From Fieldbus to Automation Cloud.
Industrial Communication Systems over two Decades

Peter Neumann
ifak
Institut f. Automation und Kommunikation
Magdeburg, Germany

WFCS 2014 Toulouse, France, 6th May, 2014
Outline

1. Introduction

2. Short DCS history and resulting requirements for Industrial Communication Systems

3. A tour around Industrial Communications, recent activities

4. Future work and outlook
Industrial Revolutions

First IR: Introduction of mechanical production plants (late 18\textsuperscript{th} century)

Second IR: Mass production based on labour division using electricity (early 20\textsuperscript{th} century)

Third IR: Automation of production processes using electronics and IT (70s)

Fourth IR: Autonomous products and decision making processes control/command added-value networks nearly in real-time (after 2020)

→ In Germany: campaign “Industry 4.0”
Outline

1. Introduction

2. Short DCS history and resulting requirements for Industrial Communication Systems

3. A tour around Industrial Communications, recent activities

4. Future work and outlook
<table>
<thead>
<tr>
<th>Decade</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1950/60</td>
<td>Conventional instrumentation → central instrumentation</td>
</tr>
<tr>
<td>1960/70</td>
<td>Process Computer → central instrumentation</td>
</tr>
<tr>
<td>1970/80</td>
<td>Microprocessor based Devices → central instrumentation</td>
</tr>
<tr>
<td>1980/90</td>
<td>Microprocessor based Field Devices → distributed instrumentation</td>
</tr>
<tr>
<td>2000</td>
<td>Migration of Office and Factory Automation → distributed instrumentation</td>
</tr>
<tr>
<td>Nowadays</td>
<td>Common handling of Factory Automation systems from the viewpoint of operation, engineering, and maintenance of production plants</td>
</tr>
<tr>
<td>Future</td>
<td>Self-organisation and automated lifecycle services</td>
</tr>
</tbody>
</table>
Generalised Scheme of an *locally distributed* Automation System

- Distributed Automation Instrumentation
  - Data Processing
  - Process visualisation
  - Fieldbus
    - Field Device
      - Sensor and Actuator Signals
    - Mechatronic Components
  - Technical Process

Peter Neumann: From Fieldbus to Automation Cloud
Geographical Distribution of Automation Systems. Possible Scenario

- Local commissioning, Maintenance etc.
- Remote expert
- Central server
- Central control room
- Local control
- Heterogeneous Network
- e.g. waste disposal
- e.g. trains
- e.g. WWTP
- e.g. rivers

Peter Neumann: From Fieldbus to Automation Cloud
Generalised Scheme of a **globally distributed** Automation System

Virtual Automation System

---

**Necessary: Integrated Industrial Communications**

Peter Neumann: From Fieldbus to Automation Cloud
Motivation for Integrated Industrial Communication

- Digital factory: formal methods are used in automation hierarchy

- Distributed applications: from sensor/actuator level to remote IT services (Tele Service, maintenance,...)

- Industrial automation and the office automation are merging and use the same communication technology
**Automation Hierarchy: Maintenance**

- **ERP**
  - Enterprise Asset Management System
  - Controls
    - e.g. Controller / DCS
      - Diagnosis
      - Condition Monitoring
  - Field
    - e.g. Field Devices
      - Maintenance relevant data
  - MES
    - Production
    - Quality
    - Inventory

Source: Bettenhausen

Peter Neumann: From Fieldbus to Automation Cloud
Resulting Requirements

- Necessary: Integrated Industrial Communications, if possible with a maximum of unique technology
- Easy vertical communication (access to data in all hierarchy levels) by using the same access methods
- Guaranty of the suitable real-time behaviour in each hierarchy level
- Suitable functional safety in the relevant hierarchy levels
- Guaranty of security (bottom up and top down), don’t forget the sensitive real-time process data
- Be aware, that industrial automation uses increasingly public infrastructure and services (Internet of things, Cloud), which can not be influenced by the automation staff. The same situation is valid for factory-internal IT departments, which are the emperors of switches and ports
Outline

1. Introduction

2. Short DCS history and resulting requirements for Industrial Communication Systems

3. A tour around Industrial Communications, recent activities

4. Future work and outlook
A tour around Industrial Communications

- Industrial Communications within factory levels
- Sensor/Actuator Communication
- Fieldbuses
- Controller Networks in Real-time classes
- Fieldbus Integration
- Industrial Wireless Communication
- Wide Area Networks in Automation
- Functional Safety
- Security
Office Communication and Automation are merging

Peter Neumann: From Fieldbus to Automation Cloud
Recent Situation: many Network Transitions

Peter Neumann: From Fieldbus to Automation Cloud
Requirements for Industrial Communication Systems

Quality of Service areas

• Non-interrupted availability of infrastructure, including Internet of things, cloud...
• Guaranty of the desired Safety Integrity Level to protect the human life/health as well as the assets,
• Automation-specific Security measures by the reasons of overall Safety,
• Suitable real-time behaviour for geographically distributed automation applications that can be offered by the used transmission technology.

Challenges

• Uninterrupted communications passing many network transitions
• Transparent data transfer paths desired
• Context-specific scalable QoS
  ▪ High availability
  ▪ Real-time behaviour in three RT classes
  ▪ Functional Safety
  ▪ Data Security
Hierarchy of Industrial Communication Systems

Automation Hierarchy

- Sensor/actuator level $\rightarrow$ Fieldbus systems $\rightarrow$ specific OSI layers
- Controller level $\rightarrow$ Fieldbus systems, Controller networks e.g. PROFINET
- Workshop level $\rightarrow$ Fieldbus Integration into Controller networks
- Management level $\rightarrow$ heterogeneous communication systems/VAN
- Business level $\rightarrow$ Virtual Automation Network/Automation Cloud
A tour around Industrial Communications

- Industrial Communications within factory levels
- Sensor/Actuator Communication
- Fieldbuses
- Controller Networks in Real-time classes
- Fieldbus Integration
- Industrial Wireless Communication
- Wide Area Networks in Automation
- Functional Safety
- Security
Wired Sensor/Actuator Communication

• **HART (Highway Addressable Remote Transducer Protocol; HART Communication Foundation)** → bidirectional digital transmission of parameters via analogue transmission lines → mostly used in Process Automation

• **ASi (Actuator-Sensor-Interface; ASi Club)** → network of actuators and sensors with binary input/output signals → any network topology (bus, star, tree) → mostly used in Factory Automation → IEC 62026-2

• **IO Link (Single-drop digital communication interface for small sensors and actuators (SDCI); IO Link Consortium)** → Point-to-point communication protocol via 24 Volt line → (IEC 61131, part 9)
HART System

PC/Host Application
RS232 or USB HART Interface
Power Supply
Field Device
250 Ohm Resistor
Handheld Terminal

www.hartcomm.org
• a point-to-point connection between the IO-Link port and the sensor or actuator,
• service data can be exchanged at the same time as process data.
• Data is transmitted by means of 24 V pulse modulation
• Gateway and communication DTM s ensure integrated device parameterization up to the sensor/actuator level. It means: Engineering tools have access to sensor data
A tour around Industrial Communications

- Industrial Communications within factory levels
- Sensor/Actuator Communication
- **Fieldbuses**
  - Controller Networks in Real-time classes
  - Fieldbus Integration
  - Industrial Wireless Communication
  - Wide Area Networks in Automation
  - Functional Safety
  - Security
Fieldbus Battle

• Twenty years ago, a Fieldbus battle took place
  ▪ At first regarding Ethernet-less approaches (many years)
  ▪ Secondly regarding Ethernet-based approaches
• At the end, a compromise was found: each party got their own Fieldbus standard → IEC 61158/IEC 61784
• Now the market decides the success of the approaches
Fieldbus

- Fieldbus Standards: IEC 61158 (Protocols); IEC 61784 (Profiles)
- Widely used Fieldbuses:
  - PROFIBUS (DP general purpose/factory automation → RS 485; PA process automation – Manchester Bus Powered) → PROFIBUS International
  - DeviceNet (general purpose) → ODVA
  - Foundation Fieldbus (process automation) → Fieldbus Foundation
  - Interbus (factory automation) → Interbus Club
# IEC 61158: Industrial communication networks - Fieldbus specifications

<table>
<thead>
<tr>
<th>Part</th>
<th>Name</th>
<th>Edition</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Overview and guidance for the IEC 61158 and IEC 61784 series</td>
<td>3</td>
<td>IS/TR</td>
</tr>
<tr>
<td></td>
<td>Publication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Physical layer specification and service definition</td>
<td>5</td>
<td>IS</td>
</tr>
<tr>
<td>3</td>
<td>Data-link layer service definition* - Type x elements - for every</td>
<td>1/2</td>
<td>IS</td>
</tr>
<tr>
<td></td>
<td>type x a special document - type 3 is PROFIBUS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Data Link Layer protocol specification* - Type x elements - for</td>
<td>1/2</td>
<td>IS</td>
</tr>
<tr>
<td></td>
<td>every type x a special document - type 3 is PROFIBUS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Application Layer service definition** - Type x elements - for every</td>
<td>1/2</td>
<td>IS</td>
</tr>
<tr>
<td></td>
<td>type x a special document - type 3 is PROFIBUS and type 10 PROFINET</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Application Layer protocol specification** - Type x elements - for</td>
<td>1/2</td>
<td>IS</td>
</tr>
<tr>
<td></td>
<td>every type x a special document - type 3 is PROFIBUS and type 10</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PROFINET</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*The present part consists of 13 subparts for the different protocol types
**The present part consists of 17 subparts for the different protocol types

Source: Felser

Peter Neumann: From Fieldbus to Automation Cloud
## IEC 61784: Industrial communication networks - Profiles

<table>
<thead>
<tr>
<th>Part</th>
<th>Name</th>
<th>Edition</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Fieldbus profiles</td>
<td>3</td>
<td>IS</td>
</tr>
<tr>
<td>2</td>
<td>Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3</td>
<td>2</td>
<td>IS</td>
</tr>
<tr>
<td>3</td>
<td>Functional safety fieldbuses</td>
<td>2</td>
<td>IS</td>
</tr>
<tr>
<td></td>
<td>Part 3-x: Functional safety fieldbuses - Additional specifications for CPF x 9 different subparts for the CPFs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Profiles for secure communications in industrial networks*</td>
<td>1</td>
<td>CD</td>
</tr>
<tr>
<td>5</td>
<td>Installation of fieldbuses - Installation profiles for CPF x</td>
<td>2</td>
<td>IS</td>
</tr>
<tr>
<td></td>
<td>for every CPF x a special document - PROFIBUS and PROFINET are CPF 3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* project moved to system security

Source: Felser
PROFIBUS Protocol Suite

There is a bundle of opportunities to implement a real Fieldbus
Recent Activities: Ethernet-based Fieldbuses

- One pair Ethernet (OPEN Alliance) → Infotainment in cars
- Basic technology: BroadR-Reach Transceiver (Broadcom) based on Gigabit Ethernet, but using only one pair
- 150 m; 100 Mbit/s; high requirements on signal processing

100 Mbps symmetrical operation using standard Ethernet PHY components

Only change is to wire-side, MAC-side remains the same

Source: OPEN Alliance
A tour around Industrial Communications

• Industrial Communications within factory levels
• Sensor/Actuator Communication
• Fieldbuses
• Controller Networks in Real-time classes
• Fieldbus Integration
• Industrial Wireless Communication
• Wide Area Networks in Automation
• Functional Safety
• Security
Controller Networks (based on Ethernet)

Real-time Classes

• **Local Soft Real-Time** approaches (Real-Time Class 1) ➔ using TCP/UDP mechanisms over shared and/or switched Ethernet networks ➔ scalable cycle time ➔ applications, where no severe problems occur, when deadlines are not met

• **Local Hard (Deterministic) Real-Time** approaches (Real-Time Class 2) ➔ using a middleware on top of the MAC layer to implement scheduling and smoothing functions ➔ cycle times from 1 to 10 ms ➔ time-critical control

• **Isochronous Real-Time** approaches (Real-Time Class 3) ➔ cycle times from <250 μs to 1 ms; tight restrictions on jitter (usually less than 1 μs) ➔ motion control
Controller Networks. Real-Time Class 1

- **PROFINET** (PROFINET International) → using Component-Based Architecture and DCOM with remote procedure call mechanism DCE RPC
- **MODBUS TCP/IP** (Schneider) → Application Layer messaging protocol for Client/Server communication between devices via different types of buses or networks
- **ETHERNET/IP** (Rockwell, ODVA) → common industrial protocol CIP (Application Layer) for different physical networks of Ethernet/IP, ControlNet and DeviceNet
- **High Speed Ethernet HSE** (Fieldbus Foundation) → Application Layer function (including Fieldbus message specification)
- **P-Net on IP** (Process Data) → using P-Net Fieldbus in an IP environment (P-Net PDUs are wrapped in UDP/IP packages)

All approaches are able to support widely used office domain protocols (SMTP, SNMP, HTTP)
PROFINET Protocol Suite

**Component Object Model**
- Component Context Management (ACCO)

**IO Object Model**
- IO Context Management
- Real-Time
- CL -RPC
- UDP
- IP

**Connection establishment**
- ACCO - Active Control Connection Object;
  CO - connection-oriented; CL – connectionless;
  RPC - Remote Procedure Call

**IEEE 802.3**
Controller Networks. Real-Time Class 2

• **PROFINET** (PROFINET International) ➔ using the Input/Output object model based on Fieldbus PROFIBUS ➔ the protocol is defined by a set of protocol machines

• **Time-Critical Control Network** Tcnet (Toshiba) ➔ using a “common memory” (virtual memory) within the Application Layer for time-critical applications; extended Data Link layer contains a scheduling functionality

• **Vnet** (Yokogawa) ➔ supports up to 254 sub networks with up to 254 nodes each. Application layer contains three Protocol machines; Data Link layer offers three services; Real-Time traffic scheduling is located on top of MAC layer.
Controller Networks. Real-Time Class 3

- **PROFINET IRT** (PROFIBUS International)
  - using a middleware on top of Ethernet MAC Layer to enable high-performance transfers, cyclic data exchange and event-controlled signal transmission.
  - Layer 7 functionality is directly linked to the middleware containing scheduling and smoothing functions → TCP/IP does not influence the PDU structure; a special Ethertype is used to identify real-time PDUs
  - PROFINET IRT adds an isochronous real-time channel to RT channels Class 2 → enables a high-performance transfer of cyclic data in an isochronous mode
  - Bandwidth is separated for cyclic RT and soft/non real-time traffic
LMPM MAC access used in PROFINET IRT

\[ 31.25 \mu s \leq T_{\text{Sendclock}} \leq 4 \text{ms} \]

- cRT - cyclic Real-Time;
- aRT - acyclic Real-Time;
- non RT - non Real-Time;
- MAC - Medium Access Control;
- LMPM - Link Layer Mapping Protocol
- Machine

Peter Neumann: From Fieldbus to Automation Cloud
Principle of synchronous data transfer

- Time Slots owned by RT communication (Bandwidth reservation)
- Not influenced by wavering TCP/IP traffic
- Switch cascading results in high QoS

Source: PNO
## Performance of PROFINET IRT

### Performance data for applications with PROFINET and IRT

<table>
<thead>
<tr>
<th></th>
<th>1 msec</th>
<th>500 µsec</th>
<th>250 µsec</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cycle time</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Amount of participants</strong></td>
<td>272</td>
<td>128</td>
<td>56</td>
</tr>
<tr>
<td><strong>Jitter</strong></td>
<td>&lt;1µs</td>
<td>&lt;1µs</td>
<td>&lt;1µs</td>
</tr>
<tr>
<td><strong>Reserve for open communication with IT-standard protocols</strong></td>
<td>50%</td>
<td>50%</td>
<td>50%</td>
</tr>
</tbody>
</table>

*) Assumed devices with 4 ports.

The restrictions of a single device must be considered.

* e.g. camera data

---

Peter Neumann: From Fieldbus to Automation Cloud 37
Controller Networks. Real-Time Class 3

- **PowerLink** (Ethernet PowerLink Standardization Group)
- Two modes:
  - Protected mode → proprietary real-time protocol on top of shared Ethernet (B&R) → cyclic exchange of real-time data
  - Open Mode → used for TCP UDP/IP based traffic
- **EtherCat** (EtherCat Technology Group) → fast backplane communication system; Two modes: direct and open
  - Direct mode: Master/Slave in an EtherCat segment with ring topology, data transfer via standard Ethernet port to other segments
  - Open mode: switched Ethernet between Ethernet-based devices
Controller Networks. Real-Time Class 3

• **Ethernet/IP with Time Synchronization** (ODVA) → using CIP Synch Protocol to enable the isochronous data transfer based on Precision Clock synchronization protocol → fully compatible with Standard Ethernet → devices without CIP Synch features can be used in the same Ethernet network

• **SERCOS III** (IG SERCOS Interface e.V.) → Master/Slave including repeaters with constant delay time, point-to-point transmission lines; each node has two communication ports, which are interchangeable; ring or line topology → the last physical slave performs the loopback function, all other work in forwarding mode
Recent Activities: Improvement of Real-time Capabilities

- Ethernet-based approaches are marching forward
  - On field level: One-pair Ethernet
  - Using switched Ethernet, since integrated switches are implemented on field devices
- The target is: Ethernet connectivity through all levels of the Automation hierarchy
- To investigate in detail (nowadays):
  - Performance of IRT approaches
  - Influence of security mechanisms (situated in Fieldbus/Controller Network devices) on performance; recommendations for security implementations
  - Usage of Time Sensitive Networks TSN
**Detailed Performance Investigation**

- For IRT: performance of the whole signal chain sensor \((t_s)\)\(\rightarrow\) actuator \((t_o)\) (IO field device \(\rightarrow\) communication system \(\rightarrow\) controller)
- Defined: generic IRT model and clearly defined models for different IRT approaches (e.g. EtherCAT; PROFINET)
- Different co-operation concepts lead to different RT performance
  - Client/Server: field devices cannot initiate communication \(\rightarrow\) central controlled Fieldbuses (e.g. EtherCAT with total frame transfer \(\rightarrow\) full frame has to pass all nodes)
  - Producer/Consumer: each Ethernet device has the same access rights (e.g. PROFINET IRT with dynamic frame packing DFP and fast forwarding \(\rightarrow\) frame becomes reduced passing Ethernet-based devices
There is a high potential for performance in complex IRT installations with a large number of nodes (Motion Control)

Steuerung S: Controller
Knoten K: Node

Sorce: Höme; Diedrich, Univ. Magdeburg
Time Sensitive Networks

- Standard Ethernet has been improved by different application areas (e.g. Entertainment, Infotainment). Important: Audio/Video Bridging AVB, multimedia on board of cars

- 802.1 working group with five active task groups: Interworking, Security, Time Sensitive Networking, Data Center Bridging and OmniRAN

- AVB requires guaranteed performance; how to do it?
  - Guaranteed high priority of data transfer (not given in best-effort-networks), but under discussion in US
  - Allocation of time slots, time-triggered operation, dynamic frame packing

- Chance: improvement of Ethernet-based services by other application areas, too, and using the results by automation community
Time Sensitive Networks

• Main areas of development
  ▪ Time synchronization
  ▪ Queuing for time-sensitive streams
  ▪ Resource and path reservation for time-sensitive streams
A tour around Industrial Communications

- Industrial Communications within factory levels
- Sensor/Actuator Communication
- Fieldbuses
- Controller Networks in Real-time classes
- Fieldbus Integration
- Industrial Wireless Communication
- Wide Area Networks in Automation
- Functional Safety
- Security
Fieldbus Integration using Segment Coupler

- Merging of Fieldbuses with different physics
Fieldbus Integration via PROFINET

Any Fieldbus

→ Merging of Fieldbuses with different physics and protocol stacks
Fieldbus Integration

Necessary Preconditions (also valid for Automation Cloud):

- Proxy Technology in Link Devices
- Mapping of objects from Fieldbus systems with different object models to PROFINET Objects \(\rightarrow\) different concepts
- Harmonisation of Engineering concepts and tools

PNO:

- for each Fieldbus (PROFIBUS, DeviceNet, INTERBUS, AS-I, CC-Link, HART, EtherCAT und CAN open) \(\rightarrow\) Integration specifications
- PROFINET is an integration network
A tour around Industrial Communications

- Industrial Communications within factory levels
- Sensor/Actuator Communication
- Fieldbuses
- Controller Networks in Real-time classes
- Fieldbus Integration
- **Industrial Wireless Communication**
- Wide Area Networks in Automation
- Functional Safety
- Security
Wireless Communications: Basic Standards

- Mobile communications standards: GSM, GPRS, UMTS, LTE, and wireless telephones (DECT).
- Lower layer standards (IEEE 802.11: Wireless LAN, and 802.15: Personal Area Networks) as basis of radio-based local networks (WLANs, Pico Networks and Sensor/Actuator Networks).
- Higher layer standards (Application Layers on top of IEEE 802.11 und 802.15.4, e.g. Wi-Fi, Bluetooth, Wireless HART*, WSAN-FA**, and ZigBee***),

* Process Automation  ** Factory Automation  ***Building Automation
Wireless HART (Process Automation)

- The protocol utilizes a time synchronized, self-organizing, and self-healing mesh architecture for Process Automation → international standard IEC 62591 (CDV release 2). The protocol supports operation in the 2.4 GHz ISM band using IEEE 802.15.4 standard radios.

- The underlying wireless technology is based on the Dust Networks' TSMP (Time Synchronized Mesh Protocol), a proprietary protocol.
Wireless HART

• TSMP enables a synchronous operation of the network nodes (called “Motes”) based on a time slot mechanism.
• It uses various radio channels (supported by MAC layer) for an end-to-end communication between distributed devices. It works comparable with a frequency hopping mechanism.
• TSMP supports star, tree as well as mesh topologies. All nodes have the complete routing function. A self-organization mechanism enables devices to acquire information of neighbouring nodes and to establish connections between them.
• Generic implementations: Emerson, WITECK consortium/Softing
ZigBee (Process Automation)

ZigBee is based on an IEEE 802.15 standard (PHY and MAC)
ZigBee distinguishes three device types:
- Coordinator ZC: root of the network tree, storing the network information and security keys. It is responsible for connection the ZigBee network to other networks.
- Router ZR: transmits data of other devices.
- End device ZED: automation device (e.g. sensor) which can communicate with ZR and ZC, but unable to transmit data of other devices.
ZigBee

The ZigBee Application Layer (APL) consists of three sub-layers:

- Application Support Layer APS (containing the connection lists of the connected devices);
- Application Framework AF and
- Zigbee Device Objects ZDO (definition of devices roles, handling of connection requests and establishment of communication relations between devices).
Wireless Sensor/Actuator Networks

WSAN-FA
• PNO Standard (Germany)
• Specification exists, two generic implementations: ABB, consortium

WIA-PA: IEC 62601, CDV release 2
• Chinese industrial wireless communication standard for Process Automation. Includes interoperation mechanism between WIA-PA and Foundation Fieldbus

ISA 100: IEC 62734 CDV release 1 approved
• Standard in IEC voting procedure (FDIS)
• Using time slot method
• Enables long frames
Recent Activities

Long Term Evolution (LTE):
• Performance evaluation of recent LTE (Release 9) in different environments
• LTE advanced Release 10 - 12:
  ▪ Multi-path transmission, frequency bundles for better throughput
  ▪ Guaranteed latency of <10 ms
  ▪ Since relay stations are very complex, should we integrate WLANs into the LTE cell?

ETSI standardisation: Frequency regulation
• Requirements of Industrial Automation → own frequency band
• Better usage of bandwidth by frequency management, mitigation mechanisms, conflict/co-existence management

Software-defined radio:
• Basic investigations
A tour around Industrial Communications

- Industrial Communications within factory levels
- Sensor/Actuator Communication
- Fieldbuses
- Controller Networks in Real-time classes
- Fieldbus Integration
- Industrial Wireless Communication
- Wide Area Networks in Automation
- Functional Safety
- Security
Remote Communication Channels over WAN

- **Non Realtime**
  - Configuration Data

- **Realtime**
  - IO data

- **Realtime**
  - Alarms

Communication Channel

- IO Controller
- IO Device

IO Input/output
CR Communication reference
Wide Area Industrial Communications

- State of the art: using Non Real-time Communications
- Opportunities of usage of heterogeneous Networks for geographically distributed automation:
  - VAN concept: infrastructure for end-to-end communication between distributed Automation Objects in heterogeneous networks → using tunneling, name-based addressing, measures to improve the availability of the end-to-end connection
  - Cloud concept: distribution of Automation Applications (for all life-time phases of an Automation System) in a heterogeneous networked environment → virtualisation of parts of needed functionality, using all features of Internet, using the IP connectivity in all hierarchy levels

Real-time communications in Automation → the Virtual Automation Network Concept
End-to-end Data Communication

This path represents the infrastructure used for the object exchange between the distributed automation functions.

From Fieldbus to Automation Cloud
Virtual Automation Network. Main Principles

- Establishment of a runtime tunnel between the connection endpoints of the geographically distributed automation objects.
- Once the runtime tunnel has been established, the exchange of the productive data (automation objects) can start and go on.
- The establishment of the connection between the application objects itself (e.g. IEC 61784-2 CPF 3 application objects to be exchanged) occurs based on the established runtime channel. This connection establishment follows the rules of the protocols which are used to realise the distributed application processes (e.g. IEC 61784-2 CPF 3),
- The VAN infrastructure enables the maintenance of the runtime tunnel based on agreed QoS
Tunneling between industrial domains
Guaranty of Availability

Mechanisms to guarantee the availability of an end-to-end communication within the heterogeneous network, especially regarding Wide Area Networks, are:

• Monitoring the actual behaviour of the selected communication path through the WAN, from the monitoring results a VAN switching can be derived,

• VAN Switching between providers or suitable transmission technologies that are configured in the VAN device communication properties

• VAN Priority mapping (mapping of the priorities of the tunnelled packets to the tunnel packets)

For more information about results of European research project “Virtual Automation Network” (2004-2009) see related publications
A tour around Industrial Communications

- Industrial Communications within factory levels
- Sensor/Actuator Communication
- Fieldbuses
- Controller Networks in Real-time classes
- Fieldbus Integration
- Industrial Wireless Communication
- Wide Area Networks in Automation
- Functional Safety
- Security
Functional Safety for Industrial Communication

- Principle: separate safety layer on top of Application layer
- Safety specification is part of the Fieldbus standard IEC 61158
- Safety profiles are part of Profile standard IEC 61784: Part 3: Functional safety fieldbuses - General rules and profile definitions (Ed. 3.0), e.g.
  - PROFIsafe (PROFIBUS, PROFINET)
  - Interbus Safety (Interbus)
  - CIP Safety (CIP) etc.
Recent Activities: Open Safety

- openSAFETY supports functions for direct data transfer between networked end devices (cross-traffic)
- Time stamps, clearly IDs of data packages etc. are used
- The protocol encapsulates safety data within a standard Ethernet
- openSAFETY-Frame consists of two sub-frames, used are copies from each other. Each sub frame has its own CRC check sum
A tour around Industrial Communications

• Industrial Communications within factory levels
• Sensor/Actuator Communication
• Fieldbuses
• Controller Networks in Real-time classes
• Fieldbus Integration
• Industrial Wireless Communication
• Wide Area Networks in Automation
• Functional Safety
• Security
Security of Industrial Automation & Control Systems

Situation:
• A modern IA&CS is highly complex and interconnected
• Multiple potential pathways exist from the outside world to process controllers
• Focusing security efforts on a few obvious pathways (typically the Enterprise/IA&CS firewall) is a flawed defence

Reasons:
• Interconnection of networks
• Use of Commercial off-the-shelf components (COTS)
• Lack of security policies and procedures

Source: Jean-Pierre HAUET, ISA Automation Conference 2012
www.kbintelligence.com/Medias/PDF/ISA_Doha_hauet.pdf
## IEC 62443

<table>
<thead>
<tr>
<th>Role</th>
<th>General</th>
<th>Asset Owner</th>
<th>System Integrator</th>
<th>Component provider</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IEC 62443-1-1 (Ed 2) Terminology, concepts and models</td>
<td>IEC 62443-2-2 Operating an IACS security program</td>
<td>IEC/TR 62443-2-3 Patch management in the IACS environment</td>
<td>IEC 62443-4-1 Product development requirements</td>
</tr>
<tr>
<td></td>
<td>IEC TR 62443-1-2 Master glossary of terms and abbreviations</td>
<td></td>
<td>IEC/TR 62443-2-4 Certification of IACS supplier security policies and practices</td>
<td>IEC 62443-4-2 Technical security requirements for IACS components</td>
</tr>
<tr>
<td></td>
<td>IEC 62443-1-3 System security compliance metrics</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IEC 62443-3-1 Security technologies for IACS</td>
<td>IEC 62443-3-2 Security assurance levels for zones and conduits</td>
<td>IEC 62443-3-3 System security requirements and security assurance levels</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The parts have different states of completion

Peter Neumann: From Fieldbus to Automation Cloud
Security of Industrial Automation & Control Systems

Defence in depth:

• provision of multiple security protections, especially in layers, with the intent to delay if not prevent an attack
• A flaw in one layer can be mitigated by capabilities in other layers
• System security becomes a set of layers within the overall network security
• Defence in depth implementation leads to divide the system into security zones, according to their functionality/criticality and to their physical location
• Security zones: grouping of logical or physical assets that share common security requirements

Source: Jean-Pierre HAUET, ISA Automation Conference 2012
www.kbintelligence.com/Medias/PDF/ISA_Doha_hauet.pdf
Security Protection Level (ISA 99)

• TSL Transport Security Layer (Banking) → for TCP Traffic
• Many organisational measures
• Not comparable methodology like Safety Integrity Level SIL for functional safety

Here: only one security aspect interesting for component provider:
• Influence of security measures encryption methods,
• Ethertype and implementation allocation on field devices
• real-time behaviour and development effort
Valuation of Recent Activities

• Bouquet of Fieldbuses → Migration of recent fieldbuses and Ethernet-based approaches → Ethernet goes to twisted pair
• Hierarchical communication architecture → Flat communication architectures → uninterrupted vertical communication using IP
• Security measures require additional resources, mostly outside the automation devices → integrated security measures inside the automation device (esp. within the communication drivers) → Security functionality must go into the nodes!
• Safety → good situation, most of the offered systems can have a standardised safety layer
Outline

1. Introduction

2. Short DCS history and resulting requirements for Industrial Communication Systems

3. A tour around Industrial Communications, recent activities

4. Future work and outlook
   - Universal IP connectivity enables better vertical factory communication
   - Widely used Wireless Communications
   - Security functionality goes to field devices
   - Automation Cloud as infrastructure of Industry 4.0
Universal IP connectivity enables better vertical factory communication

• There are two ways to enhance the IP connectivity:
  ▪ One-pair Ethernet → it enables wired connection via Ethernet down to the field area
  ▪ Wireless connection using IP-enabled wireless technologies
• Important regarding the desired connectivity of many wireless devices for Engineering and Maintenance
Widely used Wireless Communications

Actually, there are interesting topics:

• Own frequency band for Automation
• Co-existence of competing wireless technologies
• Harmonisation of functionality in wired and wireless nodes
• Requirements of factory automation on wireless technologies
• Software-defined Radio SDR
Own frequency band for Automation

- ETSI standard EN 300 328, Version 1.8.1 will be binding in 2015
- This standard regulates the access to 2,4 GHz ISM Band (mitigation of free medium, waiting, change to another frequency etc.) → not acceptable
- Unfortunately: the requirements of automation have not been considered, especially
  - the real-time requirements
  - efficient usage of valuable spectrum resource
  - Fair sharing of spectrum on different wireless systems
- Way out: Co-existence management IEC 62657-2 → each device/connection/network gets its own frequency band, adaption of power and time → effort for planning and manual co-existence management → central automatic management needed
Own frequency band for Automation

Taskforce „Regulation for Wireless Industrial Automation (IA)“

• Requirements of Automation Industry on EN 300 328 v 1.9.1 (new work item)
• Allocation of an additional frequency band outside of the 2.4 GHz Band (e.g. 5,725-5,875GHz)
• Additional medium access methods required

Alternative ?: usage of LTE Advanced (Release 10.12)

• Multipath propagation,
• frequency bundling for more throughput,
• guaranteed latencies

Source: ZVEI, ifak
Harmonisation of functionality in wired and wireless nodes

- Wireless technologies offer a large bundle of functionality, esp. security mechanisms, which are interesting for wired technologies, too.
- Both technologies are going to support IP connectivity
- There is a need for harmonisation in the field of Industrial Automation
Requirements of factory automation on wireless technologies

Important requirements:
• the real-time behaviour (see real-time classes)
• efficient usage of valuable spectrum resource
• Fair sharing of spectrum on different wireless systems

Necessary:
• Frequency management for fair usage of bandwidth
• Mitigation mechanisms
• Conflict management, self-management of resources
• Central co-existence management
Software Defined Radio SDR

- Basic idea: Opportunity to modify radio functionality → very serious requirement on frequency regulation, since specific application have to be protected, and on analogue circuits
- SDR is type of radio in which some or all of the physical layer functions are software controlled. Software control is the use of software processing within the radio system or device to select the parameters of operation*.
- Advantages:
  - Dynamic adaptation of air interface—frequency, modulation, transmission power, time course
  - flexible interference cancellation – signal estimation and minimize disturbance
  - Spectrum aggregation  simultaneous usage of large bandwidth

There is a long way towards using SDR in Industrial Automation

*ITU-R SM.2152
Security functionality goes to field devices

• Encryption is necessary for Process Automation (protection of recipes). Not so important for Factory Automation, if the senders are trustworthy

• Technical measures have to be developed
  ▪ Public Key Infrastructure
  ▪ Key Management (Zone concept/ Firewalls?)
  ▪ Asymmetric encryption

• integrated security measures inside the automation device (esp. within the communication drivers) ➔ Security functionality must go into the nodes! ➔ horizontal security ➔ Pair of keys necessary between Controller and each device ➔ many effort

• Special requirement: Security versus performance ➔ additional PDU extension for trustworthy sender identification and test pattern transfer (e.g. Hash) ➔ additional EtherType? Additional time within a real-time cycle
Wide Area Network for Distributed Automation
Desired Online Changeability of data transmission paths

Telecommunication Switch Mechanism needed

Public and Private Telecommunication Networks (wired/wireless)

Public Network 1

Private Network 1

Public Network m

Private Network n

QoS_1

QoS_k

Agreements with providers are necessary to guarantee the required QoS

Telecommunication Switch Mechanism needed

Remote industrial domain

Local industrial domain

CEP_r

CEP_l
Automation Cloud as infrastructure of Industry 4.0

There are several opportunities to use Cloud Computing in Industrial Automation with DCS:

- Using recent field communication up to Controller network, proxy owns IP connectivity and connects to the IP World with Cloud Computing
- Controller network own IP connectivity, Controller functionality could work in the Cloud
- IO devices own TP connectivity (e.g. using twisted-pair Ethernet), all functions of information processing could work in the cloud

Recent Cloud infrastructure (e.g. MS ASURE) offers Security measures (Transport Layer Security TSL)
Automation Cloud. Scenario 1

OS Operator Station
ES Engineering Station
MS Maintenance Station
RIO Remote Input/Output

Controller Network
PLC
Fieldbus
Proxy
Cloud Computing
ES
MS
RIO

Peter Neumann: From Fieldbus to Automation Cloud
Automation Cloud. Scenario 2

OS Operator Station
ES Engineering Station
MS Maintenance Station
RIO Remote Input/Output

Cloud Computing

Proxy

Fieldbus

ES

MS

OS

RIO

Peter Neumann: From Fieldbus to Automation Cloud
Automation Cloud. Scenario 3

OS Operator Station
ES Engineering Station
MS Maintenance Station
RIO Remote Input/Output

IP Connectivity of IO Devices (One-pair Ethernet)

Cloud Computing

ES
MS
OS
RIO

Peter Neumann: From Fieldbus to Automation Cloud
Advantages of using Automation Cloud

- Complex Automation function can be virtualised and run in the cloud infrastructure (e.g. PCS 7)
- Necessary performance of end-to-end connections between automation objects can be offered by cloud
- There are value-added services of the cloud infrastructure, which can be used in automation (e.g. Weather, time, rates)
Automation Cloud as infrastructure of Factory 4.0

Conditions to be fulfilled:
• Internet connectivity
• Virtualisation of functionalities in all hierarchy levels, which should run in the cloud (Digital Factory)
• Security mechanisms also in resources, which not situated in the cloud \(\rightarrow\) horizontal security in the field and controller level \(\rightarrow\) handling to be improved
• Guaranteed real-time QoS by resource assurance
• Functional Safety layers are available

There is to do a lot! I wish you success.
WFCS
Workshop Factory
Communication Systems

Toulouse,
May 5th – 7th, 2014

Prof. Dr. Peter Neumann

Institut für Automation und
Kommunikation e.V. Magdeburg
Werner-Heisenberg-Str. 1
39106 Magdeburg
Tel. +49 39 19 90 14 0
Fax: +49 39 19 90 15 90
http://www.ifak.eu
E-mail: peter.neumann@ifak.eu