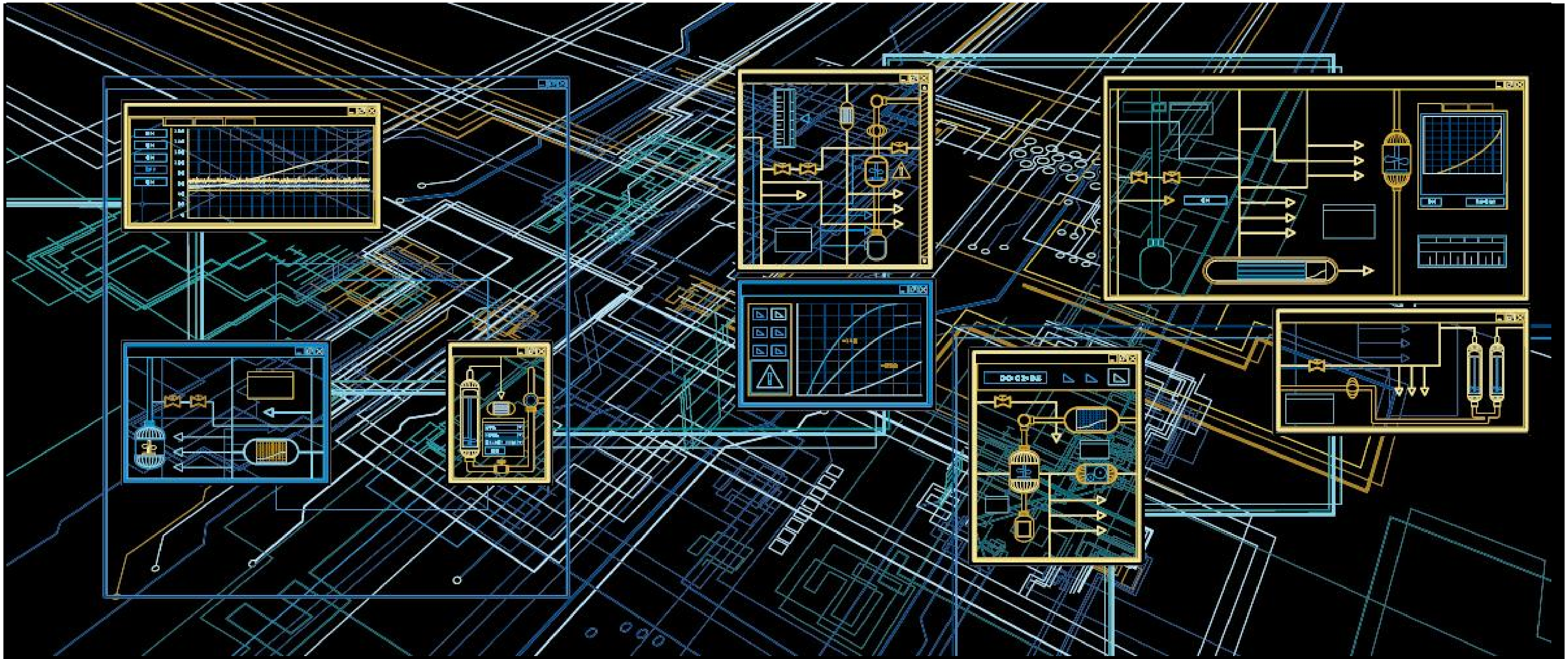


ABB Process Automation Lifecycle Services, Patrik Boo

# Cyber Security

# Secure systems, protect production

© ABB Group

# Cyber Security
## What is cyber security?

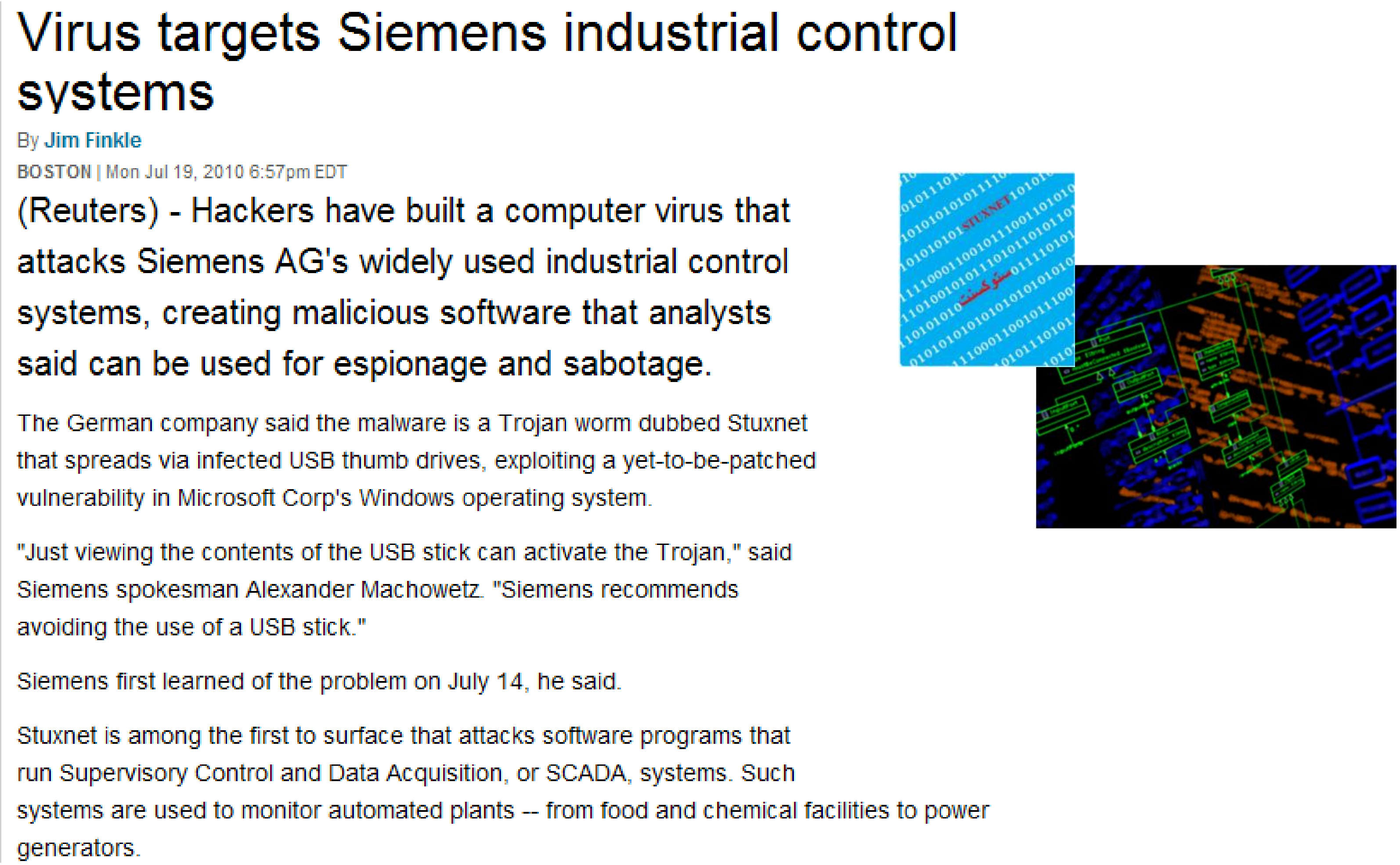
*“Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack”*

Merriam-Webster’s dictionary

**Hacking** **Malicious software** **Unauthorized use**

© ABB Group

# Cyber Security in industrial control systems
## Stuxnet: the game changer



### Virus targets Siemens industrial control systems

By Jim Finkle

BOSTON | Mon Jul 19, 2010 6:57pm EDT

(Reuters) - Hackers have built a computer virus that attacks Siemens AG's widely used industrial control systems, creating malicious software that analysts said can be used for espionage and sabotage.

The German company said the malware is a Trojan worm dubbed Stuxnet that spreads via infected USB thumb drives, exploiting a yet-to-be-patched vulnerability in Microsoft Corp's Windows operating system.

"Just viewing the contents of the USB stick can activate the Trojan," said Siemens spokesman Alexander Machowetz. "Siemens recommends avoiding the use of a USB stick."

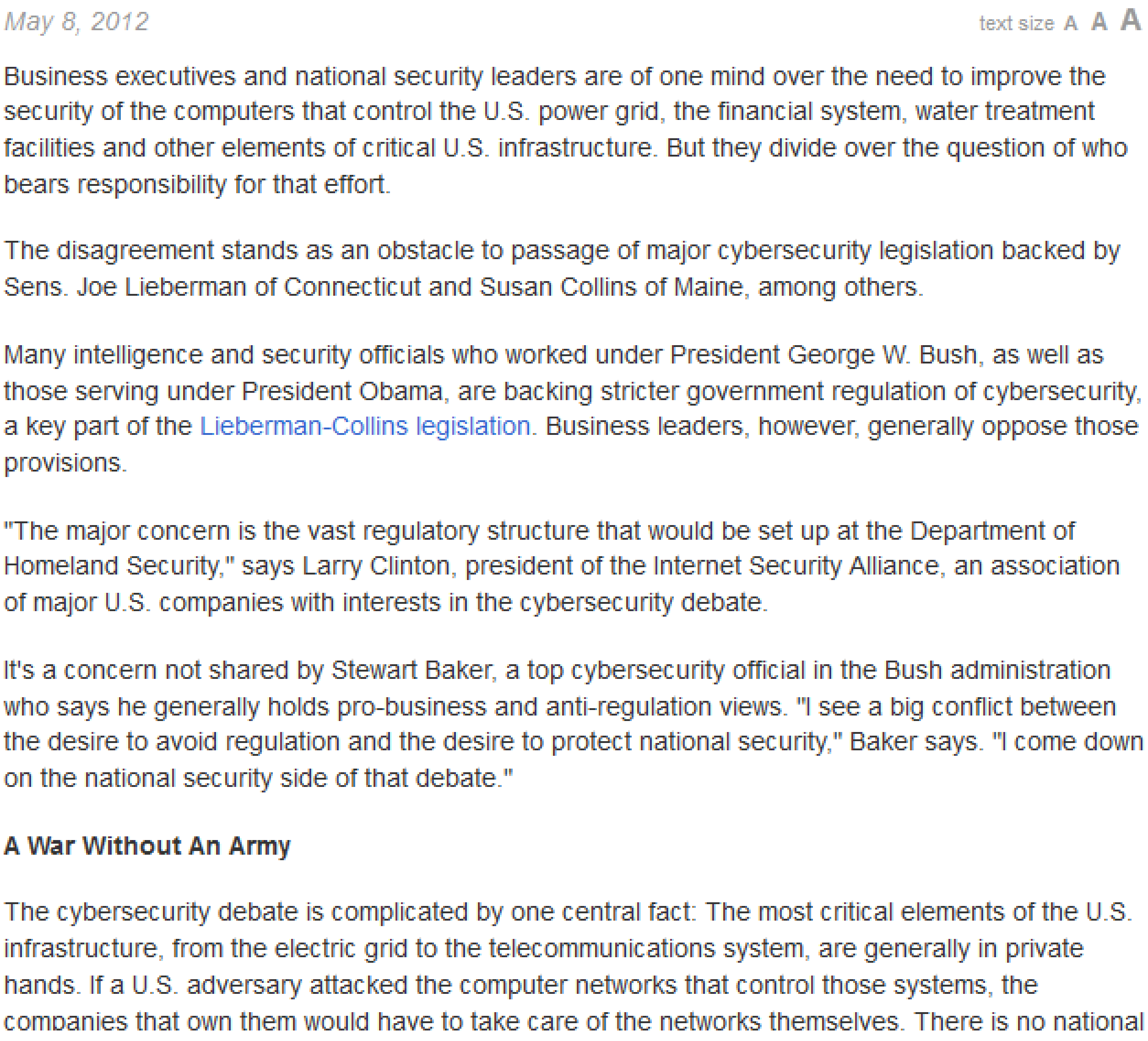
Siemens first learned of the problem on July 14, he said.

Stuxnet is among the first to surface that attacks software programs that run Supervisory Control and Data Acquisition, or SCADA, systems. Such systems are used to monitor automated plants -- from food and chemical facilities to power generators.

**Stuxnet was the first malware targeting industrial control systems**

# Bill Would Have Businesses Foot Cost Of Cyberwar

## Congress would task businesses with increasing cyber security



May 8, 2012

Business executives and national security leaders are of one mind over the need to improve the security of the computers that control the U.S. power grid, the financial system, water treatment facilities and other elements of critical U.S. infrastructure. But they divide over the question of who bears responsibility for that effort.

The disagreement stands as an obstacle to passage of major cybersecurity legislation backed by Sens. Joe Lieberman of Connecticut and Susan Collins of Maine, among others.

Many intelligence and security officials who worked under President George W. Bush, as well as those serving under President Obama, are backing stricter government regulation of cybersecurity, a key part of the Lieberman-Collins legislation. Business leaders, however, generally oppose those provisions.

"The major concern is the vast regulatory structure that would be set up at the Department of Homeland Security," says Larry Clinton, president of the Internet Security Alliance, an association of major U.S. companies with interests in the cybersecurity debate.

It's a concern not shared by Stewart Baker, a top cybersecurity official in the Bush administration who says he generally holds pro-business and anti-regulation views. "I see a big conflict between the desire to avoid regulation and the desire to protect national security," Baker says. "I come down on the national security side of that debate."

**A War Without An Army**

The cybersecurity debate is complicated by one central fact: The most critical elements of the U.S. infrastructure, from the electric grid to the telecommunications system, are generally in private hands. If a U.S. adversary attacked the computer networks that control those systems, the companies that own them would have to take care of the networks themselves. There is no national

# Cyber Security
# Enterprise IT vs. Industrial Control Systems

Enterprise IT Industrial Control Systems

| | Enterprise IT | Industrial Control Systems |
|---|---|---|
| **Primary risk impact** | Information disclosure, financial | Safety, health, environment, financial |
| **Availability** | 95 – 99%<br>(accept. downtime/year: 18.25 - 3.65 days) | 99.9 – 99.999%<br>(accept. downtime/year: 8.76 hrs – 5.25 minutes) |
| **Typical System Lifetime** | 3-5 years | 15-30 years |
| **Problem response** | Reboot, patching/upgrade | Fault tolerance, online repair |

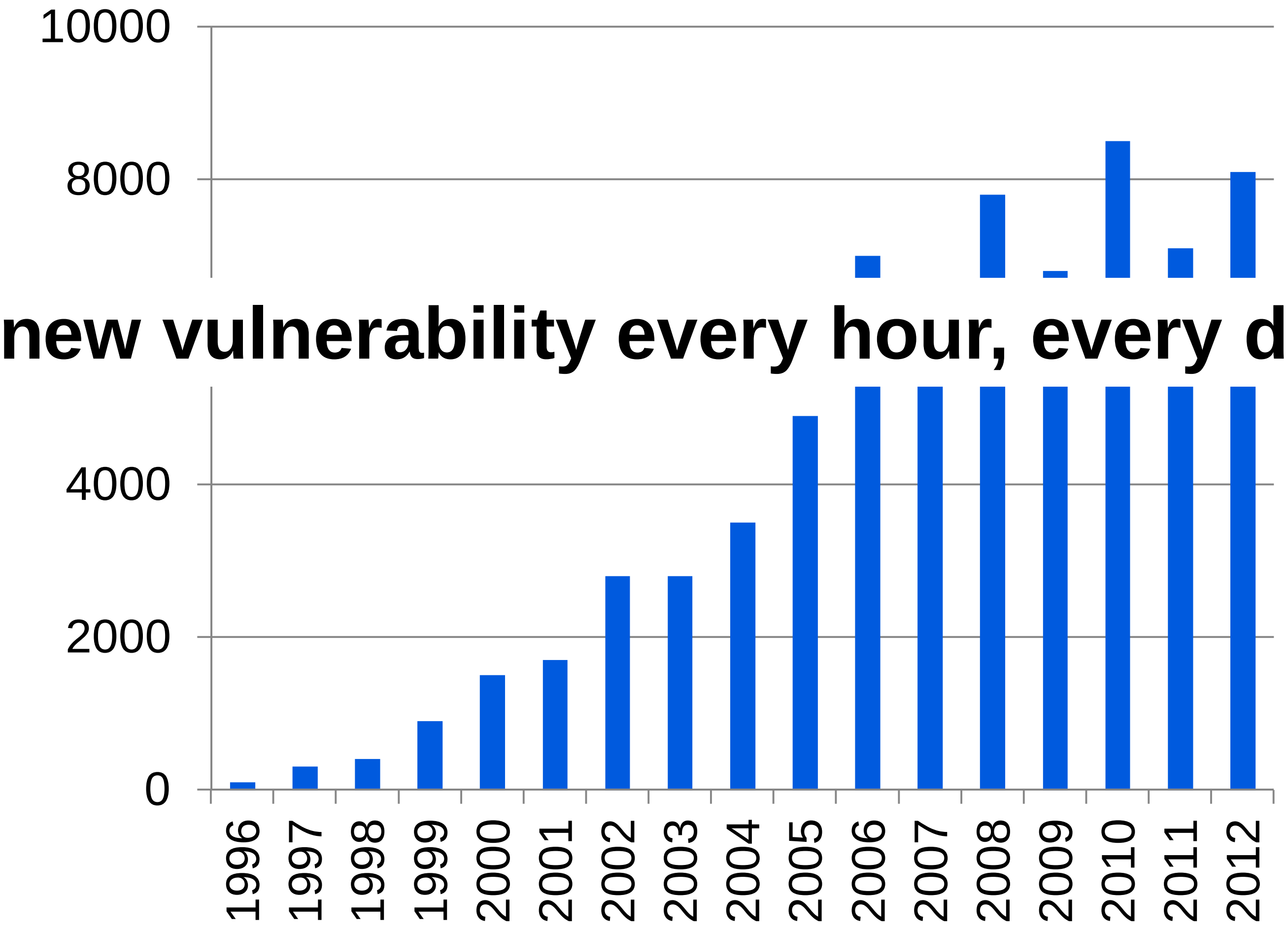
© ABB Group

# Cyber Security
## Why traditional approaches don’t work

| Action | Consequence |
|---|---|
| **Lock out accounts after three bad password tries** | Operator has no control over process for 10 minutes |
| **Install patches as soon as they are released and reboot** | A control system reboot means shutting down the whole plant, and it might take days to get everything running again |
| **Frequently update antivirus scan engine and virus definitions** | False positives might have fatal consequences |
| **Use of crypto functions to protect data in transit** | Real time constraints cannot be met due to limited resources on embedded devices |
| **Use of firewalls and intrusion detection systems** | Do you speak IEC 60870-5-104, IEC 61850, OPC, HART, ProfiNet, Modbus... |
| **Use of intrusion prevention systems** | One false positive might have fatal consequences |

**Information Systems Security is a good starting point, but approaches and technologies need to be applied with care**

# Cyber Security
## Vulnerability disclosure growth by year

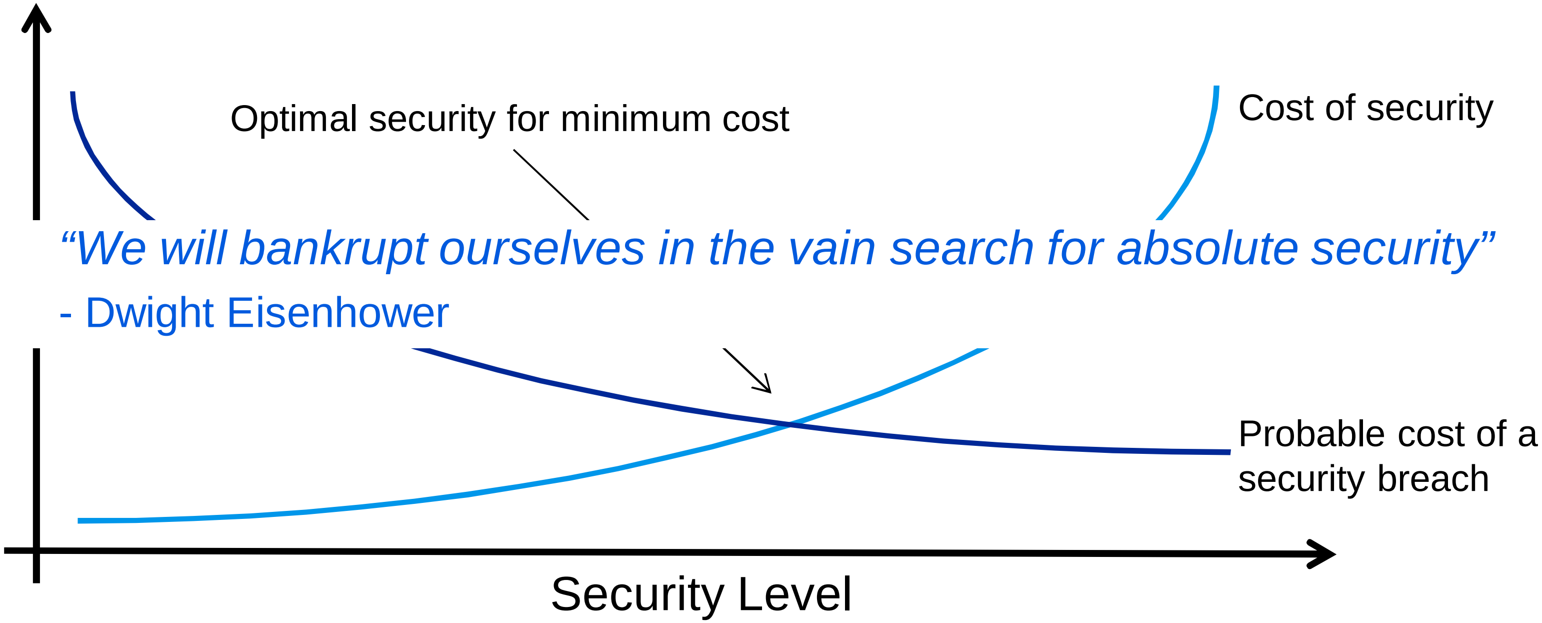


**1 new vulnerability every hour, every day.**

Source: IBM X-Force®

# Cyber Security
## Security cost

- The cost of security measures should be balanced against the achieved risk reduction
- Risk = (probability of successful attack) x (potential consequences)

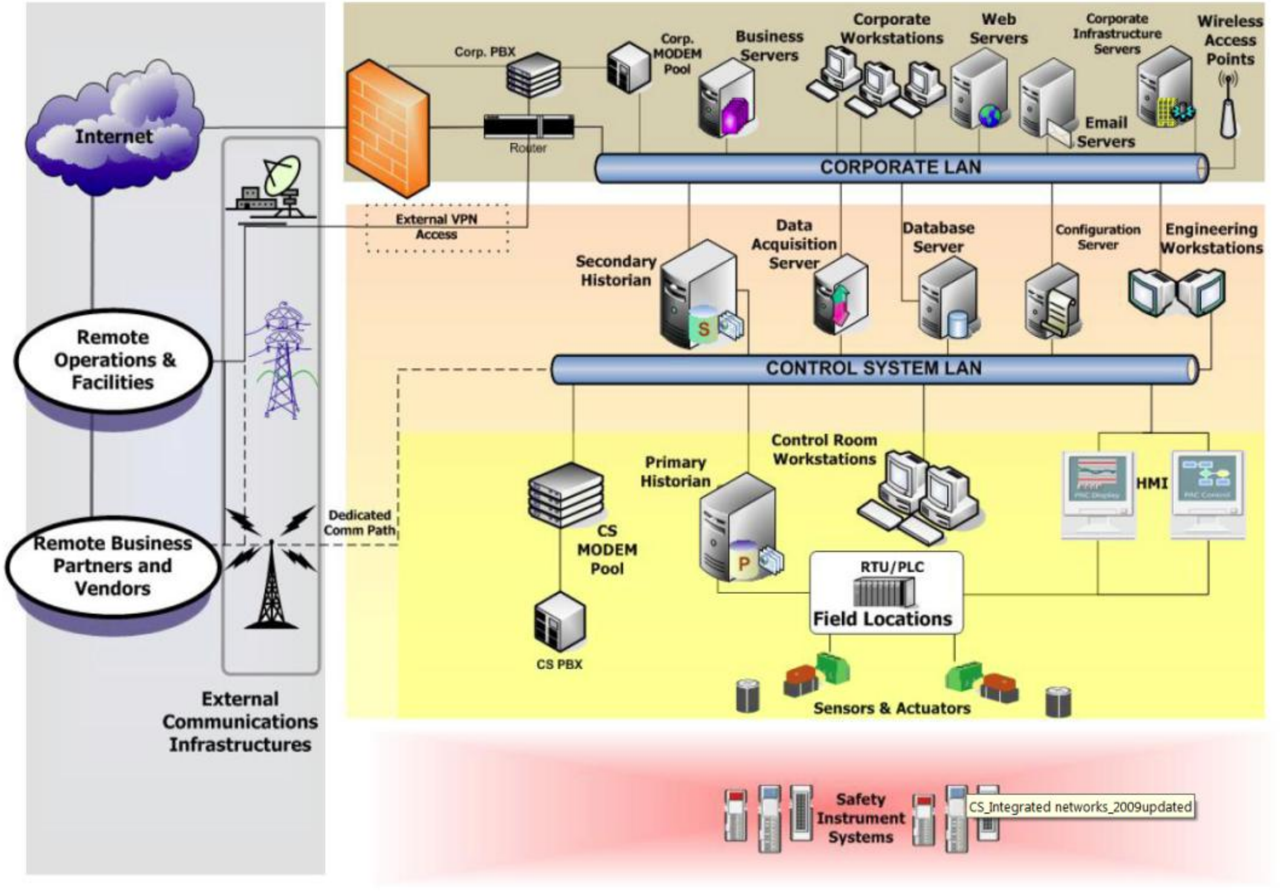


*“We will bankrupt ourselves in the vain search for absolute security”*

- Dwight Eisenhower

# Cyber Security
## The airgap myth

- The one that believe that the system is isolated will not be able to implement the best defense.



© ABB AB

# Procedures and Protocols
## Shamoon

- Destroyed 30.000+ computers.
- Insider
- *"Not a single drop of oil was lost.“*
  CEO Khalid Al-Falih
- *"In our experience in conducting hundreds of vulnerability assessments in the private sector, in **no** case have we ever found the operations network, the SCADA system or energy management system separated from the enterprise network.*
  *On average, we see 11 direct connections between those networks.”*
  Source: Sean McGurk, The Subcommittee on National Security, Homeland Defense, and Foreign Operations May 25, 2011 hearing.

© ABB Group

# Cyber Security
## If it’s worth having it’s worth stealing

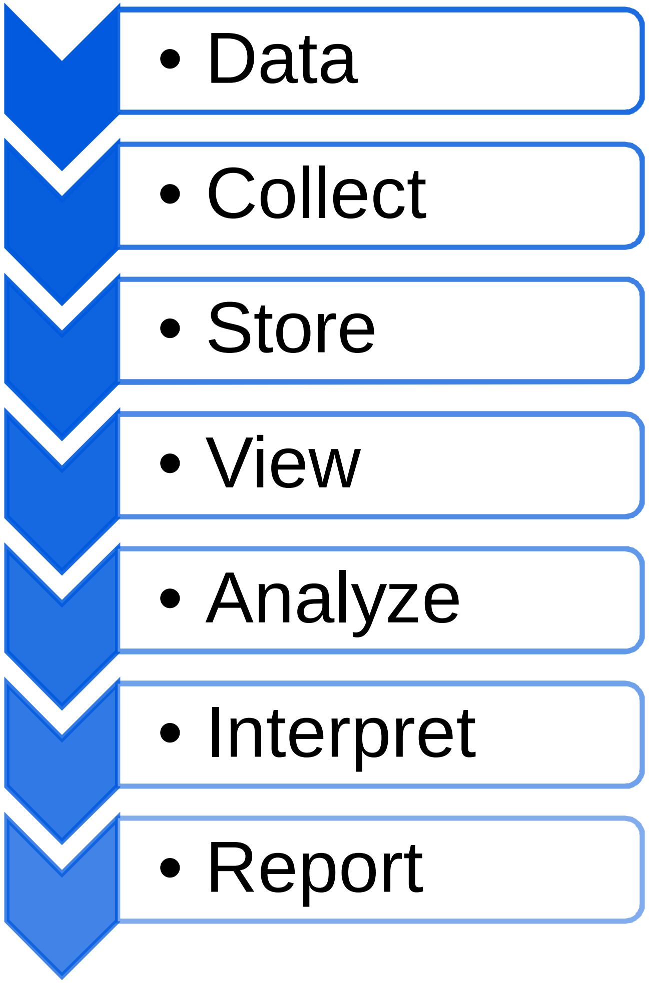
- Source Code
- Diagrams, Plans and Blueprints
- Design documents and Metrics data
- Mechanisms for infrastructure improvements
- Certificates and Credentials

Source: MSI Microsolved Inc.

# Cyber Security
## Fingerprint - Service with a defined scope

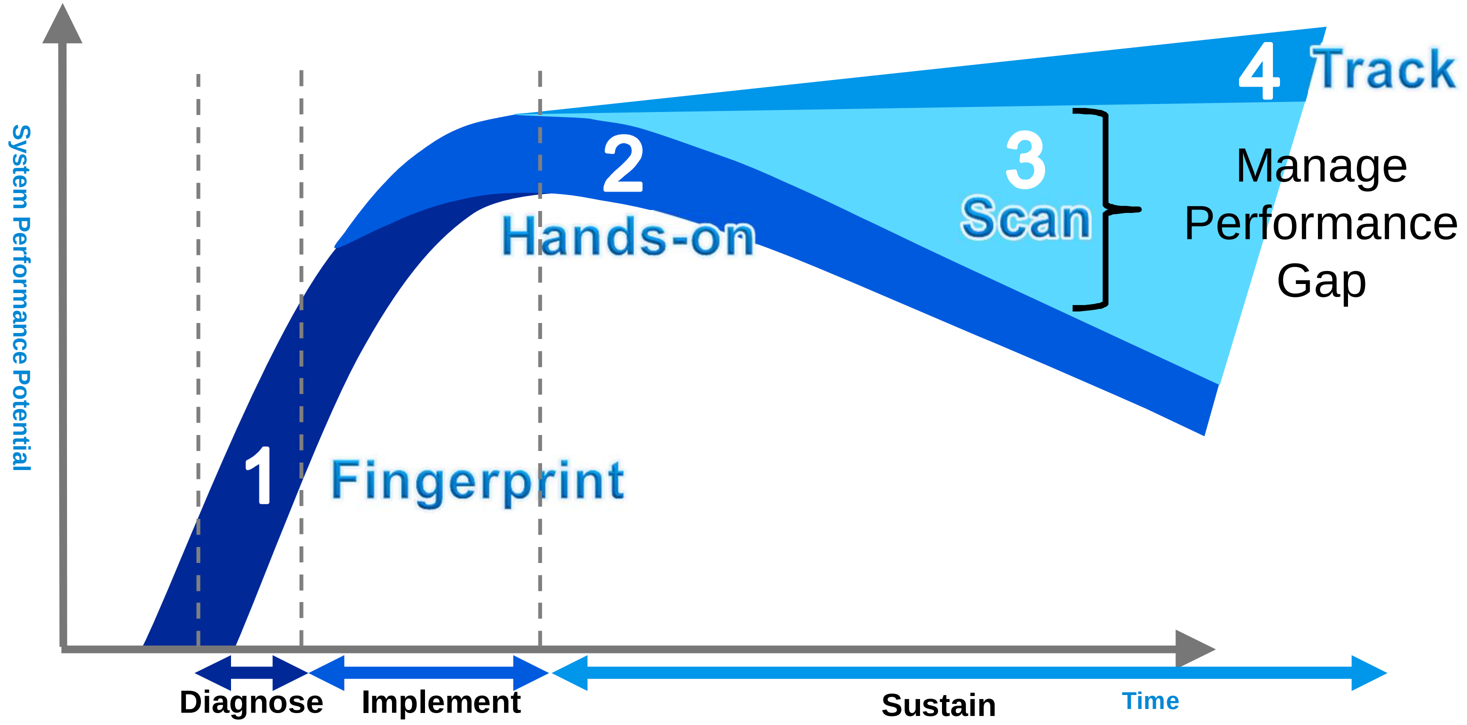
**Benefits:**

- Consistent – same everywhere
- High and even quality
- Repeatable
- Based on best practicies



- Data
- Collect
- Store
- View
- Analyze
- Interpret
- Report

# ABB Cyber Security Optimization
## Diagnose, implement and sustain performance

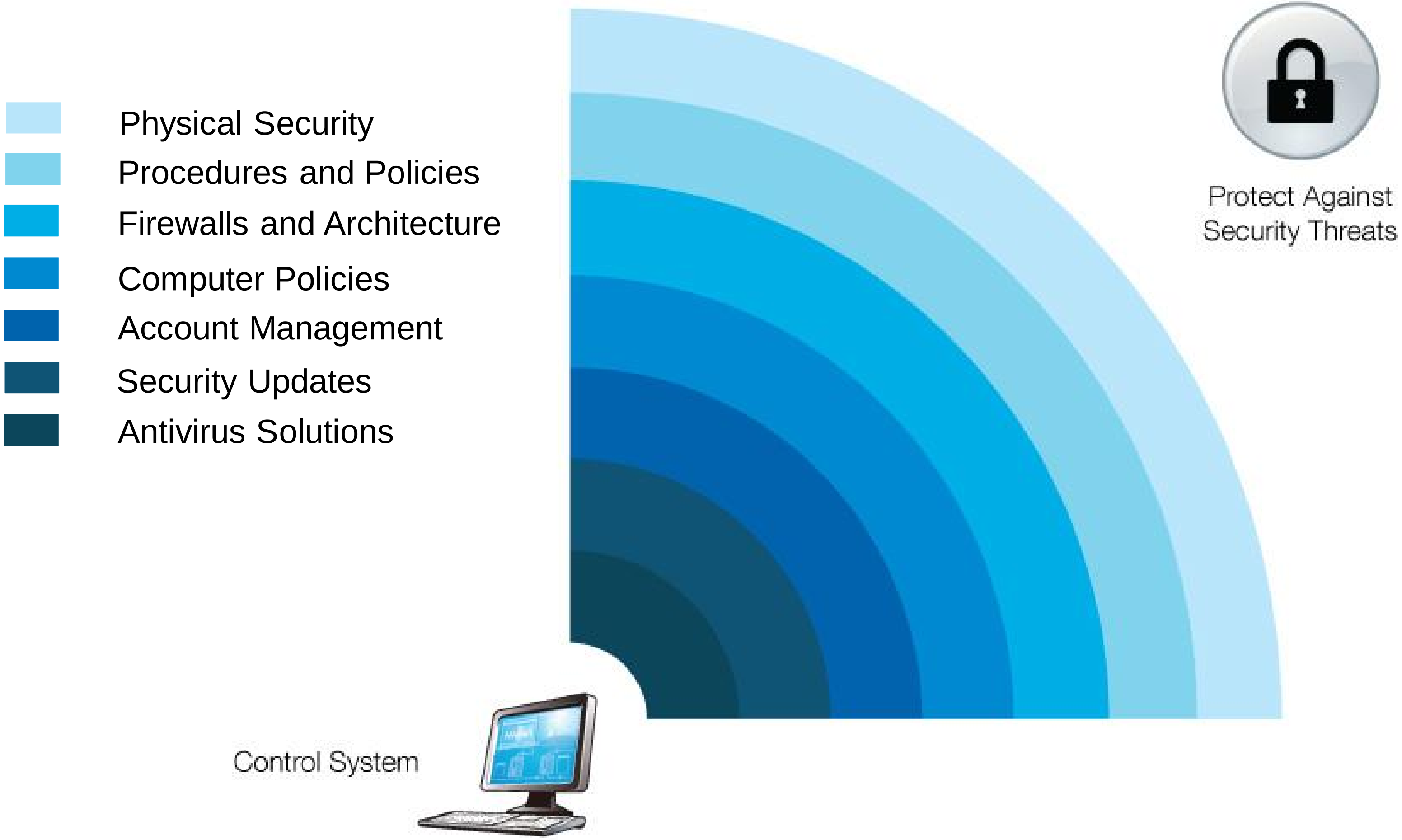


# Cyber Security Fingerprint
## What does the Fingerprint do?

- 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

**It does NOT make the system completely secure.**

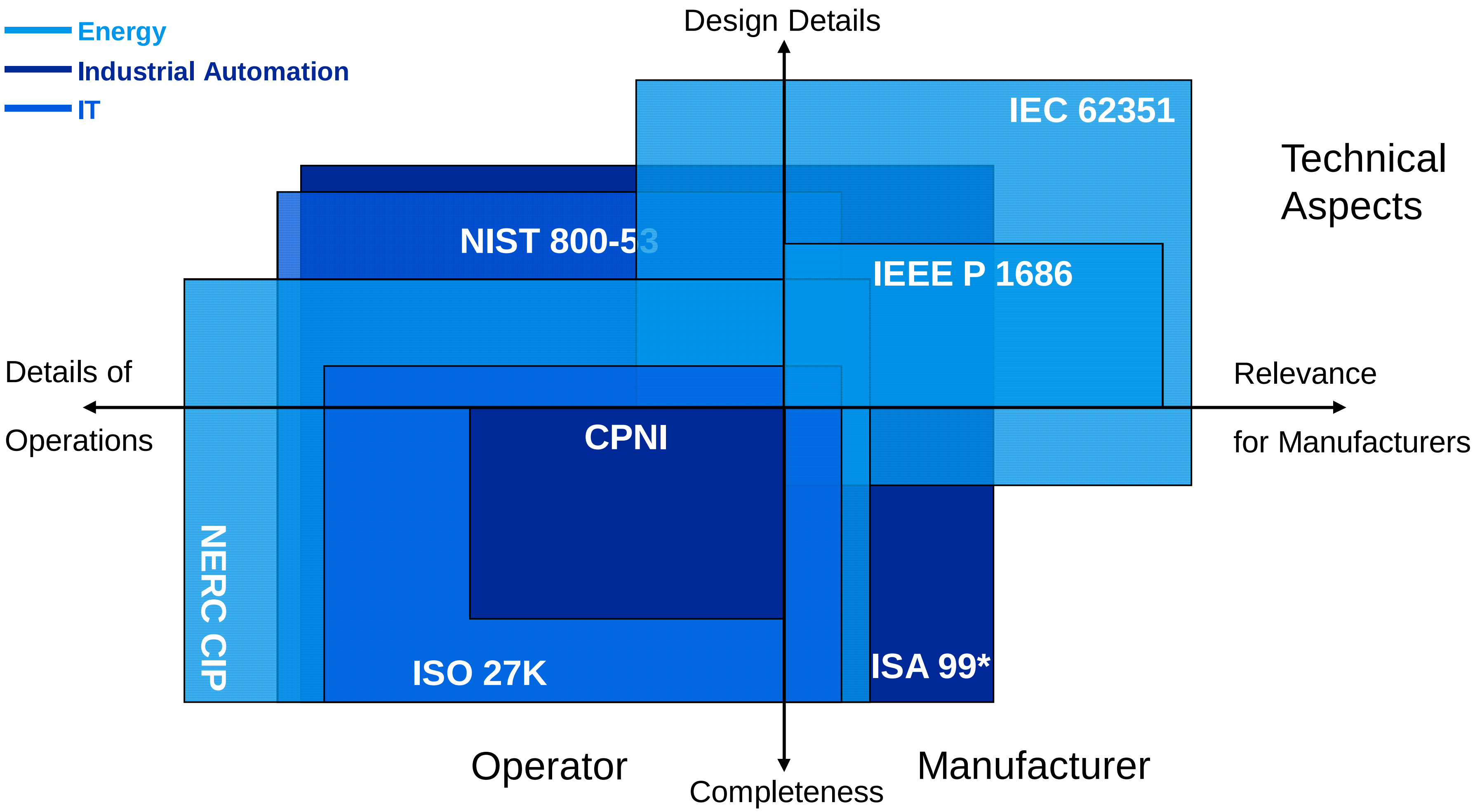
# Cyber Security Fingerprint
## Security in depth



- 🟦 Physical Security
- 🟦 Procedures and Policies
- 🟦 Firewalls and Architecture
- 🟦 Computer Policies
- 🟦 Account Management
- 🟦 Security Updates
- 🟦 Antivirus Solutions

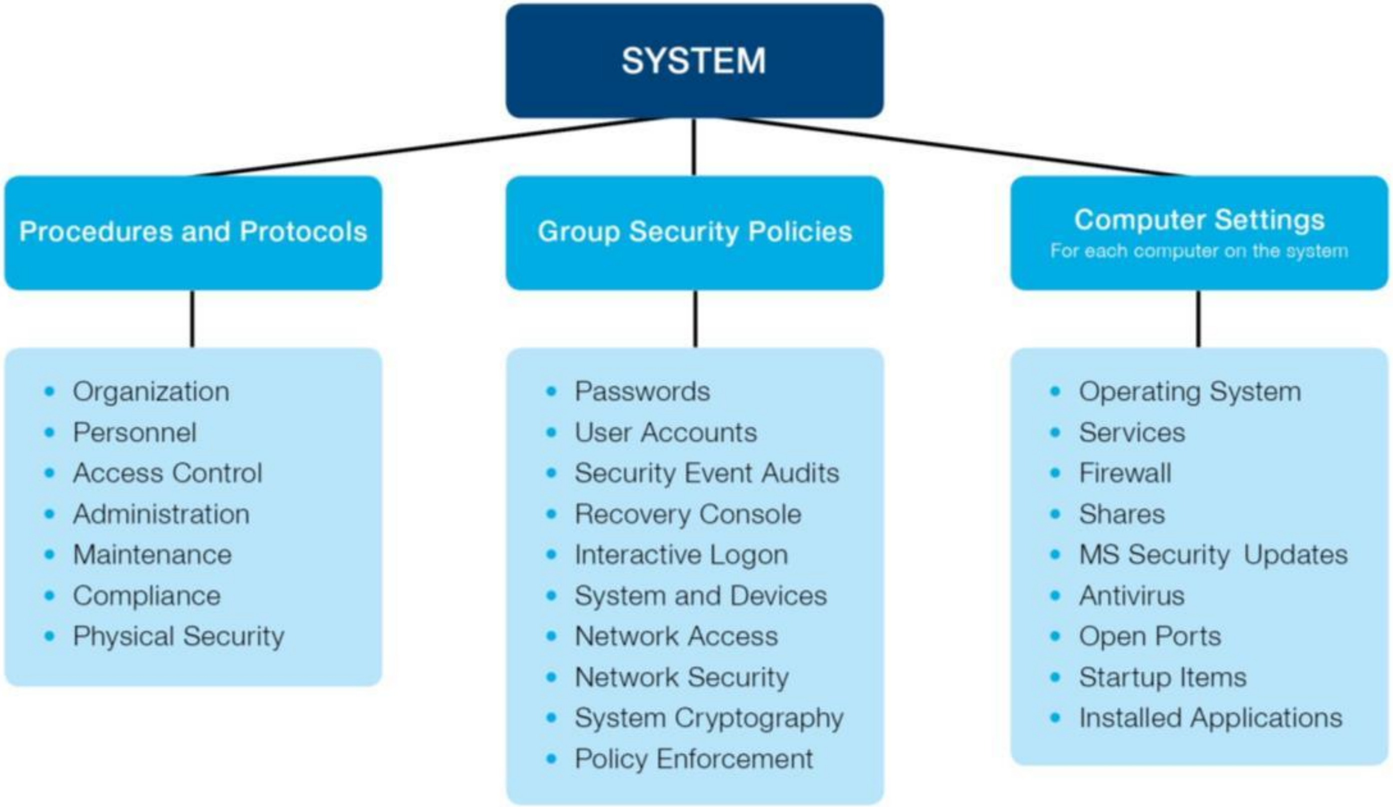
© ABB Group

# Cyber Security
## Scope and completeness of standards



* 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.

# Cyber Security Fingerprint
## Key Performance Indicators



SYSTEM

Procedures and Protocols

- Organization
- Personnel
- Access Control
- Administration
- Maintenance
- Compliance
- Physical Security

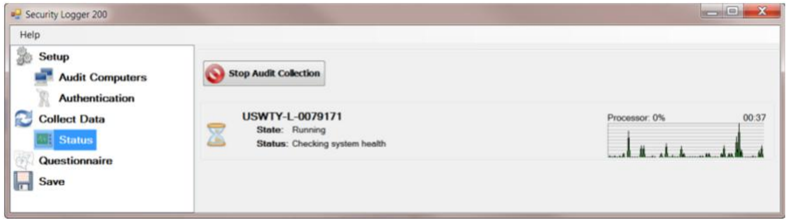
Group Security Policies

- Passwords
- User Accounts
- Security Event Audits
- Recovery Console
- Interactive Logon
- System and Devices
- Network Access
- Network Security
- System Cryptography
- Policy Enforcement

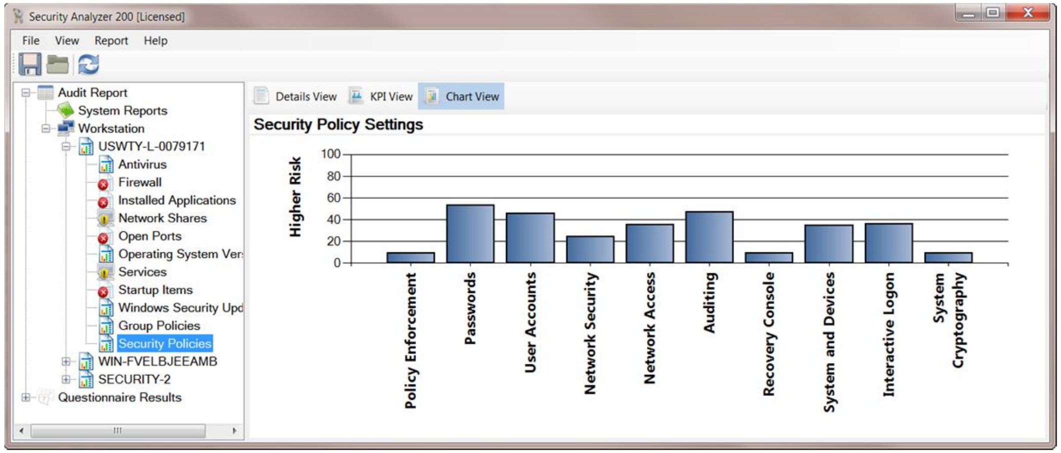
Computer Settings
For each computer on the system

- Operating System
- Services
- Firewall
- Shares
- MS Security Updates
- Antivirus
- Open Ports
- Startup Items
- Installed Applications

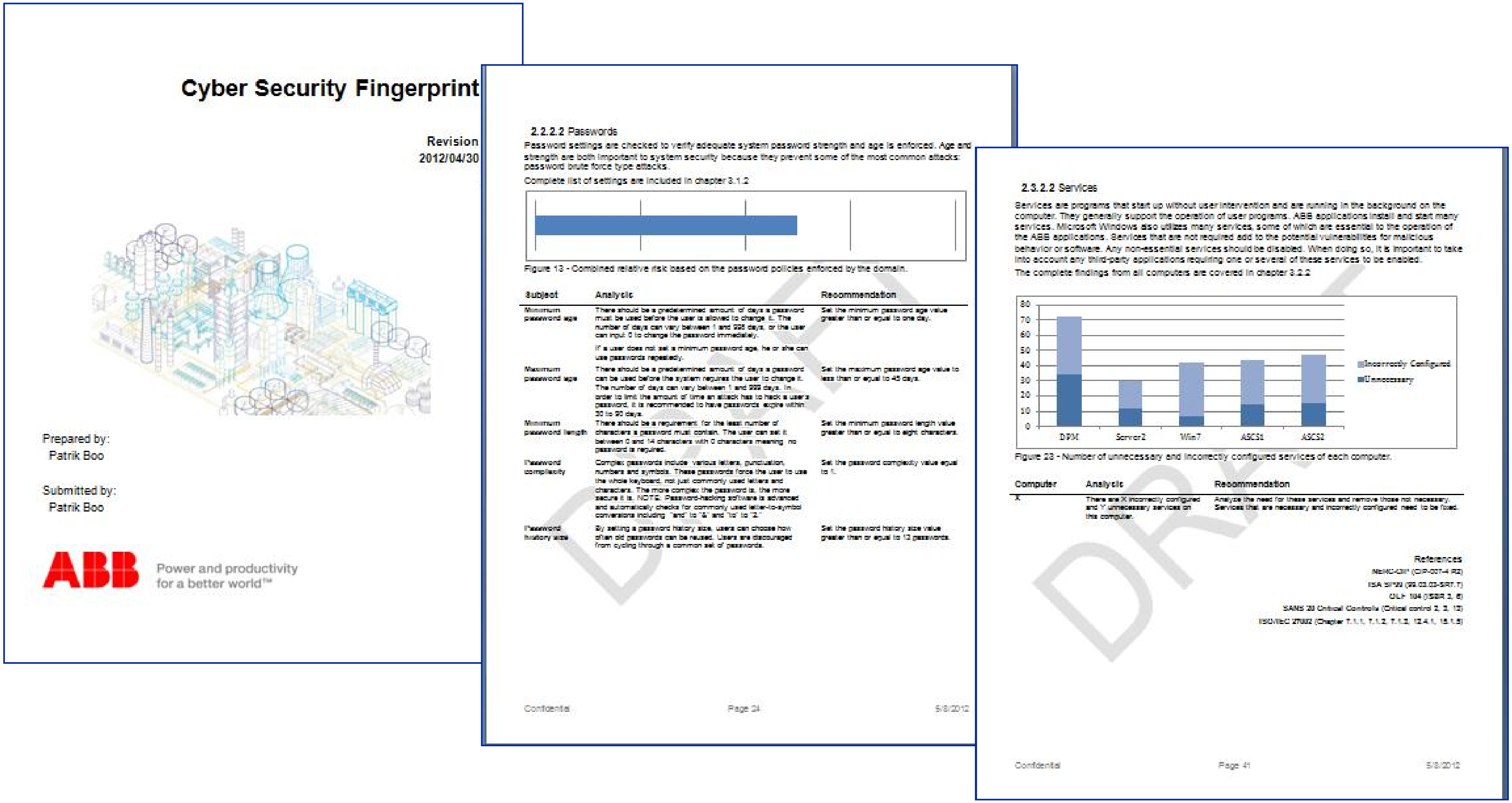
# Cyber Security Fingerprint
## Specialiced tools + interview



USWTY-L-0079171
State: Running
Status: Checking system health



# Cyber Security Fingerprint
## Report with recommendations and action plan



Cyber Security Fingerprint

Revision
2012/04/30

Prepared by:
Patrik Boo

Submitted by:
Patrik Boo

Power and productivity
for a better world™

2.2.2.2 Passwords

Password settings are checked to verify adequate system password strength and age is enforced. Age and strength are both important to system security because they prevent some of the most common attacks: password brute force type attacks.

Complete list of settings are included in chapter 3.1.2

Figure 13 - Combined relative risk based on the password policies enforced by the domain.

| Subject | Analysis | Recommendation |
|---|---|---|
| Minimum password age | There should be a predetermined amount of days a password must be used before the user is allowed to change it. The number of days can vary between 1 and 998 days, or the user can input 0 to change the password immediately.<br>If a user does not set a minimum password age, he or she can use passwords repeatedly. | Set the minimum password age value greater than or equal to one day. |
| Maximum password age | There should be a predetermined amount of days a password can be used before the system requires the user to change it. The number of days can vary between 1 and 999 days. In order to limit the amount of time an attack has to hack a user's password, it is recommended to have passwords expire within 30 to 90 days. | Set the maximum password age value to less than or equal to 45 days. |
| Minimum password length | There should be a requirement for the least number of characters a password must contain. The user can set it between 0 and 14 characters with 0 characters meaning no password is required. | Set the minimum password length value greater than or equal to eight characters. |
| Password complexity | Complex passwords include various letters, punctuation, numbers and symbols. These passwords force the user to use the whole keyboard, not just commonly used letters and characters. The more complex the password is, the more secure it is. NOTE: Password-hacking software is advanced and automatically checks for commonly used letter-to-symbol conversions including "and" to "&" and "to" to "2." | Set the password complexity value equal to 1. |
| Password history size | By setting a password history size, users can choose how often old passwords can be reused. Users are discouraged from cycling through a common set of passwords. | Set the password history size value greater than or equal to 12 passwords. |

Confidential Page 24 5/8/2012

2.3.2.2 Services

Services are programs that start up without user intervention and are running in the background on the computer. They generally support the operation of user programs. ABB applications install and start many services. Microsoft Windows also utilizes many services, some of which are essential to the operation of the ABB applications. Services that are not required add to the potential vulnerabilities for malicious behavior or software. Any non-essential services should be disabled. When doing so, it is important to take into account any third-party applications requiring one or several of these services to be enabled.

The complete findings from all computers are covered in chapter 3.2.2

Figure 23 - Number of unnecessary and incorrectly configured services of each computer.

| Computer | Analysis | Recommendation |
|---|---|---|
| X | There are X incorrectly configured and Y unnecessary services on this computer. | Analyze the need for these services and remove those not necessary. Services that are necessary and incorrectly configured need to be fixed. |

References
NERC-CIP (CIP-007-4 R2)
ISA SP99 (99.03.03-SRT.7)
OLF 104 (ISBR 3, 6)
SANS 20 Critical Controls (Critical control 2, 3, 13)
ISO/IEC 27002 (Chapter 7.1.1, 7.1.2, 7.1.3, 12.4.1, 15.1.5)

Confidential Page 41 5/8/2012

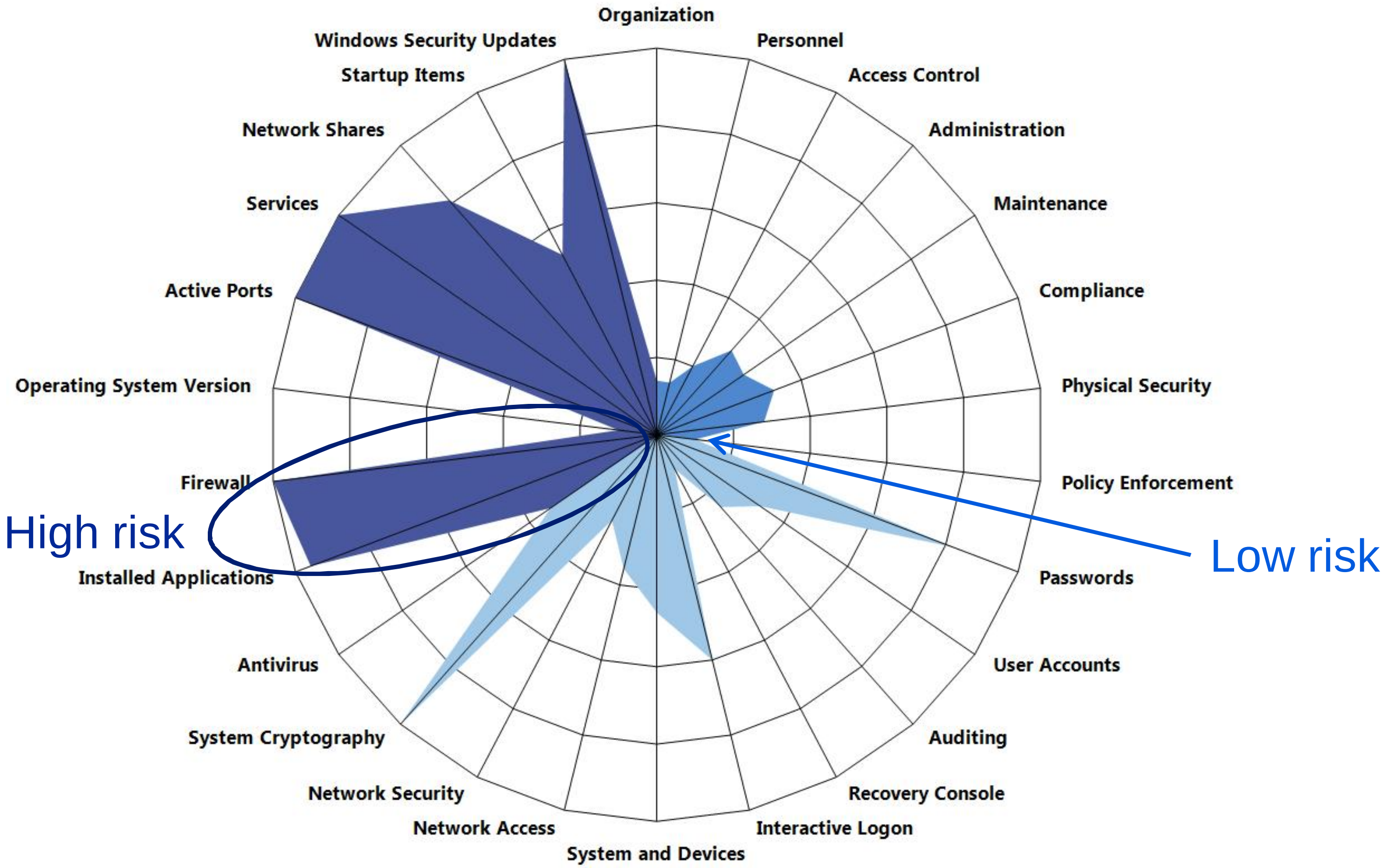
DRAFT

# Cyber Security Fingerprint
## Recommendations

| Setting | Description | Recommendation |
|---|---|---|
| **Minimum password age** | There should be a predetermined amount of days a password must be used before the user is allowed to change it. The number of days can vary between 1 and 998 days, or the user can input 0 to change the password immediately. If a user does not set a minimum password age, he or she can use passwords repeatedly. | Set the minimum password age value greater than or equal to one day. |

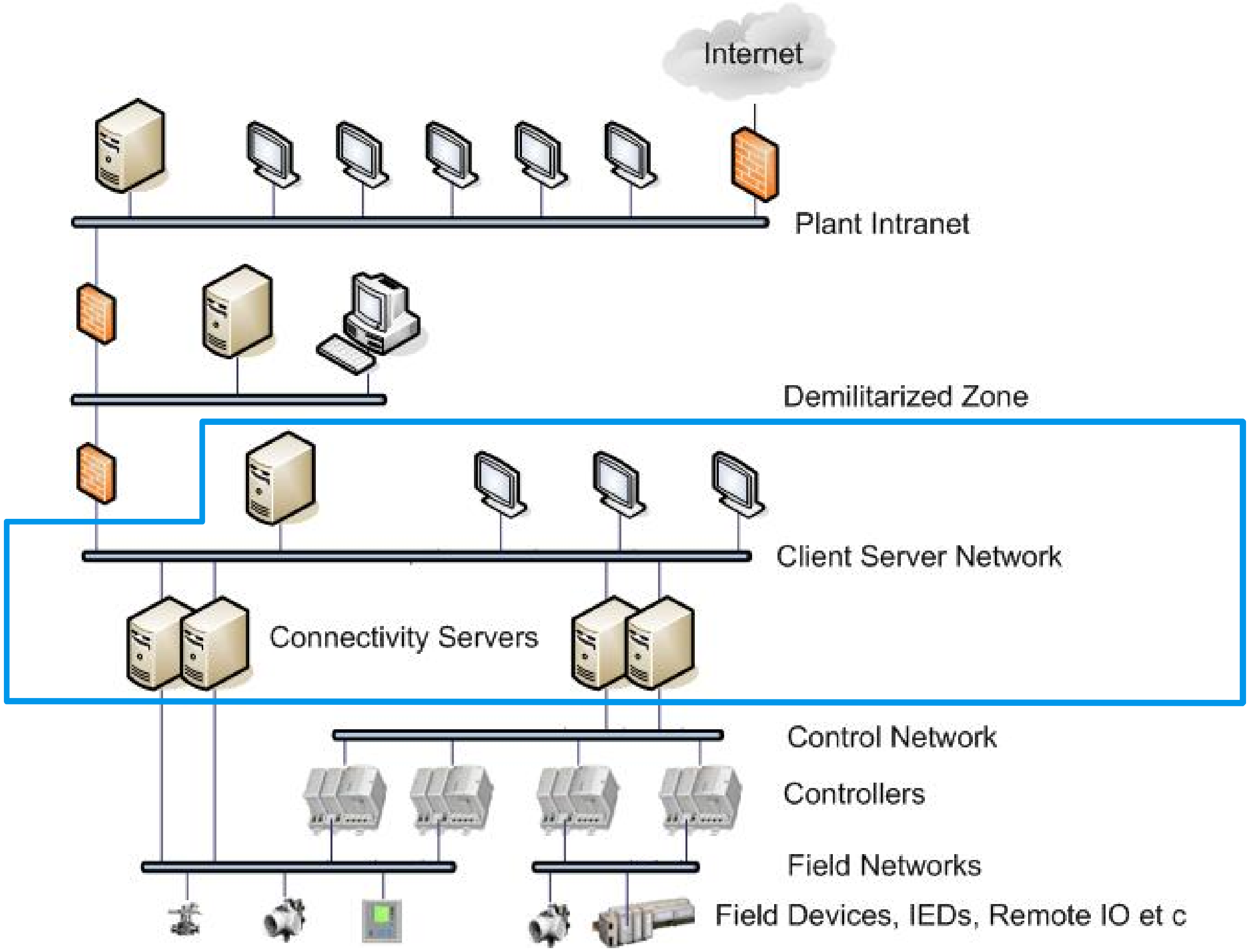
- After raw data is collected with the security logger, it's compared to the Control System Master Profile to determine where recommendations are needed.
- If the customer's data shows the setting to be below standard, the description and recommendation are included in the report.

# Cyber Security Fingerprint
## Report: Risk Profile



**While the Fingerprint is an indicator of your security status at a given time, any system, no matter how many precautions are taken, can be compromised.**

# Cyber Security Fingerprint
## Control System Architecture - what to protect



© ABB Group

# Cyber Security Fingerprint
## Success Stories

Success Story

Refinery tightens security with help of ABB Cyber
Fingerprint

A Middle Eastern petroleum refinery's comprehensive security includes military guards along the facility's perimeters and advanced cyber security measures. Even with these extensive security precautions, the company wanted to ensure that the same level of comprehensive cyber security policies and procedures were applied to its process control systems.

**Customer need**
- Review existing cyber security measures
- Identify security gaps

**ABB's response**
To ensure the facility's advanced security measures took their control systems into account, the refinery chose the ABB Cyber Security Fingerprint to identify strengths and weaknesses for defending against a cyber attack within the plant's automation systems.

The non-invasive service started by gathering data from all computers associated with the systems and from key personnel, and then compared the data to best practices with ABB's proprietary, software-based analysis tool. A resulting report provided detailed recommendations to reduce cyber security vulnerability while helping to develop a focused and sustainable security strategy for the control systems.

**Results**
Even though extensive security
the ABB Cyber Security Fingerp
improve control system security
unnecessary software was runn
or removed. Security patches fo
missing and also needed to be

In a region where cyber attacks
highly secure facility initially had
However, the depth of the repor
both act on the findings and sch
Security Fingerprints to confirm
policies and procedures are alw

**Customer Benefits**
- Comprehensive view of plant
- Better risk mitigation against
- Enhanced control system sec
  facility security
- Tighter security procedures

© 2012 ABB Inc.
ABB reserves the right to change specifications without notice.

Power and pr
for a be

Success Story

Cyber Security Fingerprint uncovers potential risk

A West Virginia-based specialty chemical facility needed to minimize the potential for a cyber security attack by finding and reducing any security vulnerabilities. In addition, the company needed to comply with the U.S. Department of Homeland Security's Chemical-terrorism Vulnerability Information (CVI) requirements to ensure safeguarding of its facilities and information. However, due to the complexity of the facility, it was difficult for the company to do an internal, comprehensive cyber security review of its control systems.

**Customer's need**
To comply with internal cyber security standards and government agency requirements, the specialty chemical producer needed a complete review of the status of its current software and computer security measures as well as an assessment of the potential for exposure from computer viruses or malware.

**ABB's response**
The ABB Cyber Security Fingerprint identifies strengths and weaknesses for defending against a cyber attack within a plant's control systems by gathering data from all servers within the control system and key personnel, and comparing them against best practices with ABB's proprietary software-based analysis tool. The resulting report provides detailed recommendations to reduce cyber security vulnerabilities while helping to develop a focused and sustainable security strategy for control systems.

With ABB's Security Logger tool, data was collected from the 30 computers at the specialty chemical facility in less than five hours without affecting the running process. Without the use of ABB's proprietary data collection tool, this process would have taken several weeks.

During the Fingerprint, ABB determines i
cyber security protection.

With automated report generation
analysts reviewed the data and pr
within a week. Automated report g
features of several ABB Advanced

Included in the report was a detail
address the issues uncovered by t
which also provided the basis for a
for the site. However, to comply w
the specifics of the Fingerprint rep

**Benefits**
- – Fast resolution for vital security
- – Comprehensive view of plant cy
- – Better risk mitigation against a c
- – A security plan established with

© 2012 ABB Inc.
ABB reserves the right to change specifications without notice.

Power and pr
for a be

Success Story

European steel mill applies ABB Cyber Security Fingerprint to find security gaps

A cold-rolling mill in Spain wanted to review the cyber security status of two process automation systems controlling the steel processing lines.

**Customer need**
- Review control system cyber security status
- Ensure software and antivirus programs were up-to-date

**ABB's response**
To address its cyber security needs, the steel mill chose the ABB Cyber Security Fingerprint, a non-invasive service that identifies strengths and weaknesses for defending against cyber attacks within a plant's process automation systems.

ABB starts by gathering information from structured interviews with key plant personnel. While these interviews take place, a proprietary software-based collection tool, Security Logger, collects information and system settings from control systems and other computers on the plant network. ABB's Security Analyzer tool is then used to calculate Key Performance Indicators (KPIs) that highlight strengths and weaknesses of control system security.

The resulting report provides recommendations to reduce cyber security vulnerabilities while helping to develop a focused and sustainable security strategy for control systems. Included in the final report is a detailed, prioritized action plan to address specific issues uncovered by the Fingerprint.

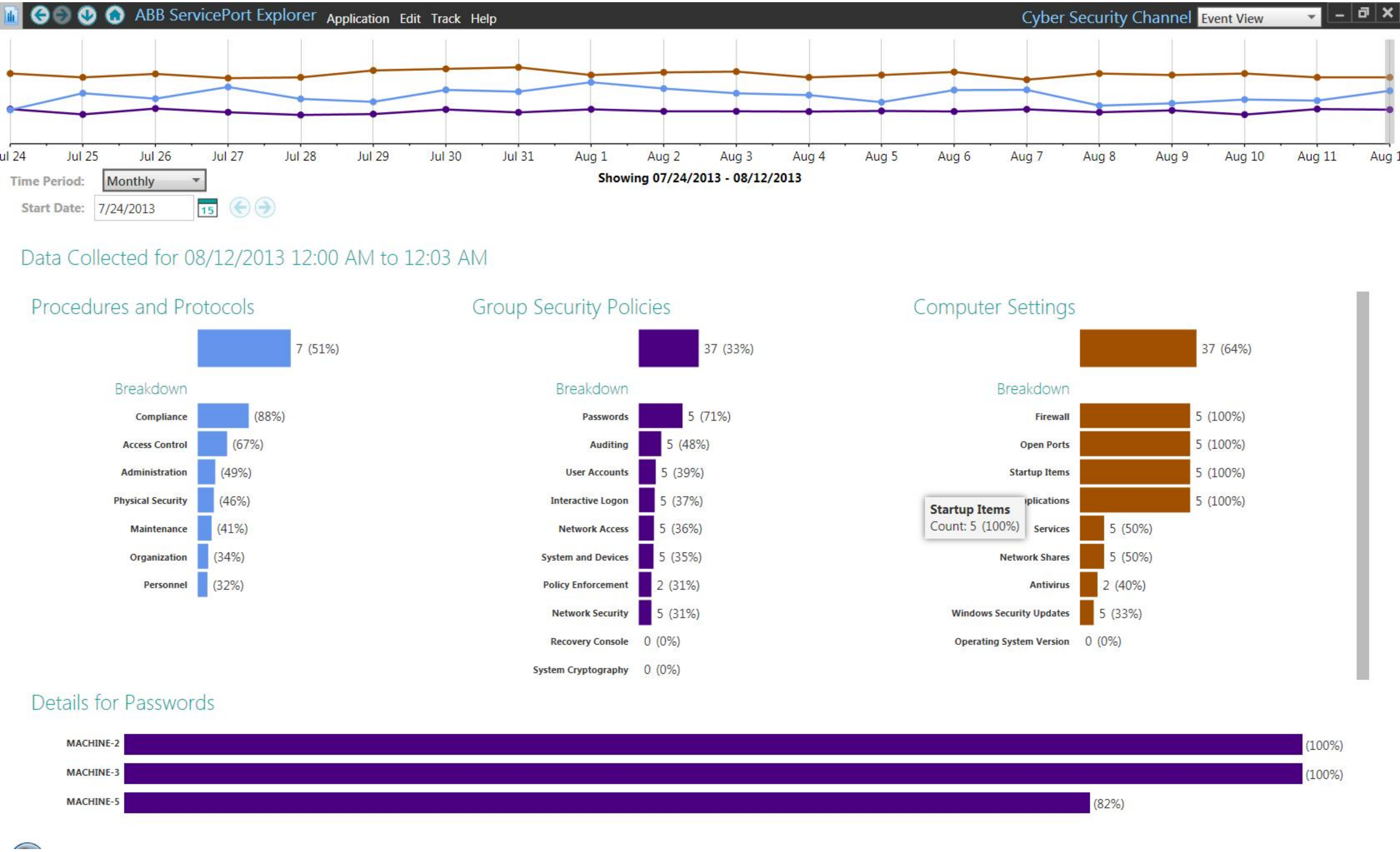
**Results**
The Cyber Security Fingerprint found the steel mill's process automation systems were running outdated versions of software that were no longer supported. Additionally, the company needed to upgrade its antivirus protection.

**Customer benefits**
- Detailed report on control system security in one man-week
- Fast resolution for important security issues
- Foundation for comprehensive cyber security plan

© 2012 ABB Inc.
ABB reserves the right to change specifications without notice.

Power and productivity
for a better world™

# Cyber Security Fingerprint
## ServicePort - Cyber Security Channel



Showing 07/24/2013 - 08/12/2013

Time Period: Monthly

Start Date: 7/24/2013

Data Collected for 08/12/2013 12:00 AM to 12:03 AM

Procedures and Protocols: 7 (51%)

| Breakdown | |
|---|---|
| Compliance | (88%) |
| Access Control | (67%) |
| Administration | (49%) |
| Physical Security | (46%) |
| Maintenance | (41%) |
| Organization | (34%) |
| Personnel | (32%) |

Group Security Policies: 37 (33%)

| Breakdown | |
|---|---|
| Passwords | 5 (71%) |
| Auditing | 5 (48%) |
| User Accounts | 5 (39%) |
| Interactive Logon | 5 (37%) |
| Network Access | 5 (36%) |
| System and Devices | 5 (35%) |
| Policy Enforcement | 2 (31%) |
| Network Security | 5 (31%) |
| Recovery Console | 0 (0%) |
| System Cryptography | 0 (0%) |

Computer Settings: 37 (64%)

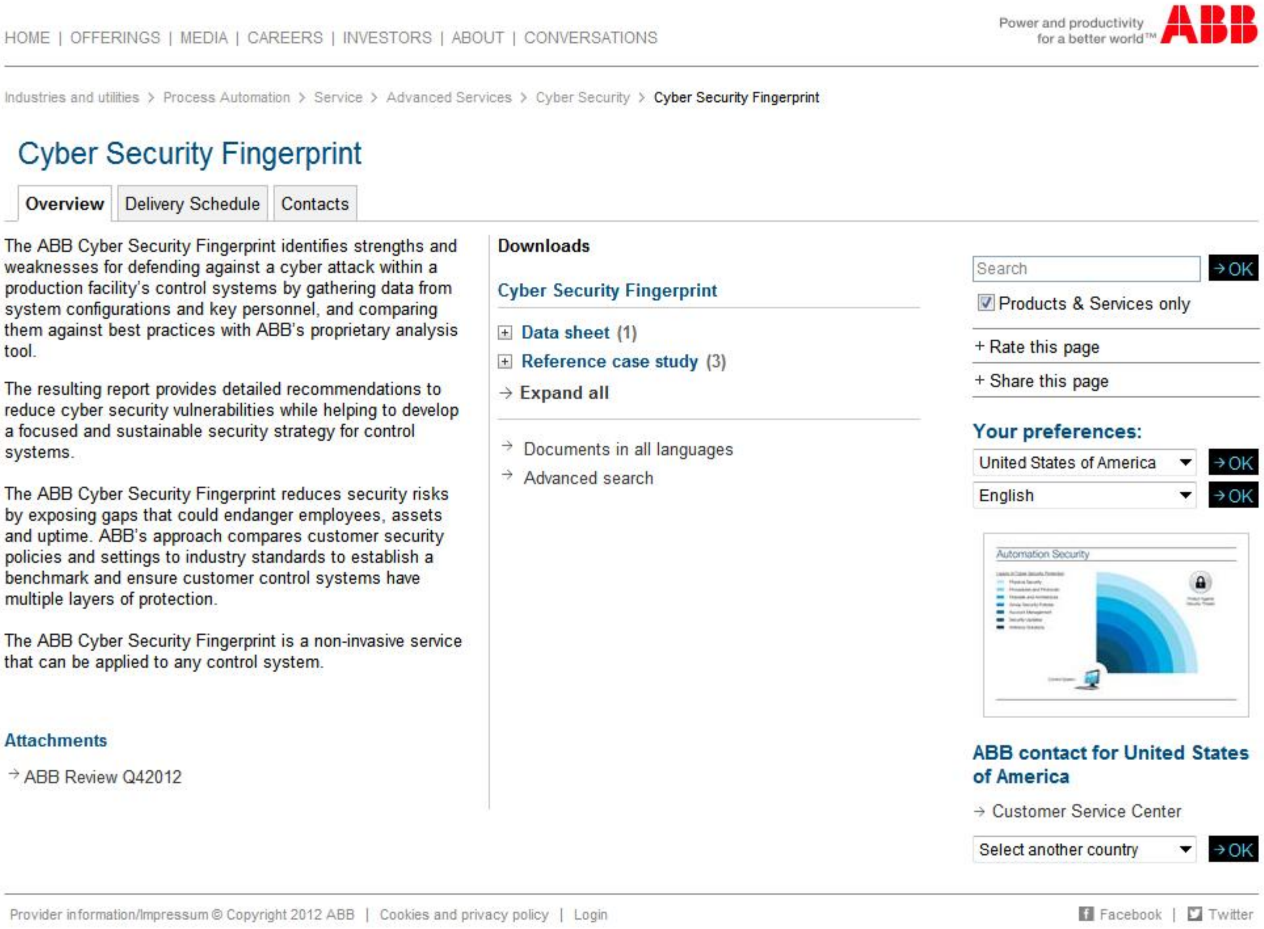
| Breakdown | |
|---|---|
| Firewall | 5 (100%) |
| Open Ports | 5 (100%) |
| Startup Items | 5 (100%) |
| plications | 5 (100%) |
| Services | 5 (50%) |
| Network Shares | 5 (50%) |
| Antivirus | 2 (40%) |
| Windows Security Updates | 5 (33%) |
| Operating System Version | 0 (0%) |

Startup Items
Count: 5 (100%)

Details for Passwords

| | |
|---|---|
| MACHINE-2 | (100%) |
| MACHINE-3 | (100%) |
| MACHINE-5 | (82%) |

# Cyber Security Fingerprint
www.abb.com



HOME | OFFERINGS | MEDIA | CAREERS | INVESTORS | ABOUT | CONVERSATIONS
Power and productivity for a better world™ ABB
Industries and utilities > Process Automation > Service > Advanced Services > Cyber Security > Cyber Security Fingerprint

## Cyber Security Fingerprint

Overview | Delivery Schedule | Contacts

The ABB Cyber Security Fingerprint identifies strengths and weaknesses for defending against a cyber attack within a production facility's control systems by gathering data from system configurations and key personnel, and comparing them against best practices with ABB's proprietary analysis tool.

The resulting report provides detailed recommendations to reduce cyber security vulnerabilities while helping to develop a focused and sustainable security strategy for control systems.

The ABB Cyber Security Fingerprint reduces security risks by exposing gaps that could endanger employees, assets and uptime. ABB's approach compares customer security policies and settings to industry standards to establish a benchmark and ensure customer control systems have multiple layers of protection.

The ABB Cyber Security Fingerprint is a non-invasive service that can be applied to any control system.

**Attachments**

→ ABB Review Q42012

**Downloads**

**Cyber Security Fingerprint**

⊞ **Data sheet** (1)
⊞ **Reference case study** (3)
→ **Expand all**

→ Documents in all languages
→ Advanced search

**Your preferences:**

**ABB contact for United States of America**

→ Customer Service Center

Select another country ▾ →OK
Provider information/Impressum © Copyright 2012 ABB | Cookies and privacy policy | Login
Facebook | Twitter

9AKK105408A9402

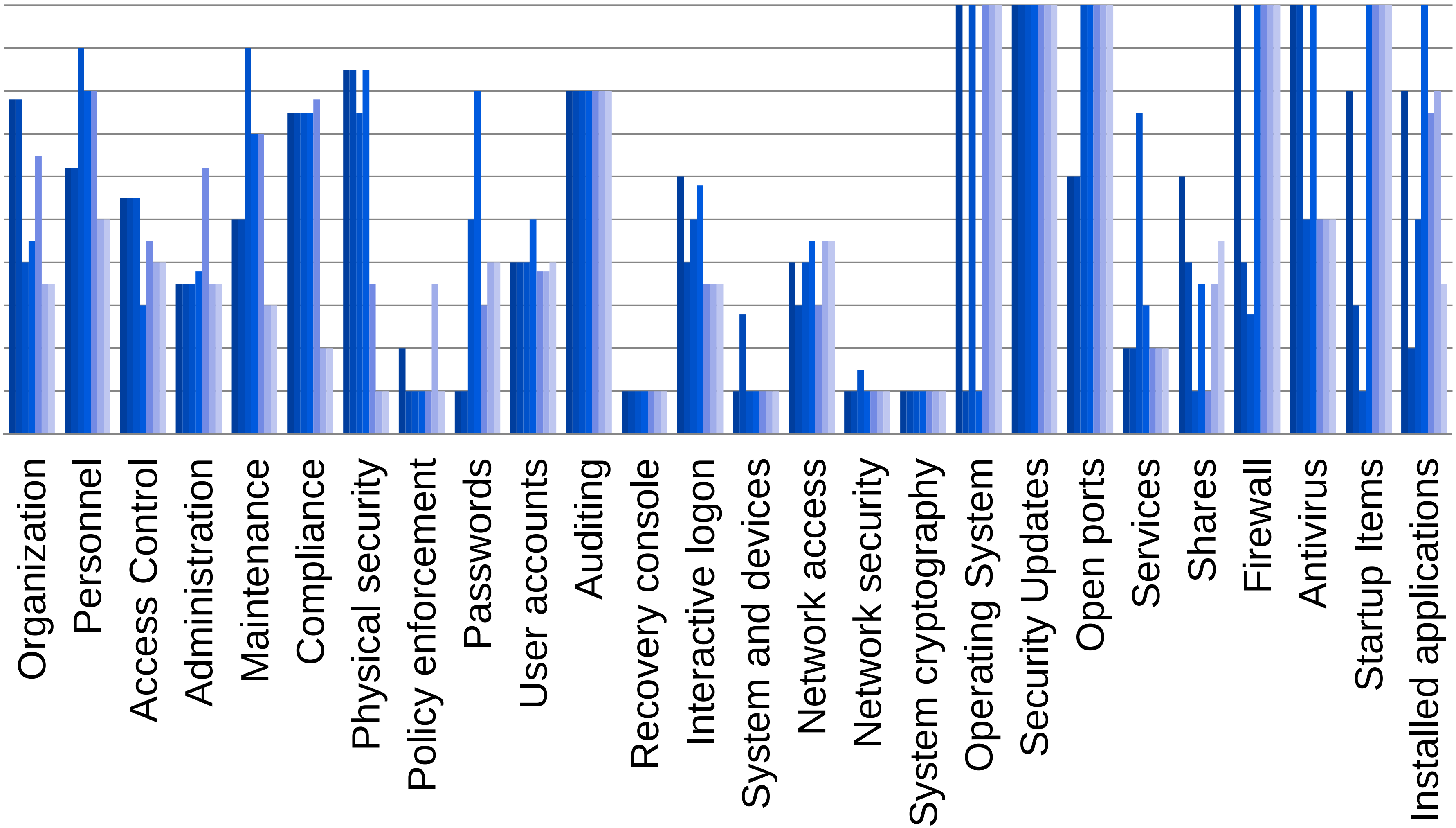
Power and productivity
for a better world™

ABB

# Security for System 800xA for all phases
## The SD$^3$ + C Security Framework

| | |
|---|---|
| Secure by Design | • Security in the Product Development Process: Requirements, Design, Implementation, Verification |
| Secure by Default | • Default installation and usage with minimal attack surface<br>• Built in functions for Defense in Depth |
| Secure in Deployment | • Support for Secure Project and Plant Lifecycle<br>• Validation of 3rd party software and solutions |
| Communication | • Correct information to those who need to know |

# Cyber Security Fingerprint
## Pilot results



# Cyber Security
## Remote access

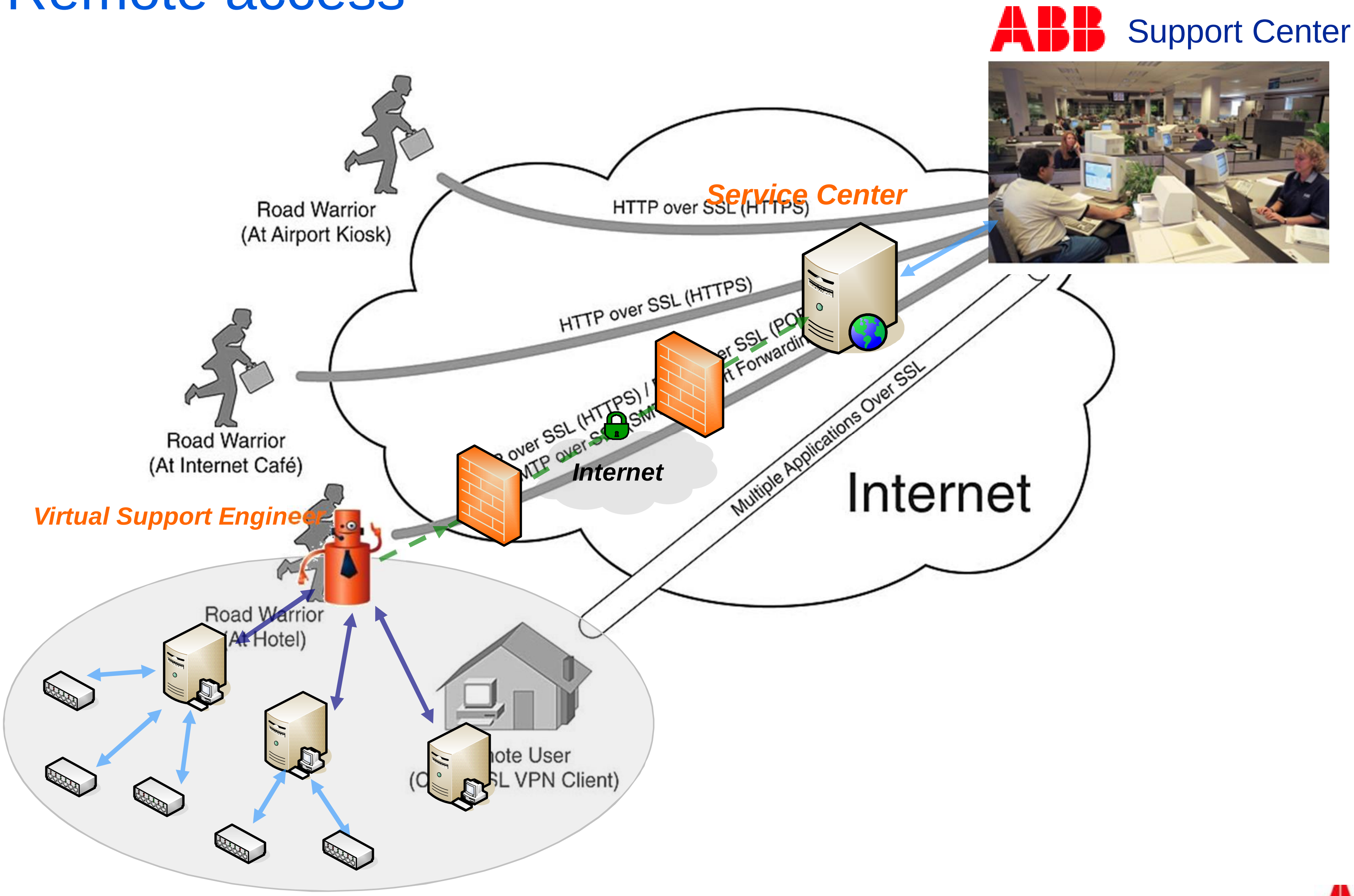


ABB Support Center
Service Center
HTTP over SSL (HTTPS)
HTTP over SSL (HTTPS)
over SSL (HTTPS) /
MTP over S SM
er SSL (POP
t Forwardin
Road Warrior
(At Airport Kiosk)
Road Warrior
(At Internet Café)
Virtual Support Engineer
Internet
Multiple Applications Over SSL
Internet
Road Warrior
(At Hotel)
ote User
(C SL VPN Client)