INDUSTRIAL AUTOMATION

“Layers of Network Protections”

a Journey into Fundamentals of OT Network Reference Architecture

November 2020

“Layers of Network Protections”

Speaker

Tobias Nitzsche

ABB Cyber Security Practice Lead (CISSP CISCM)

In this Presentation, we will provide background and technical reasoning behind the layered approach to OT network design. We will show the engineering and cyber security benefits of the reference architecture network design. And importantly, we will illustrate how reference architecture allows for an efficient (almost “plug and play”) and secure implementation of complex digital solutions, including field-to-cloud data highways, as well as adding additional services to existing network installations. It is hoped that by the end of the presentation the audience will recognize the value of the initial expenditure on implementing reference architecture design and see it as a wise and well worth long-term investment.’

Tobias.Nitzsche@de.abb.com

“Layers of Network Protections”

Agenda

1. Cyber Security challenges facing process facilities
2. Why Reference Architecture?
3. Introducing Cyber Security Reference Architectures
4. Reference Architecture Gap Assessment
5. Questions

Cyber Security challenges facing customers

Introduction – There are gains to be made in industry

Good times for Digitalization

condition monitoring – predictive maintenance – Anomaly Detection for DCS

Why Reference Architecture?

Reference Architecture

The foundation for a cyber secure system today and tomorrow

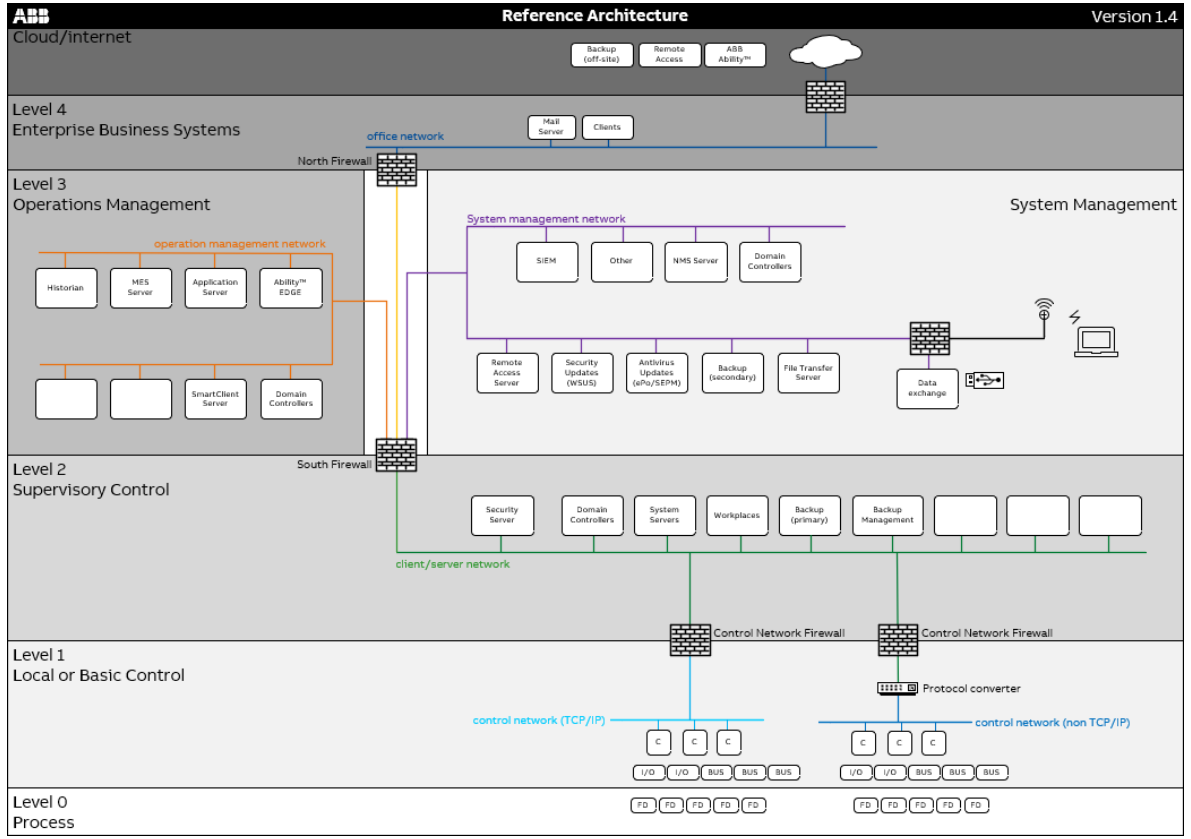
Definition

A reference architecture provides a **template solution** for an architecture for a particular domain. It also provides a **common vocabulary** with which to discuss implementations, often with the aim to stress commonality.

Benefits

Efficiently onboard new cyber security and digital solutions with no or minimal changes to the installed network/set up (aka maintain security posture)

Resilience – Compliance - Cloud Ready

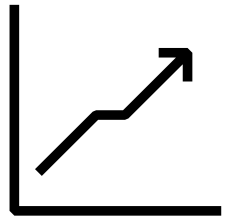


Different users

A reference architecture supports the business

Business needs

Evolving business needs require new functions features, and strong cyber security

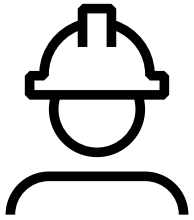


Functional drawings

A reference architecture makes it possible to meet the business needs without jeopardizing cyber security

Implementation support

Reference architecture reduces implementation times while preserving resilience



Introducing Cyber Security Reference Architectures

What is it

A proven and consistent approach to planning, implementing and deploying industrial control system networks using industry best practices and standards

Consistent

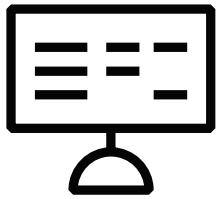
Provides a template solution for an architecture for a particular domain.

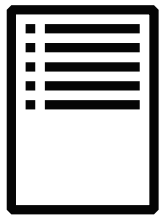
Compatible

Uses a standardized vocabulary for discussing implementations to help ensure commonality.

Compliant

Meets standards for mitigating current and future security vulnerabilities in industrial automation and control systems.



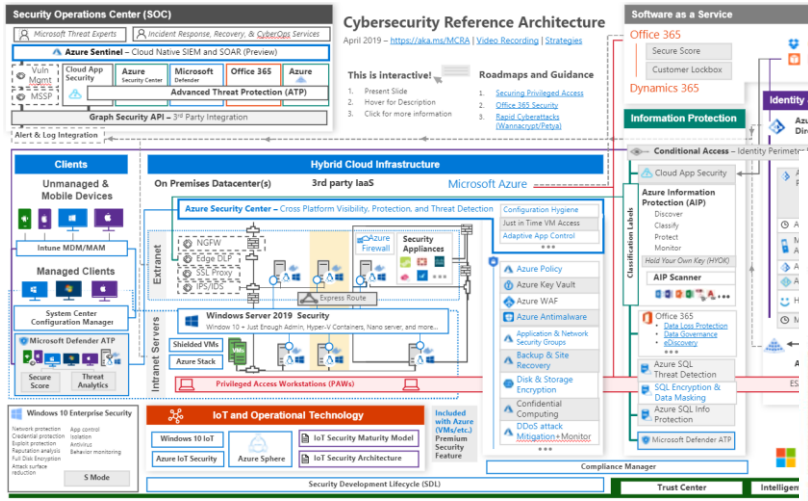


For example ready for IEC 62443 Security Level compliance

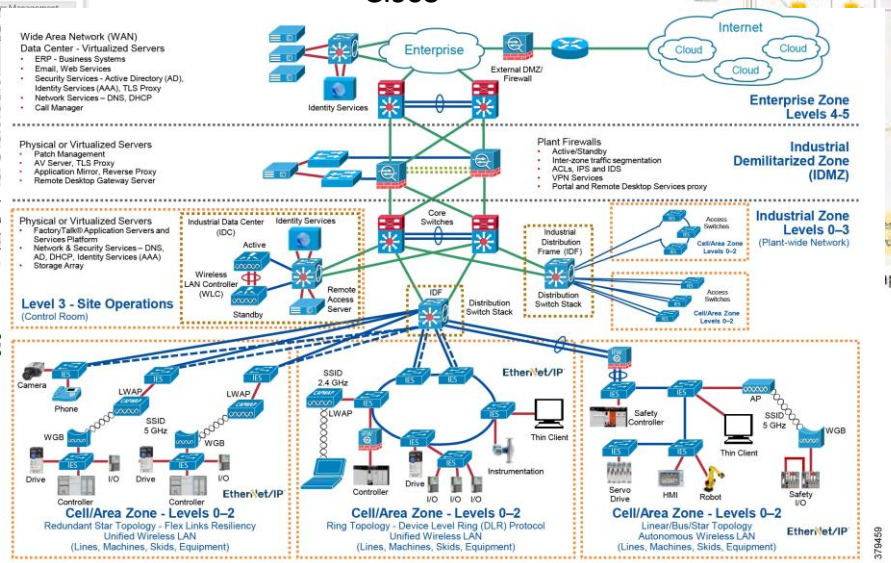
Examples of Architectures

Pick one that applies to your use case

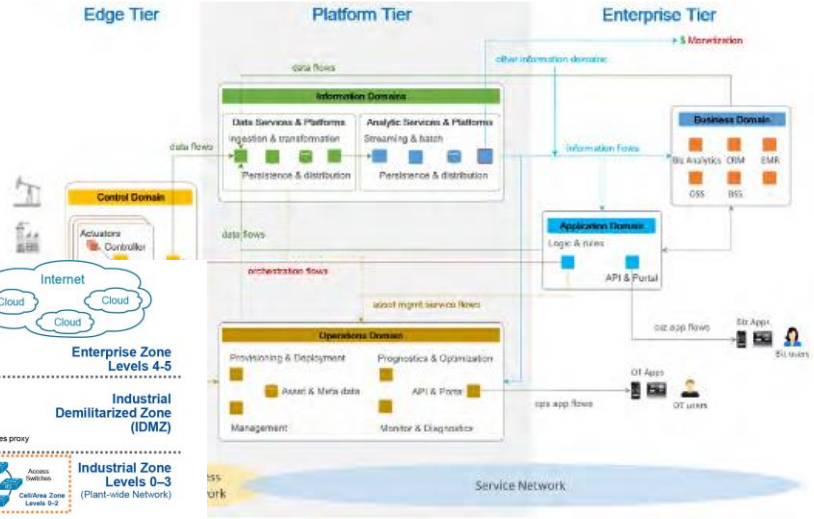
Microsoft



Cisco



IIC



pping between a three-tier architecture to the functional domains

How does it work

Leverages the same levels as detailed in the IEC 62443 reference model

Level	Description
4 **Enterprise systems**	Production scheduling, operational management and maintenance management for individual plants or sites in an enterprise
3 **Operations management**	Functions that manage workflows to produce end products
2 **Supervisory control**	Functions that monitor and control the physical process
1 **Local or basic control**	Functions that sense and manipulate the physical process
0 **Process**	Sensors and actuators directly connected to the process and process equipment

Reference Architecture

Security Levels*

Notes

The reference architecture makes it possible to design a system to achieve SL4.

However, the reference architecture doesn't suggest that by simply applying the recommendations will ensure compliance to SL4, nor does it imply that the reference architecture is certified.

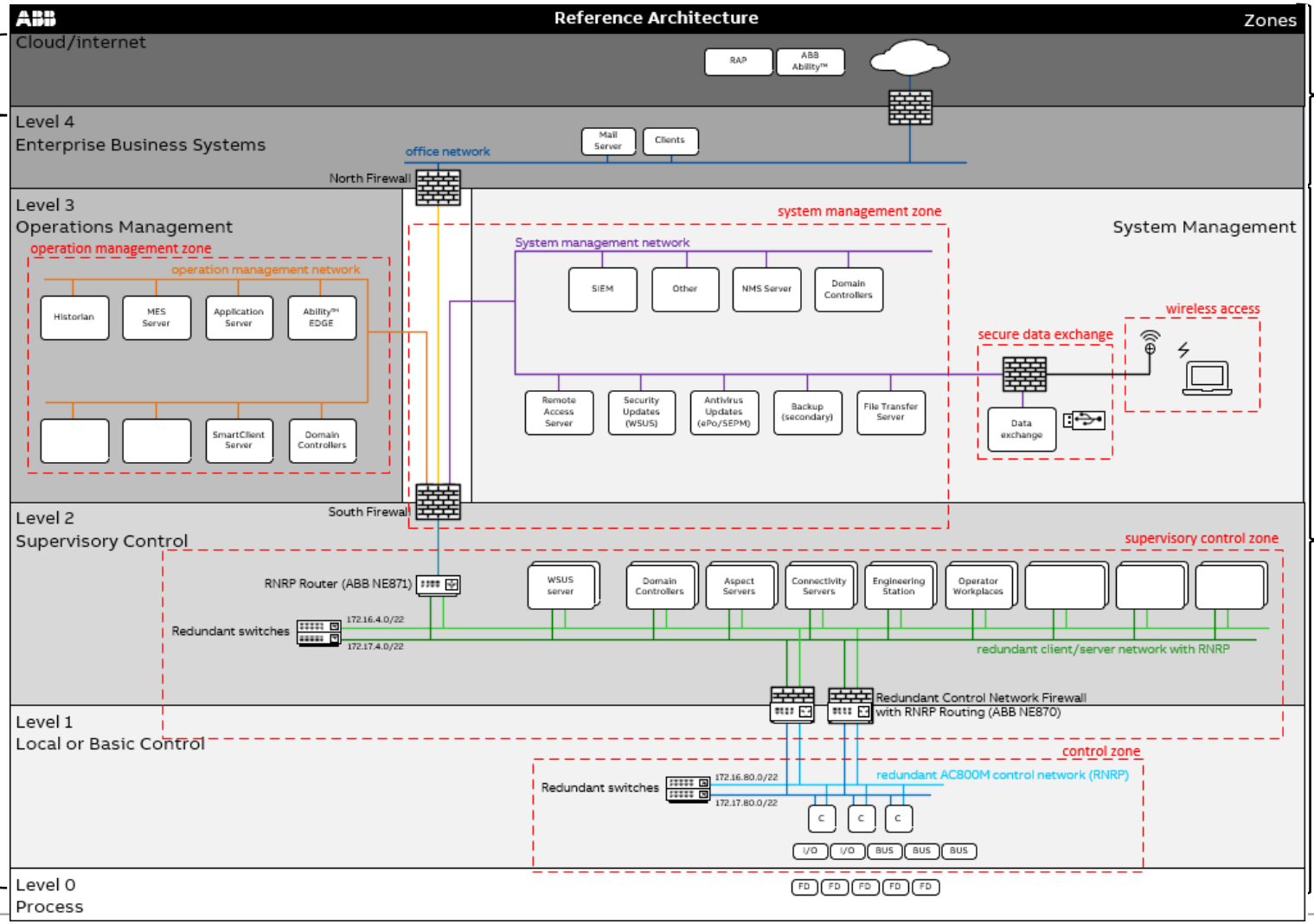
SL	Definition
1	Prevent the unauthorized disclosure of information via eavesdropping or casual exposure.
2	Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills and low motivation.
3	Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
4	Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS specific skills and high

*four SLs as defined in IEC62443-3-3:2013

Zones and Level

Cloud/internet network level

Network levels as defined in IEC 62443



Sample use case = Implement Security Updates automatically

Business View

Background

Plant needs automatic distribution of vendor-validated Microsoft security updates. Rated as security level 2,
all changes require a risk review.

Solution

ABB security update service that provides ABB-validated security patches via a secure remote connection.

Designed for the Reference Architecture where cyber security and IEC 62443 compliance are part of the development process.

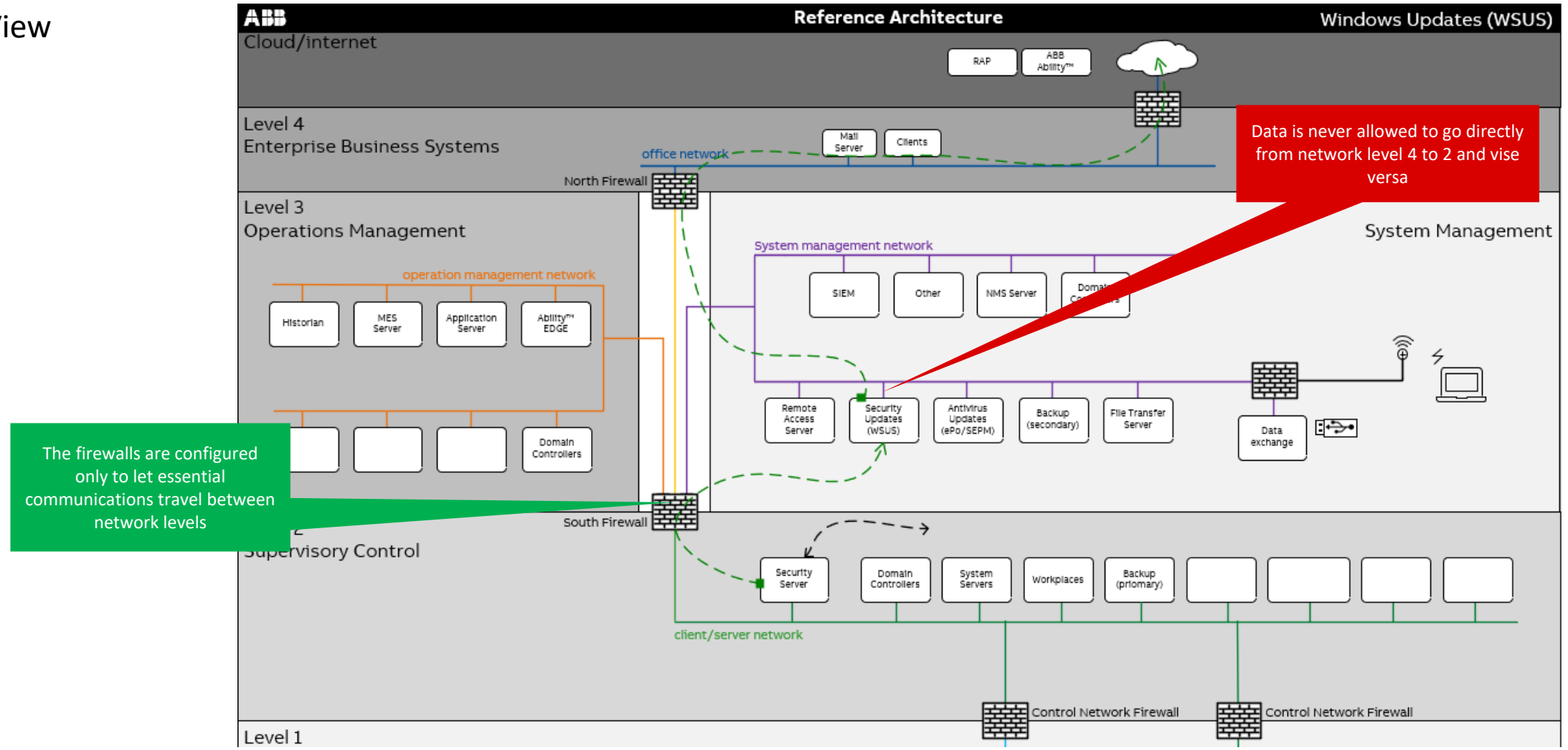
Benefits

- reduces planning and installation times
- eliminates the need for additional risk reviews
- delivers best-in-class cyber security through IEC 62443 compliance
- reduces development costs because the solution is reusable
- enhances security by reducing the cyber attack surface
- reduces the cost of implementation
- provides plants greater understanding of their network and assets

Shortens implementation times while reducing costs

Security Updates

Functional View



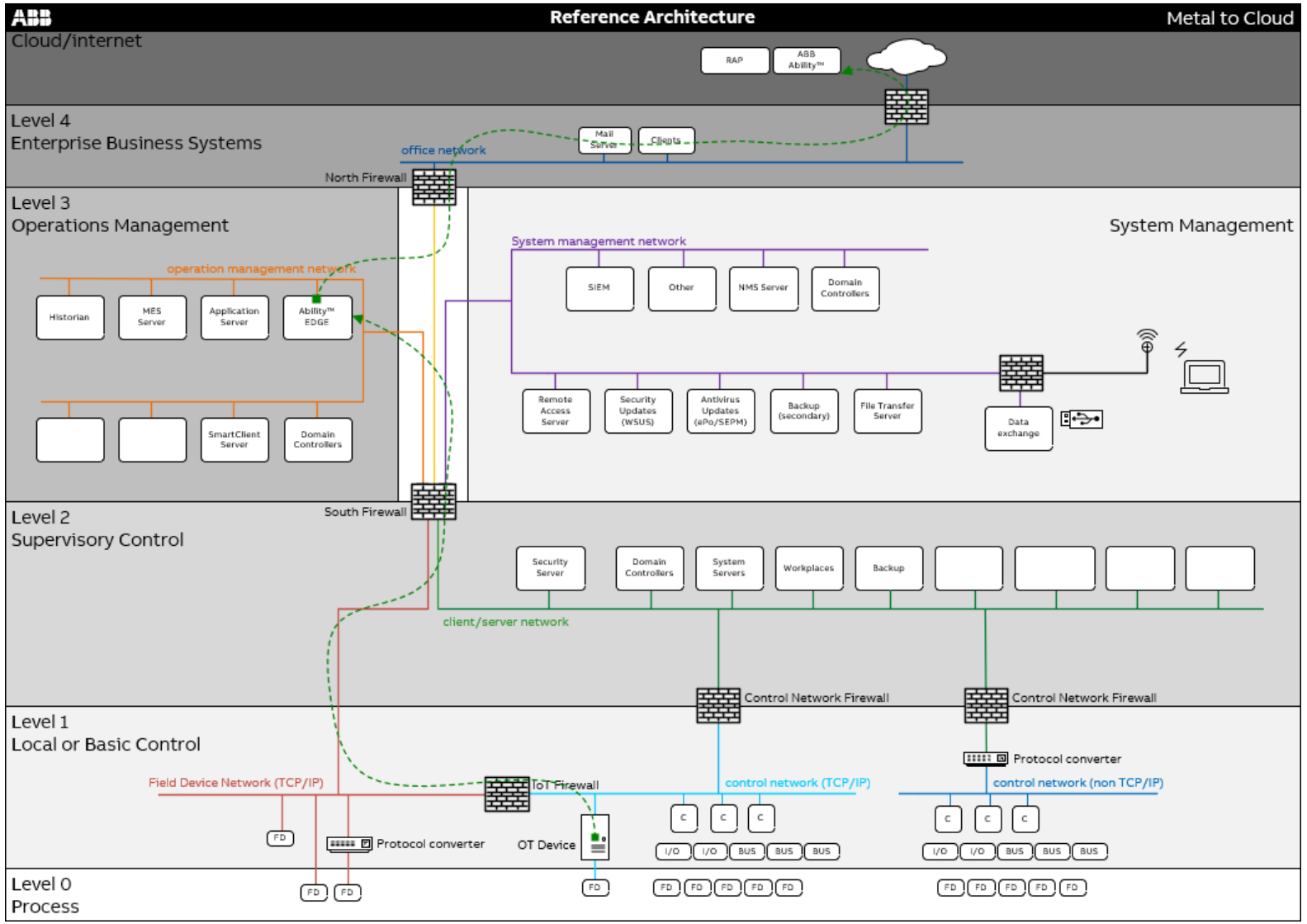
Reference Architecture

Metal to Cloud

Notes

There is data in Level 0 and 1 that can be used for data analytics in the cloud*.

Routing data through the DCS system is not efficient and expensive because it requires more I/O, more powerful CPUs, and more licenses.



* Digital Twins, Artificial Intelligence, or Machine Learning are examples of cloud analytics.

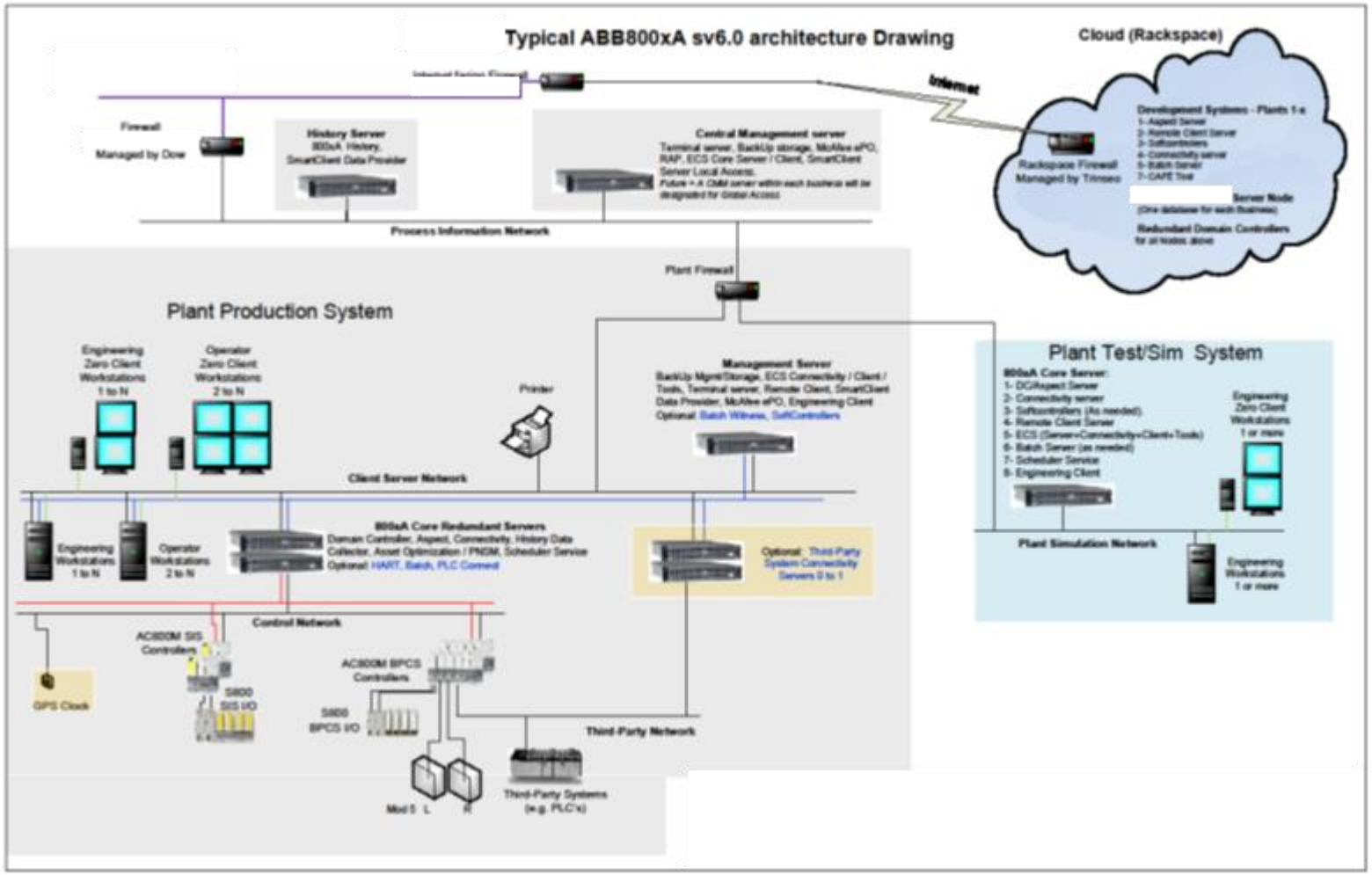
Gap Assessment

Customer ABB 800xA

Typical Architecture

Customer provided a network architecture drawing that represents their typical ABB 800xA sv6.0 system implementation.

The next slide will transform this drawing into the ABB Reference Architecture format.

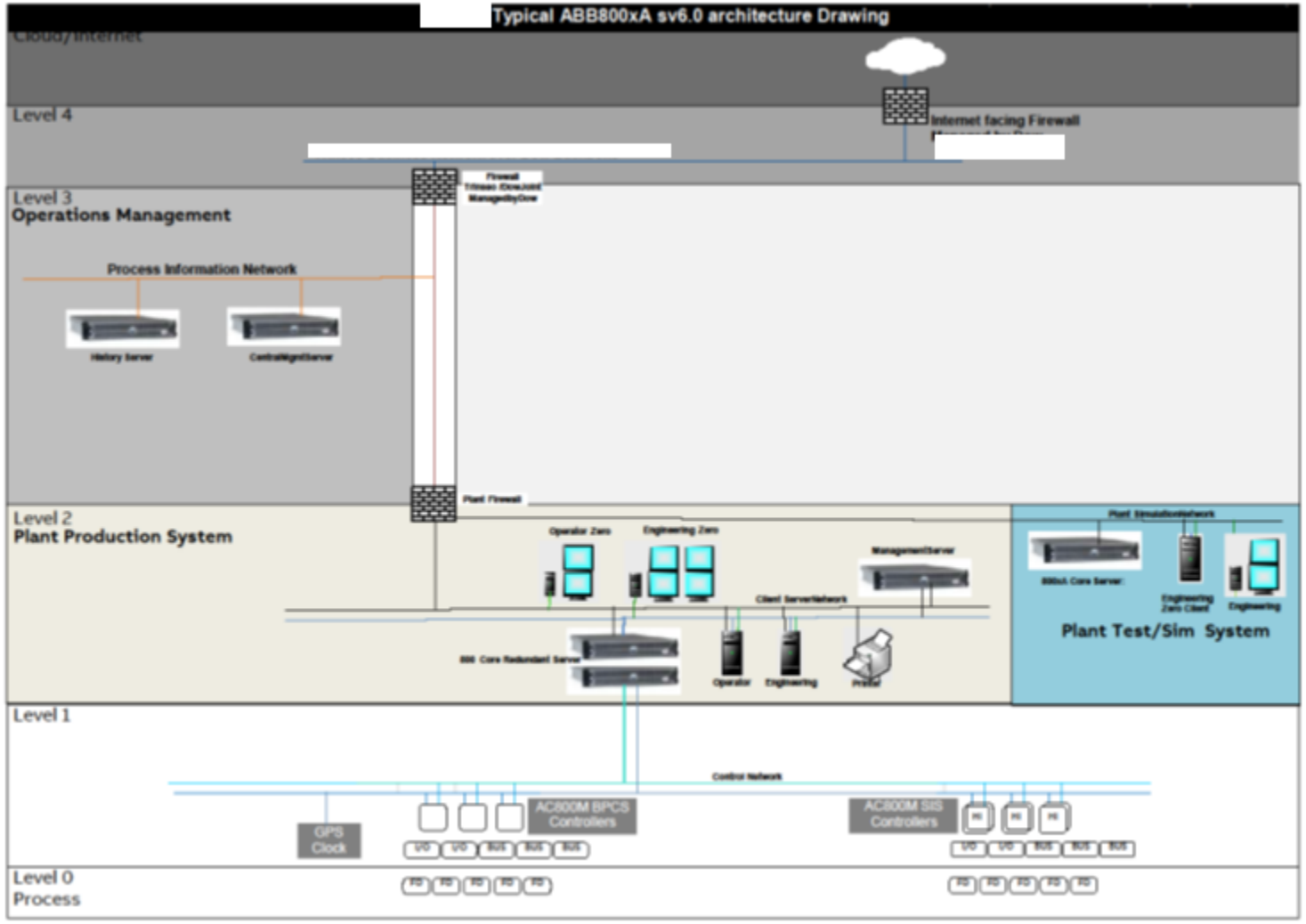


Customer Architecture

Transformed Architecture

This is a transformation of an customer's architecture into the ABB reference architecture format for easy comparison.

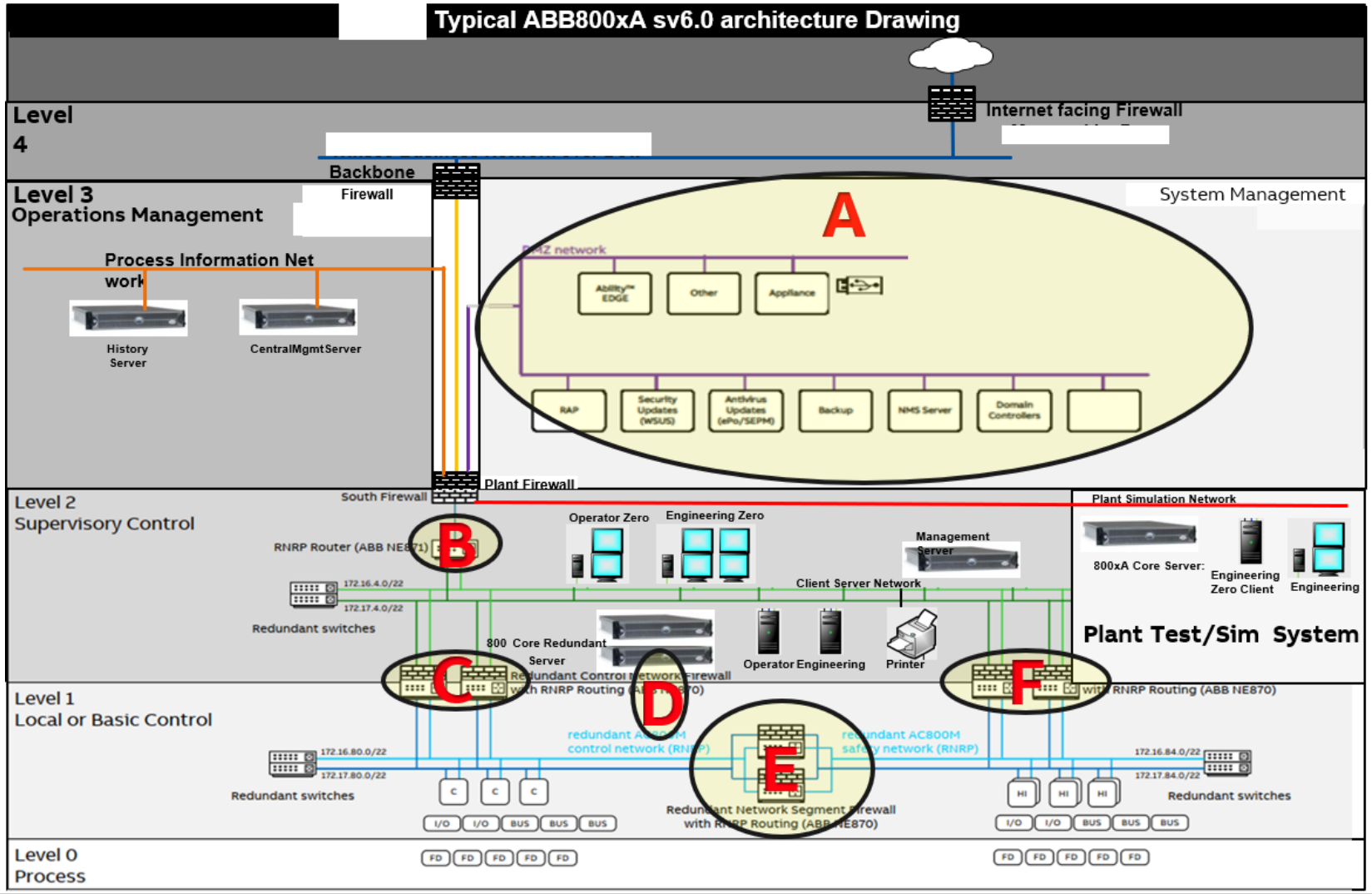
The next slide will show any gaps between the customer's current architecture and ABB's Reference Architecture.



Customer Reference Architecture Gaps

Implementation View

A. No System Management Zone
B. No RNRP routing
C. No controller firewall
D. Dual-Homed server
E. No lateral firewall
F. No safety system firewall protection



Q & A


ABB