プロトコル
外部インターフェース
システム設計技術

IEC62443-4
コンポーネント・デバイス

評価ツール：Achilles

IEC62443

標準規格

評価

制御製品

基本設計手法

セキュア技術アップ

セキュリティ対応強化制御製品を開発する

日本の制御ベンダが求めるもの

国内外で通用する日本優位の制御製品開発とサービス

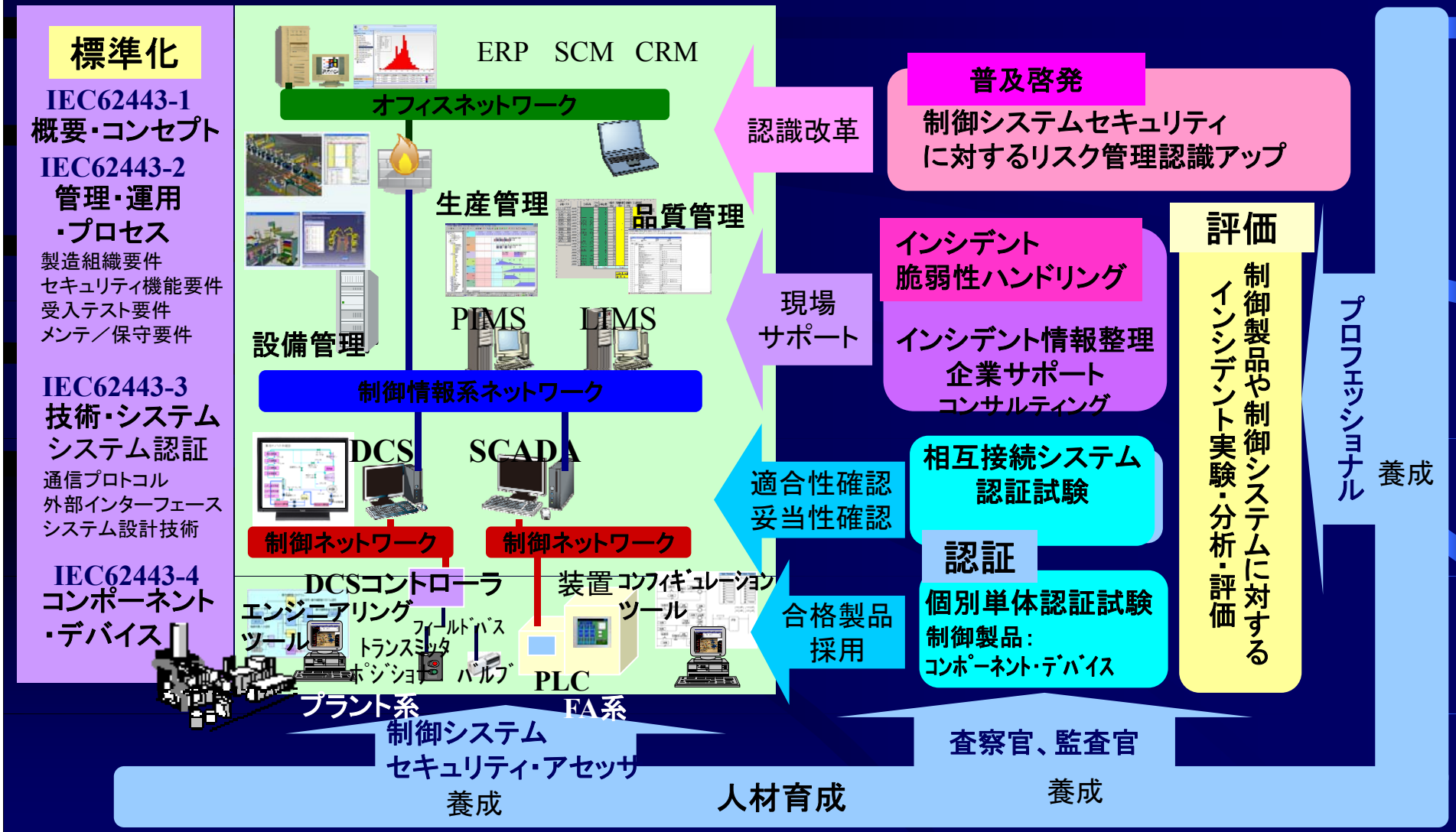
IEC62443の知識と制御製品のセキュリティ対応強化対策
高セキュア化基礎技術情報
インシデント情報
サイバー攻撃方法の最新情報
認証試験情報、評価ツール情報
業界別ユーザーセキュア基準情報
ビジネス上必要となる国際標準規格の最新情報

制御製品開発環境の健全化整備

Sierやユーザーへの取り扱いガイドラインを出して、正しい製品管理を公表していく。

1. 現場の防衛の支えとなるベンダの役割

- どうあれば良いか。（あるべき姿）



現場制御システムセキュリティ対策のポイント

- 制御システムと制御製品のセキュリティ認証機関と第三者審査官養成
- ユーザー企業によるベンダ／SIer・オーディット
- 制御システム・セキュリティ・アセッサできる人材養成
- インシデント対応トレーニングと識別ツールとコンサルティング

●制御システムセキュリティ・アセッサ

生産現場を始めとする機械設備や生産システムのリスクアセスメントを実施し、維持するために、現場の安全性を確保しながら、制御システムセキュリティ対策の妥当性を確認できる人材を育成

●セキュリティ・アセッサ・ベーシック

制御現場の制御システムセキュリティについての健全性を確保しながら、現場作業できる教育を受けた人材　⇒　現場で作業する人を対象

●セキュリティ･サブアセッサ

制御システムセキュリティアセッサの基礎知識を習得している人材　⇒　現場改善に取り組む人を対象

制御システムセキュリティ対策の妥当性確認に必要な基礎知識及び能力において、一定レベル以上の能力を有しているかの適格性を確認された者

●セキュリティ・アセッサ

セキュリティサブアセッサの知識を持ち、発揮できる人材　⇒　現場改善に取り組むシニアを対象

サブアセッサ資格の能力に加え、「更に、幅広い専門知識による制御システムセキュリティ対策の妥当性判断の総合力」の能力を有しているかの適格性を確認された者

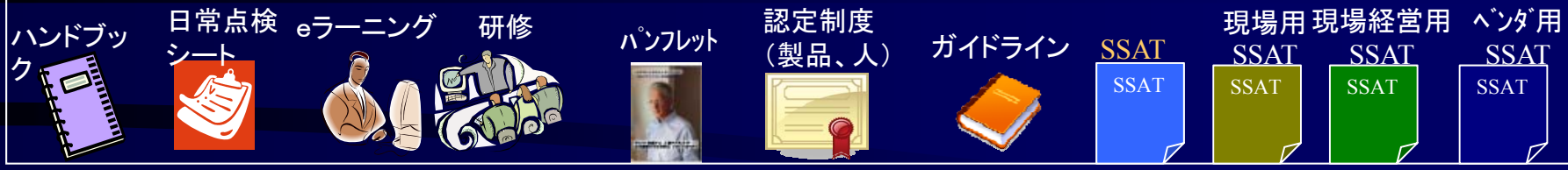
●セキュリティ･リーダー・アセッサ

アセッサのリーダーとして第三者評価ができる人材　⇒　現場改善内容を確認する責任者を対象

「第三者として制御システムセキュリティ対策の妥当性を評価する総合力」の能力を有しているの適格性を確認された者

普及啓発：あるべき姿

- 普及・啓発対象者によって認識して欲しいことが異なるので、訴求点を明確にする。
  - 縦の層：経営者向け、ミドル向け、現場向け
  - 横の層：ユーザ向け、コンポーネント・ベンダー向け、Sier向け
  - ドメイン：電力、ガス、石油、化学、交通、水道、医薬品、半導体、工作機械、自動車
- 普及啓発ツール



1. 現場の防衛の支えとなるベンダの役割

- セキュリティプロダクト／サービスのオーナーをおく
  - 制御製品のセキュリティにおける企画から保守に至るまで全責任を取る
  - 社内セキュア管理の知識と実践の教育システム
- 社会インフラ、ライフライン、基幹産業の現場を支える制御製品であるか？　:セキュア製品に関するマーケティングの重要性
  - IEC62443対象制御製品にあたる
    - ユーザー指定の制御システムセキュリティ試験で合格し、安心を提供
      - 試験を受けるのにコストがかかる。 ⇒　セキュア対策製品の価格が上がる
      - ユーザーは、サイバー攻撃で被災し、工場操業停止する損害と比較検討して妥当な金額であるかを見る。
    - サイバー攻撃に強い制御製品
    - インシデント対応の情報公開対応
      - 顧客に対する供給者責任　⇒　信頼、安心
  - IEC624432対象制御製品にあたらない
    - 今までと変わらない
      - PL法、業界法規制、RoHS、
- ユーザー向けに
  - 「セキュリティ対策の制御製品取り扱いガイドライン」

2. 制御製品開発に求められるセキュリティ対応

- サイバー攻撃に強い制御製品とは？
- 重要インフラの制御システムに使用される制御製品に求められることとは？:ISA　Secure

計装・計測制御エンジニア以外の方のために
どんな世界の話をしているのか
ちょっとだけ、予備知識として寄り道します。

制御エンジニアリングの世界

エンジニアリング知識

- 制御製品の知識

  DCS、SCADA、PLC、インバータ、バルブ、アクチュエータ、トランスミッター、センサー、生産管理、スケジューラ、設備管理、品質管理、電源装置、配電・分伝、など
- コンピュータOS、ネットワーク設計、無線通信
- プログラム言語
- 制御工学
  - フィードバック制御、フィードフォワード制御、協調制御、適応制御など
- ヒューマンインターフェース
- 生産方式と制御システム設計
- 国際標準規格：ISO、IEC、MILL
- 法規制：JIS、PL法、RoHs、ロイドなど
- GXP：GMP、GLP
- 品質保証、品質管理
- 現場管理条件

制御対象についての知識

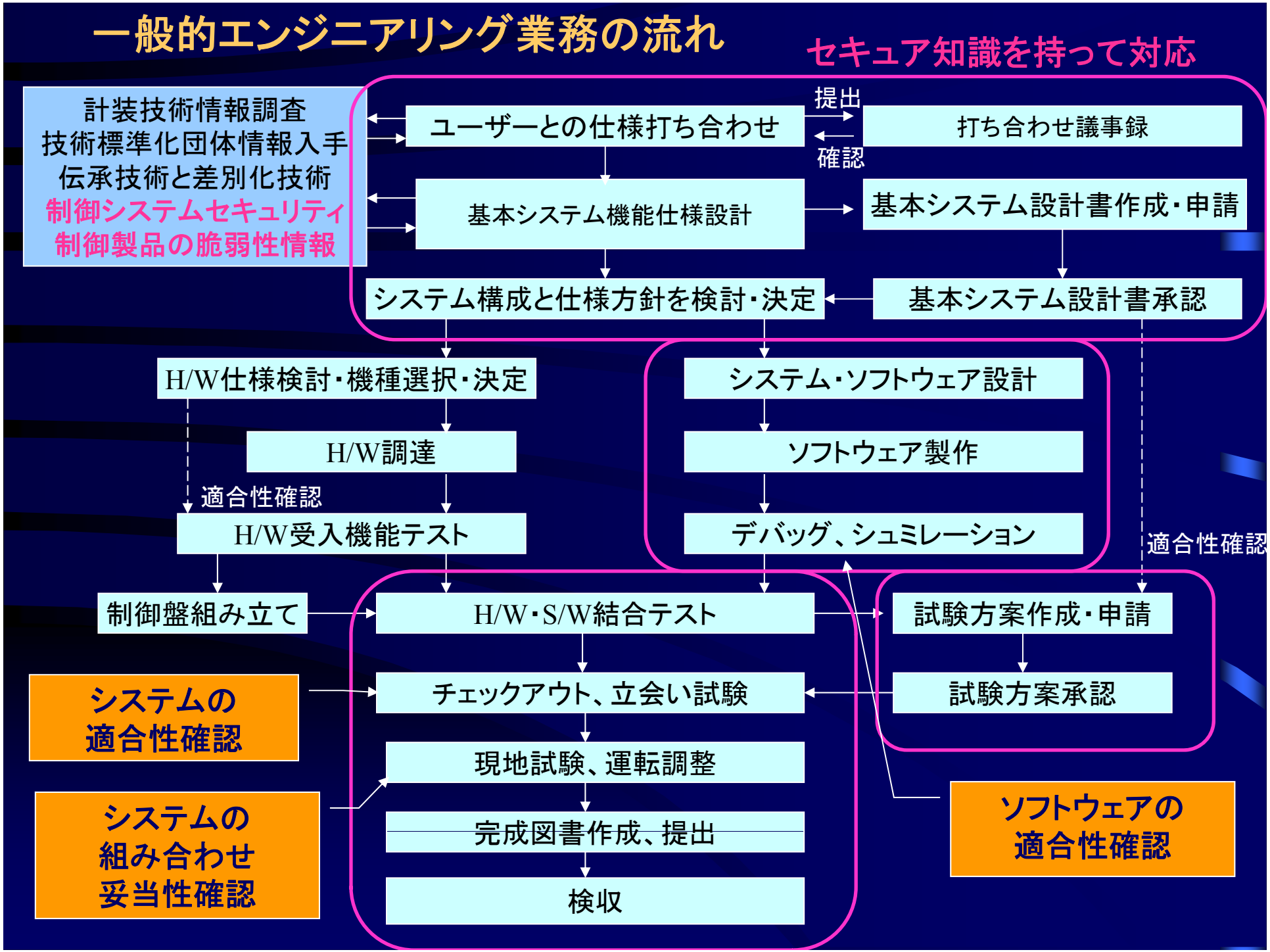
- 化学、物理学、生物学（バイオ）、流体力学、電気電子工学、電磁気学、物性工学、電気化学工学、環境学、エネルギー工学、交通工学
- 微分積分演算、行列、評価関数、

セイフティについての知識

- 本質安全対策
- 機械安全、機能安全、グループ安全
- 安全計装製品情報
- リスク評価計算

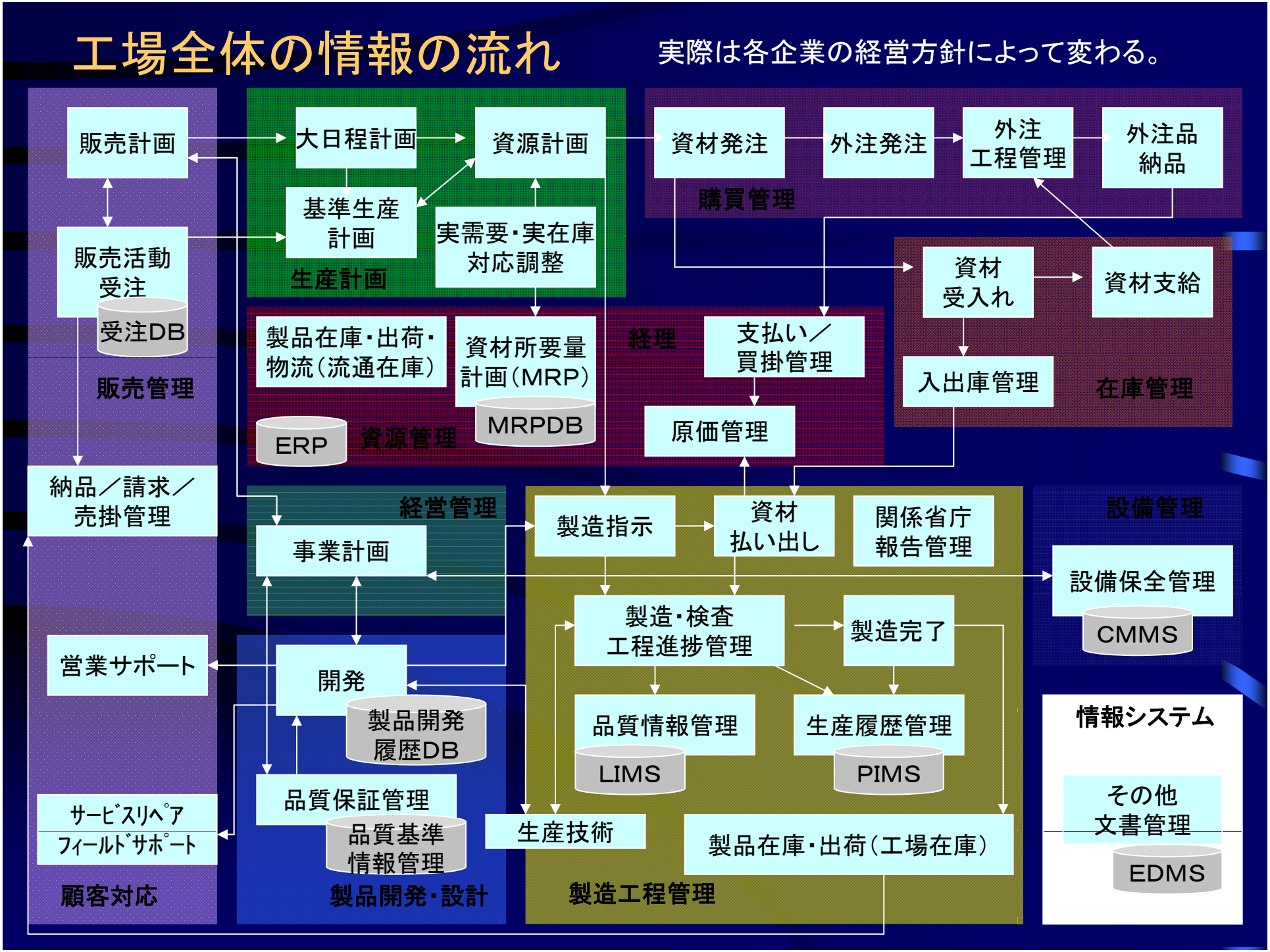
制御システムセキュリティ

- IEC62443
- CSET、SSAT
- セキュリティアセッサ

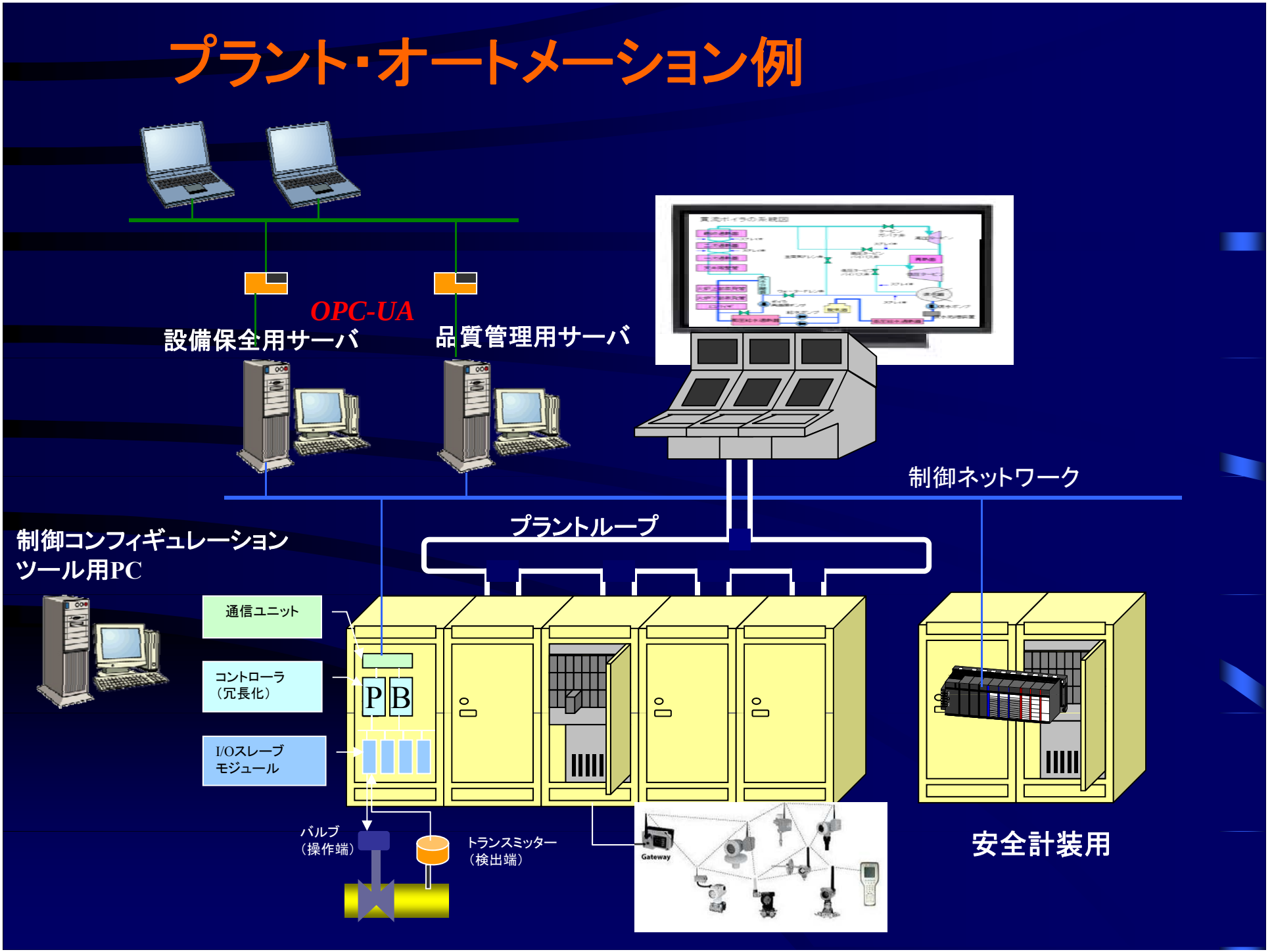

一般的エンジニアリング業務の流れ
セキュア知識を持って対応
計装技術情報調査
技術標準化団体情報入手
伝承技術と差別化技術
制御システムセキュリティ
制御製品の脆弱性情報
提出
確認
ユーザーとの仕様打ち合わせ
打ち合わせ議事録
基本システム機能仕様設計
基本システム設計書作成・申請
システム構成と仕様方針を検討・決定
基本システム設計書承認
H/W仕様検討・機種選択・決定
システム・ソフトウェア設計
H/W調達
ソフトウェア製作
適合性確認
H/W受入機能テスト
デバッグ、シュミレーション
適合性確認
制御盤組み立て
H/W・S/W結合テスト
試験方案作成・申請
チェックアウト、立会い試験
試験方案承認
システムの
適合性確認
現地試験、運転調整
システムの
組み合わせ
妥当性確認
完成図書作成、提出
ソフトウェアの
適合性確認
検収

工場全体の情報の流れ

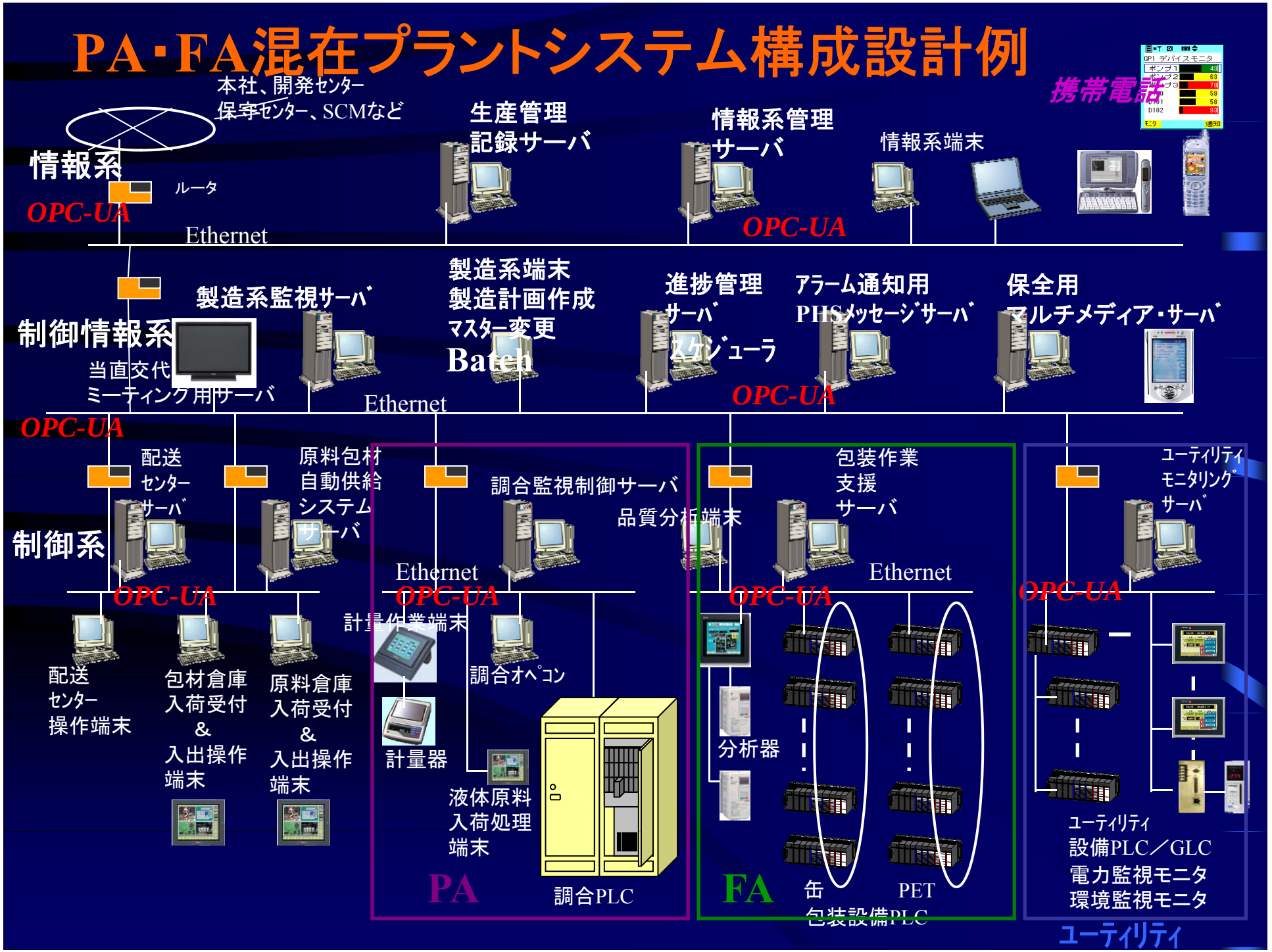
実際は各企業の経営方針によって変わる。



プラント・オートメーション例

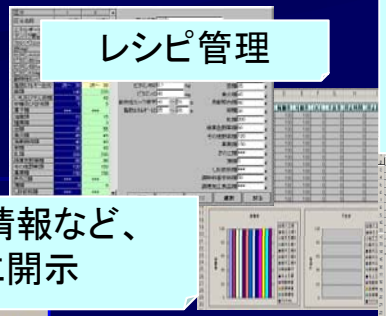


PA･FA混在プラントシステム構成設計例



アセンブリ生産での制御システム例

トレーサビリティ対応アプリケーションや
工場内管理マニュアルWebサーバとの組み合わせ



作業工程管理
作業マニュアル
メンテナンスマニュアル

管理部門

ロットごとの進捗状況、製造履歴、品質情報など、
必要な情報をあらゆる部門に瞬時に開示

製品個別情報画面

出荷情報画面

問い合わせ受付画面

Webサービス

Ethernet

OPC-UA

製造現場

製造現場データ収集システム

原料受入払出管理システム

投入調合加工管理システム

充填殺菌管理システム

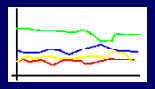
出荷ロット管理システム

OPC-UA

メリット
・原料不具合トレース
・原料コスト削減
・事故防止
・納期短縮

OPC-UA

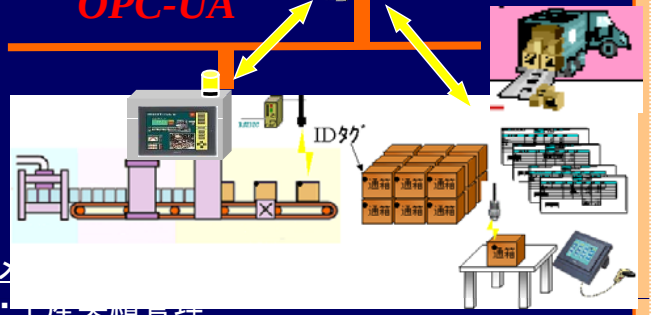
メリット
・投入ミス(時間、順番)防止
・機械加工情報収集
・熟練工情報収集
・殺菌・洗浄・点検管理
・作業履歴管理



OPC-UA

メリット
・機械加工情報収集
・充填情報トレンド監視
・生産進捗管理
・機械稼働管理

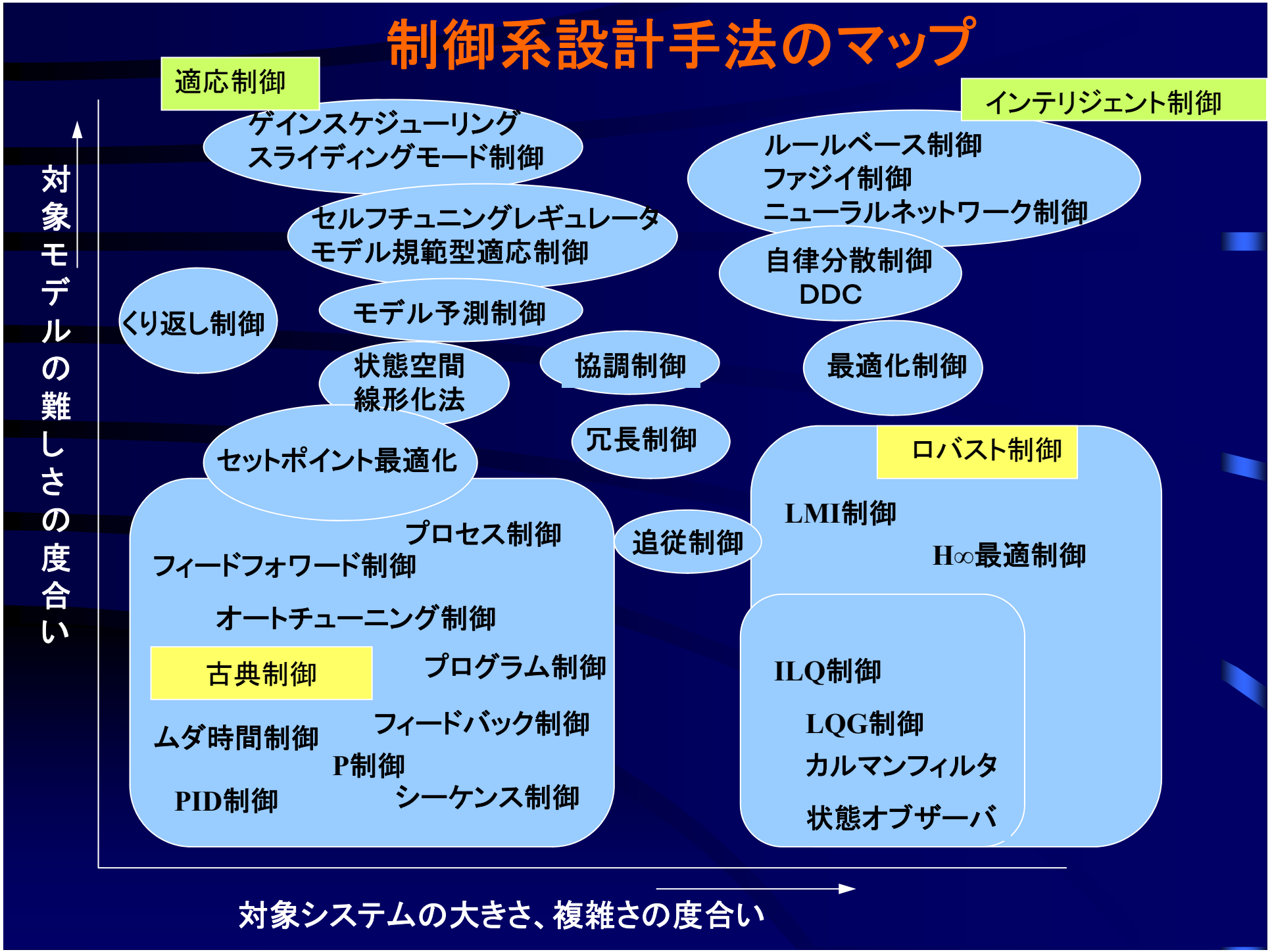
OPC-UA



・製造ロット出荷管理

生産方式の分類

大分類	方式分類		内容
加工プロセスの違いによる区分け	プロセス生産方式	バッチ生産方式	バッチ制御をベースにした生産
		連続生産方式	連続したプロセス制御をベースにした生産：ノンストップとも言われる
	アセンブリ生産方式		自動車製造、工作機械製造など組み立て工程がベースの生産
製品の種類と生産量による区分け	小品種多量生産方式		大量に材料を仕入れ、大量に生産してコストを下げる生産
	多品種少量生産方式		多様なユーザーニーズに合わせ、ジャストイン実現の生産
機械・装置の配置による区分け	フロアーショップ型生産方式		製品の加工順に装置を並べた製造現場配置の生産
	ジョブショップ型生産方式		加工機能ごとに集められて製造する機械配置の生産
組み立て方式による区分け	ライン生産方式		作業者が工程順に並んで作業する生産
	ラインセル組合せ生産方式		セルが繋がっている生産
	セル生産方式	セル生産方式	屋台方式、一人や少人数単位で組み立てを行う生産
		ハイブリッド・セル生産方式	異なる製品を扱えるセル生産
		ロボット・セル生産方式	作業者とロボットの組合せセル生産
生産指示方式による区分け	プッシュ型生産方式		生産を効率よくするために計画を立てて生産
	プル型生産方式		後工程が引き取った分だけを生産
生産指示単位による区分け	フロー生産・連続生産方式		入り口から出口まで途中止められない生産
	ロット生産・バッチ生産方式		生産工程の途中に流れのプールがあり、単位ごとの扱いができる生産
在庫方法による区分け	見込み生産方式		販売見込で、先に製造していく生産
	半見込み生産方式		途中まで製造して受注してから仕上げる生産
	受注生産方式		材料は予め集めて、受注してから製造を開始する生産
	プロジェクト型生産方式		受注してから、材料の仕込から始める生産


制御系設計手法のマップ
適応制御
インテリジェント制御
ゲインスケジューリング
スライディングモード制御
ルールベース制御
ファジイ制御
ニューラルネットワーク制御
セルフチューニングレギュレータ
モデル規範型適応制御
自律分散制御
DDC
くり返し制御
モデル予測制御
協調制御
最適化制御
状態空間
線形化法
冗長制御
セットポイント最適化
ロバスト制御
LMI制御
プロセス制御
追従制御
H∞最適制御
フィードフォワード制御
オートチューニング制御
古典制御
プログラム制御
ILQ制御
フィードバック制御
LQG制御
ムダ時間制御
P制御
カルマンフィルタ
PID制御
シーケンス制御
状態オブザーバ
対象モデルの難しさの度合い
対象システムの大きさ、複雑さの度合い

PID制御の基本式と伝達関数の式

PID制御の基本式

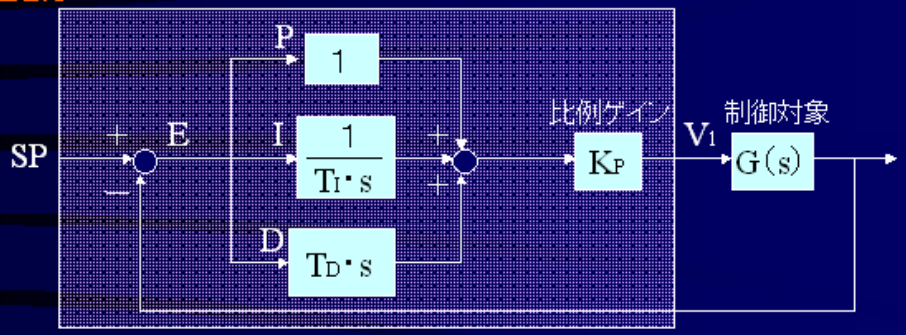
$$V_1 = K_P\left(e + \frac{1}{T_I}\int edt + T_D\frac{de}{dt}\right) + V_0$$

V1：操作量
V0：操作量の初期値
e：偏差
KP：比例ゲイン
TI：積分時間
TD：微分時間
s：ラプラス演算子
SP：セットポイント

PIDの伝達関数

$$C(s) = \frac{V(s)}{E(s)} = K_P\left(1 + \frac{1}{T_I \cdot s} + T_D \cdot s\right)$$

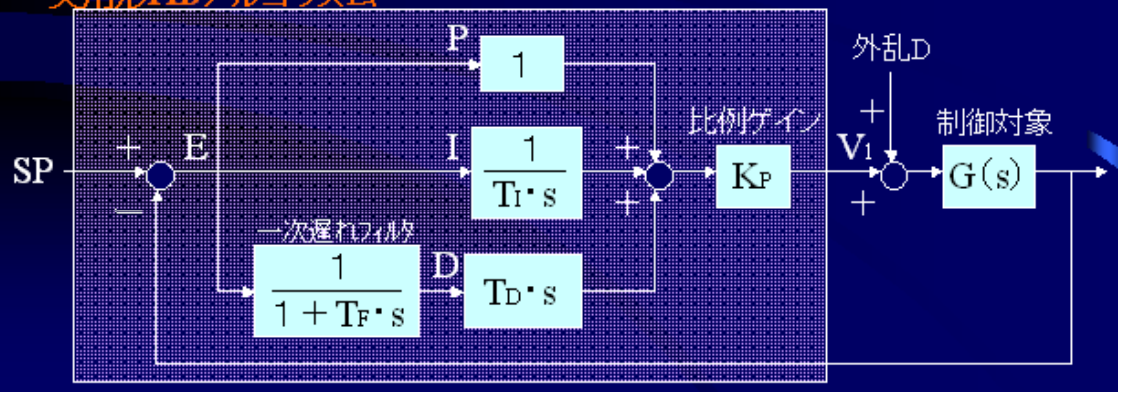
理想形PIDアルゴリズム



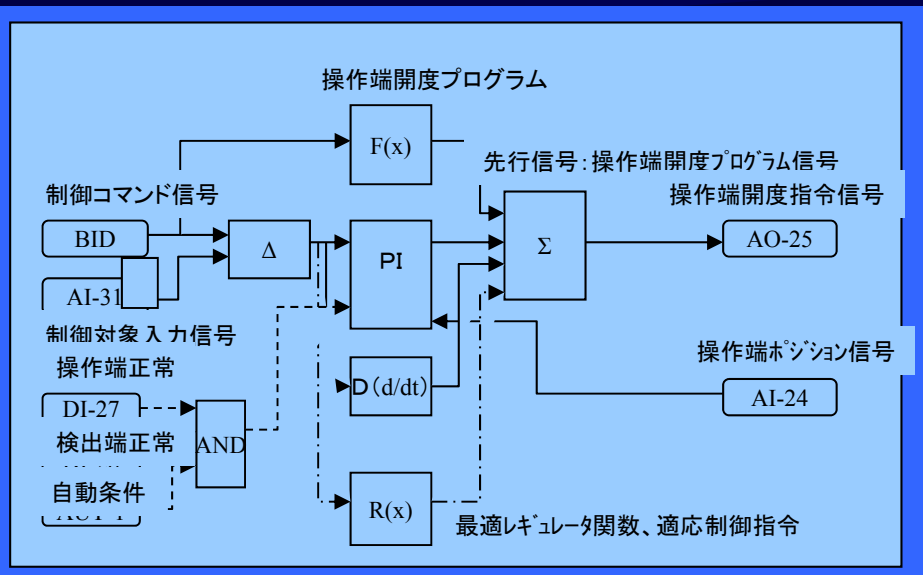
決まった時間周期で演算することで
制御が成り立っている。
だから、制御では、リアルタイムに
タイムスライスしていることが、必須条件

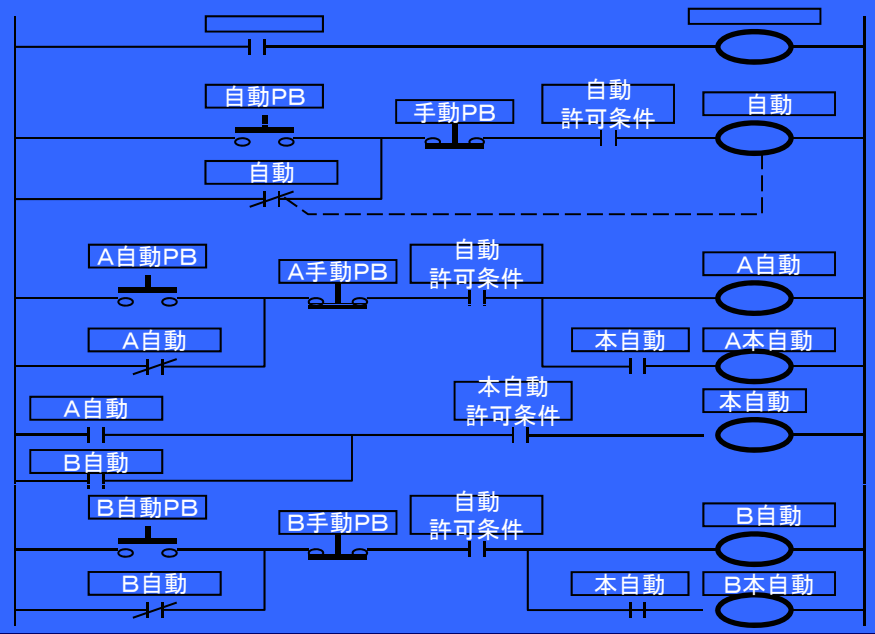
制御は、微積分演算を扱うので、制御量のサンプリングと演算とコマンド出力の処理が時間軸に対して正確であることが大切。

実用形PIDアルゴリズム



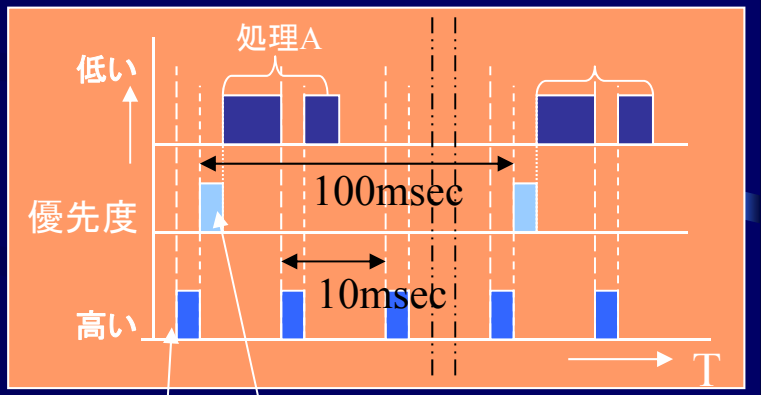
制御コンフィギュレーションとリアルタイム処理





制御は、微積分演算を扱うので、制御量のサンプリングと演算とコマンド出力の処理が時間軸に対して正確であることが大切。

100msec周期

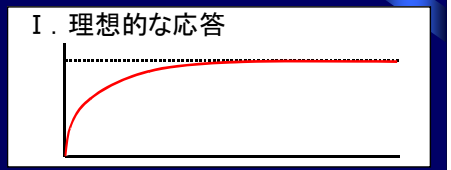


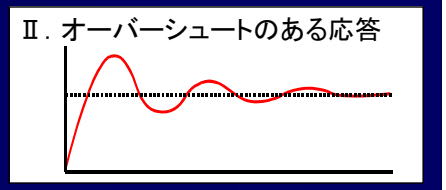
デジタル制御演算処理

アナログ制御演算処理

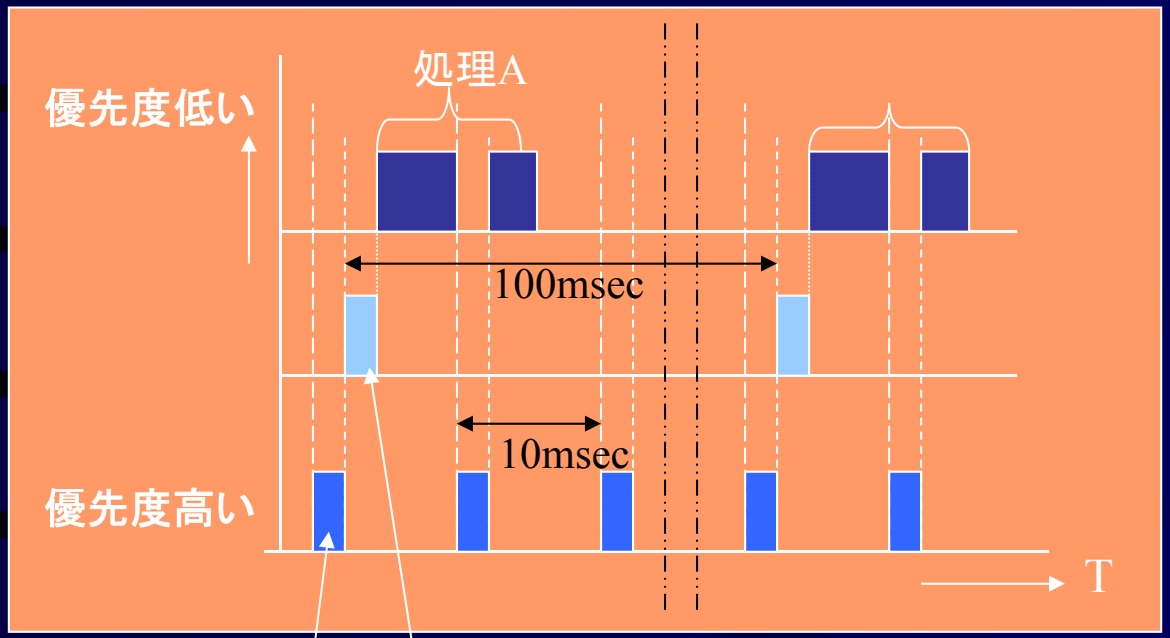
1～10msec

だから、リアルタイムOSでなければならない。





制御コントローラのリアルタイム処理



■ RTOS（リアルタイムOS）とは

リアルタイム性：単に計算処理速度が速い、レスポンス時間が短いということではなく、システムが定められた時間要件を満たして動作すること。

RTOSの機能

- マルチタスク機構
- タスク間同期（通信機能）
- 割り込み管理
- 時間管理
- メモリ管理

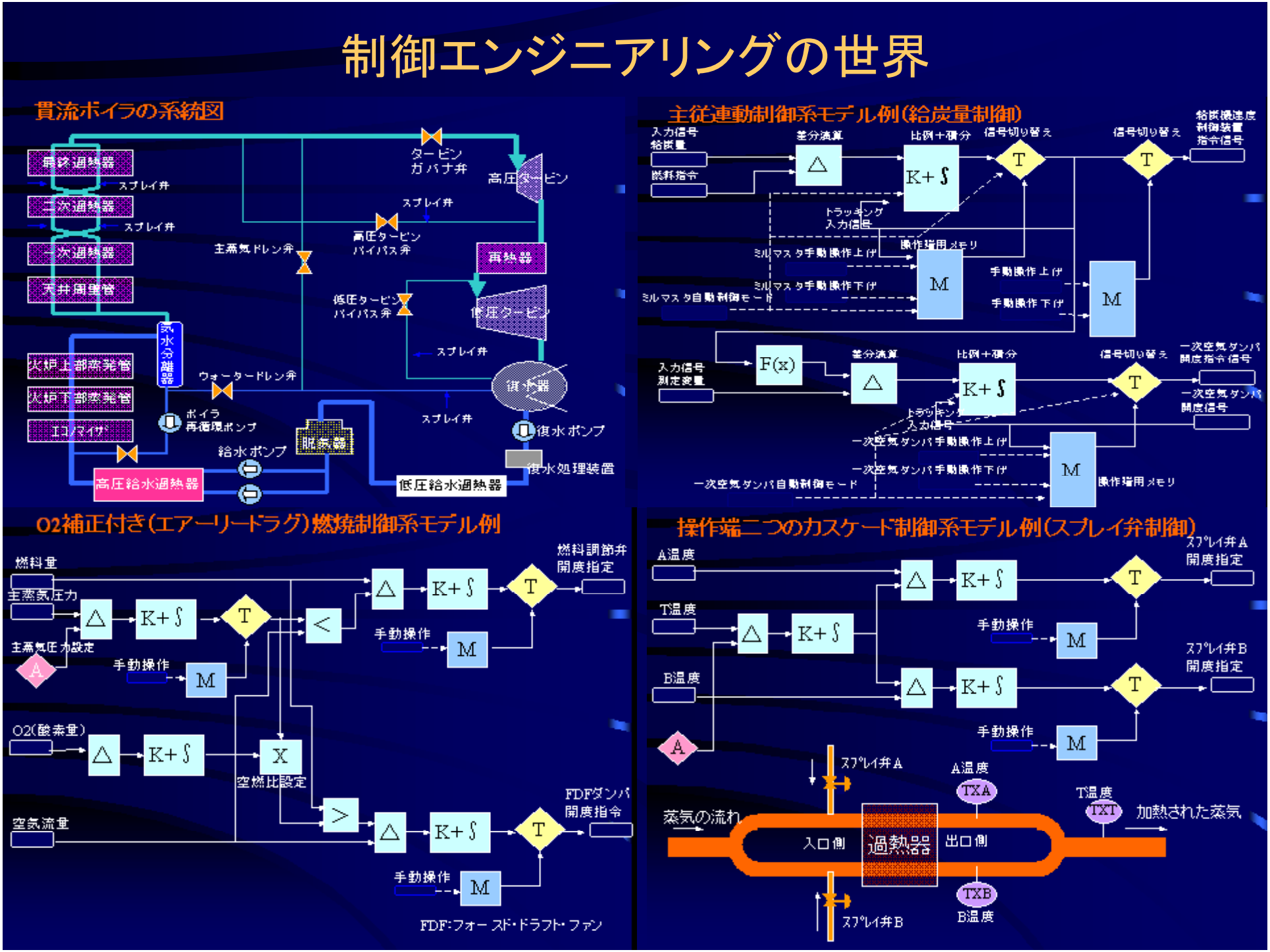
リアルタイムOS

イベントへの対応を要求時間内に実行
優先度ベースのスケジューリングがされるため、
優先度の高いイベントが頻発した場合、
優先度の高いプログラムのみが実行される

制御コンフィギュレーションツール用PC
汎用OS

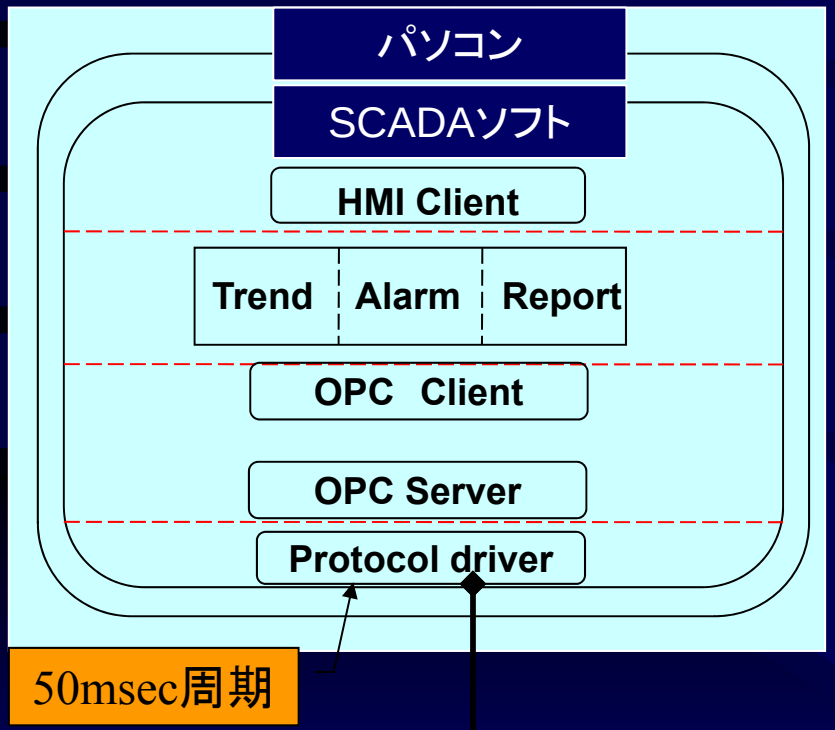
TSS、ラウンドロビン：コンピュータ全体のスループット向上
TSSにも優先順位は存在するが。優先順位の低いプログラムにもかならずCPU使用権が行く様、スケジューリングされる

制御エンジニアリングの世界

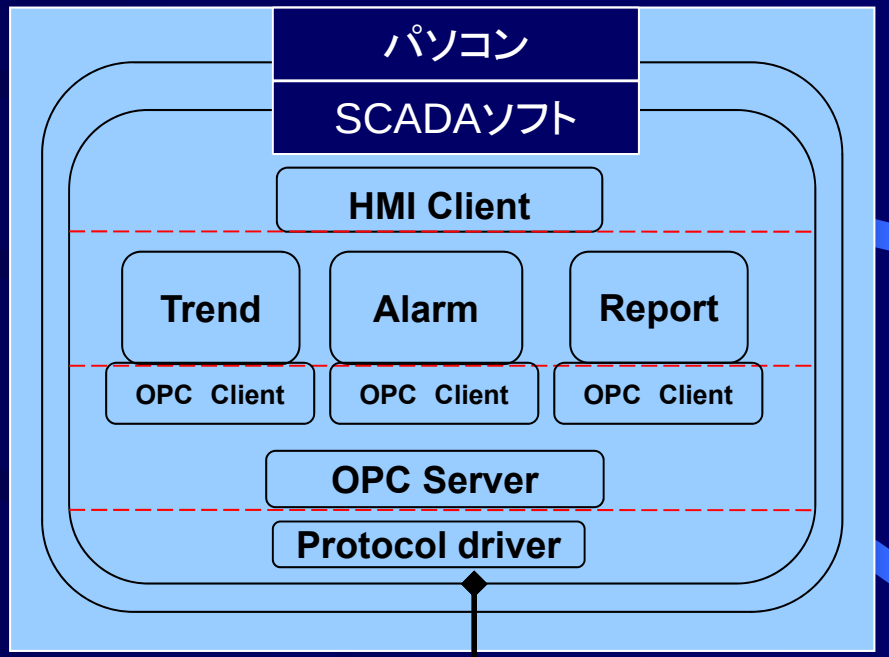


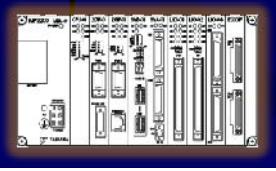
SCADAの構造

シンプルなSCADA構成



冗長化可能なSCADAの構成

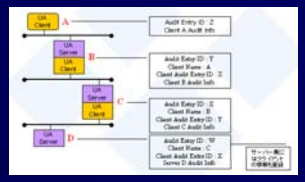


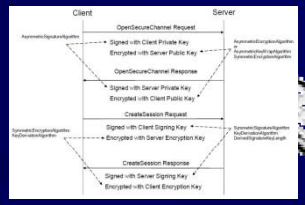


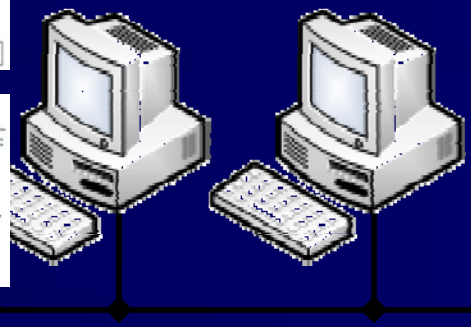
コントローラ

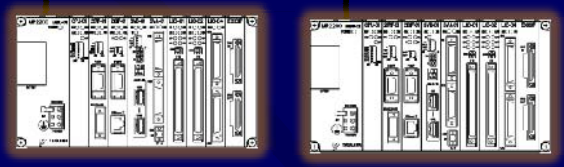
冗長化SCADAシステムアーキテクチャ

- 冗長化システムでは、
  - オンラインでのパッチあて技術
  - セキュリティ対応型通信プロトコル仕様
    - オーディット機能
    - セキュリティ設定機能
      - » 暗号化
      - » 署名



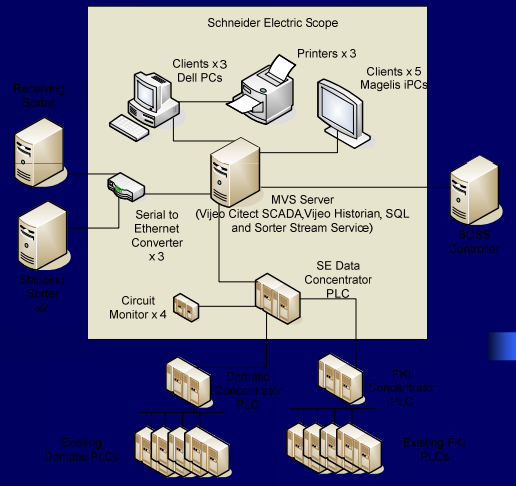




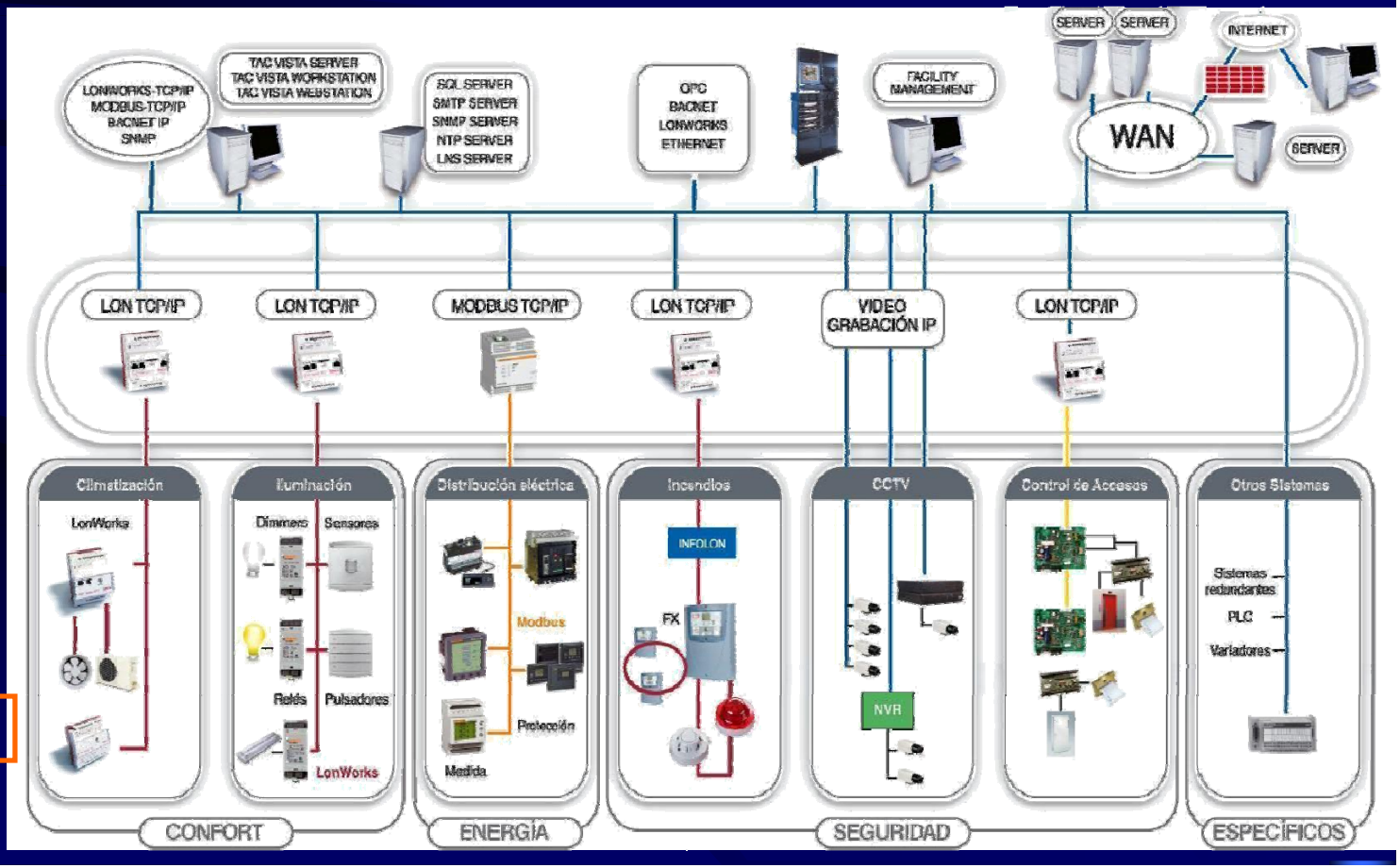


●ここに示すシステム構造は説明用に簡略化したもので、実際のソフトウェアコンポーネントの構造とは異なるものである。

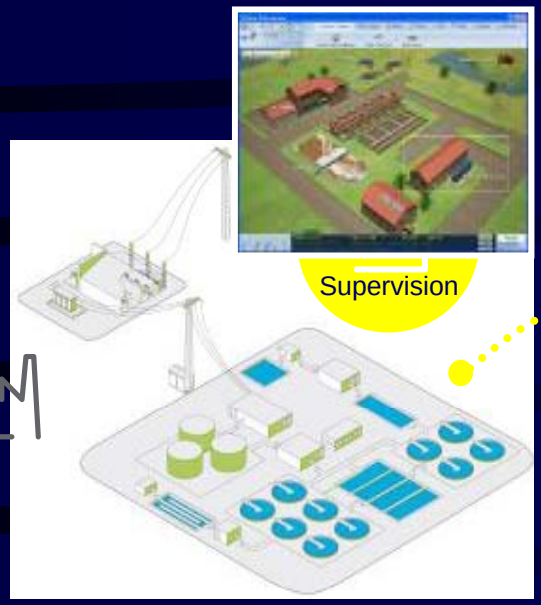
Building Management



- HVAC control
- Speed Drivers
- Lighting control
- Surveillance
- Fire Detection
- Technical Alarms
- Power Monitoring
- Power Management
- Electrical Protections
- Supervision System



スマートグリッド：コンビナート＋FEMS＋BEMS



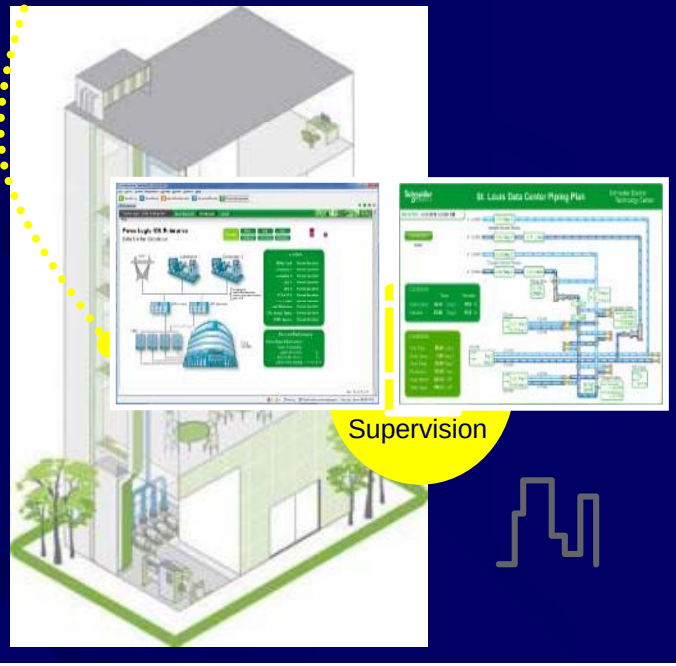
Supervision

Enterprise portal

- Safty
- Sacurity
- Saving

- **Power** management
- **Process & Machines** management
- **IT / Server Room** management
- **Building** management
- **Security** management

Supervision



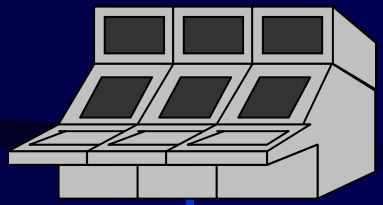
Supervision

最新の計装システム

通常のプロセス情報（従来のDCS）

操作コンソール

Asset



リモート計器室も可能

安全計装

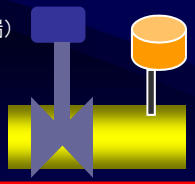
Controller

ワイアレス計器
→安価
→監視強化
→非定例計測強化

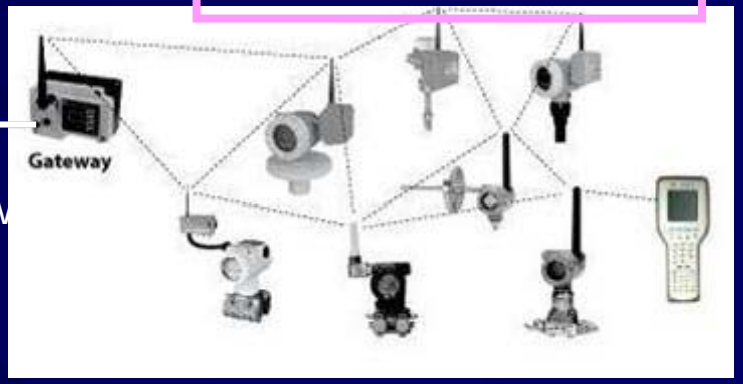
インターロック情報（計器、操作器の全ての情報）

デジタル通信

バルブ（操作端）

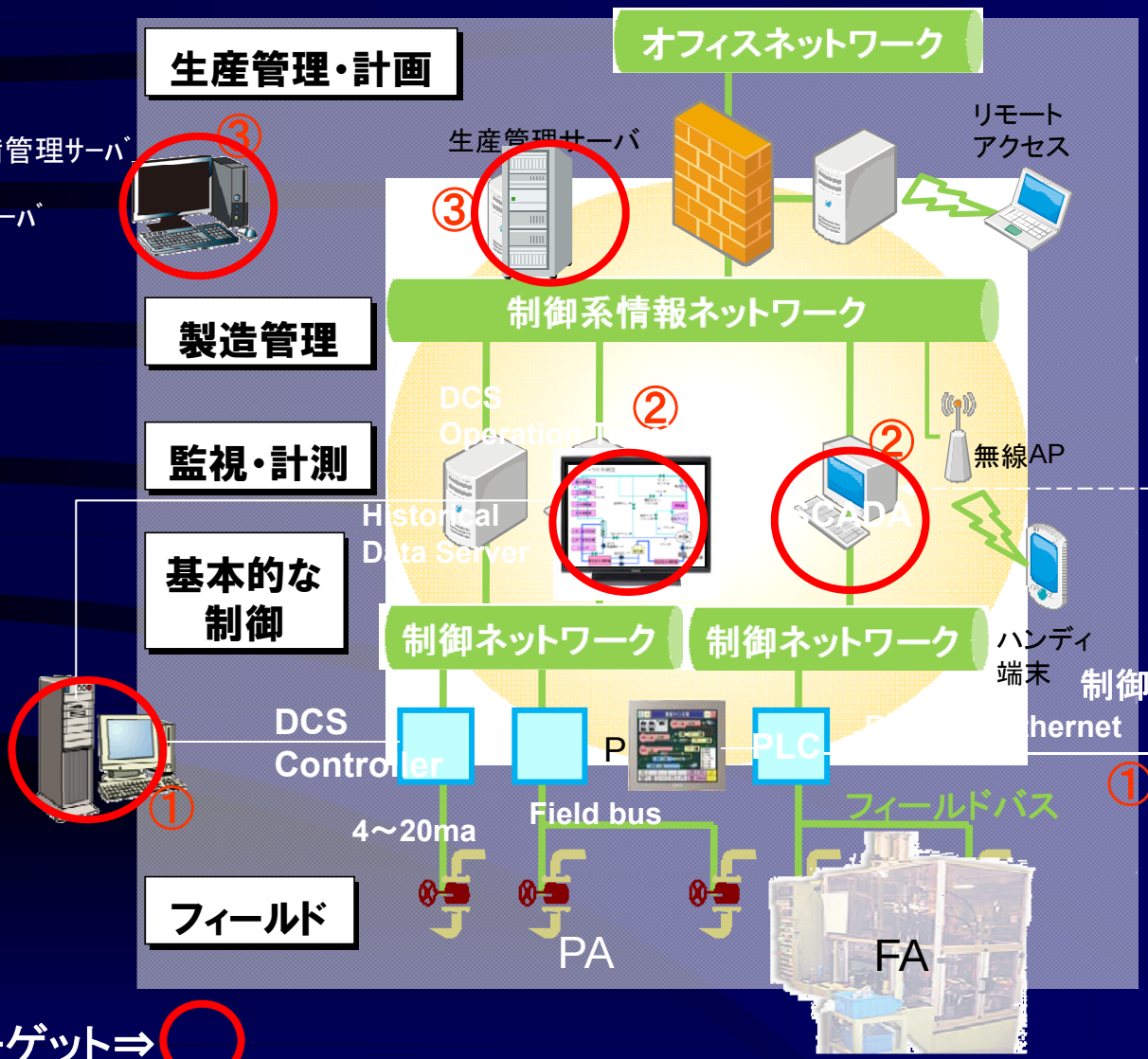


トランスミッター（検出端）



オンライン診断
→トラブル未然防止
→TBMからCBM

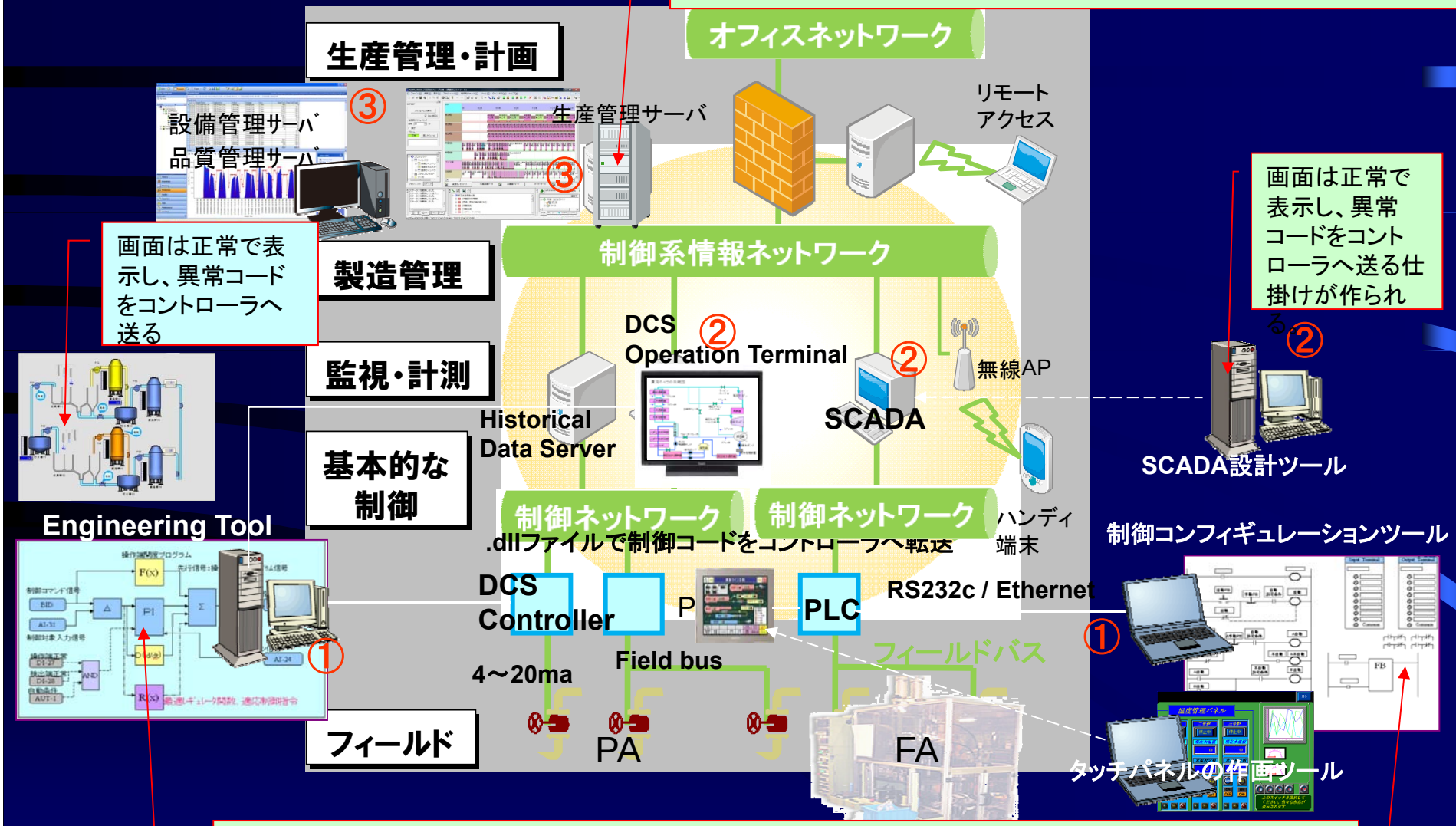
制御システムにおける攻撃対象例



攻撃目的は、装置や設備の破壊、悪品質製品生産や生産の暴走、装置ベンダの信頼失墜等

制御システムセキュリティ攻撃パターン例

生産スケジュールの製品成分レシピなどを悪品質に掏り帰る。生産数量指示を替える。コントローラへの直接指示コードを送って装置や設備にストレスを加える。



ファンクションブロックのパラメータやシーケンスロジック条件を書き換えたものと掏り替える。

制御システムにおける不具合現象

- 制御システムにおけるインシデントが起きている可能性を持つ異常現象
  - 制御動作が時々遅くなる。
  - 通信エラーが出るようになった。
  - 制御データが抜けている。
  - 制御動作変化しているべき制御データが変化していない。
  - 制御信号が突然変化する。（突変現象）
  - 壊れるはずの無い部分が壊れている。おかしなストレスがかかったと思われる。
  - 制御機器のメンテナンスチェックが終了しない。
  - 閉まっていなければならない操作端が開いている。また、その逆。
  - 再起動してしばらくは正常動作していたが、また、同じ異常になった。
  - ソフトウェア更新をしたら、異常になった。
  - USBで作業をしたら、異常が出るようになった。
  - 外部サポートを受けた後に、異常が出るようになった。
  - 制御異常現象は出ていないがインシデント発生

サイバー攻撃原因か、それ以外の原因（バグ・メカ寿命・人的作業ミス・）かの識別作業は、インシデント対策を熟知の計装制御熟知のエンジニアとサイバー攻撃分析に堪能なエンジニアの組み合わせで識別作業に当たらないと実際は難しい。

現場の不具合でのセキュリティ問題識別

制御システムにおけるインシデントが起きている可能性を持つ異常現象
1 制御動作が時々遅くなる。
制御内容を変更していない
スレーブの反応が遅くなっている可能性あり
スレーブが管轄している検出端(トランスミッター／センサー／ポジショナー)か操作端が異常になっている可能性あり
検出端(トランスミッター／センサー／ポジショナーの不具合が有るか否か調査)
スレーブモジュールが異常の可能性あり
モジュールチェッカーで診断
制御内容を変更している
制御変更内容が間違っているか調査
コントローラ内の制御ファイルを逆コンパイルして制御コンフィギュレーション内容とベリファイチェック
間違っている
目的にあった制御内容に修正
間違っていない
コントローラに異なる(不要な)コマンドorアプリケーションが動作している可能性あり
変更内容の再チェック(変更設計者による手作業)
2 通信エラーが出るようになった。
通信エラー内容を確認
スレーブ通信規定時間内反応無し
反応しないスレーブモジュールをモジュールチェッカーで検査
スレーブモジュールが異常検出したら交換
スレーブモジュールが正常であれば、操作端と通信ケーブルをチェック
操作端が異常であれば、修理
通信ケーブルが異常であれば、交換
異なる通信プロトコルが存在する
通信プロトコルの監査ツールが有る場合、その通信ログデータを調べる:通信エラー発生で制御ネットワークの通信取り合いデータをフリーズしてファイルデータを再生し、調査
設定していない通信プロトコルであれば、異常侵入された可能性有り
その通信相手をしているモジュール／PCをチェック
通信プロトコルの監査ツールが無い場合、制御ネットワークにつながるモジュールやPCを全てチェック
モジュールに異常が見つかった場合は、そのモジュールを交換
PCに異常が見つかった場合は、リフレッシュ作業を実施
異常が見つからない場合は、未知のピールスかマルウェア侵入の可能性を抱えたまま、操業継続するかどうかを判断しなければならない。
3 制御データが抜けている。
マスタとスレーブの通信周期が間に合っていない。:全データの収集が広い切れていない。
制御ネットワークにPCがつながっていない場合
通信プロトコルの監査ツールが有る場合、その通信ログデータを調べる:通信エラー発生で制御ネットワークの通信取り合いデータをフリーズしてファイルデータを再生し、調査
設定していない通信プロトコルであれば、異常侵入された可能性有り
その通信相手をしているモジュール／PCをチェック
通信プロトコルの監査ツールが無い場合、制御ネットワークにつながるモジュールやPCを全てチェック
モジュールに異常が見つかった場合は、そのモジュールを交換
PCに異常が見つかった場合は、リフレッシュ作業を実施
異常が見つからない場合は、未知のピールスかマルウェア侵入の可能性を抱えたまま、操業継続するかどうかを判断しなければならない。
制御ネットワークにPCがつながっている場合
マスターモジュールの上位に制御情報系ネットワークがつながっていて、FDT－DTMを使用している場合
上位PCからコントローラ経由でデータ収集設定していた場合
大量データ収集していた
マスターモジュールの制御通信優先設定になっていた
マスターモジュールをモジュールチェッカーで検査
マスターモジュールが異常であれば交換
マスターモジュールが正常であれば、PCから不正侵入された可能性があるためPCを調査
PCに異常が見つかった場合は、リフレッシュ作業を実施
異常が見つからない場合は、未知のピールスかマルウェア侵入の可能性を抱えたまま、操業継続するかどうかを判断しなければならない。
マスターモジュールの制御通信優先設定になっていなかった
PCから不正侵入された可能性があるためPCを調査
PCに異常が見つかった場合は、リフレッシュ作業を実施
異常が見つからない場合は、未知のピールスかマルウェア侵入の可能性を抱えたまま、操業継続するかどうかを判断しなければならない。
大量データ収集していない
PCから不正侵入された可能性があるためPCを調査
PCに異常が見つかった場合は、リフレッシュ作業を実施
異常が見つからない場合は、未知のピールスかマルウェア侵入の可能性を抱えたまま、操業継続するかどうかを判断しなければならない。
マスターモジュールの上位に情報系ネットワークがつながっていて、FDT－DTMを使用していない場合
PCから不正侵入された可能性があるためPCを調査
PCに異常が見つかった場合は、リフレッシュ作業を実施
異常が見つからない場合は、未知のピールスかマルウェア侵入の可能性を抱えたまま、操業継続するかどうかを判断しなければならない。
周期的に固定部分が抜けている
固定スレーブだけが通信エラーで反応無し
反応しないスレーブモジュールを差し替えて通信反応を確認
差し替えたスレーブモジュールが正常
反応しなかったスレーブモジュールをモジュールチェッカーで診断
差し替えたスレーブモジュールが差し替える前と同じ反応しない
通信ケーブルを確認
通信エラーが無い
マスターモジュールをモジュールチェッカーで診断
マスターモジュールが異常であれば、マスターモジュールを交換
制御エンジニアリングツールよりマスターモジュールのデータをダウンロードして、動作チェック
マスターモジュールが正常であれば、データ収集後にデータ書き換えられた可能性有り。
エンジニアリングツールのPCがマスターモジュールにつながったまま運用している場合
PCから不正侵入された可能性があるためPCを調査
PCに異常が見つかった場合は、リフレッシュ作業を実施
異常が見つからない場合は、未知のピールスかマルウェア侵入の可能性を抱えたまま、操業継続するかどうかを判断しなければならない。
制御情報系ネットワークにPCがつながっており、PCから不正侵入された可能性があるためPCを調査
PCに異常が見つかった場合は、リフレッシュ作業を実施

不具合原因の識別作業

通信ログ機能

操作ログ機能

各ログを採ってインシデント予兆を発見し、対策を提示

セキュリティ問題を含んでいる可能性を持つところ

インシデント原因識別

扱う情報が高度で
広範囲な為
専用ツールが必要

重要インフラの停められない制御システム
と
制御が停まると大きな損害がでる制御システム

- 原子力発電所の冷却制御システム
- ガス基地のコモン系統制御システム
- 石油コンビナートのコモン系統制御システム
- 鉄鋼炉の燃焼制御システム
- 半導体工場のクリーンルームの空調システム
- クラウドサーバーが入っているビルの空調制御システム

など

特徴

計装制御電源が落とせない。

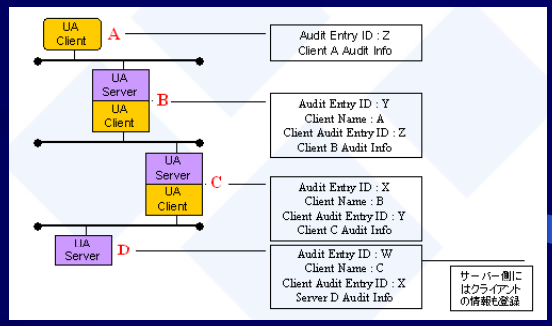
緊急時の作業は、安全制御領域までもっていって、操作端操作が手動でできるようにしてからか、定期点検時となる。

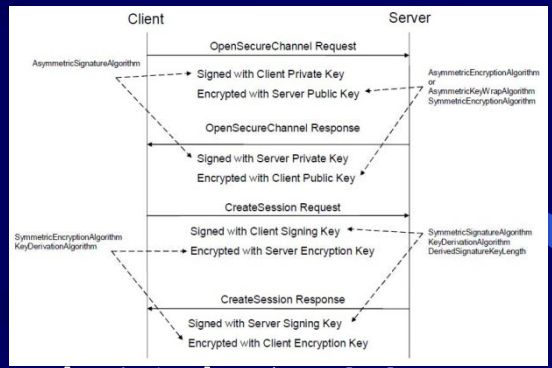
定期点検の周期が永い。

2. 制御製品開発に求められるセキュリティ対応

- サイバー攻撃に強い制御製品に求めること
  - 制御製品企画の段階から、セキュリティ対策検討を加える
    - IEC62443対象の製品とするか否か
    - OSの選択、ネットワークの仕様、通信プロトコルの選択、ログ機能の検討
  - 制御製品における高度セキュア化技術研究
  - セキュア知識を持ってプログラム開発をする
  - 製品によっては、製品内に
    - タスク通信のログ機能
    - 監査機能
  - 製品によっては、ネットワーク通信に
    - ログ機能 ⇒ 監査機能
    - 通信プロトコルは、
      - オーディット機能
      - セキュリティ設定機能
        - » 暗号化
        - » 署名

OPC-UA





- 重要インフラの制御システムに使用される制御製品に求められることとは？
  - オンラインでのパッチあて作業ができ、オンラインで切り替えられる機能
    ⇒ オンラインでのソフトウェアバージョン管理システム

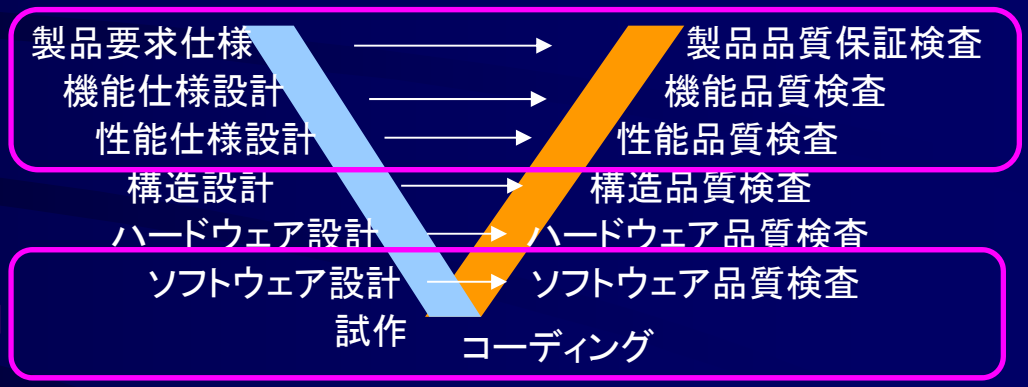
3. 製品開発の品質保証に求められるセキュリティ対応

- 製品開発の品質管理に求めること
  三現主義＋Vモデル＋セキュリティ対応
- ユーザーに対しての責任の先には、社会に対しての公益責任がある。

品質は企業製品の生命線

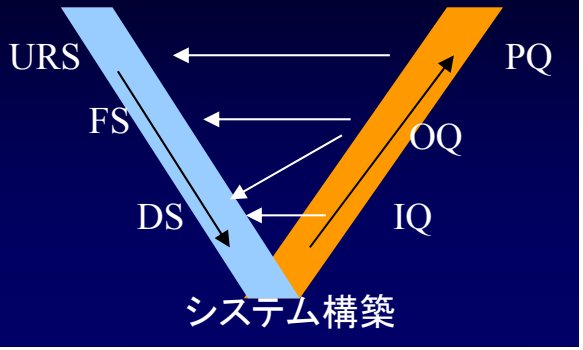
三現主義
現場
現物
現実

三現主義＋Vモデル



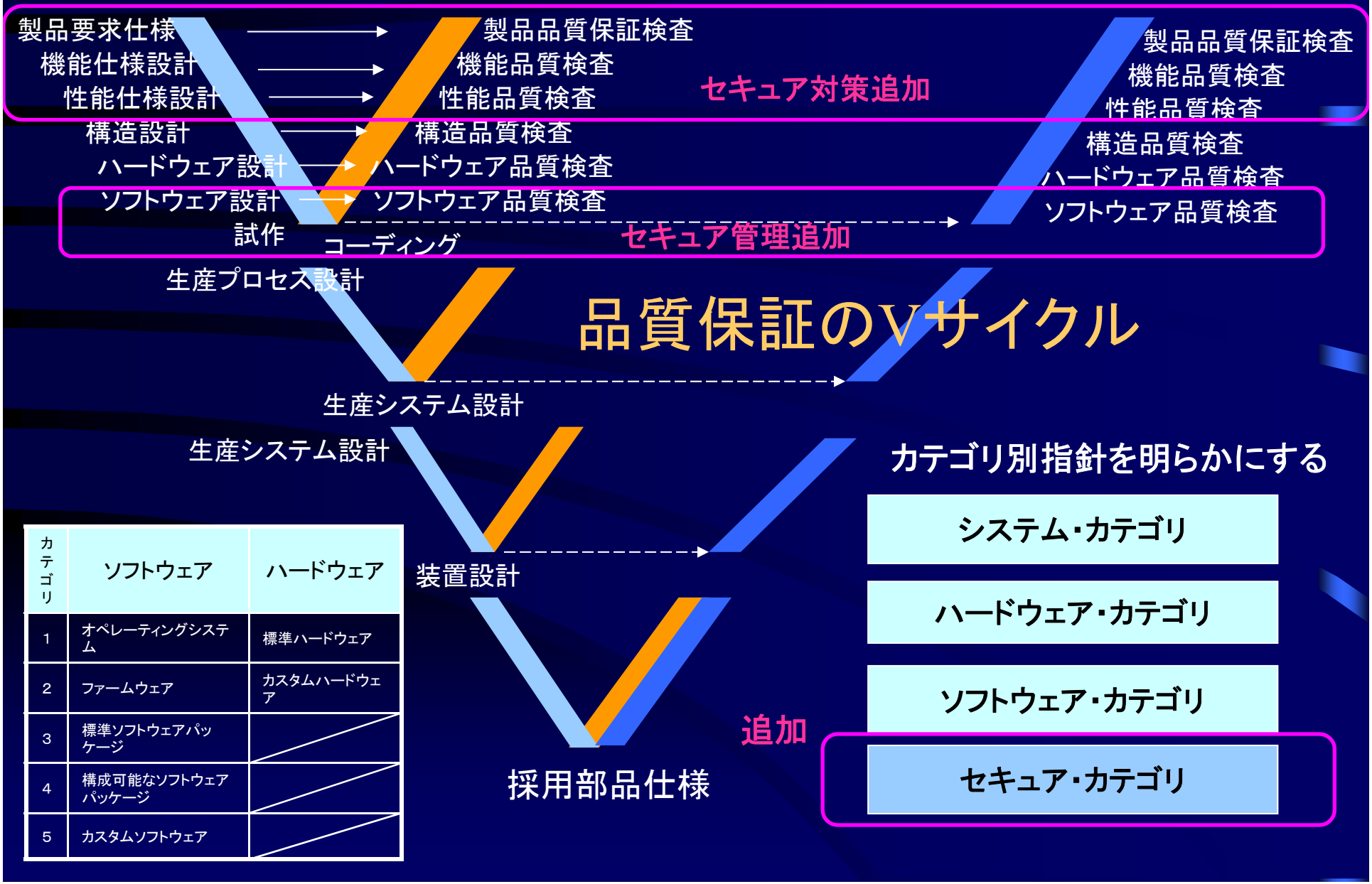
医薬・医療品業界では、GMP：Good Manufacturing Practice

ライフサイクルアプローチ



略称	用語名	概要
URS	ユーザ要求仕様書	ユーザがシステムに要求する機能要求書
FS	機能仕様書	サプライヤがURSに対応して作成する機能概要書
DS	設計仕様書	サプライヤがFSを基に作成する製作仕様書
DQ	設計の適格性確認	ユーザがサプライヤに対して実施する設計確認作業記録
FAT	工場受入試験	一般製品の工場出荷試験に相当する試験
SAT	現場受入試験	製造事業所での受入試験
IQ	設置時適格性評価	据付時の動作確認作業記録
OQ	運転時適格性評価	代表パラメータ等による動作確認作業記録
PQ	稼働性能適格性評価	運転時と同一パラメータ等による動作確認作業記録

品質保証の企業連携にセキュアカテゴリを加える



カテゴリ	ソフトウェア	ハードウェア
1	オペレーティングシステム	標準ハードウェア
2	ファームウェア	カスタムハードウェア
3	標準ソフトウェアパッケージ	
4	構成可能なソフトウェアパッケージ	
5	カスタムソフトウェア	

3. 製品開発の品質保証に求められるセキュリティ対応

- 製品開発の品質管理に求めること
  - セキュア知識を持って製品開発における品質保証管理を行なう
  - IEC62443を熟読　⇒　認識を高める。
  - 品質保証全般のテストにセキュリティ問題を加える
    - デザインレビュー項目に制御システムセキュリティ対策を加える
    - セキュア知識を持ったソースコード解析や脆弱性の洗い出し
    - 脆弱性情報・対策の履歴管理
    - サイバー攻撃を想定した品質検査
      - バリデーション
      - 適合性確認
      - 妥当性確認
      - 外注のセキュリティ対策管理
- ユーザーに対しての責任
  - ユーザーへの脆弱性情報と対策情報の公開
  - 取り扱いガイドラインに、制御システムセキュリティ対策を加える。

4. 制御製品開発環境の健全性

- 制御製品開発環境の健全性確保
  - 制御製品開発用ネットワークの隔離
    - ファイヤーウォール設置
    - ネットワーク・ケーブル
      - インターネット接続可能なケーブル
      - インターネット接続不可能なケーブル
  - セキュリティ確保、情報漏洩防止できる開発環境
- サーバーとPCネットワークのセキュリティチェック管理責任者をおく

5. 現場へのサービス対応について

- サービスに使用するPCの健全化
- 制御製品取り扱いガイドライン
  - 業界で作成する場合
    - JEMIMA、JEMA、NECAで検討して欲しい
  - ユーザー向けに
    - 「セキュリティ対策の制御製品取り扱いガイドライン」

制御システム設計にも、対策ポイントがあります。

- 設計ポイントは、
  - PCと制御ネットワークの健全性確保と区分設計
    - 階層別／生産プロセス別／情報重要度別
  - 生産システムサーバの健全性確保
  - 制御コンフィギュレーションツールの健全性確保
  - 記録媒体のセキュリティ管理
  - IEC62443-4対応制御製品
  - 制御製品供給ベンダやシステムエンジニアリング会社のオーディット

これを支える制御製品

現場対策

- 情報システムと制御システム間にファイヤーウォール設置
- PCと制御ネットワークの健全性確保
- 外部記憶媒体(USB)の扱い管理
- 生産システムサーバの健全性確保
- 制御エンジニアリングツールの健全性確保
- 制御システム不具合現象からインシデント識別手法確立
- インシデント対応の現場作業マニュアル整備
- 制御システムのリフレッシュ作業可能体制

- 制御システムの認証試験
- 制御システムネットワーク設計
  - 階層別ネットワーク設計
  - 生産プロセス別ネットワーク設計
  - 動／静脈ネットワーク設計
- エンジニアリング会社へのオーディット(監査)・認定

- 制御製品の認証試験
- 制御ベンダへのオーディット(監査)・認定
- 制御製品取り扱い制御システムセキュリティ・ガイドライン

6. インシデント対応時のベンダへのお願い

- 制御製品の脆弱性情報を隠してのインシデント対応は、間違った識別をしてしまう可能性あるので、脆弱性情報は、現場に正しく提供して欲しい。
- 制御システムの不具合原因識別能力
- 現場での原因究明識別に必要な能力
  - 情報セキュリティ
  - 制御システムセキュリティ
  - 制御システムや制御製品に関する知識・知見・対処能力
  - 業界現場常識
- 制御ベンダやシステムインテグレータとの連携

インシデント対応に必要な能力

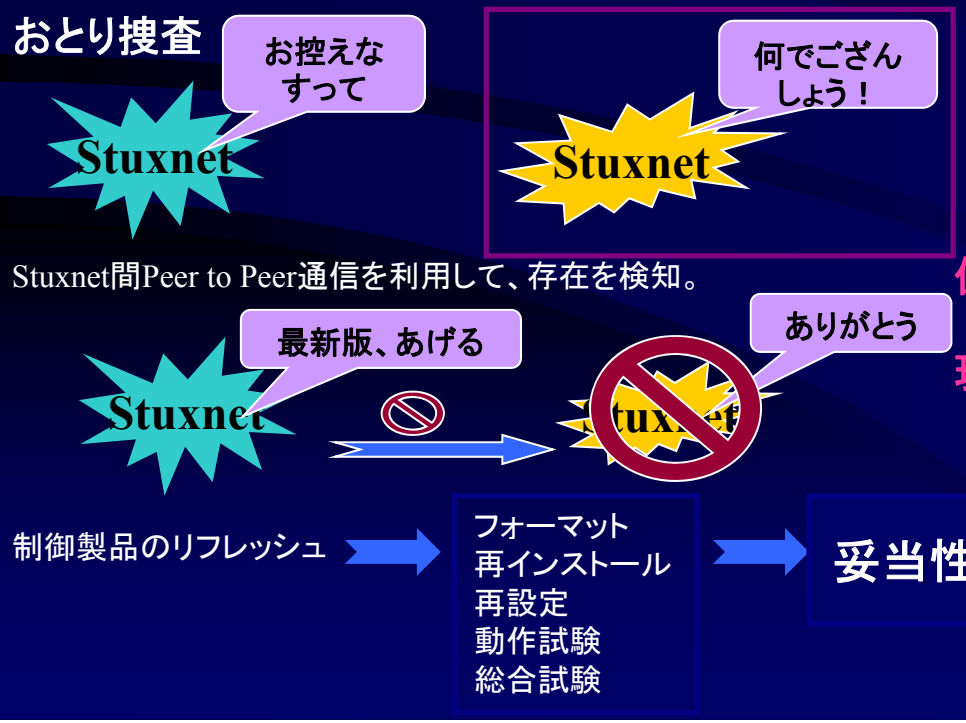
情報セキュリティ	制御システムセキュリティ	制御システム／制御製品	現場（常識）知識
情報セキュリティインシデント情報 IEC27001	現場で使用している制御製品のインシデント／脆弱性情報 IEC62443 インシデント識別能力 インシデント分析ツールとその取り扱い技能 インシデント対応リスク認識とコンサルティング能力 バリデーションへの理解力 リスク管理能力	業界標準規格 各種フィールドバス仕様 制御ネットワーク通信プロトコル 制御システム設計内容を理解する能力 制御製品（装置／操作端・検出端デバイス）ベンダ情報 制御の正常／異常動作の識別能力 制御装置の故障診断手法	機密情報管理（業界の違い） 機械安全・機能安全 リスク管理・安全確保 生産製品に関する基礎知識・危険知識 作業手順（危機回避） GXP（GMP／GLPなど） ISO

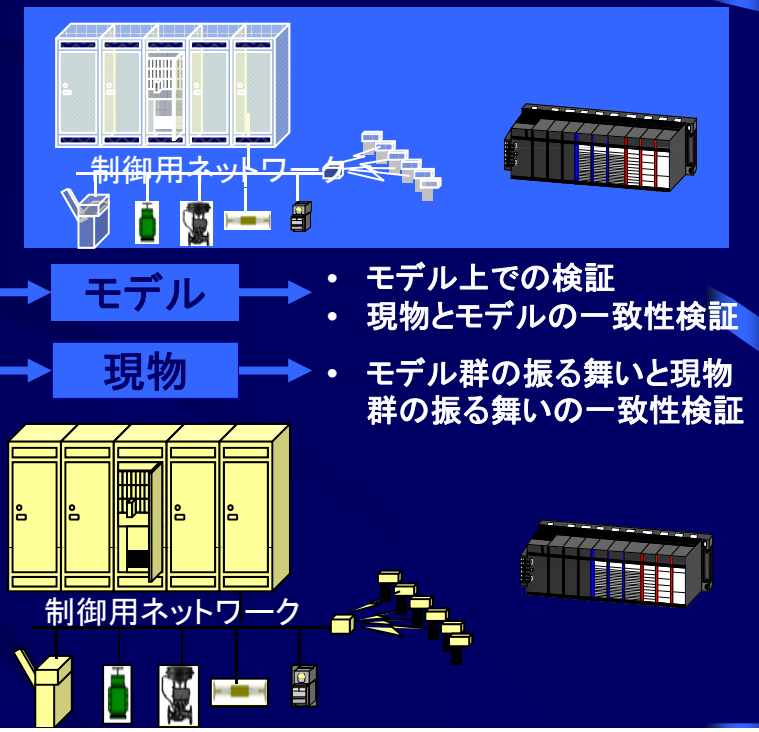
7．極めの制御システムセキュリティ対策とは、？

高度信頼性向上の技術開発

- 高信頼化制御システムを実現する為の技術開発
  - ◆ Stuxnet対策
    - ● 検知：モニタ
    - ● 機能停止：キル
    - ● 削除：クリーン
  - ◆ 振舞い監視技術による異常検出とSafety処理
    - ● コントローラ・レベル
    - ● 監視制御システム・レベル
    - ● プラント制御システム・レベル

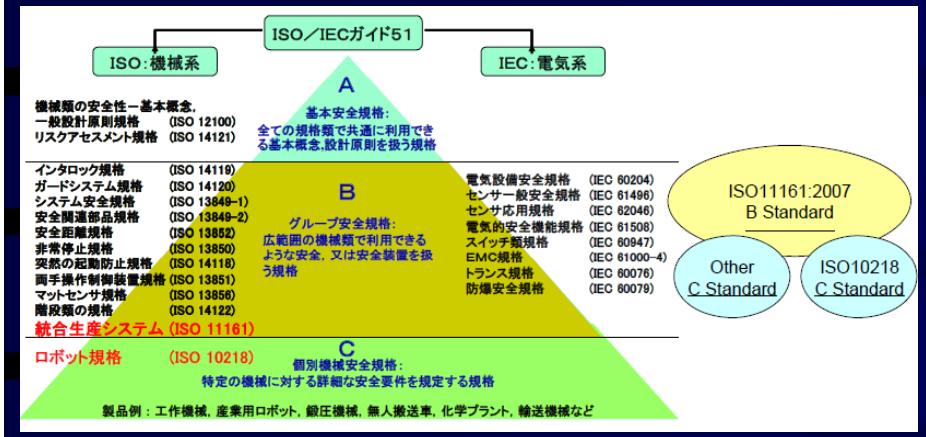
制御に悪影響を与えないで、オンラインで扱える技術が求められる。





現場は、安全操業が原則

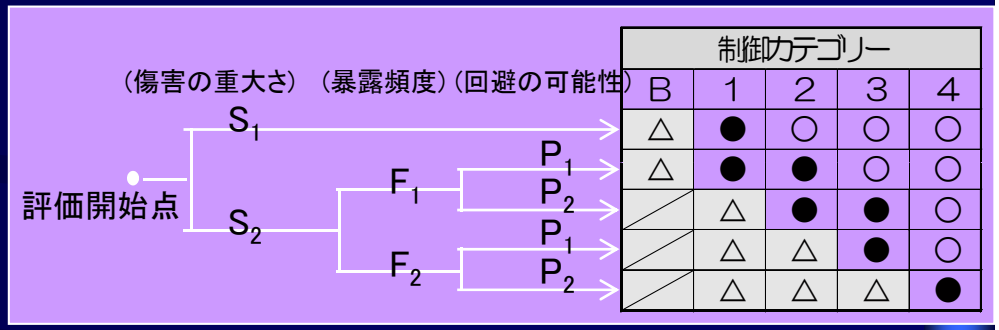
現場は、安全操業が原則なので、安全計装＋セキュリティ対策



http://www.jmf.or.jp/japanese/standard/pdf/D_1.pdf

リスク査定（見積もり）

危険度をランク分けし危険度に対応した制御カテゴリーを適用する



数値の基準：

傷害の重大さ	S：1：軽症（残傷害なし）		2：重傷（残傷害あり）
発生頻度と時間	F：1：まれに発生か短時間		2：頻繁に発生するか長時間
回避の可能性	P：1：ある場合には可能		2：困難

安全カテゴリーの選定：●：通常選定　△：追加手段を併用して選定可　○：余裕ある選定

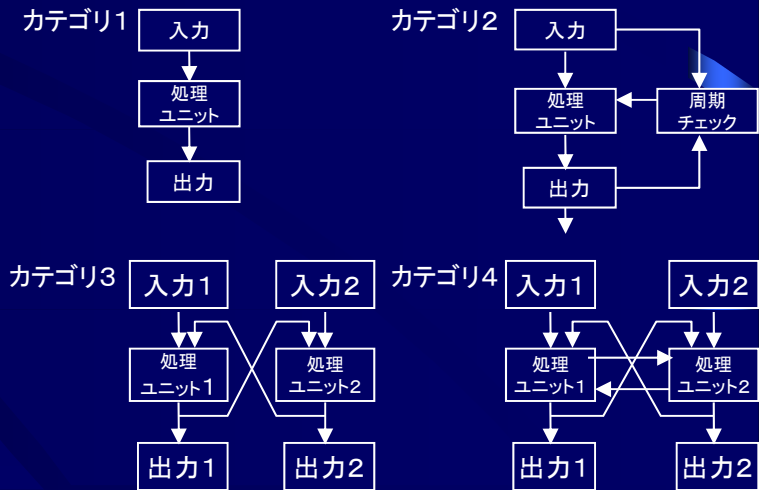
本質的安全設計対策（危険源を除去／リスク低減）

- 幾何学的要因及び物理的側面を考慮した対策
- 機械設計上の一般的技術知識を考慮した対策
- 適切な技術選択による対策
- 構成品間のポジティブな機械的作用原理を適用した対策
- 機械の安定性に関する対策
- 機械の保全性に関する対策
- 人間工学及び行動学原則を考慮した対策
- 電気的危険源防止対策
- 圧力／温度設備の危険源防止対策
- 制御システムへの本質的安全設計対策
- 安全機能故障のリスク低減対策
- 設備の信頼性を脅かす危険源防止対策
- 搬入（供給）又は搬出（取出し）作業の機械化及び自動化による危険源防止対策
- 設定（段取り等）及び保全の作業位置を危険区域外とすることによる危険源防止対策

＜JIS B 9700-1 3.19、JIS B 9700-1 4参考＞

セイフティのカテゴリは一旦決めて実現したらそれが継続するが、セキュリティのカテゴリは、未知の脆弱性が発見されたら、0レベルになる。よって、レベル維持管理できることが重要となる。

故障発生時の安全回路の一般的な構成



3Dシミュレータの活用

計画時・装置受入れ試験時・総合試験時・トレーニング用、各種確認検証用

計画時

1. 生産ライン設計での生産能力確認
2. 各プロセスでの装置の性能仕様や機能仕様の確認
3. 生産能力の計画に合った装置台数の確認
4. 装置配置の適正確認
5. 搬送機の軌道と搬送性能の確認
6. 装置と搬送機の情報伝達性能の確認
7. 故障等のシステム影響の確認

装置受入れ試験時

1. 装置単体試験でのプロセス前後のインターフェース突合せ試験
2. 装置単体性能試験

総合試験時

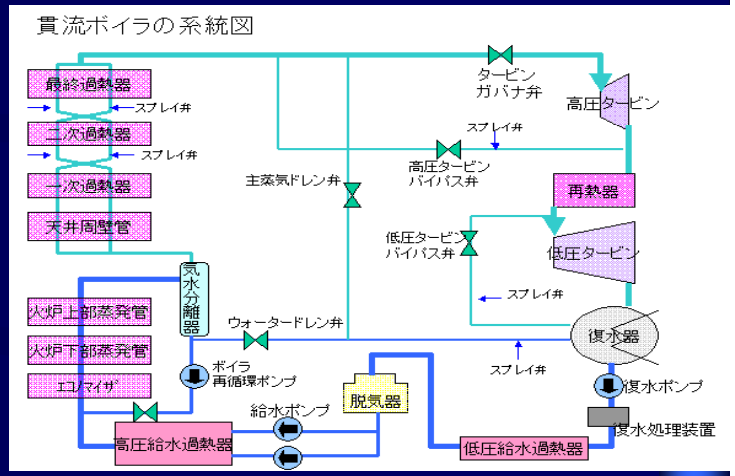
1. 総合試験・性能確認

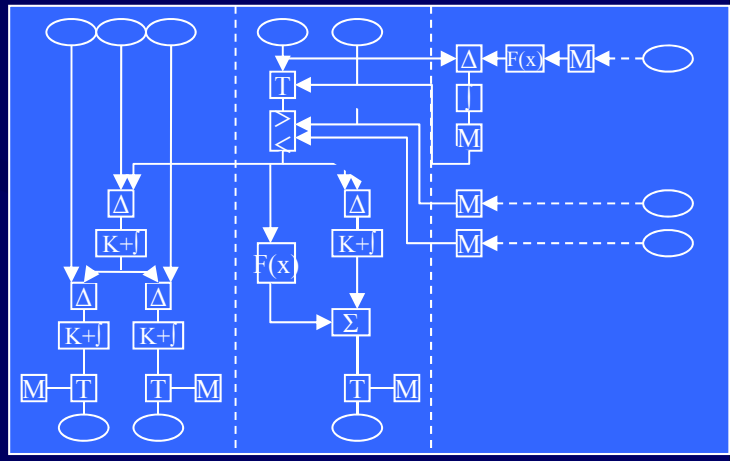
トレーニングシミュレータ

1. 新人教育用：通常運転時のトレーニング
2. 実ラインではできない異常対応トレーニング

検証用シミュレータ

1. 実ラインではできない異常時の対処確認
2. トラブル原因確認
3. 安全確認の見渡し確認
4. Know How情報蓄積の確認

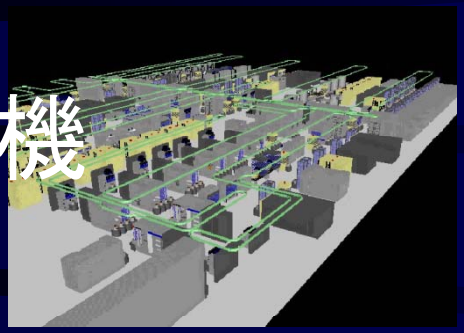




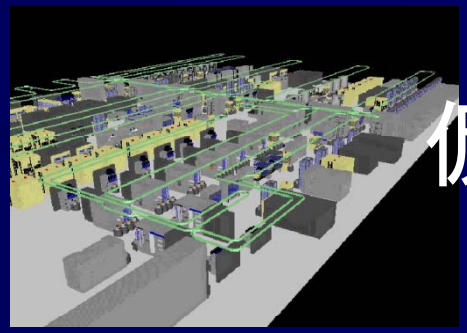
3Dシミュレータの活用

運用時　実機ラインとシミュレータを比較

実機

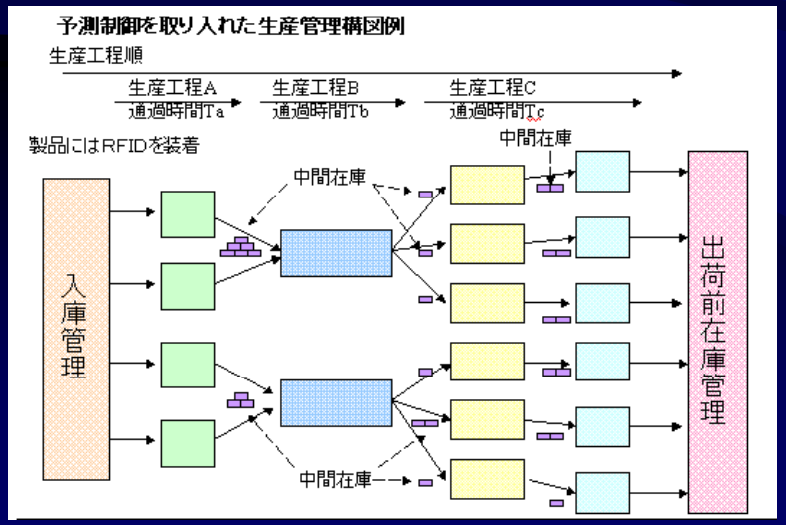


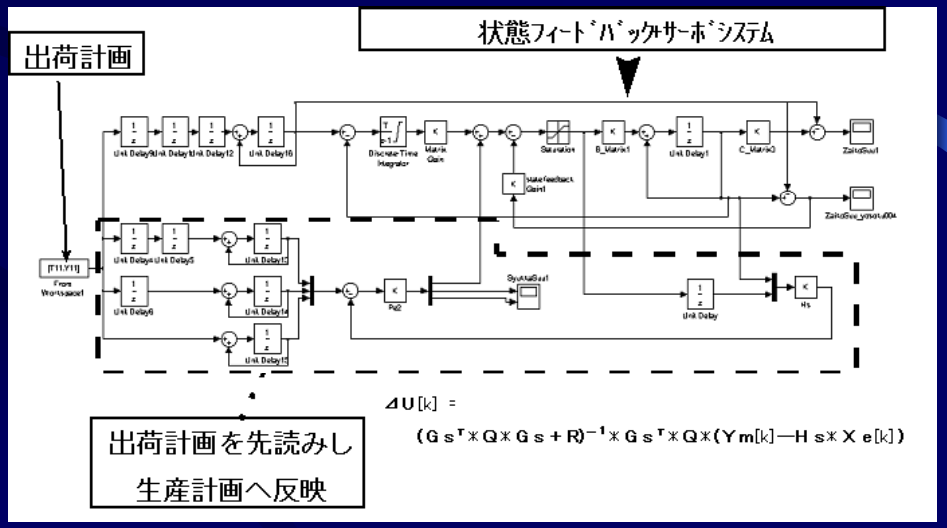
ミラーリング技術



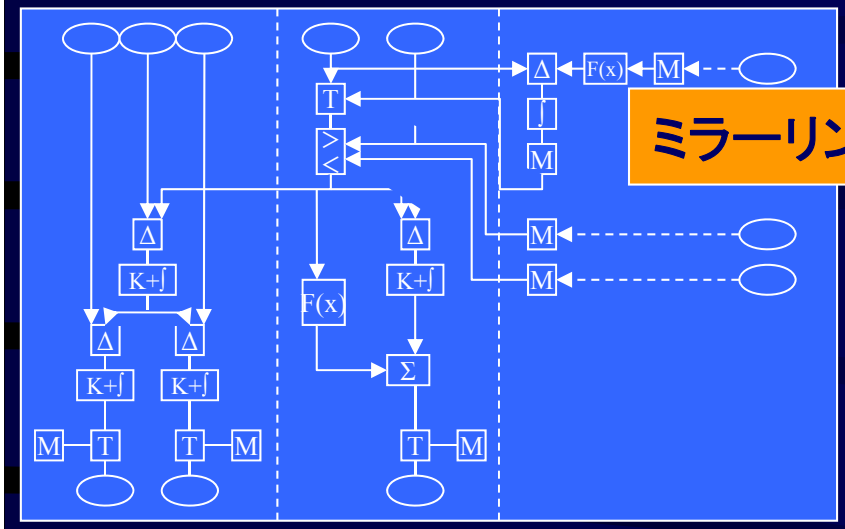
仮想

1. 実機ラインから上がってきたデータとシミュレーションを付き合わせると、実機の異常予兆をとらえて、予知保全が可能　⇒　振る舞い監視
2. 装置異常時の保管処理で生産能力をコントロール
3. 中間在庫の適正管理

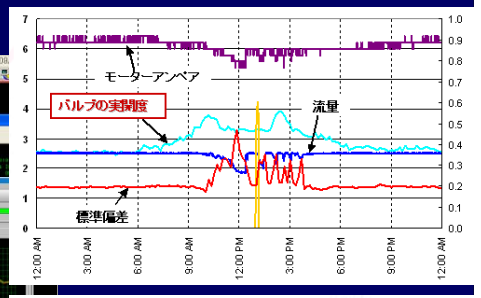


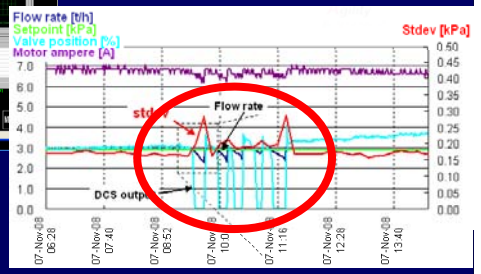


ミラーリング技術を活用した振る舞い制御監視の一例

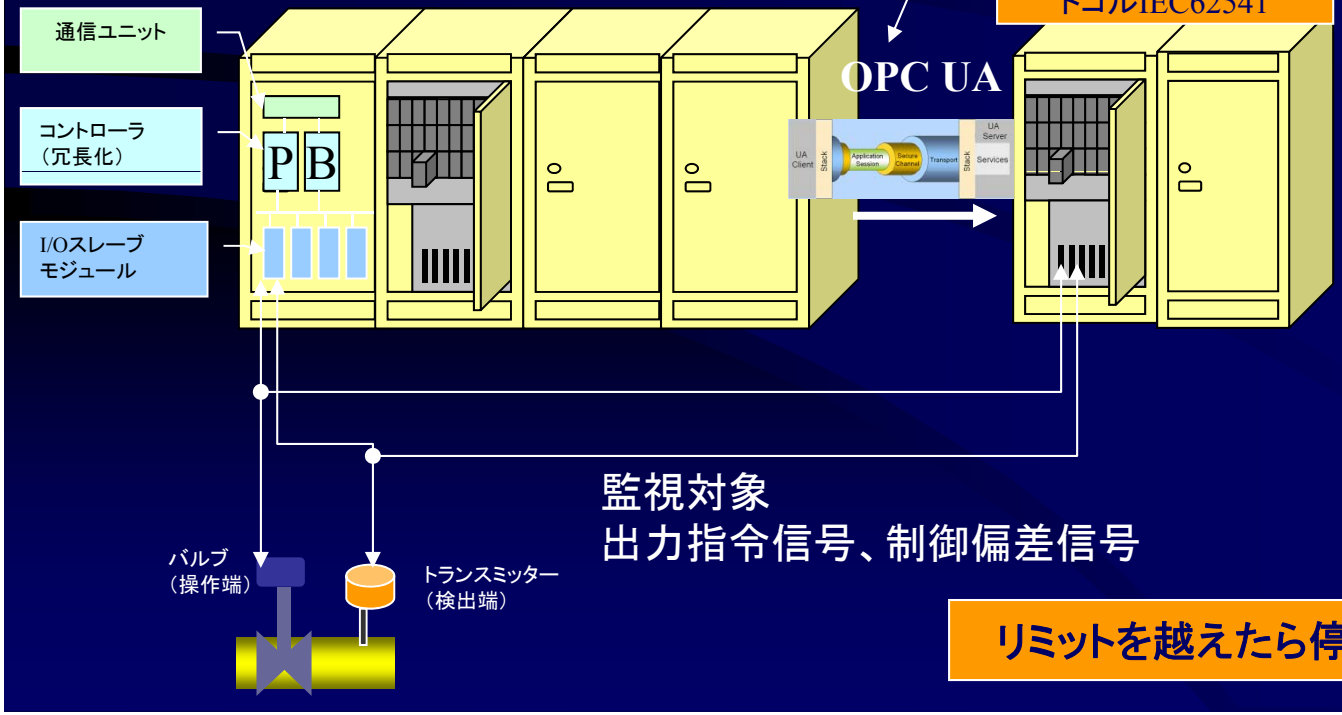


ミラーリングによる振る舞い監視

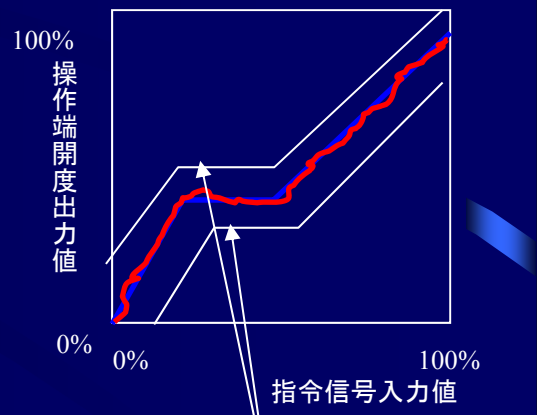




監査機能・セキュリティ機能つき通信プロトコルIEC62541



監視対象
出力指令信号、制御偏差信号



リミットを越えたら停める

制御上ありえる領域にリミット監視をつけて、異常な振る舞いを監視する。

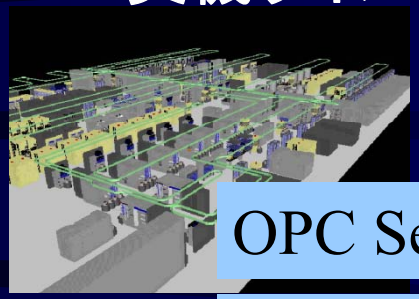
ミラーリング技術を活用した振る舞い制御監視の一例

実機ライン

Production plan

Scheduler

Command Server

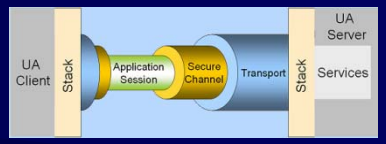


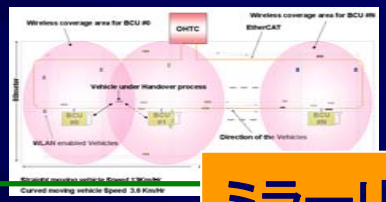
OPC Server

Wireless communication

監査機能・セキュリティ機能つき通信プロトコル IEC62541

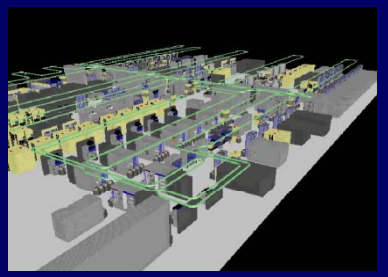
OPC-UA





3D Simulator

MATLAB



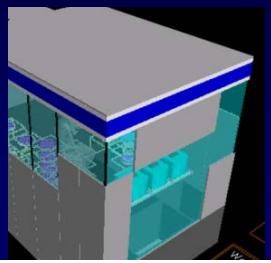
ミラーリングによる振る舞い監視

Device/Machine

Controller

EtherCAT

Sensor | Drive | Motion

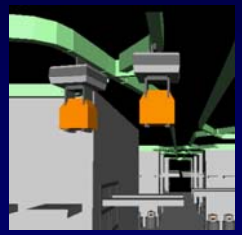


AGV

Controller

EtherCAT

Sensor | Drive | Motion



Server

Middleware

RFID

Controller

Ethernet-IP

Device-net

Integrated System

制御ベンダ／装置ベンダ／Sierに求められる
セキュリティ対策についての提言

ご清聴ありがとうございました。

制御システムセキュリティ検討タスクフォース
普及啓発WG座長
IAF/VEC事務局長　村上正志