

Embedded Systems in Industrial Applications

Trends and Challenges



IEEE Industrial Electronics Society

SIES 2007

Richard Zurawski
ISA Group, USA

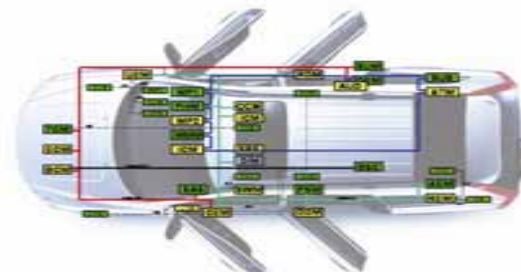
Applications Areas of Embedded Systems reported at conferences and technical events

Frequently reported



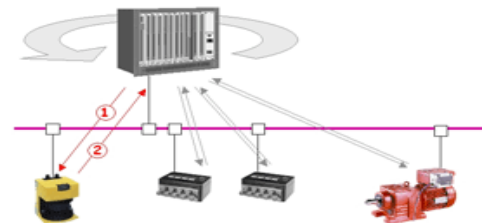
Multimedia

Start being reported



Automotive embedded systems

Seldom reported



Factory/Industrial Automation

Applications Areas of Embedded Systems

Multimedia



Reasons for demand:

- Personal communication
- Personal entertainment
- Personal comfort



Market characteristics:

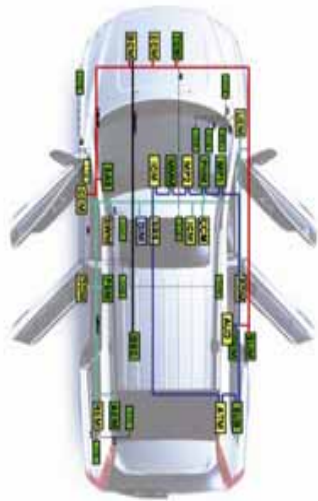
- Large volumes
- Small profit margin (competition)
- Need for constant innovation
- Short time-to-market
- High development cost



Applications Areas of Embedded Systems

Reasons for using ES:

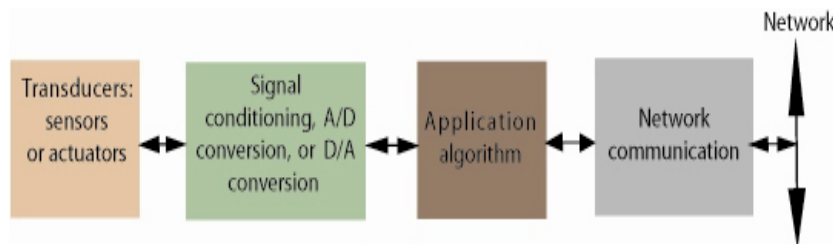
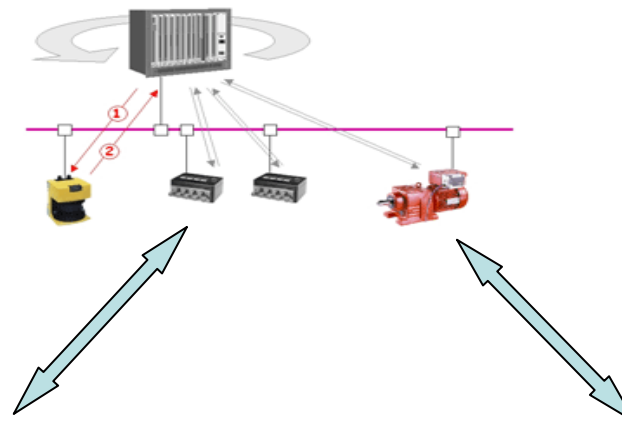
- Power train – performance/efficiency
- Body – safety (anti-locking break system, active suspension)
- Telematics – navigation, personal entertainment (video, audio equipment), etc



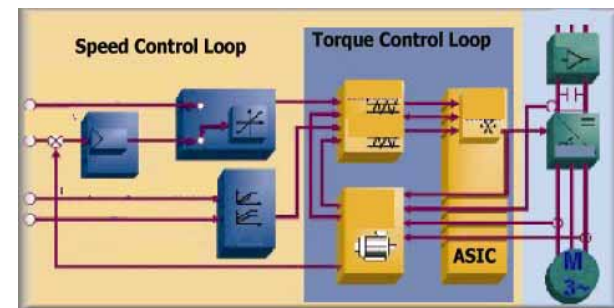
Market characteristics:

- Relatively large volume
- Small profit margin
- Need for constant innovation
- Short time-to-market
- High development cost

Factory/Industrial Automation



Integrated Networked Smart Transducer



Direct Torque Control

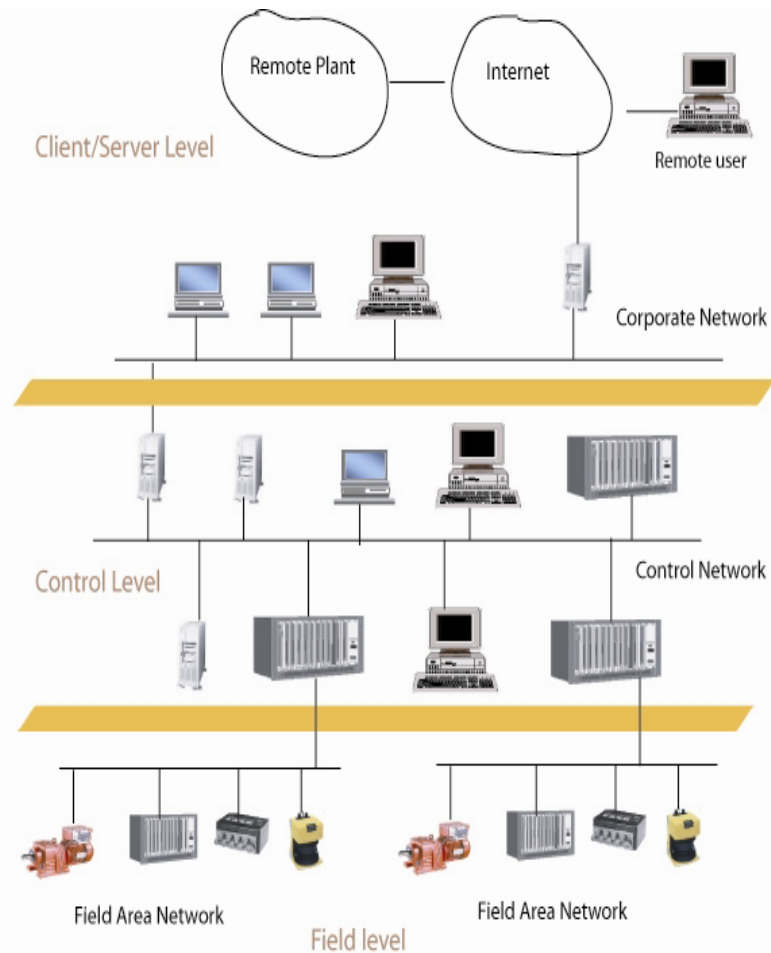
(Printed Circuit Board Assembly / SoC?)

Factory/Industrial Automation



Robot Arm:

- welding
- painting
- assembly



Distributed Control System

Industrial Requirements

Industrial requirements depend on applications; special requirements typically include:

- Availability and reliability
- Safety
- Survivability
- Security
- Real-time, deterministic response
- Power consumption
- Lifetime issues

Industrial Requirements

- **Availability and reliability**

Availability (from Wikipedia): The degree to which a system, subsystem, or equipment is operable and in a committable state at the start of a mission, when the mission is called for at an unknown, *i.e.*, a random, time. Simply put, availability is the proportion of time a system is in a functioning condition.

Reliability: The IEEE defines it as ". . . the ability of a system or component to perform its required functions under stated conditions for a specified period of time."

In general, in automation, availability and reliability are required to be very high, to minimize the cost of operation (for instance to minimize scheduled and unplanned maintenance)

Industrial Requirements

Safety & Survivability

Safety: Absence of catastrophic consequences of a system failure for property, humans, and environment

Survivability: Need for restricted modes of operation that preserve essential services in adverse operational environments

The (embedded) automation systems and plants have to be safe operational over extended periods of time, even if they continue operation in a degraded mode in the presence of a fault.

Industrial Requirements

Security

Operational **IT** security requirements:

- Confidentiality

Protecting data from unauthorized entities

- Integrity

Protecting against unauthorized data manipulation

- Availability

Data available when needed

Operational security requirements for **discrete manufacturing and process control systems**:

- Safety

- Availability

Dependability

Dependability of an automation system and plant is its ability to deliver a service as expected; integrates such quality attributes as:

- Availability
- Reliability
- Safety
- Survivability
- Security

Embedded systems used in safety critical applications such as nuclear and chemical plants, and power systems require a high level of dependability.

The dependability issue is critical for technology deployment in safety-critical systems.

One of the main bottlenecks in the development of safety-critical systems is the software development process.

Industrial Requirements

Real-time operation

Typically, (networked) embedded systems are required to operate in a reactive way (for instance, systems used for control purposes) requiring to respond within a predefined period of time, mandated by the dynamics of the process under control.

A response, in general, may be:

- **Periodic** - to control a specific physical quantity by regulating dedicated end-effector(s), or
- **Aperiodic** - arising from unscheduled events such as out-of-bounds state of a physical parameter or any other kind of abnormal conditions.

Industrial Requirements

Real-time operation & Deterministic response

Broadly speaking:

Soft real-time systems - systems which can tolerate a delay in response

Hard real-time systems - systems which require **deterministic response** to avoid changes in the system dynamics which potentially may have negative impact on the process under control, and as a result may lead to economic losses or cause injury to human operators.

The need to guarantee a deterministic response mandates using appropriate scheduling schemes, which are frequently implemented in application domain specific real-time operating systems or frequently custom designed “bare-bone” real-time executives.

Industrial Requirements

Power Consumption

Low-power design: extending life time of electronic components (lifecycle).

Wireless sensor networks – need for self-sustained energy source.

Sources of wireless power:

- Batteries, fuel cells, etc.
- From local environment: light, heat, vibration,
- Transmitted by optical and radio frequencies, sound

Industrial Requirements

Lifecycle issues

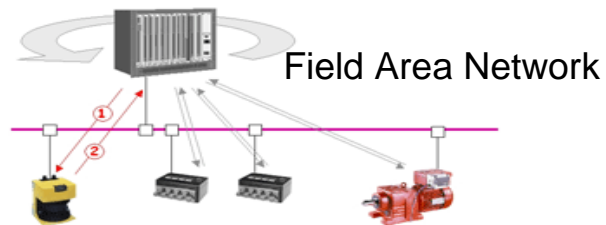
Typical lifetime of a device in an industrial environment is around 10 - 20 (plus) years

Need for:

- Increased reliability
- Robustness
- Reconfigurability
- Maintainability
- Scalability

Industrial Requirements

Connectivity



(in general) networks connecting field devices such as sensors and actuators with field controllers, programmable logic controllers (PLCs) in industrial automation, for instance, as well as man-machine interfaces, SCADA, for instance.

(a fieldbus is, in general, a digital, two way, multidrop communication link)

Benefits:

- reduced cabling
- increased flexibility
- improved system performance
- ease of system installation, upgrade, and maintenance.

Traffic characteristics:

- low data rates (data rates above 10 Mbit/s, typical of LANs, have become a commonplace in field area networks)
- small size of data packets
- typically require real-time capabilities which mandate determinism of data transfer.

Connectivity

Client/Server Level:

core protocols (i.e. UDP/TCP/IP), and other service and management protocols (i.e. SNMP, DHCP, etc.)

Traffic characteristics:

- High data rates
- Large data packets

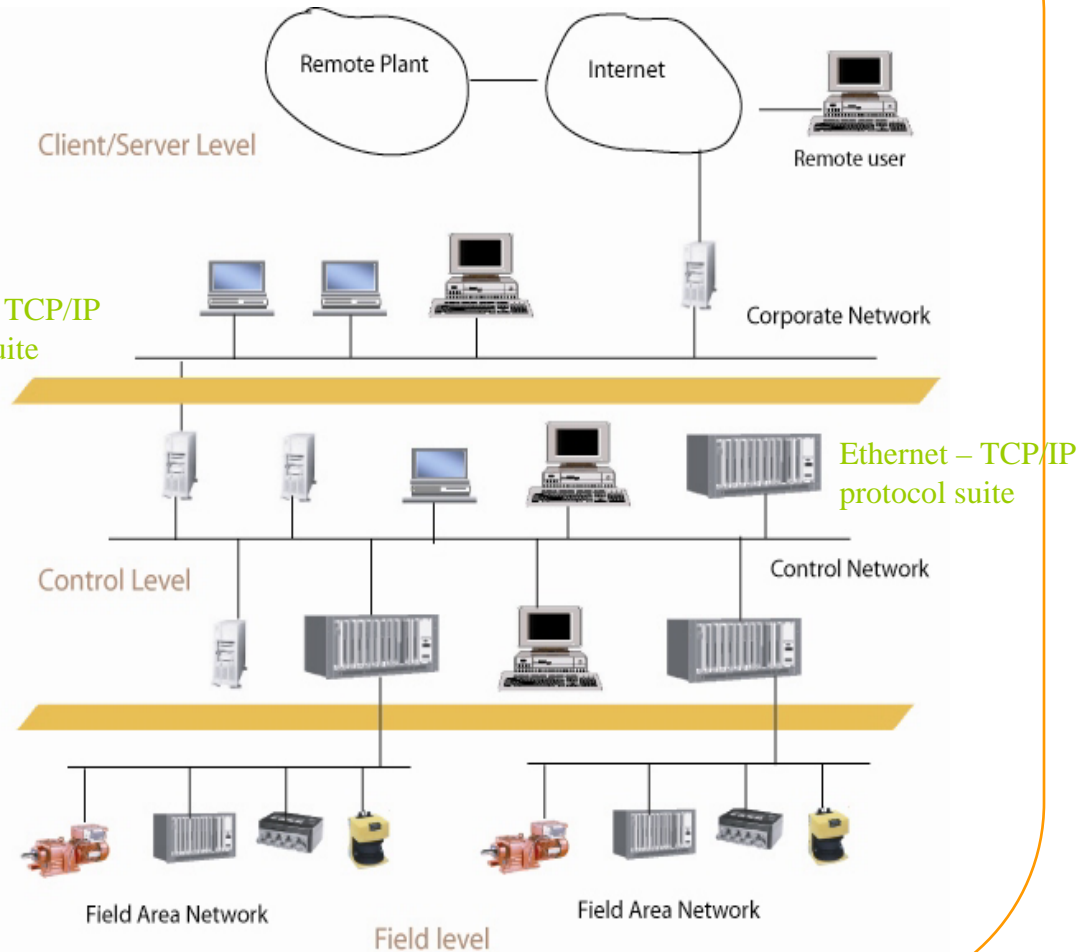
Ethernet – TCP/IP
protocol suite

Controller Networks:

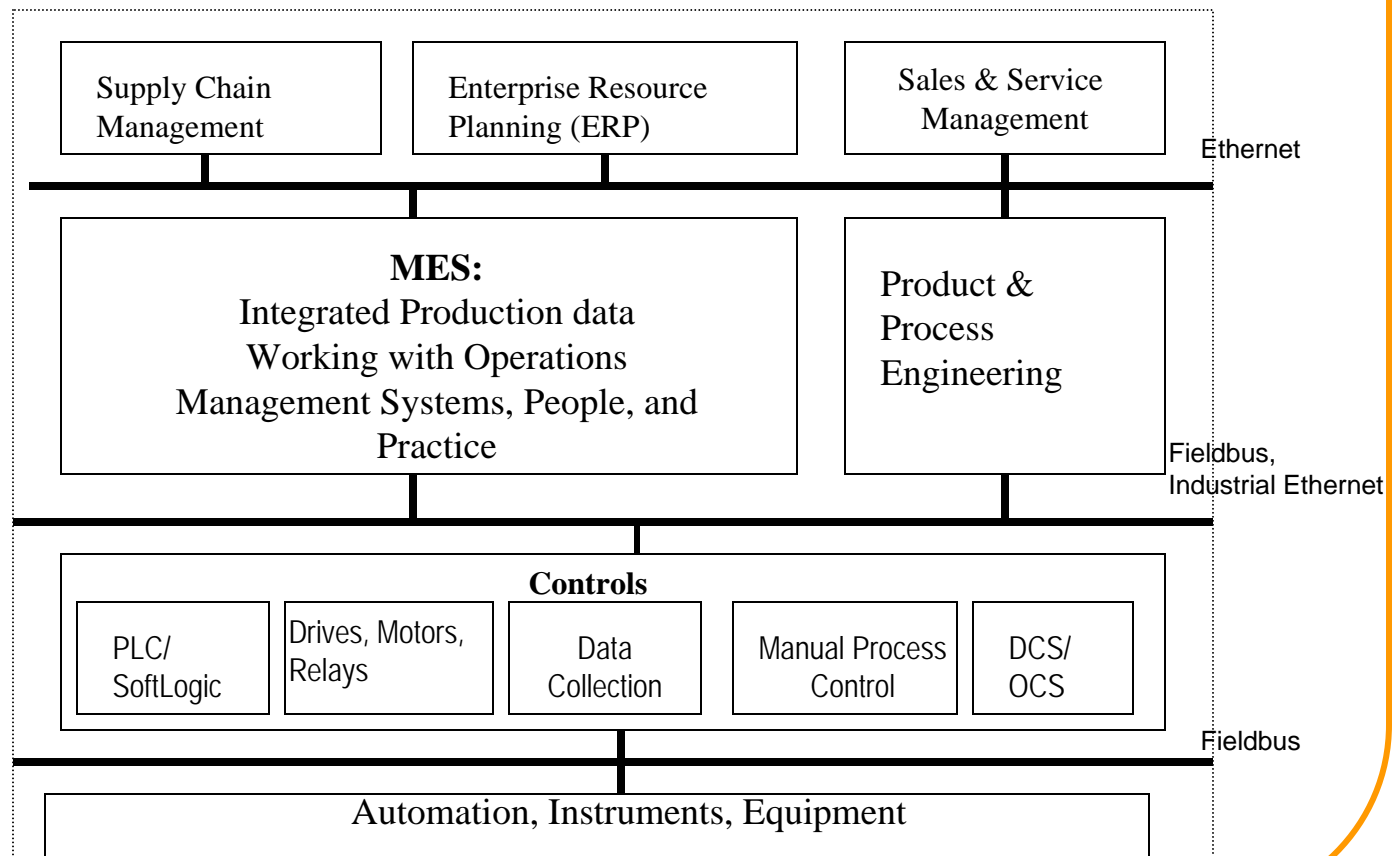
used to exchange real-time data among controllers and operator workstations used for process control and supervision

Traffic Characteristics:

- small and infrequent data packets from the field level
- (potentially) high data rates and large data packets from the business or enterprise level



MESA (Manufacturing Execution System Association) – Plant Information Model



Connectivity: Integration

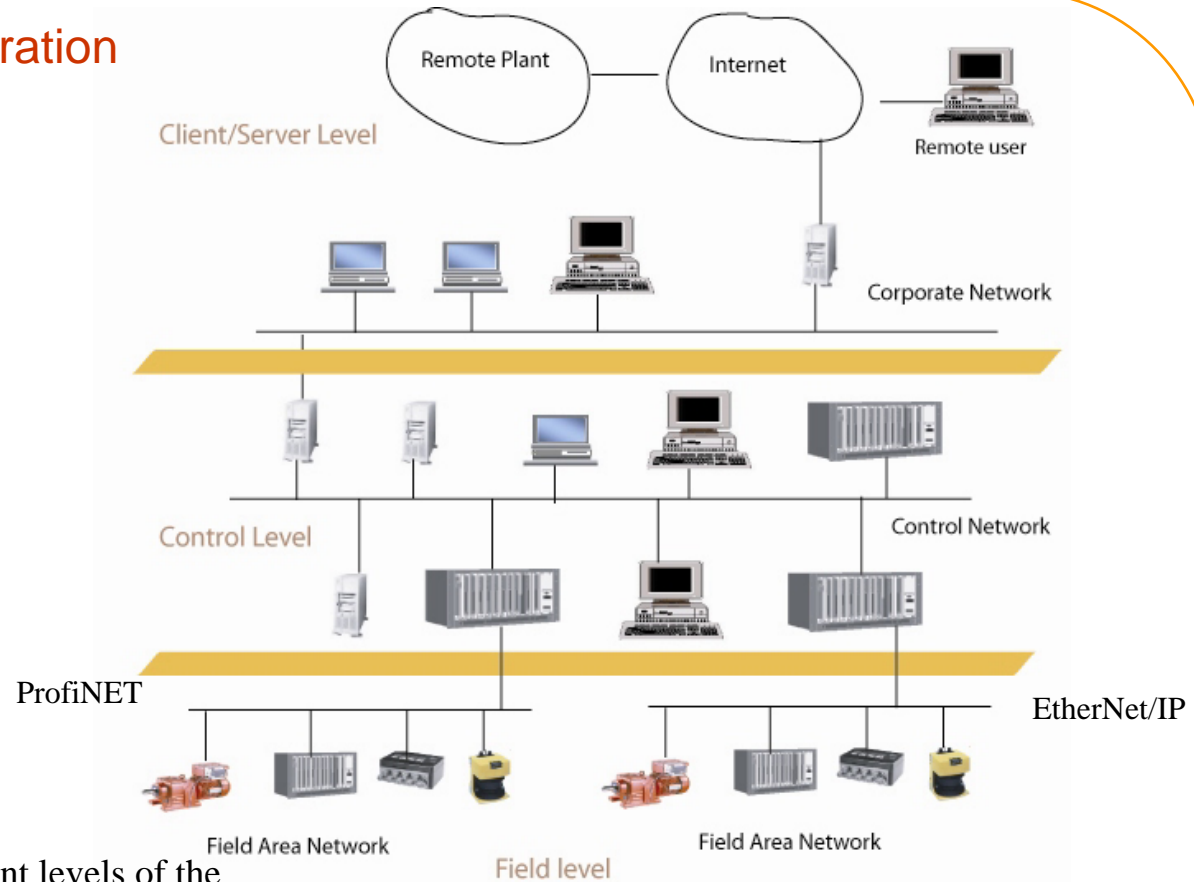
Islands of automation

The use of propriety field devices (sensors/actuators), machining tool controllers, and manufacturing/process machinery typically leads to the deployment of dedicated field area and control networks developed to link specific devices and systems. This creates “islands of automation” integrated locally around specific and frequently incompatible with others network technologies and data representations.

The integration solutions involve both communication infrastructure, and applications interfaces and data representation.

Integration

V
E
R
T
I
C
A
L



Between different levels of the automation (or organization) hierarchy: from field devices via manufacturing executions systems to business level and processes

H
O
R
I
Z
O
N
T
A
L

In the communication context, involves different plant automation units, or even separate automation sections within a unit.

Industrial Ethernet

Emerging trend in the horizontal and vertical integration: the use of the “**industrial Ethernet**”, or **Real-Time Ethernet (RTE)**, that supports real-time communication at the factory floor.

In the RTE, the random and native **CSMA/CD** arbitration mechanism is being replaced by other solutions allowing for:

- deterministic behavior required in real-time communication to support soft and hard real-time deadlines,
- time synchronization of activities required to control drives, for instance, and
- for exchange of small data records characteristic of monitoring and control actions.

Real Time Ethernet

Real-Time Ethernet (RTE): the RTE, under standardization by IEC/SC65C committee, is a fieldbus technology which incorporates Ethernet for the lower two layers in the OSI model (physical layer, and data link layer including implicitly the medium access control layer).

The three different approaches to meet real-time requirements:

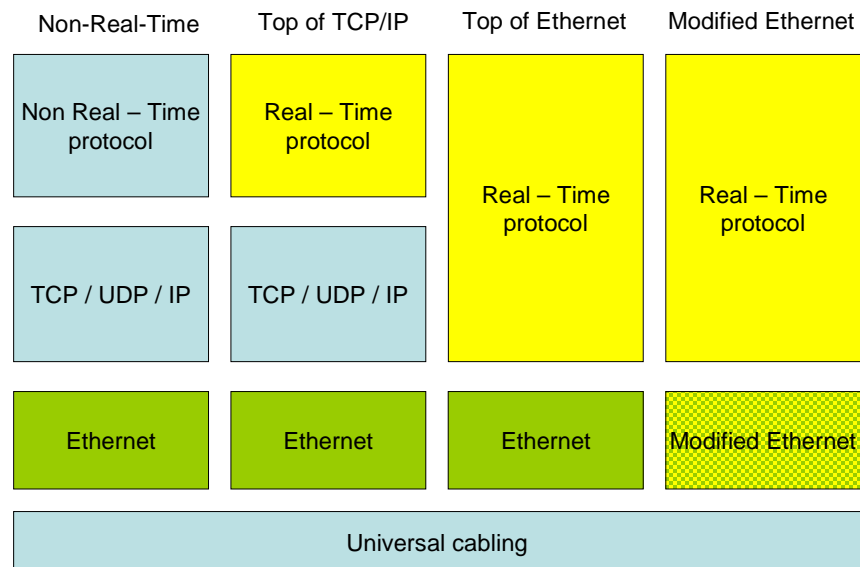
- retaining the TCP/UDP/IP protocols suite unchanged (subject to non deterministic delays), all real-time modifications are enforced in the top layer.
- the TCP/UDP/IP protocols suite is bypassed, the Ethernet functionality is accessed directly – in this case, RTE protocols use their own protocol stack in addition to the standard IP protocol stack.
- the Ethernet mechanism and infrastructure are modified.

Real Time Ethernet benefits

The direct support for the Internet technologies allows for:

- vertical integration of various levels of industrial enterprise hierarchy to include seamless integration between automation and business logistic levels to exchange jobs and production (process) data;
- transparent data interfaces for all stages of the plant life cycle;
- the Internet- and web-enabled remote diagnostics and maintenance, as well as electronic orders and transactions;
- mitigating the ownership and maintenance cost by the use of standard components such as protocol stacks, Ethernet controllers, bridges, etc.

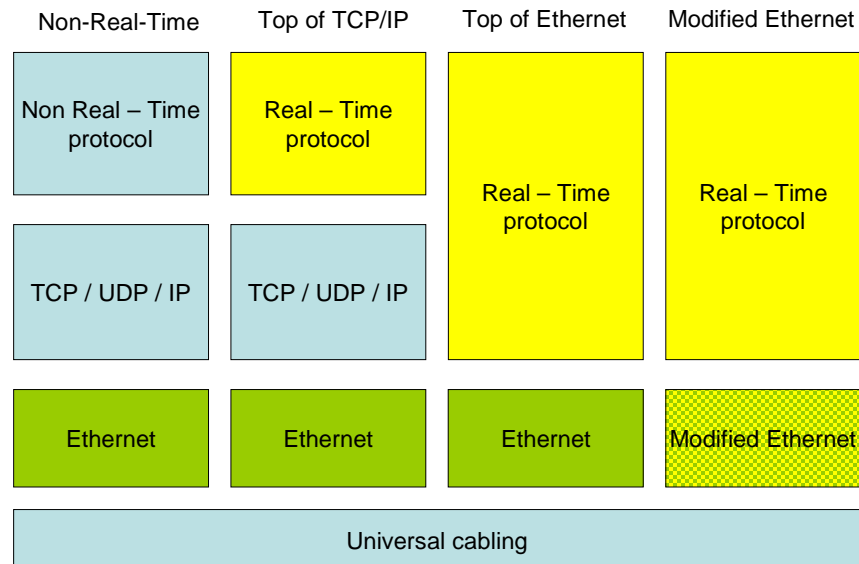
Real Time Ethernet



Possible structures of RTE

Real Time Ethernet

First approach is based on retaining the TCP/UDP/IP protocols suite unchanged (subject to non deterministic delays), all real-time modifications are enforced in the top layer.



Modbus/TPC:
defined by
Schneider Electric
and supported by
Modbus-IDA

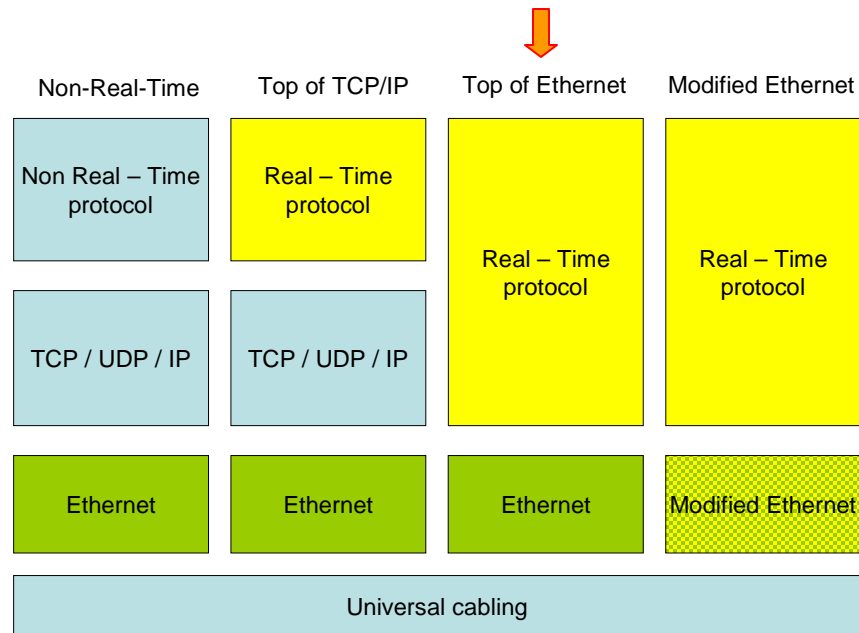
EtherNet/IP:
defined by Rockwell
and supported by the
Open DeviceNet
Vendor Association
(ODVA) and
ControlNet
International

P-Net (on IP):
proposed by the
Danish P-Net
national committee,

Vnet/IP:
developed by
Yokogawa, Japan.

Real Time Ethernet

In the second approach, the TCP/UDP/IP protocols suite is bypassed, the Ethernet functionality is accessed directly – in this case, RTE protocols use their own protocol stack in addition to the standard IP protocol stack.



- **Ethernet Powerlink** (EPL): defined by Bernecker + Rainer (B&R), and supported by the Ethernet Powerlink Standardisation Group

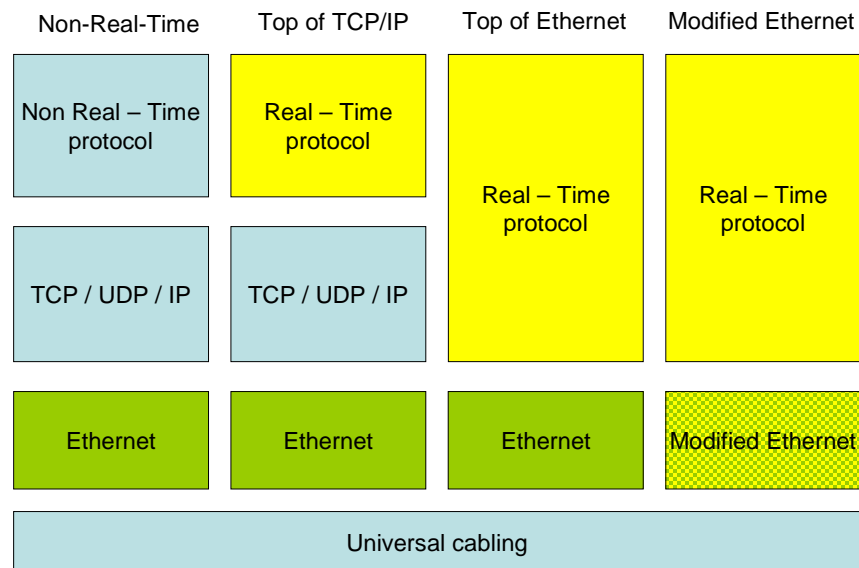
- **TCnet** (a Time-critical Control Network): a proposal from Toshiba

- **EPA** (Ethernet for Plant Automation): a Chinese proposal

- **PROFIBUS CBA** (Component Based Automation): defined by several manufacturers including Siemens, and supported by PROFIBUS International

Real Time Ethernet

In the third approach, the Ethernet mechanism and infrastructure are modified.

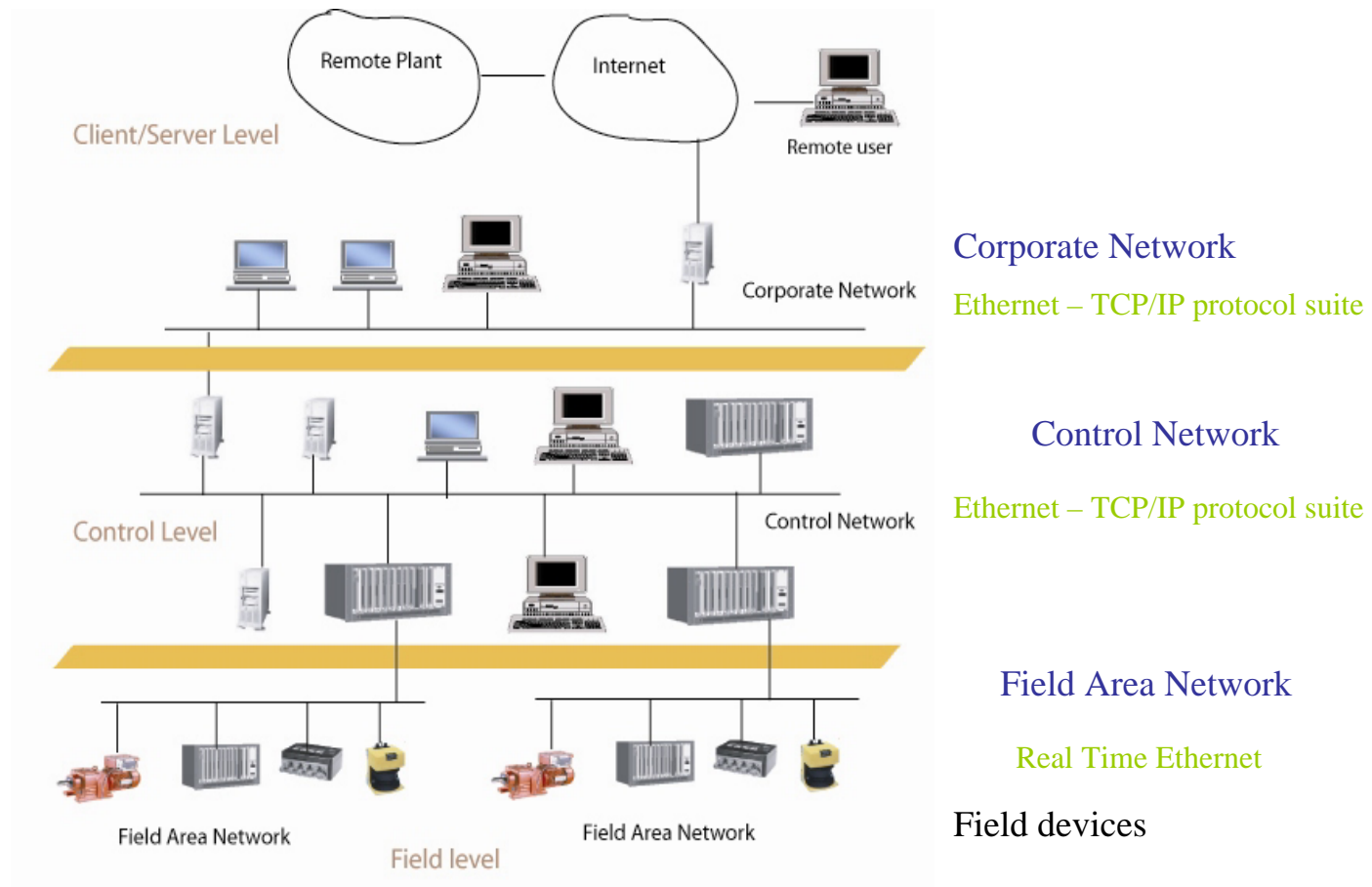


- **SERCOS III:** under development by SERCOS

- **EtherCAT:** defined by Beckhoff and supported by the EtherCat Technology Group

- **PROFINET IO:** defined by several manufacturers including Siemens, and supported by PROFIBUS International.

Security in Industrial Networked Embedded Systems



Security in Industrial Networked Embedded Systems

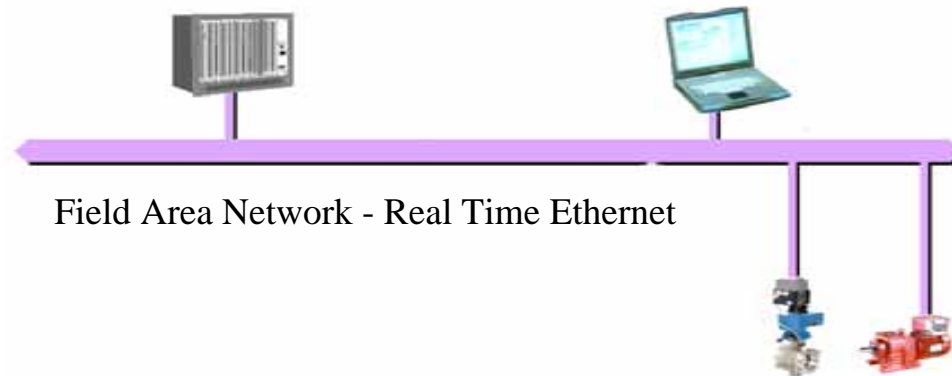
Operational security requirements for automation and process control systems:

- Safety
- System/plant availability

electronic security attacks, which may compromise the integrity of these systems and endanger plant safety

Security in Industrial Networked Embedded Systems Field Level

Fieldbuses, in general, do not have any security features. As they are frequently located at the premises requiring access permit, eavesdropping or message tampering would require a physical access to the medium. A potential solution to provide a certain level of security is the access point (PLC, for instance) control.



The emerging Ethernet based fieldbuses are more vulnerable to attack on account of using the Ethernet and the TCP/IP protocols and services. Here, the general communication security tools for TCP/IP apply.

Security in Industrial Networked Embedded Systems Device and Embedded Level

Real Time Requirements:

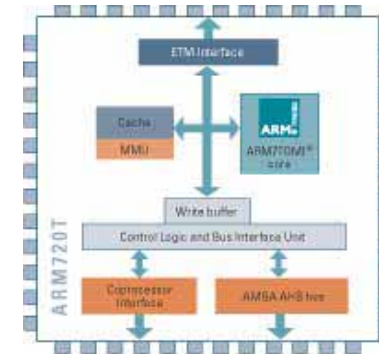
In case of a denial of service attack (DoS), the processor handles a high-level of communication interrupts potentially compromising the real-time requirements – a need for clever interrupt priority allocation and/or selection

Robustness:

A controller has to withstand autonomously a security attack such as buffer overflow to crash the system – a need for proper error and exception handling

Power Restrictions:

Battery powered embedded controllers can fail by being exposed to unnecessary processing cause by DoS attack conditions, for instance – causing battery draining

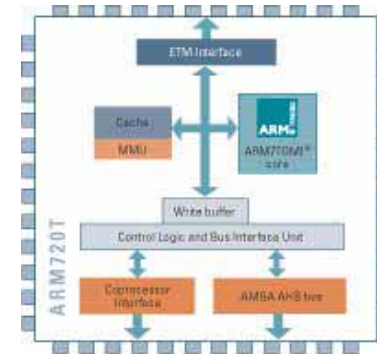


Security in Industrial Networked Embedded Systems Device and Embedded Level

Memory and Processing Limitations:

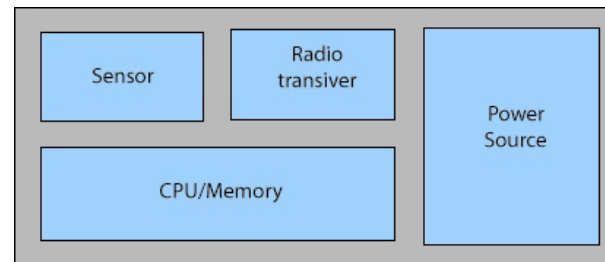
The limited computing, memory, and communication bandwidth resources of controllers embedded in the field devices pose considerable challenge for the implementation of effective security policies which, in general, are resource demanding.

This limits the applicability of the mainstream cryptographic protocols, even vendor tailored versions. The operating systems running on small footprint controllers tend to implement essential services only, and do not provide authentication or access control to protect mission and safety critical field devices. In applications restricted to the Hypertext Transfer Protocol (HTTP), such as embedded web servers, Digest Access Authentication (DAA), a security extension to HTTP, may offer an alternative and viable solution.



Wireless Sensor Networks

Wireless sensor network: (in general) a collection of spatially distributed devices with embedded sensors to measure environmental conditions.



Major characteristics:

- Self-contained
- No pre-arranged network topology: organized by nodes on ah-hoc basis.
- Ability to self-heal; network operation not affected if a node goes down

Wireless Sensor Networks in Industrial Applications

Pre-arranged network topology: determined by the discrete manufacturing or continuous process equipment arrangement or system architecture

No ability to self-heal; network and system operation is affected if a node goes down

Long life-time

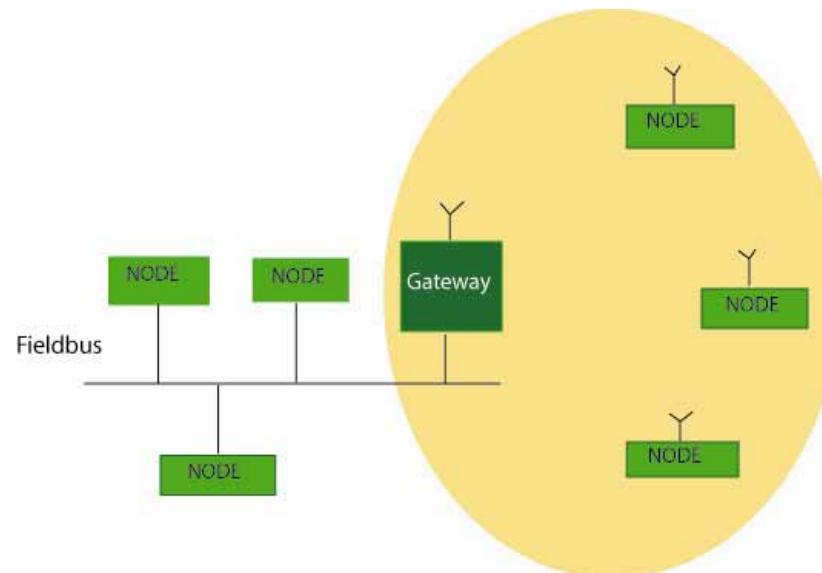
Expensive (node involved in a great deal of computing)

Wireless Sensor Networks in Industrial Applications

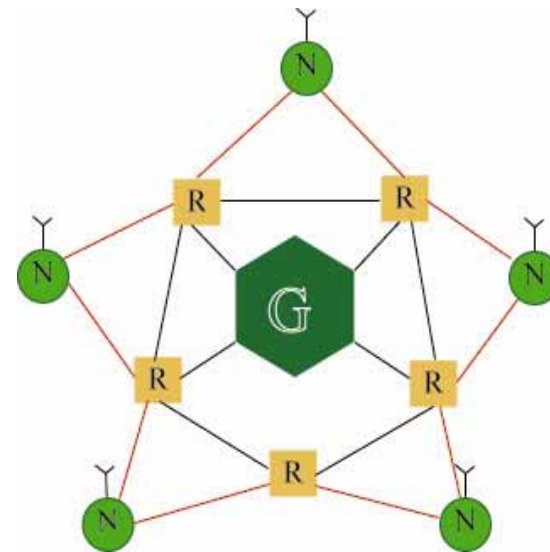
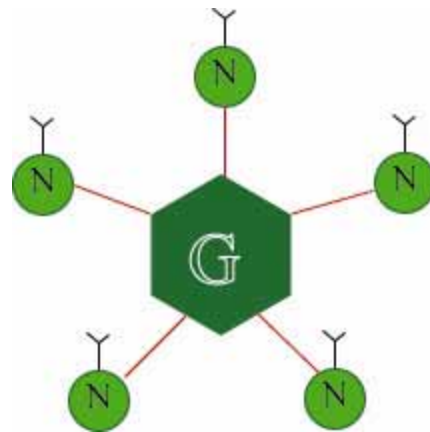
Real-time restrictions; hard bounds on the maximum delay

- discrete manufacturing – tens of mSec.
- process control – Sec.
- assets management – minutes or hours.

Hybrid wireless-wireline architecture: wireline based data distribution from the collection point



Wireless Sensor Networks in Industrial Applications



G – gateway

R- router

Common topologies used in industrial applications

Wireless Sensor Networks in Industrial Applications

Reliability; mostly through transmission redundancy:

- Space diversity – transmission through different paths
- Frequency diversity – on different frequencies
- Time diversity – several times on the same frequency
- Modulation scheme diversity – different modulation schemes

Wireless Sensor Networks in Industrial Applications

Low power consumption

Factors in minimizing power consumption:

- low power elements; CPU, for instance, runs on reduced clock rate with less on-chip functionality
- Operational regime: sleep/wakeup mode – transmission only if the value of a measured physical quantity is larger than the predetermined bound
- Communication protocol – dictates a lower bound on the power consumption

Wireless Sensor Networks in Industrial Applications

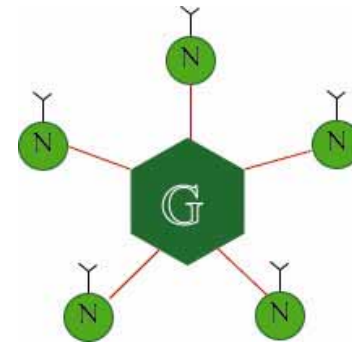
Communication Protocols:

Wireless Interface to Sensors and Actuators (WISA); a low power protocol, high performance.

Characteristics:

- Single-hop - avoids delays in intermediate nodes
- Time Division Multiplexing (TDM) – no collision; a node is alone on the channel.

Applications: discrete manufacturing if the single hop condition is met.



Wireless Sensor Networks in Industrial Applications

Communication Protocols:

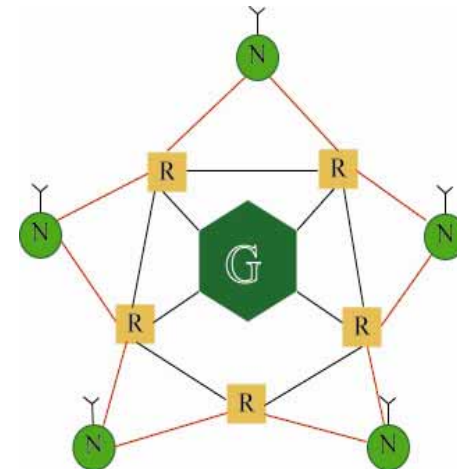
ZigBee specification (IEEE 802.15.4 protocol)

Characteristics:

Multi-hop – intermediate nodes (router nodes) to be mains powered

No timeslots allocation to messages – contention for channel access, increasing latency and power consumption

Applications: process control, asset monitoring applications, etc.



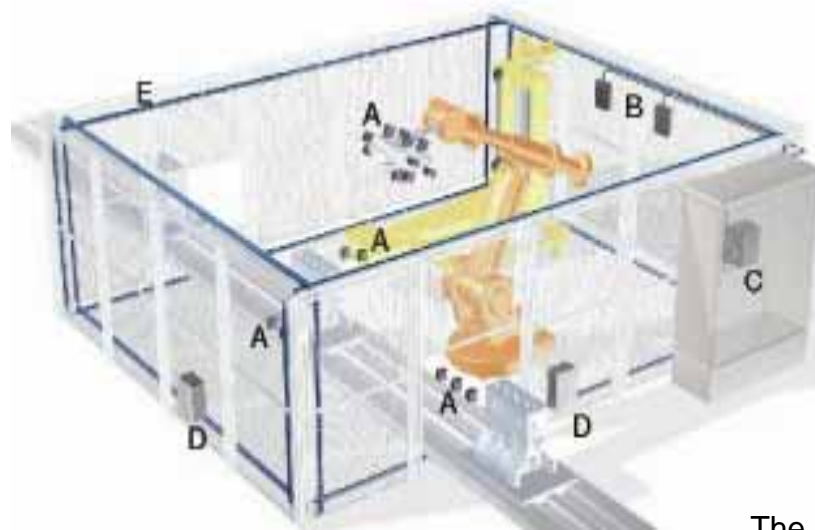
Wireless Sensor/Actuator Networks in Industrial Applications

Benefits:

- flexible installation and maintenance,
- mobile operation required in case of mobile robots,
- alleviates problems with cabling.

Wireless Sensor/Actuator Networks in Industrial Applications

ABB Wireless Robotic Cell *



WISA (wireless sensor/actuator) system to network proximity (position) sensors

The sensors communicate with a wireless base station via antennas mounted in the cell.

The base station can handle up to 120 wireless sensor/actuators and is connected to the control system via a (wireline) field bus.

To increase capacity, a number of base stations can operate in the same area.

WISA provides wireless power supply to the sensors, based on magnetic coupling.



Base station



Proximity sensor

* Figures used with permission

Wireless Sensor/Actuator Networks in Industrial Applications

Standard Bluetooth 2.4 GHz radio transceiver and low power electronics handle the wireless communication link.

To meet the requirements for high reliability, low and predictable delay of data transfer, and support for high number of sensor/actuators, a specialized RF front end was developed for the base station to provide collision free air access by allocating a fixed Time Division Multiple Access (TDMA) time slot to each sensor/actuator. (the commercially available solutions such as IEEE 802.15.1/ Bluetooth, IEEE 802.15.4/ZigBee, and IEEE 802.11 variants cannot not fulfill all the requirements.)

Frequency hopping (FH) was employed to counter both frequency-selective fading and interference effects, and operates in combination with automatic retransmission requests (ARQ).

The parameters of this TDMA/FH scheme were chosen to satisfy the requirements of up to 120 sensor/actuators per base station.

Each wireless node has a response or cycle time of 2 ms, to make full use of the available radio band of 80 MHz width.

The frequency hopping sequences are cell-specific and were chosen to have low cross-correlations to permit parallel operation of many cells on the same factory floor with low self-interference.

Opportunities and Challenges - Industrial Embedded Systems

- efficient and error-free design of SoC, and in particular Multi-Processor System-on-Chip (MPSoC), which combines the advantages of parallel processing with the high integration capability of SoC.
- evolving specific application area configurable platforms
- testing of embedded cores in SoC,
- power-aware computing,
- security in embedded systems,
- safety in networked embedded systems:
 - PROFIsafe - PROFIBUS/PROFINet
 - CIP Safety – CIP family of protocols
- standardization

Useful Sources:

Embedded Systems

Embedded Systems Handbook, ed. R. Zurawski, CRC Press/Taylor & Francis, 2005.

Networks & Networked Embedded Systems

The Industrial Communication Technology Handbook, ed. R. Zurawski, CRC Press, Florida, 2005.

Proceedings of the IEEE, Special Issue on Industrial Communication Systems, guest editor R. Zurawski, vol. 93, no.6, June 2005.

Embedded Systems in Industrial Applications

Trends and Challenges



Thank You!

Richard Zurawski
ISA Group, USA