Supervisory Control & Monitoring

Topic - Integrating Industrial Control Systems (I.C.S.)

Teacher - Prof. Elio USAI
elio.usai@unica.it
Dipartimento di Ingegneria Elettrica ed Elettronica
Università di Cagliari

References

K.L.S. SHARMA
Overview of Industrial Process Automation - 2nd edition.
Elsevier, 2017

G. MAGNANI, G. FERRETTI, P. ROCCO
Tecnologie dei sistemi di controllo - 2a edizione
McGraw-Hill Libri Italia, 2007

P. Chiacchio, F. Basile
Tecnologie informatiche per l'automazione
McGraw-Hill,Milano, 2004

N.P. Mahalik
Fieldbus Technology
Springer,Berlin, 2003

Robert Radvanovsky & Jacob Brodsky
Handbook of SCADA/Control Systems Security
CRC Press - Taylor & Francis Group, LLC, 2013

Outline

- C.I.M.
- Control Networks
- System Integration
  - I.M.S
  - P.R.M.
  - M.E.S.
  - E.R.P.
- Security issues in I.C.S.

C.I.M.

Computer **I**ntegrated **M**anufactoring

Production systems integrate by means of structures, methods and technologies that refer to the **I**nformation and **C**ommunication **T**echnology

The system integration allows for the **optimization** both of the production flow

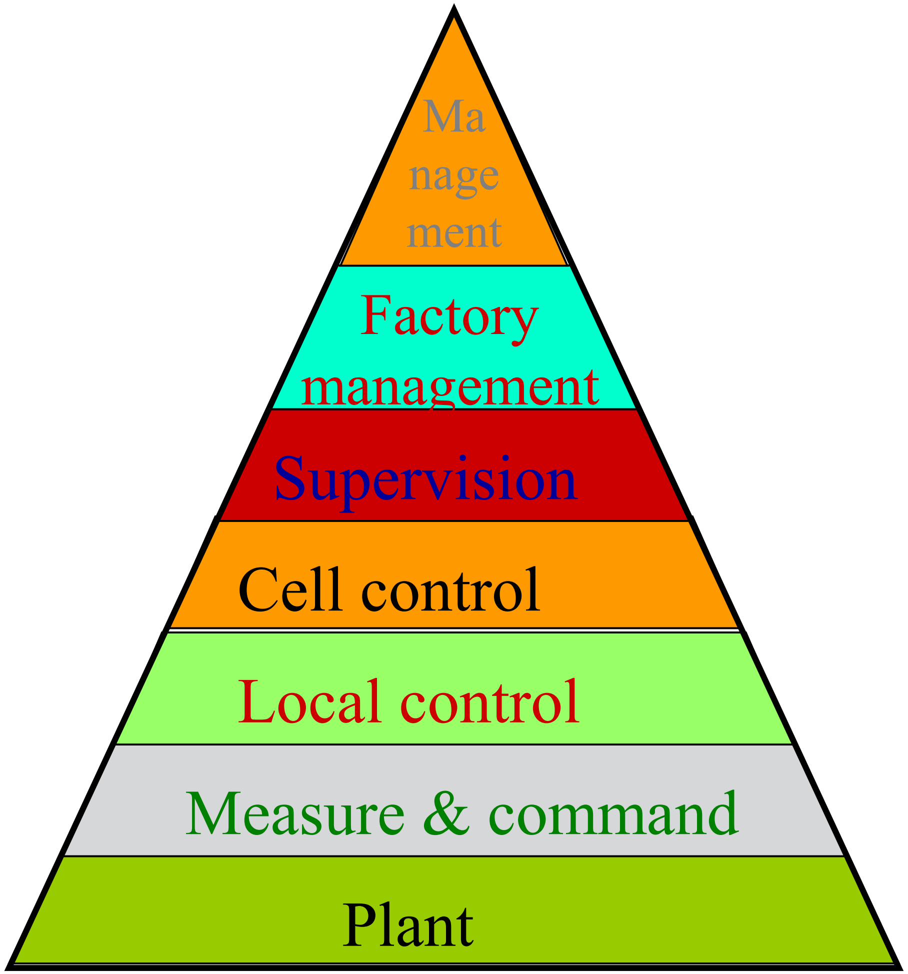
- i.e., how different processes interact each other

and of the process

i.e., how each process is carried on

C.I.M.

C.I.M. pyramid



Management servers

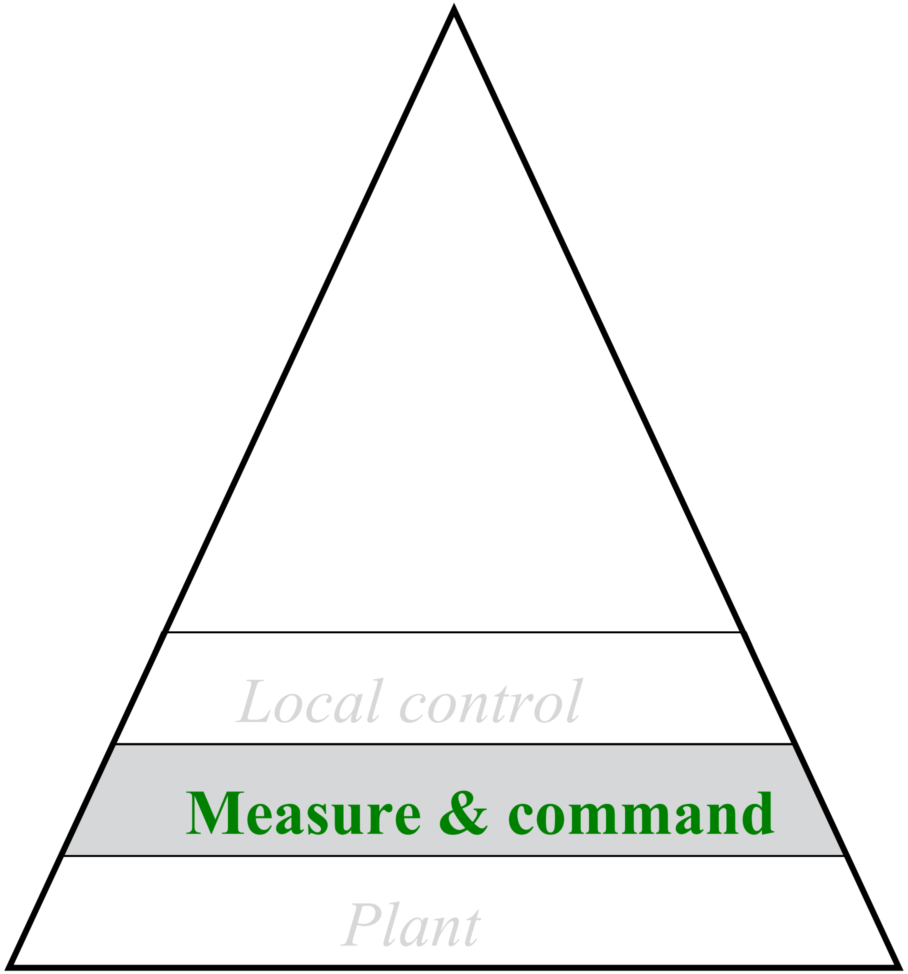
SCADA, DCS

Advanced control, PLC, DCS

PID, PLC, DCS

Sensors & actuators

C.I.M.

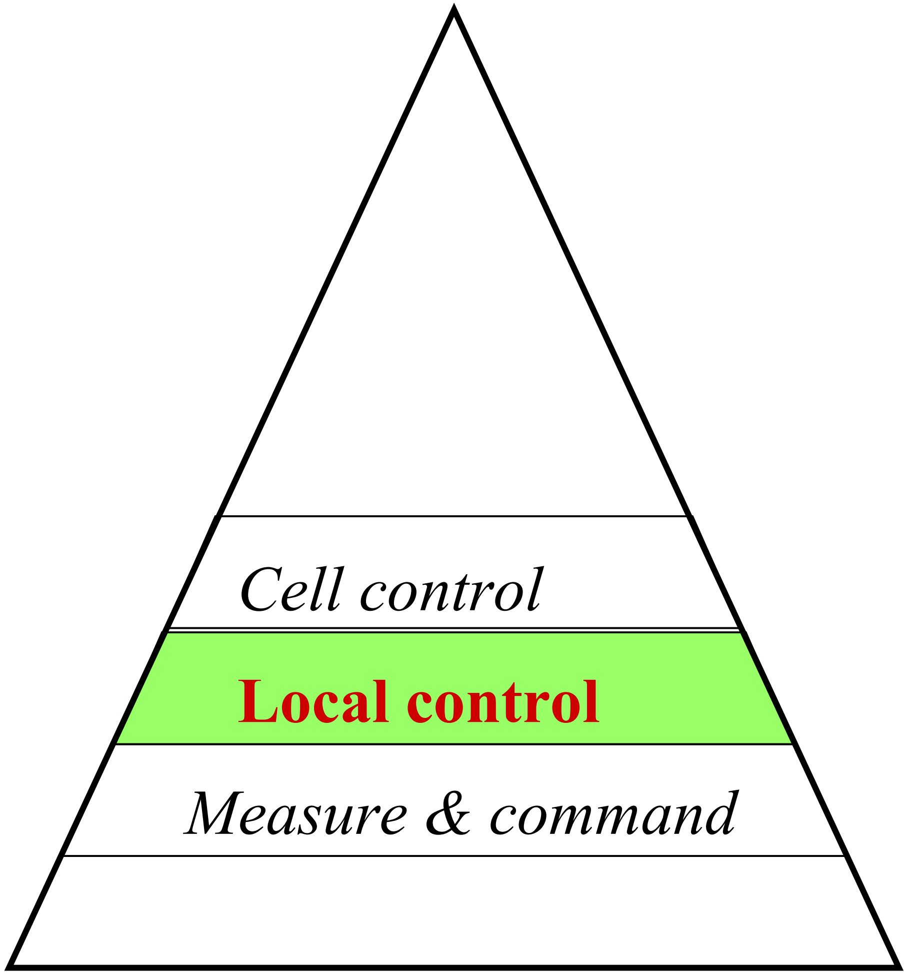


Sensors & actuators

Sensors: provide the plant variables data needed for the safe and efficient management of the plant

Actuators: allow for acting on the manipulated variable to drive the plant according to the desired specifications

C.I.M.



Based on set-points given by the Cell control, the devices and machineries are controlled to guarantee the task fulfillment

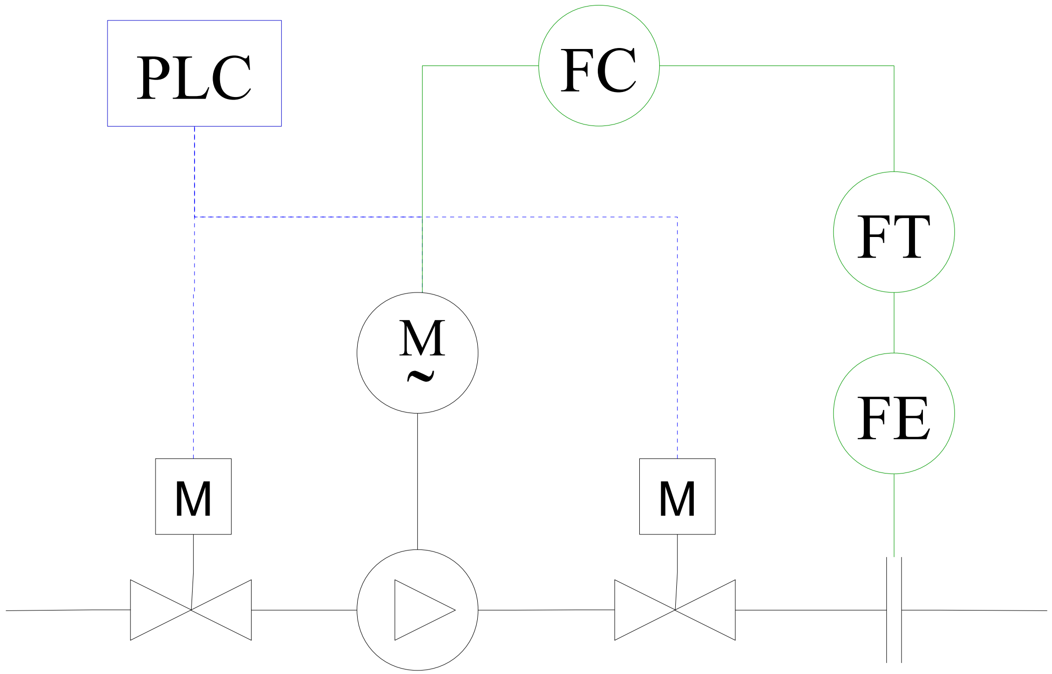
Sequential Control:
Programmable **L**ogic **C**ontroller

Process control:
Proportionale **I**ntegral **D**erivative controller

Example: control of a pump.

C.I.M.

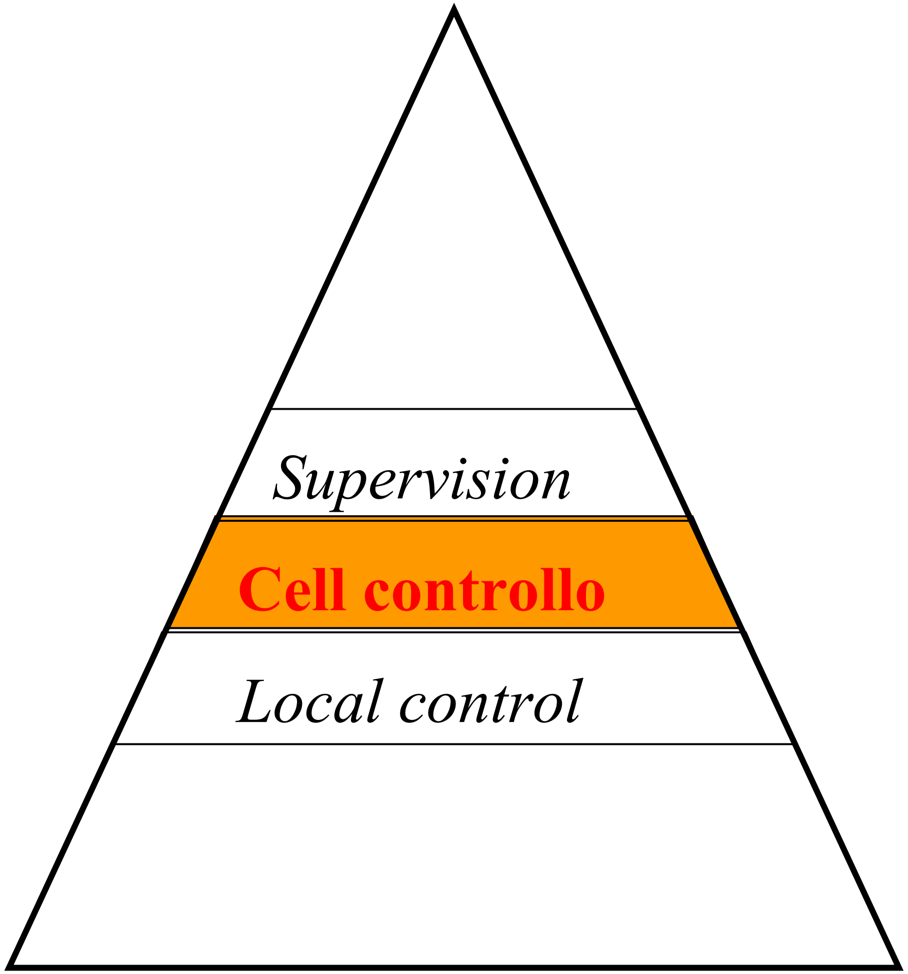
Example: control of a pump.



Sequential Control:
Define the sequence to start and stop the pump

Process control:
Regulate the flow to the desired value

C.I.M.



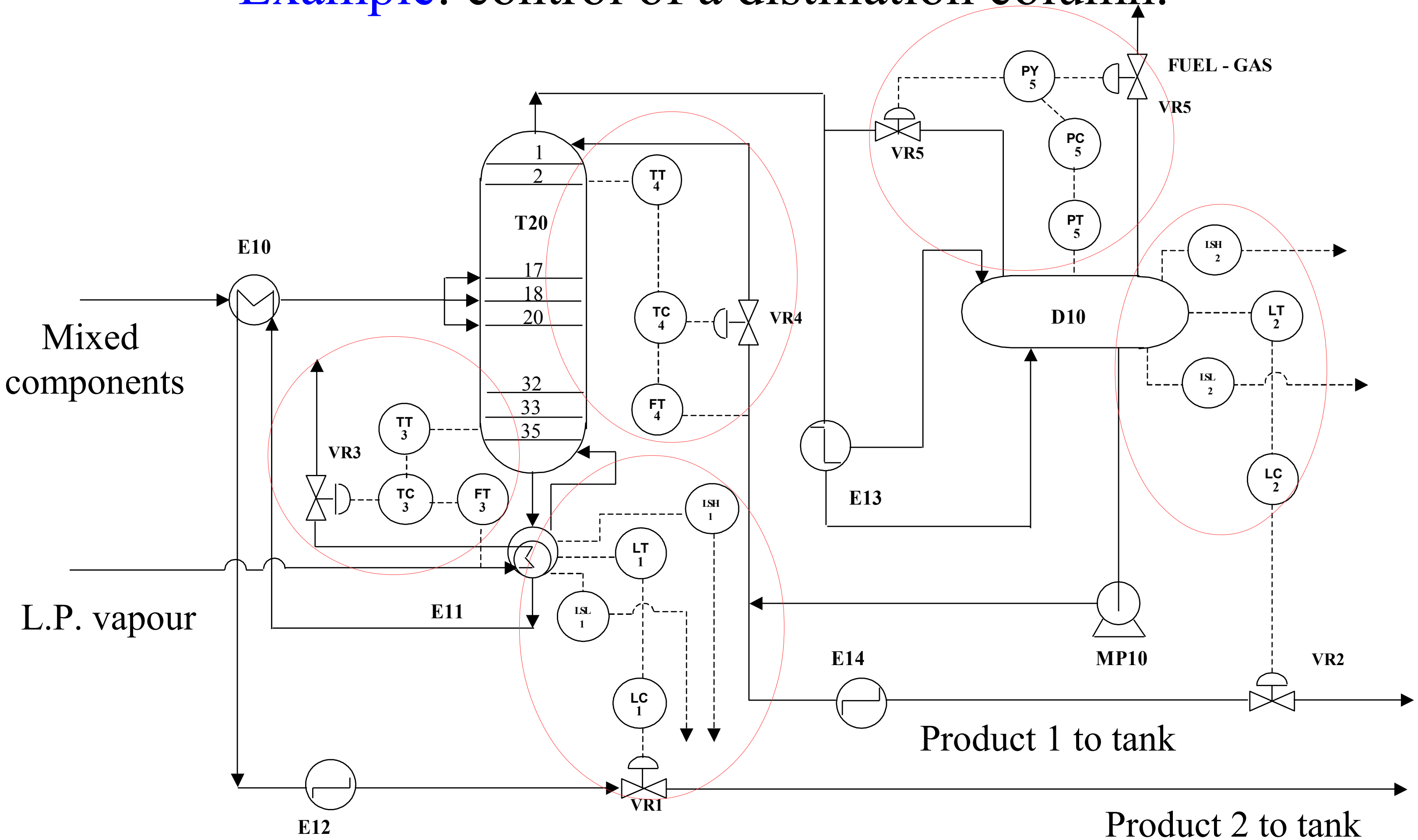
Advanced control, PLC

Taking into account the outputs of the supervisory control, the set points are defined in order to achieve the correct coordiantion of a complex system.

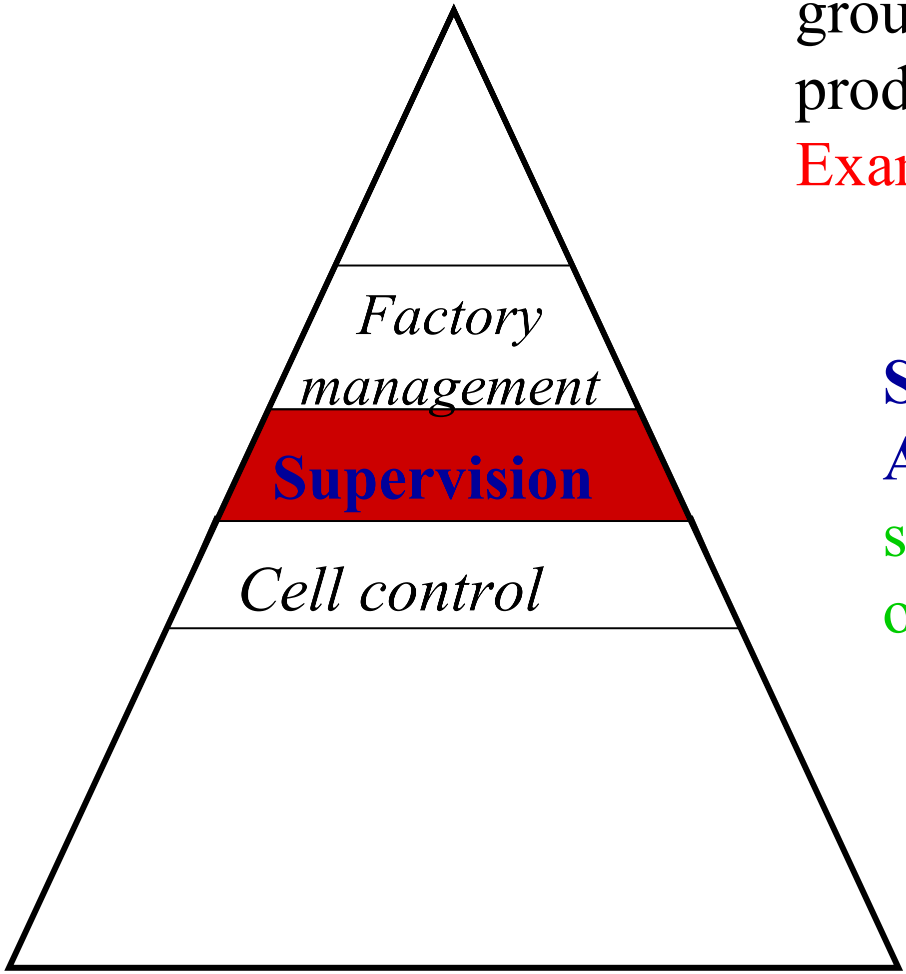
Example: control of a distillation column.

C.I.M.

Example: control of a distillation column.



C.I.M.

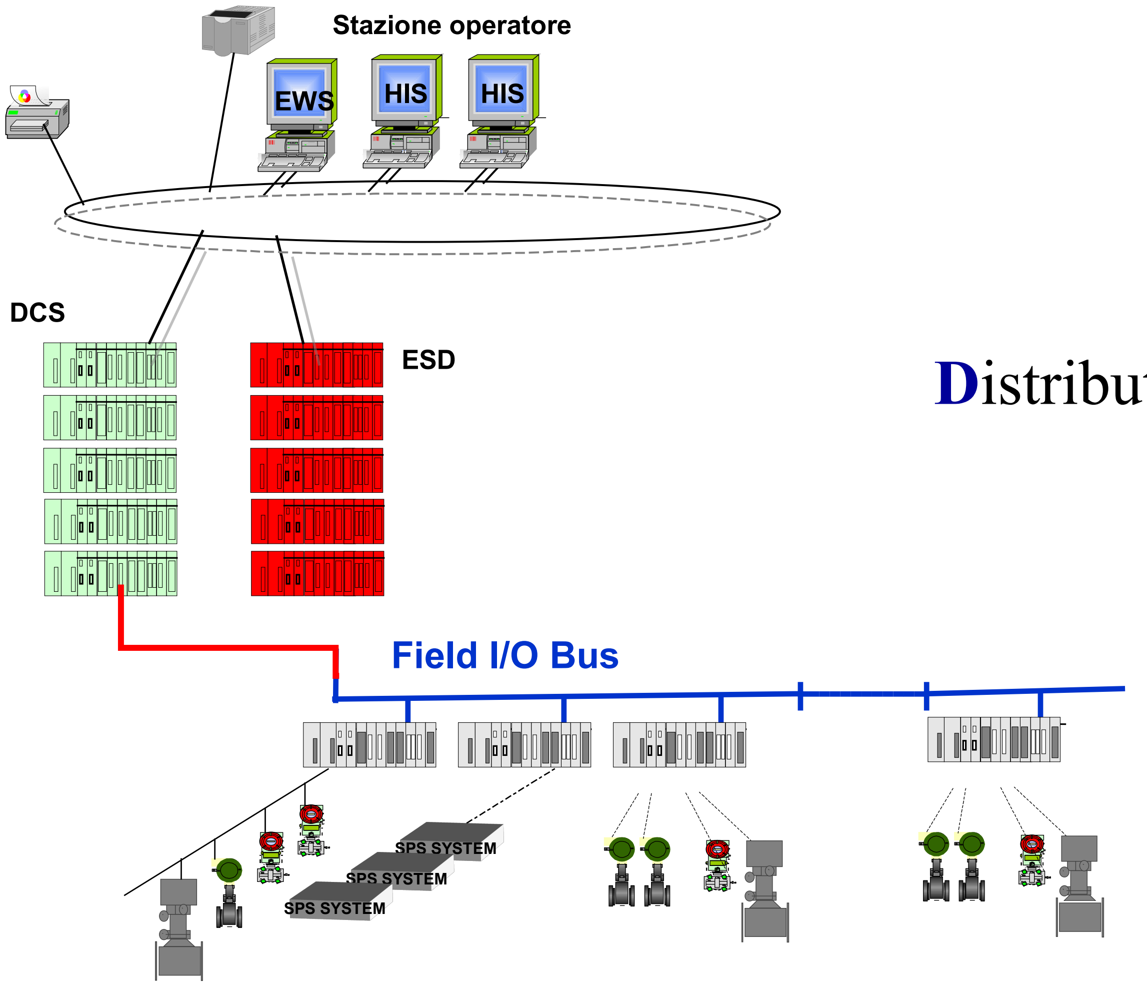


Coordination of several devices and/or group of devices to produce goods and products to sell or for further activities. Example: power plant.

Supervisory **C**ontrol **A**nd **D**ata **A**cquisition: system that acquires, stores and presents data and allows the operator to command

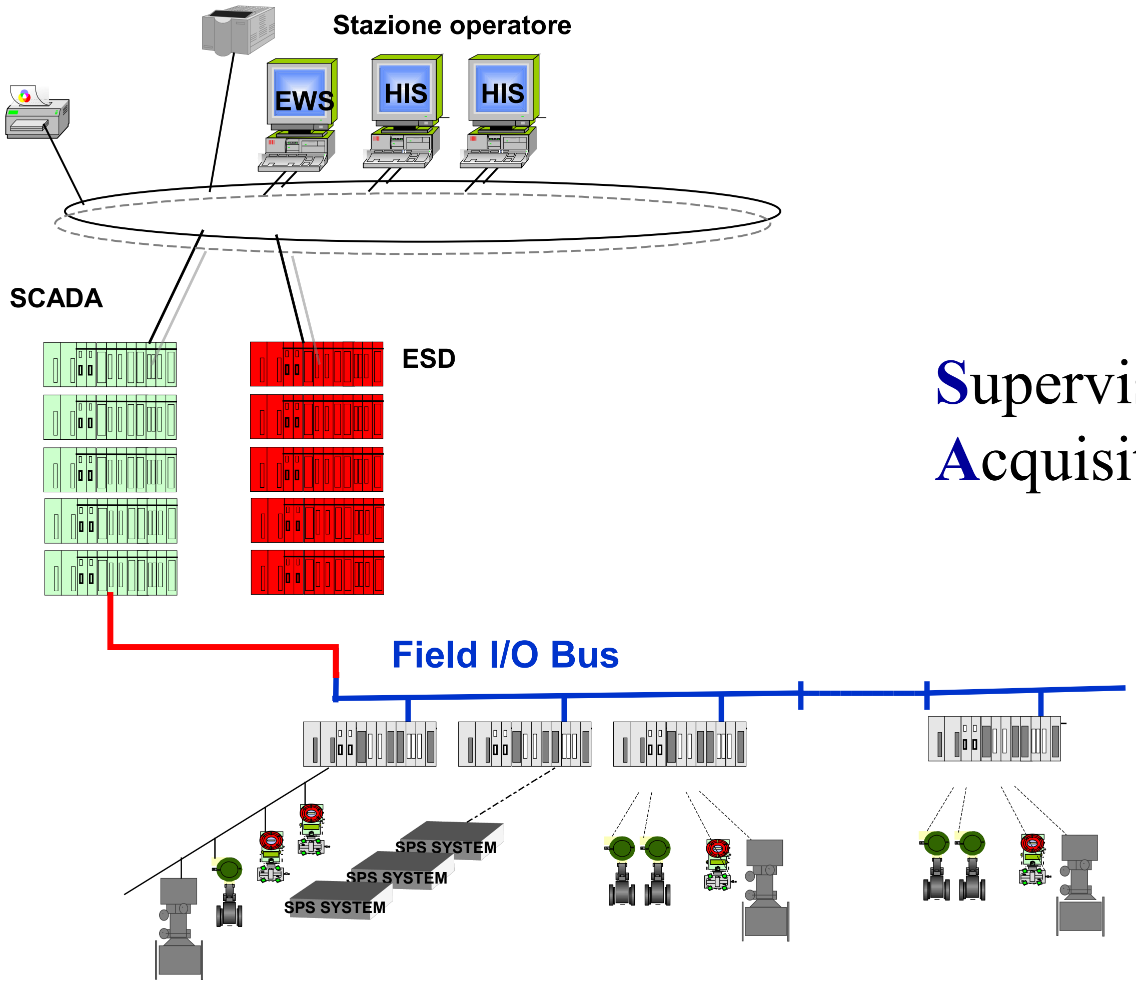
Distributed **C**ontrol **S**ystem: it is an integration of the *SCADA* with decentralise/local controllers

C.I.M.



Distributed **C**ontrol **S**ystem

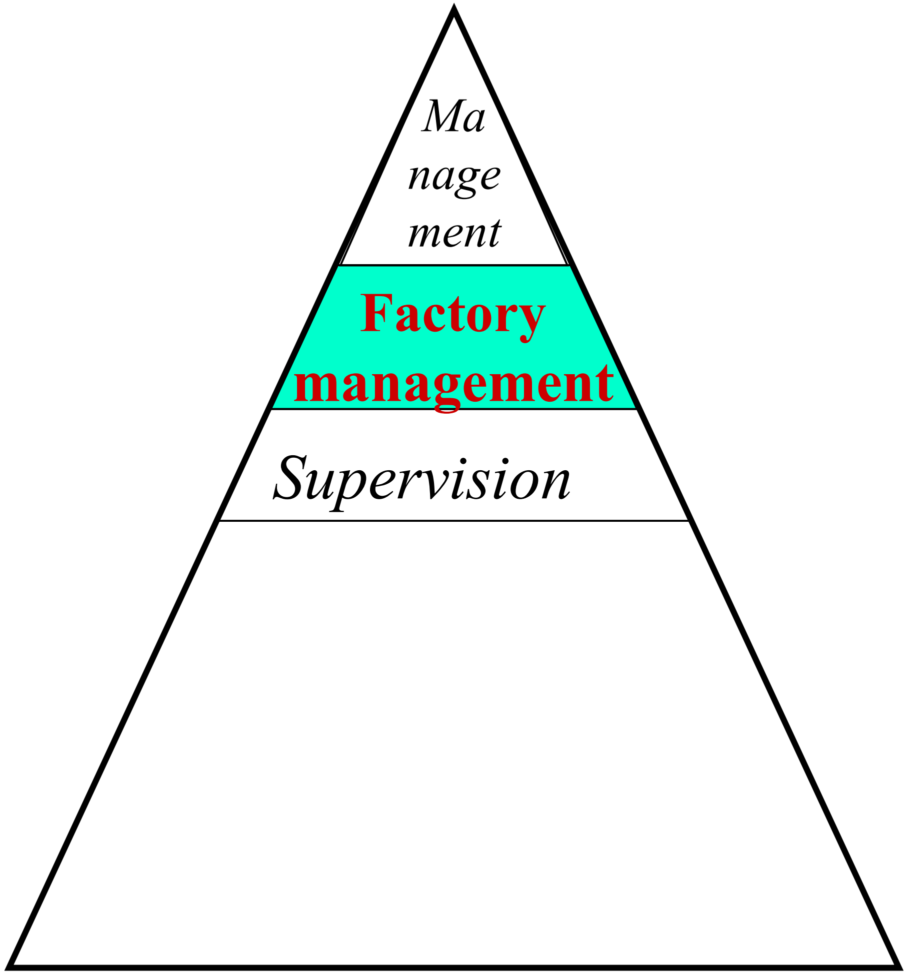
C.I.M.



Supervisory **C**ontrol **A**nd **D**ata **A**cquisition

CONTROLLERS & PLC
(RTU/RCU

C.I.M.



Management server(s)

Coordinates the administrative operations and logistics according to the scheduled plans and the actual production results

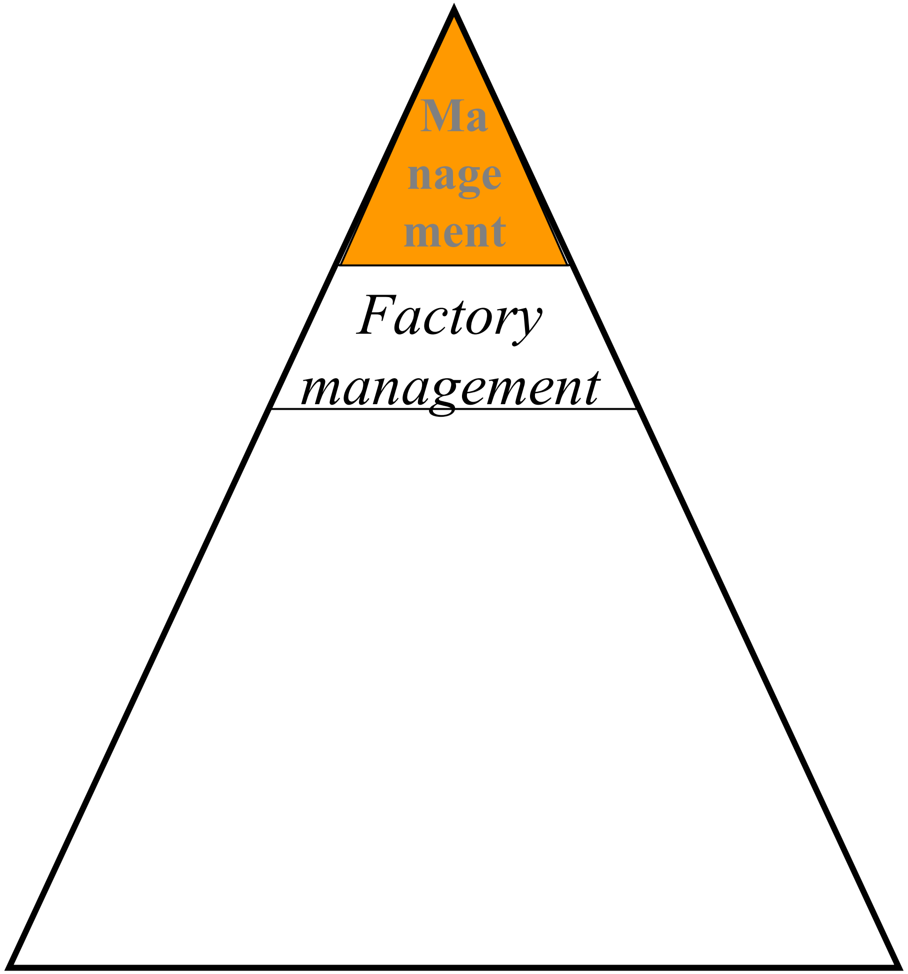
This activity is not completely automated

Manufacturing **E**xecution **S**ystems (*MES*)

Plant **I**nformation **M**anagement **S**ystem (*PIMS*)

Plant **R**esurces **M**anager (PRM)

C.I.M.



This function is devoted to define the company policies, finding opportunity and threats related to the market and to the production system.

It uses the resuming data from the factory management system to carry on a technical-economic analysis and to define the company budget.

Just few management programs available

C.I.M.

The C.I.M. system needs devices which are able to

acquire the data - sensors e trasducers

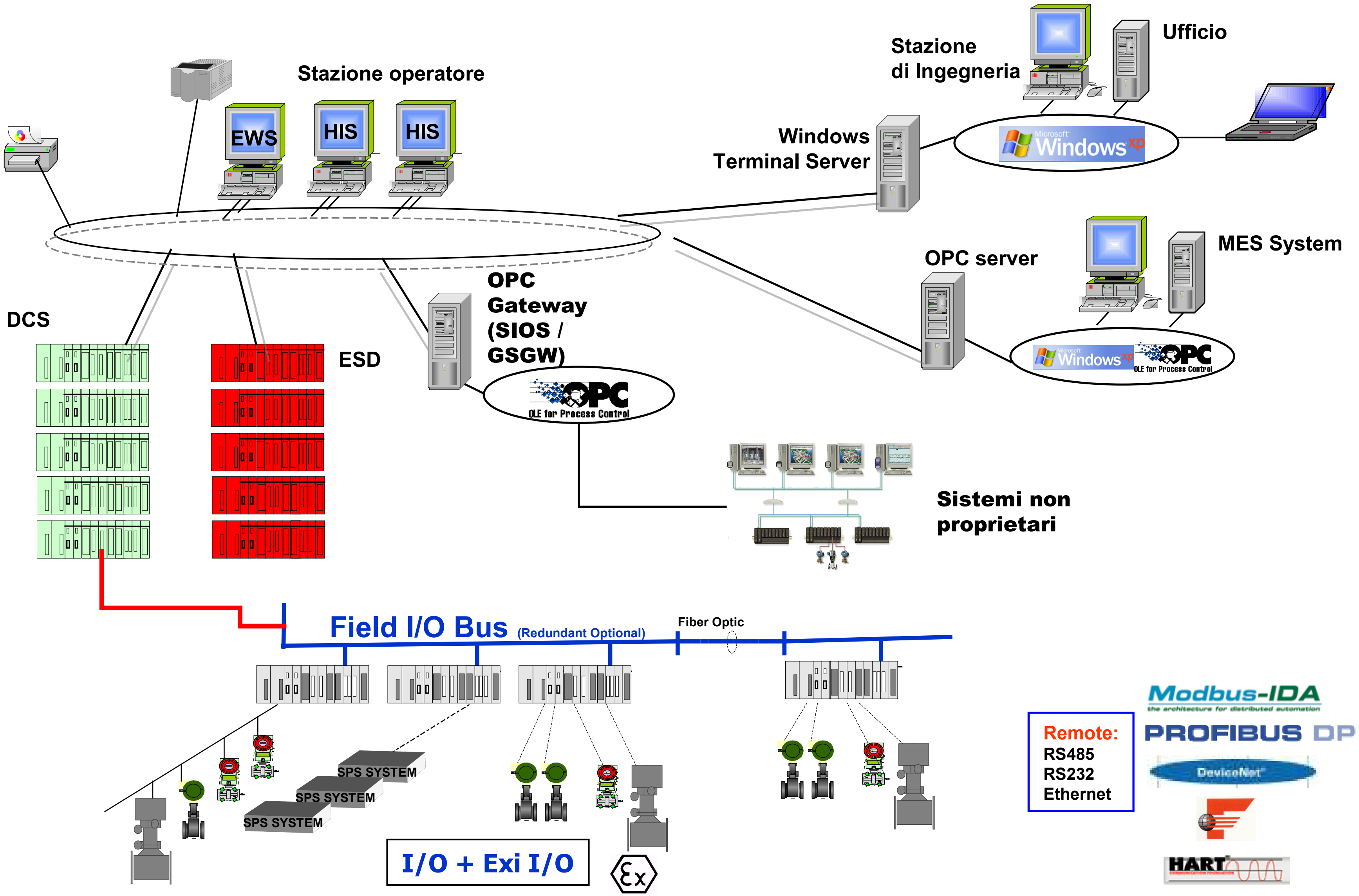
data coding - A/D e D/A converters, I/O boards

data transmission - fieldbus, ethernet, LAN, GSM

data elaboration - PID, PLC, DCS, advanced controllers

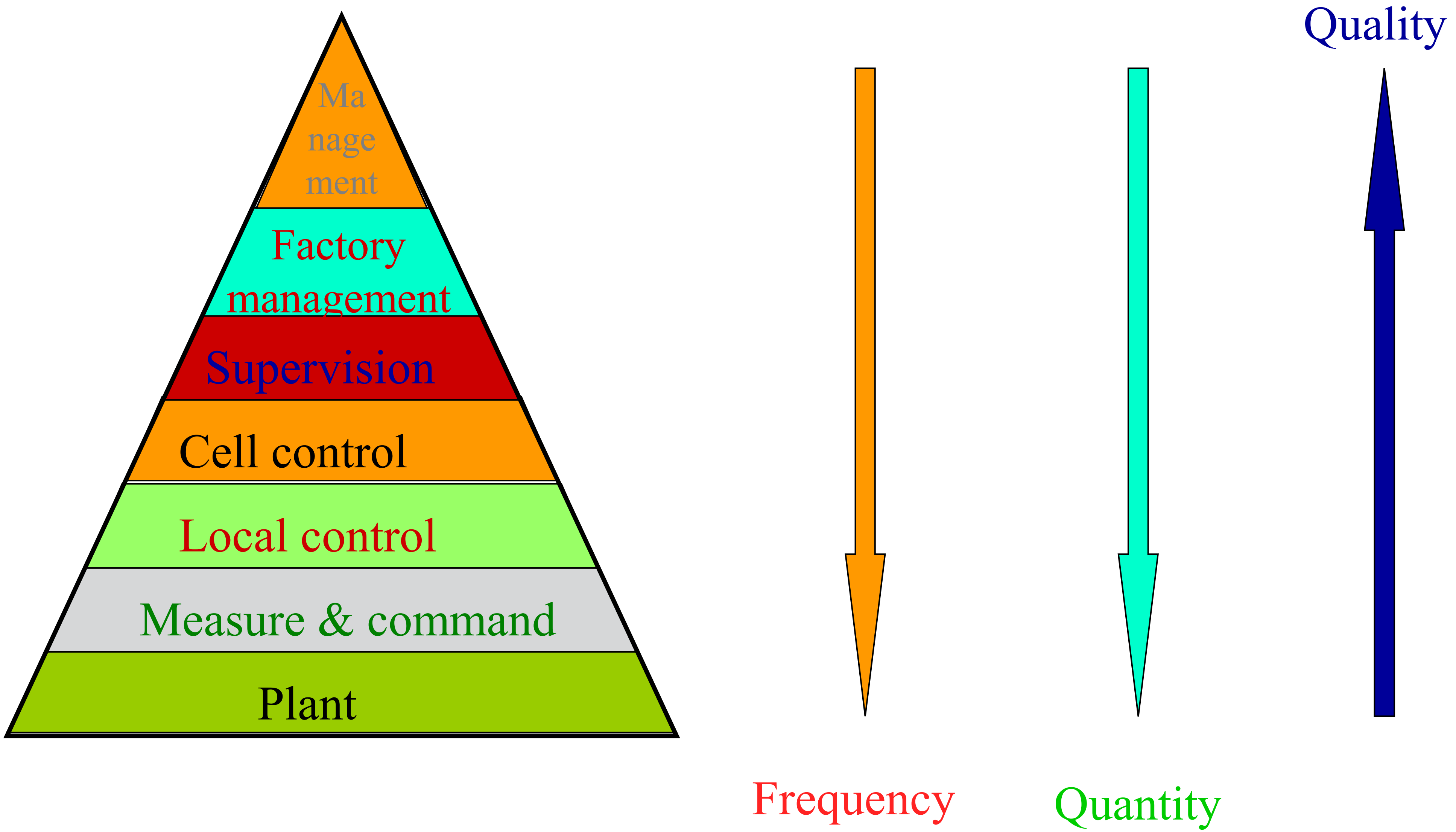
data management and presentation - SCADA, DCS, MES, PIMS, PRM

C.I.M.

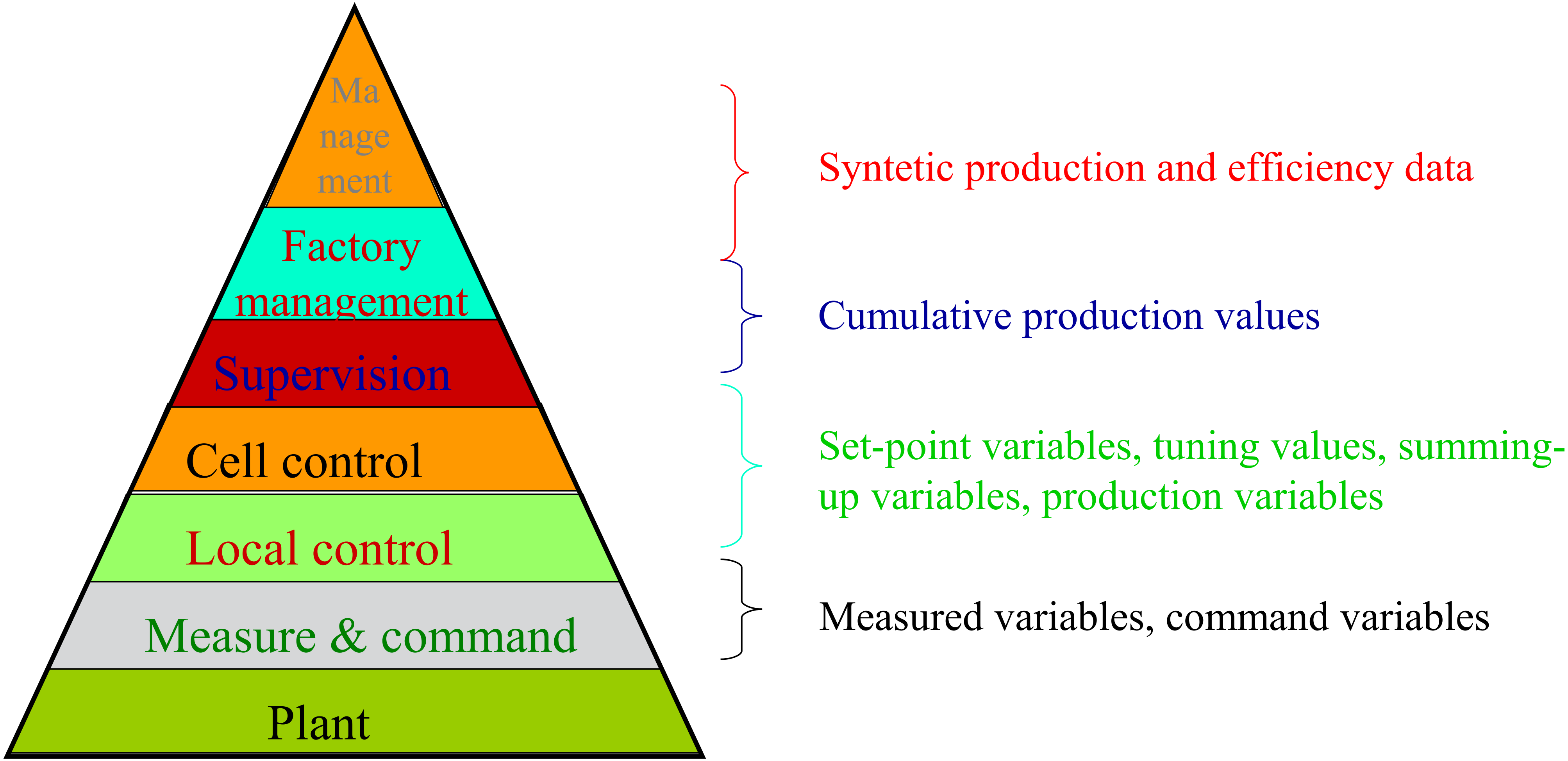


Systems for Supervision and Control - Integrating ICS

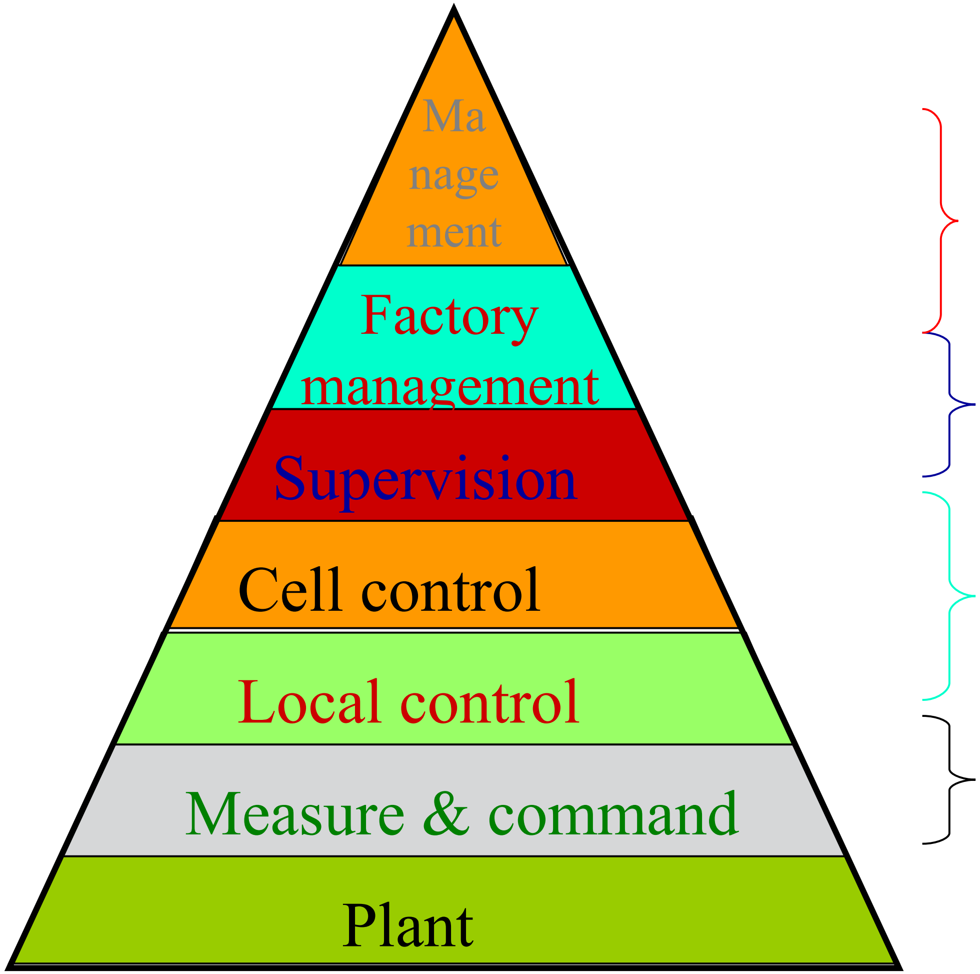
Networks


Ma
nage
ment
Factory
management
Supervision
Cell control
Local control
Measure & command
Plant
Quality
Frequency
Quantity

Networks


Ma
nage
ment
Factory
management
Supervision
Cell control
Local control
Measure & command
Plant
Syntetic production and efficiency data
Cumulative production values
Set-point variables, tuning values, summing-up variables, production variables
Measured variables, command variables

Networks



Syntetic data with daily update

Not many simple data with daily update

Not so many simple data, possibly with a certain refresh time interval

Many and frequent elementary data, possibly with a certain relatively short refresh time interval

Networks

I.S.O. - O.S.I. Model

International **S**tandard **O**rganisation

Open **S**ystem **I**nterconnection

It is a reference model for communication networks

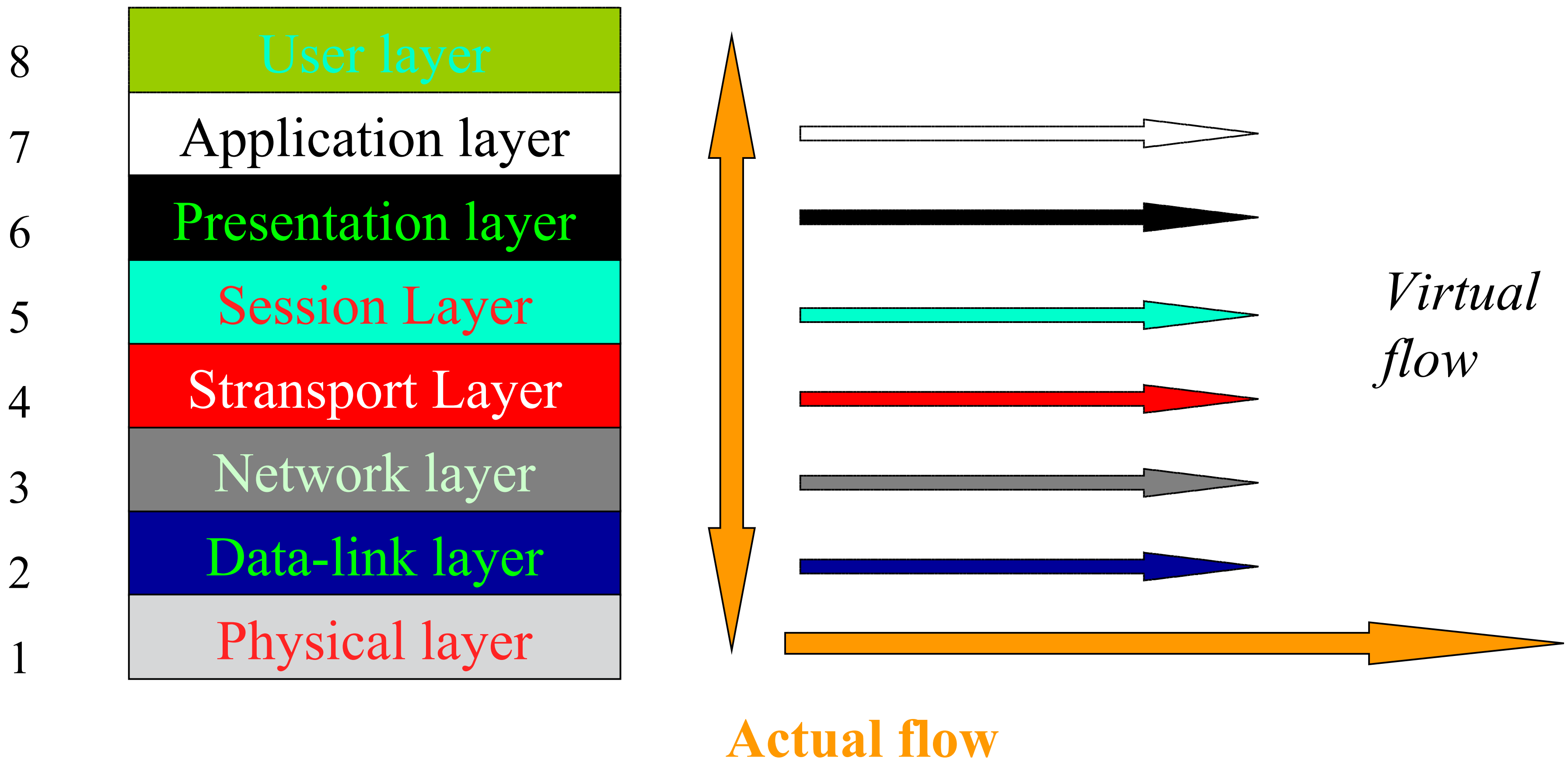
It is a gerarchical model with layers

Phisically, each layer is connected only with its upstream and downstream layers

Functionally, each layer implemented in a communication device is connected to the same layer in the other connected devices

Networks

I.S.O. - O.S.I. Model



Networks

I.S.O. - O.S.I. Model

User
Application
Presentation
Session
Trasport
Network
Data link
Physical layer

Physical Layer

It is constituted by the devices and structures that guarantee the device connections: **channel**

- Cupper cables
- Optical fiber cables
- Electromagnetic waves

Bit coding

Network topology and type

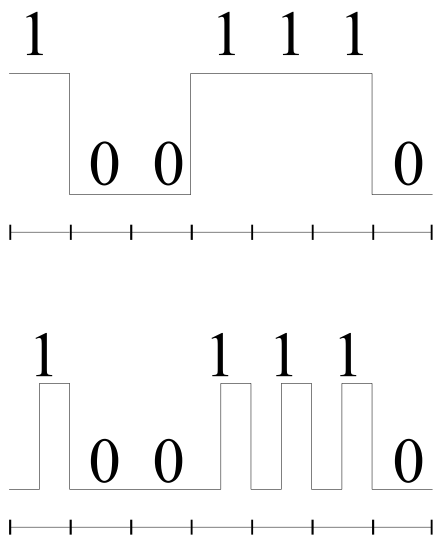
Networks

I.S.O. - O.S.I. Model

User
Application
Presentation
Session
Trasport
Network
Data link
Physical layer

Physical Layer

Bit coding



Networks

I.S.O. - O.S.I. Model

User
Application
Presentation
Session
Trasport
Network
Data-link layer
Physical

Data-Link Layer

Defines the structure of the frame: **frame coding**

Defines the rules to allow the devices to access the network: **network management**

Networks

I.S.O. - O.S.I. Model

- *User*
- *Application*
- *Presentation*
- *Session*
- *Trasport*
- *Network*
- **Data-link layer**
- *Physical*

Data-Link Layer

frame coding

<table>
<tr><td colspan="2">Init</td><td colspan="3">recipient</td><td colspan="3">sender</td><td colspan="9">body</td><td colspan="2">end</td><td>ck</td></tr>
<tr><td>1</td><td>1</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>0</td><td>0</td><td>1</td></tr>
</table>

The structure of the frame and the rules to access the network depend on the network protocol

Networks

I.S.O. - O.S.I. Model

User
Application
Presentation
Session
Trasport
Network layer
Data-link
Physical

Network Layer

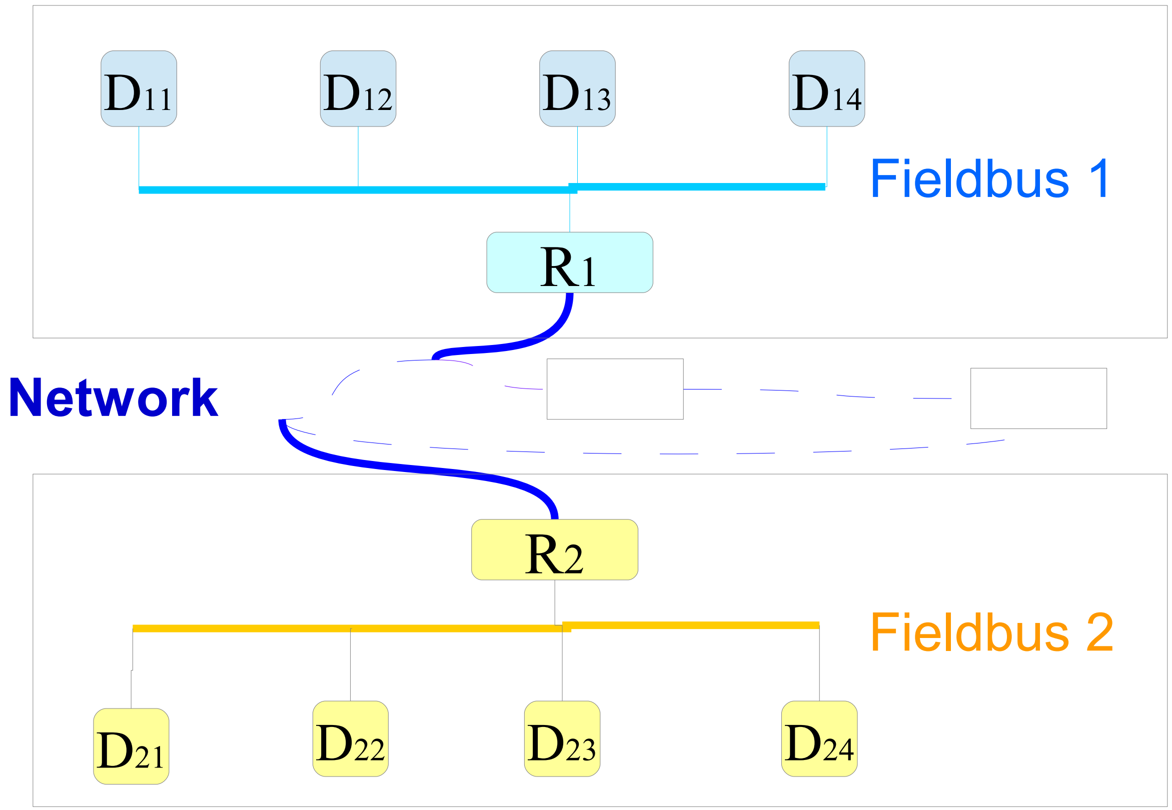
Allow for the data transfer between devices not connected to the same physical network: **data addressing and routing**

Networks

I.S.O. - O.S.I. Model

User
Application
Presentation
Session
Trasport
Network layer
Data-link
Physical

Network Layer



Networks

I.S.O. - O.S.I. Model

User
Application
Presentation
Session
Trasport layer
Network
Data-link
Physical

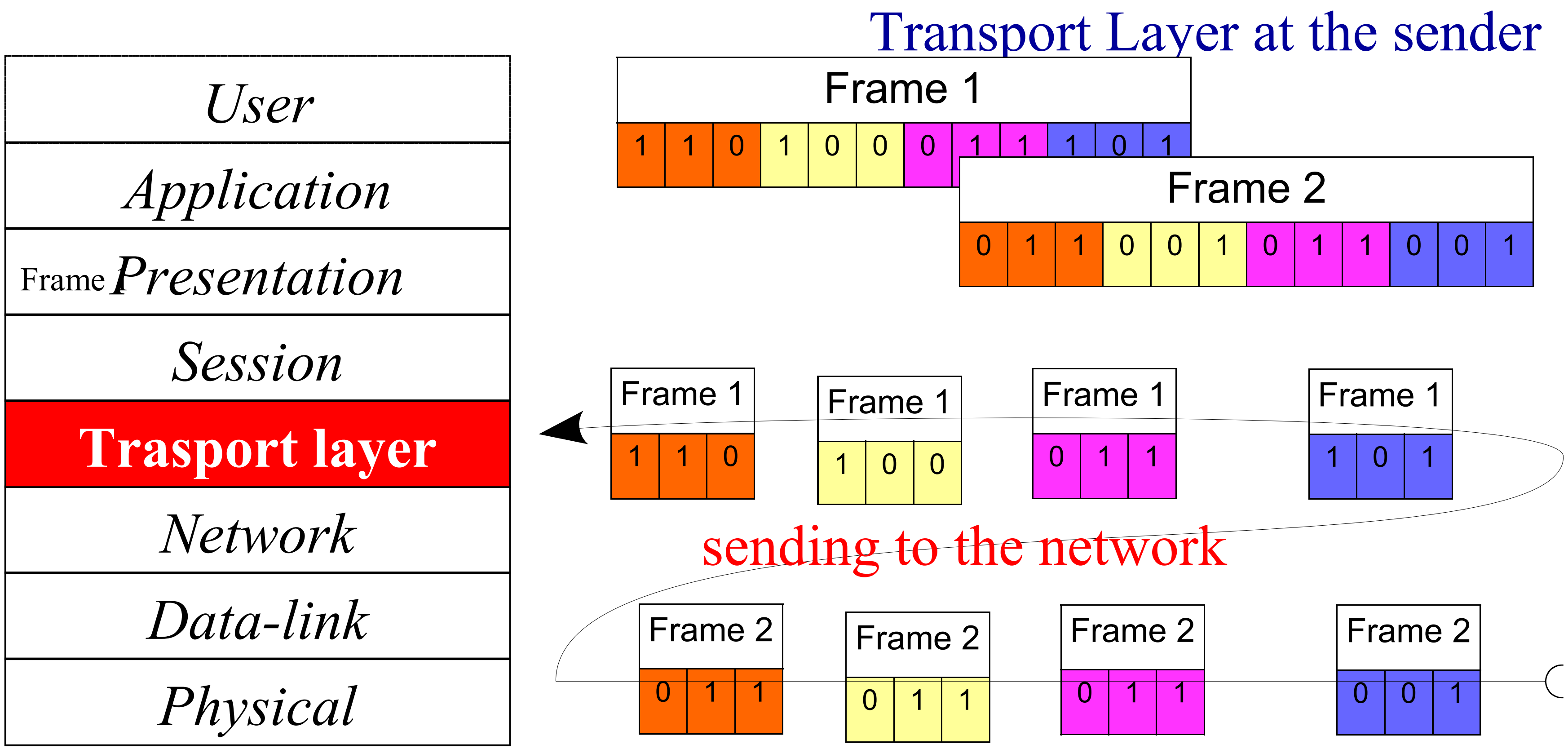
Transport Layer

Assures that the frame is correctly sent and received:

- **the frame is cutted into packets which are sent individually and the frame is reconstructed at the receiver**
- **Router congestion managing**

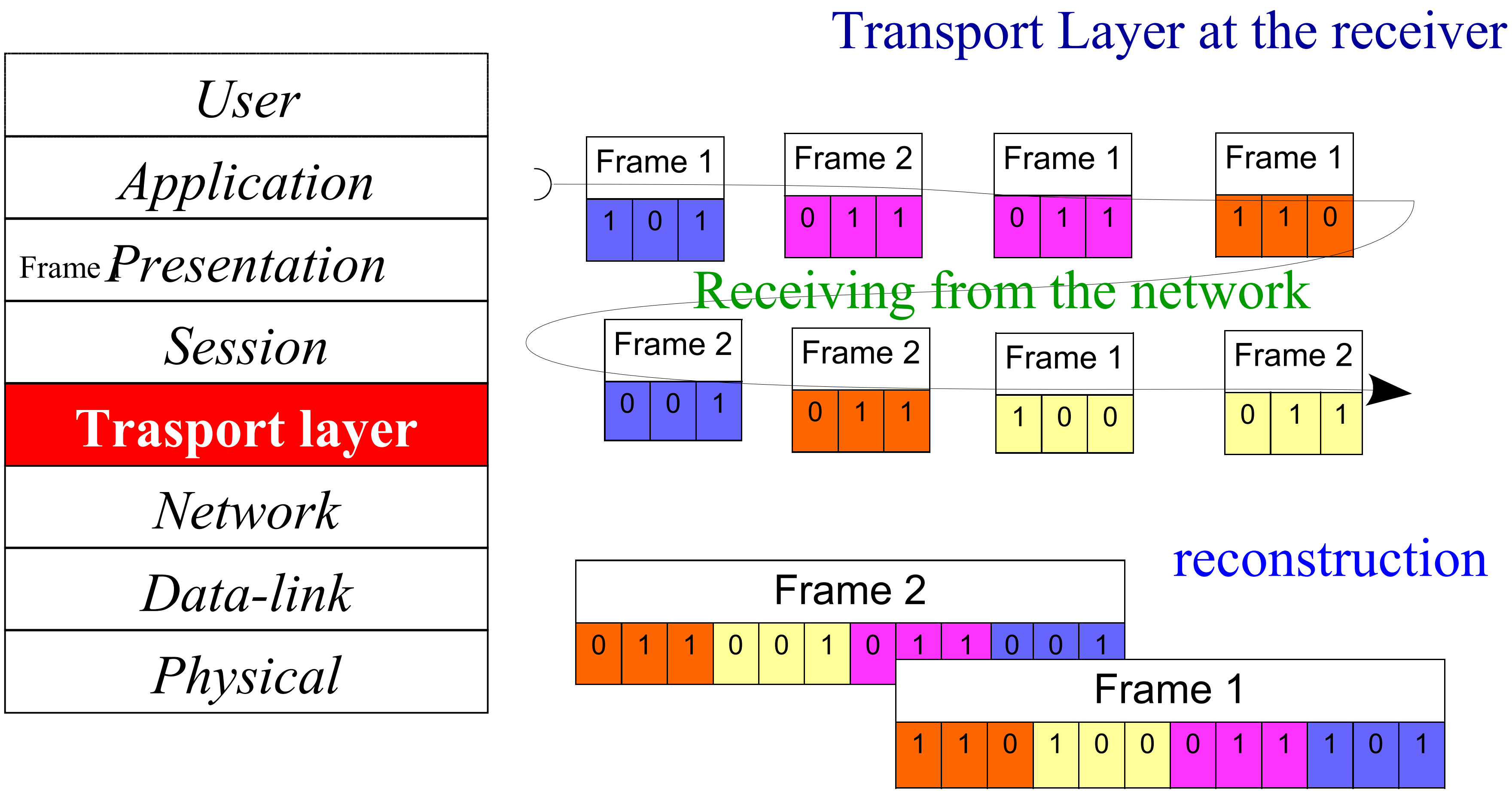
Networks

I.S.O. - O.S.I. Model



Networks

I.S.O. - O.S.I. Model



Networks

I.S.O. - O.S.I. Model

User
Application
Presentation
Session layer
Trasport
Network
Data-link
Physical

Session Layer

Allows two devices to communicate in a synchronized way:

- **remote connection management**
- **recovering of packet losses in the communication**

Networks

I.S.O. - O.S.I. Model

User
Application
Presentation layer
Session
Trasport
Network
Data-link
Physical

Presentation Layer

Allows for associating the correct information to each frame:

recontruction of the received information (e.g., cryptography)

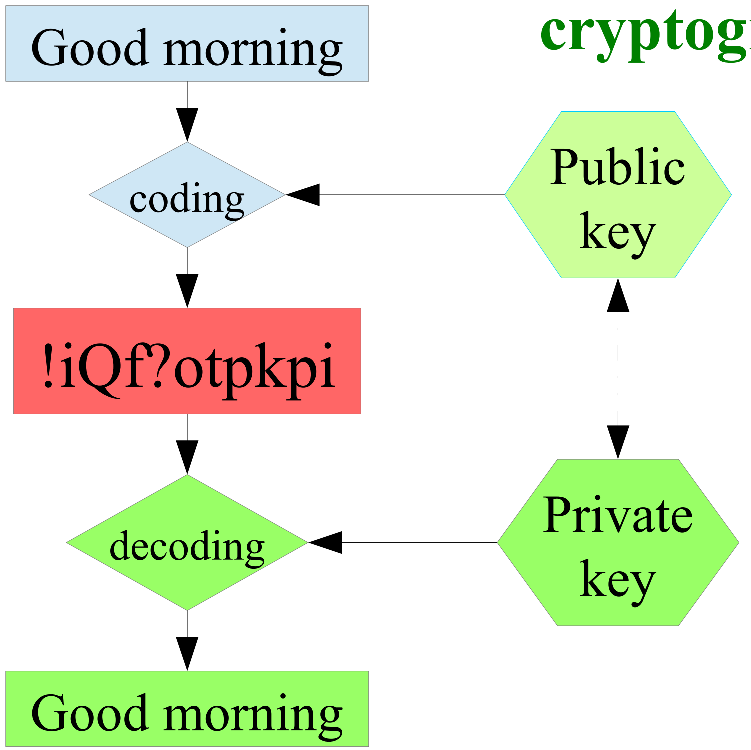
Networks

I.S.O. - O.S.I. Model

User
Application
Presentation layer
Session
Trasport
Network
Data-link
Physical

Presentation Layer

cryptography



Networks

I.S.O. - O.S.I. Model

User
Application layer
Presentation
Session
Trasport
Network
Data-link
Physical

Application Layer

Allows the applications to use the data in a proper way: **application interface**

e.g.,

- Mail clients
- File transfer applications

Networks

I.S.O. - O.S.I. Model

User layer
Application
Presentation
Session
Trasport
Network
Data-link
Physical

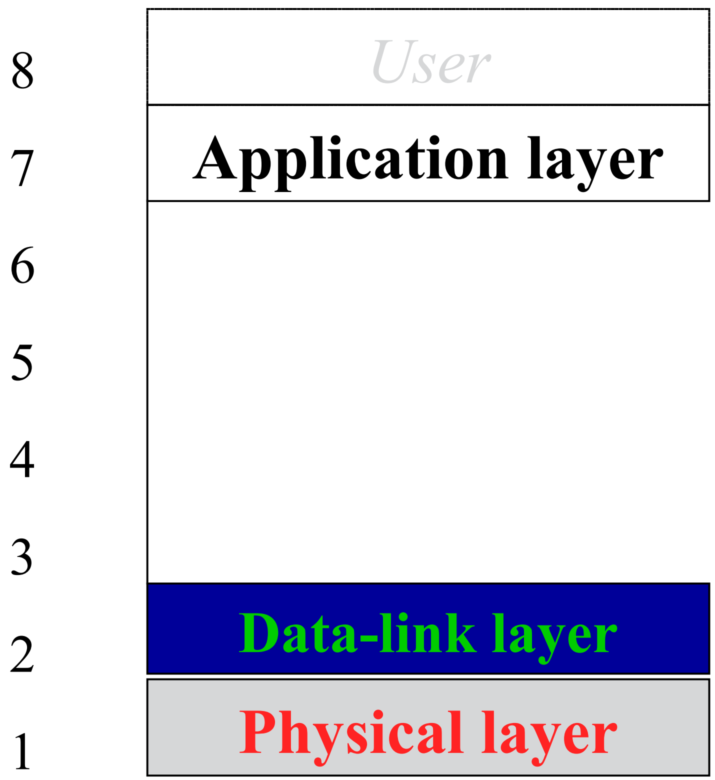
User Layer

Allows the data to be well recognised and understood by the user: **man/machine interface**

This layer is not fully classified and not usually present, at least formally

Networks

Fieldbus - L.A.N.



the $3^{rd} \div 6^{th}$ layers are usually not implemented: each node is connected either physically or logically to the same network.

The 8^{th} (optional) is rarely implemented: just the nodes with the presence of the operator

The 1^{st} e 2^{nd} layers are the most critical for the control purposes

Networks

Physical channel: **cupper cables**

Twisted pair: a pair of twisted isolated cupper strings allow an electrical signal to be trasmitted between/among different devices. Possibly a metallic shield protect the cable from electromagnetic disturbances.

Standard EIA: RS 232, RS 232C, **RS 485**, RS 422

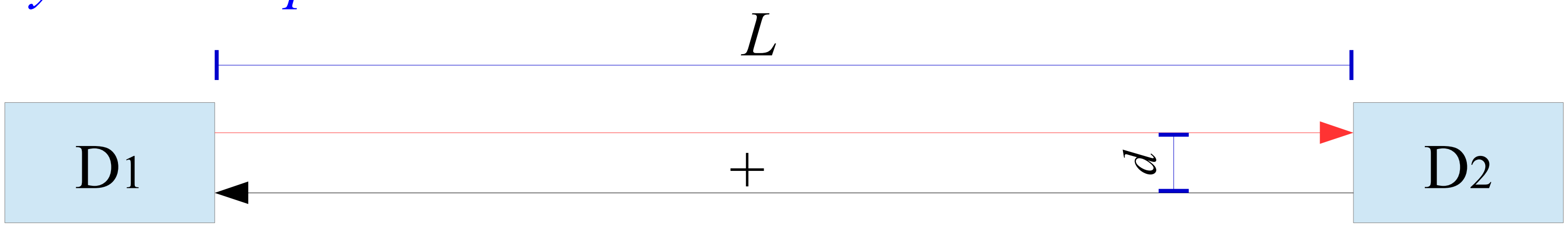
Standards are mostly based on voltage differences between two cables with respect to a reference node/cable: less sensitivity to voltage drops due to the cable lenght

Higher voltages allow for longer cables, i.e., a greater distance between communication devices

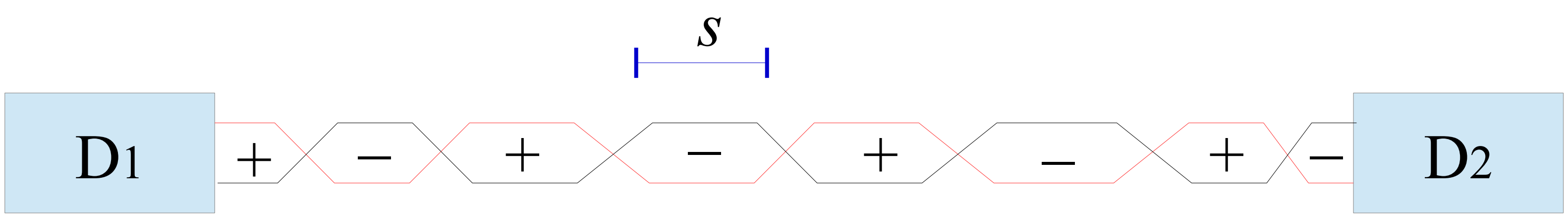
Networks

Physical channel: **cupper cables**

Why Twisted pair?



$$A = L \cdot d$$

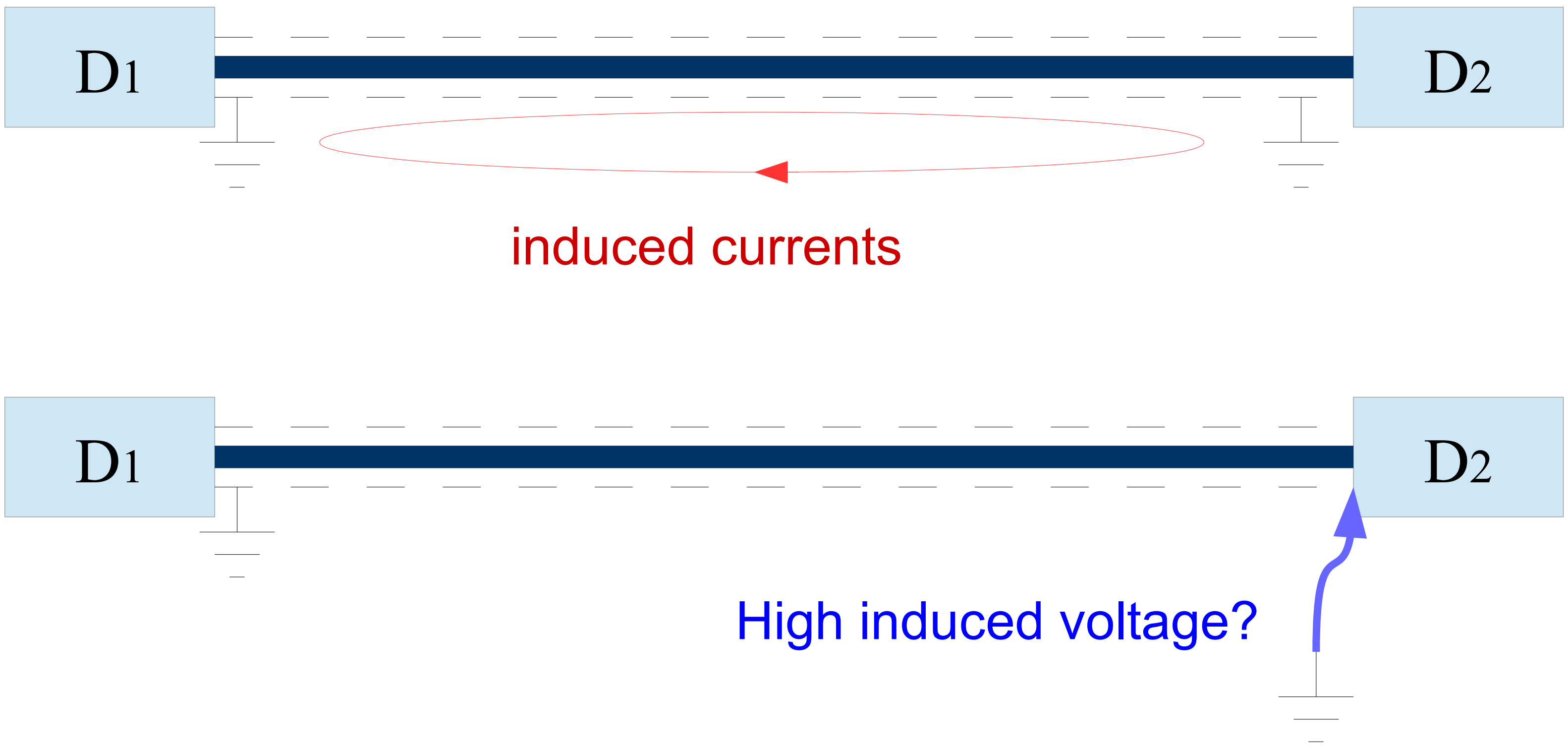


$$A \leq s \cdot d$$

Networks

Physical channel: **cupper cables**

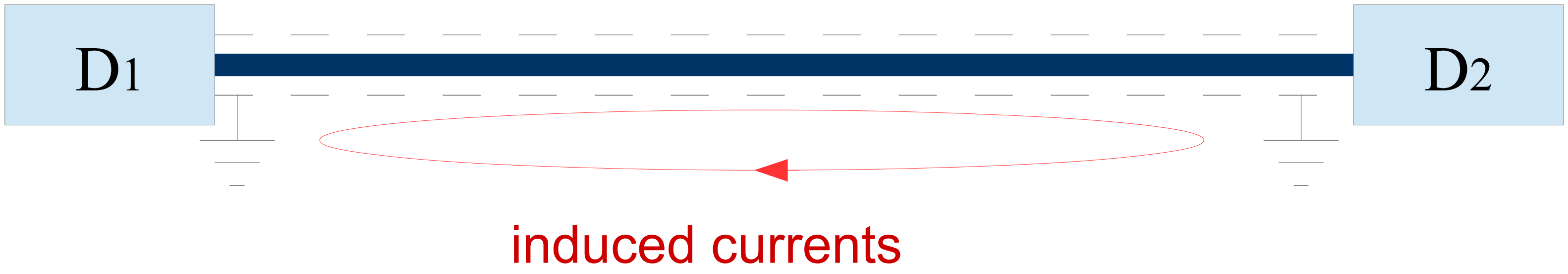
Overvoltages and/or parasitic currents on the shield?

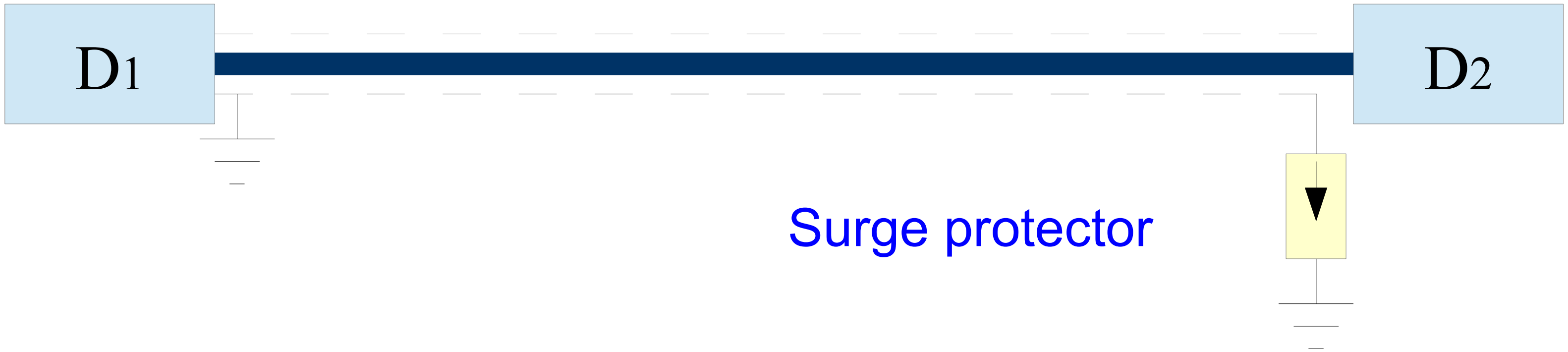


Networks

Physical channel: **cupper cables**

Overvoltages and/or parasitic currents on the shield?





Networks

Physical channel: **guided waves**

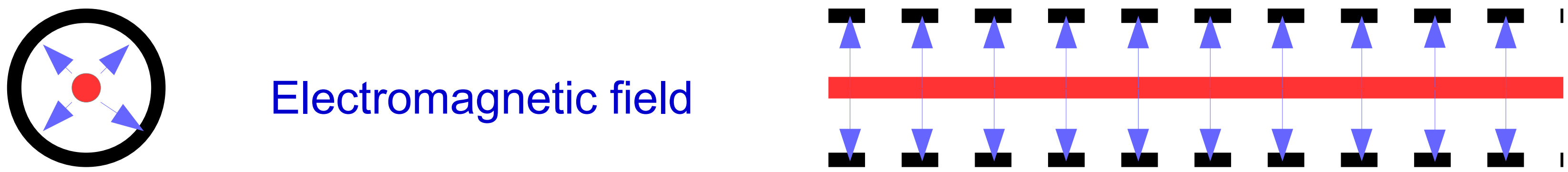
Coaxial cable: **Thin** type for relatively long connections with lot of nodes; **Thick** type for short connection between nearby nodes.

Optical fiber: Modern optical communication networks are equiped with optical splitters, amplifiers and joints such that, usually, the opto-electronic conversion is present at the end side only. It allows for long distance transissions but it is costly and not easy to expand.

Networks

Physical channel: **guided waves**

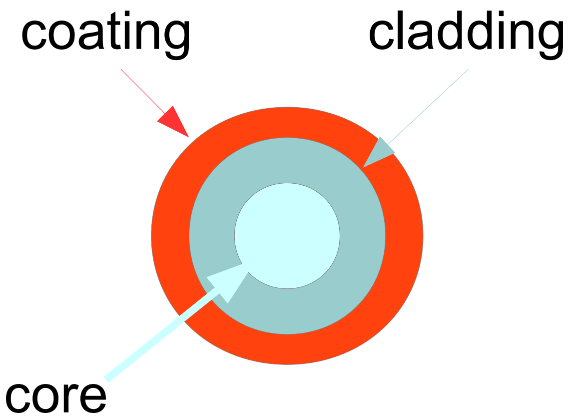
Coaxial cable: it is constitued by two cupper concentric string and tube. The electromagnetic field is confine into the cilindrical gap

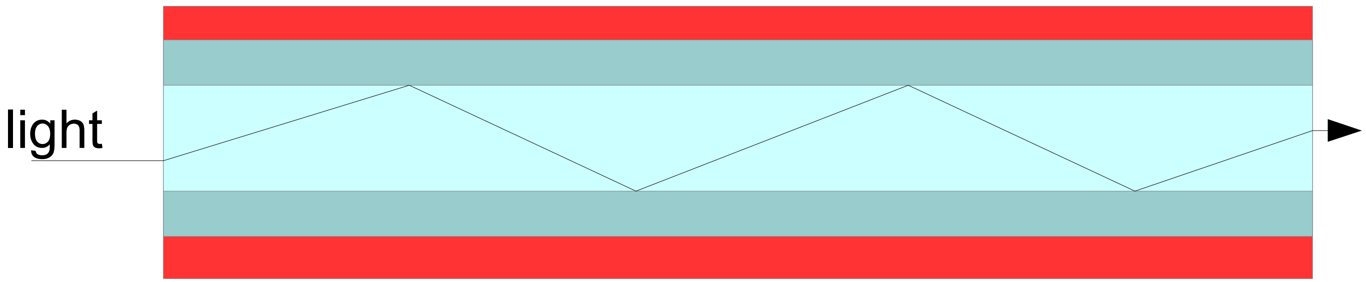


Networks

Physical channel: **guided waves**

Optical fiber: the light is confined inside a glass wave guide because of different refraction index between core and cladding.





Networks

Physical channel: **elettromagnetic waves**

Wireless transmission at prescribed frequencies

It is difficult to guarantee the connection in industrial environment beacuse of the presence of iron structures and electromagnetic fields

Possibility of electircal interferences and loss of connection

It is simple to implement in existing structures and sites

Various protocols available: Bluetooth, ZigBee, Wi-Fi, etc

Networks

Criteria for choosing the physical channel

distance between nodes – voltage drops

environment – electromagnetic compatibility and disturbances

amount of data to transmit - bandwidth

expansion perspectives – is it easy to connect a new node?

Most used: twisted pair, standard RS 485
Tendency: optical fiber, wireless

Networks

Topology

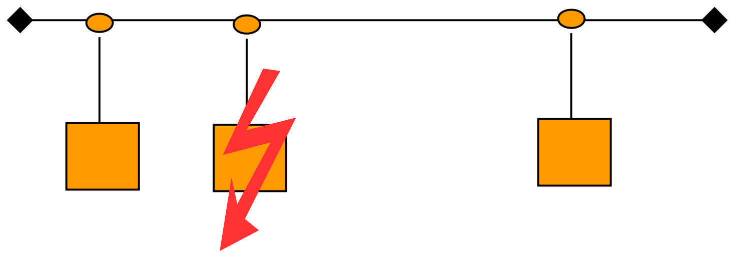
Bus

Each node is connected to the bus by means of a short drop cable. At the bus ends there are impedence adaptors such that the electromagnetic wave reflection is lavoided, or limited at least.

- New nodes are easily connected
- Simple installation
- Full reliability for faults at nodes and limited problems at the first fault
- Limited lenght of the bus

Networks

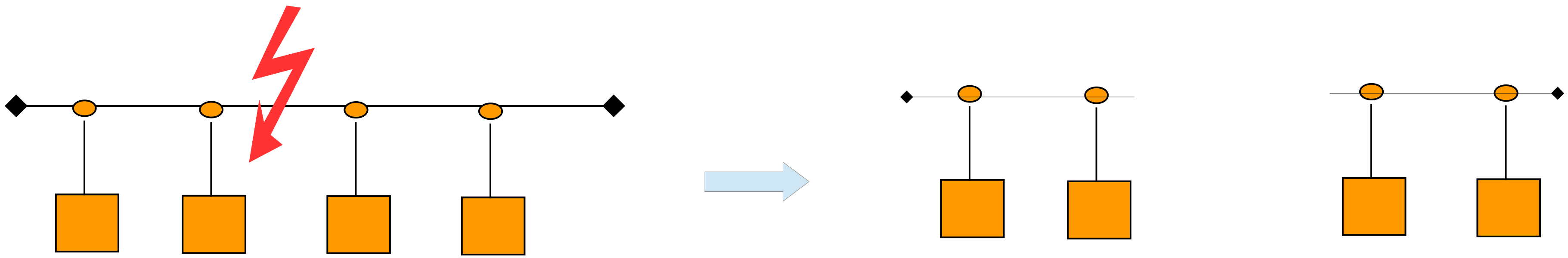
Topology



Bus

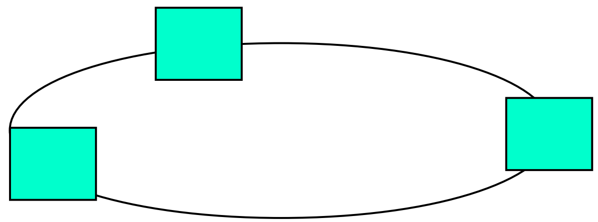
Each node is connected to the bus by means of a short drop cable. At the bus ends there are impedence adaptors such that the electromagnetic wave reflection is lavoided, or limited at least.

- Full reliability for faults at nodes and limited problems at the first fault



Networks

Topology



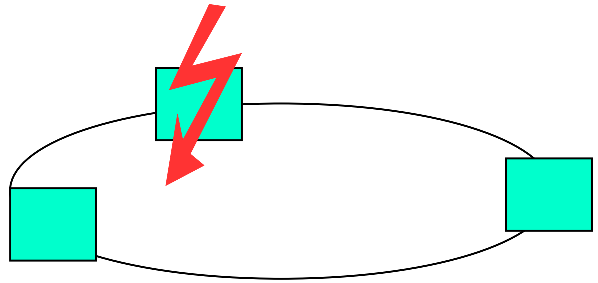
Daisy- chain ring

The node are connected by a bus in a circular way. Each node receives and retransmits the signal on the bus.

- New nodes are quite easily connected
- Connecting a new node implies the bus opening durin installation
- Full reliability at first fault
- Bus lenght depending on the number of nodes

Networks

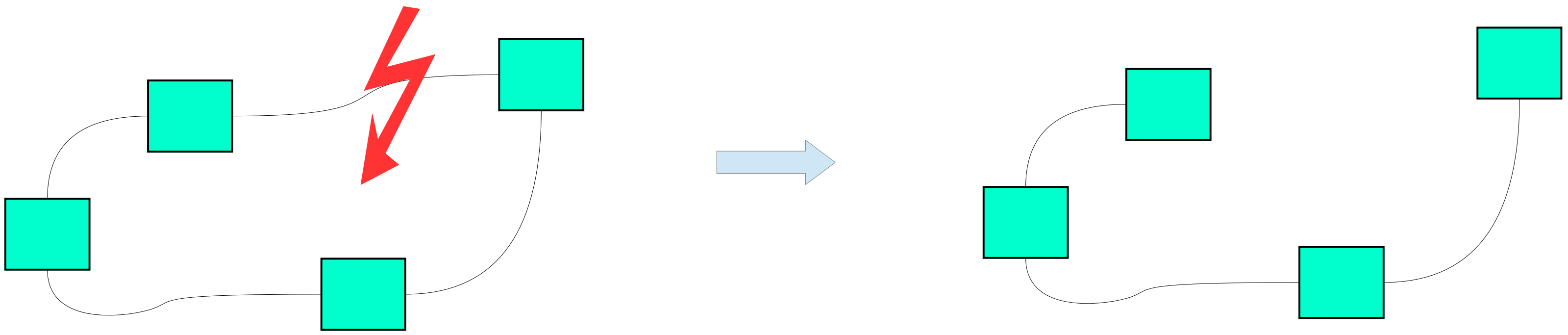
Topology



Daisy- chain ring

The node are connected by a bus in a circular way. Each node receives and retransmits the signal on the bus.

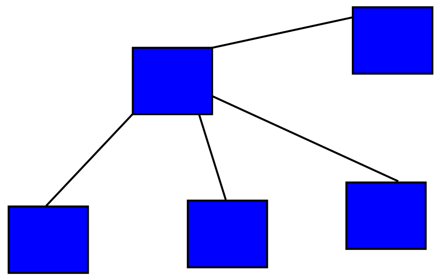
- Full reliability at first fault apart from fault on device



Networks

Topology

Star

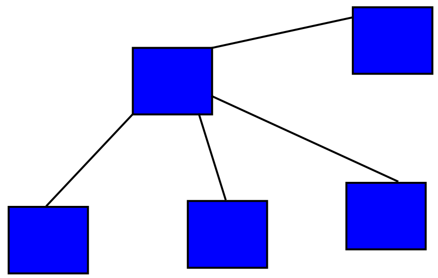


All nodes are connected to the same central node that is also the gateway of the LAN to the external network.

- New nodes are quite easily connected
- Installation can be expensive for more that 4 nodes
- Full reliability for faults at nodes
- Critical fault at the central node

Networks

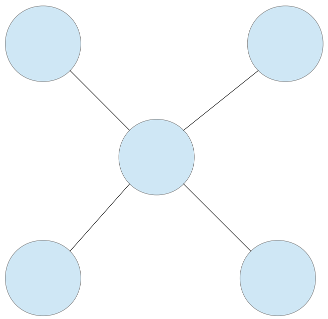
Topology



Star

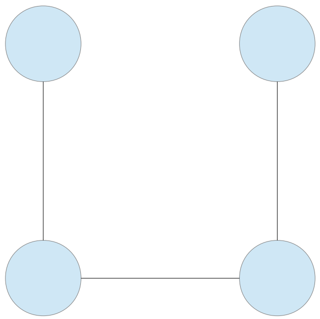
All nodes are connected to the same central node that is also the gateway of the LAN to the external network.

- Installation can be expensive for more than 3/4 nodes



$$L = 2\sqrt{2}\,l$$

5 devices

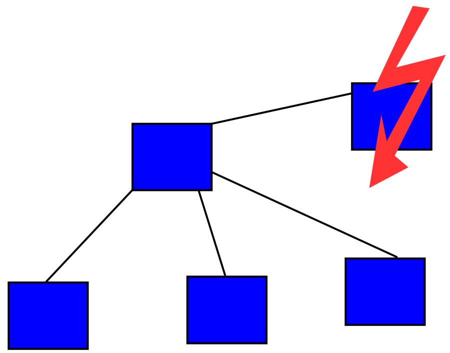


$$L = 3\,l$$

4 devices

Networks

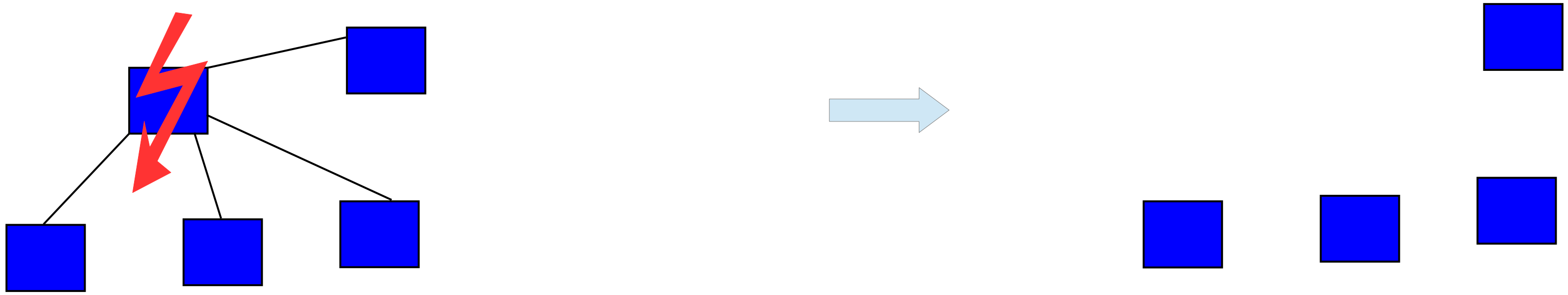
Topology



Star

All nodes are connected to the same central node that is also the gateway of the LAN to the external network.

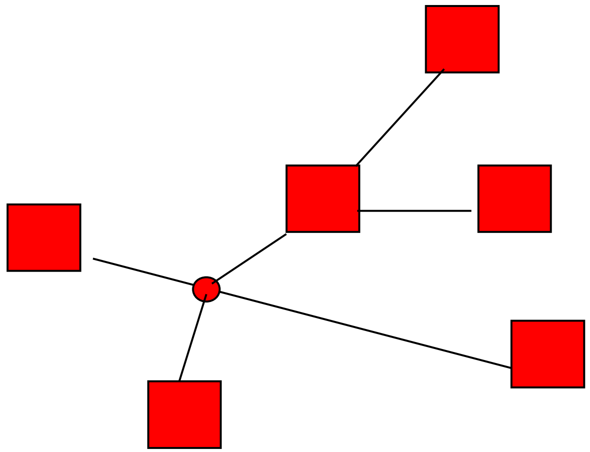
- Full reliability for faults at nodes
- Critical fault at the central node



Networks

Topology

Tree



It is a complex topology that combines two or more elementary topologies.

- New nodes are quite easily connected
- Simple installation
- Reliability

Networks

Criteria for choosing the topology

distance between nodes – installation expanses

environment – robustness with respect to faults

amount of data to transmit – max number of connected nodes

expansion perspectives - is it easy to connect a new node?

Most used: bus
Tendenza: tree

Networks

Cannel management

byToken: information transmission is defined and managed by means of a special code (TOKEN). The devices that got the Token can transmit the information within a pre-defined maximum time interval; once the allowed time has expired the code must be sent to another device.

It is a **deterministic network**

Token bus - IEEE 802.4: implemented on a bus topology with a twisted-pair of coaxial cable; the token passing is define by a prescribed sequence

Token ring - IEEE 802.5: the implementation is as for the Token bus but the token passing is defined by the sequencial position on the physical ring

Networks

Determinism:

In a **deterministic network** the maximum time interval between two subsequent communication from the same device is defined

In a **not deterministic network** the maximum time interval between two subsequent communication from the same device is not assured, i.e., some information could not be sent

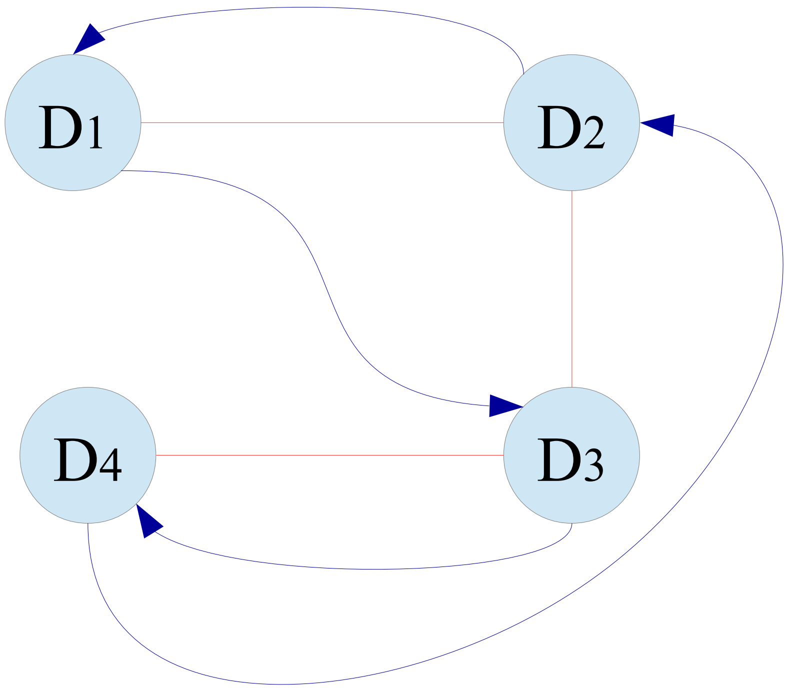
In a network, the maximum time interval between sending depends on:

- Bandwidth of the network
- Number of devices connected to the network
- Speed of the I/O boards on each device
- Network protocol, i.e., limitation on the massage lenght

Networks

Cannel management

byToken bus:



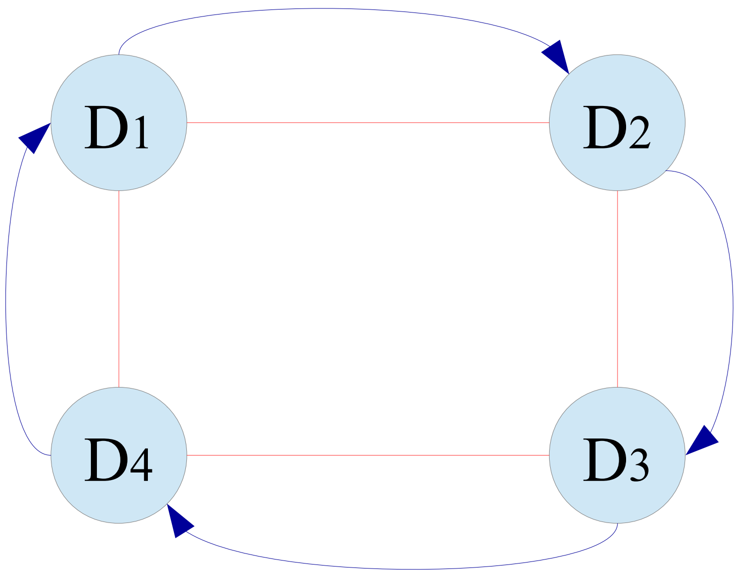
The path of the token is circular

The sequence of the token passing does not reflect the network connection

Networks

Cannel management

byToken ring:



The path of the token is circular

The sequence of the token passing reflects the network connection

Networks

Management

Master-Slave: there is a main node (the master) that gives the permission to transmit to each secondary node (slave).

It is a **deterministic network**

- Can be integrated with other criteria (e.g., Token)
- Priorities should be carefully handled
- It has a centralised nature that imples not very high transmission speeds
- Easy to implement and manage/update

Networks

Management

Master-Slave:

One device, the MASTER, fully manage the communication of the other devices, SLAVES, connected to the network

Centralised management

Networks

Magement

Publisher-subscriber: a network manager enrole each device to a group to read and send specific data. All members of the group can read the data sent by the members (similarly to a social network)

It is a **deterministic network**

- It does not allow for a simple management of priorities
- It has a centralised nature that imples not very high transmission speeds
- Quite complex to implement and manage/update

Networks

Management

Muliple access: all connected devices can transmit and receive data independently. If two or more device access the channel at the time a collision occurs and it has to be managed

MACS-CD (multiple access carrier sense-collision detection): when a collision occurs a random time delay is assigned to each involved device. It cannot transmit data during such a time delay.

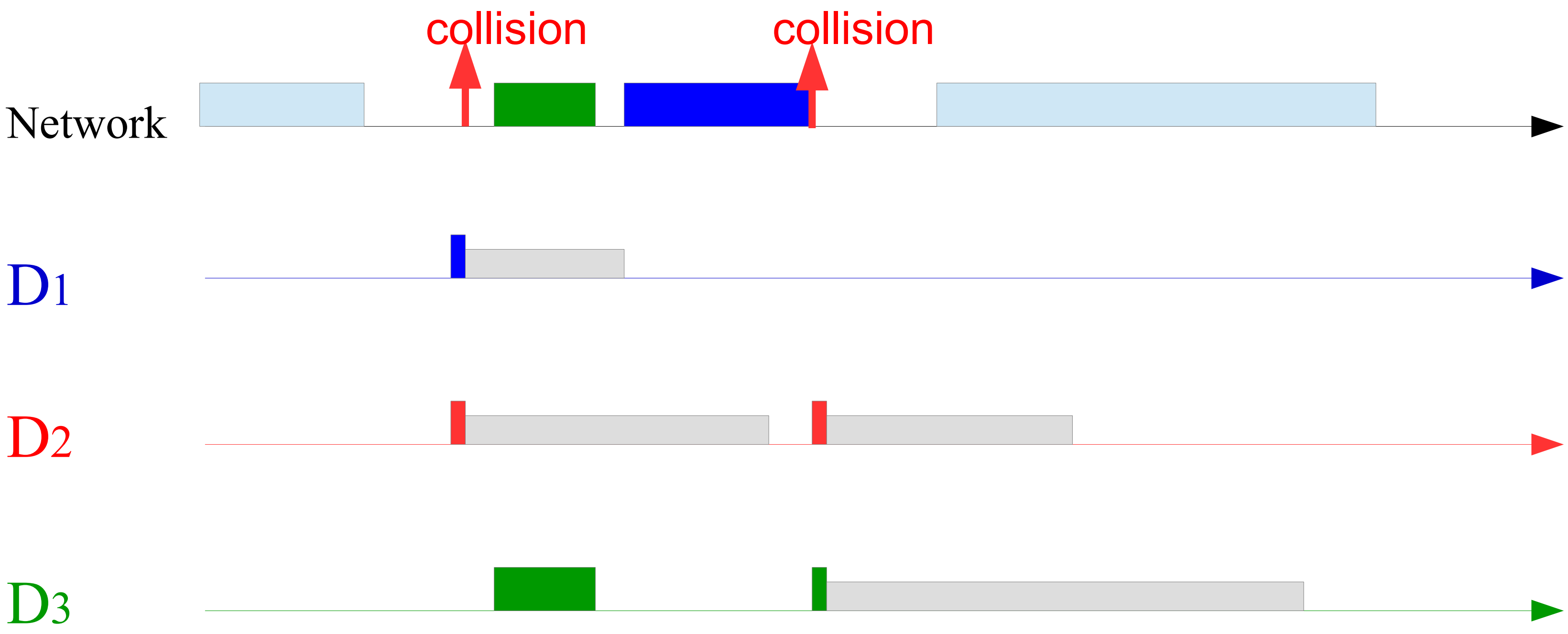
MACS-BA (multiple access carrier sense-bit arbitration): when a collision occurs the data are comparede bit-by-bit and only the data with highest rank is transmitted

It is a **not deterministic network**

Networks

Management

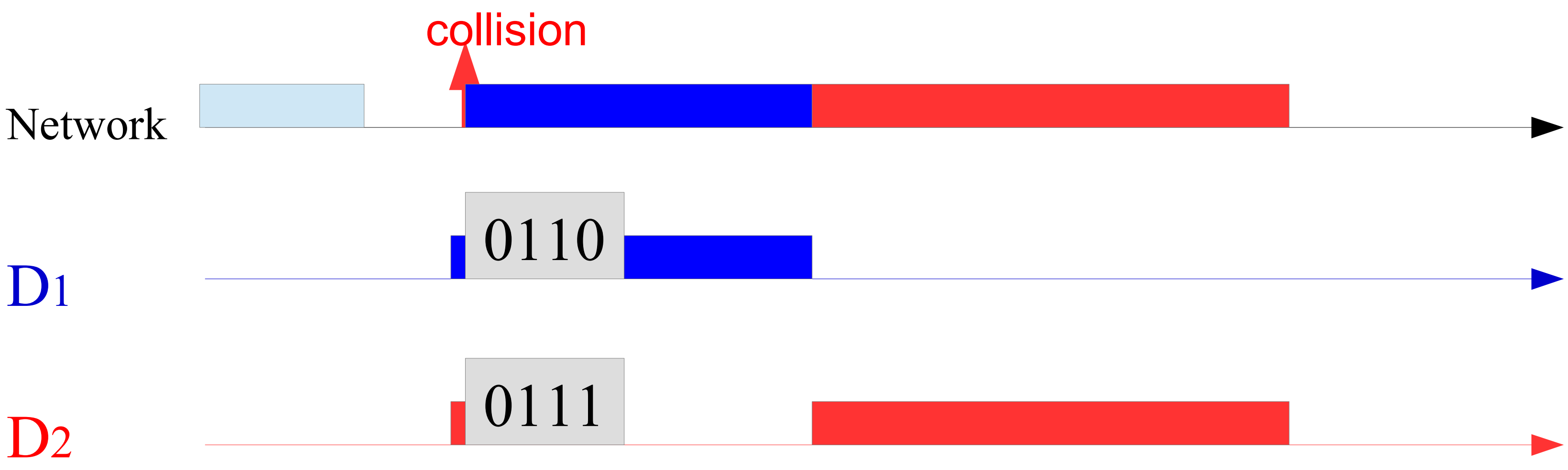
MACS-CD (multiple access carrier sense-collision detection): it could happen that a device (*D_2 in the example*) is not allowed to send messages.



Networks

Management

MACS-BA (multiple access carrier sense-bit arbitration): it could happen that a device (*D2 in the example*) is not allowed to send the message, but the other colliding one (*D1 in the example*) transmits, and there is no inibition time period.



Networks

Criteria for choosing the protocol

Critical data flow – determinism

Quality of the datum – priority management

Amount of data to transmit – max number of connected nodes

Expandability – is it easy to allow new nodes to be connected?

Most used: Token ring/bus,Master-Slave
Tendency: Industrial Ethernet

Networks

caratteristiche	Profibus DP	Interbus S	Modbus +	Foundation Fieldbus	ControlNet	DeviceNet	Ethernet
Data Rate b/s	9.6kb/s – 12Mb/s	500kb/s	1Mb/s	31.25kb/s	5Mb/s	125 -250 - 500kb/s	10Mb/s – 10Gb/s
Tecnica di Comunicazione	Mono - Multi Mast. Slaves	Master Slave	Mono - Multi Mast. Slaves	Mono - MultiMas t. Slaves	Produtt. Cons .	Produtt. Cons.	Dipende
Metodo d'Accesso	Token + M/S	M/S	Token	Token	CTDMA	CSMA/ NBA	CSMA/ CD
Tipo di mezzo	Twisted pair Fibre ott.	Twisted pair	Twisted pair Fibre ott.	Twisted pair Fibre ott.	Coax Fibre ott.	Twisted pair e altri	vari
Nodi Max	126	512	64	32	99	64	dipende
Determinismo	si	si	si	si	si	no	no
Bus Powered	no	no	no	si	no	si	no
Topologia	lineare	anello	lineare	Lineare albero	Lineare Stella albero	lineare	varie
Segmenti Max	1200x7rip. 9600m	13km	450x3rip 1800m 3km con F.O.	1900m	5km	500m	dipende
Standard Physical Layer	EN50254 IEC61158	EN50254 IEC61158	PROPR.	EN50170 IEC61158	EN50170 IEC61158	EN50325 IEC62026	IEEE802

Networks

Industrial Ethernet

Pros

- High data-rate: up to 1 Gbit/s with Gigabit Ethernet and Cat5e/Cat6 cables or optical fibers
- Increased distance between devices
- Standard devices are needed: switch, router, printer, etc
- Several nodes can be connected to the same branch
- Peer-to-peer architectures can be implemented
- Better interoperability

Networks

Industrial Ethernet

Cons

- Existing control networks should be updated
- Strong limits for the implementation of Real-Time applications with the TCP/IP protocol
- More difficulty in managing of the TCP/IP packets with respect to serial data
- Increased dimension of of the packets (64 bytes) with respect to those in the standard control networks (1÷8 bytes)
- Possible large latency of the data (time delays)

Networks

Industrial Ethernet

Characteristics of possible internet networks configuration

- **TCP/IP**: to send not critical data and to control plants with time constants not less than 100 ms
- **Real-Time**: I/O applications with elaboration time up to 10 ms
- **Isochronous Real-Time**: control applications for devices with time constants less than 1 ms (electrical drive)

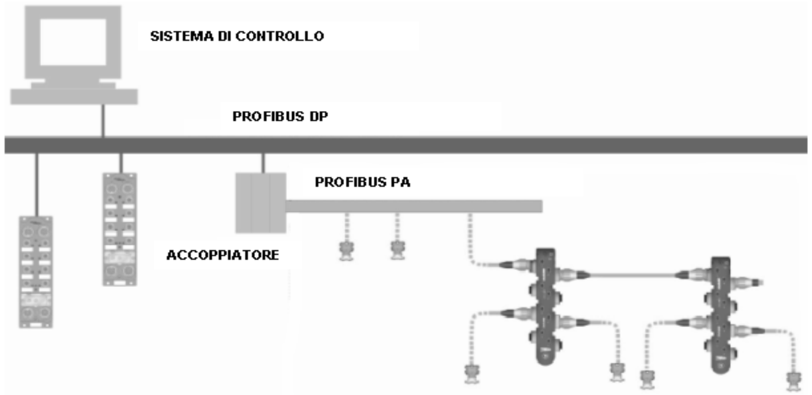
Networks

Industrial Ethernet

Available Protocols

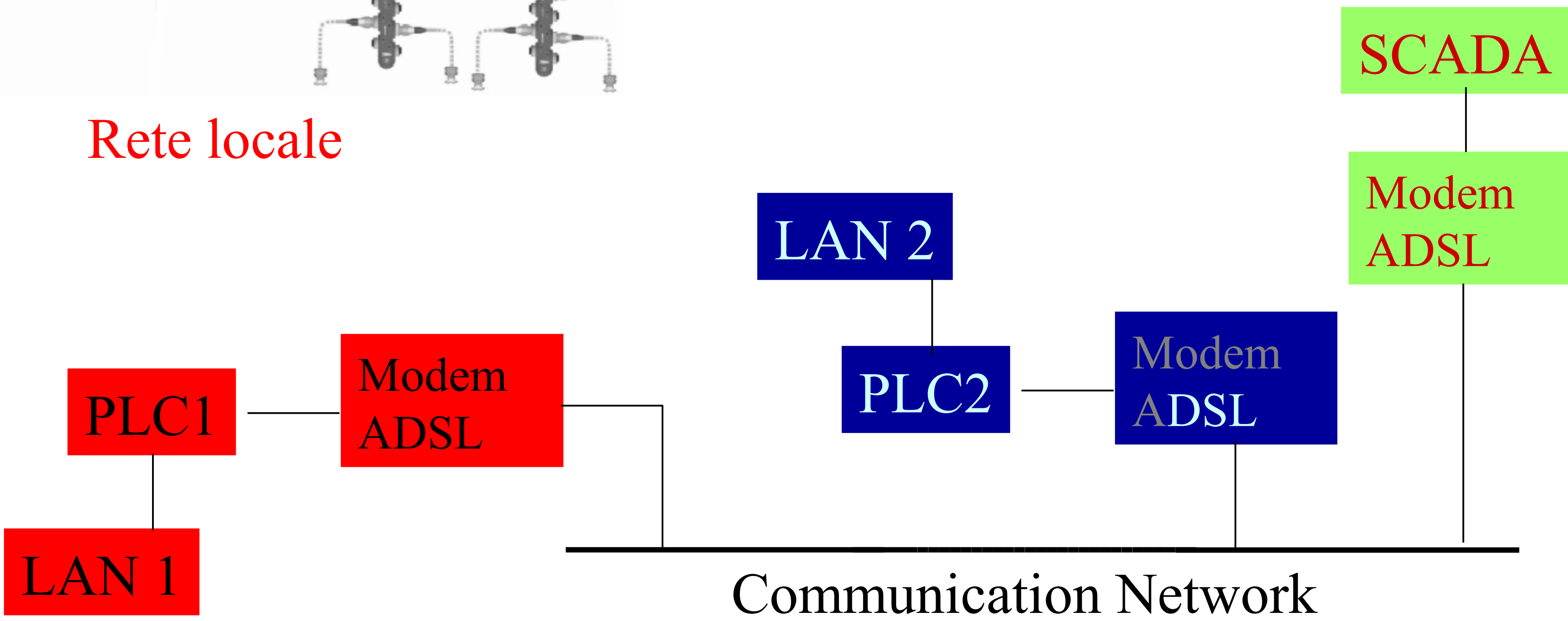
- EtherCAT
- EtherNet/IP
- PROFINET
- POWERLINK
- SERCOS III
- CC-Link IE
- Modbus/TCP

Networks



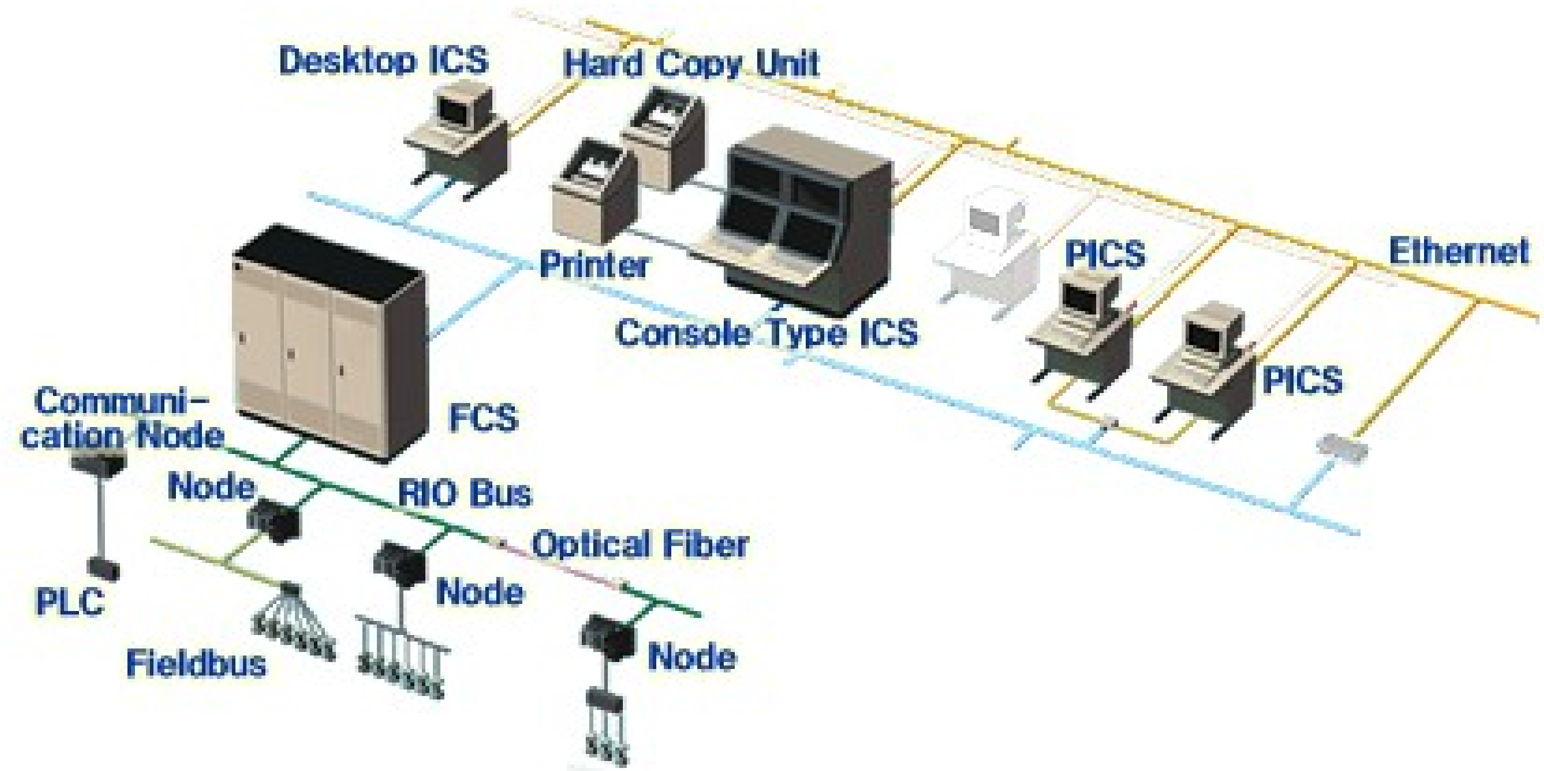
Rete locale

Far away plants

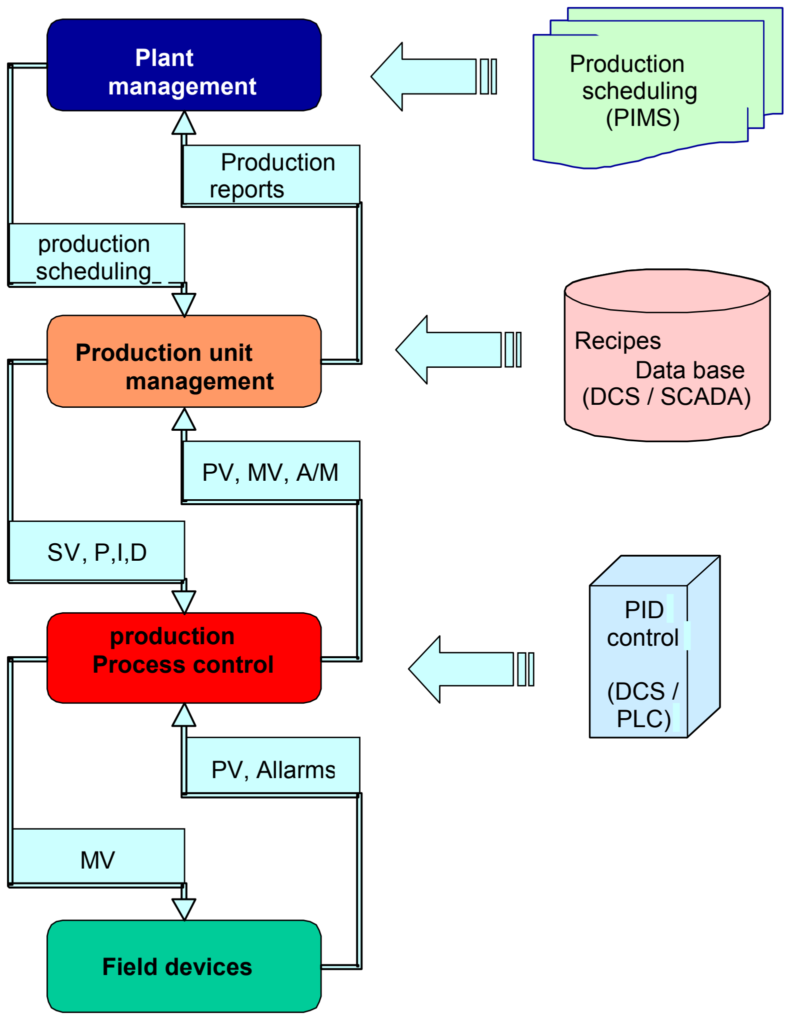


Networks

Nearby plants



System Integration



Information flow in production processes

System Integration

Communication flow in an industrial production system

ERP

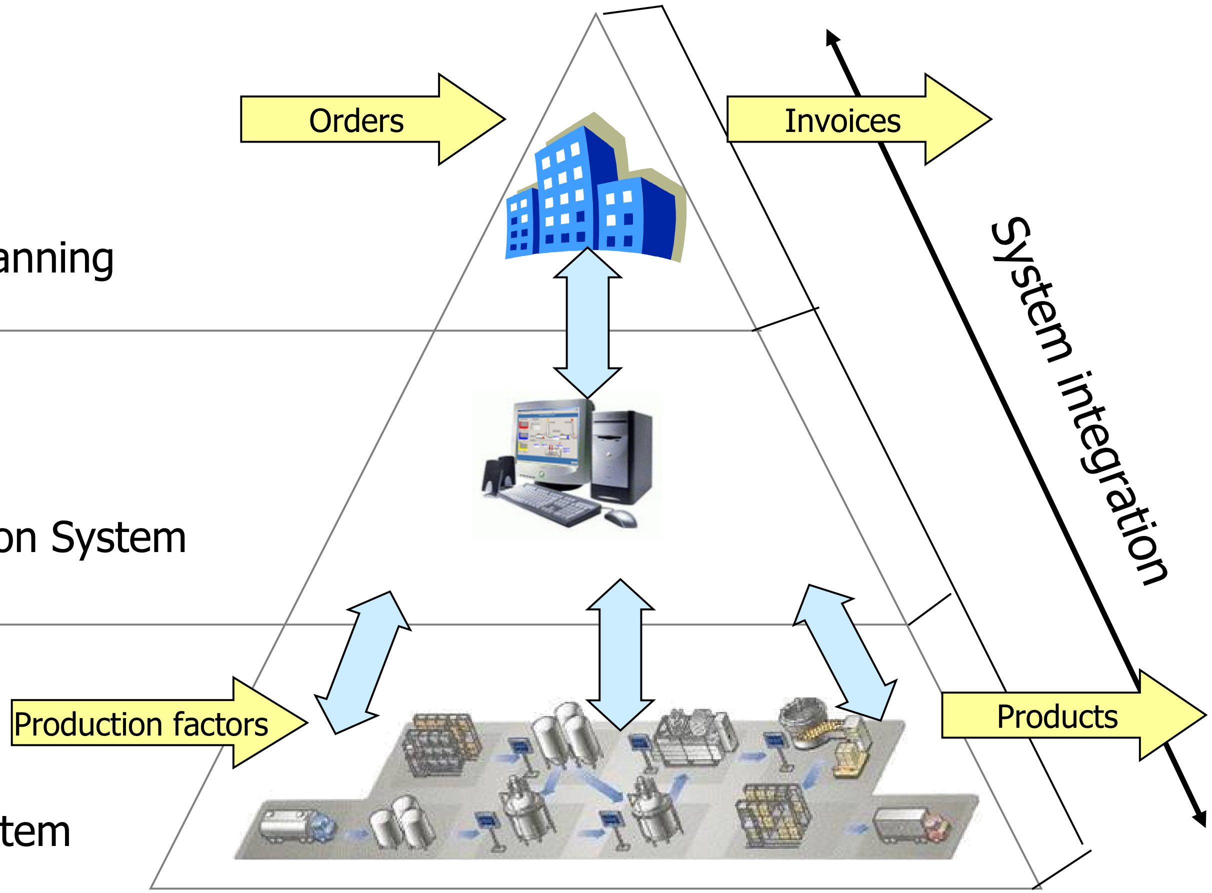
Enterprise Resource Planning

MES

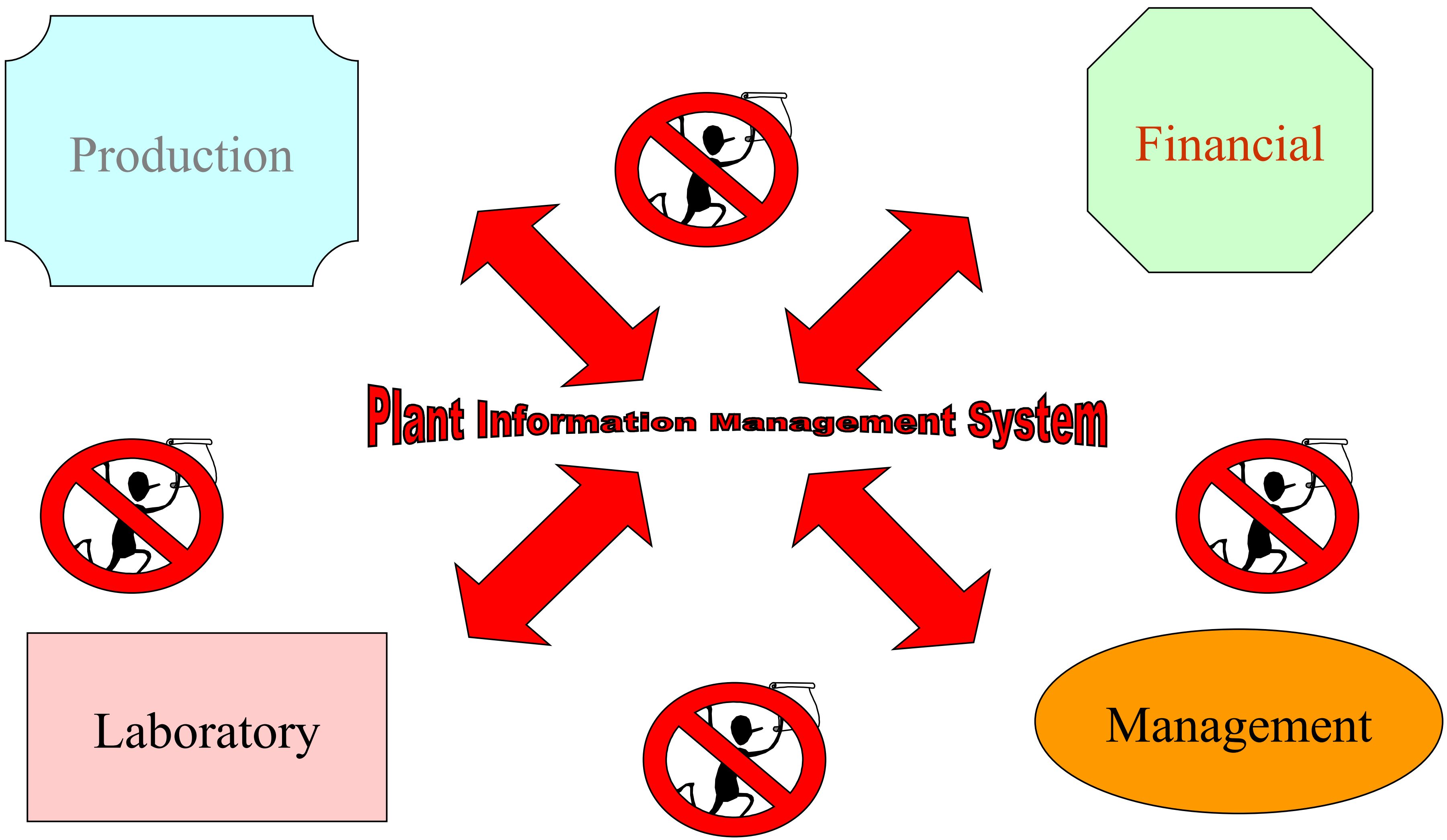
Manufacturing Execution System

PCS

Production Control System

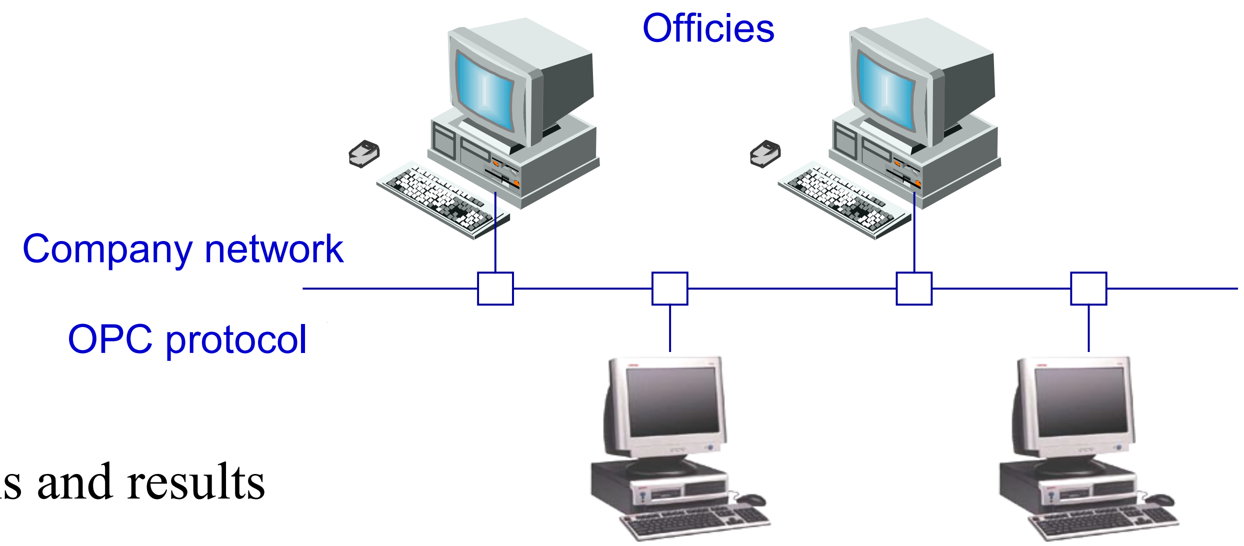


System Integration – I.M.S.



Systems for Supervision and Control - Integrating ICS

System Integration – I.M.S.



Remote supervision

Working instructions

Alarm analysis

Correlations between actions and results

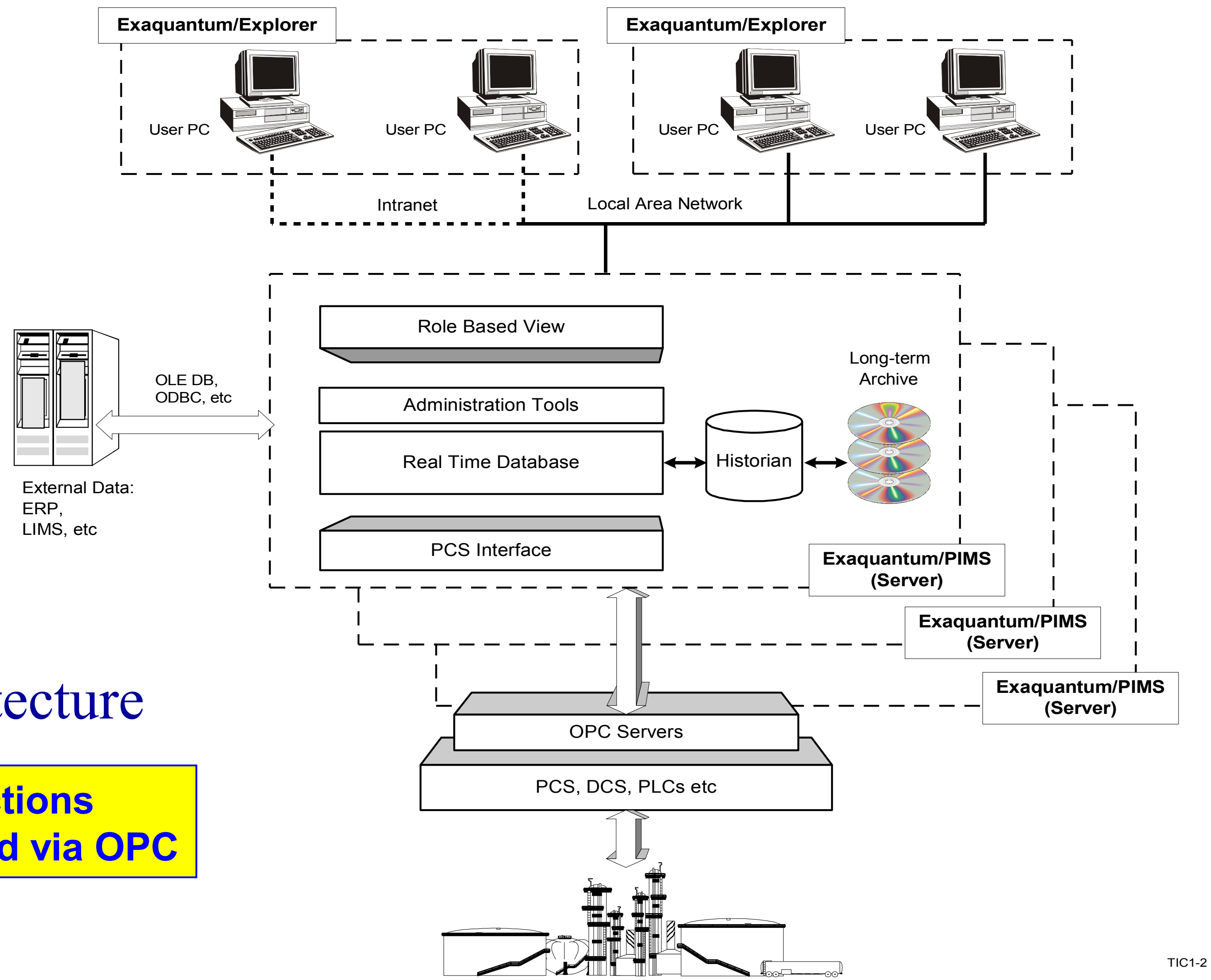
Design and supervision of control loops

Data storage and reading

Analysis and re-design (parameters checking and identification, mass and energy balance energia)

On-line economic evaluatio of the production results

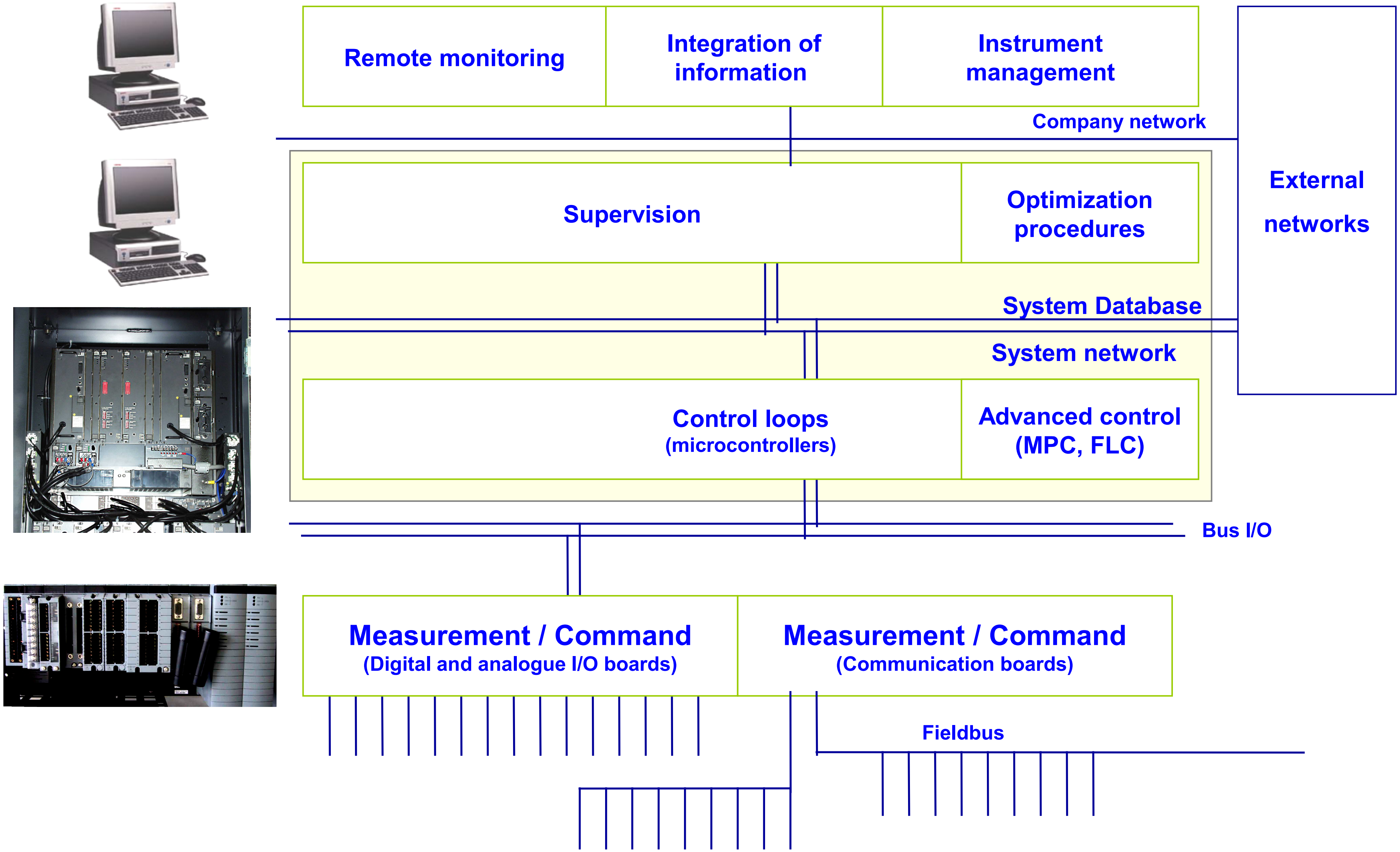
System Integration – I.M.S.



Plant IMS architecture

- **Client/Server connections**
- **RTDB SQL is updated via OPC**

System Integration – I.M.S.

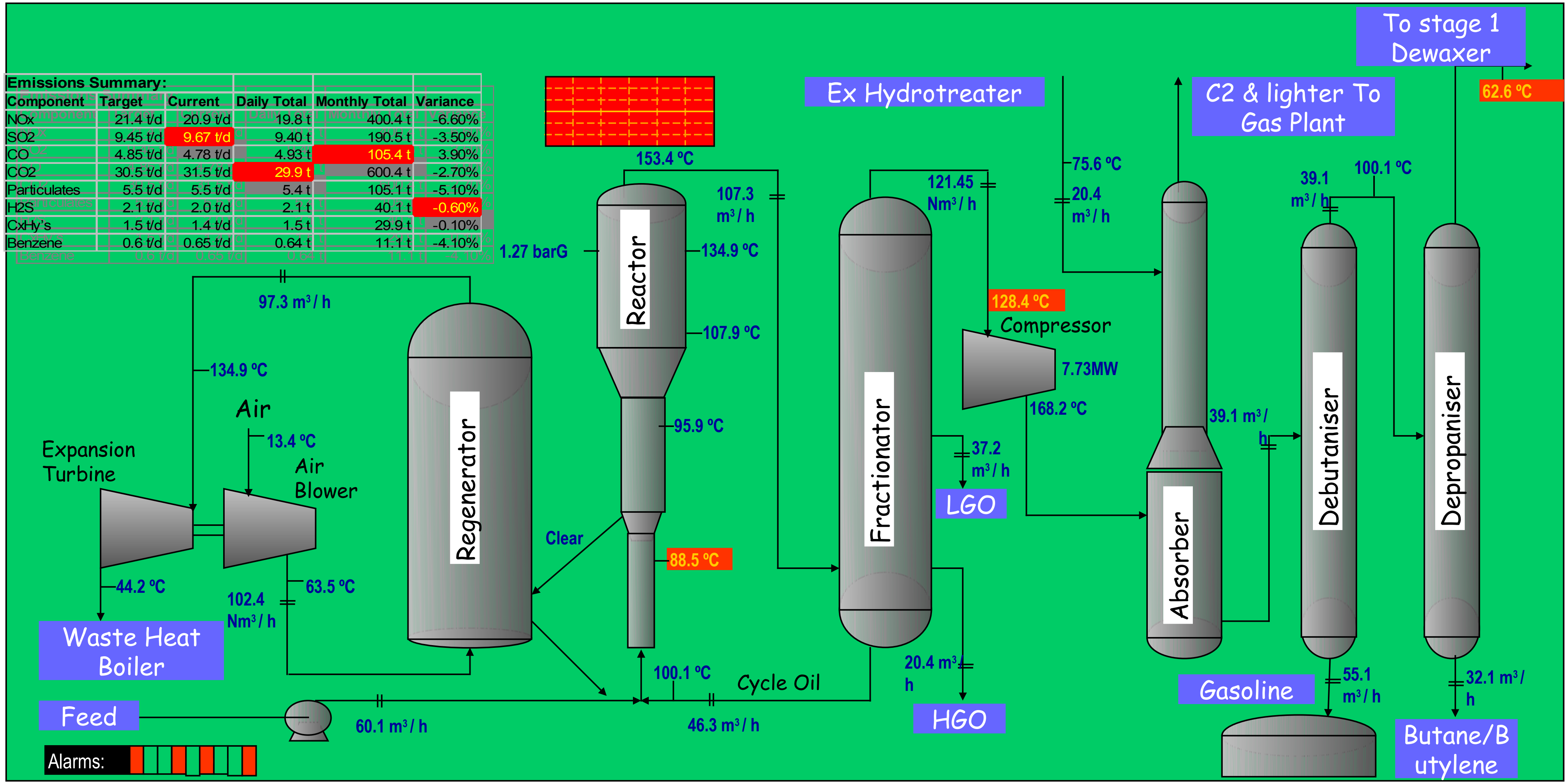


System Integration – I.M.S.

- **Real time udate of the Data-Base**
  - Automatic data synchronisation between DCS and Data-Base
  - No manual update of the data-base
- **More available data for analysis**
  - All data are directly acquired from the field sensors
- **Presentation via web-browser**
  - Simple generation of drawings from the DCS
- **Automatic reporting**
  - Excel interface are available
  - Automatic reporting directly from process measurements
- **Design based on a Windows platform**
  - Interfaces to SQL, Excel are available as well as Drag&Drop
  - Open standard (VB, ActiveX DCOM, SQL)
- **The data are not compressed**
  - Less data corruption
- **Direct connection between production and management**
  - The system can be connected to SAP

System Integration – I.M.S.

Operator's view of the plant at monitor

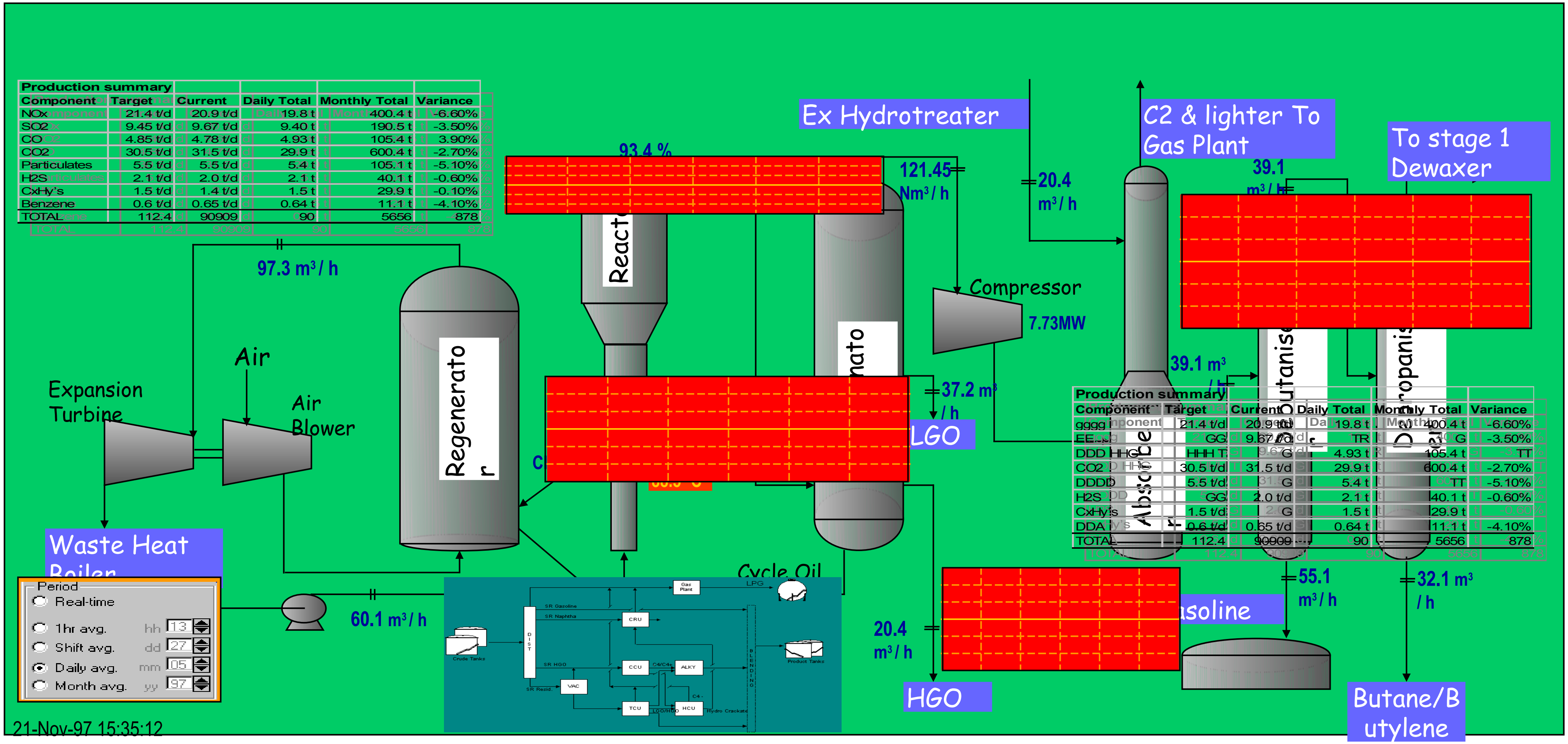


Emissions Summary:

Component	Target	Current	Daily Total	Monthly Total	Variance
NOx	21.4 t/d	20.9 t/d	19.8 t	400.4 t	-6.60%
SO2	9.45 t/d	9.67 t/d	9.40 t	190.5 t	-3.50%
CO	4.85 t/d	4.78 t/d	4.93 t	105.4 t	3.90%
CO2	30.5 t/d	31.5 t/d	29.9 t	600.4 t	-2.70%
Particulates	5.5 t/d	5.5 t/d	5.4 t	105.1 t	-5.10%
H2S	2.1 t/d	2.0 t/d	2.1 t	40.1 t	-0.60%
CxHy's	1.5 t/d	1.4 t/d	1.5 t	29.9 t	-0.10%
Benzene	0.6 t/d	0.65 t/d	0.64 t	11.1 t	-4.10%

System Integration – I.M.S.

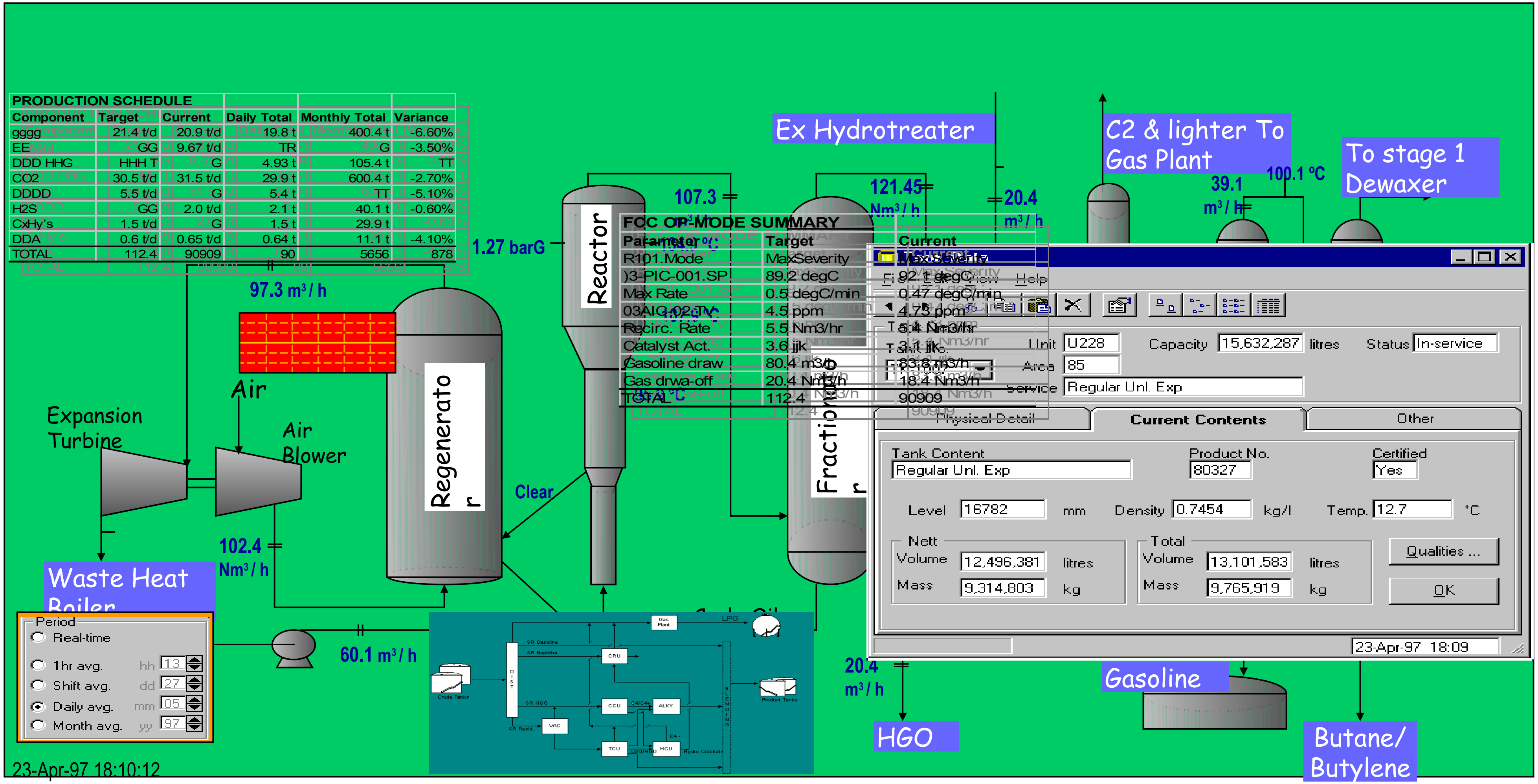
Plant manager's view at desk



Systems for Supervision and Control - Integrating ICS

System Integration – I.M.S.

Manager's view of the plant at office



Systems for Supervision and Control - Integrating ICS

System Integration – I.M.S.

Example of a periodic report directly created by Excel

8:10	30/06/98	Methanol 1 Daily	05/03/95 08:08:25	Report 1

Days Operated: **60.84**

Checked by:	
Approved by:	

PRODUCTION

T503	9.15	Ton/Day		
T502	39.90	Ton/Day		
P. MEOH (Total)	49.05	Ton/Day	Planned	100.00
Production Rate	49.05%	%		
C. MEOH	0.77	Ton/Day	Planned	100.00
Production Rate	0.77%	%		
Sum of the Month	3030.94	Ton/Month		
Plan of the Month	3000.00	Ton/Month		
Achivement	101.03%	%		

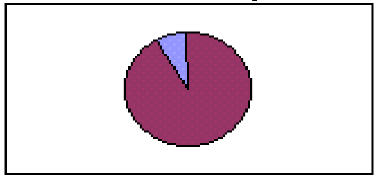
TRANSFER

C. MEOH to Distillation	0.77	Ton/Day
P. MEOH to Quay Tank	49.05	Ton/Day

STOCK

P. MEOH	TK-801-A	39.90	Ton
	TK-801-B	9.15	Ton
	TOTAL	49.05	Ton
C. MEOH	TK-802-A	35.95	Ton
	TK-920-B	99.98	Ton
	TOTAL	135.93	Ton

MEOH Purity

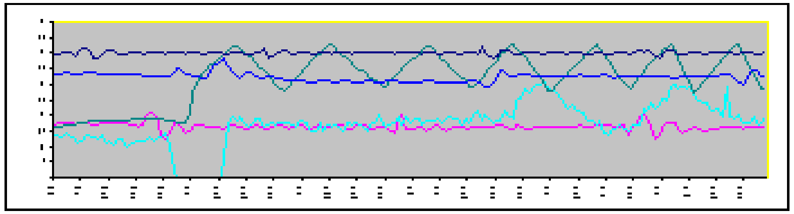


REFORMER OPERATION RATE

No, 1 Reformer	4.72%	%
No, 2 Reformer	0.49%	%

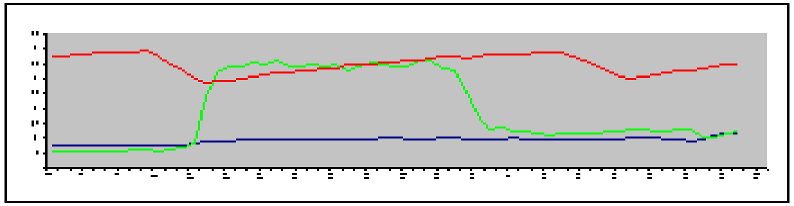
CONSUMPTION & UNIT CONSUMPTION

NG	39.90	NM3/Day	39.90	NM3/Day
(P. MEOH) HHV Base	9.15	NM-Kcal/Ton	9.15	NM-Kcal/Ton
(C. MEOH) HHV Base	0.77	NM-Kcal/Ton	0.77	NM-Kcal/Ton
Sea Water	11.80	Ton/Day	11.80	Ton/Day
Potable Water	0.00	Ton/Day	0.00	Ton/Day
Waste Water	35.95	Ton/Day	35.95	Ton/Day
Elec Power	99.98	Ton/Day	99.98	Ton/Day



ANALYSIS

	ETCH (ppm)	Acetone (ppm)	Water (ppm)	SG	Factor	Purity
PMA:	39.90	34.20	0.00	9.15		
CMA:	9.15		35.95	0.77	11.80	35.95
S/C 1:	0.77	R/D:	99.98	L/N:	0.00	
S/C 2:	11.80					

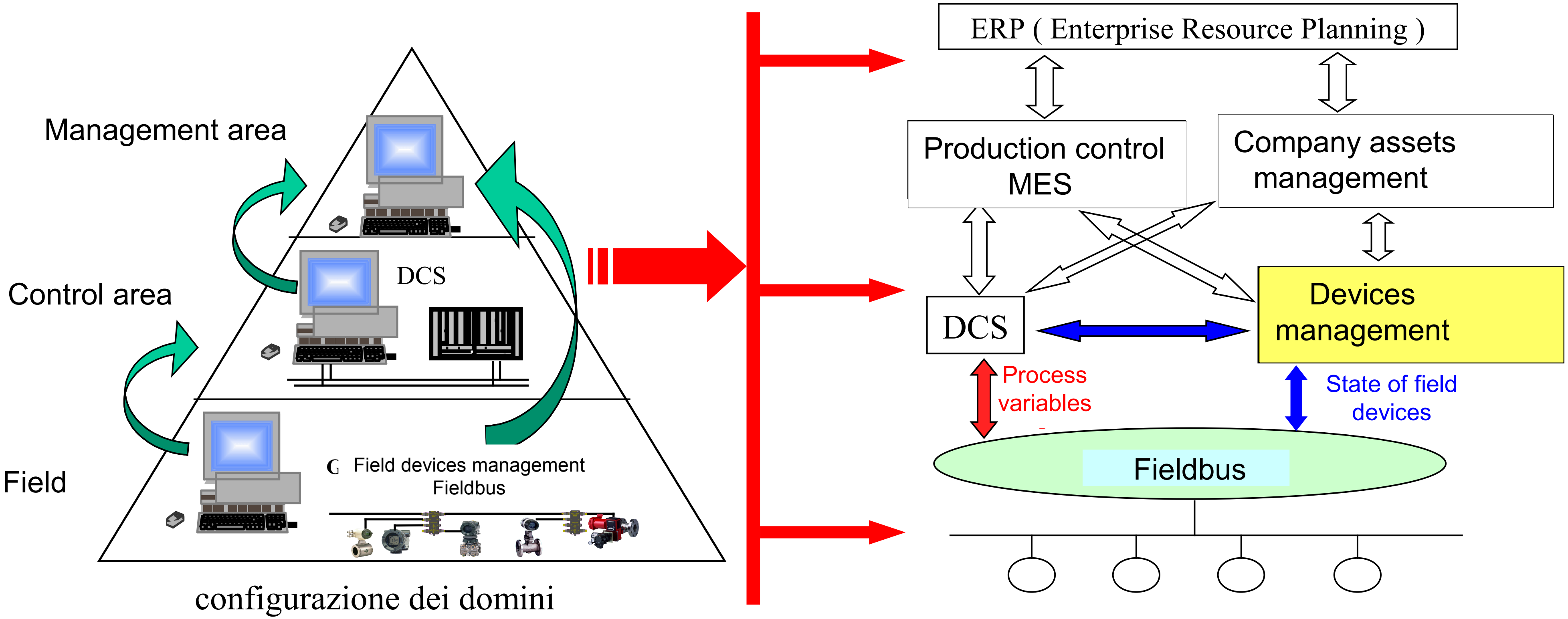


GAS COMPOSITION (%)

	CO2	CH4	N2	C2H6	C3H8	C4H10	MW	HHV Kcal/NM3	LHV Kcal/NM3	
NG	13.30%	3.05%	0.26%	3.93%	0.00%	11.98%	33.33%	11.40%	22.75%	231.74 100.00%

Plant Resource Manager (PRM)

The maintenance of the field devices can be integrated in the factory management system by means of a direct connection to the field



System Integration – P.R.M.

Such a system allows for some facilities:

- Fault diagnosis
- Parameter tuning of the measurement devices
- Maintenance scheduling

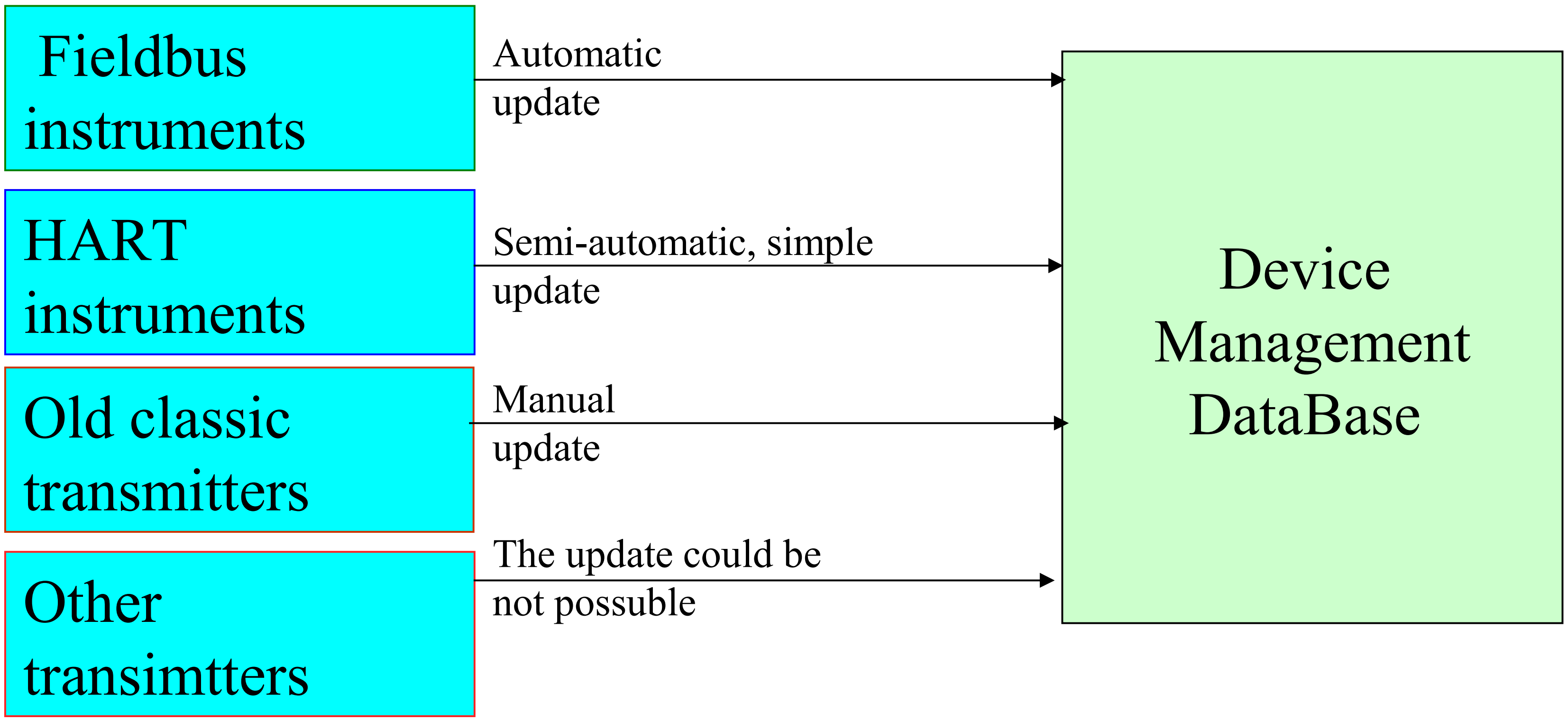
Diagnosis involves several devices and components:

- communication networks
- I/O boards and microprocessors
- sensors
- actuators and equipments

The **P**lant **R**esource **M**anager is an information system that integrates the management of all equipments with the factory/company management system

System Integration – P.R.M.

The effectivenss of the PRM dipends mostly on the characteristcs of the measurement devices



System Integration – P.R.M.

The P.R.M. Data-Base. Conteins all data and information that are useful and necessary to the management of the field devices :

General information - label , type, model, producer, serial number, ….

This info are useful for buying it as well as its spare parts

Installation data - range , span , firmware, ….

This info are needed for the tuning

Historical data - events, tuning, diagnosis , maintenance actions, ….

This info are useful for diagnosis

Maintenance instructions – medium time before fault (MTBF), maintenance cadence, spare parts, ….

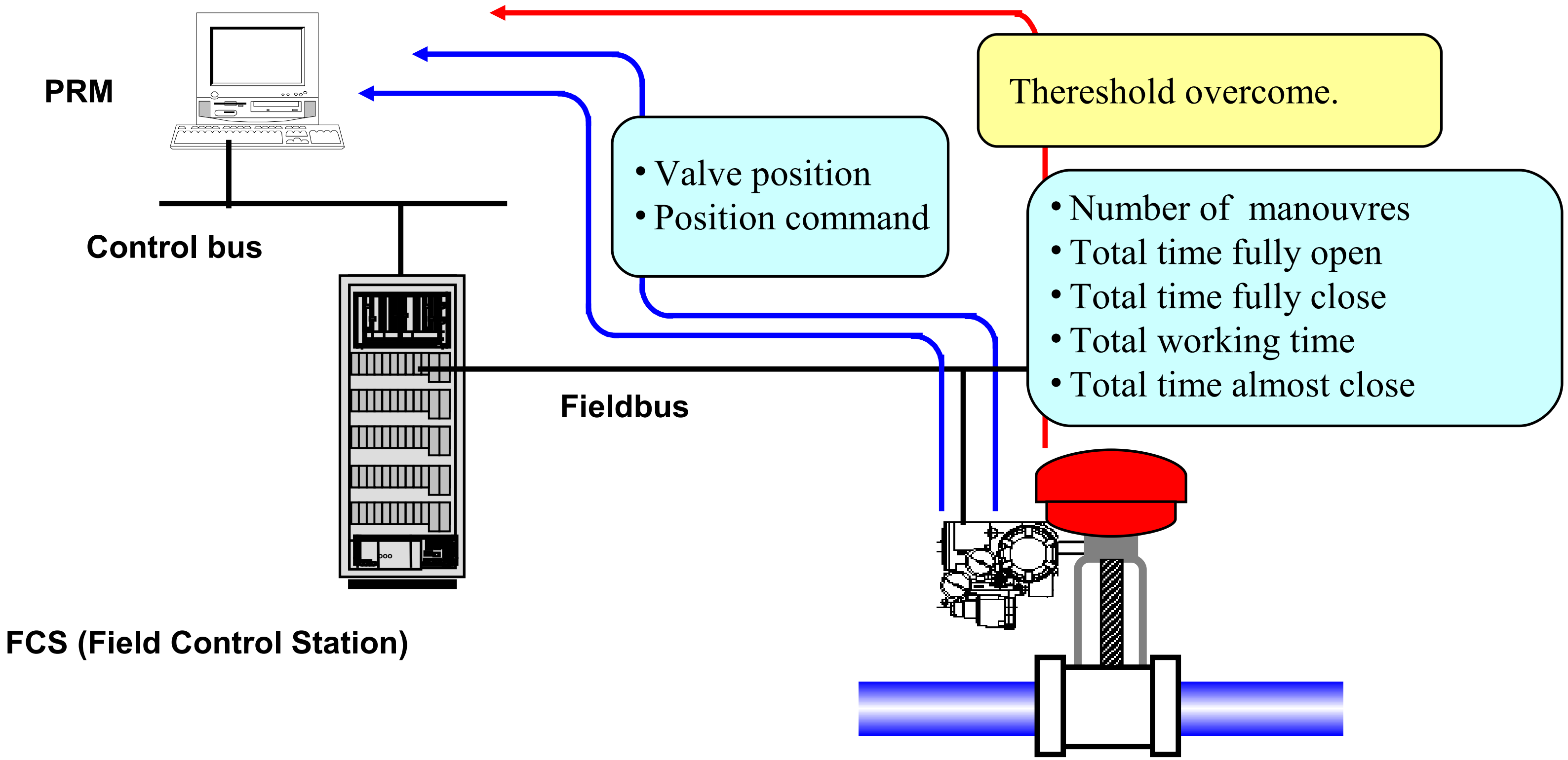
This info are useful for maintenance management and scheduling

Technical data and instructions – minstallation and users manual, data sheet, ….

This data are needed usual management

System Integration – P.R.M.

- Example of a valve connected to the PRM
  - All variables and parameters considered as critical for maintenance are monitored



Manufactory Execution System (M.E.S.)

M.E.S. is a complex **applicative software system**

- integrates different modules,
- aims to monitor and manage the enterprise production
- directly connected to plant I.M.S.
- mainly used by administrative offices
- can be connected to the E.R.P.

It is a bridge between the production and the management divisions of the enterprise

System Integration – M.E.S.

Main functions of M.E.S. are:

- collect data from the I.M.S.
- monitoring the state of advancement of the production
- management of the resources needed for production
- tracking of the product and of the production system
- monitor and manage logistic
- monitor the quality of production

Enterprise Resource Planning (E.R.P.)

E.R.P. is a complex **applicative software system**

- integrates different modules
  - *industrial accounting*
  - *product design*
  - *asset management*
  - *management of human resources*
  - ………..
- collect data from the I.M.S. and the M.E.S.
- register decisions and proposals

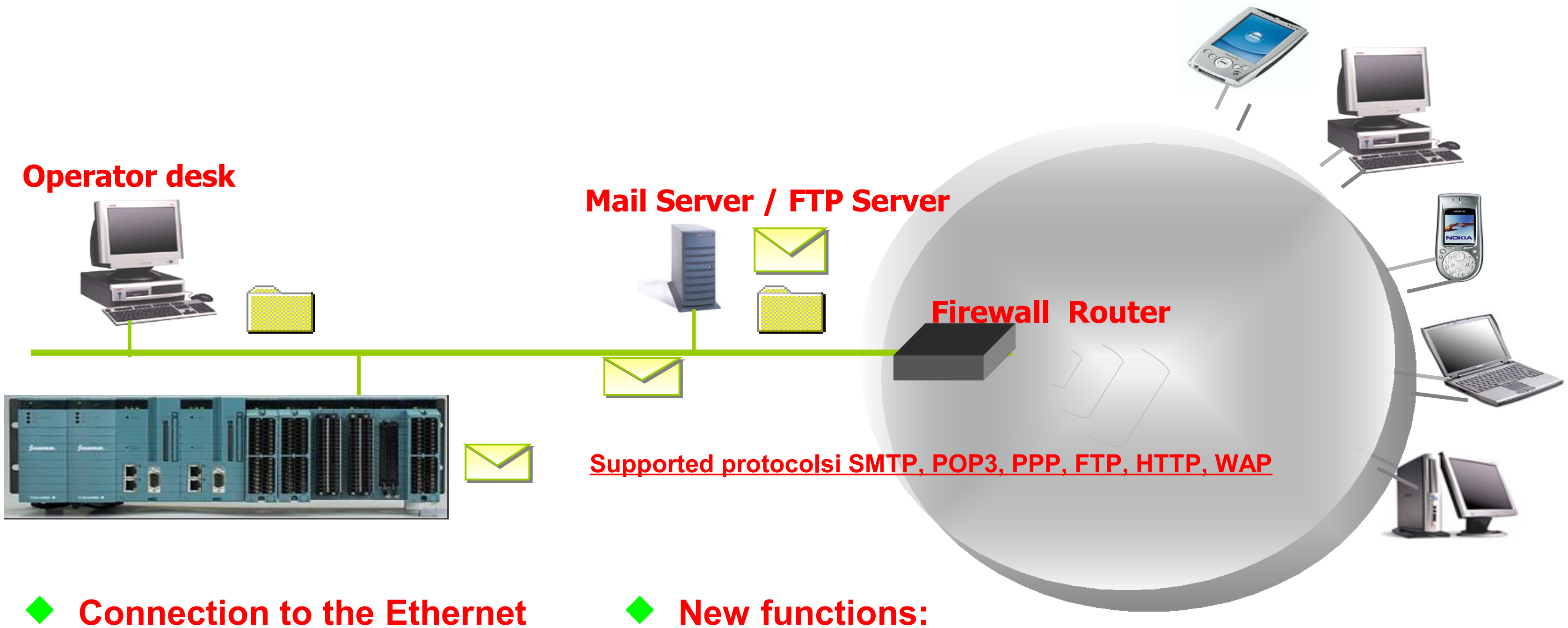
It is a high level management tool to monitor and manage a multi-divisional enterprise

System Integration – E.R.P.

Main functions of E.R.P. are:

- increase the efficiency
- decrease the economic risk
- increase the effectiveness and timeliness of management decisions
- increase the coordination of the enterprise divisions
- improve the management of resources, both human and material

Connecting to the www



- Connection to the Ethernet by means of:
  - LAN/WAN
  - VPN
  - Telephon lines
  - GSM
  - Radio waves, satellite
- New functions:
  - Web monitoring via Internet
  - FTP
  - e-mail
  - SMS
  - JAVA / HTML programming

Security issues in I.C.S.

Safety and Security in I.C.S.

Safety: the property of protecting from the effects of accidental faults and failures in the plant devices such that the injuries to people and the damages to the plant are limited at a certain level of **risk**.

Security: the property of protecting the system from threats by external, or internal, actors to cause damns to the system or give unproper advantages to the attacker, at a certain level of **risk**.

Security issues in I.C.S.

Safety and Security in I.C.S.

The level of both Safety and Security is a probabilistic variable, connected to the concept of **Risk**.

$$R_i = \sum_j c_j * d_{ji} * p_i$$

R_i : risk associated to the i^{th} event

p_i : probability that the i^{th} event occurs

d_{ji} : probability that the j^{th} damage is caused by the i^{th} event

c_j : cost associated to the j^{th} damage

Security issues in I.C.S.

Safety and Security in I.C.S.

The level of both Safety and Security is a probabilistic variable, connected to the concept of **Risk**.

$$R_i = \sum_j c_j * d_{ji} * p_i$$

To limit the risk it is needed to decrease the probabilities p_i and d_{ij} by a proper design of the system, possibly increasing the construction or production costs C_i

$$\Delta R_i \quad vs \quad \Delta C_i$$

?

Security issues in I.C.S.

Safety and Security in I.C.S.

Safety:
The level of safety in an I.C.S. can be improved by properly design the process, the devices and the control system.
It is a competence of process and control engineers.

Security:
The level of security in an I.C.S. can be improved by properly design the computer and the network systems.
It is a competence of computer and communication engineers.

Security issues in I.C.S.

Safety and Security in I.C.S.

Safety:

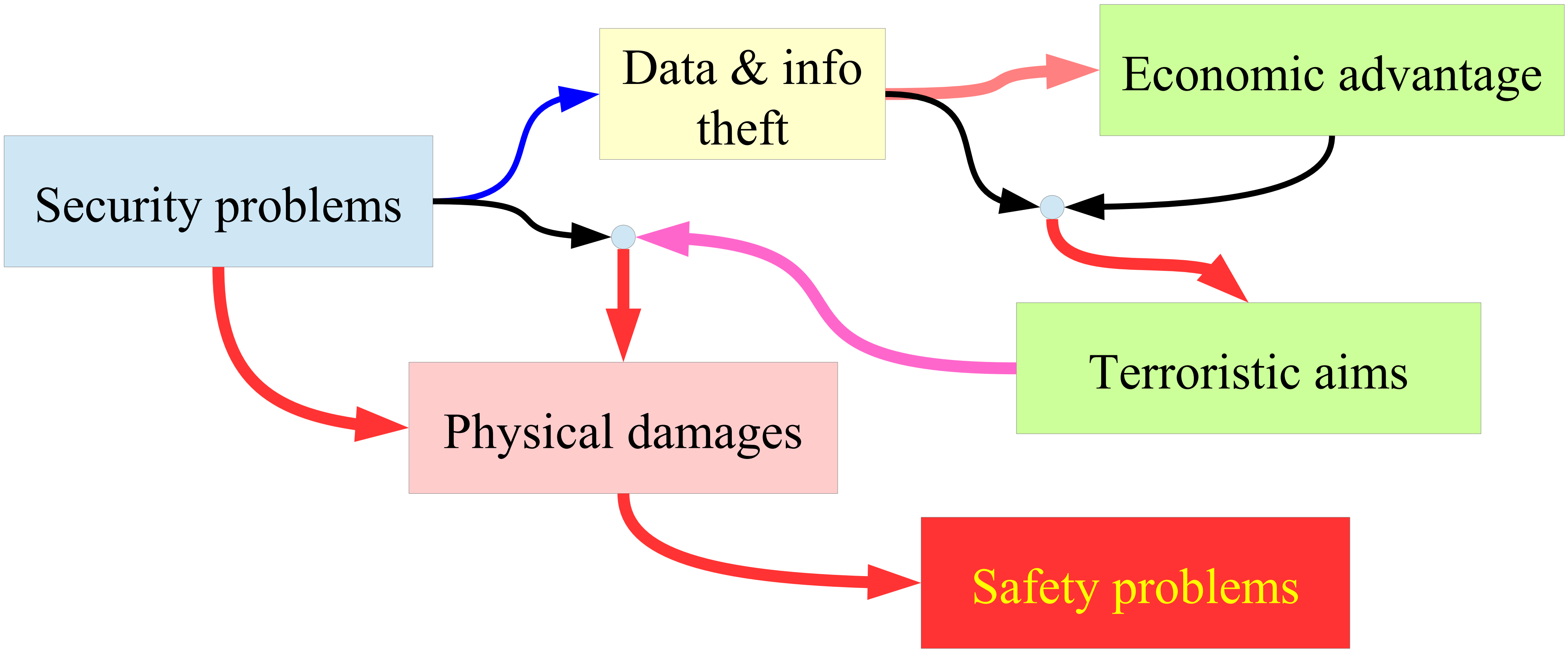
The level of safety is guaranteed by using redundance and /or increasing the strenght of devices to physical stresses, e.g., over-voltages and over-pressures with respect to nominal values.

Security:

The level of security is guaranteed by using proper codes and applications to detect threats, e.g., firewalls, intrusion-detection systems, and systems configurations, e.g., proxy, redundance.

Security issues in I.C.S.

Safety and Security in I.C.S.



Need of integrated design with respect to safety and security

Security issues in I.C.S.

Different characteristics and priorities in ICS and ICT

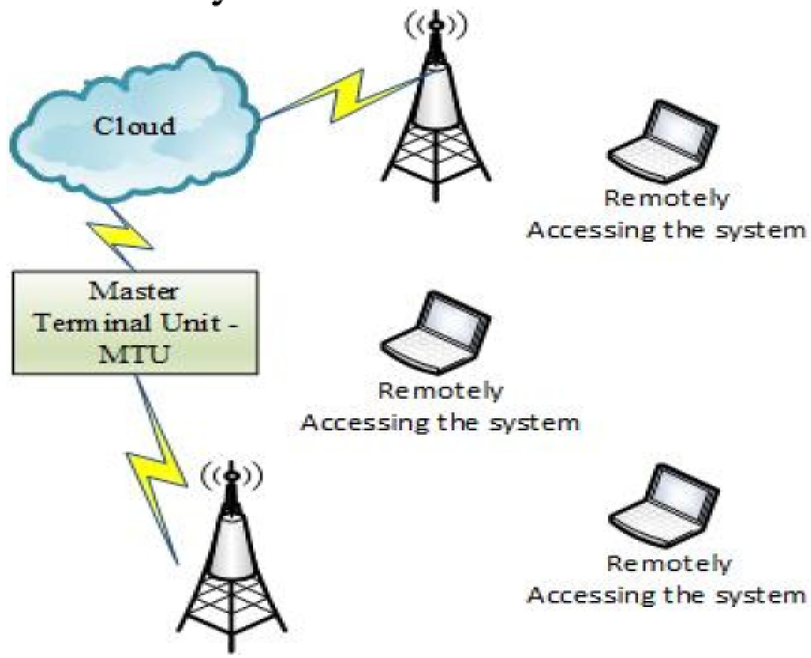
ICS Priority	**ICT** Priority
Data availability	Data availability
Data reliability	Data reliability
Data confidentiality	Data confidentiality
Data security	Data security

Can a unsecure data be rialiable?

Security issues in I.C.S.

Increased risk when distributed computing systems are used

Fourth generation IoT-cloud based SCADA systems



The use of IoT devices can imply a reduced use of VPNs that increases the number of weak points in the network and in the information systems as well

Certified cloud system usually are more secure than local data center of small enterprise

Security issues in I.C.S.

Causes of increased cyberattack risk to ICS

- Adoption of standardized technologies (*known vulnerabilities*)
- Connectivity of many control systems and control devices via, through, within, or exposed to unsecured networks (*Internet included*)
- Implementation constraints of existing security technologies and practices within the existing control systems infrastructure (*oldness of ICS*)
- Widespread availability of technical information about control systems on the WWW (*de-classified info*)

Security issues in I.C.S.

Causes of increased cyberattack risk to ICS

- Adoption of simple login procedures to allow for quick reaction during critical situations
- Use of the same User ID and PSWD to remote operation and maintenance of many devices
- Share the same profile (User ID and PSWD) among different operators
- Allow dealers to access plant devices for technical purposes

Security issues in I.C.S.

Cyberattack type to ICS

- Modify or block the information flow in the control network
- Change the parameters or the algorithms in the controller
- Send false information to the supervisory system to induce wrong action by the operators
- Modify or alter control system software or firmware such that the net effect produces unpredictable results
- Interfere with the activity of the safety system
- Direct modification of the codes in unsurveilled remote units

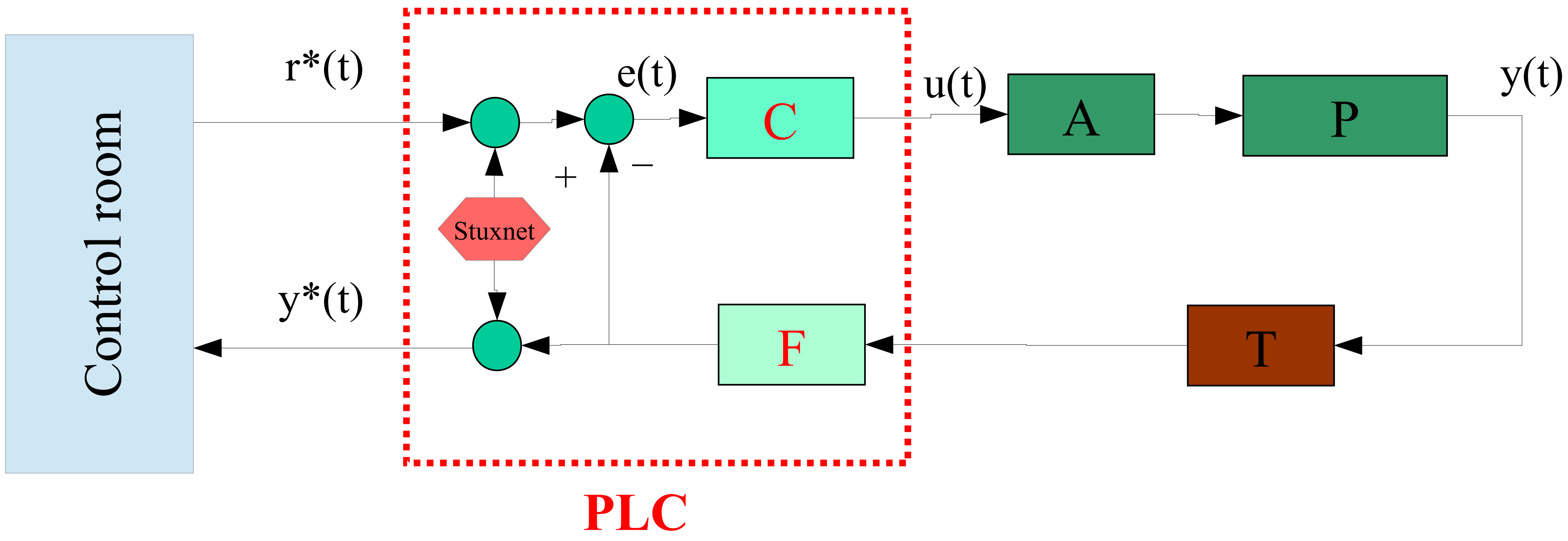
Security issues in I.C.S.

Cyberattack type to ICS: ***the* Stuxnet *example***

- Stuxnet is a worm + rootkit + link
- Exploit some weakness of Windows operating system
- Interfere with and changes the control code of Siemens PLC and control sytsem (WinCC, Step7, S7-300)
- Hide itself from antivirus and from operator supervision
- Spred itself through the network to control systems based on Siemens software (WinCC, Step7)

Security issues in I.C.S.

Cyberattack type to ICS: ***the Stuxnet example***



Security issues in I.C.S.

Cyberattack type to ICS

Internal: due to careless behaviour of the users

External: due to structural weakness of the system

↓

Different and properly designed counter-measures

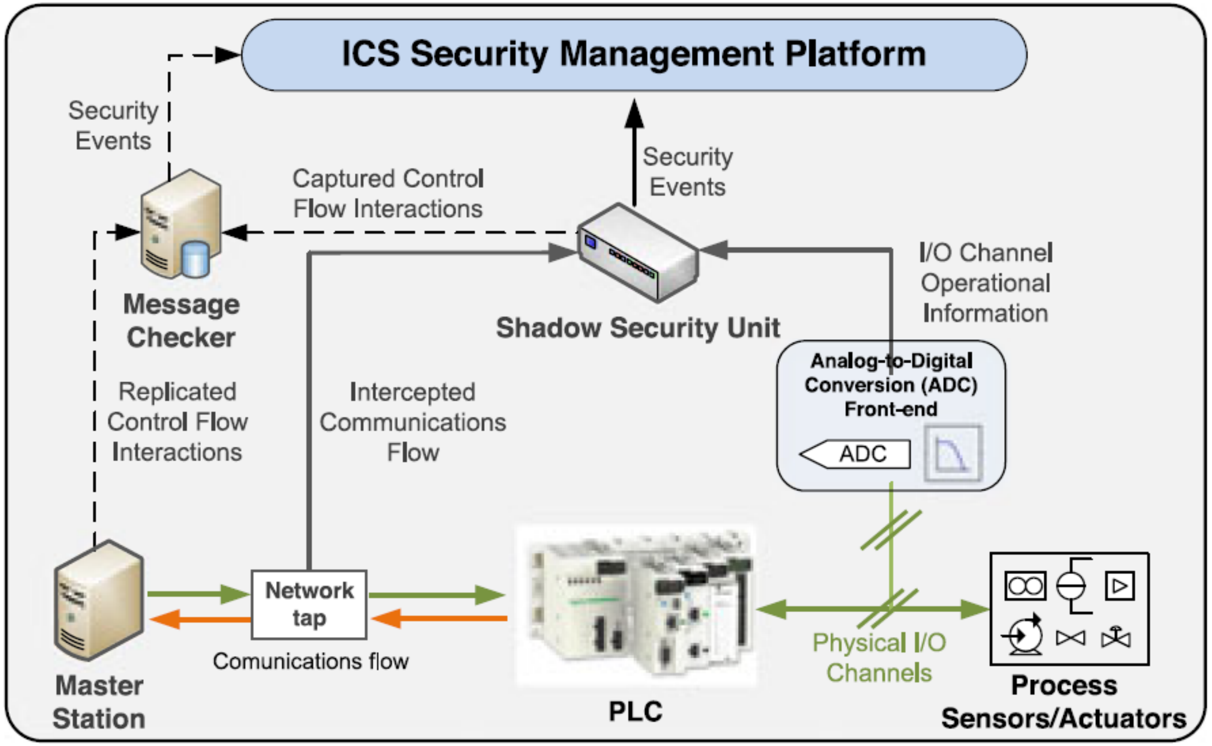
Security issues in I.C.S.

Countermeasures to decrease the cyber-intrusion risk

- Network segregation/separation (air-gap)
- Check and analysis of the connections
- Check and track logins
- Compartimental design of the system
- Analysis of the network trafic
- Continuous update of the OS and of the applications
- Check of the memories integrity
- Implementation of anti-virus/malware, firewall softwares
- Installation of proxy devices

Security issues in I.C.S.

Additional structures for diagnosis and monitoring are needed



A system for diagnosis is addeded to continuously verify the congruence of the data transmitted in the control network among PLC/DCS/SCADA and RTU