1. Industry 4.0, some aspects

http://www.gipsa-lab.grenoble-inp.fr/%7Ejean-marc.thiriet/mistre/mistre.html

MISTRE

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

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

Cours (master MISTRE)

- Supervision et réseaux
  - 12 heures de cours

- TP, et un peu de TD
  - 3 séances de 4 heures par groupe
  - 2 groupes

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, transport 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.

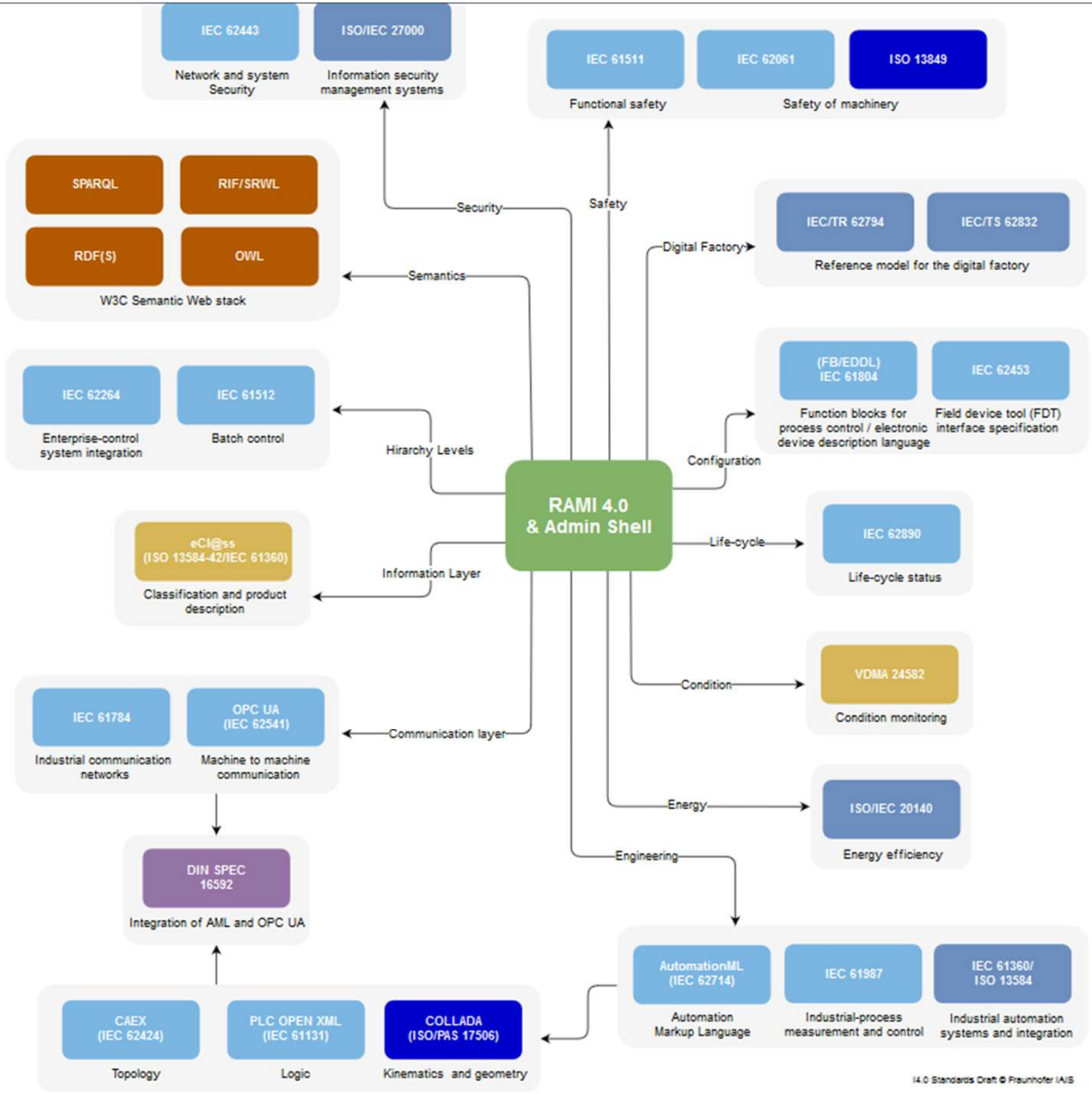
« New » networks: 5G

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)

RJ45

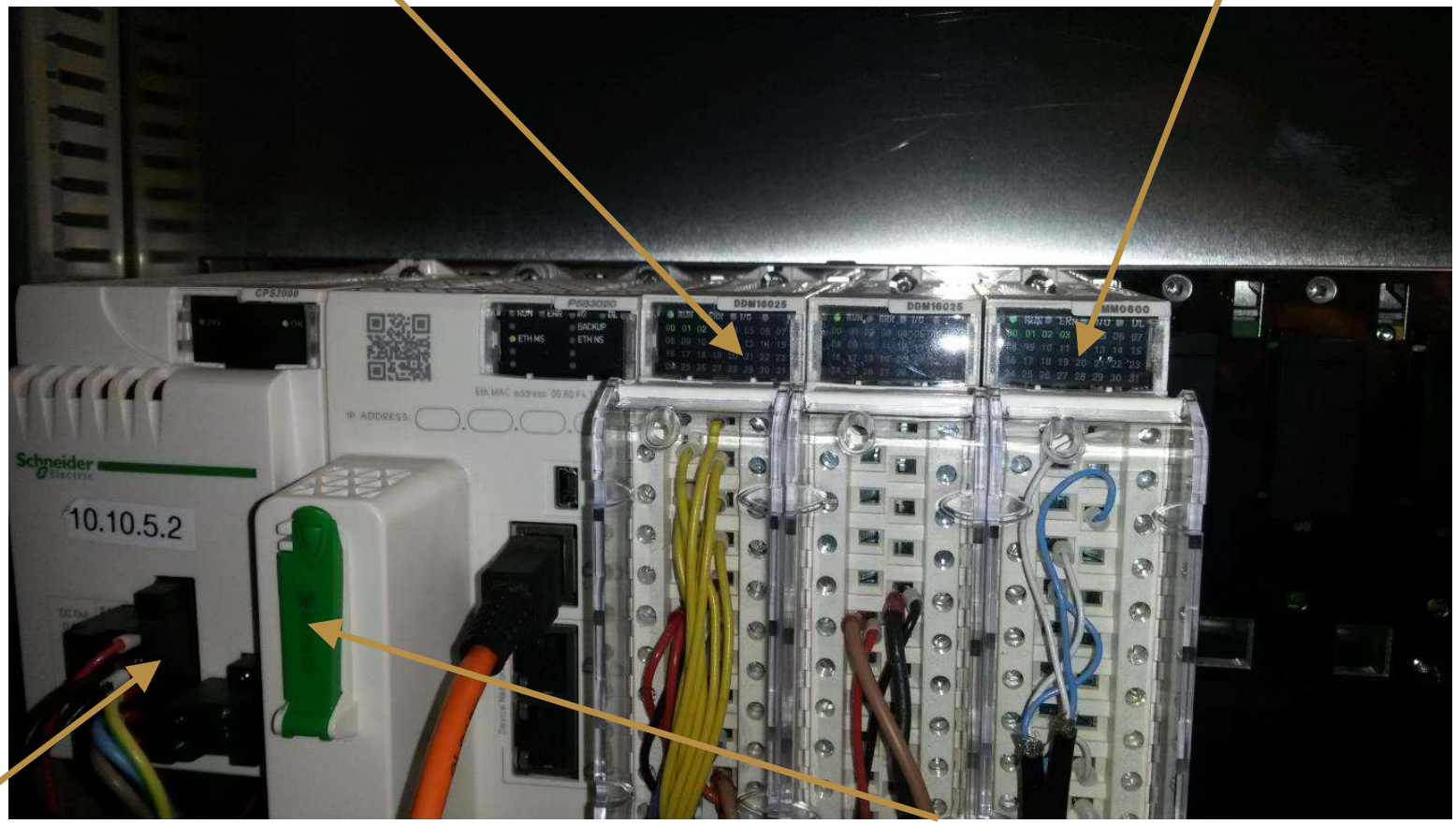
Free slots

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:

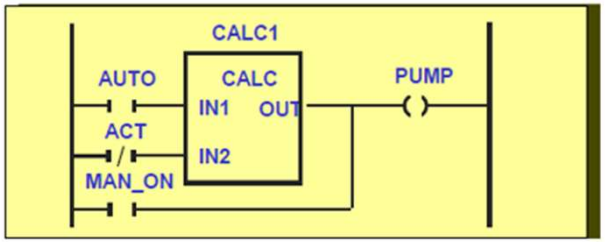
The use of **Ladder Logic** was significant in the rapid acceptance of the **"084"** because the very same engineers and electricians who designed and maintained Factory Automation Systems could also program an **"084"**. Ladder Logic was simply an electronic version of the elementary electrical diagram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

PLC Languages: IEC 61131

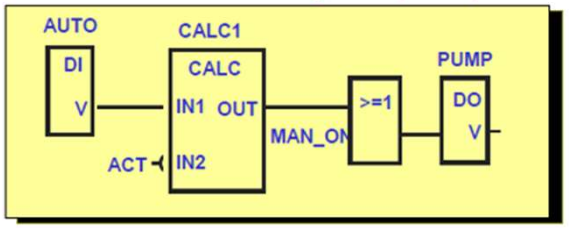
Instruction List (IL)

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

Ladder Diagram (LD)



Function Block Diagram (FBD)

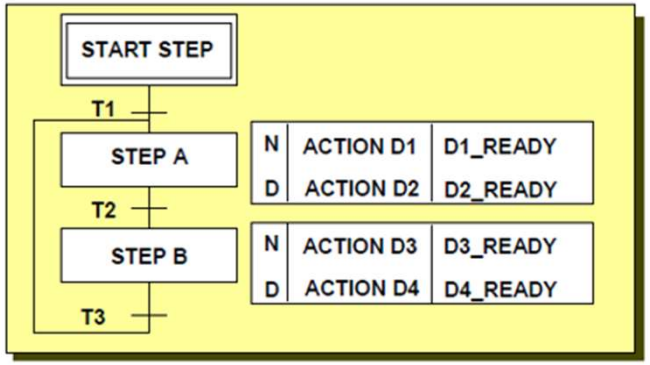


Structured Text (ST)

```
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
```

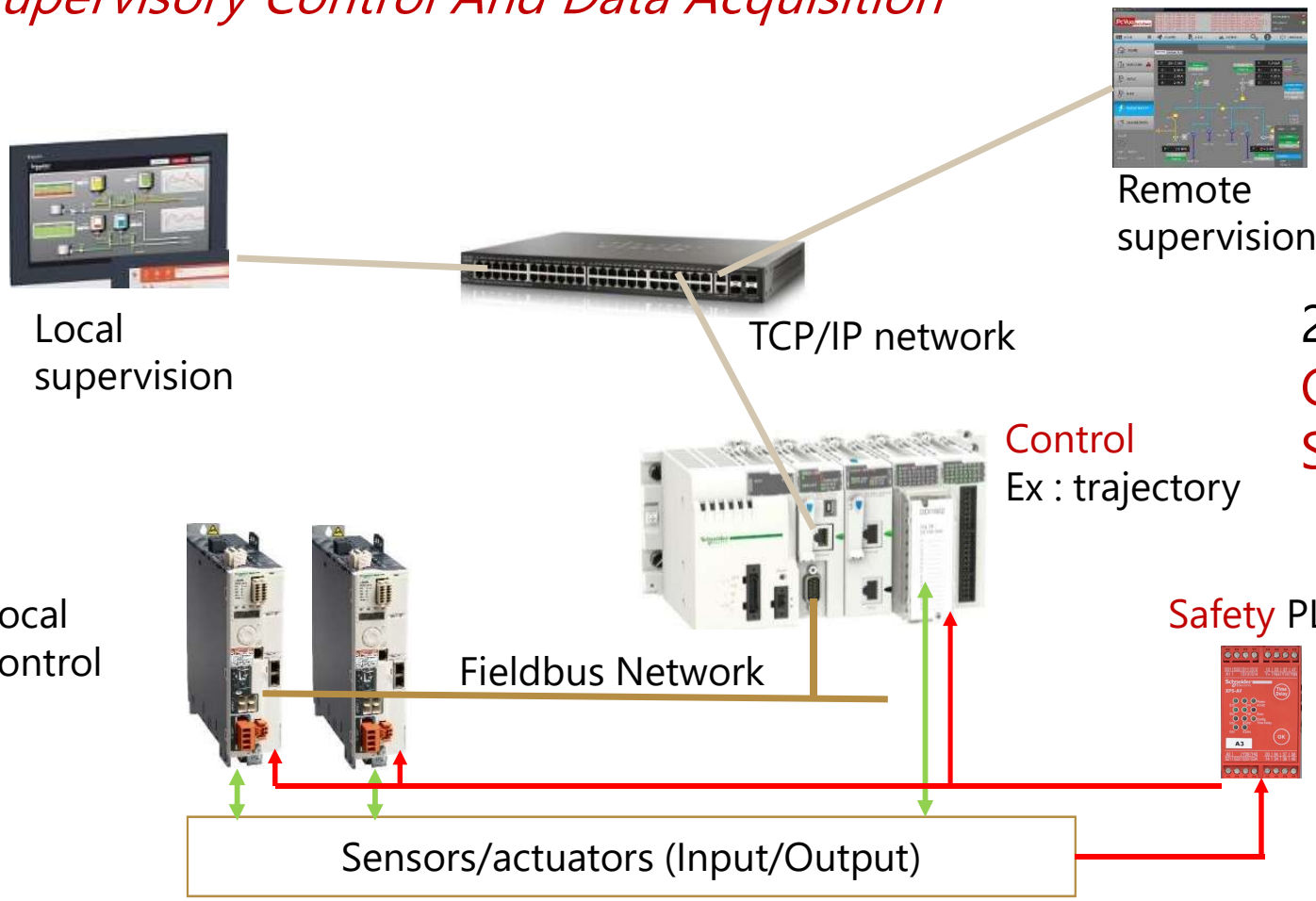
Sequential Flow Chart (SFC)



GRAFCET

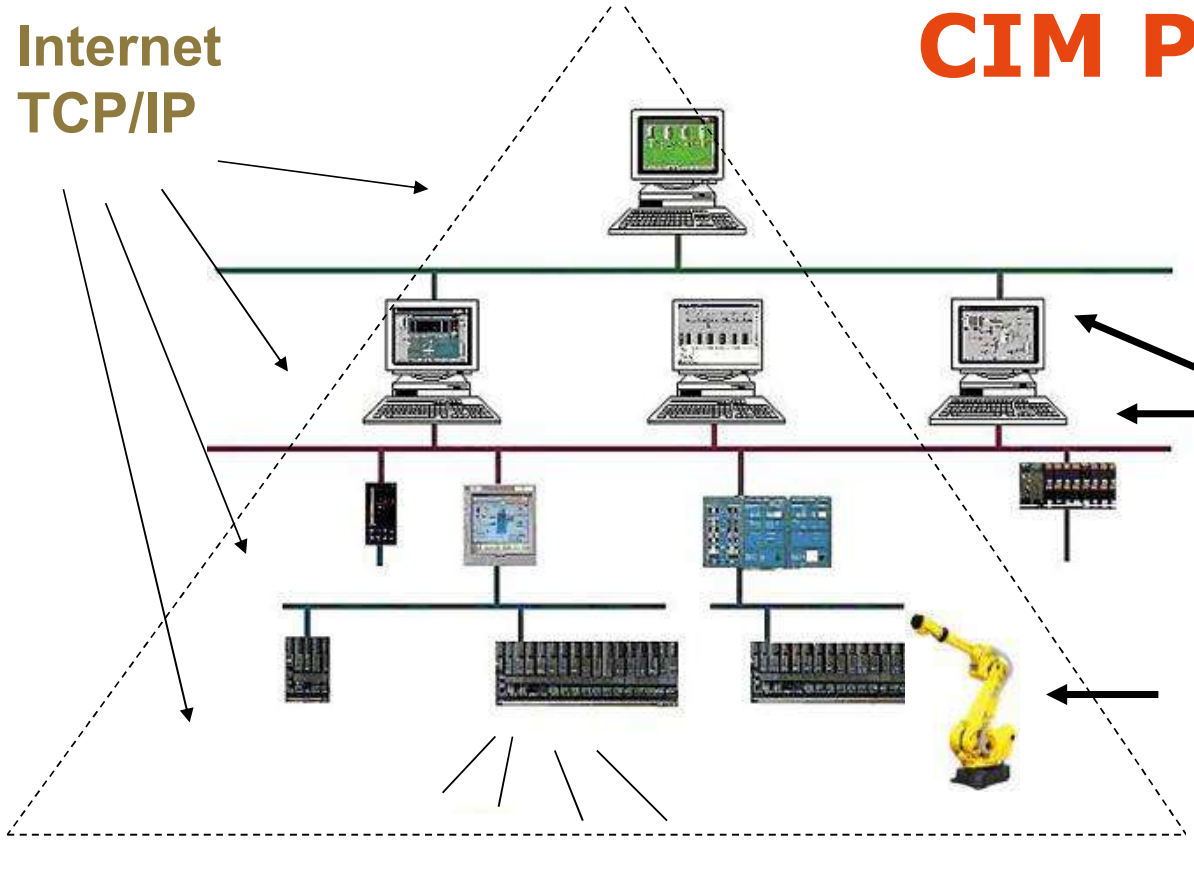
An example

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

Example of a SCADA

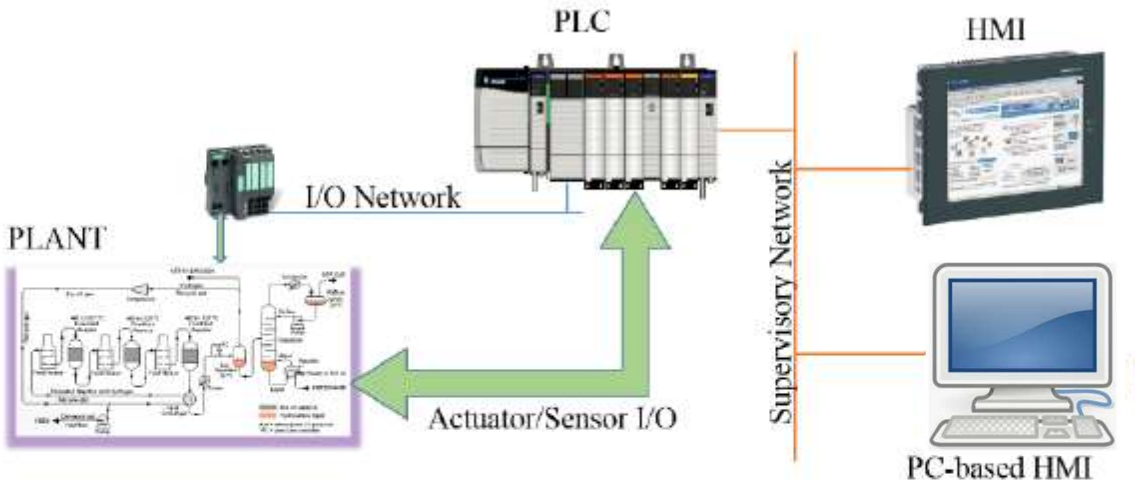
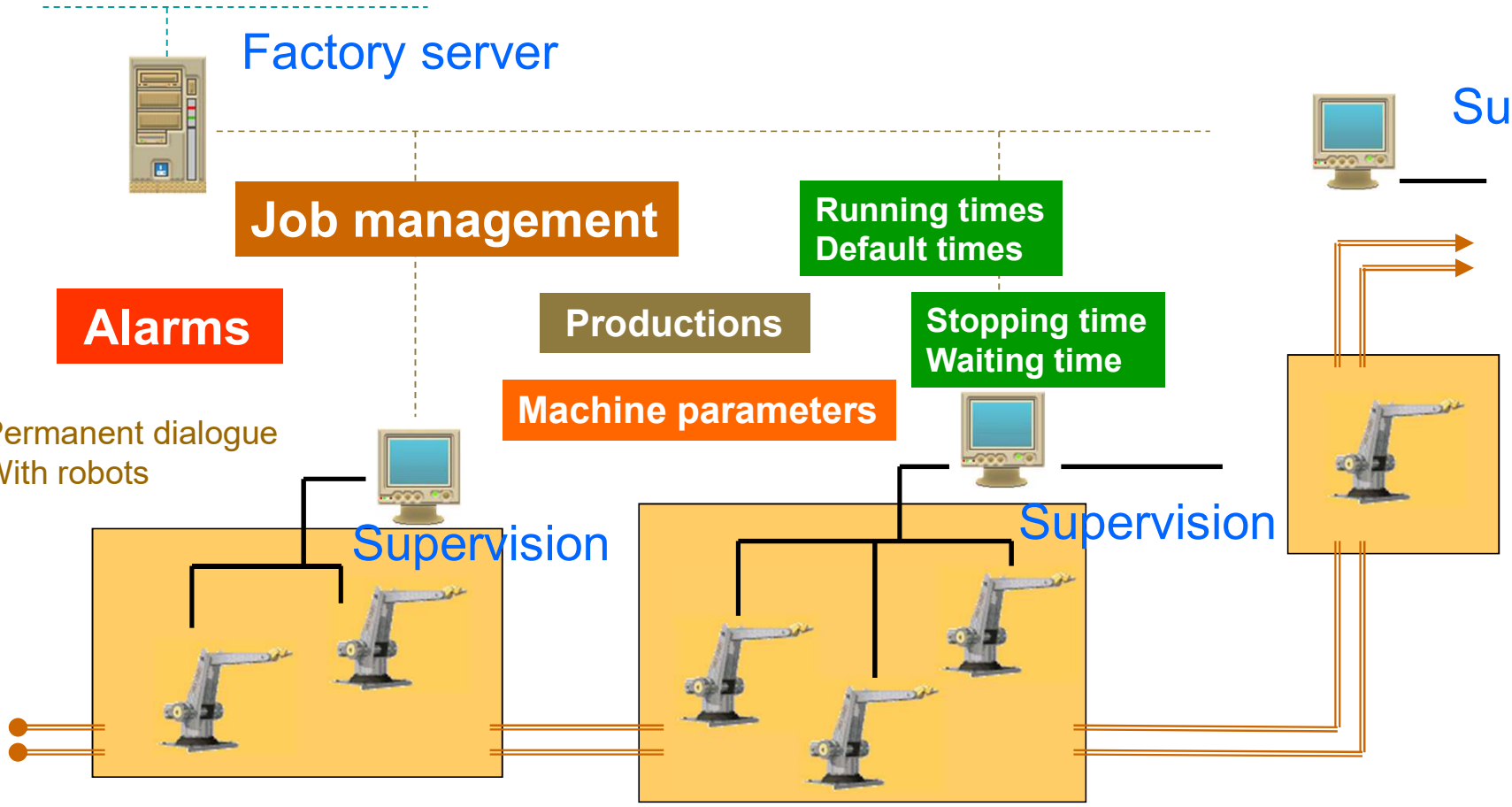


Figure 1. The simple SCADA system

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...

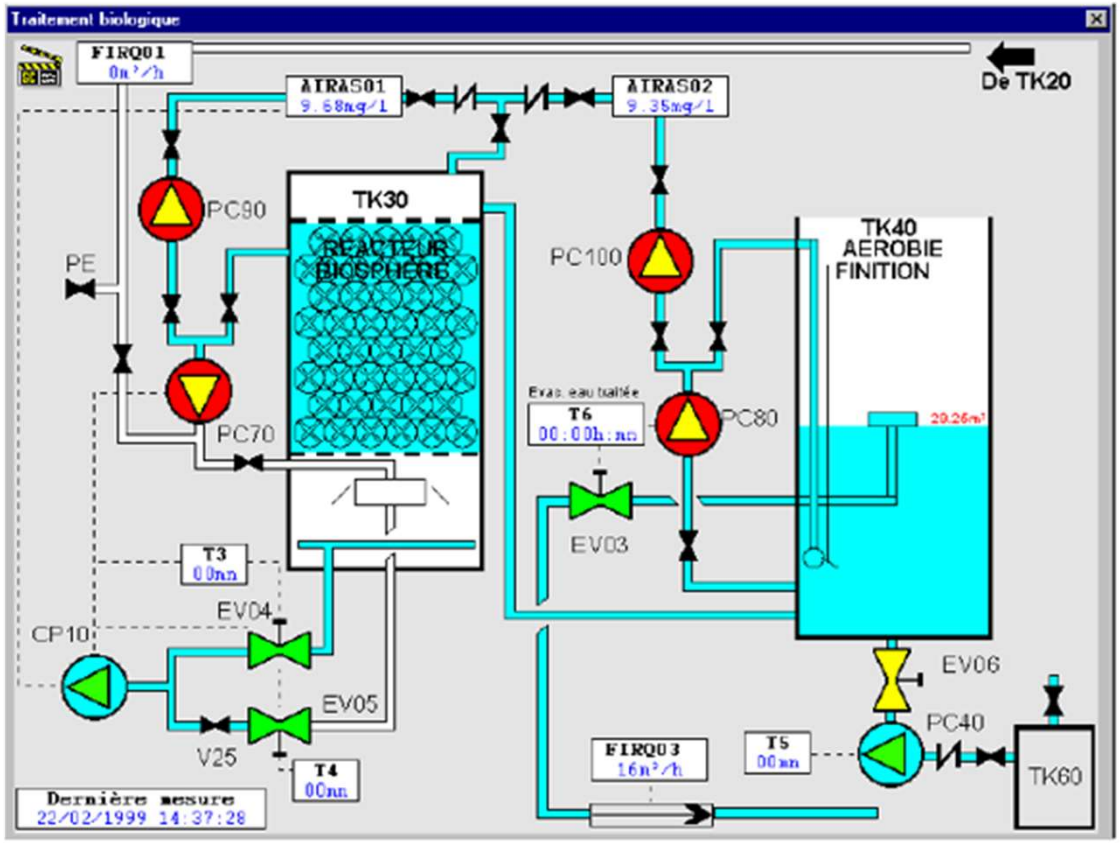
Supervision



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

Supervision functions

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

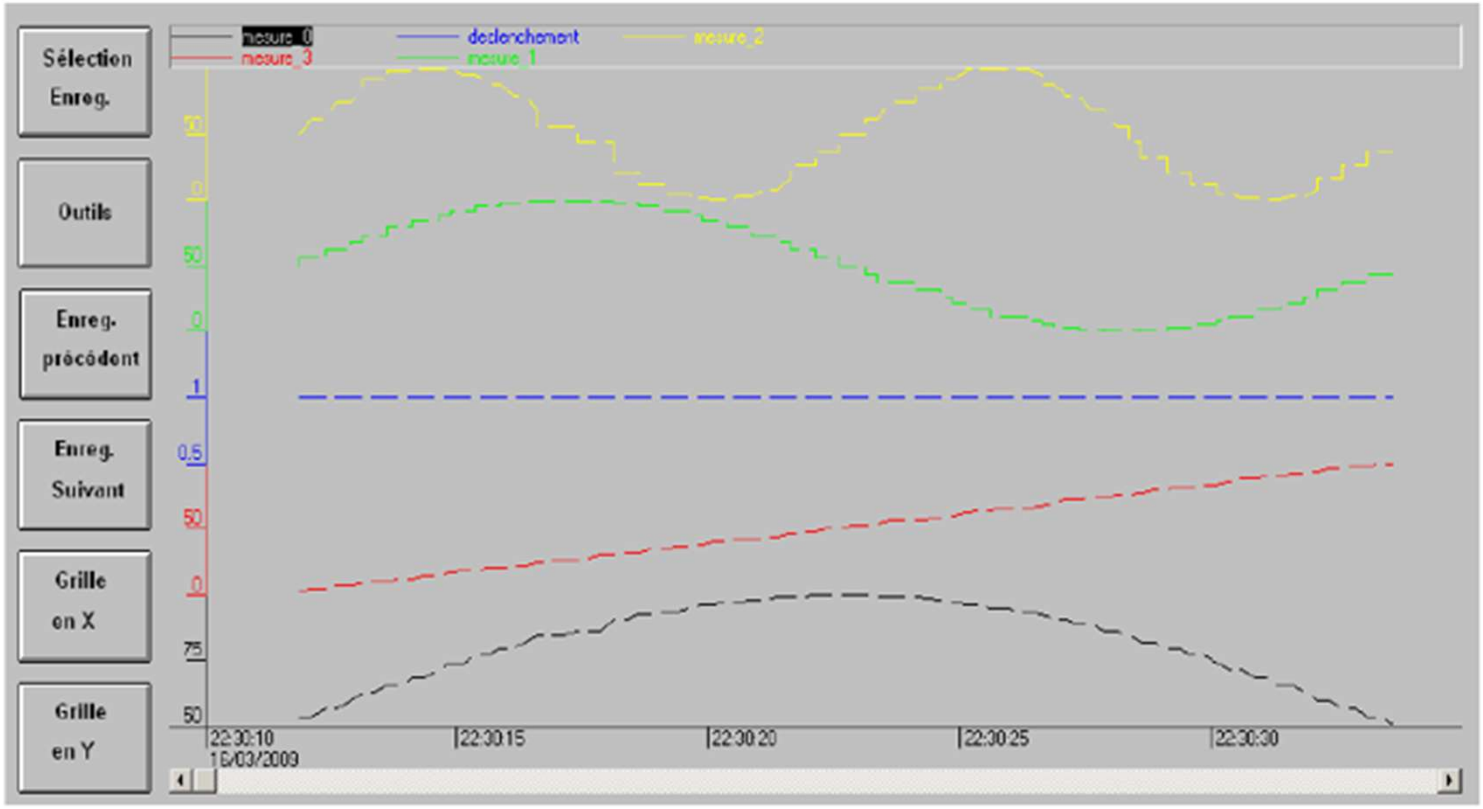


Supervision functions

Curves:

- gives a graphical representation of different process data

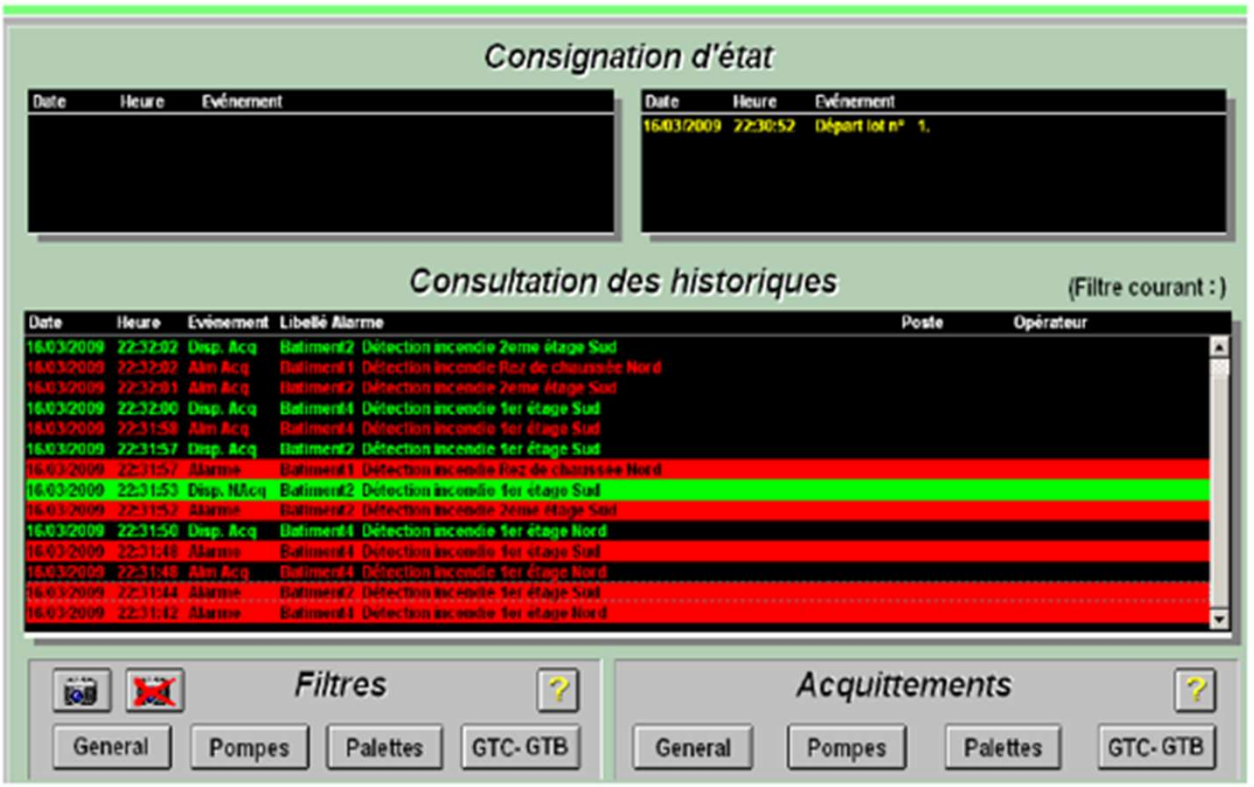
- gives the tools to analyze the historical variables



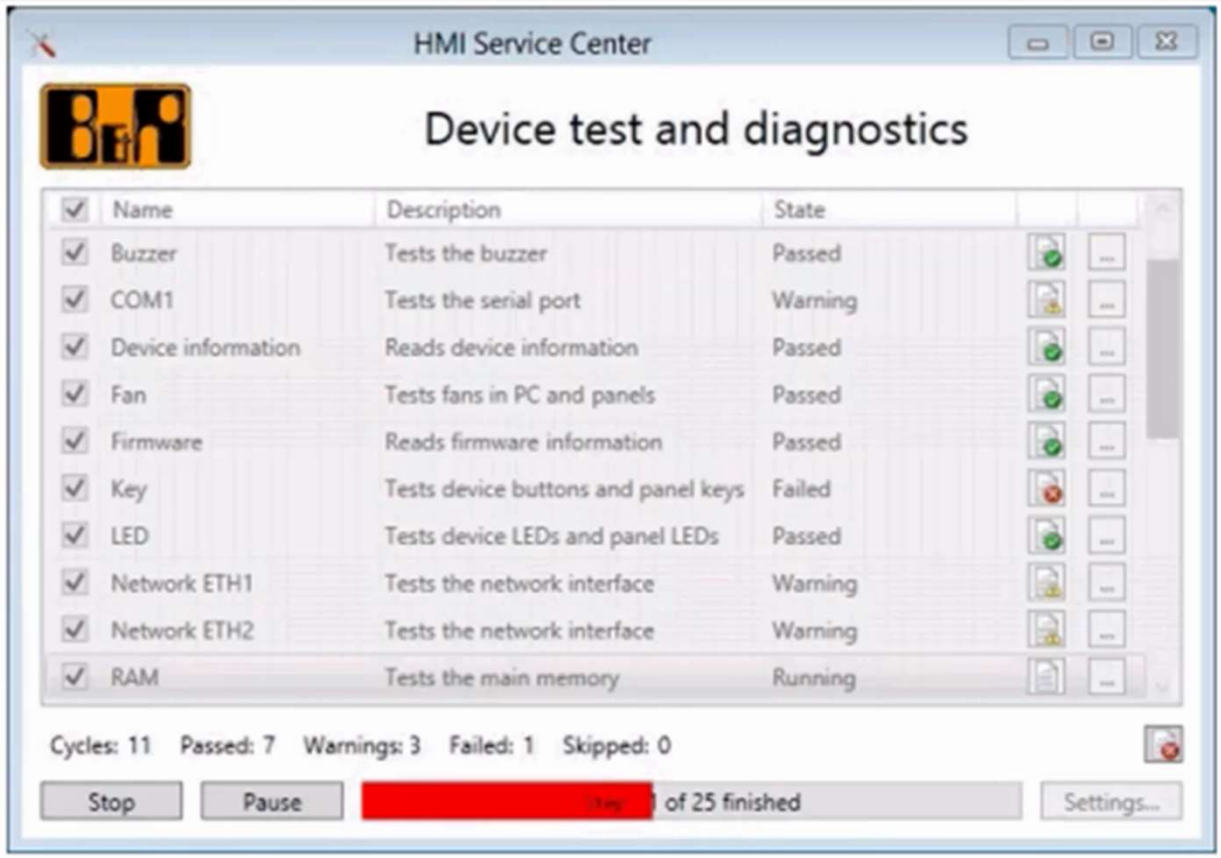
Supervision functions

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)

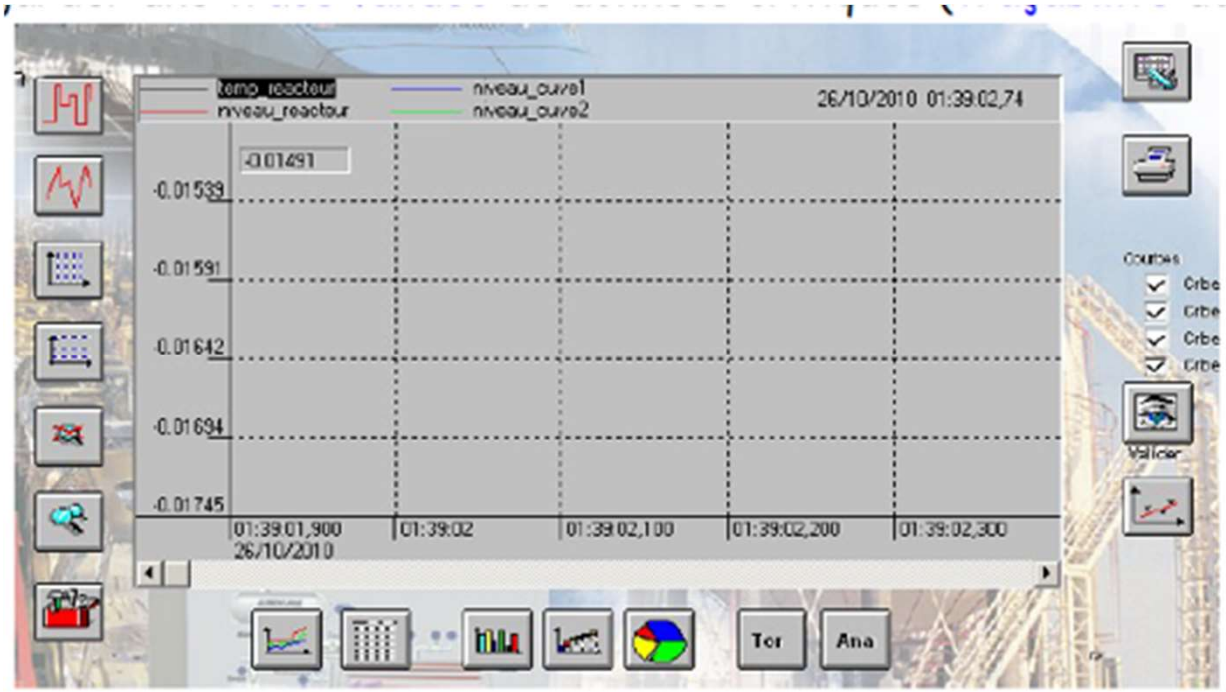
Other related aspects: robustness, resilience (ability to maintain the system as well as possible in a situation of "attacks")

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

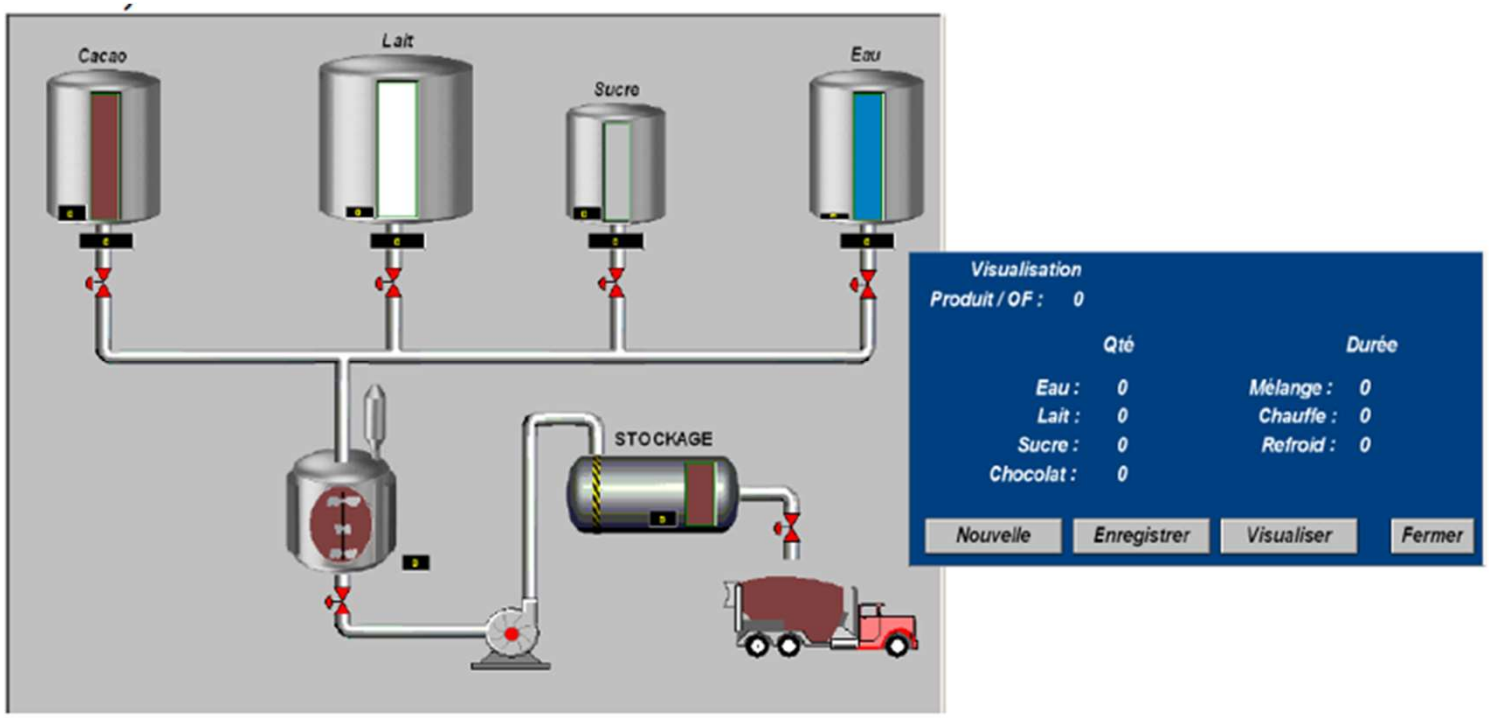
Supervision functions

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)



Other aspects of Industry 4.0

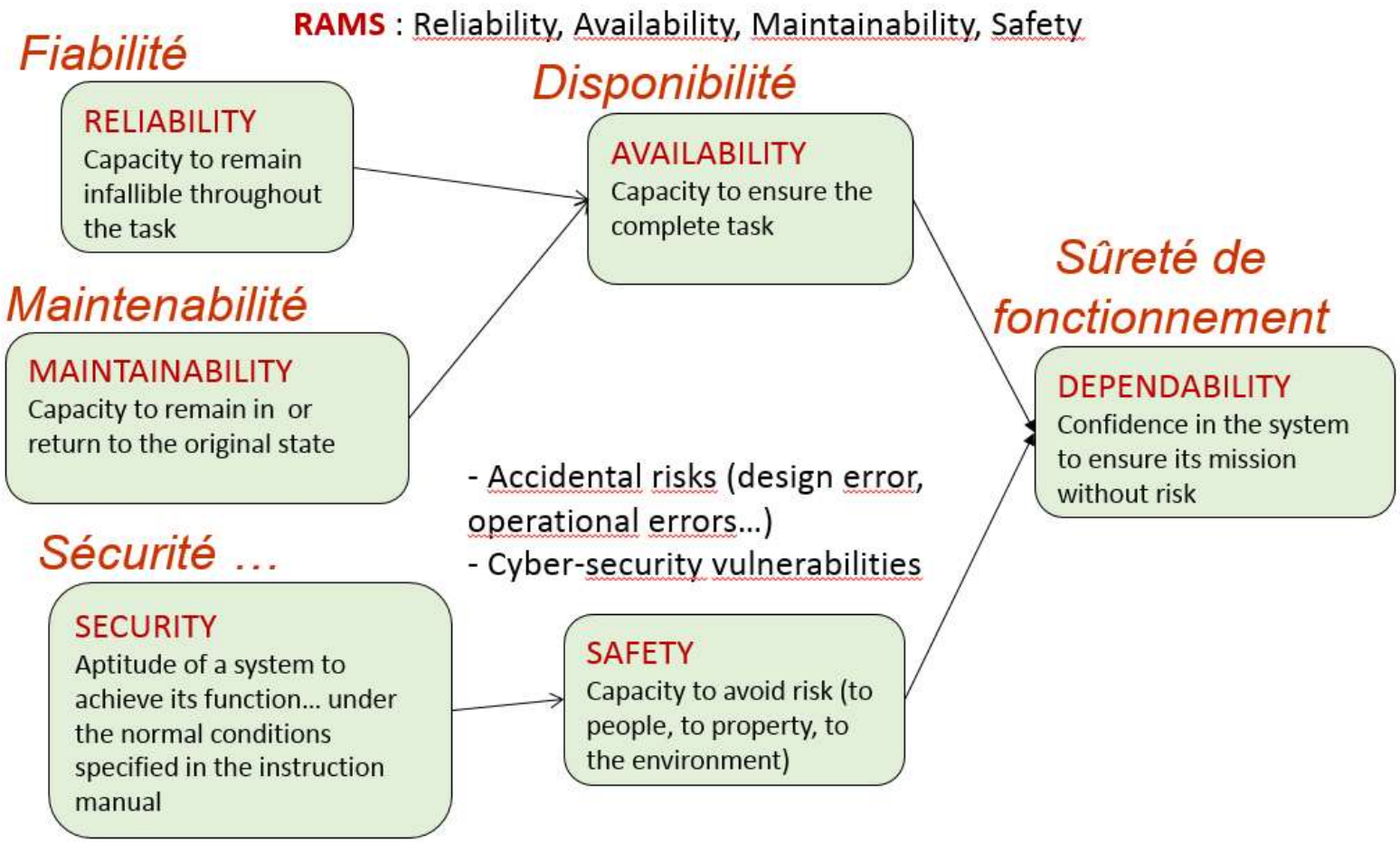
1. Description of the Main Industrial sector using PLC - Industry 4.0
2. Challenges: Safety & Cyber-security
3. **Maintenance**
4. **Logistics & Organisation**
5. **Production**
6. **Supervision**
7. **Robotics in Industry**
8. Conclusion
9. References

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 Challenges: Safety

Dependability



Paramètres de sûreté de fonctionnement

MTTF: *Mean Time To Failure,* durée moyenne de fonctionnement avant défaillance, espérance mathématique de la durée de fonctionnement avant défaillance.

MTBF: *Mean Time Between Failures,* moyenne des temps de bon fonctionnement, espérance mathématique de la durée de bon fonctionnement

MTTR*: Mean Time To Repair (Recovery , Restoration),* durée moyenne de panne ou moyenne des temps pour la remise en état de fonctionnement, espérance mathématique de la durée de panne

MDT: *Mean Down Time,* espérance mathématique de la durée d'indisponibilité

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

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

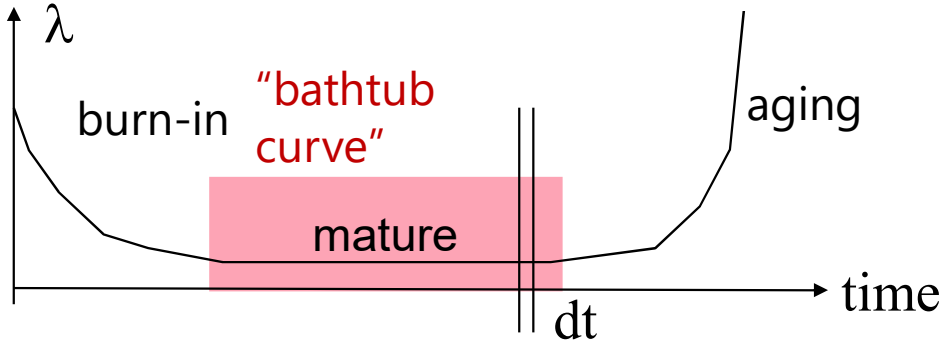
M(t) : probability that the system will be restored within a specified period of time *t*.

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 ?

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

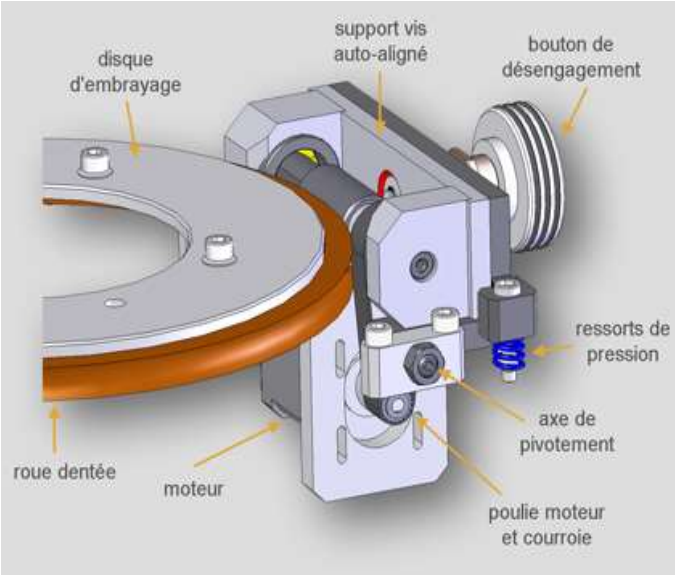


Failure rate **λ(t)** = probability that a (good) element fails during the next time unit dt

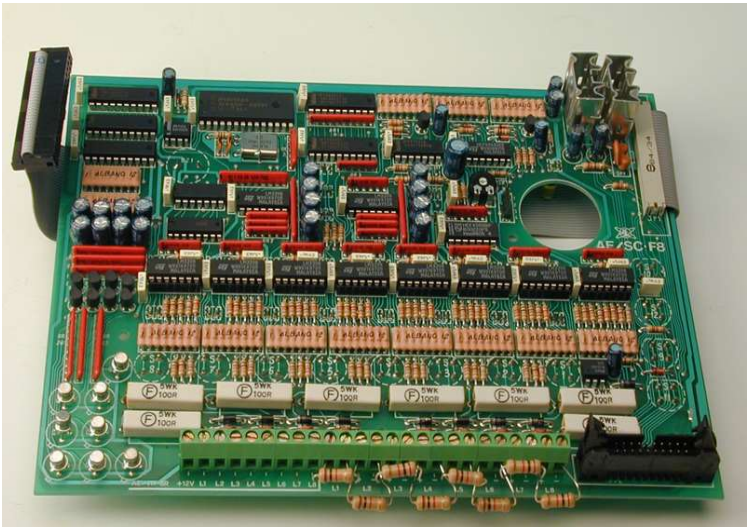
Dependability of classical Components

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

Mechanical systems

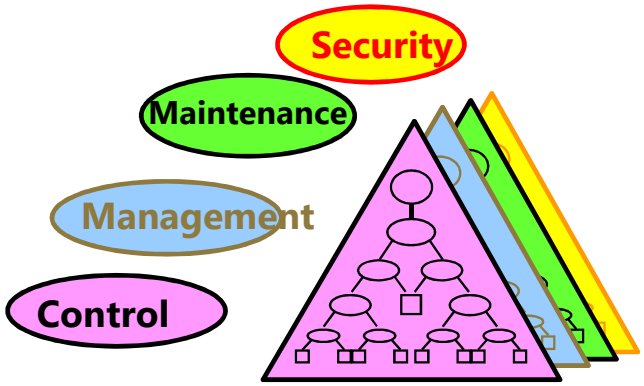


• Electronic systems



Context: Automation system evolution

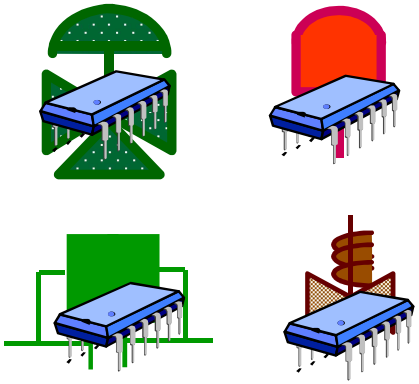
Needs:



Increased number of services

More complex architectures

Components :

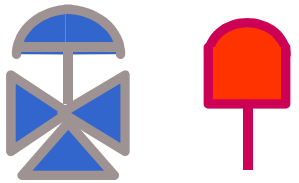


Various capacities and functionalities availability

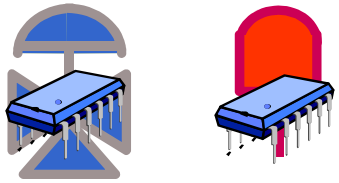
Dependability hard to evaluate and to qualify

From analog to digital and from smart to intelligent…

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

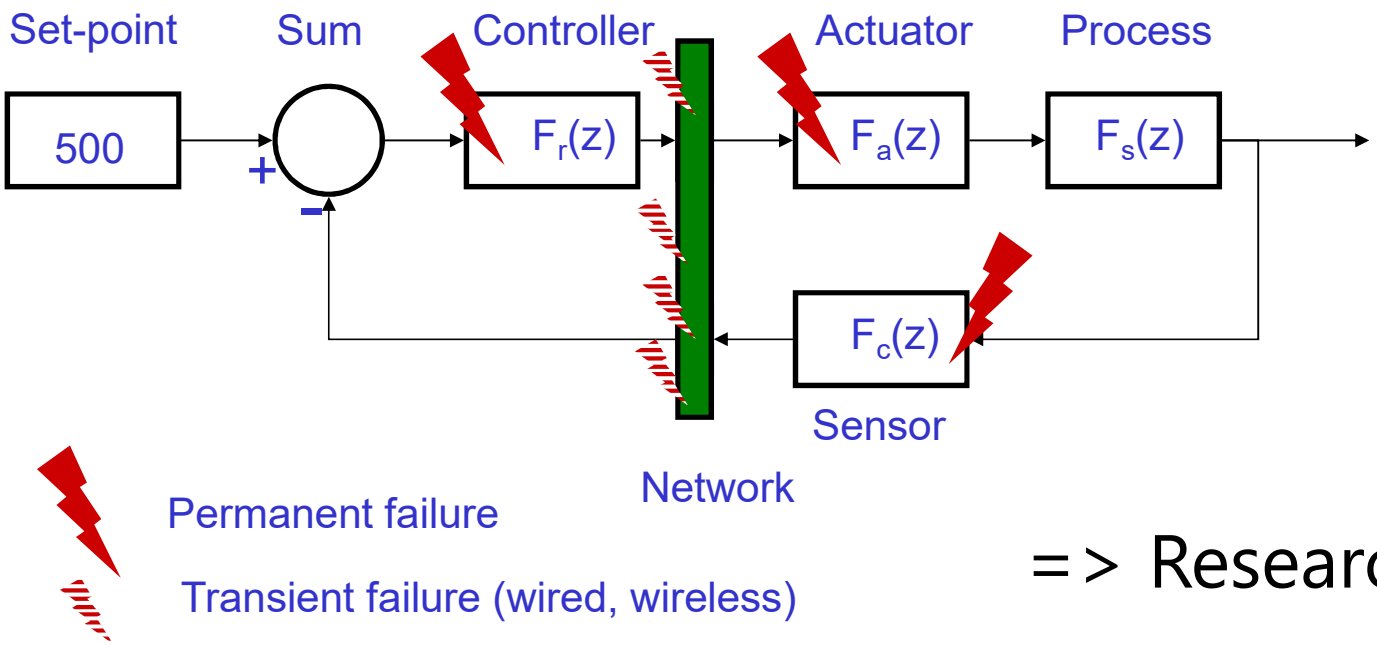


- Digital sensors and actuators
  - A/D Interfaces, processing units, delays…
  - Software, implementation



- « Smart » sensors and actuators
  - Embedded intelligence, local decision
- « Intelligent » 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	$10^{-1} < PFDavg < 10^{-2}$	$10^{-5} < \lambda < 10^{-6}$

Sûreté de fonctionnement = science des défaillances

- Défaillance : cessation de l'aptitude d'une entité à accomplir une fonction requise
  - Il faut définir la fonction concernée
    - ex 1 : assurer la communication entre deux sites
    - ex 2 : **assurer la mise à disposition des données informatiques** (en local et à distance)
  - Il faut préciser le critère de cessation de celle-ci
    - ex 1 : QUANTITATIF : le débit est ≤ à un certain %age d'une valeur de référence
    - ex 2 : QUALITATIF : la perte, ou la destruction irrémédiable de données stratégiques pour l'entreprise

Sûreté de fonctionnement
= ANALYSE DE RISQUE => Maîtrise des risques

- **Identifier** les défaillances de manière la plus exhaustive
  - Crash de disques durs
  - Incendie ou inondation de locaux de sauvegarde…
  - Ports ouverts sur un réseau
- **Evaluer l'importance** de chacune des défaillances (niveau de risque)
- **Prévoir** les défaillances (utilisation de modèles d'évolution)
  - Vétusté des composants informatiques
  - Probabilité d'attaques par des tiers de ports vulnérables
- A toute **observation** d'une défaillance, on associera des **mesures** (statistiques, rendement) => enrichir les modèles de prévision
- **Maîtriser** les défaillances
  - Réduction de leur occurrence
  - Prévention contre les conséquences (réduction de l'impact)
  - Tolérance

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 %

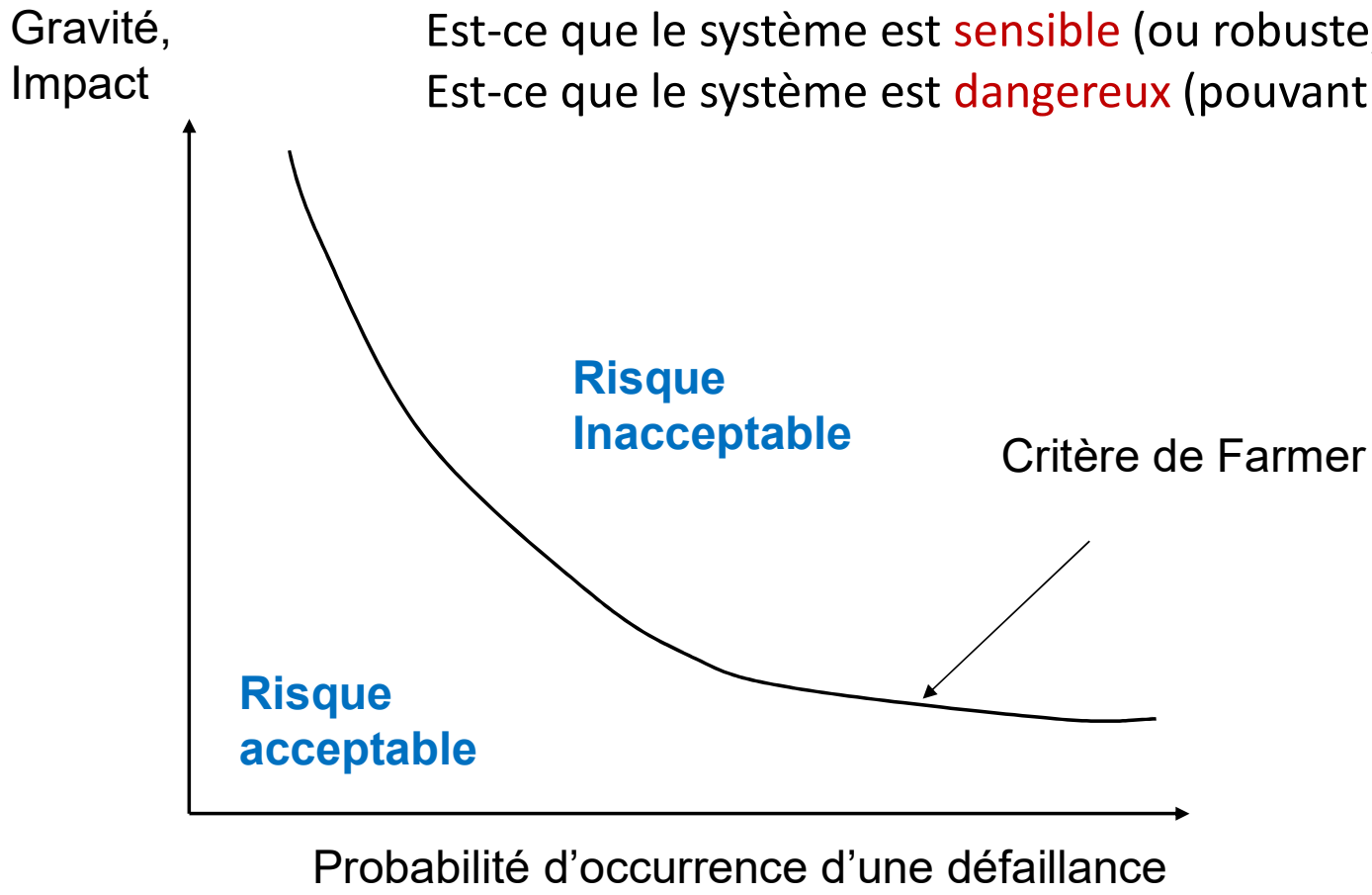
Elements of risks (Vulnerability)

- 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)

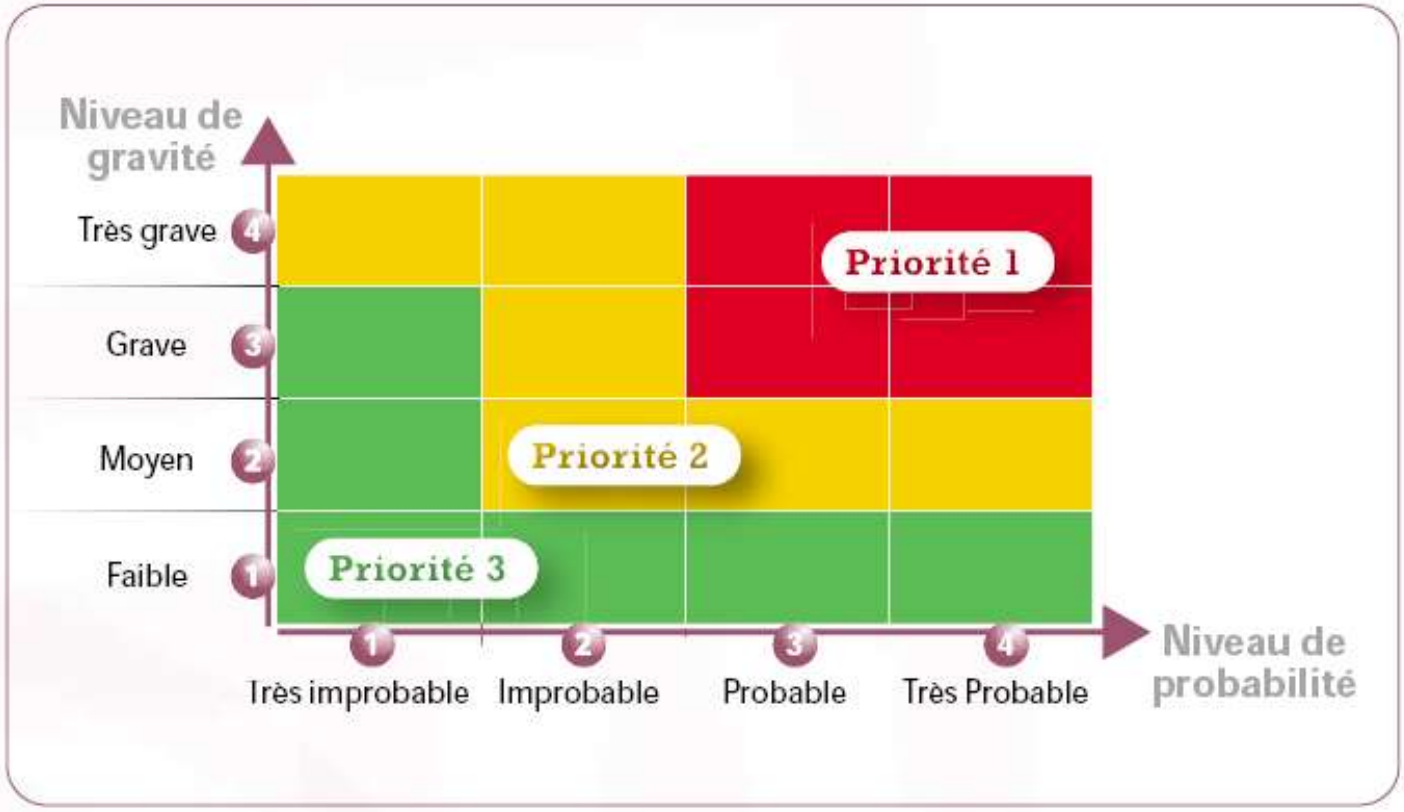
  - Most of the time, more than one control is employed to protect an asset.
  - Ex : the threat is an employee stealing trade secrets and selling them to the competitor
  - To address this threat, we may:
    - implement an information classification policy,
    - monitor outgoing e-mails,
    - prohibit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

Loi Gravité-Probabilité

Est-ce que le système est sensible (ou robuste, tolérant) aux défaillances ?
Est-ce que le système est dangereux (pouvant avoir un fort impact) ?



Evaluation des risques, évaluation de la gravité

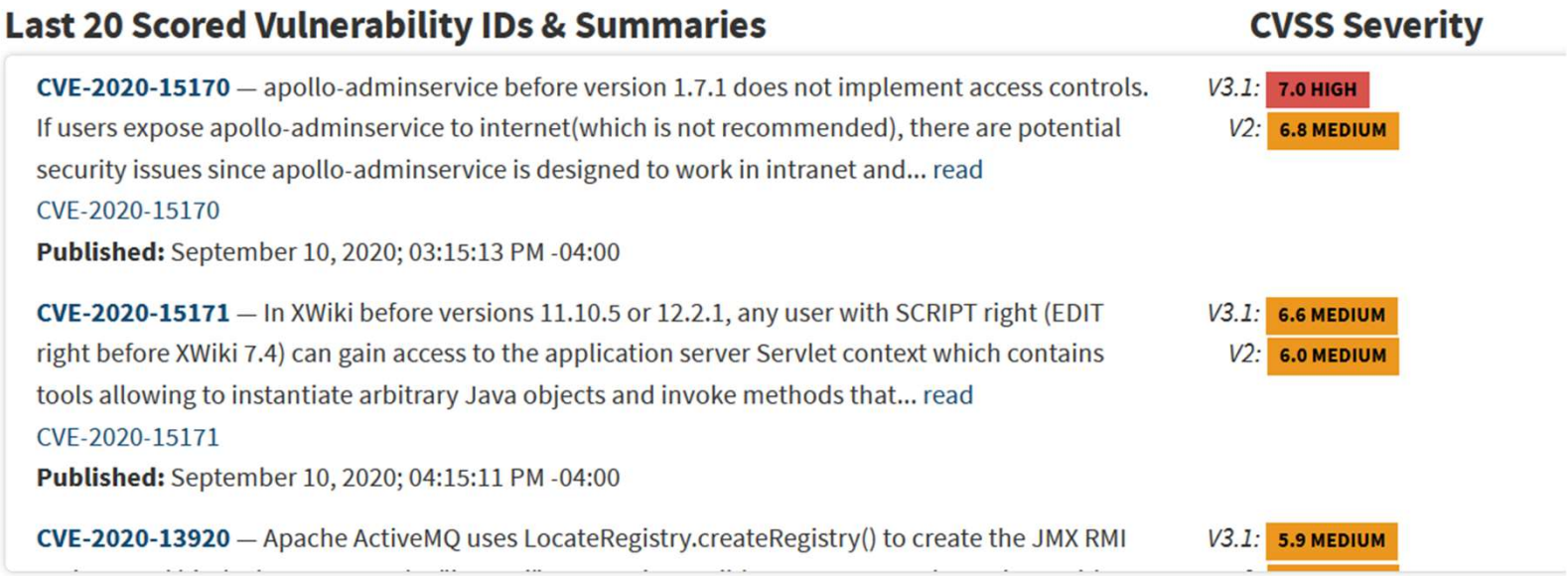


Exemple

Danger (cause)	Situa-tion dange-reuse	Evéne-ment dange-reux	Risque de …	Consé-quence	Gravité	Proba-bilité	Priori-tés	Obser-vations
Eclate-ment d'un pneu	Dérap-page du véhicu-le	Une vis dans le pneu	Acci-dent	Mort des passa-gers	4 (haut)	1 (bas)	2 (int.)	Avoir une roue de se-cours

Brainstorming

- Security risks around networks and information systems
- https://nvd.nist.gov/



Last 20 Scored Vulnerability IDs & Summaries | **CVSS Severity**

CVE-2020-15170 — apollo-adminservice before version 1.7.1 does not implement access controls. If users expose apollo-adminservice to internet(which is not recommended), there are potential security issues since apollo-adminservice is designed to work in intranet and... read
CVE-2020-15170
Published: September 10, 2020; 03:15:13 PM -04:00
V3.1: 7.0 HIGH
V2: 6.8 MEDIUM

CVE-2020-15171 — In XWiki before versions 11.10.5 or 12.2.1, any user with SCRIPT right (EDIT right before XWiki 7.4) can gain access to the application server Servlet context which contains tools allowing to instantiate arbitrary Java objects and invoke methods that... read
CVE-2020-15171
Published: September 10, 2020; 04:15:11 PM -04:00
V3.1: 6.6 MEDIUM
V2: 6.0 MEDIUM

CVE-2020-13920 — Apache ActiveMQ uses LocateRegistry.createRegistry() to create the JMX RMI
V3.1: 5.9 MEDIUM

Brainstorming: https://www.cert.ssi.gouv.fr/

ALERTES DE SÉCURITÉ

Les alertes sont des documents destinés à prévenir d'un danger immédiat

8 septembre 2021	CERTFR-2021-ALE-019	Vulnérabilité dans Microsoft Windows	Alerte en cours	
6 septembre 2021	CERTFR-2021-ALE-018	Vulnérabilité dans Atlassian Confluence Server et Data Center	Alerte en cours	
27 août 2021	CERTFR-2021-ALE-017	Multiples vulnérabilités dans Microsoft Exchange	Alerte en cours	
2 juillet 2021	CERTFR-2021-ALE-014	[MaJ] Multiples vulnérabilités dans Microsoft Windows	Alerte en cours	
13 juillet 2021	CERTFR-2021-ALE-015	Multiples vulnérabilités dans SolarWinds Serv-U	Alerte en cours	

AVIS DE SÉCURITÉ

Les avis sont des documents faisant état de vulnérabilités et des moyens de s'en prémunir

9 septembre 2021	CERTFR-2021-AVI-692	Multiples vulnérabilités dans les produits Palo Alto Networks
9 septembre 2021	CERTFR-2021-AVI-691	Multiples vulnérabilités dans Cisco IOS XR
9 septembre 2021	CERTFR-2021-AVI-690	Vulnérabilité dans ownCloud
9 septembre 2021	CERTFR-2021-AVI-689	Multiples vulnérabilités dans F5 BIG-IP
9 septembre 2021	CERTFR-2021-AVI-688	Multiples vulnérabilités dans Google ChromeOS
9 septembre 2021	CERTFR-2021-AVI-687	Vulnérabilité dans Xen
9 septembre 2021	CERTFR-2021-AVI-686	Multiples vulnérabilités dans WordPress
8 septembre 2021	CERTFR-2021-AVI-685	Multiples vulnérabilités dans les produits Fortinet

Egalement les systèmes industriels

des données, une exécution de code à distance et un contournement de la fonctionnalité de sécurité.

MULTIPLES VULNÉRABILITÉS DANS LES PRODUITS INTEL

CERTFR-2018-AVI-432 • *Publié le 12 septembre 2018*

De multiples vulnérabilités ont été découvertes dans les produits Intel. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire, un déni de service et une atteinte à la confidentialité des données.

MULTIPLES VULNÉRABILITÉS DANS GOOGLE CHROME

CERTFR-2018-AVI-431 • *Publié le 12 septembre 2018*

De multiples vulnérabilités ont été découvertes dans Google Chrome. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur.

MULTIPLES VULNÉRABILITÉS DANS ADOBE FLASH PLAYER ET COLD FUSION

CERTFR-2018-AVI-430 • *Publié le 12 septembre 2018*

De multiples vulnérabilités ont été découvertes dans Adobe Flash Player et Cold Fusion. Elles permettent à un attaquant de provoquer une exécution de code arbitraire, une atteinte à l'intégrité des données et une atteinte à la confidentialité des données.

MULTIPLES VULNÉRABILITÉS DANS SCADA LES PRODUITS SIEMENS

CERTFR-2018-AVI-429 • *Publié le 11 septembre 2018*

De multiples vulnérabilités ont été découvertes dans SCADA les produits Siemens. Elles permettent à un attaquant de provoquer un déni de service à distance, une atteinte à la confidentialité des données et une élévation de privilèges.

Prescriptions, Méthodes pour l'analyse de risques

- **Méthodes**

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

Déontologie

- Etudiants

  => signer une charte informatique

- Administrateur Réseau/Systèmes

  => responsabilité

- L'utilisation des méthodes décrites dans ce cours engage la responsabilité des utilisateurs !

Références

- 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
- EPFL, Industrial Automation course
- P_RAYMOND_BTS_MAI_Les_API
- W. Bolton, Automates programmables industriels, Dunod, 2015.
- Duc Tran Trung , Cybersecurity risk assessment for Unmanned Aircraft System, PhD, Univ. Grenoble Alpes, Feb. 2021
- 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

Références

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