



4. Safety and Cyber-security 1

<http://www.gipsa-lab.grenoble-inp.fr/~jean-marc.thiriet/asean/asean.html>

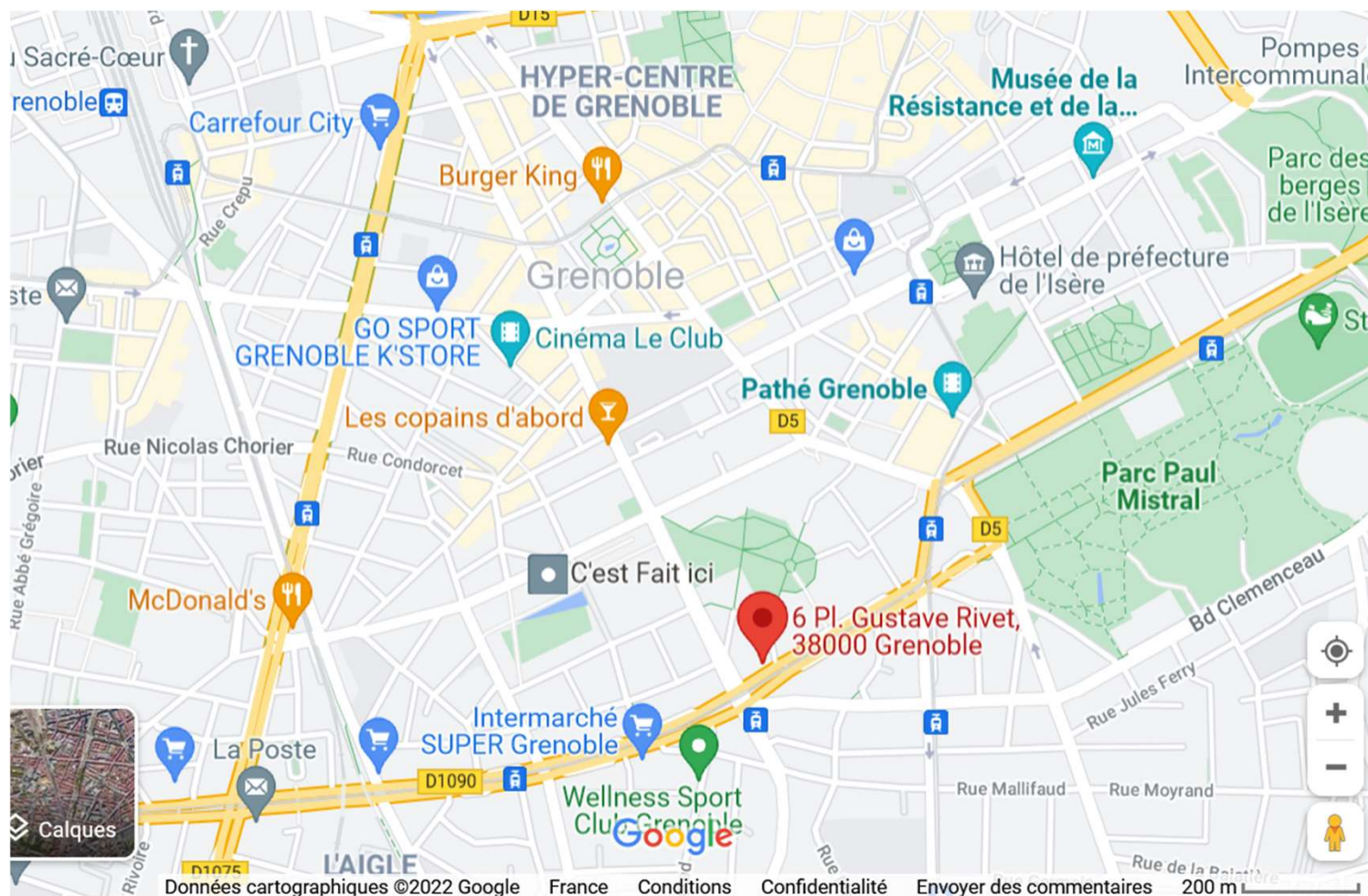


Asean-Factori 4.0 project

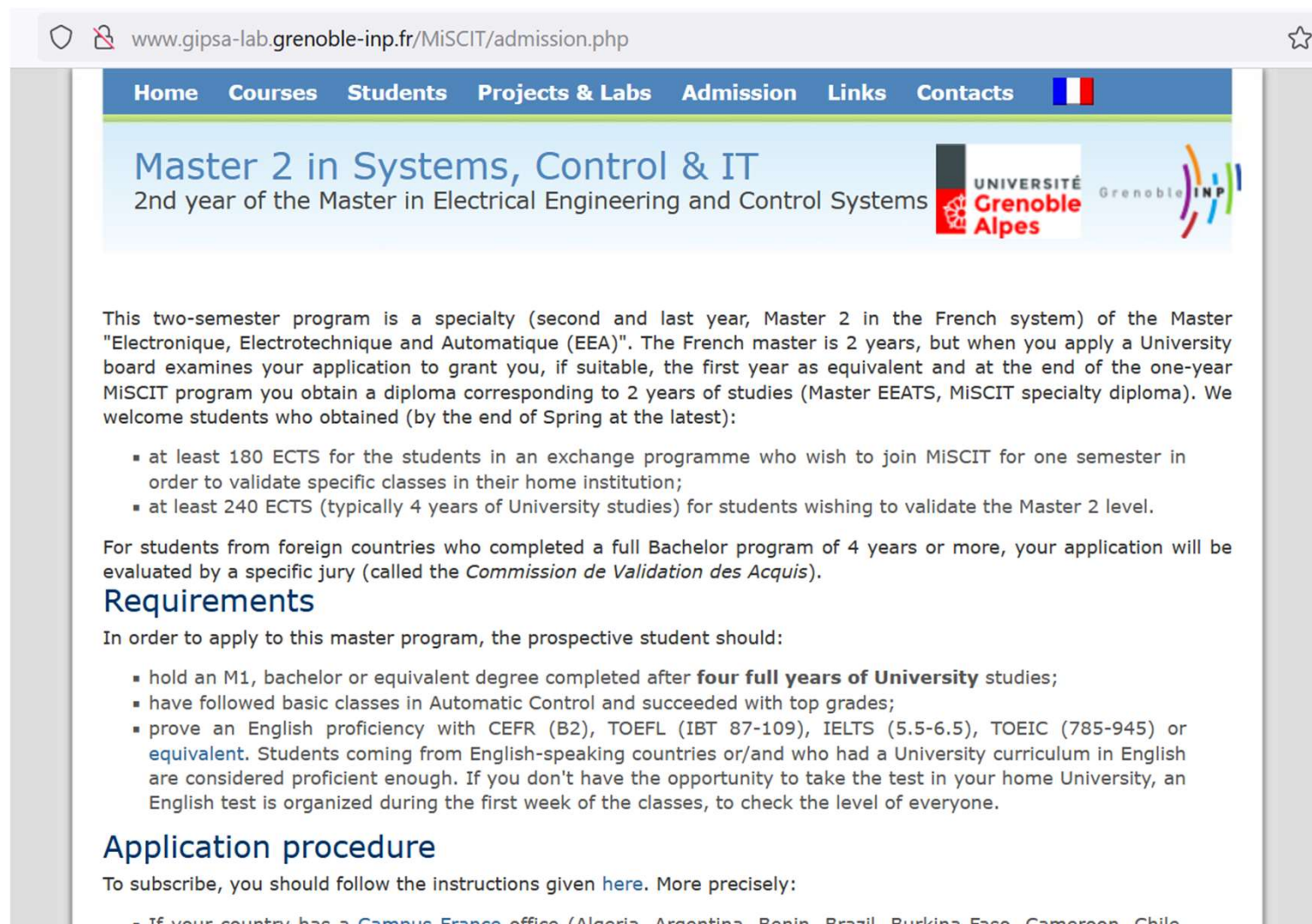
**Grenoble, 31st January,
11th February 2022**

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

UGA Grenoble – February 2022



Tram C, E
Bus 16

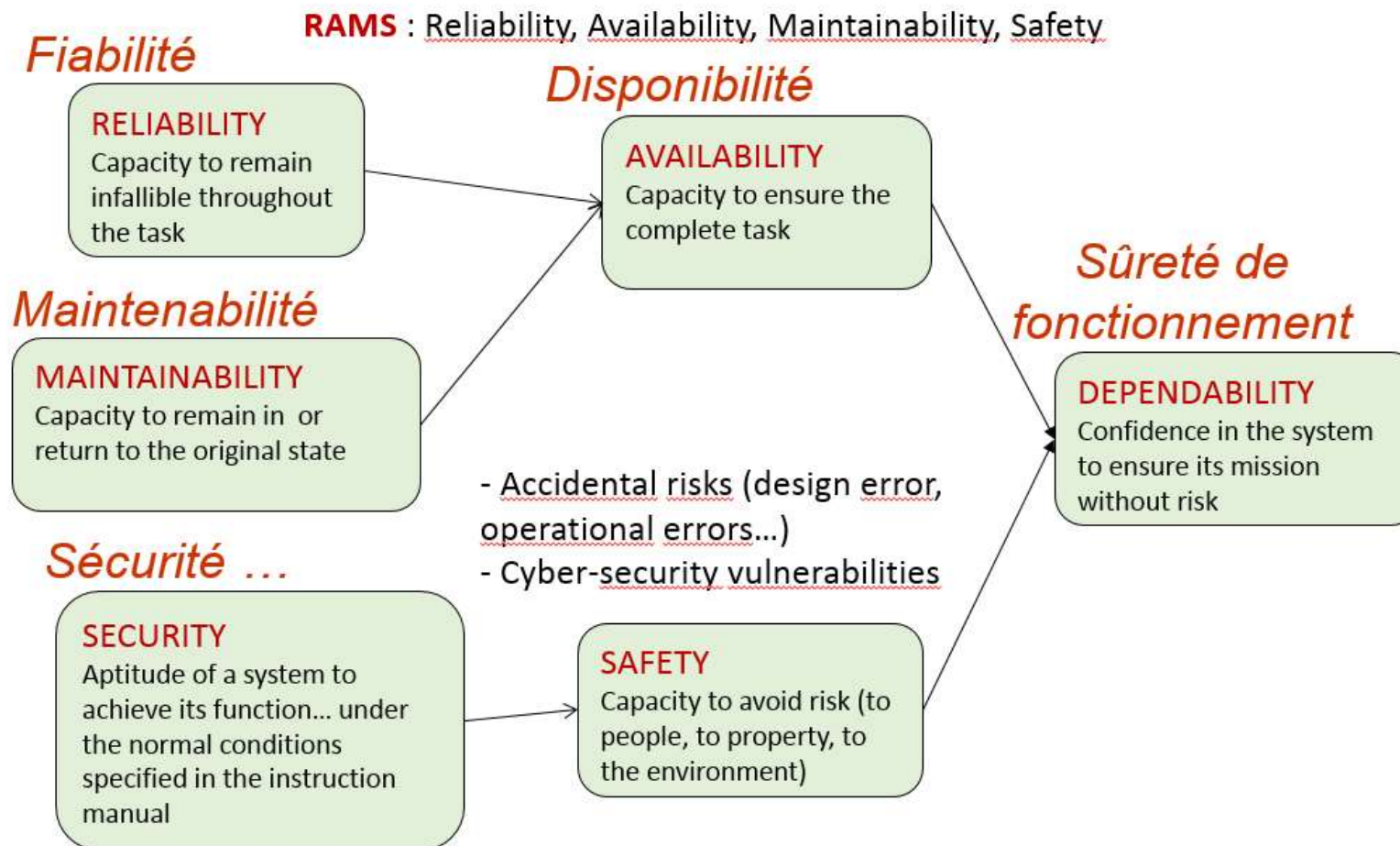


The screenshot shows a web browser window with the URL www.gipsa-lab.grenoble-inp.fr/MiSCIT/admission.php. The page has a blue navigation bar with links: Home, Courses, Students, Projects & Labs, Admission, Links, and Contacts. A French flag is also present. The main heading is "Master 2 in Systems, Control & IT" with the subtitle "2nd year of the Master in Electrical Engineering and Control Systems". Logos for "UNIVERSITÉ Grenoble Alpes" and "Grenoble INP" are displayed. The text describes a two-semester program as a specialty of the Master "Electronique, Electrotechnique and Automatique (EEA)". It states that the French master is 2 years, but a University board can grant the first year as equivalent. Students obtain a diploma corresponding to 2 years of studies (Master EEATS, MiSCIT specialty diploma). Requirements include at least 180 ECTS for exchange students or 240 ECTS for students wishing to validate the Master 2 level. For foreign students, a full Bachelor program of 4 years or more is evaluated by a specific jury. The page also lists requirements for prospective students: hold an M1, bachelor or equivalent degree completed after four full years of University studies; have followed basic classes in Automatic Control and succeeded with top grades; prove an English proficiency with CEFR (B2), TOEFL (IBT 87-109), IELTS (5.5-6.5), TOEIC (785-945) or equivalent. The application procedure section states that instructions are given [here](#). A list of countries with Campus France offices is provided: Algeria, Argentina, Benin, Brazil, Burkina Faso, Cameroon, Chile.

Emmanuel Witrant <emmanuel.witrant@gipsa-lab.grenoble-inp.fr>

Some 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 $(0, t>.$

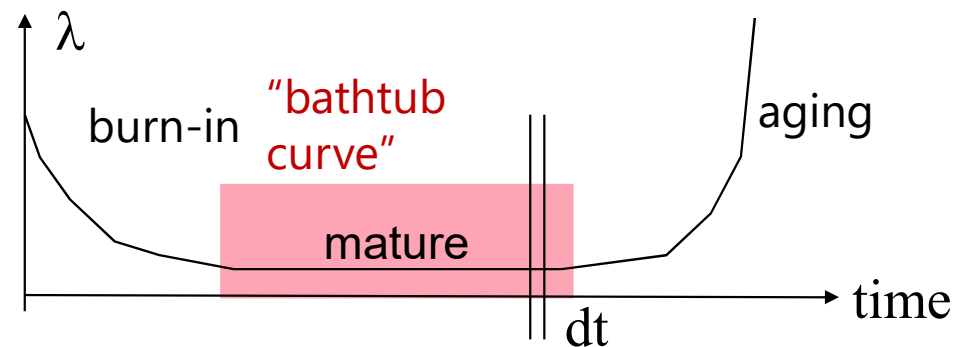
M(t) : probability that the system will be restored within a specified period of time t .

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 ?

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

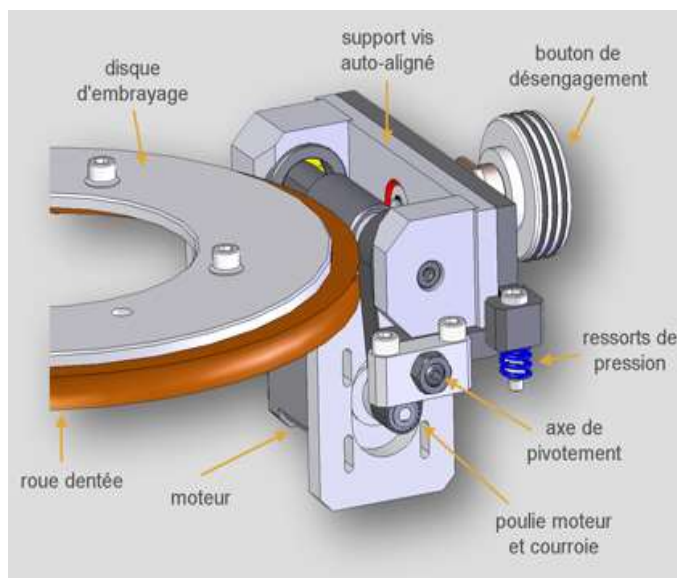


Failure rate **$\lambda(t)$** = probability that a (good) element fails during the next time unit dt

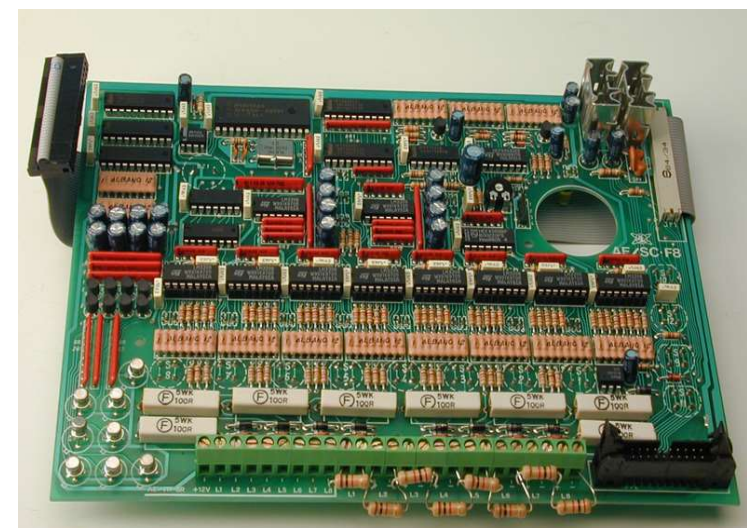
Dependability of classical Components

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

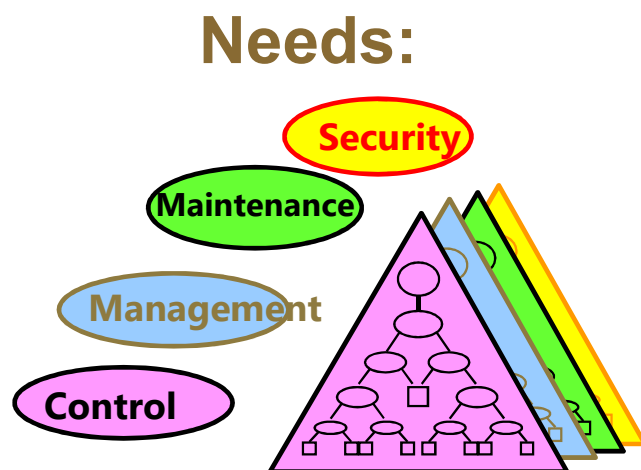
Mechanical systems



• Electronic systems

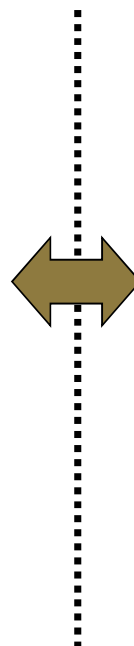
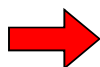


Context: Automation system evolution

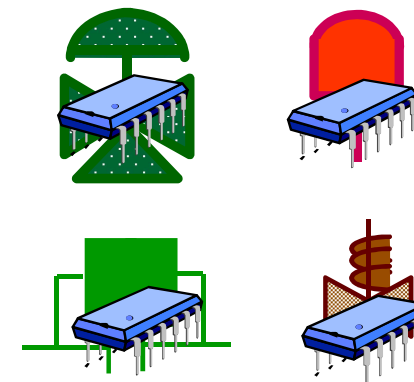


Increased number of services

More complex architectures



Components :



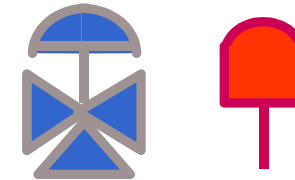
Various capacities and functionalities availability

Dependability hard to evaluate and to qualify

From analog to digital and from smart to intelligent...

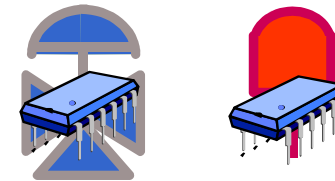
► Analog sensors and actuators

- 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

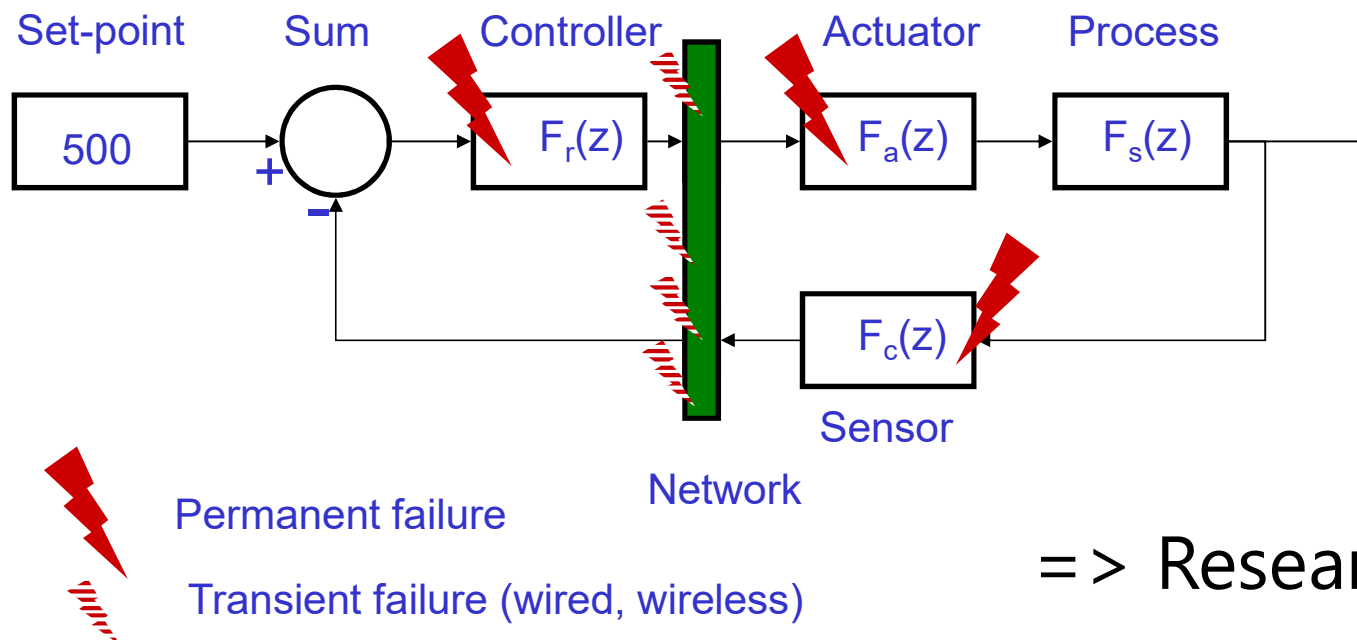
► « Intelligent » sensors and actuators

- Communicating Interface
- Diagnostic, 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)*

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	$10^{-4} < \text{PFD}_{\text{avg}} < 10^{-5}$	$10^{-8} < \lambda < 10^{-9}$
SIL3	$10^{-3} < \text{PFD}_{\text{avg}} < 10^{-4}$	$10^{-7} < \lambda < 10^{-8}$
SIL2	$10^{-2} < \text{PFD}_{\text{avg}} < 10^{-3}$	$10^{-6} < \lambda < 10^{-7}$
SIL1	$10^{-1} < \text{PFD}_{\text{avg}} < 10^{-2}$	$10^{-5} < \lambda < 10^{-6}$

Problems:

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

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 $\leq$ a certain %age of a reference value
 - ex 2: QUALITATIVE: the loss, or irremediable destruction of strategic data for the company

= 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...)

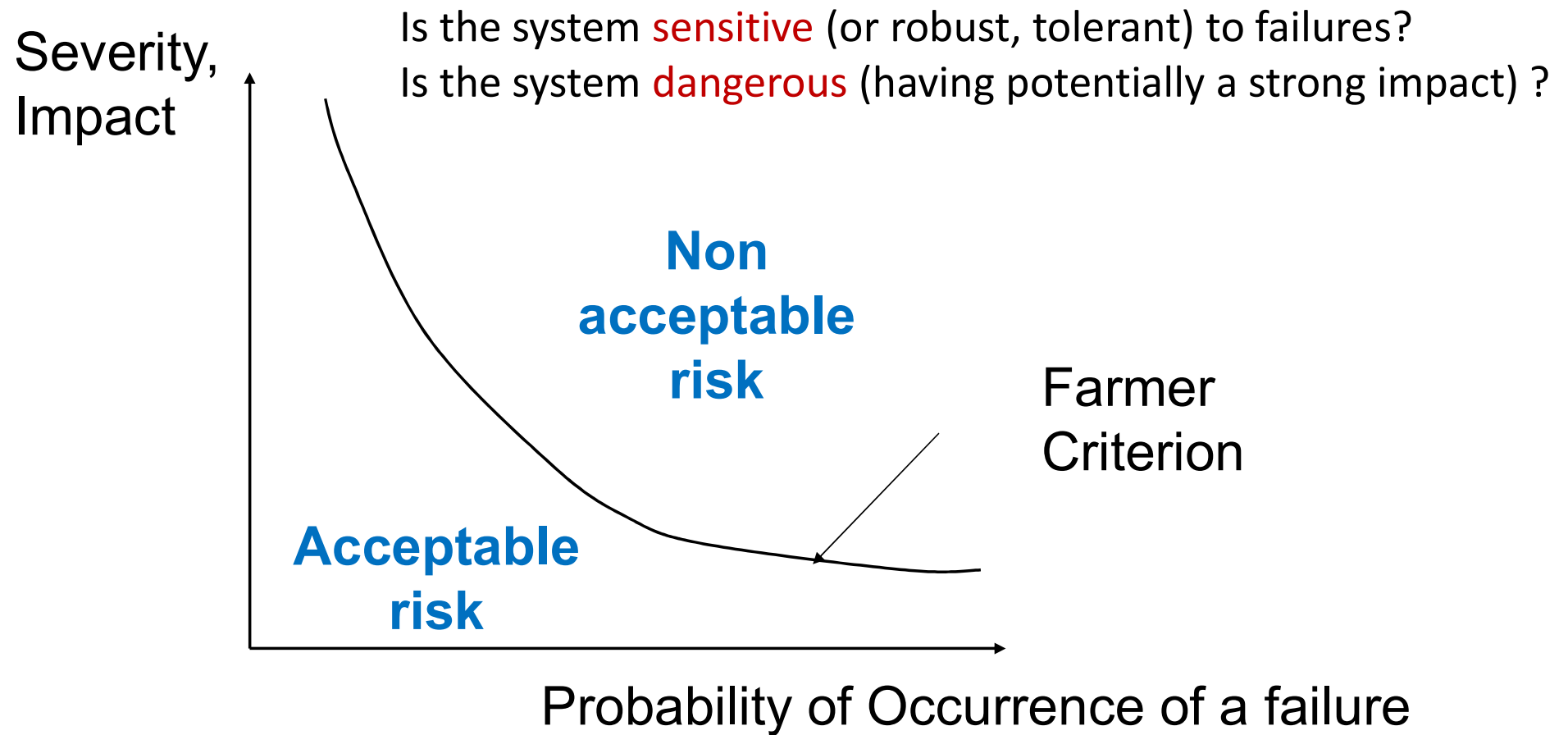
Elements of risks (Threat)

- 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 : $0.7 \times 0.33 = 0.231$ or 23.1 %

Elements of risks (Vulnerability)

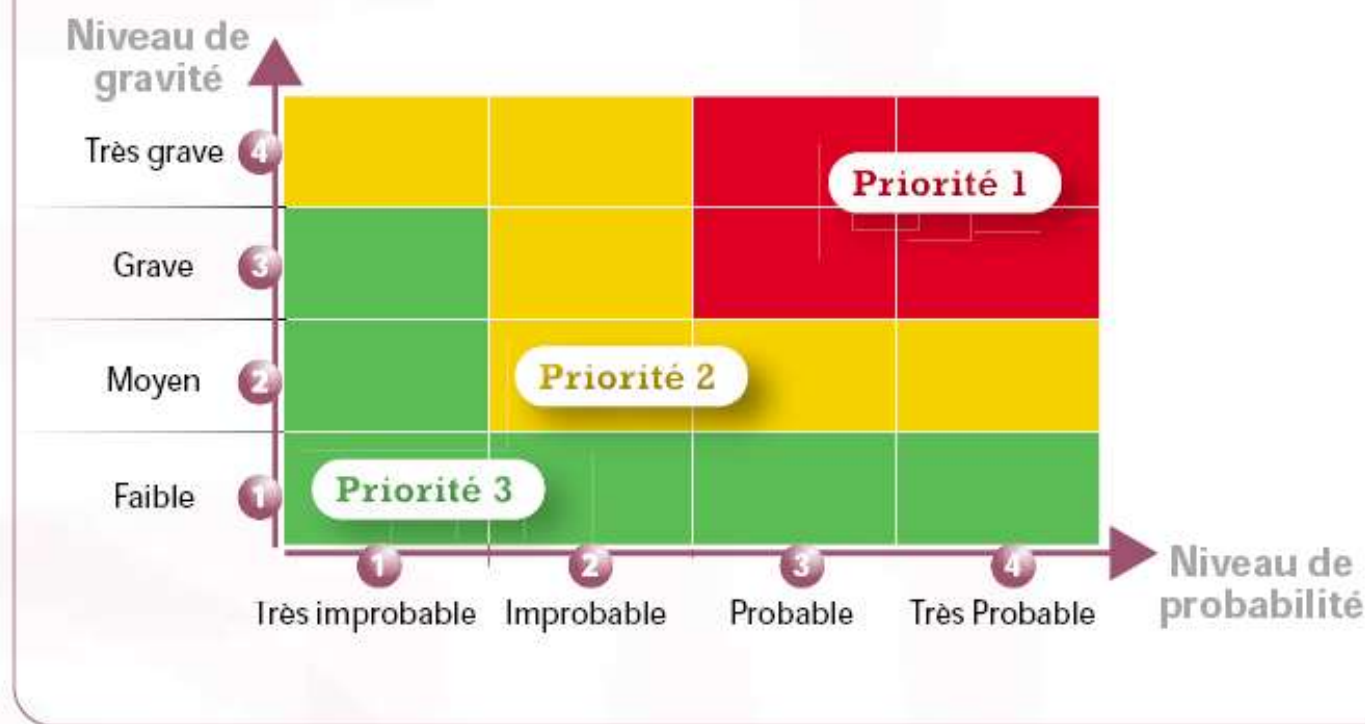
- Vulnerability (*vulnérabilité*)
 - Absence or weakness of cumulative controls protection in a particular asset
 - Estimated as percentages based on the level of control weakness
 - Control Deficiency (cd) is calculated by subtracting the effectiveness of the control by 100% -
ex : if we estimate that 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



Risks evaluation, evaluation of the severity

**Gravité =
Severity**



Example

Danger (cause)	Dangerous situation	Dangerous event	Risk of...	Consequence	Severity	Probability	Priorities	Observations
Explosion 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**

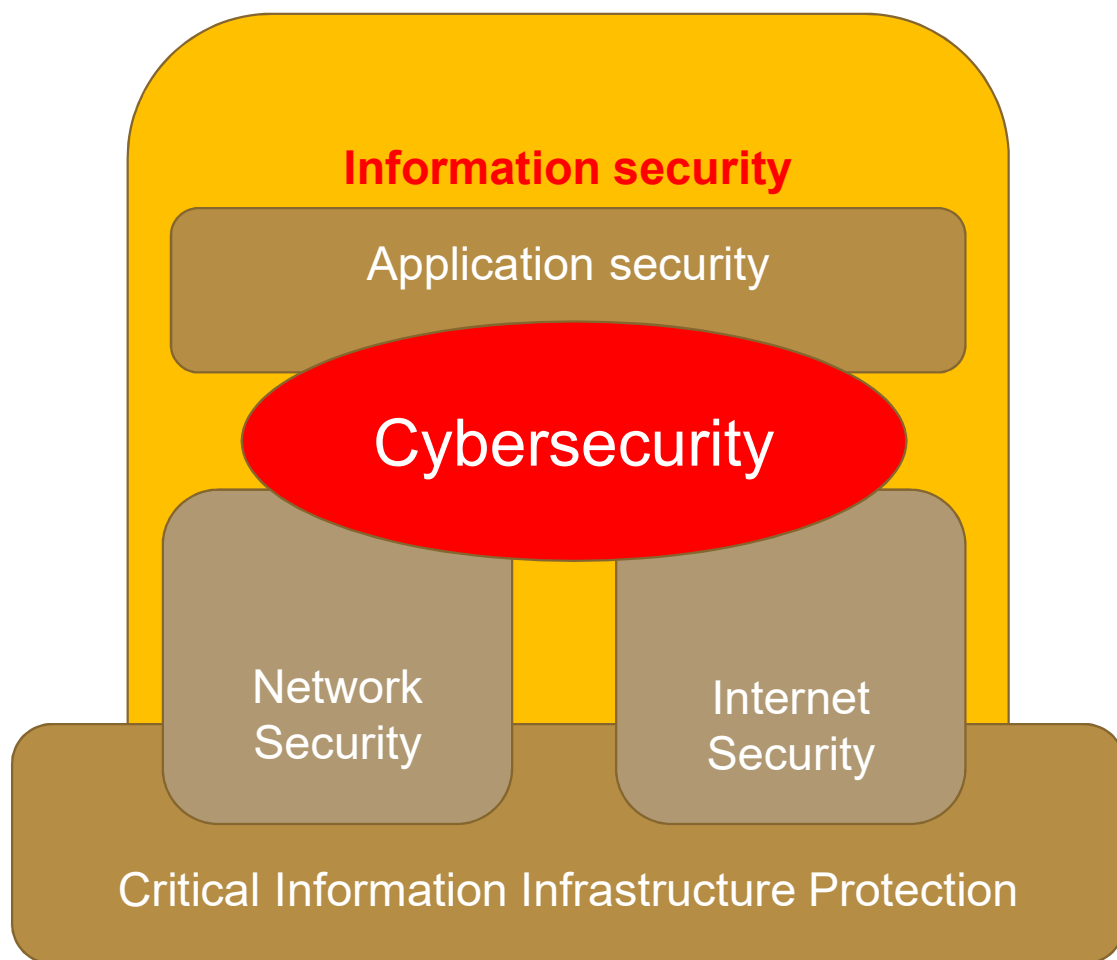
1. US standard NERC-CIP-002-3 Critical Cyber Asset Identification
2. US standard NIST.IR 7628 Guidelines for smart grid security
3. ISA/IEC 62443 Security for Industrial Automation and Control Systems
4. EU efforts about smart grid security
5. ANSSI Classification method and key measures

Cyber-Security

Some preliminary questions about cybersecurity (from Stéphane)

- What do you have to secure ?
 - Physical process, computers, networks, applications, data, people ?
- What do you mean by secure ?
 - Have to define a policy.
- Against which threats ?
 - There is no “absolute security”.
 - Vulnerabilities
 - Threat available resources
- What to do ? (choice of controls)
- How to do ? (security management)

General cybersecurity guidelines – ISO 27032



- CIIP : protection of critical industrial systems
- IS : General information security
- Application security : manage risk associated with application use (code, data, users)
- Network security : secure external and internal communication within organizations
- Internet security : protection of Internet-related services

Basic information security

- ISO 27000
- Information security : preservation of confidentiality ,integrity and availability of information CIA Triad
- In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved
- Resilience may also be of interest

CIA Triad

- **Confidentiality**: property that information is not made available or disclosed to unauthorized individuals, entities, or processes
 - Preserving **authorized restrictions** on information access and disclosure, including means for **protecting personal privacy and proprietary information**
- **Integrity** : property of accuracy and completeness
 - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity
- **Availability** property of being accessible and usable on demand by an authorized entity
 - Ensuring **timely and reliable** access to and use of information.
- Proof :
- Authenticity property that an entity is what it claims to be
- Non-repudiation : ability to prove the occurrence of a claimed event or action and its originating entities
- Reliability property of consistent intended behavior and results

Cybernetics from Greek κυβερνήτης (*kubernêtês*) => Used 19th and 20 century => ideas of control and communication

Cyber : Greek *kubernân*, to govern

Today used for everything relative to the « digital » world (internet, web...)

Cyber-security:

- Cyber security comprises technologies, processes and controls that are designed to protect systems, networks and data from cyber attacks. Effective cyber security reduces the risk of cyber attacks, and protects organisations and individuals from the unauthorised exploitation of systems, networks and technologies (<https://www.itgovernance.co.uk/what-is-cybersecurity>)
- État recherché pour un système d'information lui permettant de résister à des événements issus du cyberspace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense. (ANSSI, <https://www.ssi.gouv.fr/entreprise/glossaire/c/>)

Convergence between IT and cyber-physical systems (CPS)



US Black-out, 2003

- Integrity of the information and communication infrastructure
- Challenge: DEPENDABILITY (RAMS Reliability, Availability, Security & Safety, Maintainability)



EMBEDDED SYSTEMS

Drones
Autonomous vehicles
Connected objects

Maroochy shire, Stuxnet, CrashOverride

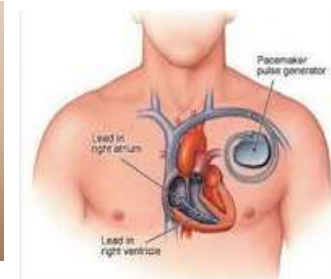
INFRASTRUCTURE

Industrial
Control
Systems (ICS)

Smart grids



Cyber attack ukrainian power network,
Dec. 2015



Overview of cyber attacks against ICS systems (from PhD Peter Matousek)

Year	Attack	Place
1982	Explosion of Siberian gas pipeline caused by a trojan which reset pump speeds and valve settings	Soviet Union
1997	Knock out of Worcester air traffic control communication	MA, USA
2000	Maroochy shire sewage spill	Australia
2003	Crash of the Safety Parameter Display System in Davis-Bess nuclear power plant by Slammer worm	OH, USA
2003	Shutting down of CSX train signaling system by Sobig virus	FL, USA
2005	Zotob virus knocked 13 of Daimler-Chrysler's manufacturing plants	USA
2010	Stuxnet virus damaged Iranian centrifuges by increasing and decreasing their speed and pressure beyond normal levels	Iran
2014	Disrupted control system in German steel mill	Germany
2015	Power outage off Ukrainian power plant distribution caused by BlackEnergy malware	Ukraine
2016	Industroyer malware attack on Ukrainian power grid	Ukraine
2017	Cyber-espionage attack against aerospace and energy industry by APT33 group	USA
2019	Cyber attack against chemical giant Bayer	Germany
2019	Intrusion attack against U.S. Energy sector by KA-MACITE group	USA
2019	Cyber attack against Kudankulam nuclear power plant	India
2020	Compromising supply chain of Solarwinds software used in industrial environment	USA
2021	Ransomware attack against oil distribution company Colonial Pipeline	USA

FIREWALLS DÉDIÉS AUX RÉSEAUX INDUSTRIELS

Une cyber-attaque peut impacter l'outil de production et provoquer :

- Une marche irrégulière ou dégradée
- Des arrêts intempestifs
- L'activation d'actions dangereuses pour les biens et les personnes
- Un arrêt complet avec rançon pour pouvoir redémarrer
- Le vol de données de fonctionnement pour utilisation ultérieure

Comparison between ICS and classical IT systems

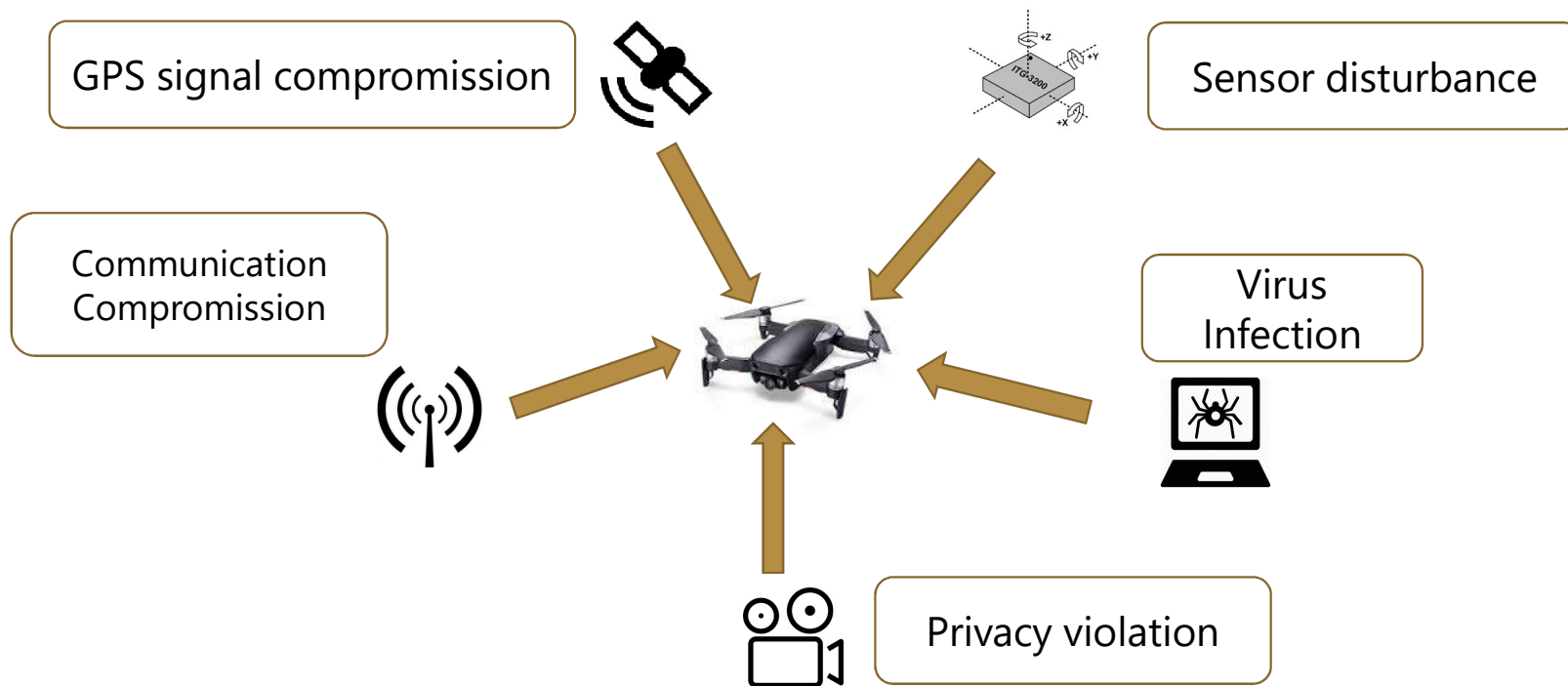
**IT
Information
Technology**

**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

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 completeness

Ex: methodologies in the industrial domain

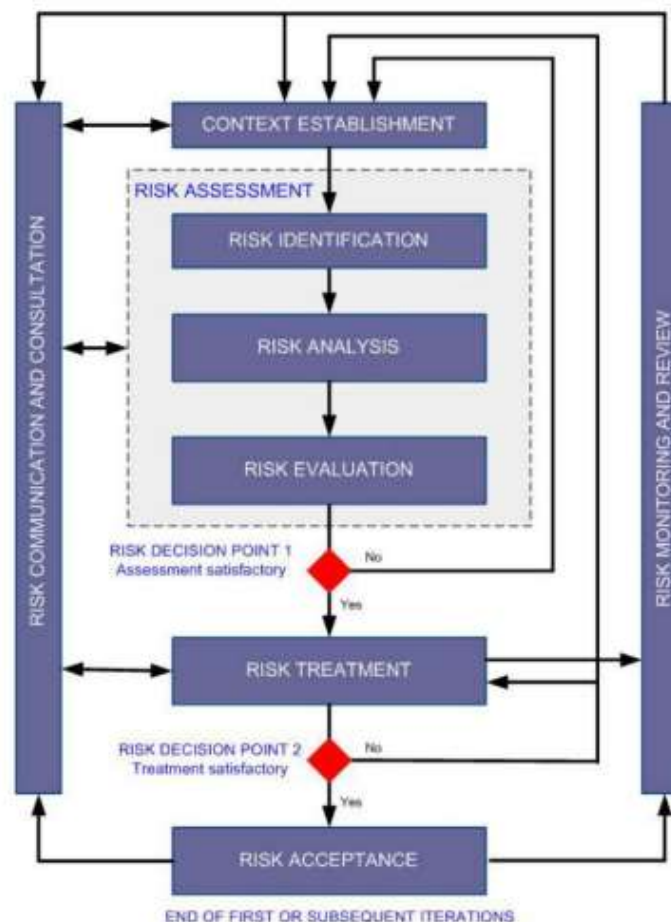
○ **ISO27005 Standard:** Information security risk management
Propose a work-flow

○ **MEHARI[12]:**

- IT Security in companies
- Databases
- Security Evaluation Tools

○ **ED202A/DO326A Standard:**

- Avionics security
- During the process of aircraft development



Risk Assessment: Safety and Cyber-security

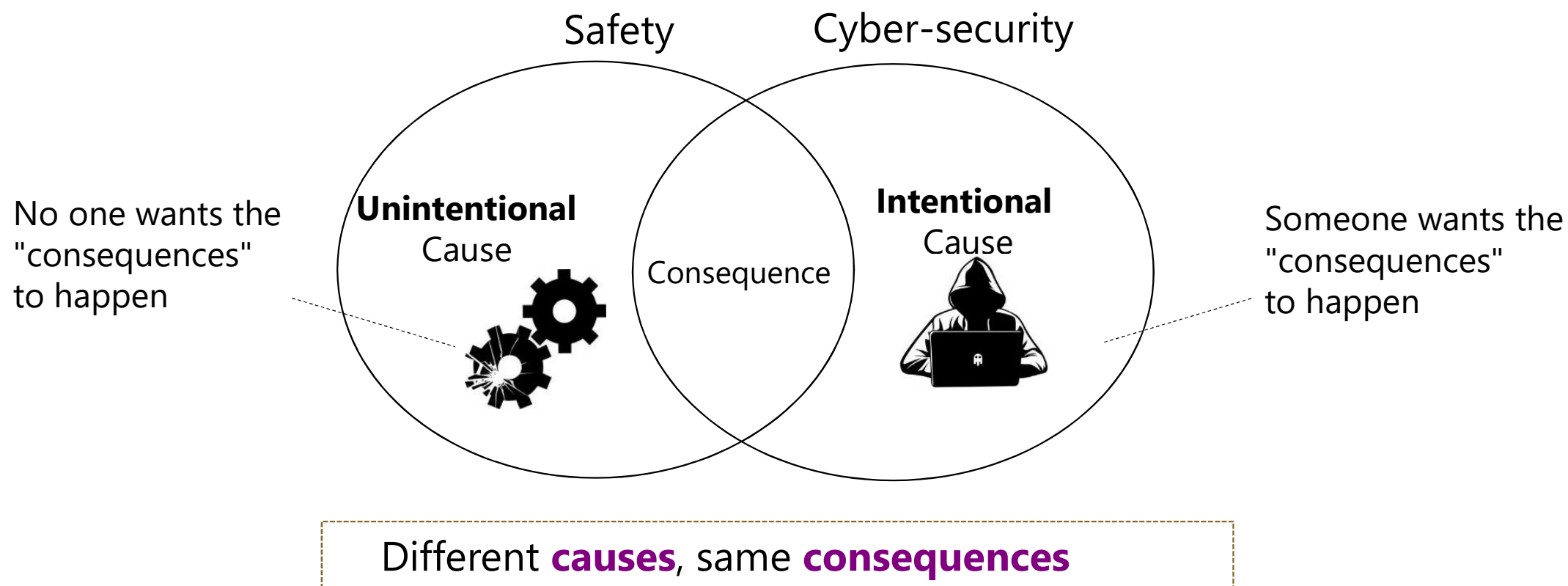
[Phd TRAN Trung Duc 2021]

Safety
 Cyber-security
 Safety et Cyber-security

Reichenbach et al 2012	Puys et al. 2017	Schmittner et al. 2014	Mäurer et al 2019	
Schneier 1999	Abdo et al. 2017	Idrees et al 2009	Haass et al 2018	Kharchenko et al. 2018
Gorbenko et al. 2006	Kmenta et al. 1998	Wang et al. 2009	Fussell et al. 1970	Nikodem et al. 2018
MÉHARI	IEC 62443	ISO/SAE 21434	ED 203	
ISO 27005	IEC 61508	IEC 61508	ARP 4761	SORA
IT	ICS (Industry Control System)	Cars	Aeronautics	Drone

Safety and Cyber-security

[Phd TRAN Trung Duc 2021]



Attacks?

Why do pirates take an interest in organizations IT or individuals computers ?

- Motivations change
 - 80s and 90s: lots of enthusiastic hackers
 - Nowadays: Mostly organized and thoughtful actions



Why do pirates take an interest in organizations IT or individuals computers ?

• Cyber Delinquency:

- Individuals attracted by the lure of gain
- The "hacktivists"
- Political, religious, etc.
- Direct competitors of a targeted organization
- Civil servants in the service of a country
- Mercenaries acting for the account of sponsors...



Types of targets

- **Convenient target** (*cible opportune*)
 - By "chance": detected by the pirates in the search of least protected machines or servers
 - What to do?: update the systems
 - To test the system (try to find faults)
- **Chosen target** (*cible de choix*)
 - Precise Target: strategic interest of the company ...

Types of attacks (1/3)

- DoS (Denial of service) : To decrease the system capabilities
 - DDoS (Distributed DoS) : idem but with an attack coming from several sites (<http://grc.com/dos/grcdos.htm>)
 - SYN Flood: the attacker floods a system with SYN synchronization packets in order to initiate connection requests (these requests are never finished) => strong exploitation of the processor resources, memory, network cards => Denial of service
 - UDP Flood: attack which submerges a system with UDP packets => prevent it from treating the valid requests for connection (often on the DNS port 53) (ICMP Flood: idem to submerge a system with ICMP messages (Internet Control Message Protocol) by using the Ping utility)
 - Ping of Death: possibility to "ping" with a too huge packet which can cause a whole range of uncontrolled reactions on the targeted system: Denial of service, shut down, freezing or restarting

Types of attacks (2/3)

- Scan of ports: Packets sent by using the port numbers in order to scan available services, hoping that a port answers
- Eavesdropping: the goal is to violate the confidentiality of the communication (by sniffing packets on the local area network or by intercepting wireless communications)
- Man-in-the-middle: the attacker acts between the two ends of the communication as if he were the awaited interlocutor: harmful effects on the confidentiality and possibly the integrity

Types of attacks (3/3)

- Java/ActiveX/ZIP/EXE: dangerous Java components or Active X hidden in Web pages, Trojan dissimulated in a ZIP/TAR or EXE file
- Breaking into a system: by violating the authentication or the access control, the attacker obtains the possibility of controlling the communication: effects on the confidentiality and the integrity
- Virus: shortcuts the authentication and the access control with the aim of carrying out destroying code: effects on the availability of the machine and/or the network
- Trojan: virus hidden in a function usually used, program being carried out on the pirated machine to send information to the pirate
- Worm (*ver*): explore and automatically exploits the faults of a system, without action of the user => problems of availability

Detection of attacks

- By human beings (culture)
- By specialised software or hardware (anti-virus, firewalls)
- By ports normally non open (alert scans)
- By abnormal reactions
 - During connections, when you are absent
 - Of the applications (slow, double validation)
- By abnormal overloads
 - Network resources
 - Processor, disk, memory resources
- By invalid data
- By data losses

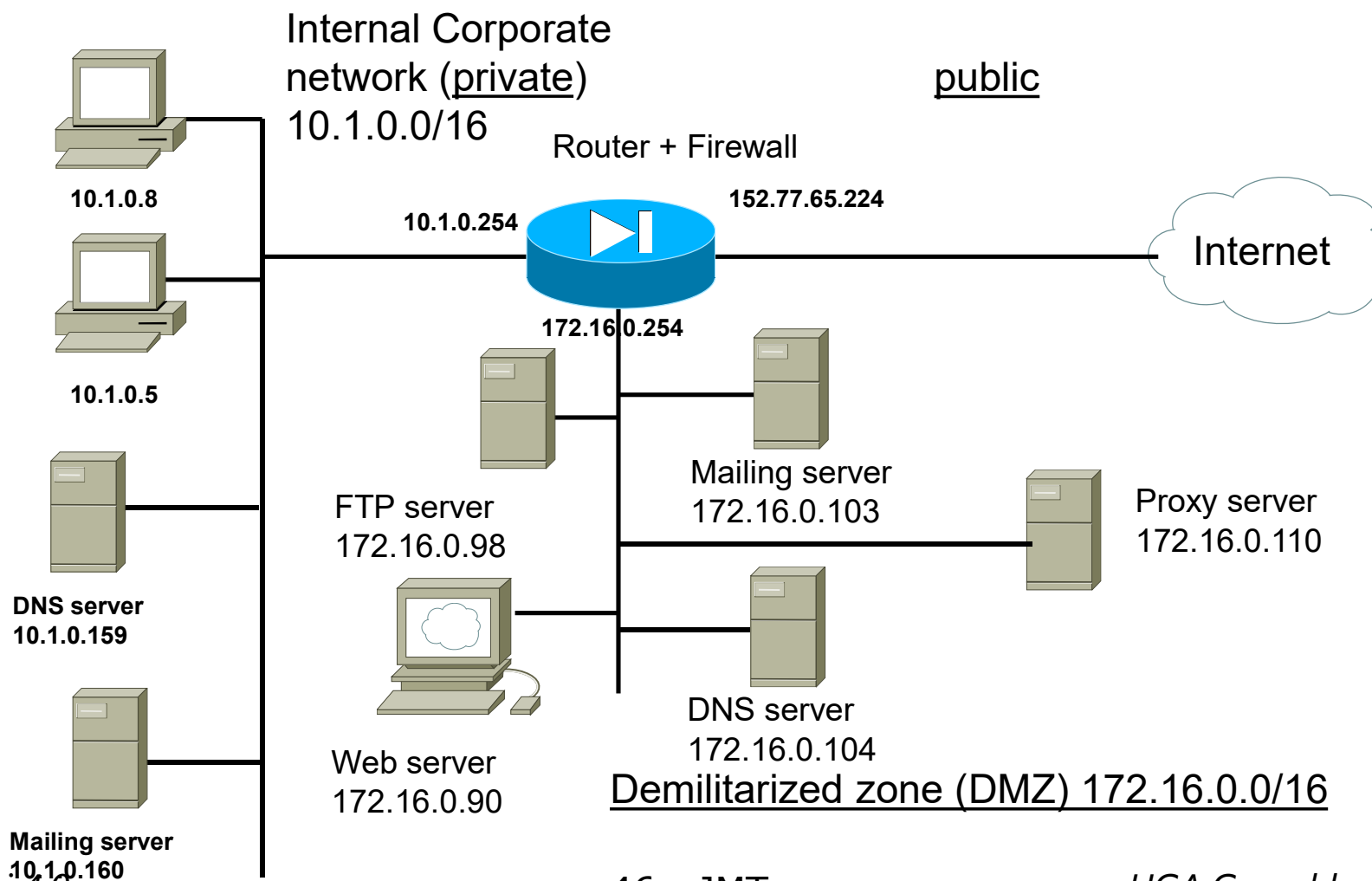
Every abnormal event should incite to remain very
“attentive” !

Organizations for security

- CERTA (Centre d'Expertise gouvernemental de Réponses et de Traitements des Attaques Informatiques / French governmental Center of Expertise for Answers and Treatments of the Data-processing Attacks)
 - www.certa.ssi.gouv.fr
- SANS (SysAdmin, Audit, Network, Security)
 - www.sans.org
 - Research on information security
- SCORE (Security Consensus Operational Readiness Evaluation)
 - www.sans.org/score
 - Community of professionals in security
- ISC (Internet storm center)
 - <http://isc.sans.org>
 - Logs (journal) concerning detections of intrusion
- ANSSI
 - www.ssi.gouv.fr
 - Agence Nationale de Sécurité des Systèmes d'Information

Firewalls, Demilitarized Zone

A network with a **firewall/router**...



Stateful firewall: Dynamic ACL

- **Dynamic** filtering
 - **Stateful inspection firewall:** packet filters that take into consideration OSI-layer 4 (**particularly TCP**) => if a connection is authorized, every packet within this exchange will be implicitly accepted
 - Dynamic entries for responses to the TCP, UDP, ICMP requests
 - Does not require to keep open the static ports (the ports remain open only during the time of the session)
- Follow-up/monitoring of the TCP sequence numbers
 - Monitoring of the sequence numbers of the input and output packets to follow-up communication flows
 - Protection against “man in the middle” attacks and session hackings

Dynamic ACL

- Follow-up of specific applications (example of protocols)
 - Cu-SeeMe (port 7648): PTP videoconference
 - FTP (port 21)
 - HTTP (port 80 or 8080)
 - HTTPS (port 443)
 - DNS (Domain Name Server): port 53
 - H.323 (port 1720): multi-media communication (VoIP, video, audio)
 - ICMP: repairing of problems (administrator) + used by the pirates => to let pass only ICMP messages generated inside the network
 - MCGP (Media Control Gateway Protocol, port 2427): VoIP
 - MSRPC (Microsoft Remote Procedure Call Protocol, port 135): communication of inter-systems process

Example

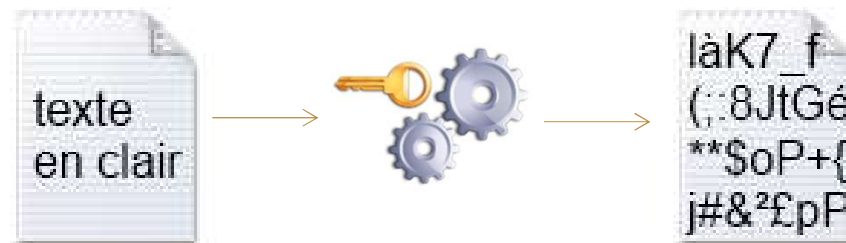
- ACL (Access Control List)
- Access-list list_number Order (Permit/Pass or Deny/Block) Protocol (4th, 3rd, 2nd layer) source (machine or a network) Destination (machine or a network) port number (application)
- Access-list 121 Permit TCP/UDP 10.10.10.0/24 any http
- Access-list 121 Permit TCP/UDP 10.10.10.0/24 DNS_SERVER dns
- Access-list 121 Deny any any any any
- Access-list 121 Permit TCP/UDP 10.10.10.0/24 any 80
- Access-list 121 Permit TCP/UDP 10.10.10.0/24 DNS_SERVER 53
- Access-list 121 Deny any any any any

Cryptography basics

a. Definitions

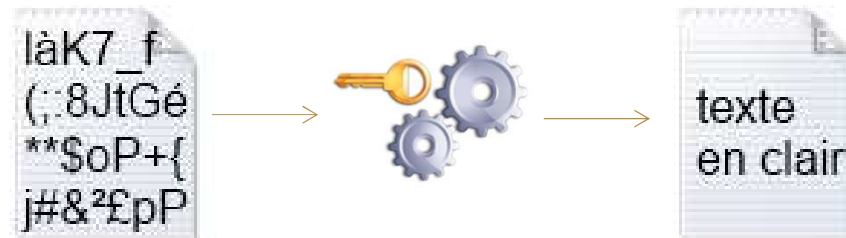
Encryption

Transform data such that it became unreadable. Only authorized entities may read the encrypted data.



decryption

Transform data previously encrypted such that it became readable. Only authorized entities may decrypt data

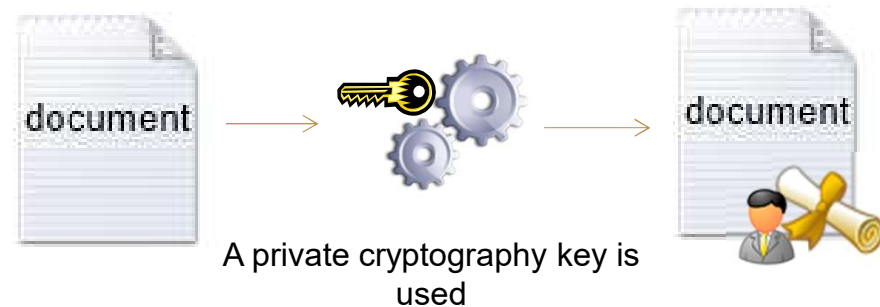


Cryptography basics

a. Definitions

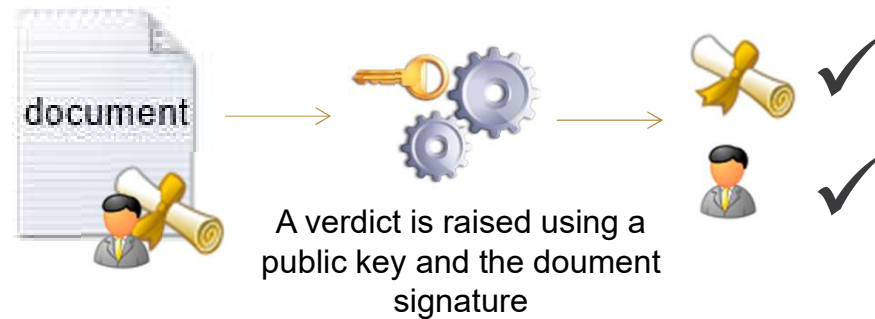
Sign

Create an electronic signature that uniquely identifies data and sender.



Signature check

Checks that the data was not tampered and the sender is genuine.



Cryptography basics

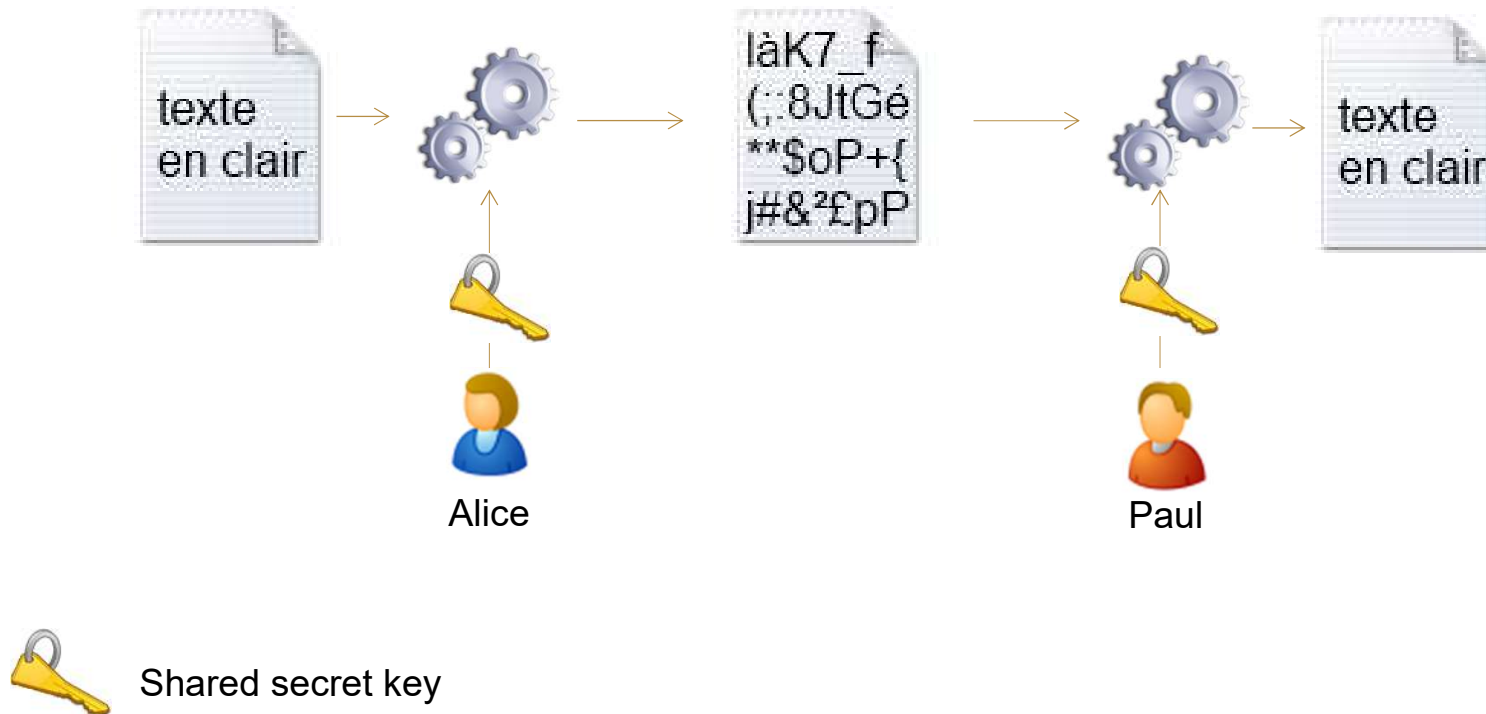
Symmetric encryption

- The same key is used to encrypt and decrypt the document
- The weak point is that key has to be kept secret !
- Faster than the asymmetric encryption

Cryptography basics

Symmetric encryption

- Alice wants to send a secure message to Paul



Cryptography basics

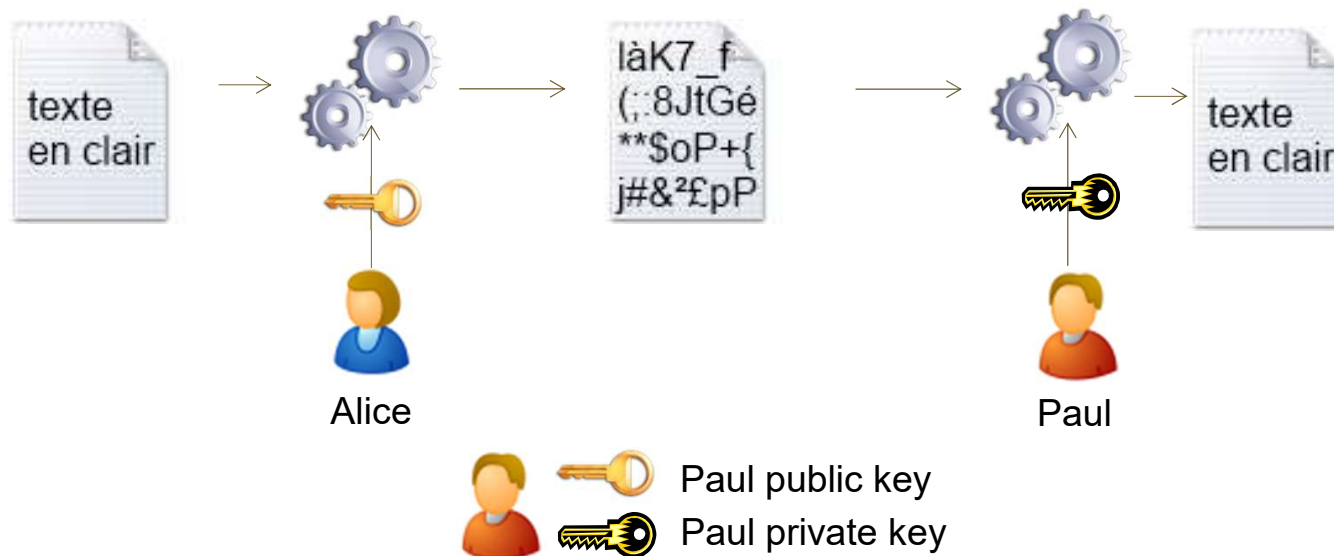
Asymmetric encryption

- Two different keys are used, one to encrypt the second one to decrypt:
 - Public key : anyone can obtain this key ;
 - Private key : only the owner has access, it has to be kept secret
- The two keys are mathematically related
 - Knowing the public key does not allow effective calculation of the private key
 - Each use owns two key : the private that must not be communicated and the public key which can be given to anyone.

Cryptography basics

Asymmetric encryption

- Alice wants to send an encrypted message to Paul
 - Alice encrypts the message with Paul public key ;
 - Only Paul may decrypt the message using his private key;
 - Notes :
 - Alice never needs (and she cannot) use Paul's private key !
 - Alice does not need to use her own keys in this example while she does not sign the message.



Cryptography basics

Symmetric vs asymmetric encryption

Symmetric encryption

- Faster (XOR functions, logical functions)
- Short keys (512 bits are enough)

Advantages

Asymmetric encryption

- Keys are ease exchanged. Ony public keys hve to be exchanged
- A Public Key Infrastructure can ba managed

Disadvantages

- Keys are difficult to be exchanged as secrecy has to be kept.
- It is not possible to manage the secret shared keys guaranteeing the secrecy...

- Operations are long (modulo exponential)
- Needs longer keys (at least 4096 bits) ;

Some well known algorithms

- AES.

- RSA.

Cryptography basics

Electronic signature

Insures that data was not tampered and the sender is genuine. If the signature is not valid that means that the sender identity is missused or the the data was modified

Note :

- **Electronic signature does not insure confidentiality**, but integrity and proof;
- **When one encrypts a message it is recommended to sign it also** in order to grant the sender identity

Cryptography basics

Electronic signature

1. A hash (fixed size code) is generated from the message;
 - Hash computing algorithm are public. The hash is not a secret. ;
 - The chance to obtain the same hash from two different message is very small.
2. The signature algorithm uses the hash and the private key to generate the authentication key (the actual signature) ;
3. The sender will send the message and the signature ;
4. The receiver computes the hash;
5. The receiver checks the authenticity using the public key of the sender, the hash and the signature

Cryptography basics

Security certificates

An important issue is related to the authenticity of the keys themselves



Anyone can obtain the public key of everybody using key servers. How may one be sure **that « Public key of Paul » actually belongs to Paul** and it was not generated by someone who missused Paul identity ?

Another point : when visiting a web site (a bank) how can one be sure that the web site is genuine and not a fake ?

- Solution : security certificates.

Cryptography basics

Security certificates

A security certificate (digital certificate, public key certificate, identity certificate) is **a file** containing :

- The **Public key** of a person (corporate of web site) ;
- Identity details of the owner (name, address) . ;
- The **digital signature** of a trusted entity that issued the certificate.;
- Information related to the validity of the key, allowed usage etc.

The trusted entity will :

- **Check the identity** of the person asking for the certificate;
- **Creates the certificate** after verification, **and digitally signs it** (with the private key of the trusted entity) ;
- **Keeps up to date a list of certificates which were retired** (for example if the key was compromised).

Cryptography basics

Security certificates

How to recognize a trusted entity ?

- Directly integrated by the editors in the operating system and browsers;
- User may add new certificates if it chooses to trust them.

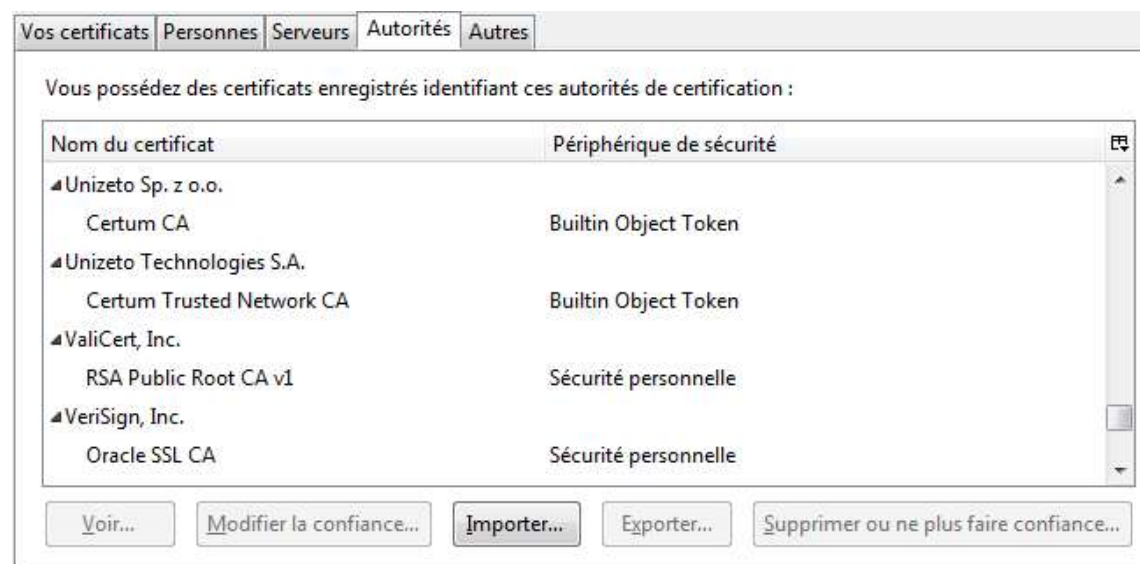


Image : magasin de certificats de Firefox

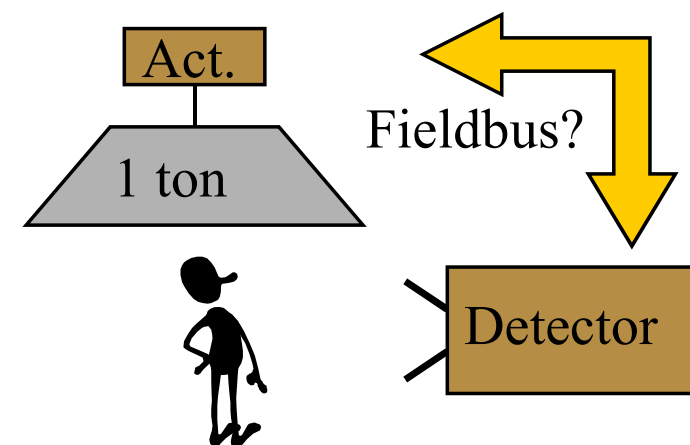
Some references

- J.F. Aubry, Nicolae Brnzei – 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, Feb. 2021
- Blaise Conrard – Cours sur les Réseaux de Sécurité – Université de Lille

Safety Networks

Safety networks

- 2 aspects of operational safety (see also IEC 61508)
 - Reliability, Maintainability, Availability
- For networks:
 - Offer network **monitoring** and administration services
 - Allow the implementation of **redundancy mechanisms** (master, medium...), watchdog...
- Safety
 - Ensure the non-occurrence of dangerous events



Safety and networks

- Objective
 - Extend networks from the « control" function to the "safety" function.
- Interests
 - Gain of **implementation**
 - Easy detection and localization of **faults**
- Obstacles
 - Technical: **response time** required is often shorter than for the control function
 - Constraint: for any fault the system should switch to a **safe mode**...
 - **Regulations**: compliance with normative aspects, need for certification

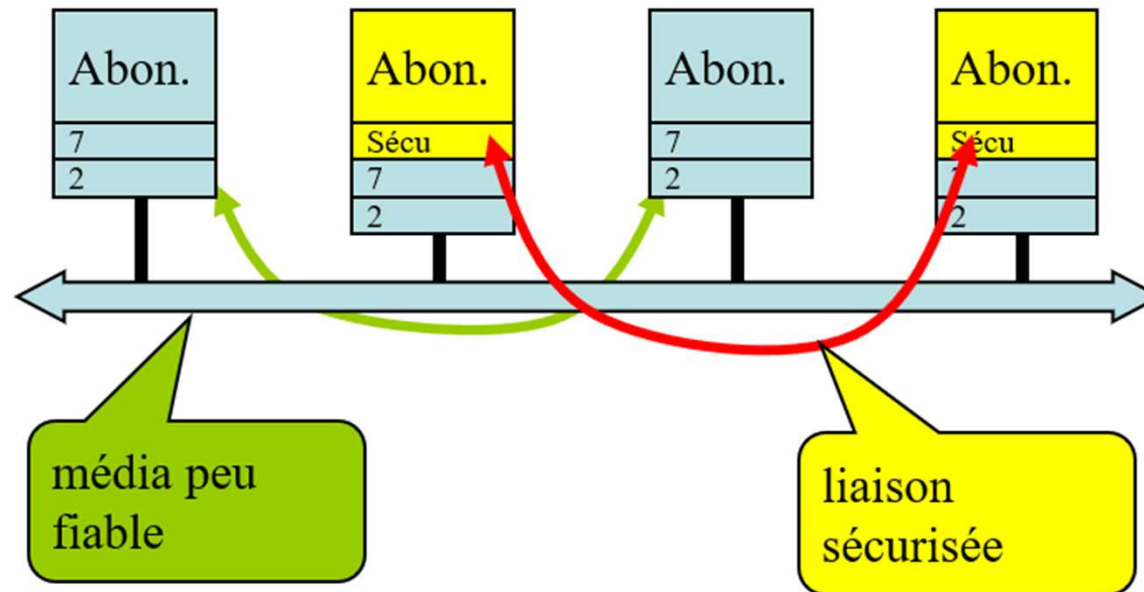
Safety by levels (EN 954)

Cat.	Prescriptions / Behaviour
B	a fault can lead to the loss of the safety function
A1	idem but with a lower probability thanks to proven principles
A2	a fault → loss of the safety function between control intervals
A3	for a single fault, the safety function is assured
A4	for several faults, the safety function is assured

Safety and networks

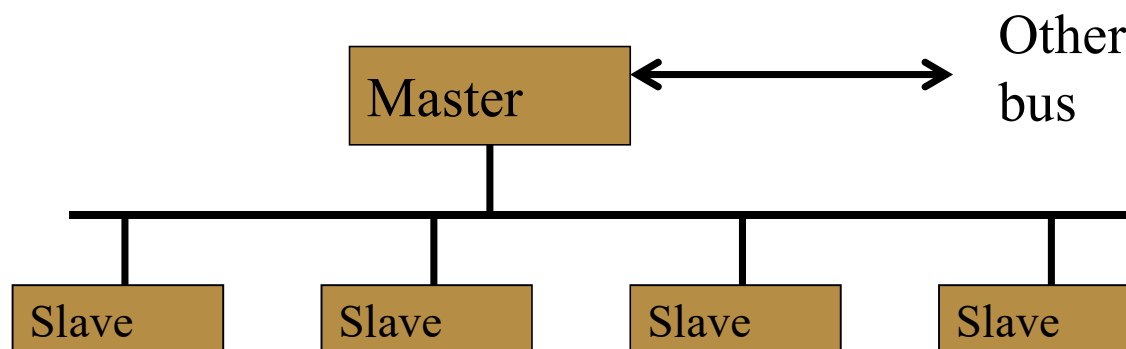
Commonly used principle :

- secure overlay



General information:

- Developed by the companies SICK and PILZ
- 1 master / several slaves (up to 60)
- Standard cable (2 conductors)
- Tree topology (500m at 125Kb, 100m at 500kb)
- Response time between 20 and 100ms

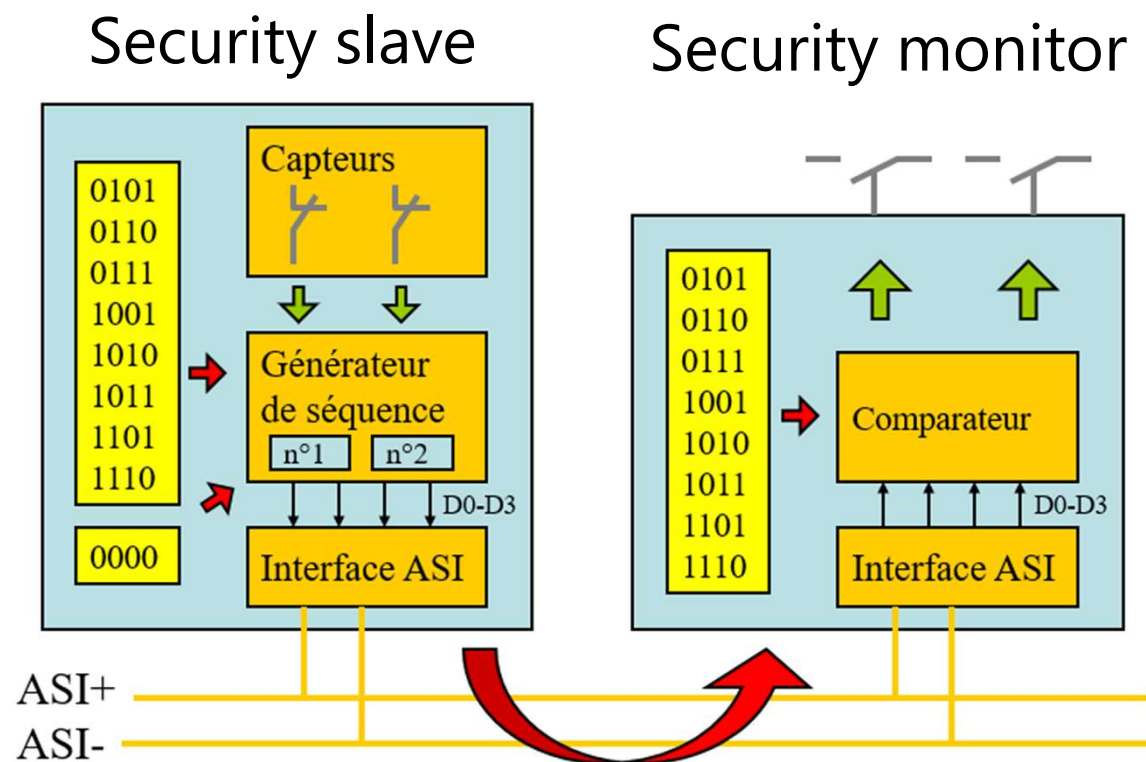


ASI Safety at Works

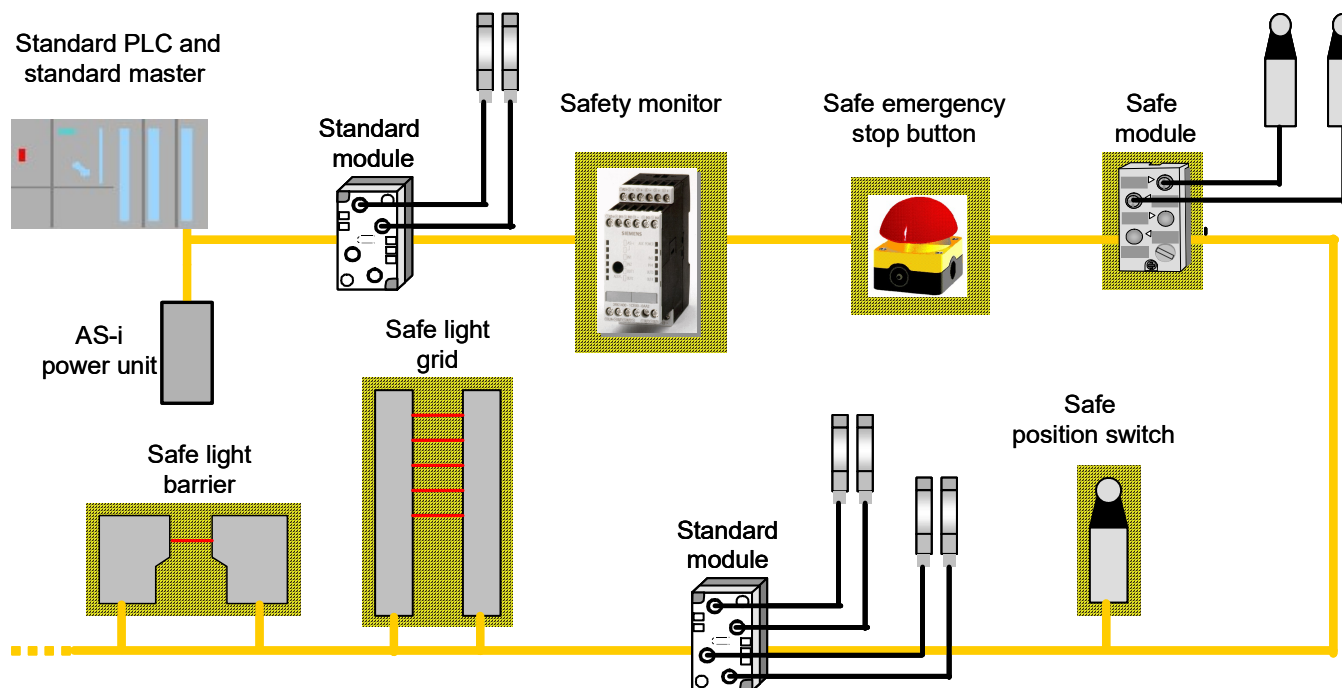
ASI Safety at Works: transmission sequence

Principle

- extension to the classical AS-i protocol
- A safety monitor added – continuous monitoring
- Specific safety code table for each slave
- Power supply stop by the monitor (safety relay)
(stop, com. interruption, mess. corrupt, response delay)



ASI Safety at Works



Advantages

- cabling reduction
- Safety and non-safety on one bus
- Groups of safety signals
- EN 954 – 1 category 4 compliant
- Certified: TUV and BIA
- No AS-i wiring changes needed

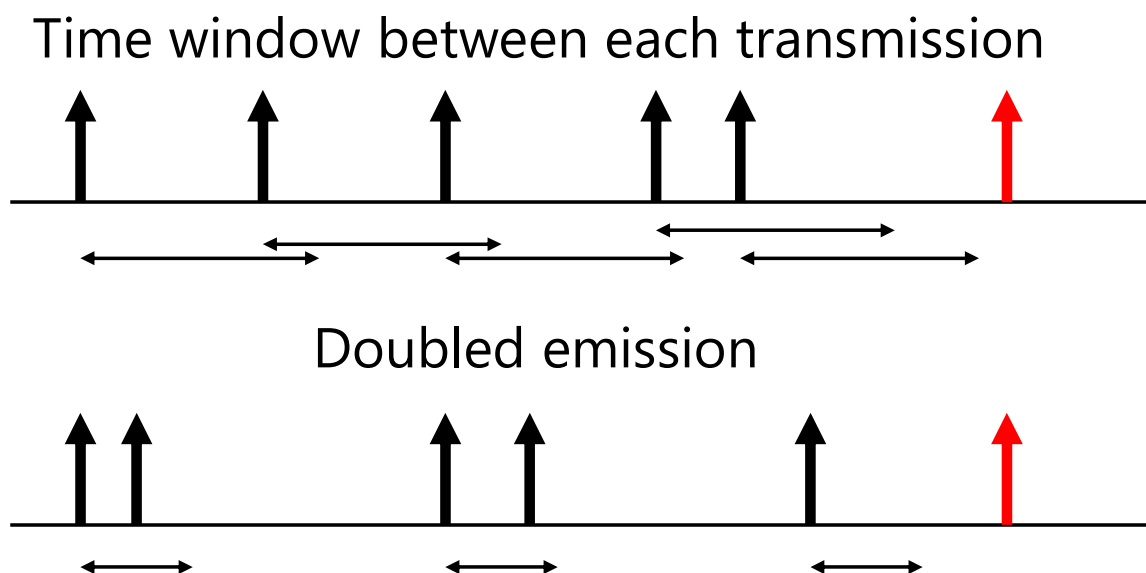
ASI Safety at Works

- ASI is a standard communication bus with finite and fast response times, dedicated to sensors-actuators: it contains error detection and recognition mechanisms (see chapter 5) [SCH 01], [LET 02]. The idea of "ASI Safety at work" is to extend the capabilities of ASI in order to add properties to make it safe and to mix operation traffic with safety traffic on the same bus; users can thus extend their existing installation with safety components.
- The principle is based on the co-existence, on the same network, of conventional components and safety components. A monitor is used to evaluate both safety-related signals and safety-related systems such as emergency stop devices and light curtains.
- This monitor is passive, it does not transmit any communication. The role of the monitor is to listen to all safety traffic and to detect consecutive sequences of four zero bits. Four consecutive zeros indicate that something has gone wrong, either a user has triggered a safety system and pressed an emergency stop, or faults have been detected on the communication bus or on one of the components. Without worrying about the cause of the error, as soon as four consecutive bits are detected at zero, the monitor puts the system in the fallback position that has been programmed. It is possible to have several monitors on the network, each controlling a part of the automation system.
- The safety components can be connected to the ASI Safety at work network via a safety slave. The ASI Safety at work network has been certified by TÜV and BIA as category 4 in accordance with EN 954-1 [Std 954]. Translated with www.DeepL.com/Translator (free version)

CAN Open Safety

Security CANOpen:

- Difficulties related to non-deterministic access, but arbitration → estimated maximum time
- Use of 2 watch dogs:



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-EI%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
 J.F. Aubry – Cours de Sûreté de Fonctionnement, INPL Lorraine, 2005.
 J.C. Laprie & al. – Guide de la sûreté de fonctionnement – Cépaduès, 1995.
 A. Villemeur – Sûreté de fonctionnement des systèmes industriels – Editions Eyrolles, Paris, 1988.
 S. Ghernaouti-Helie – *Sécurité informatique et réseaux*, 4^{ème} édition – Dunod, 2013
 Security for industrial communication systems, Dacfe Dzong, Martin Naedele, Thomas P. Von Hoff, Mario Crevatin, pp. 1152-1177, Proceedings of the IEEE, Vol. 93, n° 6 "Industrial Communication Systems", June 2005
 La sécurité des réseaux-First steps, Tom Thomas, Cisco Press, 2005
 Les réseaux, édition 2005, G. Pujolle, Eyrolles 2004
 Course of Jean-Luc Noizette, ESSTIN, Nancy
 G. Avoine, P. Junod, P. Oechslin – Sécurité informatique, exercices corrigés – Vuibert, Paris, 2006.
 S. Mocanu – courses, G-INP, Grenoble.
Sécurité et espionnage informatique : connaissance de la menace APT, Cédric Pernet, Eyrolles
Guide d'autodéfense numérique, éditions Tahin Party
Cybertactique : Conduire la guerre numérique, Bertrand Boyer, Nuvis
Learn Social Engineering, Dr E. Orzkaya, 2018, Packt

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

Merci pour votre attention
Merci pour votre attention



សូមអរគុណចំពោះការយកចិត្តទុកដាក់
របស់អ្នក។ (KH)

ຂອບໃຈຫຼາຍໆ ສໍາ ລັບຄວາມສົນໃຈຂອງ
ທ່ານ (LAO)

ขอบคุณมากสำหรับความสนใจของคุณ
(TH)

**Merci pour votre
attention**

**Thank you for your
attention**

