Judith Rossebø, Principal Scientist, ABB Corporate Research, 6.09.2013

Cyber Security in Industrial Sensor and Mobile Systems

Wireless in Industrial Automation

- Oil & Gas

- Utilities/Smart Grid

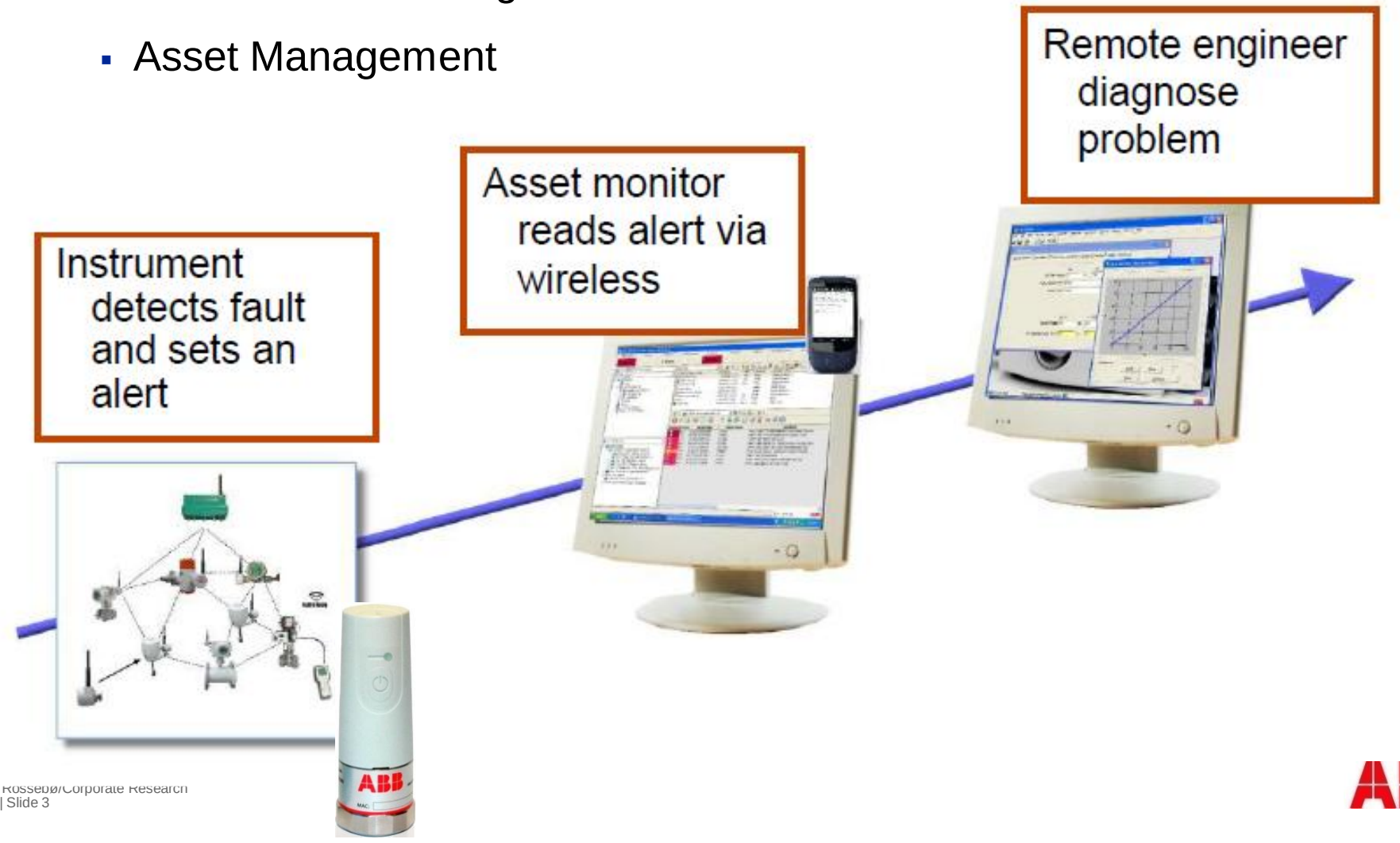
- Mining

- Smart Cities

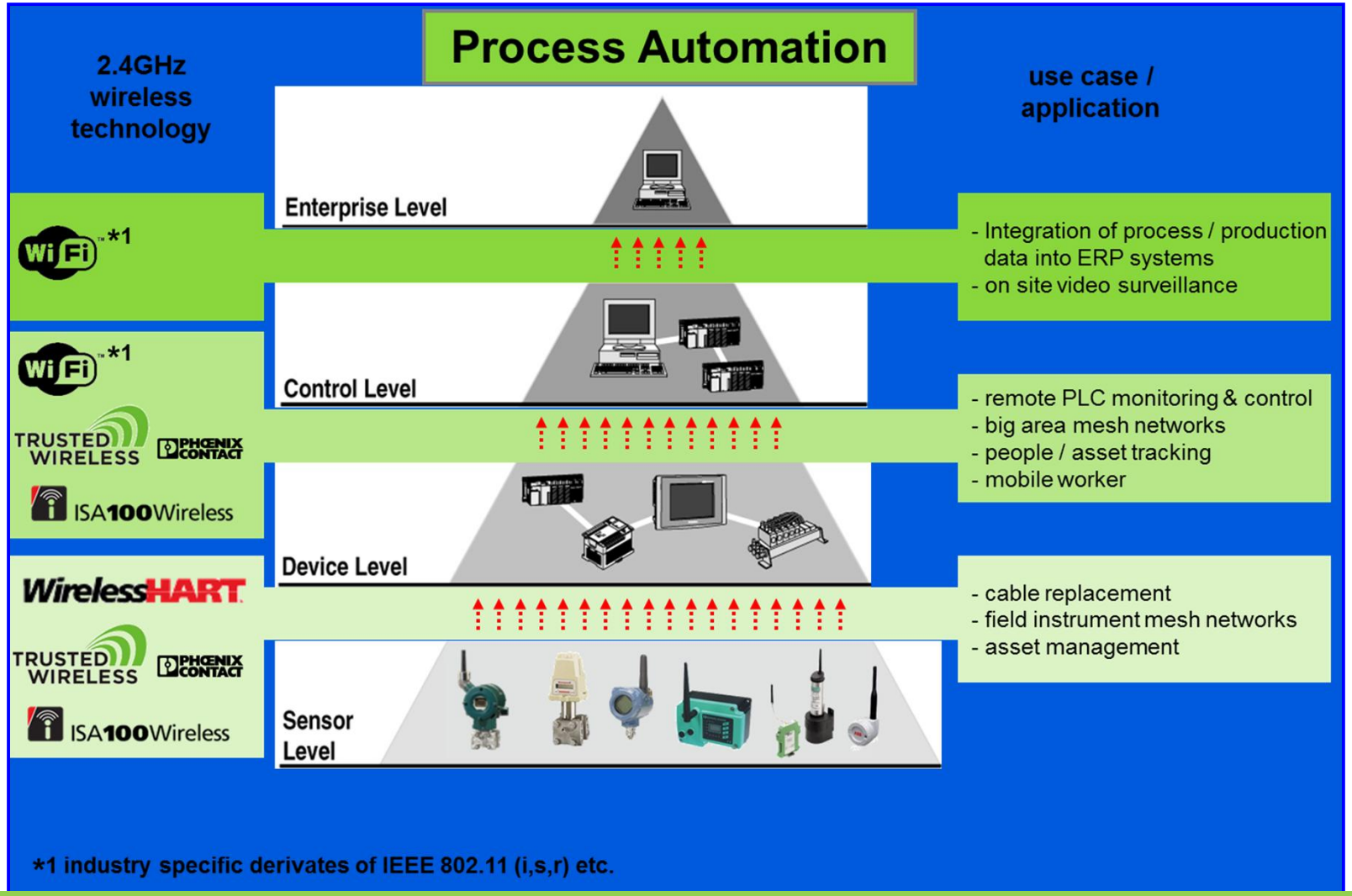
- Ports

Wireless Sensor Networks for Industrial Automation and Control Systems

- Process Monitoring
- Condition Monitoring
- Asset Management



Wireless in Industrial Automation



Wireless Stds in use: IEC 62591, IEC 62601, IEC/PAS 62734, IEC 61784-1, IEEE 802.1, IEEE 802.3, IEEE 802.11, IEEE 802.15.1, IEEE 802.15.4, etc.

Industrial Automation Systems
Requirements on wireless and mobile systems

- For the sensor and actuator type of applications in industrial automation, the main requirement is the real time behaviour:
  - Determinism for process industry.
  - Low latency and determinism for factory automation.

Needs for Factory and Process Automation	
Determinism	Temporal certainty
Short Latency	Fast response
Coexistence	Management of Coexistence
Robustness	Availability of transmission link
Range	Extensive plants and NLOS (no line of sight)
Frequ. Band	1,5 GHz … 6 GHz

Industrial Automation and Control Systems
Cyber Security – Incidents

- In 2001, a former employee repeatedly hacked into the SCADA system that controlled a Queensland, Australia sewage treatment plant, releasing about 264,000 gallons of raw sewage into nearby rivers and parks.
- In 2006, a foreign hacker penetrated security of a water filtering plant in Harrisburg, PA through the Internet and planted malicious software capable of affecting the plant's water treatment operations.
- In 2008, a teenage boy hacked into the track control system of the Lodz, Poland city tram system, derailing four vehicles, after adapting a television remote control so it could change track switches
- In 2010 Stuxnet is reckoned to have infected Iranian computers after being copied onto USB sticks left in locations known to be used by Iranian nuclear scientists and their contacts. It then spread into computer systems and took over the connected control systems, spinning centrifuges to dangerous speeds in order to damage the systems.


Schoolboy hacks into city's tram system

The boy, described as a 'genius'and some of the equipment he used

By Graeme Baker
12:01AM GMT 11 Jan 2008


Stuxnet virus targets and spread revealed

By Jonathan Fildes
Technology reporter, BBC News

Stuxnet may have been designed to target Iran's nuclear programme

Electricity Grid and Smart Metering
Cyber Security – Incidents

CIA: Hackers demanding cash disrupted power

Electrical utilities in multiple overseas cities affected

By Ted Bridis

The Associated Press

updated 6:06 p.m. ET, Fri., Jan. 18, 2008

WASHINGTON - Hackers literally turned out the lights in multiple cities after breaking into electrical utilities and demanding extortion payments before disrupting the power, a senior CIA analyst told utility engineers at a trade conference.

The X10 jammer designed by researchers to hack home automation systems through power lines. *Photo courtesy of David Kennedy and Rob Simon*

LAS VEGAS – Hacking the grid took on new meaning at the DefCon hacker conference on Friday when two independent security researchers demonstrated two tools they designed to hack home and business automation and security systems that operate though power lines.

THE WALL STREET JOURNAL.

WSJ.com

TECHNOLOGY | APRIL 8, 2009

Electricity Grid in U.S. Penetrated By Spies

The SmartMeter backfiring privacy issue

Posted on May 12, 2011 by Anthony Watts

The promise was to help you control your electricity bill by becoming more aware of your energy use. The downside is that with the data gathered, other people and businesses can also become more aware of your habits, like when you go to work, go on vacation, etc. Is the potential energy savings worth the invasion of privacy trade-off? I sure don't think so. I really don't want PG&E or anyone else for that matter knowing how I live my life inside my own home.

Industrial Automation vs Enterprise IT
A different set of challenges

	Enterprise IT	Industrial Automation
Object under protection	Information	Physical process
Risk impact	Information disclosure, financial loss	Safety, health, environment, financial
Main security objective	Confidentiality, Privacy	Availability, Privacy
Security focus	Central Servers (fast CPU, lots of memory, …)	Distributed System (possibly limited resources)
Availability requirements	95 – 99% (accept. downtime/year: 18.25 days - 3.65 days)	99.9 – 99.999% (accept. downtime/year: 8.76 hrs – **5.25 minutes**)
Problem response	Reboot, patching/upgrade, isolation	Fault tolerance, online repair

Cyber Security Goals

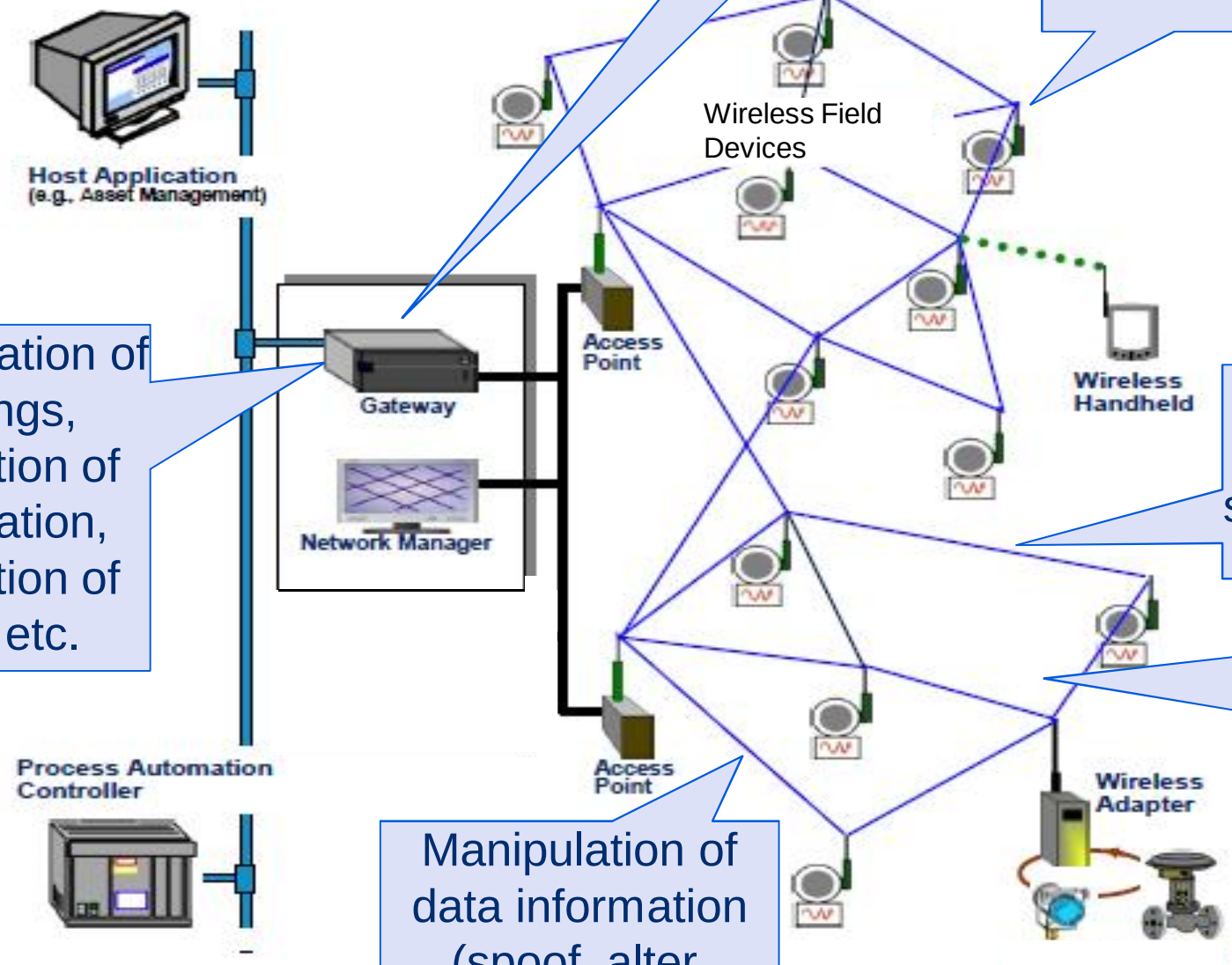
The goals of Cyber Security are

- Availability–avoid denial of service
- Integrity–avoid unauthorized modification
- Confidentiality–avoid disclosure
- Authentication–avoid spoofing / forgery
- Authorization–avoid unauthorized usage
- Auditability–avoid hiding of attacks
- Non-repudiation–avoid denial of responsibility

Cyber security has

- Functional aspects (e.g., user authentication, firewall)
- Quality aspects (e.g., testing, policy, defense in depth)

Wireless Sensor Network
What are the threats?



Manipulation in GW of settings in the wireless sensor network

Fake device joins the network

Manipulation of settings, corruption of application, corruption of data etc.

Jamming of the wireless sensor network

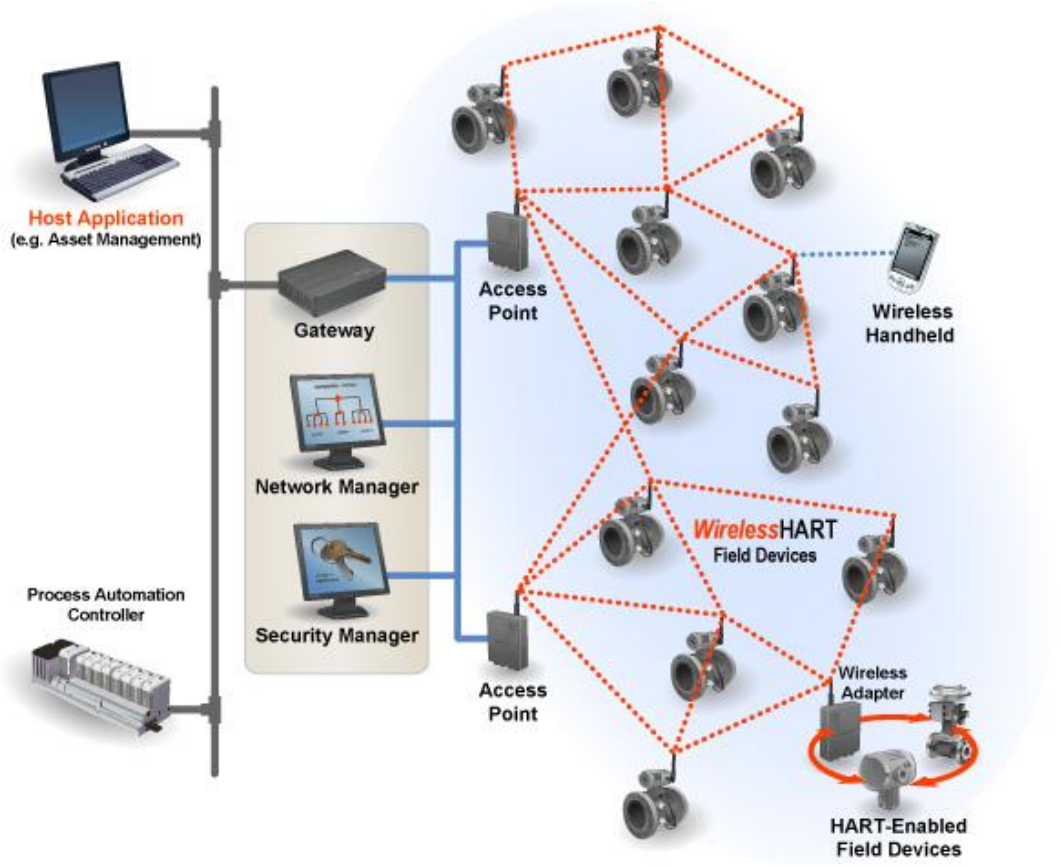
Eavesdropping on the wireless sensor network

Manipulation of data information (spoof, alter, replay)

Protection of Wireless Sensor Networks
Threat analysis

- Authenticity of Communication Peers – to prevent threat of packet manipulation, prevent malicious nodes from accessing the network
- Confidentiality of information – to prevent an attacker from eavesdropping on the network, monitoring the network for traffic analysis
- Integrity of information – to prevent attackers from manipulating the information exchanged
- Availability of Information – to prevent attackers from working at different layers to disrupt the availability of information (jamming at the physical layer, flooding at the transport layer etc.)

Wireless HART for Process Measurement and Control

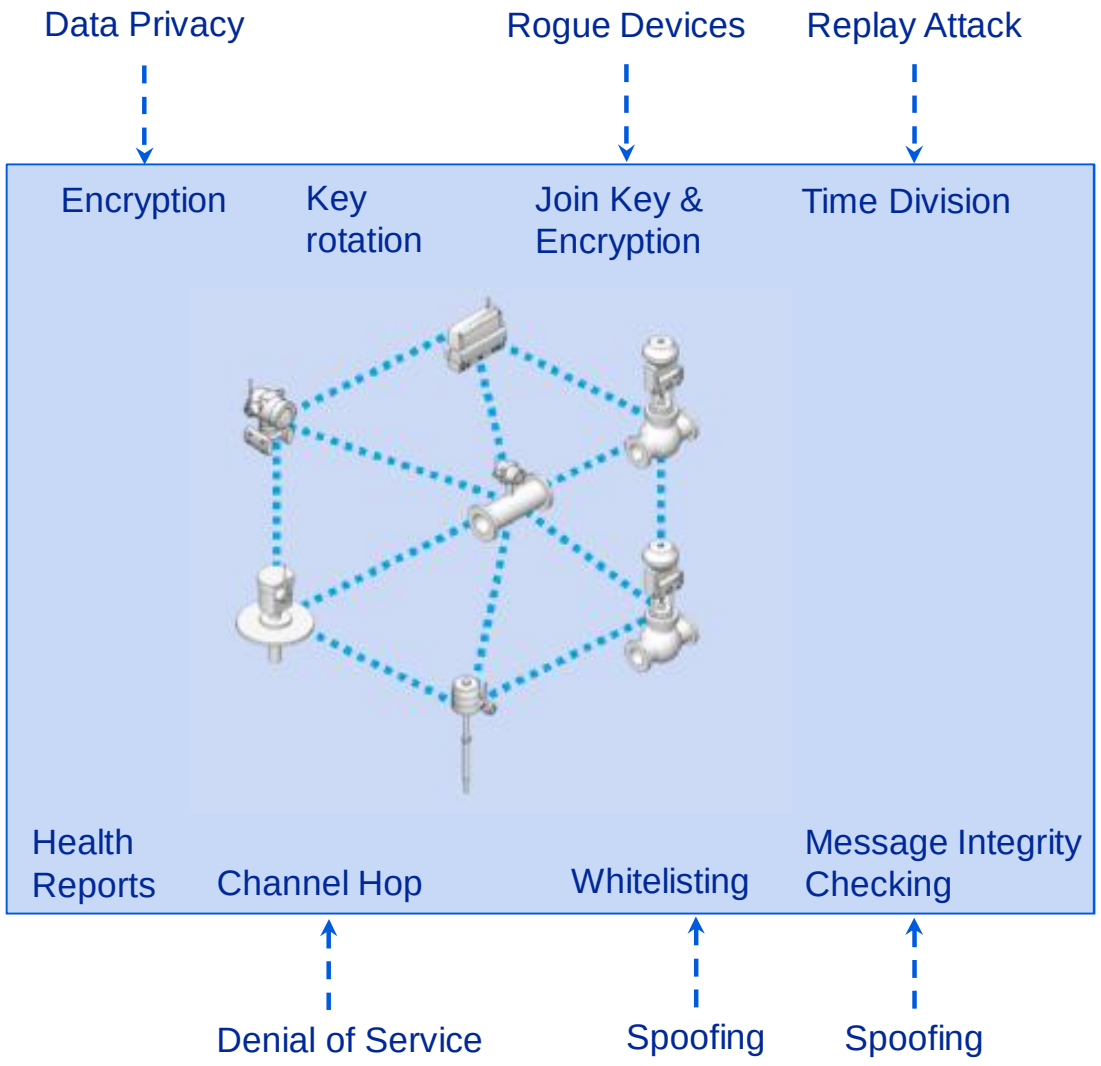


- Data Protection
  - Confidentiality
  - Integrity
- Network Protection
  - Availability

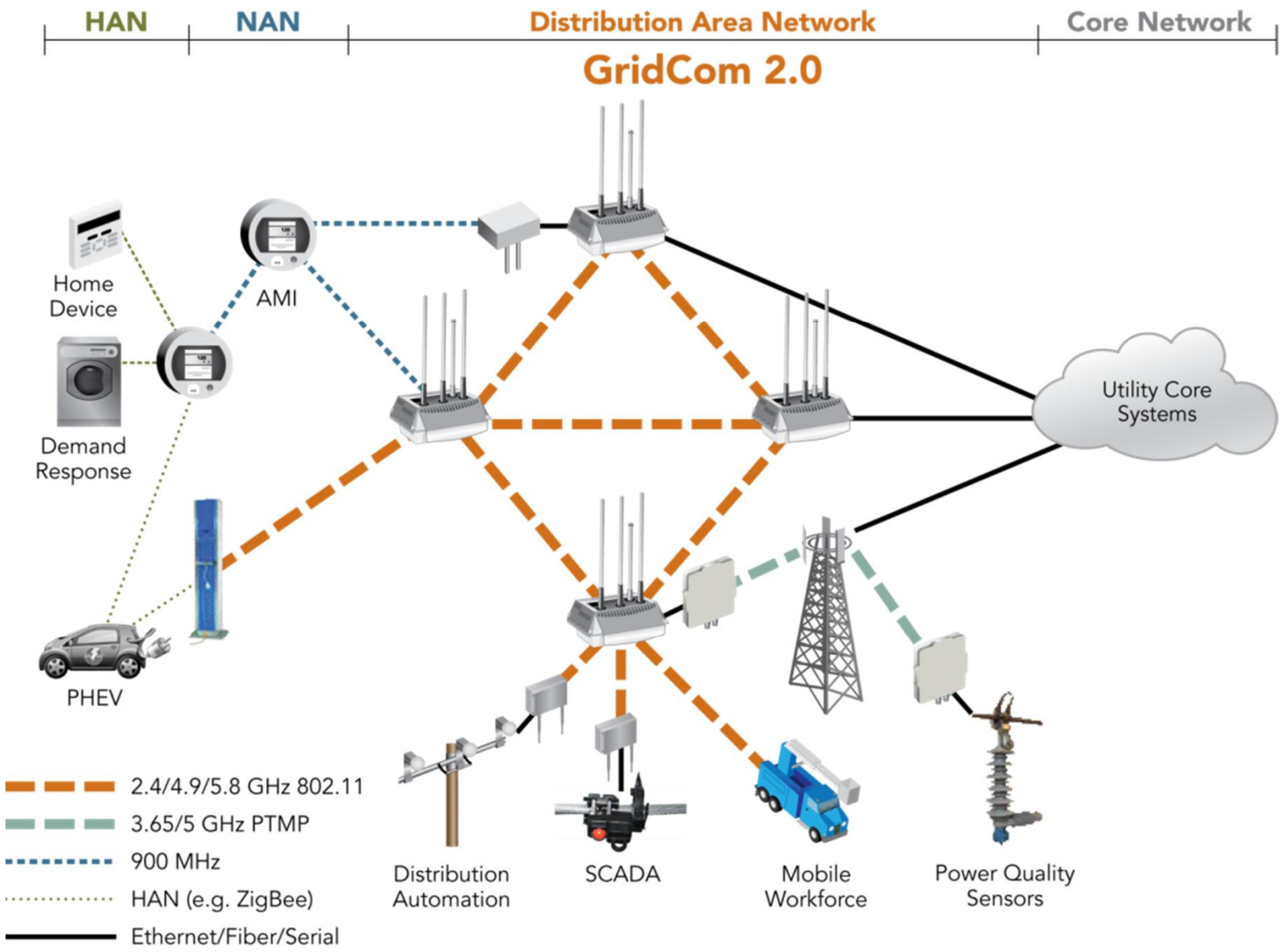
- Prevent eavesdropping
  - Secure join procedure
- Authenticate devices
  - Encrypt messages
- Ensure message integrity
  - Ecrypt messages

Understanding WirelessHART Security

- Data is valuable
  - Ensure it is not altered or read
- Multilayer security
  - Data encryption
  - Data authentication
  - Device authentication
  - Network monitoring



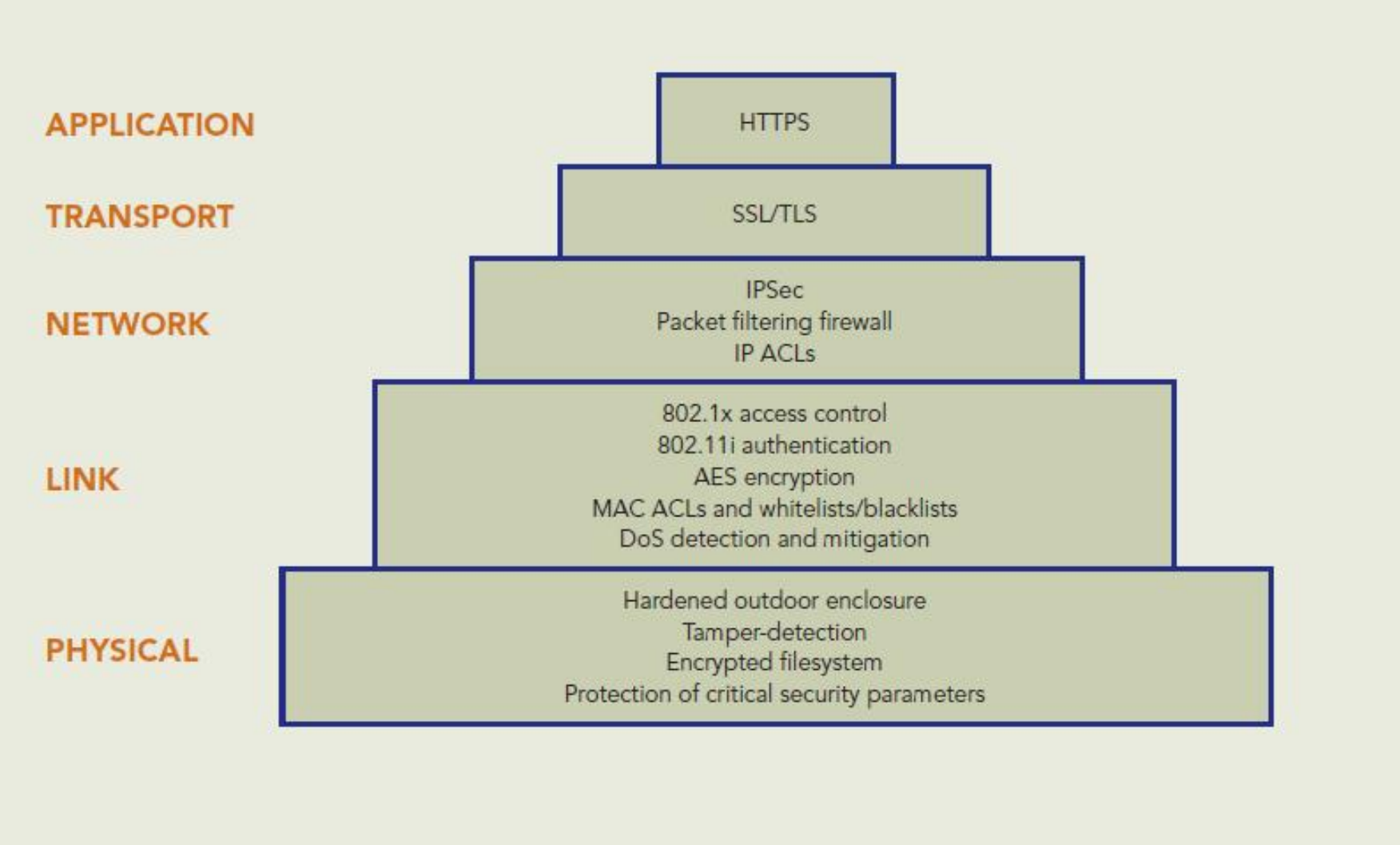
Reliable Wireless IP network
ABB Tropos Distribution Area Network



functional requirements for security of the wireless distribution network

- Availability and performance - system integrity and availability are maintained even under adverse conditions such as external attacks or peak loads
- Network Access Control - strong authentication and authorization requirements on devices and users
- Network resource and end-point protection - The distribution area network needs to be capable of protecting itself from attacks and unauthorized access
- Secure end-to-end data transmission - must support in addition to ensuring that there are no violations of confidentiality, privacy and data integrity
- Traffic segmentation across application boundaries – mechanisms to effectively segregate different classes of traffic to maintain inter-subsystem security and privacy
- Secure network configuration, operation and management - Only authorized network operators must be able to alter the operation of the network elements

ABB Tropos multi-layer security



Conclusions

- Wireless systems are being used more and more in industrial automation and control systems. The future trend is to connect more than instruments; provide a wireless backbone for everything in the plant, localization capabilities are increasing in importance
- Spectrum is a limited resource; the 2,4 GHz spectrum is highly suited for industrial wireless and there different, standard-based wireless are used and coexist in the 2,4-GHz-band for Industrial Automation
- Security in industrial wireless systems must be addressed at different layers and requires both protection and detection mechanisms
- Security is not just a matter of technology, it is primarily about people, relationships, organizations and processes working in tandem to prevent an attack
- Privacy and security concerns should not be understimated
  - Systems need to be established with security embedded across systems and with quick and decisive responses to suspected breaches or problems

Power and productivity
for a better world™