

Magnus Hammar, 800xA User Group, 041216

# Cyber Security & Network Equipment

# Cybersecurity & Network equipment

- Cybersecurity update
- Wired network equipment
  - Trends & Drives
  - Main benefits





BU CT Sales and Marketing 2015

# Control Systems Academy 800xA 6.0 Cyber Security Update

# Cybersecurity. Why is it important?

## Examples of recent events

FINANCIAL TIMES

ft.com/global/economy

September 23, 2010 7:39 pm

### Stuxnet worm causes worldwide alarm

By Joseph Menn and Mary Watkins

No one knows the ultimate goal of the Stuxnet worm, which targets industrial machinery and factories. It could destroy gas pipelines, cause oil refineries to explode. Perhaps it already has.

**Forbes**

INVESTING | 10/21/2011 @ 12:27PM | 9,193 views

### 'Duqu' Virus Likely Handiwork Of Sophisticated Government, Kaspersky Lab Says

+ Comment Now + Follow Comment

The Duqu Trojan probably a government tool. What is it looking for? And which country is looking for it remains a mystery.

regular threats, like botnets, are not. Duqu, considered the most sophisticated of

**the guardian** | **The Observer**

News | Sport | Comment | Culture | Business | Money | Life & style

News | Technology | The networker

Series: The networker

### How Flame virus went undetected for everything for

The Flame virus went undetected for a security firm. Now they need to protect the world's PCs from malware.

**BBC**

News | Sport | Weather | Capital | Culture | Show

## NEWS TECHNOLOGY

Home | UK | Africa | Asia | Europe | Latin America | Mid-East | US & Canada | Business | Health | Sci/Environment

17 August 2012 Last updated at 14:22 GMT

### Shamoon virus targets energy sector infrastructure

A new threat targeting infrastructure in the energy industry has been uncovered by security specialists.

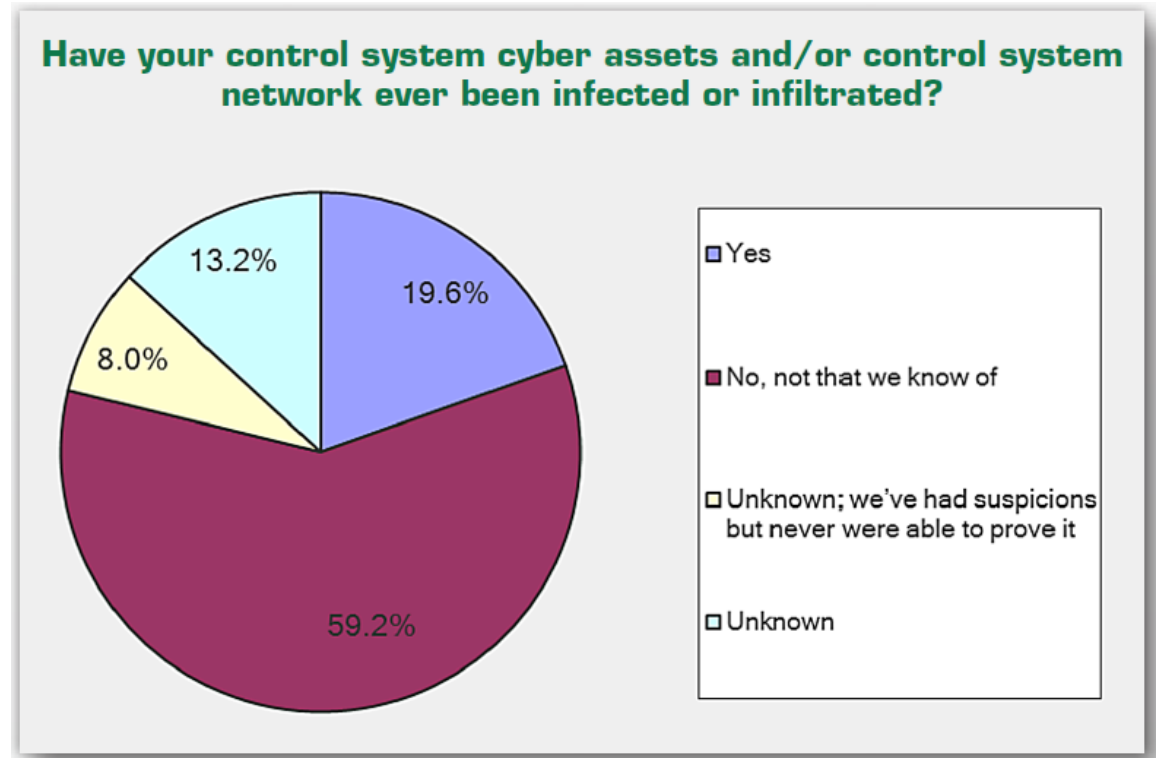
The attack, known as Shamoon, is said to have hit "at least one organisation" in the sector.

Shamoon is capable of wiping files and rendering several computers on a network unusable.

On Wednesday, Saudi Arabia's national oil company, Saudi Aramco, is Saudi Arabia's national oil provider.

# Cybersecurity. Why is it important?

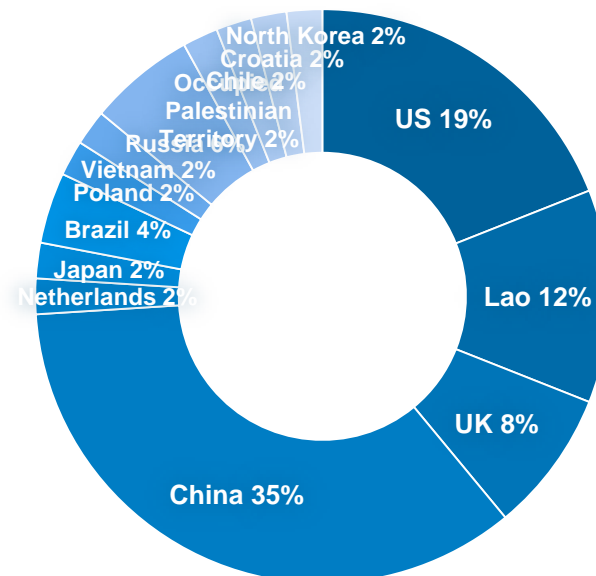
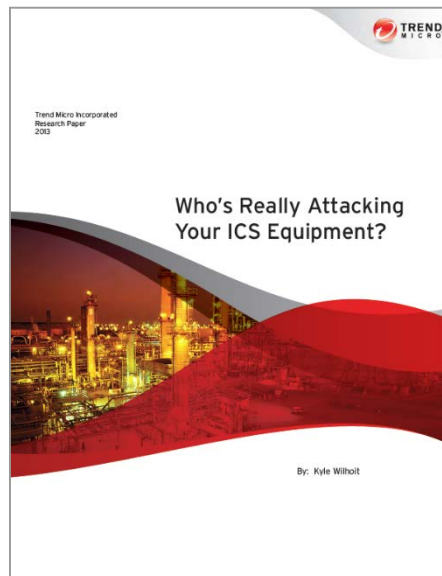
Anonymous US Survey  
made by the SANS Analyst  
Organization (2013)  
covering most major  
Industries



# Why is it important?

## Other real case examples

1. IT department use vulnerability scanning tools
2. Neeris brought in by USB-stick
3. A control system could be targeted with 39 attacks in 28 days!





# What is Cyber Security?

## Summary



**Hacking**



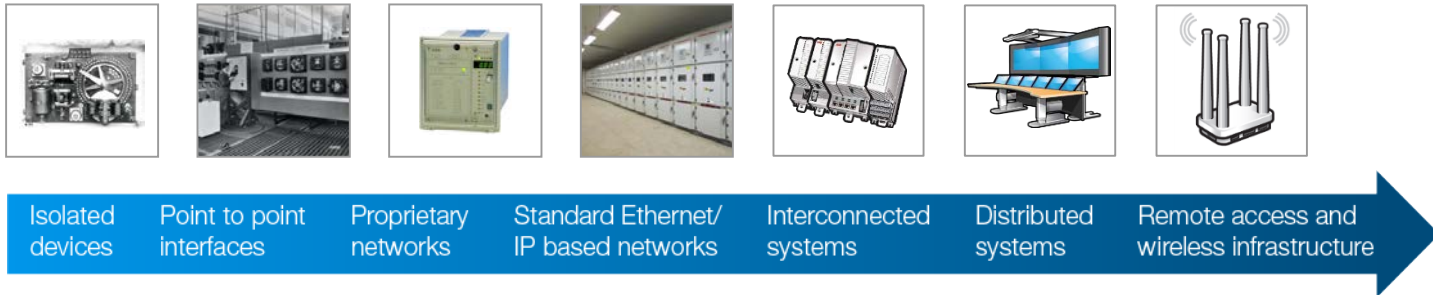
**Malicious  
software**



**Employee  
Mistake**

# What is Cyber Security?

## Why is it an issue?



Threats to standard IT systems largely also apply to ICS



IT focused criminal ecosystem

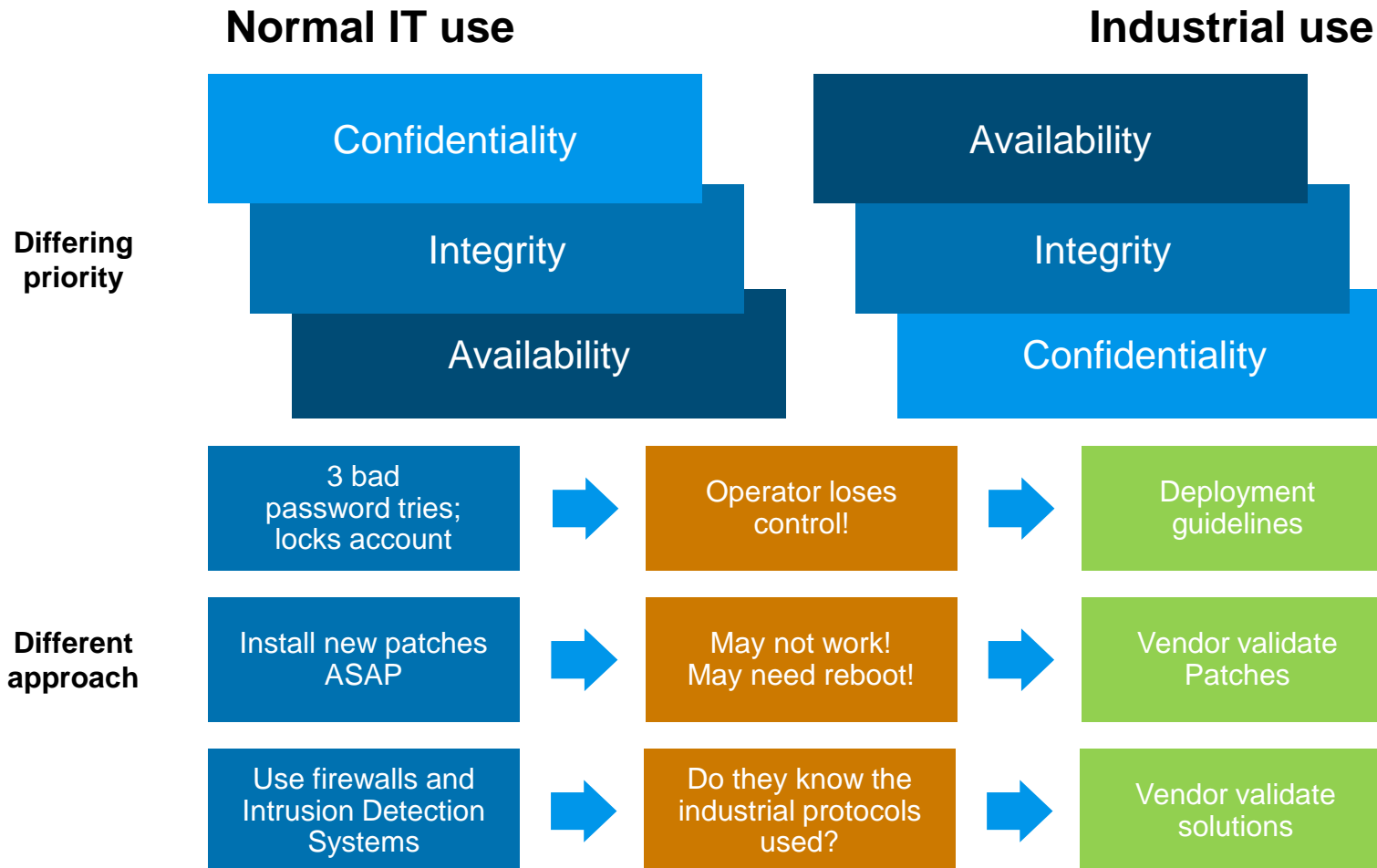


**Increased risk!**



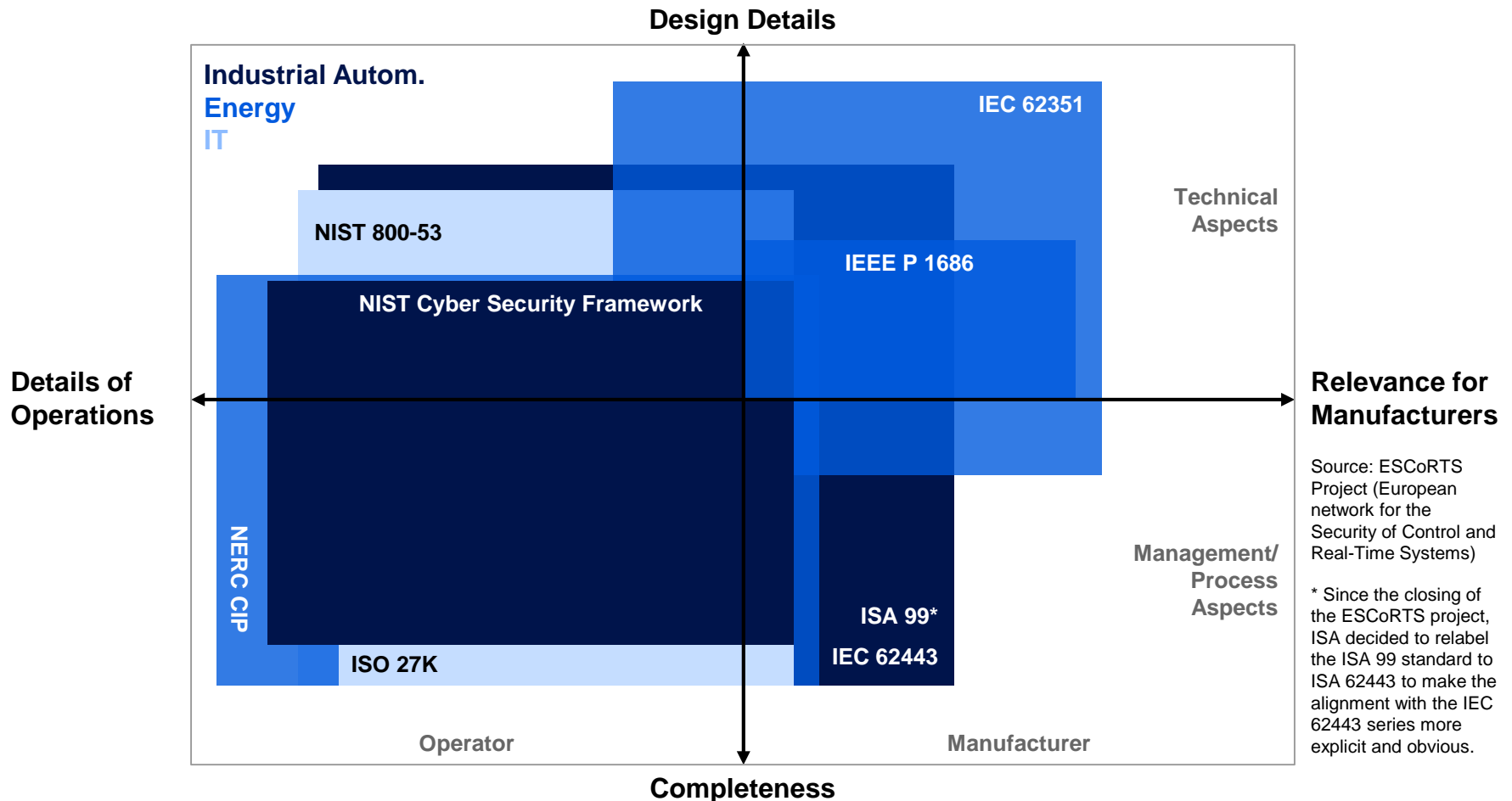
# Cyber security best practices

## Normal IT vs. Industrial best practices



# Cyber security best practices

## A lot of support available



# Cyber security best practices

## Defense in Depth

**The coordinated use of multiple security measures, addressing people, technology, and operations.**

Physical Security

Procedures and Policies

Firewalls and Architecture

Computer Policies

Account Management

Security Updates

Antivirus Solutions



# How ABB works with Cyber Security

## The SD<sup>3</sup> + C Security Framework used for 800xA



### Secure by Design

Security in the Product Development Process:  
Requirements, Design, Implementation, Verification

### Secure by Default

Default installation and usage with  
minimal attack surface  
Built in functions for Defense in Depth

### Secure in Deployment

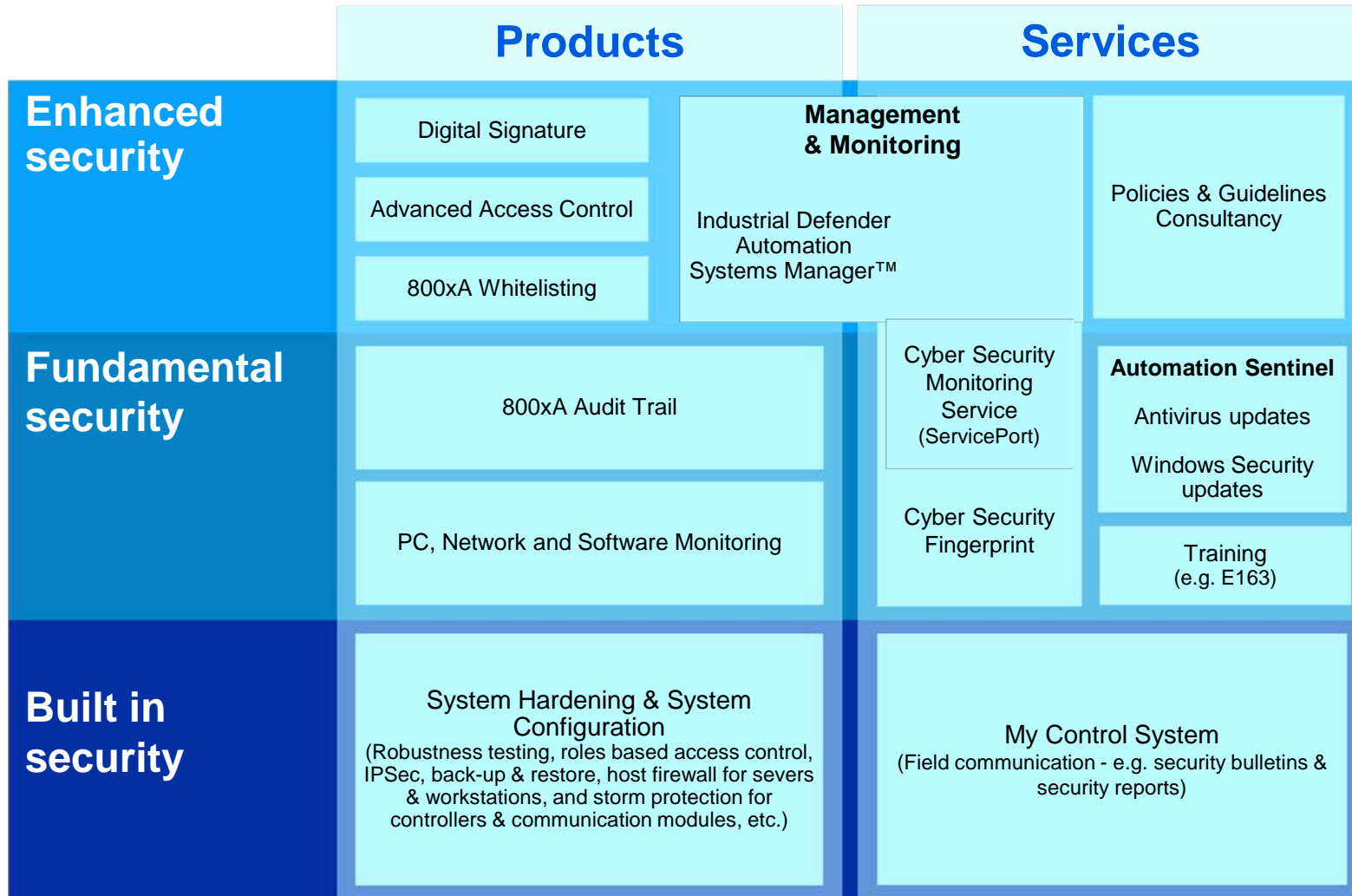
Support for Secure Project and Plant Lifecycle  
Validation of 3<sup>rd</sup> party software and solutions

### Communication

Correct information to those who need to know

# 800xA Extended Security

## A modular approach

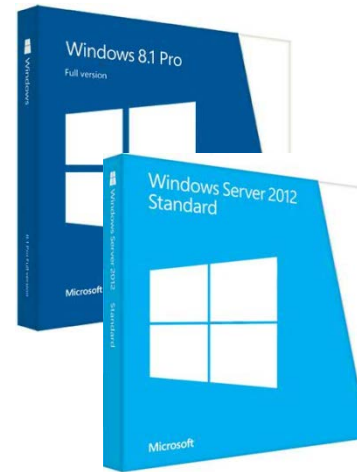


# What is new in 6.0?

Future proof and easier to keep secure



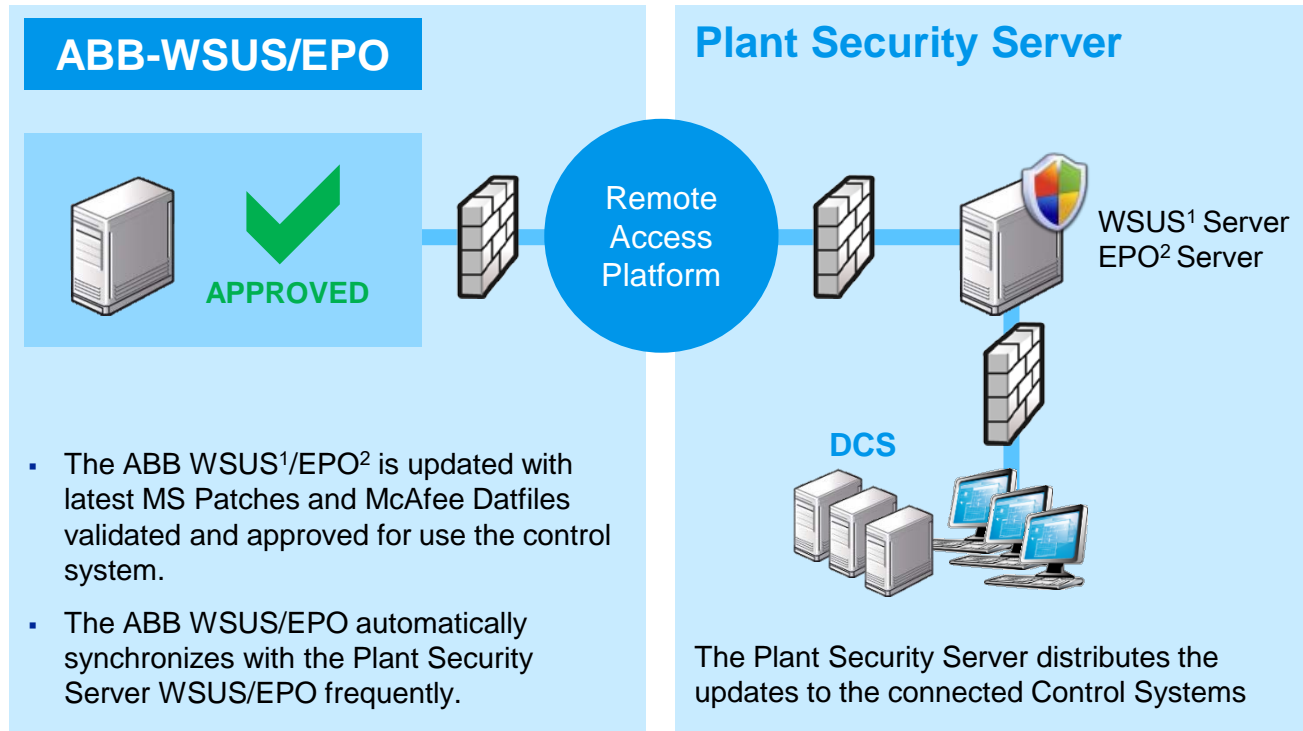
- Based on Windows 8.1 & Server 2012 R2
- Improved Cyber Security robustness testing
- Windows UAC - User Account Control
- Digital system code signing of applications
- Faster access to approved Microsoft security updates and anti virus definition files



**The most secure system  
available without  
compromising functionality**

# What is new in 6.0?

## Download from ABB WSUS/EPO



Pilot phase Q1-2, 2014

<sup>1</sup> Windows Security Update Service

<sup>2</sup> McAfee ePolicy Orchestrator







# 800xA Networks

# Ethernet in industrial applications

## Trends & drivers



### Trends & drivers:

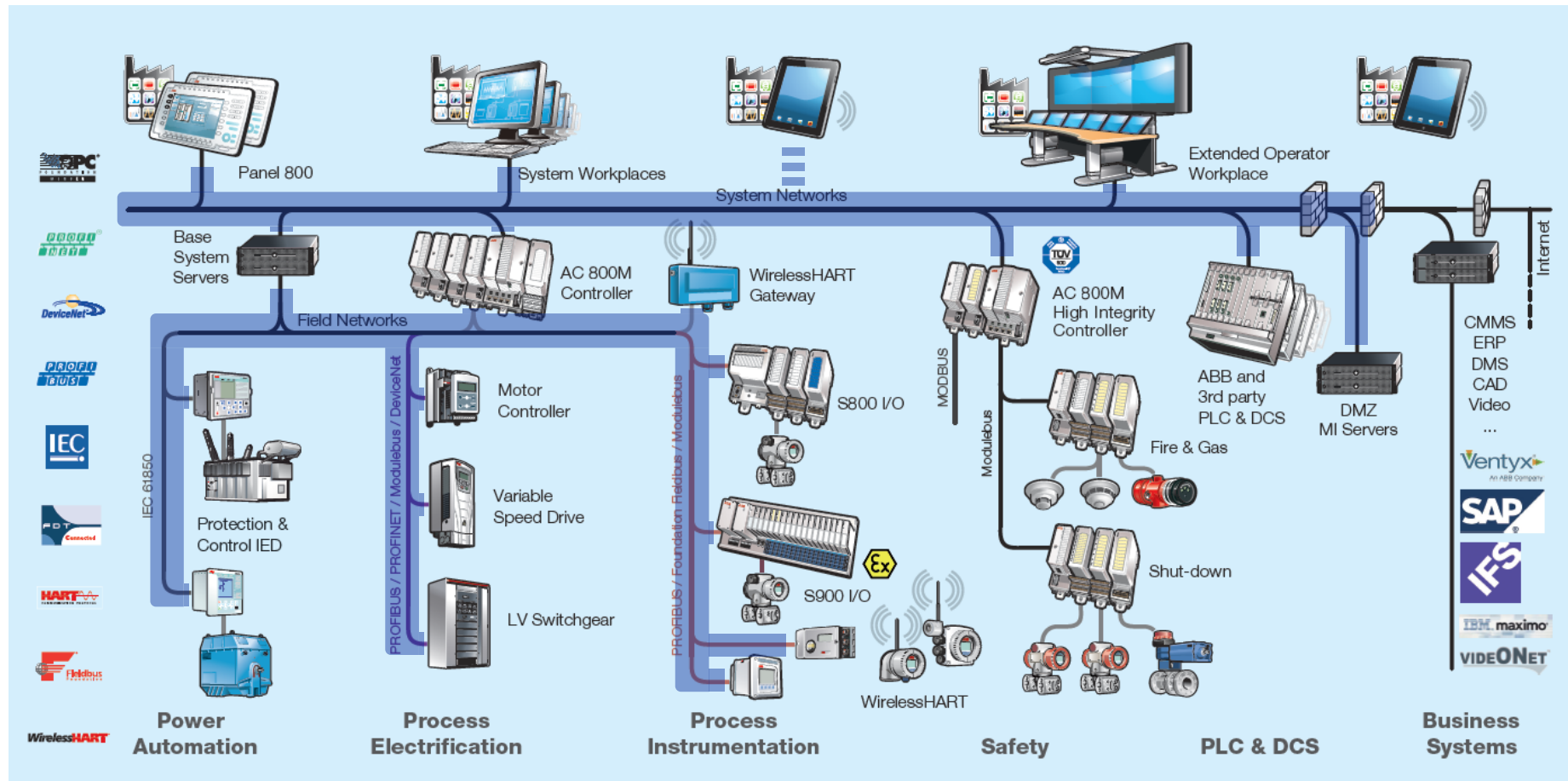
- Increasing use of PROFINET, IEC 61850, EtherNet/IP, etc.
- Ethernet reach the field to a greater extent.
- Cyber security focus
- Remained focus on reliability & availability
- Mobility

### Leads to:

- More & more functionality in network equipment, but harder to configure.
- Increased focus on monitoring of IT assets to ensure stable systems.
- Wireless deployment of automation networks

# System 800xA

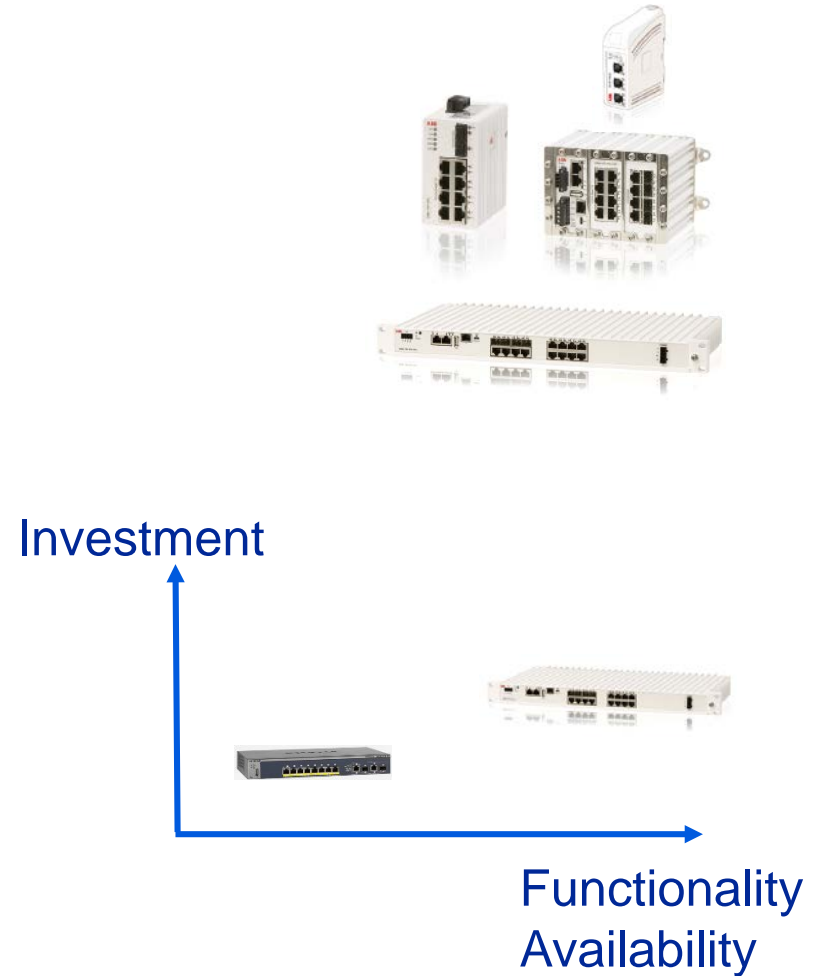
## Modern DCS depend on a reliable network



# 800xA Network Switches

## Key benefits

- ABB can now take full responsibility also for the networks in our Control System deliveries
- Detailed supervision makes it possible to detect and solve network related problems early
- Designed for industrial use gives high availability, also in tough environments



# 800xA Networks

## Fully supported by ABB

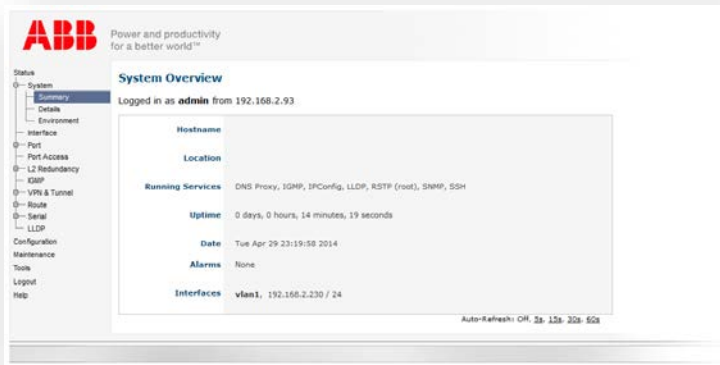
- Preconfigured for 800xA.
- Integrated detail status monitoring & alarming.
- **Fully supported by ABB.**

Type of equipment	Configuration support	Architecture support	Software support (E.g. firmware)	Hardware support
<u>Non</u> Industrial IT certified				
Industrial IT certified	✓	✓		
800xA Networks	✓	✓	✓	✓

**When questions arise, you can always  
turn to ABB.**

# 800xA Networks

## Preconfigured for 800xA



- Switches are preconfigured for use with 800xA.
- Only two settings are needed to get up and running:
  - Change the default IP.  
(If more than one switch is used.)
  - Set speed & half/full duplex.  
(Especially for AC800M.)

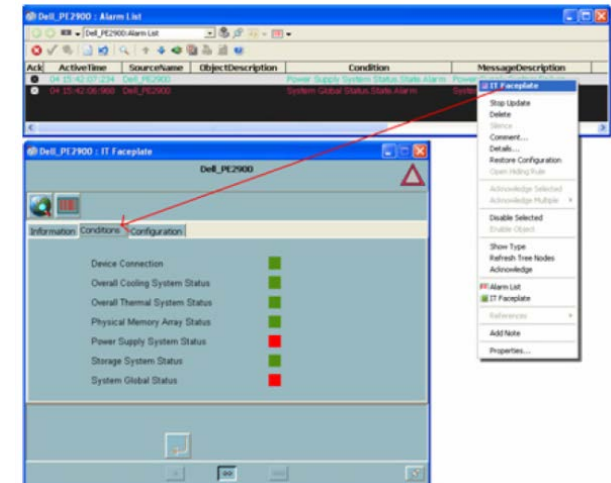
**Increased engineering efficiency  
&  
Reduced risk of misconfiguration =  
Increased uptime**

# 800xA Networks

## Enhanced network monitoring – PNSM Intro

PNSM enables embedded monitoring of IT-assets in System 800xA. The following types of equipment can e.g. be monitored:

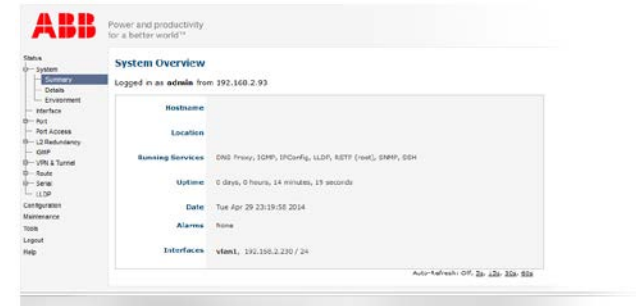
- Servers
- Workstations
- Switches
- Firewalls



D-00134:Asset Reporter

D-00134- Asset Condition View

Severity	AM Name	Condition	Sub Condition	Description	Timestamp	Quality Status
1	Overall Cooling System Status	State	Normal		5/7/2008 9:11:40 AM	good
1000	Power Supply System Status	State	Alarm	Power Supply System Failure	5/7/2008 9:11:40 AM	good
1	Storage System Status	State	Normal		5/7/2008 9:11:40 AM	good
1	Device Connection	State	Normal		5/7/2008 9:11:40 AM	good
1	Physical Memory Array Status	State	Normal		5/7/2008 9:11:40 AM	good
1	Overall Thermal System Status	State	Normal		5/7/2008 9:11:40 AM	good
1000	System Global Status	State	Alarm	System Global Status is not OK.	5/7/2008 9:11:40 AM	good





# 800xA Networks

## Enhanced network monitoring

- Preconfigured for 800xA.
- **Integrated detail status monitoring & alarming.**
- Fully supported by ABB.

Attribute monitored	IIT certified	800xA Networks
Device general health (summary alarm)	✓	✓
Power supply status	✓	✓
Port connected		✓
Port lockdown		✓
Device temperature		✓
Traffic (Packets per second & per port)		✓
Input Error Rate (% of bad/dropped packages)		✓



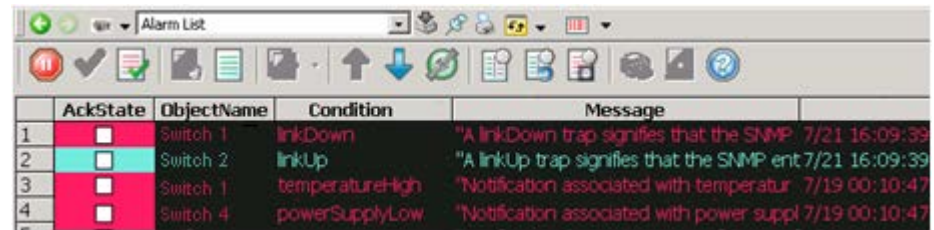
**Early identification of network issues, before problems arise.**  
**=**  
**Increased uptime.**

# 800xA Networks

## Enhanced network monitoring

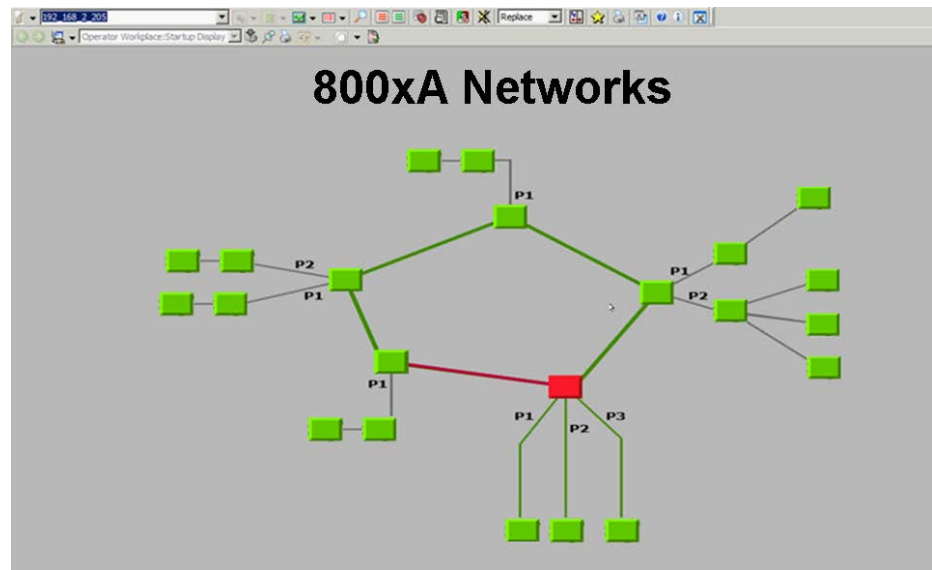
- Preconfigured for 800xA.
- **Integrated detail status monitoring & alarming.**
- Fully supported by ABB.

- Faceplates, documentation, trends, and alarm lists, is easily accessible using standard aspect/object technology.



	AckState	ObjectName	Condition	Message
1	<input type="checkbox"/>	Switch 1	linkDown	"A linkDown trap signifies that the SNMP 7/21 16:09:39
2	<input type="checkbox"/>	Switch 2	linkUp	"A linkUp trap signifies that the SNMP ent 7/21 16:09:39
3	<input type="checkbox"/>	Switch 1	temperatureHigh	"Notification associated with temperatur 7/19 00:10:47
4	<input type="checkbox"/>	Switch 4	powerSupplyLow	"Notification associated with power suppl 7/19 00:10:47

- Graphical representation of the network can be created to easily identify where in the network an issue arisen.
- Solution is integrated into Maintenance Workplace.



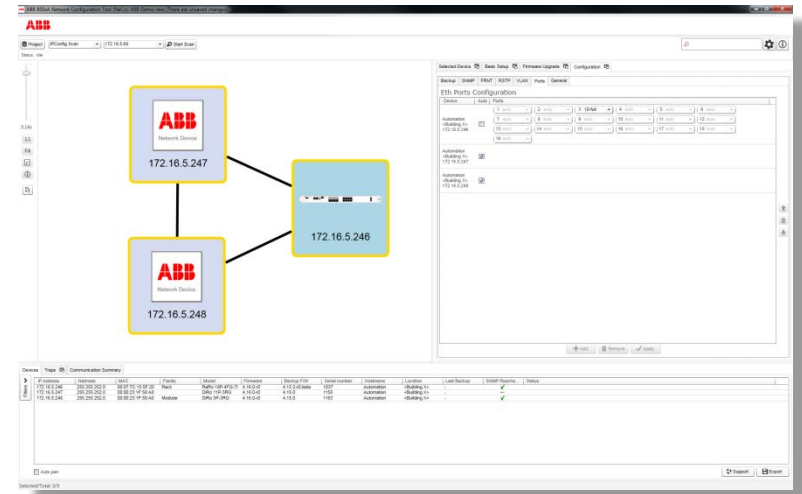
# 800xA Networks Portfolio



	NE840	NE820	NE810	NE801	NE802
Ports	19	19	10	5	5
- Gbps	4 (SFP) 7 (RJ45)	4 (SFP) 7 (RJ45)	2 (SFP)		1 (SFP) 4 (RJ45)
- 10/100 Mbps	8 (RJ45)	8 (RJ45)	8 (RJ45)	1 (LC) 4 (RJ45)	
Managed	✓	✓	✓	Lightly**	Lightly**
RSTP	✓	✓	✓		
Ring redundancy	FRNT (20ms recovery time)	FRNT (20ms recovery time)	FRNT (20ms recovery time)		
VLAN	IEEE 802.1Q	IEEE 802.1Q	IEEE 802.1Q		
Quality of Service	4 queues	4 queues	4 queues		
G3 compliant	✓	✓	✓	✓	✓
Temperature range	-40 to +55°C	-40 to +70°C	-40 to +70°C	-25 to +70°C	-40 to +70°C
Fanless	✓	✓	✓	✓	✓
Marine certification	DNV	DNV	DNV	DNV	DNV
Power supply	110/230V AC	Redundant 24V DC	Redundant 24V DC	Redundant 24V DC	Redundant 24V DC

# 800xA Networks Portfolio

- **NeCo** – Easy-to-use configuration tool
  - Draw 2D graphical representation automatically.
  - Upload new firmware in a bulk manner.
  - Bulk configuration
- Wide range of **SFPs**
  - LC connectors
    - Multi mode & single mode
    - 0.55 – 120km range
    - Possible to monitor
  - RJ45 connectors

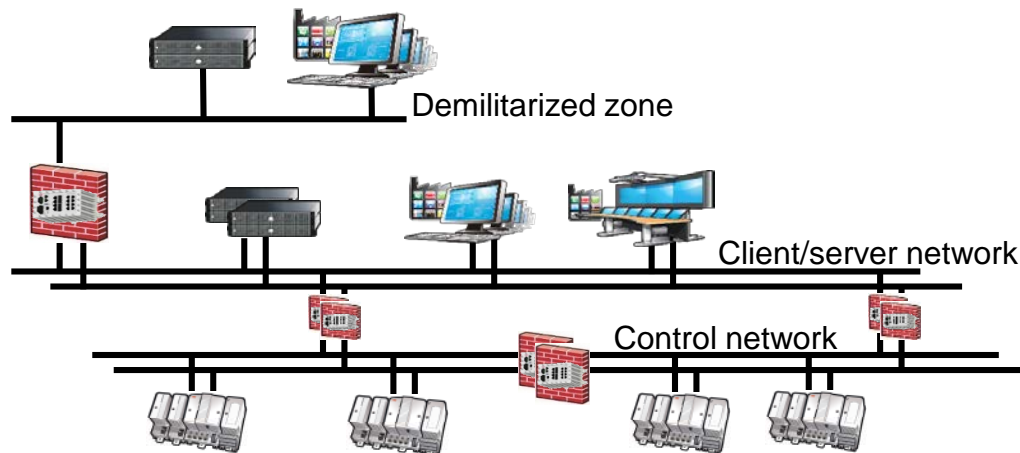


# 800xA Networks

## RNRP Routers

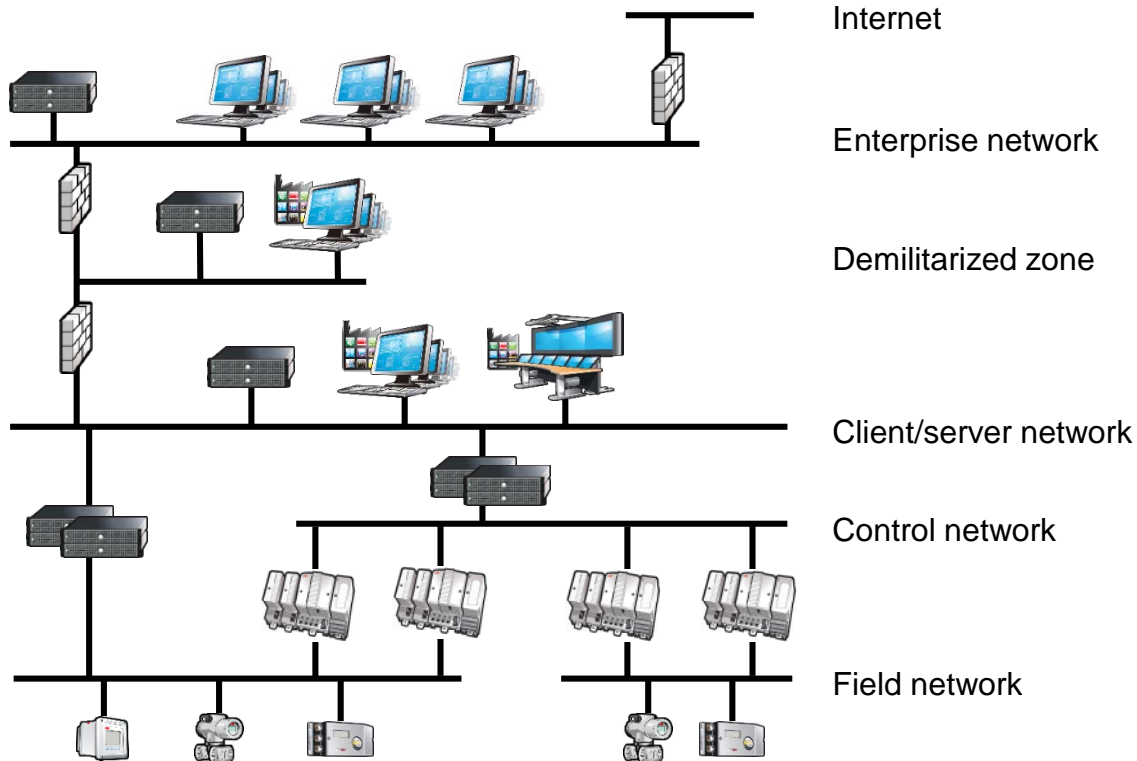
- RNRP – Redundant Network Routing protocol
- RNRP Routers
  - Will have same ruggedness and functionality as existing Network Equipment + RNRP and firewall
  - Makes it possible to separate network areas with full redundancy without using windows computers
  - Can connect from redundant Client/Server network to single DMZ network
  - Makes it possible to separate Safety networks without using windows PCs for separation

	NE870	NE871
Ports	11	3
- Gbps	3 (RJ45)	3 (RJ45)
- 10/100 Mbps	8 (RJ45)	
Managed	✓	✓
Routing	✓	✓
- RNRP	✓	✓
Firewall	✓	✓



# What about networking security?

## Security zones - Layers, Traditional design

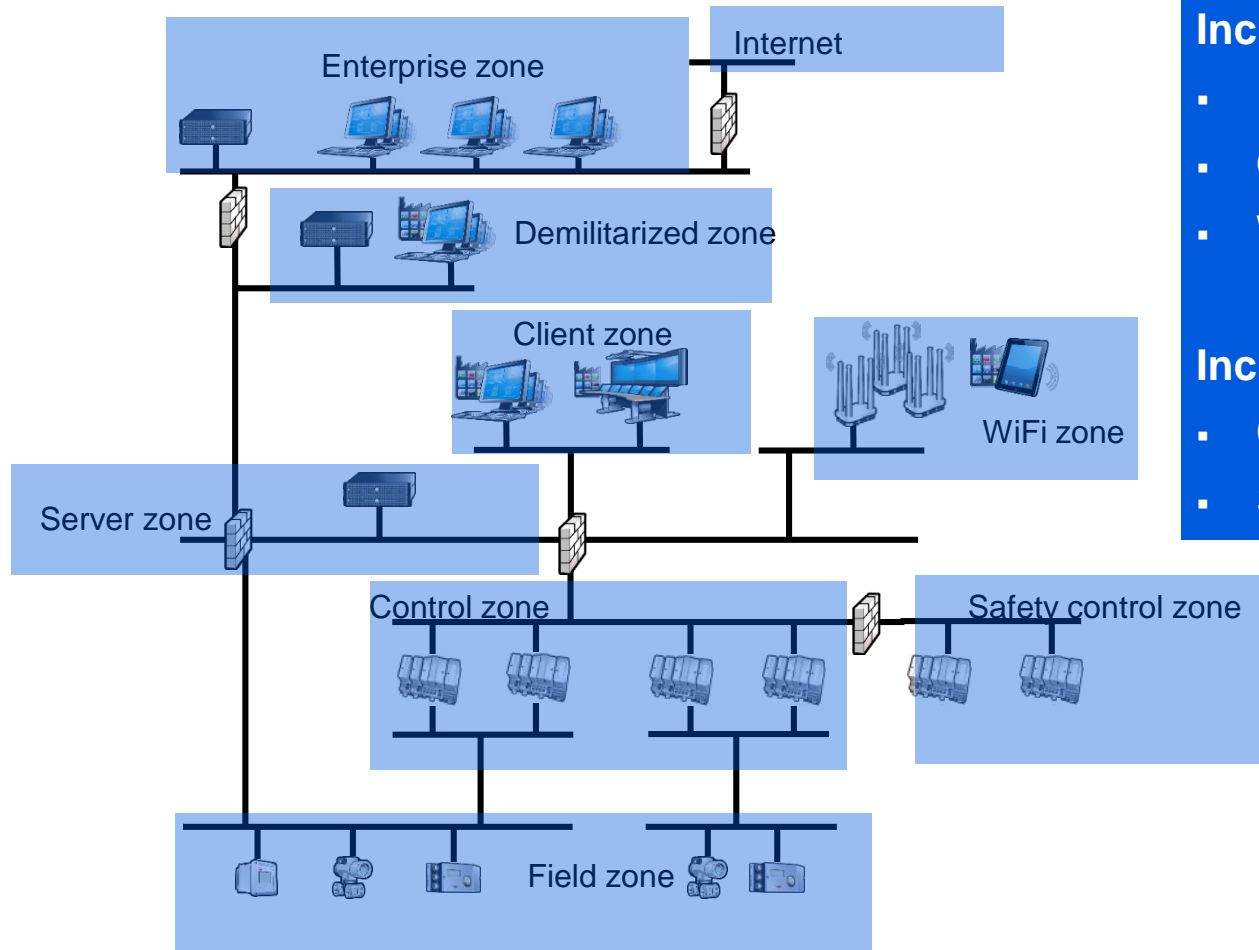


Is the risk the same throughout the entire system?

$$\text{Risk} = \text{Likelihood} \times \text{Impact}$$

# What about networking security?

## Security zones, an example



### Increased incident likelihood:

- Enterprise network?
- Obsolete Windows nodes?
- Wireless networks?

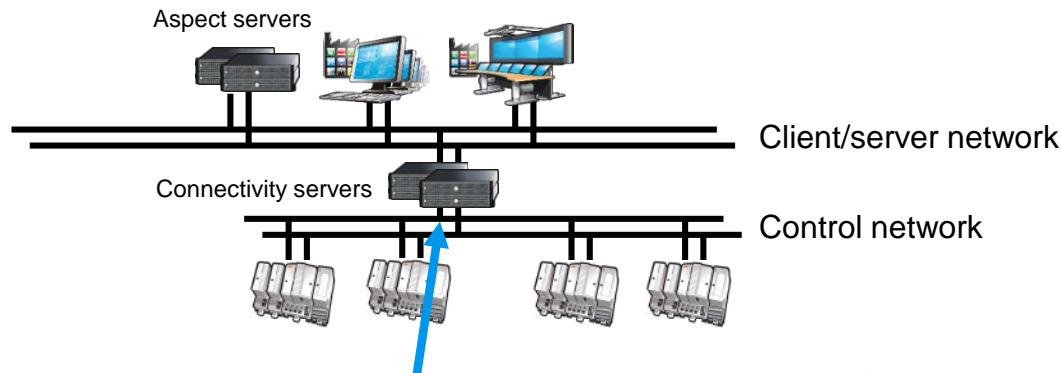
### Increased incident impact:

- Control Networks?
- Safety networks?



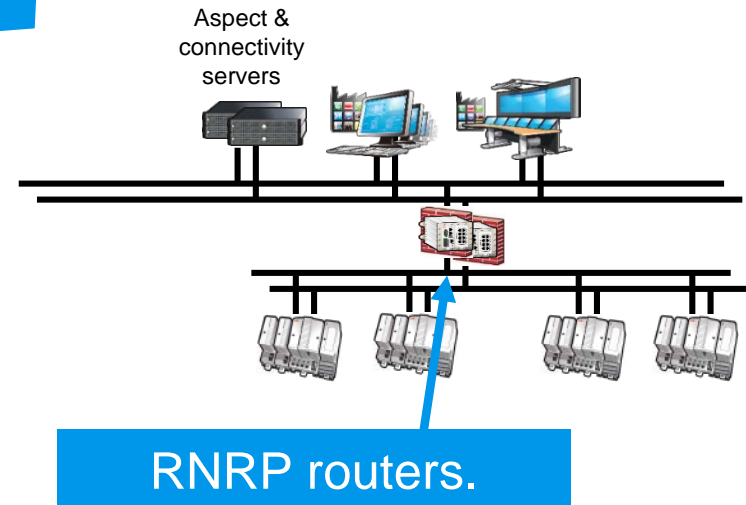
# What about networking security?

## RNRP networks today & tomorrow



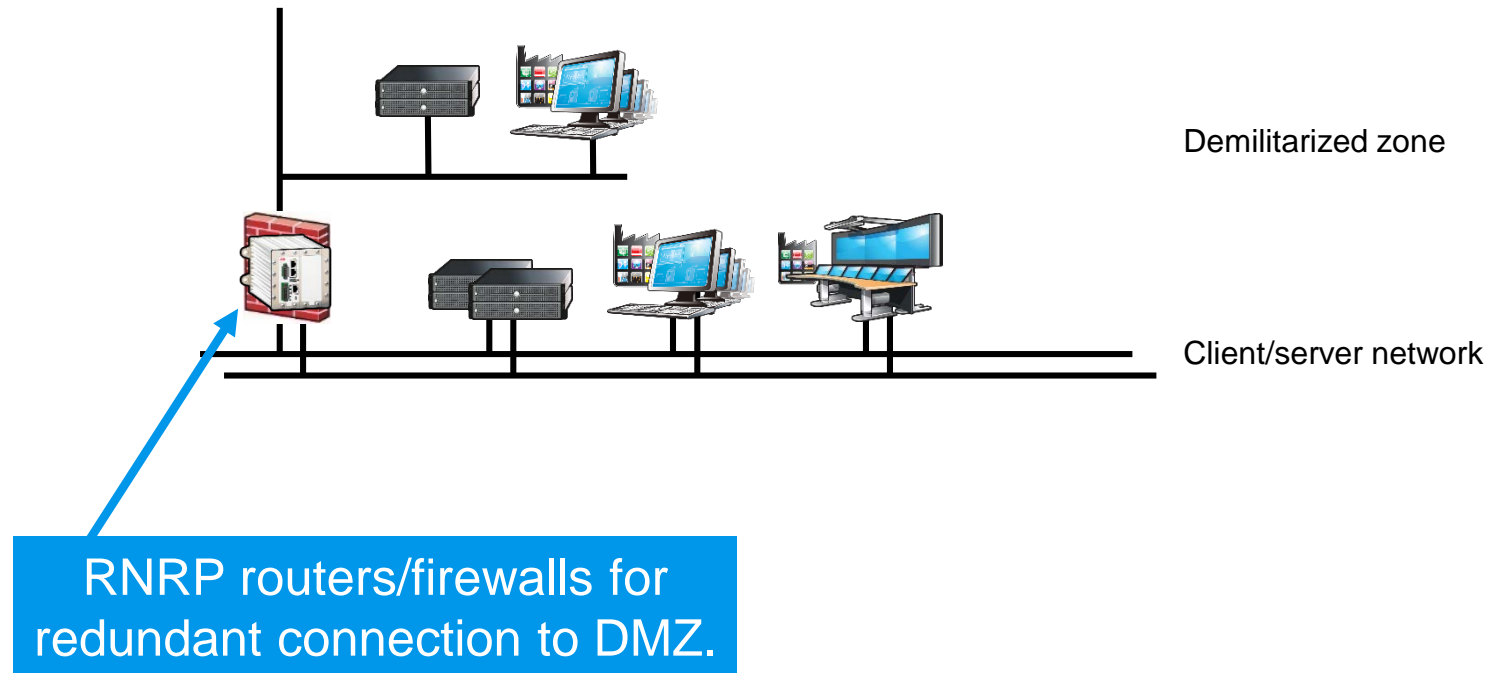
Connectivity servers also work as RNRP routers.

Increased availability,  
enhanced security, &  
decreased maintenance.



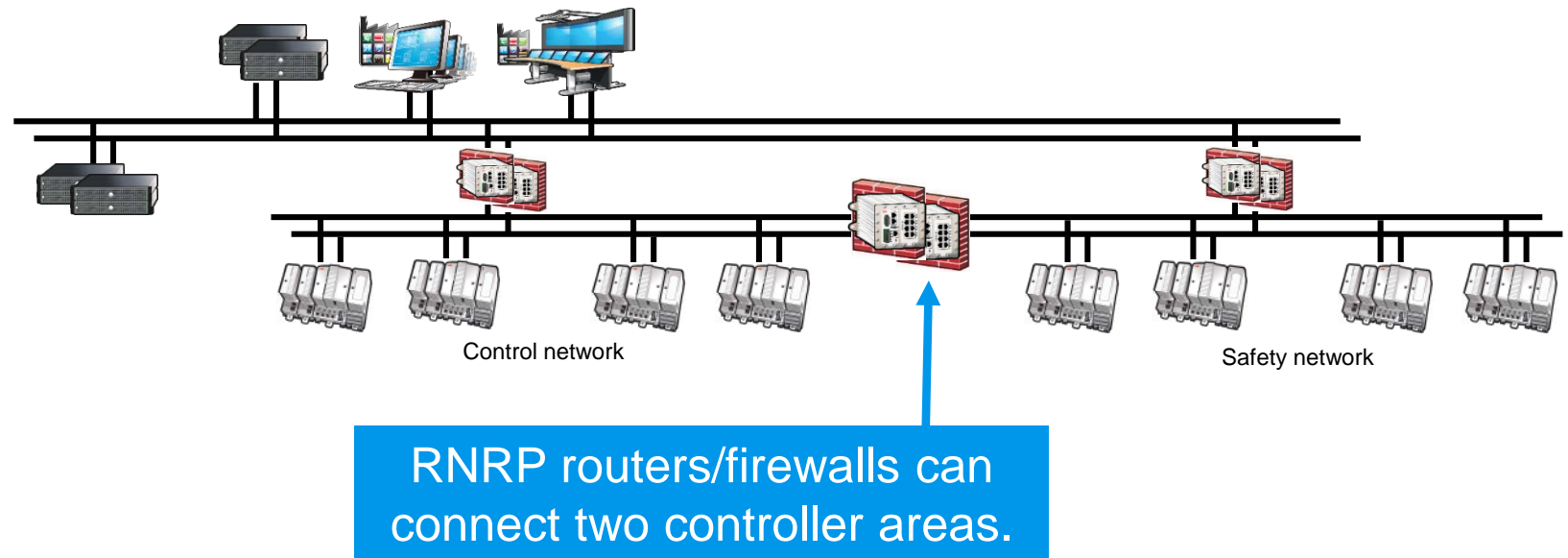
# What about networking security?

## RNRP networks tomorrow – Connect to DMZ



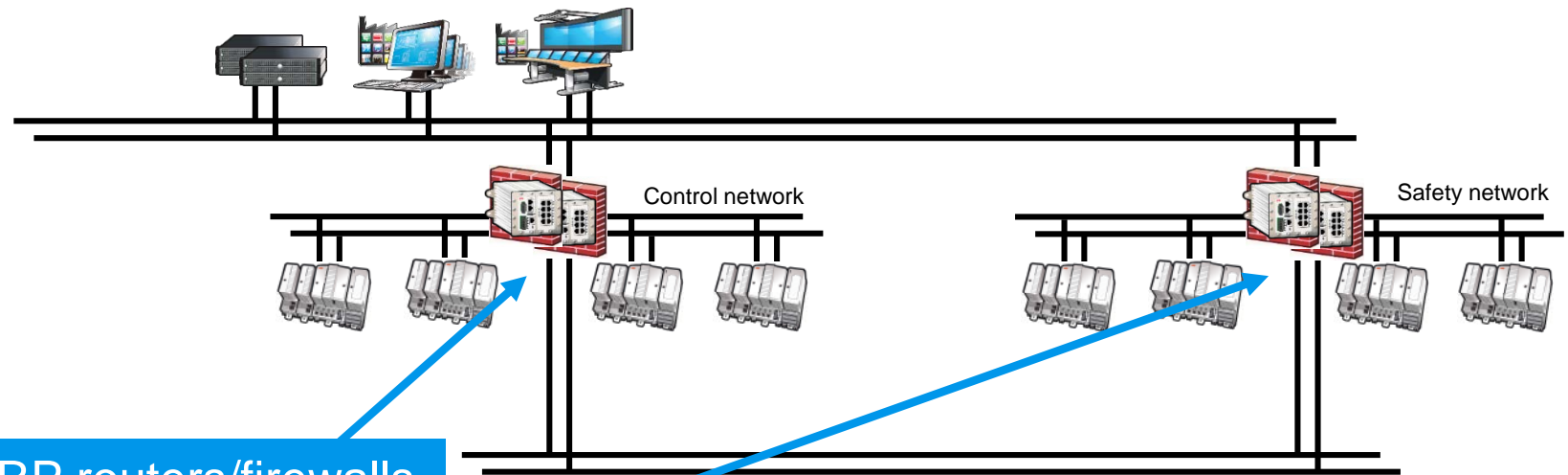
# What about networking security?

## RNRP networks tomorrow - Connect controller networks



# What about networking security?

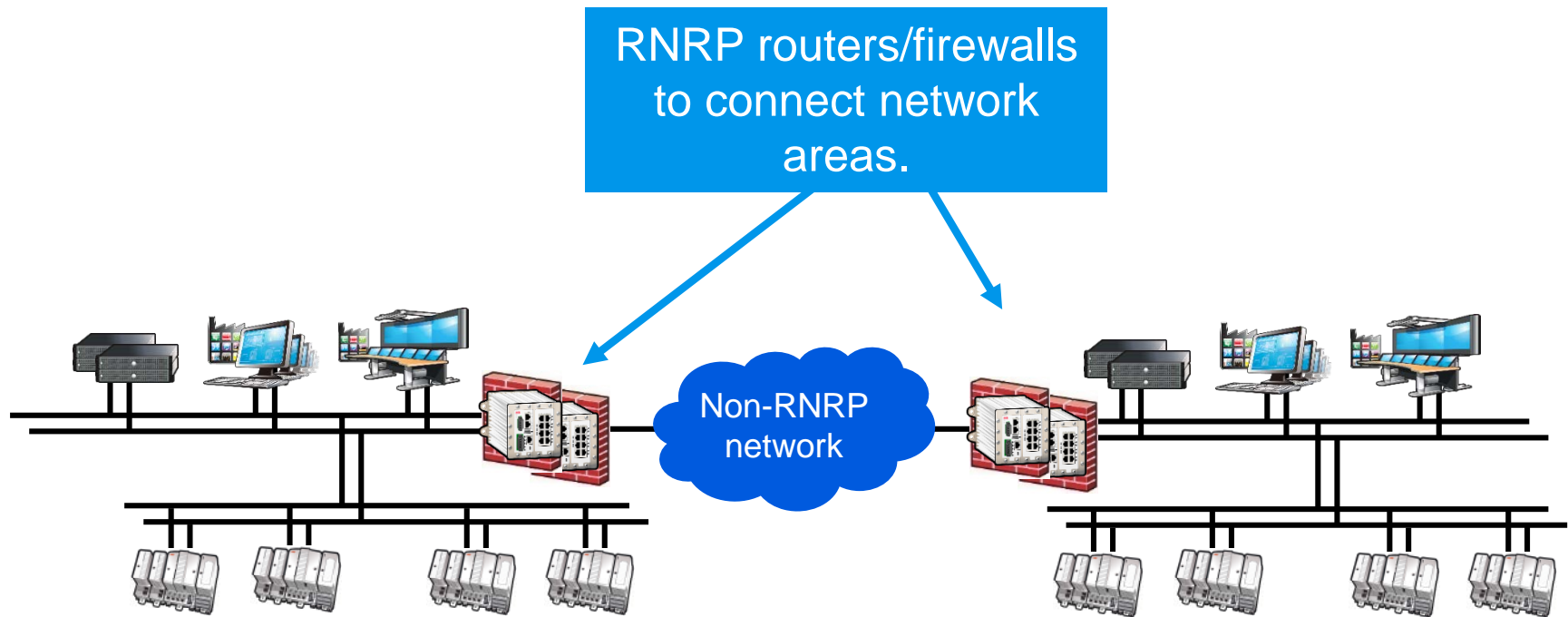
## RNRP networks tomorrow – Connect controller networks



RNRP routers/firewalls to connect controller networks to a controller backbone, if >2 controller networks.

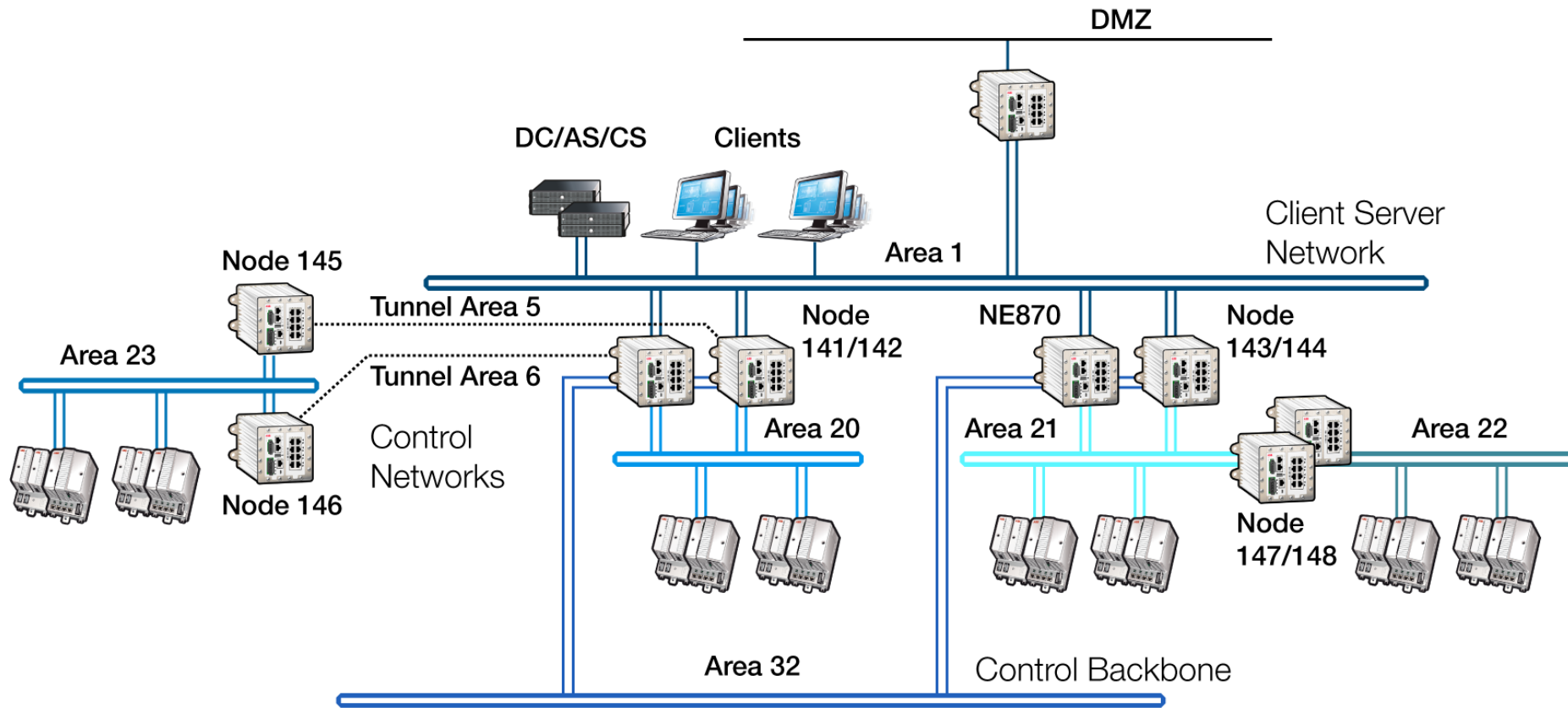
# What about networking security?

## RNRP networks tomorrow – Tunnel area



# What about networking security?

## RNRP router/firewall use cases



Power and productivity  
for a better world™

