ユーティリティ制御システム ネットワークの情報共有とセキュリティ

Improving Cyber Security on Networked Monitoring and Control Systems for Utility Facilities

制御システムセキュリティカンファレンス2009,
JPCERT/CC, 2009/2/19

高野 正利　トヨタ自動車(株)
Masatoshi Takano, Toyota Motor Corporation
計測自動制御学会　産業応用部門　ネットワーク部会
Technical Committee on Instrument and Control Networks,
The Society of Instrumentation and Control Engineers (SICE)

アウトライン
Table of contents

1. プラントシステムへの要求と課題
Vision of ICS

2. プラントシステムのセキュリティ
Cyber security for ICS

3. まとめ
Conclusion

1. プラントシステムへの要求と課題

Vision of ICS

1) ヒューマンインターフェースの進化

Human-centered interfaces

2) プラントデータの情報共有

Information sharing through systems

3) 柔軟に変化へ適用できるインフラシステム

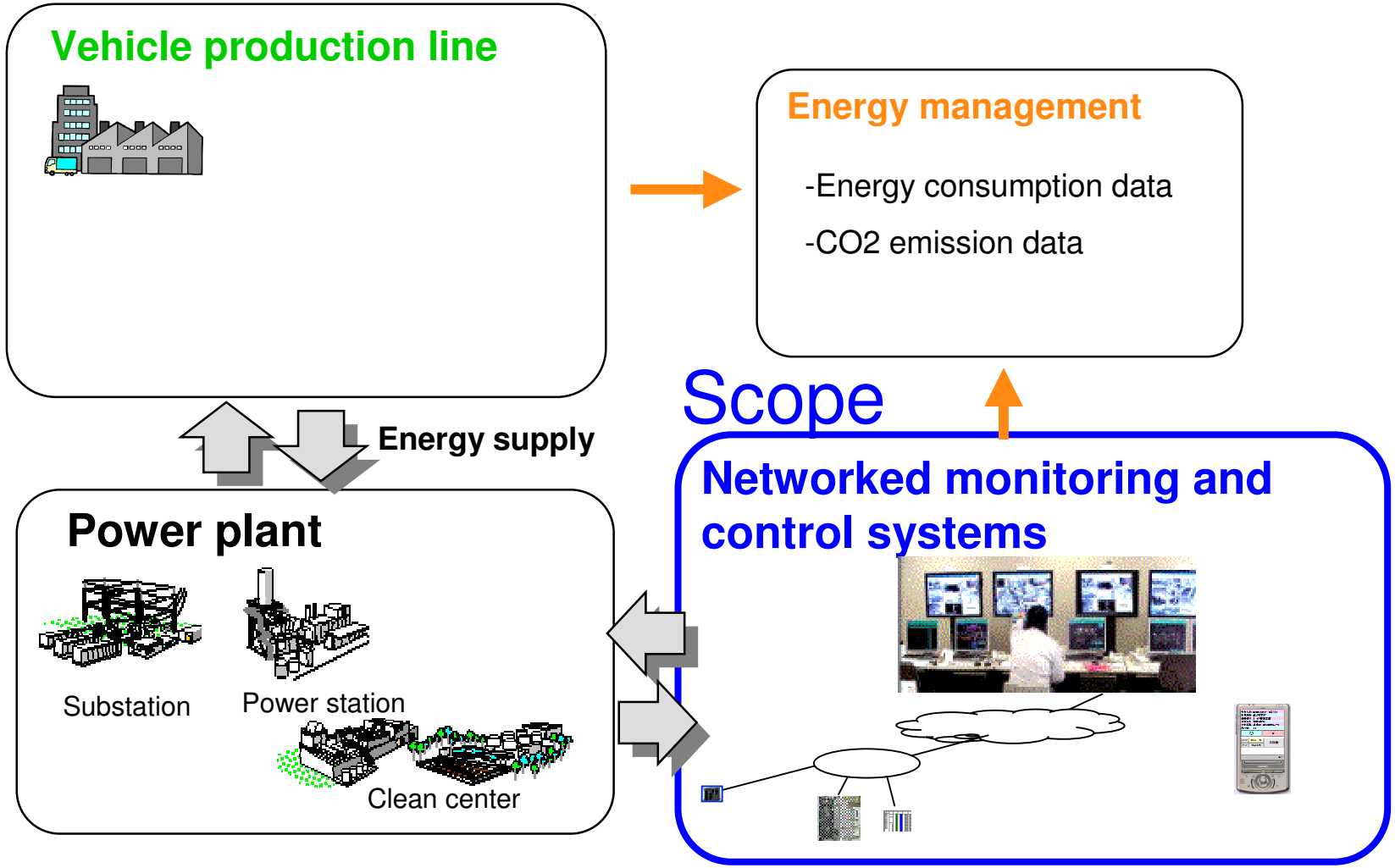
Flexible reconfiguration

対象となるネットワーク型プラントシステム

Scope: Networked monitoring and control systems used in critical infrastructures such as in utility facilities

ネットワーク型プラントシステム

Network-based ICS



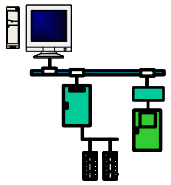
1) ヒューマンインターフェースの進化

Human-centered interfaces

Computer-centered → *Human-centered*

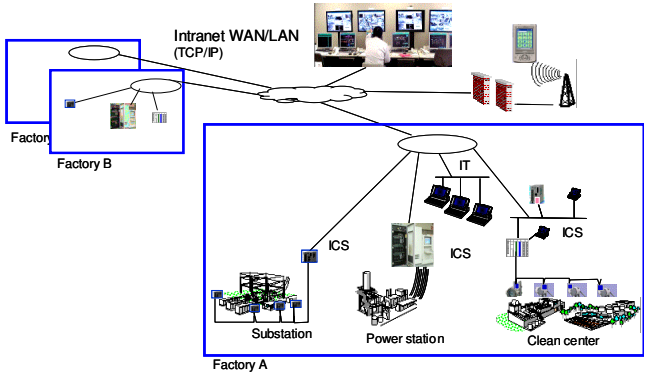
個別（ローカル）

Stand alone /LAN



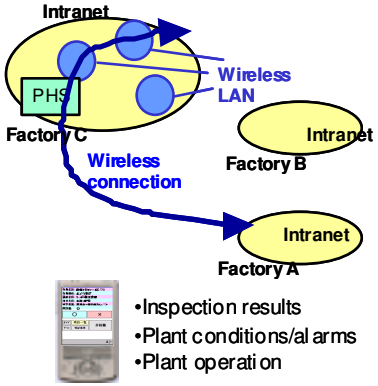
広域ネットワーク監視

Wide area network



どこでも運転監視

Remote operations in any location



ITシステムと共通のネットワーク

Common network sharing with IT systems

シームレス通信

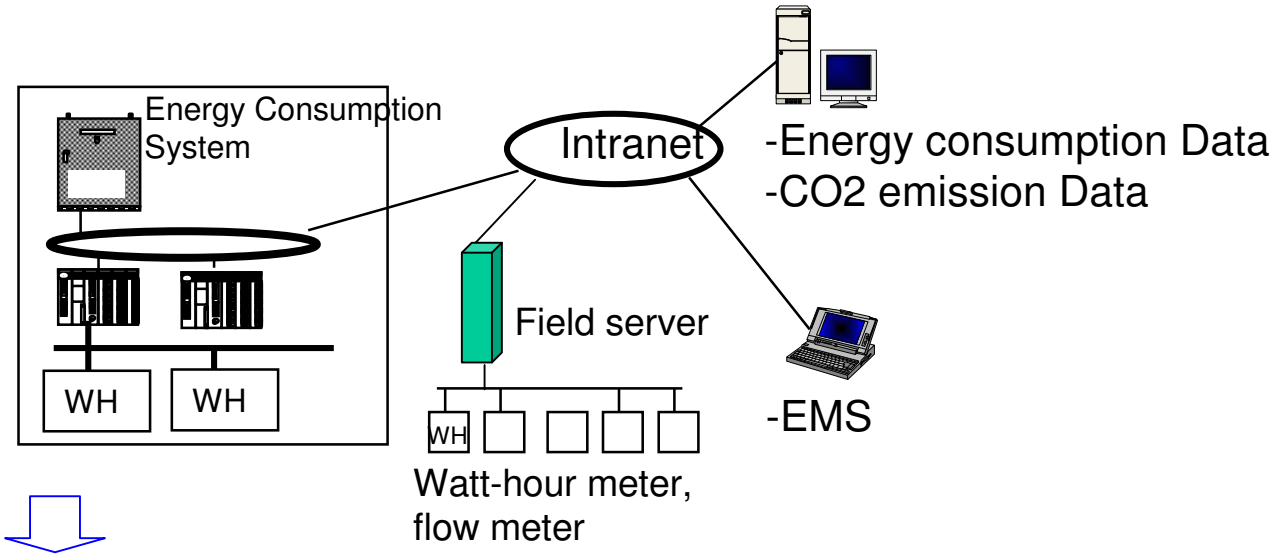
Seamless communication

2) プラントデータの情報共有

Information sharing

・工程別エネルギー使用量の日常管理
・各マネジメントレベルでの活用

Daily check system of energy consumption volume per each manufacturing department
Data sharing on energy consumption at each level



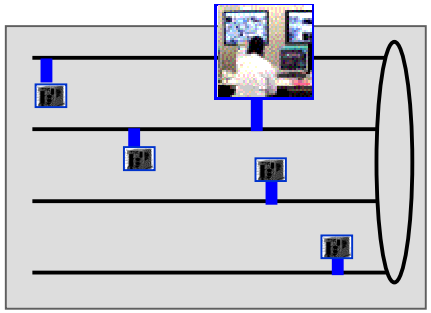
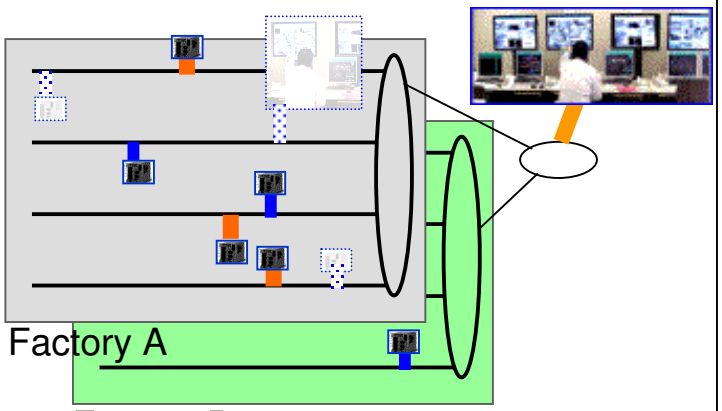
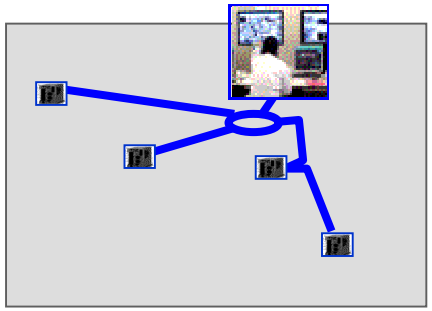
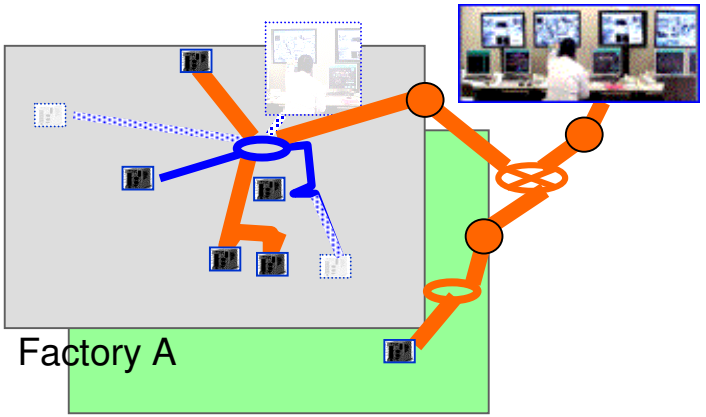
シームレス通信
Seamless communication

Connectivity between systems on a local and global basis contributes to information sharing.

3) 変化へ適用できるインフラシステム

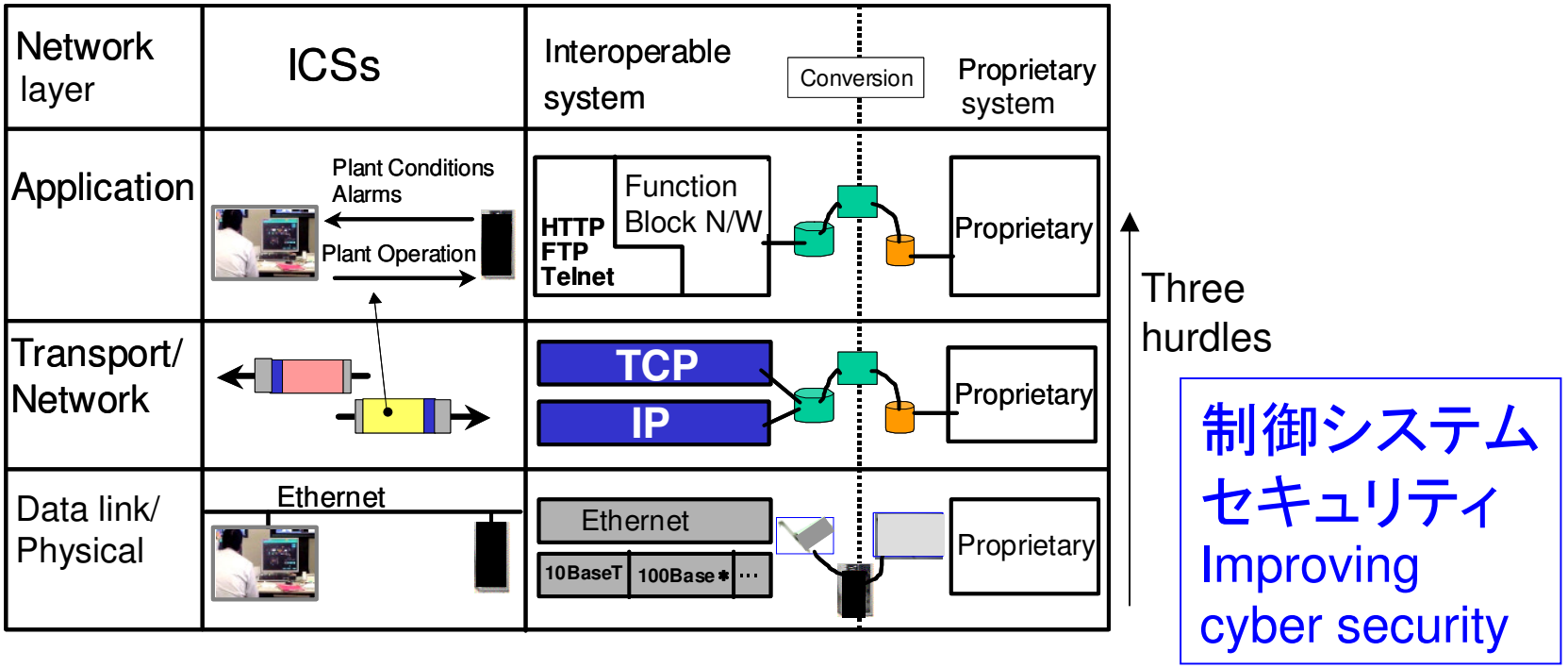
Flexible reconfiguration

Initial network
Additional network for change

制御ネットワーク Plant network	導入当初 Initial	生産ライン，運転監視の変更 Adaptation to new production lines	適用度 Effect
基幹ネットワークの共用 Use of TCP/IP network sharing with IT			最少限のネットワーク工事で適応可能 Minimum additional network
プラントシステム独自ネットワーク Proprietary network			ネットワークの大幅な再構築 工場間の専用線要 Reconstruction

シームレス通信
Seamless communication

TCP/IPによる
制御システムと情報システムとの接続
Plant control system must be connected with plant business systems.
Control networks need to employ TCP/IP/Ethernet.



2. プラントシステムのセキュリティ

Cyber security for ICS

1) ITとは異なるアプローチ

Difficulties of ICS cyber security/ Seeing in a different light

2) 岐路にあるプラントシステム

Crossroads of ICS

3) 考えられる脆弱点

The vulnerabilities of today's ICS

4) 最小限のプラットフォームサービス

Minimum platform service

5) 多階層での防御（例）

Defense-in-depth strategy

1) ITとは異なるアプローチ

Difficulties of ICS cyber security

Category	IT systems	ICSs
Status	State-of-the-art	A couple of generations behind IT
Update mechanism	Employ online real-time update mechanisms for security patches or virus pattern files Minor monthly update Major annual update, or on a more frequent basis Life cycle: 3 to 4 years	Might not run security software, or may require processes to discover whether new security patches or virus pattern files work correctly Minor annual update Life cycle: 10 to 15 years
Examination	Have almost no checks on applications	Examine the availability and performance impacts of using the security software
Computing capacity	Can expand	Are difficult to expand

1) ITとは異なるアプローチ（続き）

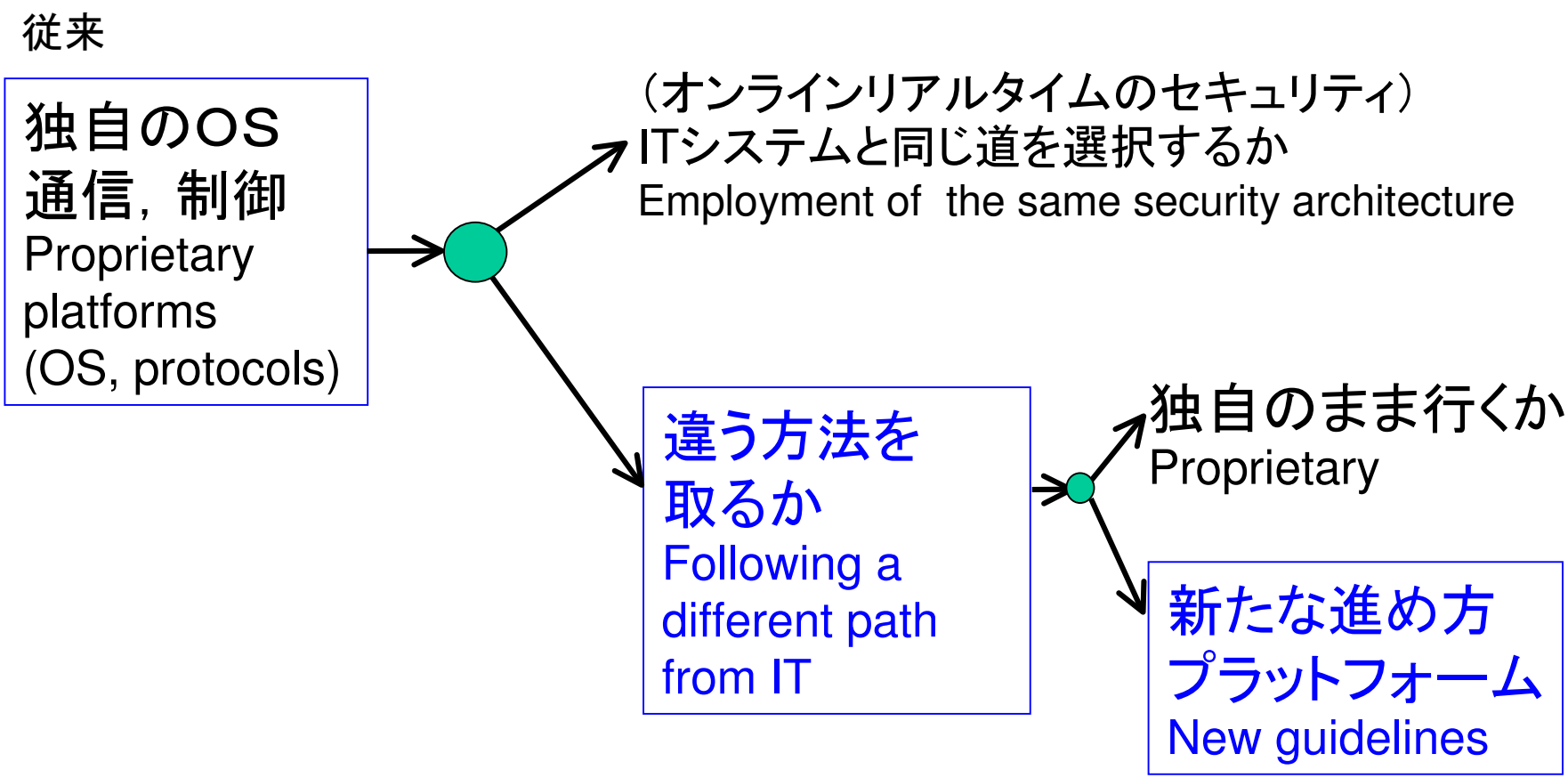
Seeing in a different light

- The secret of proprietary protocols for controller level communications does not protect the systems.
- Patched systems have also unknown vulnerabilities which can result in zero day attacks.

- The availability of ICS controllers should have priority over database servers or human interfaces of ICS.
- Unusual execution of control software causes operation disruptions because ICSs are used in critical infrastructure such as utility facilities control systems.

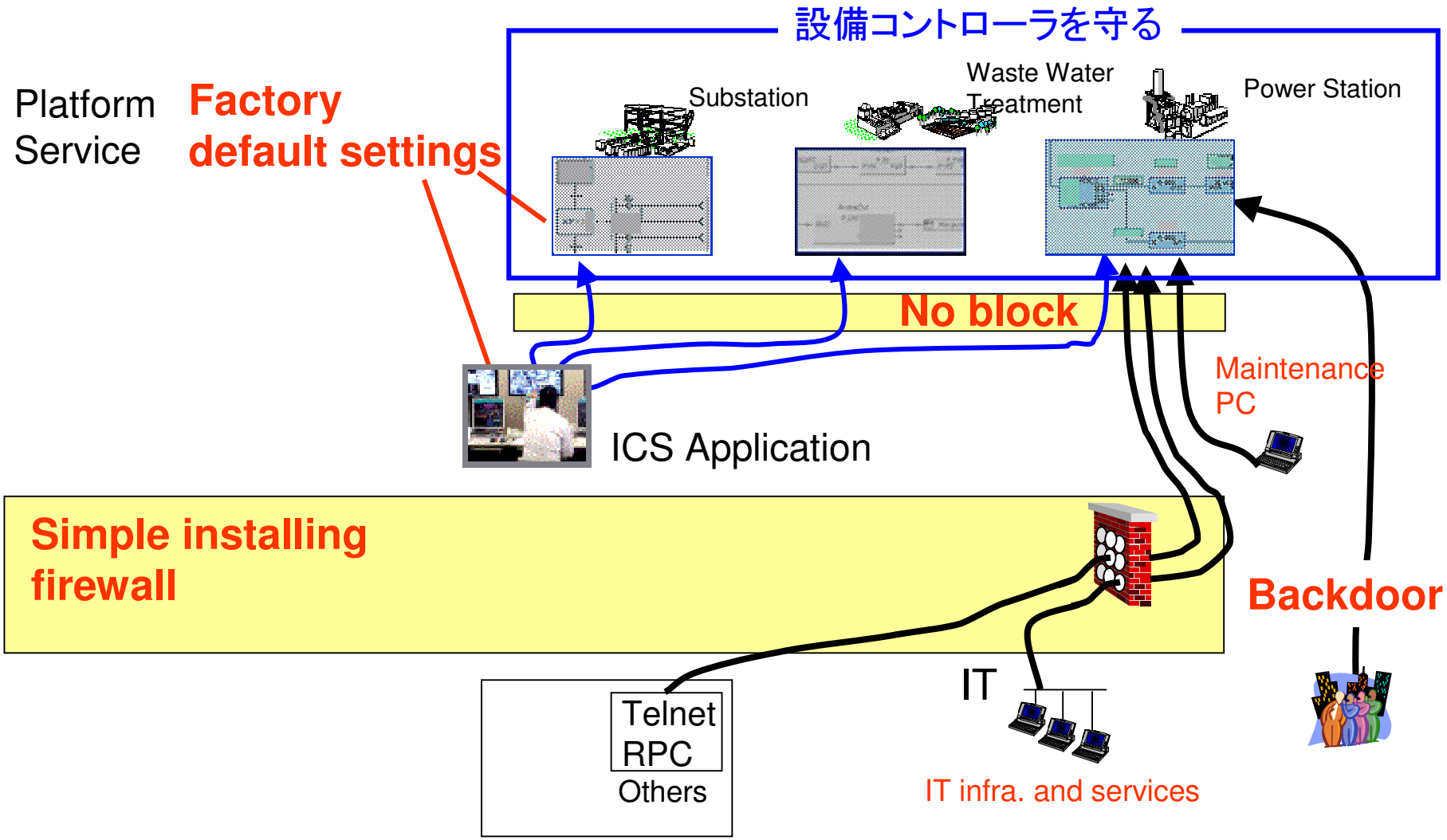
2) 岐路にあるプラントシステム

Crossroads of ICS



3) 考えられる脆弱点

The vulnerabilities of today's ICS

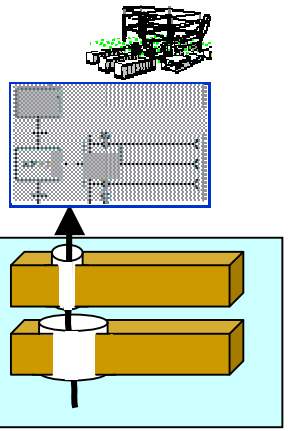


4) 最小限のプラットフォームサービス

Minimum platform service

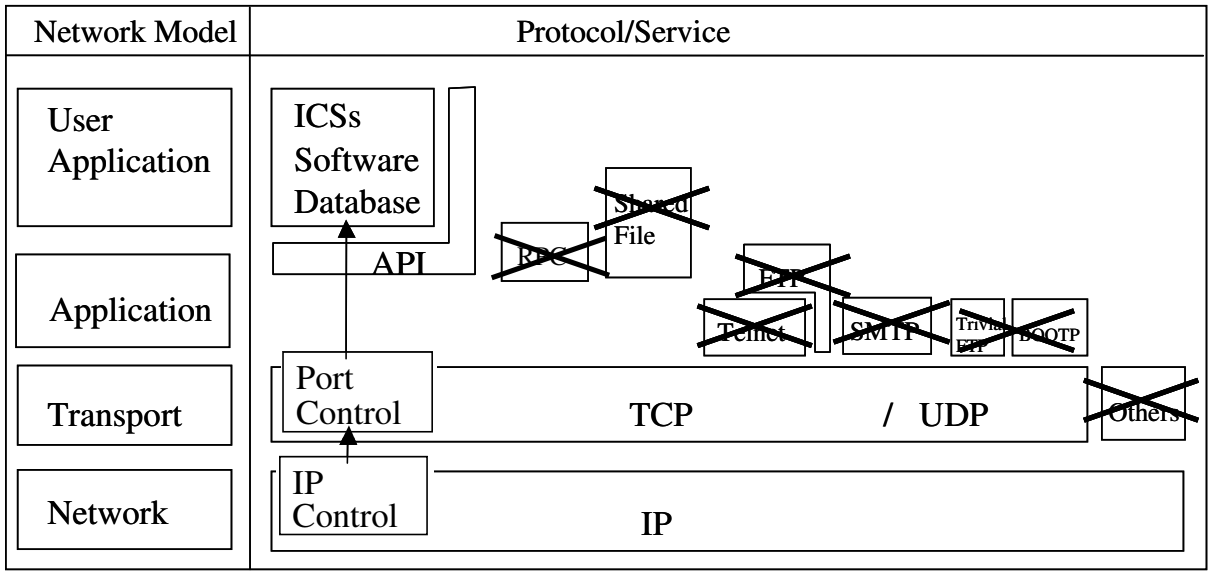
Minimum Platform Service

Limitation of Application
-ICS Control software,DB



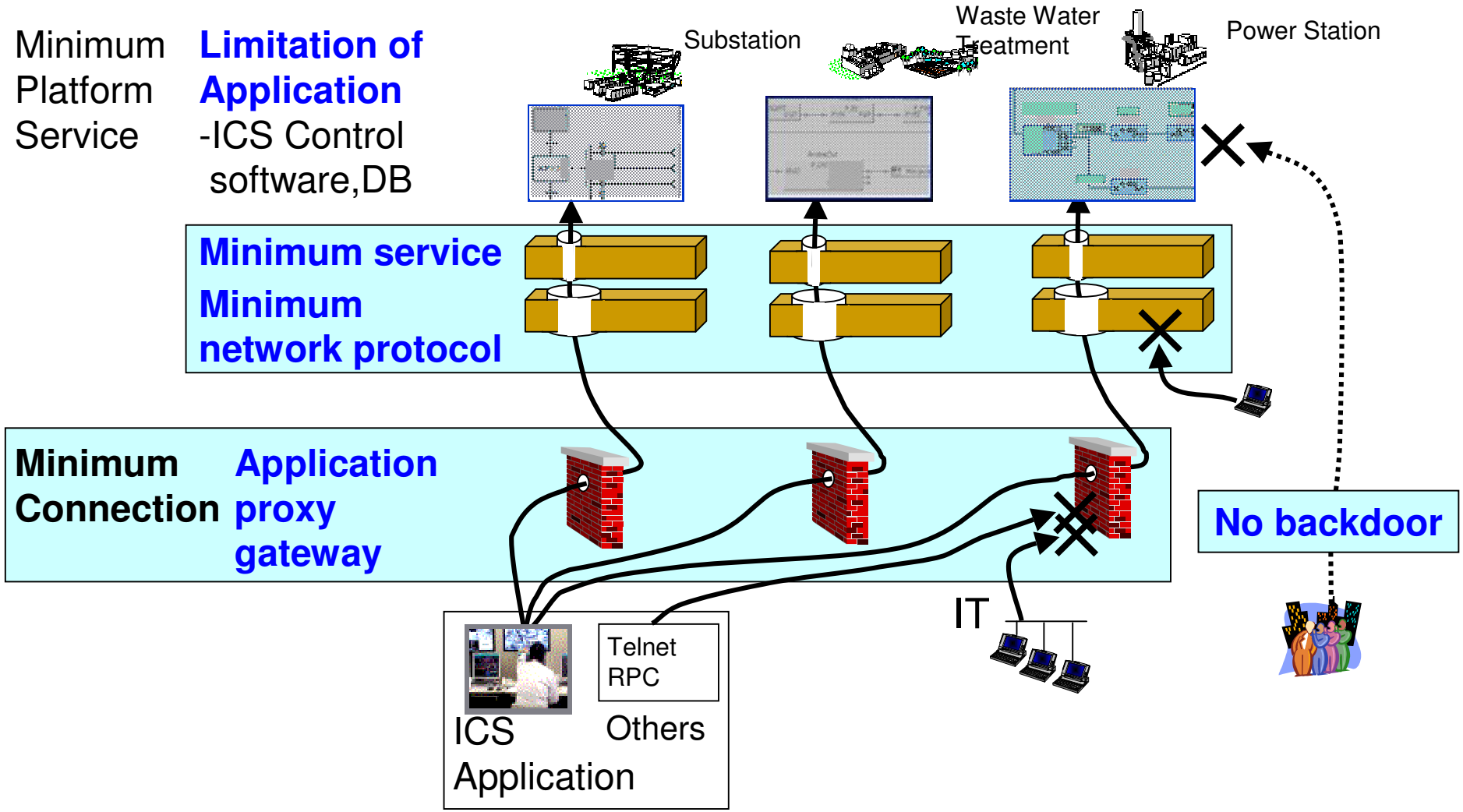
Remove unused services.

The application layer adopts only control functions and the network layer employs only TCP/IP.



5) 多階層での防御(例)

Defense-in-depth strategy



3. まとめ
Conclusion

サーバではなく,
設備を制御しているコントローラを守ることが最優先
（組み込みシステムにもセキュリティ問題あり）

・最小限のソフト，通信ドライバの組み込み
Minimize platform services and network connections.
・Application proxy gatewayの必要に応じた採用
・多階層防御
Defense-in-Depth strategy
Cyber security defense must be layered to reduce the risk of security incidents.

→多層防御により，現場をある期間（1Yはそのまま）は維持

参考文献

Masatoshi Takano, Sustainable Cyber Security for Utility Facilities Control System based on Defense-in-Depth Concept, SICE Annual Conference 2007

Masatoshi Takano, Human-Centered Industrial Control Systems through Seamless Communication and Flexible Reconfiguration , SICE Annual Conference 2008