PUBLIC

# ABB ICS Cyber Security Reference Architecture

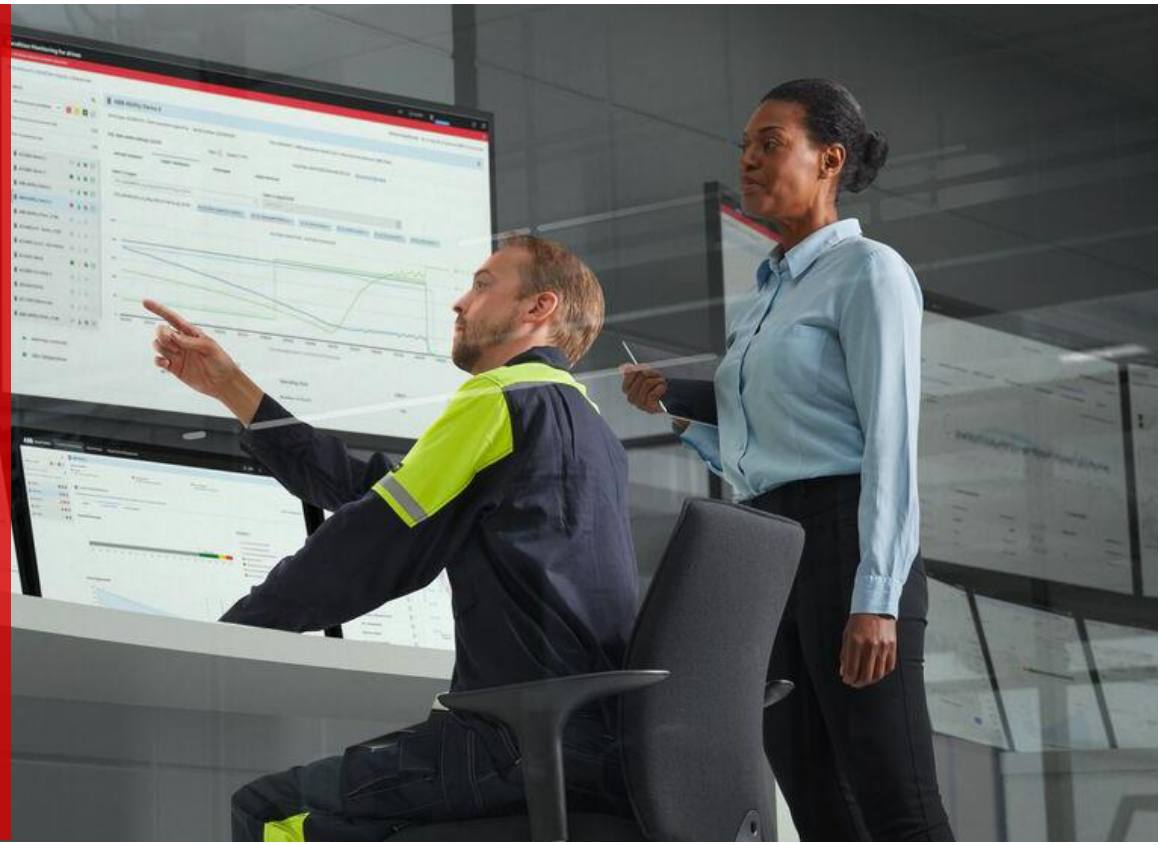
## Introduction

June 2021

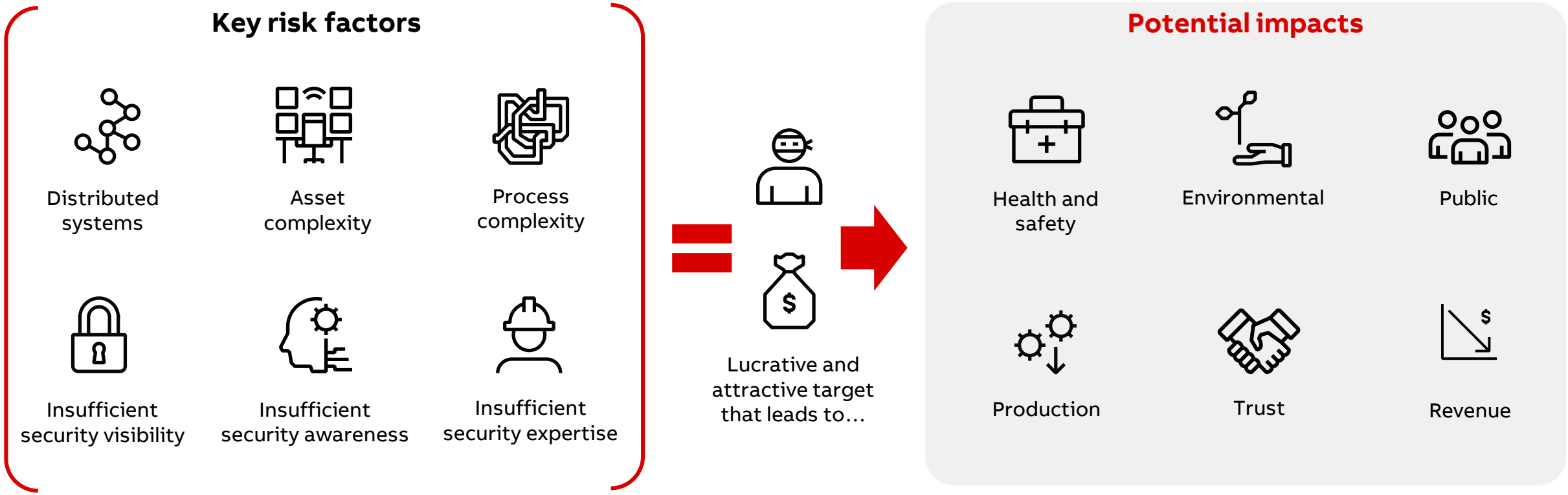
# ABB ICS Cyber Security Reference Architecture

## Agenda

1. Introduction
2. Foundational principles
3. Implementation Examples

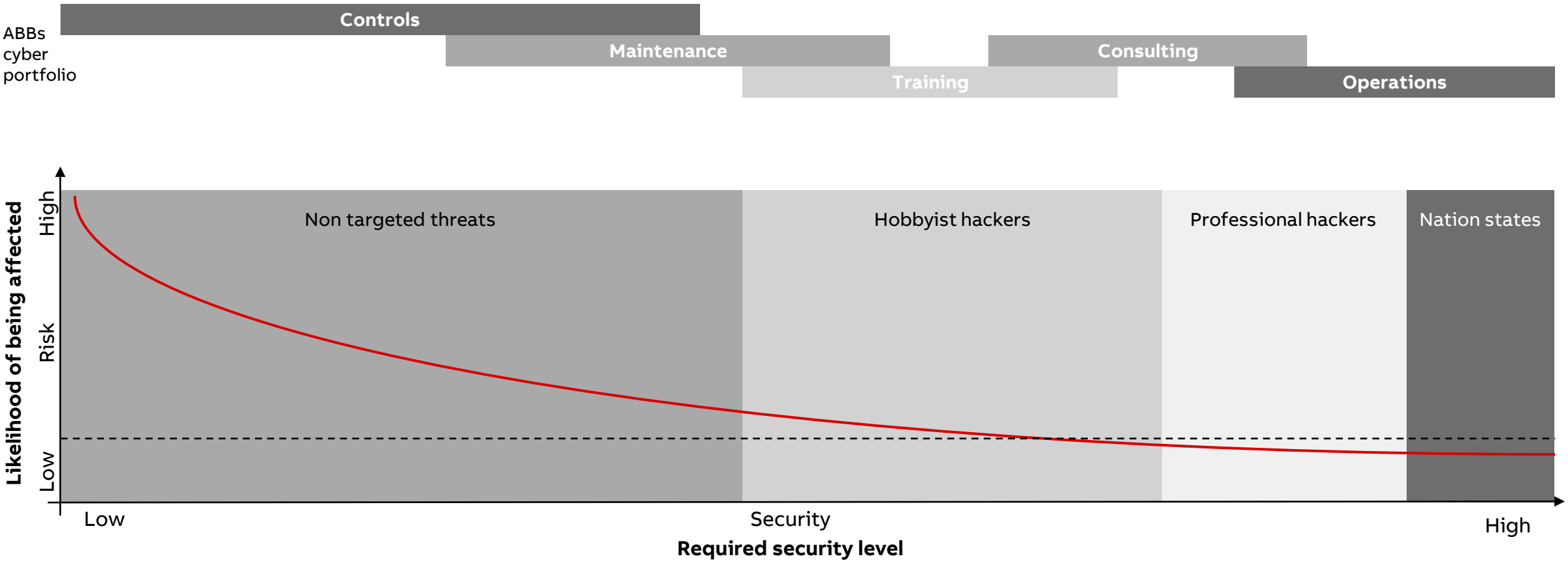


# Industrial companies face elevated cyber security risks



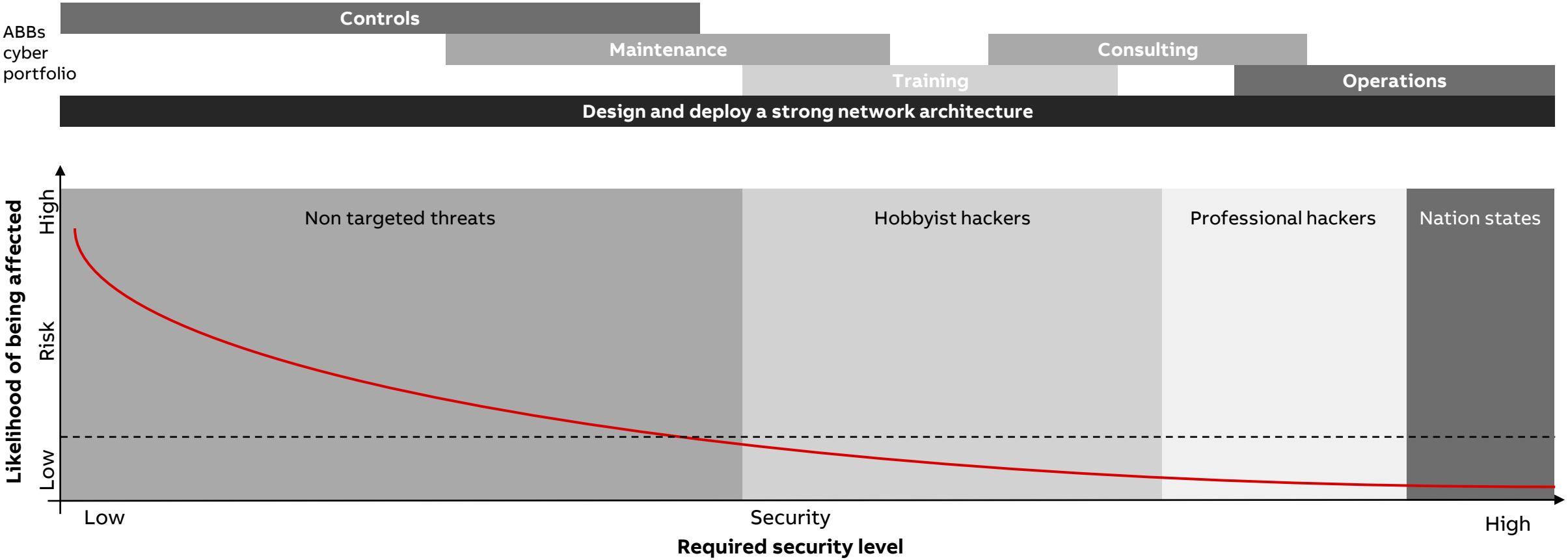
# ABB Ability™ Cyber Security Services

## Reducing risk – ABBs cyber security portfolio helps to reduce the likelihood of cyber incidents



# ABB Ability™ Cyber Security Services

## Reducing risk – A strong network architecture reduces risk



# ABB ICS Cyber Security Reference Architecture

Introduction

## What is it?

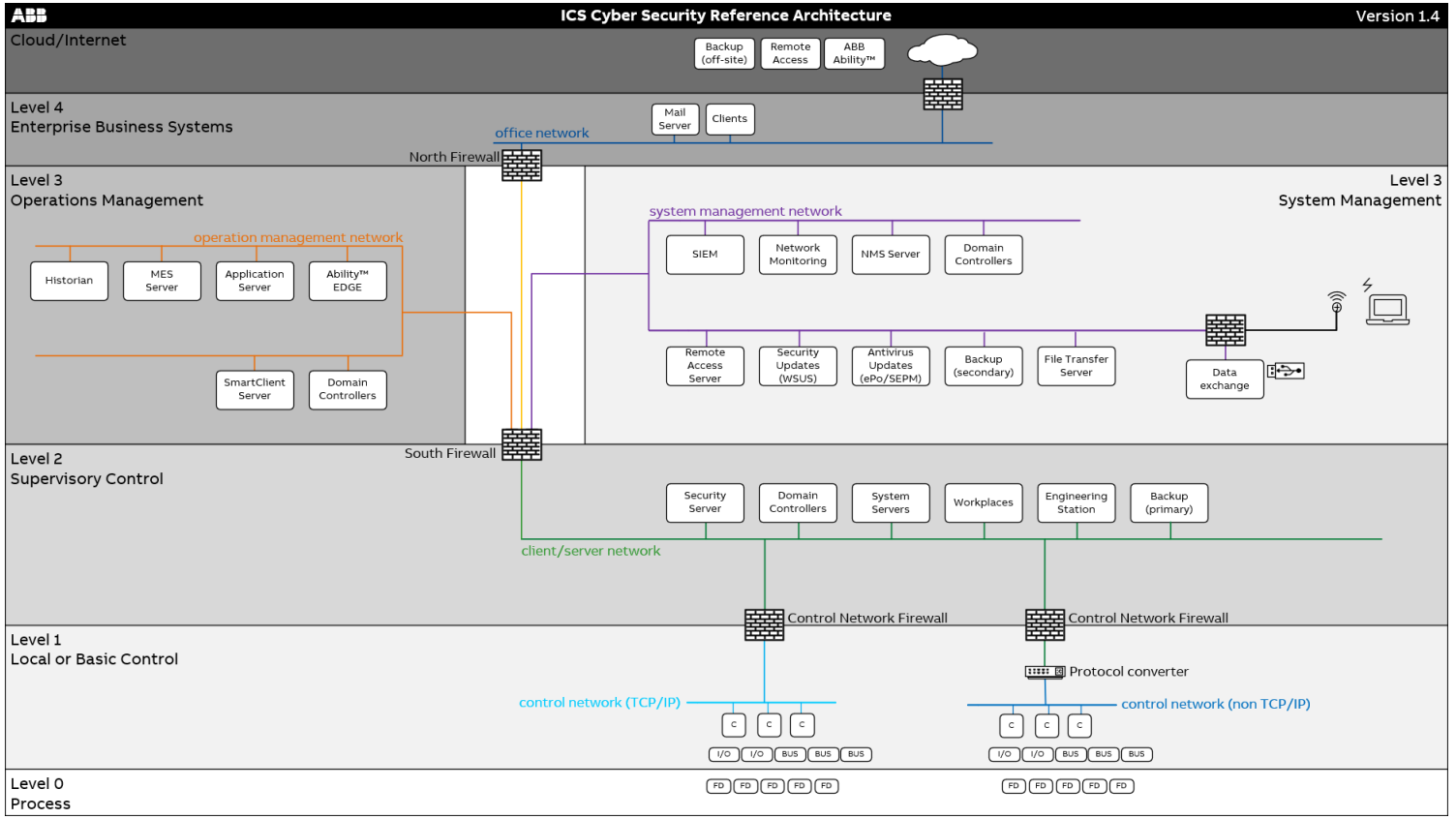
A reference architecture provides a **template solution** for an architecture for a particular domain. It also provides a **common vocabulary** with which to discuss implementations, often with the aim to stress commonality.

**Your guide for a cyber secure architecture.**

## What is it NOT!

- It is not a guarantee that a system is secure or invulnerable from cyber-attacks.
- It does not guarantee to pass external audits.
- The reference architecture is not developed with a specific (DCS) system in mind.

**Always follow product manuals to ensure proper functionality and system availability.**



# ABB ICS Cyber Security Reference Architecture

IEC62443-3-3:2013

## Security levels

| | Description |
|---|---|
| **1** | Prevent the **casual** or **coincidental** circumvention of zone and conduit segmentation. |
| **2** | Prevent the **intended** circumvention of zone and conduit segmentation by entities using simple means with **low resources, generic skills,** and **low motivation**. |
| **3** | Prevent the **intended** circumvention of zone and conduit segmentation by entities using **sophisticated means** with **moderate resources**, **IACS specific skills**, and **moderate motivation**. |
| **4** | Prevent the **intended** circumvention of zone and conduit segmentation by entities using **sophisticated means** with **extended resources**, **IACS specific skills**, and **high motivation**. |

## Functional requirements

| | Sections |
|---|---|
| 1 | Identification and authentication control |
| 2 | Use control |
| 3 | System integrity |
| 4 | Data confidentiality |
| **5** | **Restricted data flow** |
| 6 | Timely response to events |
| 7 | Resource availability |

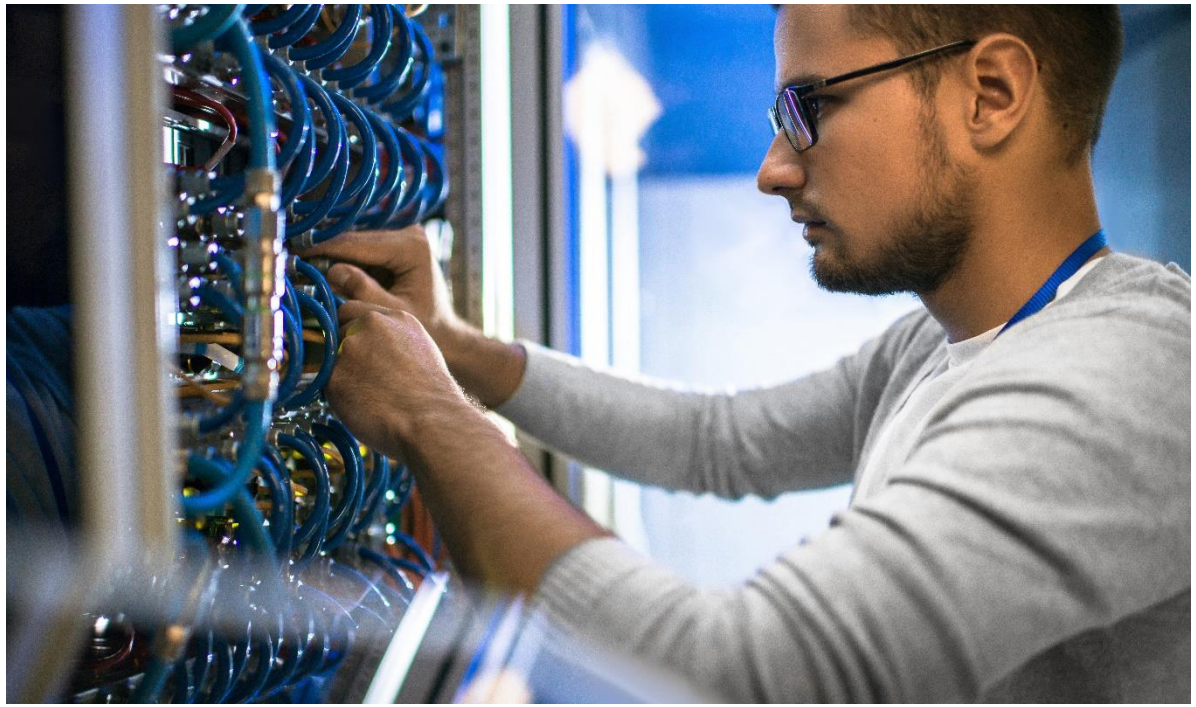
# ABB ICS Cyber Security Reference Architecture

IEC62443-3-3:2013

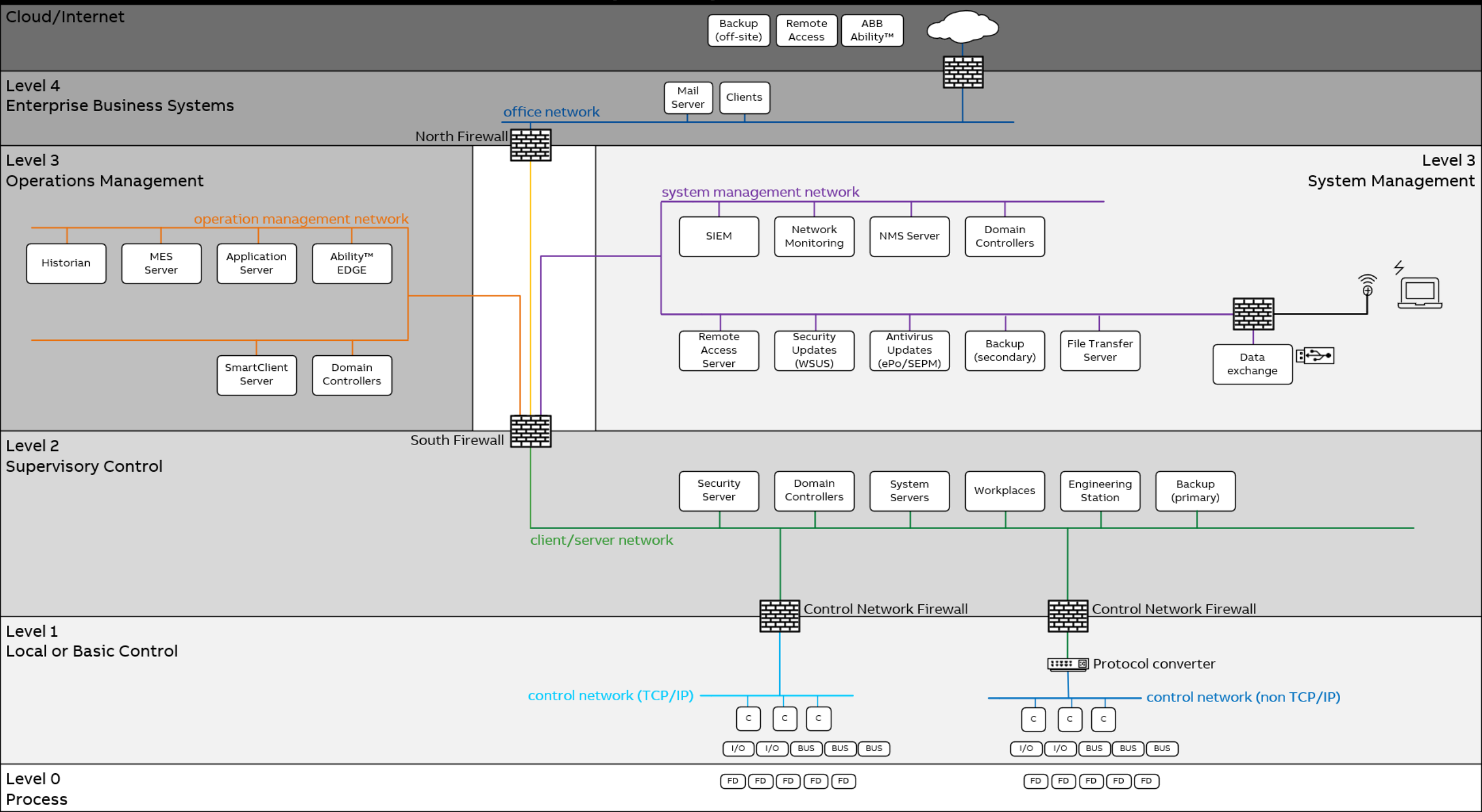
## Our assessment

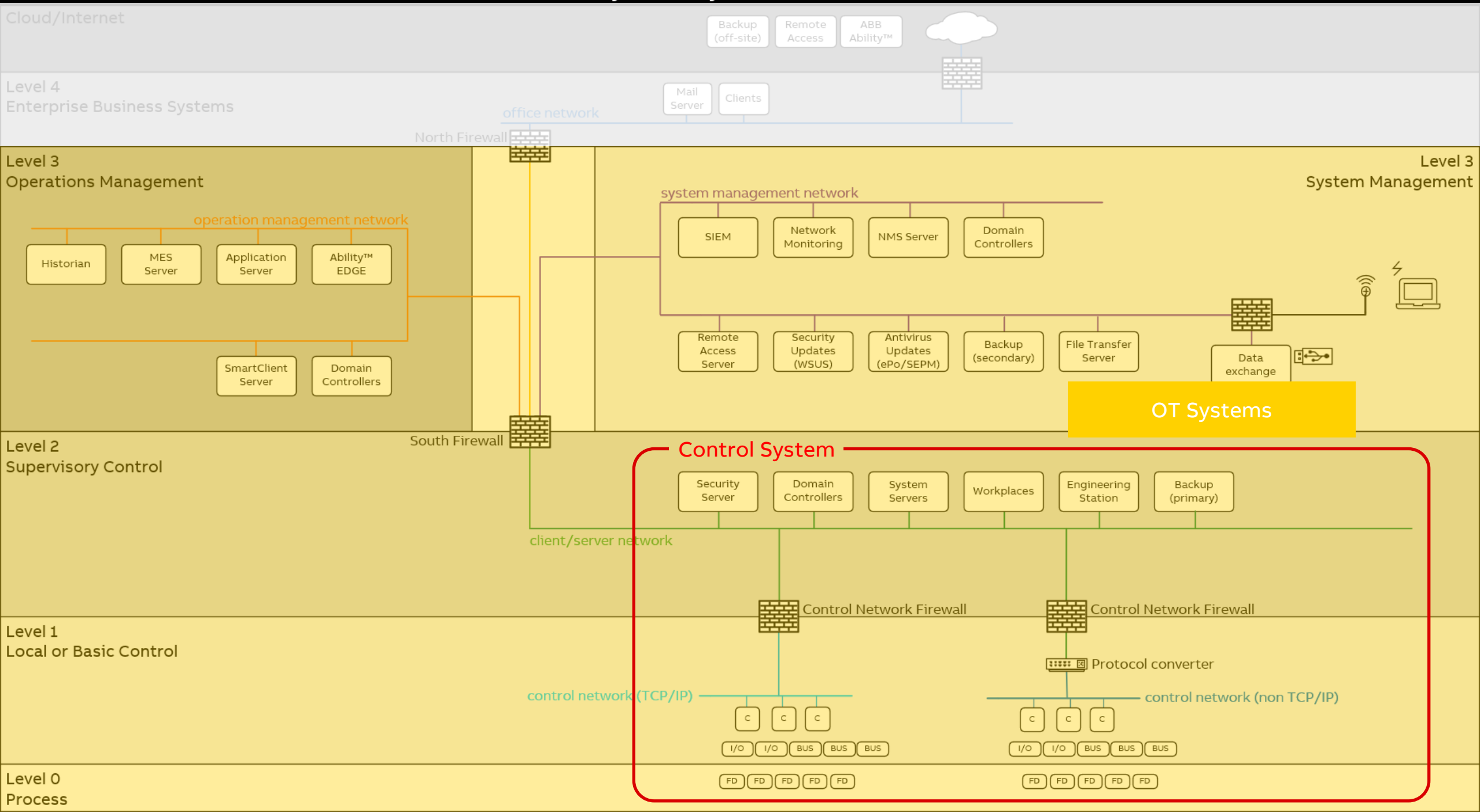
**The reference architecture makes it possible to design a system to achieve SL4.**

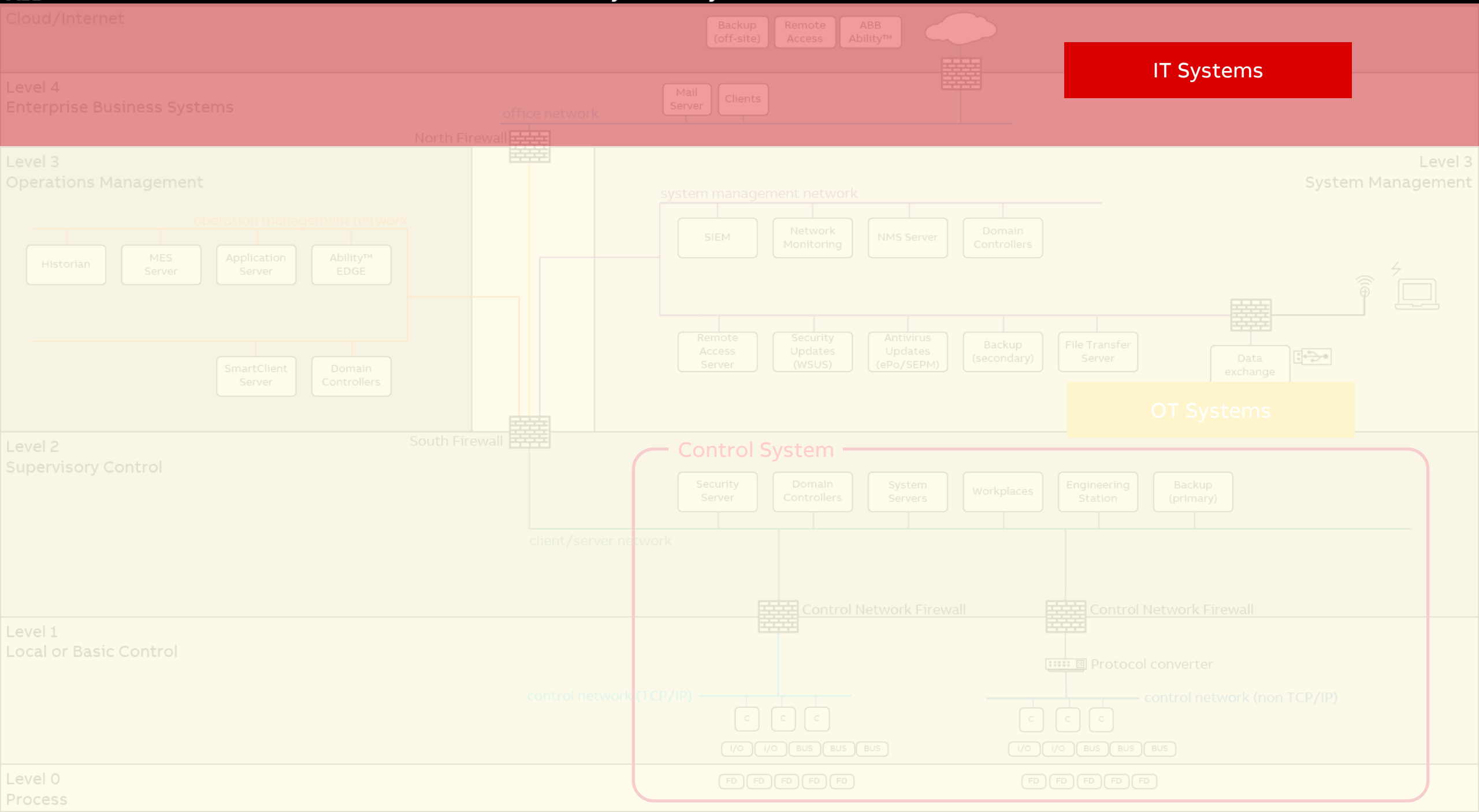
However, the reference architecture doesn't suggest that by simply applying the recommendations will ensure compliance to SL4, nor does it imply that the reference architecture is certified.

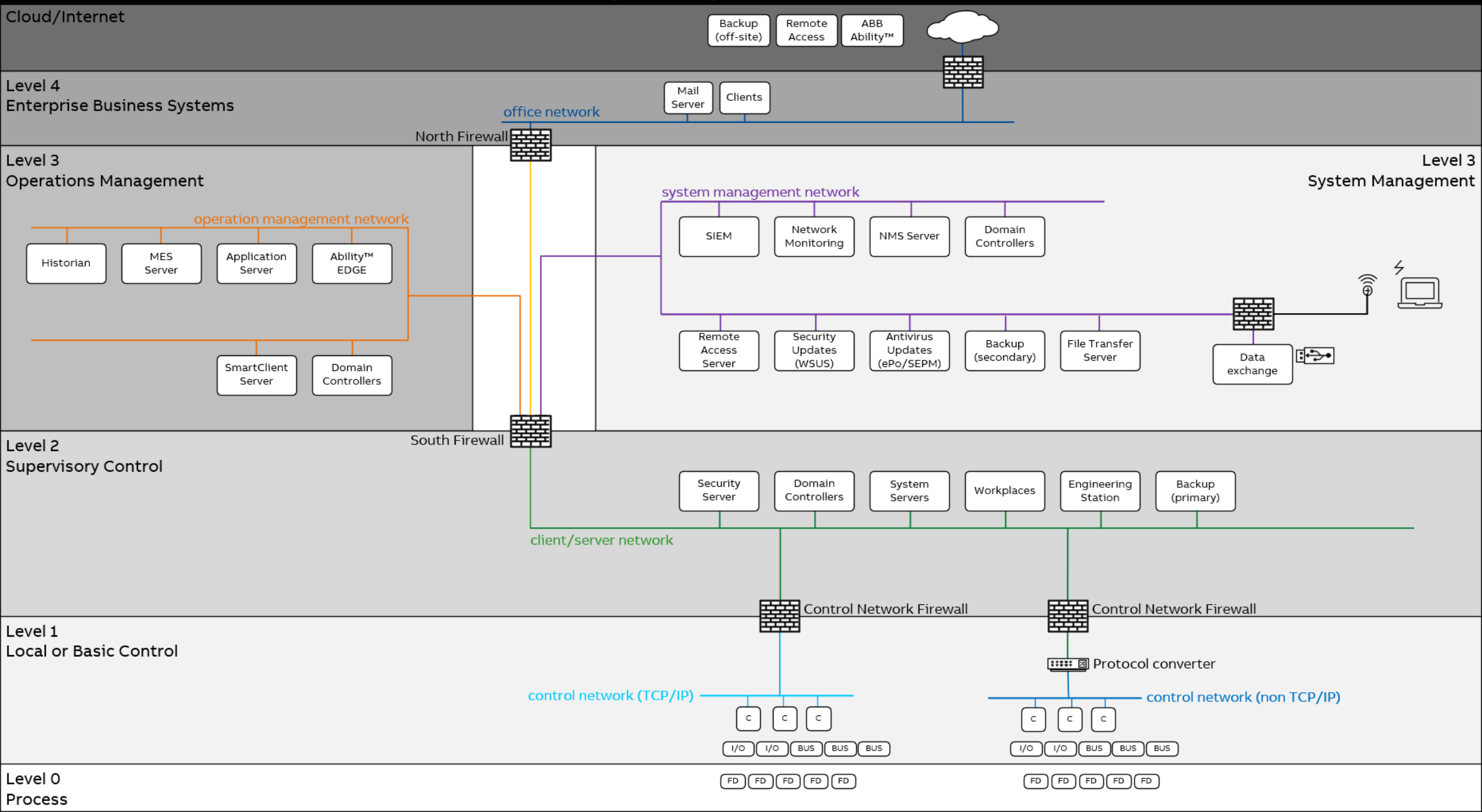


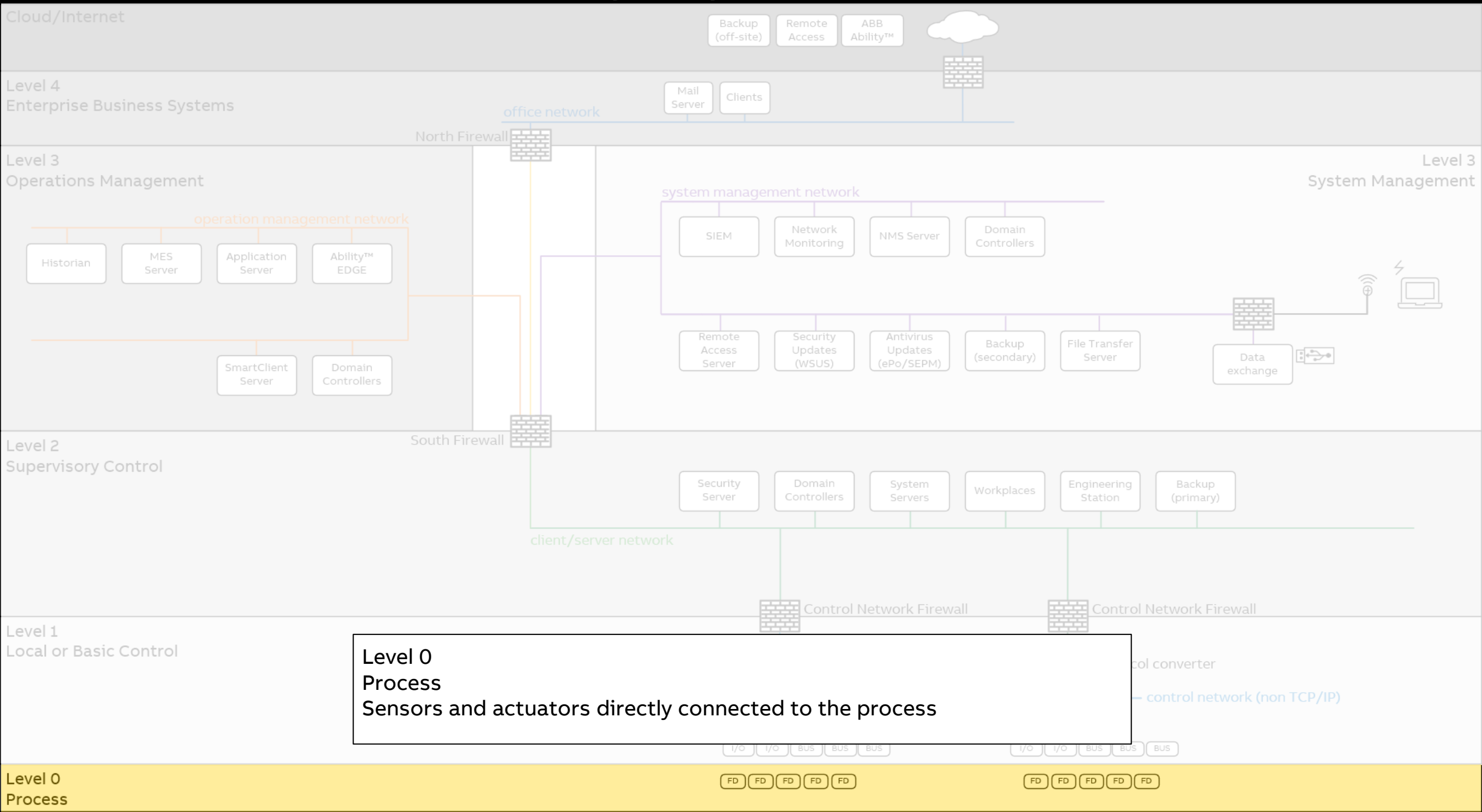
**Compliance requires hard work and can never be bought.**


Cloud/Internet
Backup (off-site)
Remote Access
ABB Ability™
Level 4
Enterprise Business Systems
Mail Server
Clients
office network
North Firewall
Level 3
Operations Management
operation management network
Historian
MES Server
Application Server
Ability™ EDGE
SmartClient Server
Domain Controllers
Level 3
System Management
system management network
SIEM
Network Monitoring
NMS Server
Domain Controllers
Remote Access Server
Security Updates (WSUS)
Antivirus Updates (ePo/SEPM)
Backup (secondary)
File Transfer Server
Data exchange
South Firewall
Level 2
Supervisory Control
Security Server
Domain Controllers
System Servers
Workplaces
Engineering Station
Backup (primary)
client/server network
Control Network Firewall
Control Network Firewall
Level 1
Local or Basic Control
Protocol converter
control network (TCP/IP)
control network (non TCP/IP)
C
I/O
BUS
Level 0
Process
FD

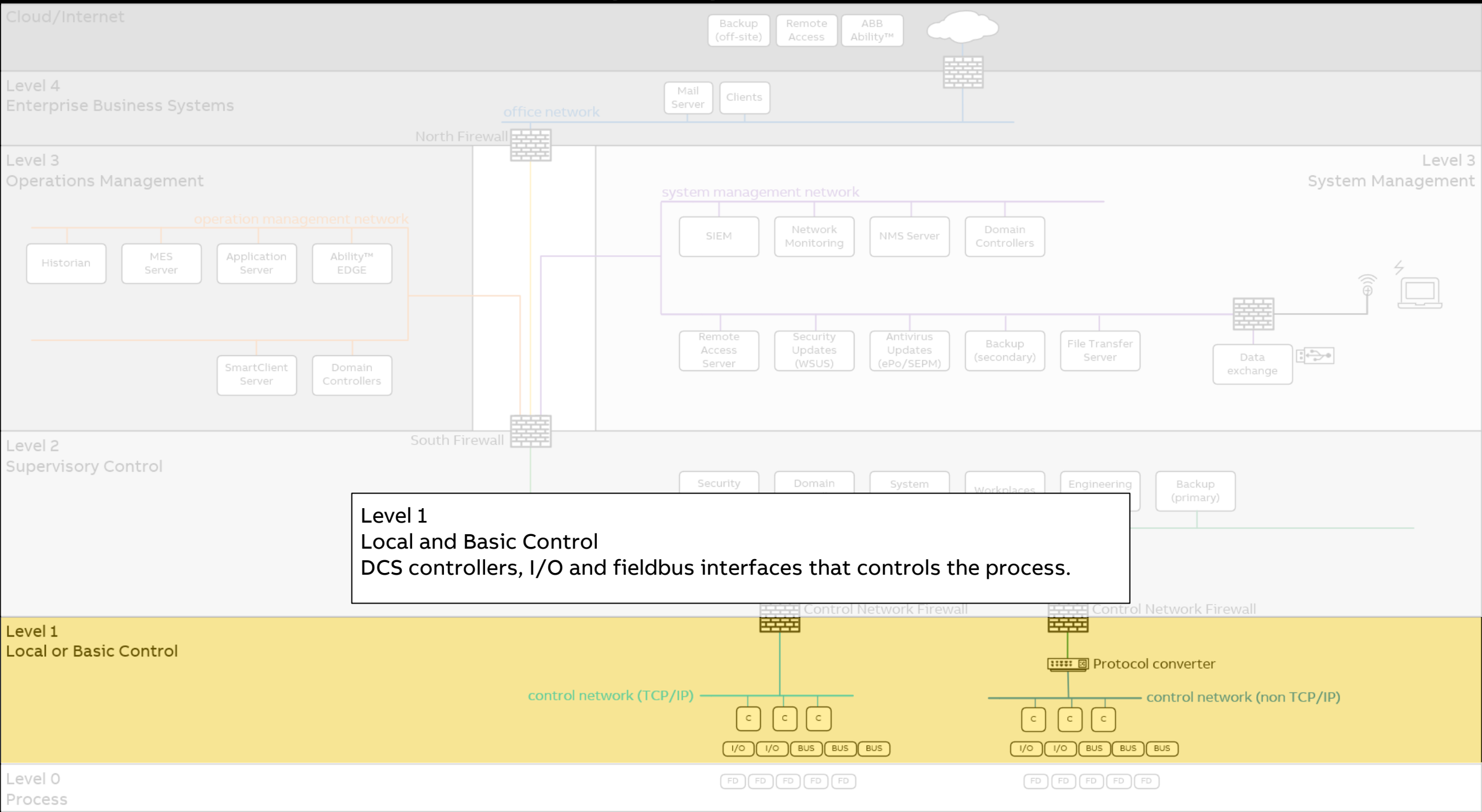

Cloud/Internet
Backup (off-site)
Remote Access
ABB Ability™
Level 4
Enterprise Business Systems
Mail Server
Clients
office network
North Firewall
Level 3
Operations Management
operation management network
Historian
MES Server
Application Server
Ability™ EDGE
SmartClient Server
Domain Controllers
Level 3
System Management
system management network
SIEM
Network Monitoring
NMS Server
Domain Controllers
Remote Access Server
Security Updates (WSUS)
Antivirus Updates (ePo/SEPM)
Backup (secondary)
File Transfer Server
Data exchange
OT Systems
South Firewall
Level 2
Supervisory Control
Control System
Security Server
Domain Controllers
System Servers
Workplaces
Engineering Station
Backup (primary)
client/server network
Control Network Firewall
Control Network Firewall
Level 1
Local or Basic Control
Protocol converter
control network (TCP/IP)
control network (non TCP/IP)
C
I/O
BUS
Level 0
Process
FD

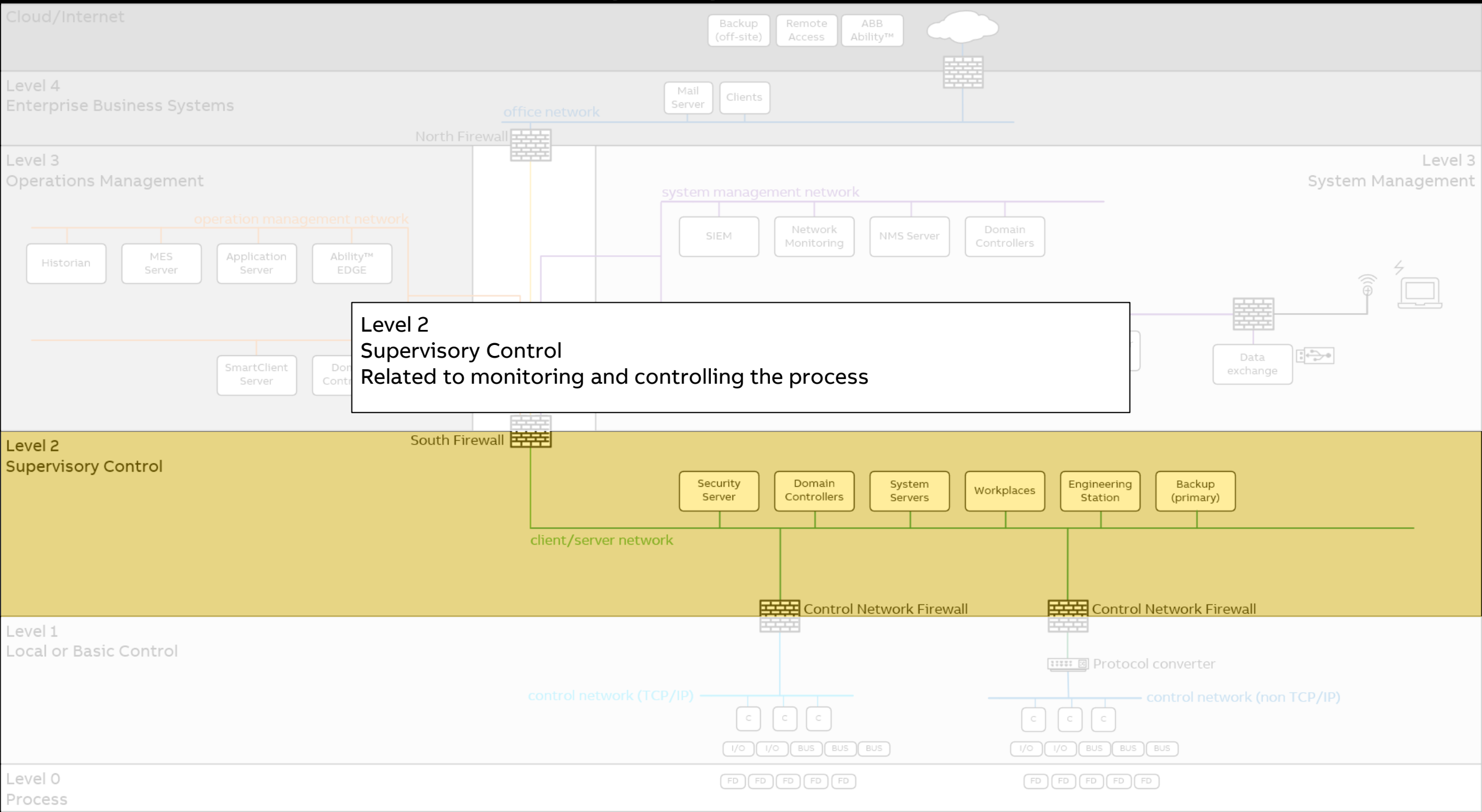

Cloud/Internet
Backup (off-site)
Remote Access
ABB Ability™
IT Systems
Level 4
Enterprise Business Systems
Mail Server
Clients
office network
North Firewall
Level 3
Operations Management
operation management network
Historian
MES Server
Application Server
Ability™ EDGE
SmartClient Server
Domain Controllers
Level 3
System Management
system management network
SIEM
Network Monitoring
NMS Server
Domain Controllers
Remote Access Server
Security Updates (WSUS)
Antivirus Updates (ePo/SEPM)
Backup (secondary)
File Transfer Server
Data exchange
OT Systems
South Firewall
Level 2
Supervisory Control
Control System
Security Server
Domain Controllers
System Servers
Workplaces
Engineering Station
Backup (primary)
client/server network
Control Network Firewall
Control Network Firewall
Level 1
Local or Basic Control
Protocol converter
control network (TCP/IP)
control network (non TCP/IP)
C
I/O
BUS
FD
Level 0
Process

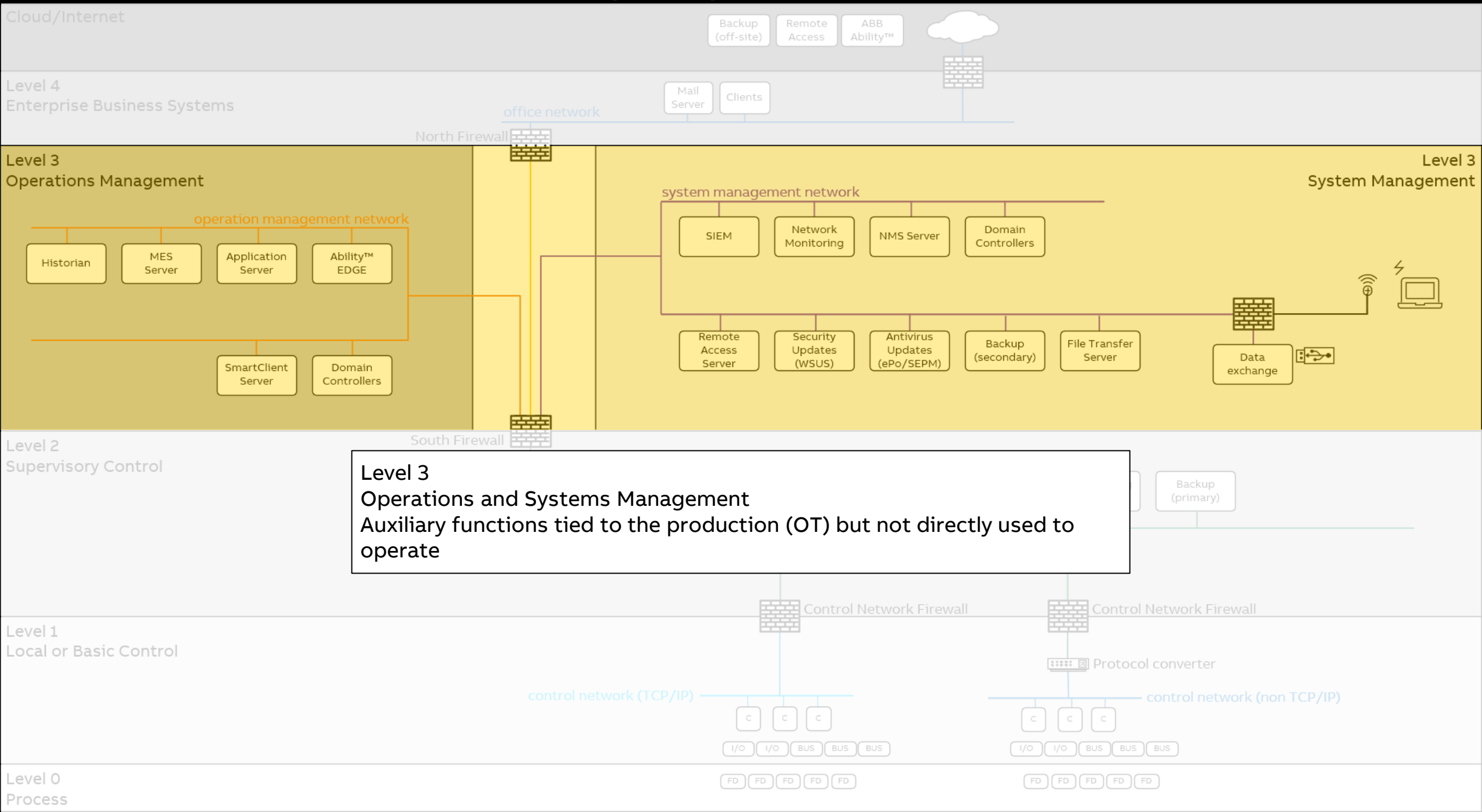

Cloud/Internet
Backup (off-site)
Remote Access
ABB Ability™
Level 4
Enterprise Business Systems
Mail Server
Clients
office network
North Firewall
Level 3
Operations Management
operation management network
Historian
MES Server
Application Server
Ability™ EDGE
SmartClient Server
Domain Controllers
Level 3
System Management
system management network
SIEM
Network Monitoring
NMS Server
Domain Controllers
Remote Access Server
Security Updates (WSUS)
Antivirus Updates (ePo/SEPM)
Backup (secondary)
File Transfer Server
Data exchange
South Firewall
Level 2
Supervisory Control
Security Server
Domain Controllers
System Servers
Workplaces
Engineering Station
Backup (primary)
client/server network
Control Network Firewall
Control Network Firewall
Level 1
Local or Basic Control
Protocol converter
control network (TCP/IP)
control network (non TCP/IP)
C
I/O
BUS
Level 0
Process
FD



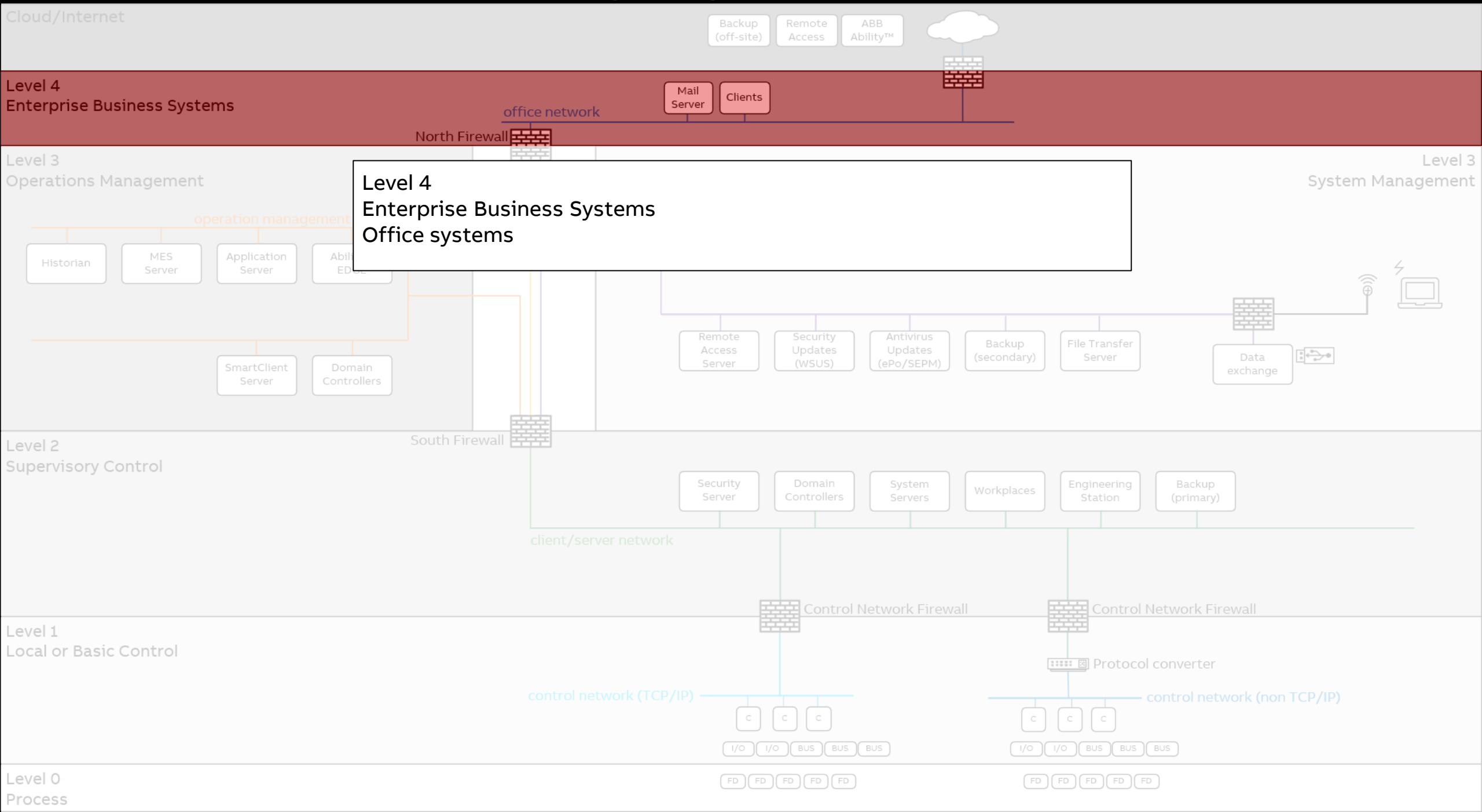

Level 0
Process
Sensors and actuators directly connected to the process


Cloud/Internet
Backup (off-site)
Remote Access
ABB Ability™
Level 4
Enterprise Business Systems
Mail Server
Clients
office network
North Firewall
Level 3
Operations Management
operation management network
Historian
MES Server
Application Server
Ability™ EDGE
SmartClient Server
Domain Controllers
Level 3
System Management
system management network
SIEM
Network Monitoring
NMS Server
Domain Controllers
Remote Access Server
Security Updates (WSUS)
Antivirus Updates (ePo/SEPM)
Backup (secondary)
File Transfer Server
Data exchange
South Firewall
Level 2
Supervisory Control
Security
Domain
System
Workplaces
Engineering
Backup (primary)
Level 1
Local and Basic Control
DCS controllers, I/O and fieldbus interfaces that controls the process.
Level 1
Local or Basic Control
Control Network Firewall
Control Network Firewall
Protocol converter
control network (TCP/IP)
control network (non TCP/IP)
C
I/O
BUS
Level 0
Process
FD

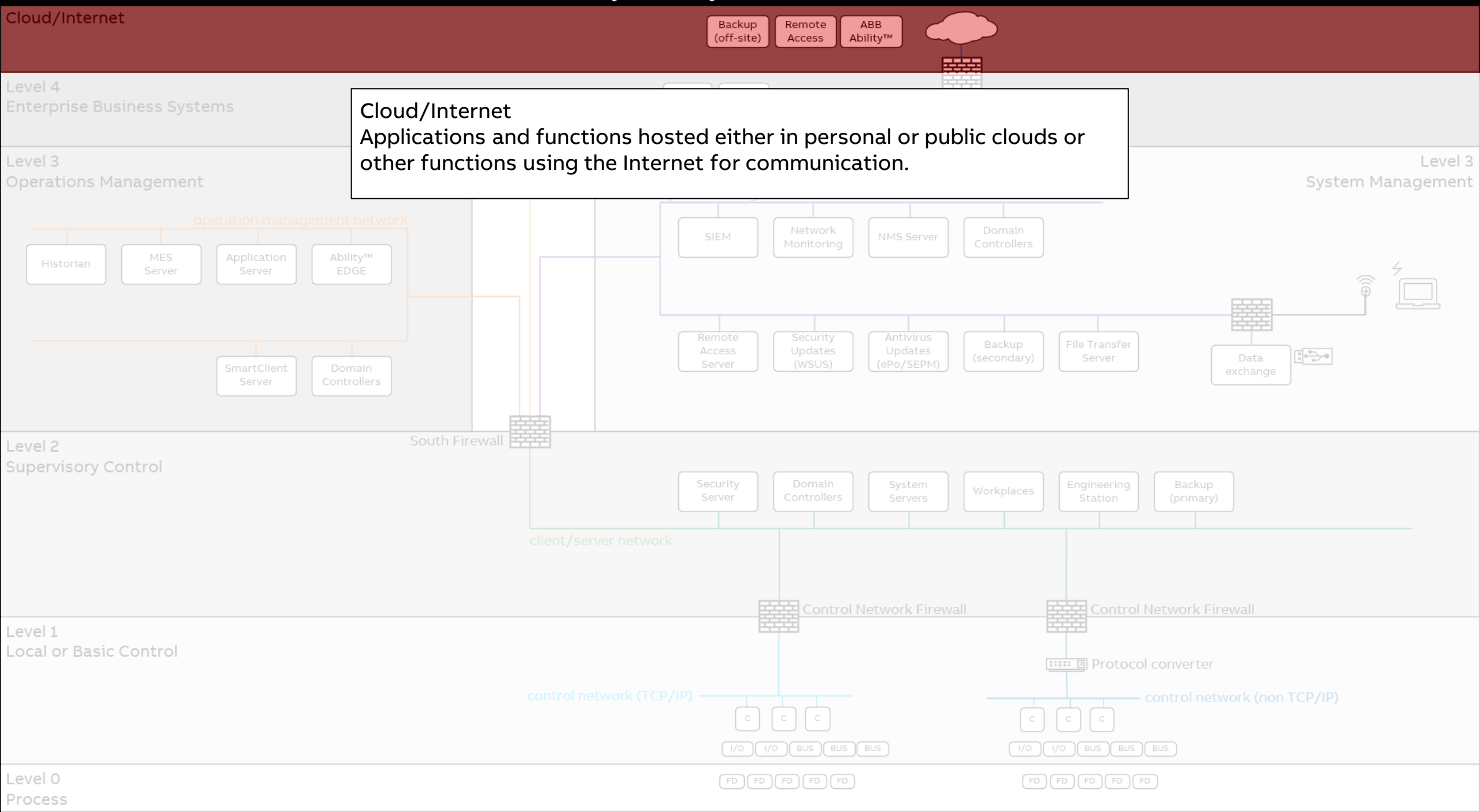

Cloud/Internet
Backup (off-site)
Remote Access
ABB Ability™
Level 4
Enterprise Business Systems
Mail Server
Clients
office network
North Firewall
Level 3
Operations Management
Level 3
System Management
system management network
SIEM
Network Monitoring
NMS Server
Domain Controllers
operation management network
Historian
MES Server
Application Server
Ability™ EDGE
SmartClient Server
Data exchange
Level 2
Supervisory Control
Related to monitoring and controlling the process
South Firewall
Level 2
Supervisory Control
Security Server
Domain Controllers
System Servers
Workplaces
Engineering Station
Backup (primary)
client/server network
Control Network Firewall
Control Network Firewall
Level 1
Local or Basic Control
Protocol converter
control network (TCP/IP)
control network (non TCP/IP)
C
I/O
BUS
Level 0
Process
FD



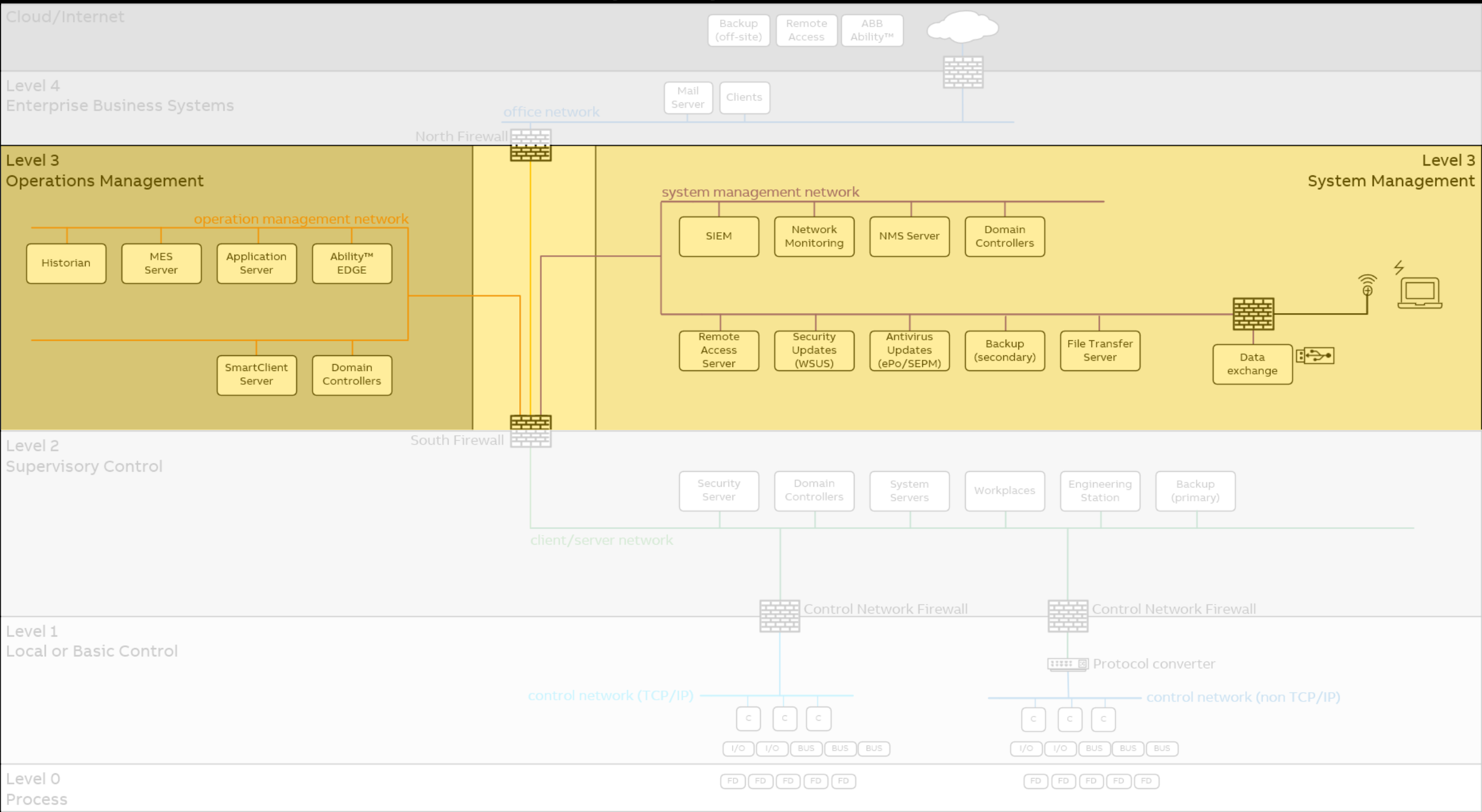

Level 3
Operations and Systems Management
Auxiliary functions tied to the production (OT) but not directly used to operate

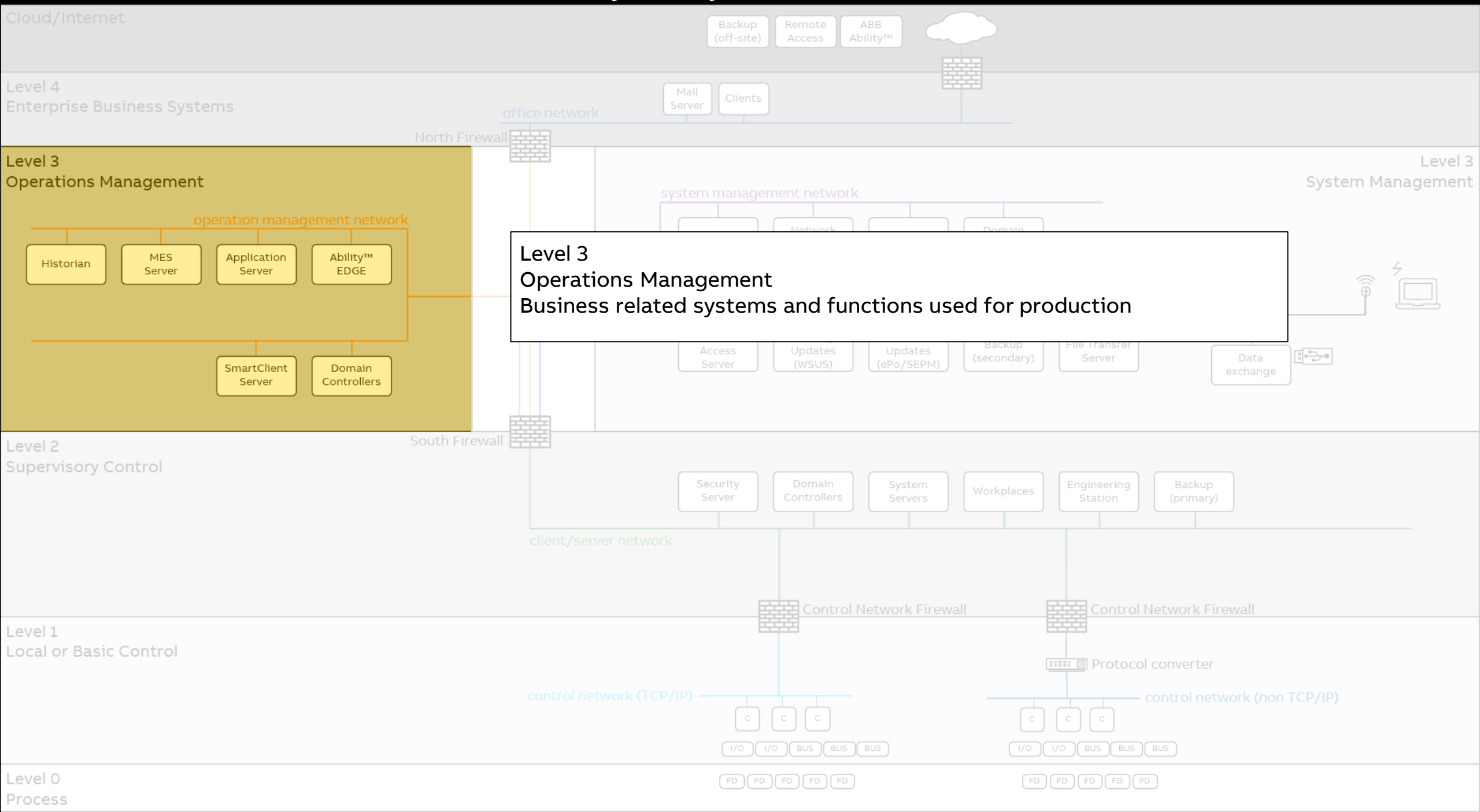


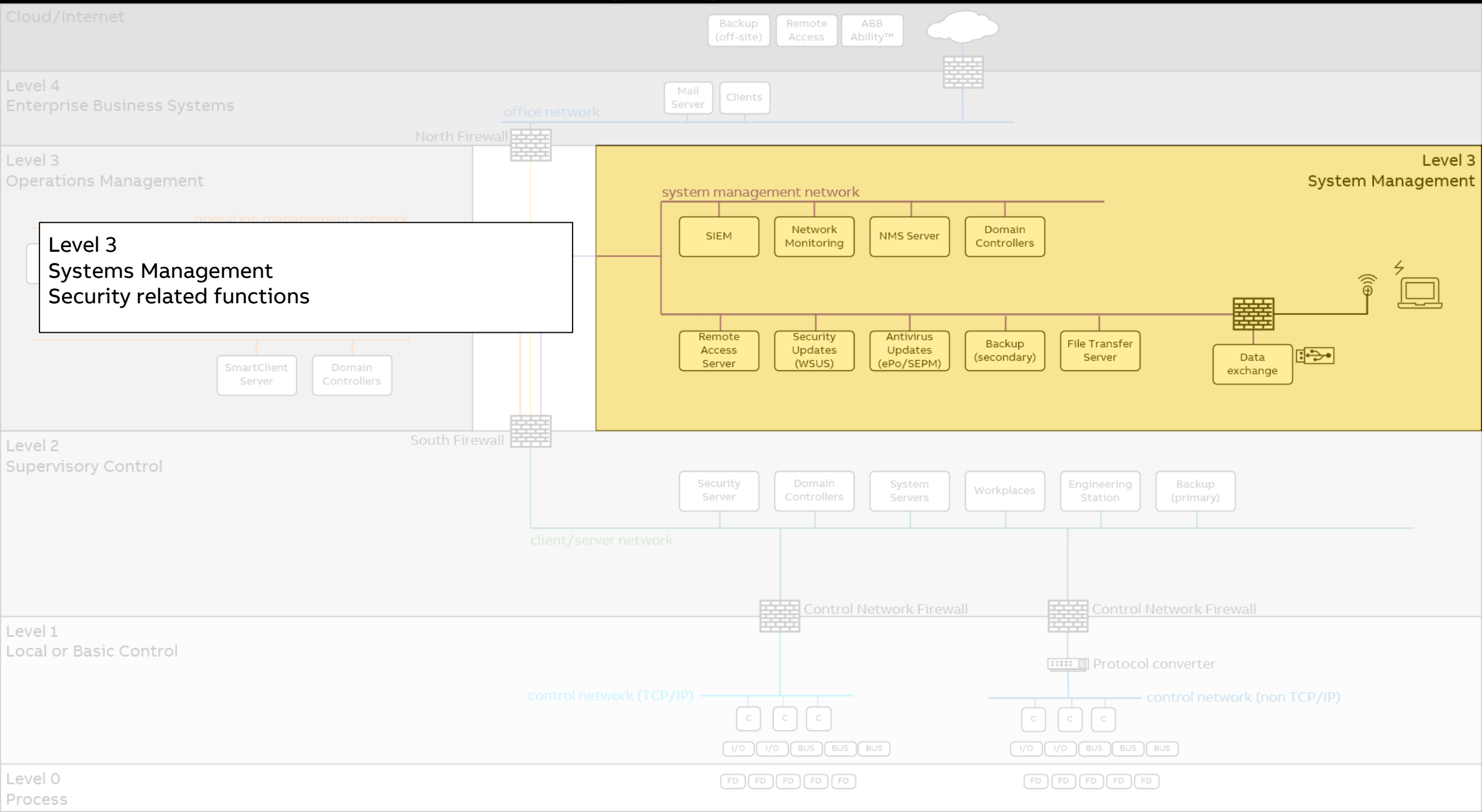

Level 4
Enterprise Business Systems
Office systems




Cloud/Internet
Applications and functions hosted either in personal or public clouds or other functions using the Internet for communication.


Cloud/Internet
Backup (off-site)
Remote Access
ABB Ability™
Level 4
Enterprise Business Systems
Mail Server
Clients
office network
North Firewall
Level 3
Operations Management
operation management network
Historian
MES Server
Application Server
Ability™ EDGE
SmartClient Server
Domain Controllers
Level 3
System Management
system management network
SIEM
Network Monitoring
NMS Server
Domain Controllers
Remote Access Server
Security Updates (WSUS)
Antivirus Updates (ePo/SEPM)
Backup (secondary)
File Transfer Server
Data exchange
South Firewall
Level 2
Supervisory Control
Security Server
Domain Controllers
System Servers
Workplaces
Engineering Station
Backup (primary)
client/server network
Control Network Firewall
Control Network Firewall
Level 1
Local or Basic Control
Protocol converter
control network (TCP/IP)
control network (non TCP/IP)
C
I/O
BUS
Level 0
Process
FD


Cloud/Internet
Backup (off-site)
Remote Access
ABB Ability™
Level 4
Enterprise Business Systems
Mail Server
Clients
office network
North Firewall
Level 3
Operations Management
operation management network
Historian
MES Server
Application Server
Ability™ EDGE
SmartClient Server
Domain Controllers
Level 3
System Management
system management network
Access Server
Updates (WSUS)
Updates (ePo/SEPM)
Backup (secondary)
File Transfer Server
Data exchange
Level 3
Operations Management
Business related systems and functions used for production
South Firewall
Level 2
Supervisory Control
Security Server
Domain Controllers
System Servers
Workplaces
Engineering Station
Backup (primary)
client/server network
Control Network Firewall
Control Network Firewall
Level 1
Local or Basic Control
Protocol converter
control network (TCP/IP)
control network (non TCP/IP)
C
I/O
BUS
Level 0
Process
FD




Level 3
Systems Management
Security related functions

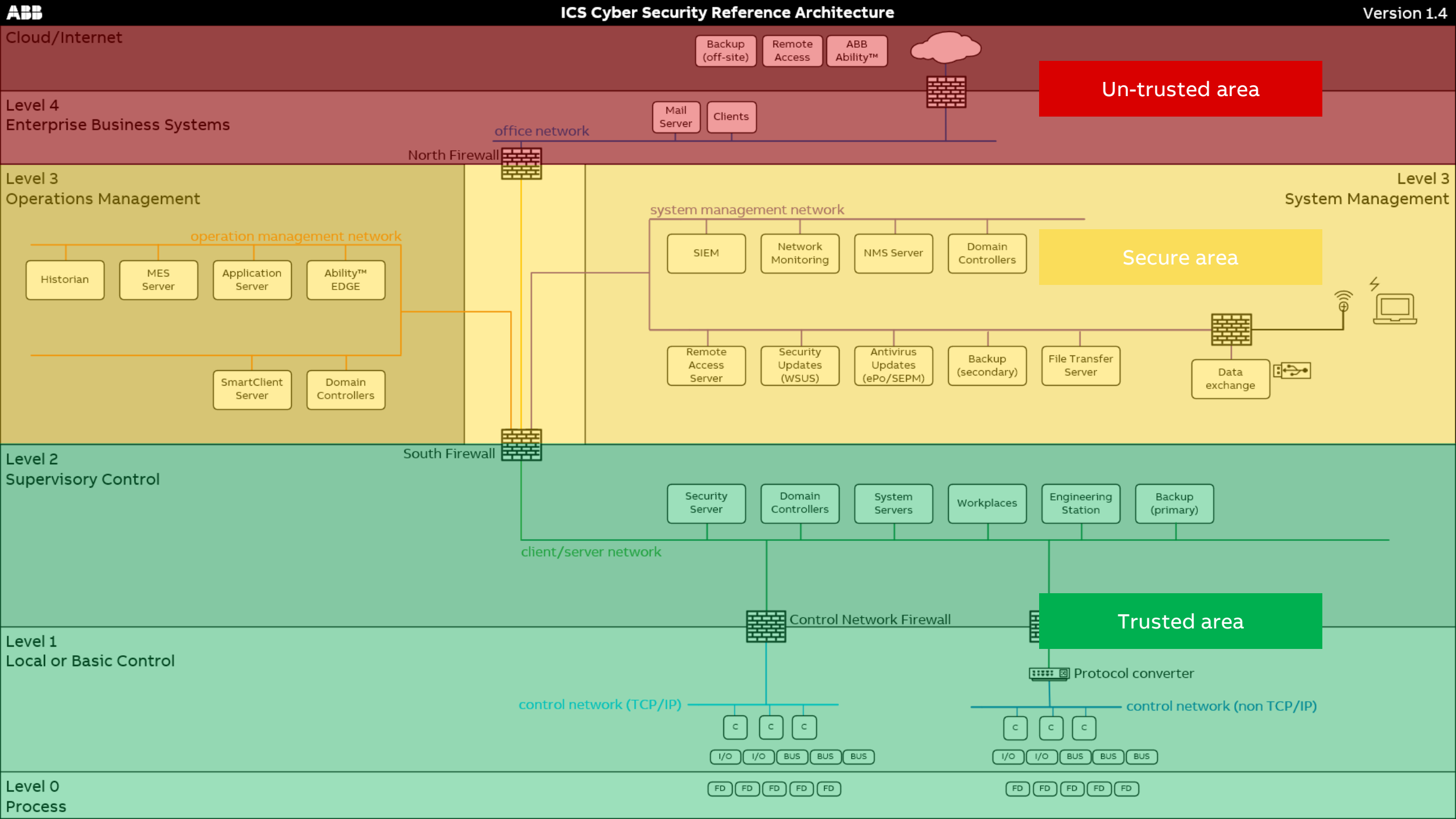


ABB
ICS Cyber Security Reference Architecture
Version 1.4
Cloud/Internet
Backup (off-site)
Remote Access
ABB Ability™
Un-trusted area
Level 4
Enterprise Business Systems
Mail Server
Clients
office network
North Firewall
Level 3
Operations Management
operation management network
Historian
MES Server
Application Server
Ability™ EDGE
SmartClient Server
Domain Controllers
Level 3
System Management
system management network
SIEM
Network Monitoring
NMS Server
Domain Controllers
Secure area
Remote Access Server
Security Updates (WSUS)
Antivirus Updates (ePo/SEPM)
Backup (secondary)
File Transfer Server
Data exchange
South Firewall
Level 2
Supervisory Control
Security Server
Domain Controllers
System Servers
Workplaces
Engineering Station
Backup (primary)
client/server network
Control Network Firewall
Trusted area
Level 1
Local or Basic Control
Protocol converter
control network (TCP/IP)
control network (non TCP/IP)
C
I/O
BUS
Level 0
Process
FD

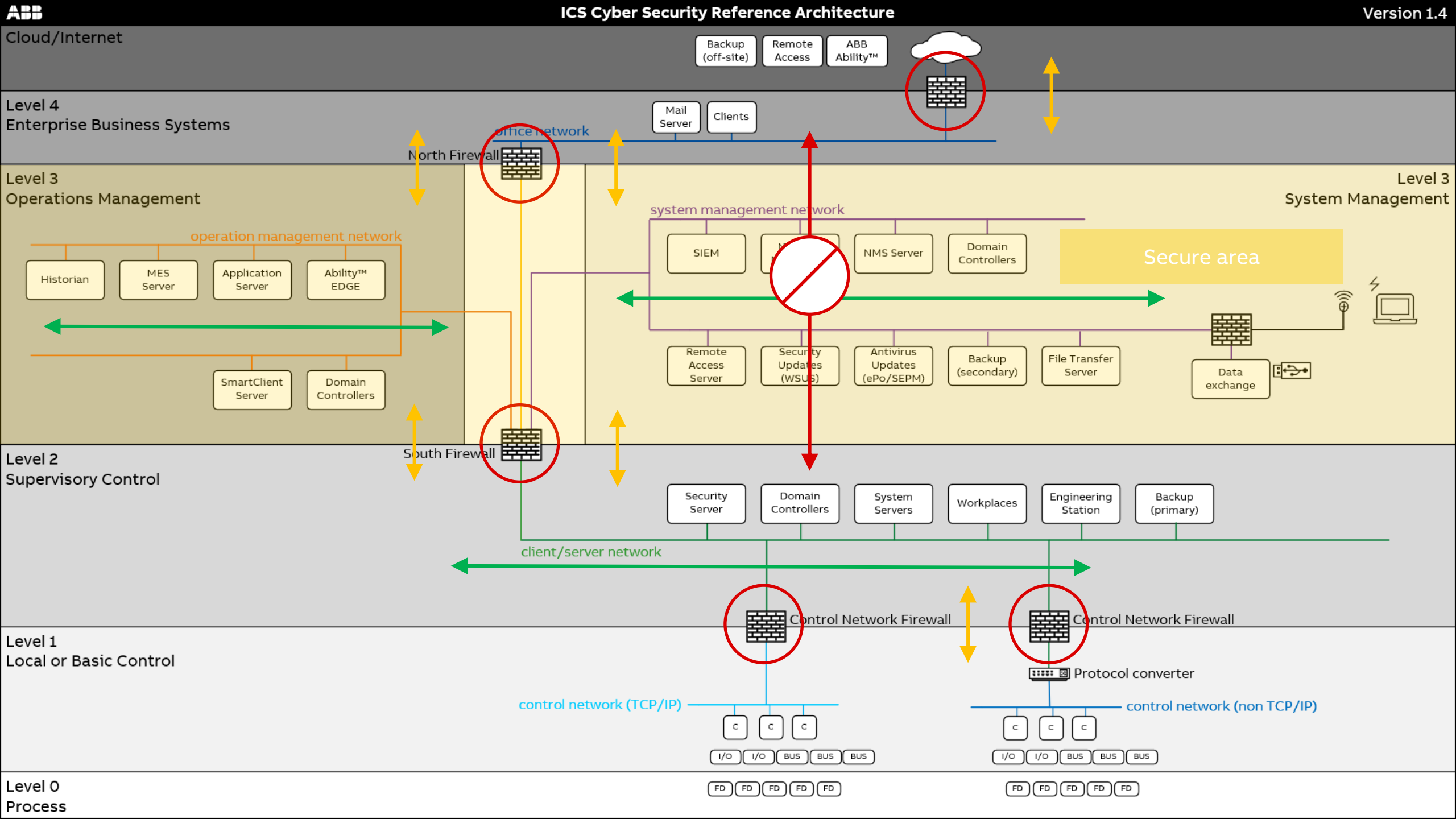


ABB
ICS Cyber Security Reference Architecture
Version 1.4
Cloud/Internet
Backup (off-site)
Remote Access
ABB Ability™
Level 4
Enterprise Business Systems
Mail Server
Clients
office network
North Firewall
Level 3
Operations Management
operation management network
Historian
MES Server
Application Server
Ability™ EDGE
SmartClient Server
Domain Controllers
Level 3
System Management
system management network
SIEM
NMS Server
Domain Controllers
Secure area
Remote Access Server
Security Updates (WSUS)
Antivirus Updates (ePo/SEPM)
Backup (secondary)
File Transfer Server
Data exchange
South Firewall
Level 2
Supervisory Control
Security Server
Domain Controllers
System Servers
Workplaces
Engineering Station
Backup (primary)
client/server network
Control Network Firewall
Control Network Firewall
Level 1
Local or Basic Control
Protocol converter
control network (TCP/IP)
control network (non TCP/IP)
C
I/O
BUS
Level 0
Process
FD

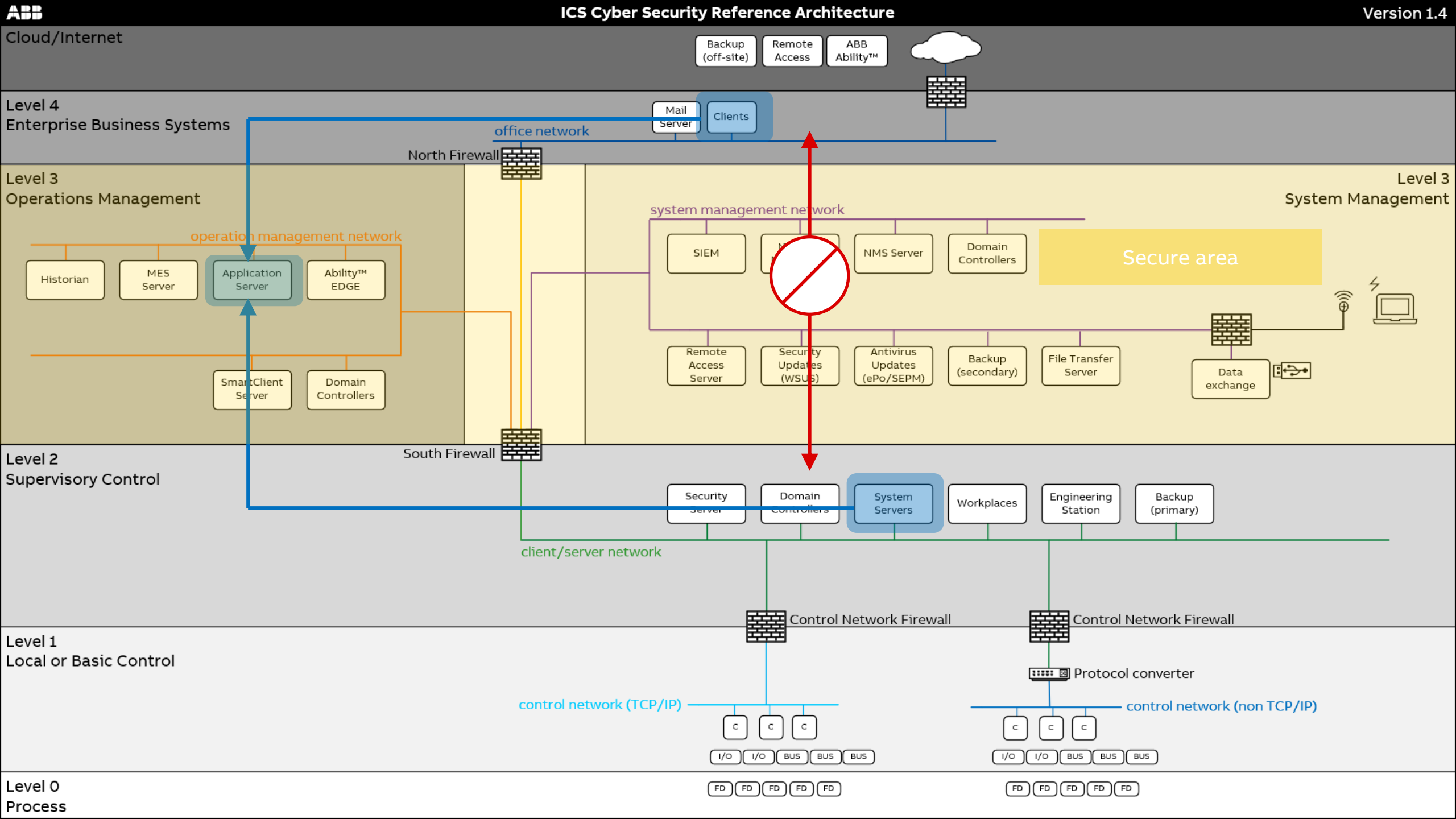
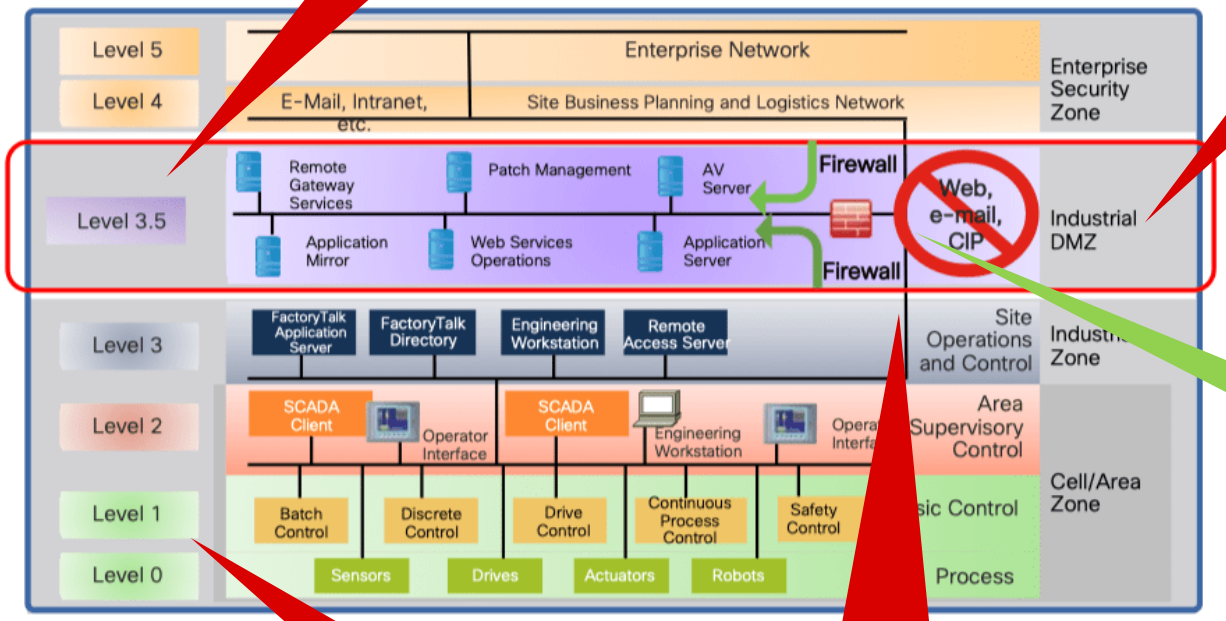
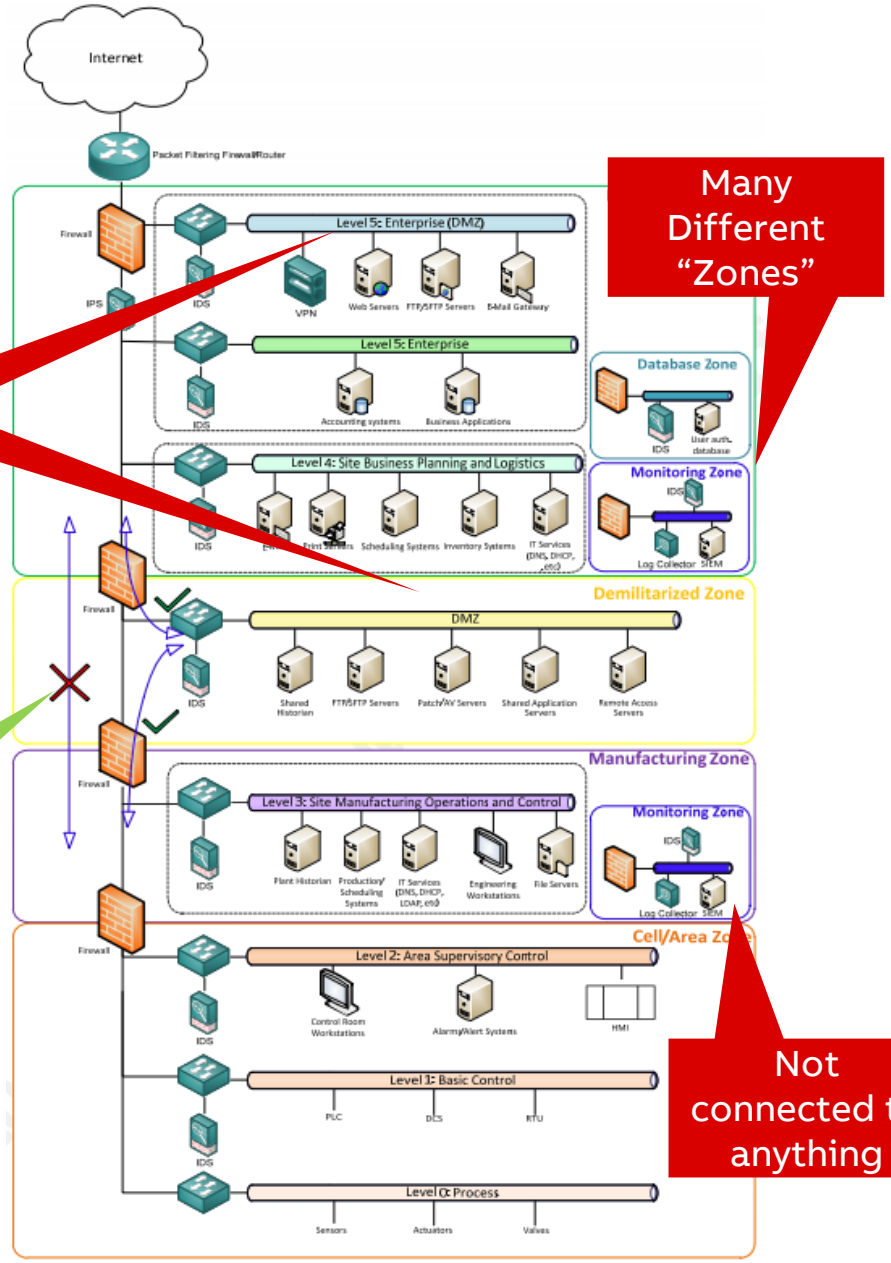


ABB
ICS Cyber Security Reference Architecture
Version 1.4
Cloud/Internet
Backup (off-site)
Remote Access
ABB Ability™
Level 4
Enterprise Business Systems
Mail Server
Clients
office network
North Firewall
Level 3
Operations Management
operation management network
Historian
MES Server
Application Server
Ability™ EDGE
SmartClient Server
Domain Controllers
Level 3
System Management
system management network
SIEM
NMS Server
Domain Controllers
Secure area
Remote Access Server
Security Updates (WSUS)
Antivirus Updates (ePo/SEPM)
Backup (secondary)
File Transfer Server
Data exchange
South Firewall
Level 2
Supervisory Control
Security Server
Domain Controllers
System Servers
Workplaces
Engineering Station
Backup (primary)
client/server network
Control Network Firewall
Control Network Firewall
Level 1
Local or Basic Control
Protocol converter
control network (TCP/IP)
control network (non TCP/IP)
C
I/O
BUS
Level 0
Process
FD

# ABB ICS Cyber Security Reference Architecture

## Commonly used drawings




Half (.5) Levels

Demilitarized Zone (DMZ)

Many Different "Zones"

Same Basic Principles

Combined Level 1 and 0

No firewalls shown between Levels

Not connected to anything

# ABB ICS Cyber Security Reference Architecture

Use-case 1

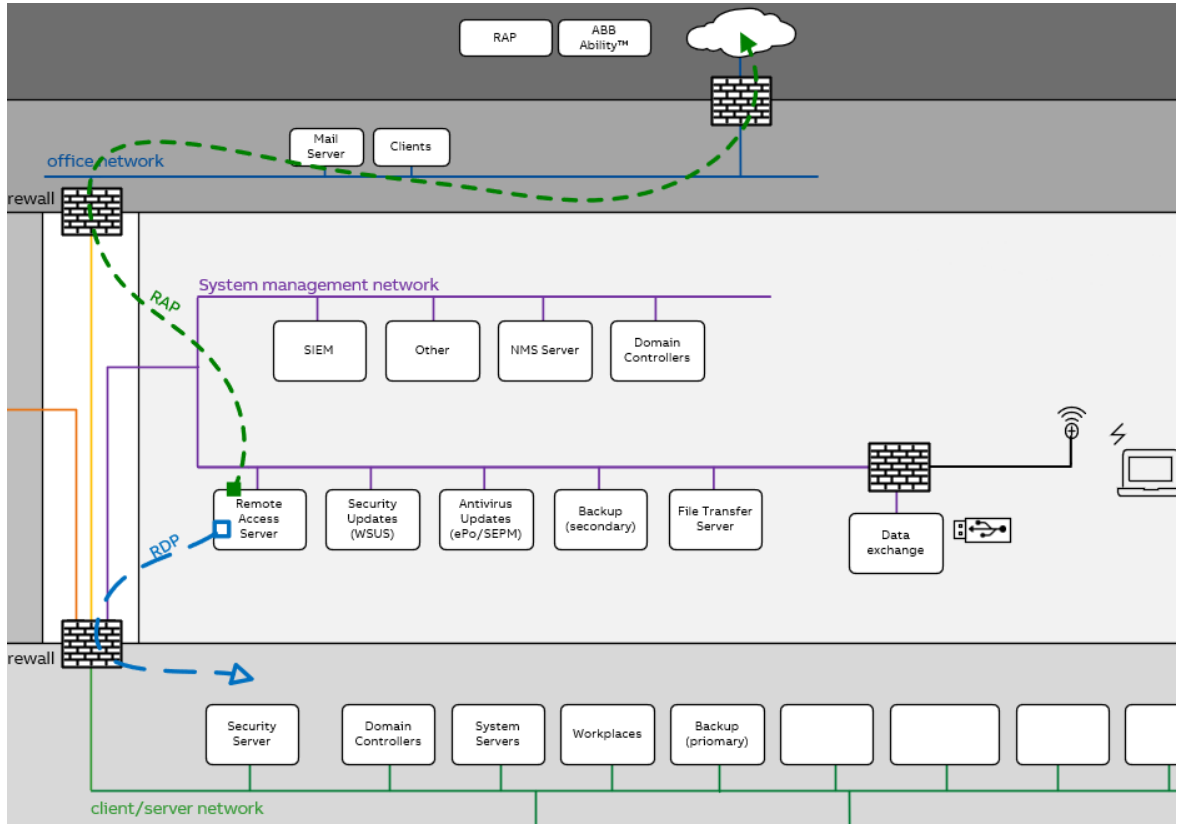
## Remote access

### Customer

*“We realize that remote access is valuable, but we are concerned that it isn't secure or will break our compliance.”*

### ABB

Remote access is an integral part of many of our services and with the recommendations in the architecture it can de implemented without increasing the risk or break compliance.



# ABB ICS Cyber Security Reference Architecture

Use-case 2

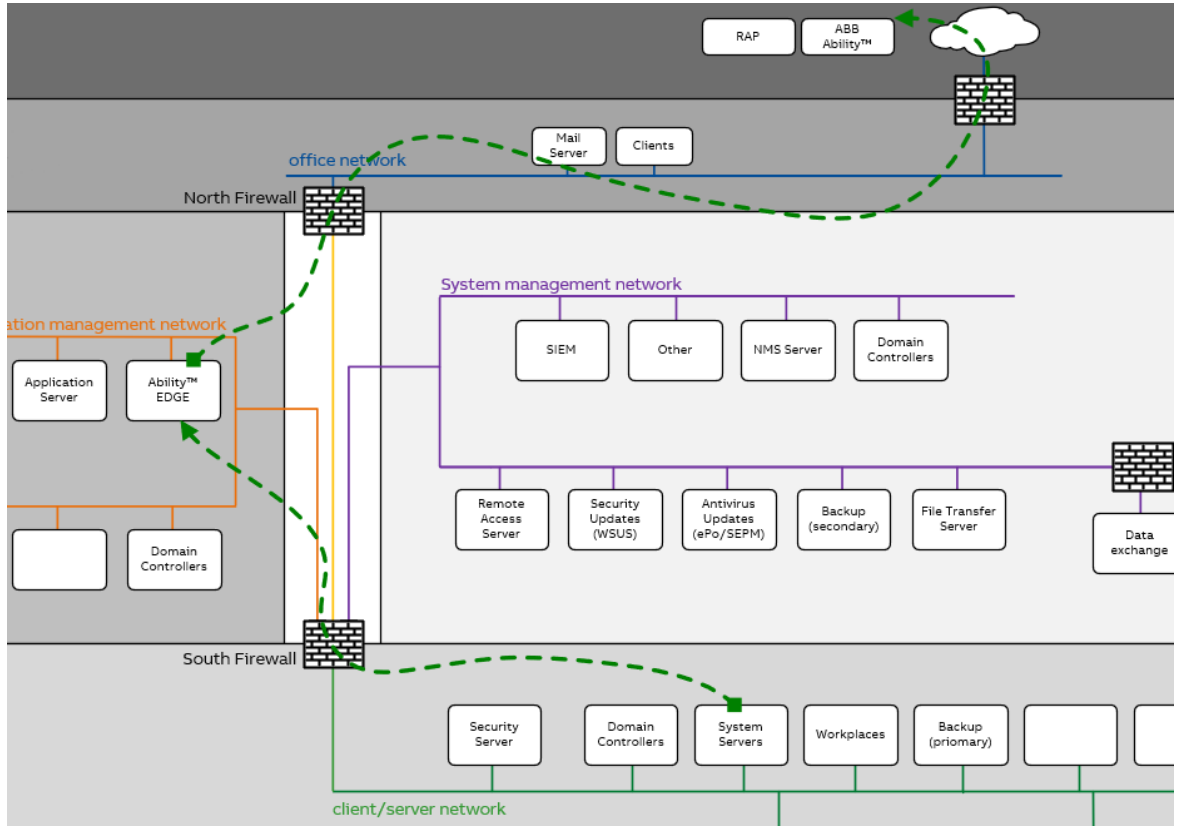
## IoT Gateways (or any buzzword)

### Customer

*“We see the value in [insert buzzword here] but don't think it can be done securely.”*

### ABB

We created the architecture with this in mind. Correctly implemented, you can reap the benefits of these new technologies with only negligible increased cyber risk.



# ABB ICS Cyber Security Reference Architecture

Use-case 3

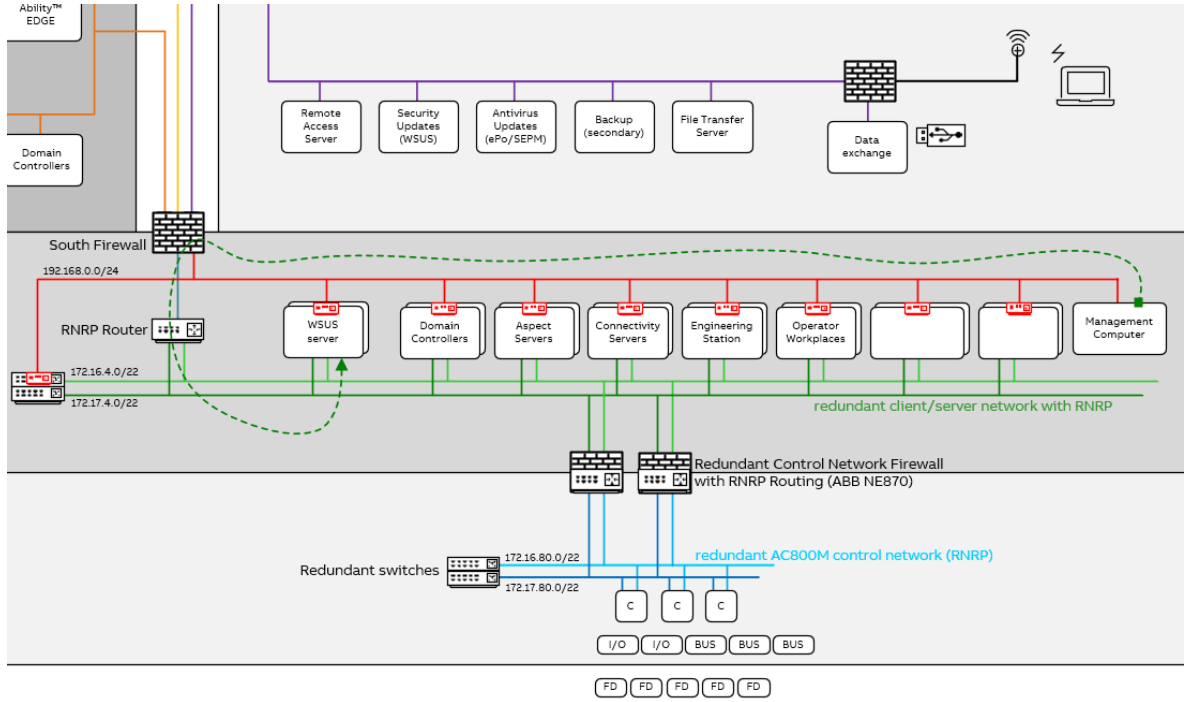
## Management Networks

### Customer

*“We were expecting to implement a management network in our design. As it's not shown on the reference architecture, is this prohibited?”*

### ABB

Sure we can do that. It's not part of our standard design, but our experts have provided us with guidance to set this up securely.



# ABB ICS Cyber Security Reference Architecture

Use-case 4

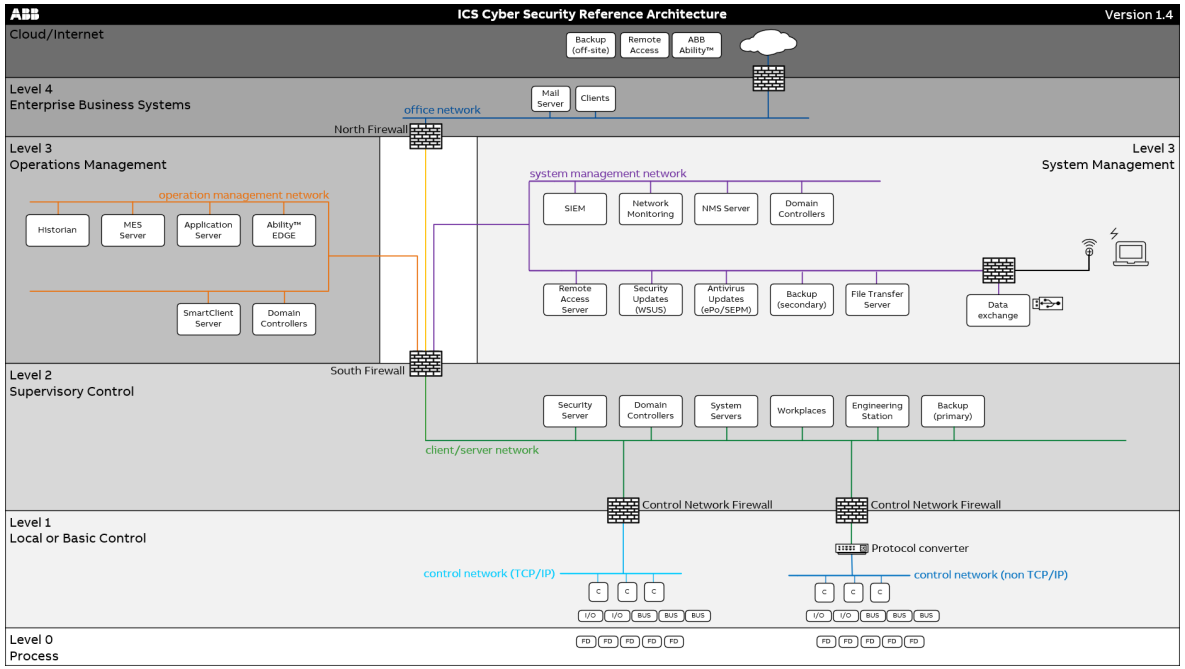
## Compliance

### Customer

*“My CISO told me that I must get my control system certified by the end of the year. Will the reference architecture make me compliant?”*

### ABB

No, but implementing the architecture will help you meet some of the compliance requirements related to data control and architecture.



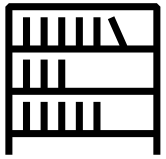
# ABB ICS Cyber Security Reference Architecture

## Conclusion

### Resource

The reference architecture is the keystone of OT security and your go to document

- ABB provides recommendations, not rules
- The architecture is highly flexible
- Applies to any OT system or device



### Compliance

The reference architecture is the foundation of cyber security compliance

- Rooted in IEC62443
- Address Functional Requirement 5
- Maintain compliance while adopting new technologies

### Digital Enabler

The reference architecture is an enabler for the implementation of digital services

- Securely connect to other systems and clouds
- Collect data without reducing security
- Remote access to reduce maintenance cost

**Mitigate cyber security risks with a solid architecture for your OT systems**


ABB