IT-Security Challenges For The Smart Factory

WFCS 2012
Industry Day ”Automation for intelligent systems”

Dirk Seewald
Chief Executive Officer
Innominate Security Techn. AG

protecting industrial networks

Innominate
Security Technologies

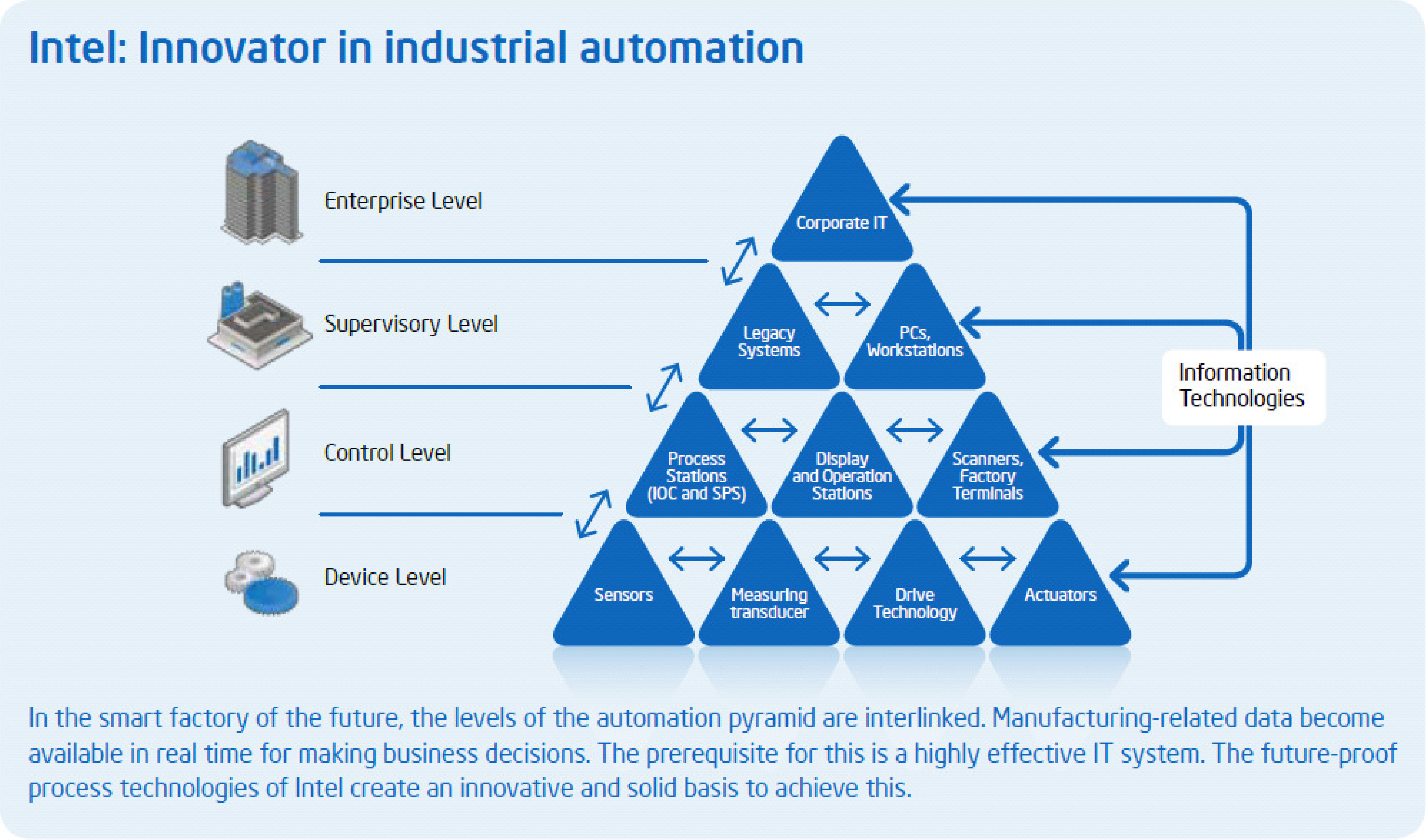
Who Is Innominate And What Do We Do

Innominate is a leading provider of network security products and solutions.

We offer major manufacturers, operators and integrators a patent-protected range of software and appliance products specifically designed for securing industrial environments and marketed under the mGuard brand.

Innominate
Security Technologies

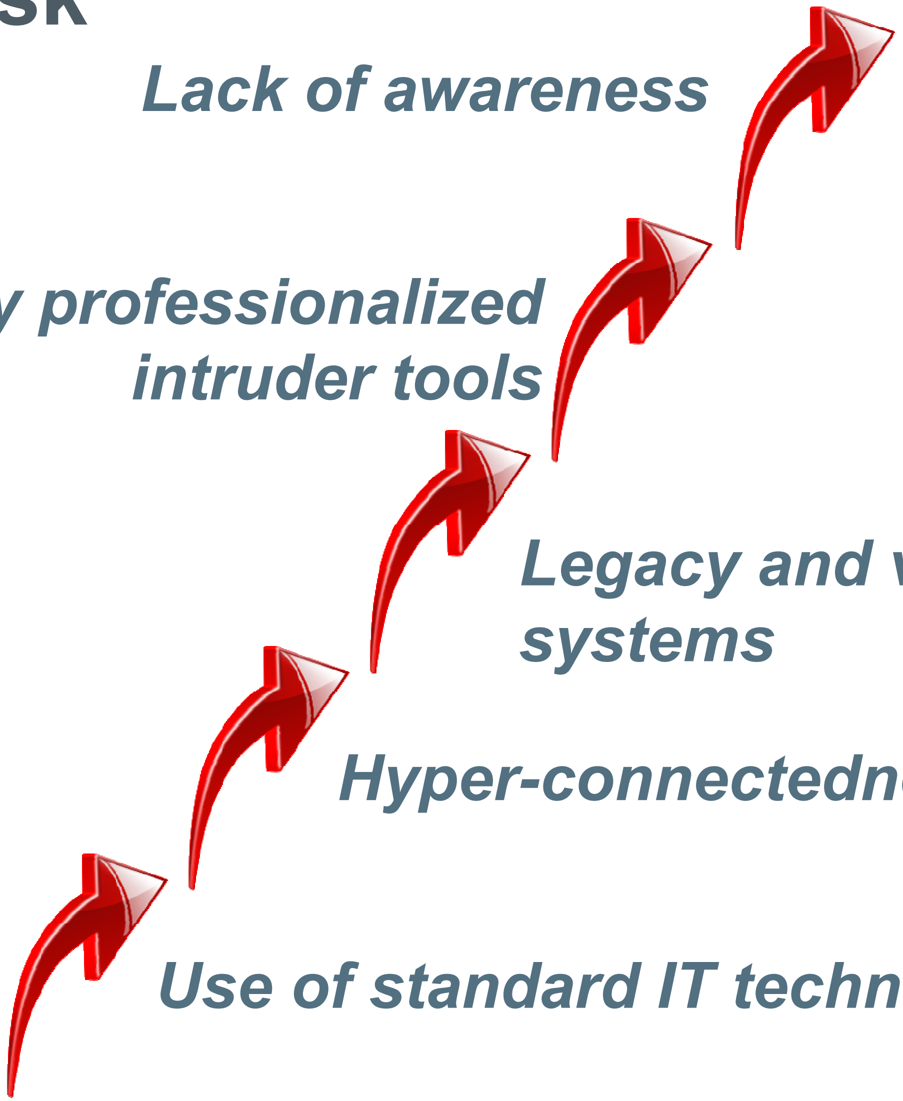
The Smart Factory



Intel: Innovator in industrial automation

In the smart factory of the future, the levels of the automation pyramid are interlinked. Manufacturing-related data become available in real time for making business decisions. The prerequisite for this is a highly effective IT system. The future-proof process technologies of Intel create an innovative and solid basis to achieve this.

The Quickly Accelerating Security Risk



Lack of awareness

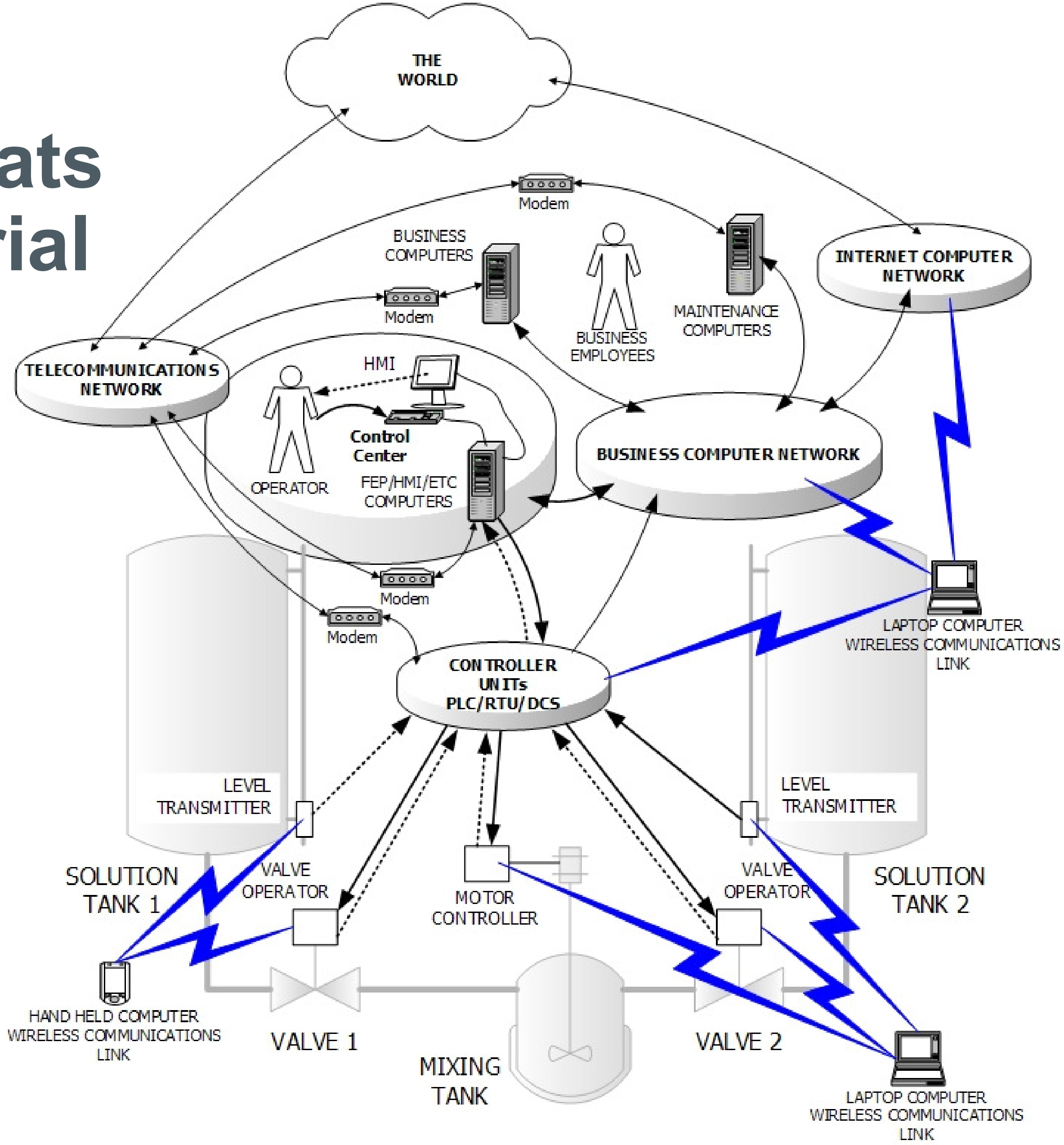
Highly professionalized intruder tools

Legacy and vulnerable systems

Hyper-connectedness

Use of standard IT technology

ICS-CERT Cyberthreats To Industrial Control Systems

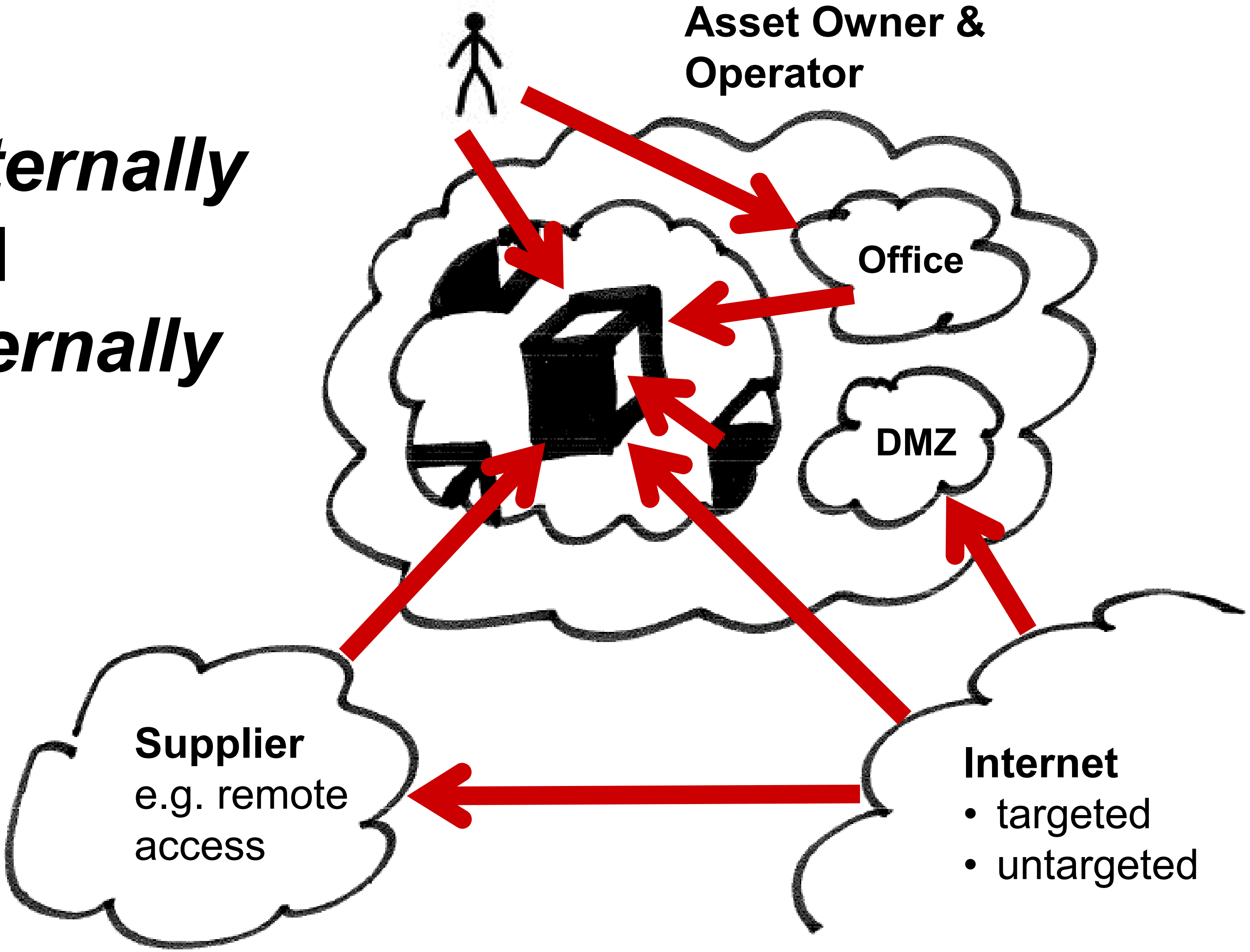


Cyberthreats From The Operator‘s Perspective

Externally

and

internally

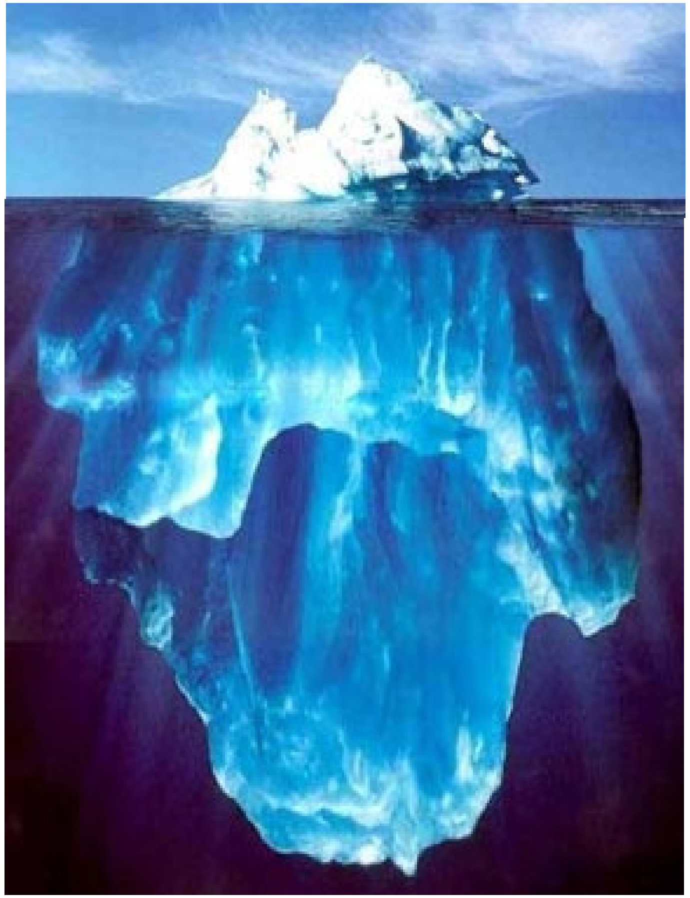


Is It Real?

- **89%** of all SCADA networks
  are connected to the office networks *
- **80%** of corporate firewalls are seriously misconfigured **
- **32%** of all PLCs did not react anymore after a simple DoS attack ***
- **78%** of all security events were unintentional, **40%** thereof due to faulty equipment ****

* Dr. Paul Dorey, CISO at BP, Process Control Systems Forum 2006
** Study A. Wool, IEEE Computer Magazine, June 2004
*** TOCSSiC Projekt, CERN, 2006
**** RISI Database, 2010

The Potential Damage Is Enormous



- Loss of production

- Human life
- Ecological damage
- Liability risk
- Penalties
- Corporate image
- Corporate value
- National security

Fundamental Operating Priorities

Traditional IT	Industrial IT
Operation at **business hours**	**Interruption-free** operations, 24x7
Confidentiality and **integrity** have highest priority	**Availability** has highest priority
IT security first	**Physical process first**
Patching and updating is **established**	Patching and updating is **partly difficult, if not impossible**
Standardized IT for the processing of data and information	**Specialized** IT for control of physical processes
No real time requirements, **higher latency often acceptable**	**Guaranteed response times** required, even real time
Operating term is **years**	Operating term is **decades**

Source: H. Honecker, BSI, KELI 2010

CIA vs. AIC – Fundamental Requirements Differ Substantially

Traditional IT

Confidentiality

Integrity

Availability

Industrial IT

Confidentiality

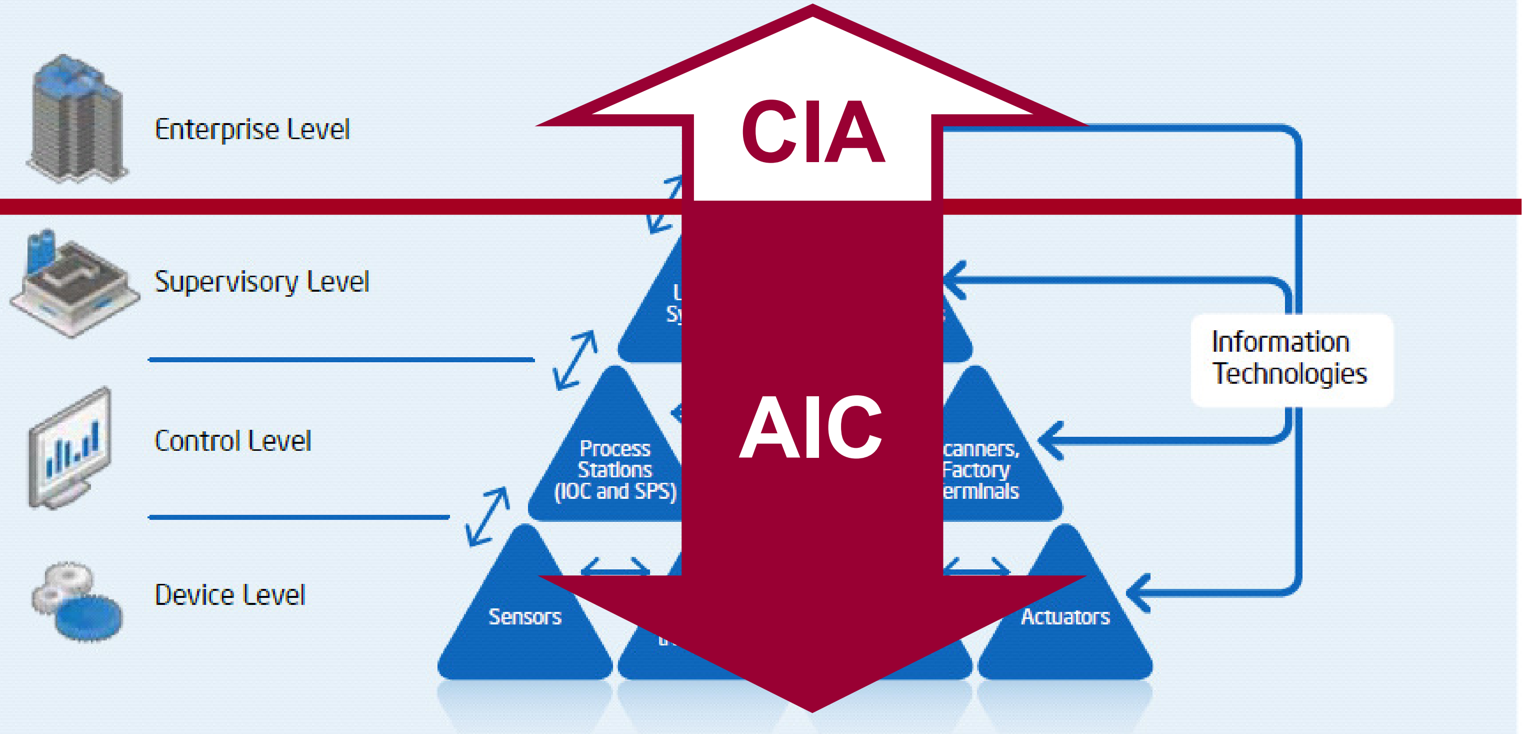
Integrity

Availability

Photos courtesy of FreeDigitalPhotos.net

The Switch From CIA To AIC Happens Within The Smart Factory System

Intel: Innovator in industrial automation



In the smart factory of the future, the levels of the automation pyramid are interlinked. Manufacturing-related data become available in real time for making business decisions. The prerequisite for this is a highly effective IT system. The future-proof process technologies of Intel create an innovative and solid basis to achieve this.

Emerging Standards For Industrial Cybersecurity

ESCoRTIS Consortium: worldwide 37 relevant standards, guidelines, provisions, 24 thereof are classified as „highly relevant“ for plant operators

ISA, IEC, BSI, VGB, NAMUR, BDEW, …

„Defense in Depth“

Photos courtesy of FreeDigitalPhotos.net

Key Technical Security Risks Can Be Effectively Mitigated

Key Security Risks	Defense Techniques
Overload („Denial of Service“)	Bandwith limitation, firewall, redundancy
Unauthorized change of data	Authentization, firewall, anti-virus scanner
Unauthorized extraction of data	Authentization, firewall
Unauthorized logging of data transmission	Encryption
Execution of non-authorized or compromised code	Anti-virus scanner, „Application whitelisting“, IDS

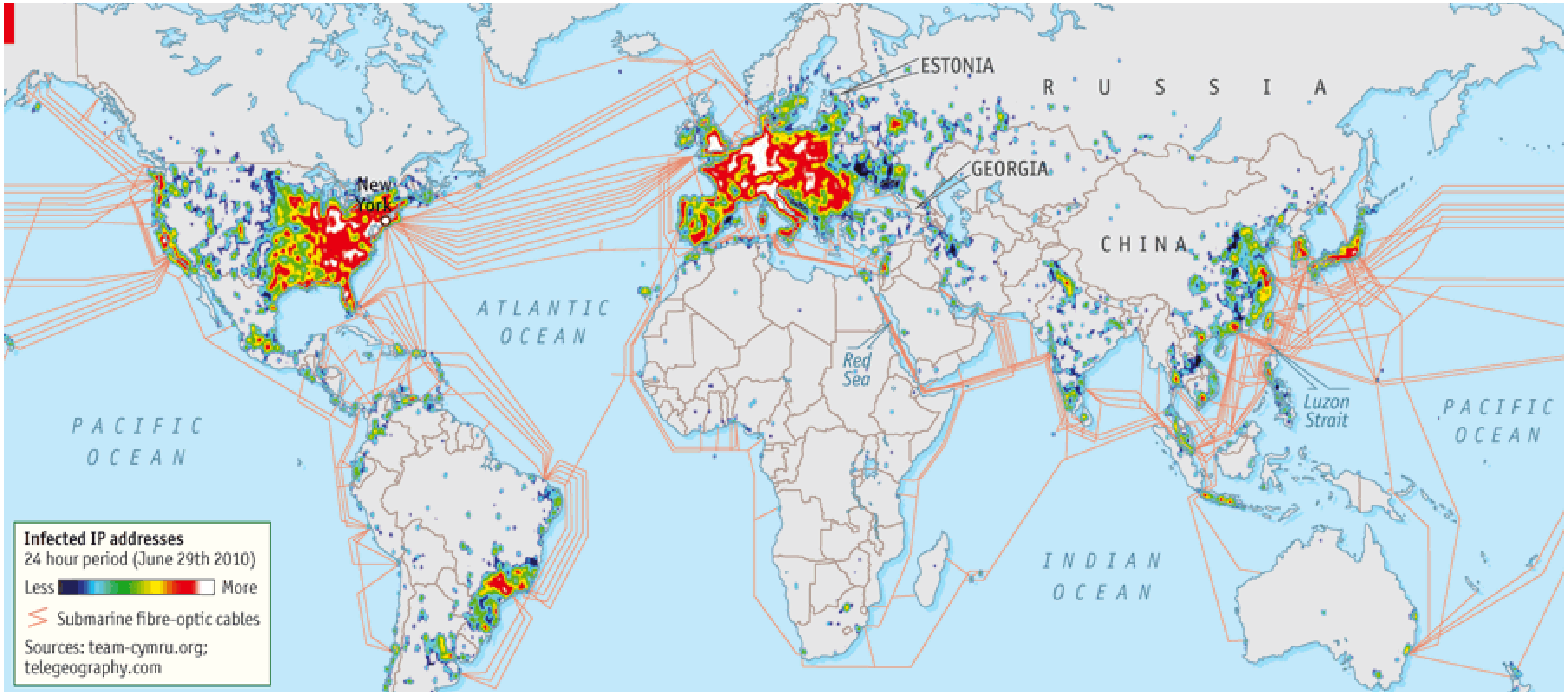
Key Technical Security Risks Can Be Effectively Mitigated

Key Security Risks	Defense Techniq
Overload („Denial of Service“)	Bandwith limitation redundancy
Unauthorized change of data	Authentizatio ti- virus scann
Unauthorized extraction of data	Authent all
Unauthorized logging of data transmission	En
Execution of non-authorized o compromised code	scanner, „Application ting“, IDS

mGuard

Thank You.

Map of infected IP addresses as of June 29, 2010



Sources: team-cymru.org; telegeography.com