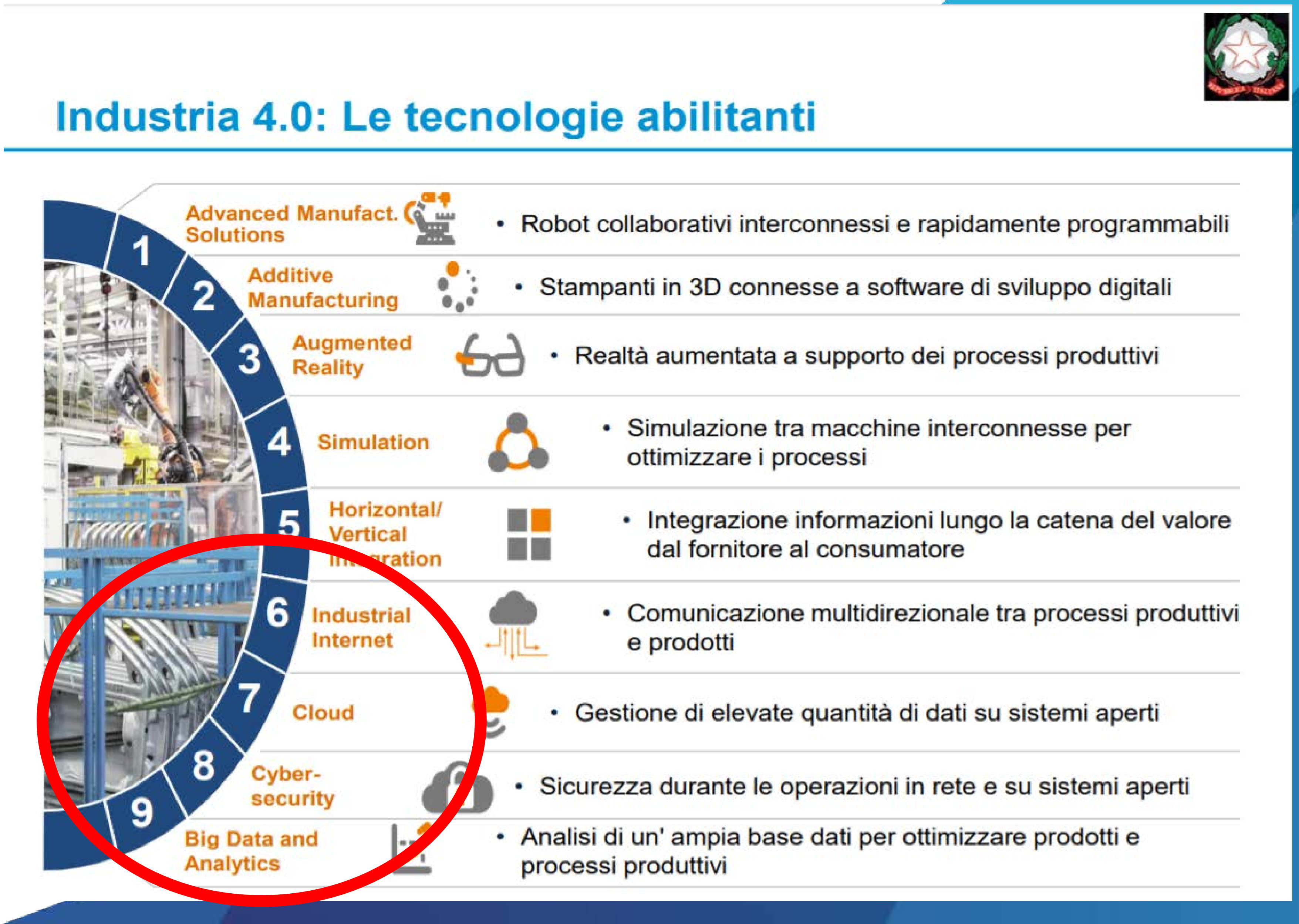
OT/ICS/IIOT CYBER SECURITY RISKS AND INDUSTRY4.0/PHARMA4.0

Enzo M. Tieghi, CEO, ServiTecno Italy – GE Digital Alliance Partner

- ISPE Italy Affiliate
- CSA Cloud Security Alliance Italia
- CLUSIT

etieghi@servitecno.it
https://it.linkedin.com/in/etieghi

INDUSTRY4.0 & CYBER SECURITY



Industria 4.0: Le tecnologie abilitanti

1. Advanced Manufact. Solutions
   - Robot collaborativi interconnessi e rapidamente programmabili
2. Additive Manufacturing
   - Stampanti in 3D connesse a software di sviluppo digitali
3. Augmented Reality
   - Realtà aumentata a supporto dei processi produttivi
4. Simulation
   - Simulazione tra macchine interconnesse per ottimizzare i processi
5. Horizontal/ Vertical Integration
   - Integrazione informazioni lungo la catena del valore dal fornitore al consumatore
6. Industrial Internet
   - Comunicazione multidirezionale tra processi produttivi e prodotti
7. Cloud
   - Gestione di elevate quantità di dati su sistemi aperti
8. Cyber-security
   - Sicurezza durante le operazioni in rete e su sistemi aperti
9. Big Data and Analytics
   - Analisi di un' ampia base dati per ottimizzare prodotti e processi produttivi

Where are these systems to be protected?

Well, everywhere in you Facility: Industrial Processes, Buildings, Packaging, Logistics, Manufacturing & Infrastructures (Power, HVAC, WFI, etc.)

Where and What are these systems to be protected?

- **DCS (Distributed Control Systems)**
- **PLC and relates Busses(Programmable Controllers)**
- **SCADA/HMI plant flooor networks**
- **Historians, Database, etc.**
- **DNC/CNC, Robot, AGV, 3D-Printers (additive Mfg)**
- **MES, EBRS & Production Management Systems, Traceability, Track and Trace, Efficiency monitoring and Analysis, OEE, etc.**
- **LIMS, QA/QC, Calibration Systems, Measurement and Smart Instrumentation**
- **Remote connections and remote Assett Performance Monitoring and Maintenance (Portals, CMMS, IoT, Industrial IoT, etc.)**
- **Plant Lan, Connected Smart Building and Facility/Building BMS, HVAC, WFI, …**
- **…**

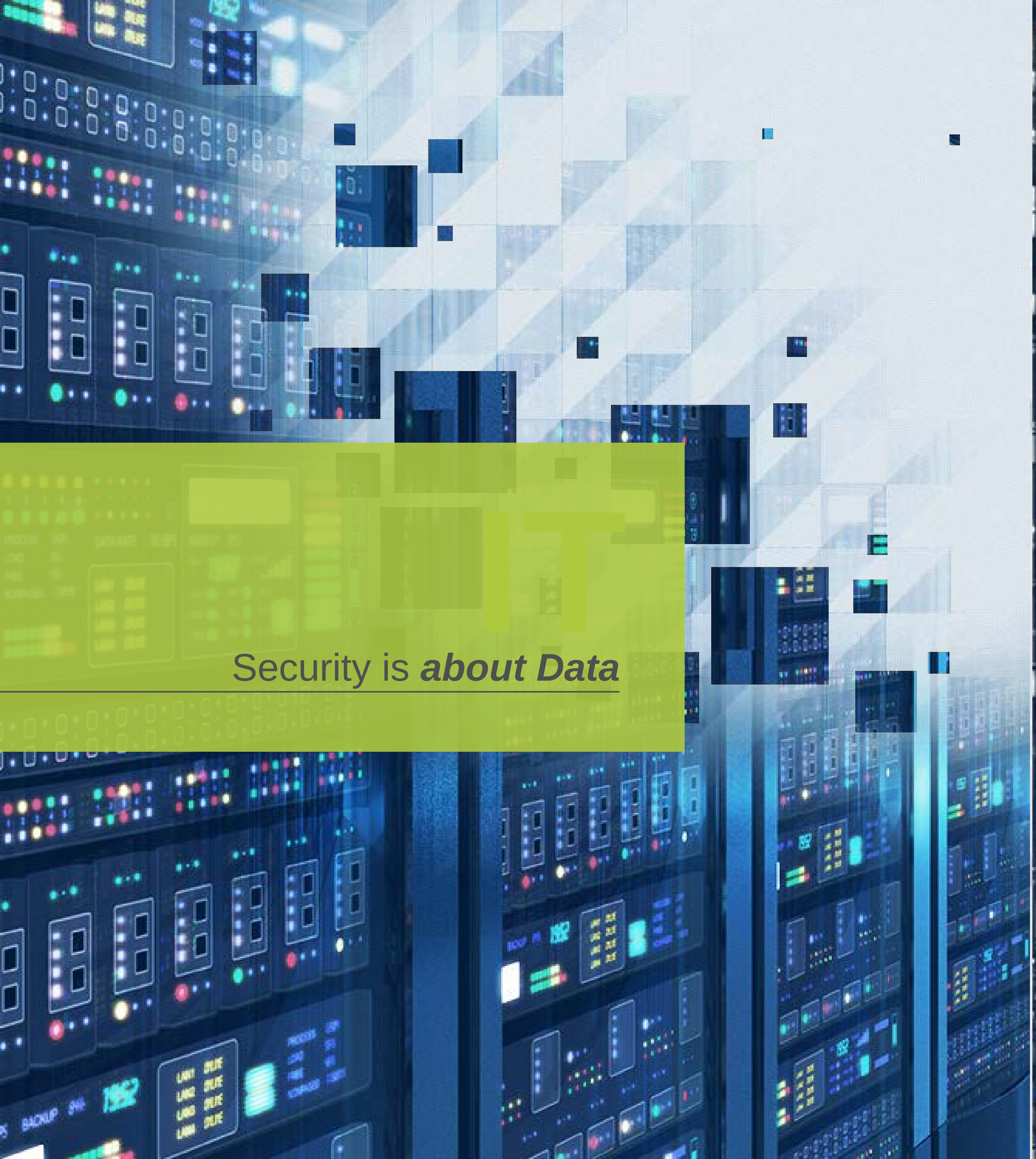
I

WHAT’S THE

IT BIG OT

DIFFERENCE?

O



IT

Security is ***about Data***

OT

Security is ***about Critical Assets & Operation Continuity***

RISK and SAFETY

People
Environment
Assets

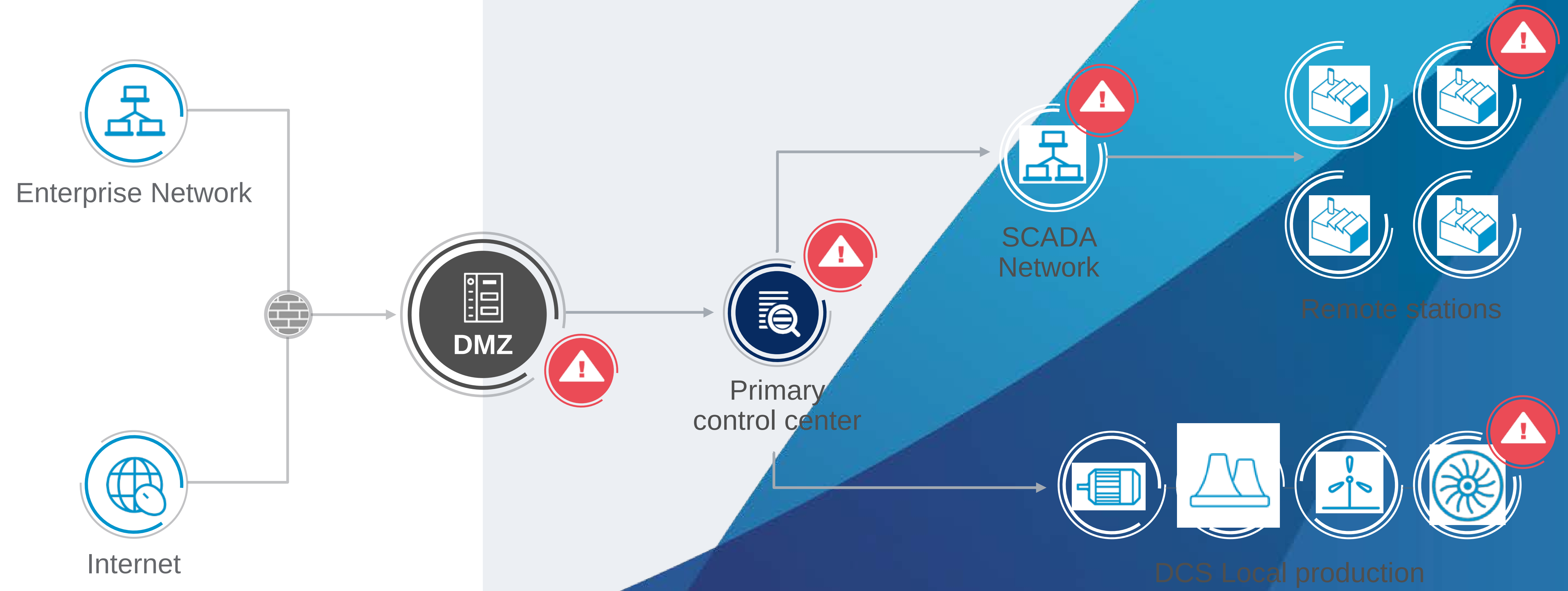
UPTIME & PRODUCTION

Quality and **P**erformance

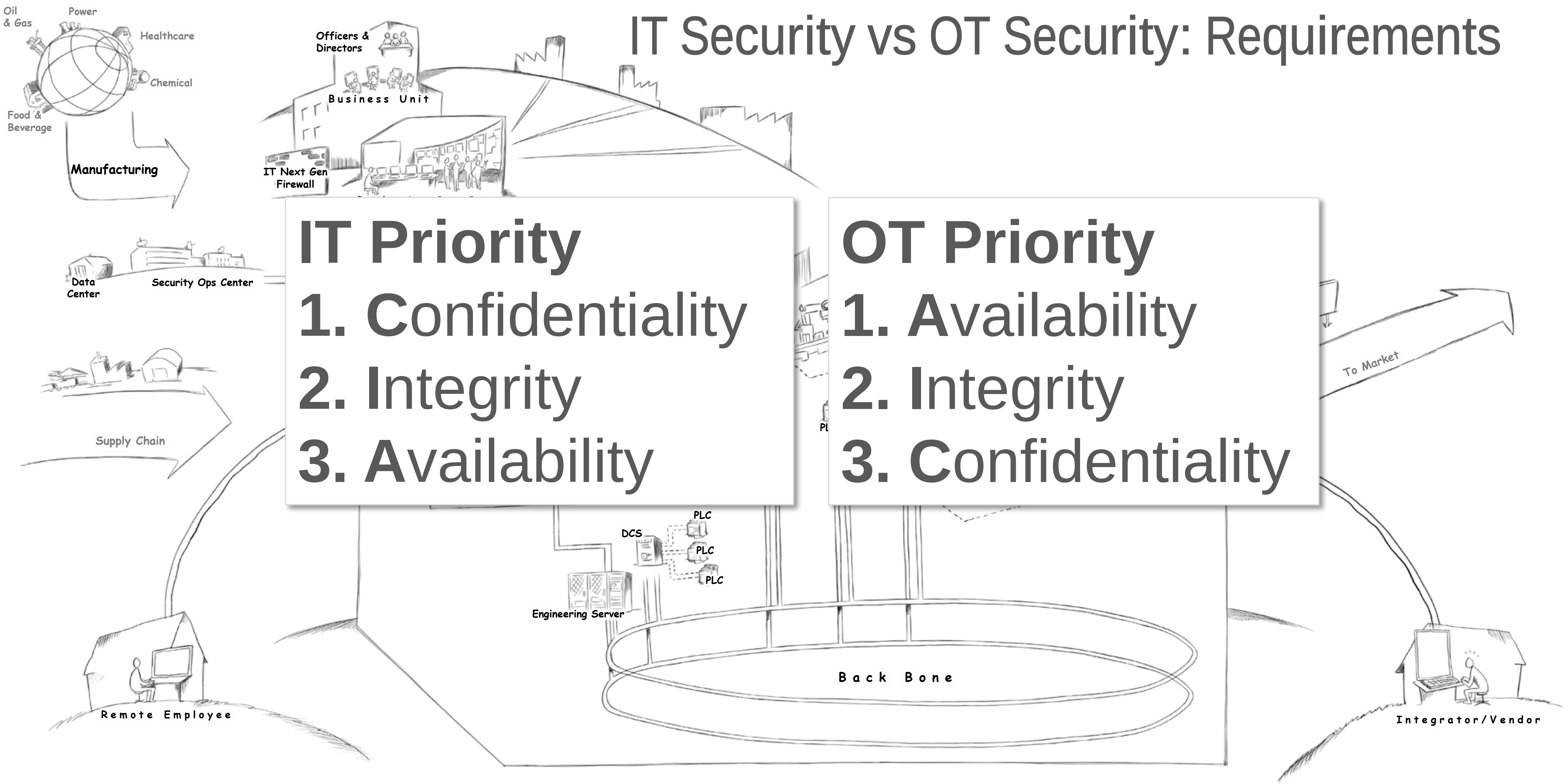
Different (Wider?) ATTACK SURFACE

IT
Protect the Data

OT
Protect the Assets



IT Security vs OT Security: Requirements



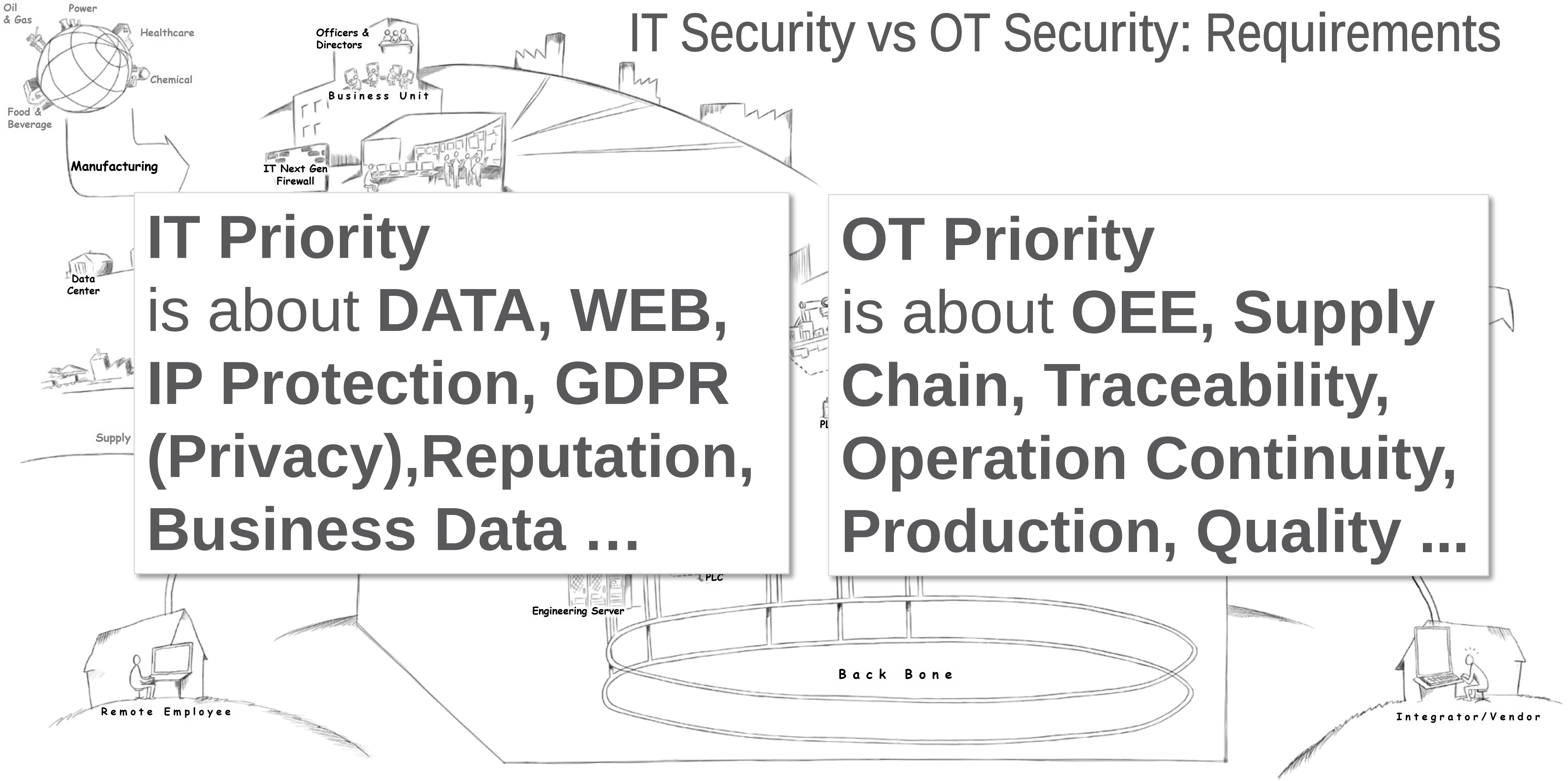
IT Priority

1. Confidentiality
2. Integrity
3. Availability

OT Priority

1. Availability
2. Integrity
3. Confidentiality

IT Security vs OT Security: Requirements

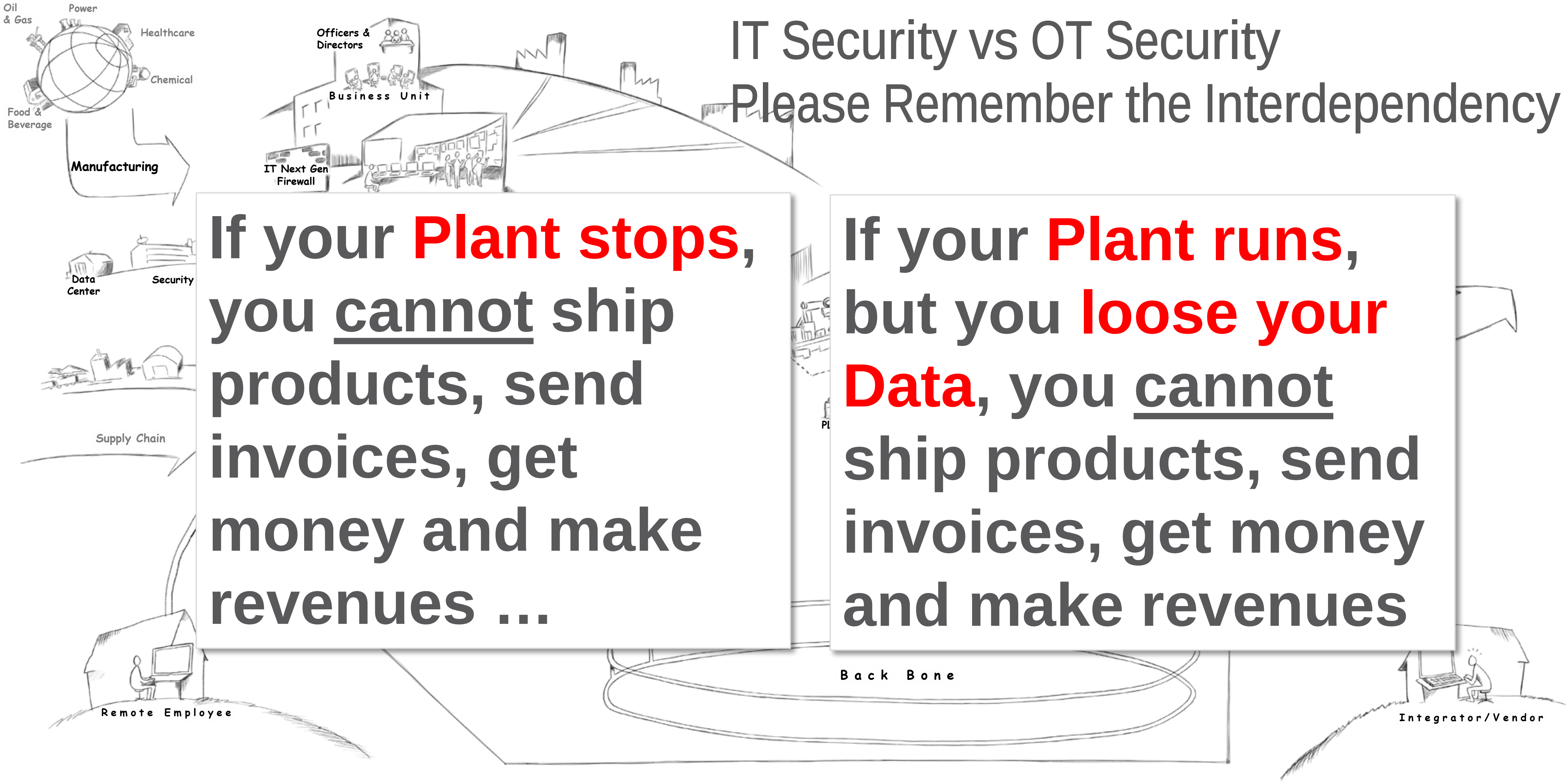


IT Priority
is about **DATA, WEB, IP Protection, GDPR (Privacy),Reputation, Business Data …**

OT Priority
is about **OEE, Supply Chain, Traceability, Operation Continuity, Production, Quality ...**

ISPE

IT Security vs OT Security
Please Remember the Interdependency

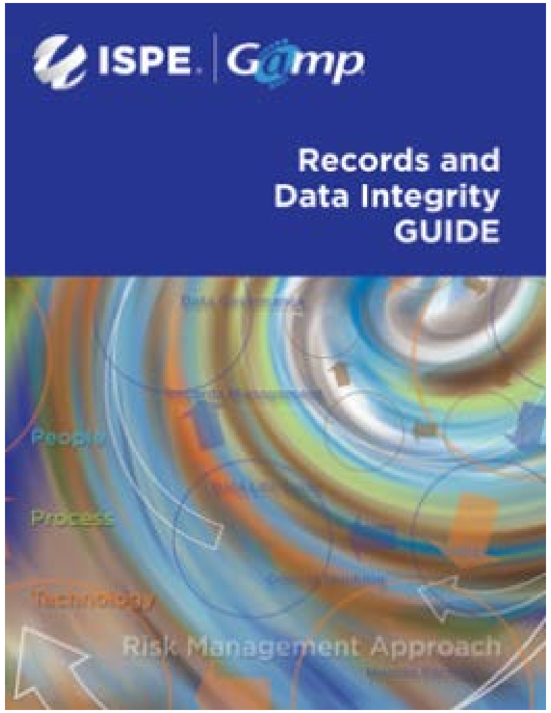


If your **Plant stops**, you <u>cannot</u> ship products, send invoices, get money and make revenues …

If your **Plant runs**, but you **loose your Data**, you <u>cannot</u> ship products, send invoices, get money and make revenues

ISPE

Talking about DATA means “Data Integrity”: most of ALCOA+ means “Think about Security”



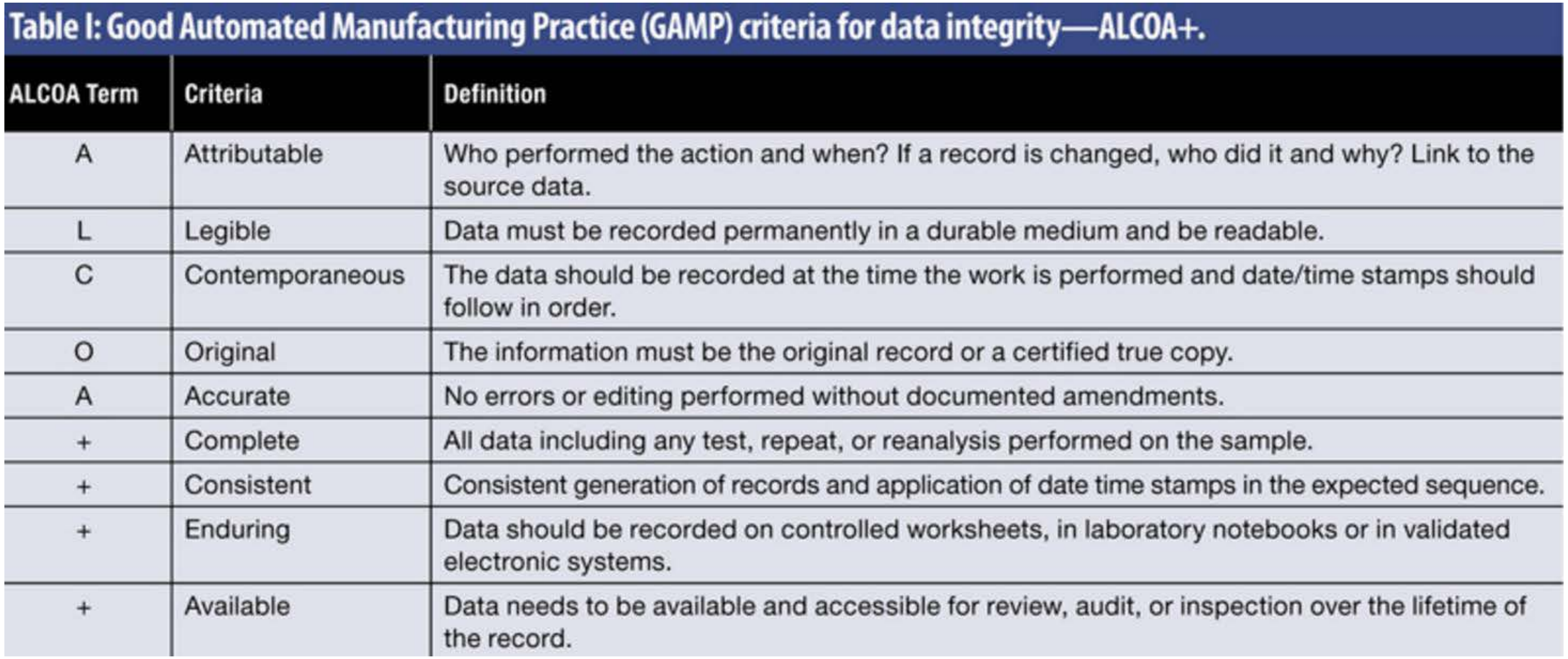
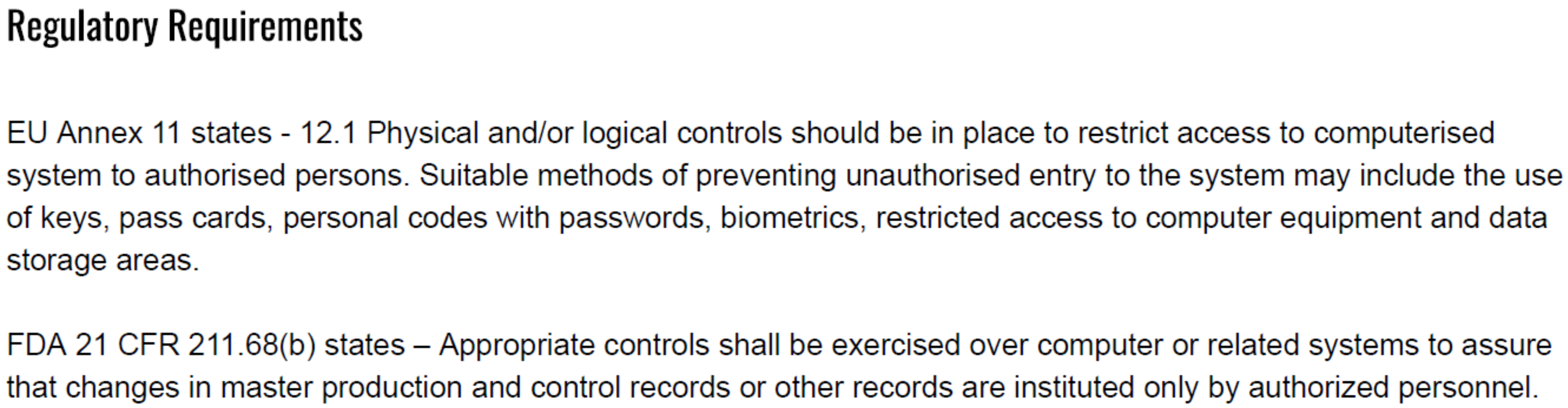


Table I: Good Automated Manufacturing Practice (GAMP) criteria for data integrity—ALCOA+.

ALCOA Term	Criteria	Definition
A	Attributable	Who performed the action and when? If a record is changed, who did it and why? Link to the source data.
L	Legible	Data must be recorded permanently in a durable medium and be readable.
C	Contemporaneous	The data should be recorded at the time the work is performed and date/time stamps should follow in order.
O	Original	The information must be the original record or a certified true copy.
A	Accurate	No errors or editing performed without documented amendments.
+	Complete	All data including any test, repeat, or reanalysis performed on the sample.
+	Consistent	Consistent generation of records and application of date time stamps in the expected sequence.
+	Enduring	Data should be recorded on controlled worksheets, in laboratory notebooks or in validated electronic systems.
+	Available	Data needs to be available and accessible for review, audit, or inspection over the lifetime of the record.

Security is not (only) “Access Control”

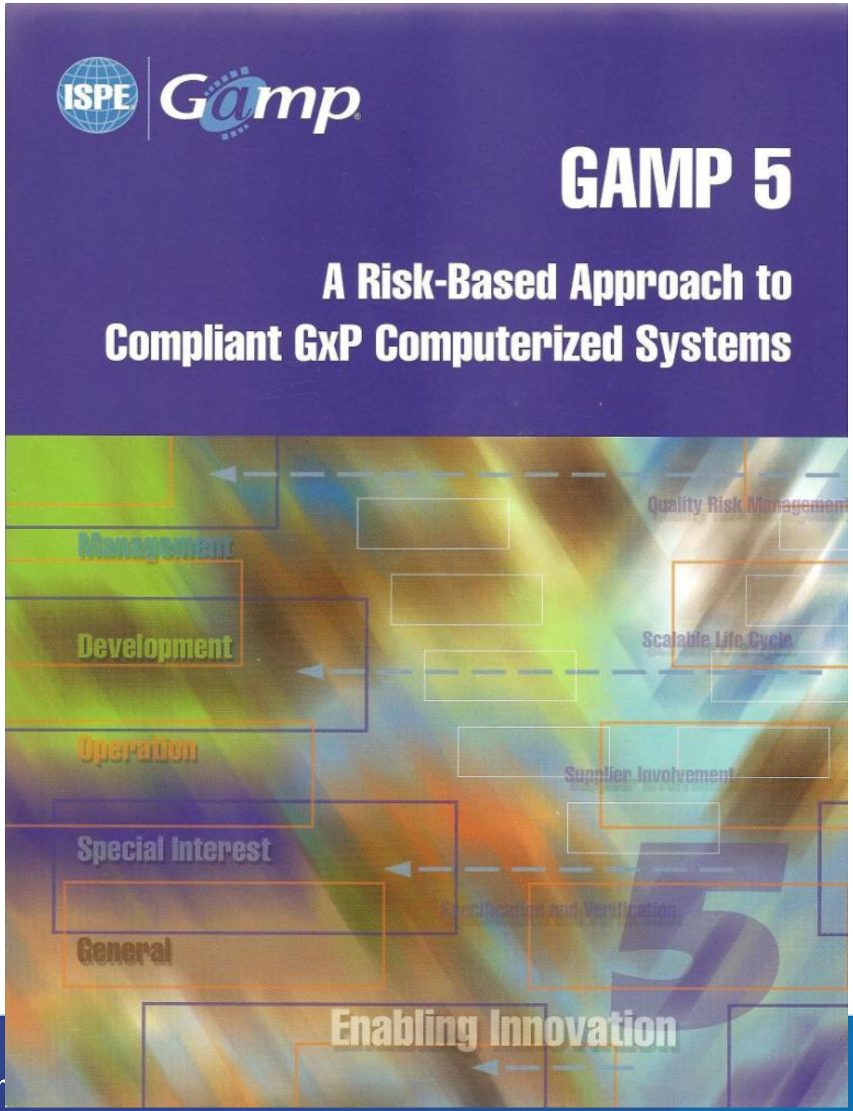


Regulatory Requirements

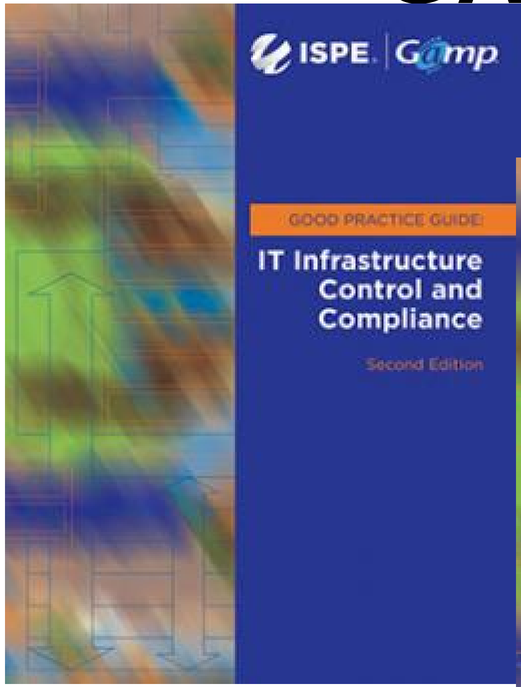
EU Annex 11 states - 12.1 Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.

FDA 21 CFR 211.68(b) states – Appropriate controls shall be exercised over computer or related systems to assure that changes in master production and control records or other records are instituted only by authorized personnel.

GAMP® 5 and Security: A Risk-Based Approach to Compliant GxP Computerized Systems



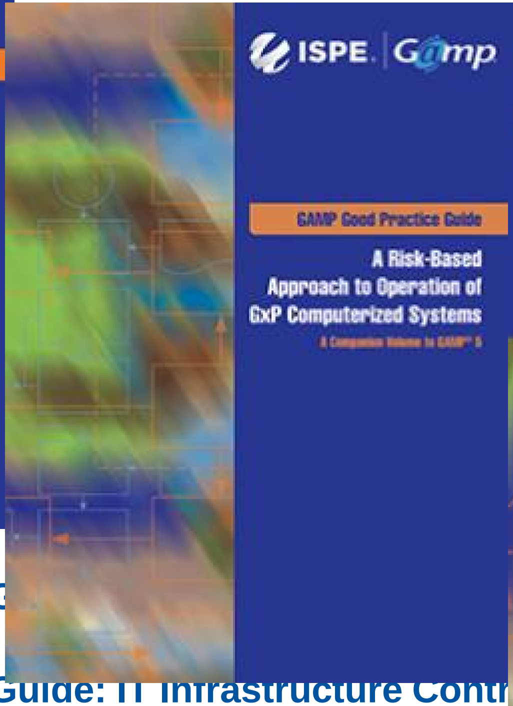
GAMP® Good Practice Guides, and Security


ISPE | Gamp

GOOD PRACTICE GUIDE

IT Infrastructure Control and Compliance

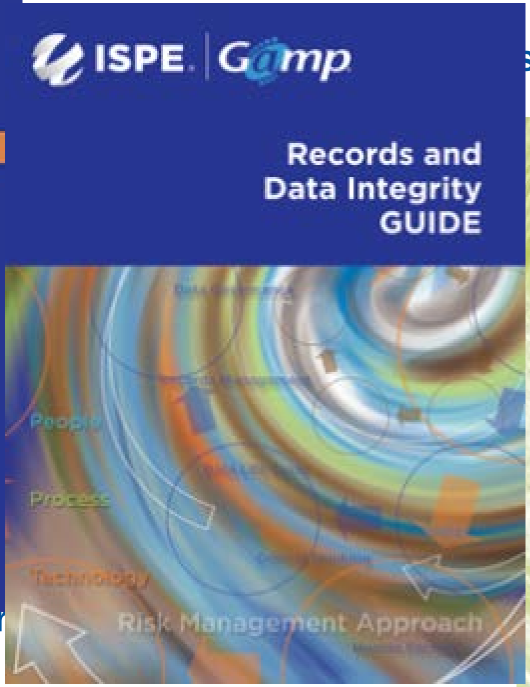
Second Edition


ISPE | Gamp

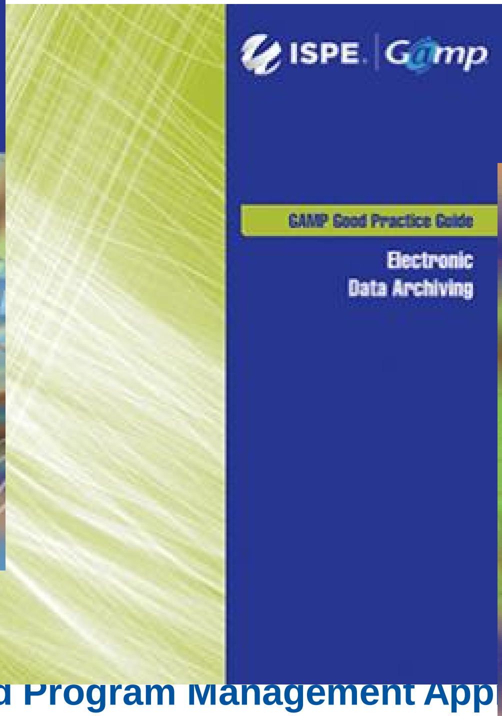
GAMP Good Practice Guide

A Risk-Based Approach to Operation of GxP Computerized Systems

A Companion Volume to GAMP® 5


ISPE | Gamp

Records and Data Integrity GUIDE


ISPE | Gamp

GAMP Good Practice Guide

Electronic Data Archiving

ISPE | Gamp

GAMP Good Practice Guide

A Risk-Based Approach to GxP Process Control Systems

Second Edition

uide: A Risk-Based Approach to Electronic Records and Signatures

to GxP Compliant Laboratory Computerized Systems (Second Edition)

stems (Second Edition)

ion Volume to GAMP 5

GAMP® Good Practice G

GAMP® Good Practice Guide: IT Infrastructure Contr

GAMP® Good Practice Guide: Legacy Systems

GAMP® Good Practice Guide: Manufacturing Execution Systems – A Strategic and Program Management App

GAMP® 5: Table of Appendices

Security Management

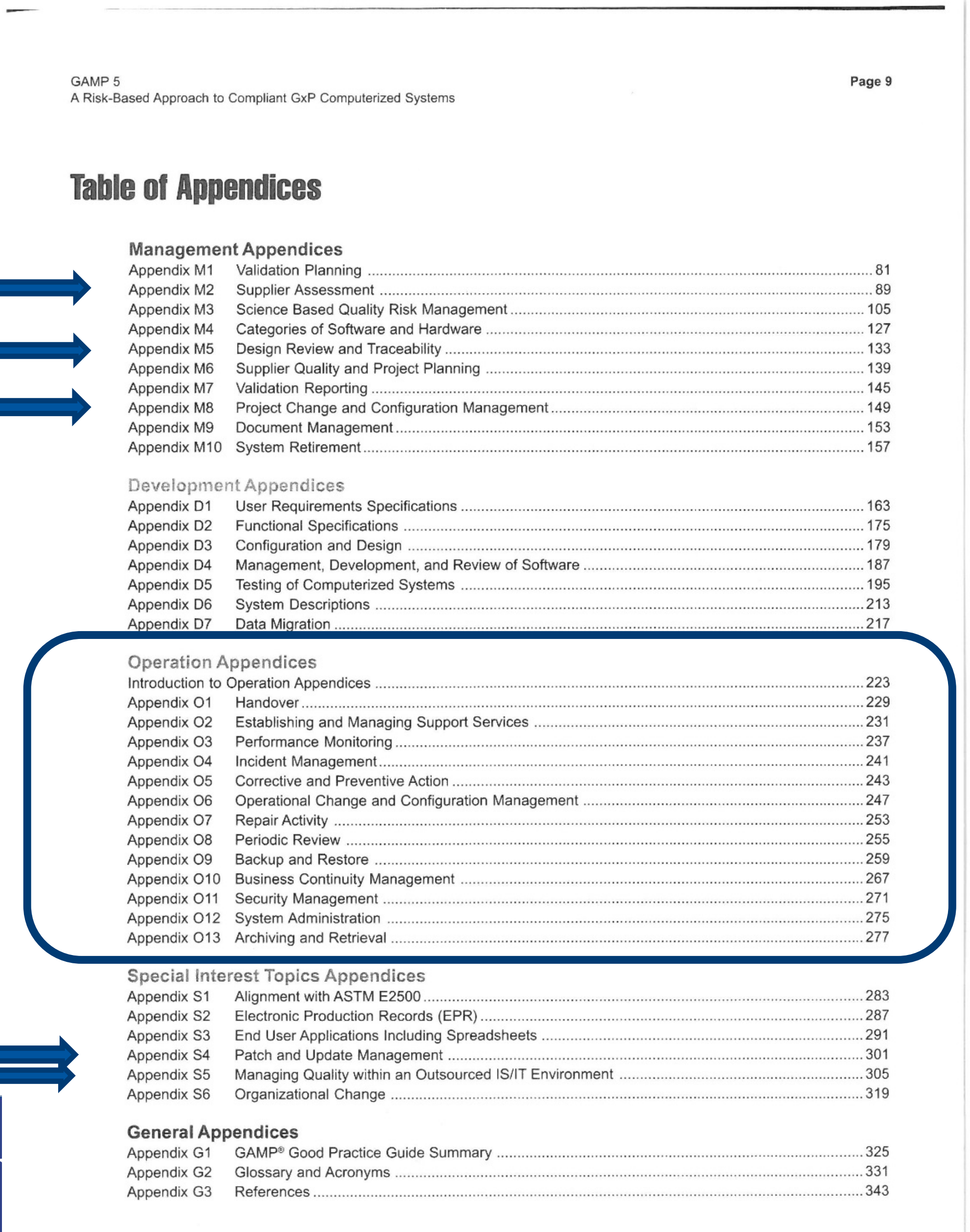


Table of Appendices

Management Appendices

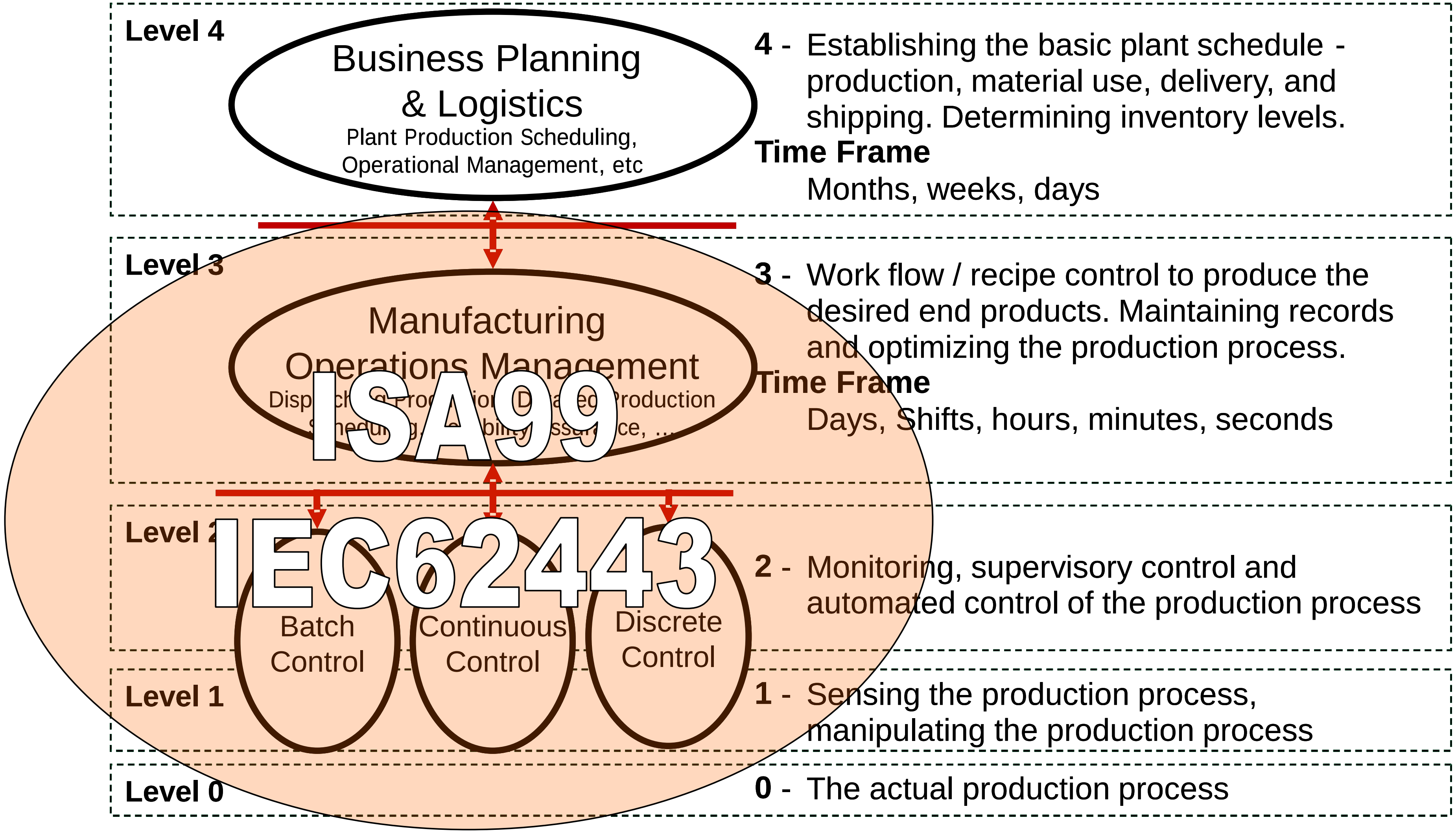
Development Appendices

Operation Appendices

Special Interest Topics Appendices

General Appendices

ANSI/ISA95 Functional Hierarchy: ISA99/IEC62443, IT vs OT Security


Level 4
Business Planning & Logistics
Plant Production Scheduling, Operational Management, etc
Level 3
Manufacturing Operations Management
Dispatching Production, Detailed Production Scheduling, Reliability Assurance, ...
ISA99
Level 2
IEC62443
Batch Control
Continuous Control
Discrete Control
Level 1
Level 0

4 - Establishing the basic plant schedule - production, material use, delivery, and shipping. Determining inventory levels.

Time Frame

Months, weeks, days

3 - Work flow / recipe control to produce the desired end products. Maintaining records and optimizing the production process.

Time Frame

Days, Shifts, hours, minutes, seconds

2 - Monitoring, supervisory control and automated control of the production process

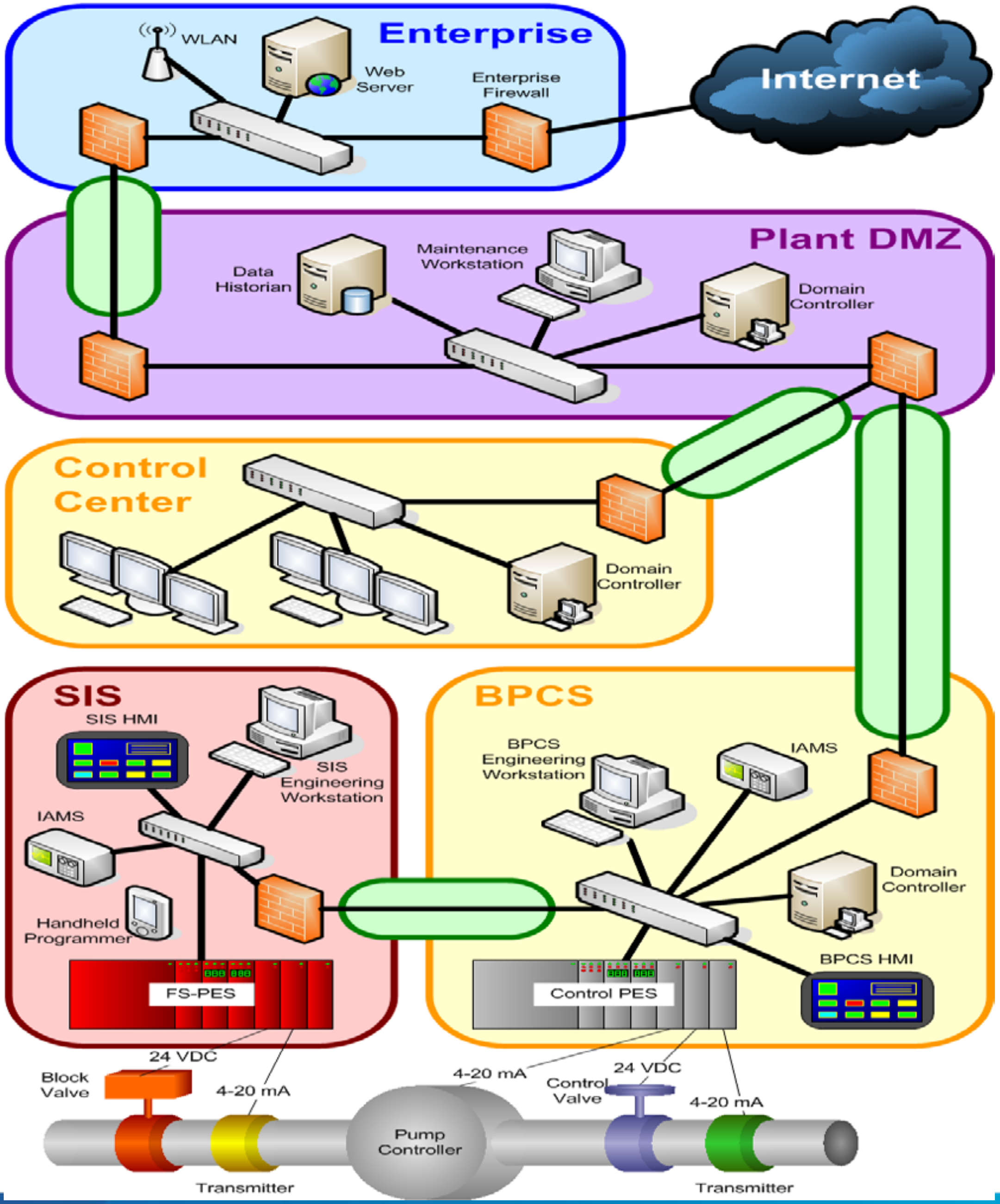
1 - Sensing the production process, manipulating the production process

0 - The actual production process

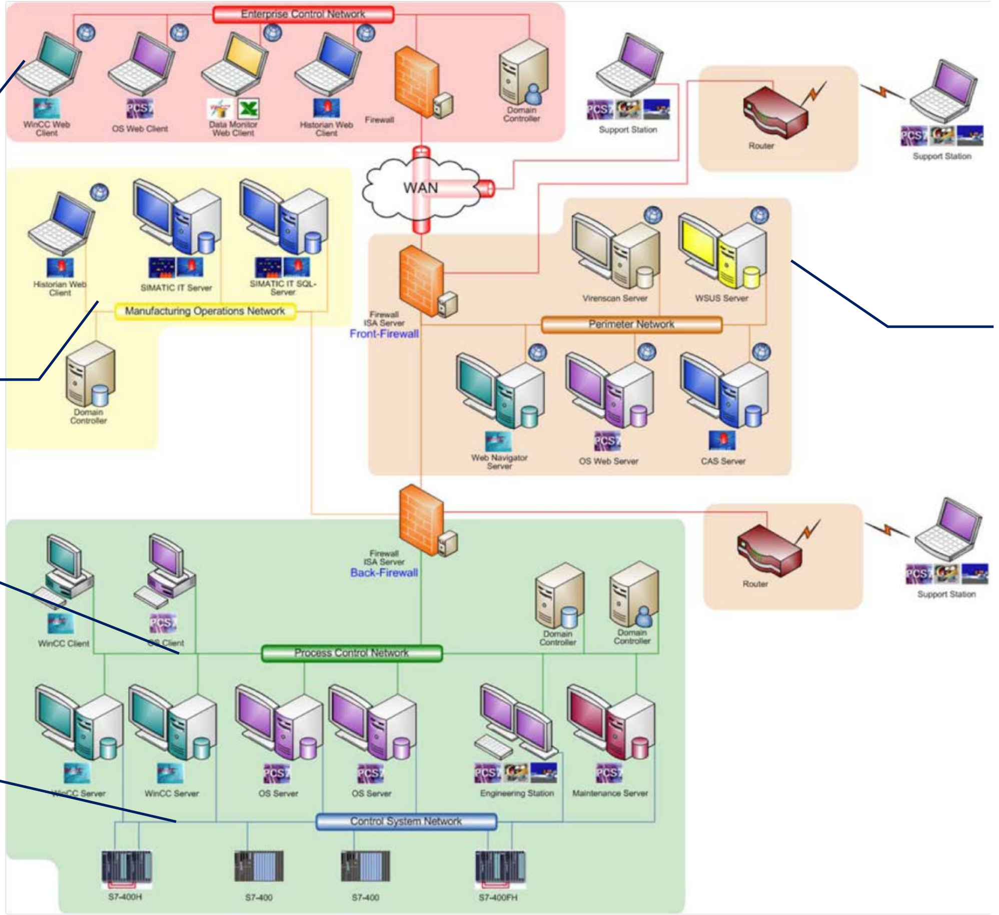
Network/System Segmentation using ISA99/IEC62443

- **Limit the ingress and egress points through Zone boundaries**
- **Protect the connections between Zones**
- **Zones & Conduits are logical**

For practical purposes, match Zones to network architecture as much as possible



Esempio di “Security Architecture” nei sistemi di automazione e controllo



Enterprise Control Network

Manufacturing Operations Network

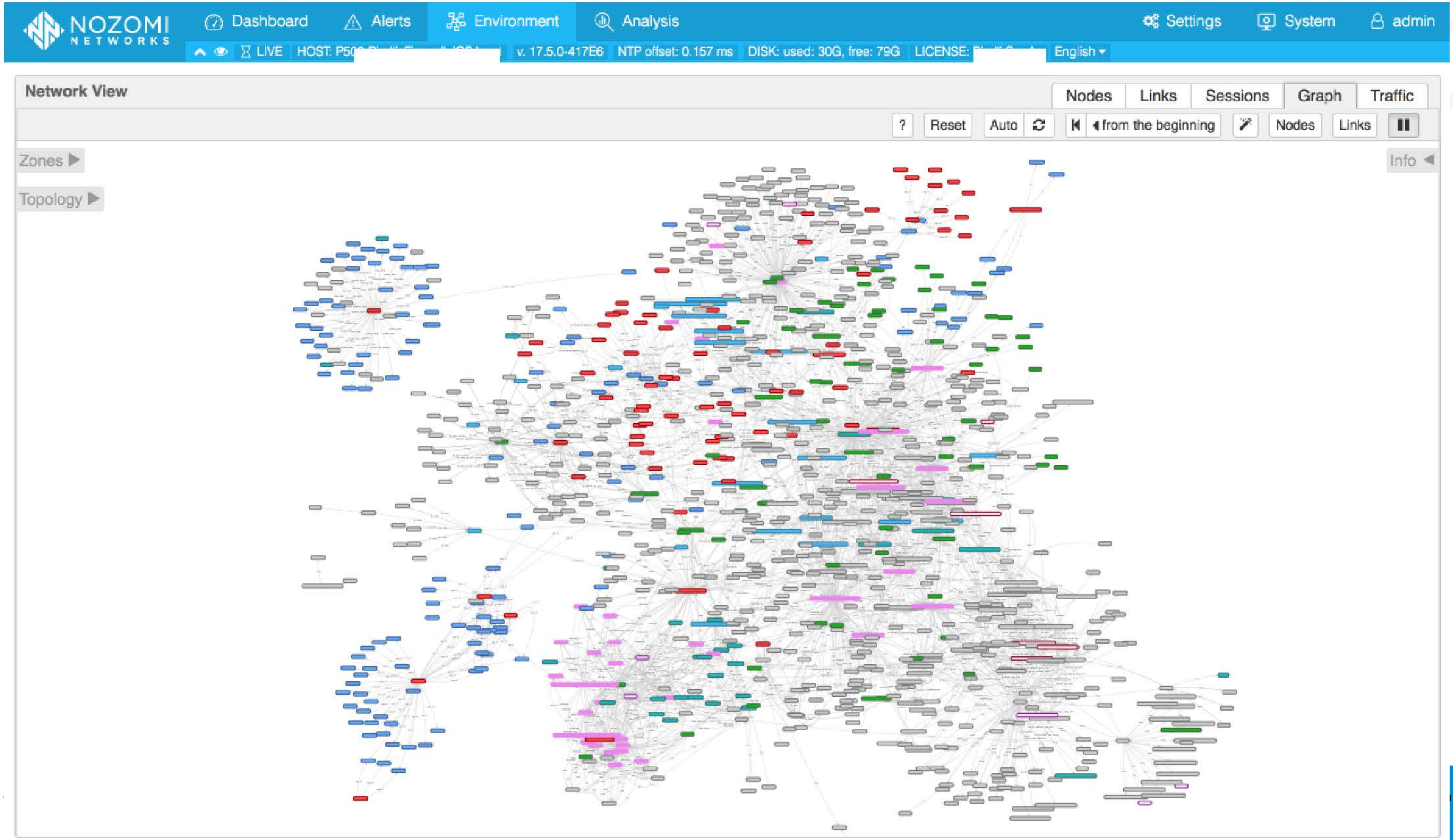
Process Control Network

Control System Network

Perimeter Control Network

Use Case 1: Network Visualization and Monitoring

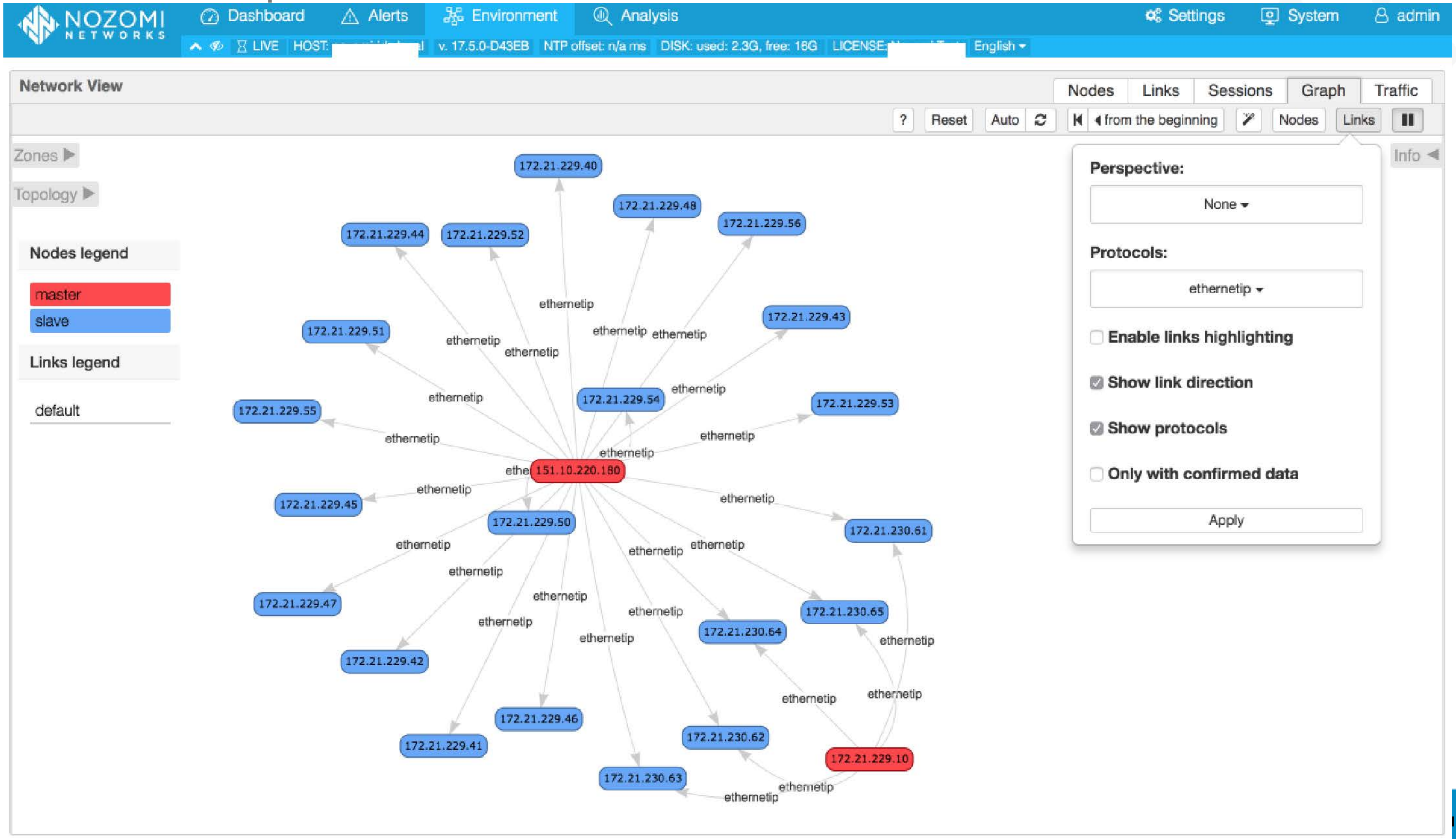
From a ”tangled” situation …



LIVE HOST: P50[redacted] v. 17.5.0-417E6 NTP offset: 0.157 ms DISK: used: 30G, free: 79G LICENSE: [redacted] English

Use Case 1: Network Visualization and Monitoring

....with two clicks the operator can filter the communications of interest …



HOST: [redacted] v. 17.5.0-D43EB NTP offset: n/a ms DISK: used: 2.3G, free: 16G LICENSE: [redacted]

Perspective: None

Protocols: ethernetip

☐ Enable links highlighting

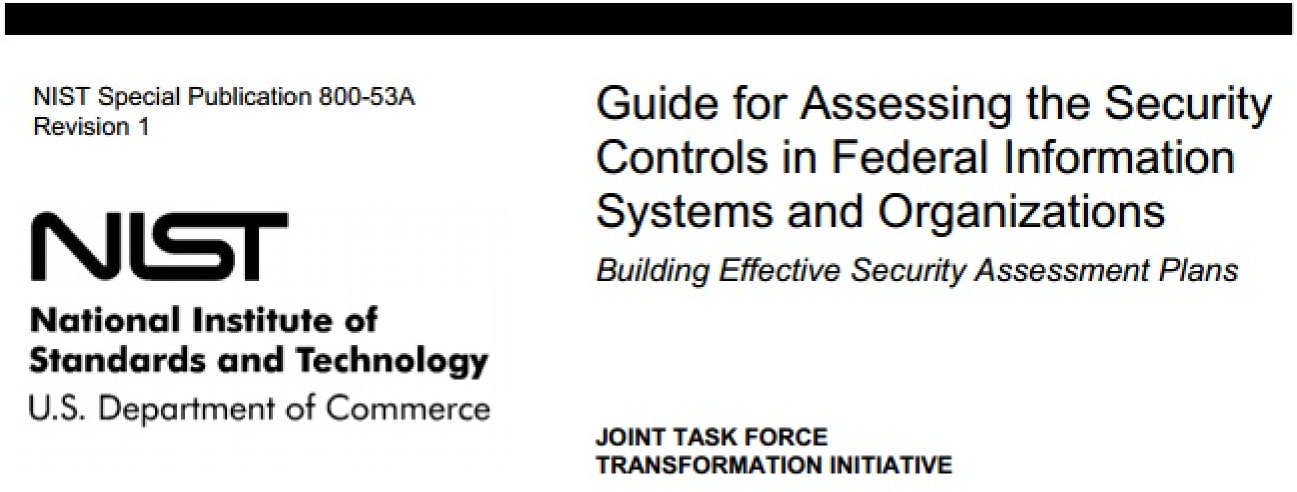
☑ Show link direction

☑ Show protocols

☐ Only with confirmed data

Apply

NIST: SP800-53, SP800-82, SP800-144, SP800-183



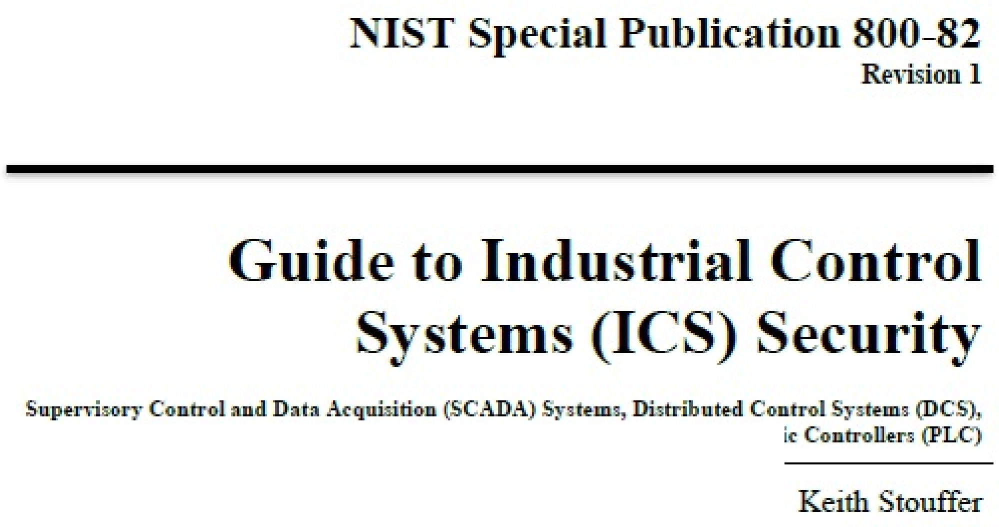
NIST Special Publication 800-53A
Revision 1

National Institute of Standards and Technology
U.S. Department of Commerce

Guide for Assessing the Security Controls in Federal Information Systems and Organizations

Building Effective Security Assessment Plans

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

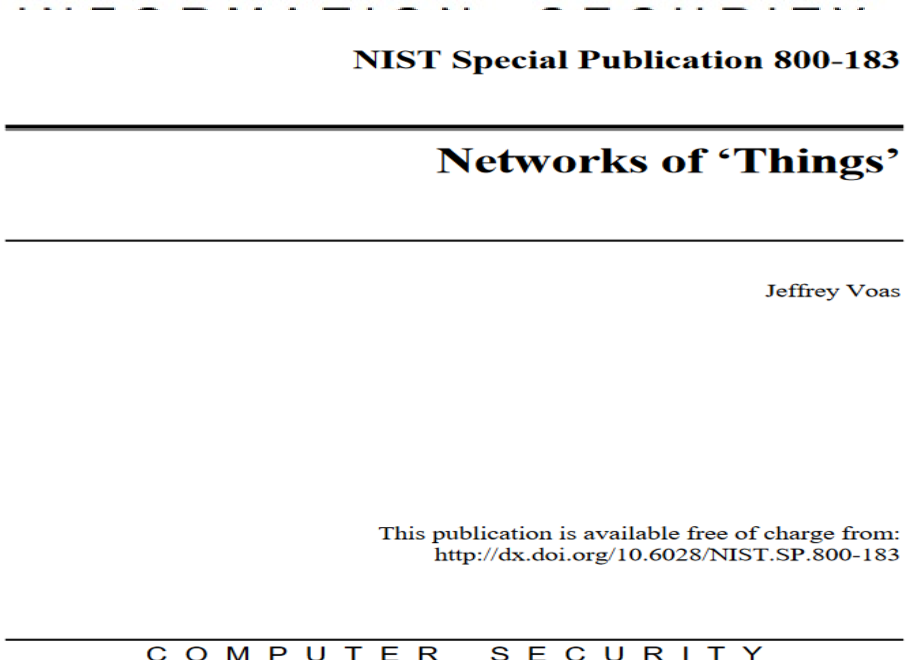


NIST Special Publication 800-82
Revision 1

Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS),
ic Controllers (PLC)

Keith Stouffer
Joe Falco
Karen Scarfone



INFORMATION SECURITY

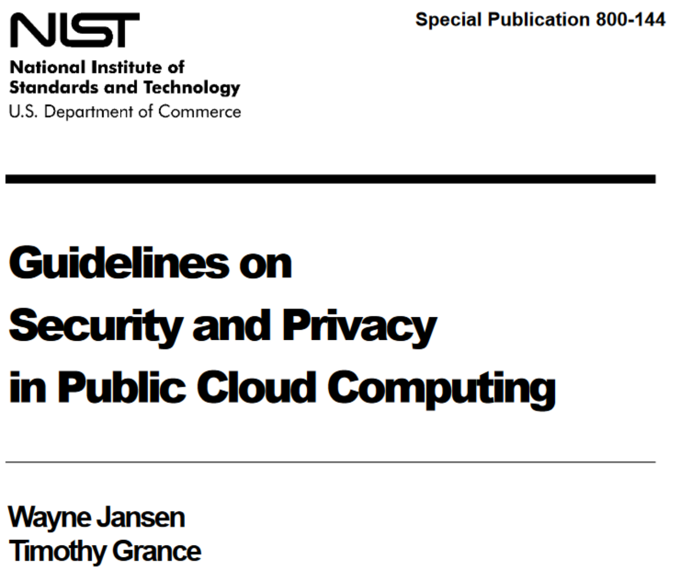
NIST Special Publication 800-183

Networks of 'Things'

Jeffrey Voas

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-183

COMPUTER SECURITY



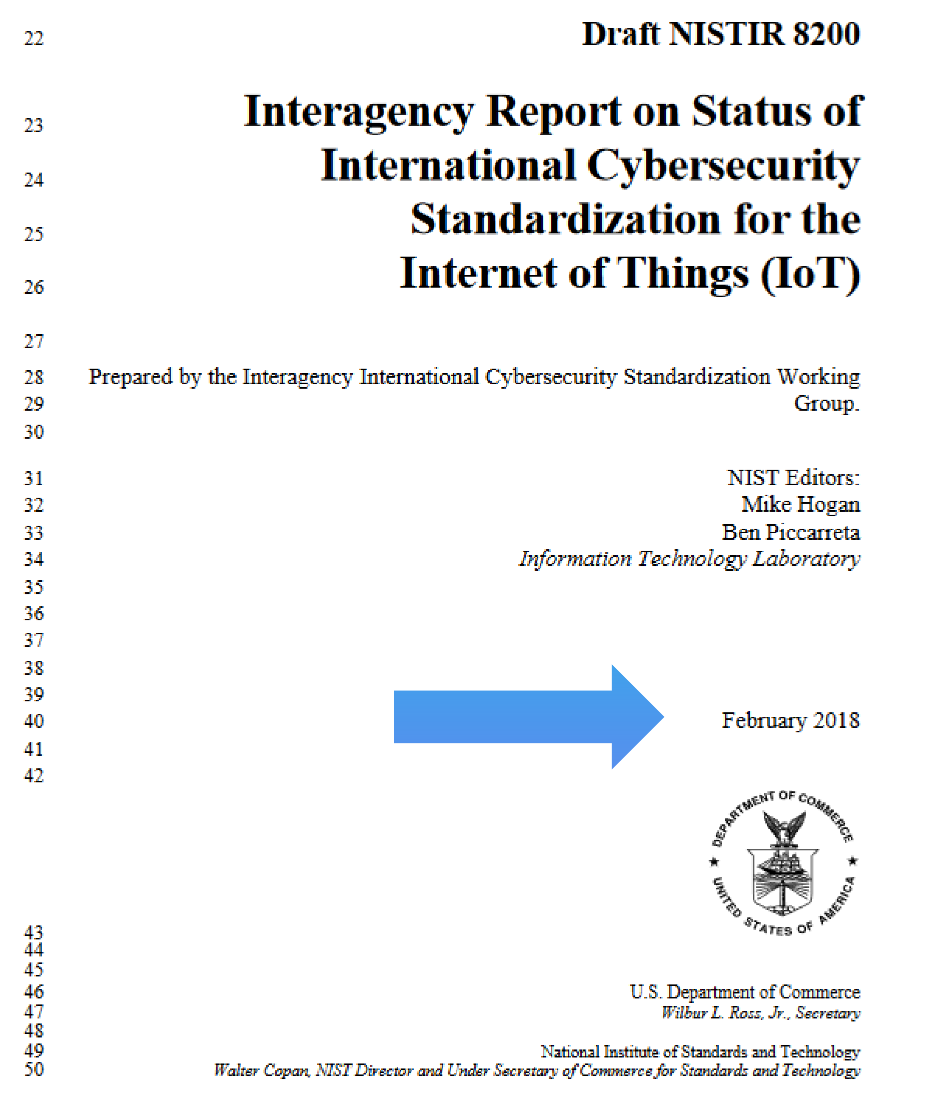
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-144

Guidelines on Security and Privacy in Public Cloud Computing

Wayne Jansen
Timothy Grance

Which standard for IoT Cybersecurity?



Draft NISTIR 8200

Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)

Prepared by the Interagency International Cybersecurity Standardization Working Group.

NIST Editors:
Mike Hogan
Ben Piccarreta
Information Technology Laboratory

February 2018

DEPARTMENT OF COMMERCE ★ UNITED STATES OF AMERICA ★

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

NISTIR 8200 (Draft): Security vs. Privacy

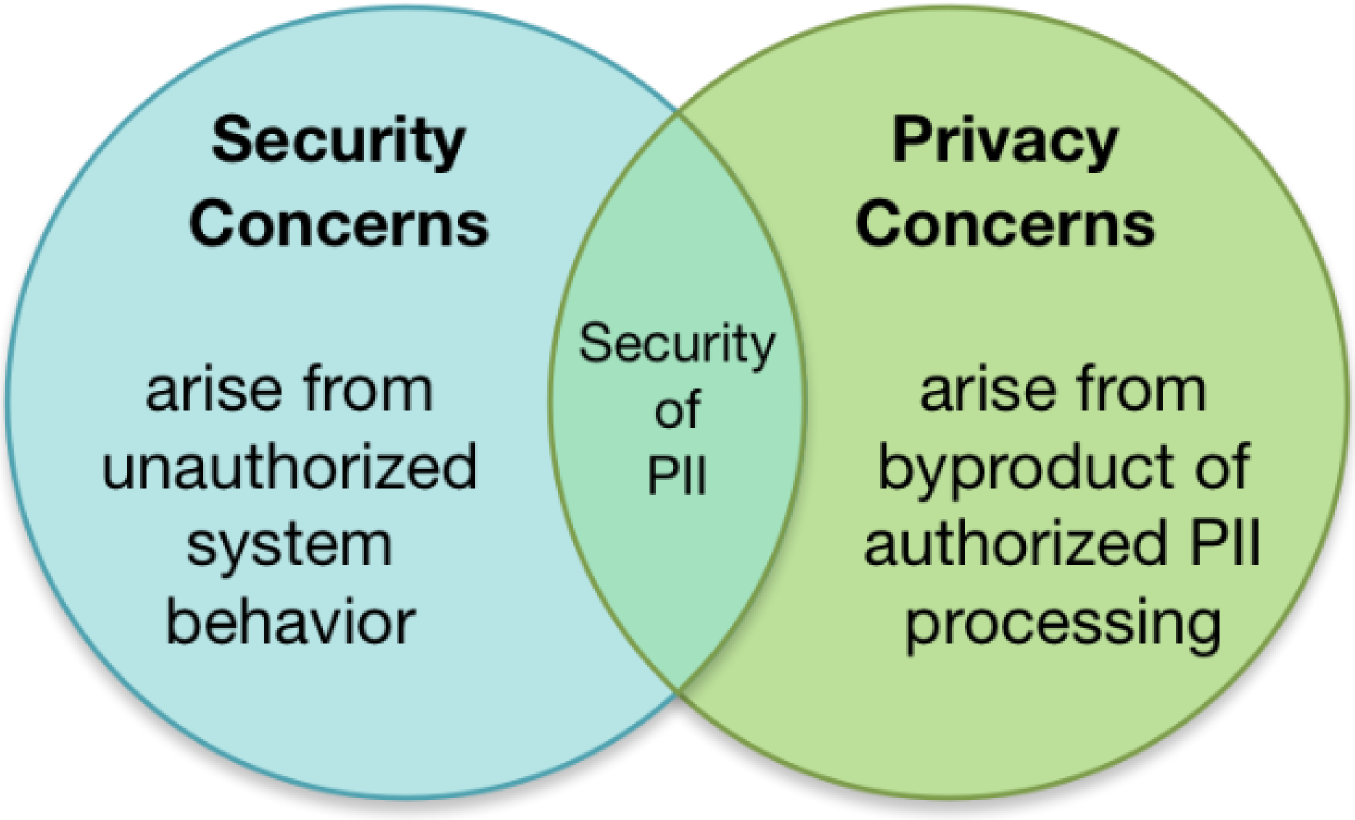

Security Concerns
arise from unauthorized system behavior
Security of PII
Privacy Concerns
arise from byproduct of authorized PII processing

Figure 2: Relationship Between Information Security and Privacy

(* PII: Personally Identifiable Information)

NISTIR 8200 (Draft): Capabilities of an IoT Component

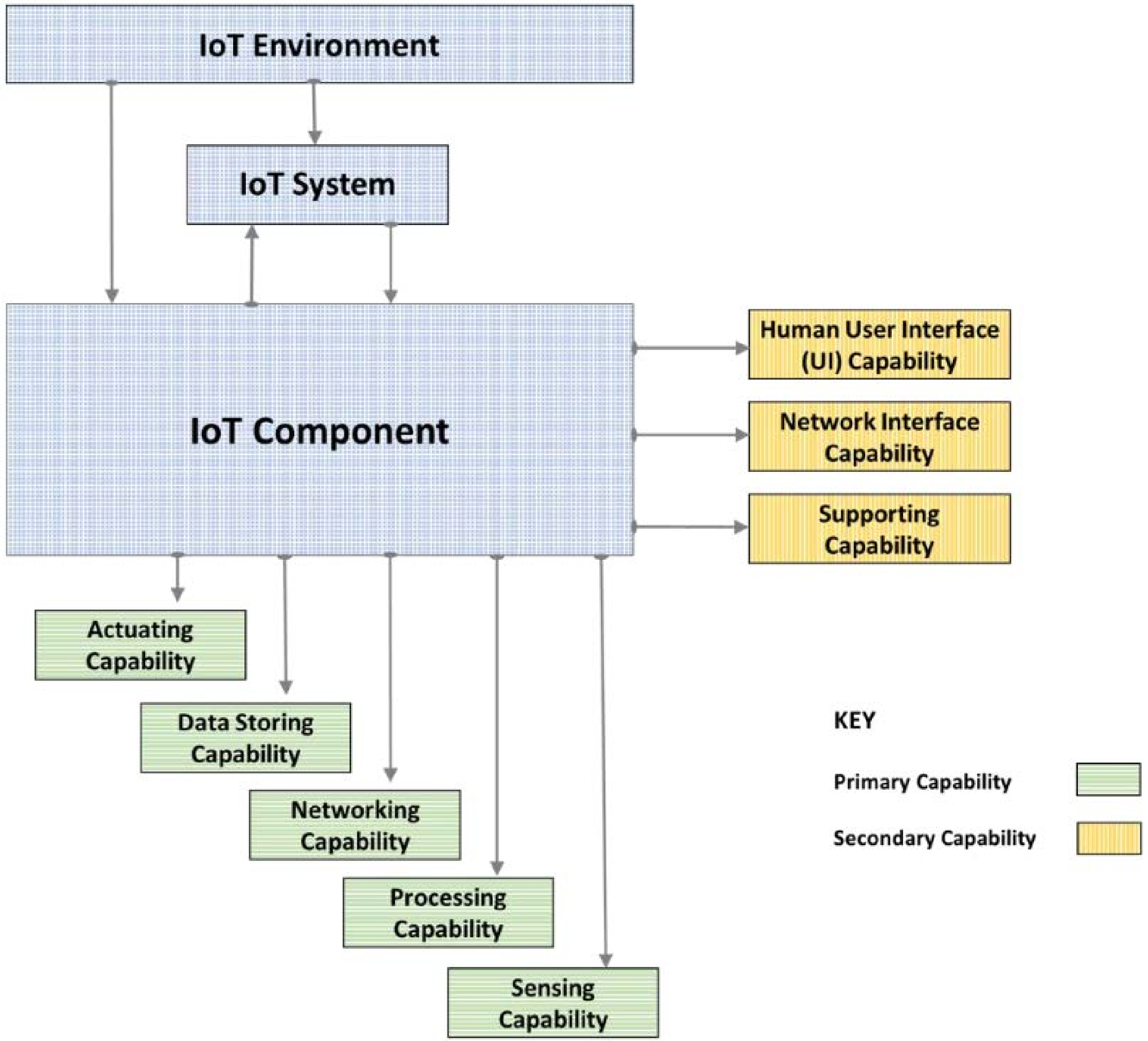
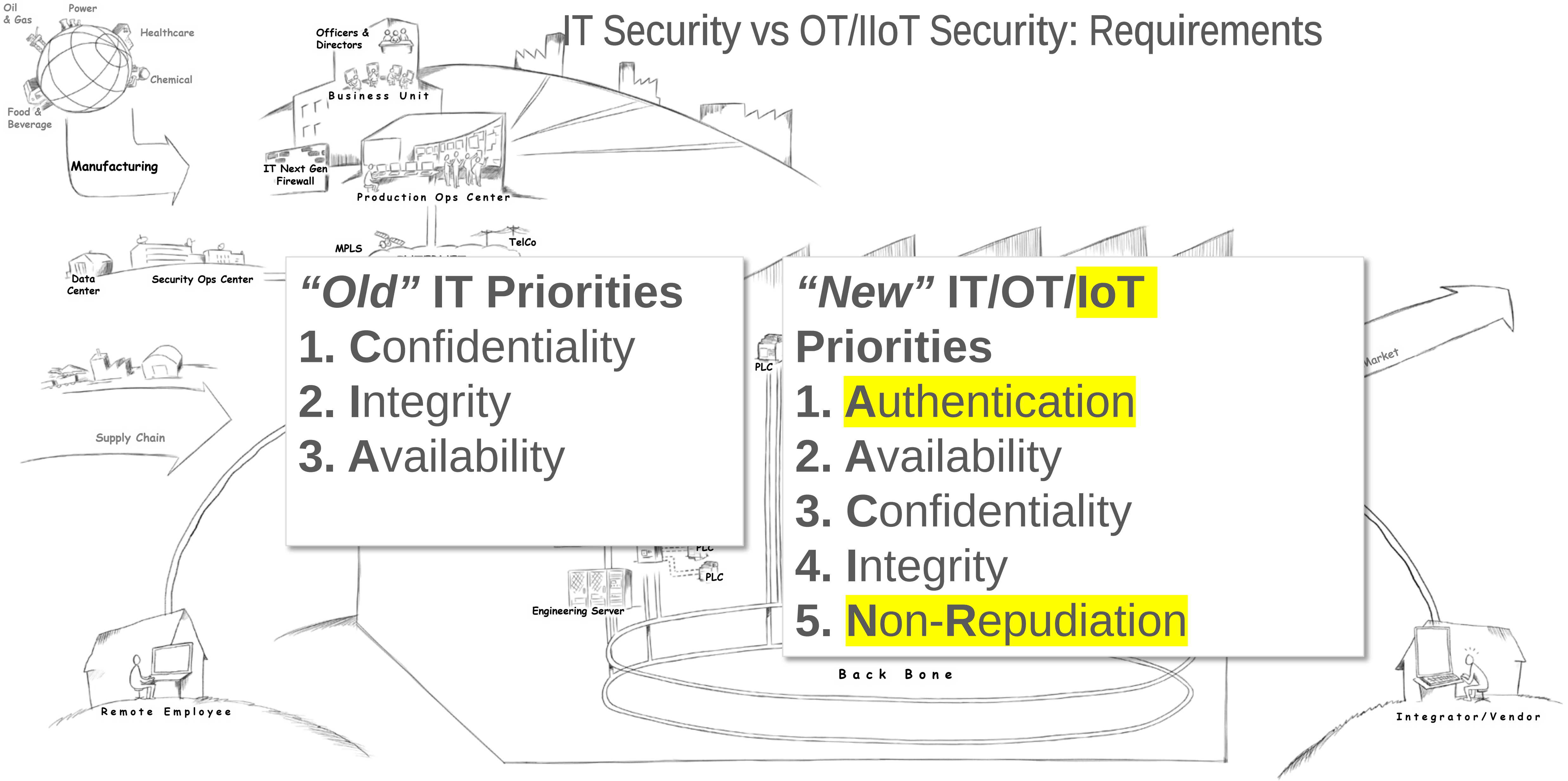


Figure 2 – Capabilities of an IoT Component.

IT Security vs OT/IIoT Security: Requirements



“Old” IT Priorities

1. Confidentiality
2. Integrity
3. Availability

“New” IT/OT/IoT Priorities

1. Authentication
2. Availability
3. Confidentiality
4. Integrity
5. Non-Repudiation

NISTIR 8200 (Draft): Health IoT Example (Precision Medicine)

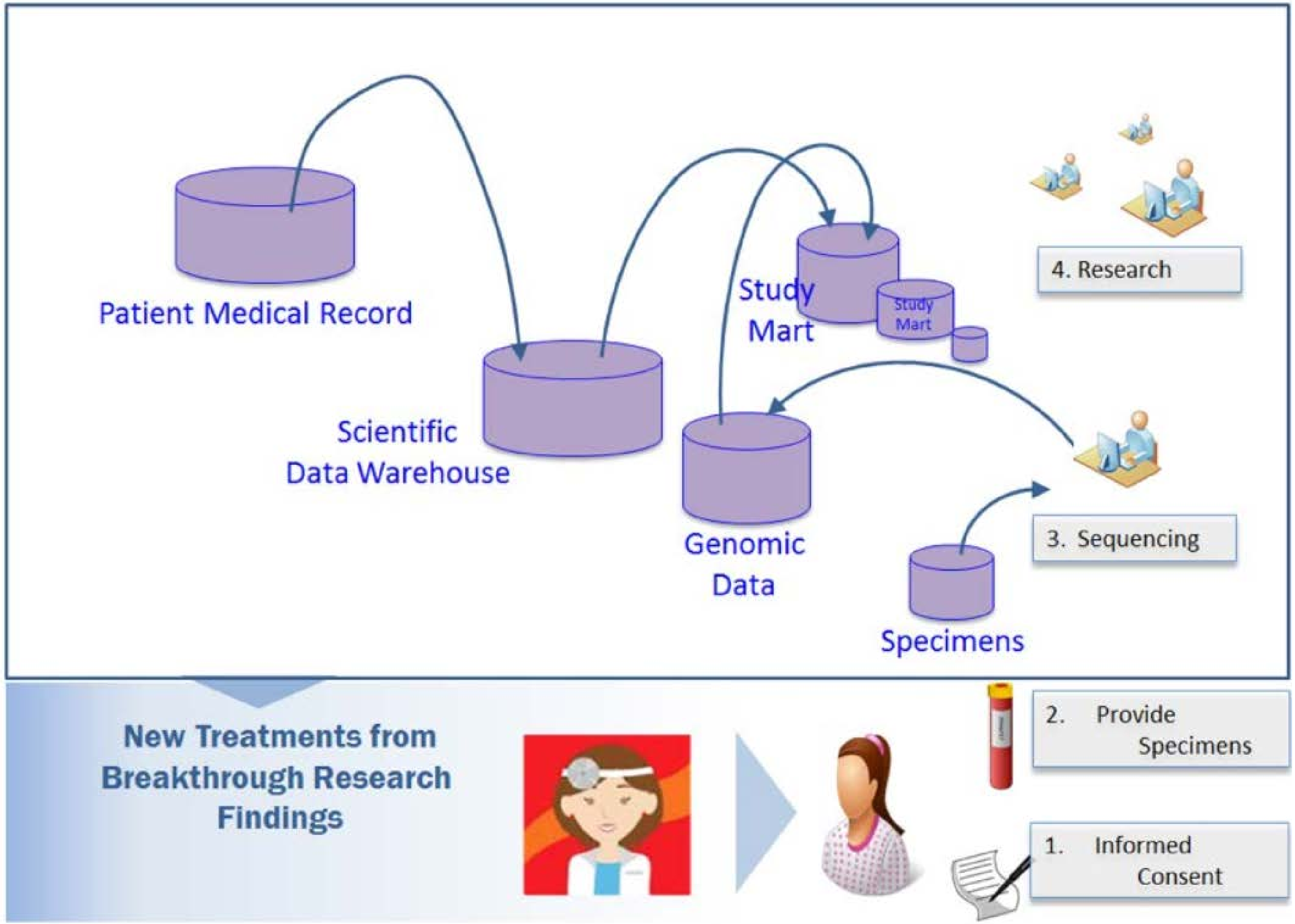


Figure 6 – Precision Medicine Research Case

NISTIR 8200 (Draft): Health IoT Example (Diabetes /Nutrition)

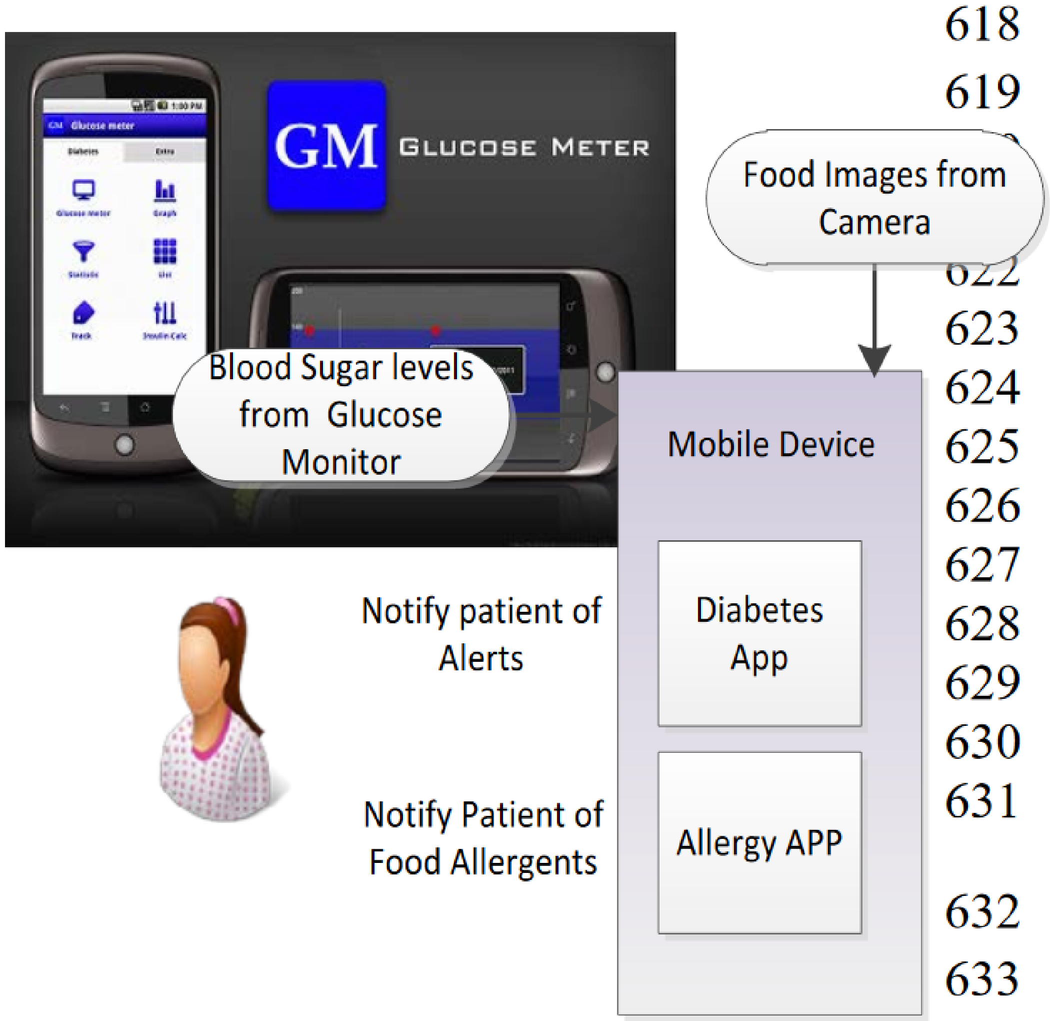


Figure 7 – Diabetes Treatment/Allergen Identification

NIST IR 8200 (Draft): Smart Building Example

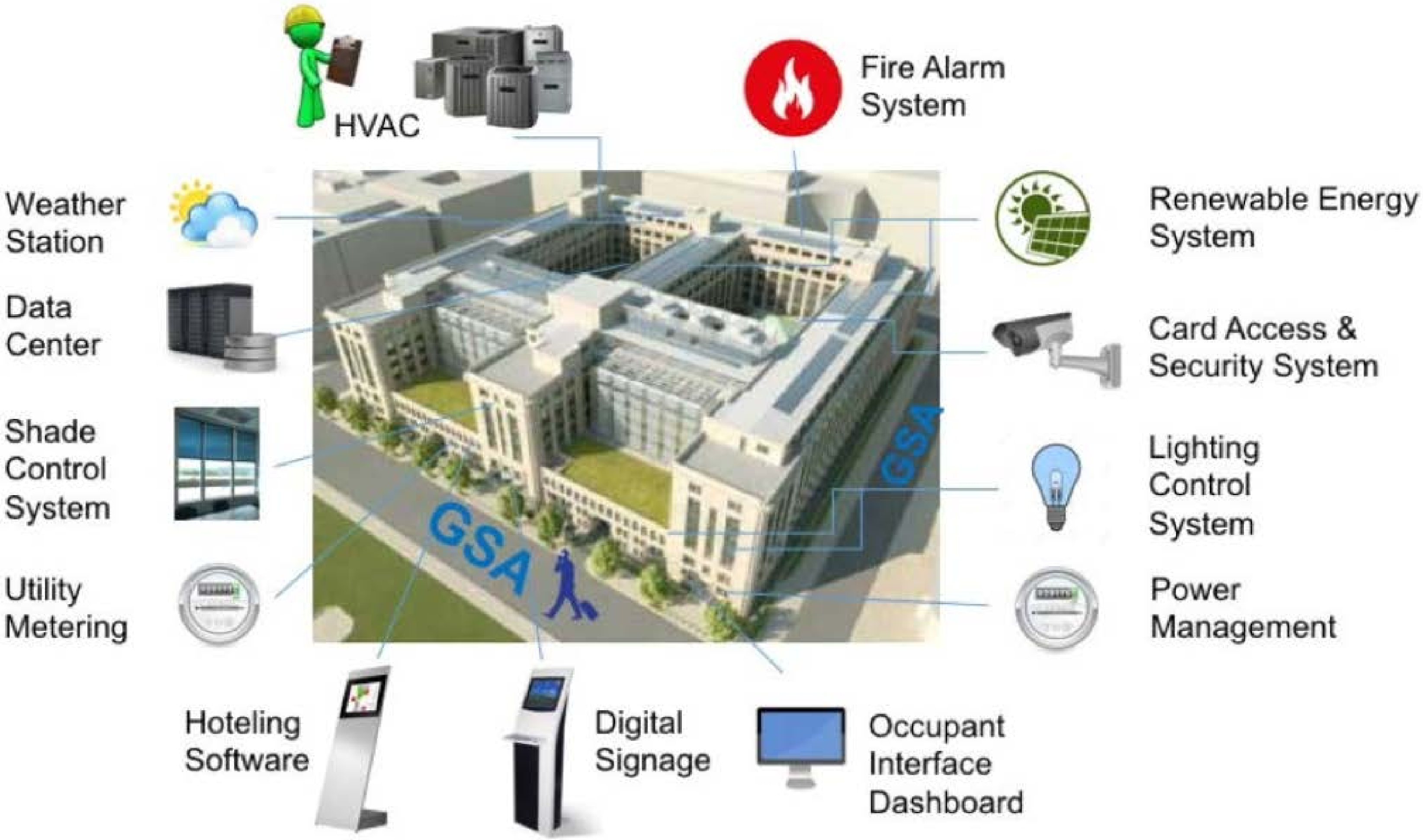


Figure 8 – IoT for the GSA Smart Building

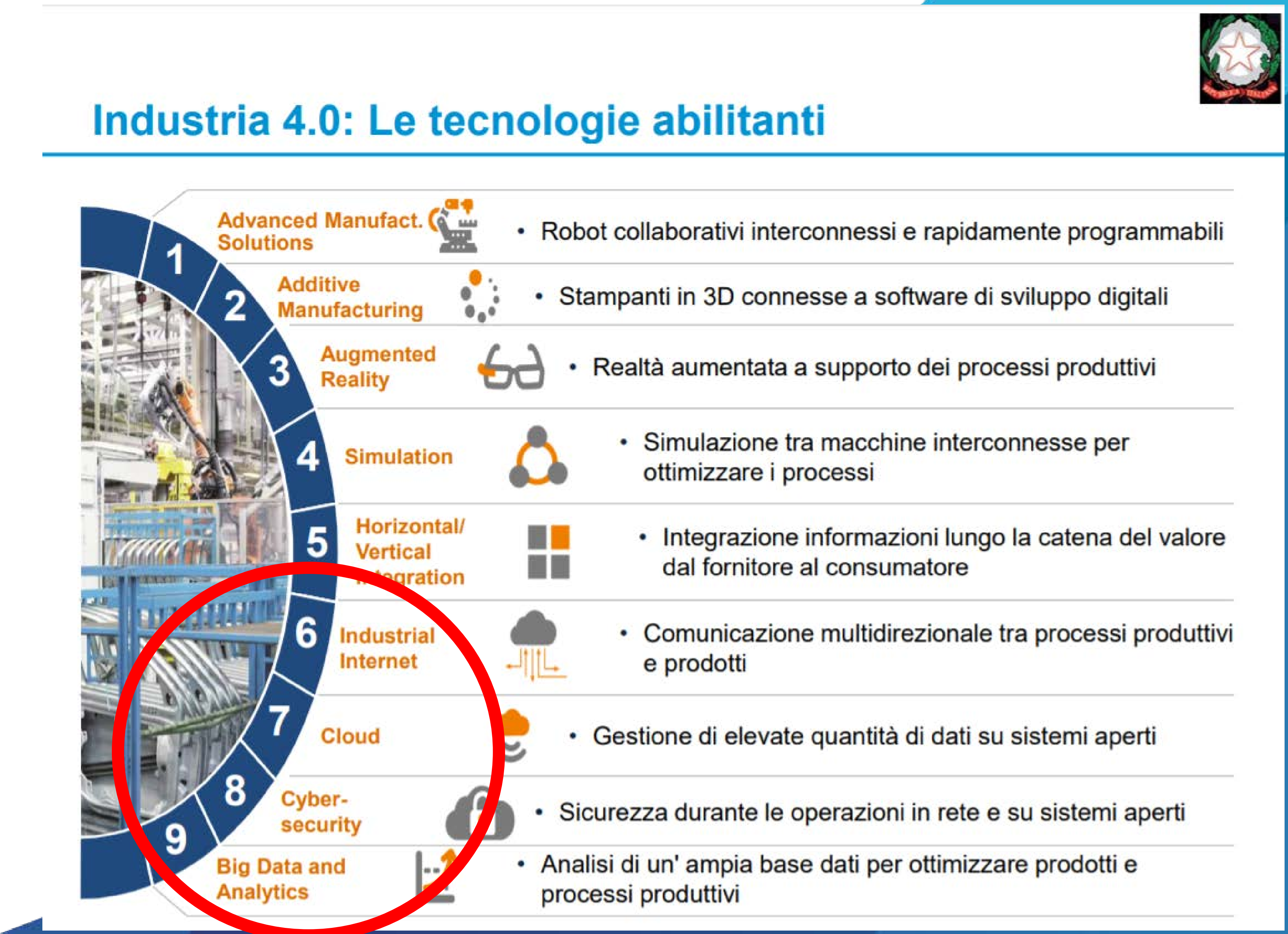
INDUSTRY4.0 & CYBER SECURITY

ISPE®

- **Industrial Internet**
- **Cloud**
- **Big Data, Analytics**
- **IoT, IIoT**
- **Digital Twins**

needs different protection approach

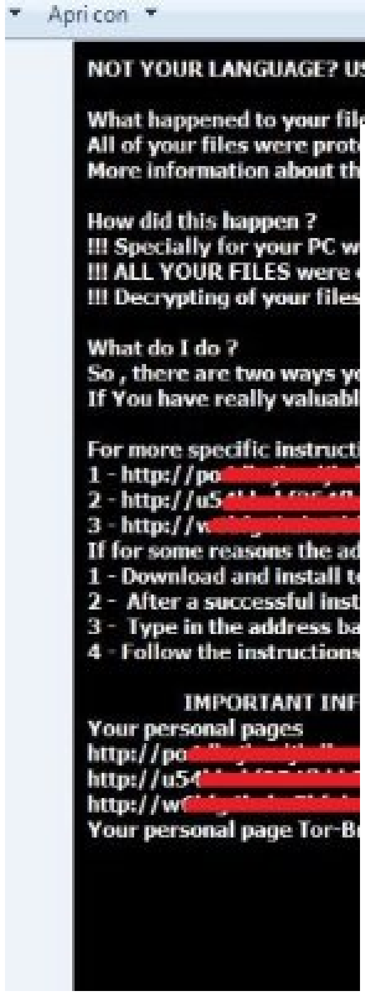
CSA cloud security alliance®



Industria 4.0: Le tecnologie abilitanti

1	Advanced Manufact. Solutions	• Robot collaborativi interconnessi e rapidamente programmabili
2	Additive Manufacturing	• Stampanti in 3D connesse a software di sviluppo digitali
3	Augmented Reality	• Realtà aumentata a supporto dei processi produttivi
4	Simulation	• Simulazione tra macchine interconnesse per ottimizzare i processi
5	Horizontal/ Vertical Integration	• Integrazione informazioni lungo la catena del valore dal fornitore al consumatore
6	Industrial Internet	• Comunicazione multidirezionale tra processi produttivi e prodotti
7	Cloud	• Gestione di elevate quantità di dati su sistemi aperti
8	Cyber-security	• Sicurezza durante le operazioni in rete e su sistemi aperti
9	Big Data and Analytics	• Analisi di un' ampia base dati per ottimizzare prodotti e processi produttivi

Which is the «real» THREAT today?



NOT YOUR LANGUAGE? USE https://translate.google.com

What happened to your files ?
All of your files were prot
More information about th

How did this happen ?
!!! Specially for your PC w
!!! ALL YOUR FILES were
!!! Decrypting of your files

What do I do ?
So , there are two ways y
If You have really valuabl

For more specific instructi
1 - http://po [redacted]
2 - http://u5 [redacted]
3 - http://w [redacted]
If for some reasons the ad
1 - Download and install t
2 - After a successful inst
3 - Type in the address ba
4 - Follow the instructions

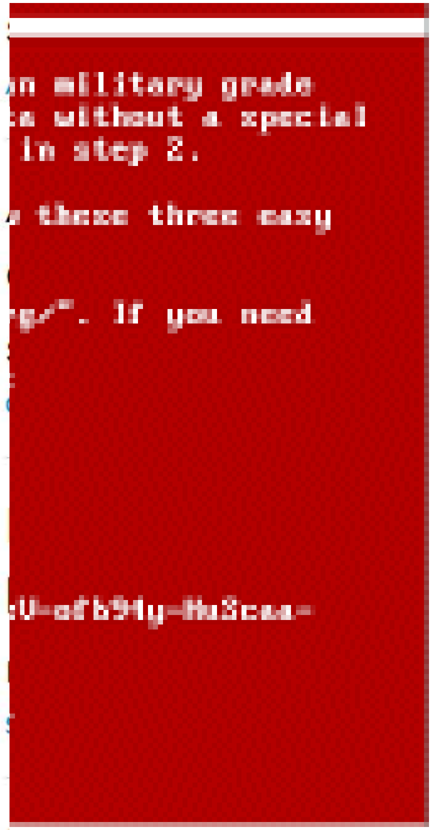
IMPORTANT INF
Your personal pages
http://po [redacted]
http://u54 [redacted]
http://w [redacted]
Your personal page Tor-B

3 November 2017 10:36

Merck reveals losses in sales due to cyber-attack

RSS Print

Merck has revealed, in its third quarter earnings report, that the manufacturing disruptions related to the cyber-attack that happened earlier in the year led to $135 million in lost sales.



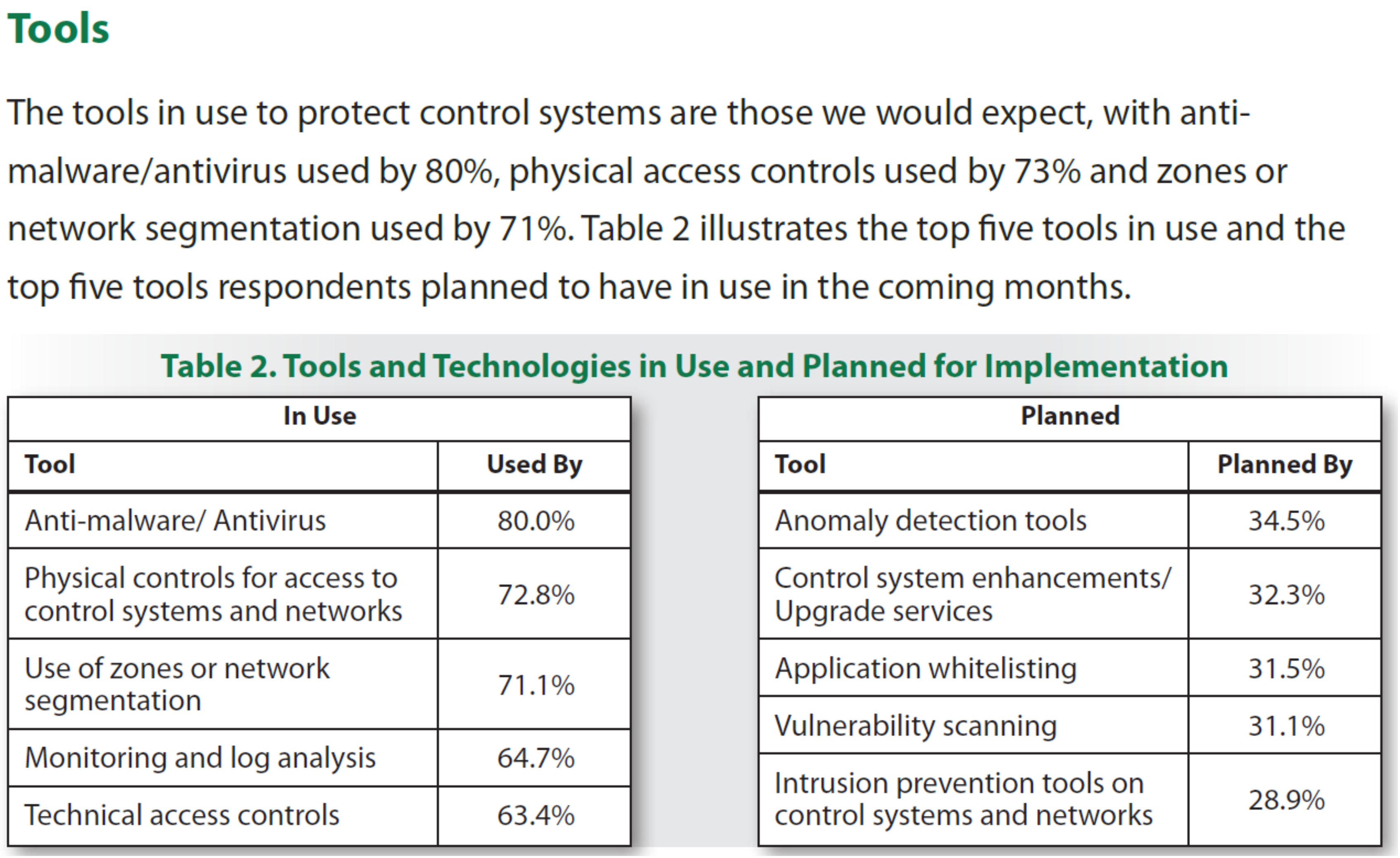
n military grade
s without a special
in step 2.

these three easy

g/". If you need

U-afb9Hy-Hu3cea-

ICS/OT Cyber risk mitigation Security trends



Tools

The tools in use to protect control systems are those we would expect, with anti-malware/antivirus used by 80%, physical access controls used by 73% and zones or network segmentation used by 71%. Table 2 illustrates the top five tools in use and the top five tools respondents planned to have in use in the coming months.

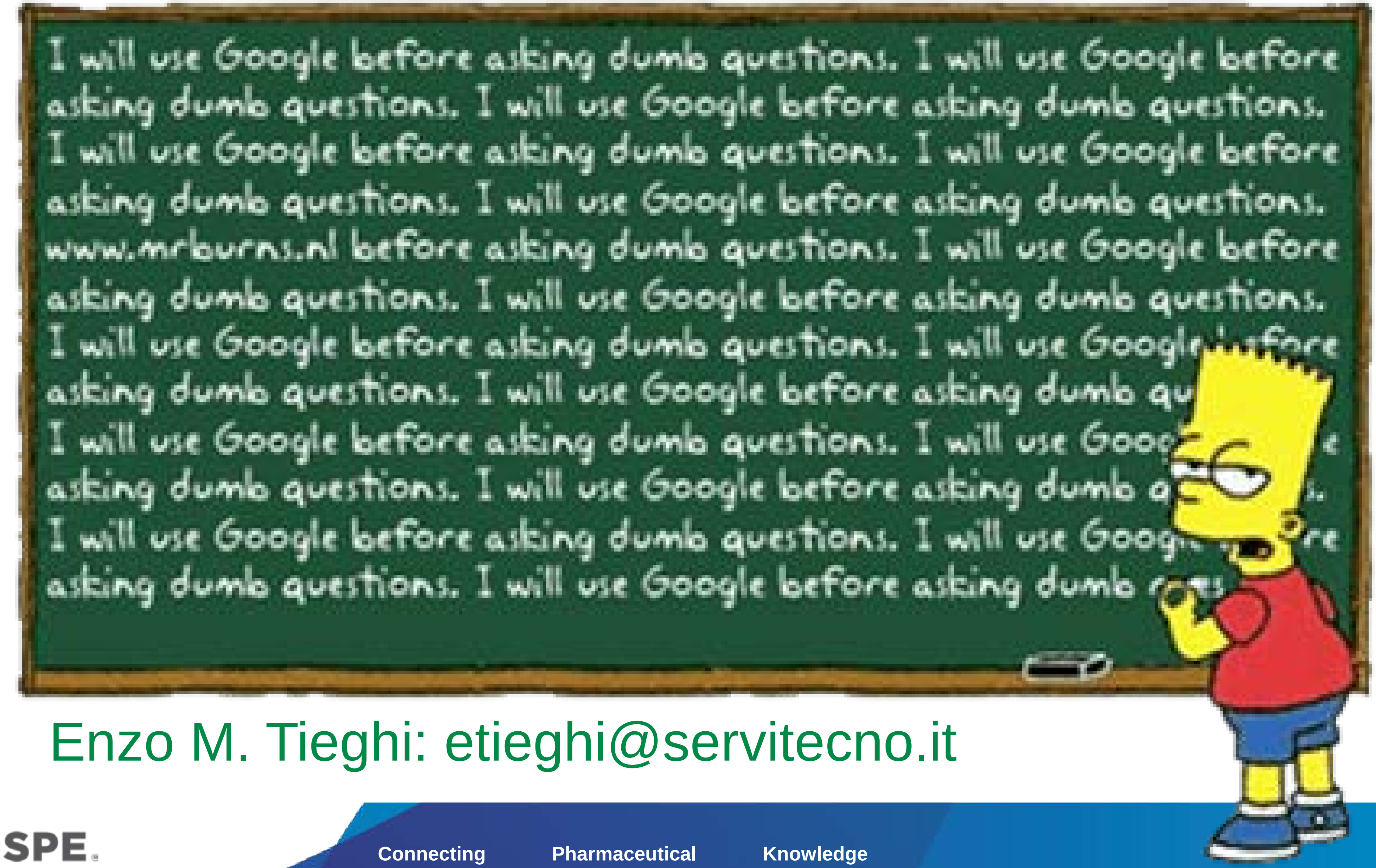
Table 2. Tools and Technologies in Use and Planned for Implementation

In Use	
Tool	**Used By**
Anti-malware/ Antivirus	80.0%
Physical controls for access to control systems and networks	72.8%
Use of zones or network segmentation	71.1%
Monitoring and log analysis	64.7%
Technical access controls	63.4%

Planned	
Tool	**Planned By**
Anomaly detection tools	34.5%
Control system enhancements/ Upgrade services	32.3%
Application whitelisting	31.5%
Vulnerability scanning	31.1%
Intrusion prevention tools on control systems and networks	28.9%

Technology might help ?

Questions?


I will use Google before asking dumb questions. I will use Google before
asking dumb questions. I will use Google before asking dumb questions.
I will use Google before asking dumb questions. I will use Google before
asking dumb questions. I will use Google before asking dumb questions.
www.mrburns.nl before asking dumb questions. I will use Google before
asking dumb questions. I will use Google before asking dumb questions.
I will use Google before asking dumb questions. I will use Google before
asking dumb questions. I will use Google before asking dumb qu
I will use Google before asking dumb questions. I will use Goog e
asking dumb questions. I will use Google before asking dumb q s.
I will use Google before asking dumb questions. I will use Goog re
asking dumb questions. I will use Google before asking dumb ques

Enzo M. Tieghi: etieghi@servitecno.it