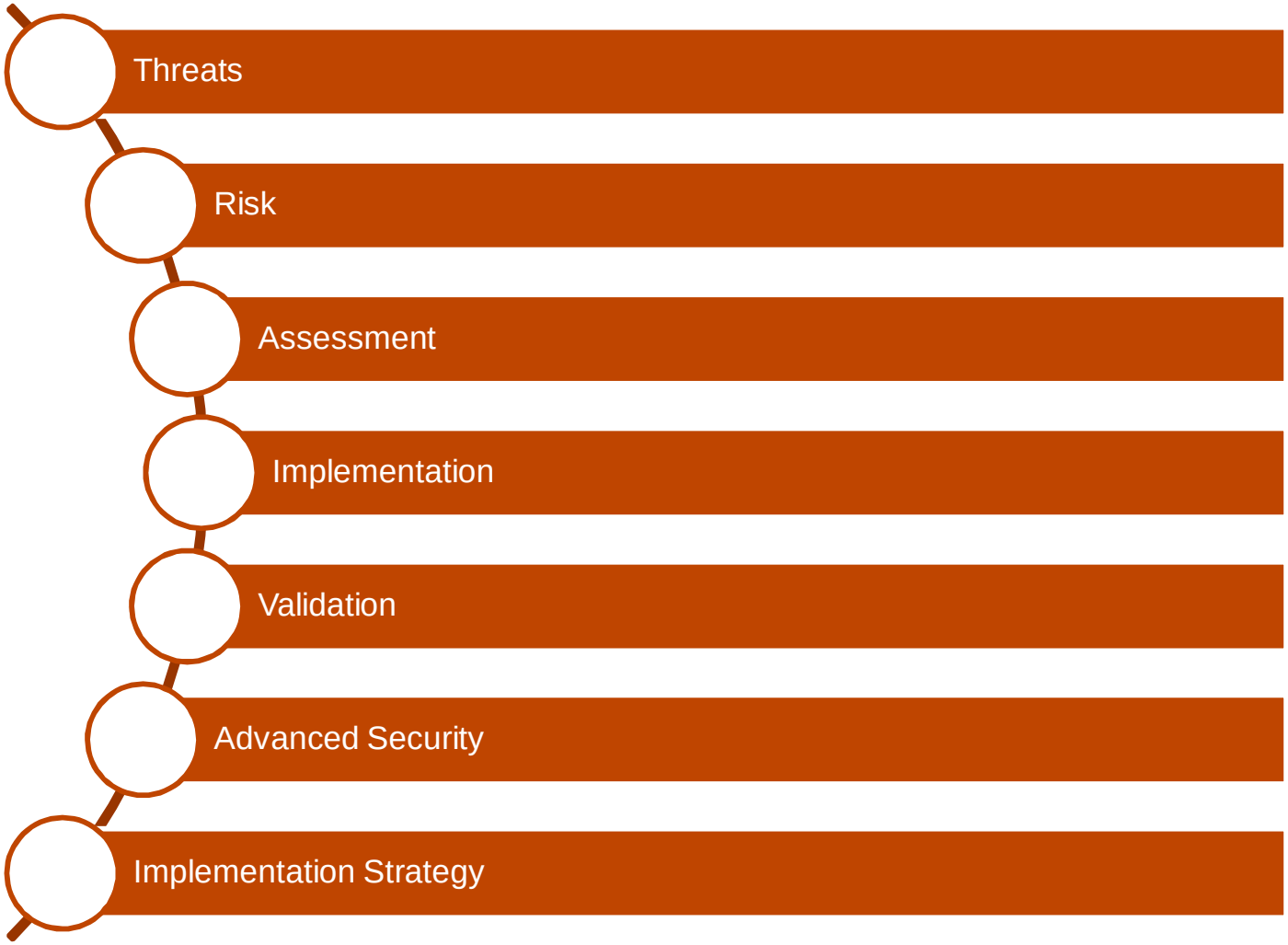
ABB Automation Days, Madrid, May 25th and 26th, Patrik Boo

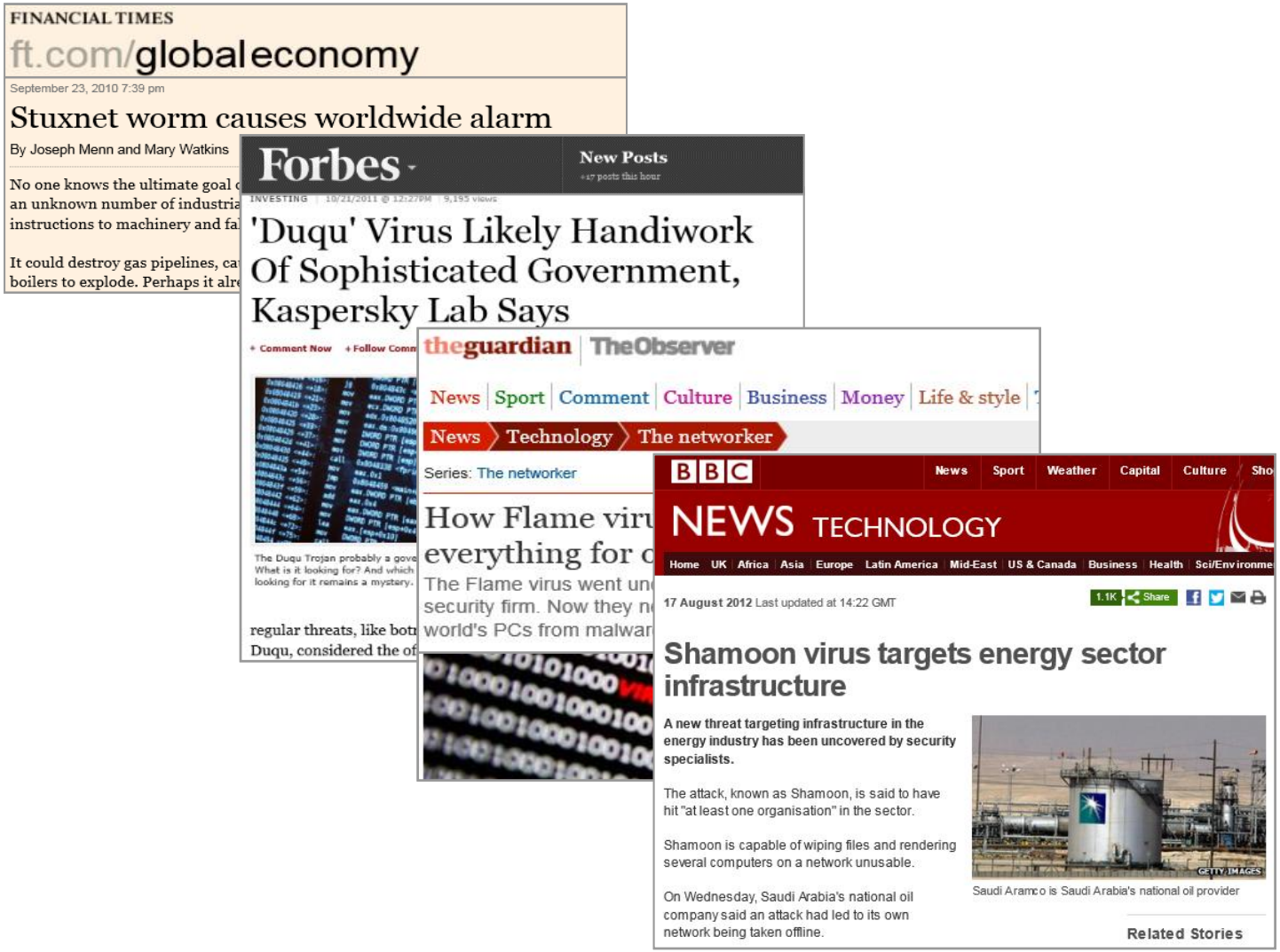
What do you need to know about cyber security?

Power and productivity for a better world™

What do you need to know about cyber security?
Agenda



What do you need to know about cyber security?
Examples of events



What do you need to know about cyber security?
What is Cyber Security?

“Measures taken to protect a computer or computer system against unauthorized access or attack”

Merriam-Webster’s dictionary

Hacking

Malicious software

Unauthorized use

What do you need to know about cyber security?
Why is cyber security an issue?

Isolated devices → Point to point interfaces → Proprietary networks → Standard Ethernet/ IP based networks → Interconnected systems → Distributed systems → Remote access and wireless infrastructure

Threats to standard IT systems largely also apply to ICS

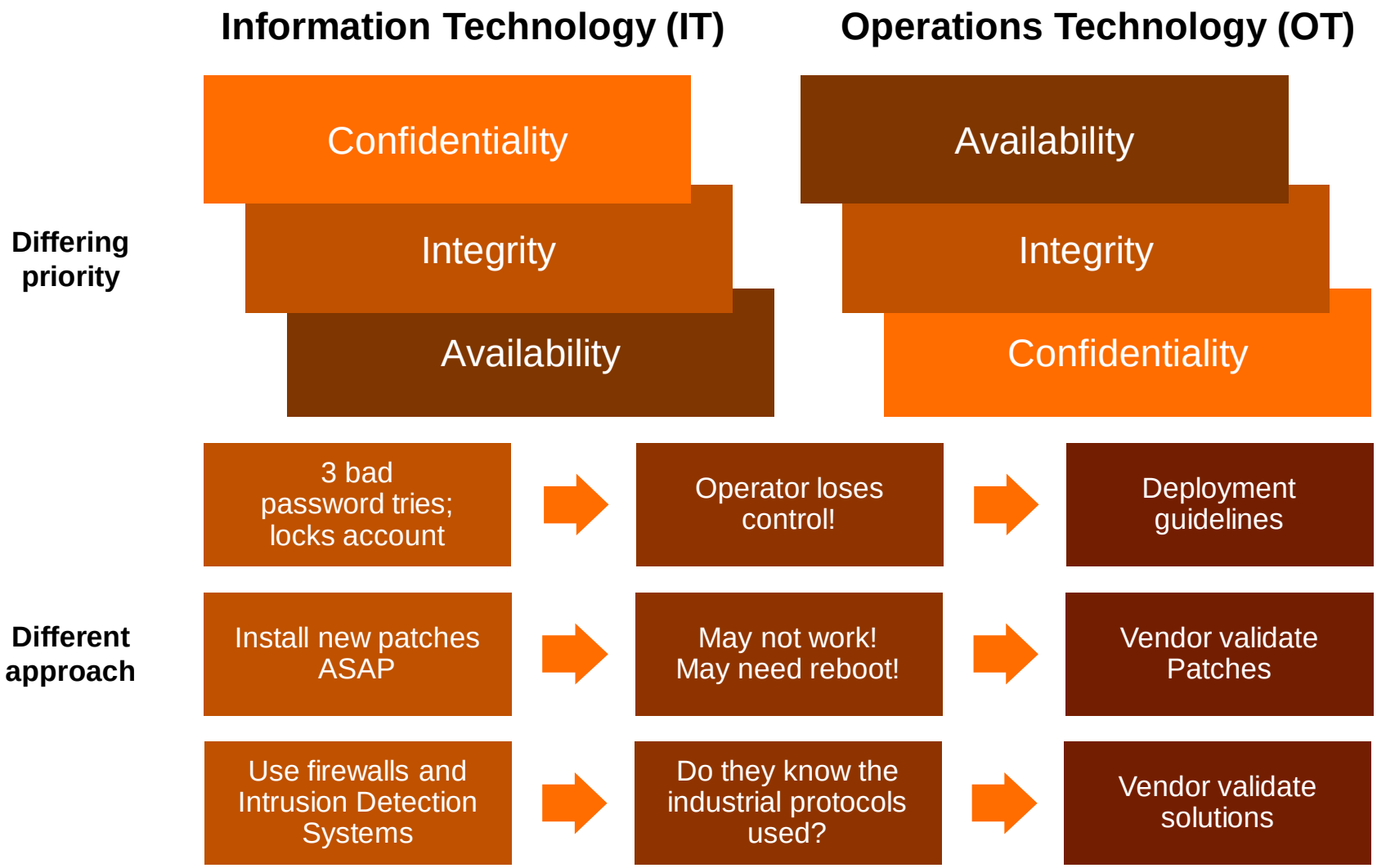
+

IT focused criminal ecosystem

↓

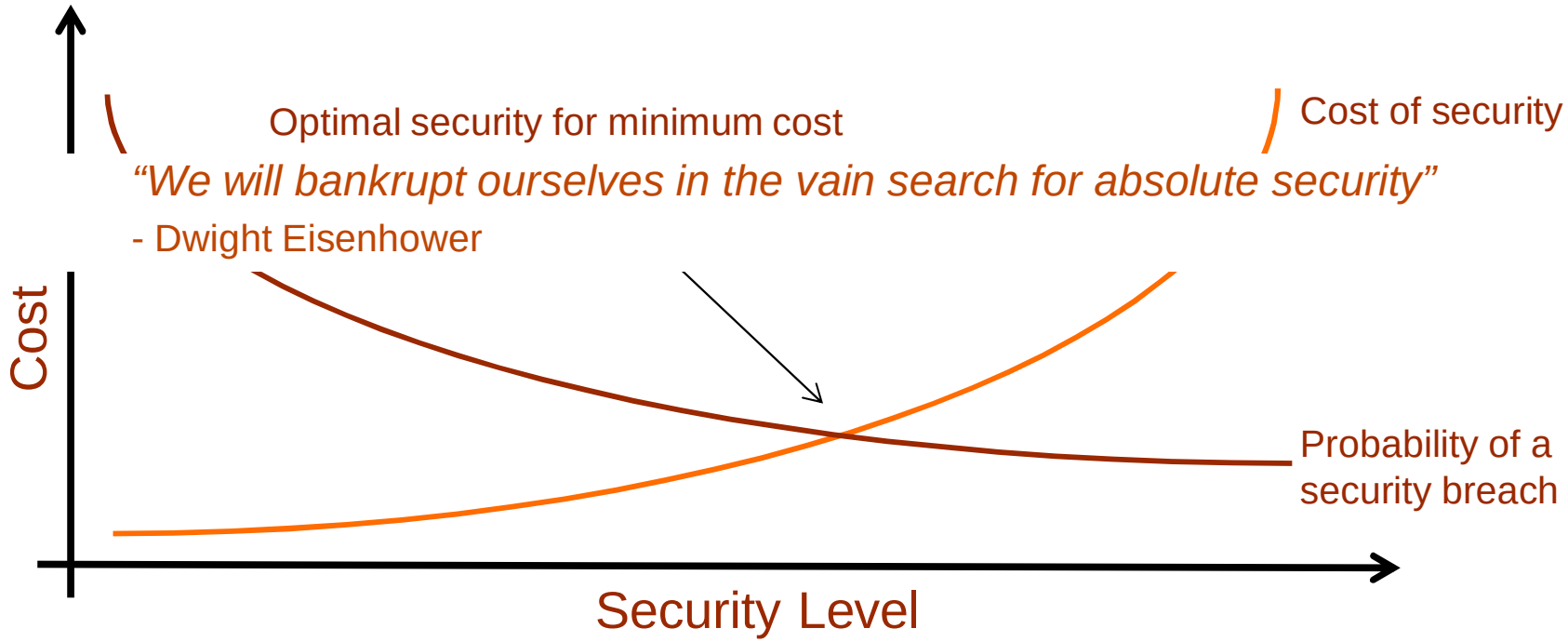
Increased risk!

What do you need to know about cyber security?
IT vs. OT best practices

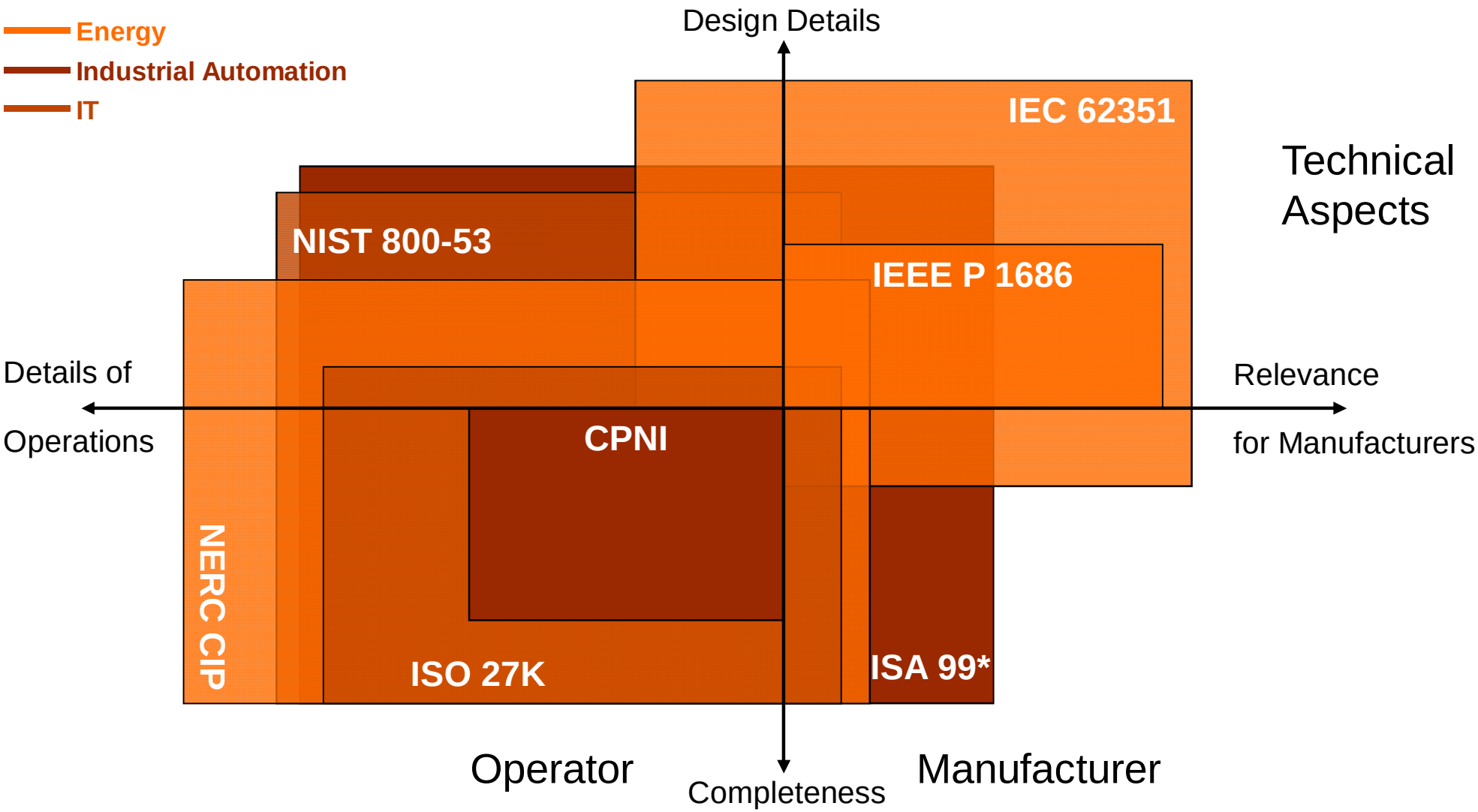


What do you need to know about cyber security? Risk and cost

- The cost of security measures should be balanced against the desired risk reduction
- Risk = f(threat, vulnerability, consequences)

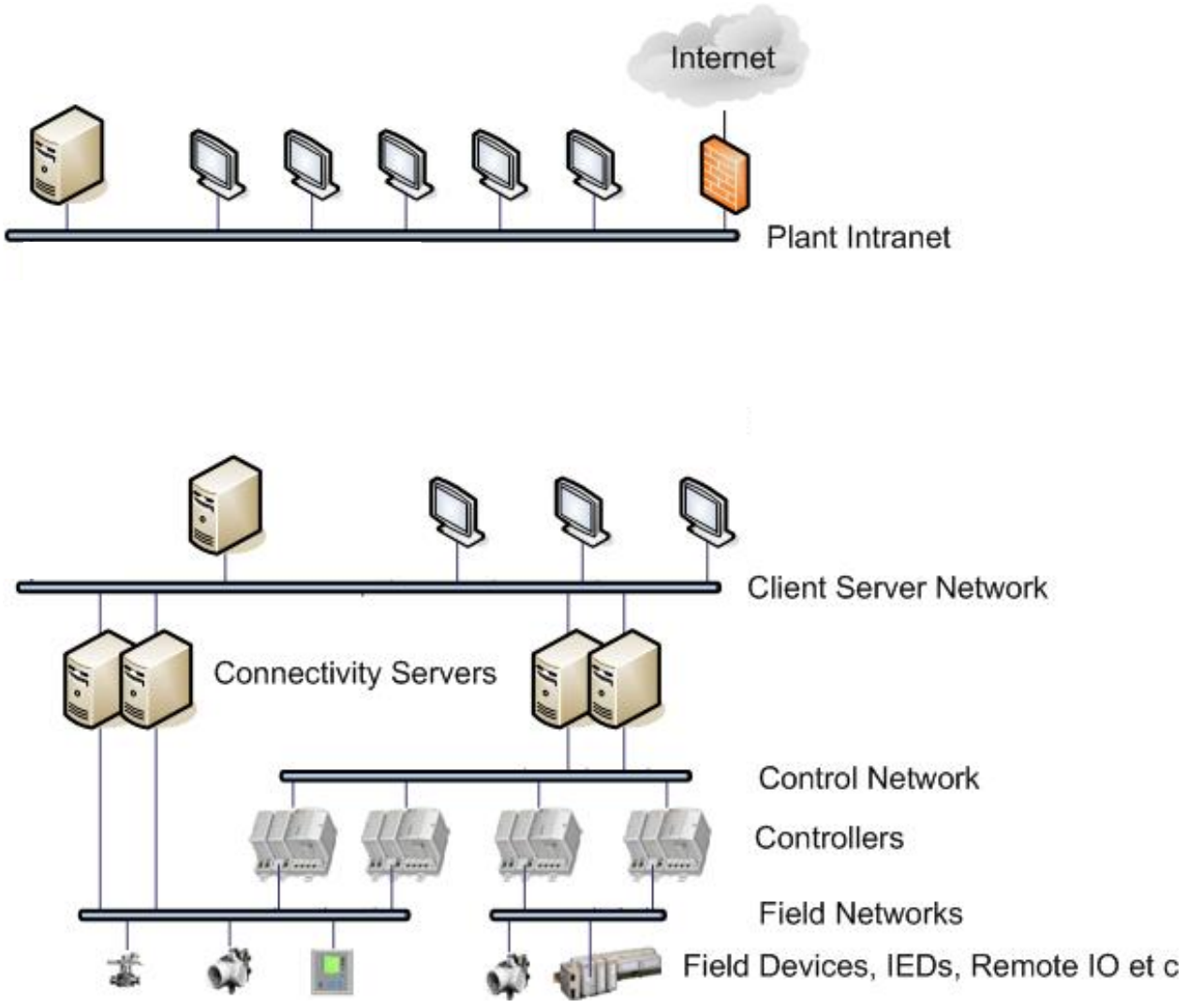


What do you need to know about cyber security?
Cyber Security standards and best practices

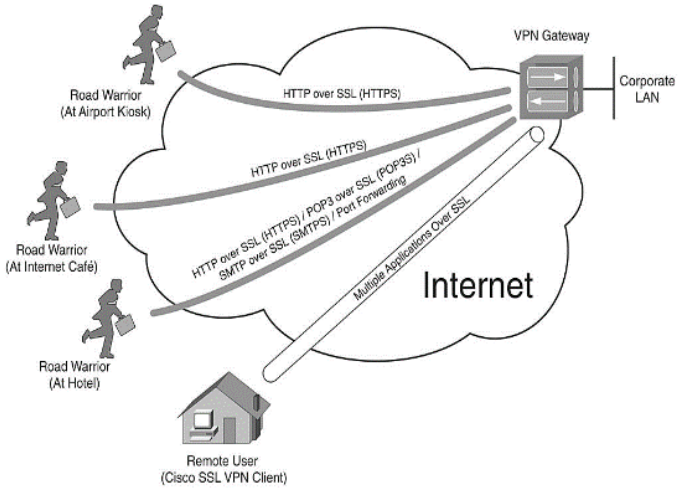


* Since the closing of the ESCoRTS project, ISA decided to relabel the ISA 99 standard to ISA 62443 to make the alignment with the IEC 62443 series more explicit and obvious.

What do you need to know about cyber security?
Connectivity / and the myth of Air gaps

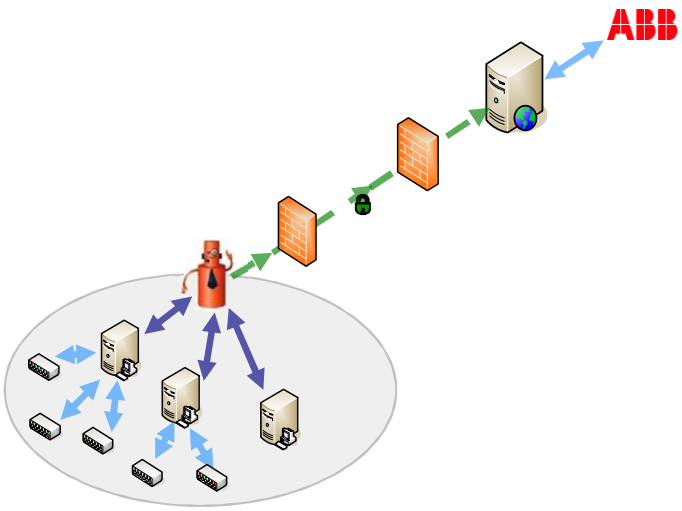


What do you need to know about cyber security?
Remote access



Remote connection via VPN

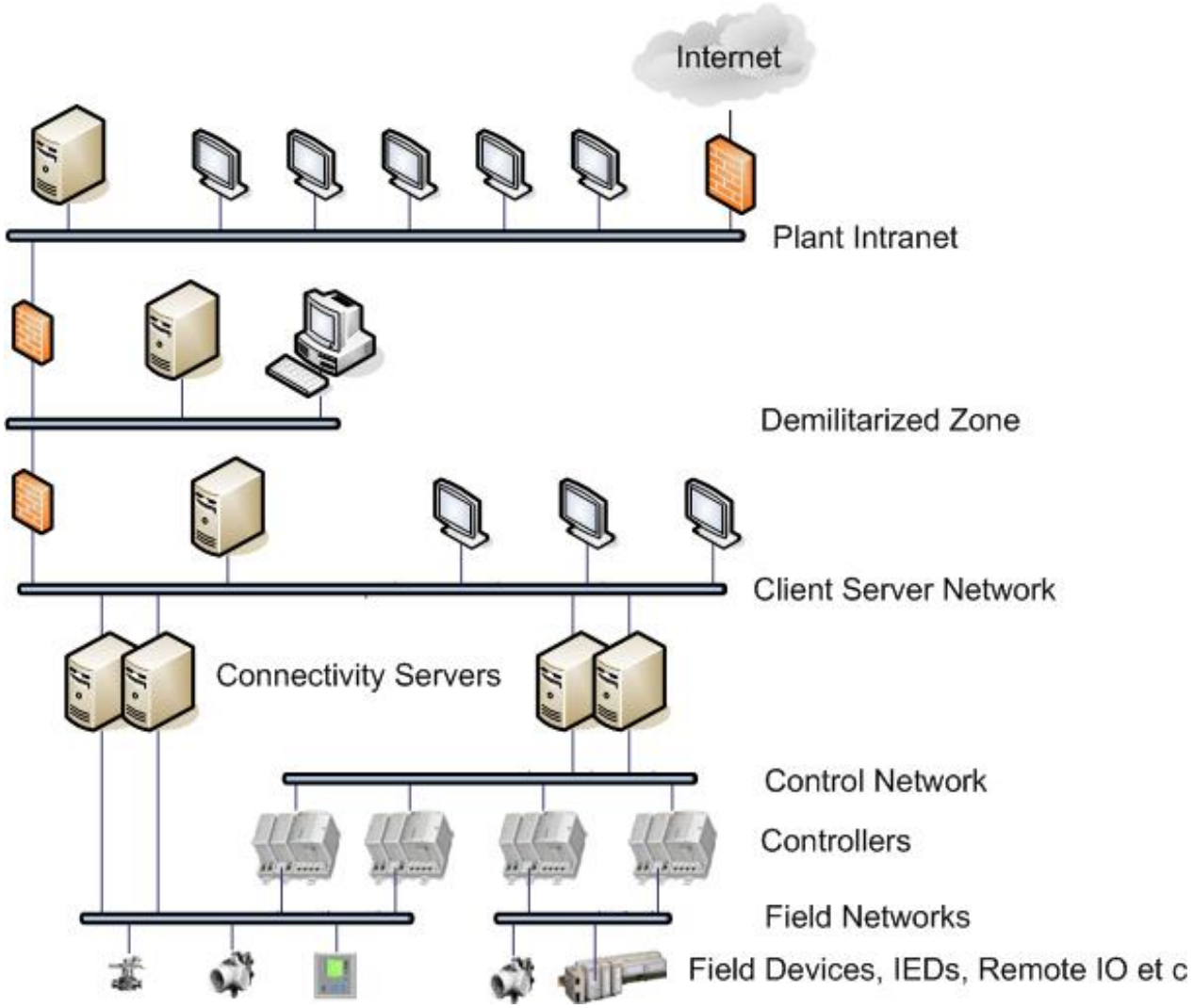
- IT solution, not designed to ICS
- Access control issues
- Hard to make compliant
- NOT RECOMMENDED



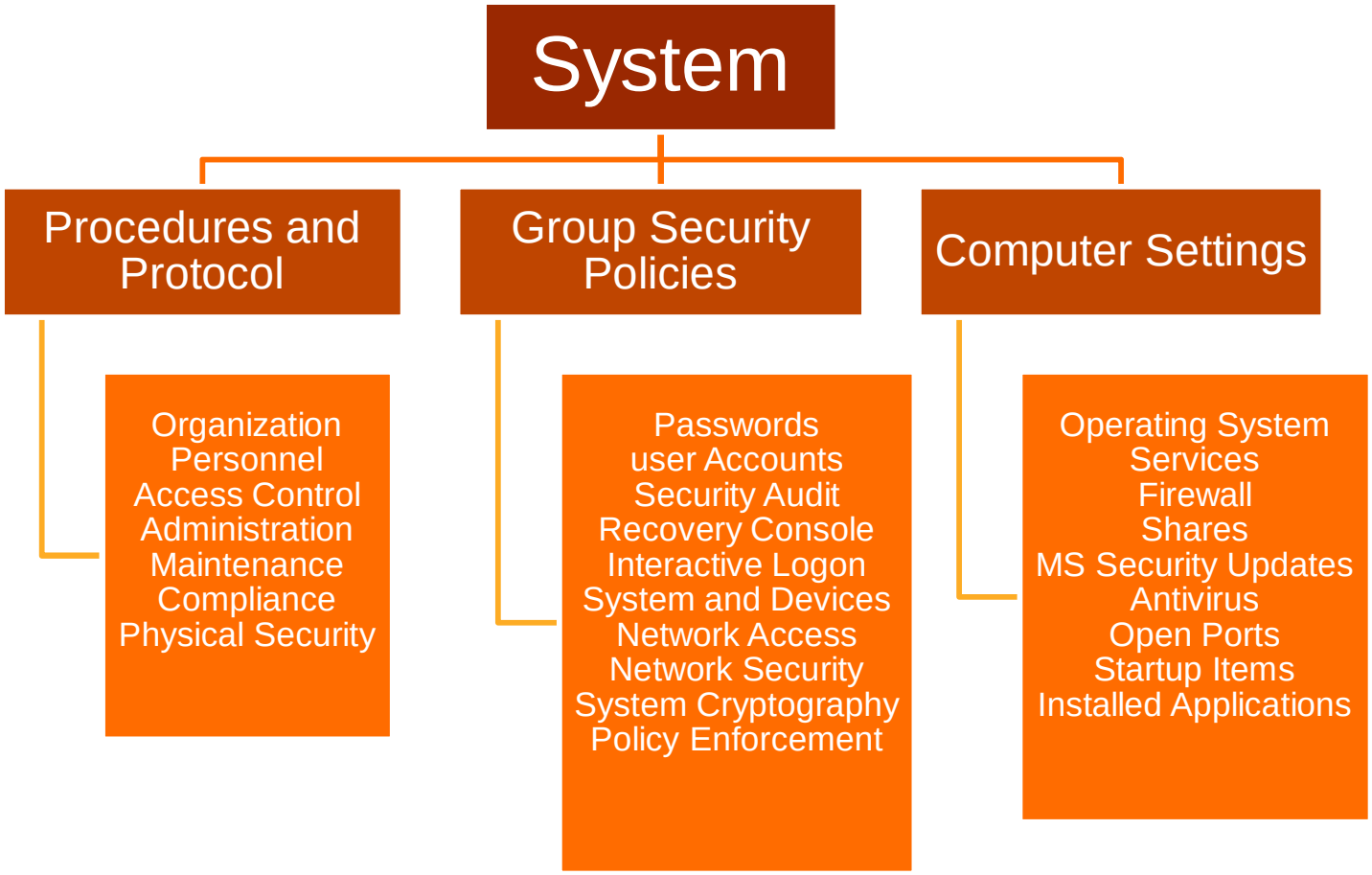
Remote connection via RAP

- Designed for ICS
- Access control schema
- Cyber security compliant
- RECOMMENDED

What do you need to know about cyber security?
Control System Architecture - what to protect



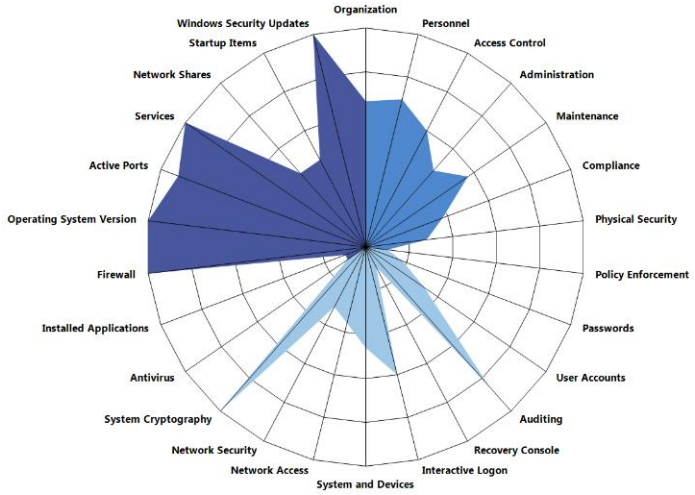
What do you need to know about cyber security?
Things to check



What do you need to know about cyber security?
One way to protect the DCS on the factory floor

- Switches on the cabinet doors
  - Door opens -> alarm goes off
  - Alarm goes off -> control room will investigate

What do you need to know about cyber security?
Cyber Security Fingerprint - where to start



Nothing can make a control system completely secure.

- Provides a comprehensive view of your site's cyber security status
- Identifies strengths and weaknesses for defending against an attack within your plant's control systems
- Reduces potential for system and plant disruptions
- Increases plant and community protection
- Supplies a solid foundation from which to build a sustainable cyber security strategy

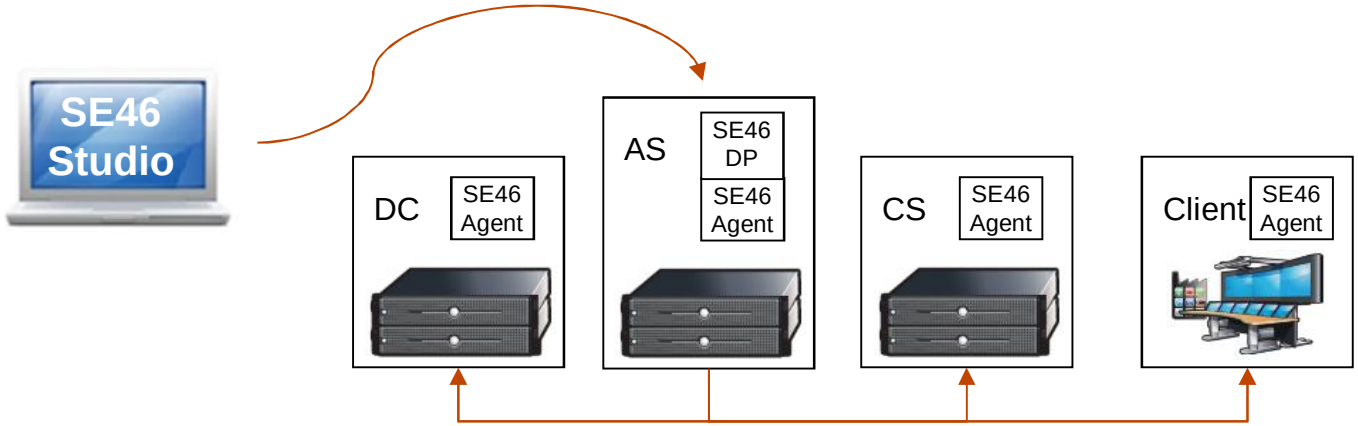
What do you need to know about cyber security? Time flies

2001

April 8th 2014

What do you need to know about cyber security? 800xA Whitelisting SE46

- Whitelisting SE46: Only SW with valid Application Ce800xA certificate (AppCert) allowed to run.
  - The alternative approach is blacklisting, e.g. antivirus.
- SE46 runs on existing 800xA nodes: No extra HW needed
- Integration with Industrial Defender:
  SE46 log events collected for centralized analysis.



What do you need to know about cyber security?
Modern vs Legacy Systems

	Modern System	Legacy System
+	• Supports modern cyber security measures • Familiar interface • COTS	• Sometimes proprietary hardware, software and communication
-	• Affected by modern threats • Networked systems • COTS	• Unsupported = no patches • Modern defenses not supported

=	• Apply best practices
	  • DMZ
	  • Antivirus
	  • Security Patching
	  • etc.
		• Upgrade
		• Strengthen other measures
		  • Physical security
		  • Procedures & Protocol
		  • etc.

Cyber Security
Implementation Strategy - Challenges

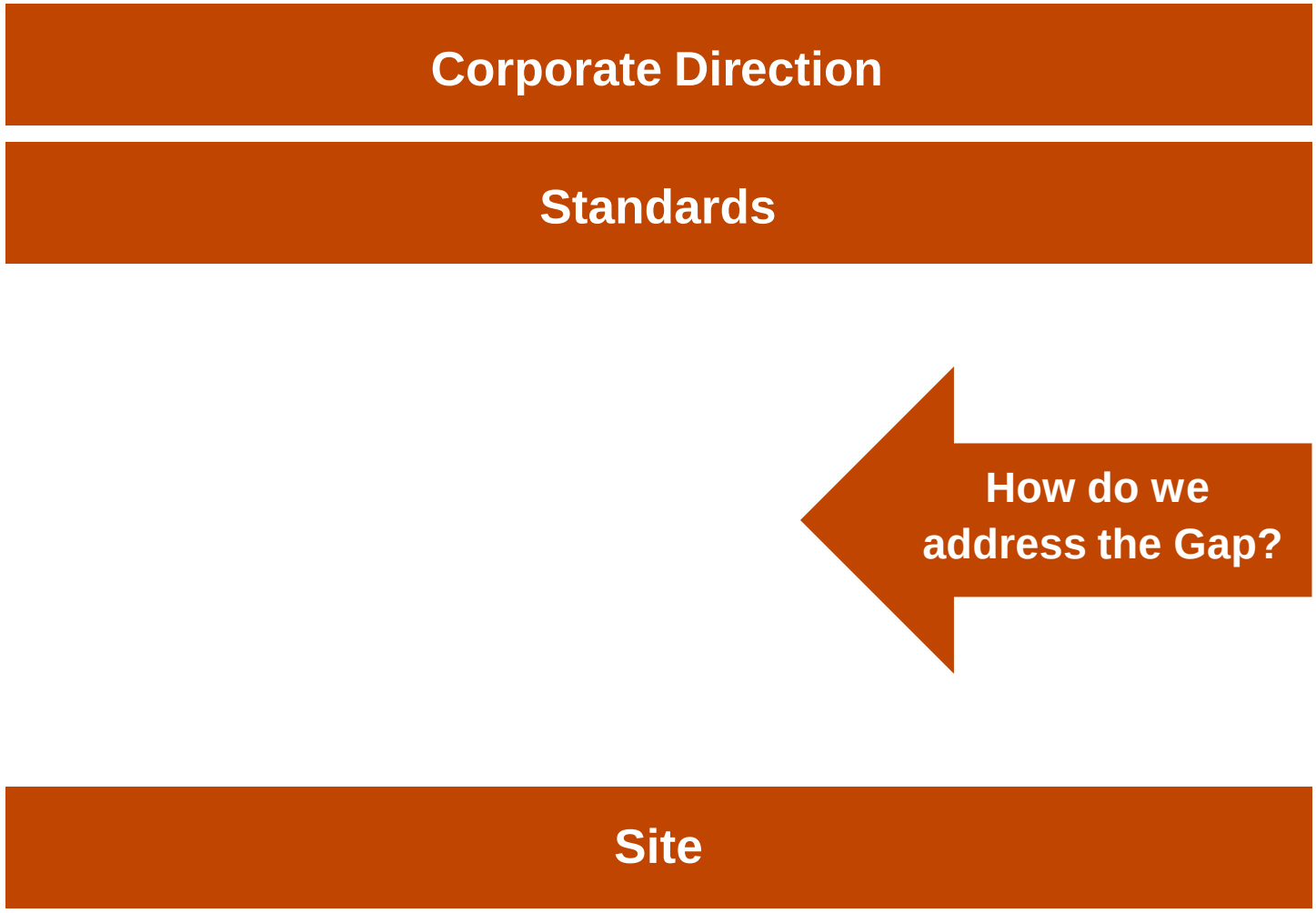
- Identify and balance the following:
  - Management needs
  - Security needs
  - Safety needs
  - Regulatory needs
  - Site ability to deliver

Cyber Security
Corporate vs Site

- Corporate
  - Corporate would like to use same approach as already deployed on desktop environment via IT
    - Why re-invent the wheel or buy $$$ new products?
  - Strategy for corporation – align approach with IT security, but maintain separation.
    - Insure IT solutions will work with A&PC needs.
    - SIEM / IDS / Anti-virus / patching / incident reporting
  - Multiple vendors – different issues / different solutions
    - Siemens / Honeywell
    - ABB / Emerson / Yokogawa / Invensys
- Site
  - Site process control practitioners do not want association with IT
  - Ownership of equipment (turf wars)
    - *"If it breaks, I need to fix it. IT support is 8x5, I need 24x7"*
  - Trust issues
    - Initial programs (on learning curve) left bad memories
  - IT security v. process control freedoms
    - *"I want to do 'IT' my way"*
  - Time constraints
    - *"I have my 40 hour job to do plus 2 other corporate initiatives"*

Cyber Security
Closing the Gap

Top Down Design / Bottom Up Implementation



Cyber Security
Choosing Leaders

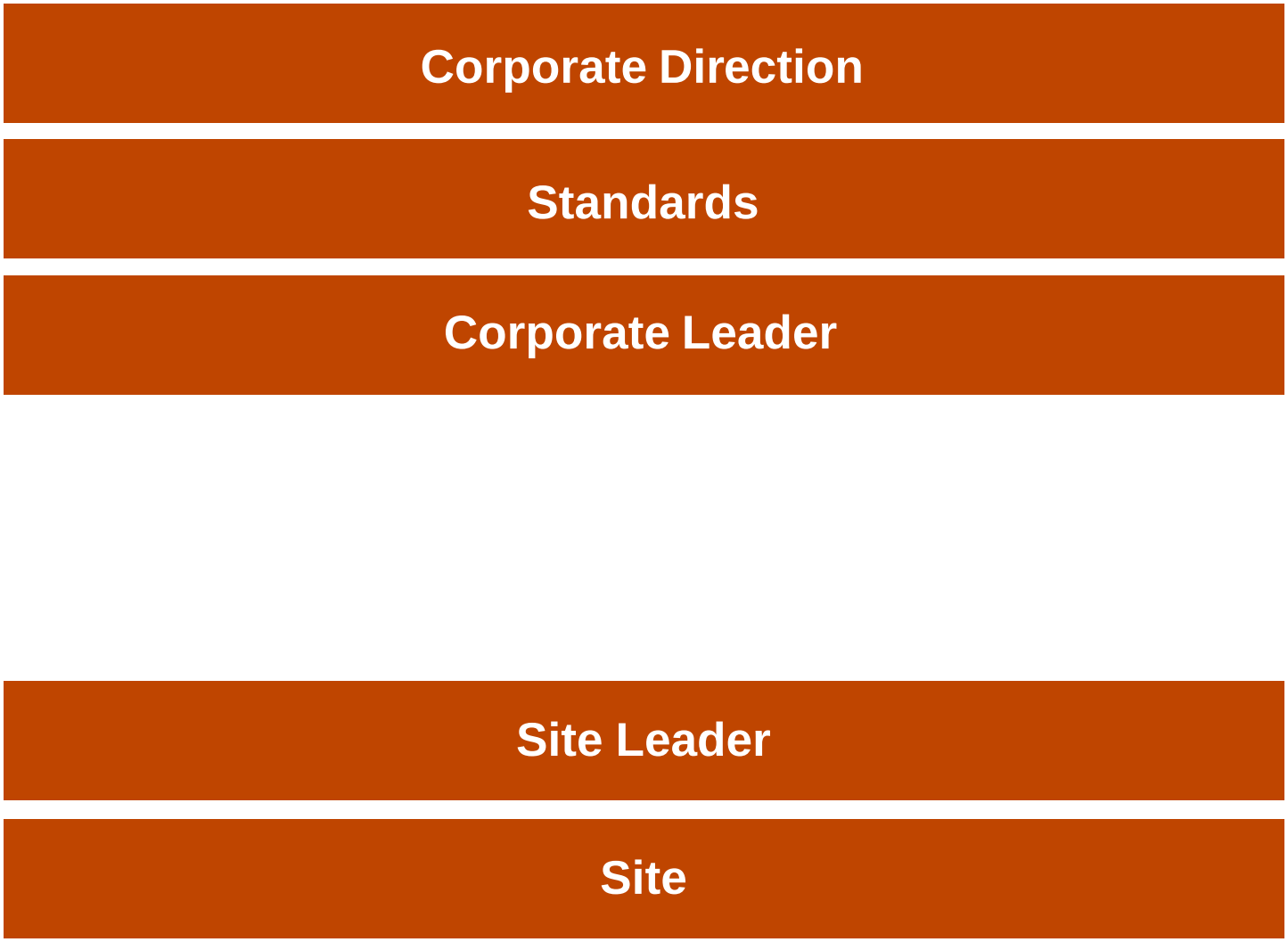
Choose a Corporate leader

- Access to corporate leadership
- Expresses ideas clearly
- Knows process control network
- Knows process control working parameters
- Knows Cyber Security – or can learn

Choose a Site leader

- Ability to manage multiple tasks
- Access to site leadership
- Knows Process Control Systems

Cyber Security
Closing the Gap – Choosing Leadership

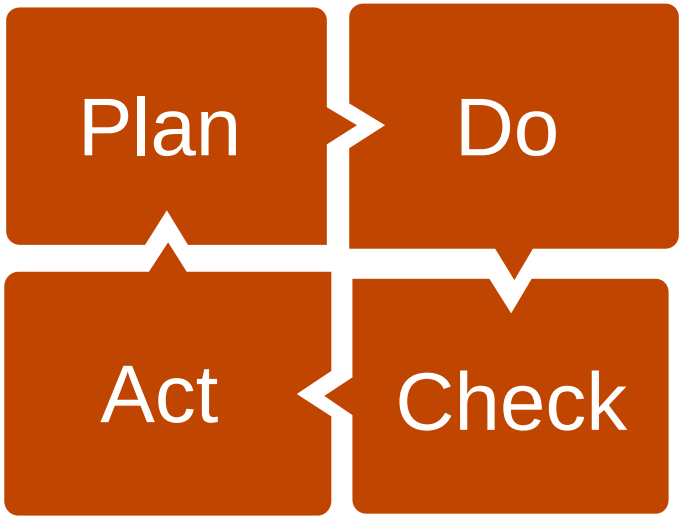


Cyber Security
Site Activity – Project

- No corporate project authorized
  - Utilized site resources via influence

- SWAT team approach at first site
  - Visited site
  - Outlined Gaps
  - Developed plan with site and IT
  - Used MS Project to track
  - Provided services as needed
  - Worked next 4 months w/ site to close gaps

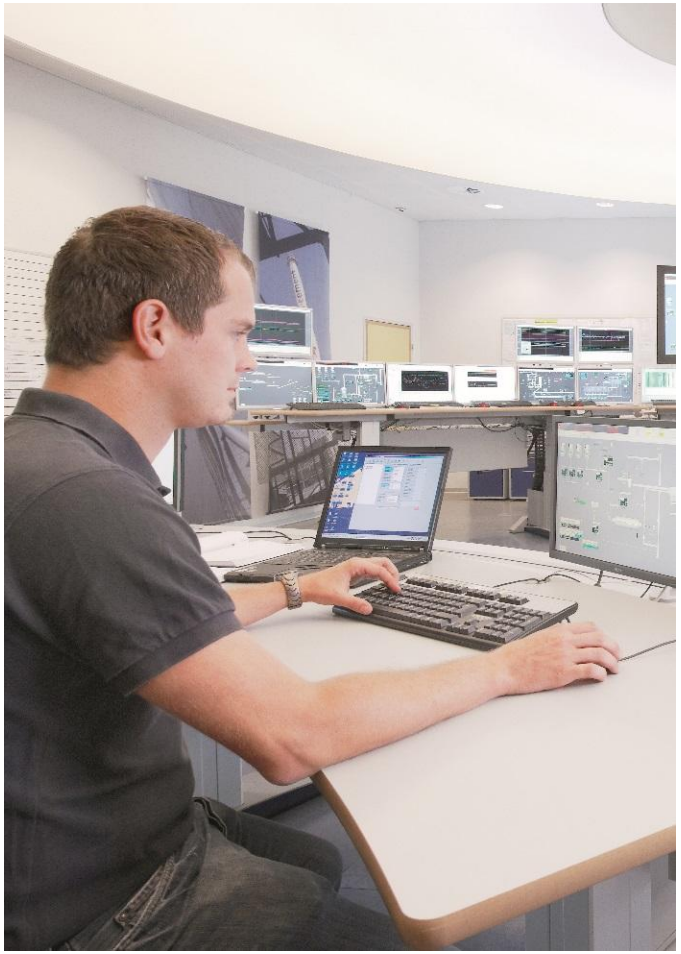
Cyber Security
Site Activity – Sustain



- Not one and done
  - Need to sustain this activity
  - Follow standards
  - Stay current and connected to corporate cyber security

Cyber Security
Closing the Gap – Site Activity

Cyber Security
Completing the picture



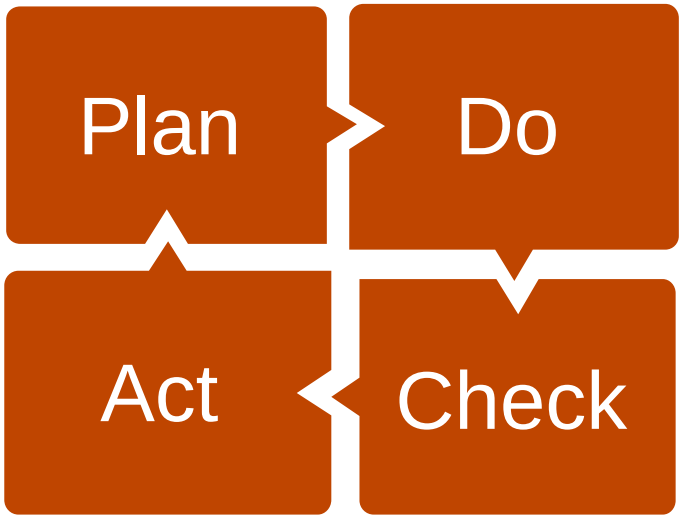
- Leveraging solutions to others – shared common solutions
  - Tap corporate SMEs (Subject Matter Experts)
  - Corporate Windows patching service
  - IDS – Network and Host
  - Anti-virus delivery
  - SIEM (Security Incidents and Events Monitor)
  - Whitelisting
  - Corporate delivered GPO policy updates (currently manual process)

Cyber Security
Completing the picture

- Communicate communicate, communicate
  - quarterly meeting,
  - monthly steering team with immediate management,
  - periodic meetings with Regional Leadership Team,
  - periodic meetings with plant managers

- Be available
  - work with vendors
  - assist site in performing work
  - continuous dialog
  - follow-up with sites

Cyber Security
Sustain – Corporate Activity



- Refresh Standards
- Align with global regulations
- Monitor industry trends
- Monitor Cyber Activity
- Monitor US-CERT* Incident response
- Stay current and connected to sites

Cyber Security
Closing the Gap – Leveraged Solutions

What do you need to know about cyber security? Final thoughts

"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts."

Eugene H. Spafford

Contact information

If you have further questions , please contact us at:

PRESENTER	Patrik Boo
COMPANY	ABB
CONTACT PHONE	(804) 931-4596
CONTACT E-MAIL	patrik.boo@us.abb.com

Power and productivity
for a better world™