

# Virtual Automation Networks – the Future of Industrial Communications

Peter Neumann  
Institut für Automation und Kommunikation Magdeburg  
Steinfeldstraße 3, D-39179 Barleben, GERMANY  
peter.neumann@fak-md.de  
<http://www.ifak-md.de>

Milestone „Information and Communication Technologies in Control“  
Prague, 7<sup>th</sup> September 2005

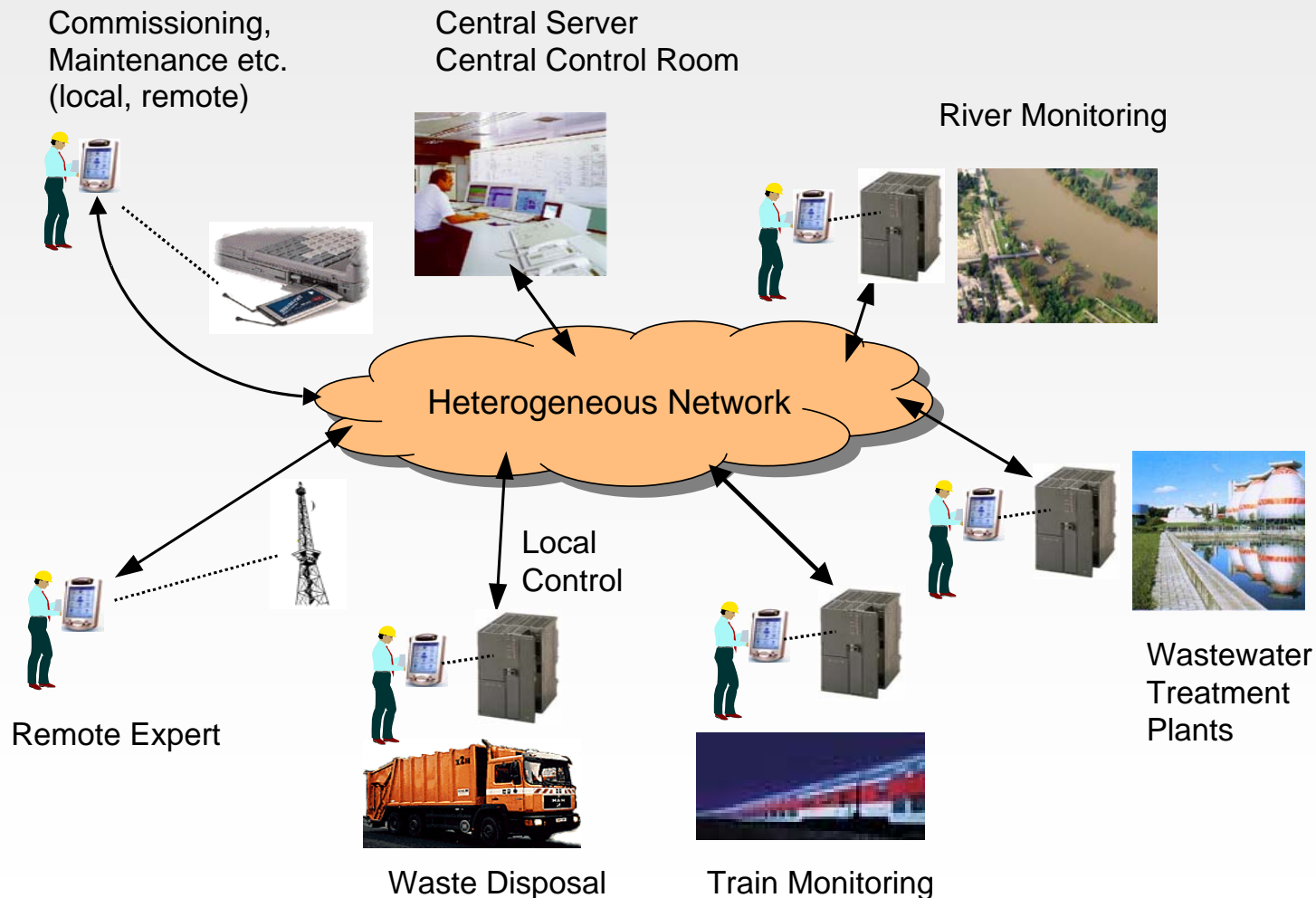
# Virtual Automation Networks – the Future of Industrial Communications

- Virtual Automation Network – what does it mean?
  
- Main Fields of Interest
  
- The European Integrated Project “Virtual Automation Networks”
  - The Focus
  - The Consortium
  - The Work Packages
  - The Initial Conditions

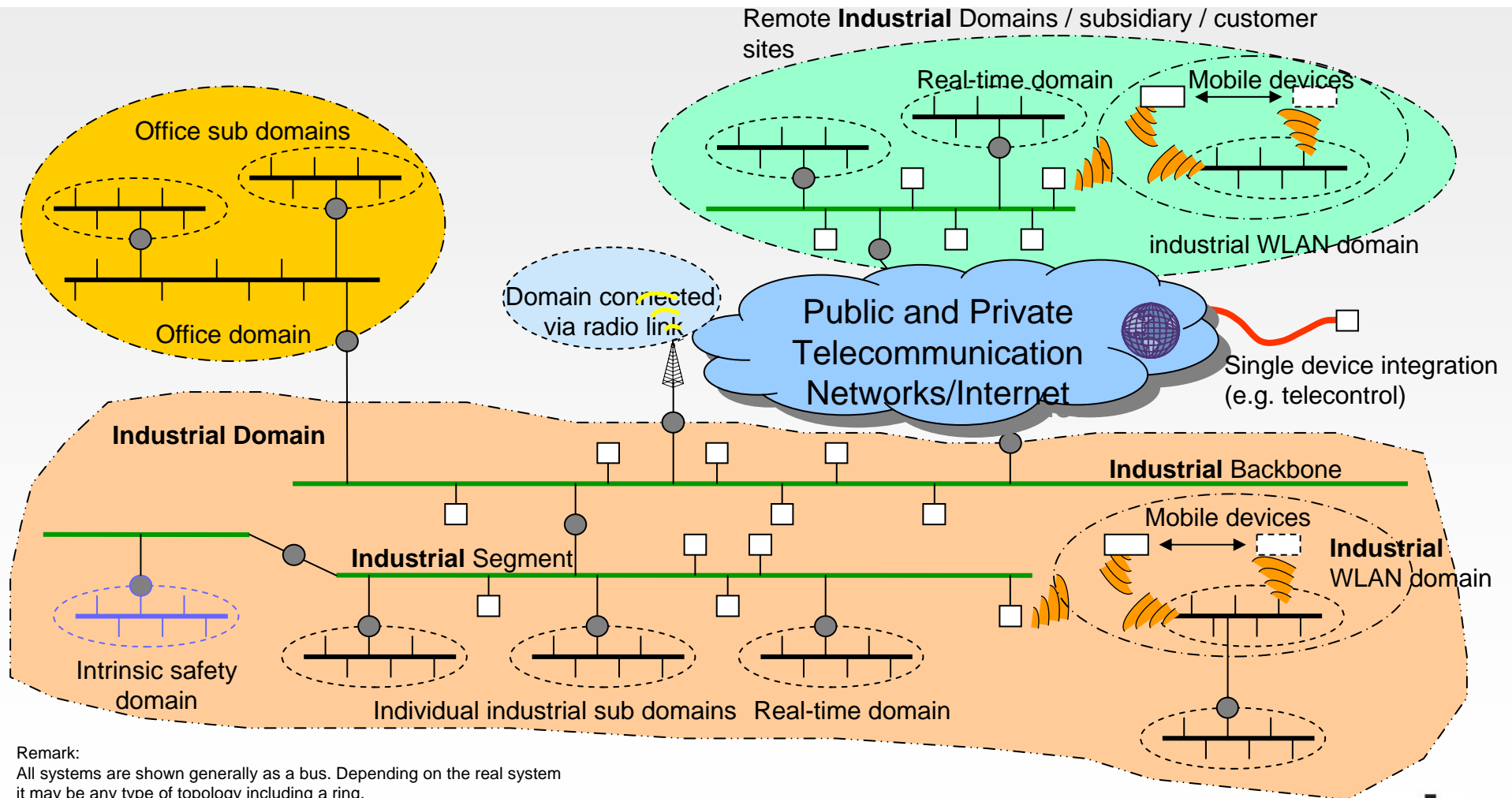
# Virtual Automation Networks – the Future of Industrial Communications

- Virtual Automation Network – what does it mean?
  
- Main Fields of Interest
  
- The European Integrated Project “Virtual Automation Networks”
  - The Focus
  - The Consortium
  - The Work Packages
  - The Initial Conditions

# Possible Scenario of a Geographically Distributed DCS



# The Virtual Automation Network



Remark:  
 All systems are shown generally as a bus. Depending on the real system  
 it may be any type of topology including a ring.

## What is a Virtual Automation Network?

- ❑ A VAN is a heterogeneous network
- ❑ A VAN consists of
  - Wireless or/and wired LANs
  - Internet (or parts)
  - Public wireless or wired telecommunication systems
  - Private wireless or wired telecommunication systems
- ❑ Geographically distributed application programmes (co-operating to fulfil a control application) are connected via the VAN
- ❑ The end-to-end connection has to guarantee
  - Privacy
  - Required scalable real-time behaviour
  - Safety
  - scalable Security
- ❑ VPNs of the office domain do not offer enough required mechanisms. IPv6 offers mechanisms only partially

# Virtual Automation Networks – The Future of Industrial Communications

- Virtual Automation Network – what does it mean?
  
- Main Fields of Interest
  
- The European Integrated Project “Virtual Automation Networks”
  - The Focus
  - The Consortium
  - The Work Packages

## Desired Research and Development Results

- ❑ an open automation architecture, platform and infrastructure covering specific industrial and automation needs, to perform a *dynamic industrial communication environment* for a life cycle covering management of production and manufacturing systems, automation products and services
- ❑ adoptions of office IST technologies extended by the required new functionalities in automation systems
- ❑ integration concepts and guidelines for private and public Ethernet and Internet based networks, consisting of wired and wireless, local and wide area networks
- ❑ *scalable* real-time, safety and security technologies and capabilities over all levels of a (virtual) network
- ❑ standardised interoperable solutions
- ❑ embedded devices communication architectures

## What is new?

- ❑ Data throughput between geographically distributed connection end points with guaranteed Quality of Service
- ❑ QoS contains *scalable* Real-time behaviour, Safety and Security over heterogeneous communication networks
- ❑ The metrics to describe the QoS are very different in the participating sub-networks within the local area as well as in the wide area. It is aimed to define the necessary “*overall*” *metric*
- ❑ There are (many) network transitions between the participating sub-networks. A method to describe the “*transition chain*” is necessary.

## General Needs

Necessary are:

- ❑ Concepts for guaranty of *desired end-to-end performance in heterogeneous LAN/WAN networks*
- ❑ Special mechanisms for *Security* with scalable security in different zones
- ❑ Special mechanisms for *functional Safety* in combined wired and wireless networks
- ❑ General *wireless communication concept* including local and wide area telecommunication networks

## The Real-time Classes

- ❑ *Class 1:* soft real-time (scheduling on top of UDP/TCP): scalable cycle time (in the range of 100ms); used in factory floor and process automation (monitoring, process control)
- ❑ *Class 2:* hard real-time (scheduling on top of MAC): cycle time 1...10ms. Used for control
- ❑ *Class 3:* isochronous real-time (with time/clock synchronisation and routing with time schedule): cycle time 250 $\mu$ s...1ms; jitter less than 1 $\mu$ s. Used for motion control.
- ❑ Additionally: non real-time (diagnosis, commissioning [configuration, parameterisation], maintenance)

## State of the Art – Real-time class 1

Systems, which are using Ethernet-TCP/IP, offer response time in the millisecond range. The data transmission is based on the best effort principle.

### **Examples:**

- ❑ **Ethernet/ IP** (Rockwell, ControlNet International, Open DeviceNet Association) → Control and Information Protocol CIP
- ❑ **High Speed Ethernet HSE** (Fieldbus Foundation)
- ❑ **Interface for Distributed Automation IDA** (MODBUS-IDA Group, Schneider)
- ❑ **PROFINET CBA** (PROFIBUS user organisation, Siemens). An open source code and various exemplary implementations/portations for different operating systems are available on the PNO Website.

## State of the Art– Real-time class 2

- ❑ Middleware on top of the MAC layer of Ethernet, scheduling the hard real-time and soft real-time/ non real-time traffic.
- ❑ In academic and industrial research, different scheduling strategies and smoothing concepts has been investigated

### ***Example:***

- ❑ **PROFINET RT, PROFINET IO** (PROFIBUS user organisation, Siemens)

PROFINET IO allows a mid-term substitution of any fieldbus by PROFINET IO, because the PROFINET IO specification includes the potential features of the fieldbus systems. The integration of four fieldbus systems (PROFIBUS, Interbus, DeviceNet, ASI) via PROFINET IO has been presented at the Hanover fair 2005

## State of the Art– Real-time class 3

- ❑ **Powerlink** (Ethernet PowerLink Standardisation Group EPSG, Bernecker & Rainer), developed for Motion Control, uses a proprietary real-time protocol on top of the *shared* Ethernet. Using 100 Mbps Ethernet, Cycle times of 400  $\mu$ s or less in applications, Network jitter  $\leq 1\mu$ s
- ❑ **EtherCAT** (Beckhoff), developed as a fast backplane communication system, uses Bus Terminal Controllers to support active (event-driven) sending and receiving of data via Ethernet. The routing functionality ADS (Automation Device Specification) enables local and remote communication via any connection route
- ❑ **PROFINET IRT** (PROFINET user organisation, Siemens), developed for any industrial applications, uses a middleware on top of Ethernet MAC layer to enable high-performance transfer, cyclic data exchange and event-controlled signal transmission. The layer 7 functionality is directly linked to that middleware. Using 100 Mbps *switched* Ethernet: Cycle times of 250  $\mu$ s (35 nodes) to 1 msec (150 nodes) in applications, Network jitter  $\leq 1\mu$ s

## State of the Art– Real-time Standardisation (local area)

- ❑ The international standardisation activities are concentrated in IEC SC65C WG 11 “Real-time Ethernet”.
- ❑ Approaches of various user organisations are established there as Public Available Specifications PAS. These PAS have not been harmonised yet.

## State of the Art– Real-time (wide area)

Using Wide Area Networks, the stock of existing communication technologies becomes broader:

- ❑ all appearances of the Internet (mostly with best effort quality of services)
- ❑ public digital wired telecommunication systems (ISDN, DSL etc.)
- ❑ public digital wireless telecommunication systems (GPRS-based, UMTS-based)
- ❑ private wireless telecommunication systems, e. g. trunk radio systems.

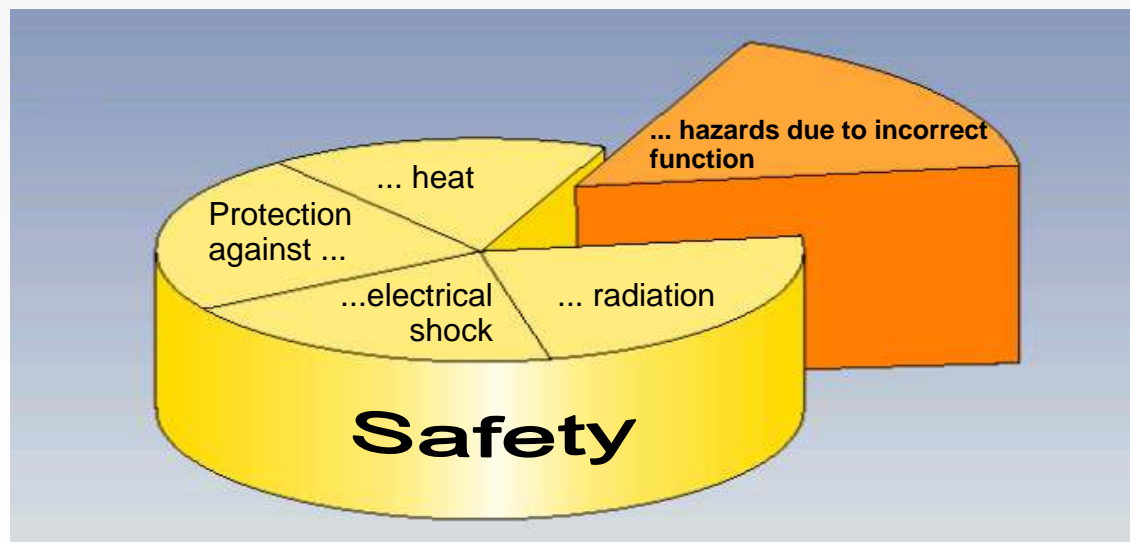
Using these technologies within the automation domain there are many private protocols over leased lines, tunnelling mechanisms etc. Most of the Radio Networks can be used in non real-time applications, some of them in soft real-time applications (but industrial environments and ISM Band limit the applications).

## State of the Art– Real-time (wide area)

- ❑ The usage of wide area networks within the automation domain in the VAN sense is new and has to be investigated just as the uninterrupted commercial availability.
- ❑ Since the Internet or other telecommunication systems are general-purpose communication systems, the infrastructure and business model preconditions for the selection of requested QOS within a spectrum of available communication services of various providers have not been investigated suitably and have to be developed.
- ❑ This means, in analogy to the “switched” Ethernet in LANs, a **WAN switching mechanism** has to be developed for this selection, i.e. choosing dynamically the network type and/ or network provider, which guarantees the required QOS.

## The Problem of Safety

- ❑ Safety means protection against hazards (movement, heat, radiation, electrical shock, etc.)
- ❑ “Functional Safety” means protection against hazards caused by incorrect function
- ❑ Safety includes the communication via heterogeneous network



## Functional Safety in Industrial Communications

### What is “functional Safety”?

- ❑ “Functional Safety” means protection against hazards caused by incorrect function. Safety includes the communication via heterogeneous networks.
- ❑ Caused by the distribution of data via the communication networks, the safety of these networks becomes more and more important regarding the functionality of an automation system.
- ❑ There is a need to meet defined Safety Integrity Levels (SIL), see (IEC 61508), e.g. Residual Error Probability  $\leq 10^{-7}$  errors/h for SIL 3. The communication part requires a residual error probability of  $\leq 10^{-9}$  errors/h for SIL 3 (1% of  $10^{-7}$ ; the other 99% are required for sensors, PLCs, and actuators etc.).

## State of the Art - Functional Safety

Measures to avoid the influence of the failures (falsified addresses, loss or damage of data, delay) could be:

- numbering transmitted data,
- observation of transmission time (time expectation),
- authentication using passwords (identification),
- optimised CRC (redundancy).

One principle to use communication systems for safety applications is to consider the communication channel as a so-called "Black Channel" → see IEC SC65C WG 12

**The safety measures will be realised in a separated safety layer that is situated between communication protocol and application.**

With this principle, an existing communication system can be used as it is

## State of the Art and requested investigations - Functional Safety

### Examples:

- ❑ the PROFIBUS user organisation has specified safety profiles for PROFIBUS and PROFINET (PROFIsafe profile),
- ❑ the Interbus Club specified a safety layer for Interbus.

### Necessary Investigations:

- ❑ how can TCP/IP-oriented networks be extended for the transfer of safety-related data in automation systems?
- ❑ how fulfil VAN safety codes the SIL requirements - especially for different types of communication media? The results should be introduced in the IEC standardisation activities on “Communications for functional safety” (IEC SC65C WG 12).

## The problem of Security

### Situation:

- ❑ Today's automation islands are relatively secure against attacks. The usage of Internet-based technologies compared with today's automation islands requires a common security concept for distributed automation using Virtual Automation Networks
- ❑ Typical types of assaults are: eavesdropping, hacker attacks, data corruption, unauthorised access, espionage, sabotage, loss, theft, and operator errors.
- ❑ Important is, that the threats are coming from inside and outside an enterprise.
- ❑ Nowadays, in Germany a procedure started under the umbrella of ZVEI to harmonise the various activities of different organisations (ZVEI, PNO, NAMUR, VDMA, VDA...)

## The problem of Security

The security of control systems distinguishes **three aspects**:

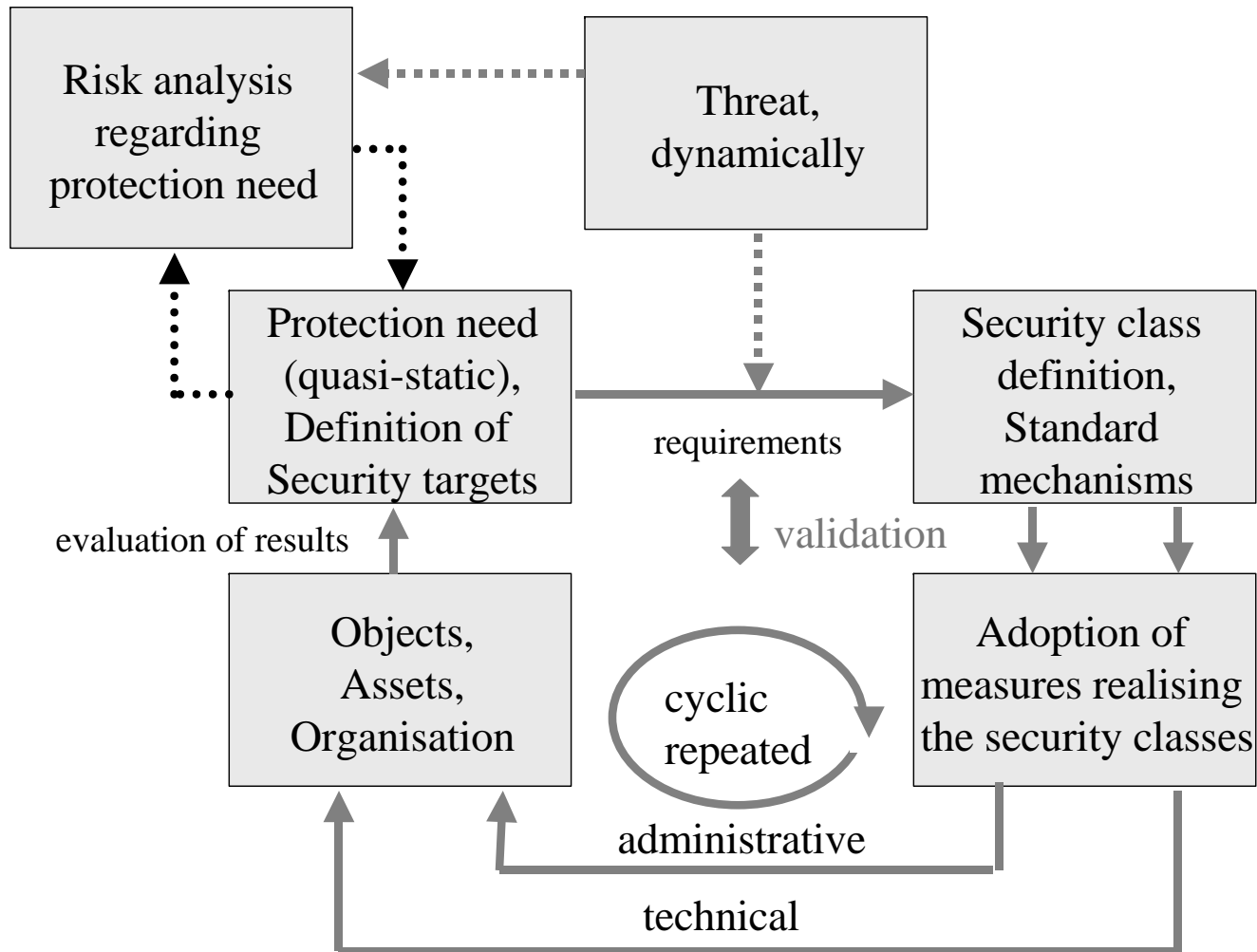
- ❑ **Data communication security:** protection of data transfer between components of control systems, operator stations, and with external remote devices. That leads to a three zones model
- ❑ **Physical security:** protection against local manipulation, destruction and unauthorised physical access (e.g. memory sticks)
- ❑ **Operational security:** protection by administrative measures as authentication, availability, desired operation conditions etc. → it plays an important rule

## Basic Requirements - Security

**Basic requirements**, especially in the automation domain, are:

- ❑ ability to use hierarchical concepts of control systems architecture. It means that there are segments, which can be protected separately
- ❑ control system underlies different changes during the operation phase. The security concept has to support reconstructions (including „back documentation“)
- ❑ availability should not be influenced by security mechanisms
- ❑ security mechanisms have to enable security updates
- ❑ “open door” effect of wireless communications, which cannot be influenced by administrative measures, has to be compensated by technical measures
- ❑ new business models (new scenarios) for external commissioning and maintenance/asset management by external service organisations lead to new security risks (or conditions). There are links of external (heterogeneous) communication networks to internal enterprise networks with sensible data exchange

## Security risks, classes and measures



## State of the Art – Security Standardisation Activities

The situation regarding standardisation of security in automation is as follows:

- ❑ there is a number of basic standards for IT security to be also used in the industrial environment
- ❑ The US has the outrider role for the standardisation of security in automation.
  - The committee ISA SP99 “Manufacturing and Control Systems Security” focuses on improvement of confidentiality, integrity, and availability of components or systems used for manufacturing or control and provides criteria for procuring and implementing secure control systems.
  - The first two technical reports TR1 “Security Technologies for Manufacturing and Control Systems”, and TR2 “Integrating Electronic Security into the manufacturing and Control Systems Environment” has been published in 2004

## State of the Art – Security Standardisation Activities

- ❑ The actual activities in IEC TC 57 “Power Systems Control and associated communications” and IEC SC65C WG 13 “Cyber Security” regarding the use of security mechanisms in the automation have a very early status.
- ❑ Additionally, the ISO/IEC JTC/SC27 “IT Security Techniques” is of interest for the security development in the automation domain.
- ❑ Stabilising the IEC standards needs time until 2006/2007. The IEC TC 65 decided to shift the IEC SC65C WG13 “Cyber Security” (regarding communication systems) to the TC 65 and extended the focus to “System Security”. That procedure will consume so much time, that there will be a noticeable delay.

## State of the Art - Wireless Industrial Communications

There are Radio add-ons for wired systems and other wireless Radio communication systems, e.g.

- ❑ WLANs: IEEE 802.11b, IEEE 802.11a, IEEE 802.11g
- ❑ Bluetooth 1
- ❑ Bluetooth 2, ZigBee (IEEE 802.15)
- ❑ Ultra Wide Band Systems.

Most of these Wireless Radio Networks can be used in non real-time applications, some of them in soft real-time applications (but industrial environments and ISM band limit their applications).

## State of the Art - Wireless Industrial Communications

- ❑ The **WLAN** technology is more and more used in the higher architecture levels of the automation hierarchy, but also in the shop floor.
- ❑ **Bluetooth** has been successfully introduced in industrial short-range applications, operating in the same local area as WLAN with good results
- ❑ **Ultra Wideband Systems** are becoming more and more important for sensors and indoor location-based services. The co-existence of WLAN and UWB installations within same local area seems to be possible.

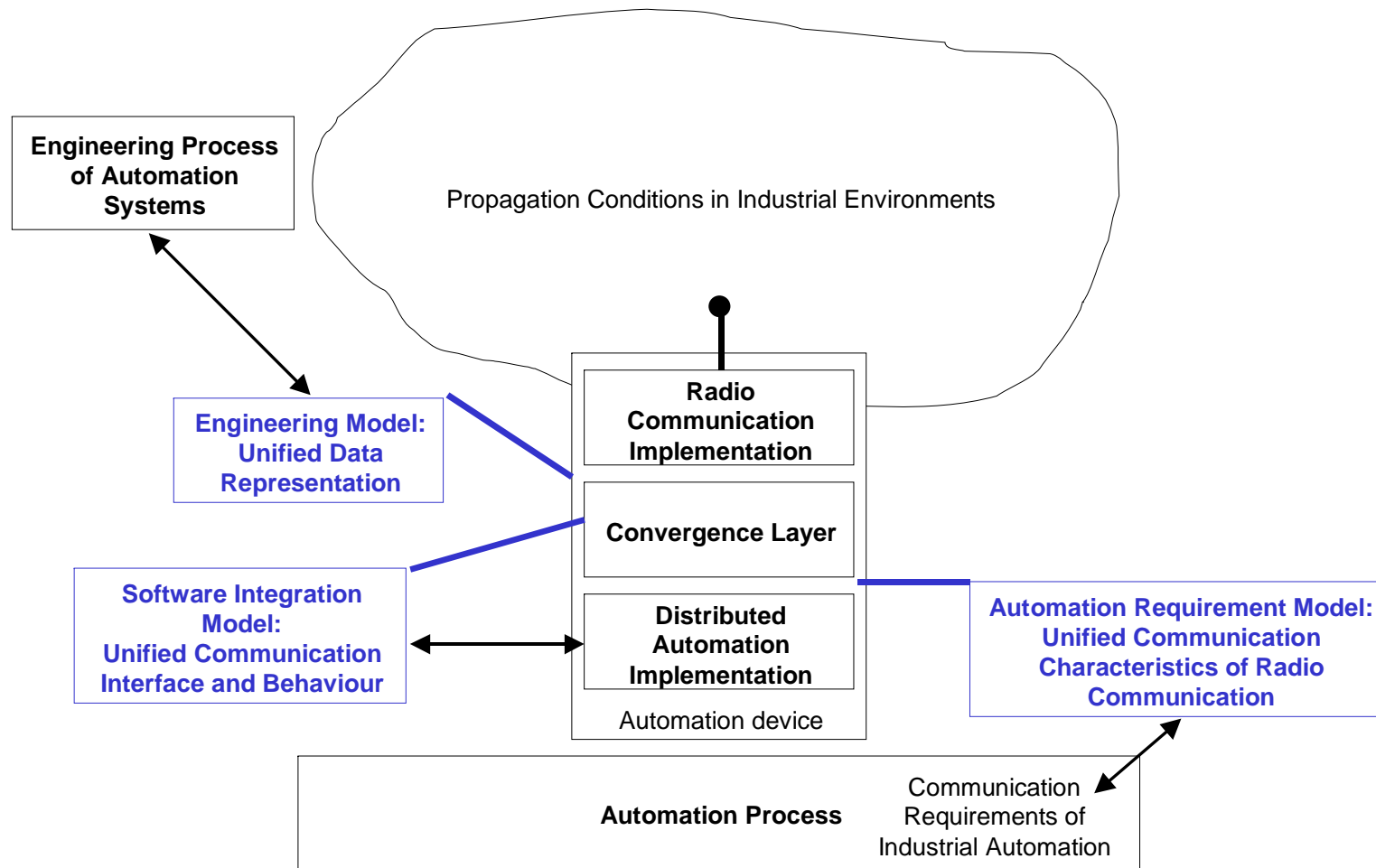
## State of the Art - Wireless Industrial Communications

- ❑ **ZigBee** should be introduced to connect the automation devices at the field level, especially in the process automation, because it will operate on a lower baud rate.
- ❑ But the specification of the higher layer protocols has not been finished. Thus, many vendors experiment with the available hardware to test their properties. There are positive but also negative results
- ❑ The recent activities are directed to the application domain Building Automation.
- ❑ Nevertheless, ZigBee has the potential to become a standard for wireless Monitoring & Control in industrial & commercial environments.

## Aspects of Integrating Radio based Implementation into Automation Applications

- ❑ Today for each technology the radio implementation has to be individually integrated into the automation device.
- ❑ Additionally, regarding the short innovation cycles and the related frequent replacement of radio communication, the potential of savings is obvious, which could be achieved by replacing the individual integration by using a general approach with unified convergence layer models.
- ❑ Moreover, the process of integration has to be recognised as a general approach including requirements, design and maintenance engineering. This task has not been part of the European RFieldbus project.

# Aspects of Integrating Radio based Implementation into Automation Applications



## Virtual Automation Networks – the Future of Industrial Communications

- Virtual Automation Network – what does it mean?
  
- Main Fields of Interest
  
- The European Integrated Project “Virtual Automation Networks”
  - The Focus
  - The Consortium
  - The Work Packages

## The VAN Focus

- ❑ The VAN project focuses on an important part of a *flexible manufacturing automation* scheme: the required industrial communication network for local and wide-area connection between the geographically distributed parts of the automation functions (over heterogeneous networks)
- ❑ The main focus is directed on the *Industrial Communications* with its specific requirements in real-time, safety and security
- ❑ The developed solutions shall be applicable for the integration into industrial embedded devices with limited resources
- ❑ The VAN project will provide innovative solutions, extensions and standards dedicated to industrial environments, to fill the existing gap between office technologies and industrial automation technology
- ❑ VAN focused on a new dimension of uniform networking of production and manufacturing processes

## The VAN Consortium

15 partners from 6 European countries (Germany, France, Spain Italy, Czech Republic, Poland):

- ❑ Siemens (Co-ordinator), D
- ❑ Arinstein, PL
- ❑ AUCOTEAM, D
- ❑ Brno University of Technology, CZ
- ❑ CARTIF, E
- ❑ Fidia S.p.A., I
- ❑ Heitec AG, D
- ❑ ifak Magdeburg, D
- ❑ MCM S.p.A., I
- ❑ Phoenix Contact, D
- ❑ Politecnico di Milano, I
- ❑ Schneider Electric, F
- ❑ Teleport Sachsen-Anhalt GmbH, D
- ❑ University of Magdeburg, Center Verteilte Systeme CVS, D
- ❑ Forschungszentrum Karlsruhe, D

## The VAN Work Packages

