ABB CYBER SECURITY

ICS Cyber Security Reference Architecture

Drawings

Notice

This document contains information about one or in ABB products and may include a description of or a reference to one or more standards that may be generally relevant to the ABB products. The presence of any such description of a standard or reference to a standard is not a representation that all of the ABB products referenced in this document support all of the features of the described or referenced standard. In order to determine the specific features supported by a particular ABB product, the reader should consult the product specifications for the particular ABB product.

ABB may have one or more patents or pending patent applications protecting the intellectual property in the ABB products described in this document.

The information in this document is subject to change without notice and should not be construed as a commitment by ABB. ABB assumes no responsibility for any errors that may appear in this document.

Products described or referenced in this document are designed to be connected and to communicate information and data through network interfaces, which should be connected to a secure network. It is the sole responsibility of the system/product owner to provide and continuously ensure a secure connection between the product and the system network and/or any other networks that may be connected.

The system/product owners must establish and maintain appropriate measures, including, but not limited to, the installation of firewalls, application of authentication measures, encryption of data, installation of antivirus programs, and so on, to protect these products, the network, its system, and interfaces against security breaches, unauthorized access, interference, intrusion, leakage, and/or theft of data or information.

ABB performs functionality testing on the products and updates that we release. However, system/product owners are ultimately responsible for ensuring that any product updates or other major system updates (to include but not limited to code changes, configuration file changes, third-party software updates or patches, hardware change out, and so on) are compatible with the security measures implemented. The system/product owners must verify that the system and associated products function as expected in the environment in which they are deployed.

In no event shall ABB be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, nor shall ABB be liable for incidental or consequential damages arising from use of any software or hardware described in this document.

This document and parts thereof must not be reproduced or copied without written permission from ABB, and the contents thereof must not be imparted to a third party nor used for any unauthorized purpose.

The software or hardware described in this document is furnished under a license and may be used, copied, or disclosed only in accordance with the terms of such license.

This product meets the requirements specified in EMC Directive 2014/30/EU and in Low Voltage Directive 2014/35/EU.

The crossed–out wheeled bin symbol on the product and accompanying documents means that used electrical and electronic equipment (WEEE) should not be mixed with general household waste. If you wish to discard electrical and electronic equipment (EEE), please contact your dealer or supplier for further information.

Disposing of this product correctly will help save valuable resources and prevent any potential negative effects on human health and the environment, which could otherwise arise from inappropriate waste handling.

Trademarks and copyright

Ability is a trademark of ABB.

All rights to copyrights, registered trademarks, and trademarks reside with their respective owners.

Copyright © 2023 ABB. All rights reserved.

Release: January 2023

Document ID: 9AKK108467A7612

Revision: A

Table of contents

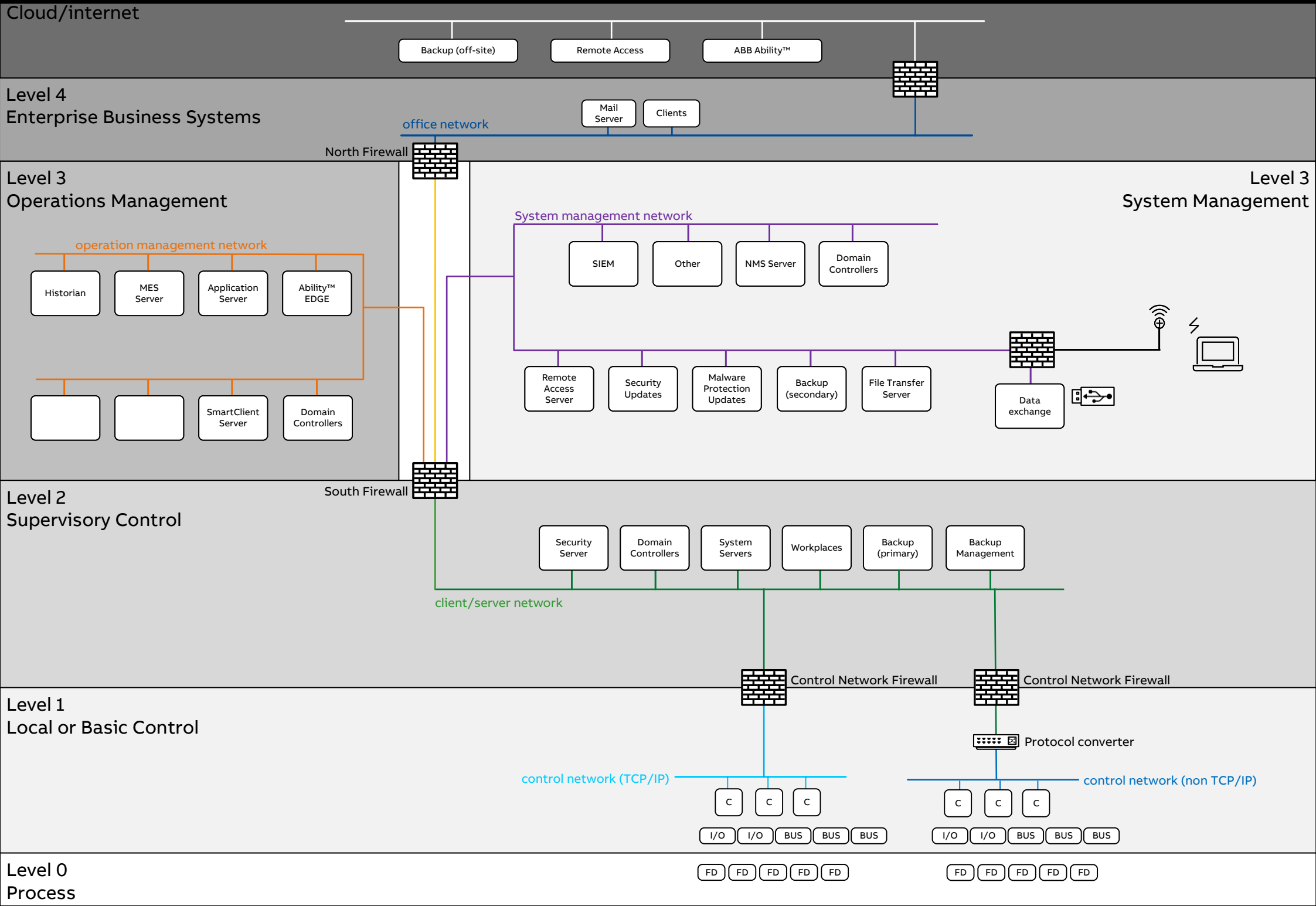
Generic 3
Zones 4
System 800xA 5
System 800xA with CS as routers 6
S+ with IET loop 7

1. Purpose and basic description

To help our customers apply the concepts of the Reference Architecture, the team has developed a set of drawings to help illustrate how specific setups and functions can be used.

ICS Cyber Security Reference Architecture

Generic 4:3



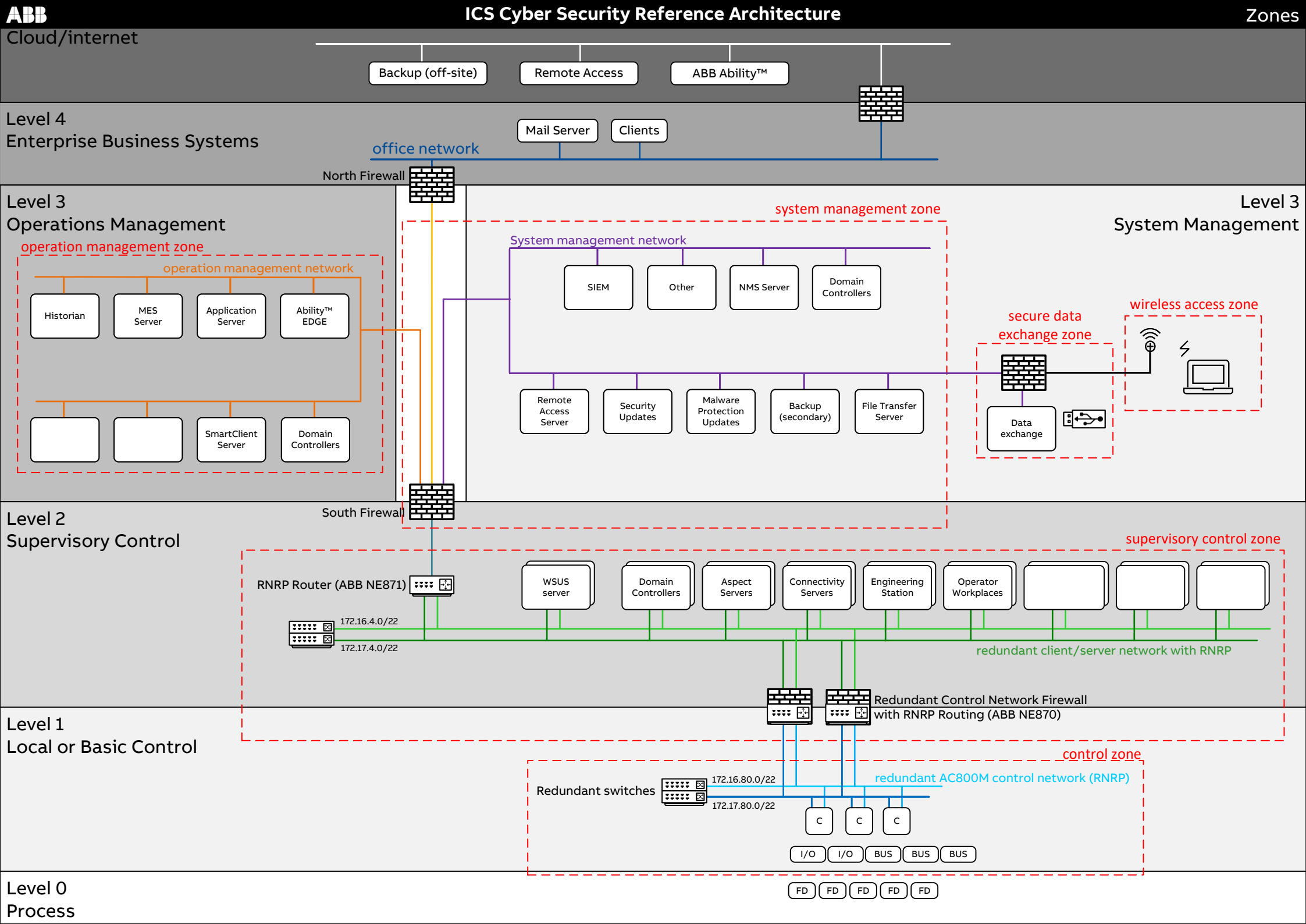
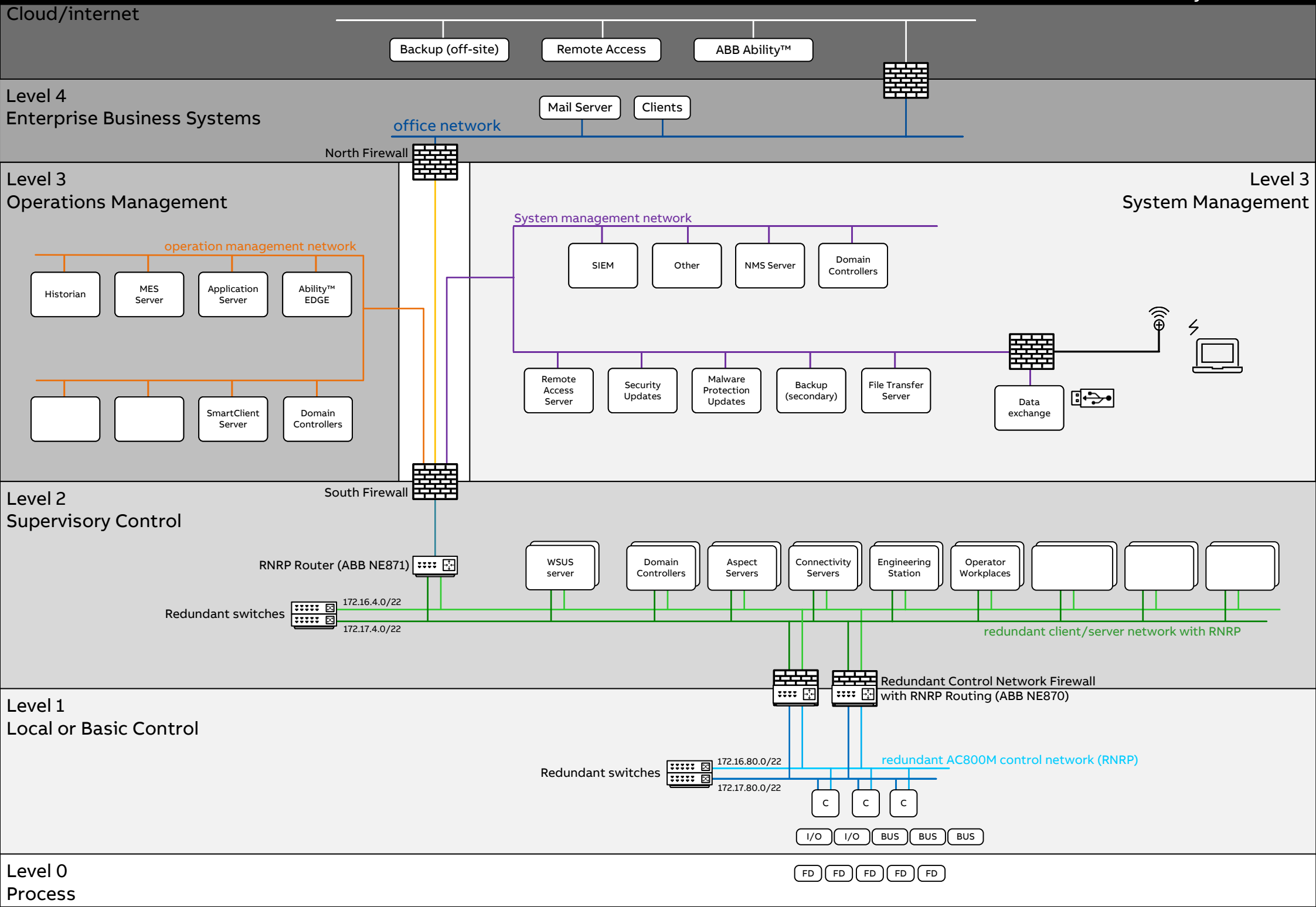


ABB
ICS Cyber Security Reference Architecture
Zones
Cloud/internet
Backup (off-site)
Remote Access
ABB Ability™
Level 4
Enterprise Business Systems
Mail Server
Clients
office network
North Firewall
Level 3
Operations Management
operation management zone
operation management network
Historian
MES Server
Application Server
Ability™ EDGE
SmartClient Server
Domain Controllers
system management zone
System management network
SIEM
Other
NMS Server
Domain Controllers
Remote Access Server
Security Updates
Malware Protection Updates
Backup (secondary)
File Transfer Server
Level 3
System Management
secure data exchange zone
Data exchange
wireless access zone
South Firewall
Level 2
Supervisory Control
supervisory control zone
RNRP Router (ABB NE871)
172.16.4.0/22
172.17.4.0/22
WSUS server
Domain Controllers
Aspect Servers
Connectivity Servers
Engineering Station
Operator Workplaces
redundant client/server network with RNRP
Redundant Control Network Firewall
with RNRP Routing (ABB NE870)
Level 1
Local or Basic Control
control zone
Redundant switches
172.16.80.0/22
172.17.80.0/22
redundant AC800M control network (RNRP)
C
C
C
I/O
I/O
BUS
BUS
BUS
Level 0
Process
FD
FD
FD
FD
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
Other
NMS Server
Domain Controllers
Remote Access Server
Security Updates
Malware Protection Updates
Backup (secondary)
File Transfer Server
Data exchange
South Firewall
Level 2
Supervisory Control
RNRP Router (ABB NE871)
Redundant switches
172.16.4.0/22
172.17.4.0/22
WSUS server
Domain Controllers
Aspect Servers
Connectivity Servers
Engineering Station
Operator Workplaces
redundant client/server network with RNRP
Redundant Control Network Firewall with RNRP Routing (ABB NE870)
Level 1
Local or Basic Control
Redundant switches
172.16.80.0/22
172.17.80.0/22
redundant AC800M control network (RNRP)
C
C
C
I/O
I/O
BUS
BUS
BUS
Level 0
Process
FD
FD
FD
FD
FD

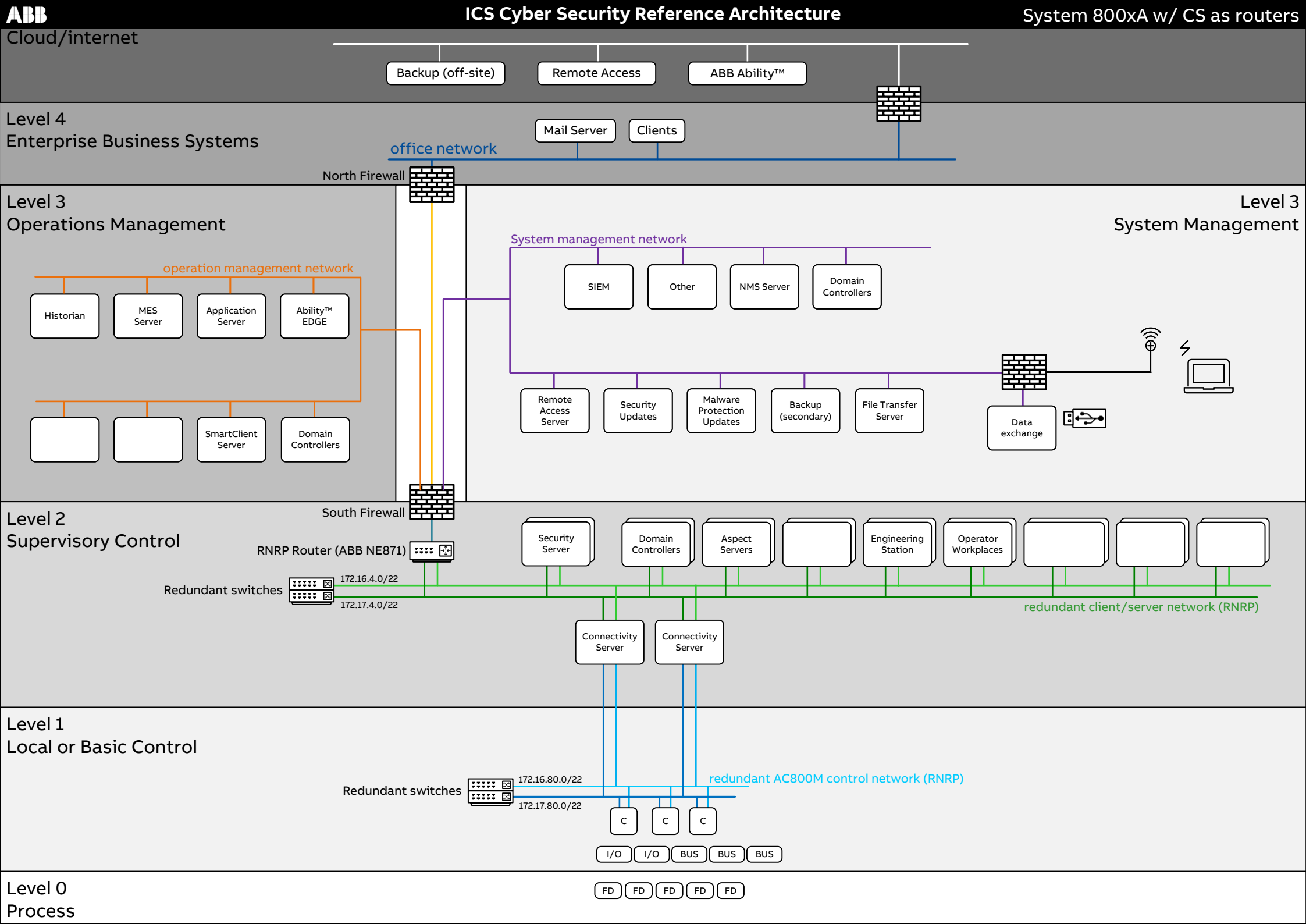


ABB
ICS Cyber Security Reference Architecture
System 800xA w/ CS as routers
Cloud/internet
Backup (off-site)
Remote Access
ABB Ability™
Level 4
Enterprise Business Systems
Mail Server
Clients
office network
North Firewall
Level 3
Operations Management
Level 3
System Management
System management network
operation management network
Historian
MES Server
Application Server
Ability™ EDGE
SmartClient Server
Domain Controllers
SIEM
Other
NMS Server
Domain Controllers
Remote Access Server
Security Updates
Malware Protection Updates
Backup (secondary)
File Transfer Server
Data exchange
South Firewall
Level 2
Supervisory Control
RNRP Router (ABB NE871)
Security Server
Domain Controllers
Aspect Servers
Engineering Station
Operator Workplaces
Redundant switches
172.16.4.0/22
172.17.4.0/22
redundant client/server network (RNRP)
Connectivity Server
Connectivity Server
Level 1
Local or Basic Control
Redundant switches
172.16.80.0/22
172.17.80.0/22
redundant AC800M control network (RNRP)
C
C
C
I/O
I/O
BUS
BUS
BUS
Level 0
Process
FD
FD
FD
FD
FD

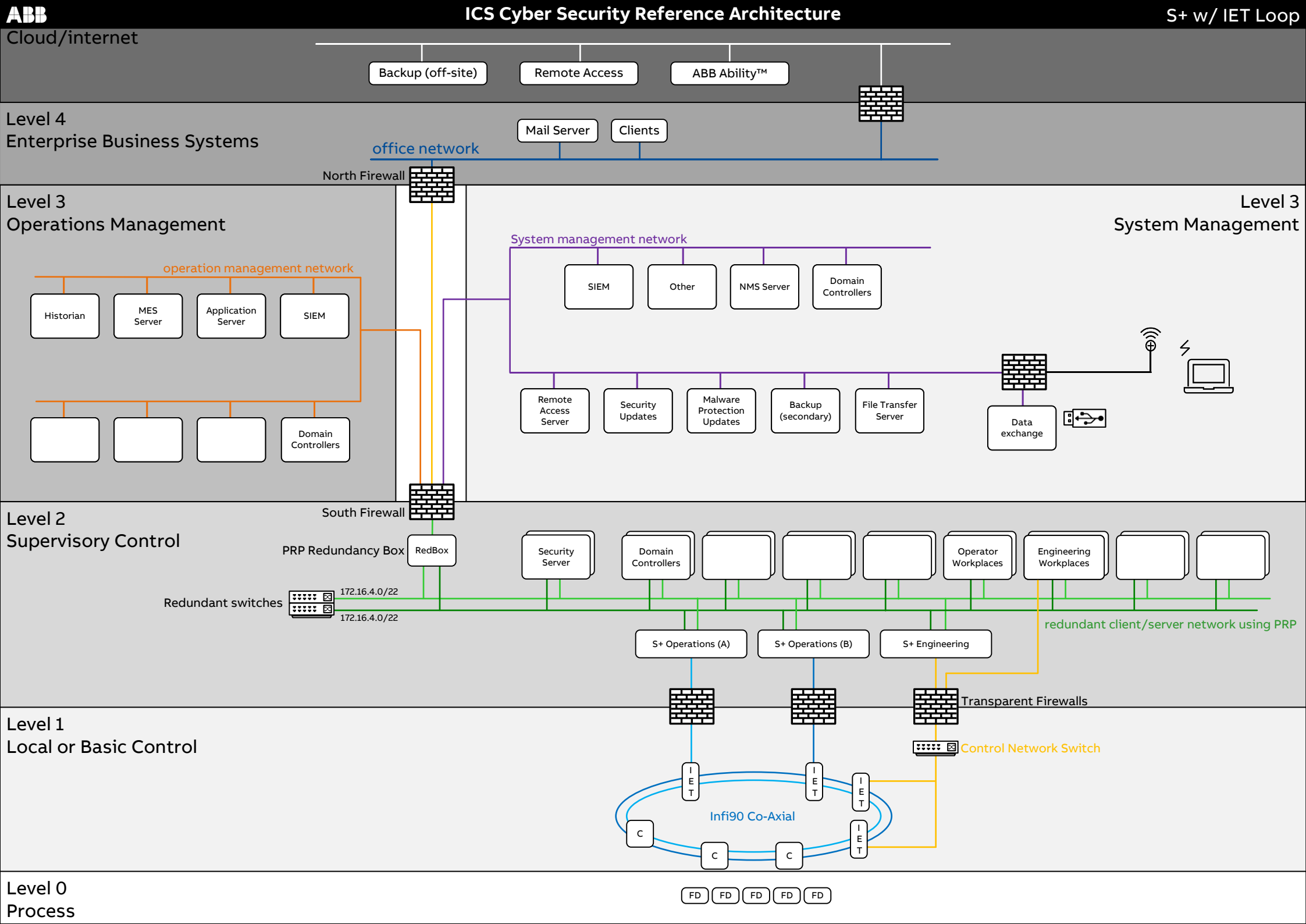


ABB
ICS Cyber Security Reference Architecture
S+ w/ IET Loop
Cloud/internet
Backup (off-site)
Remote Access
ABB Ability™
Level 4
Enterprise Business Systems
Mail Server
Clients
office network
North Firewall
Level 3
Operations Management
operation management network
Historian
MES Server
Application Server
SIEM
Domain Controllers
Level 3
System Management
System management network
SIEM
Other
NMS Server
Domain Controllers
Remote Access Server
Security Updates
Malware Protection Updates
Backup (secondary)
File Transfer Server
Data exchange
South Firewall
Level 2
Supervisory Control
PRP Redundancy Box
RedBox
Security Server
Domain Controllers
Operator Workplaces
Engineering Workplaces
Redundant switches
172.16.4.0/22
172.16.4.0/22
redundant client/server network using PRP
S+ Operations (A)
S+ Operations (B)
S+ Engineering
Transparent Firewalls
Level 1
Local or Basic Control
Control Network Switch
IET
IET
IET
IET
Infi90 Co-Axial
C
C
C
Level 0
Process
FD
FD
FD
FD
FD

Visit us

www.abb.com/cybersecurity