Concept of Industry 4.0: some challenges and means

Asean-Factori 4.0 project

Grenoble, 26th May 2021

jean-marc.thiriet@univ-grenoble-alpes.fr

UGA-1-a-Description of the Main Industrial sector using PLC
UGA-1-b-Maintenance,
UGA-1-c-Logistics & Organisation
UGA-1-d-Production
UGA-1-e-Supervision
UGA-1-h-Robotics applications in Industry 4.0; Vision
UGA-1-f-Some concepts of Dependability/Safety
UGA-1-g-Risk analysis

Condensed CV

jean-marc.thiriet@univ-grenoble-alpes.fr

UGA Université Grenoble Alpes

Docteur (Ph.D.) Université Henri Poincaré Nancy 1: February 1993

* Associate Pr. Université Henri Poincaré Nancy 1 1993-2005
* Habilitation à Diriger des Recherches UHP-Nancy 1: December 2004
  DEPENDABILITY OF INTELLIGENT DISTRIBUTED CONTROL SYSTEMS
* Full Professor Univ. Grenoble Alpes since 2005
  Head of the GIPSA-Lab Research Lab (April 2011-December 2015)
  Research in the dependability of automation systems which integrates communication networks (Networked Control Systems) and cyber-security of cyber-physical systems (smart grids, drones)
  Teaching in networks, network security, signal processing, automatic control
  Education projects
  - Asean-Factori 4.0
  - SALEIE: Strategic ALignment of Electrical and Information Engineering in European Higher Education Institutions

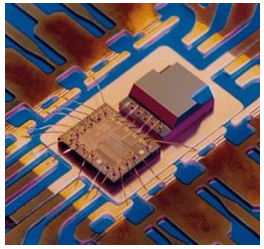
At the heart of Europe

Institut de Technologie du Cambodge

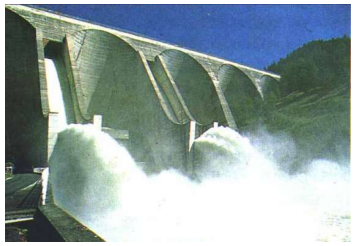
Grenoble
3h by train from Paris
1h40 by car from Geneva

Dynamic environment
Population: 680,000
60,000 students,
15% of which foreigners

Some Fields of research in Grenoble (70 Research Centres)



Smart systems
Nano-techno
Energy
Water
Environment
Transportation



5 International laboratories and instruments

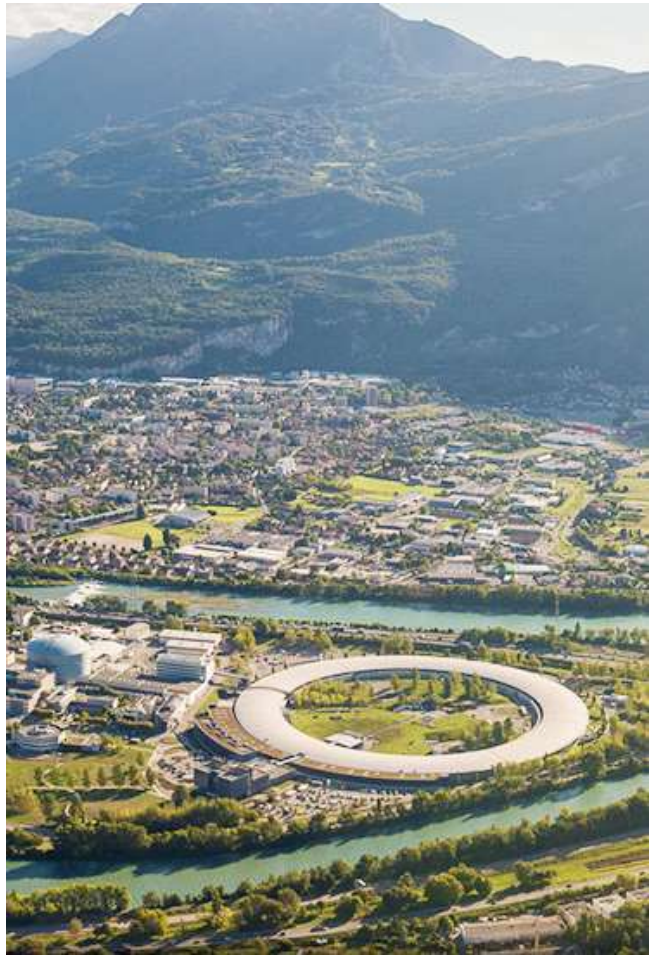
- ESRF, ILL, EMBL, GHMFL, IRAM

8 National research organizations

- CNRS, CEA, Inria, Inserm, INRAE, CRSSA, IRD, CHU Grenoble Alpes

Major companies

- Sun Microsystems, HP, Orange, STMicroelectronics, Schneider Electric, Alstom, Xerox, Thales…



UGA facts and figures

- **60,000** students
- **3,400** PhD students (45% international)
- **7,500** employees, of which
  - **5,500** academic
  - **2,000** staff
- **€ 512m** budget per year
- **82** laboratories
- **100**+ research centers
- **1** teaching hospital
- **175** hectares of campus

Outline of the presentation

1. Description of the Main Industrial sector using PLC - Industry 4.0
2. Challenges: Safety & Cyber-security
3. Maintenance
4. Logistics & Organisation
5. Production
6. Supervision
7. Robotics in Industry
8. Conclusion
9. References

1. Description of the Main Industrial sector using PLC

Industry 4.0

From Industry 1.0 to Industry 4.0…

Industry 1.0 : mechanization, mechanical energy (water, steam), ex: agriculture , XIXth century

Industry 2.0 : mass production, electricity, ex: car factory
~from 1920s to 1970s

Industry 3.0 : automation (robots) => First PLCs (Programmable Logic Controllers)
computer, ex: pharmacy, food, 1980

Industry 4.0 : Cyber-physical systems, communication (virtual tools: Cloud), ex: smart cities, Nowadays

From Industry 1.0 to Industry 4.0…

Purposes: Production, minimal cost

- Production strategy => to product
- Maintenance strategy => to take care of the production tools
- Logistics and organization strategy => to organize production and maintenance in the best way

Industry 4.0: some challenges

Certification

Organisation

L'usine du futur devrait faire la part belle à la 5G plutôt qu'aux réseaux LPWAN. Ces derniers pourront servir cependant à l'optimisation des bâtiments.

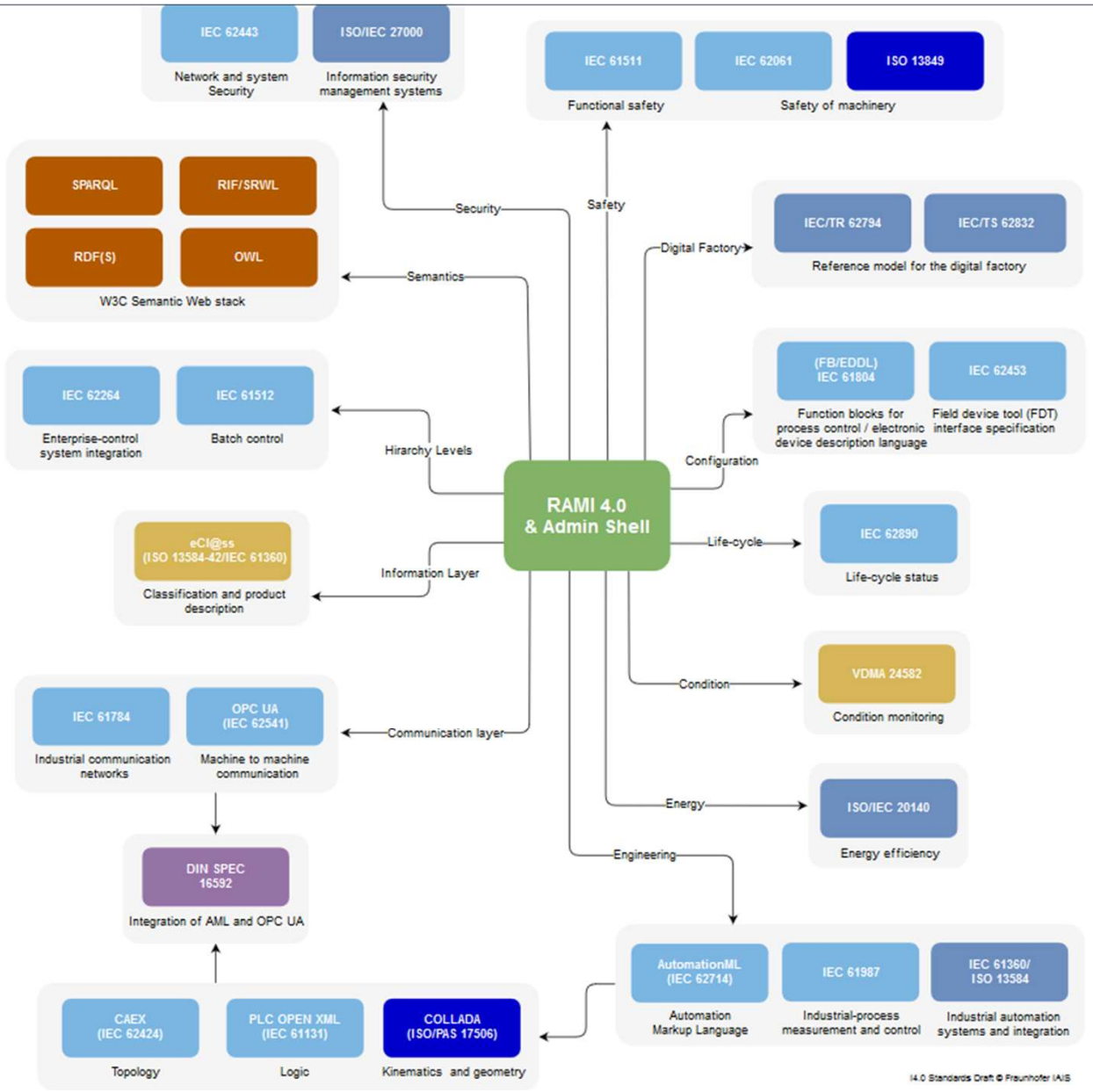
« New » networks: 5G

Certification

Standards…

State of the Art
Best practises
In security

Quality
Assurance
processes



PLC (Programmable Logic Controller)

Digital Inputs (0/1)

Digital Outputs (0/1)

Analog Inputs and Outputs
(from ex: Vmin to Vmax)

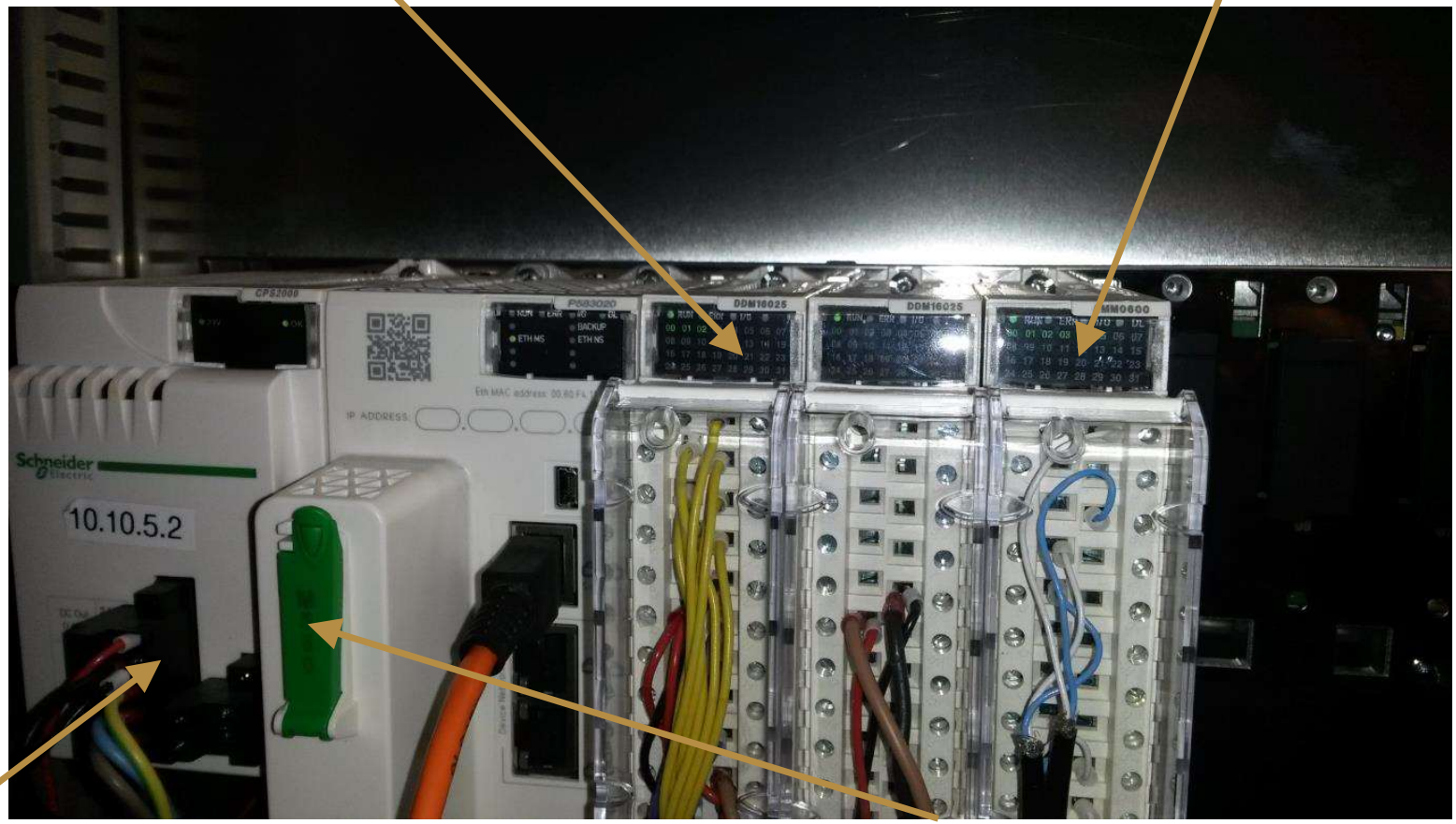
Free slots

Power Unit

Central Unit + Communication Interfaces
(Ethernet and CAN (fieldbus))

Digital Inputs and Outputs

Analog Inputs and Outputs



Power Unit

Central Unit + Communication Interfaces
(Ethernet and CAN (fieldbus))

The first PLC, model 084, was invented by Dick Morley in 1969

The "084" - Details

The **"084"** consisted of three major components mounted on two vertical rails, one of which was hinged to allow for service access to the front and back.

Ladder Logic:

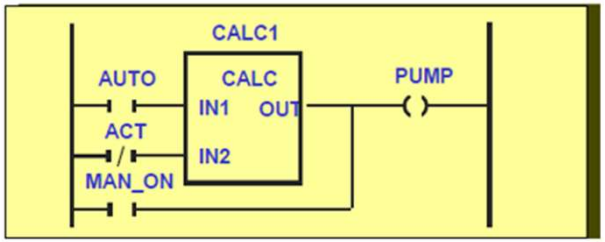
The use of **Ladder Logic** was significant in the rapid acceptance of the **"084"** because the very same engineers and electricians who designed and maintained Factory Automation Systems could also program an **"084"**. Ladder Logic was simply an electronic version of the elementary electrical diagram that they already used -- not the case for other types of control systems being designed at the time.

PLC Languages: IEC 61131

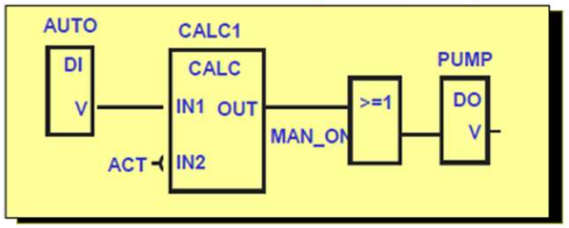
Instruction List (IL)

```
A: LD   %IX1 (* PUSH BUTTON *)
   ANDN %MX5 (* NOT INHIBITED *)
   ST   %QX2 (* FAN ON *)
```

Ladder Diagram (LD)



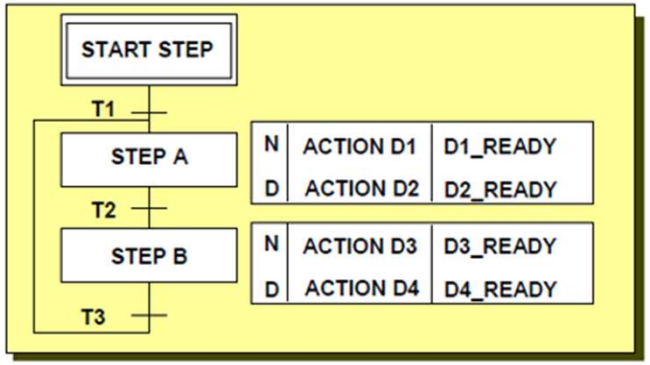
Function Block Diagram (FBD)



Structured Text (ST)

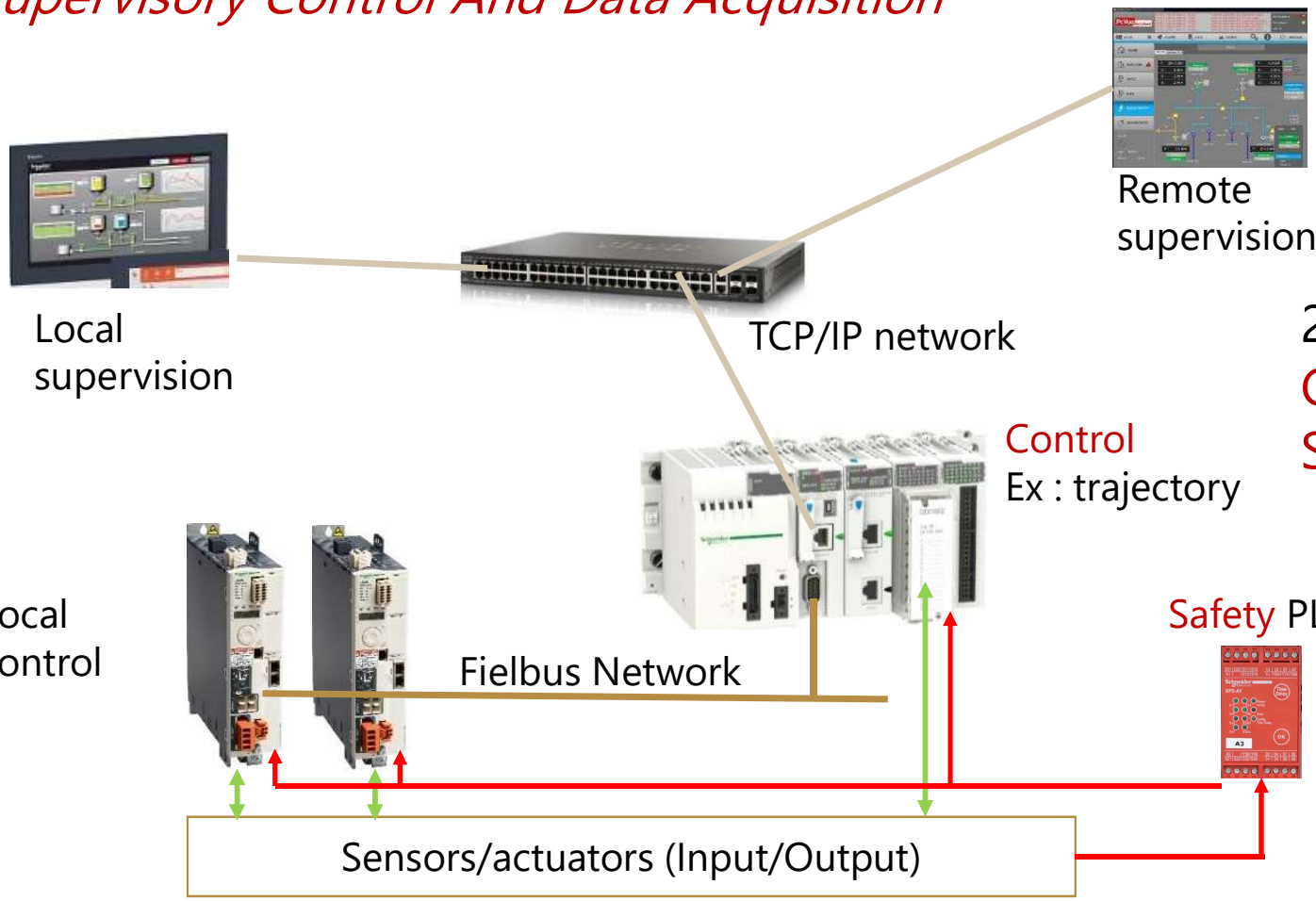
```
VAR CONSTANT X : REAL := 53.8 ;
Z : REAL; END_VAR
VAR aFB, bFB :  FB_type; END_VAR

bFB(A:=1, B:='OK');
Z := X - INT_TO_REAL (bFB.OUT1);
IF Z>57.0 THEN aFB(A:=0, B:="ERR");
ELSE  aFB(A:=1, B:="Z is OK");
END_IF
```

Sequential Flow Chart (SFC)



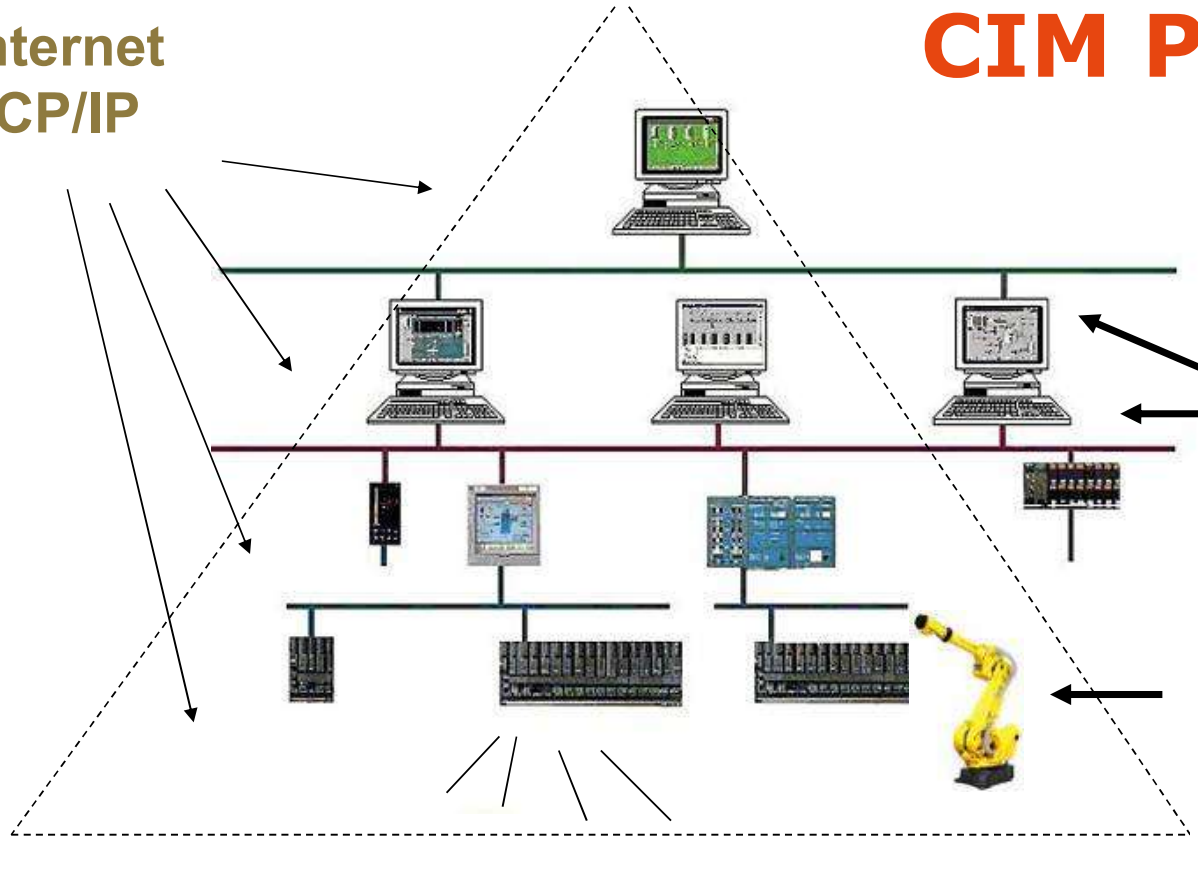
An example

SCADA: Supervisory Control And Data Acquisition



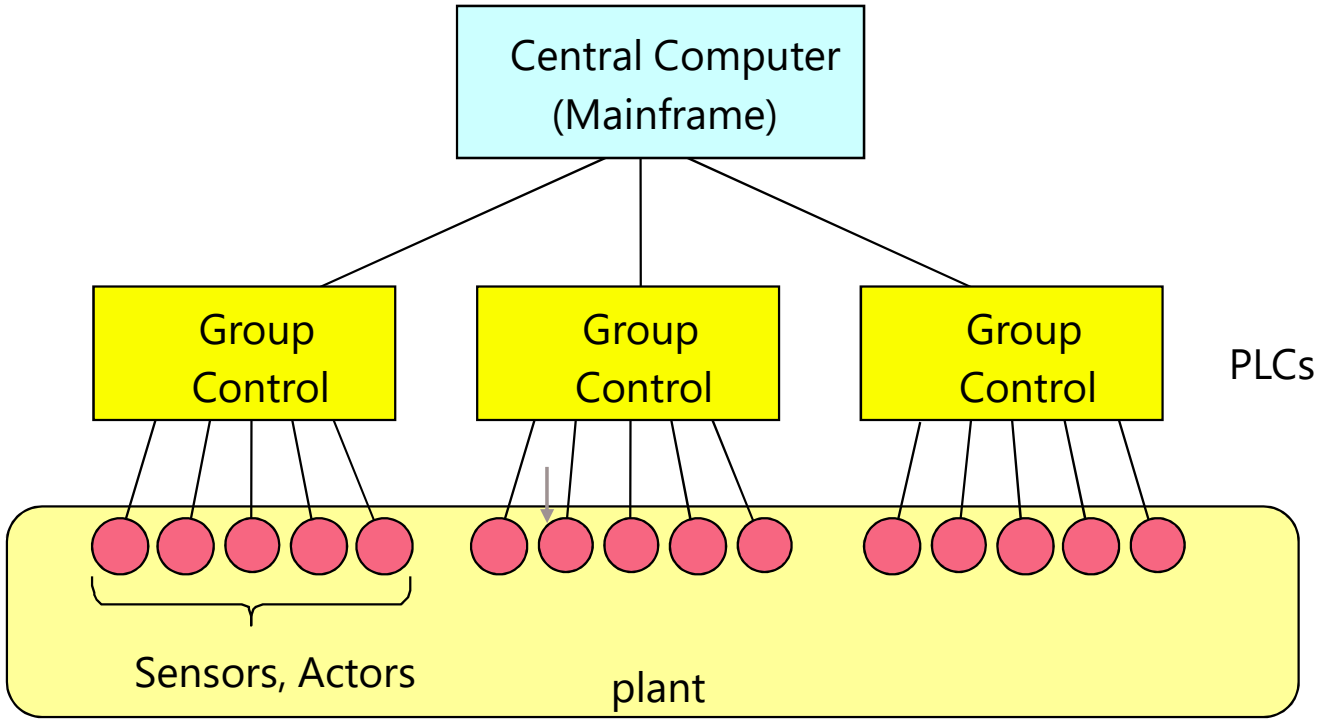
2 important aspects:
Control
Safety

CIM Pyramid



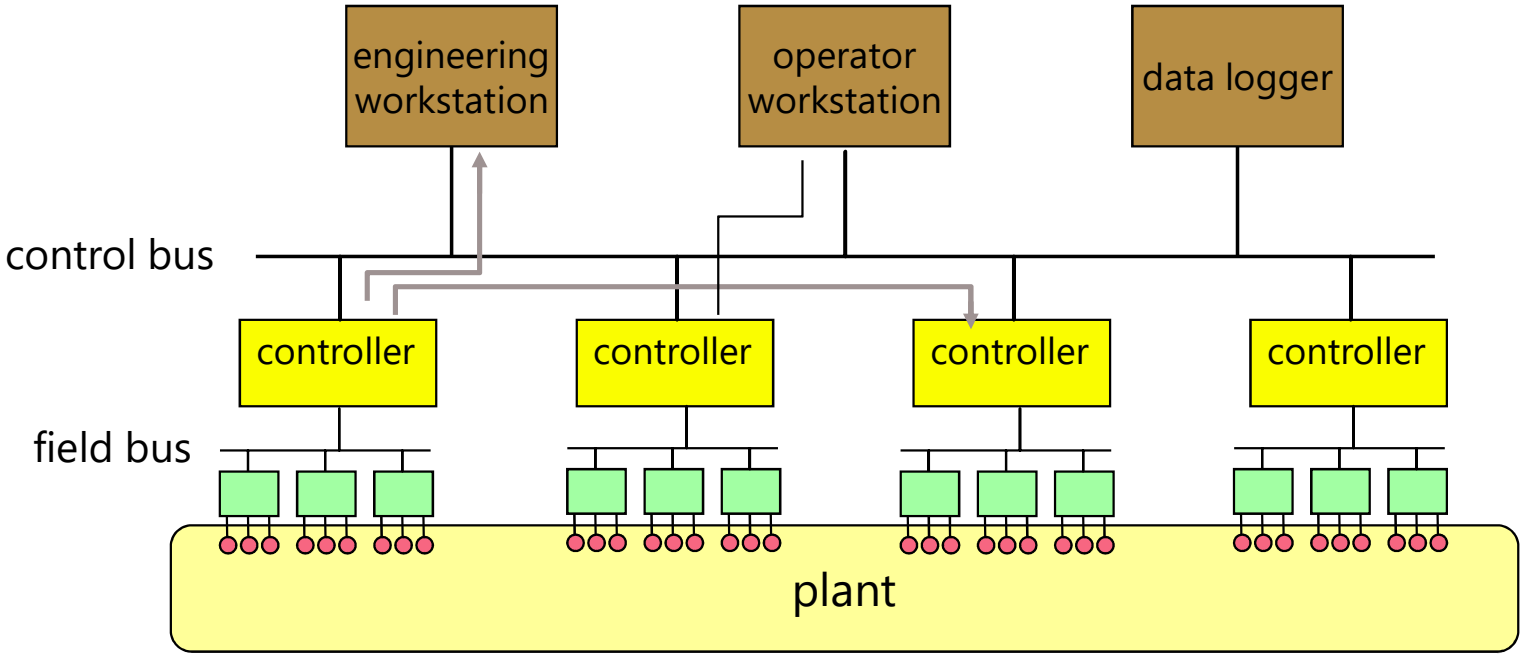
Computer-integrated manufacturing (**CIM**)
Describe the complete automation of manufacturing processes
Several network layers

Centralized Control Architecture



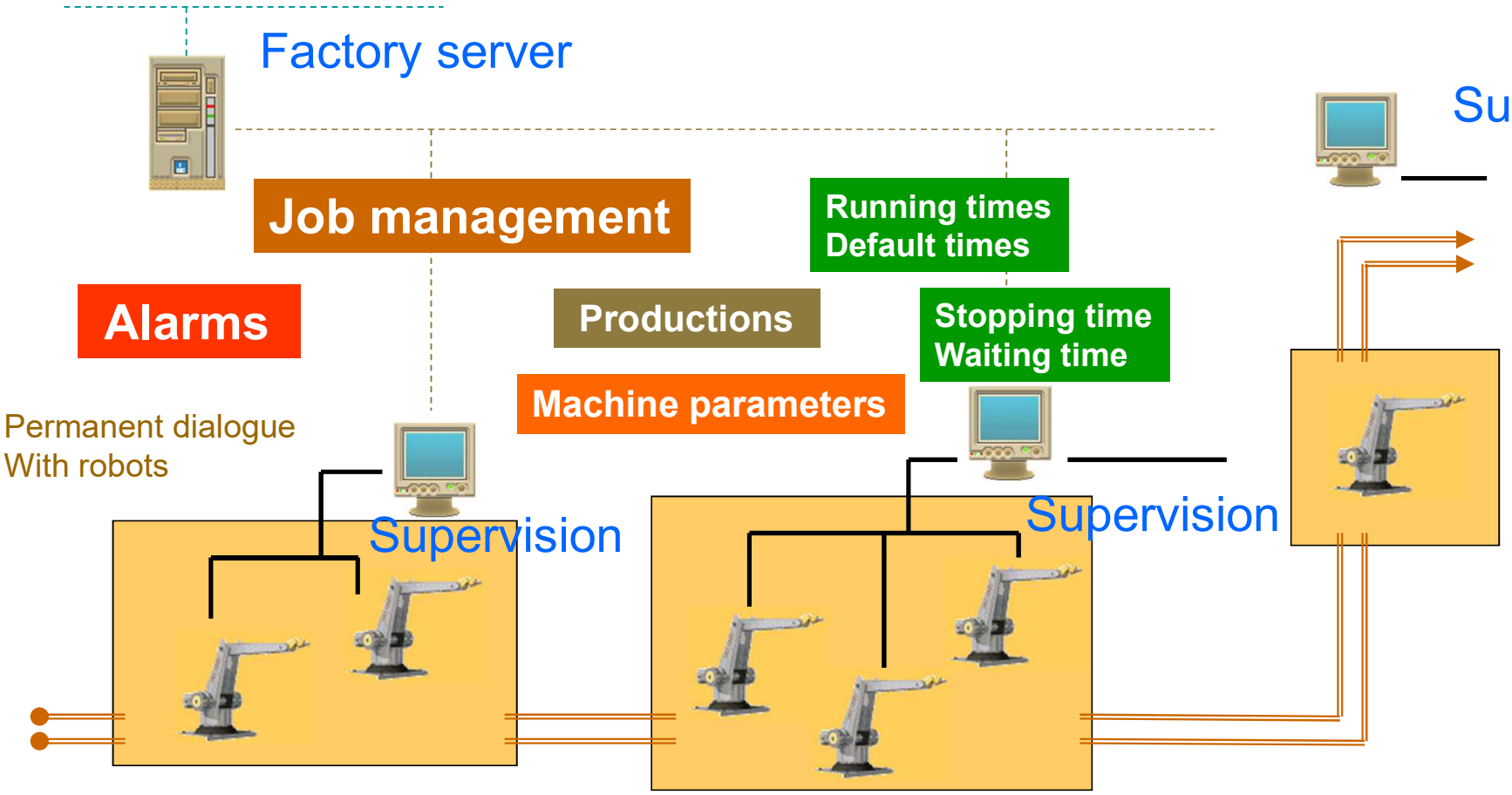
Classical, hierarchical, centralised architecture.
The central computer only monitors and forwards commands to the PLCs

Decentralized Control System (DCS)



All controllers can communicate as peers (without going through a central master), restricted only by throughput and modularity considerations.

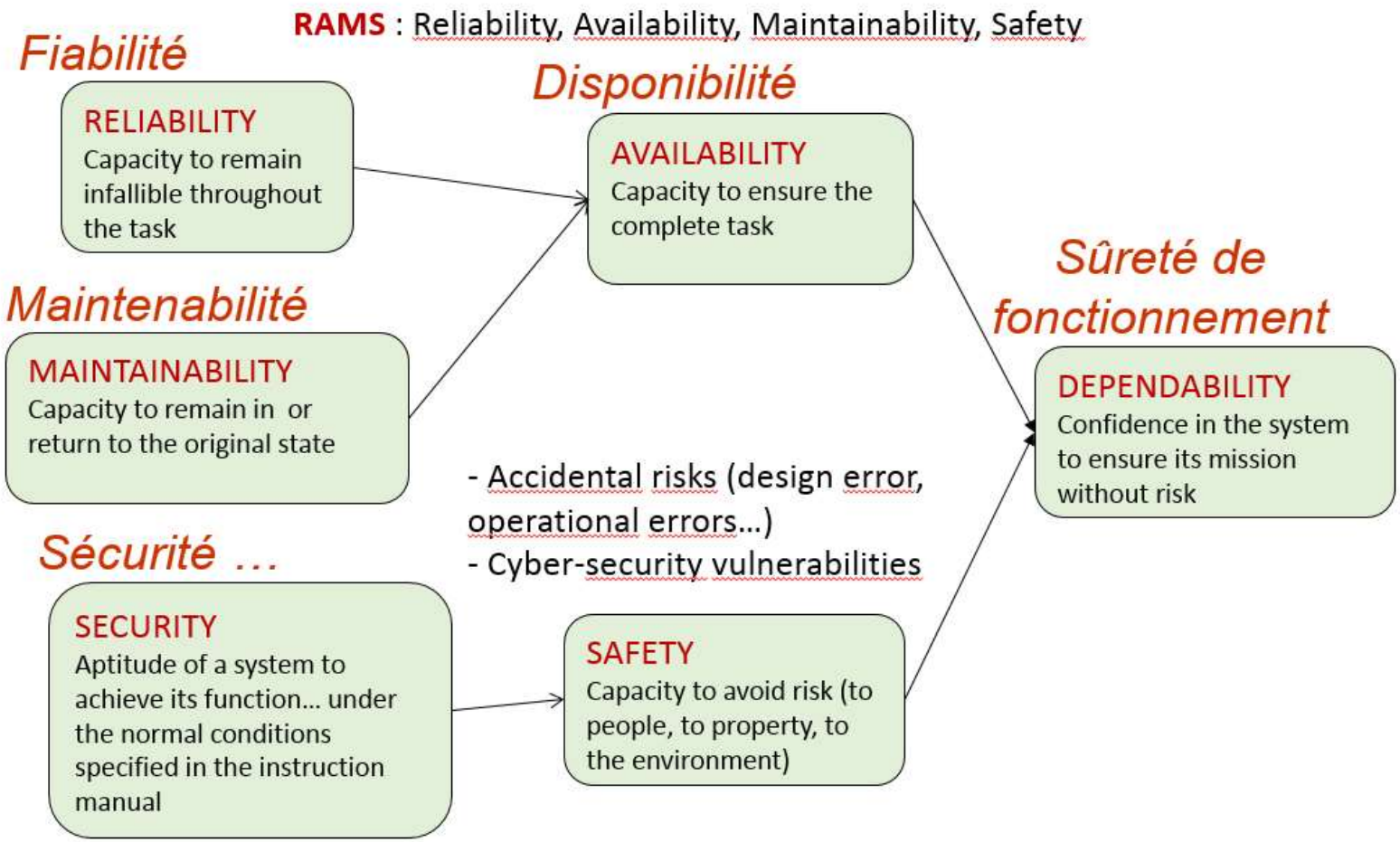
Supervision



Supervisors
Collect and process information from the robots
Basis of the factory's information system

2. Challenges: Safety & Cyber-security

Dependability



Some dependability parameters

MTTF: Mean Time To Failure: average duration before a failure occurs ; mathematical expectation of the operating time before failure

MTBF: Mean Time Between Failures, average uptime ; mathematical expectation of the service life

MTTR: Mean Time To Repair (Recovery, Restoration), average downtime or average time to restore to working order ; mathematical expectation of downtime

$$MTTF = \int_0^\infty R(t)dt \qquad MTTR = \int_0^\infty [1 - M(t)]dt$$

R(t) : probability that the system stays in the operating state without failure over the entire time interval (0,t>.

M(t) : probability that the system will be restored within a specified period of time *t*.

Safety
= the Science of Failures

- Failure: interruption of the capacity of an entity to carry out a necessary function
  - The function concerned should be defined
    - ex 1: to ensure communication between two sites
    - ex 2: to ensure the accessibility of data (locally and remotely)
  - the criterion of interruption of this function must be specified
    - ex 1: QUANTITATIVE: the flow is ≤ a certain %age of a reference value
    - ex 2: QUALITATIVE: the loss, or irremediable destruction of strategic data for the company

Safety
= Risks Analysis => Risk Management

- **To Identify** failures in a more exhaustive manner
  - Crashing of hardware disks
  - Burning down, or flooding of premises containing backups
  - Open ports on a network
- **To evaluate the severity** of each failure (level of risk)
- **To envisage** the failures (use of evolution models)
  - 'Outdatedness' of the data-processing components
  - Probability of attacks by third parties on vulnerable ports
- At each **observation** of a failure, we should associate the appropriate **measurement** (statistical) => to improve the forecasting models
- **To control the** failures
  - Reduction of their frequency
  - Preventive measures against the consequences (reduction of the impact)
  - Tolerance

Elements of risks (Asset)

- Asset (*actif*)
  - Represented by monetary value
  - Anything of worth that can be damaged, compromised, or destroyed by an accidental or deliberate action
  - A asset's worth is generally far more than the simple costs of replacement (image, legal issues…)

Elements of risks (Threat)

- Threat (*menace*)
  - Potential event that, if realized, would cause an undesirable impact
  - Two factors plays in the severity of a threat: degree of loss and likelihood of occurrence
    - Exposure factor: degree of loss (percentage of asset loss if a threat is realized) – ex: if we estimate that a fire will cause a 70 % loss of asset values if it occurs, the exposure factor is 70 % or 0.7
    - Annual rate of occurrence: likelihood that a given threat would be realized in a single year in the event of a complete absence of control – ex : if we estimate that a fire will occur every three years, the annual rate of occurrence will be 33 %, or 0.33
    - => A threat can be calculated as a percentage by multiplying the exposure factor by the annual rate of occurrence. Ex : 0.7*0.33 = 0.231 or 23.1 %

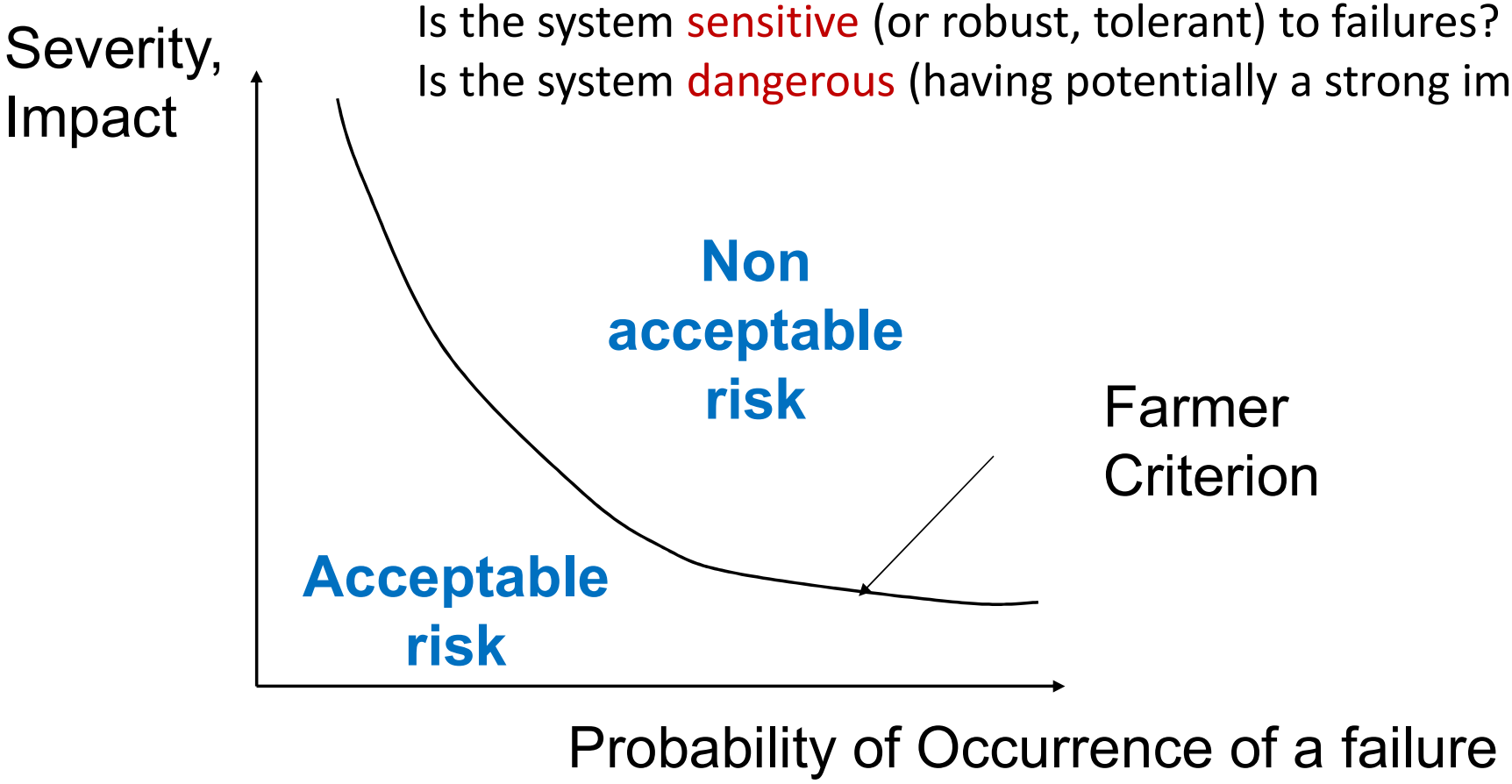
Elements of risks (Vulnerability)

- Vulnerability (*vulnérabilité*)
  - Absence or weakness of cumulative controls protection in a particular asset
  - Estimated as percentages based on the level of control weakness
  - Control Deficiency (cd) is calculated by subtracting the effectiveness of the control by 100% - ex : if we estimate that our industrial espionage controls are 70 % effective, so 100 % - 70 % = 30 % (CD)

  - Most of the time, more than one control is employed to protect an asset.
  - Ex : the threat is an employee stealing trade secrets and selling them to the competitor
  - To address this threat, we may:
    - implement an information classification policy,
    - monitor outgoing e-mails,
    - prohibit the use of portable storage devices,
    - …

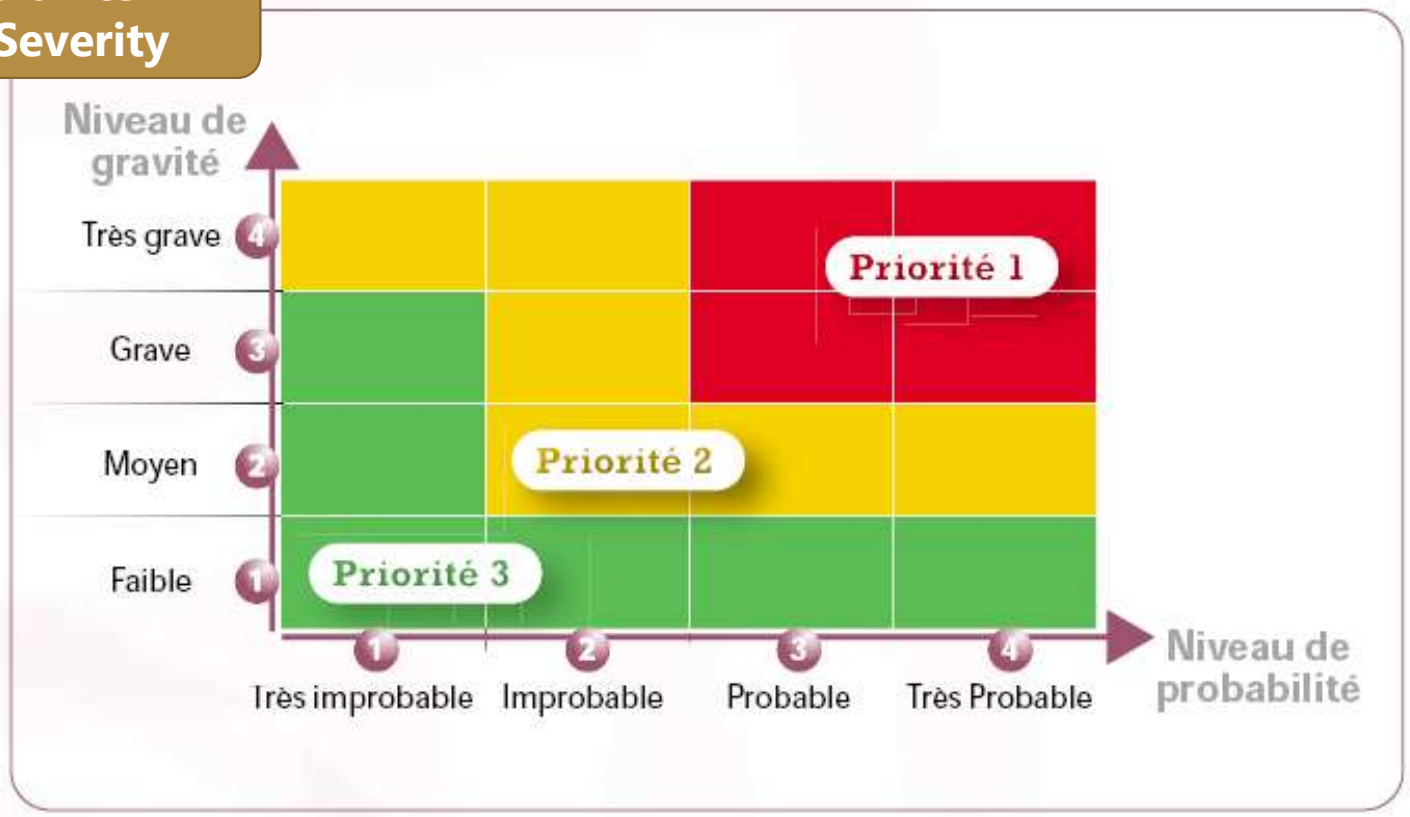
Severity-probability law

Is the system sensitive (or robust, tolerant) to failures?
Is the system dangerous (having potentially a strong impact) ?



Risks evaluation, evaluation of the severity

Gravité = Severity



Example

Danger (cause)	Dange-rous situa-tion	Dangerous event	Risk of…	Consequence	Severity	Probability	Priorities	Observations
Explo-sion of a tyre	Car sliding	Screw in the tyre	Accident	Killing people in the car	4 (high)	1 (low)	2 (int.)	Having a sparewheel …

Prescriptions, Methods for risk analysis

- **Methods**

1. FMEA (Failure Mode and Effect Analysis)/AMDE
2. HAZOP (Hazard and Operability Study)
3. Preliminary Hazard Analysis
4. MEHARI (Method for Harmonized Analysis of Risk) (FR, CLUSIF)
5. EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité, FR, ANSSI)
6. OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation, US-CERT)
7. CRAMM (CCTA Risk Analysis and Management Method, UK CCTA (Central Communication and Telecommunication Agency))

- **Prescriptions**

1. US standard NERC-CIP-002-3 Critical Cyber Asset Identification
2. US standard NIST.IR 7628 Guidelines for smart grid security
3. ISA/IEC 62443 Security for Industrial Automation and Control Systems
4. EU efforts about smart grid security
5. ANSSI Classification method and key measures

Comparison between ICS and classical IT systems

IT Information Technogy

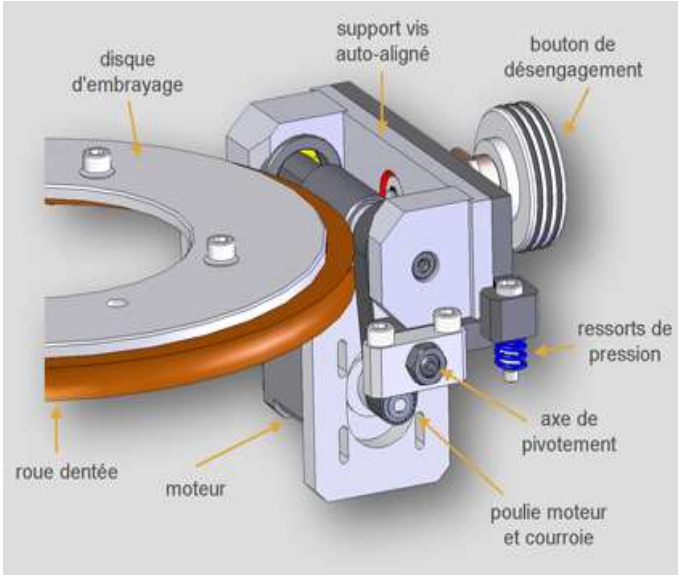
ICS Industrial Control System

Category	IT systems	ICS systems
Cyber security culture	Awareness of risks Methods and tools	Recent
Life duration	3-5 years	> 20 years
Performance	Throughput	Latency Real-time constraints
Resources	Abundant	Limited
Networks Protocols topologies	Numerous connection points Dynamic topologies	Fixed topologies “Simple” protocols Defined communication strategy, scheduling
Performances	Delays and jigs acceptable	Real time, critical time Strict time constraints
Availability	Some tolerance on degradations, depending on situations	High availability Inacceptable loss of connection (depends) Advance planning
Resource constraints	Available resources	Design for industrial processes Limited processing and memory resources
Targeted properties	Confidentiality Integrity Availability	Timeliness Availability Integrity Confidentiality

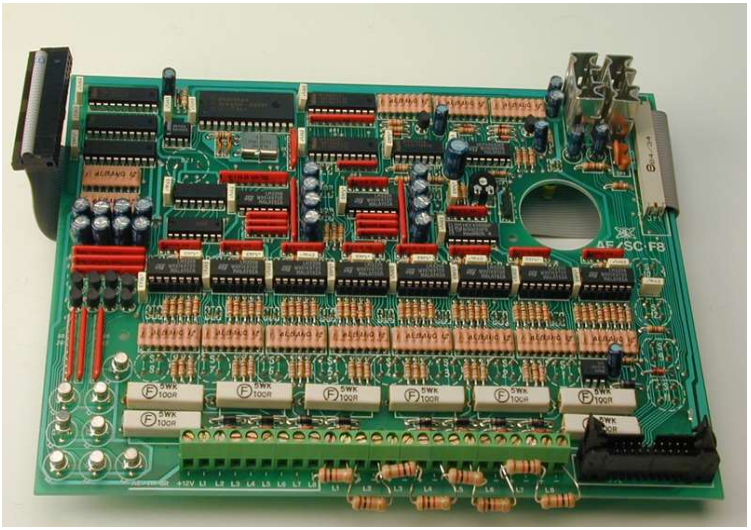
Dependability of classical Components

- System wear-out
- Topology (architecture) of the system
- « Average » use
- Permanent failures

Mechanical systems



• Electronic systems

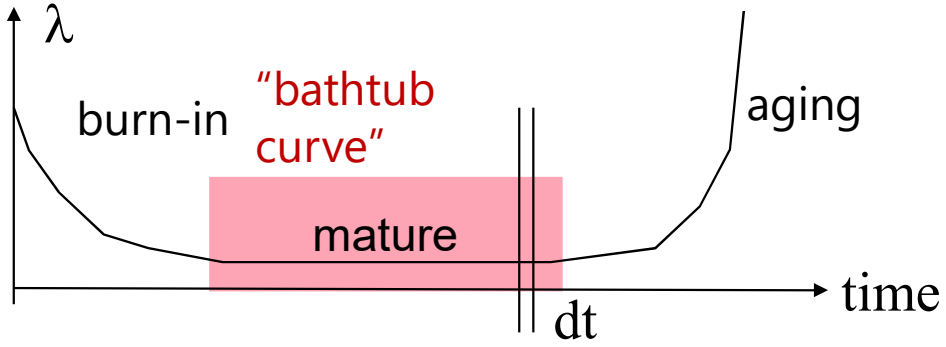


Ex: Reliability

Reliability **R(t)** = probability of one (initially good element) of not having failed until time t

Experiment: How many bulbs fail per time unit ?

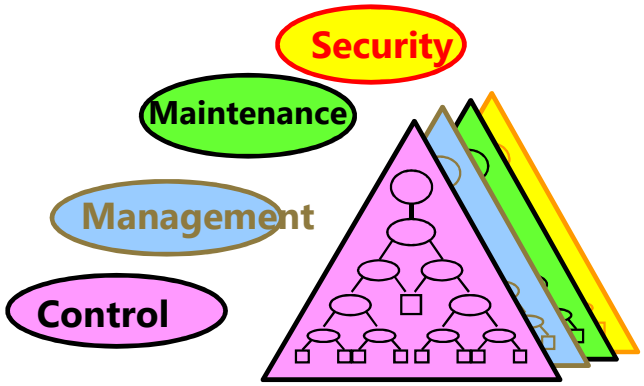
$$\lambda(t) = -\frac{dR(t) / dt}{R(t)}$$



Failure rate **λ(t)** = probability that a (good) element fails during the next time unit dt

Context: Automation system evolution

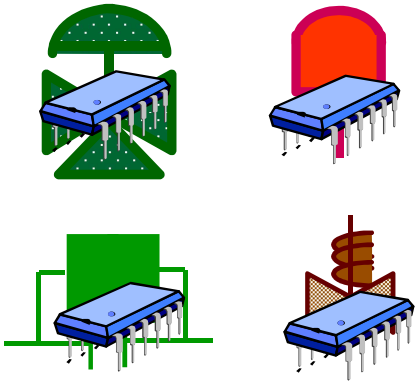
Needs:



Increased number of services

More complex architectures

Components :

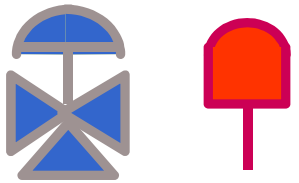


Various capacities and functionalities availability

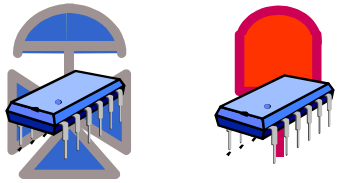
Dependability hard to evaluate and to qualify

From analog to digital and from smart to intelligent…

- Analog sensors and actuators
  - Hardware and analytical Redundancies
  - « Classiques" studies of dependability

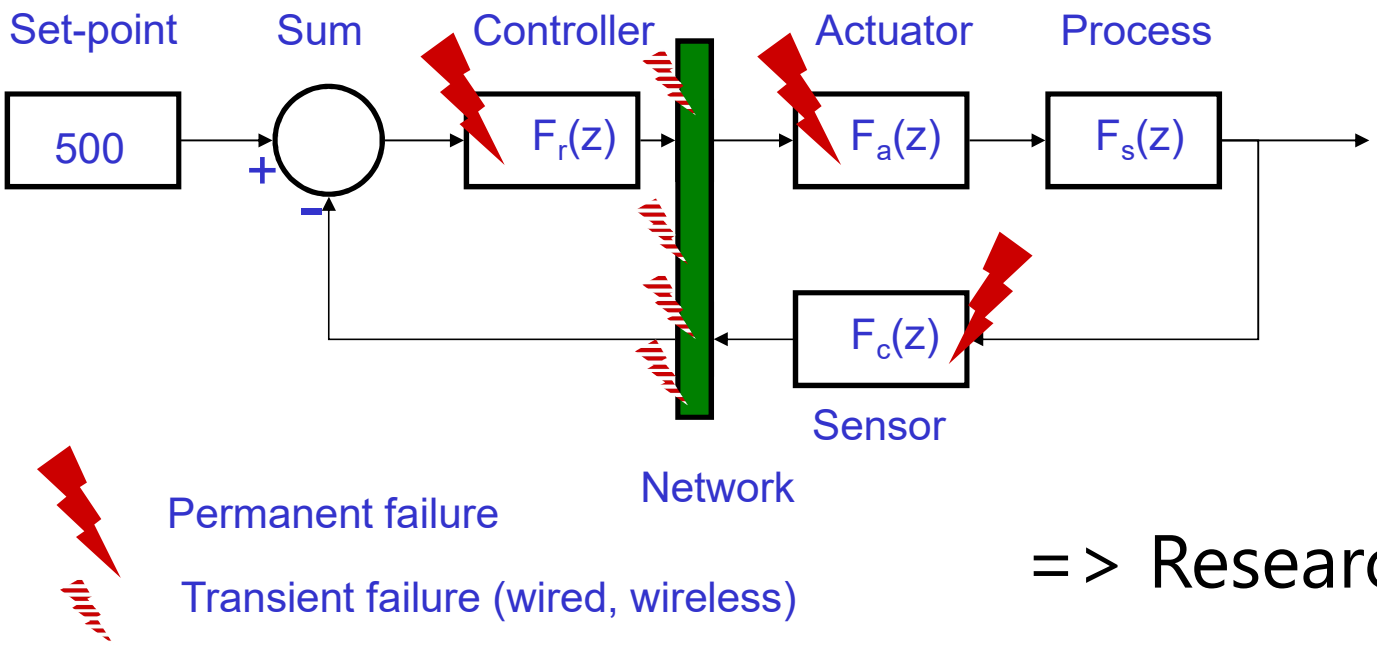


- Digital sensors and actuators
  - A/D Interfaces, processing units, delays…
  - Software, implementation



- « Smart » sensors and actuators
  - Embedded intelligence, local decision
- « Intelligents » sensors and actuators
  - Communicating Interface
  - Diagnosic, monitoring, checking, embedded decision
  - Instrument contributing of the global « intelligence » of the system
- Intelligence vs. Complexity => consequences on Dependability ?

Failures integration



=> Research aspects

Failure Modes
- Continuous/sampled
- Discrete events

Time scales
-Speed (modulation rate, throughput) of the networks
-System time constant
-Time between failures

Safety Integrated Level (SIL)

- Generic standard IEC-**61508**/IEC-61511

  Functional safety of electrical/electronic/programmable electronic safety-related systems

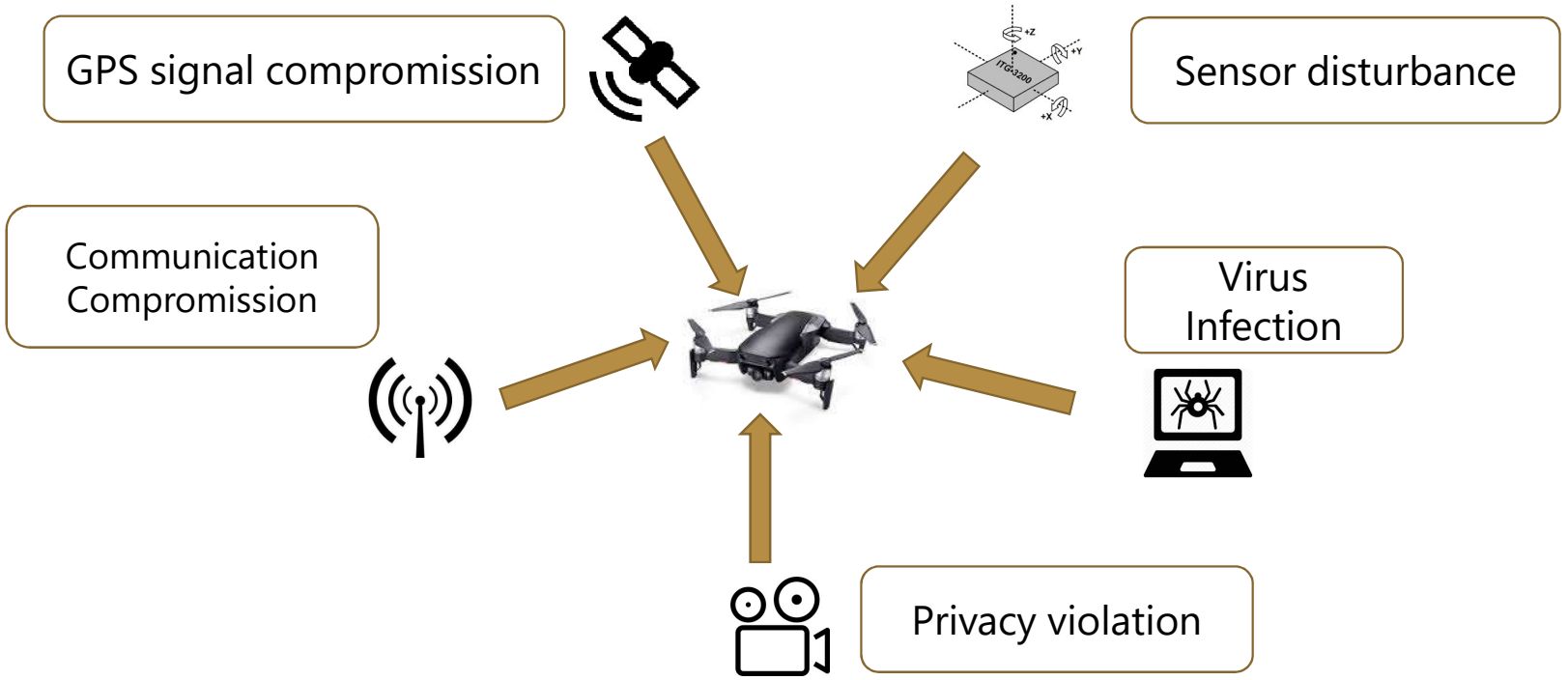
- SIL (*Safety Integrated Level*)

Problems:
- SIL of a component
- SIL of physical architecture
- SIL of a functional architecture
- SIL of a computer and network-based architecture

Prescriptions of a security system and corresponding SIL levels		
SIL	Demand operation Average **probability of failure on demand (PFD)** Failure rate per year	Continuous operation λ Failure rate per hour
SIL4	$10^{-4} < PFDavg < 10^{-5}$	$10^{-8} < \lambda < 10^{-9}$
SIL3	$10^{-3} < PFDavg < 10^{-4}$	$10^{-7} < \lambda < 10^{-8}$
SIL2	$10^{-2} < PFDavg < 10^{-3}$	$10^{-6} < \lambda < 10^{-7}$
SIL1	$10^{-1} < PFDavg < 10^{-2}$	$10^{-5} < \lambda < 10^{-6}$

Cyber-security of flying drones

Vulnerability of the drone:



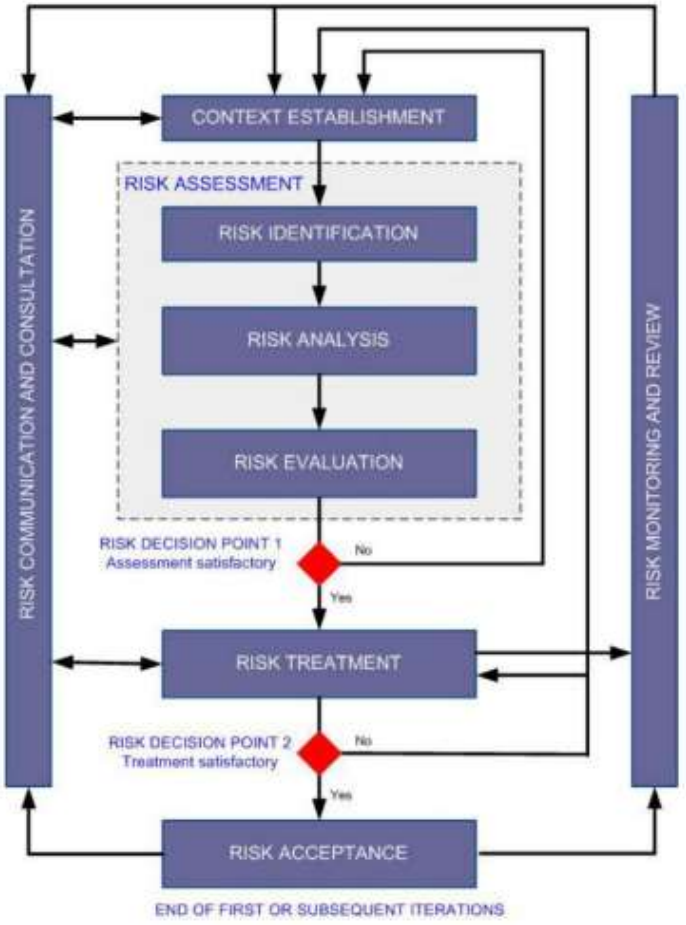
Need of a methodology to get a cartography of the drone security in a systematic way and to ensure completude

Ex: methodologies in the industrial domain

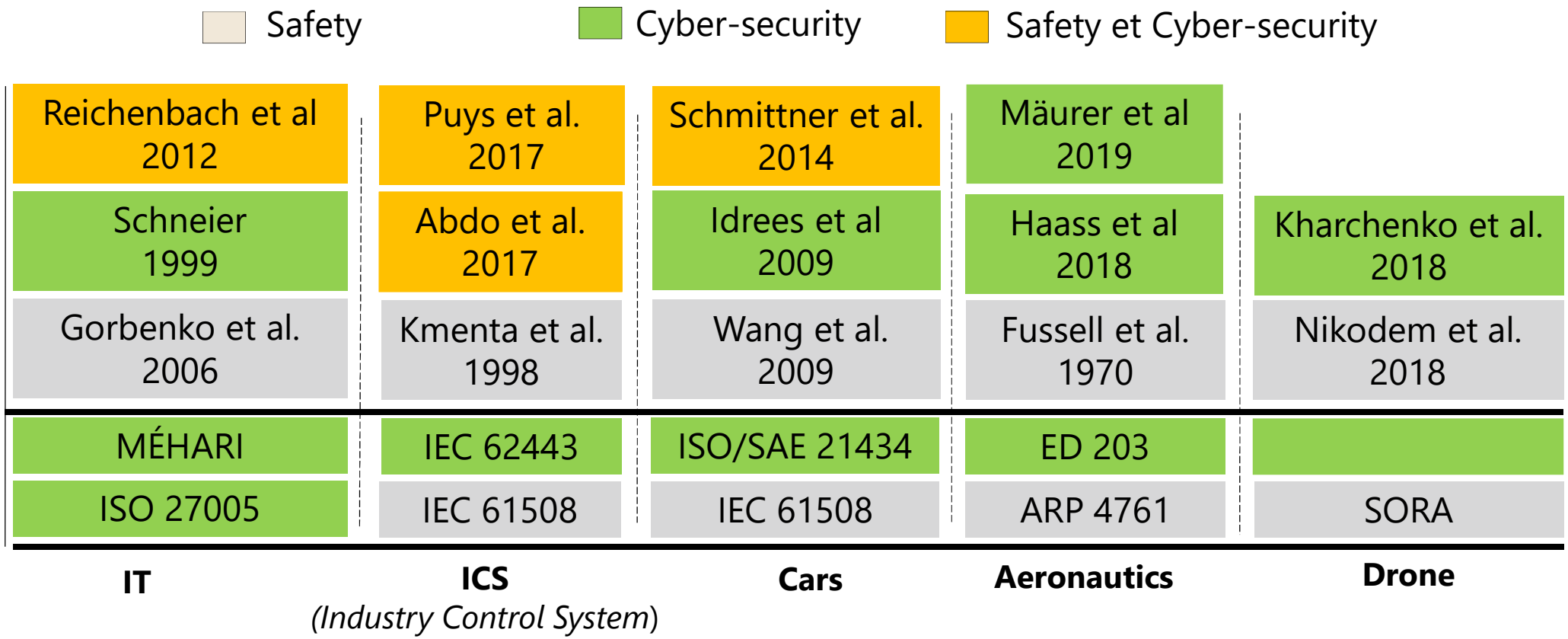
- **ISO27005 Standard**: Information security risk management
  Propose a work-flow

- **MEHARI[12]:**
  - IT Security in companies
  - Databases
  - Security Evaluation Tools

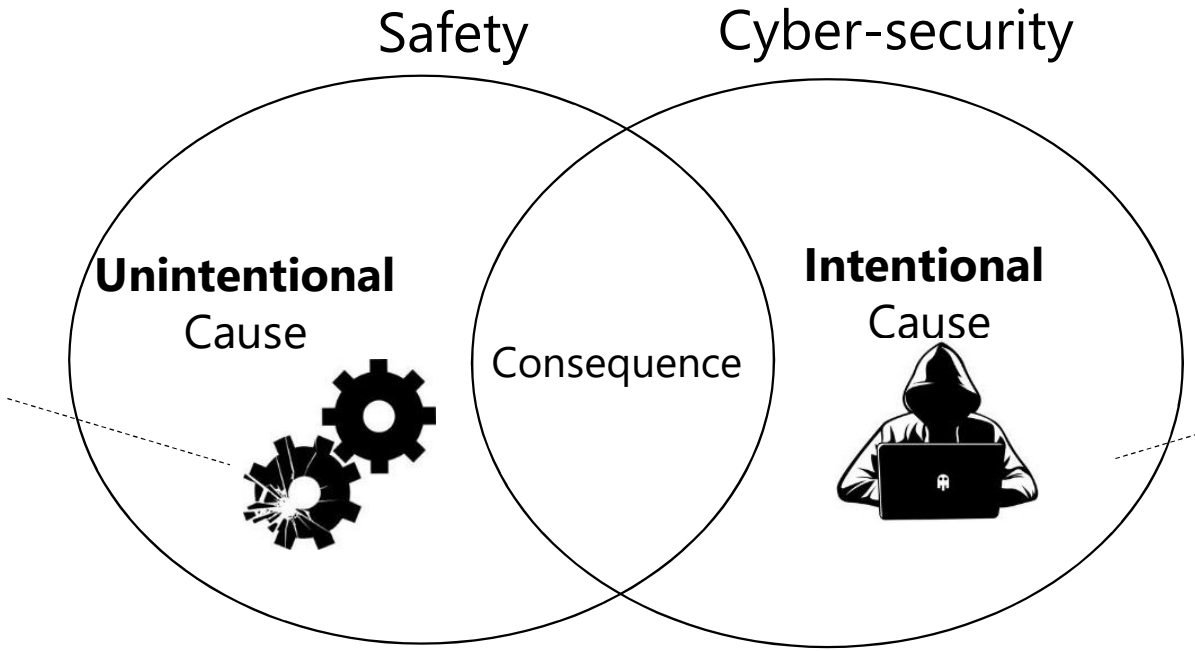
- **ED202A/DO326A Standard:**
  - Avionics security
  - During the processus of aircraft development



Risk Assessment: Safety and Cyber-security



Safety and Cyber-security



No one wants the "consequences" to happen

Someone wants the "consequences" to happen

Different **causes**, same **consequences**

3. Maintenance

Maintenance

According to the AFNOR (French standardisation) definition, maintenance aims at maintaining or restoring an asset in a specified state so that it is able to provide a specific service

Choice of a maintenance strategy

Depends on:

- Knowledge of the equipment, age, state and life span of these different devices
- Probability of breakdowns; low or high
- Ease of intervention
- Possession of spare parts
- The means available at the time of the intervention.
- **a-The events which are at the origin of the action**
- Reference to a schedule
- Subordination to a type of predetermined events (self-diagnosis, information of a sensor, measurement of a wear...)
- Appearance of a failure

Choice of a maintenance strategy

b-Maintenance methods that are respectively associated with them

- Corrective maintenance
- Systematic preventive maintenance
- Conditional preventive maintenance

c- The maintenance operations themselves: Inspection, control, troubleshooting, repair, overhaul, renovation, etc.

d- Related activities : Improvement maintenance, new works, safety, etc.

Maintenance methods

Choice between maintenance methods

- within the framework of the maintenance policy
- must be made in agreement with the company's management
- it is necessary to be informed of the management's objectives and of the maintenance policy decisions
- it is also necessary to know
  - the operation and characteristics of the equipment;
  - the behavior of the equipment in operation;
  - the conditions of application of each method;
  - the maintenance costs and the costs of lost production.

Corrective Maintenance

- **Definition**: Maintenance performed after a failure
- **Failure** : Alteration or cessation of the ability of an asset to perform the required function
  - **Partial** failure: Alteration of the ability of an asset to perform the required functions
  - **Complete** failure : Cessation of the ability of a good to perform the required function
- **Purpose**: to restore lost qualities necessary for the use of the equipment
- **Defects, breakdowns or various damages** requiring corrective maintenance lead to:
  - an immediate or very short term unavailability of the affected equipment
  - depreciation in quantity or / and quality of the services provided

Preventive Maintenance

- **Definition** : Maintenance performed according to predetermined criteria, with the intention of reducing the probability of failure of an asset or the degradation of a service rendered
- Avoid failures of the materials during use =>cost analysis must show gain
- Goal of preventive maintenance
  - Increase the life of the equipment
  - Decrease the probability of in-service failures
  - Reduce the downtime in case of overhaul or breakdown
  - Prevent and also foresee costly corrective maintenance interventions
  - Allow to decide the corrective maintenance in good conditions
  - Avoid abnormal consumption of energy, lubricants, etc.
  - Reduce the maintenance budget
  - Eliminate the causes of serious accidents

4. Logistics & Organisation

Interest of logistics for companies

- Strong influence on activity
- Transversal function concerning all departments
- Allows Depts to be linked as efficiently as possible
- Part of the value chain

- Competitiveness tool
  - improve the coordination of the company's services
  - mobilize services to pursue a common objective
    - customer satisfaction
  - In some sectors, logistics can be a competitive advantage.

Objectives
- short term: optimization of daily physical flows
- medium to long term: implementation of action plans to optimize production and storage parameters

Management of logistics

Logistics = managing everything that concerns the transport and storage
- vehicles needed for transport,
- company suppliers,
- warehouses,
- handling...,
- optimizing their circulation to minimize costs and delays.

Carried out thanks to the company's information systems. To be efficient:
- Use a clear and identical coding for each function of the company
- Use the remote transmission of information

The objective of the company's logistics function is to coordinate the products in circulation so that the products circulate continuously (to reduce delivery times) and to group the products together (to reduce costs).

Management of logistics

The company's logistics chain manages flows as efficiently as possible to reduce the following main costs: procurement costs, routing costs, production costs, storage costs.

Logistics management relies on indicators to measure the performance of the system in place and to detect the points on which the company must improve, such as

- For supplies: availability rate and delivery times
- For warehousing: monitoring of stock value, loss of value and stock coverage
- For transport: average cost per product and filling rate of the means of transport

5. Production

Production

Industrial production has three interacting elements:
The CUSTOMER has an immediate or deferred NEED for a PRODUCT made by the COMPANY.

Basic definitions
- COMPANY: The standard [AFNOR, FR] defines the company as a "System directed and organized in services whose purpose is to generate added value".
- CUSTOMER: In the same source, the customer is: "The person or entity for whom the product was designed for".
- PRODUCT: The Value Analysis presents the product as "what is (or will be) provided to a customer to meet his need" [AFNOR]. This definition therefore corresponds to the final product marketed by the company.

Production: needs

- CAPACITY: The CAPACITY of a resource is the maximum quantity of work units that can reasonably (or theoretically) be achieved in a given time period and under certain within the framework of certain working hypotheses.

Example:

- Bottling line with a capacity of 6000 bottles/hour.
- Numerically controlled lathe with a capacity of 36 hours/week.
- LOAD: The LOAD of a resource corresponds to a planned demand over a given period of time

period and expressed with the same unit as the capacity. For a given resource, the load must of course be less than or equal to the capacity.

The definition of the PRODUCT presented it as corresponding to the NEED of a CUSTOMER. For the company, two situations can arise, depending on whether the product corresponds to :

- an immediate NEED, which means that the delivery time acceptable to the customer is zero

6. Supervision

Exemple de SCADA

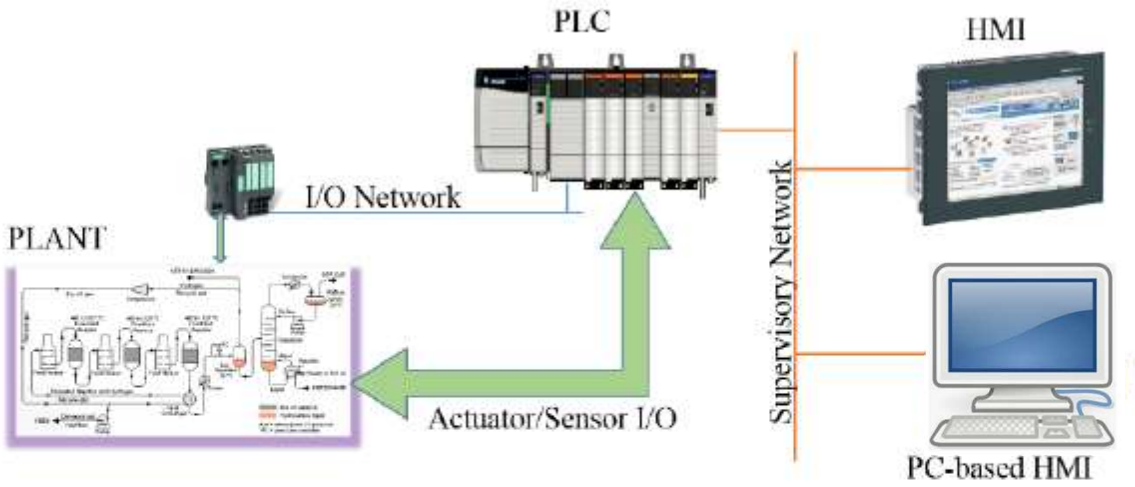
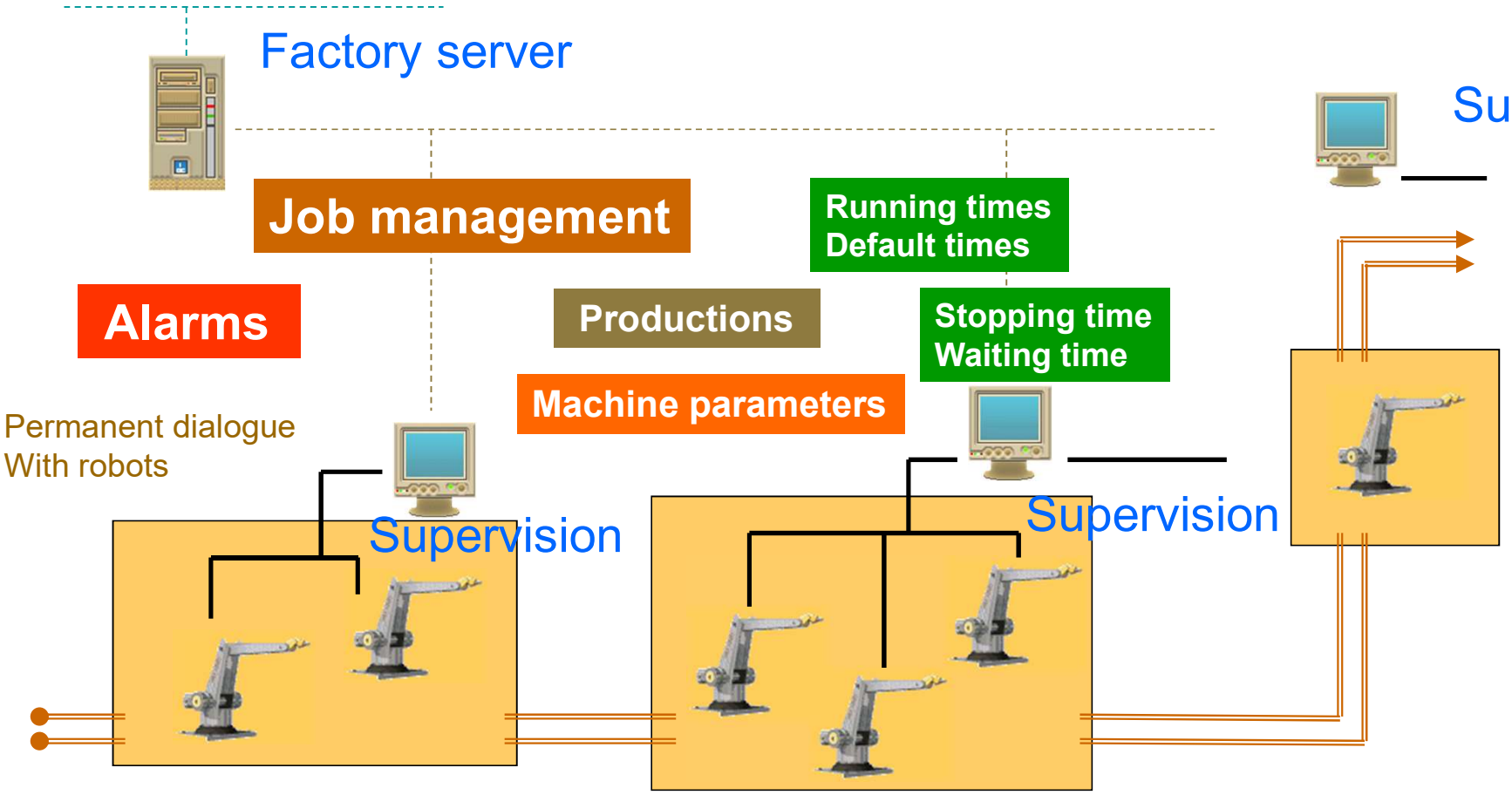


Figure 1. The simple SCADA system

Supervisory Control And Data Acquisition

Supervision : computerized monitoring and control of automated manufacturing processes
- Data acquisition
- Manual or automatic modification of process control parameters
- Use of PLCs, special machines, robots...

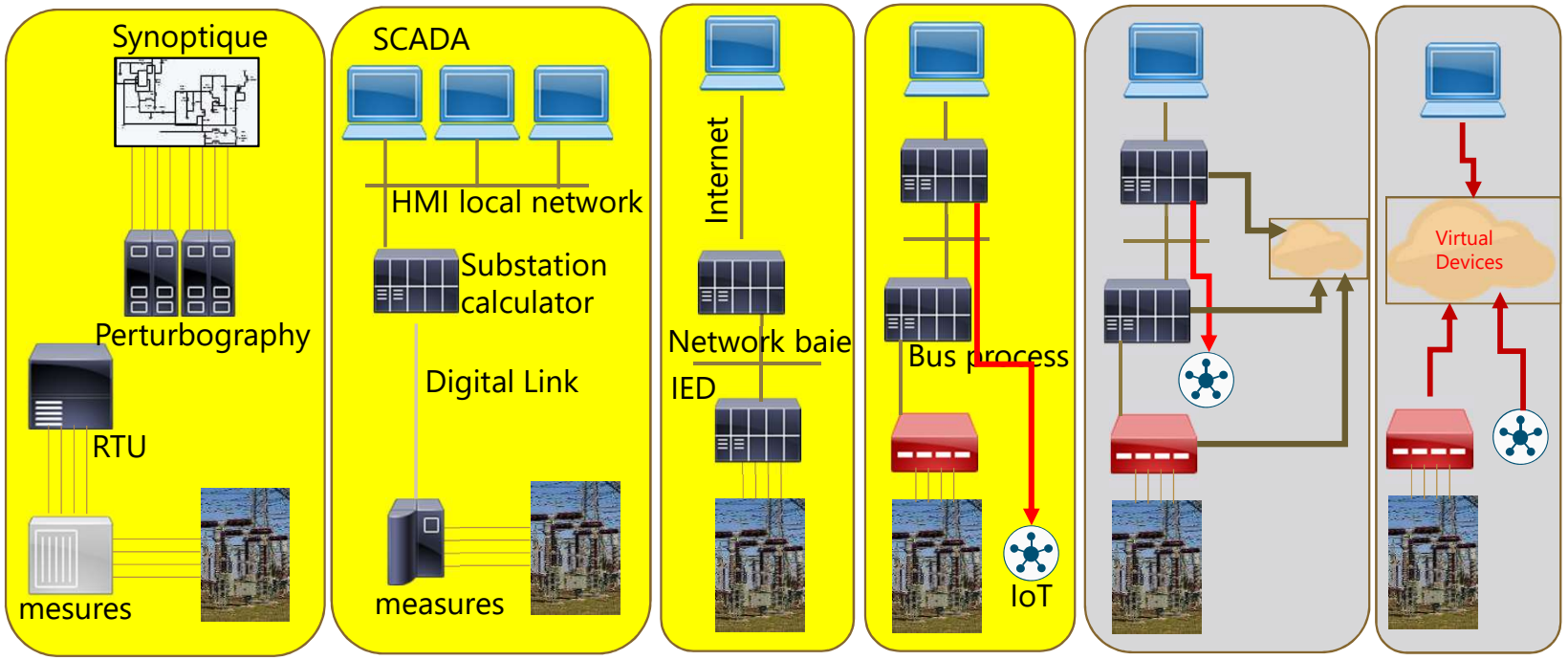
Supervision



Supervisors
Collect and process information from the robots
Basis of the factory's information system

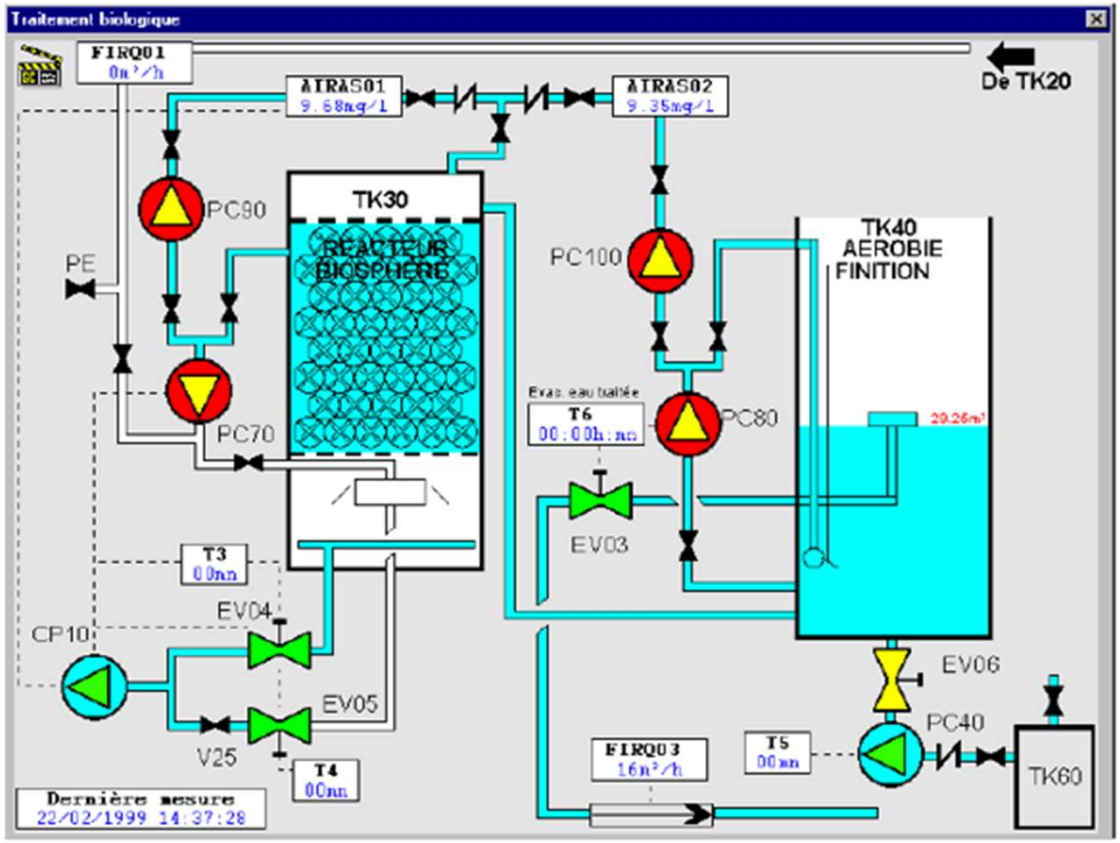
Supervision and Cloud technologies

- Example : evolution of the electrical substation



Supervision functions

Synoptic: essential function of the supervision, provides a synthetic, dynamic and instantaneous representation of all the means of production of the unit

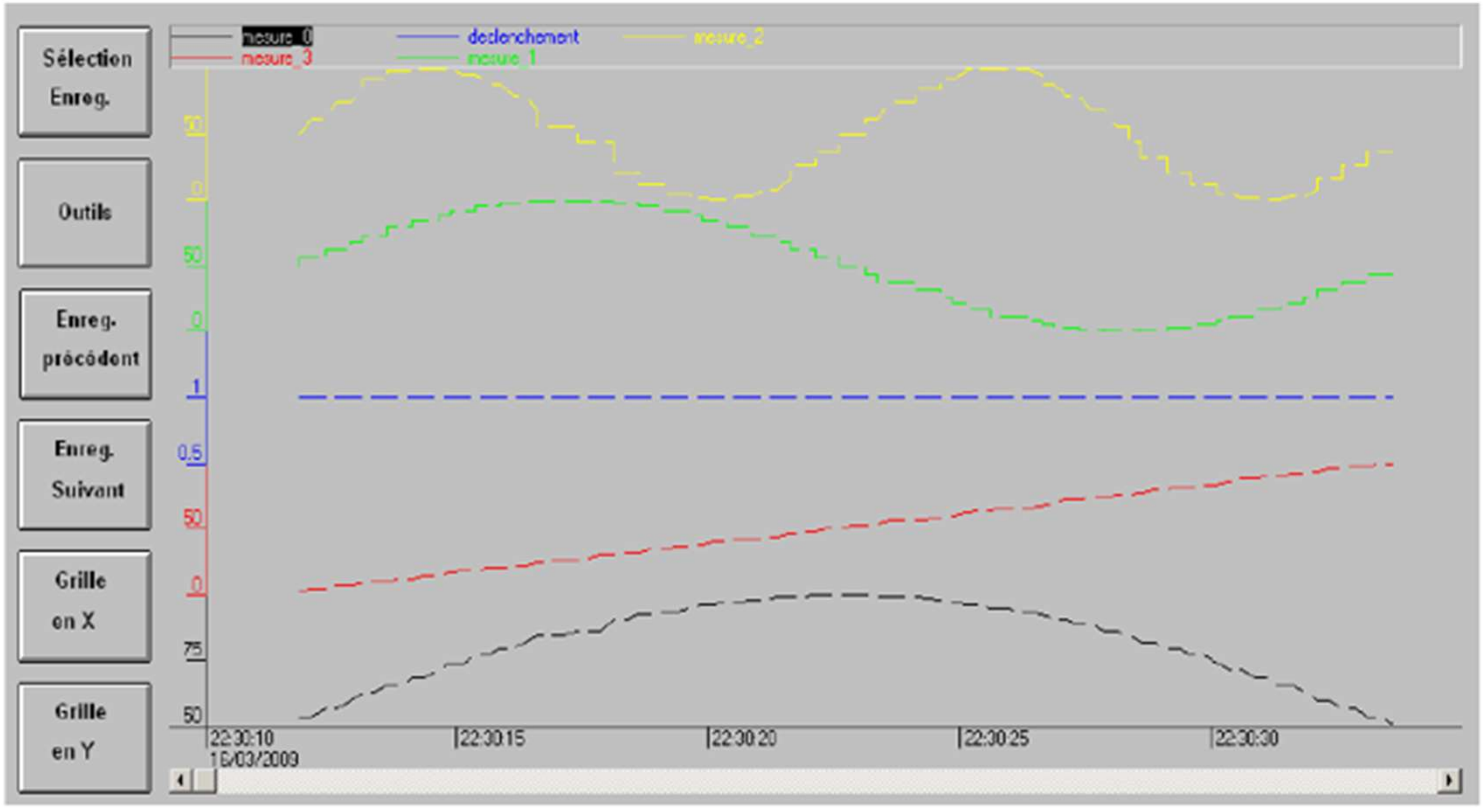


Supervision functions

Curves:

- gives a graphical representation of different process data

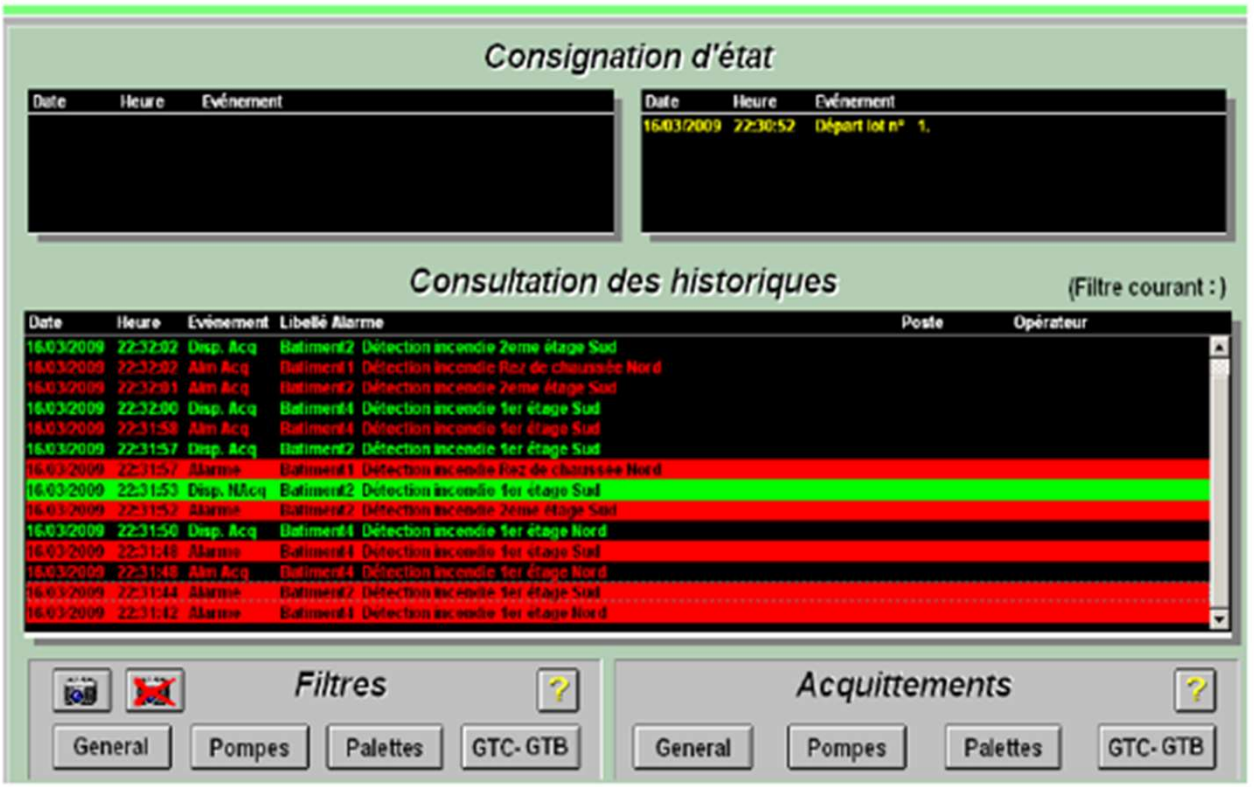
- gives the tools to analyze the historical variables



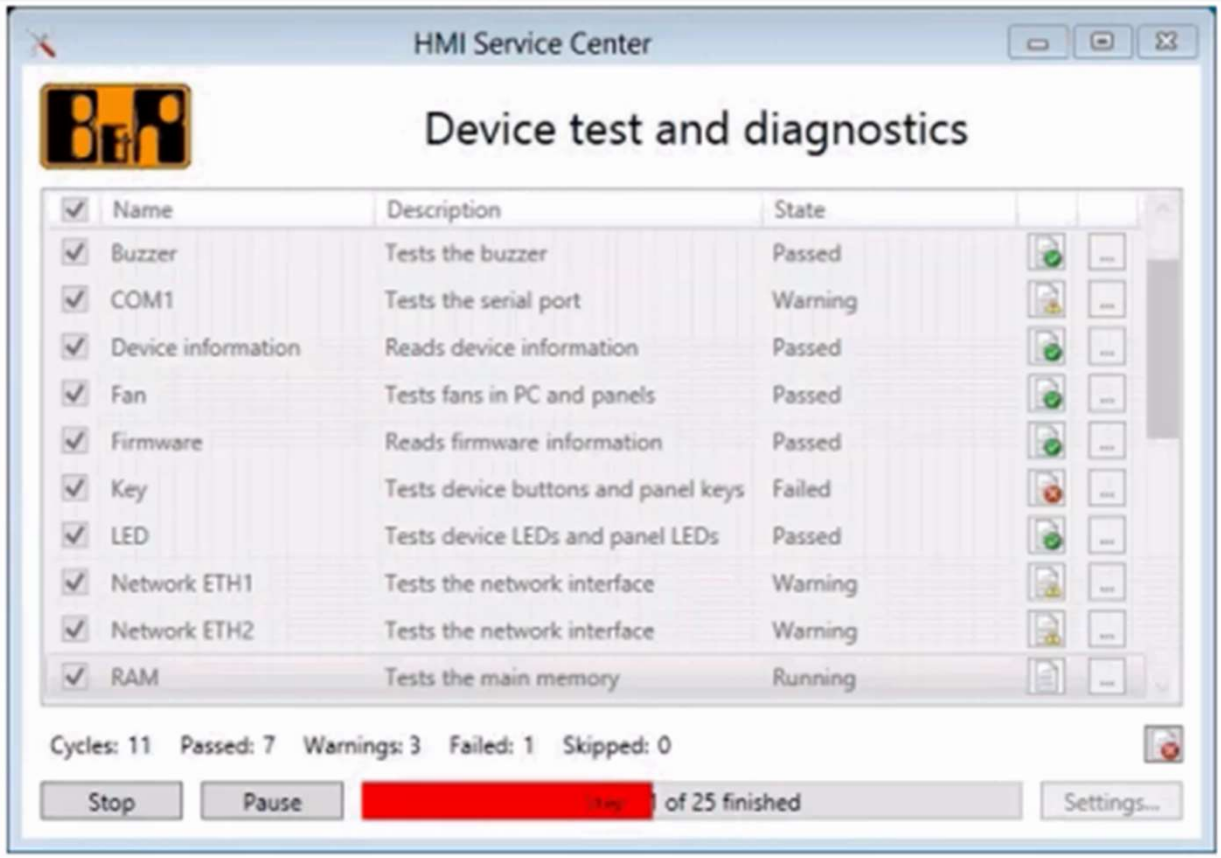
Supervision functions

Alarms

- Calculates in real time the conditions for triggering alarms
- Displays all alarms according to priority rules
- gives management tools
- ensures the recording of all the steps of the alarm processing



Supervision functions



Alarms

Circumscribe the cause of the feared event (cause of the incident)
Limit the impact of the event, protect (consequences)
Be able to assess the system after the incident: repair, reconfigure (total and partial redundancies)
Reconstruct, recover the system: time required for it to be operational again, what happens and what are the recovery steps? (Activity Return Plan)

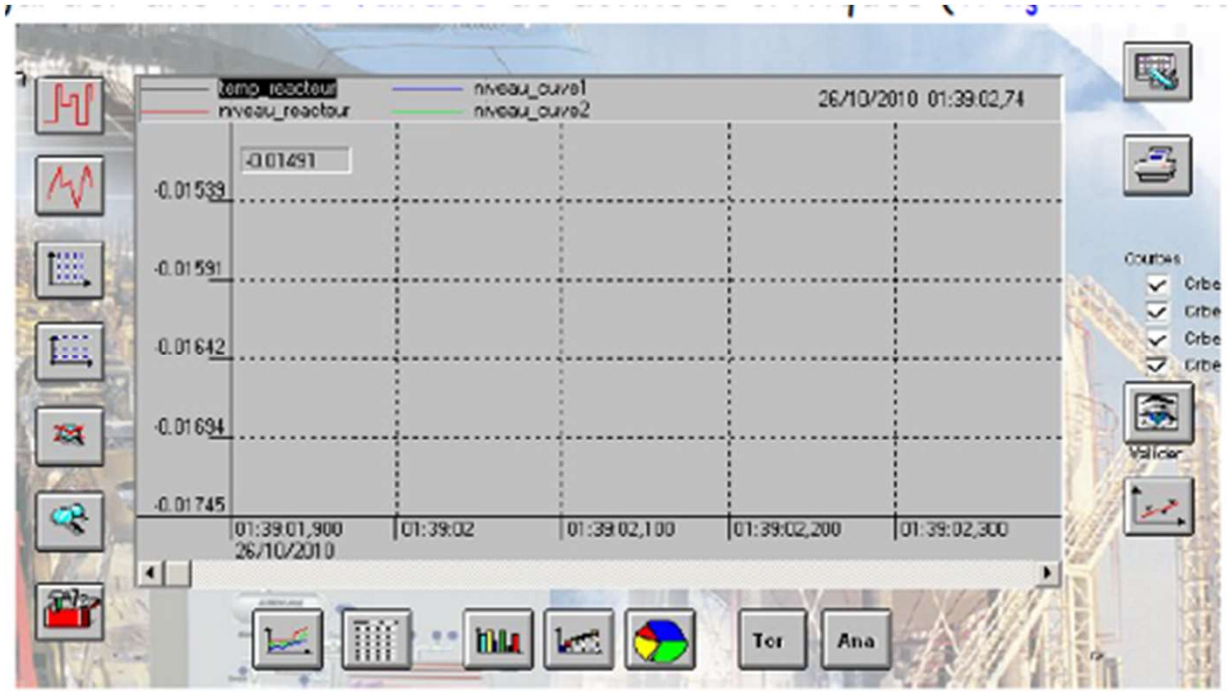
Other related aspects: robustness, resilience (ability to maintain the system as well as possible in a situation of "attacks")

Alarms detection

- TP (true positive) corresponds to correctly identified alarms
- FP (false positive) corresponds to authentic behavior identified as faulty
- TN (True Negative) corresponds to the correct rejection of authentic behavior
- FN (False Negative) corresponds to undetected failures
- Two metrics are used to evaluate the performance of alarm detection
  - True Positive Rate TPR=TP/(TP+FN)
    => 1 if no False Negative
  - False Positive Rate FPR=FP/(FP+TN)
    => 0 if no False Positive

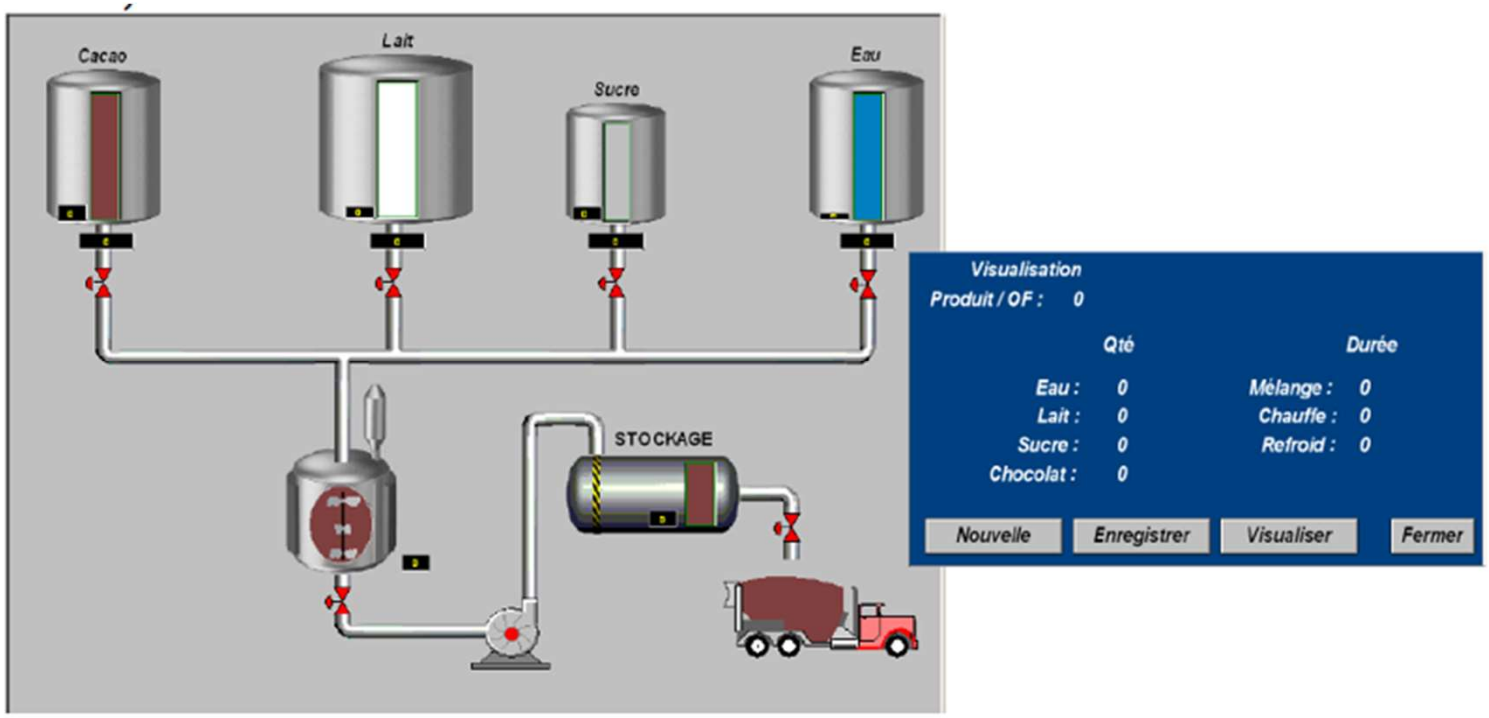
Supervision functions

Historicization of the process:
- Allows the saving of time-stamped events (selective archiving)
- provides search tools in the archived years
- provides the possibility to run the synoptic again with archived data (replay function)
- allows to keep a validated trace of critical data (traceability of production data)



Supervision functions

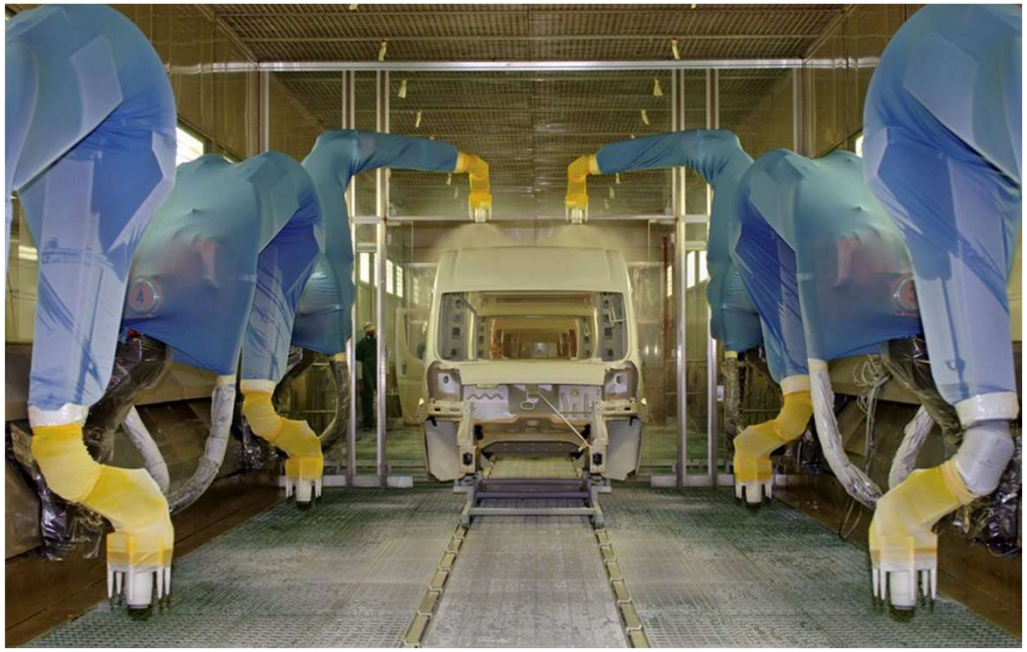
Management of production lines and recipes:
- Provides a tool for managing production batches
- Manages the parameters of the machines for each batch (recipes)



7. Robotics applications in Industry 4.0

Robotics

End 1970s

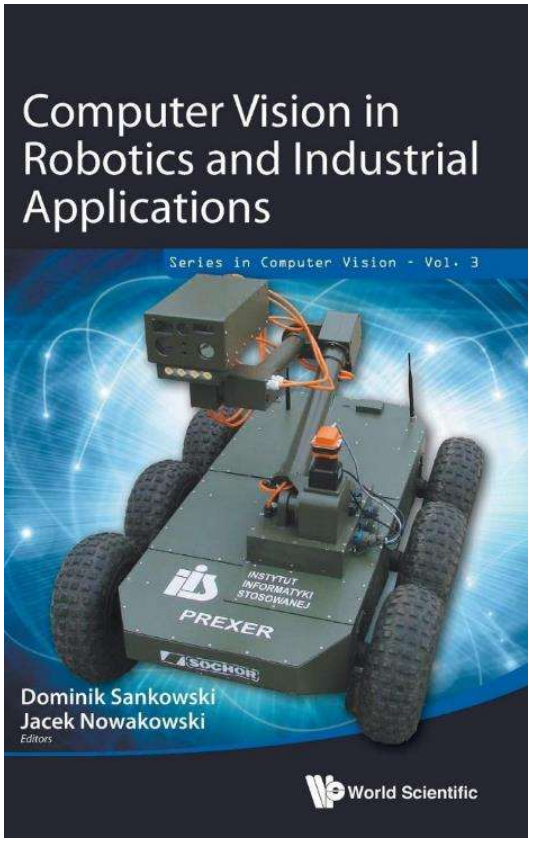


2020s: Many dimensions

Robotics

Training an Industrial Robot Using AI

Robotics & Visions



Vision-guided robotics

2D-Vision
3D-Vision
Radars
Lasers

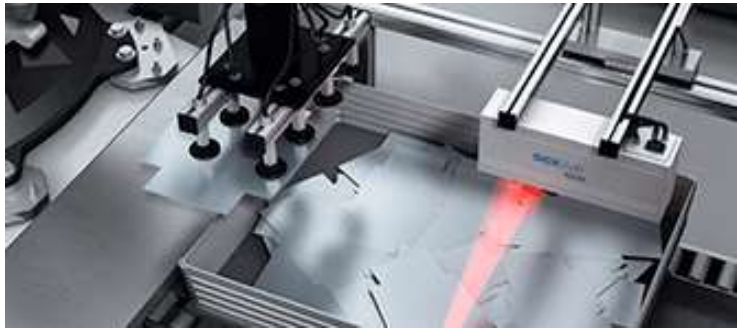
Robotics

Industrial Robots in Extreme Conditions

Robotics

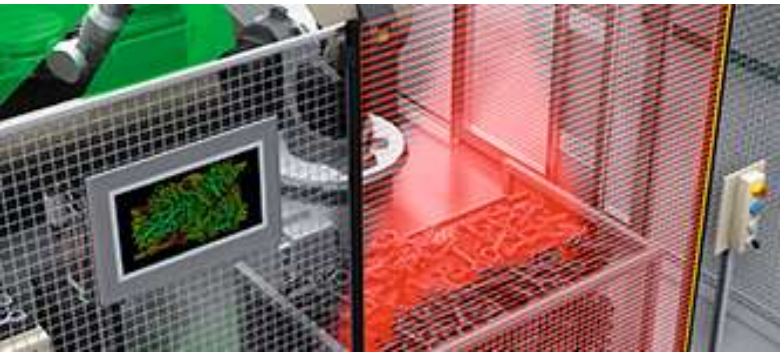
Autonomous trans-pallet

Robotic preparation of parts orders on the assembly line



Automated part picking (bulk items)

Simplified guidance of a Universal Robots robot



Locating parts in boxes

Picking up raw components for assembly

On-line quality control

3D sampling on tape

Robotics

COBOT

Industrial
Collaborative
Robot

Global Industrial Robot Market 2020 by Manufacturers, Type and Application, Forecast to 2025

https://www.marketsandresearch.biz/report/98579/global-industrial-robot-market-2020-by-manufacturers-type-and-application-forecast-to-2025

Robotics

Robots have long been used in industry, but they are evolving to be more autonomous, interact with each other, and work more safely with humans

Cobots, or collaborative robots, are much less scary and take care not to hurt people. Cobots are equipped with sensors and software so that they do not need to be separated from human workers. In the factory of the future, cobots will assist the human operator

When it comes to safety, an ISO(10218) 34 standard specifies and describes requirements and recommendations for safety around robots in the industrial setting only. But since 2016, a new ISO 15066 35 standard addresses human-robot interaction in industry, and gives specifications on the safety of cobots to be implemented.

8. Conclusion

Conclusions

- Industry 4.0
  - Concept around Information Systems (from the « field » (sensors, actuators) to the higher levels of management in the companies)
  - Various functionalities: Production, but also Maintenance, Logistics, Transport
  - Robotics is an important aspect (for Production, Maintenance, Transport…)
- PLC, Programmable Logic Controller
  - « Industrial » computer
  - Inputs/outputs to be connected to physical processes
  - Communication networks
    - Fieldbus networks, « Industrial networks », for interactions between PLC (ex: Master/slave), I/O interactions with PLC
    - Classical networks for supervision
    - More and more in the Cloud (virtual devices) => Cyber-security challenges
- « Integration » IT (Information Technology)/ICS (Industrial Control Systems)
- Challenges in Dependability/Safety and in « Cyber-Security » => Convergence between these concepts
  - Risk Analysis, risk management

Some references

- J.F. Aubry, Nicolae Brinzei – Systems Dependability Assessment, Modeling with Graphs and Finite State Automata, Wiley, Fév. 2015.
- J.C. Laprie & al. – Guide de la sûreté de fonctionnement – Cépaduès, 1995.
- A. Villemeur – *Sûreté de fonctionnement des systèmes industriels* – Editions Eyrolles, Paris, 1988.
- C. Davis, M. Schiller, K. Wheeler - *IT Auditing: using control to protect assets* – 2007, Mc Graw Hill
- Cours Stéphane Mocanu, ENSE3, Industrial Communication Labs, 2016
- Cours Emmanuel Simeu, Polytech Grenoble, Supervision
- Patrick Monassier, cours CESI 2009, Informatique industrielle.
- Pierre Bonnet, cours Université de Lille, Introduction à la supervision, 2010
- EPFL, Industrial Automation course
- P_RAYMOND_BTS_MAI_Les_API
- Transmissions et réseaux, S. Lohier & D. Présent, Dunod, Paris, 2003.
- Cours Stéphane Mocanu, ENSE3, Industrial Communication Labs, 2016
- Cours Emmanuel Simeu, Polytech Grenoble, Supervision
- Cours de Blaise Conrard, Polytech Lille.
- Patrick Monassier, cours CESI 2009, Informatique industrielle.
- Pierre Bonnet, cours Université de Lille, Introduction à la supervision, 2010
- G. Boujat et P. Annaya, Automatique industrielle en 20 fiches, Dunod, 2007
- W. Bolton, Automates programmables industriels, Dunod, 2015.
- Duc Tran Trung , Cybersecurity risk assessment for Unmanned Aircraft System, PhD, Univ. Grenoble Alpes

Some references

https://www.technologuepro.com/cours-automate-programmable-industriel/Les-automates-programmables-industriels-API.htm

http://www.est-usmba.ac.ma/coursenligne/GE-S2-M8.1-Automatismes%20logiques%20Industriels-CRS-El%20Hammoumi.pdf

http://colasapoil.free.fr/HEI/HEI5%20TC/Maintenance/h5_tc_maintenance_coursv2_coursv2_1783.pdf

https://www.cours-gratuit.com/cours-divers/cours-sur-les-definitions-methodes-et-operations-de-la-maintenance

https://www.manager-go.com/logistique/organisation-de-la-logistique.htm

https://www.lecoindesentrepreneurs.fr/logistique-entreprise/
https://d1n7iqsz6ob2ad.cloudfront.net/document/pdf/5346e085efe6e.pdf

https://www.icours.com/cours/economie/la-production

https://perso.imt-mines-albi.fr/~fontanil/THESE/5_Partie1_p13_43.pdf

Merci pour votre attention
Merci pour votre attention

jean-marc.thiriet@univ-grenoble-alpes.fr

UGA
Université
Grenoble Alpes

សូមអរគុណចំពោះការយកចិត្តទុកដាក់របស់អ្នក។

Merci pour votre attention

Thank you for your attention