Integration, Security, and Synchronization

Thilo Sauter
Danube University Krems

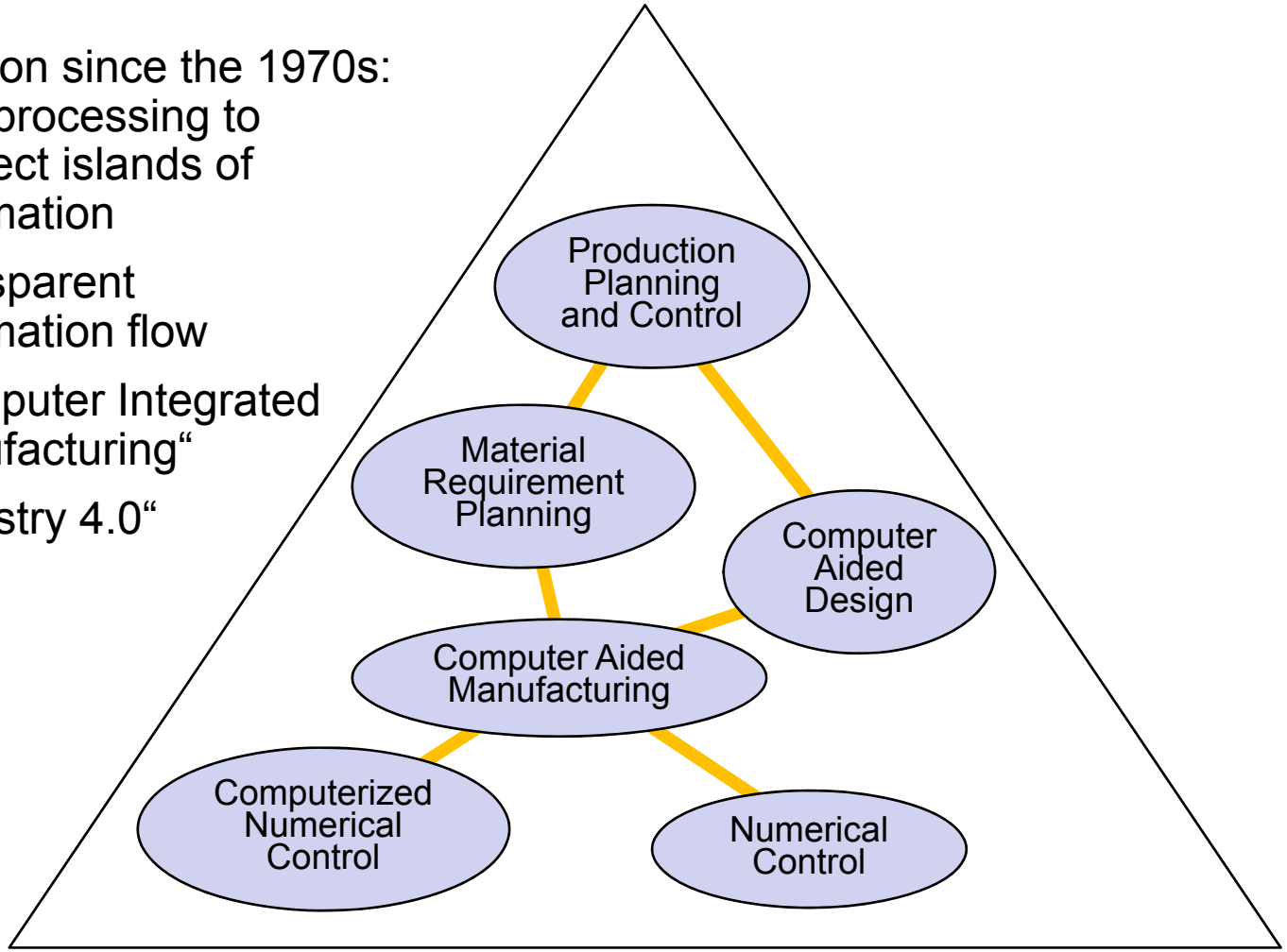
Center for Integrated Sensor Systems

Contents

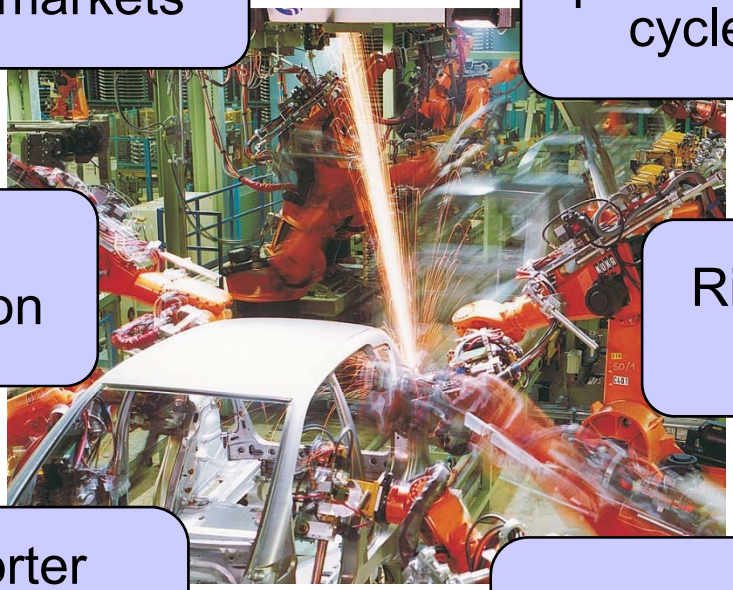
- Motivation
  - The big picture
- Integration aspects
  - Network interconnections
  - Hybrid wired/wireless networks
- Synchronization
  - The quest for accuracy
  - Localization of mobile devices
- Security
  - The big challenges
  - Practical solutions

Integration in Automation

- A vision since the 1970s: data processing to connect islands of automation
- Transparent information flow
- „Computer Integrated Manufacturing“
- „Industry 4.0“



Demand for Flexibility in Manufacturing



Volatile markets

Shorter product life cycles

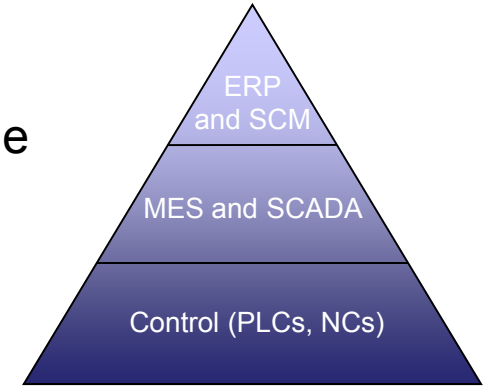
Product individualization

Rising product varieties

Shorter production times

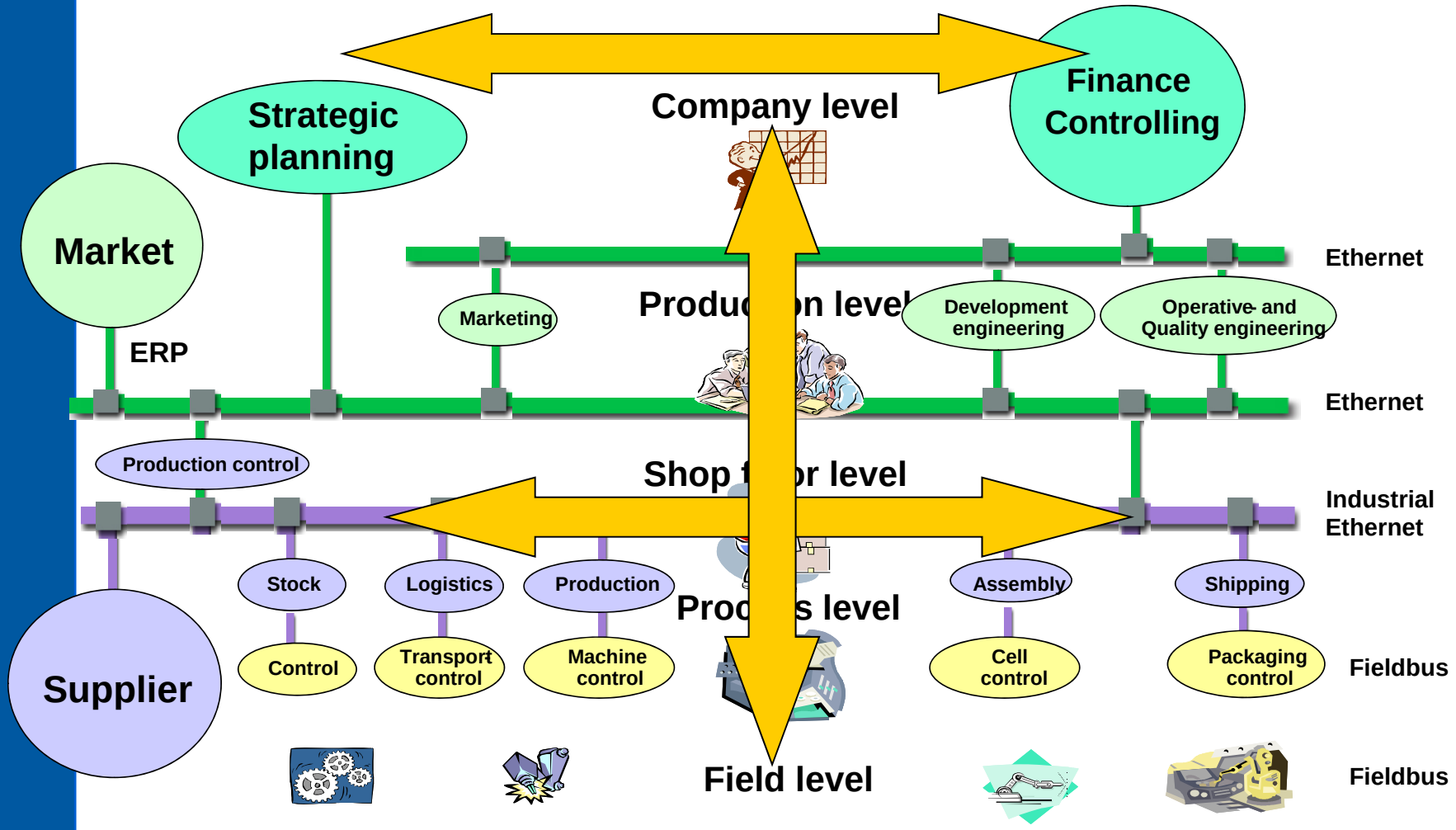
Plant life cycle costs

Need for Information Exchange and Integration

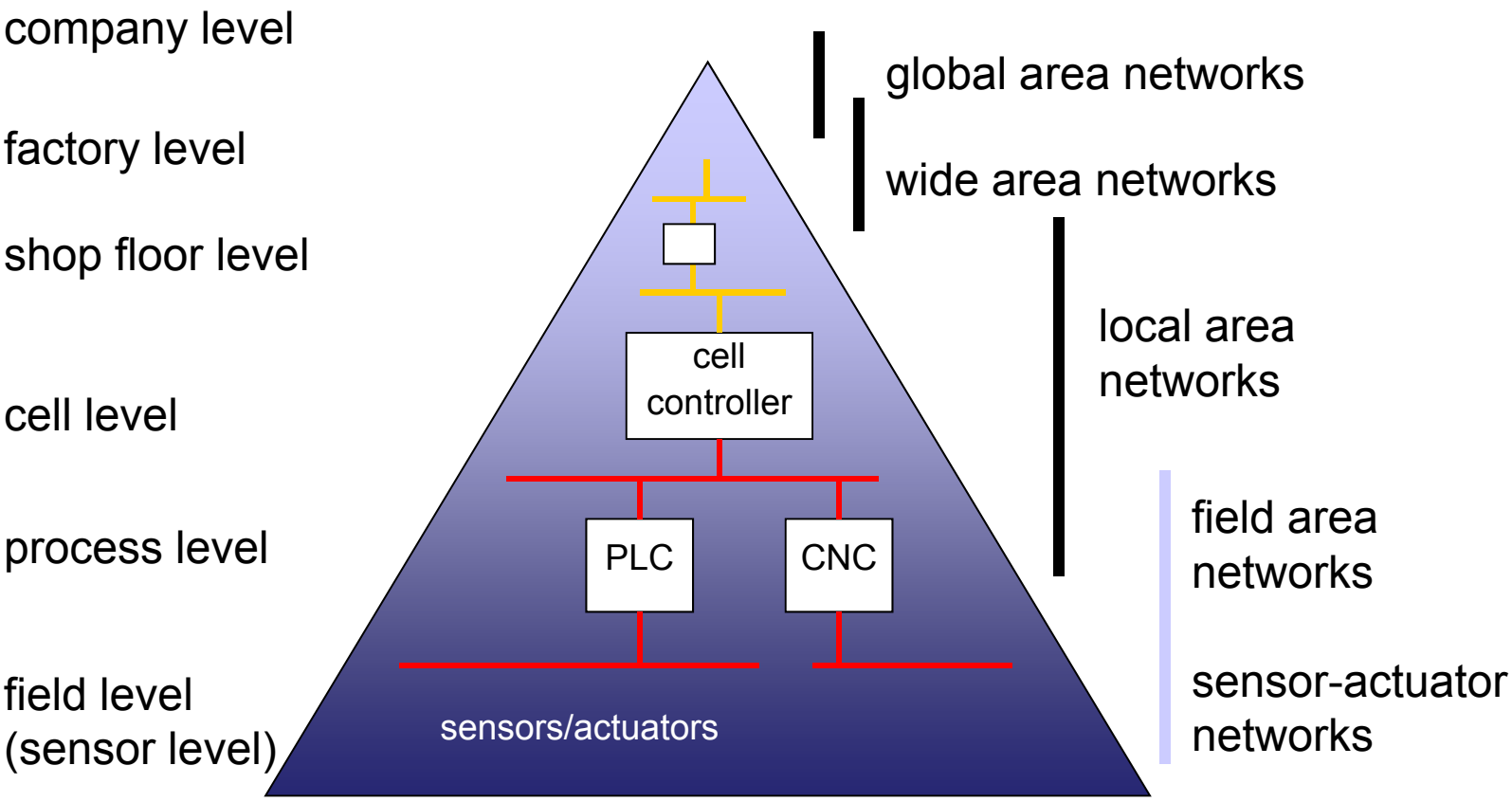


- Better access to production data during runtime
  - Resource planning
  - Agile manufacturing for small volume production
  - Quality control and product tracking
  - Asset management
- Access to plant data during setup and maintenance
  - System configuration during commissioning
  - Reconfigurability and flexibility
  - Life cycle management
  - No longer clearly distinguishable from runtime operation
- Integration along the value chain
  - Between companies (suppliers and customers)
  - On the highest level
  - Not time critical (in an automation sense)

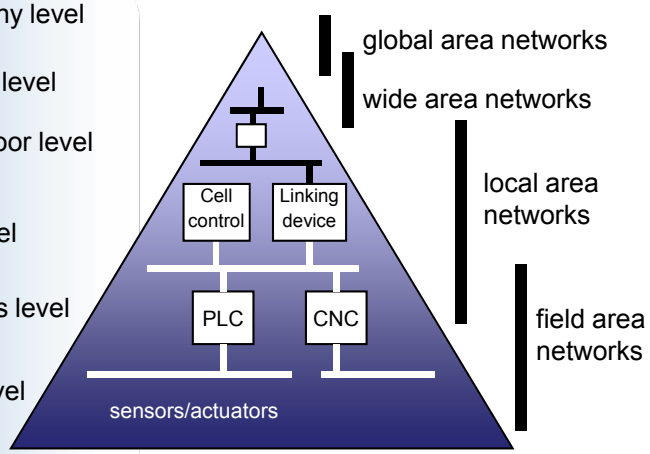
Vertical and Horizontal Integration



An Old Idea: the CIM Pyramid



The Automation Pyramid



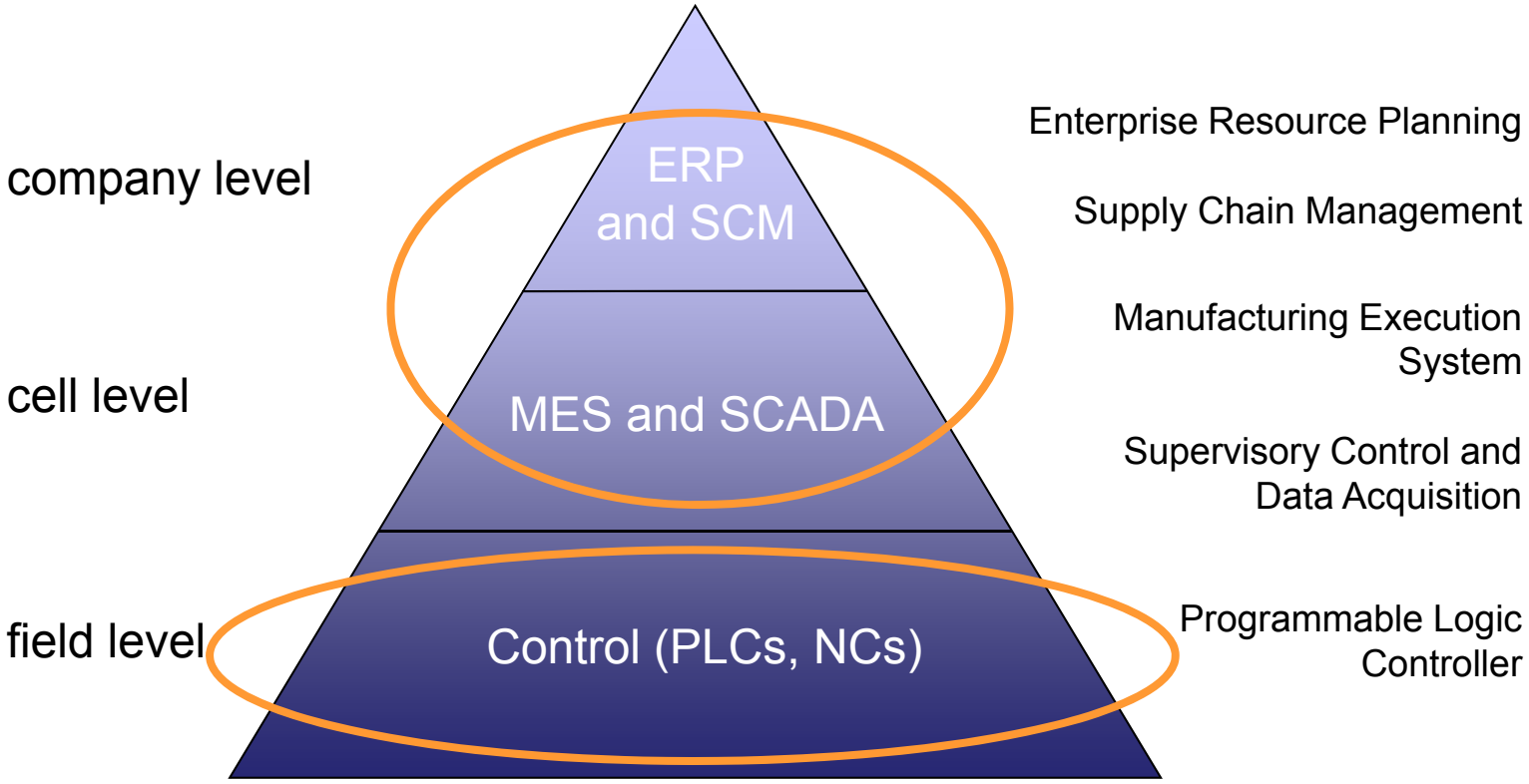
AMRF 1982	Esprit P 932 1988	ISO TC184 1988	1993	1999	ISA 95 2003
facility	facility	enterprise	plant	enterprise	(company)
shop	shop	facility, plant	factory		plant
cell	cell	section, area	cell, line	cell, line	shop
workstation	workstation	cell	workstation	workstation	cell
equipment	automation module	station	device	device	work station
		equipment	process	process	process

- 1974 (!): Computer Integrated Manufacturing
  - Combine “pieces of puzzles”, connect automation islands (MRP, CAD/CAM)
  - Create a multi-level network structure
  - Provide transparent data flow between the levels
- No uniform way to structure the information flow
  - Various versions of the automation pyramid
  - Depending on the application domain (manufacturing, process industry)

* T. Sauter, S. Soucek, W. Kastner, D. Dietrich, The Evolution of Factory and Building Automation, *IEEE Industrial Electronics Magazine*, vol. 5, no. 3, 2011, pp. 35-48.

Automation Pyramid Today – Functional View

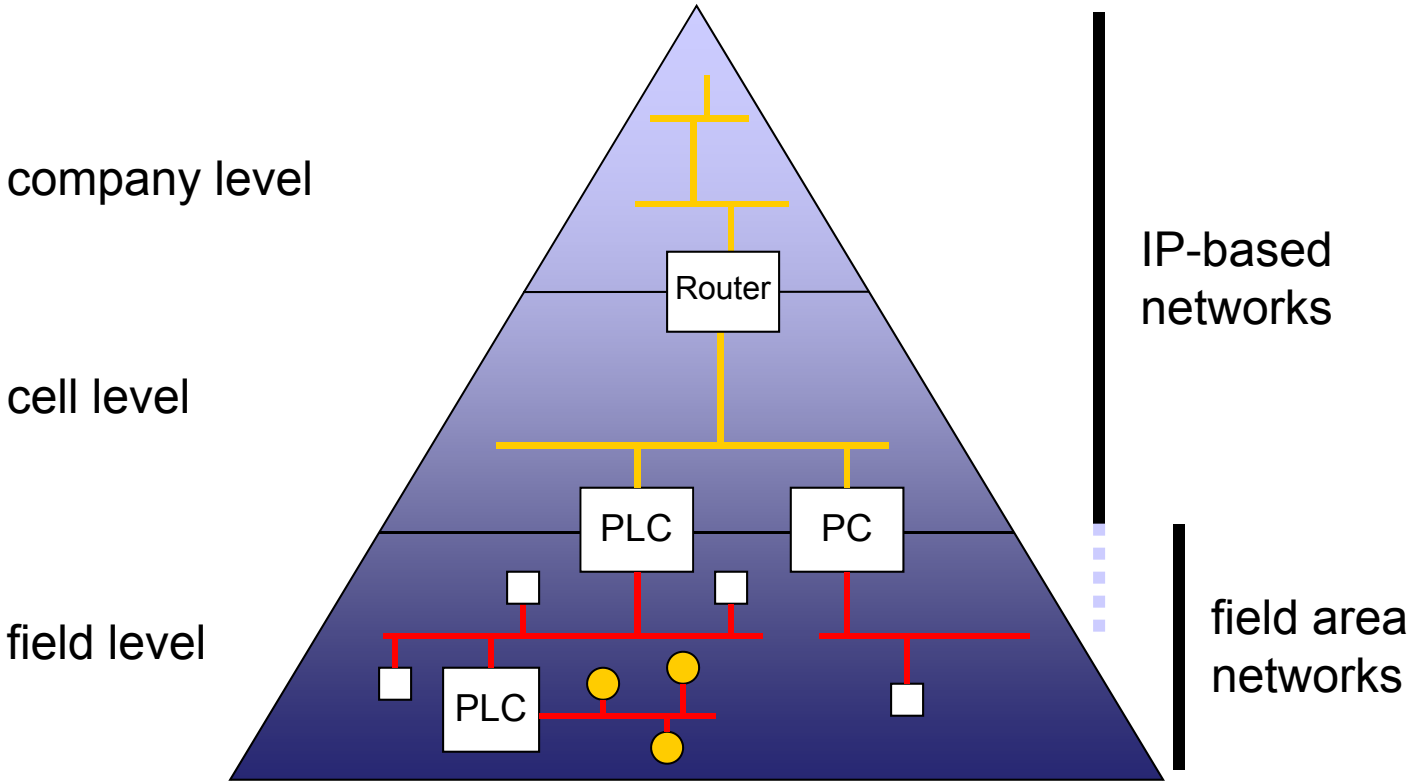
- Reduced to three levels
  - One for planning and strategic decisions
  - Two for factory floor



* T. Sauter, The Continuing Evolution of Integration in Manufacturing Automation, *IEEE Industrial Electronics Magazine*, vol. 1, no. 1, 2007, pp. 10-19.

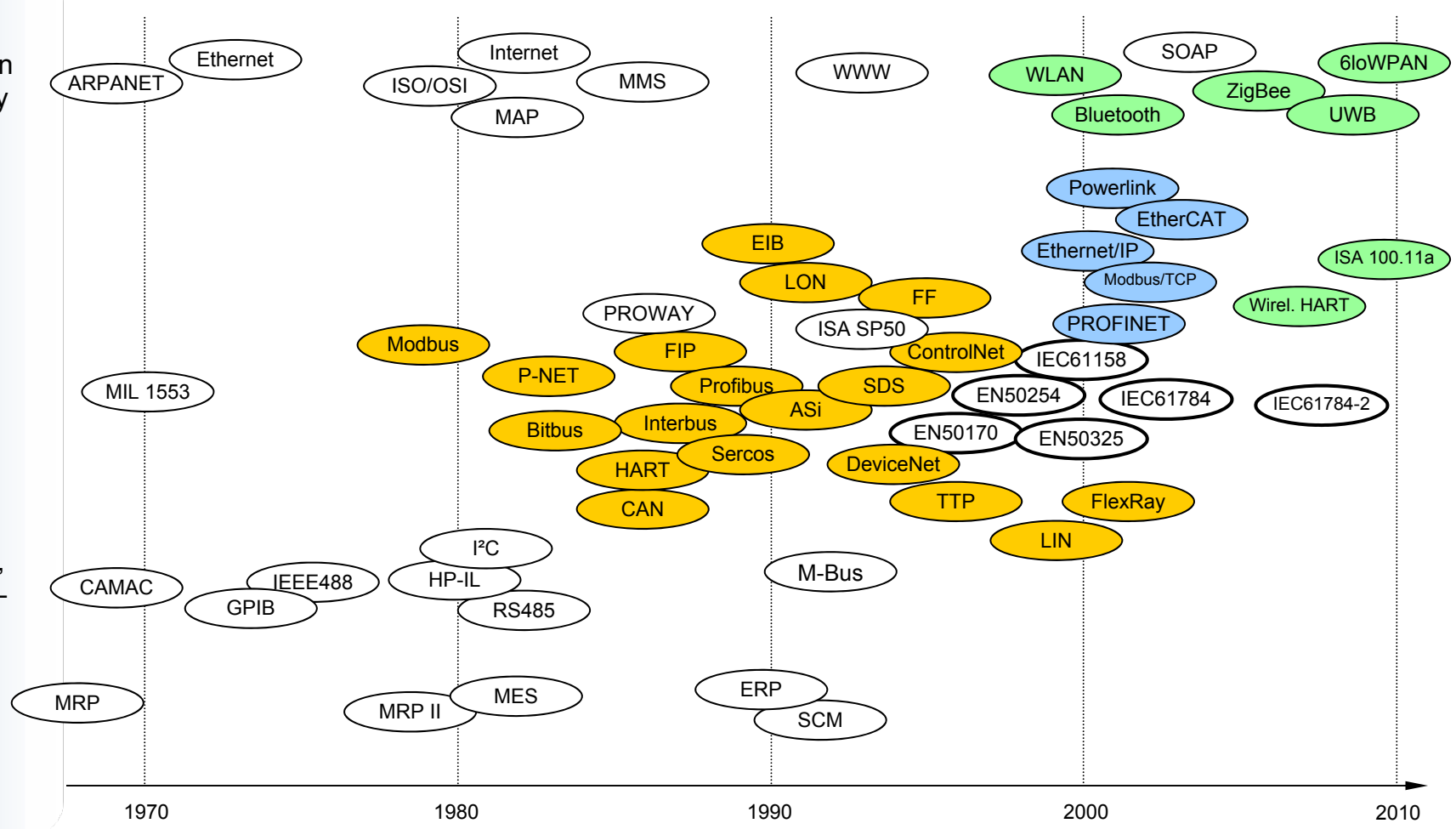
Automation Pyramid Today – Topological View

- Only two network types
  - IP-based networks and LANs
  - Dedicated automation networks (fieldbus systems, real-time Ethernet)



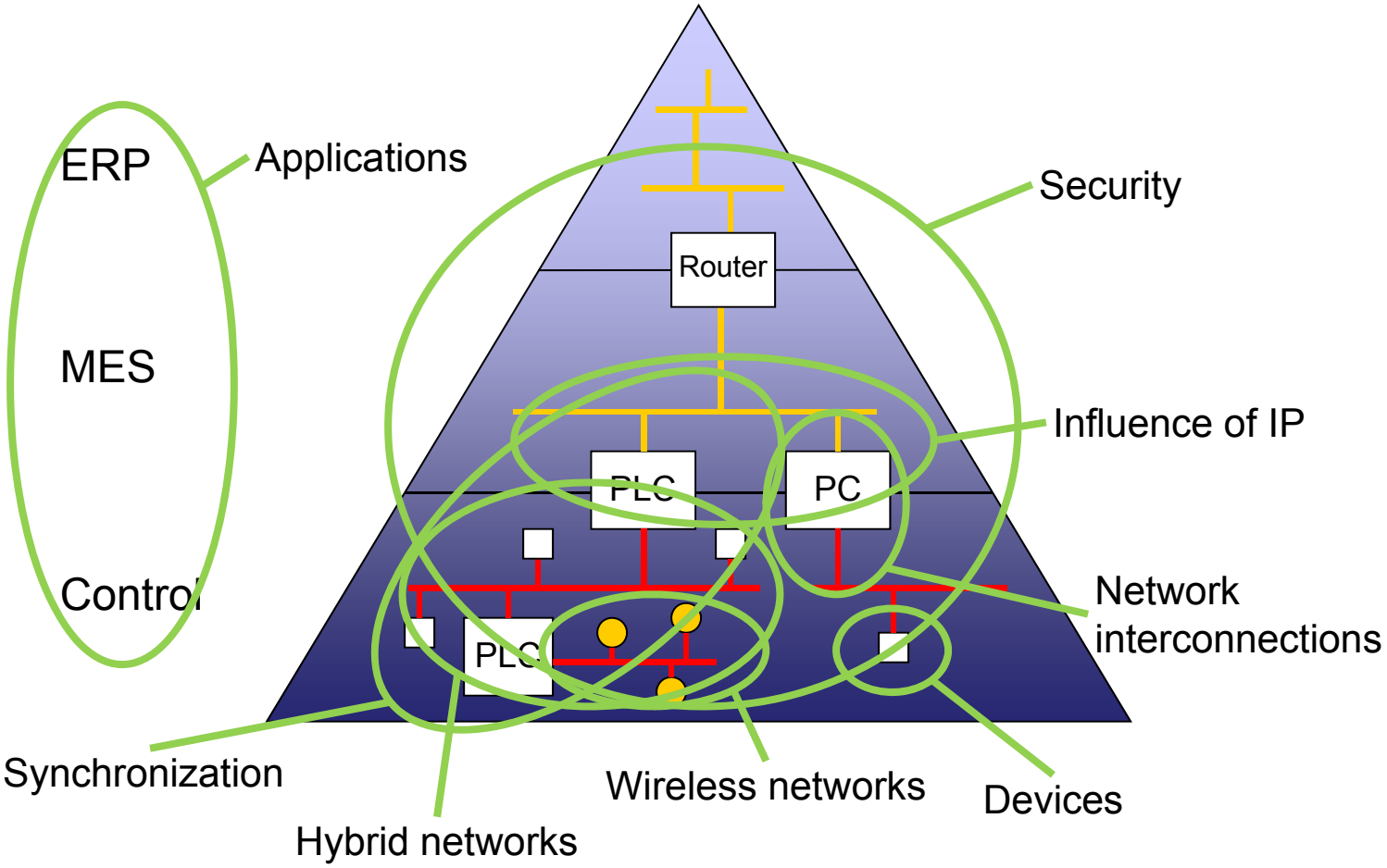
* M. Lobashov and T. Sauter, Vertical Communication from the Enterprise Level to the Factory Floor - Integrating Fieldbus and IP-based Networks, *IEEE ETFA*, Prag, 2006, pp. 1214-1221.

Milestones in Automation



* T. Sauter, The Three Generations of Field-level Networks – Evolution and Compatibility Issues, *IEEE Trans. on Industrial Electronics*, vol. 57, no. 11, 2010, pp. 3585-3595.

Challenges for Integration?



Contents

- Motivation
  - The big picture
- Integration aspects
  - Network interconnections
  - Hybrid wired/wireless networks
- Synchronization
  - The quest for accuracy
  - Localization of mobile devices
- Security
  - The big challenges
  - Practical solutions

Network Interconnections

- Originally meant to be part of a comprehensive infrastructure
  - Vertical integration

company level

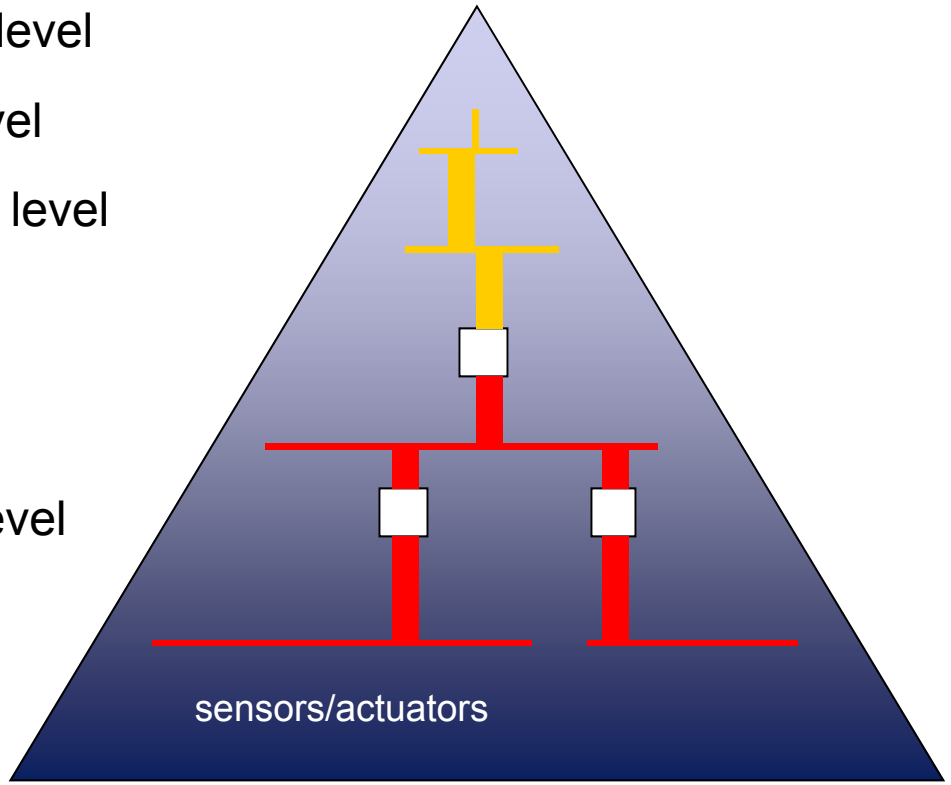
factory level

shop floor level

cell level

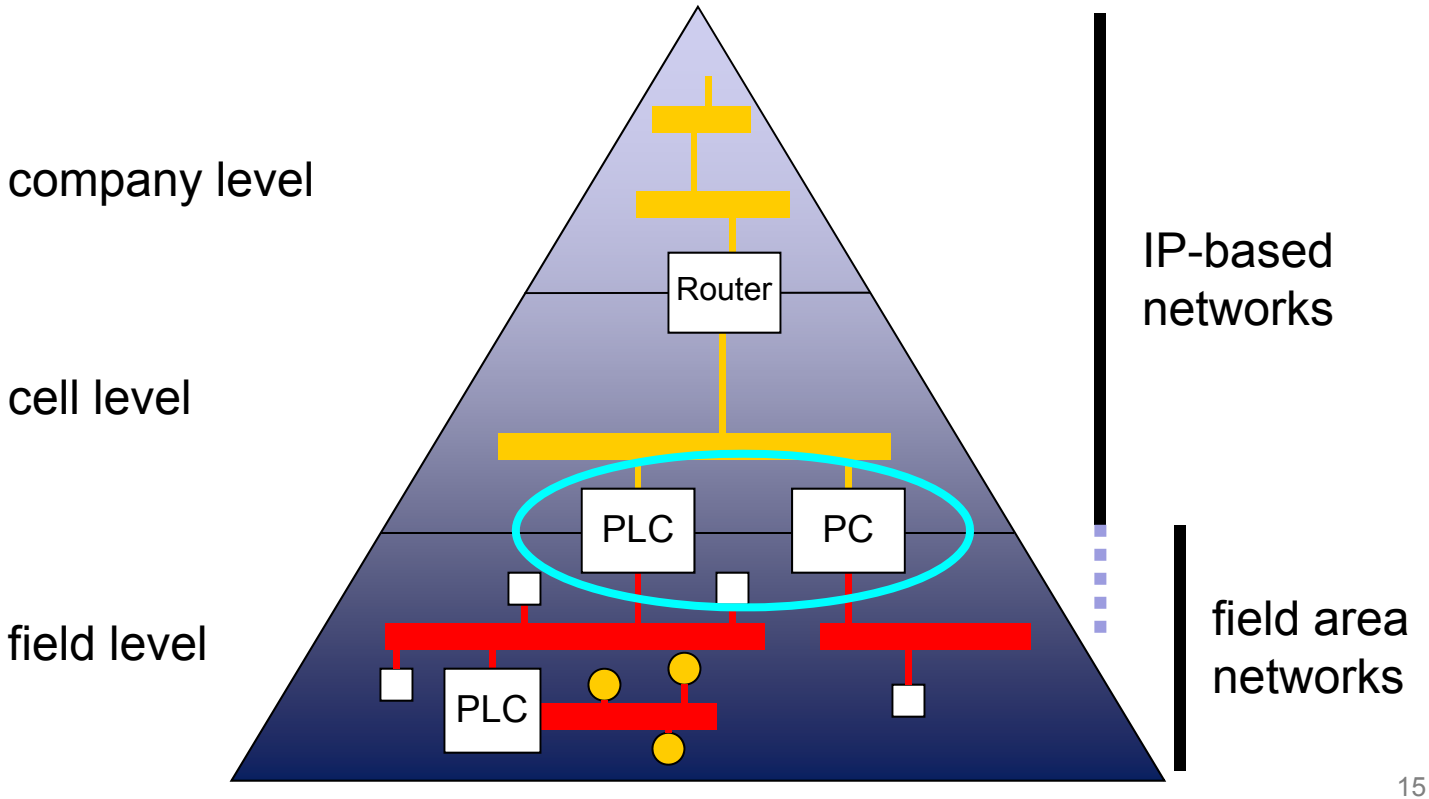
process level

field level



Network Interconnections

- ...but developed as islands
  - Horizontal integration



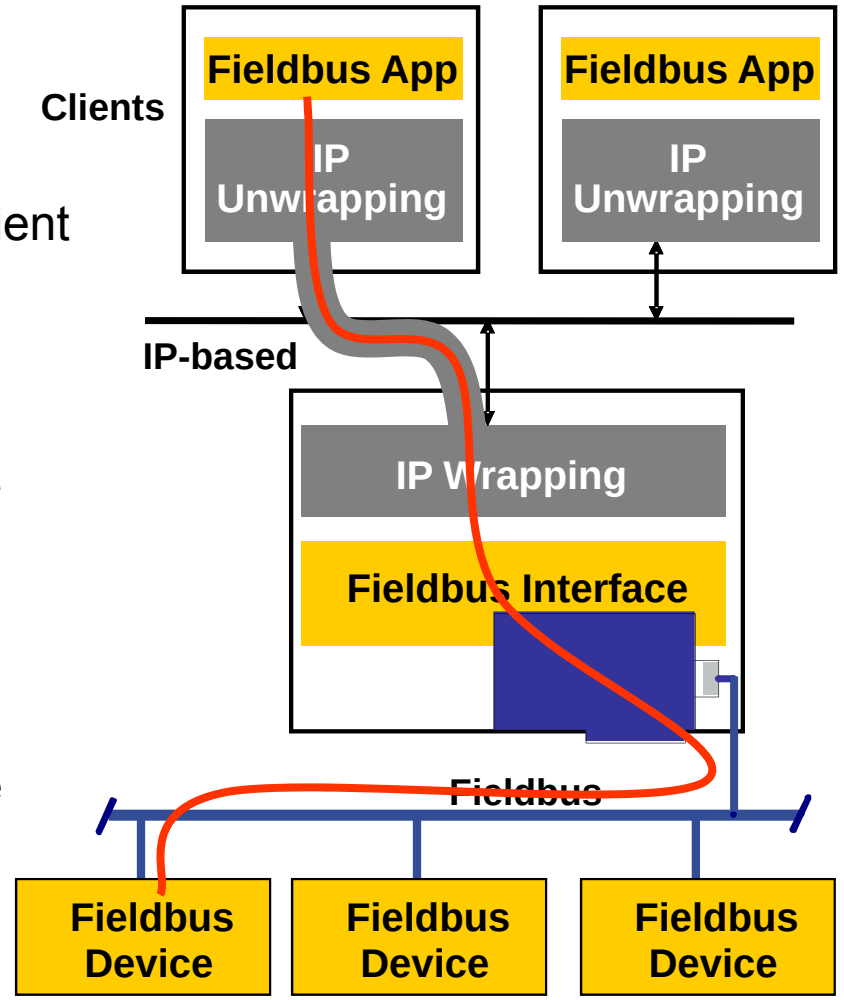
Network Interconnections

- Primary goal
  - Connection of two different network types
  - Automation networks vs. office networks
  - In many cases fieldbusses and IP-based networks (LANs)
  - Accessibility of automation data from office level

- Topological view
  - One dedicated node links the networks (access point)
  - Different possibilities to handle data and protocols
  - Different ways to distribute data processing between the access point and end nodes (centralized vs. decentralized)

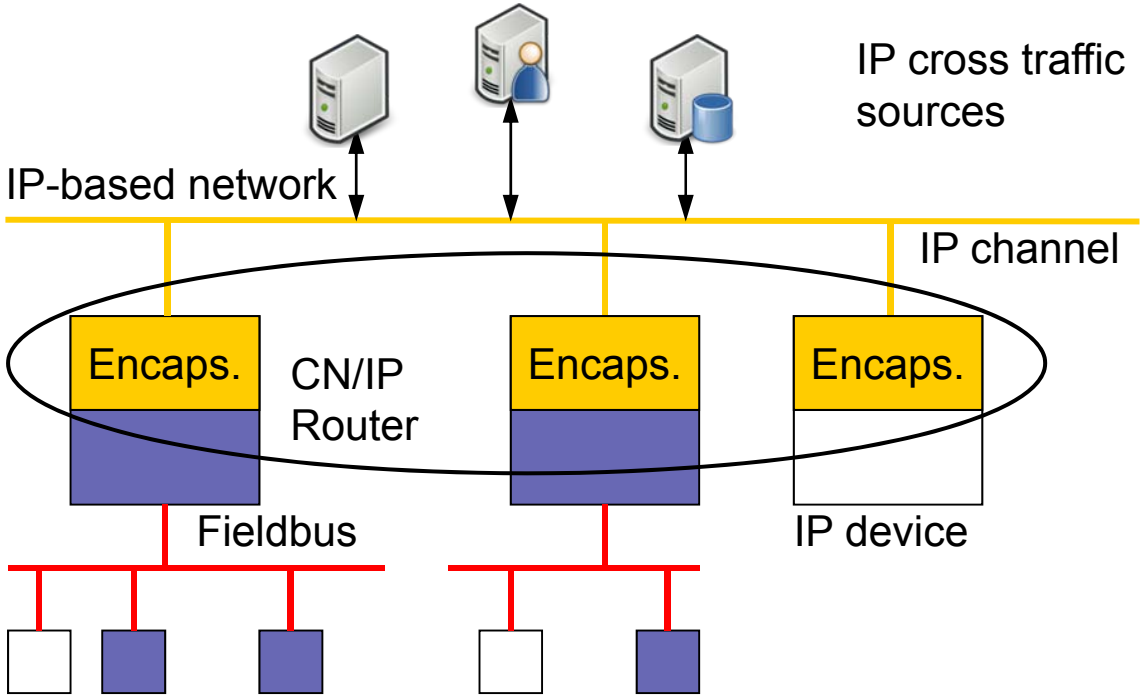
Possibility 1: Fieldbus over Internet

- Tunnelling of fieldbus protocol
- Fieldbus knowledge at client side needed
  - Special software required
  - Experienced user
- Not fieldbus-independent
  - Nor user-friendly
- Used for network-based control
  - IP network as backbone
  - Interconnection of remote segments
  - Horizontal integration



Tunneling Solution – EIA-852

- Packet-oriented data transmission
  - Often deterministic in the fieldbus
- Interconnection of fieldbus segments over IP
  - Definition of an IP channel as UDP tunnel for field-level packets

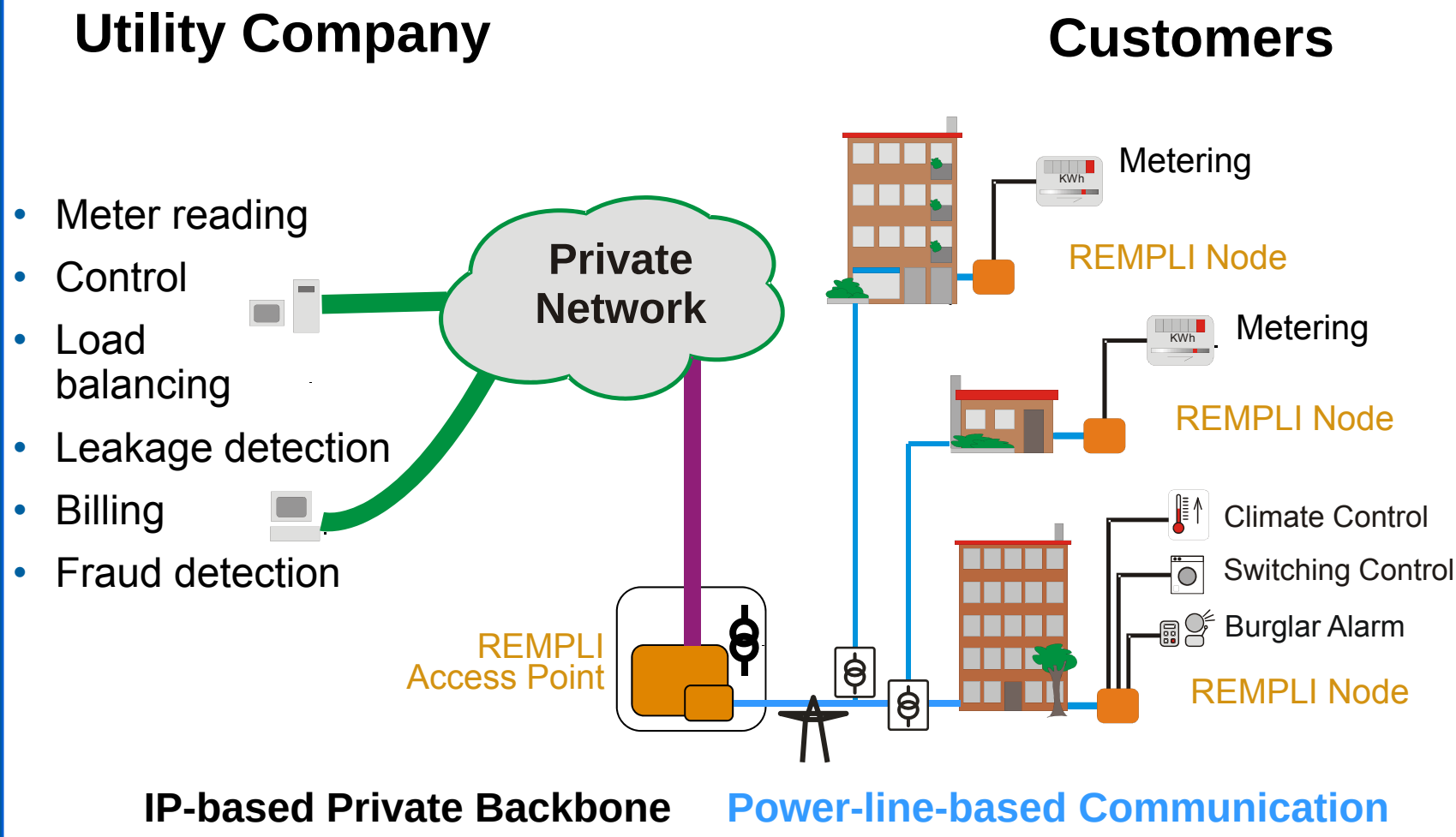


* S. Soucek and T. Sauter, Quality of Service Concerns in IP-based Control Systems, *IEEE Trans. on Industrial Electronics*, 2004, vol. 51, no. 6, 2004, pp. 1249-1258.

EIA-852

- Standard for remote interfacing of fieldbusses
  - Definition and management of IP channels
  - Peer-to-peer transmission of fieldbus data packets
  - Communication based on UDP
- Two possible network devices
  - Pure IP-based device
  - Control network device connected by tunnelling routers
- Various data flow control mechanisms
  - Sequence numbers for packets to allow for (re-)ordering
  - Recognition of missing packets
  - Dropping or intermediate storage (escrow) of late packets
  - Packet bunching in single UDP frames to save bandwidth
  - Time stamping to identify stale packets

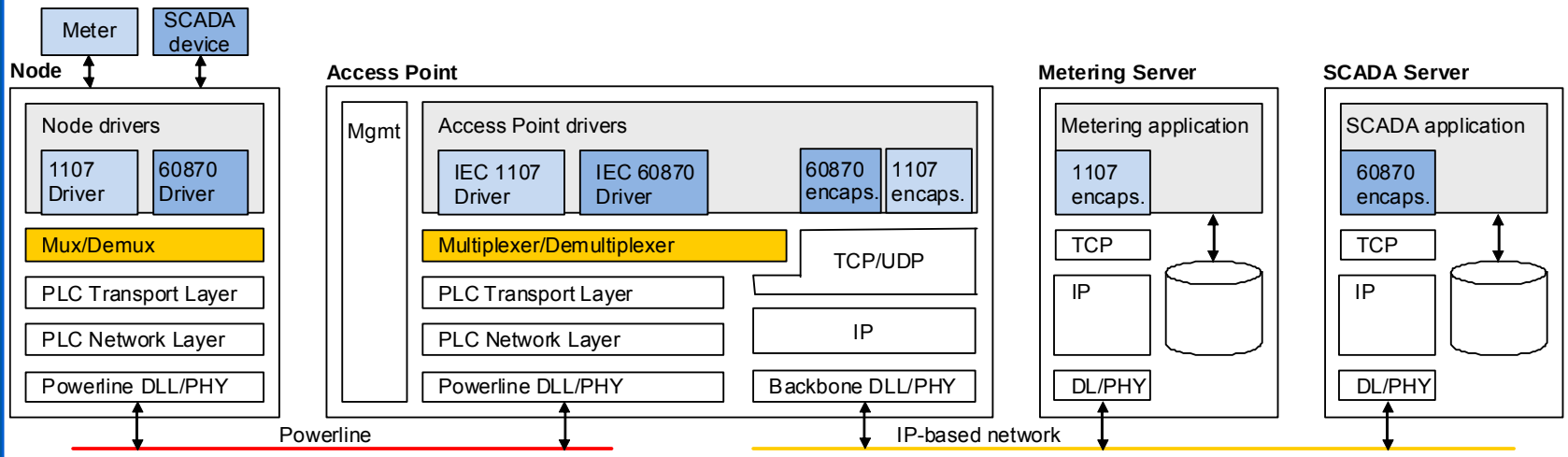
Communication in Smart Grids



* T. Sauter and M. Lobashov, End-to-end Communication Architecture for Smart Grids, *IEEE Trans. on Industrial Electronics*, vol. 57, no. 4, 2011, pp. 1218-1228.

Communication Architecture for Smart Grids

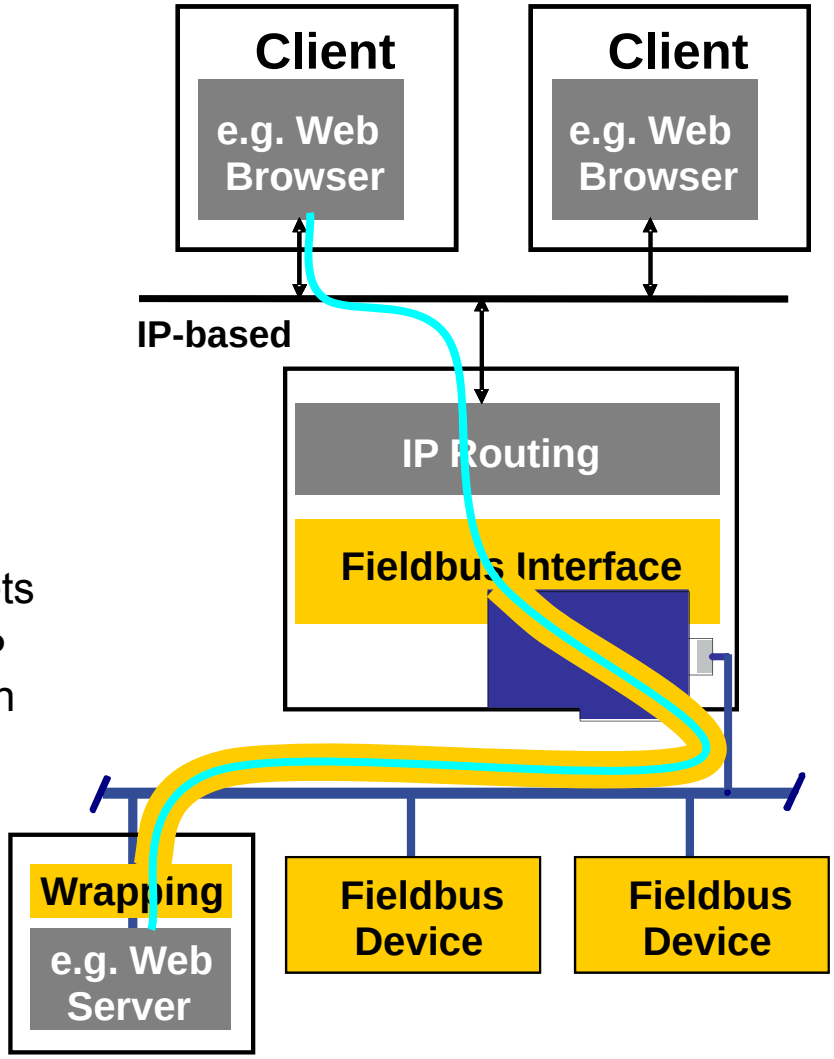
- Transparency for application protocols
  - Certification problems for billing data
  - Gateway not reasonable
  - Tunnelling solution preferred despite timing problems



* T. Sauter and M. Lobashov, End-to-end Communication Architecture for Smart Grids, *IEEE Trans. on Industrial Electronics*, vol. 57, no. 4, 2011, pp. 1218-1228.

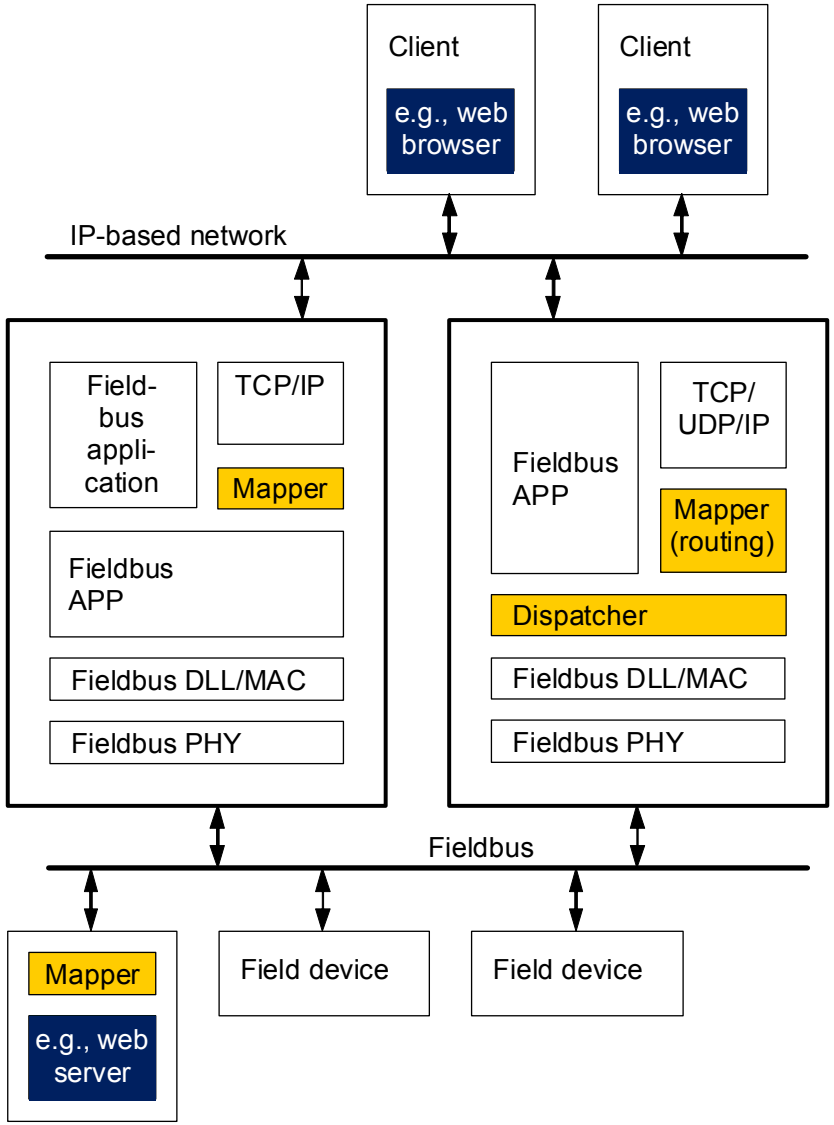
Possibility 2: Internet over Fieldbus

- Tunnelling of IP
- Special software at field device needed
  - IP+ stack
  - Probably web server
  - Data formatting
- Probably inefficient
  - Fieldbus performance
  - Segmentation of IP packets
  - Problems with timing of IP channel (response time) in slow fieldbusses
- Used for, e.g., device management



Software Architecture for Access Point

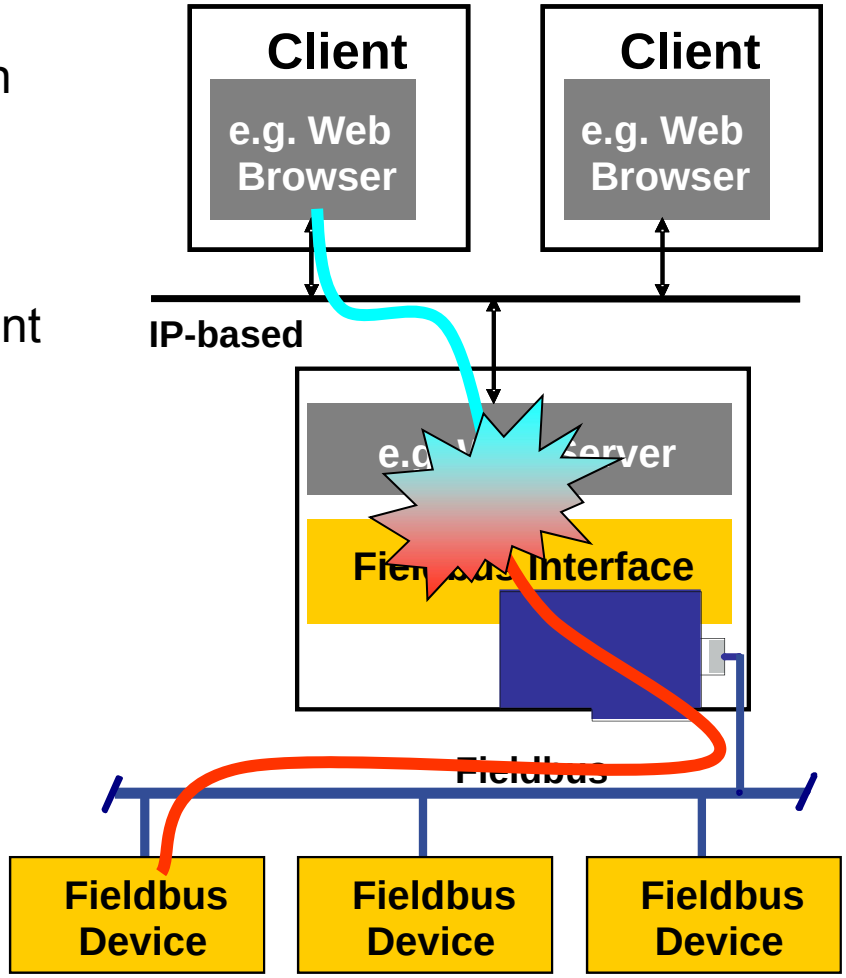
- Two essential problems
  - Traffic handling
  - Addressing
- Scheduling needed
  - No distortion of normal fieldbus operation
  - Two possibilities to insert IP traffic
  - Dispatching required if IP channel in parallel to application layer
- Addressing
  - “Tunnel” has different exits
  - Address mapping
  - Routing for IP traffic (probably NAT)



* T. Sauter, Fieldbus Systems – Embedded Networks for Automation, in: R. Zurawski (Ed.), *Networked Embedded Systems Handbook*, CRC Press, 2009, pp. 20-1 – 20-64.

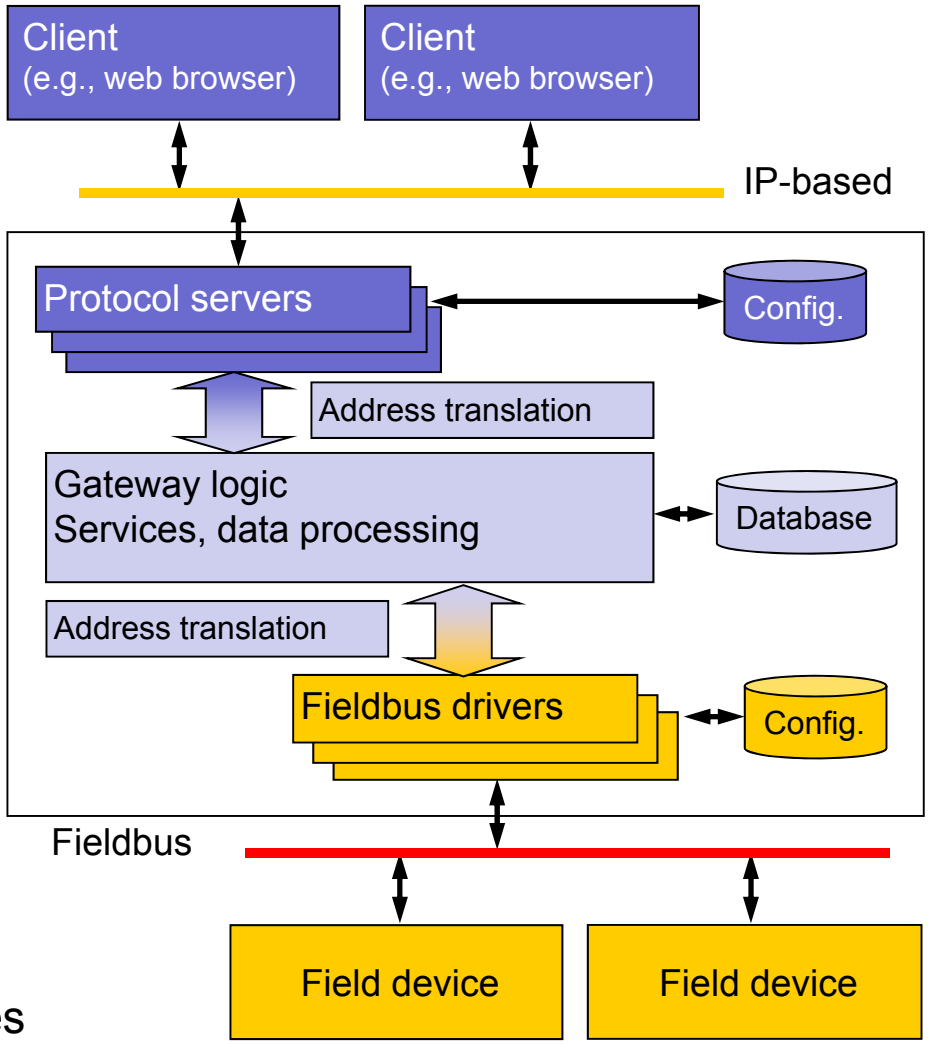
Possibility 3: Gateway

- Conversion at application layer
  - Translate data
  - Translate protocols
- Standard software at client side
  - Fieldbus-independent
  - User-friendly
- Proxy functionality
  - e.g., Profinet proxy for Profibus DP devices
- Possibility to include autonomous services
  - Process image



Gateway Architecture

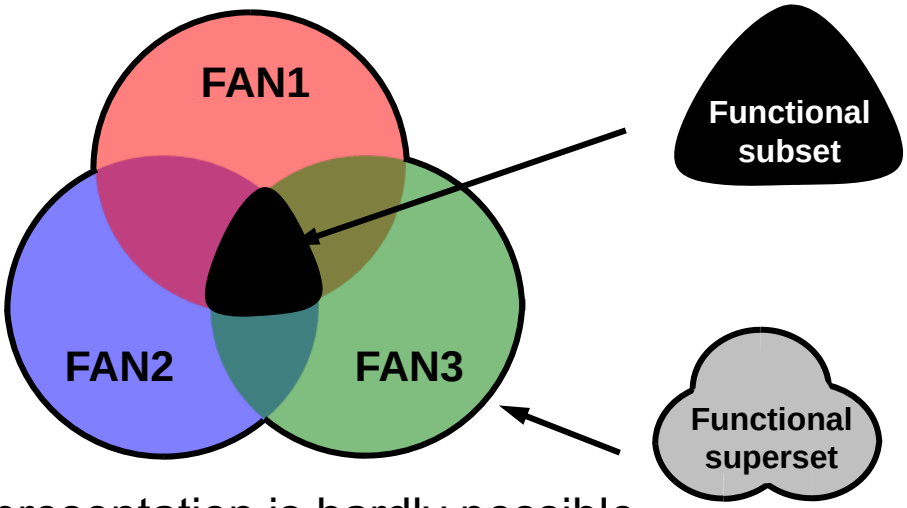
- Inclusion of fieldbus data in standard applications
  - Network management tools
  - Directory service tools
  - Databases
- Modular structure possible
  - Depends on implementation efforts
- Data point list
  - Function-oriented (flat list)
  - Structure-oriented (three-level hierarchy)
- Autonomous functionalities
  - Logging
  - Data monitoring
- Note: no real-time capabilities



* T. Sauter, Fieldbus Systems – Embedded Networks for Automation, in: R. Zurawski (Ed.), *Networked Embedded Systems Handbook*, CRC Press, 2009, pp. 20-1 – 20-64.

The Dilemma of Interoperability

- How to deal with different fieldbus functionality and data types?
  - Data abstraction entails loss of information/precision
- E.g., representation of a switch object
  - Boolean parameter (on/off)
  - Boolean parameter (on/off) and percentage value (high power switches)



- Universal fieldbus object representation is hardly possible
  - Despite lots of efforts (NOAH, IEC 61804)
- Note: Interoperability also needed on IP side
  - Client applications

* T. Sauter and M. Lobashov, How to Access Factory Floor Information using Internet Technologies and Gateways, *IEEE Trans. on Industrial Informatics*, vol. 7, no. 4, 2011, pp. 699-712.

Industrial **Inter**net

- XML is the de-facto standard for description of automation data
  - Formal and concise
  - Uncomplicated and human readable
  - Separation between data, their description, and presentation
  - Most important: supports automated processing
- SOAP as generic high-level communication protocol
  - Designed for distributed architectures
  - Simple, lightweight protocol to share data
  - Uses XML Schemas and (mostly) HTTP
  - Broad support on all computing platforms
- Web services as yellow-page services for distributed systems
  - Standardized method for advertising devices and services
  - Specifies only abstract interfaces
  - Very flexible and platform-independent
  - Workflows on top of web services define actual processes
- Service-oriented architectures as latest trend

Efficiency?

- Response to “Read Data Point”, custom protocol

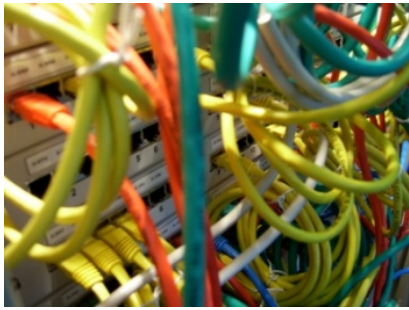
```
0 Pump1.Flow 1118849341.7106250 10.0
```

- Response to “Read Data Point”, OPC XML-DA

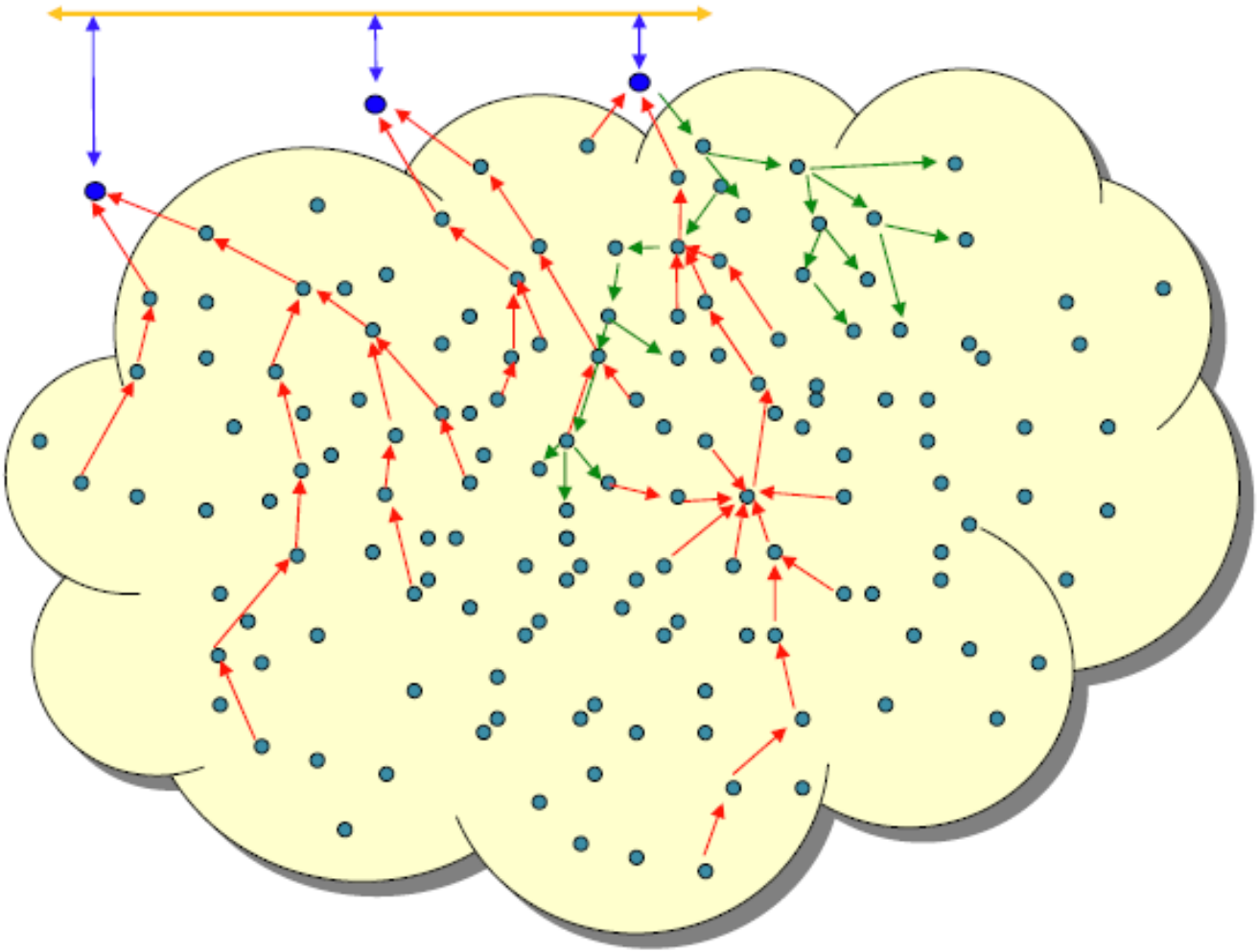
```
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope
 xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<soap:Body>
      <ReadResponse
    xmlns="http://opcfoundation.org/webservices/OPCDA/">
      <ReadResult RcvTime="2005-06-15T17:29:01.0649250+01:00"
                  ReplyTime="2005-06-15T17:29:01.0806200+01:00"
                     ClientRequestHandle="Handle1"
    RevisedLocaleID="en"
                  ServerState="running"/>
      <RItemList>
            <Items ItemName="Pump1.Flow" valuetype="xsd:float"
           TimeStamp="2005-06-15T17:29:01.7106250+01:00">
                        <Value xsi:type="xsd:float">10.0</Value>
            </Items>
      </RItemList>
      </ReadResponse>
</soap:Body>
</soap:Envelope>
```

Wireless Networks in Automation

- Reduction of wiring
  - Widely scattered, mobile nodes
  - Harsh environmental conditions
- Flexible infrastructures
  - Reconfigurable production systems
  - Flexibility support through the network
- Several available technologies
  - IT standards: WLAN, Bluetooth, WPAN
  - Automation standards: Wireless HART, ISA100.11a
- Challenges
  - Scalability and interoperability
  - Resource limitations on mobile nodes
  - Network planning and co-existence issues

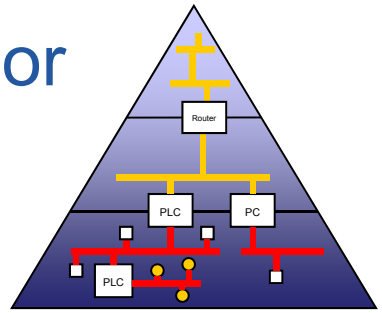


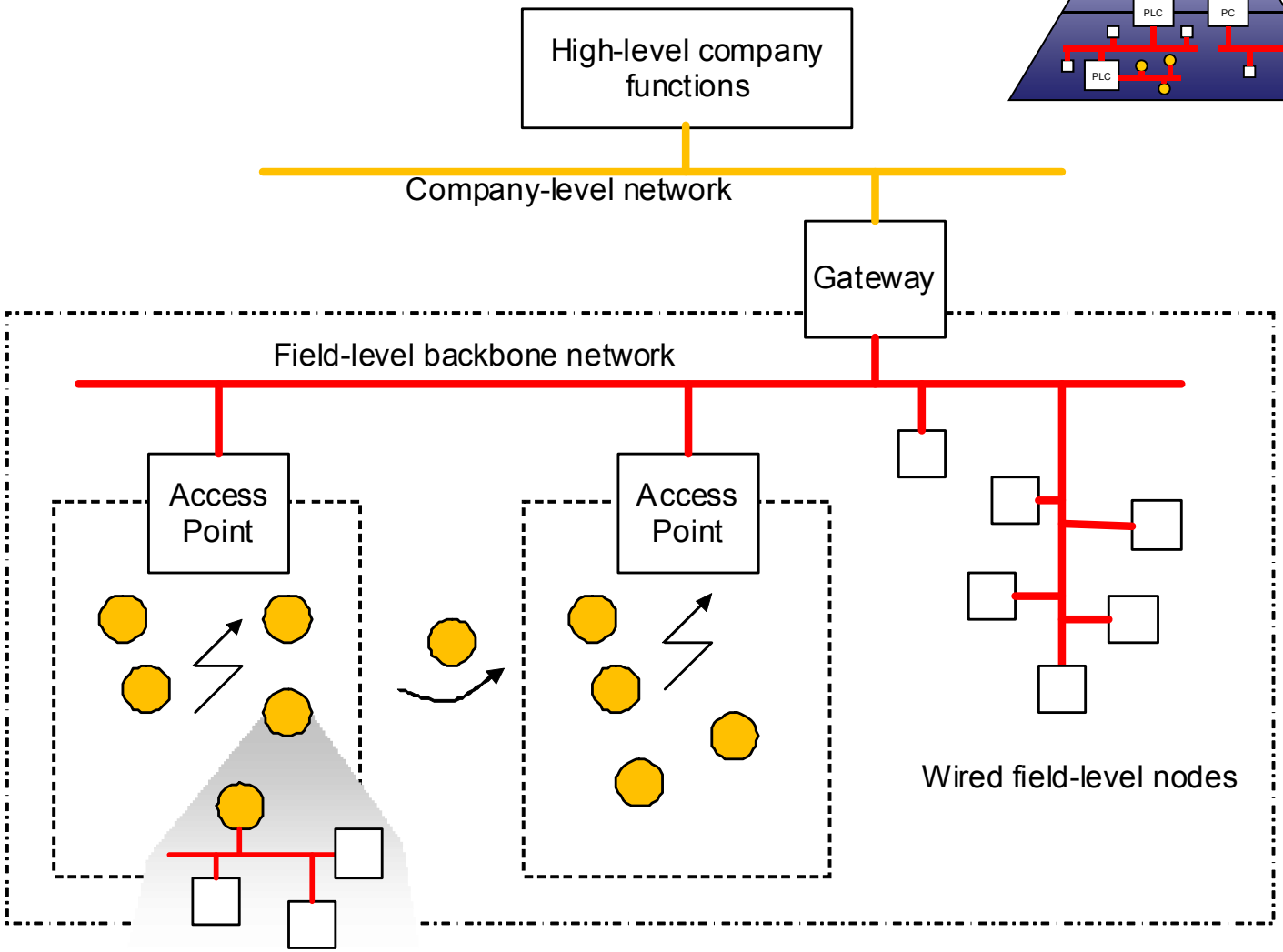
Wireless Sensor Network Vision



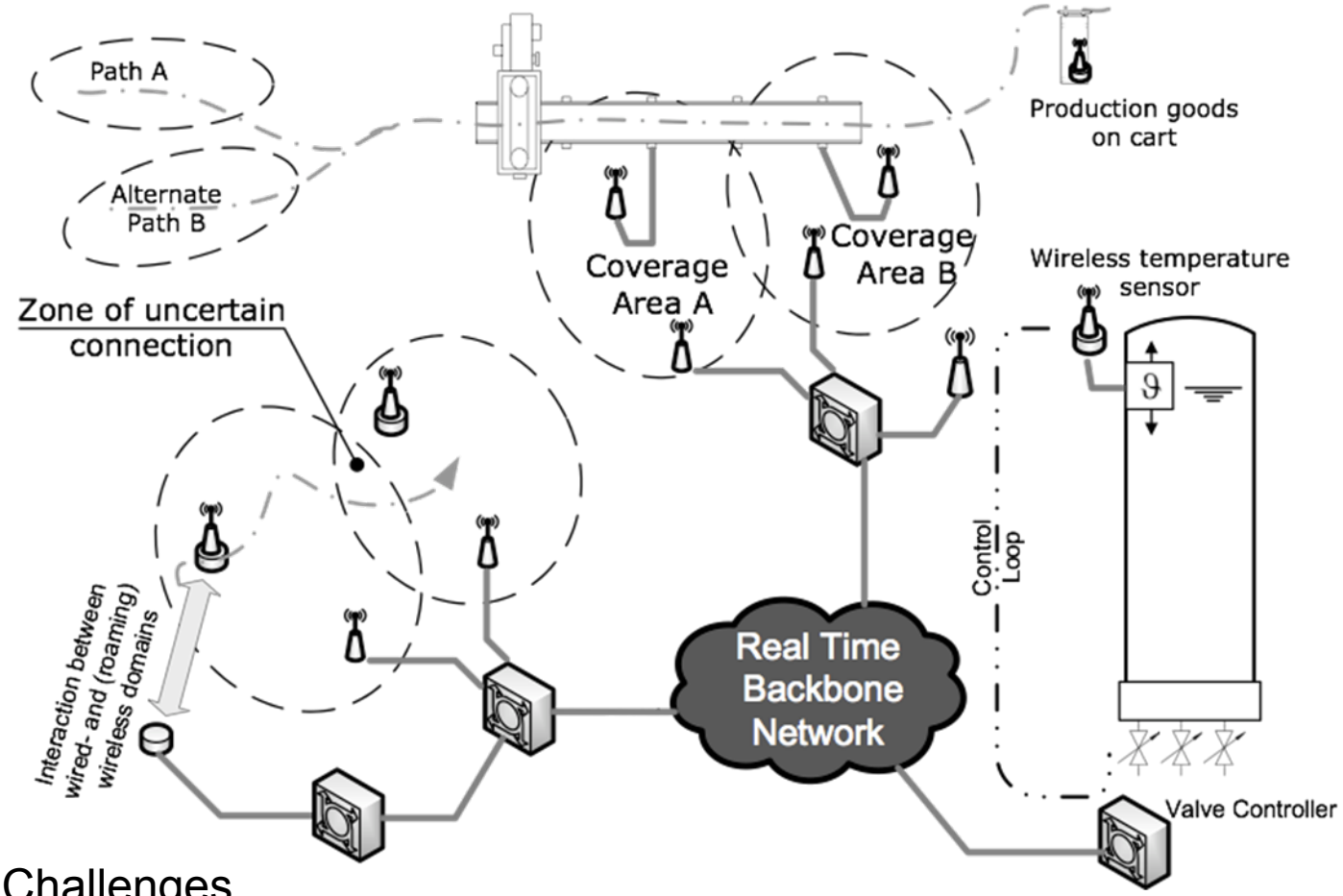
Center for Integrated Sensor Systems

Hybrid Networks on the Factory Floor





Hybrid Networks for Automation

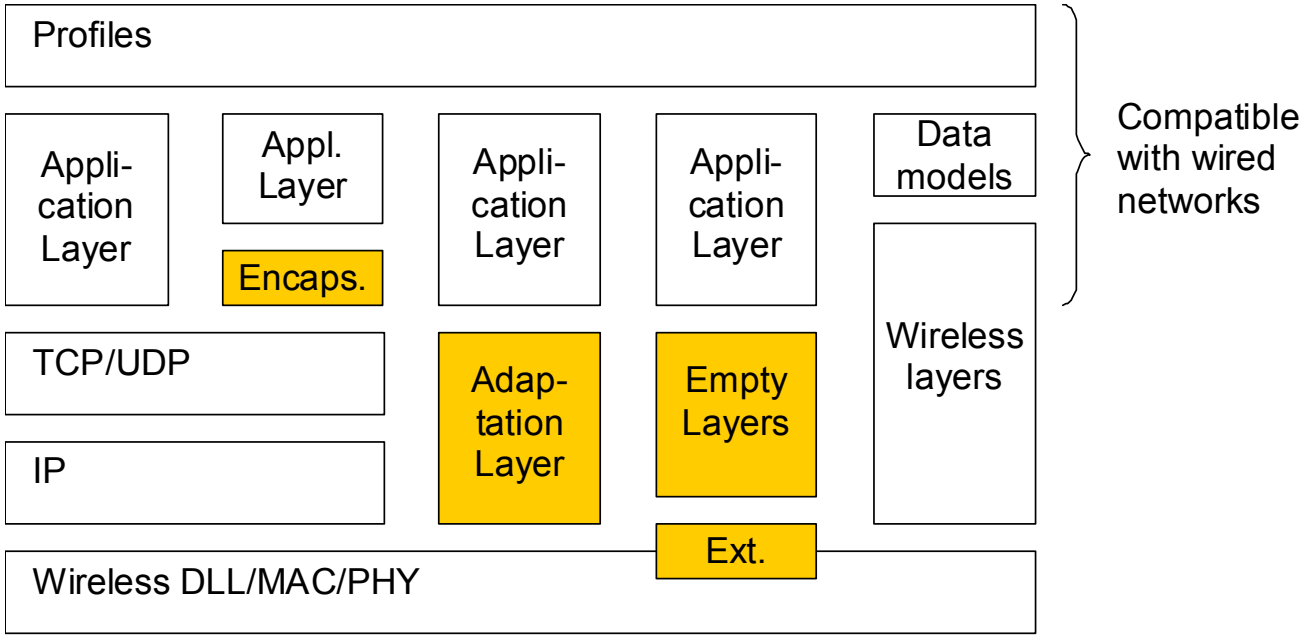


- Challenges
  - Large distances
  - Multiple Cells
  - Tracking and handover
  - Uniform real-time domain
  - Preservation of timing
  - Mastering network complexity

* T. Sauter, J. Jasperneite, and L. Lo Bello, Towards New Hybrid Networks for Industrial Automation, *IEEE ETFA*, Palma de Mallorca, 2009, pp. 1-8.

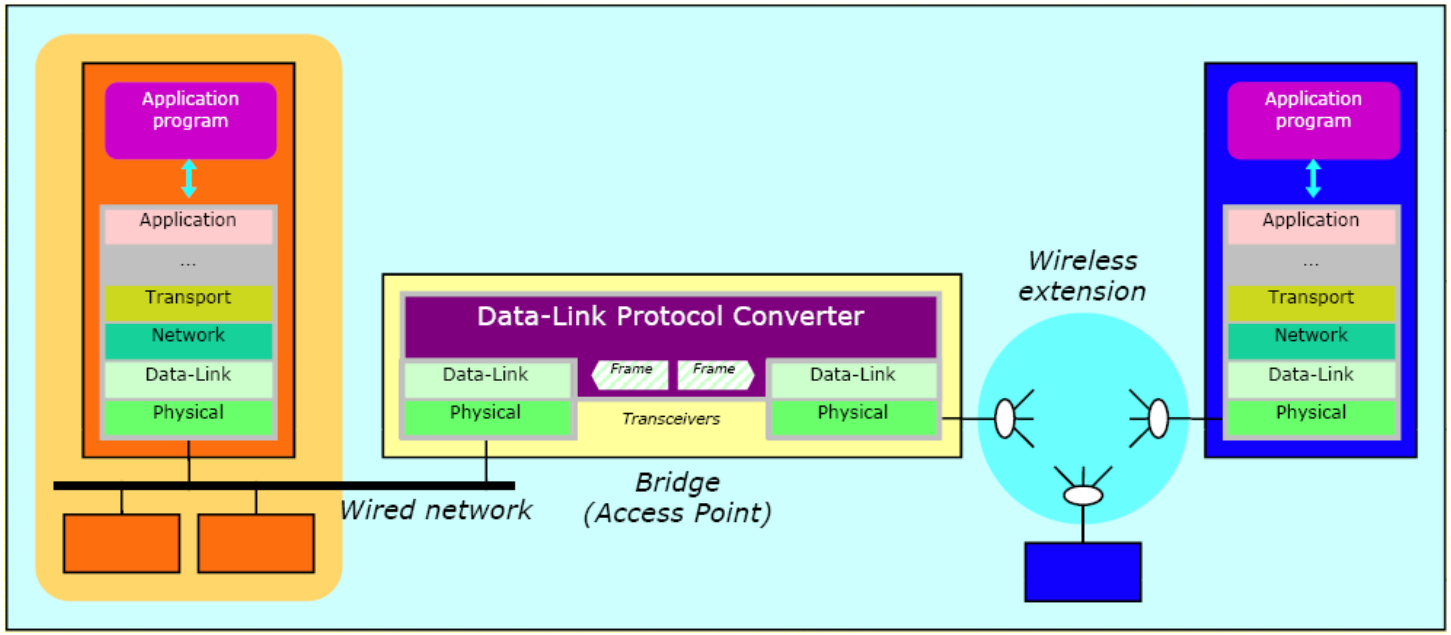
Achieving Compatibility with Wired Networks

- Similar approach as with Industrial Ethernet
  - Re-use of higher protocol layers



Interconnection on Data Link Layer (Bridge)

- Transparent flow of frames between the two systems
- Typical example: Access Points
  - Interconnection of wired and wireless network (WiFi)

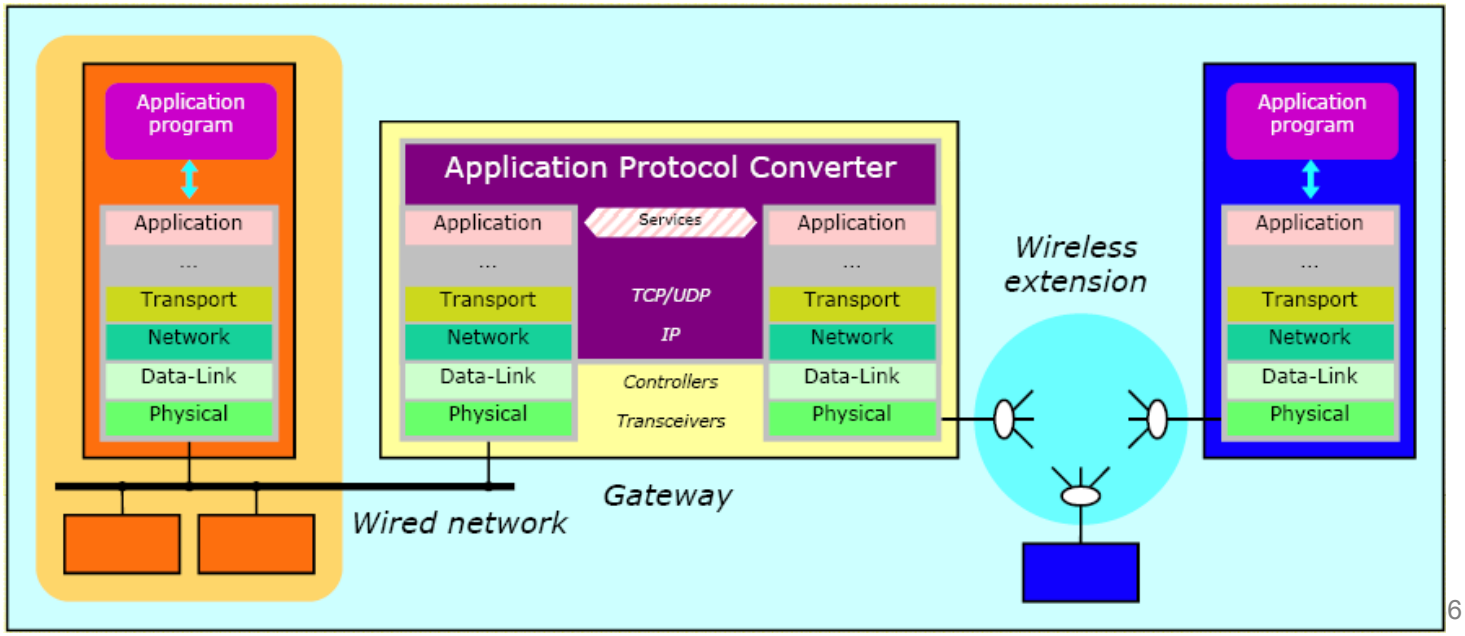


Data Link Layer Extensions

- Practically not feasible for fieldbusses
- Possible for some RTE networks
  - Attention to RT behavior
- In principle possible for IEEE 802.15.4
  - Even if data rate is quite low
  - Not suitable for LLC Type 1 services (non-confirmed connectionless)
- In principle possible for WLAN
  - Bridge functionality of Access Point
  - DLL protocols of RTE networks are typically different from legacy Ethernet
  - Better possibility: interconnection at higher layers using TCP/UDP

Interconnection on Application Layer (Gateway)

- Fully compliant with the protocol stacks of both networks
  - Transparent flow of application layer PDUs
  - Most versatile concept
- May operate as proxy
  - More services than a gateway
  - represents parts of a network as if they were a single node

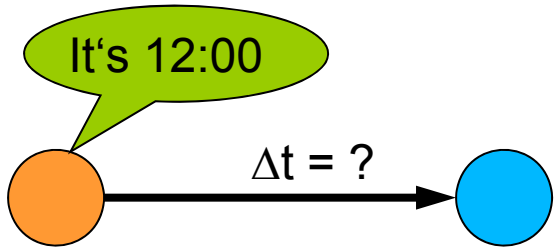


Contents

- Motivation
  - The big picture
- Integration aspects
  - Network interconnections
  - Hybrid wired/wireless networks
- Synchronization
  - The quest for accuracy
  - Localization of mobile devices
- Security
  - The big challenges
  - Practical solutions

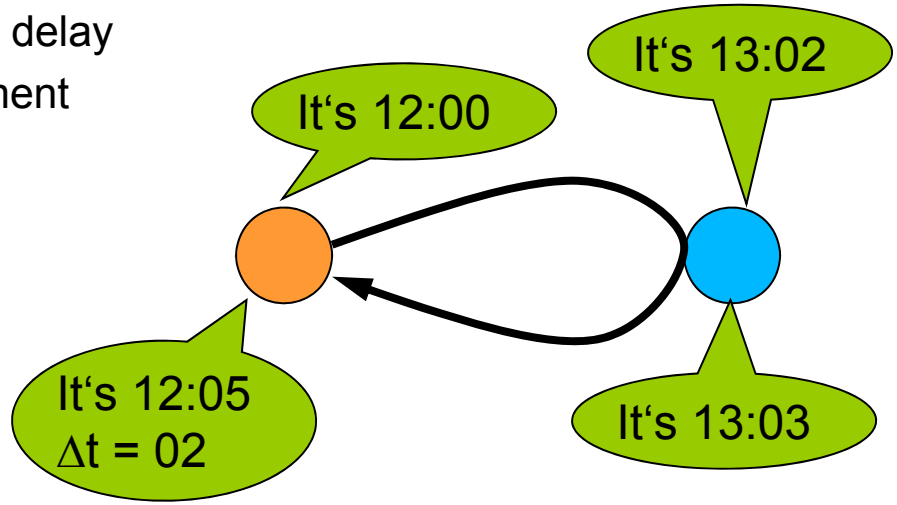
Clock Synchronization Principles

- Time is sent from reference clock to client
  - “Reference broadcast”
  - Network delay deteriorates result
  - Must be added to transmitted value



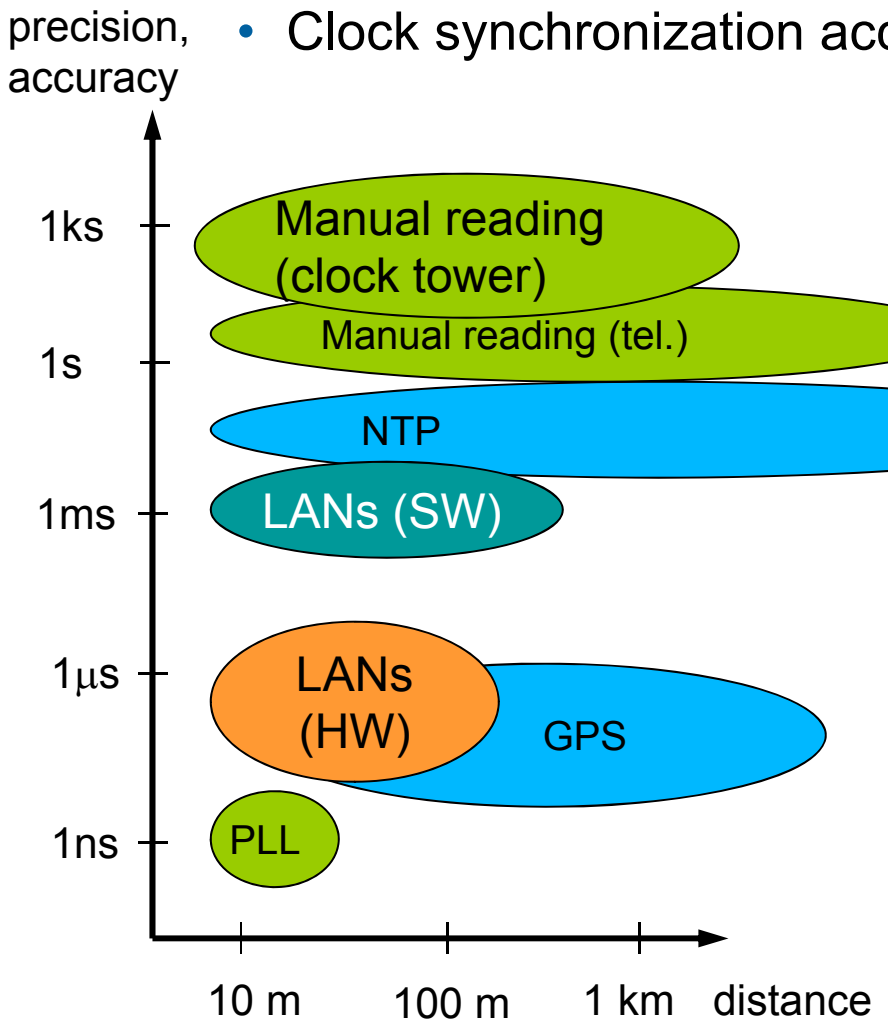
- Network delay must be measured
  - Round-trip delay
  - Timestamps are inserted in messages
  - Node knows communication delay
  - Jitter deteriorates measurement

- Special case: syntonization
  - Just frequency distribution
  - No absolute time



Various Approaches

- Clock synchronization accuracy in distributed systems



internal clock synchronization

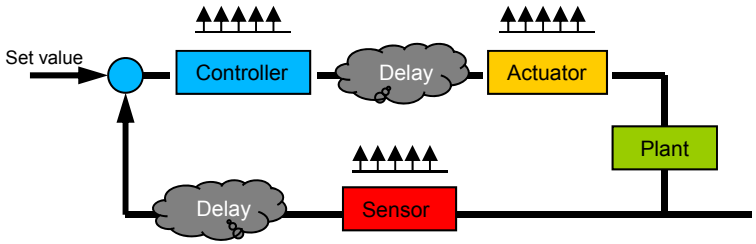
$$| C_p(t) - C_q(t) | \leq \varepsilon \quad \forall \{p,q\}$$

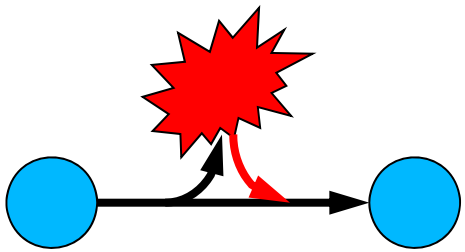
external clock synchronization

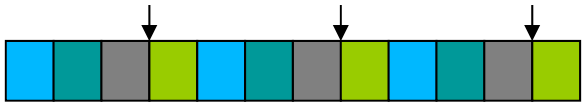
$$| C_p(t) - t | \leq \varepsilon \quad \forall p$$

What for? – Application Fields

- Distributed measurement systems
  - Synchronized data sampling
- Distributed control systems
  - Correlation of sensor signals
  - Synchronization of actors
- Reliable data transmission
  - Safety-critical systems
- Secure data transmission
  - Avoidance of replay attacks
- Network access
  - Basis for TDMA schemes

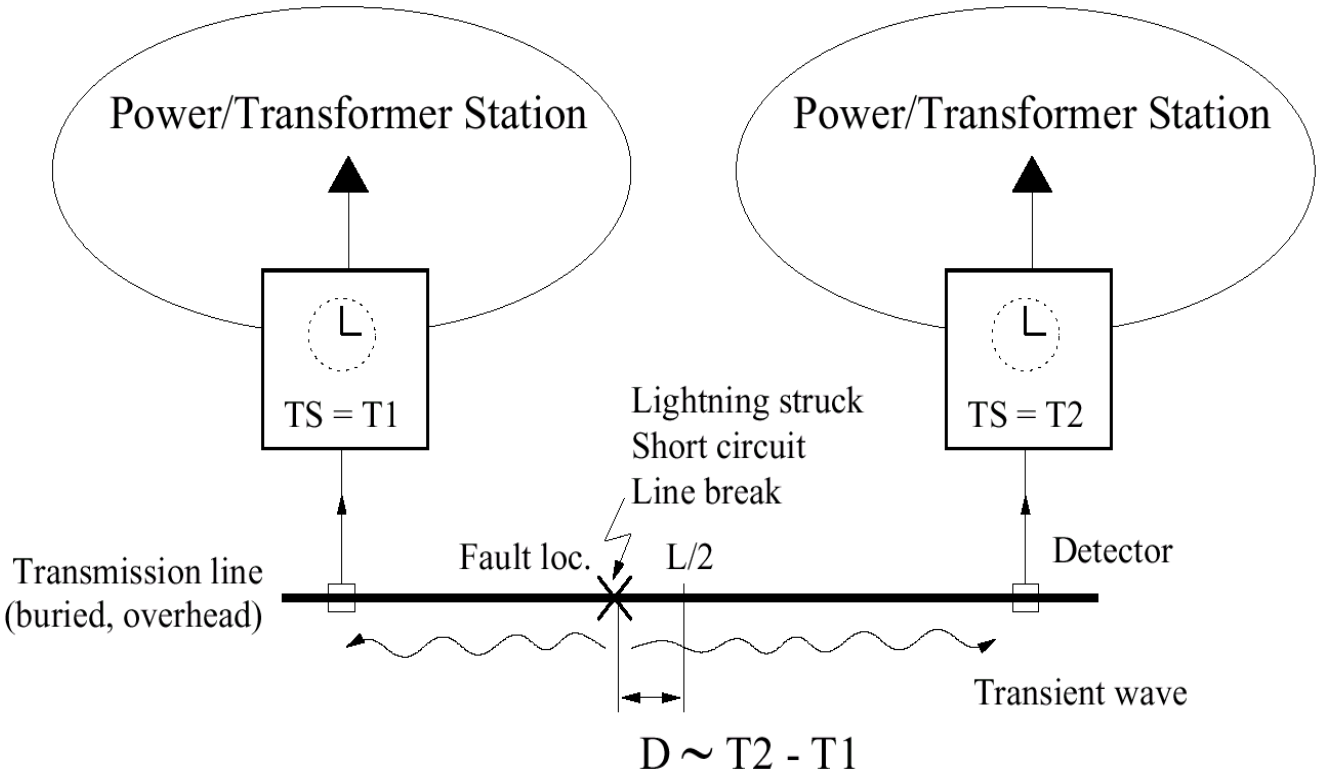




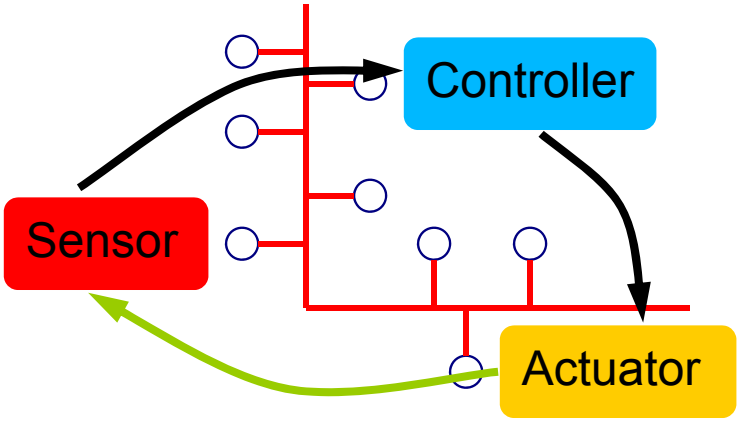


Distributed Measurements

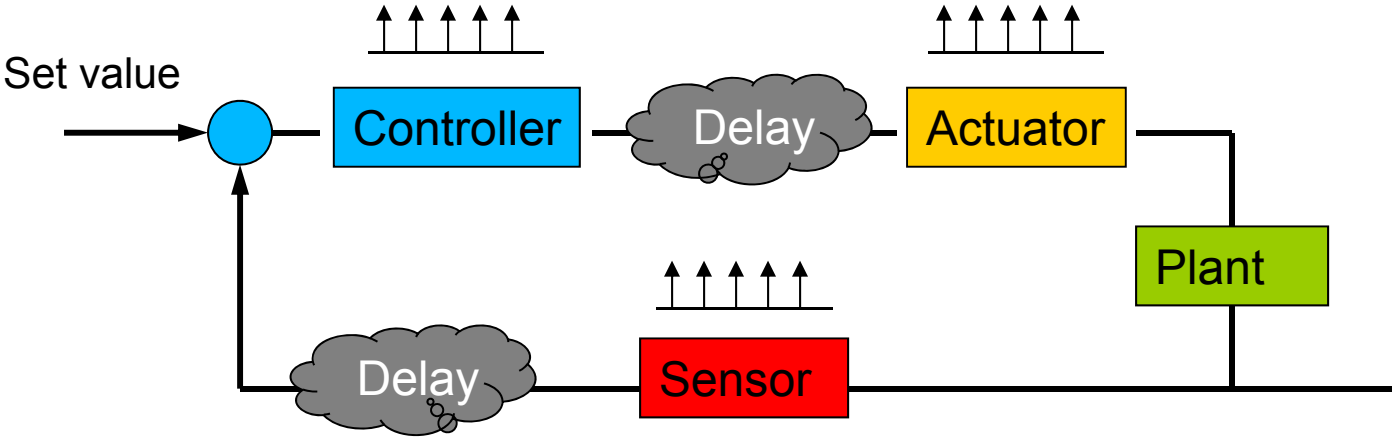
- Detection of power line failures
  - Delay analysis of transient signals
  - Location range ± 10 m ⇒ 10 ns accuracy



Network-based Control Systems



- Fieldbus/Ethernet means
  - Sampling of data
  - Network/processing time
  - Introduction of (variable) delays
  - Delays can be held constant with synchronized clocks
  - Correlation of sensor/actuator actions

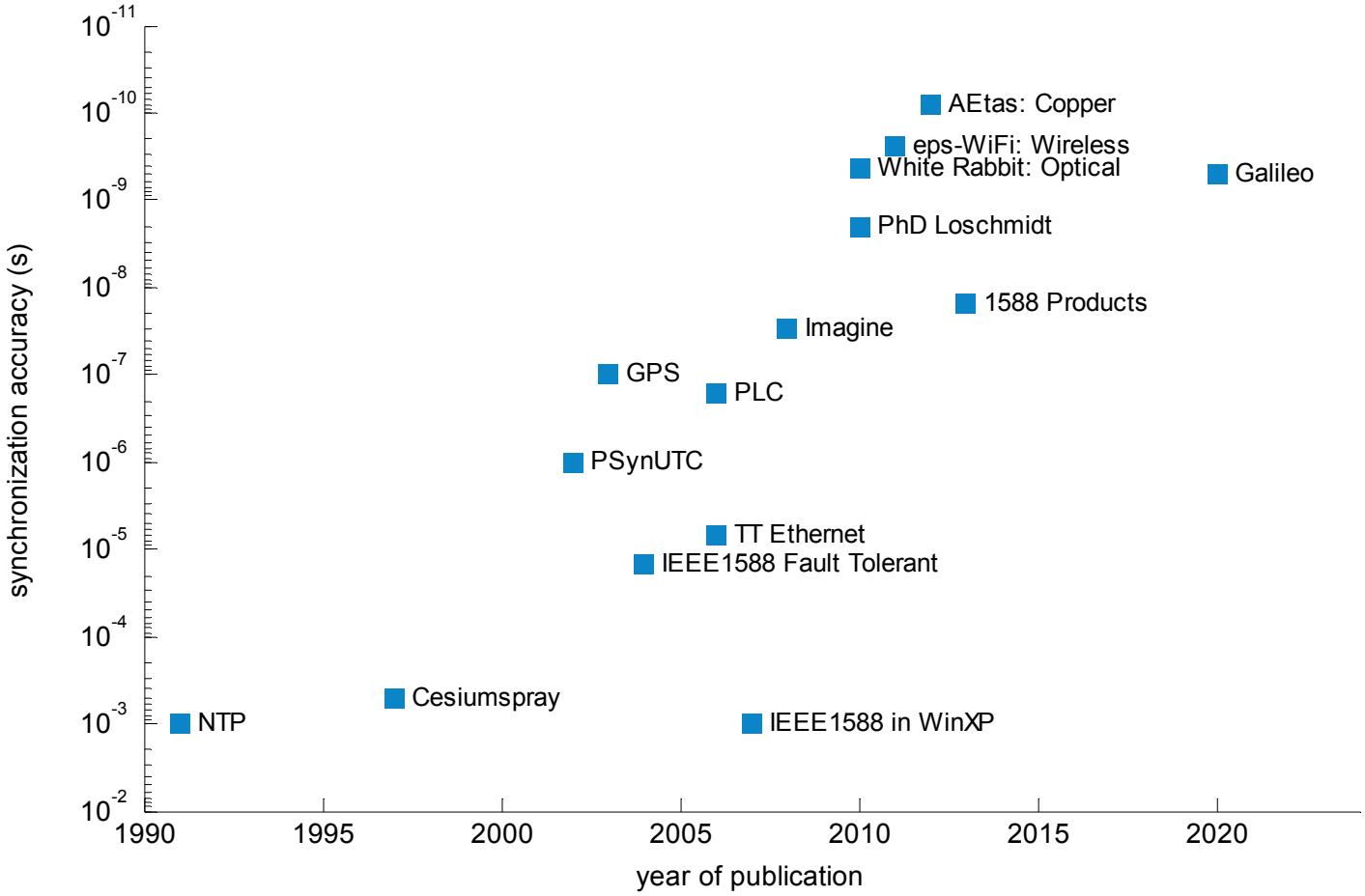


Large Scale Physics: CERN – LHC Timing

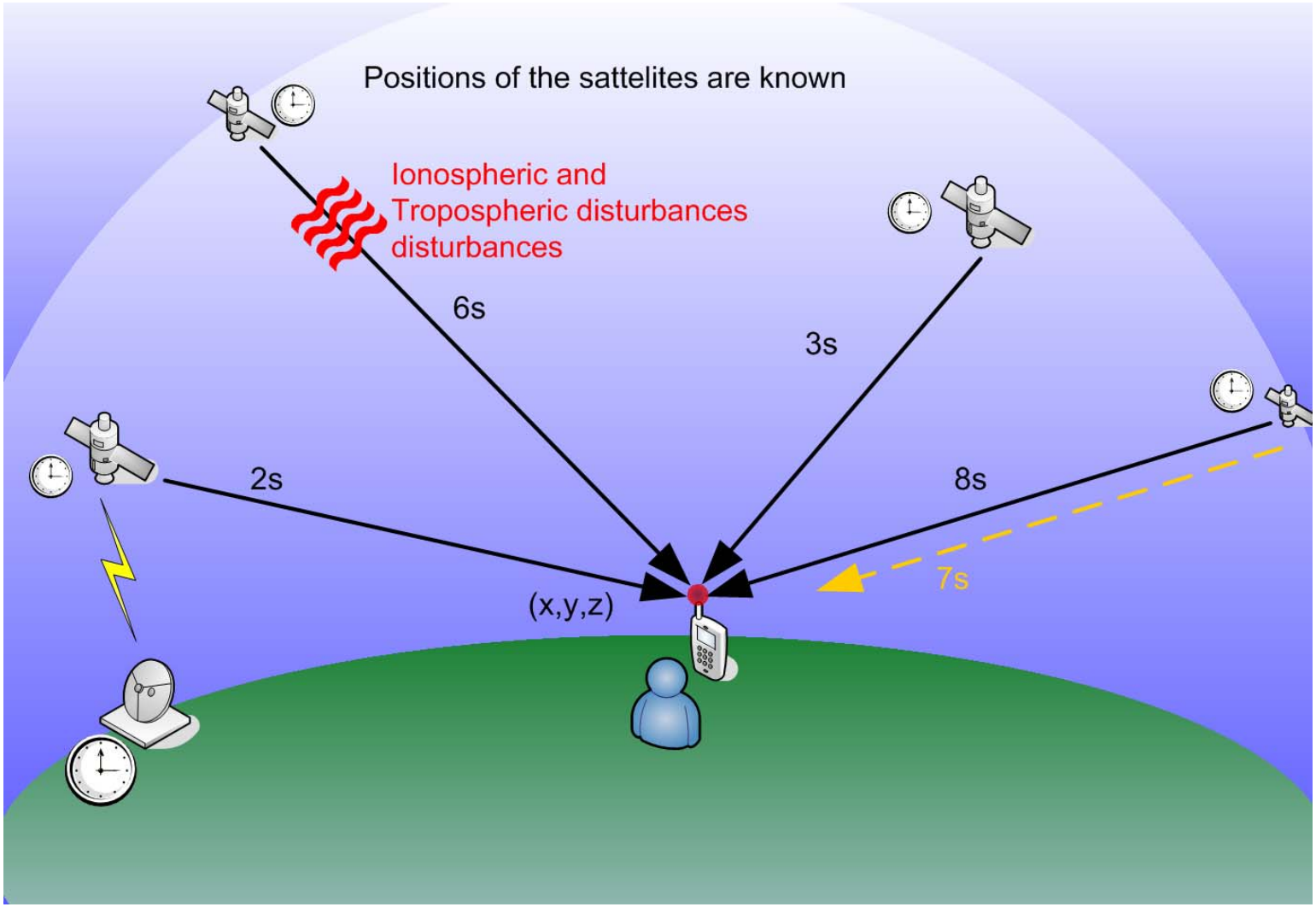
- Large-Scale Distributed Network
  - Timing system is needed to control the magnets of the accelerator ring
  - 2000 nodes
  - Circumference: 27 km
  - Tough timing requirements (100 ps)

- Typical example
  - Emergency shutoff
  - Energy in the beam has to be lead out in a controlled way
  - Time to react ~0.5-3 s

Clock Synchronization Accuracy

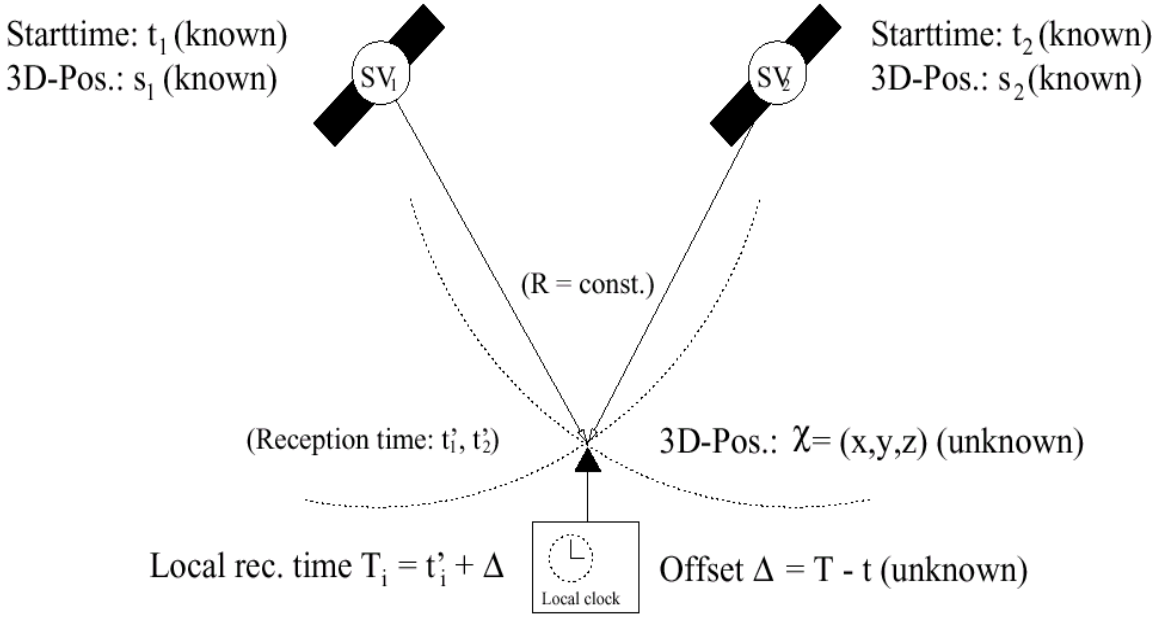


GPS


Positions of the sattelites are known
Ionospheric and
Tropospheric disturbances
disturbances
6s
3s
2s
8s
7s
(x,y,z)

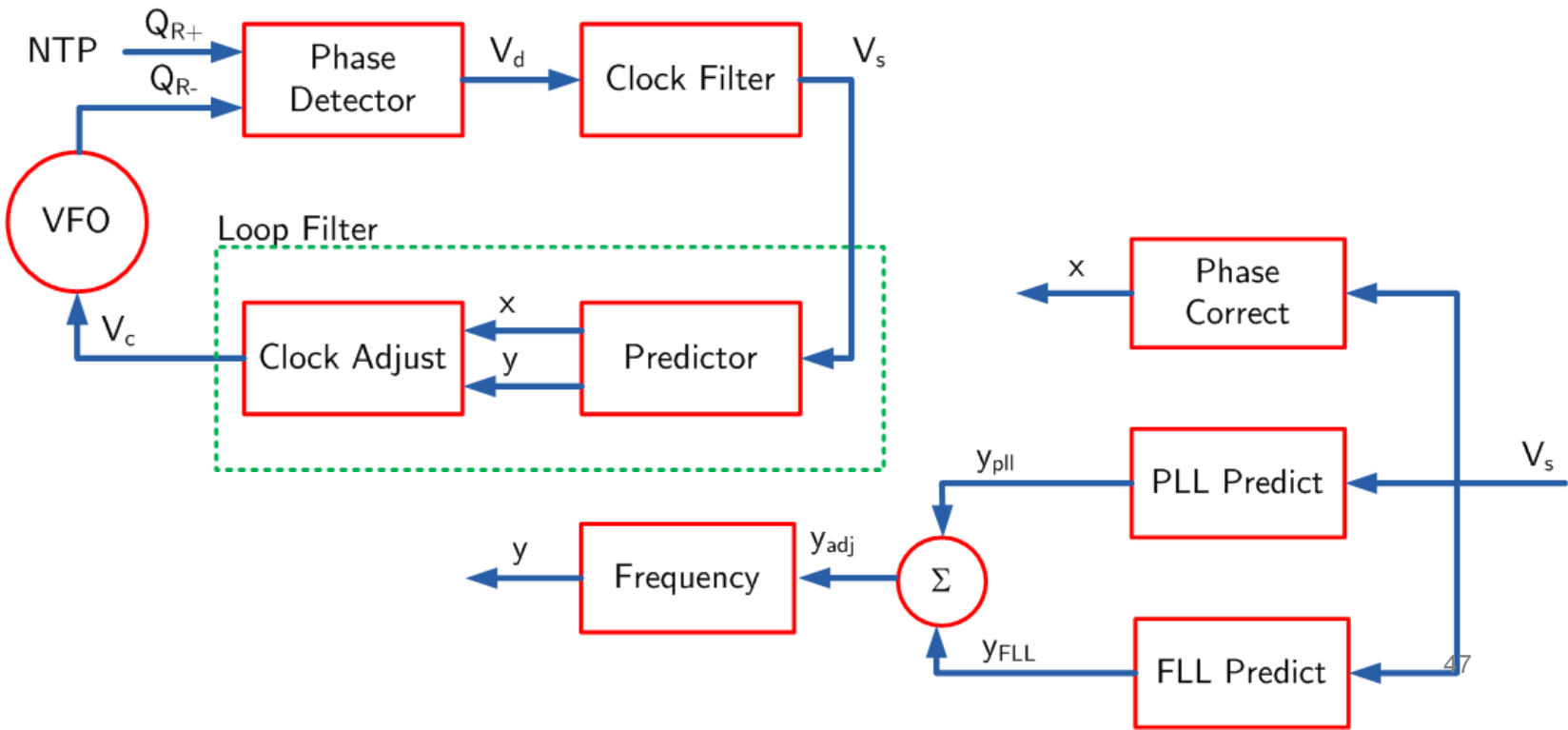
Clock Synchronization at GPS Receiver

- 4 satellites to determine (x,y,z) and Δ
- 1 satellite is sufficient for Δ if (x,y,z) is known
  - If Δ is constant



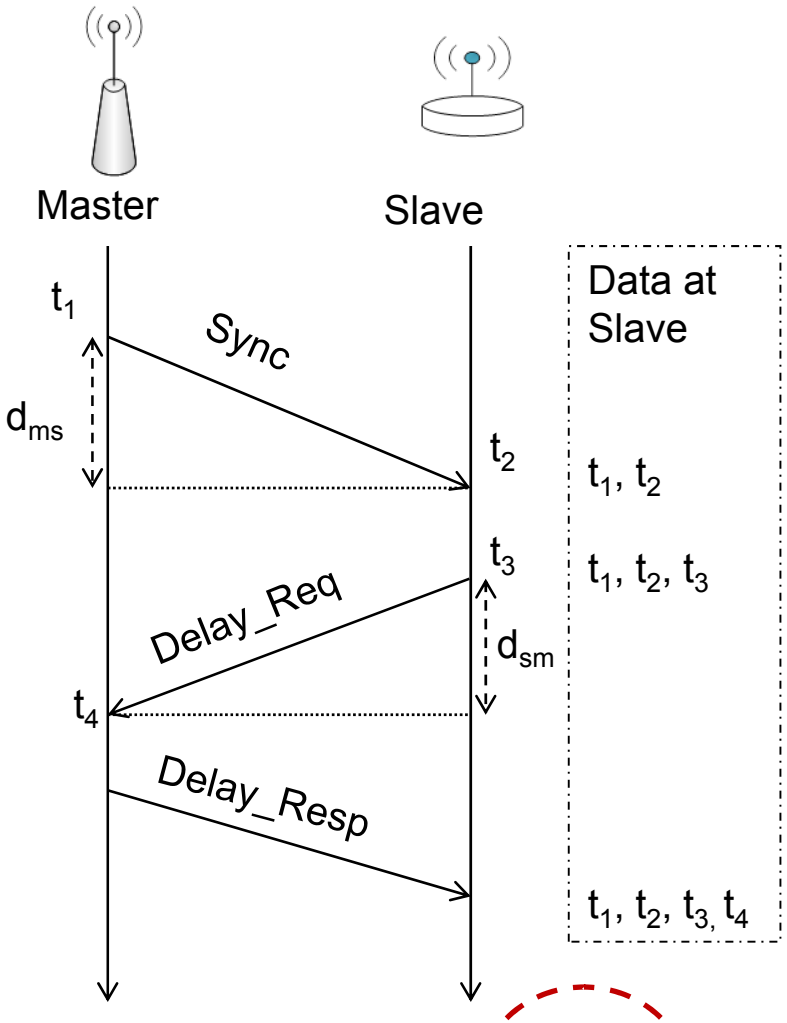
NTP - Network Time Protocol

- Structure
  - Minimum-weight spanning tree of time servers
  - Remote clock reading of all peer time servers
  - Well engineered statistical algorithms for data filtering and clock selection



IEEE 1588 Standard

- IEEE Standard (2002)
  - Origin in instrumentation and measurement
- Master-Slave based
  - “best master” election
  - Stratum based (clock quality)
- Defines protocol for time information exchange
  - PTP (Precision Time Protocol)
  - Network-independent
  - Mostly Ethernet-based
  - „Delay Request“ and „Delay Response“ packets
- No actual synchronization algorithm

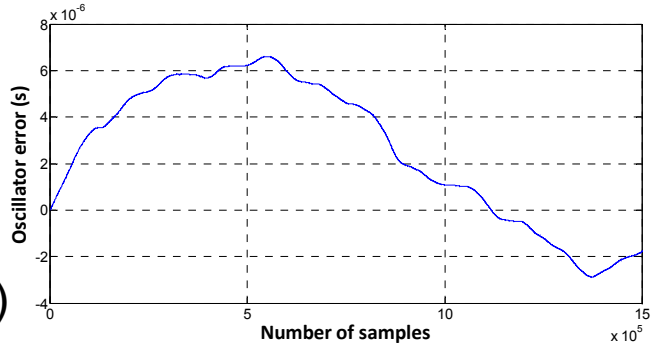


$$Offset = \frac{(t_2 - t_1) - (t_4 - t_3)}{2} \pm \frac{d_{ms} - d_{sm}}{2}$$

$$Delay = \frac{(t_2 - t_1) + (t_4 - t_3)}{2}$$

What Remains: Oscillator Drift

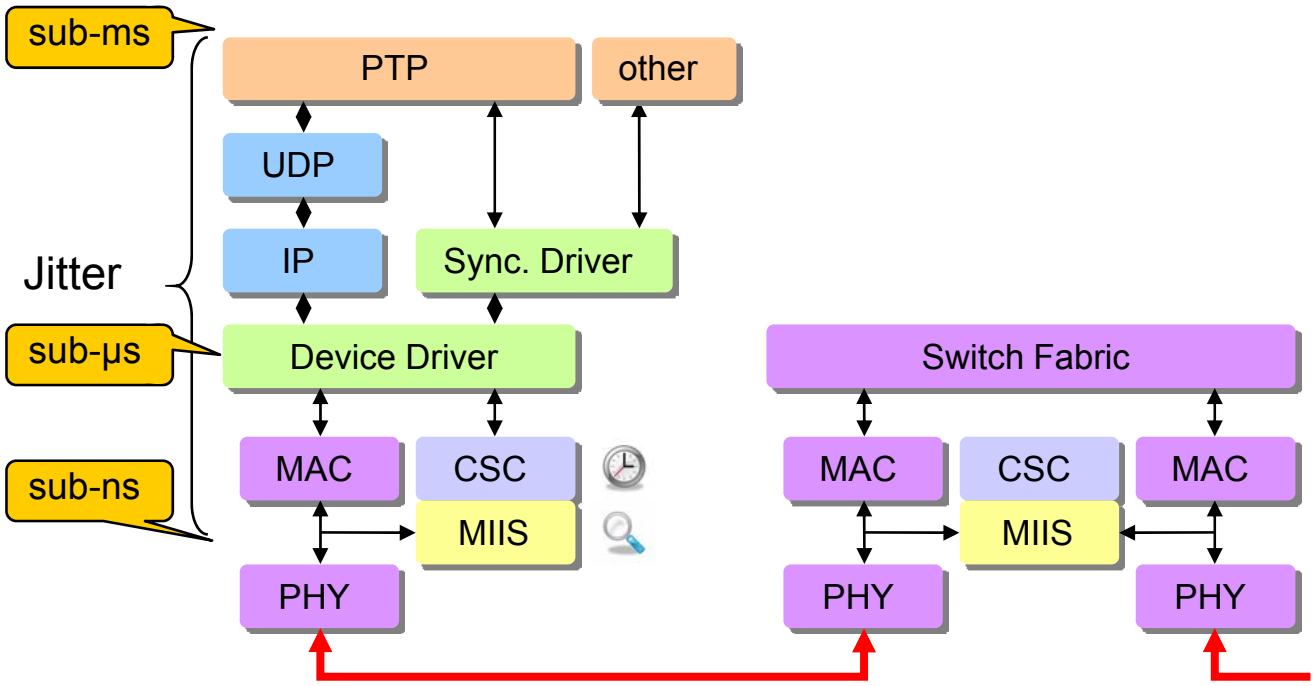
- External crystal oscillator (XO, TCXO, MCXO, OCXO)
  - Temperature influence can be controlled
  - Integrated heating or active compensation
  - Higher production costs
- How to compensate for residual drift?
  - $C(t)= (at+b) + \varepsilon_o(t)$
  - Linear model only very coarse
- Pure adjustment of value (clock state)
  - Simple and stable procedure (algorithm)
  - Drift variances are not corrected
- Rate Adjustment
  - Current state is adjusted regularly
  - Clock rate difference is monitored over several periods
  - Increment value is tuned



* G. Gaderer, P. Loschmidt, and T. Sauter, Improving Fault Tolerance in High-Precision Clock Synchronization, *IEEE Trans. on Industrial Informatics*, vol. 6, no. 2, 2010, pp. 206-215.

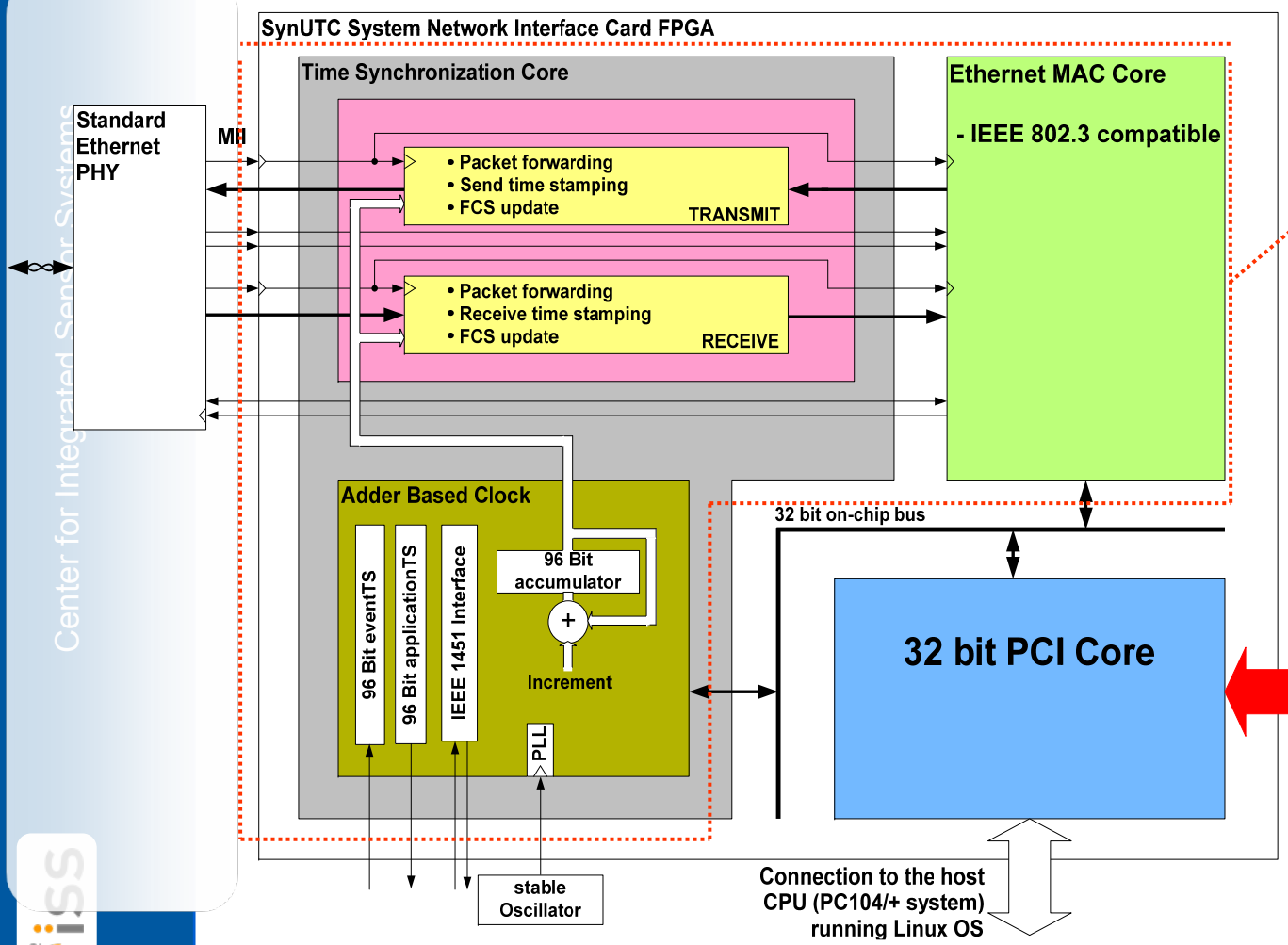
Where to Timestamp?

- Timestamp jitter reduces accuracy
- Timestamping as “low” as possible in protocol stack
- Hardware timstamps are better than software timestamps
  - But higher implememtation effort



* R. Höller, T. Sauter and N. Kerö, Embedded SynUTC and IEEE 1588 Clock Synchronization for Industrial Ethernet, *IEEE ETFA*, Lisbon, 2003, pp. 422-426.

Implementation for Network Interface Card



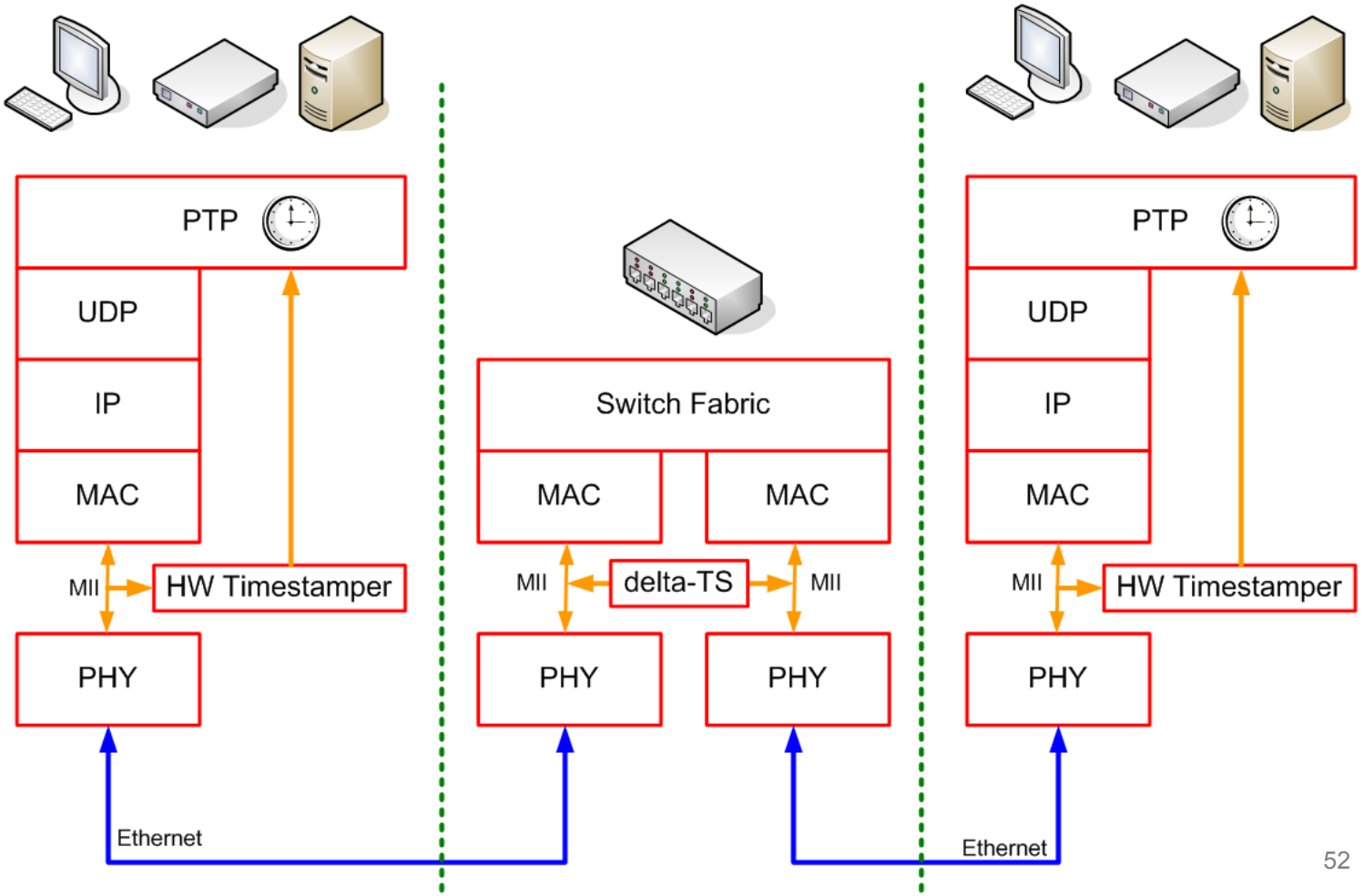
Easy integration in an Ethernet MAC IP Core

32 bit CPU Core
- -uCLinux operating system
- -IP/UDP stack
- -IEEE 1588 PTP stack
- -Clock synchronization algorithm

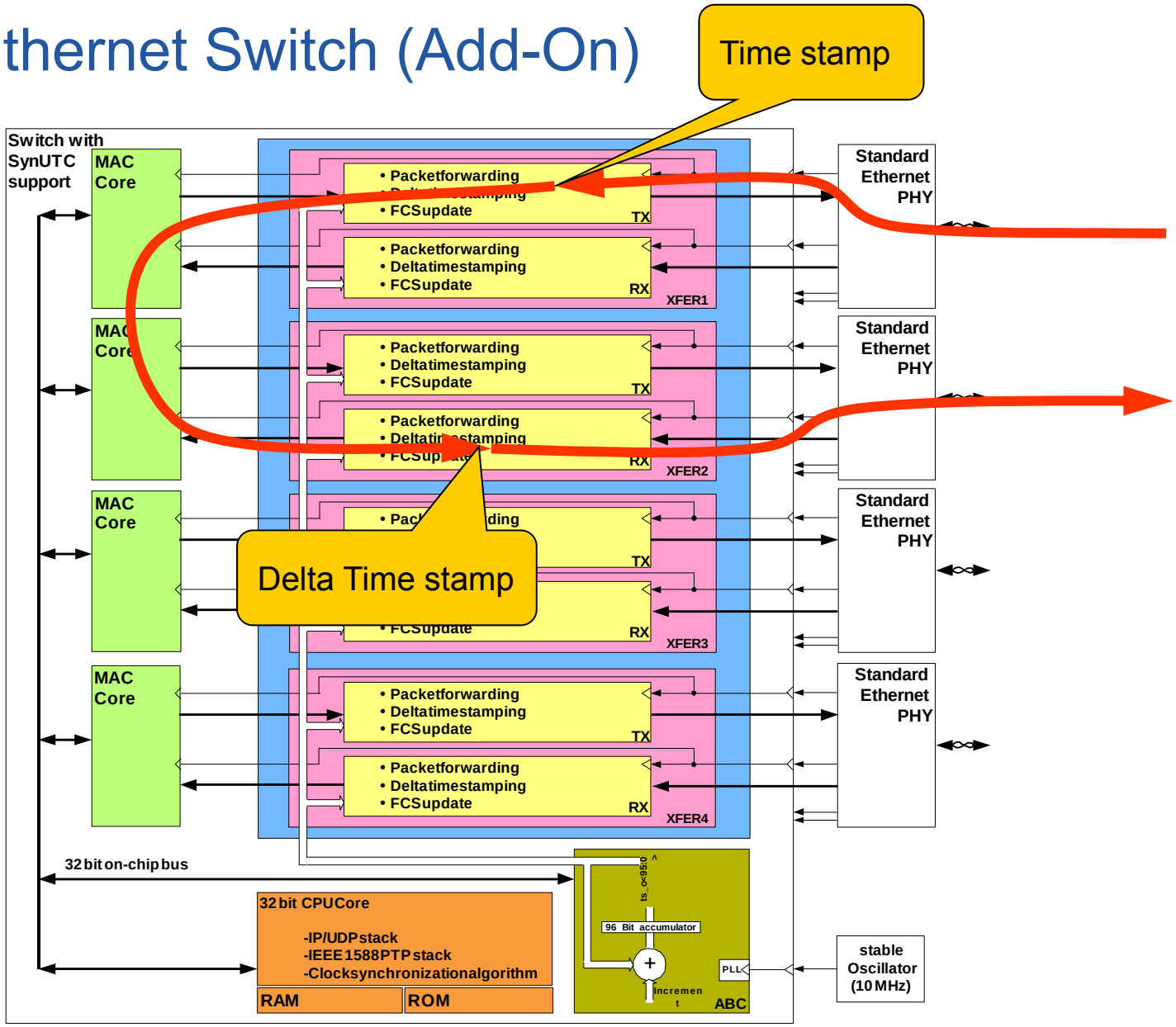
RAM | ROM

The Need for “Transparent Clocks”

- For switches or other relay nodes

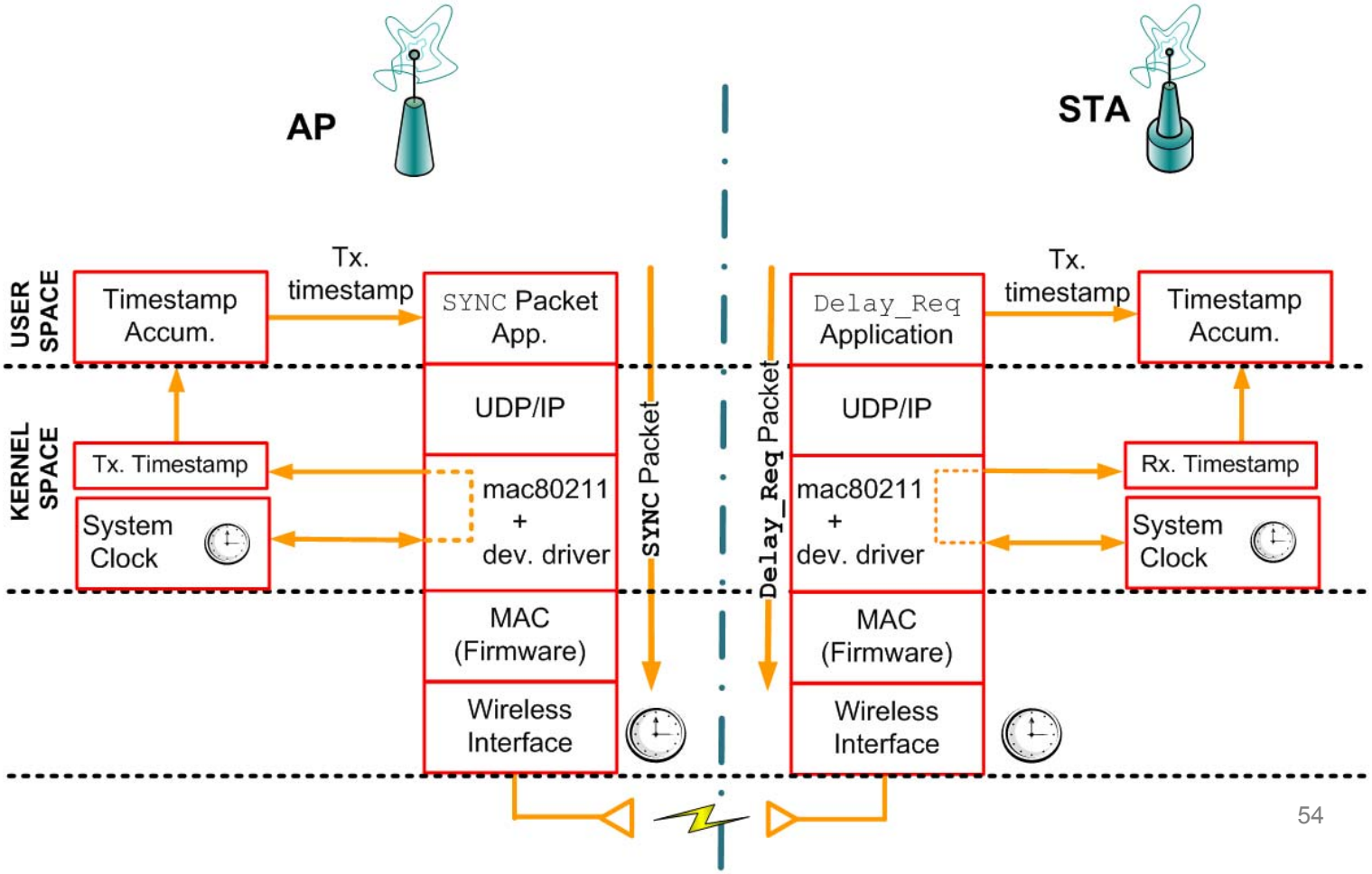


Ethernet Switch (Add-On)

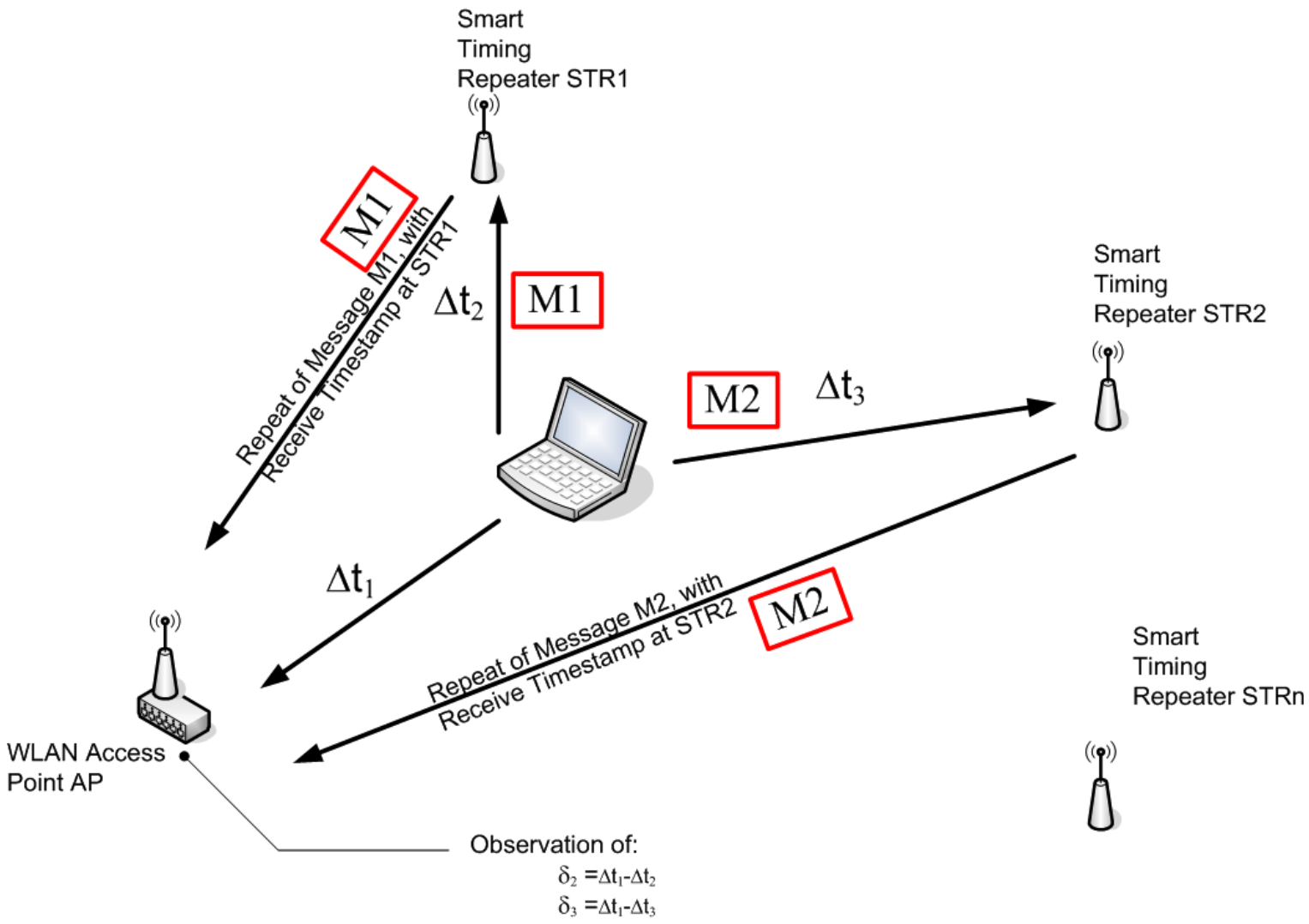


Synchronizing Clocks with WLAN

- Same idea as in Ethernet
  - Attach to interface between PHY and MAC



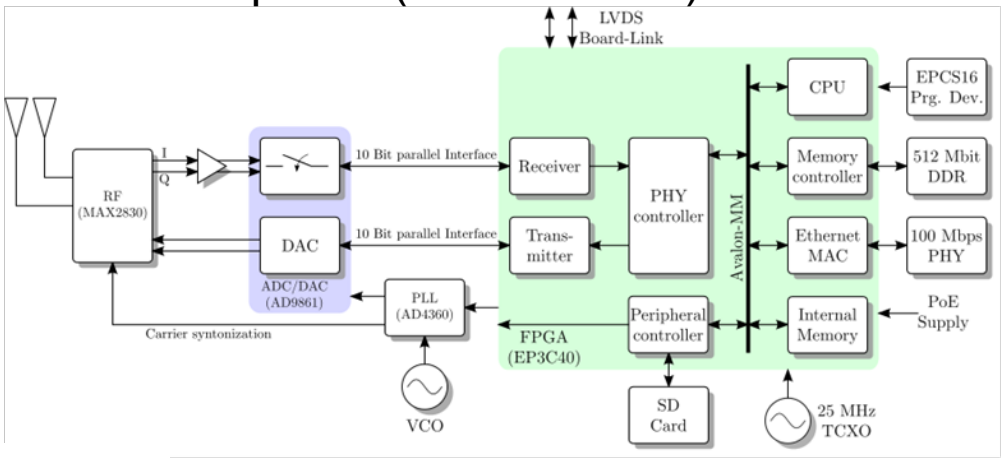
TDoA Localization of Mobile Nodes

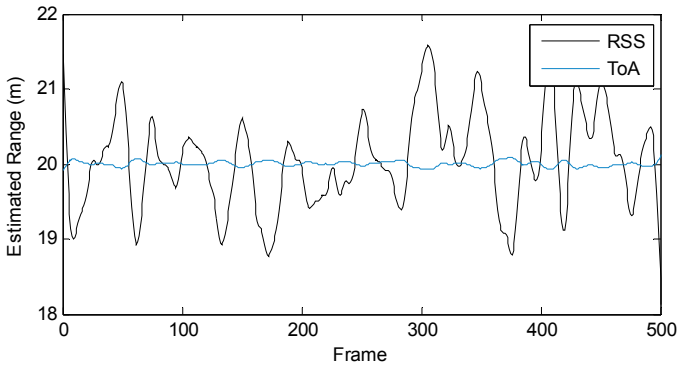


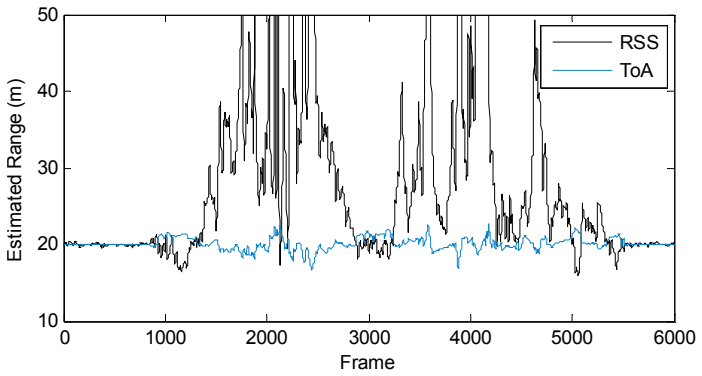
* P. Loschmidt, G. Gaderer, and T. Sauter, Clock Synchronization for Wireless Positioning of COTS Mobile Nodes, *IEEE ISPCS*, Wien, 2007, pp. 64–70.
* G. Gaderer, T. Sauter, F. Ring, and A. Nagy, A novel, wireless sensor/actuator network for the factory floor, *IEEE Sensors*, Hawaii, Nov. 2010, pp.940-945.

TDoA Localization of Mobile Nodes

- Time-based measurement more accurate than signal strength
- Dedicated WLAN hardware with 40 ps timestamp jitter
- Precise synchronization of access points (1 ns ~ 30 cm)

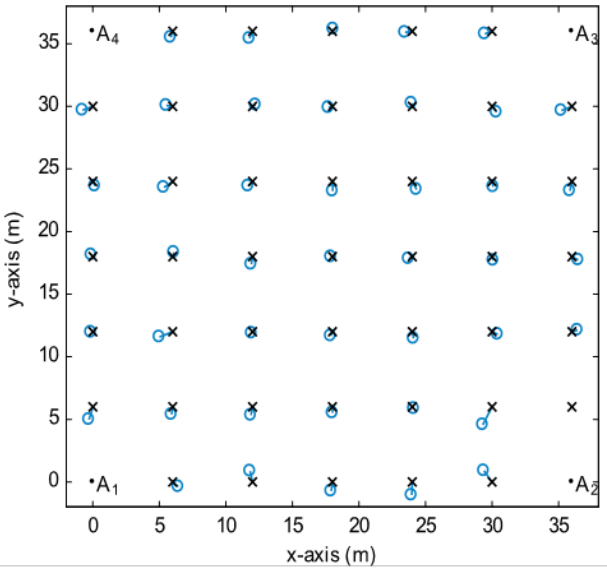


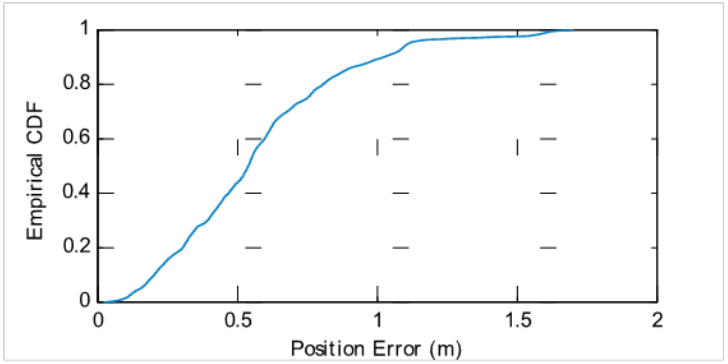


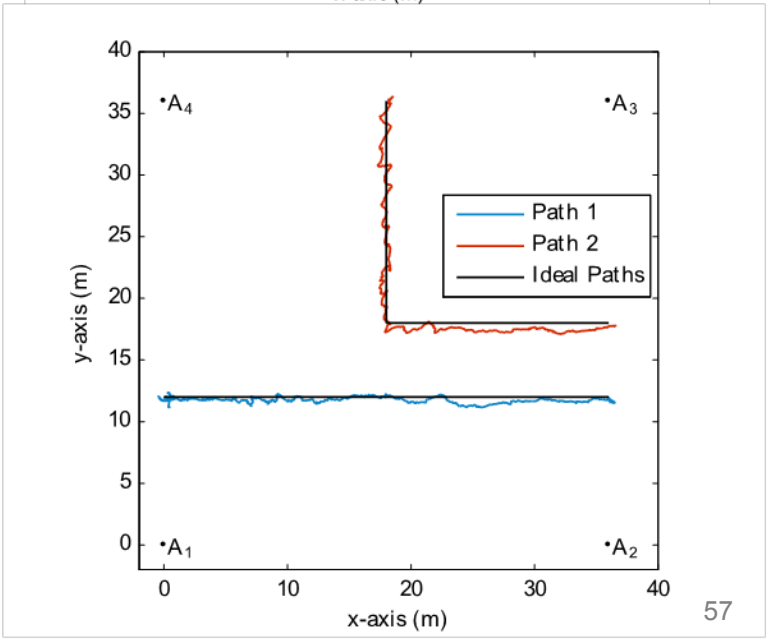


* R. Exel and T. Sauter, A comparison of time- and RSS-based radio localization for the factory floor, *IEEE WFCS*, Lemgo, 2012, pp.13-20.

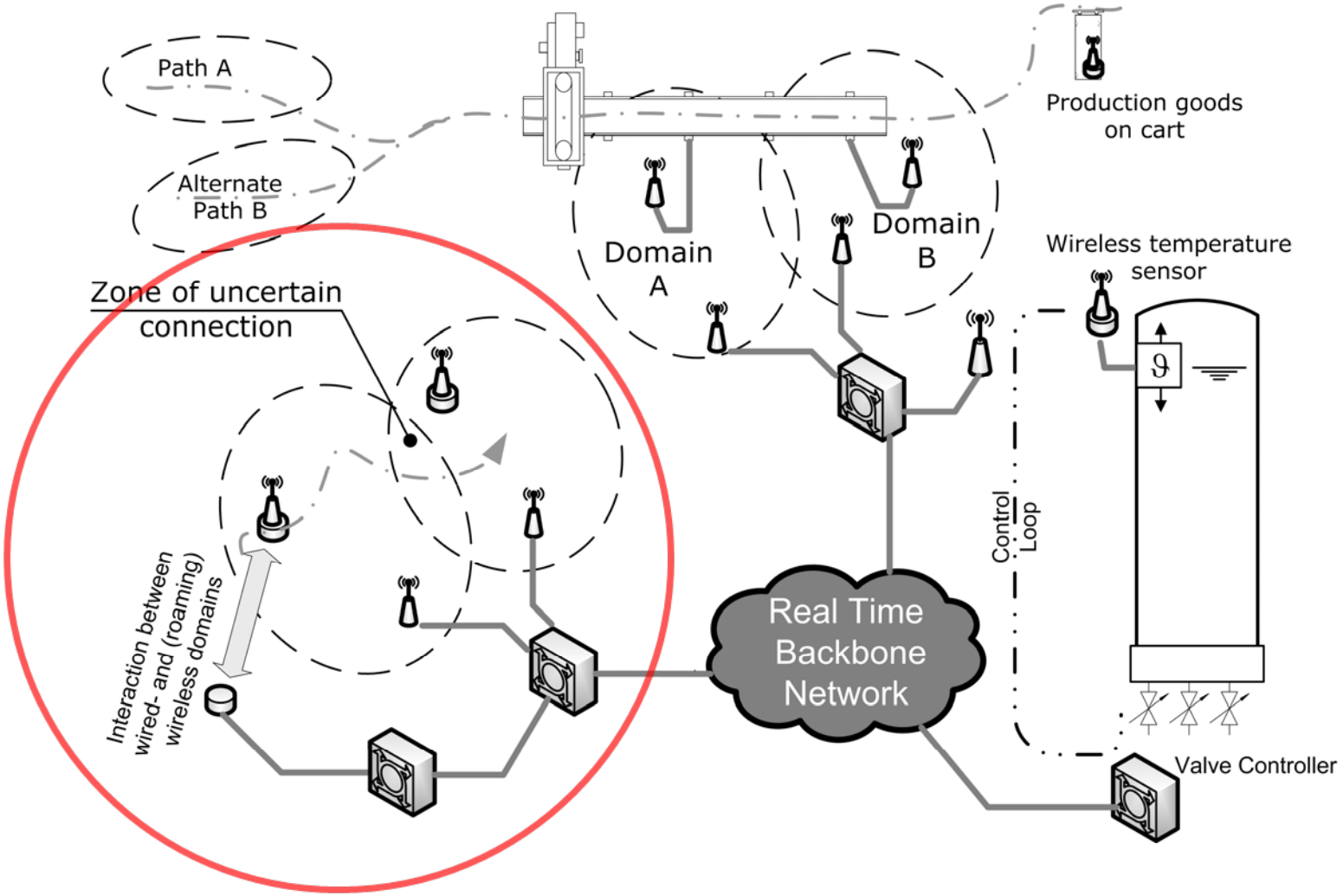
2D Measurement Results





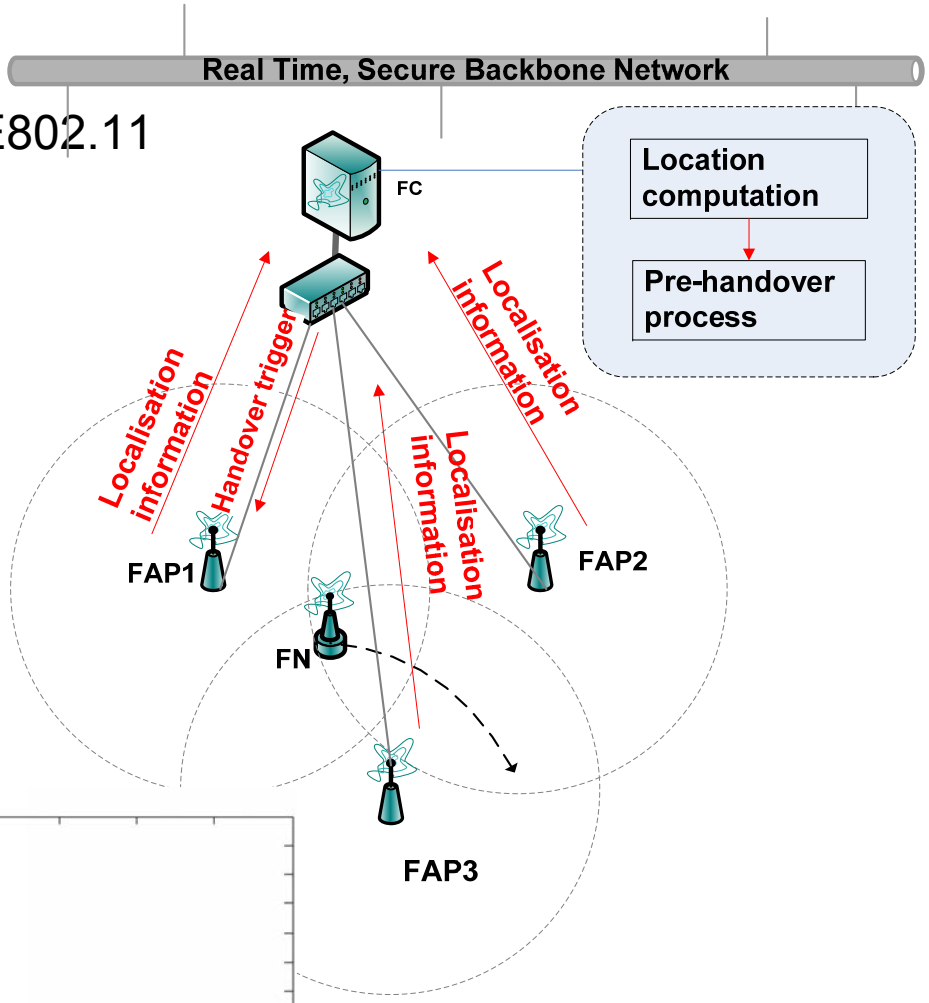


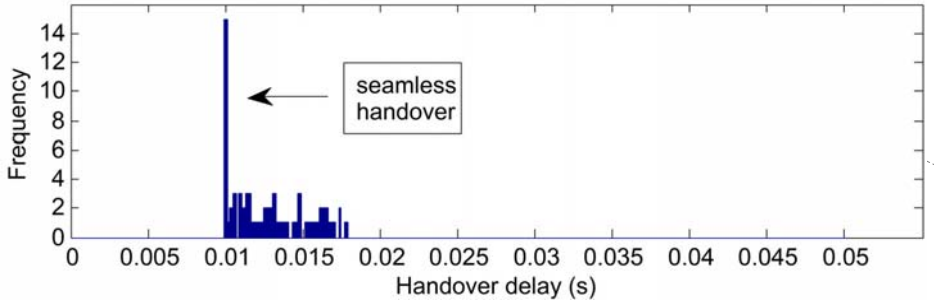
Application Scenario: Real-Time



Location-based Handover

- Channel switching in IEEE802.11
  - Detect channel loss
  - Scan channels
  - New authentication
  - Typical 2.3 s
- Improvement by location awareness
  - Advance bandwidth reservation
  - No scanning necessary





* T. Sauter, J. Jasperneite, and L. Lo Bello, Towards New Hybrid Networks for Industrial Automation, *IEEE ETFA*, Palma de Mallorca, 2009, pp. 1-8.

Contents

- Motivation
  - The big picture
- Integration aspects
  - Network interconnections
  - Hybrid wired/wireless networks
- Synchronization
  - The quest for accuracy
  - Localization of mobile devices
- Security
  - The big challenges
  - Practical solutions

Security vs. Safety

- Safety…
  - Protection of humans
  - Protection of equipment
  - Prevention of catastrophic system failures
  - “Measured” in safety integrity levels (SIL) defining residual failure probabilities
  - Requires (among others) hard real time communication and design for dependability

- Security...
  - Protection of data against misuse
  - Prevention of alteration, eaves-dropping, replay...
  - Detection of attacks
  - Requires (among others) cryptographical methods and proper system design

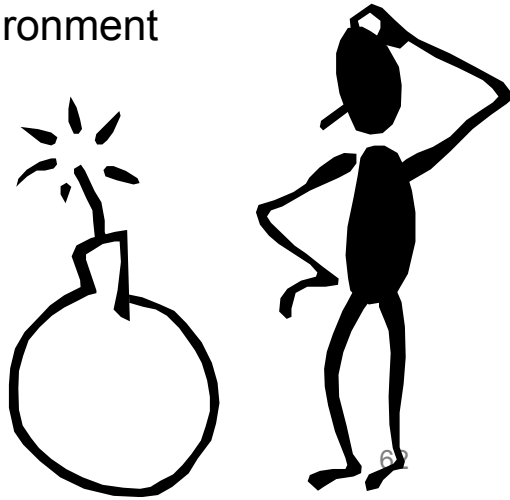
Networking and Security

- For long time a non-topic
  - (Automation) islands need no protection
  - Centralized controllers with dumb peripherals
  - (Network) security is tedious to design and implement
  - “Let’s concentrate on the basic features first…”

➔ Networks were designed without view to security

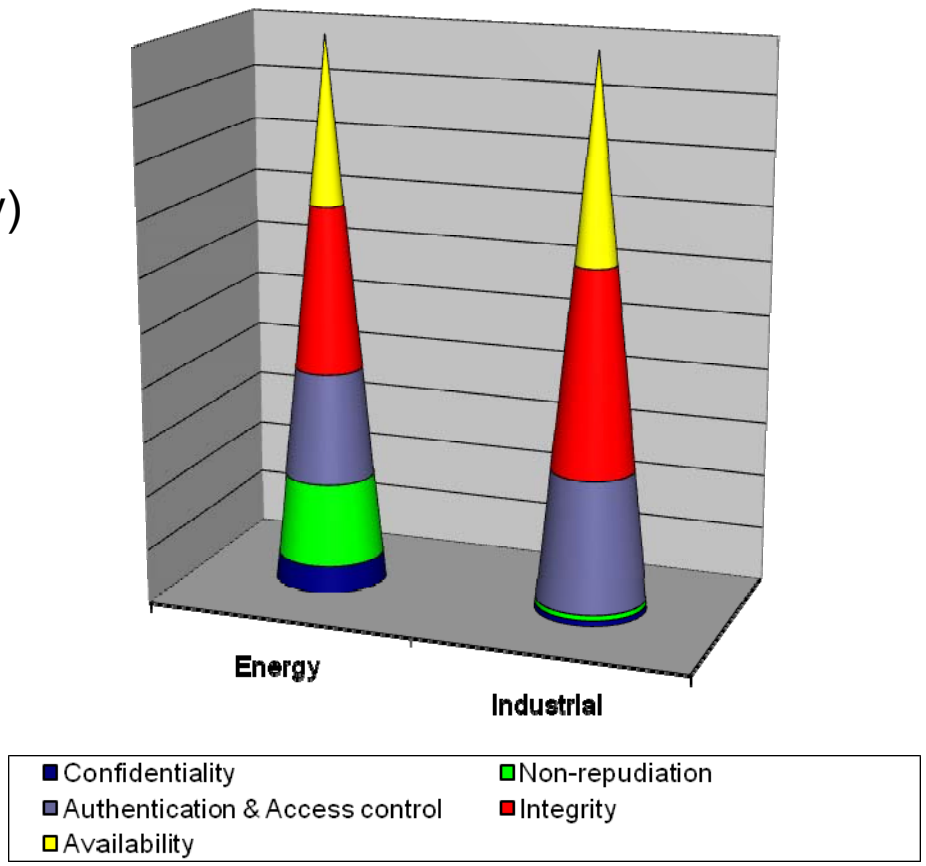
- (Vertical) integration changes the situation
  - Relatively closed (Intranet) or open (Internet!) environment
  - Trend towards distributed systems
  - IT-like platforms also used in automation
  - Increasing threats from outside (viruses, automated attacks)

➔ Security ought to be an issue



Security Goals

- Confidentiality (privacy)
- Integrity
- Availability
- Authentication
- Authorization and access control
- Non-repudiation



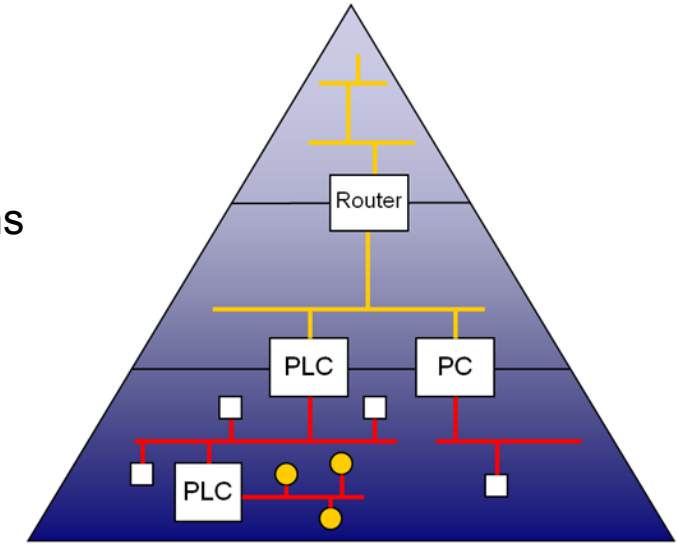
- Requirements vary strongly in different application areas

So, let‘s introduce Security

- Principle of Kerckhoff (1883)
  - The security of a system should only rely on the secrecy of the used credentials (keys)
  - An algorithm can only be assumed to be safe when it is publicly reviewed
  - No security by obscurity!
- Don‘t invent anything new, employ what is already known
  - IT security building blocks
  - Crypto algorithms
  - Security tokens

Where are the Problems?

- Heterogeneous networks and environments
  - IP-based on the higher levels vs. real-time on the lower ones
  - Standard Internet, fieldbus systems, industrial Ethernet, wireless
- More (mobile) IT components on the factory floor
  - Vulnerability of operating systems (Melissa)
  - General-purpose PC-like platforms for PLCs (Stuxnet)
- No end-to-end solutions
  - No built-in security features on field-level
  - Insufficient resources for IT-grade add-ons
- Twofold need for security mechanisms
  - Horizontally inside the network levels
  - Vertically across network boundaries



Further Problems – Security vs. Interoperability

- Goals of interoperability
  - Automatic configuration (ad-hoc networking)
  - Plug and Play/Participate/Produce
  - Extensibility of installations
  - Open system
- Goals of security
  - “What is not explicitly allowed is forbidden”
  - Access restriction to permitted entities
  - No intrusion via attachment of external (mobile) devices
  - Closed system

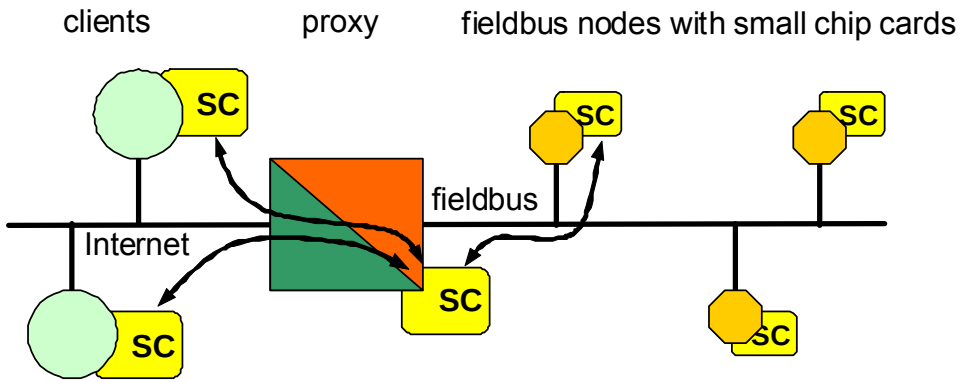
Further Problems – Physical Access

- Claude Shannon: “The enemy knows the system.”

- Automation hardware not always under the control of the owner
  - Worst case: building automation, energy distribution
  - Easy access for potential hackers
  - Tamper-proof hardware in distributed systems is difficult

Further Problems – Embedded Systems vs. IT standards

- Automation often poses real-time requirements
  - Not very relevant in classical IT security
  - En/decryption may introduce unacceptable delays
- Embedded systems are no high-performance platforms
  - Limited computing power
  - Limited bandwidth
  - Still, security mechanisms should be strong
- Use of dedicated security tokens
  - Bottleneck serial interface



* P. Palensky and T. Sauter, Security Considerations for FAN-Internet Connections, *IEEE WFCS*, Porto, 6.-8. Sep. 2000, pp. 27-35.
* A. Treytl and T. Sauter, Security Concept for a Wide-Area Low-Bandwidth Power-Line Communication System, *ISPLC*, Vancouver, 2005, pp. 66-70.

Performance Issues in Crypto Algorithms

- Asymmetric algorithms
  - Large block size (RSA: 128 bytes and above)
  - Long computing times
  - Not suitable for real-time applications
- Symmetric algorithms
  - Block length comparable to payload in low-level networks
  - Keys more problematic to distribute
  - Much faster
- Promising: ECC
  - Asymmetric with benefits of symmetric algorithms
  - Short blocks (typ. 20 bytes)
  - Not yet widely supported in hardware (smart cards)

Algorithm	Block Size	Execution time
3-DES	8 bytes	n.a. (23 µs*)
DES	8 bytes	n.a. (35 µs*)
IDEA	8 bytes	n.a.
Blowfish	8 bytes	n.a.
AES (128-bit key)	16 bytes	12.195 ms
AES (128-bit key) CBC	16 bytes	13.536 ms
AES (128-bit key) CFB	16 bytes	15.663 ms

Execution times on 8051 with 4 MHz
* With hardware support

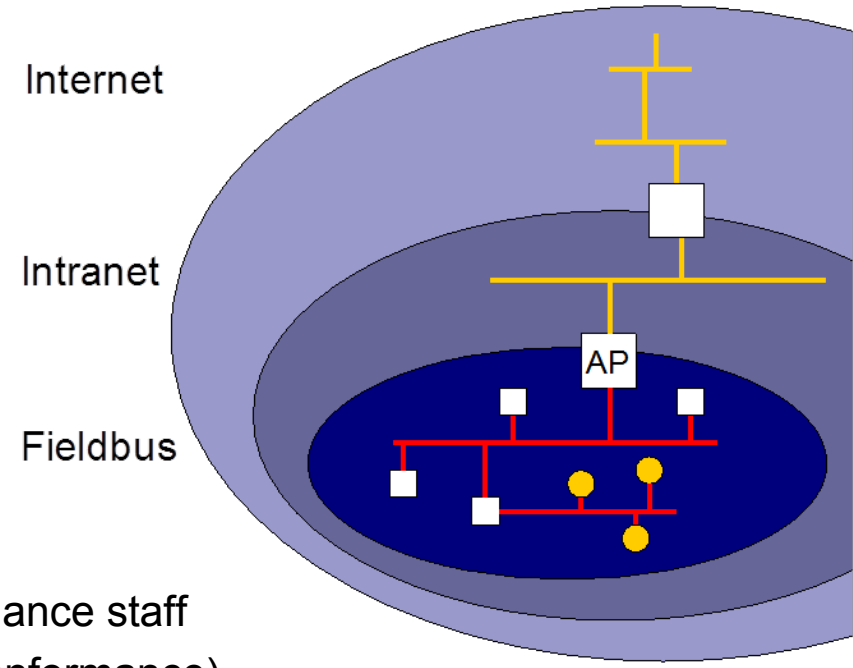
Troubles Continued – Organizational Issues

80:20

- Security is mostly an organizational issue
  - Security policy on the basis of a threat analysis
  - Definition of assets to be protected and appropriate measures
- Key management as central problem
  - Key derivation and/or distribution
  - Particularly problematic in large distributed systems

Defense in Depth Approach

- Multi-layer model with different zones
  - Access control at the borders between the zones
  - Relaxed requirements inside the zones
- Internet
  - Standard IP security
  - Firewalls to block attacks
- Intranet
  - Standard IP security
  - Limited user groups
- Isolated network
  - Access only by insiders/maintenance staff
  - Individual solutions (standard conformance)



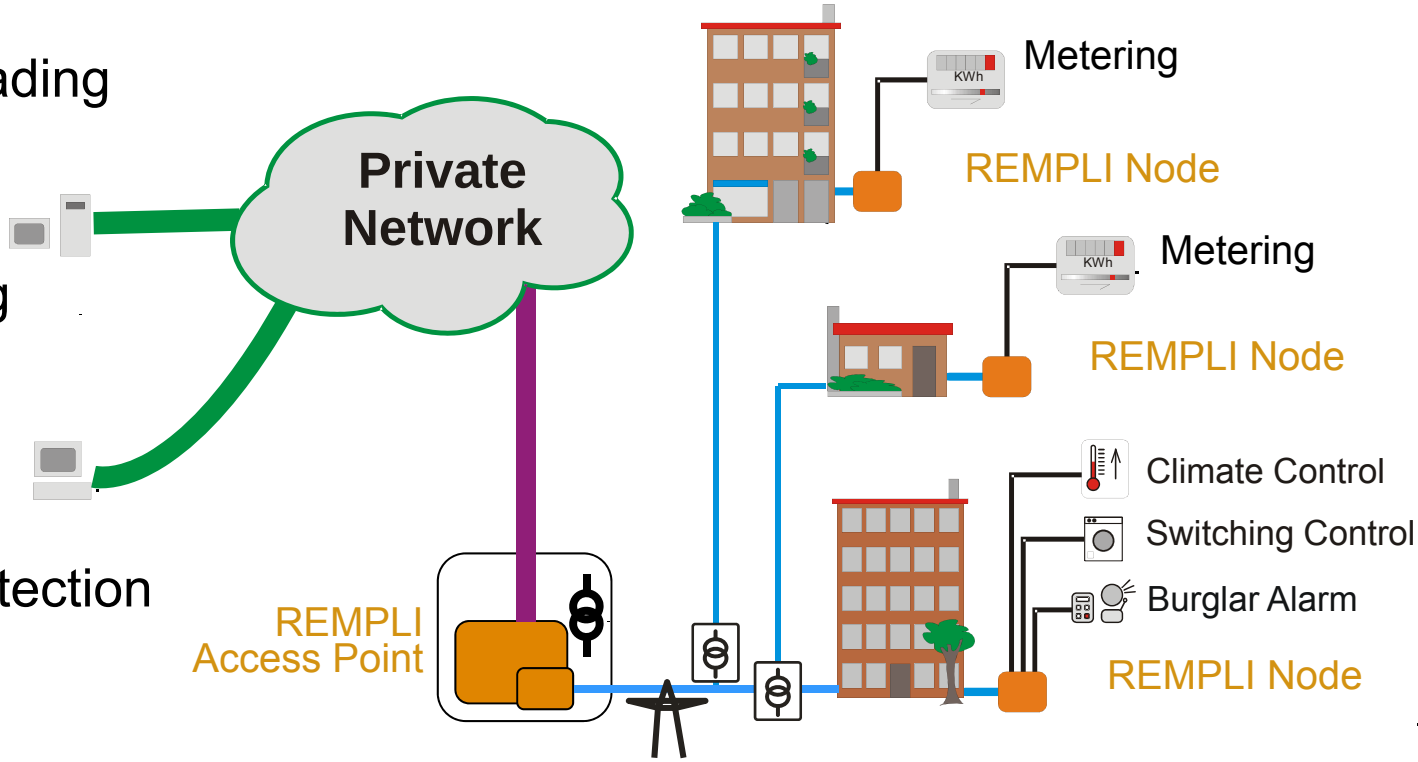
* Ch. Schwaiger and T. Sauter, Security Strategies for Field Area Networks, *IEEE IECON*, Sevilla, 2002, pp. 2915-2920.
* A. Treytl, T. Sauter, and C. Schwaiger, Security Measures in Automation Systems - a Practice-Oriented Approach, *IEEE ETFA*, Catania, 2005, vol. 2, pp. 847-854.

Example Powerline Communication

Utility Company

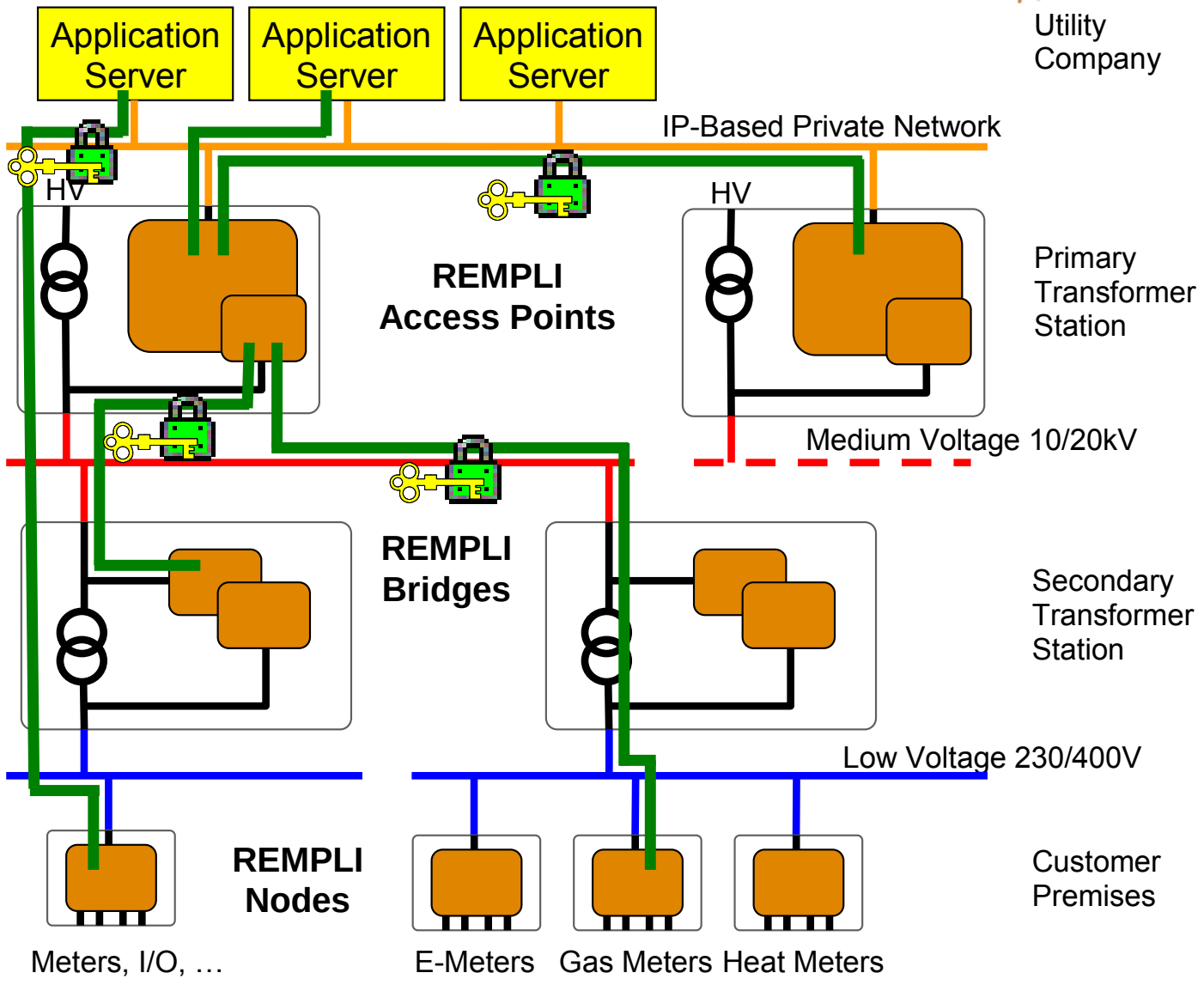
- Meter reading
- Control
- Load balancing
- Leakage detection
- Billing
- Fraud detection

Customers



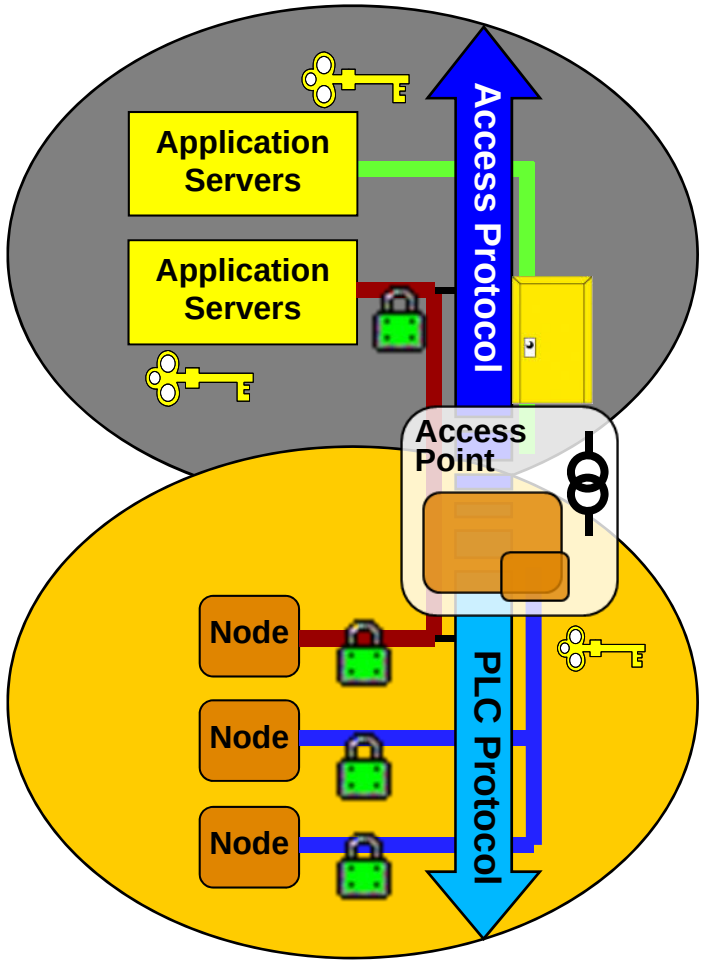
IP-based Private Backbone **Power-line-based Communication**

Communication Architecture



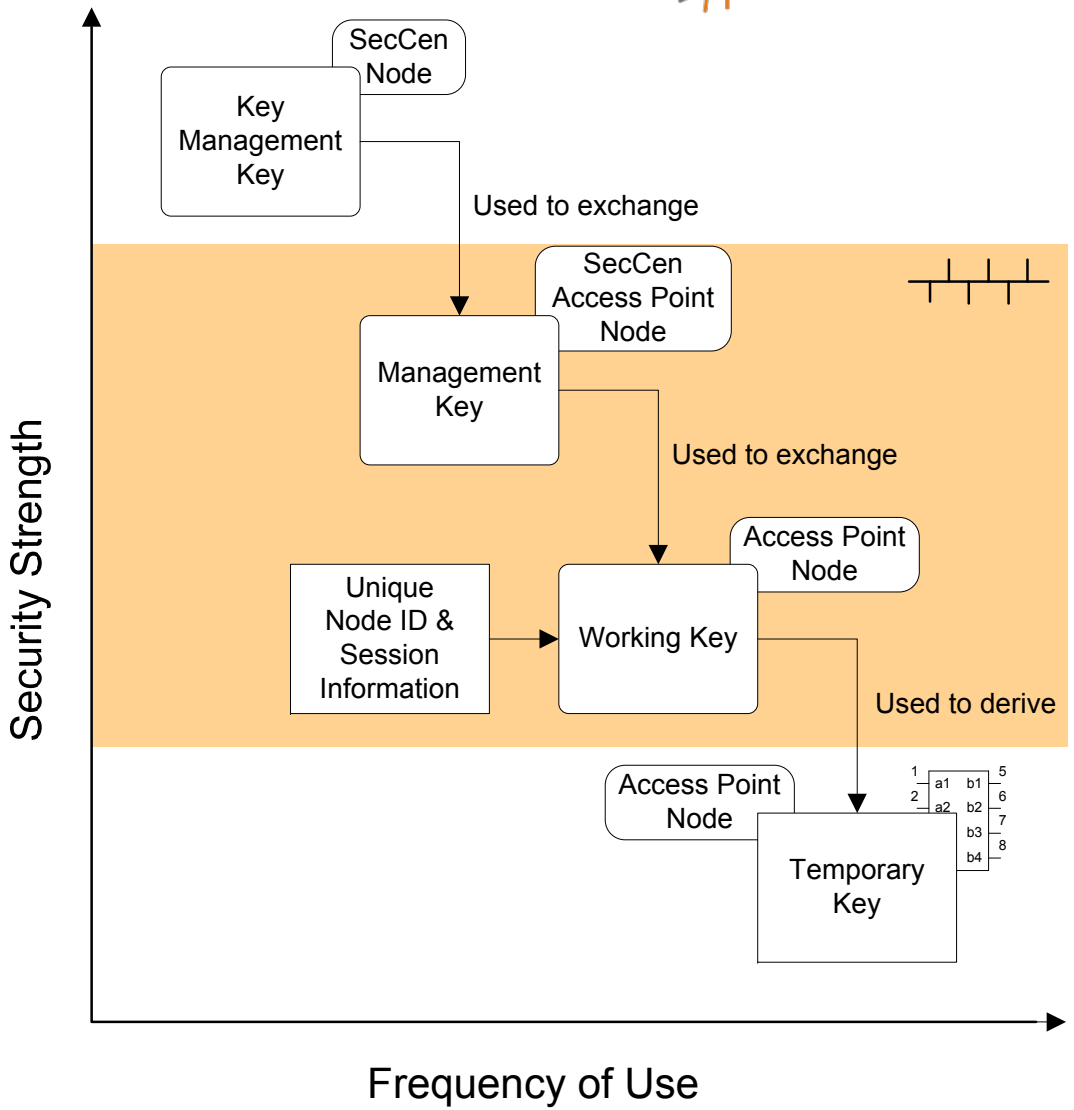
Boundary Conditions

- Limited bandwidth
  - 30-100 kbit/s
  - 20% packet loss
- Small packet size
  - 20 to 50 byte payload
  - Up to 100 kB application data
  - Only MAC possible
- End-to-end communication
  - Upper limits for packet delay
  - Security measures critical
- Low-cost node processor
  - 8051
  - Smart card as security module
  - Symmetric 3-DES block



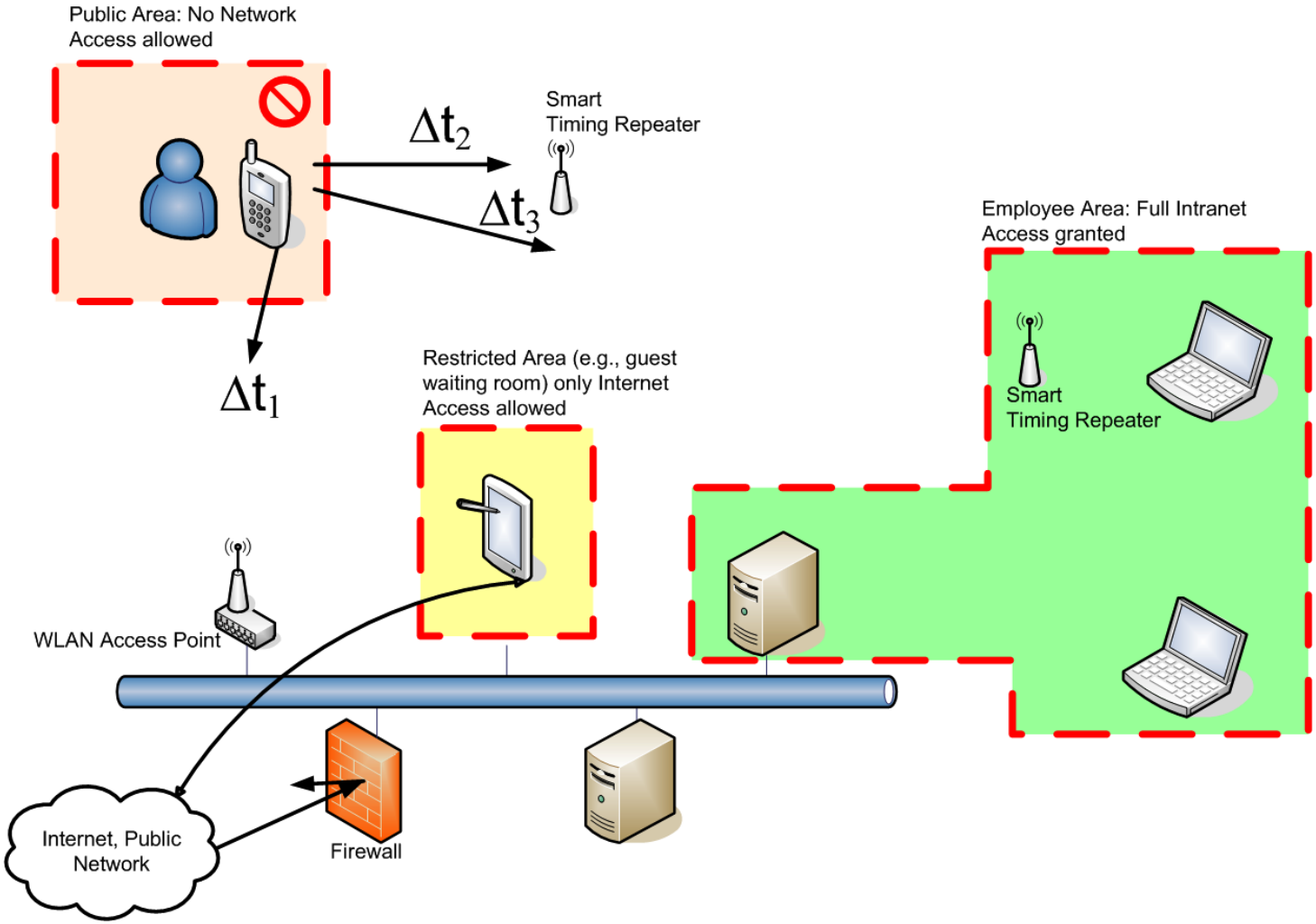
Key Distribution System

- Online key replacement
- Limited smart card capacity
  - Scalability
  - Limited payload to impede cryptanalysis
- Symmetric keys
  - Small blocks
  - Execution time
- Limited lifetime for low-level keys



* A. Treytl and T. Sauter, Security Concept for a Wide-Area Low-Bandwidth Power-Line Communication System, *ISPLC*, Vancouver, 2005, pp. 66-70.

Location-based Security Enhancement



* A. Treytl, T. Sauter, H. Adamczyk, S. Ivanov, and H. Trsek, Security Concepts for Flexible Wireless Automation in Real-Time Environments, *IEEE ETFA*, Palma de Mallorca, 2009, pp. 1-8.

Contact

Thilo Sauter
Center for Integrated Sensor Systems
Viktor Kaplan Strasse 2
A-2700 Wiener Neustadt

Thilo.Sauter@donau-uni.ac.at
http://www.donau-uni.ac.at/ziss