FACTORI 4.0
Erasmus +

UGA
Université
Grenoble Alpes

SOME CONSIDERATIONS ON DEPENDABILITY ISSUES AND CYBER-SECURITY OF CYBER-PHYSICAL SYSTEMS

Jean-Marc THIRIET, Univ. Grenoble Alpes

cnrs Grenoble INP UNIVERSITÉ Grenoble Alpes UMR 5216

Convergence between IT and cyber-physical systems

US Black-out, 2003

Industrial Control Systems (ICS)

Smart grids

Cyber attack ukrainian power network, Dec. 2015

- Integrity of the information and communication infrastructure

→ Challenge: DEPENDABILITY (RAMS Reliability, Availability, Security & Safety, Maintainability)

Drones
Autonomous vehicles
Connected Objects

Maroochy shire, Stuxnet, CrashOverride

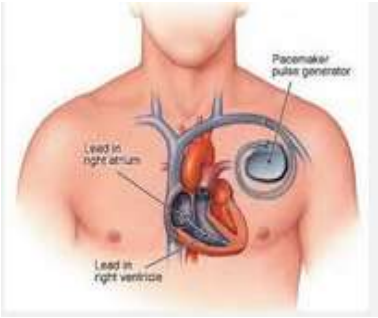
Cyber-physical systems

Remote-control and autonomous Vehicles

- Embedded circuits
- Smart devices
- Embedded networks
- Wireless networks
- Internet of things
- Ubiquitous networks
- Ambient intelligence
- Smart grids
- Health
- …

Sensor and actuators networks

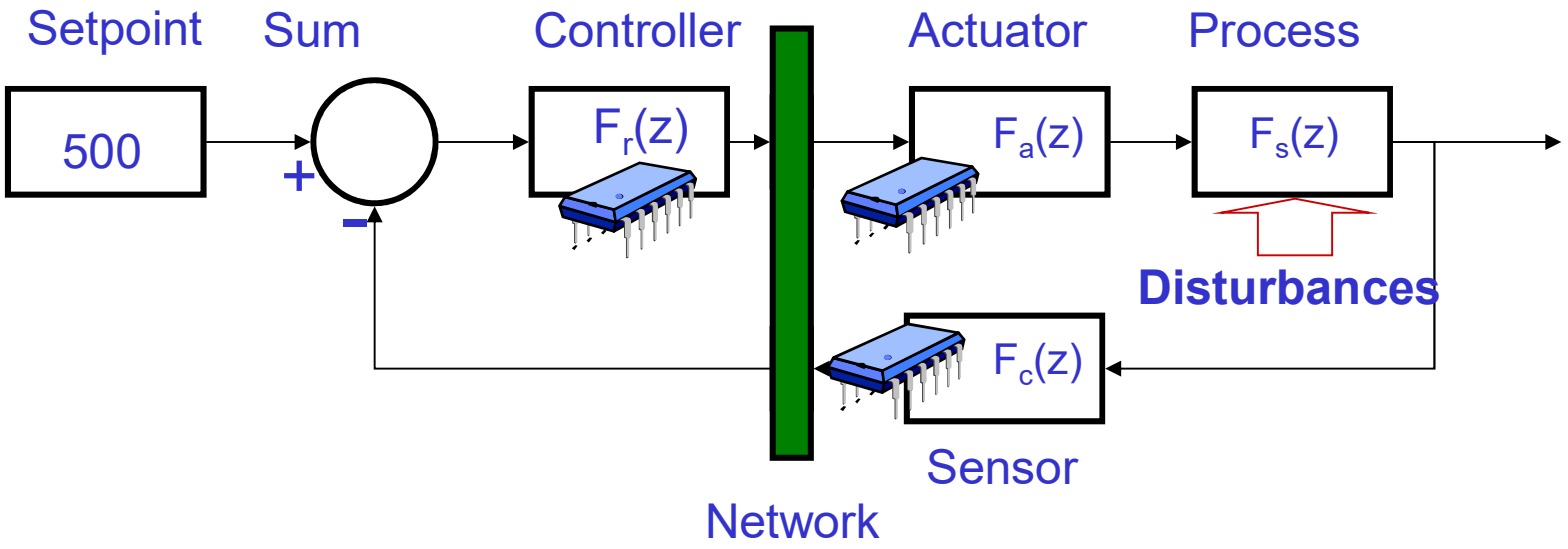
Embedded systems, Internet of things



Overview

1. **Problematics and vocabulary**
2. Dependability, safety, functional safety, security (RAMSS)
3. Risk analysis
4. Some considerations on networks, Safety networks
5. Dependability of networks and networked control systems
6. Cyber-security
7. Applications to cyber-physical systems
8. Discussions & Conclusions

Networked Control Systems (NCS)

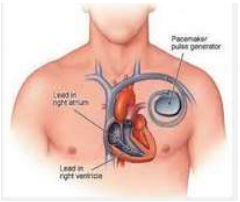


1. Continuous/sampled Components → Hybrid System
2. Discrete events-components
3. Network influence → Time Delay system
   1. Delays
   2. Jig
   3. Packet loss

Quality of Service and Quality of Control for Safer Networked Control Systems (SafeNCS)

Communication networks are more and more used in control-based applications with real-time and/or critical constraints.
Communication and Control aspects need so to be seen from a global point of view. Communication (networks) is shared between various applications, and some aspects such as wireless communication and mobility needs to be taken into account in the design of SafeNCSs. Two examples of SafeNCS can be:

A drone with very strict real-time constraints => control-oriented,
A pacemaker which is remote-supervised from time to time, the infrastructure should protect strongly the integrity of supervision => security-oriented



Cyber-security of industrial systems is now a crucial issue => impact of cyber-security to the safety of networks
In both cases, focusing on control and/or on security aims at guaranteeing **safety**

Quality of Service and Quality of Control for Safer Networked Control Systems (SafeNCS)

Quality of service aims at guaranteeing the best communication aspects, focusing mainly on:

- security aspects: to protect the communication, in order to protect confidentiality of exchanges, integrity of data and control, authentication of actors of the SafeNCS.
- availability of the network, for the considered control application, by allowing the network to control the distribution of throughput as a function of the requirements of the applications (priorities of applications). For that, we can study the network protocols and mechanisms as well as the infrastructure.

Quality of control deals with the need of "automatic control" from the point of view of control, diagnosis, supervision...

- stability which means to guaranty the controllability of the system, despite the potential unavailability of the network
- performance which should be the best as possible in a varying environment, taking account of minimal levels of security, stability and safety.

The presentation will present the problems, propose some approaches and results, and orientations concerning the study of Safe Networked Control Systems

Synthesis on the concepts

1. Dependability : Confidence in the system to ensure its mission without risk (or with a risk management)
   => Co-design approach (Network QoS ⇔ System QoC)
2. Functional safety: part of the overall safety that depends on a system or equipment operating correctly in response to its inputs [IEC]
3. Cyber-security: Cyber security is the protection of systems, networks and data in cyberspace [www.itgovernance.co.uk]
4. Networked Control Systems: Control System closed through a network
5. Complex systems, infrastructure, distributed systems
6. Embedded system, autonomous system, connected objects, IoT
7. ICS : Industrial Control Systems
8. Cyber-physical systems (CPS): Marrying physicality and computation [persyval-lab.org]
9. Our interest: To analyse CPS from the point of view of the potential impact of the system in the physical world (dependability point of view) due to a cyber-attack (attack in the digital world) and define the ways to protect it

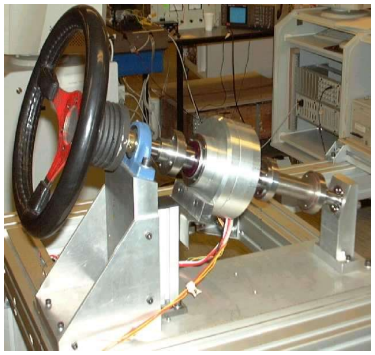
Overview

1. Problematics and vocabulary
2. **Dependability, safety, functional safety, security (RAMSS)**
3. Risk analysis
4. Some considerations on networks, Safety networks
5. Dependability of networks and networked control systems
6. Cyber-security
7. Applications to cyber-physical systems
8. Discussions & Conclusions

Safety/Dependability level (RAMS) of a networked based system, wired networks

- Steering by wire
  - Probability that the vehicle doesn't turn, when it is requested
  - Probability that the vehicle turns unexpectedly
- Difficult evaluation
  - Network more complex than a set of point-to-point links
  - Network more complex than a delayed system
  - Network-system Interaction

Drive shaft



X by wire, steering by wire

Dependability of networked-based systems (Wireless Network)

1st vehicle (controlled)

X by wire, brake by wire

2nd vehicle (following the 1st one)

Automated driving (virtual train)

- Braking Function
  - First vehicle
    - Probability that the vehicle does not brake when it is asked for
    - Probability the vehicle brakes without any request
  - Second vehicle
    - Probability that it receives a braking information from the 1st vehicle, if everything is correct for the first vehicle
    - …
- Existing system

  Verification model (formal approach, Monte-Carlo simulations)
- Non existing system

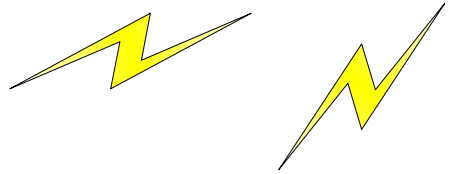
  Design model: « ideal » model + dependability constraints

Embedded system (Embedded wired network + Remote wireless communication) with strong dynamics

Drone-helicopter

Definition of the mission

- Weak dynamics (normal displacement straight ahead)
- Strong dynamics (ex : slaloms between trees)
- Disturbed communication environment (e.m. disturbances, trees…)



Quality of service of the network

- High in critical situation
- High in strong dynamic situations (if remote-control)
- Lower other time

Dependability

RAMS : Reliability, Availability, Maintainability, Safety

Fiabilité

RELIABILITY
Capacity to remain infallible throughout the task

Disponibilité

AVAILABILITY
Capacity to ensure the complete task

Maintenabilité

MAINTAINABILITY
Capacity to remain in or return to the original state

Sûreté de fonctionnement

DEPENDABILITY
Confidence in the system to ensure its mission without risk

- Accidental risks (design error, operational errors…)
- Cyber-security vulnerabilities

Sécurité …

SECURITY
Aptitude of a system to achieve its function… under the normal conditions specified in the instruction manual

SAFETY
Capacity to avoid risk (to people, to property, to the environment)

Dependability Parameters

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*.

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

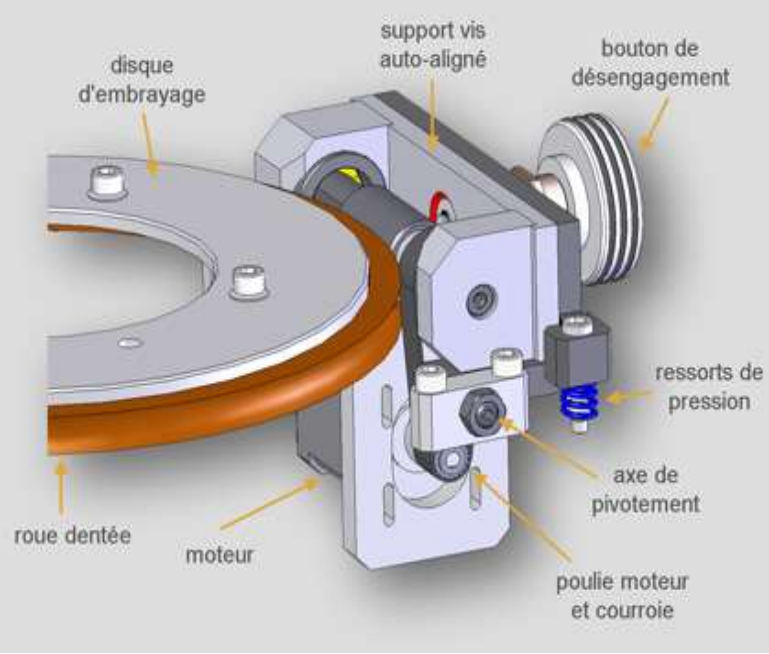
  ex 1: the flow is ≤ a certain %age of a reference value

  ex 2: the loss, or irremediable destruction of strategic data for the company

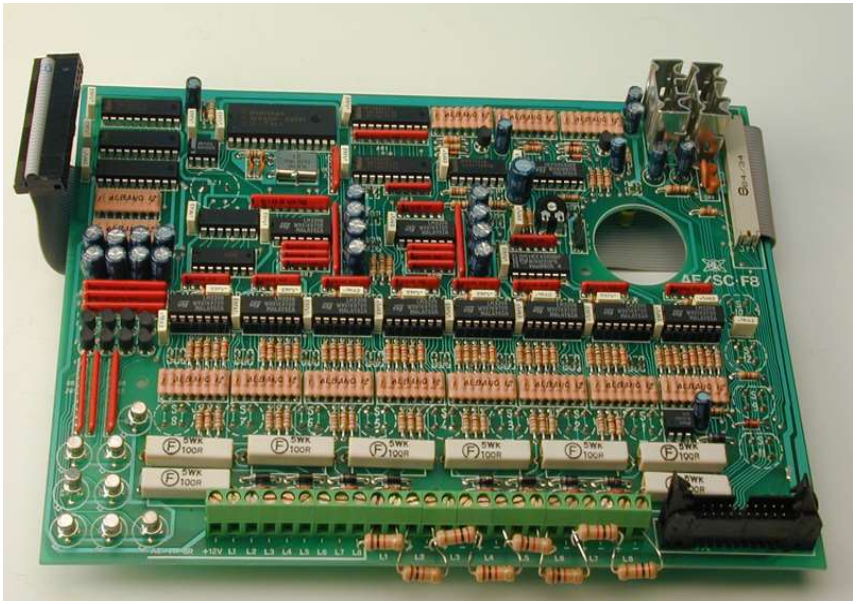
Dependability of classical Components

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

Mechanical systems

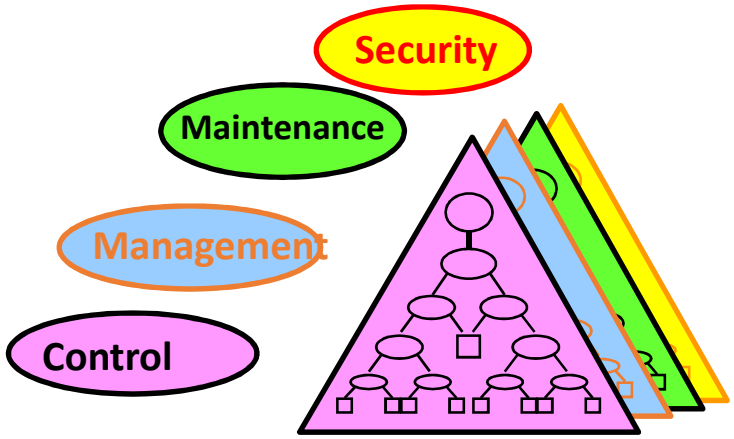


- Electronic systems



Context: Automation system evolution

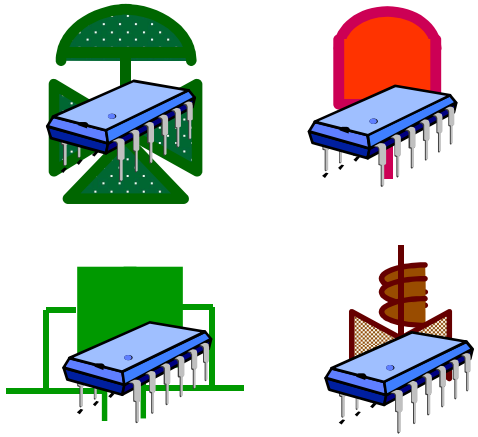
Needs:



Increased number of services

More complex architectures

Components :

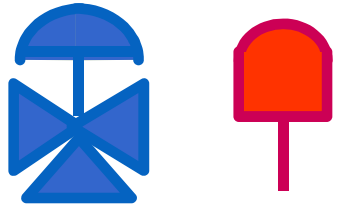


Various capacities and functionalities availability

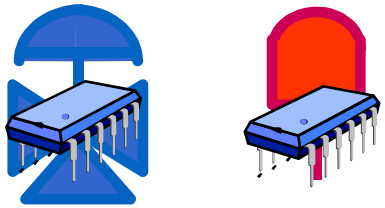
Dependability hard to evaluate and to qualify

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
- « 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 ?

Functional safety: Safety Integrated Level (SIL)

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

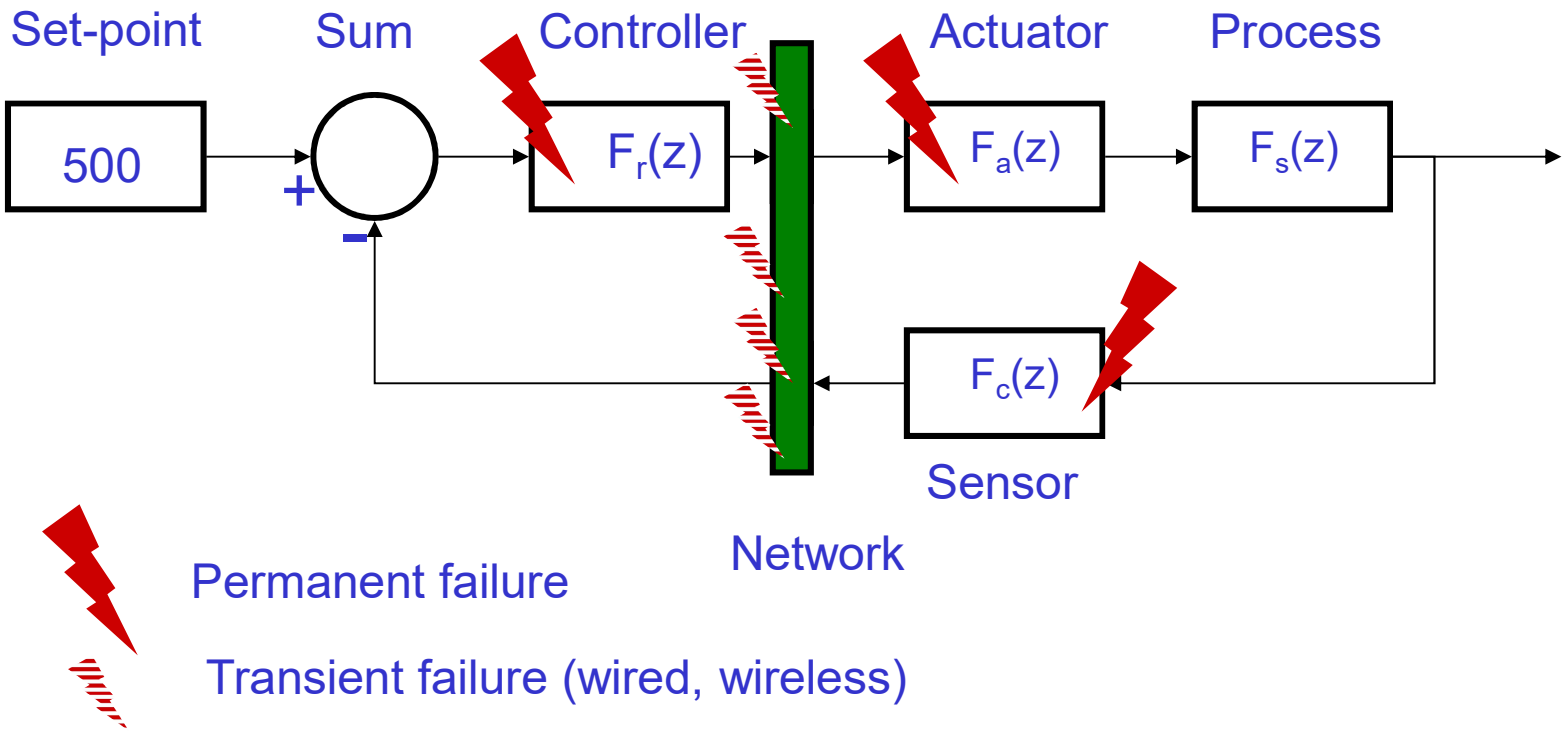
  Functional safety of electrical/electronic/programmable electronic safety-related systems

- 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	$10^{-1} < PFDavg < 10^{-2}$	$10^{-5} < \lambda < 10^{-6}$

Failures integration



Failure Modes

- Continuous/sampled
- Discrete events

Time scales

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

Overview

1. Problematics and vocabulary
2. Dependability, safety, functional safety, security (RAMSS)
3. Risk analysis
4. Some considerations on networks, Safety networks
5. Dependability of networks and networked control systems
6. Cyber-security
7. Applications to cyber-physical systems
8. Discussions & Conclusions

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)

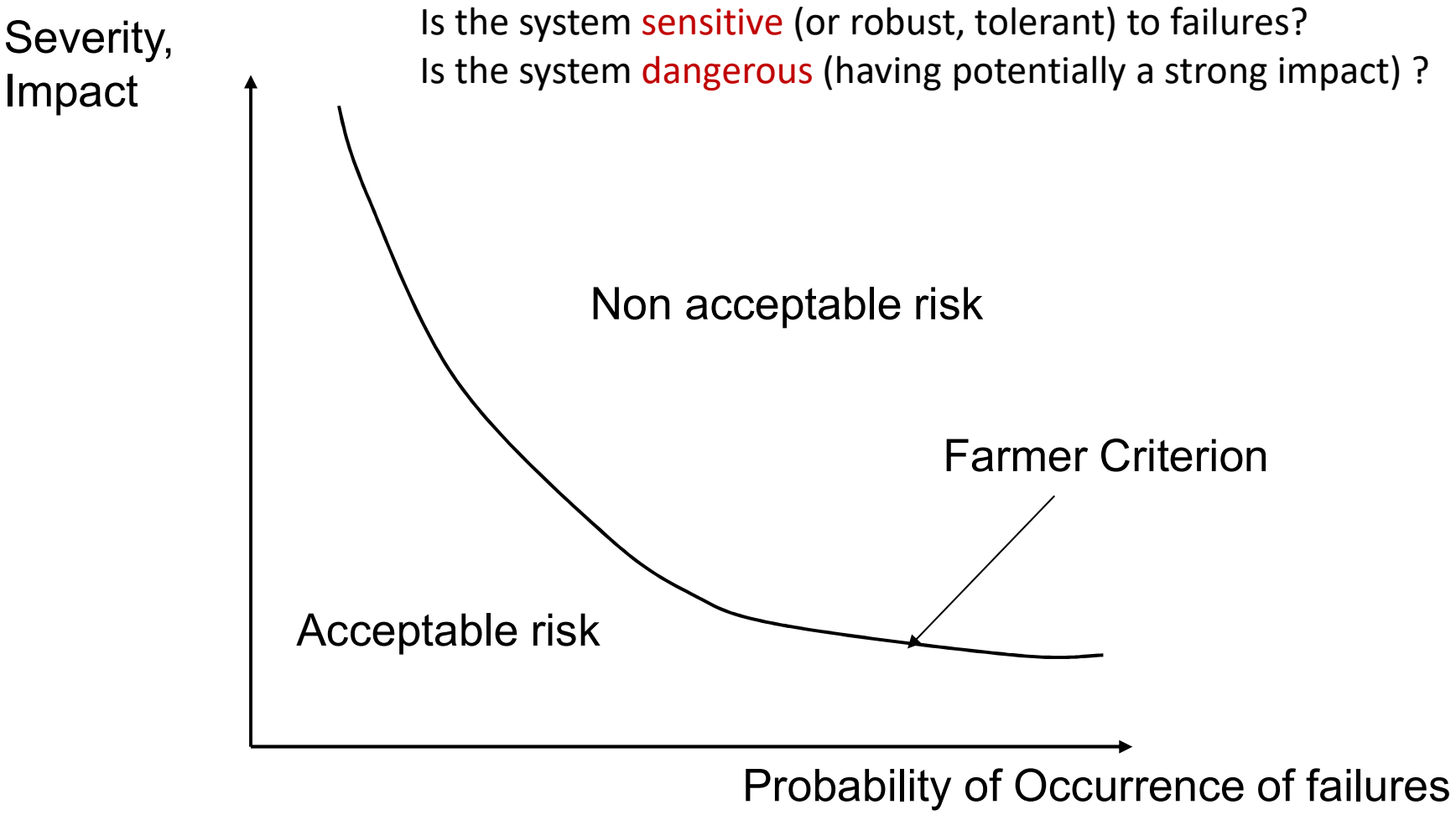
- 'Outdatedness' of the data-processing components
- Probability of attacks by third parties on vulnerable ports

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

Risk analysis: Severity-probability



Elements of risks (asset, threat, vulnerability)

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 (asset, threat, vulnerability)

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 that a given threat would be realized in a single year in the event of a complete absence of control – ex : if we stimate 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 (asset, threat, 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)

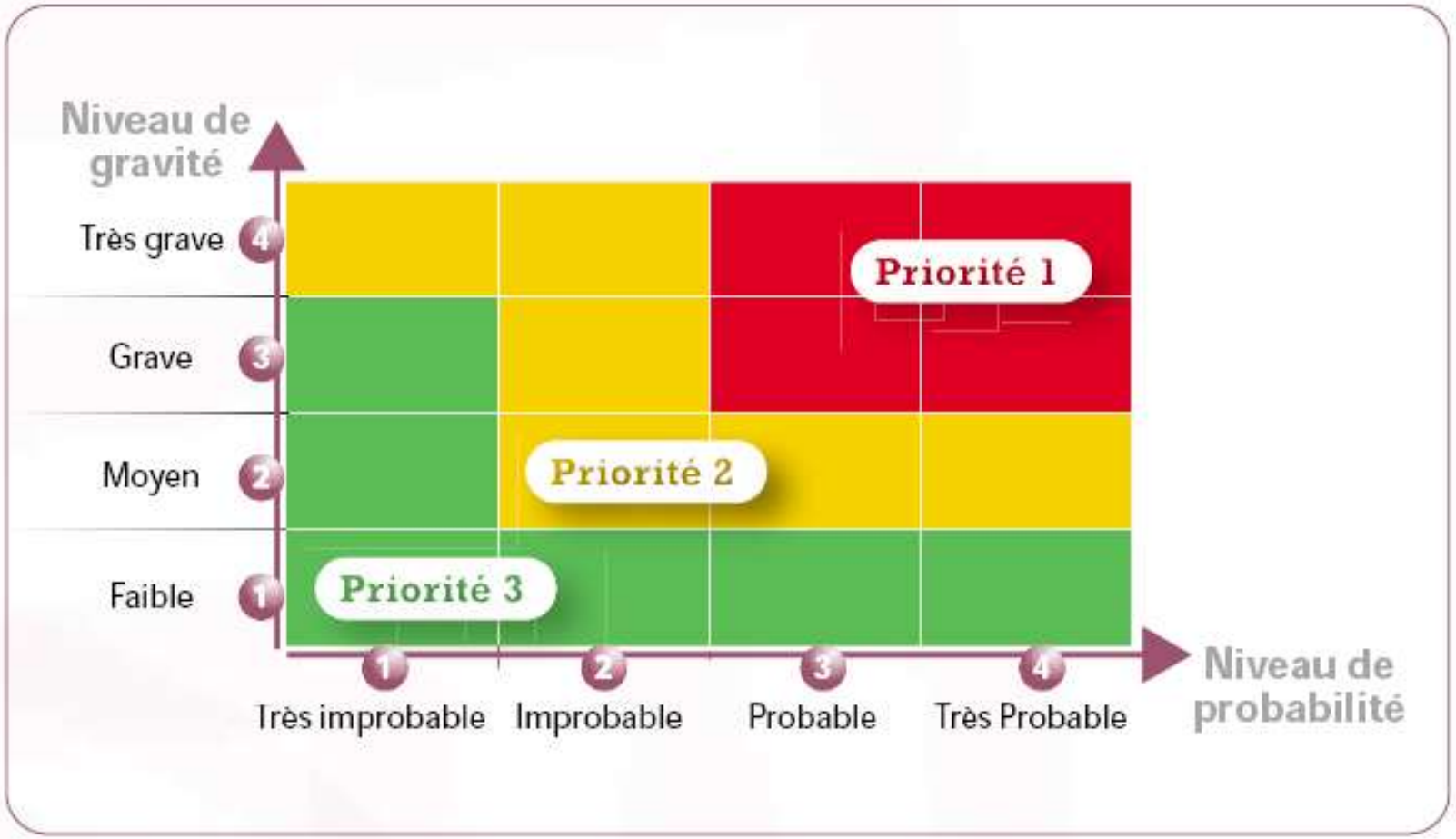
- Most of the time, more than one control is employed to protect an asset.

Ex : the threat is an employee stealing trade secrets and selling them to the competitio

To counter this threat, we may

- implement an information classification policy,
- monitor outgoing e-mail,
- prohibit the use of portable storage devices
- …

Risks evaluation, evaluation of the severity



Example

Danger (cause)	Dange-rous situa-tion	Dange-rous event	Risk of…	Conse-quence	Severi-ty	Proba-bility	Priori-ties	Obser-vations
Explo-sion of a tyre	Car sliding	Screw in the tyre	Acci-dent	Killing people in the car	4 (high)	1 (low)	1 (low)	Having a spare wheel…

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 gris security
3. ISA/IEC 62443 Security for Industriel Automation and Control Systems
4. EU efforts about smart grid security
5. ANSSI Classification method and key measures

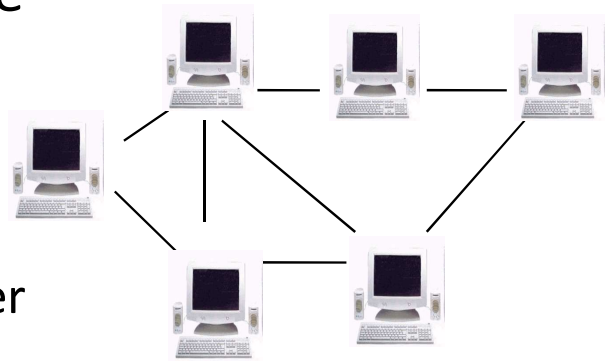
Overview

1. Problematics and vocabulary
2. Dependability, safety, functional safety, security (RAMSS)
3. Risk analysis
4. Some considerations on networks, Safety networks
5. Dependability of networks and networked control systems
6. Cyber-security
7. Applications to cyber-physical systems
8. Discussions & Conclusions

Access mode: Random Access

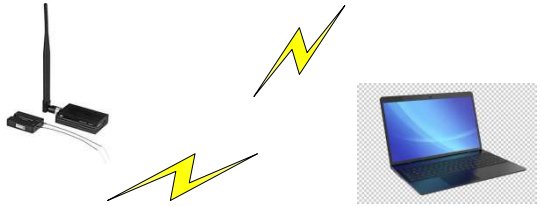
CSMA/CD (Carrier Sense Multiple Access /Collision Detection)

- Carrier Sense
- Multiple Access : Several hosts can access simultaneously: collision risks
- When a collision occurs:
  1. transmission of a jamming sequence
  2. after a delay: new attempt
  3. abandon after too many failures
- Collision Detection and processing (probabilist protocol, no priority)
  - Ex: Ethernet, each host can transmit whenever



Non determinist

Access mode: Random Access



CSMA/CA (*Carrier Sense Multiple Access / Collision Avoidance*)

For wireless networks, CSMA/CD not possible

It is not possible from a host to have a view on all the other hosts (transmission range)

Transmitter host listening to the network

If free during a certain time (*DIFS : Distributed Inter Frame Space*),

the host send a RTS frame (*Request to Send*, information about the size of data to be transmitted and the speed required)

The receiver (or the access point) acknowledges with a CTS (Clear To Send) frame

to allow the transmission (authorization)

The transmitter then send the data to be transmitted

When all the data are received, the receiver send an ACK (*Acknowledgement*) frame

The other hosts wait during a certain time (estimated time from the known data size and transmission speed)

Collision Avoidance (ex : Wi-Fi 802.11, 802.15.4 6LowPAN)

Non determinist

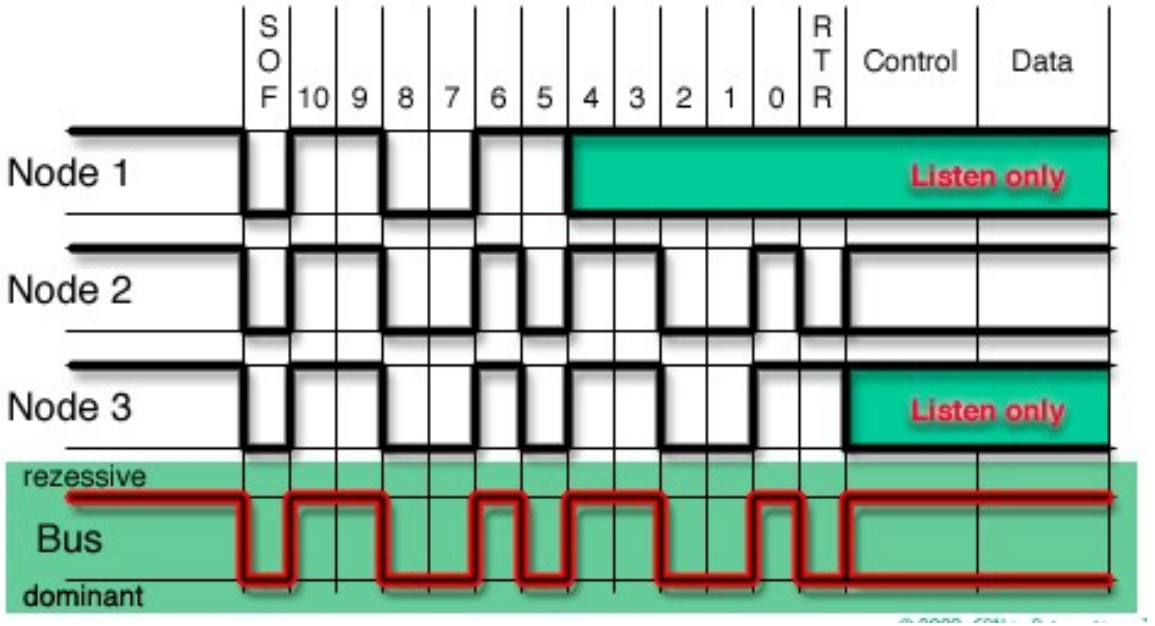
Access mode: CSMA/AMP
Arbitration by Message Priority

Ex. of Fieldbus networks

Scheduling of messages as a function of priorities

(ex : CAN network, Controller Area Network),

Partially determinist (configuration strategy)



Access Mode: Controlled access

Waiting until having the right to transmit (avoid any conflict)

centralised management:
1 host controlling accesses

decentralised management:
many hosts controlling accesses

Centralised access by "polling" :

Each station can transmit in turn according to a predefined schedule.

Need:
1. of an access controller
2. a scrutation table

Ex : WorldFIP network

Determinist (for determinist traffic)

Decentralised access (ex : Token Ring)

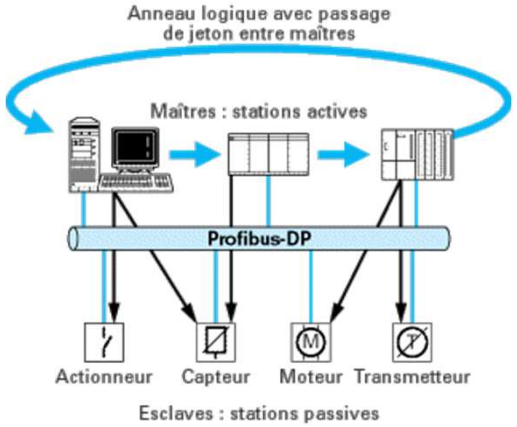
A token running in a logical ring

Right to transmit and access control held by the token owner

time-limited possession of the token

Ex : ProfiBUS network

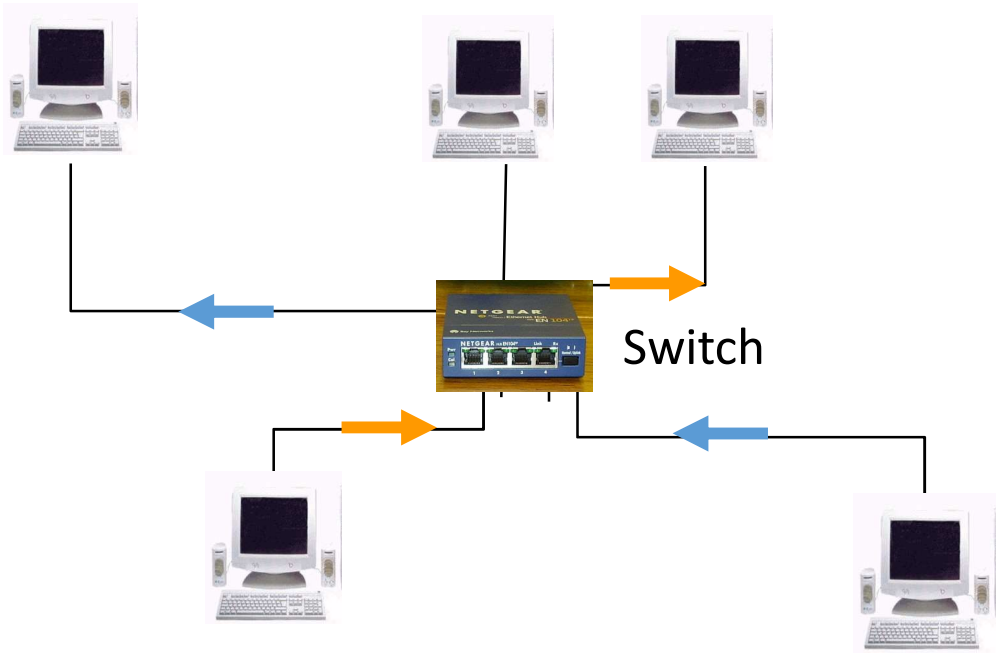
Partially determinist (configuration strategy)



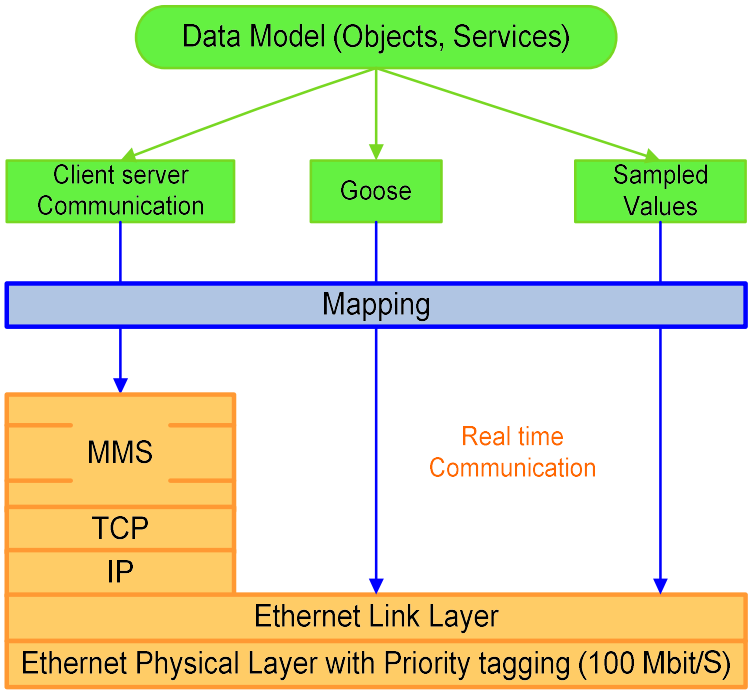
Switched Ethernet

Ethernet = collisions

Switches: delimitation of « free collisions » zones



IEC 61850
Communications aspects based on Switched Ethernet => for Smart Grids



- Satisfying real time performance by the standard in developing extension cards that can transmit critical real-time signals at serial network level
- Development of a new appliction layer allowing to track the dialogue according to the IEC 61850 standard
- New equipment design playing the role of Ethernet switch/ IEC 61850 converter and data concentrator

Wireless networks

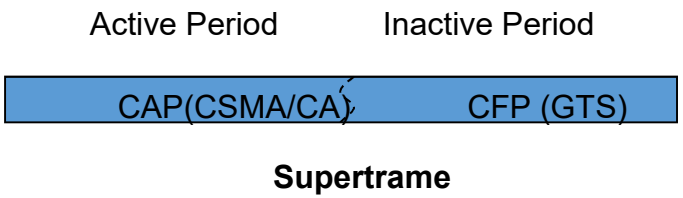
See also 6LowPAN (802.15.4)…

ZigBee	Wi-Fi
IEEE 802.15.4	IEEE 802.11b
2.4-2.4835 GHz (world), 902-928 MHz (USA) and 868-870 MHz (Europe)	2,4 GHz,
from 10 to 75m	46 m indoor, 92 m outdoor
250 kb/s (2.4 GHz), 40 kb/s (915 MHz), and 20 kb/s (868 MHz)	1, 2, 5.5, 11, 54 Mb/s
2^{16}=65536 Number of nodes	32
100-1000+ Batteries life duration	0,5-5
30 ms Time to find a new node in the network	Up to 3s
Reliability, low Power, low Cost	Speed, Flexibility
Home, building, industrial monitoring and control (for small, cheap microprocessors, low rate control networks)	Web, Email, Video. (for PCs, laptops, PDAs)

Real Time (critical time) Wireless network (if the physical layer works!)

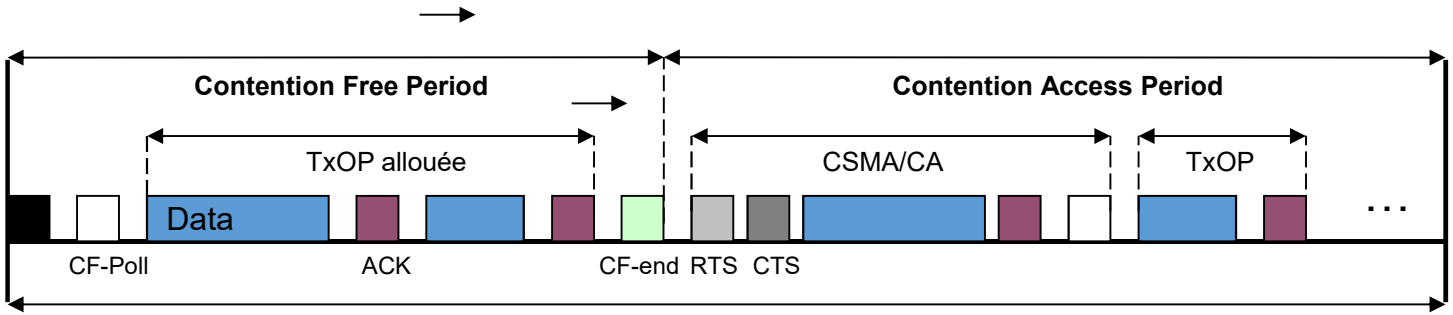
Zig-Bee (on 802.15.4)

– Superframes :



CAP (Contention Access Period) : all the nodes can transmit in a random way respecting the slot duration CSMA/CA
CFP (Contention Free Period) : Allow to garanty an access to a node during a certain amount of time (measured as a number of GTS slots) : **GTS (Guaranteed Time slots)** : Dedicated time slots (the coordinator can allocate one or several slots to a node, in particular for time garanties)

Wi-Fi 802.11e



Superframe

Networks « Defaults »

- Delays: some tolerance (jig)
- Losses: (re-transmission, regeneration, fault tolerances)
  - [Kim]. CSD (control system deadline),
  - [Babak] [Zhang] stability of distributed systems with packet losses
- Alterations
  - Alteration detection thanks to error code detector
  - Error corrections (if corrector code)
  - Fault-tolerant functioning (missing data reconstruction)
- Desynchronisation (clock protocol, external clock)
- Electromagnetic disturbances
- Overload due to the shared network (protocol)

Delays

- Determinist Network (controlled access)
  - Task 1 : every T=0,01 s.
  - Task 2 : every T=0,02 s.
  - Task 3 : every T=0,01 s.
- 1 3 2 1 3 1 3 2 1 3 1 3 2 1 3
  - Task 2 periodic
  - Tasks 1 and 3 are periodic with some « jig »
- Causes of the delays
  - Transfer time
  - Synchronisation policy (time-driven, event-driven,…)
  - Access mode (random, controlled)
- Types of delays
  - Average delay (bounded, not bounded)
  - worst-case delay
- Non determinist network (random access)
  - Priority
  - Re-transmission of tasks following error detection

Wireless networks

- Same problems as wired networks +
- Electromagnetic disturbances (more sensitive)
- Network not always available (normal functioning)
  - Non visibility, delays due to reflections (non direct reception)
  - Not always « on » because of energy consumption (embedded system)
- Disturbances linked to the mobility
  - Transmitter-receiver distance
  - Obstacles between transmitter and receiver
  - Need to have a service traffic (connection, routing…)
- Evolutive topology (mobile stations, communication between a mobile and several ground stations), (hand-over, roaming)

CONSEQUENCES

- Throughput decreasing
- Communication loss (« non negligible » loss of frames)
- Greater sensitivity to hacking

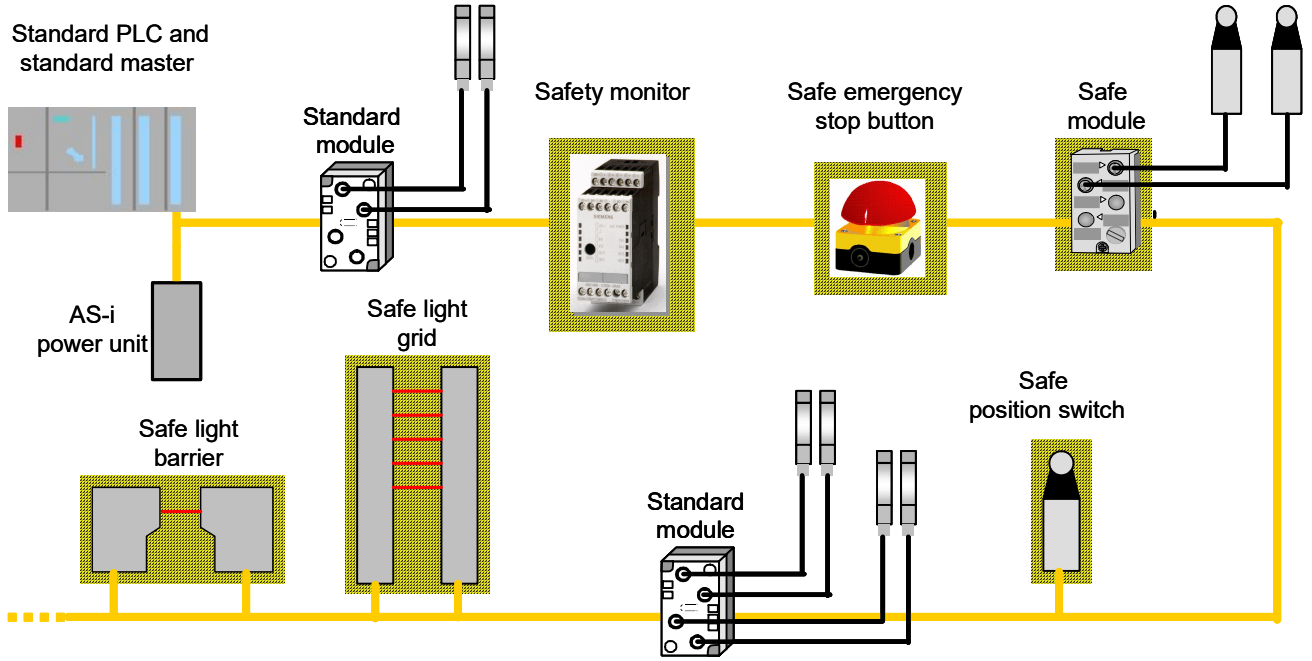
Safety networks

- Safety-Bus p, one of the first network designed for safety
- 2 safety protocols based on the lower CAN layers : **CANopen-Safety** and **TTP** (Time-Triggered Protocol),
- FlexRay, designed for dependable automotive applications,
- ProfiBus who became **ProfiSafe**, thanks to the safety extension,
- ASI Safety at Work, safety extension of the low level ASI network.

- Periodic frames (watch dog)
- Redundancies (wires, redundant transmission, heterogeneous redundancy)
- Safety monitor (ex with ASI) : Passive element detecting suites of 4 consecutive zeros representative of a problem
    A user has triggered a security system and pressed an emergency stop defaults were detected on the communication bus or a component
- Secure communication between safe components (CRC, acknowledgment, verification of transmission time => specific frames for security)

Safety networks: AS-i Safety at Work

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)



Advantages

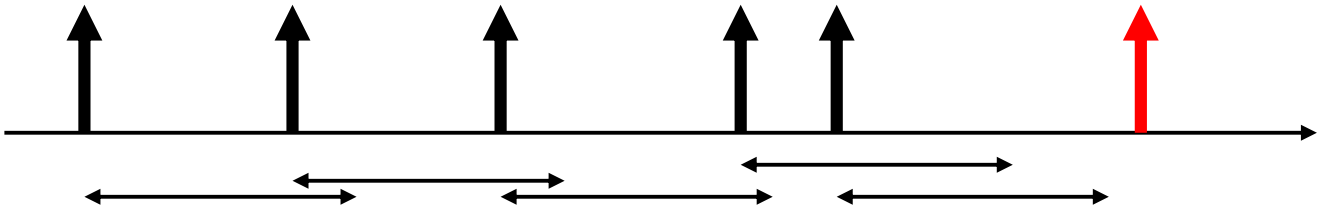
- cabling reduction
- Safety and non-safety on one bus
- Groups of safety signals
- EN 954 – 1 category 4 compliant
- Certified: TUV and BIA
- No AS-i wiring changes needed

Safety networks: CANOpen Safe

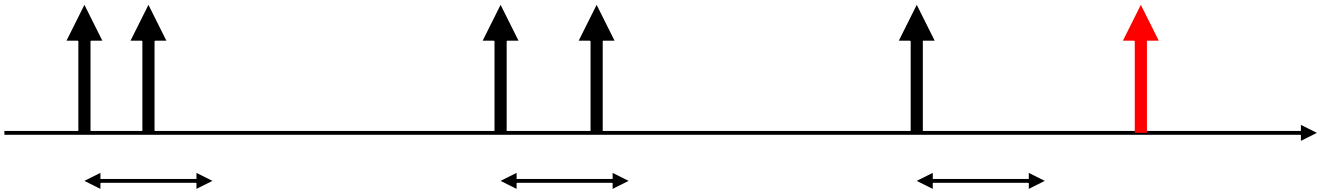
Difficulties due to the non-determinist access,
bus arbitration → maximum delay can be estimated

Use of 2 watch dogs

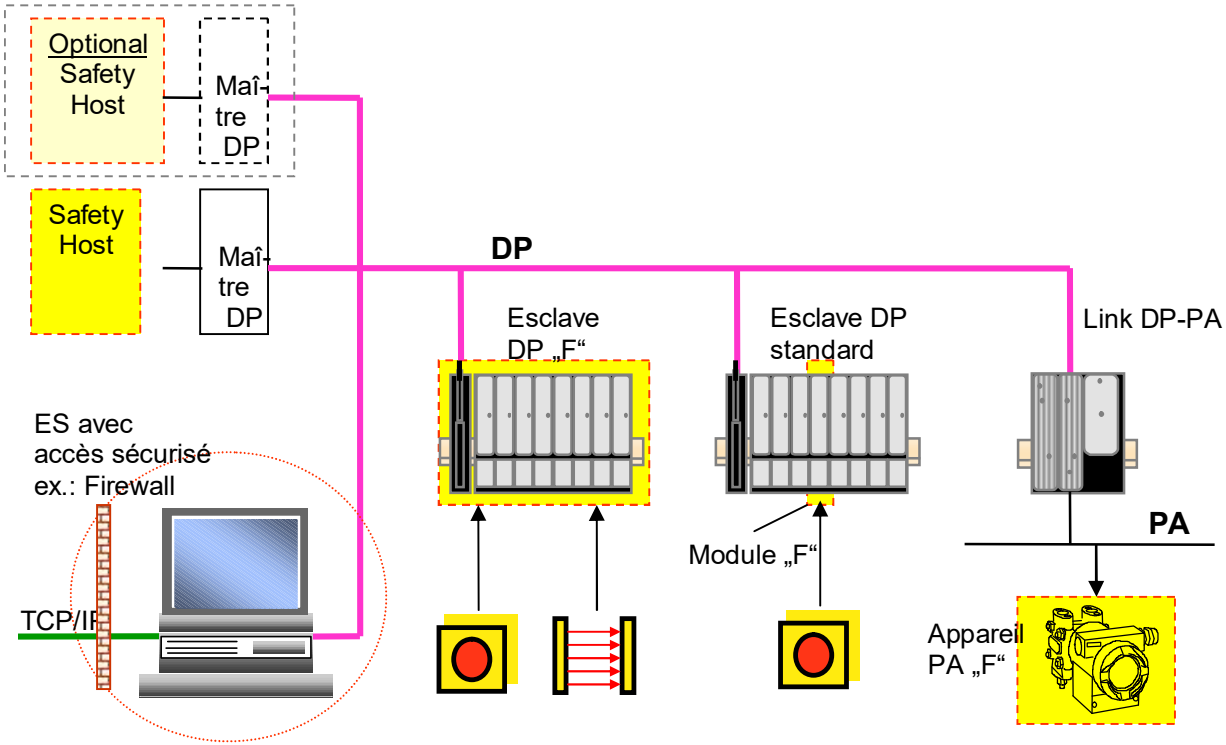
Time window between each trans.



Doubled Emission (redundancy)



Safety networks: Profisafe



Conclusion on Networks

- Protocol quality
  - %age of time to send data
  - Need to retransmit ?
  - Important service traffic…
  - Determinism?
- Determinism
  - Difficult with wireless networks
  - Need of a « closed » network
- « Disturbances » (electro-magnetic dist., loss of connection because of distance, impact of mobility)
  - Negligible for wired networks
  - Important for wireless => need of control applications, robust to the network…
    - Setting of redundancies (multi-bursts, multi-canal, multi-stations…)
- Safety networks

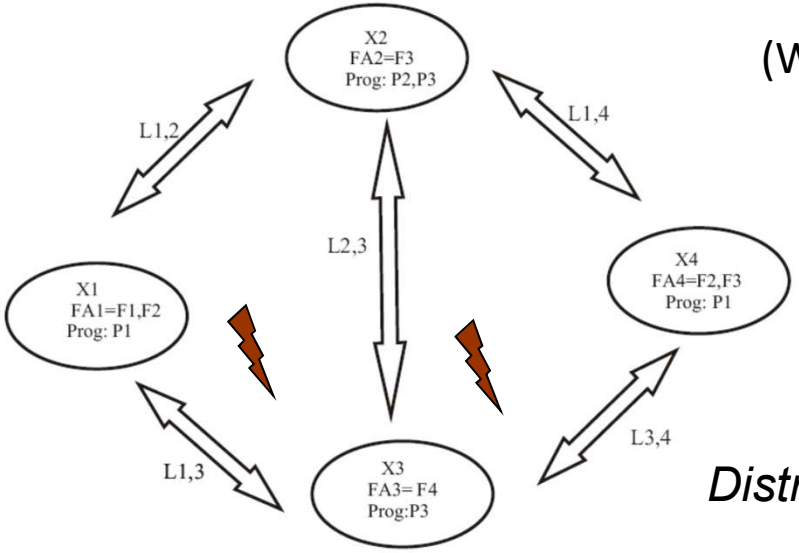
Overview

1. Problematics and vocabulary
2. Dependability, safety, functional safety, security (RAMSS)
3. Risk analysis
4. Some considerations on networks, Safety networks
5. Dependability of networks and networked control systems
   - 5.1 Dependability of the network
   - 5.2 Dependability evaluation in the case of a perfect network
   - 5.3 Dependability evaluation in the case of a Non perfect network
   - 5.4 Dependability evaluation in the case of a Non perfect network, network-system interactions
   - 5.5 Approaches based on the dependability evaluation Networked Controlled Systems
6. Cyber-security
7. Applications to cyber-physical systems
8. Discussions & Conclusions

Network dependability

- Evaluation of the network « alone »
  - Quality of service of the communication
  - Sensitivity to disturbance
- Network seen as a simple communication link
- Network seen as several "independent" communication "strands"

Integration of the communication function in the reliability study (distributed system, Independent links)



(Wang et al, 2002) and (Lin et al, en 2001)

$FA_1 = \{F_1, F_2\}$ $PRG_1 = \{P_1\}$ $FN_1 = \{F_1, F_2, F_3\}$

$FA_2 = \{F_3\}$ $PRG_2 = \{P_2, P_3\}$ $FN_2 = \{F_1, F_2, F_4\}$

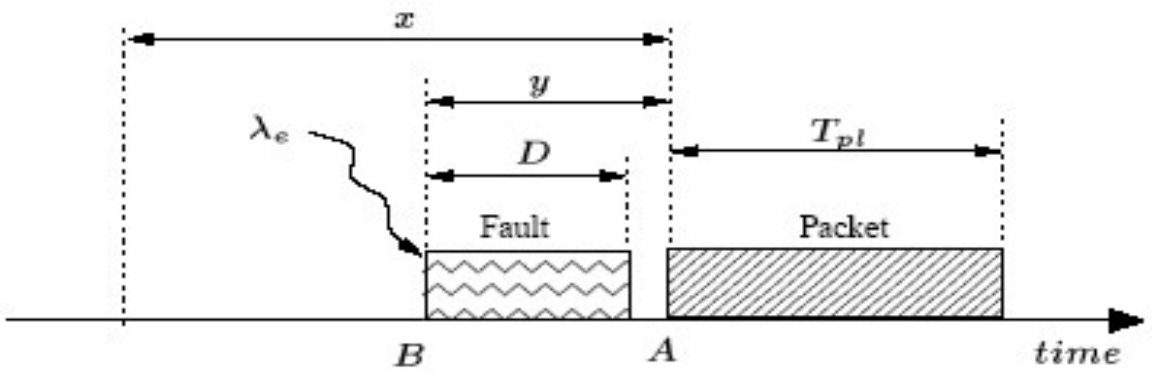
$FA_3 = \{F_4\}$ $PRG_3 = \{P_3\}$ $FN_3 = \{F_1, F_2, F_3, F_4\}$

$FA_4 = \{F_2, F_3\}$ $PRG_4 = \{P_1\}$

Distributed System with 4 nodes and 5 links

- Each link has two states: running state and failure state
- Link failure rates are independent and exponentially distributed
- Link repair rates are independent and exponentially distributed
- During one time unit, only one link can fall down or be repaired

Integration of the communication function in the reliability study (distributed system, Network approach)



- [Tindell] Response time and transient faults
- [Navet et al], [Portugal et al] probability that a message misses its tolerated delay
  One message misses its delay → failure of the communication function
- [Portugal and Carvalho] : Markov chains-based approaches for the evaluation of the unavailability of the communication function (permanent faults)

- **These approaches take into account the communication function but do not take into account the application which lay on this network**

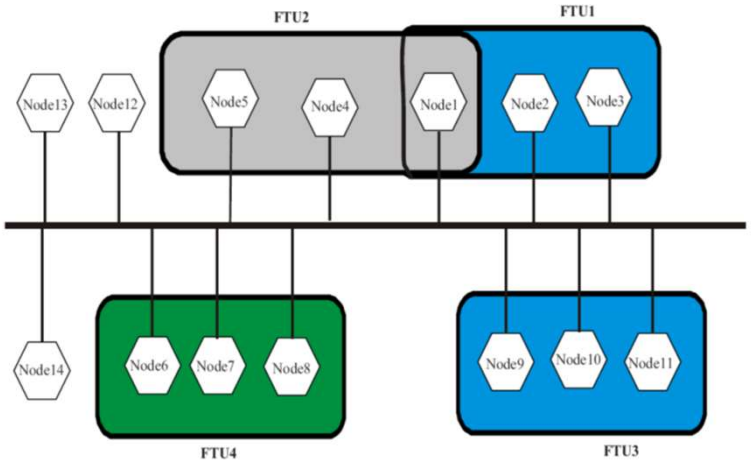
Conclusion Networks and Dependability

- Communication function-oriented approach
- Gives the possibility to measure the Network Quality of Service
- Allow to certify communication (ex : Safety networks)
- Don’t take into account interactions with the system
  - System state
  - Failure succession (ex : component « chatting »)
  - Network load rate as a function of sollicitations
  - Priority level (criticality) of the information to be transmitted as a function of the system state and/or the environment

Overview

1. Problematics and vocabulary
2. Dependability, safety, functional safety, security (RAMSS)
3. Risk analysis
4. Some considerations on networks, Safety networks
5. Dependability of networks and networked control systems
   - 5.1 Dependability of the network
   - 5.2 Dependability evaluation in the case of a perfect network
   - 5.3 Dependability evaluation in the case of a Non perfect network
   - 5.4 Dependability evaluation in the case of a Non perfect network, network-system interactions
   - 5.5 Approaches based on the dependability evaluation Networked Controlled Systems
6. Cyber-security
7. Applications to cyber-physical systems
8. Discussions

Comparison of Dependability parameters for various architectures of a distributed system



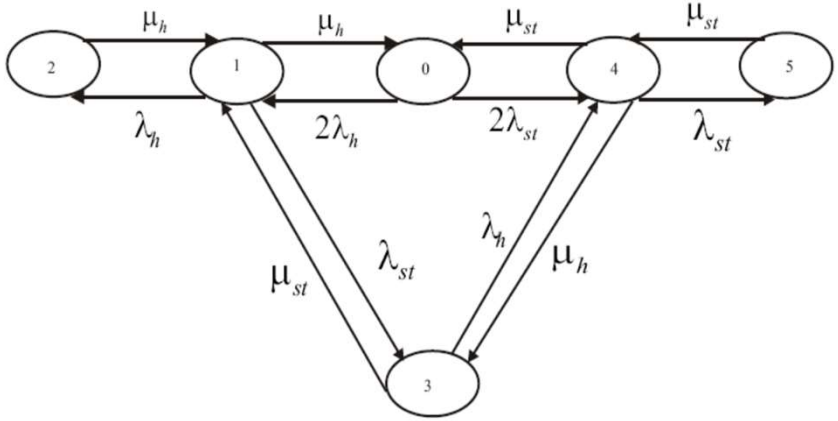
[Pimentel et Salazar]

- Various components (nodes)
- Nodes are grouped within Fault Tolerance Units (FTU)
- One FTU is running if at least one of its node is running
- The system is running if every FTU are running (4 in this example)
- The network is perfect (always running)
- Evaluated parameter: *MTTFF - Mean Time To First Failure*
- Stochastic Petri Nets model + Monte-Carlo simulations

Markov chain-based Approach for the evaluation of availability

[Lai & al, 2002]

- Assumptions :
- Same hardware failure rates (exponential distribution with mean value) for every components
- Idem for software failure rates
- Two possible states (harware and software)
  - (1) operational
  - (2) failed
- Permanent failure
- Repair time including failure detection and repairation
  - Exponential distribution with mean value for hardware and software components
- Independent failures (no common cause failures)
- One site is operational if both associated hardware and software are also in good condition

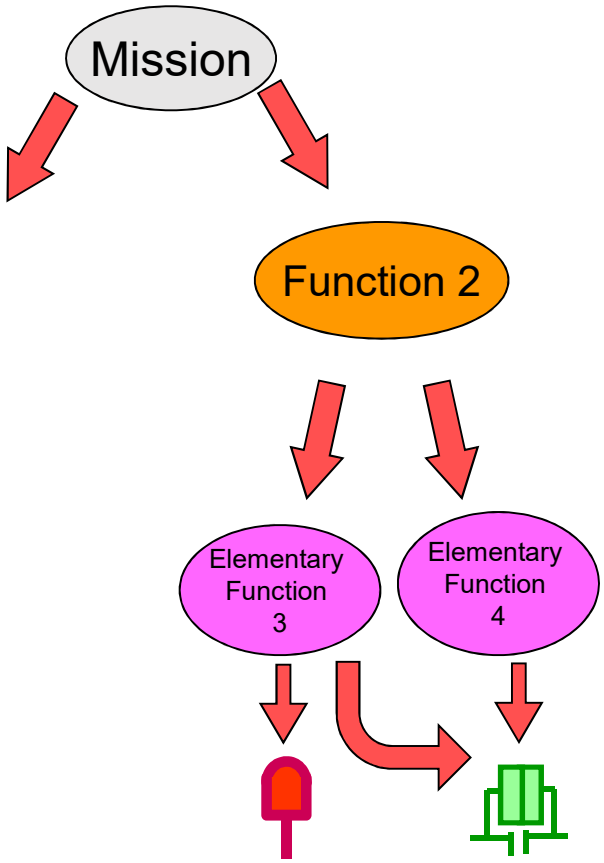


State 0: initial state, all components are in good condition
State 1: hardware failure, 1 site working
State 2: 2 hardware failures, system failure
State 3: 1 hardware and 1 software failures, system failure
State 4: 1 software failure, 1 site working
State 5: 2 software failures, system failure

Overview

1. Problematics and vocabulary
2. Dependability, safety, functional safety, security (RAMSS)
3. Risk analysis
4. Some considerations on networks, Safety networks
5. Dependability of networks and networked control systems
   - 5.1 Dependability of the network
   - 5.2 Dependability evaluation in the case of a perfect network
   - 5.3 Dependability evaluation in the case of a Non perfect network
   - 5.4 Dependability evaluation in the case of a Non perfect network, network-system interactions
   - 5.5 Approaches based on the dependability evaluation Networked Controlled Systems
6. Cyber-security
7. Applications to cyber-physical systems
8. Discussions & Conclusions

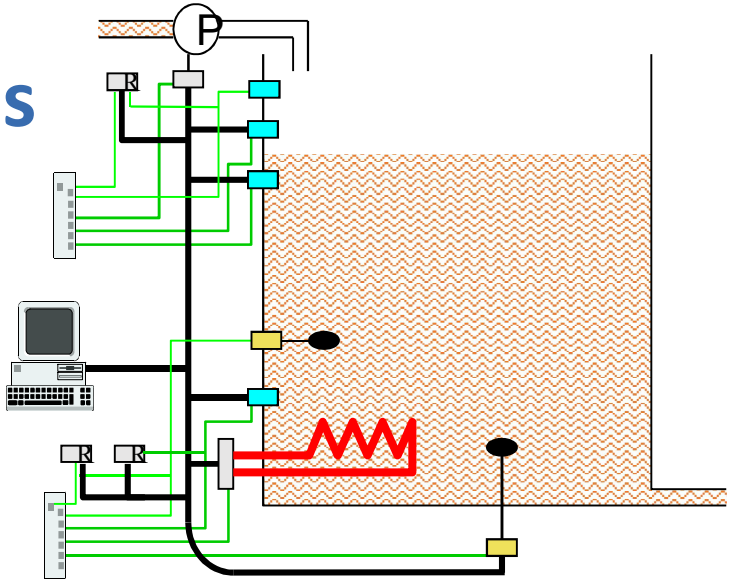
Evaluation of availability and reliability of a networked architecture (design phase)



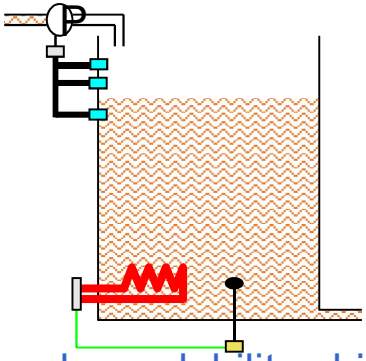
- States => availability
- Failures propagation => reliability
- Use of binary decision diagrams
- ! Common Cause Failures !

[Conrard]

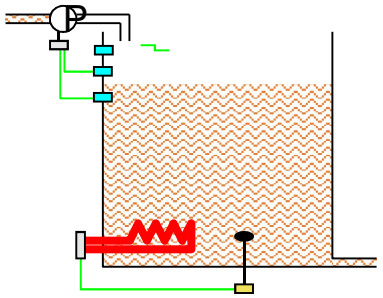
Results



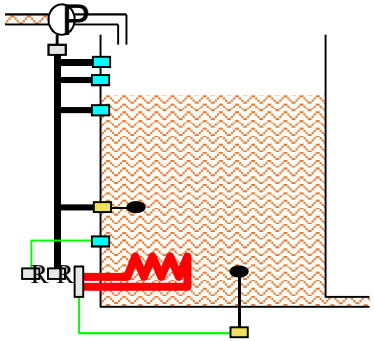
- Preliminary hardware architecture



- Increase dependability objectives
  - Safer solution (networks + intelligents components)



- according to dependability objectives
  - More economic solution



- Increase reliability objectives
  - Even more safer solution

Overview

1. Problematics and vocabulary
2. Dependability, safety, functional safety, security (RAMSS)
3. Risk analysis
4. Some considerations on networks, Safety networks
5. Dependability of networks and networked control systems
   - 5.1 Dependability of the network
   - 5.2 Dependability evaluation in the case of a perfect network
   - 5.3 Dependability evaluation in the case of a Non perfect network
   - 5.4 Dependability evaluation in the case of a Non perfect network, network-system interactions, based on the dynamics of the system
   - 5.5 Approaches based on the dependability evaluation Networked Controlled Systems
6. Cyber-security
7. Applications to cyber-physical systems
8. Discussions & Conclusions

Dynamic evaluation of dependability

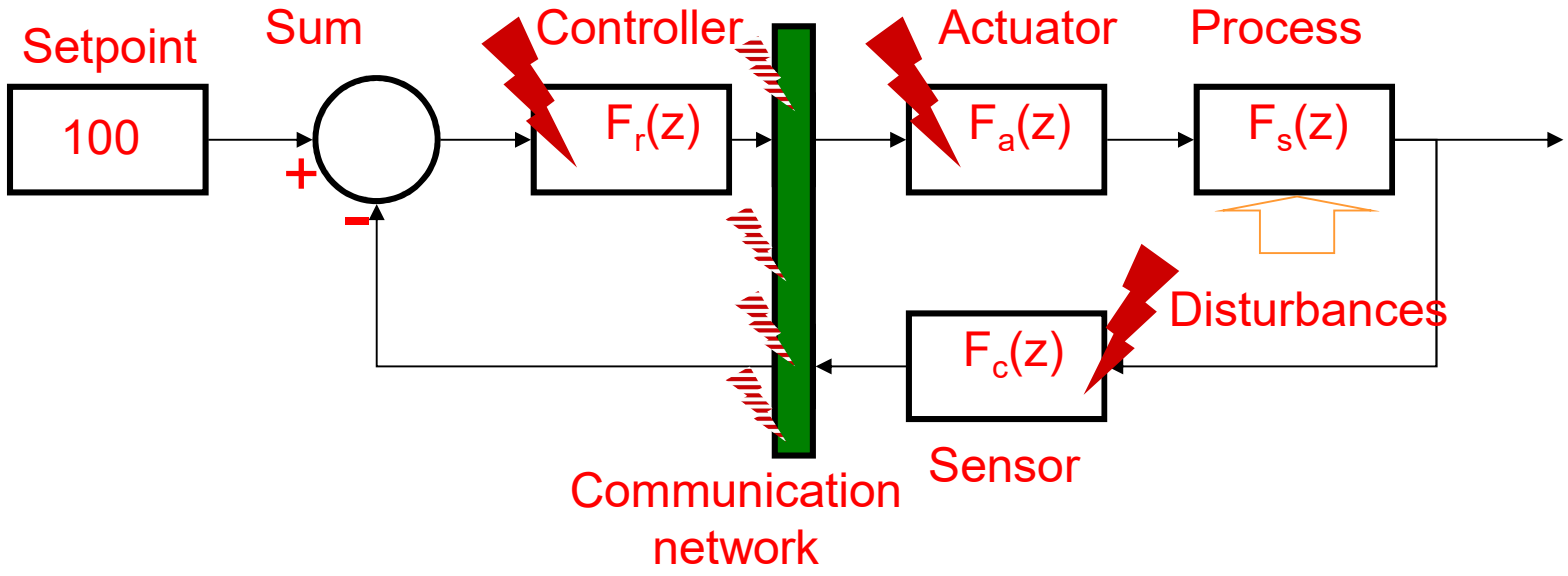
Step - Modelling

Functional model of the components

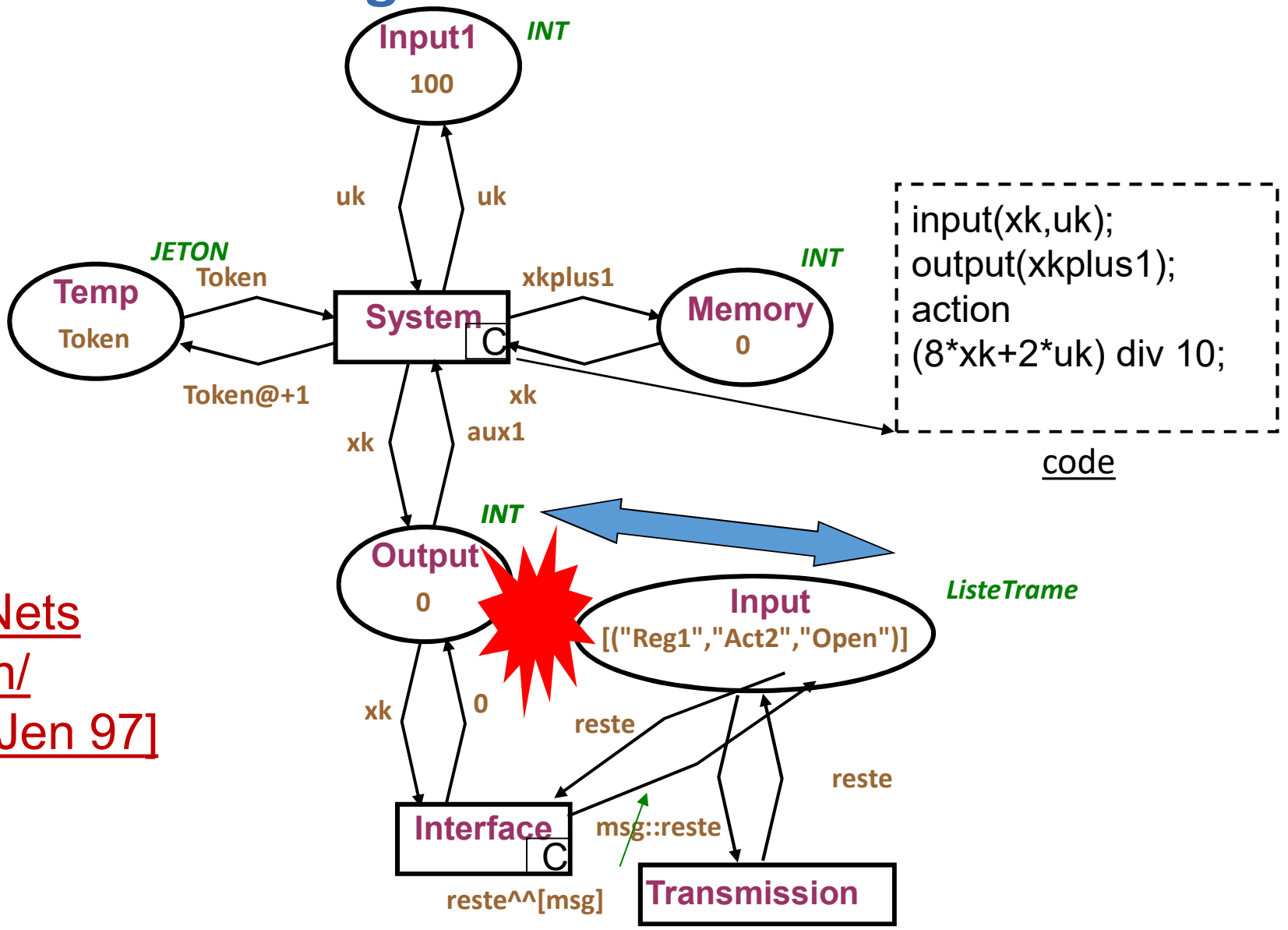
⇒ dysfunctional model of the components

⇒ Unified model of the components

⇒ Interconnection of the components

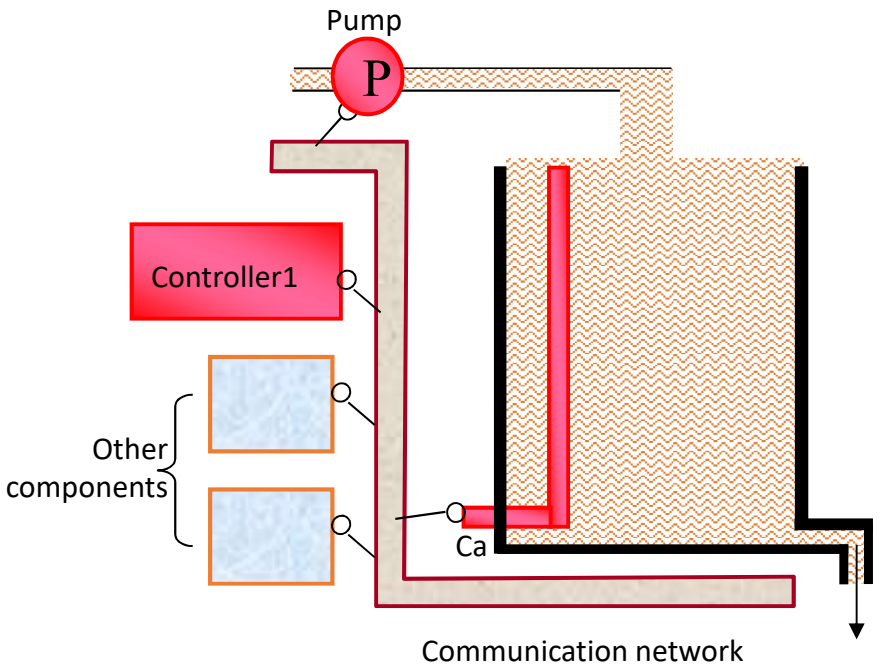


Hierarchical Design

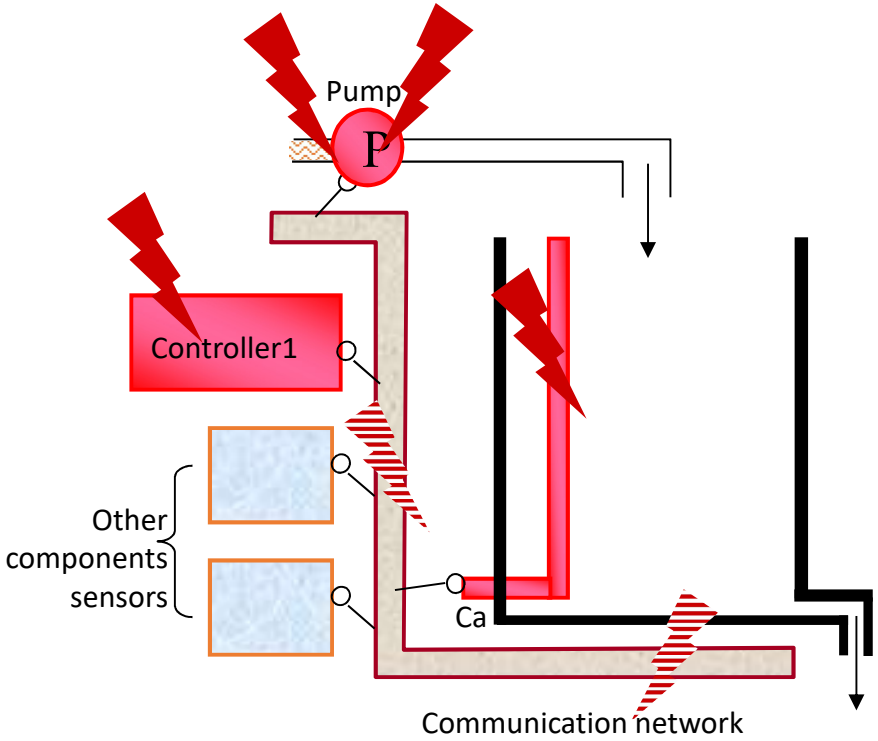


Petri Nets Design/ CPN [Jen 97]

Presentation of a system



Study of failure modes



6 events:

1. Controller failure
2. Sensor failure

Actuator failure

3. Wear-out
4. Blocking

Network errors

5. Loss of a frame
6. Alteration of a frame

[Barger]

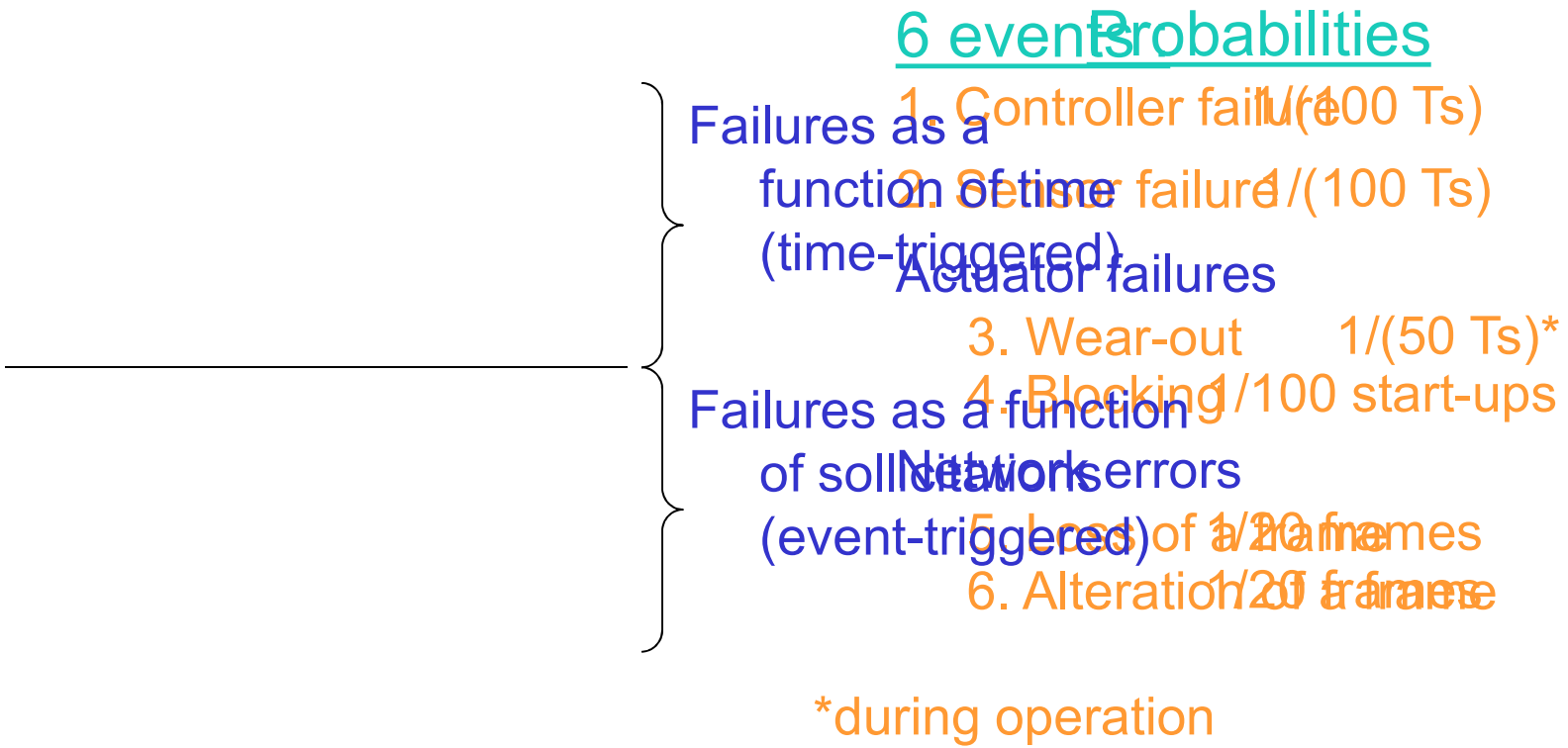
Mission
1. Fill the tank
2. Keep the level

➔ Failure Mode: Do not fill

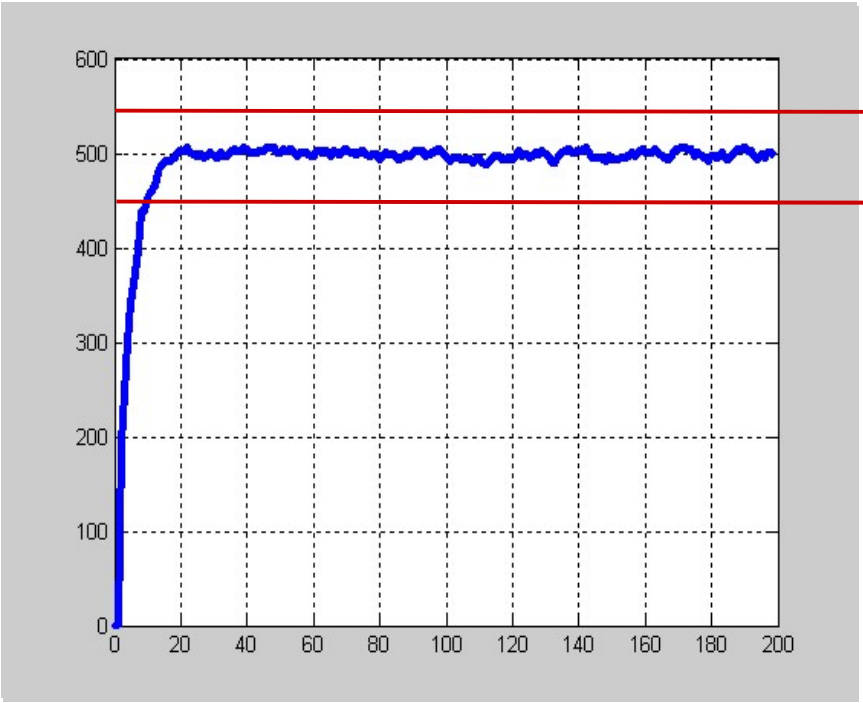
➔ Do not keep

Scenarios

Results of the study of the failure modes



Monte Carlo simulations



11% ***Does not keep the level***

83% ***succeed***

6% ***Does not fill***

Results

Total simulations	Results		
	Does not fill	***Succeed***	***Does not keep the level***
6734	389	5620	725
100%	6%	83%	11%

Conclusions

Networks events and influence are not always important➔ The overflow is generally due to other events

Problem: 50% scenarios leading to an error contains only problems linked with the communication network

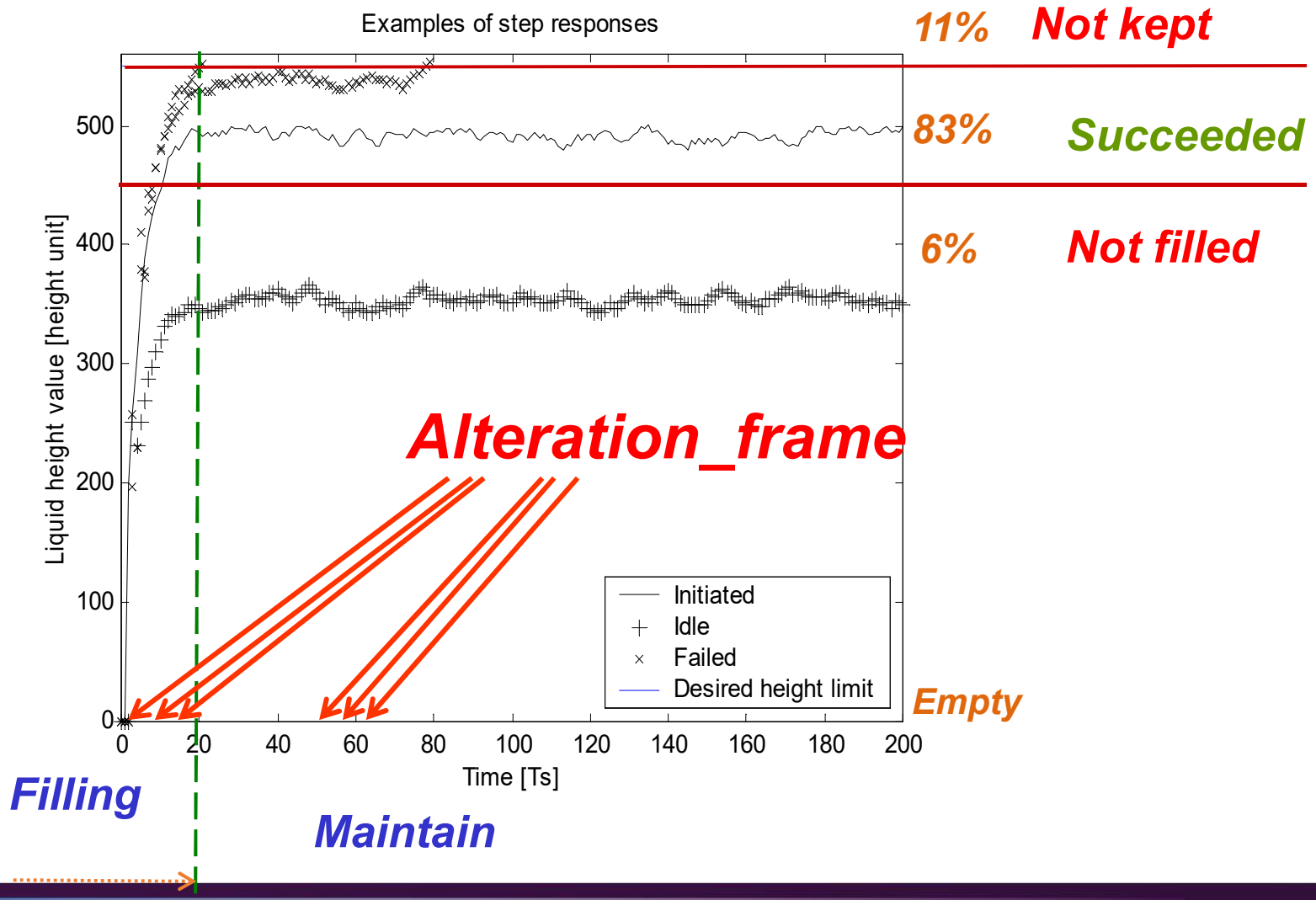
➔Need of another analysis approach:
dynamic analysis

The consequence of a network error depends on the system state

*State in the control meaning (internal variable, level)

Taking account of the history (functional and malfunctional) of the system

Importance of a scenario: Function of the state of the system



Overview

1. Problematics and vocabulary
2. Dependability, safety, functional safety, security (RAMSS)
3. Risk analysis
4. Some considerations on networks, Safety networks
5. Dependability of networks and networked control systems
   - 5.1 Dependability of the network
   - 5.2 Dependability evaluation in the case of a perfect network
   - 5.3 Dependability evaluation in the case of a Non perfect network
   - 5.4 Dependability evaluation in the case of a Non perfect network, network-system interactions
   - 5.5 Approaches based on the dependability evaluation: Networked Controlled Systems
6. Cyber-security
7. Applications to cyber-physical systems
8. Discussions & Conclusions

Dependability of NCSs, Tools

- Systems users have ever-increasing nonfunctional requirements on the quality of the systems

  Performance, reliability, availability, etc.

  probability to have a critical failure in one hour< 10^{-8} (IEC 61508/SIL4)

  SIL = Safety Integrated Level

- Difficulties with NCS:

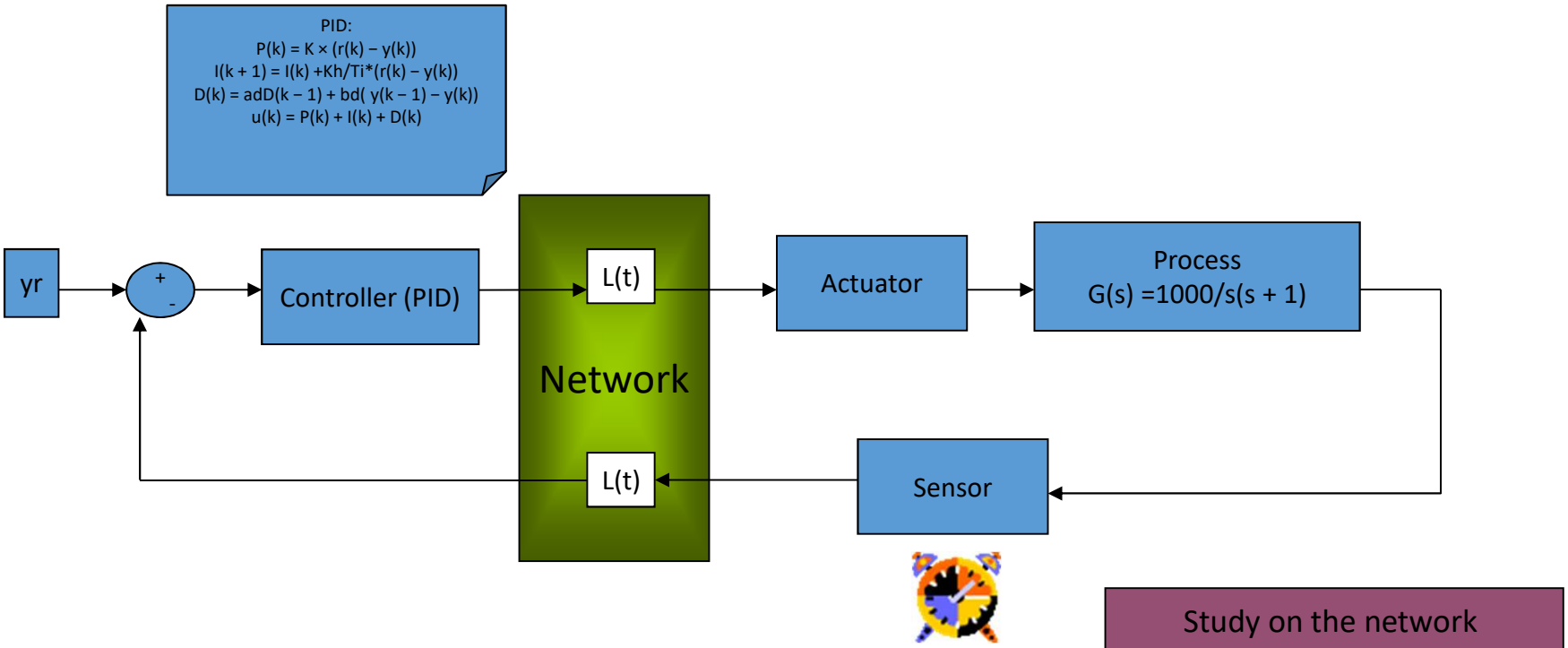
  the system is sequential: depending on the occurrence's order of a given sets of events, the undesirable event may, or may not appear

  it is non coherent: a failure can (at least for a certain time) mask another one, therefore delaying the occurrence of the undesirable event

  components are not "Boolean": they have several failure modes.

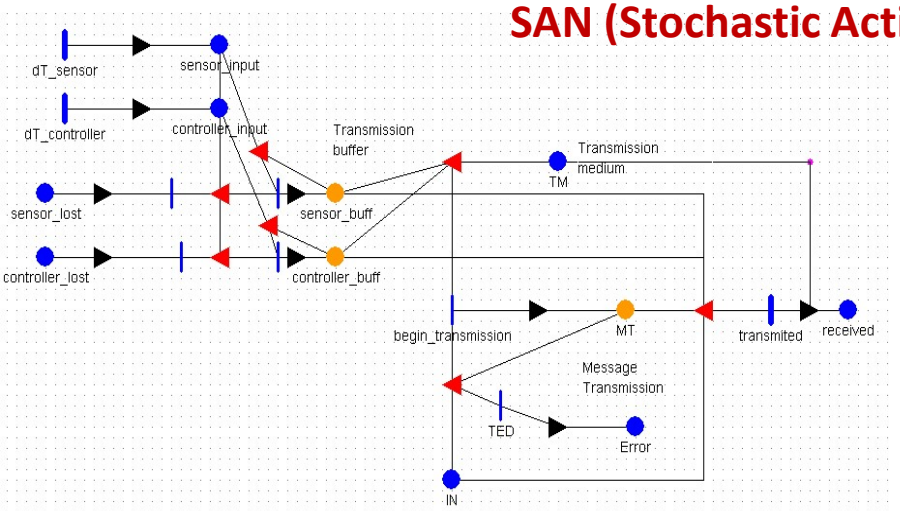
- How to assess dependability parameters for an NCS? (impact of the lost messages on the system reliability)

Proposed approach

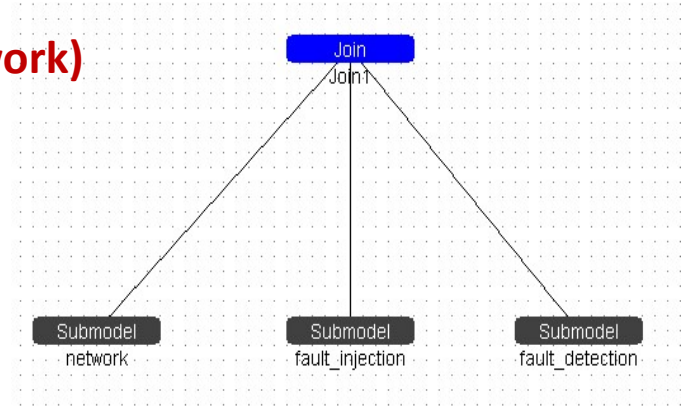


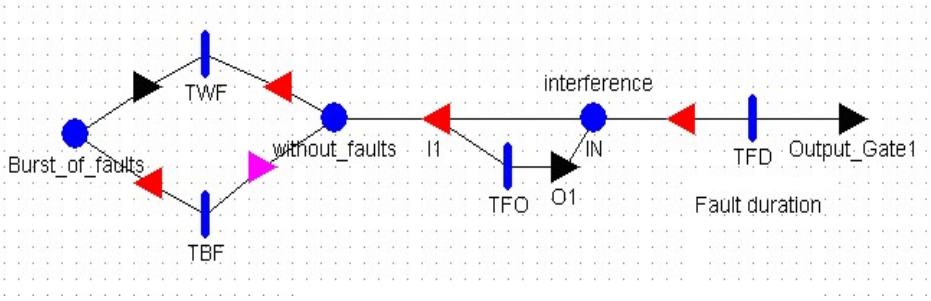
Study on The Network (CAN, Control Area Network)

SAN (Stochastic Activity Network)

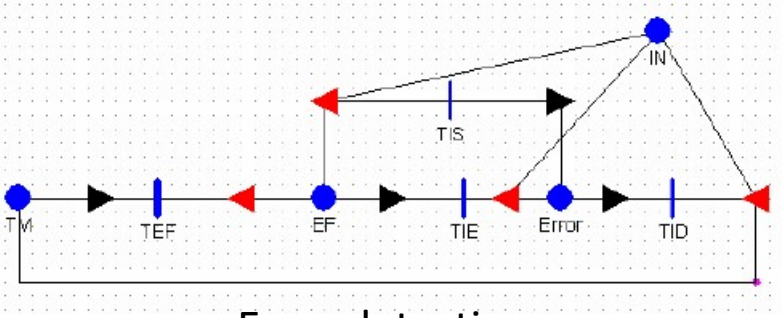


Network





Fault injection (Navet 2000 Portugal)



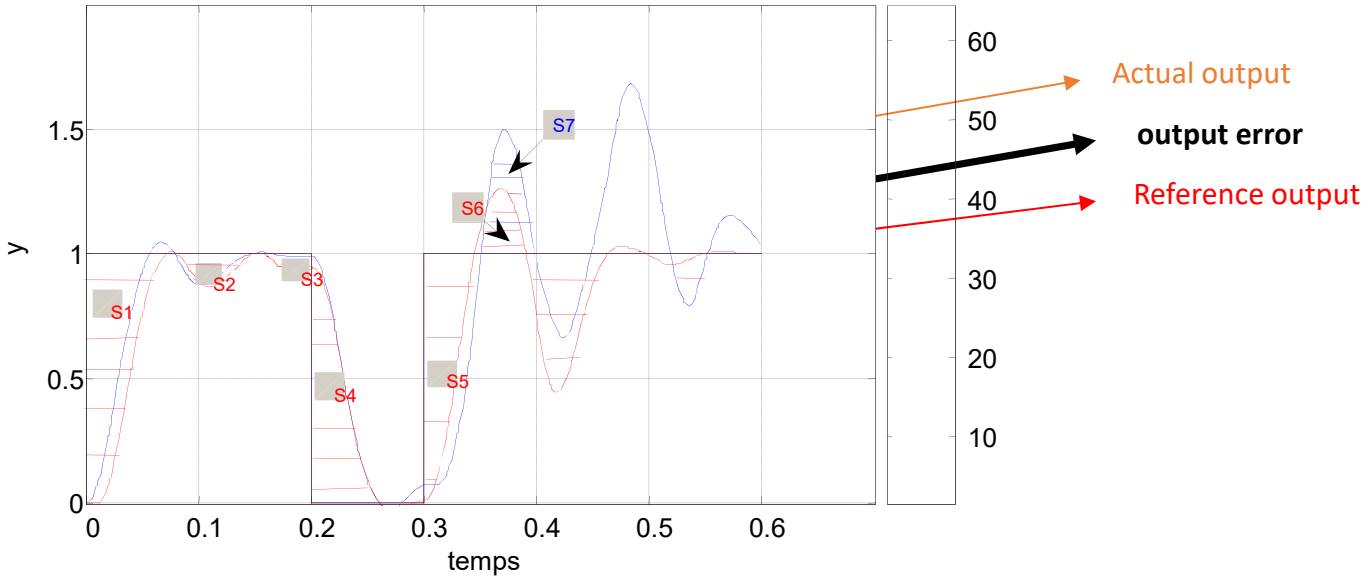
Error detection

Example

Impact of lost messages on the system reliability

- Red, 10 % packet losses
- Blue, 20 % packet losses

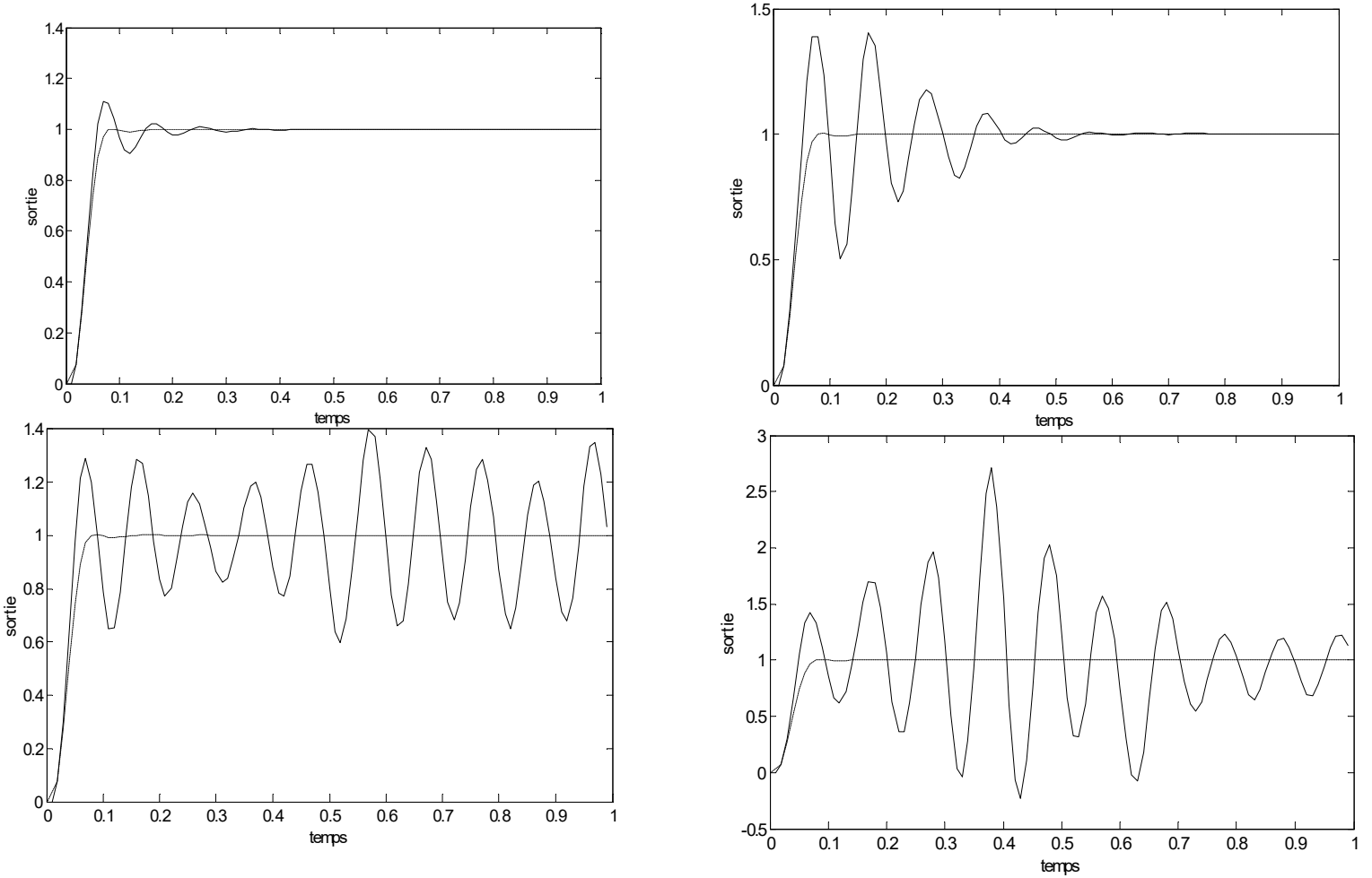
How we detect a failure situation?



Results for a classical NCS

Composed Model

Process=1000/s(s+1) Ts=0.01s
Delays « uniformly » distributed between 0%Ts and 60%Ts



Failure Modes

- Failure per overshoot
- Failure per response time
- Failure per stability

Knowledge about transient faults probabilities (variable delays, message losses)

Probability for the system failure

Conclusions

-Type of network

- Model of the system
- Behaviour of the system
- Continuous time
- Events
- Combination (hybrid) of time-based and event-based properties
- Analysis of the parameters sensitivity

Overview

1. Problematics and vocabulary
2. Dependability, safety, functional safety, security (RAMSS)
3. Risk analysis
4. Some considerations on networks, Safety networks
5. Dependability of networks and networked control systems
6. Cyber-security
   - 6.1 Concepts
   - 6.2 Attacks
   - 6.3 Infrastructure, DMZ
   - 6.4 Cryptography and applications
   - 6.5 IDS, Virus
7. Applications to cyber-physical systems
8. Discussions & Conclusions

Safety and security: definitions

- Security: definition (from EN 292 standards)

  Aptitude of a system to achieve its function… under the normal conditions specified in the instruction manual…

- Safety

  Aptitude of an entity to avoid revealing critical or catastrophic events => likely to affect people, equipment, the environment

- **Confidentiality & Integrity**

  Aptitude of one entity to safeguard the confidentiality and the integrity of information

Definitions of terms related to the reliability and the security for applications such like data- processing networks (1/2)

Direct Properties of Security

- Confidentiality (*confidentialité*): preventing the visualization of information by unauthorized persons

- Integrity *(intégrité)*: preventing the non-detection of modifications of information by unauthorized persons

- Authentication *(authentification)*: allowing the identity check of users

Property linked to security

- Availability *(disponibilité)*: *preventing* unauthorized persons access in order to guaranty the use by authorized users

Definitions of terms related to the reliability and the security for applications such like data- processing networks (2/2)

- Authorization *(autorisation)*: preventing access to the system by unauthorized persons

- Auditability *(auditabilité)*: possibility of rebuilding the complete history of the system from recordings of histories

- Non "repudiability" *(non répudiabilité)*: possibility of providing irrefutable proof of the perpetrator of an action on the system

- Protection from third parties: preventing serious damage linked to an attack (pirating) by third parties.

Security principles

- Physical security
  - Energy sources (electricity (power supplies)…)
  - Environmental protection (fire, temperature, moisture/fungi/fungus (humidity)…)
  - Protection of access, traceability of accesses
- Exploitation security
  - Back up plan, recovery plan
  - Emergency help plan
  - Management of the computer park, configurations and updates
  - Management of the incidents and follow-ups until resolution
  - Analysis of accountancy and logging files
  - Management of the maintenance contracts
- Logical security
  - Mechanisms of security by software: Identification, Authentication, Authorization
  - Cryptography mechanisms
  - Effective password management
  - Antivirus
  - Classification of data: Degree of sensitivity (normal, confidential…)
- Applicative security
  - Development Methodology (respect of the development standards suited to the technology employed)
  - Programmed checks, tests
  - security of the software packages (choice of the suppliers, interfaces security)
  - Contracts with subcontractors (responsibility clauses)
  - Migration plan of critical applications
  - Validation and audit of programs

Overview

1. Problematics and vocabulary
2. Dependability, safety, functional safety, security (RAMSS)
3. Risk analysis
4. Some considerations on networks, Safety networks
5. Dependability of networks and networked control systems
6. Cyber-security
   - 6.1 Concepts
   - 6.2 Attacks
   - 6.3 Infrastructure, DMZ
   - 6.4 Cryptography and applications
   - 6.5 IDS, Virus
7. Applications to cyber-physical systems
8. Discussions & Conclusions

Types of targets, types of attacks

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 …

The types of attacks are classified in two categories:

Passive attacks

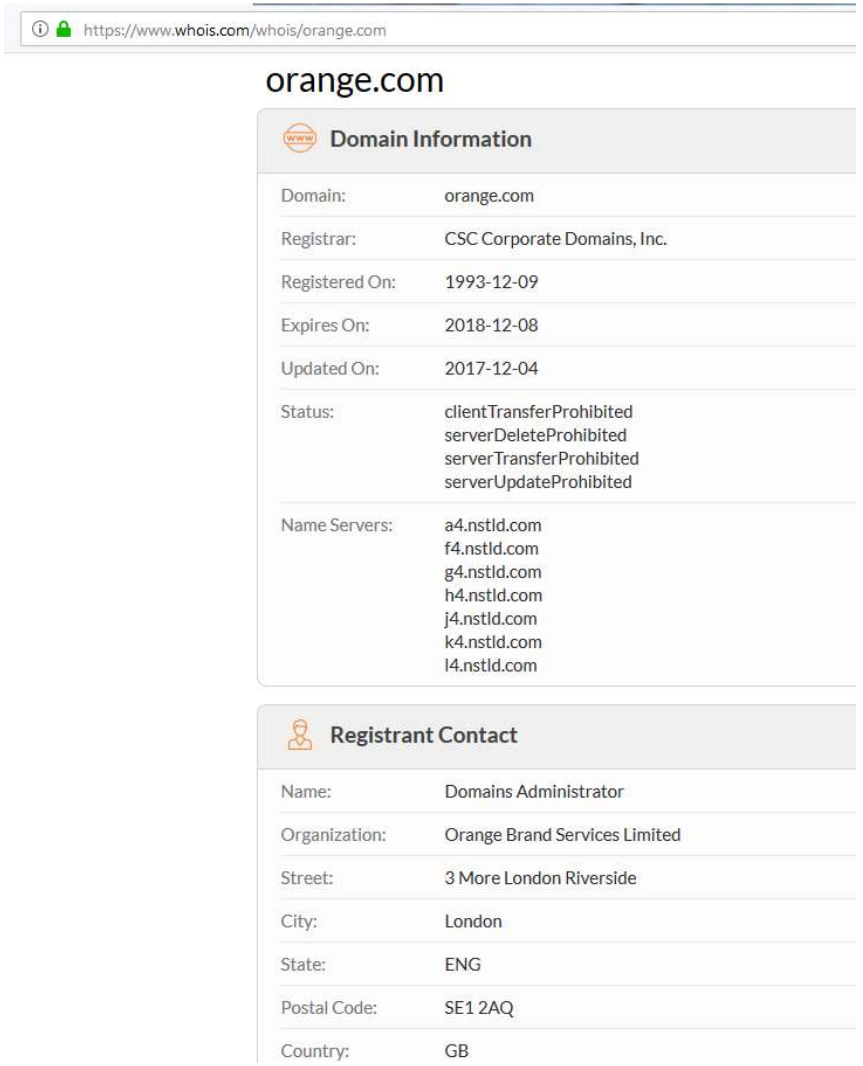
- Interception, listening

Active attacks

- Modification
- Interruption
- Denial of service

Attacks 1/6: Recognition and collection of information

- Domain names, DNS servers, blocks of assigned IP addresses
- IP addresses accessible from outside
- Services presenting a valid target
  - www, ftp, e-mail…
- Types of machines on which the services are carried out
  - Operating systems and number of version => use of the exploitable known faults
- Type of firewall and IDS (Intrusion Detection System)
- User names, groups, routing tables, SNMP information
- Physical location of the equipment and systems
- Used network protocols (IP, IPv6, IPSec, SSL/TLS)
- Cartography of the network
- Type of access connections
  - Traditional access (frame relay, broad band)
  - Wi-Fi Access
- Approach by “social engineering” (consists in questioning people and recovering information by trapping them)
  - Information on the people, their names, telephone numbers, situation in the company, addresses…



Attacks 2/6: Scan of the services and the ports

- Detailed Scan of a target (NMAP = Network Mapper)

Attacks 3/6: Enumeration

- Extraction of information on the valid accounts and the resources
  - Network resources and shared resources
  - Users and groups (as a function of the Operating system)
  - Applications
  - Character strings sent in response by the equipment

Attacks 4/6: Obtaining an access

- Tackle at the operating system level
  - Use of the functionalities of the O.S.
- Tackle at the application level
  - Use of the functionalities of the application
- Attack benefiting from a bad configuration
  - “Opened” system, default configuration (administrator name and password!), many activated functionalities
- Attack using lodged scripts
  - Scripts available on the system and sometimes activated by default (Unix/Linux)
  - Détournement de requêtes SQL lors de l’interrogation d’une base de données via interface web
- Automated Attack (ex: scan of port 80 of a whole C-class block of addresses in order to seek a fault)
- Targeted Attack : much rarer but difficult to detect (experienced pirates)

Attacks 5/6: Extension of the acquired privileges

If the pirate succeeded in entering on the system with a “weak” password => extension of the rights (authorizations)

- To carry out code to obtain privilege
- To seek to decipher other passwords
- To scan for non ciphered passwords
- To seek possible inter-network relations
- To identify badly configured files or shared resources permissions

Attacks 6/6: Cover the traces

To dissimulate to the administrator the fact that one penetrated the system

-Windows: To eliminate the entries (inputs) in the event logs and the registers

-Unix: to empty the file of history (execution of the program *log wiper*)

-! The attacker cleans the log files but does not remove them!

Attacks types

Deny Of Service DOS

Sniffing, to get information

Scanning, to get information

Social engineering

Cracking

Spoofing, to remote-control the process,

Man in the middle

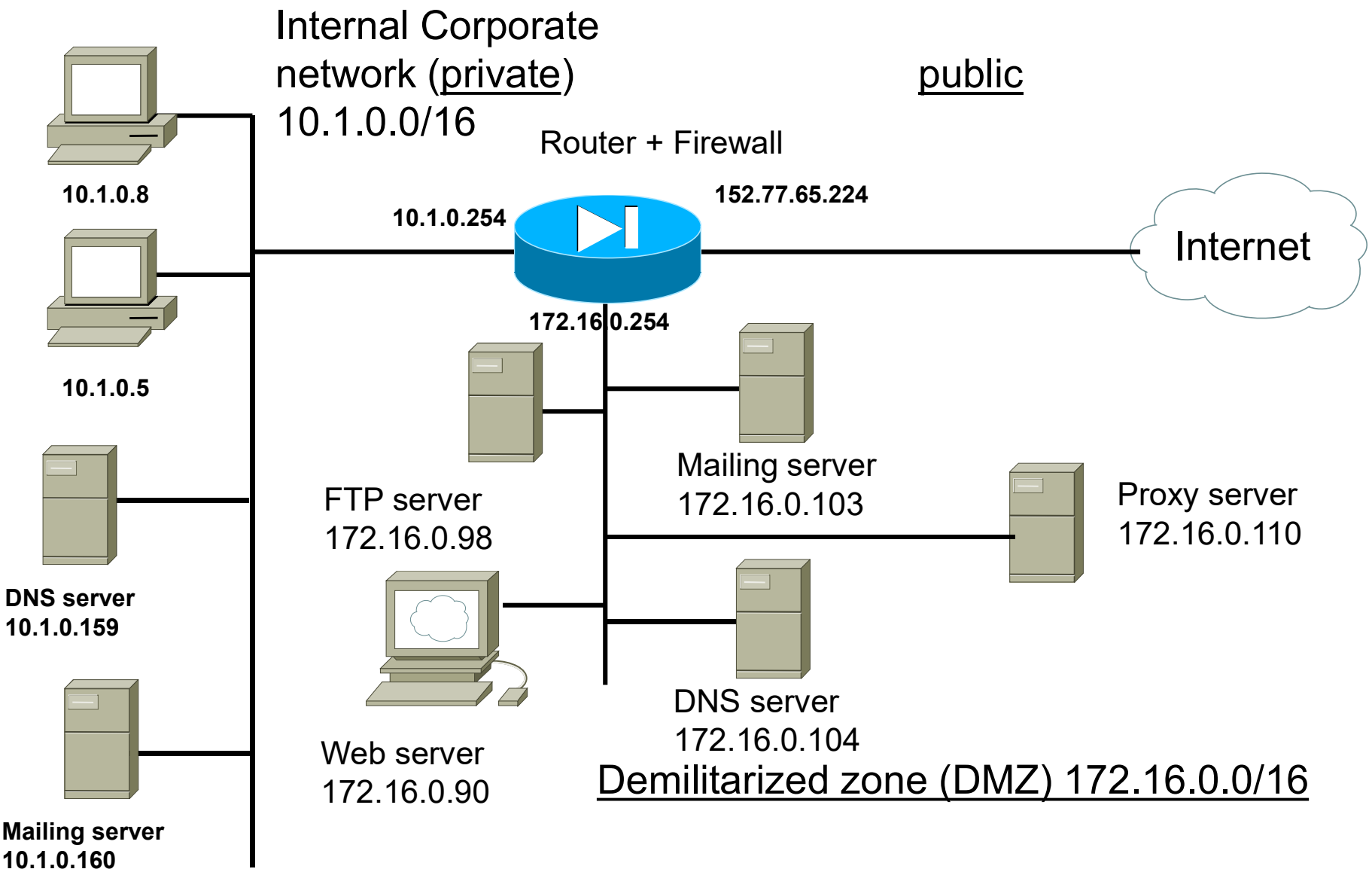
Hijacking

Buffer overflow

Overview

1. Problematics and vocabulary
2. Dependability, safety, functional safety, security (RAMSS)
3. Risk analysis
4. Some considerations on networks, Safety networks
5. Dependability of networks and networked control systems
6. Cyber-security
   - 6.1 Concepts
   - 6.2 Attacks
   - 6.3 Infrastructure, DMZ
   - 6.4 Cryptography and applications
   - 6.5 IDS, Virus
7. Applications to cyber-physical systems
8. Discussions & Conclusions

A network…


Internal Corporate
network (private)
10.1.0.0/16
public
Router + Firewall
10.1.0.8
10.1.0.254
152.77.65.224
Internet
10.1.0.5
172.16.0.254
Mailing server
172.16.0.103
FTP server
172.16.0.98
Proxy server
172.16.0.110
DNS server
10.1.0.159
DNS server
172.16.0.104
Web server
172.16.0.90
Demilitarized zone (DMZ) 172.16.0.0/16
Mailing server
10.1.0.160

Stateful firewall: Dynamic Access Control List

- Dynamic filtering
  - **Stateful inspection firewall**: packet filters that take into consideration OSI-layer 4 (TCP, UDP)
  - 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

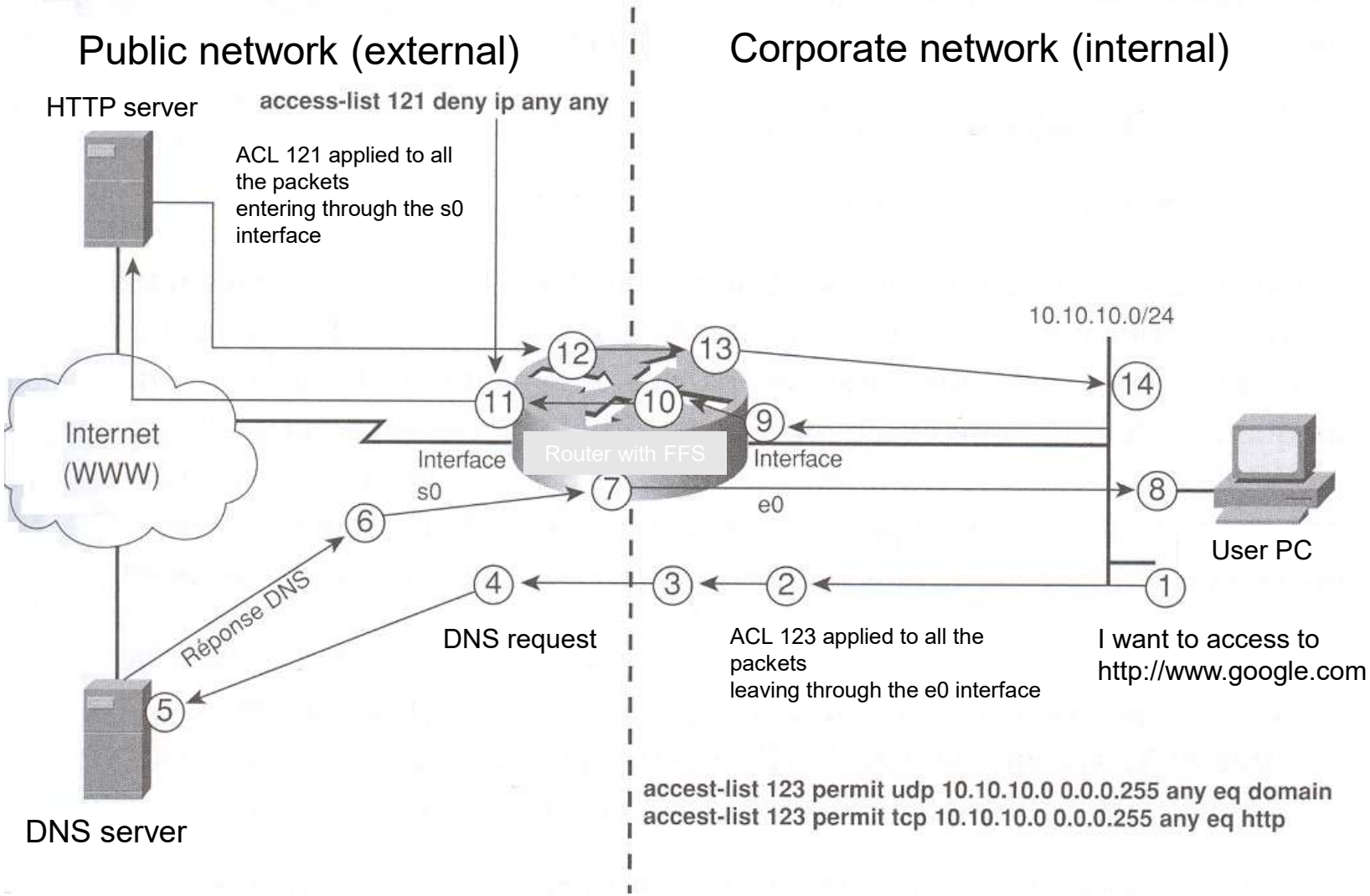
Ex: 121 ACL applied to router input, from Internet to LAN

Action Prot Adr. S. Adr. D. Serv./Port

```
ip address 192.168.254.1/30
ip address group 121 in
access-list 121 permit tcp any any eq 22
access-list 121 permit udp any any gt 1023
access-list 121 permit icmp any any gt 1023
access-list 121 permit icmp any any echo-reply
access-list 121 permit icmp any any unreachable
access-list 121 permit icmp any any administratively-
prohibited
access-list 121 permit icmp any any time-exceeded
access-list 121 permit icmp any any packet-too-big
access-list 121 permit tcp any 64.24.14.60 eq ftp
access-list 121 permit tcp any 64.24.14.61 eq smtp
access-list 121 permit tcp any 64.24.14.61 eq domain
access-list 121 permit udp 64.24.14.61 eq domain
```

1 action: permit/deny
4 parameters

Example


Public network (external)
Corporate network (internal)
HTTP server
access-list 121 deny ip any any
ACL 121 applied to all the packets entering through the s0 interface
10.10.10.0/24
Internet (WWW)
Interface s0
Router with FFS
Interface e0
User PC
Réponse DNS
DNS request
ACL 123 applied to all the packets leaving through the e0 interface
I want to access to http://www.google.com
DNS server
accest-list 123 permit udp 10.10.10.0 0.0.0.255 any eq domain
accest-list 123 permit tcp 10.10.10.0 0.0.0.255 any eq http

Some considerations on security for CPS

Everything which is not explicitely authorized is forbidden by default

In depth-security

- Global vision of the security strategy and implementation (not a juxtaposition of security mechanisms…)
- Security everywhere (internal, external)
- Application-oriented firewall

Some issues of security

- Organisational approach (security policy, human aspects, saving policy, management of users)
- Methodological approach (firewall configuration, attacks strategies and defense…)
- Technological approach (network, topology, servers, hardware and software firewalls, security protocols)
- Theoretic approach (cryptology, virology)
- Testing (quality) approach (checking, testing, audit…)

Question of implementation on low-resource embedded systems

Overview

1. Problematics and vocabulary
2. Dependability, safety, functional safety, security (RAMSS)
3. Risk analysis
4. Some considerations on networks, Safety networks
5. Dependability of networks and networked control systems
6. Cyber-security
   - 6.1 Concepts
   - 6.2 Attacks
   - 6.3 Infrastructure, DMZ
   - 6.4 Cryptography and applications
   - 6.5 IDS, Virus
7. Applications to cyber-physical systems
8. Discussions & Conclusions

Some issues of cryptography

To guarantee as well as possible

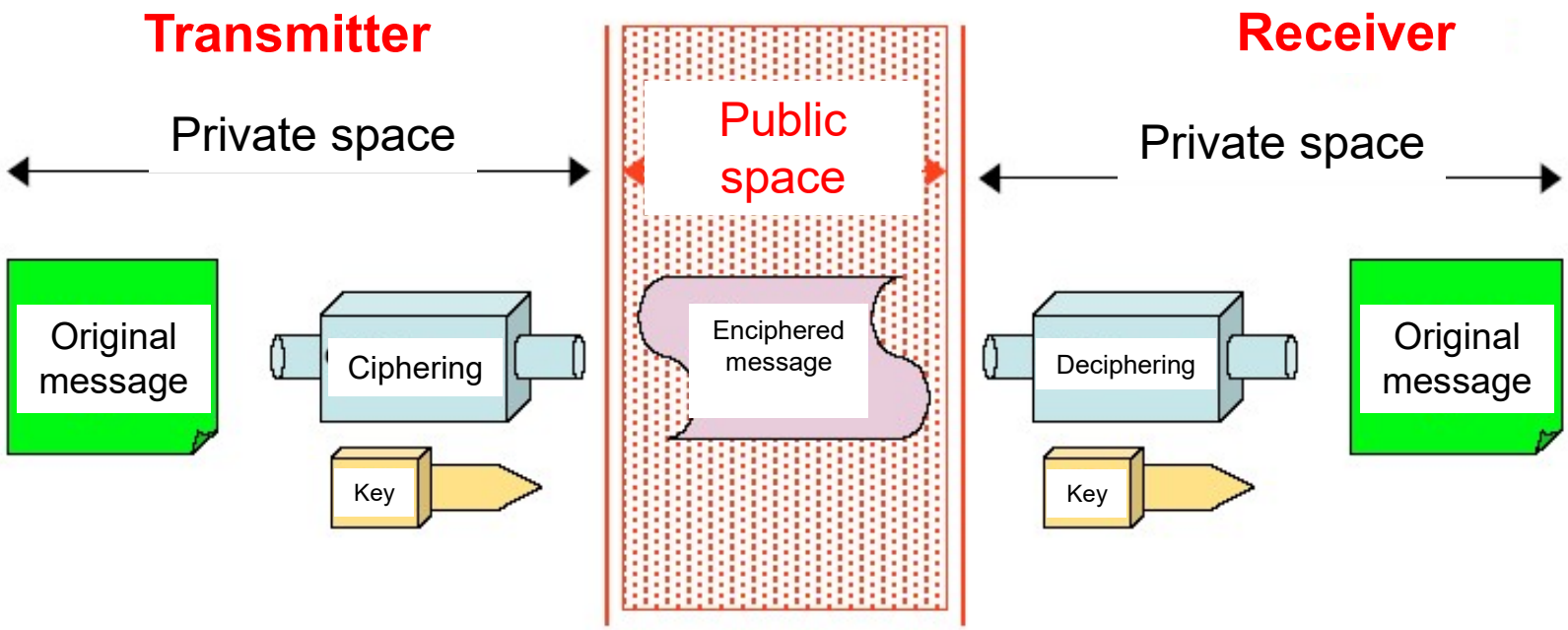
- Confidentiality
- Authenticity
- Integrity

of data (or information) exchanged

Two strategies

- Symetric cryptography
- Assymetric cryptography
- Hybrid cryptography

Symetric Cryptography (*common, shared* secret key)



- ✓ The same key is used for enciphering and deciphering
- ✓ Problem: how to transfer the key

Symetric cryptography: Caesar ciphering

Replacement of a letter by another

Robustness?

- Identical frequency contents
- Can be easily “broken” easily starting from a message of 28 letters…

Example: shift of two letters towards the line

- *Bonjour* => Dqplqwt

Another example: shift of a letter towards the left

- IBM => HAL (“2001: A Space Odyssey”)

Symetric cryptography: poly-alphabetical codes

- Let's consider an alphabet {A, B, C, D}

text t / key k	A B C D
A	C D B A
B	D C A B
C	C A B D
D	B D A C

plaintext: ABCB ACCB AACB B

Key: DBBC BAAC DDBB C

Encrypted text: BCAA DBBA BBAC A

- Require very large size keys not to be very vulnerable …

Symetric cryptography: Operations at the bit level
Distance permutations

- d1=1, d2 = 01, d3 = 001, d4= 0001…
- Distance permutation (di, dj)
- Example: TS
- Form substitution
- Example (d1, d2, d3, d4) substituted by (d2d3, d3d1, d1d4, d1d3)
=> increases the size of the data

TS

54 53

0101 0100, 0101 0011

d2 d2 d2 d4 d2 d3 d1

d3d1 d3d1 d3d1 d1d3 d3d1 d1d4 d2d3

0011 0011 0011 1001 0011 10001 01001

- Then to decipher…

Symetric cryptography: Operations at the bit level
Distance permutations: exercise

- Encipher *BON* by substituting (d1, d2, d3, d4, d5, d6) by (d2d3, d3d1, d1d4, d1d3, d2d4, d5d6) with d1=1, d2 = 01, d3 = 001, d4= 0001…

BON

42, 4F, 4E

Symetric cryptography: Inversion of bits according to a random suite

$(a_n) = (2, 14, 7, 11, 74, 25, 32, 37, 152, 99, 7)$

$\Rightarrow (b_n) = (2, 6, 7, 3, 2, 1, 0, 5, 0, 3, 7)$

F= 01001010 10010101 00101001 00010100 11010110 11110001

And

F'= 01**1**0100**01** 100**0**0101 00**0**01001 0**1**010100 **0**1010**0**10 **0**11**0**000**0**

Bit 2 Bit 6 Bit 3 Bit 2…

Symetric cryptography: Inversion of bits according to a random suite: exercise

BON with the random suite

$(a_n) = (3, 4, 11, 27, 32, 25, 12, 153, 77, 7)$

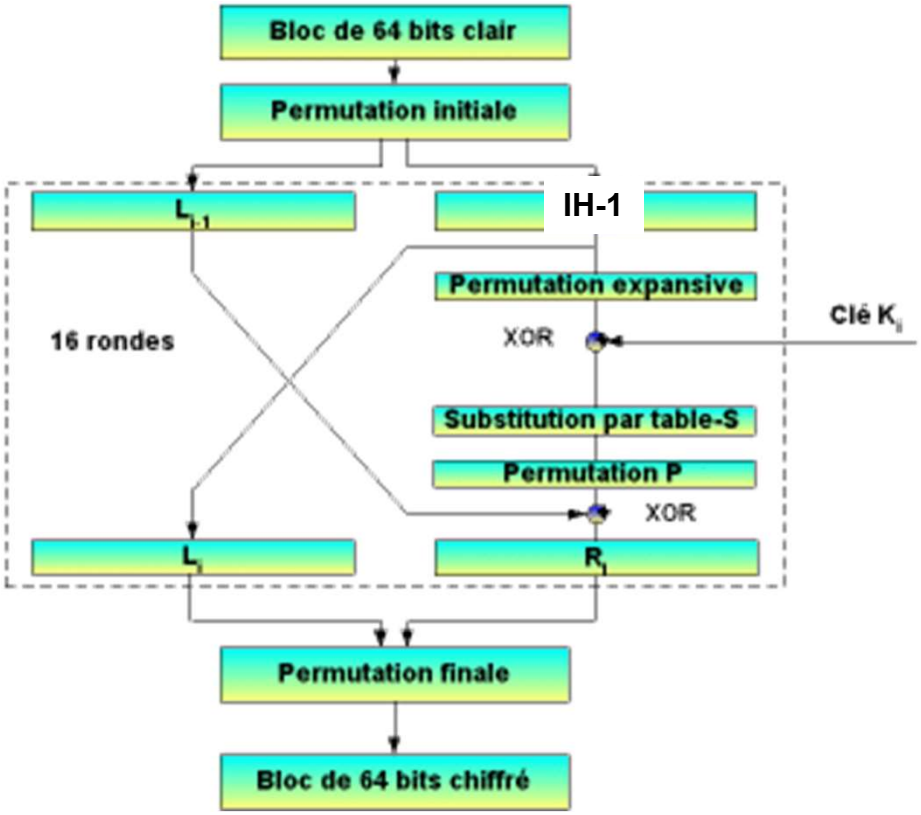
We work on 9-bit packets

42, 4F, 4E

Symetric cryptography: The standard algorithm for enciphering: IBM DES (Data Encryption Standard)

- Created 1977
- At first for classified or secret documents
- Today software and smart cards industry
- Enciphering and deciphering speed (rapidity)
  - Can be developed in less than 200 lines
  - Very fast on dedicated electronic charts
    - Smart cards
    - Electronic systems of telecommunications
- Implementation on Unix, Windows and MacOs available on Internet (chalmers.se/pub for example)

Symetric cryptography: The standard algorithm for enciphering: IBM DES (Data Encryption Standard)



- Based on XOR functions
- Sequential logics
- Sure
- Rapid
- Easy to implement

but

- Need to exchange the key
  - Problem of security during the transmission of the key

Symetric cryptography: Flow encryption vs. Block encryption *(chiffrement par flot, par bloc)*

- DES and classical symetric algorithms are based on block encryption, which means that the message/file to encrypt is divided into blocks
- For some applications, it is interesting to encrypt the message/file at once. Encryption may be achieved without waiting for other data.
- This technics is used for devices with electric consumption constraints (ex: smart phones)
- Based on linear feedback shift register (registre à décalage à rétroaction linéaire)

Symetric cryptography: Symetric algorithms

3DES (triple DES)

- It consists in using three times the DES algorithm with three keys k_1, k_2 et k_3 : m'=$DES_{k1}(DES_{k2}(DES_{k3}(m)))$
- Alternative with 2 keys and by using twice the algo of encrypting and once the algo of decoding: m'=$DES_{k1}(DES^{-1}_{k2}(DES_{k1}(m)))$, this alternative is considered more secure
- Another alternative: program TRAN (ripem.msu.edu/pub/crypt/other/tran.shar)
- DESX (DES XORed), GDES (Generalized DES), RDES (Randomized DES)

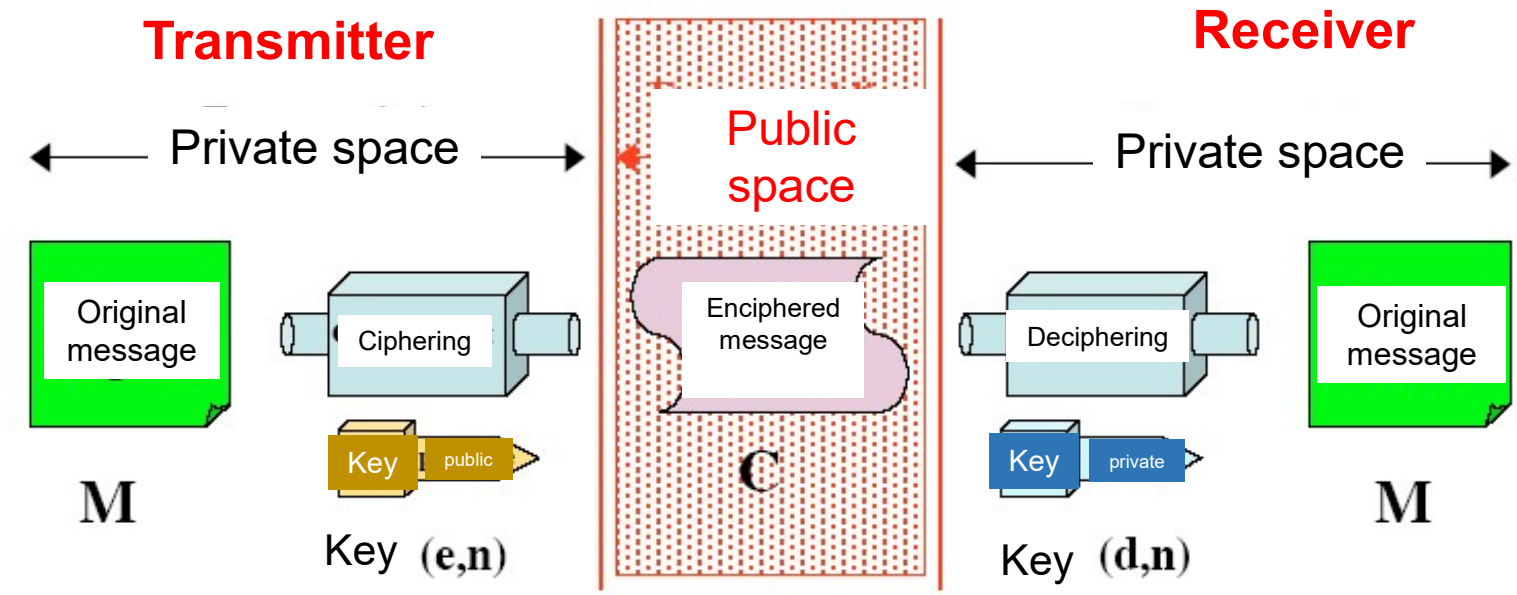
AES (Advanced Encryption Standard)

- Developed to replace DES and offer a better security
- N.B. At the end of 2003, the American department of defense approved its authorization
- Used in IPSec (secured IP) and IKE (Internet Key Exchange)

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080110bb6.html

Assymetric Cryptography (couples of private and public key)

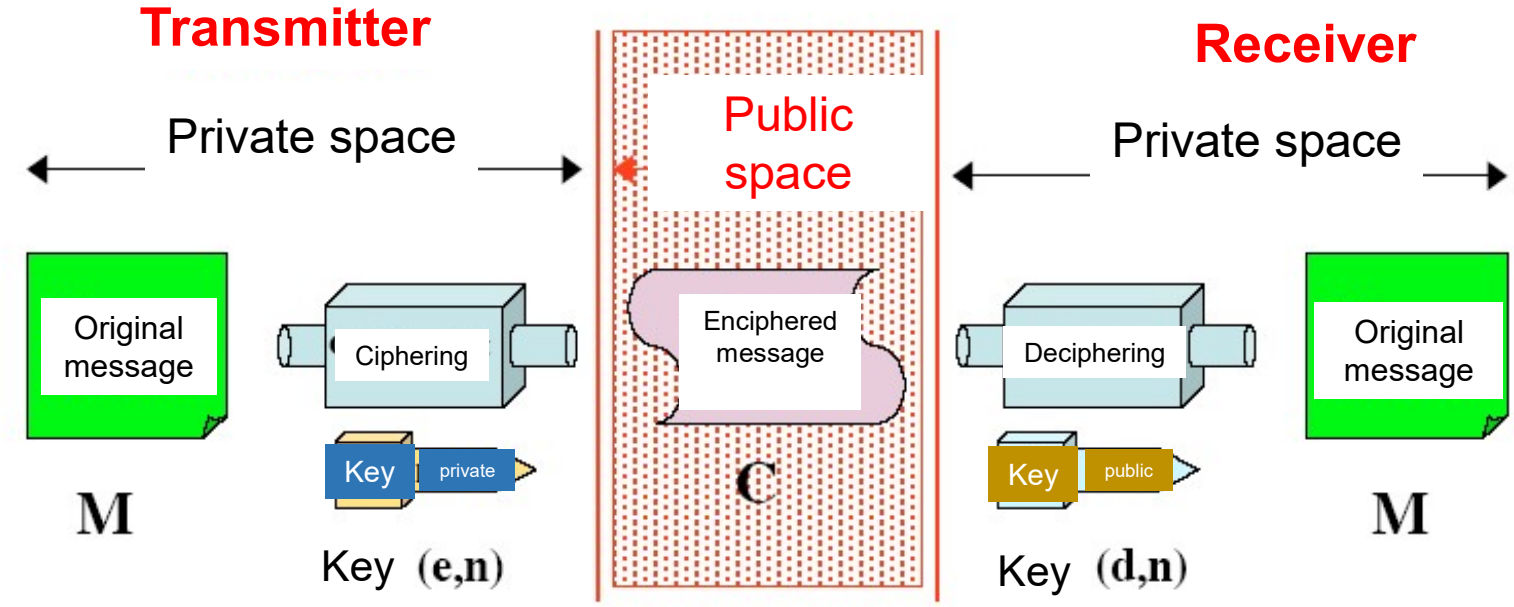
Protection of **confidentiality** = private key on the **receiver** side)



- ✓ Encryption is achieved thanks to the **public** key
- ✓ Warrant that the owner of the private key ONLY can **decrypt** the message

Assymetric Cryptography (couples of private and public key)

Protection of **authentication (signature)** = private key on the **transmitter** side)



- ✓ Encryption is achieved thanks to the **private** key
- ✓ Warrant that the owner of the private key ONLY can **sign** the message

Assymetric Cryptography: RSA ciphering Protocol

Proposed in 1977 by the cryptologists Rivest, Shamir and Adleman

Based on the modular exponentiation (trap function)

Main applications

- Sending of confidential messages to a person
- Authentication by any person of the message sent by an individual
- Authentication by password (smart cards, bank cards)

Security based on the impossibility of carrying out the factorization of a large number of a few hundreds of digits in a reasonable time

- The user selects two large prime numbers p and q, then multiplies them to obtain n=p.q (integer modulating the RSA protocol)

Assymetric Cryptography: RSA

The algorithm is remarkable by its simplicity. It is based on the prime numbers.

To encipher a message:

c = m^e mod n

To decipher: **m = c^d mod n**

m = clear message
c = encrypted message
(e, n) constitutes the public key
(d, n) constitutes the private key
n is the result of the multiplication of 2 prime numbers
^ is the power function (a^b: a power b)
mod is the operation of modulo (remainder of the *integer division*)

Assymetric Cryptography: RSA

Creation of a pair of keys

It is simple, but the **e**, **d** and **n** should be chosen with care! And the calculation of these three numbers is delicate.

Methodology:

- The user selects two large prime numbers p and q, and multiplies them to obtain n=p.q (integer modulating the RSA protocol), We should choose p and q with equivalent sizes.

  It is advised that n is higher or equal to 512 bits

- Take a number **e** which does not have any factor in common with

  (p-1) (q-1).

- Calculate **d** such as **ed mod (p-1)(q-1) = 1**

The couple **(e, n)** constitutes the public key.

(d, n) is the private key.

Various other rules are to be respected for the use of these prime numbers so that the algorithm cannot be “broken”

Prime numbers

Largest Known Prime Number:

$2^{77\,232\,917}-1$

Found in December 2017, composed of 23 249 425 digits

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223…

Assymetric Cryptography: RSA

https://www.cs.drexel.edu/~jpopyack/IntroCS/HW/RSAWorksheet.html

Let's encipher the message "**HELLO**". Let's take first the ASCII code (into decimal) of each character and one puts them end to end:

m = 72-69-76-76-79

Then, it is necessary to cut out the message in blocks which is composed of less digits than **n**. **n** is composed of 4 digits, one thus will cut out our message in blocks of 3 digits:

726 976 767 900
(let's complete with zeros)

Then one encrypt each one of these blocks:

726^13 mod **21209** = 11600
976^13 mod **21209** = 5705
767^13 mod **21209** = 16590
900^13 mod **21209** = 3565

The encrypted message is **11600.5705.16590.3565**. One can decipher it with d:

11600^1609 mod **21209** = 726
5705^1609 mod **21209** = 976
16590^1609 mod **21209** = 767
3565^1609 mod **21209** = 900

I.e. the digit suite: **726976767900**.
We find the clear message: **72 69 76 76 79**: "**HELLO**".

Symetric vs. Assymetric Cryptography

1. Symetric
    1. Very simple operations (logical functions)
    2. Easy to implement (limited resources)
    3. How to exchange the key between the sender and the receiver and to be sure there are to “man-in-the-middle”
2. Asymetric
    1. “Complex” operations (exponential modulo),
    2. Needs calculation resources
    3. Private keys kept unique and secure, exchange of public keys only
3. Combine the advantages of both

    => Hybrid cryptography

Hybrid cryptography: generation of a sharing key

Two users will design a common key which will be useful for them only

ASSYMETRIC ASPECT

They choose n the multiple of 2 prime numbers p and q and an integer a (a and n can be known (not confidential))

Then each one chooses an integer X belonging to [1, n-1] and calculates the integer $Y=a^X \bmod n$

We obtain two couples (X_1,Y_1) and (X_2, Y_2) where the values Y_1 and Y_2 will be published

HYBRID ASPECT

Each one of them can then calculate the key $c=a^{X1X2} \bmod n$ because $c=(Y1^{X2} \bmod n)=(Y2^{X1} \bmod n)$

R: Each one knows its own X only

Security comes from the fact that it is impossible in a reasonable time to obtain the key C by the calculation of a discrete logarithm (unfeasible in a reasonable time taking into account the size of p and q)

SYMETRIC ASPECT

Users can now exchange encrypted data using a Symetric system with the common key c

Hybrid cryptography: generation of a sharing key: exercise

Generate a shared key with your neighbor

(ex:

a=3 et n=14 (public values (known)) n=2*7

X_1 = 4 (secret value known only by the participant on the left)

X_2 = 3 (secret value known only by the participant on the right)

Cryptography: Some considerations on breaking a 768-bit RSA key

- From an Inria document, 2010.

- Key used for bank cards

- To break the key, find the prime numbers which compose the key: it is a number composed of 232 figures (2^{768})…

- Need efficient algorithm

- Need large calculation capacities: use of Grid'5000 => 1544 computers with more than 5000 cores.

- Collaboration with CH, JP, NL, DE : on average 1700 cores used during one year of calculation…

- One week by using the supercomputer *Jaguar* (from *Oak Ridge National Laboratory*) if available (not such computers in Europe…)

- The purpose was to show if it is possible to break using grid of « classical » computers

- Next step: to break a 1024 bit-key => it should be possible around 2020

- Advise from ANSSI (2010):

  Use at least 1536 bit-keys for applications until 2010

  Use at least 2048 bit-keys for application beyond 2010

Conclusions on cryptography

- Hybrid cryptography
- Difficult implementation of assymetric cryptography
- Integrated in the certificates
- Integrated in security protocols (IPSec, SSL/TLS)
- Integration of cryptography and more generally of security mechanisms in industrial applications

Overview

1. Problematics and vocabulary
2. Dependability, safety, functional safety, security (RAMSS)
3. Risk analysis
4. Some considerations on networks, Safety networks
5. Dependability of networks and networked control systems
6. Cyber-security
   - 6.1 Concepts
   - 6.2 Attacks
   - 6.3 Infrastructure, DMZ
   - 6.4 Cryptography and applications
   - 6.5 IDS, Anti-Virus
7. Applications to cyber-physical systems
8. Discussions & Conclusions

Intrusion detection and response

- Purpose: to detect and respond to network attacks and malicious code (anti-virus)

- Malicious code

  Intended to harm, disrupt, or circumvent computer and network functions (viruses, trojan horses, worms…)

- Network attacks

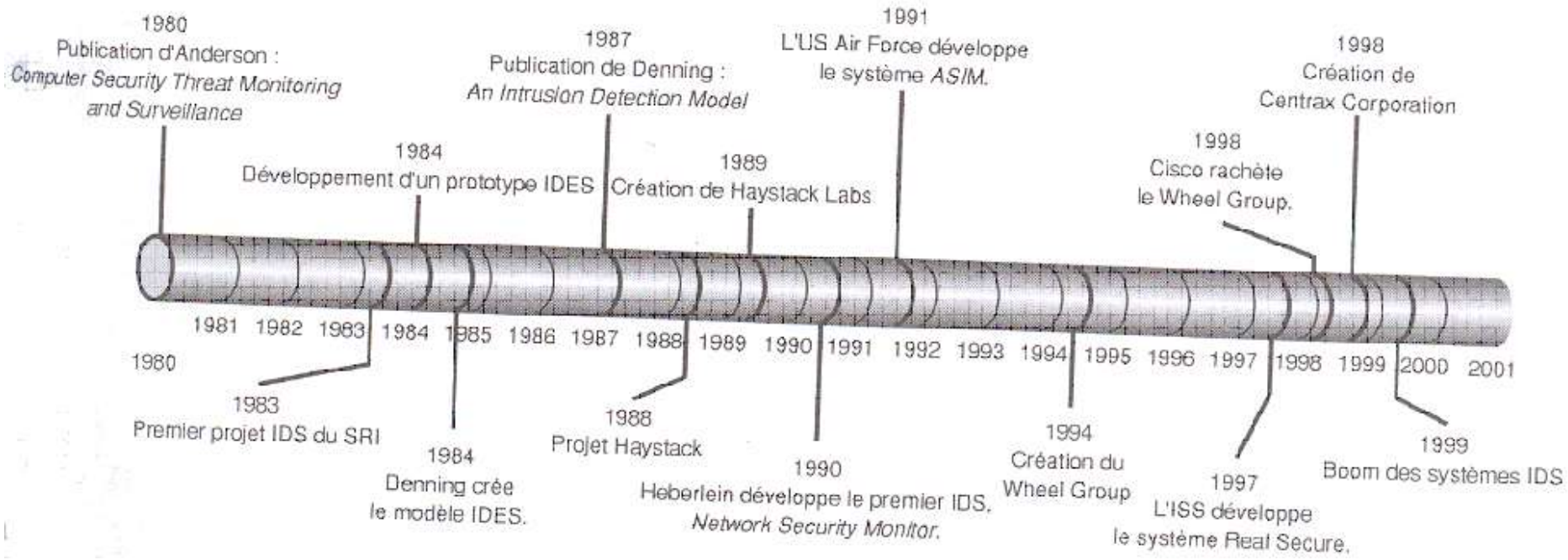
  Modification attacks: unauthorized alteration of information

  Repudiation attack: denial that an event or transaction ever occurred

  Denial-of-service attack: actions resulting in the unavailability of network resources and services, when required

  Access attacks: unauthorized access to network resources and information

History of the development of IDS (for IT)



Today, the products implement concepts dating from the years 1980

Signature-based IDSs

Signature-based IDSs: signature or attributes that characterizes an attack are stored for reference (if there is a match, a response is initiated)

Advantages

- Low false alarm rates
- Standardized (generally)
- Understandable by security personnel

Disadvantages

- Failure to characterize slow attacks that extend over a long period of time
- Only attack signatures that are stored in the database are detected
- Knowledge database needs to be maintained and updated regularly
- Because knowledge about attacks is very focused (dependent on the operating system, version, platform, and application), new, unique, or original attacks often go unnoticed

Statistical anomaly-based IDSs

Statistical anomaly-based or behavior-based IDSs: dynamically detects deviations from the learned patterns of « normal » user behaviour and trigger an alarm when an intrusive activity occurs

Needs to learn the « normal » usage profile (which is difficult to determine)

Advantages

- Can dynamically adapt to new, unique, or original vulnerabilities
- Not as dependent upon specific operating systems as a knowledge-based IDS

Disadvantages

- Does not detect an attack that does not significantly change the system-operating characteristics
- High false alarm rates. High positive are the most common failure of behavior-based ID systems
- The network may experienced an attack at the same time the intrusion detection system is learning the behaviour

Functionalities of IDS: Responses to the detected intrusions

Active answers

- -To undertake an aggressive action against the intruder
  - (! Attention with legality!)
- -To restructure the network architecture
  - To isolate the attacked system
  - To modify the environment parameters which made the intrusion possible
- -To supervise the attacked system
  - To collect information in order to understand the intrusion
  - To identify the author of the intrusion and his approach
  - To identify security failures

Passive answers

- -Generation of an alarm
- -Emission of a SMS message towards the administrator

Some tools (for IT)

- -Snort, Suricata, Bro, Cisco secure IDS, Billy Goat, Enterasys

Overview

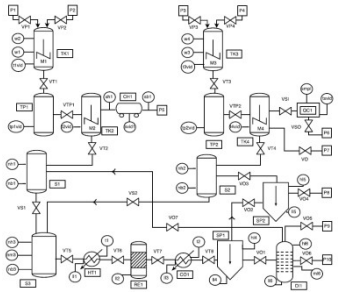
1. Problematics and vocabulary
2. Dependability, safety, functional safety, security (RAMSS)
3. Risk analysis
4. Some considerations on networks, Safety networks
5. Dependability of networks and networked control systems
6. Cyber-security
7. Applications to cyber-physical systems
   - 7.1 Considerations on Intelligent Control systems
   - 7.2 Intrusion detection on GOOSE messages for smart grids
   - 7.3 Processus-oriented detection attacks
   - 7.4 Risk analysis of a drone
8. Discussions & Conclusions

Industrial control Systems [Stouffer 2011]

Generic term regrouping

SCADA (Supervisory Control And Data Acquisition)

- Distributed on several geographical areas



DCS (Distributed Control Systems)

- Just in a local zone

other configurations based on **PLC** (Process Logic Controller)

Evolution of ICS systems

- Previously isolated and using proprietary protocols
- Security not taken into account (security by obscurity)
- Now more and more connected for economic reasons
- Use of classical IT solutions (architecture, OS, network protocols)
- More vulnerable to attacks

Comparison between ICS and classical IT systems

Category	IT systems	ICS systems
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

ICS Specificities

	Information Technology	*Operation Technology*
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
Security Attributes	Cyber sécurity: Confidentiality Integrity Availability	Dependability: Availability Reliability Safety

Some other considerations on ICS

- Define the model of trust
- Define the model of threats
- Vulnerabilities linked to security procedures and policy
- Vulnerabilities linked to the architecture
- Vulnerabilities linked to networks

- Control systems
  - Communication: protocole, flow
  - Tasks: state, scheduling
  - Resources: memory, cpu, traffic
  - Data and control flows: timestamp, values intervalles

Overview

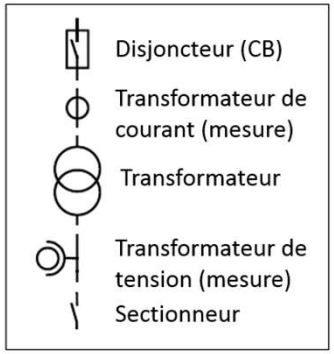
1. Problematics and vocabulary
2. Dependability, safety, functional safety, security (RAMSS)
3. Risk analysis
4. Some considerations on networks, Safety networks
5. Dependability of networks and networked control systems
6. Cyber-security
7. Applications to cyber-physical systems
   - 7.1 Considerations on Intelligent Control systems
   - 7.2 Intrusion detection on GOOSE messages for smart grids
   - 7.3 Processus-oriented detection attacks
   - 7.4 Risk analysis of a drone
8. Discussions & Conclusions

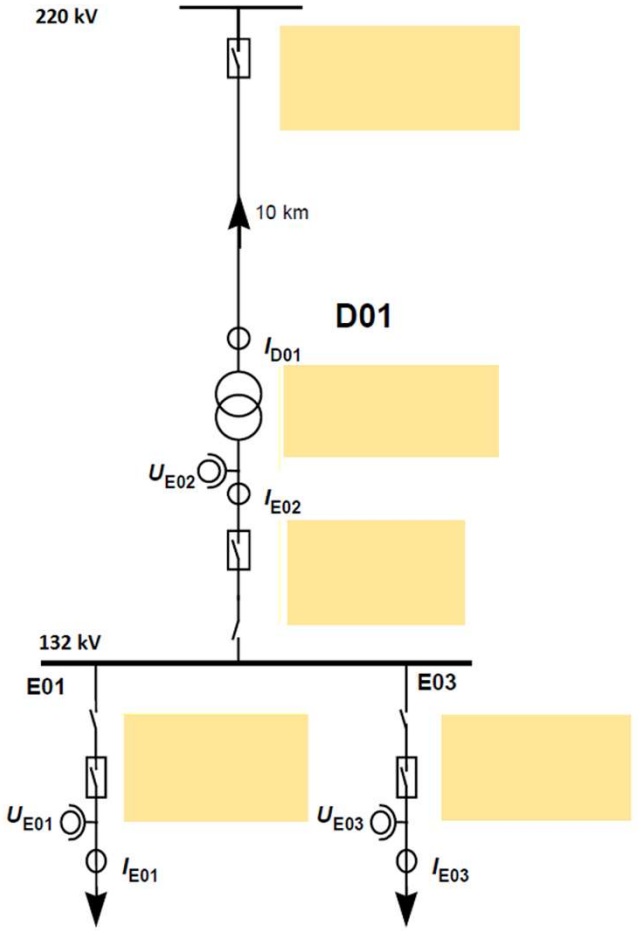
Analyse des risques cyber sécurité d'un poste IEC 61850 typique 1/3

- Objectifs
  - Comprendre le risque de cyber attaque sur le transfert de données IEC 61850
  - Comprendre l'impact sur le fonctionnement optimal et sûr du poste
- Attributs de sécurité
  - Disponibilité
  - Fiabilité
  - Sûreté
- Méthodologie
  - Simple
  - Description fonctionnelle du système (VS. une implémentation particulière)

Analyse des risques cyber sécurité d'un poste IEC 61850 typique 2/3

- Système
- **Primaire** (réseau électrique) → transport et distribution électrique
- **Secondaire** (système d'automatisation du poste - SAS) → contrôle, supervision, protection et monitoring



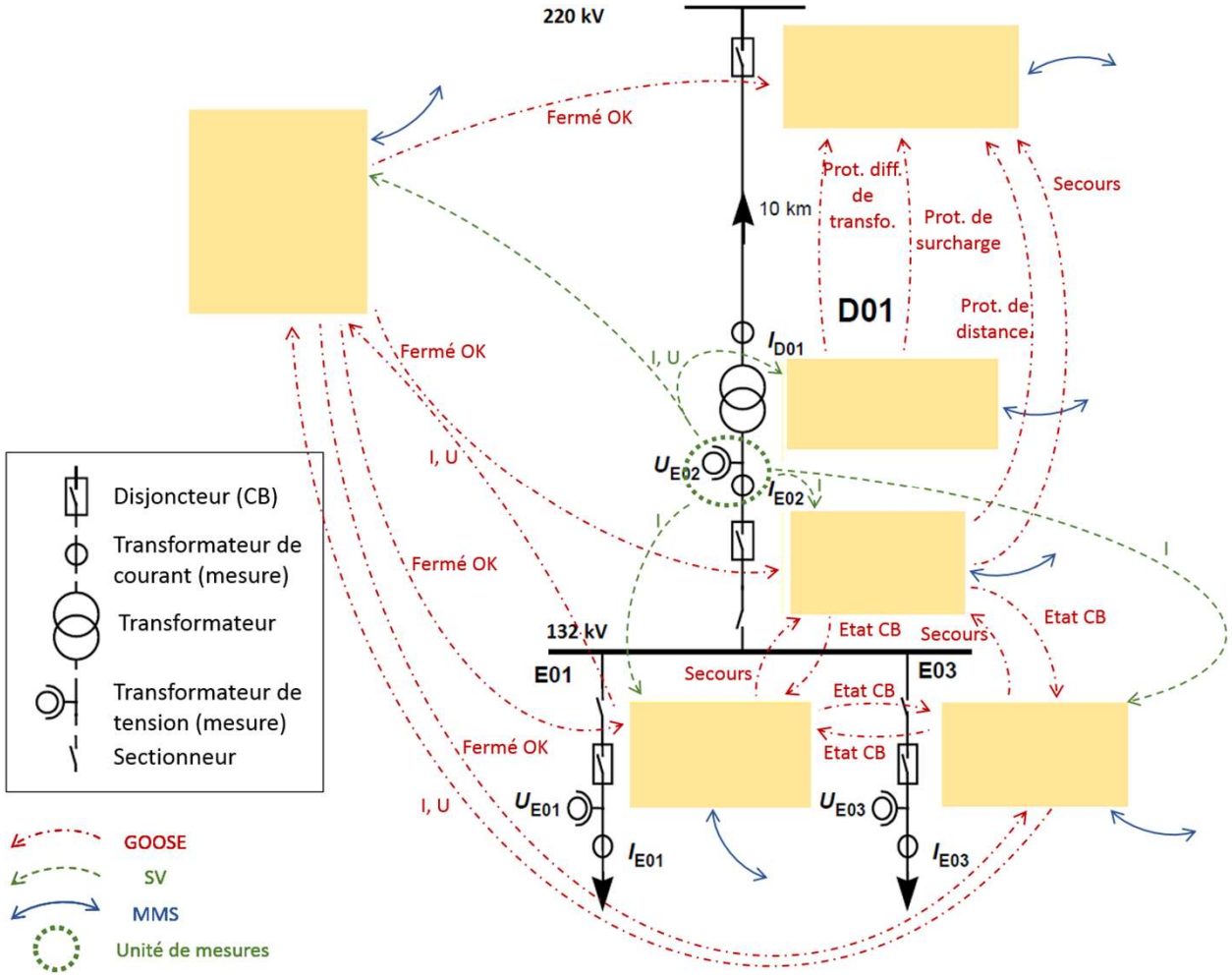


Exemple d'un poste de transport de petite taille

Analyse des risques cyber sécurité d'un poste IEC 61850 typique 2/3

- Système
- **Primaire** (réseau électrique) → transport et distribution électrique
- **Secondaire** (système d'automatisation du poste - SAS) → contrôle, supervision, protection et monitoring

- Fonctions distribuées basées sur la communication

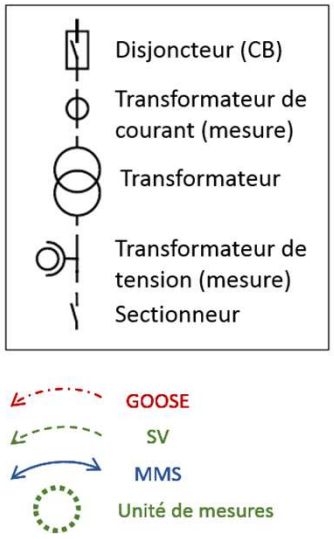


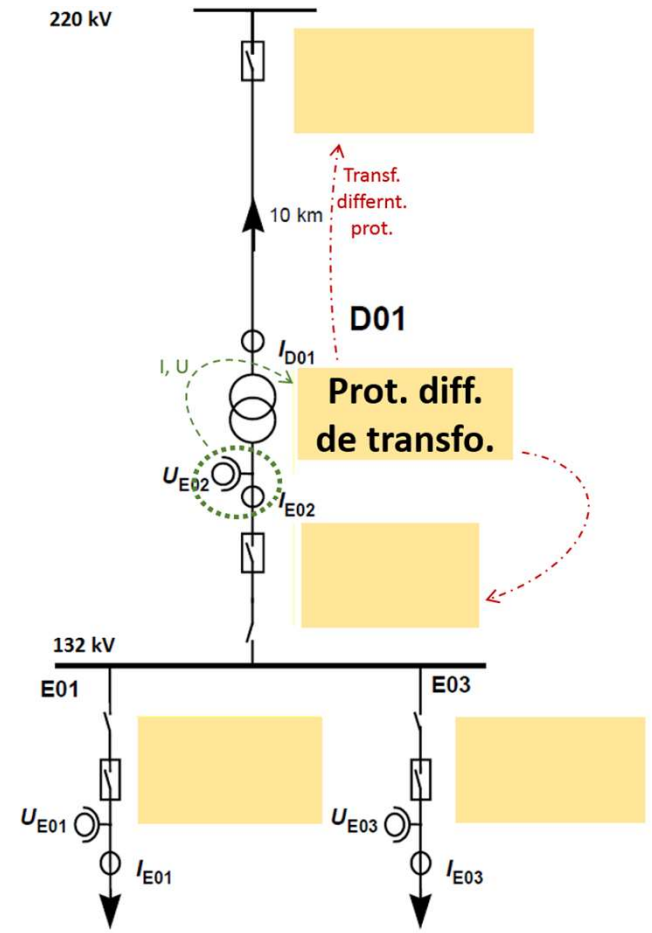
Exemple d'un poste de transport de petite taille

Analyse des risques cyber sécurité d'un poste IEC 61850 typique 2/3

- Système
- **Primaire** (réseau électrique) → transport et distribution électrique
- **Secondaire** (système d'automatisation du poste - SAS) → contrôle, supervision, protection et monitoring

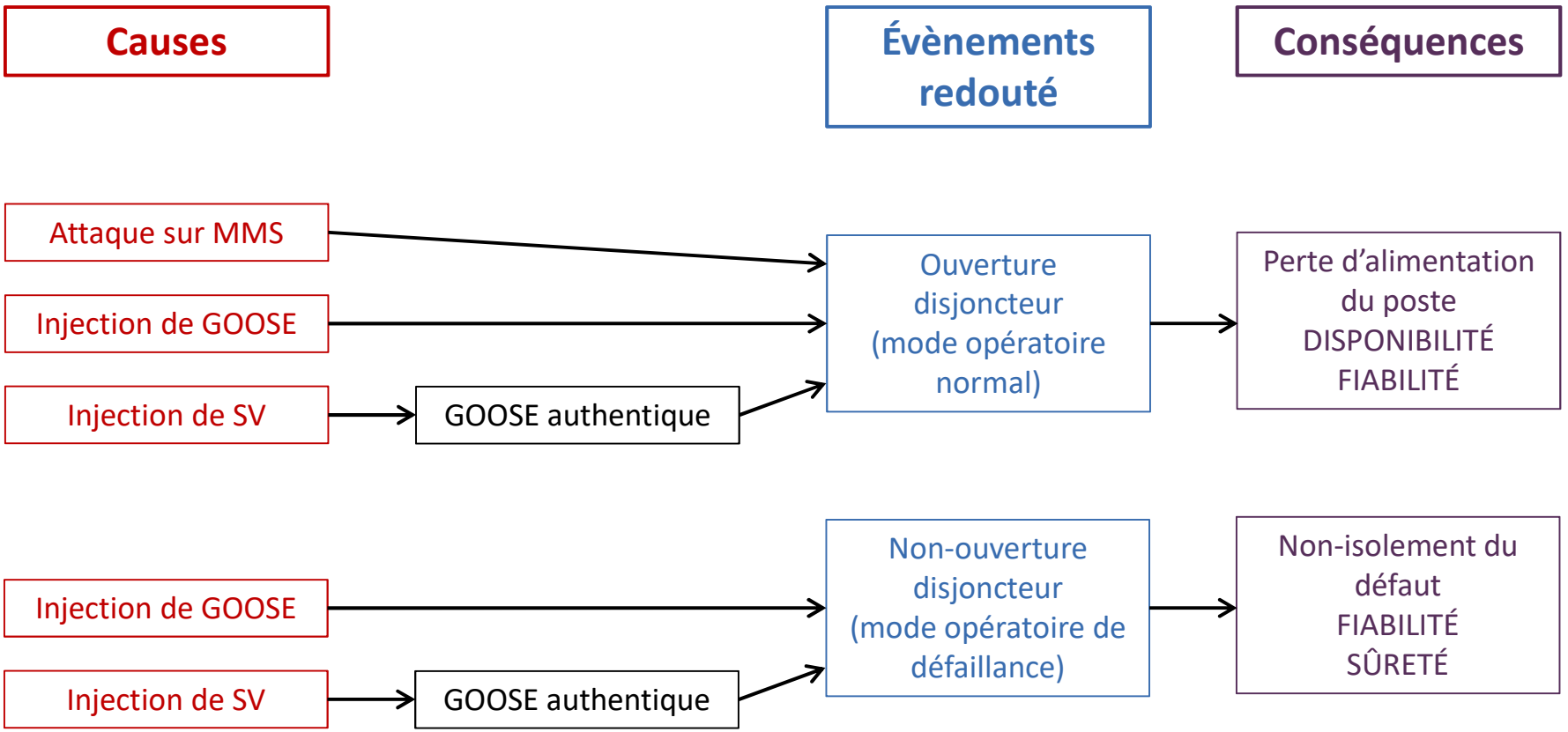
- Fonctions distribuées basées sur la communication





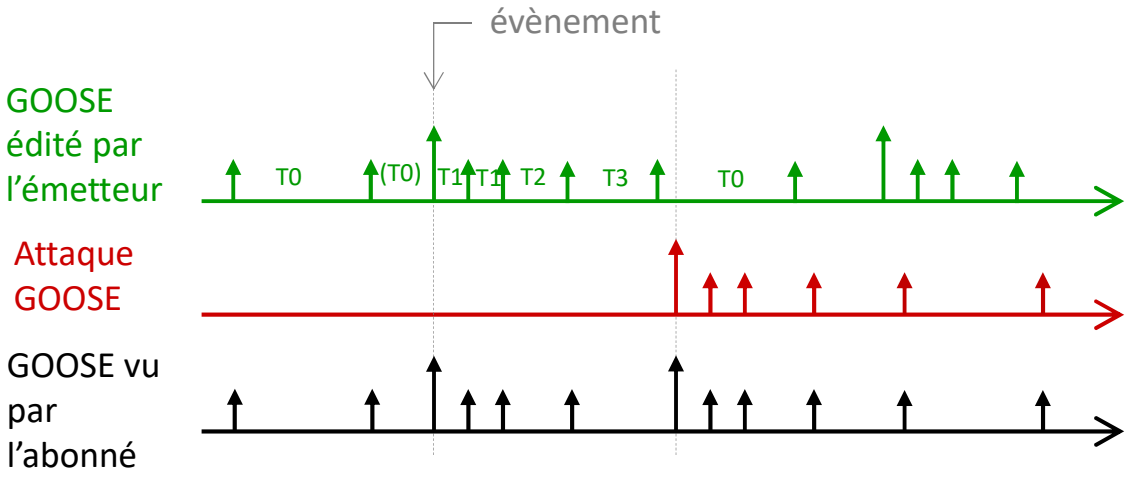
Exemple d'un poste de transport de petite taille

Analyse des risques cyber sécurité d'un poste IEC 61850 typique 3/3



Fiabilité et injection de faux messages GOOSE

- Mécanisme de transfert de données GOOSE
  - Editeur / abonné
  - Broadcast
  - Compteurs : Numéro d'état (*State number - StNum*) et numéro de séquence (*Sequence Number - SqNum*)



Mécanisme de transfert du protocole GOOSE … et exploit

T0	Retransmission en conditions stables
(T0)	Cycle de retransmission en conditions stables peut être interrompu par un évènement
T1	Délai de retransmission le plus court, après un évènement
T2, T3	Le délai de retransmission double jusqu'à T0

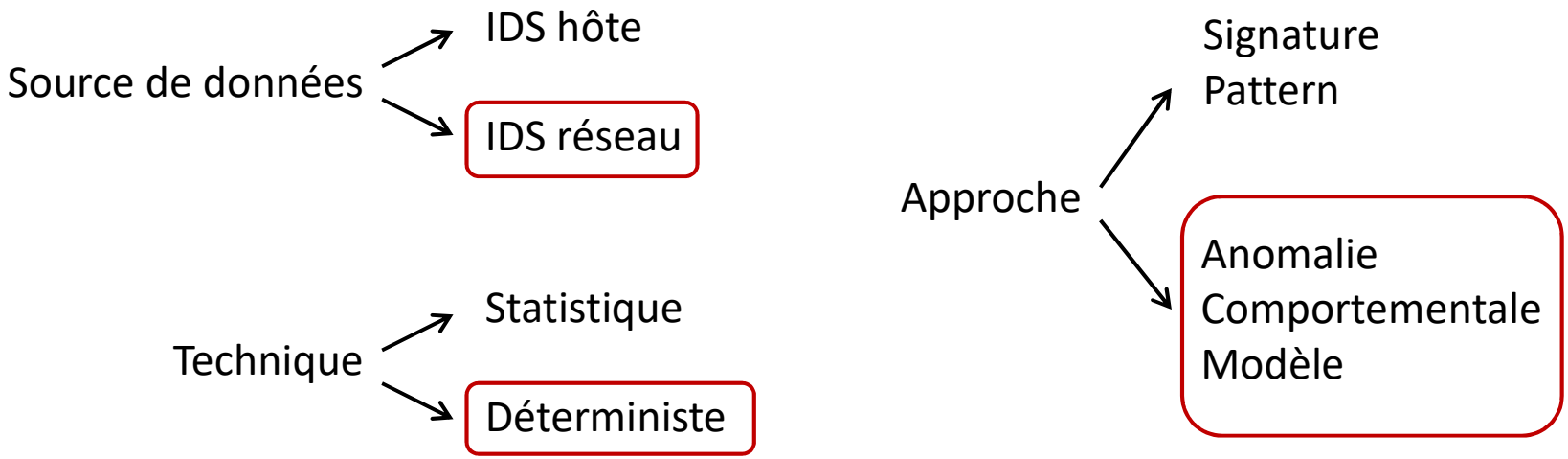
Approche de détection d'intrusion

- La détection d'intrusion est une mesure clé pour une sécurité "end-to-end"

(IEC 62351 "Gestion des systèmes de puissance et échange d'informations associé - Sécurité des communications de données")

- Détection d'Intrusion : "service de sécurité qui monitore et analyse les événements système dans le but de détecter, et avertir en temps-réel ou presque temps-réel, toute tentative d'accès aux ressources du système de façon non autorisée"

(IEC 62443 "Sécurité des automatismes industriels et des systèmes de commande")



Système de détection d'intrusion réseau pour la communication GOOSE, approche déterministe et basée anomalies 1/3

Ethernet				Ethernet	
@ destination	@ source	Ethertype 0x88b8	APDU	Pad	CRC

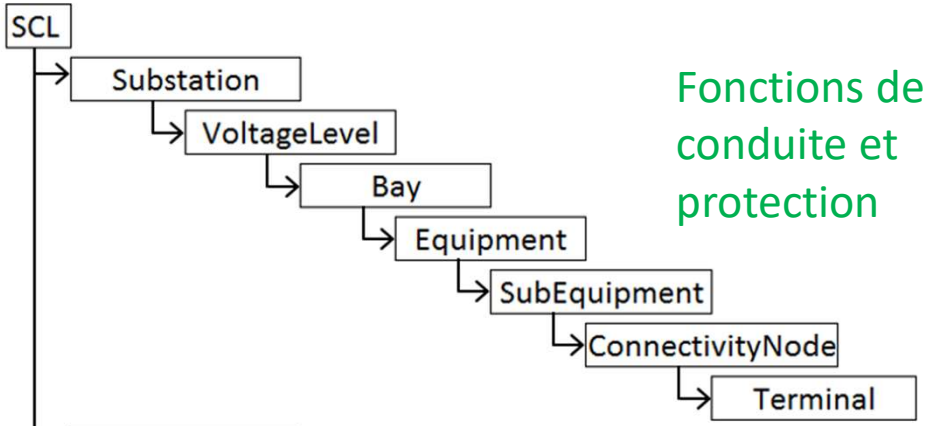
Structure simplifiée d'une trame GOOSE

- Vérification d'une trame unique
  - Définition du protocole (ex. : valeur d'un champ)
  - Origine/destination (ex. : couple @ source / @ destination)
  - Configuration du système de communication (ex. : paramétrage du mécanisme de transfert GOOSE)
  - Configuration de l'application GOOSE
- Vérification multi-trames :
  - Profil de temps
  - Séquence de messages

Système de détection d'intrusion réseau pour la communication GOOSE, approche déterministe et basée anomalies 2/3

- Information sur le vocabulaire et la grammaire du protocole ainsi que la structure de la communication
  - Norme
  - Fichiers de configuration SCL

- *"Substation Configuration Language"*
  - Fichier "*Substation Configuration Description*"



Fonctions de conduite et protection

Structure d'un fichier SCL

Système de détection d'intrusion réseau pour la communication GOOSE, approche déterministe et basée anomalies 3/3

- Extraction d'informations d'identification et de paramétrage pour le PDU
- Directement ou indirectement

- Anomalies ≠> vulnérabilités
  - Adresse de destination MAC
  - APPID (*Application Identifier*)
- Anomalies ? vulnérabilités
  - Adresse source MAC
- Anomalies => vulnérabilités
  - Horodatage T (IEC 62351)

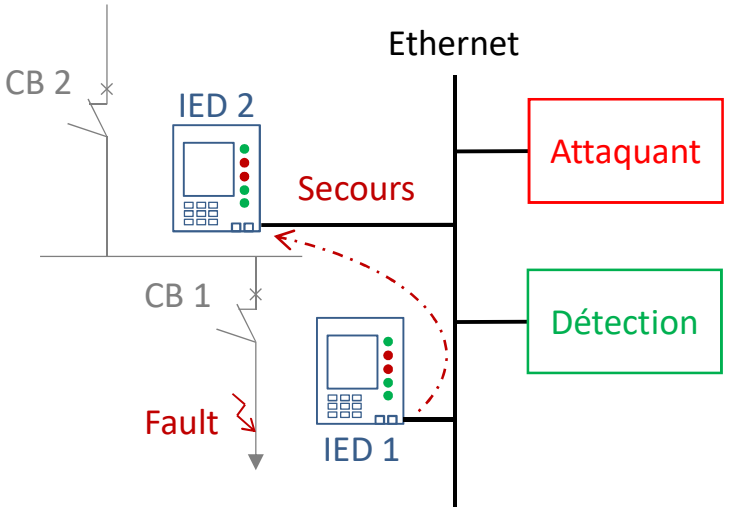
GoCBRef	*GOOSE Control Block Reference*
TimeAllowedToLive	
DatSet	*Data Set*
GoID	*GOOSE Identifier*
T	*Time*
StNum	*State Number*
SqNum	*Sequence Number*
Test	
ConfRev	*Configuration Revision*
NdsCom	*Needs Commissioning*
NumDatSetEntries	*Number of Data Set Entries*
AllData	
Security	

Structure du PDU GOOSE

Implémentation

- Validation de l'approche en C avec les sources de Tcpdump
  - Vérification de l'ensemble des propriétés intra et inter trames GOOSE
- Dissémination avec Bro
  - Intégration d'un analyseur syntaxique de GOOSE
  - Script de vérification du mécanisme de transfert GOOSE
  - Temps d'analyse d'une trame (161 octets) = ~ 2.3ms

  VS. 0.3ms, 32 règles couvrant MMS, SV et GOOSE [YAN2017]



Architecture de test

https://github.com/bro/bro/pull/76

[YAN2017] Yang et al., Multidimensional Intrusion Detection System for IEC 61850 based SCADA Networks, 2017

Contributions

- Etudes des vulnérabilités de la communication IEC 61850
  - Analyse de risques cyber sécurité IEC 61850
  - Test d'injection de fautes sur le protocole GOOSE
  - Preuve de faisabilité d'injection de fausses données GOOSE
- Modélisation IDS pour l'IEC 61850
  - Extension au modèle d'information IEC 61850 dédiées à la détection d'intrusion
- Développement et implémentation de notre approche de détection comportementale déterministe
  - IDS réseau, basé anomalies, déterministe pour GOOSE
  - Spécification de règles à partir des fichiers de configuration
  - Deux implémentations (Tcpdump, Bro)
- Proposition d'architecture du système de contrôle résiliente aux attaques GOOSE

Overview

1. Problematics and vocabulary
2. Dependability, safety, functional safety, security (RAMSS)
3. Risk analysis
4. Some considerations on networks, Safety networks
5. Dependability of networks and networked control systems
6. Cyber-security
7. Applications to cyber-physical systems
   - 7.1 Considerations on Intelligent Control systems
   - 7.2 Intrusion detection on GOOSE messages for smart grids
   - 7.3 Processus-oriented detection attacks
   - 7.4 Risk analysis of a drone
8. Discussions & Conclusions

Détection d'intrusions dans les systèmes de contrôle industriels

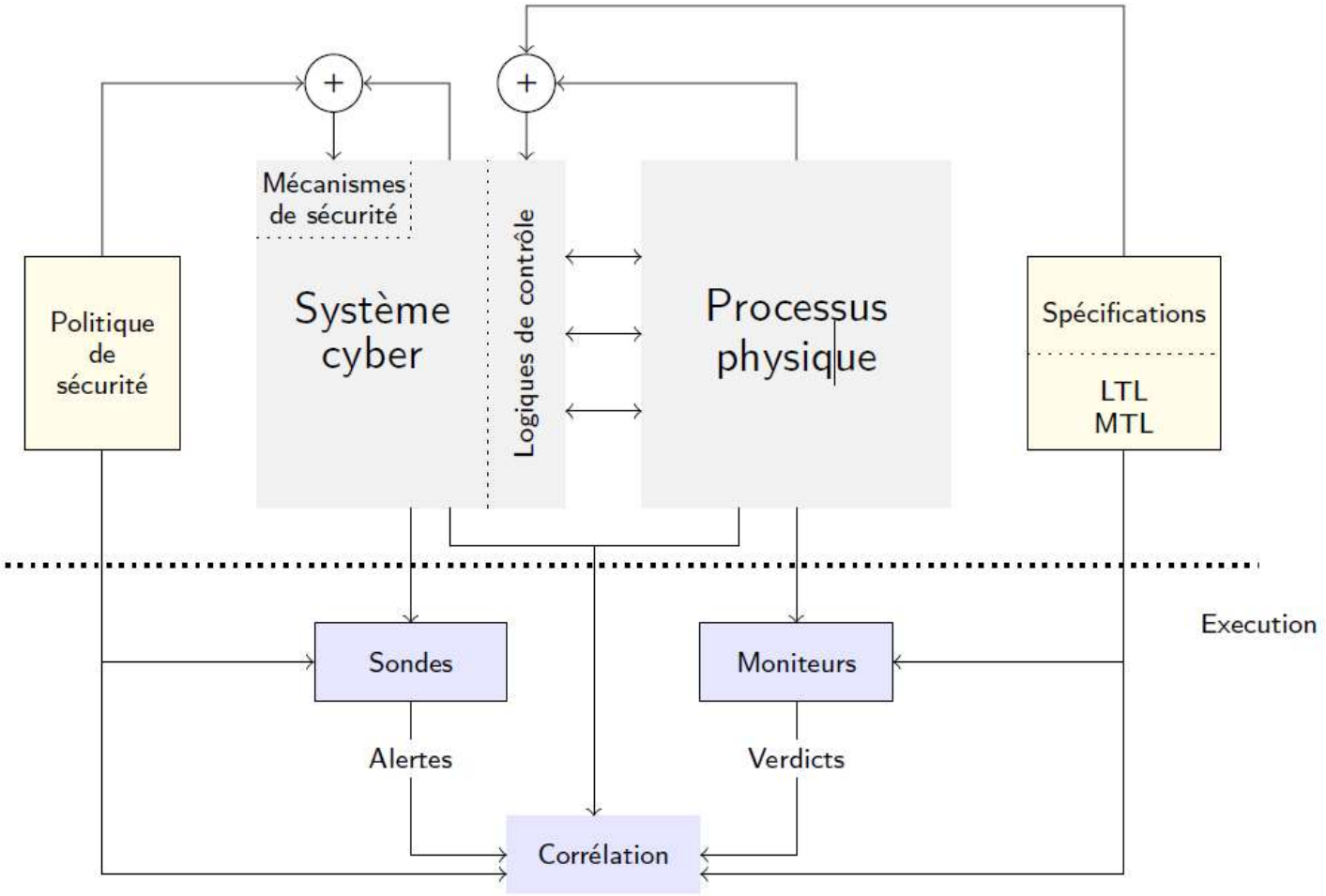
Motivation

- Les systèmes industriels sont de plus en plus connectés aux systèmes d'information traditionnels
- Utilisation de solutions IT classiques (architecture, OS, protocoles réseaux)
- Surface d'attaque accrue

Détection d'intrusions

- Nécessité de tenir compte des spécificité des systèmes industriels : présence d'un processus physique
- Mieux comprendre les faux positifs

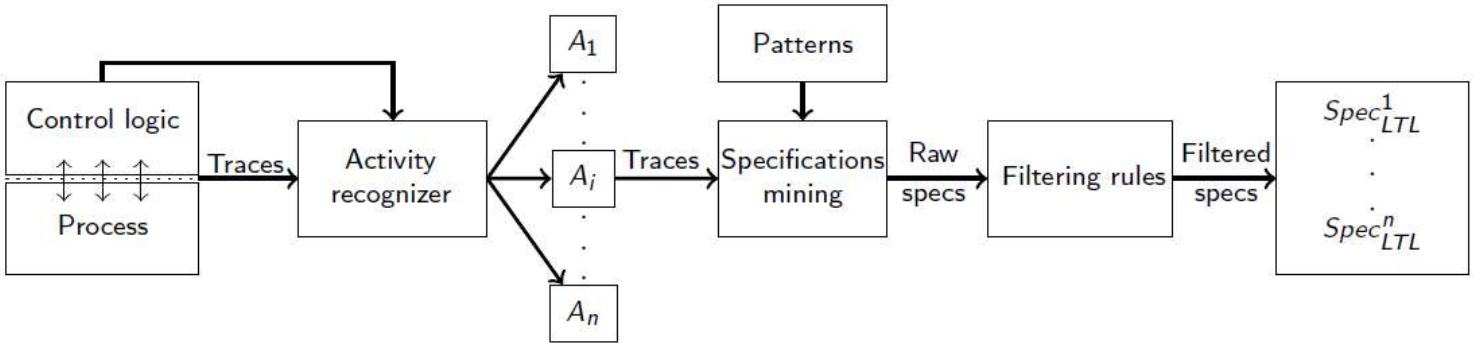
Global approach: correlations between IDS probes (Cyber system) and safety monitors (Physical process)



Détection d'attaques orientée processus : Inférences de spécification

Motifs de spécifications

- L'écriture manuelle de spécifications est fastidieuse
  - → Inférer les spécifications à partir de traces d'exécutions
  - → Se baser sur des **motifs de spécifications**
- Les motifs de spécifications représentent des propriétés souvent utilisées pour la vérification formelle [Dwyer, 1999] :
  - **Nature :** absence, universalité, ordre
  - **Portées :** avant, après, ou entre des états/événements



Inférence de spécifications : fouille par portées

- **Observation :** les traces d'exécution générées par les logiques de contrôle sont hautement structurées
- **Idée :** diviser l'espace des propriétés instanciables selon les portées afin d'éviter la vérification de propriétés inutiles
- Une propriété inutile est une propriété qui n'est pas **falsifiable**

Exemple

- Pour la trace : $\{vp1,m1\},\{p1,m1\},\{vp2,p1\},\{p1,p2\},\{end\},\{end\}\ldots$
- Une propriété instanciée possible est : $absence\_after(vp1^{\uparrow}, m1^{\uparrow})$
- Cette propriété n'est pas falsifiable car $vp1^{\uparrow}$ n'est jamais vraie sur la trace.
- Toutes les propriétés ayant pour portée $vp1^{\uparrow}$ ne sont pas falsifiables et peuvent être ignorées.

Inférence de spécifications : fouille par portées

Vérification de la falsifiabilité

- La falsifiabilité est déterminée à l'aide de ***moniteurs auxiliaires*** tournant en parallèle avec les moniteurs associés à la vérification d'une instance
- Si, pour une trace donnée, une propriété n'est jamais violée mais que le moniteur auxiliaire associé indique la non falsifiabilité de la propriété, celle-ci est ignorée et la portée associée est mise en liste noire
- Différentes politiques possibles sur plusieurs traces

Filtrage de spécifications

Règles de filtrage

- Introduction de règles de filtrage afin de réduire le nombre important de spécifications inférées
- Règles de la forme :

$$\frac{\psi_1, \quad \psi_2, \quad \forall \sigma \in \Sigma^\omega, \sigma \models \psi_2 \Rightarrow \psi_1}{\mathit{filter}(\psi_2)}$$

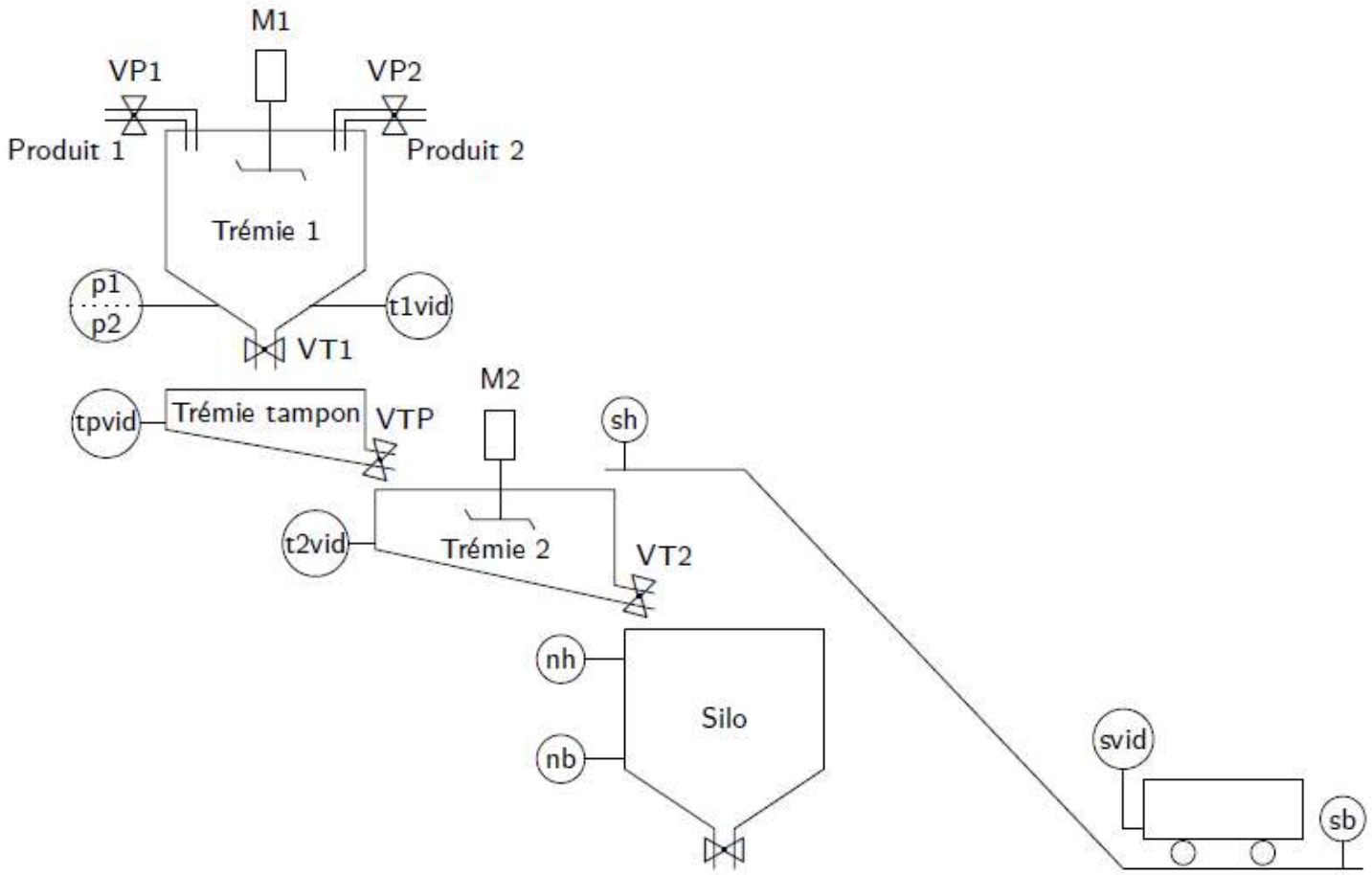
- Exemple :

$$\frac{\mathit{universality\_after}(X, Y), \quad \mathit{absence\_after}(X, Y^{\uparrow})}{\mathit{filter}(\mathit{universality\_after}(X, Y))}$$

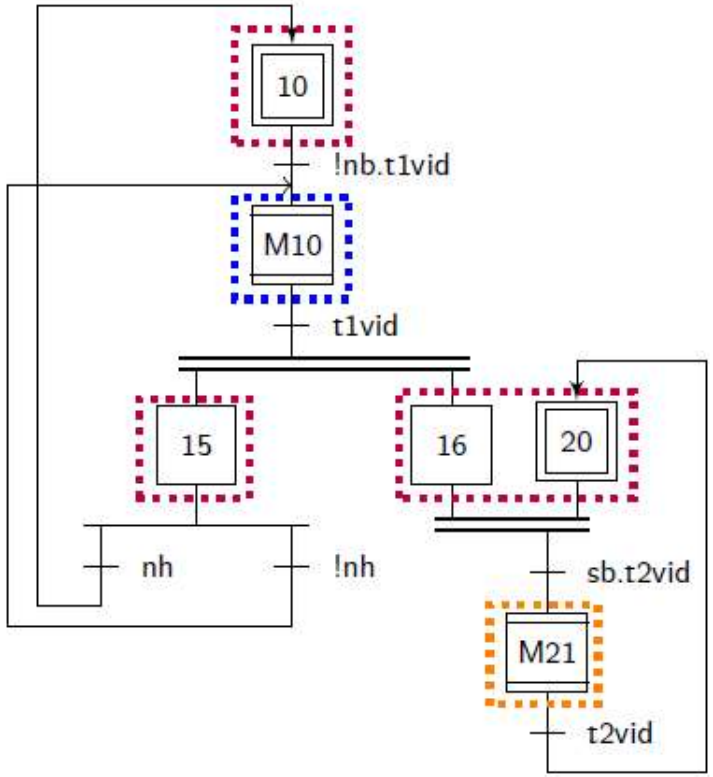
- Ces règles représentent des relations logiques entre les spécifications inférées

Evaluation

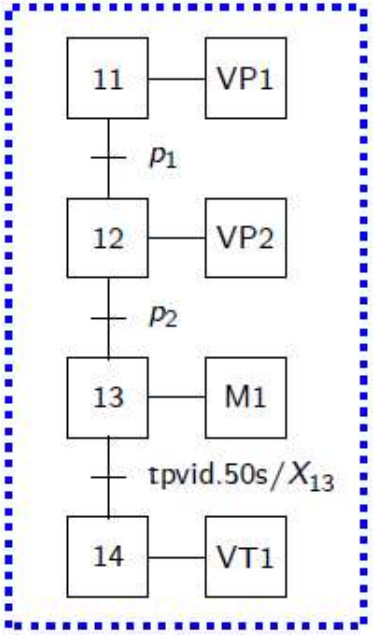
[Foulard, 1997]



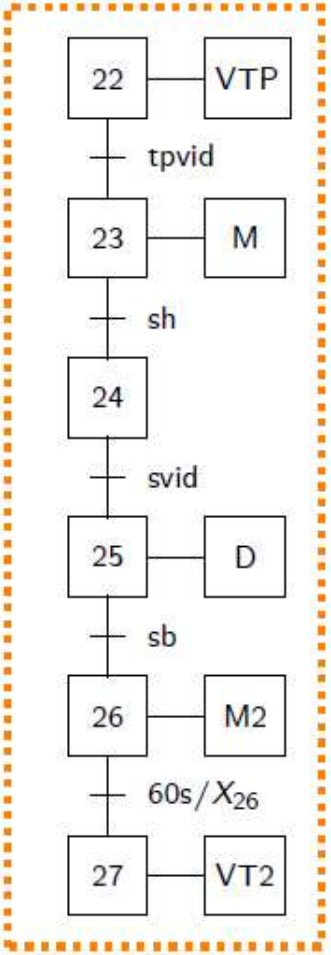
Evaluation



Macro étape M10



Macro étape M21



Evaluation

Comportement permis

- **Activité 1**
  - Ouvrir/fermer la vanne V1 tant que le poids P1 n'est pas atteint. Aucune manipulation permise après.
  - Ouvrir/fermer la vanne VT1 après l'arrêt du moteur M1. Aucune manipulation permise avant.
- **Activité 2**
  - Ouvrir/fermer la vanne VT2 après l'arrêt du moteur M2. Aucune manipulation permise avant.

Quelques attaques effectuées

- Ouverture de VP2 après le démarrage de M1
- Ouverture de VT1 avant l'arrêt de M1
- Enclenchement de M1 avant P2
- Ouverture de VT2 avant l'arrêt de M2

Evaluation

Inférence de spécifications

Activité	Texada 1	Texada 2	Fouille par portées
Activité 1 (242 entrées sur 11 exécutions)	11m15	1m38	45s
Activité 2 (215 entrées sur 8 exécutions)	10m6	1m14	55s

Plateforme : Intel Dual Core i5 2.4 GHz , 4Go de RAM
Texada : [Lemieux, 2015]

Détection d'attaques

Alert	Type	Properties violated	Interpretation
Alert 1 (act. 1)	TP	$absence\_between(m1^{\uparrow}, p1^{\downarrow}, vp2^{\uparrow})$ $absence\_between(m1^{\uparrow}, p2^{\downarrow}, vp2^{\uparrow})$	*vp2* opened after starting *m1* (attack)
Alert 3 (act. 1)	FP	$absence\_global(vt1^{\downarrow})$ $absence\_after\_until(m1^{\downarrow}, p1^{\downarrow}, vt1^{\downarrow})$	*vt1* closed after *m1* is stopped (legitimate action)
Alert 5 (act. 2)	TP	$absence\_before(m2^{\downarrow}, vt2^{\uparrow})$	*vt2* opened before the end of the mixing task (attack)

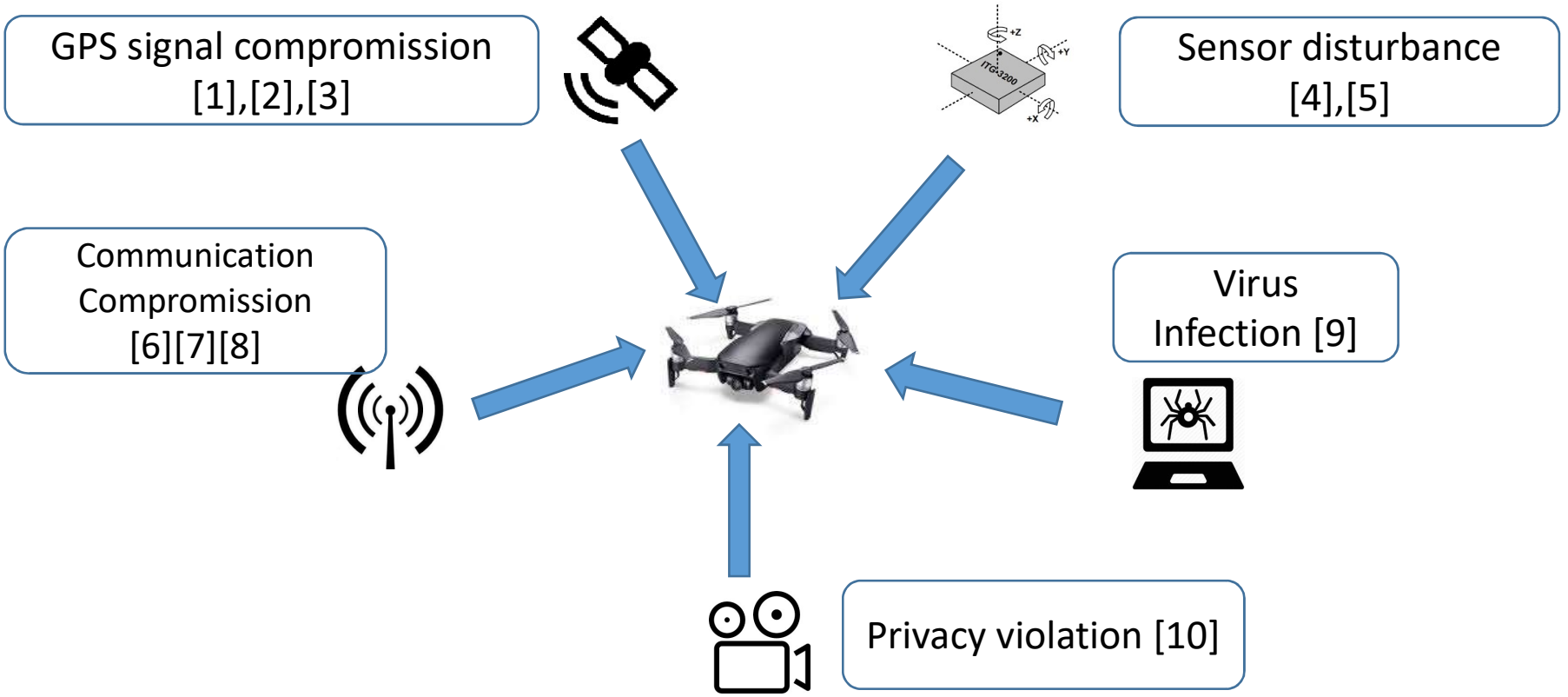
* TP : True Positive, FP : False Positive

Overview

1. Problematics and vocabulary
2. Dependability, safety, functional safety, security (RAMSS)
3. Risk analysis
4. Some considerations on networks, Safety networks
5. Dependability of networks and networked control systems
6. Cyber-security
7. Applications to cyber-physical systems
   - 7.1 Considerations on Intelligent Control systems
   - 7.2 Intrusion detection on GOOSE messages for smart grids
   - 7.3 Processus-oriented detection attacks
   - 7.4 Risk analysis of a drone
8. Discussions & Conclusions

Cyber-security of flying drones

Vulnerability of the drone:



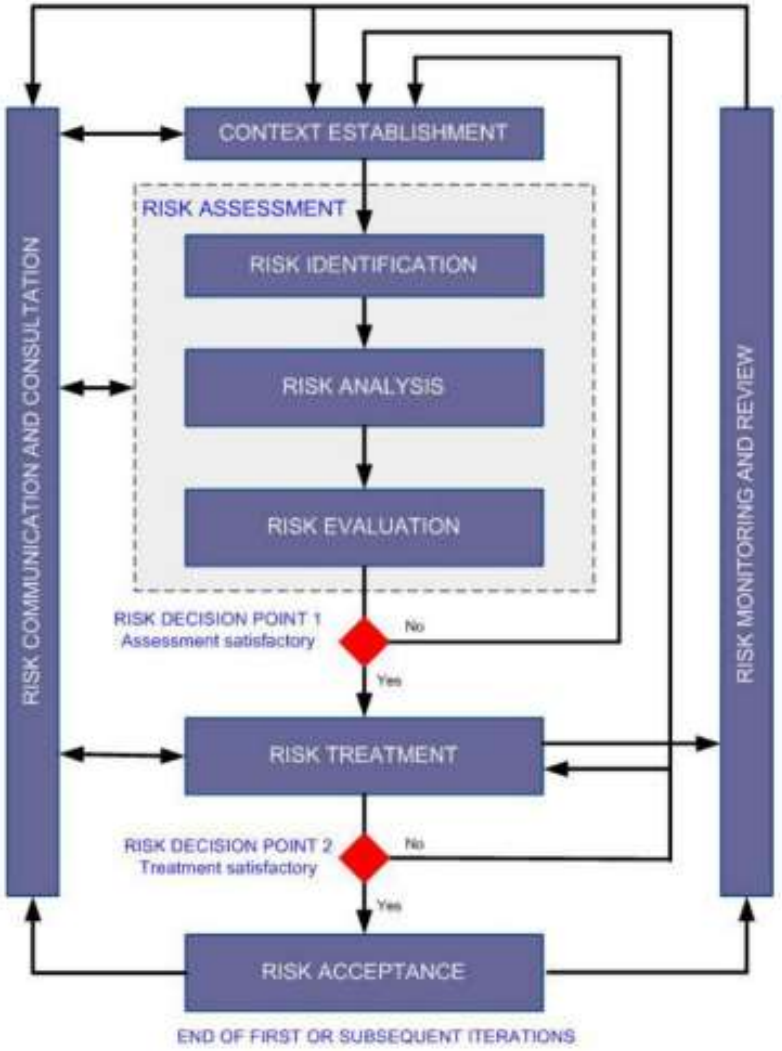
Need of a methodology to get a cartography of the drone security in a systematic way and to ensure completude

Methodologies in the industrial domain

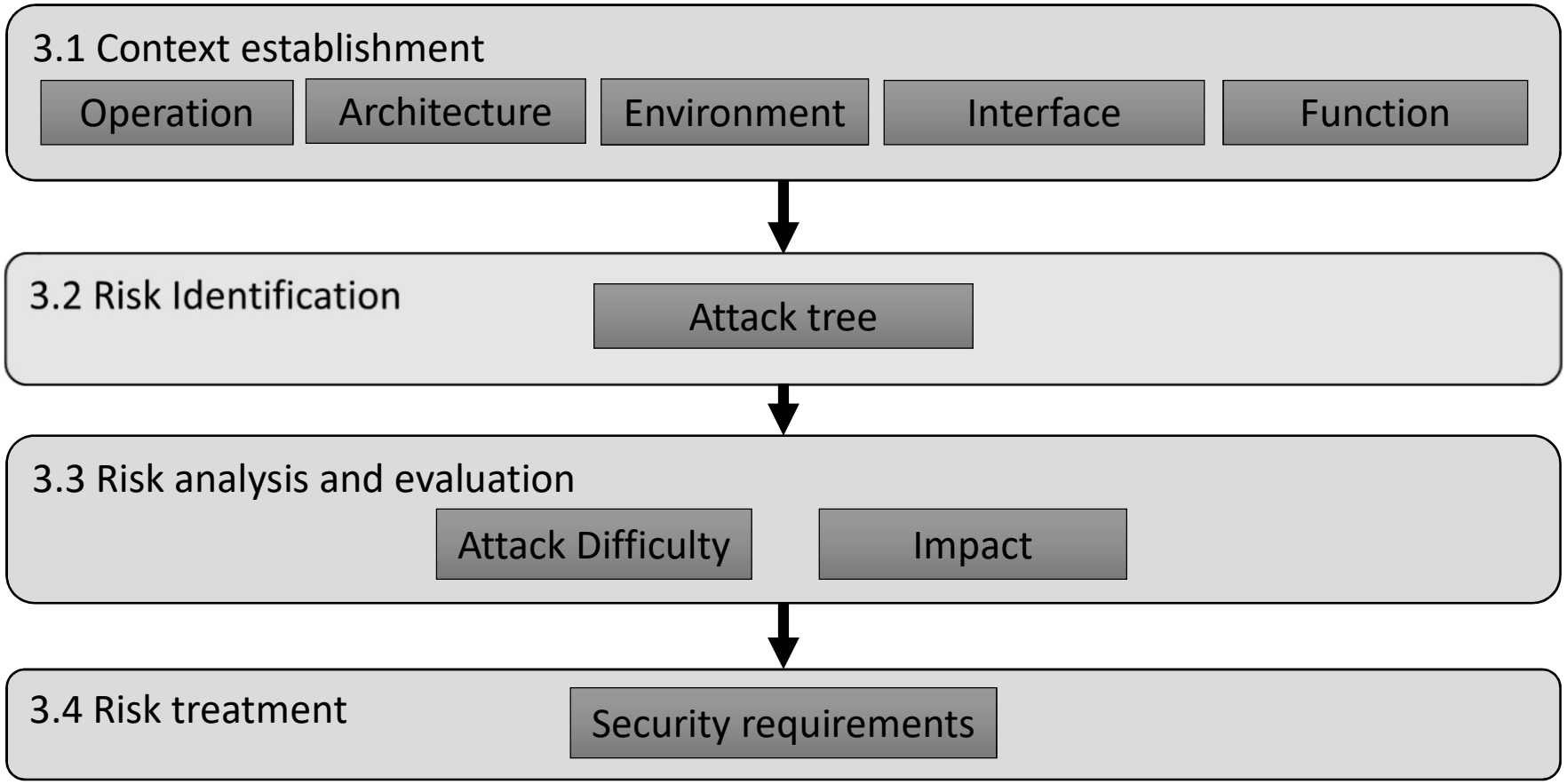
- **ISO27005 Standard**: Information security risk management [11].
  Propose a work-flow[12]

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

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



Proposed methodology



Example of Steps of the methodology

Operation Description – based on SORA, Risk Assessment for unmanned airborne Mobility **[15]**

- How, when, where and under which constraints the system runs
- Automation level of the system and operators involvement
- Procedure for operation, maintenance
- Procedure for safety

Steps of the methodology

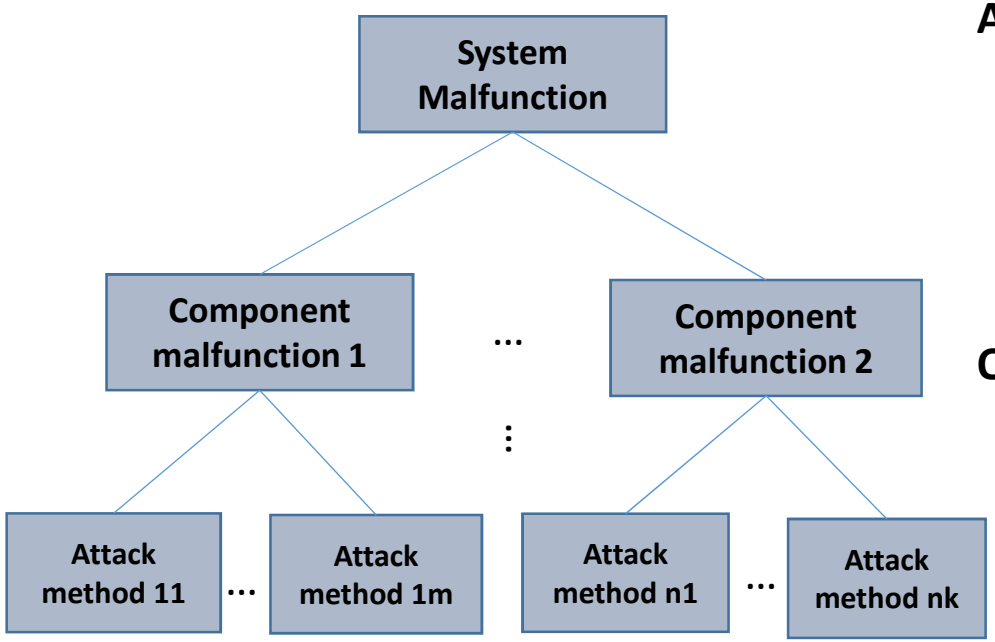
Interface [based on DO 202 standard]

- List of *entry points (inputs)* of environment elements interacting with the system
- Details of data flows crossing each interface
- Details the elements of the security environment for each interface

Steps of the methodology

3.2 Risk Identification

Attack tree



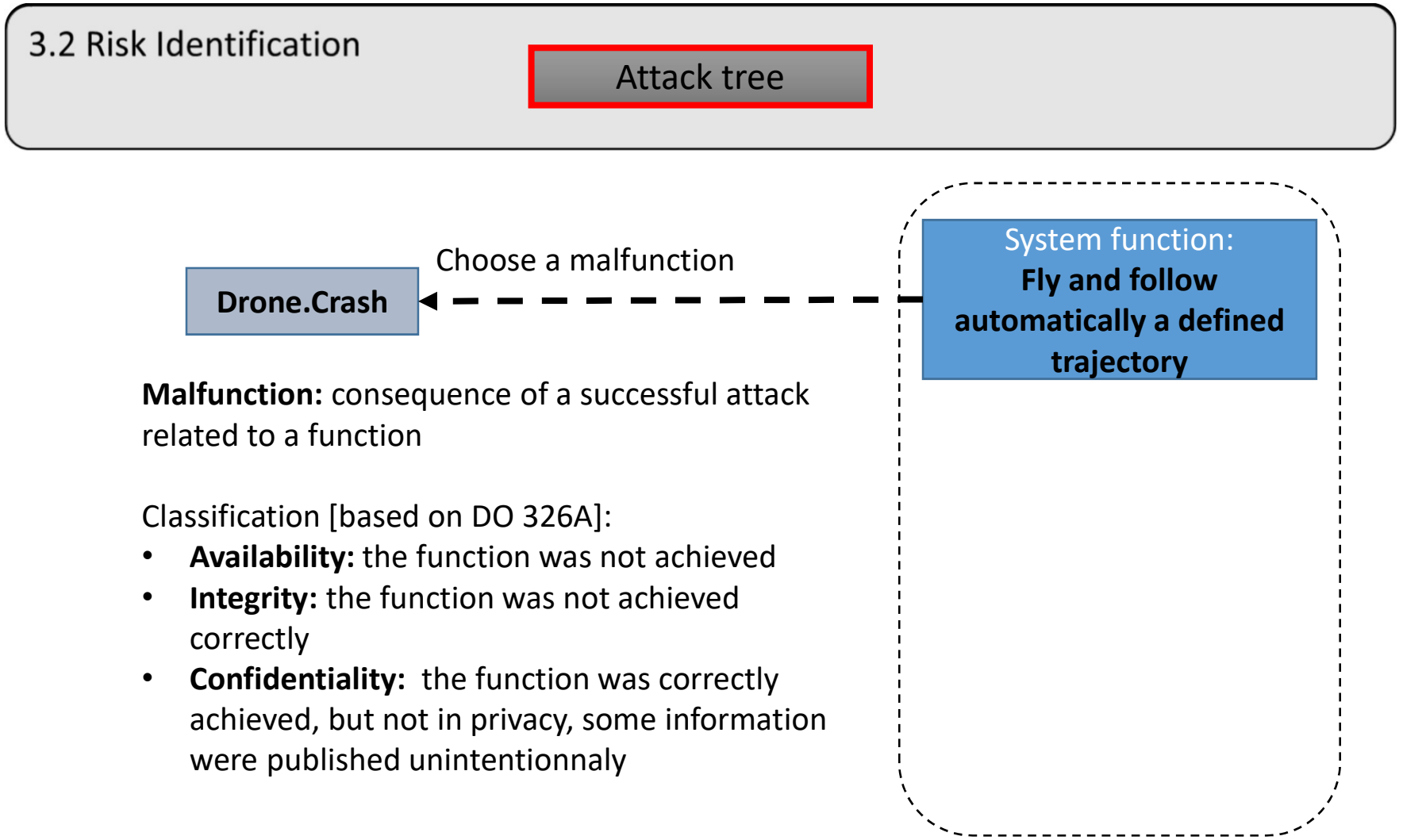
Attack tree:

- Presented by B. Schneier (1999)[17]
- Deductuve reasoning
- Used in various applications : cars [14], aeronautics [19], Smartgrids [18], Drones [20]

Objectives

- List of the risks
- Understand the risks
- Facilitation of the steps of definition of security exigences

Steps of the methodology

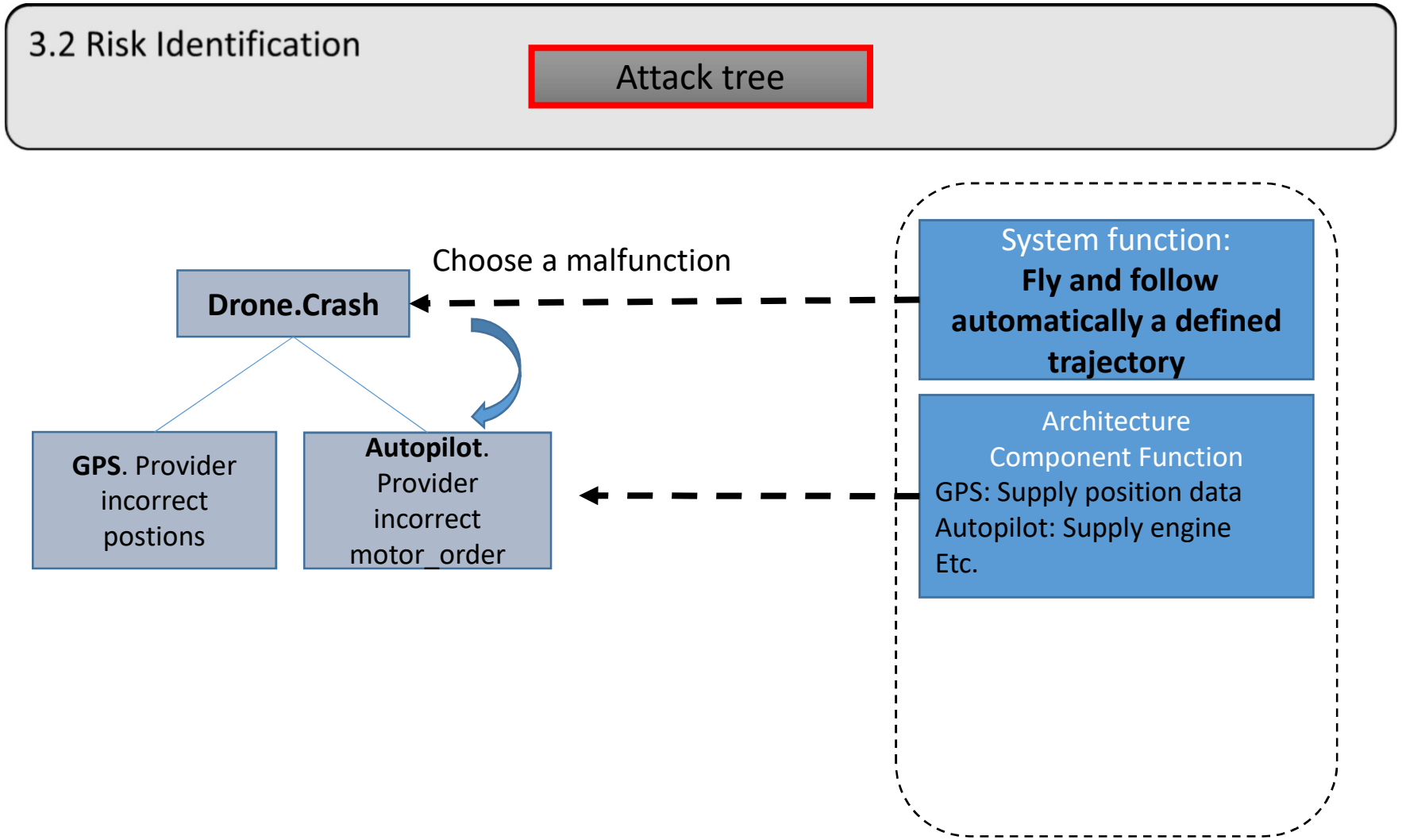


Malfunction: consequence of a successful attack related to a function

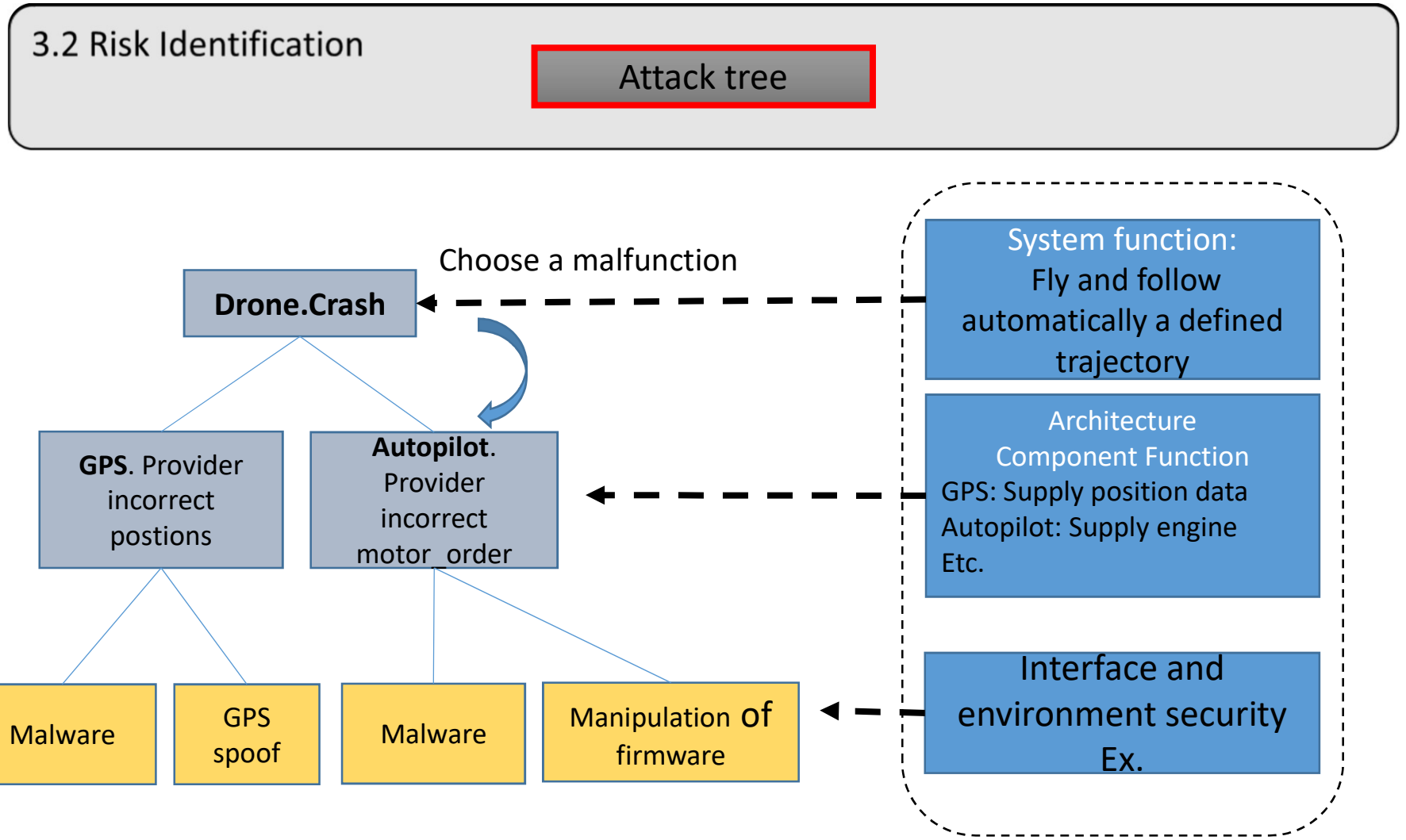
Classification [based on DO 326A]:

- **Availability:** the function was not achieved
- **Integrity:** the function was not achieved correctly
- **Confidentiality:** the function was correctly achieved, but not in privacy, some information were published unintentionnaly

Steps of the methodology



Steps of the methodology



Steps of the methodogy

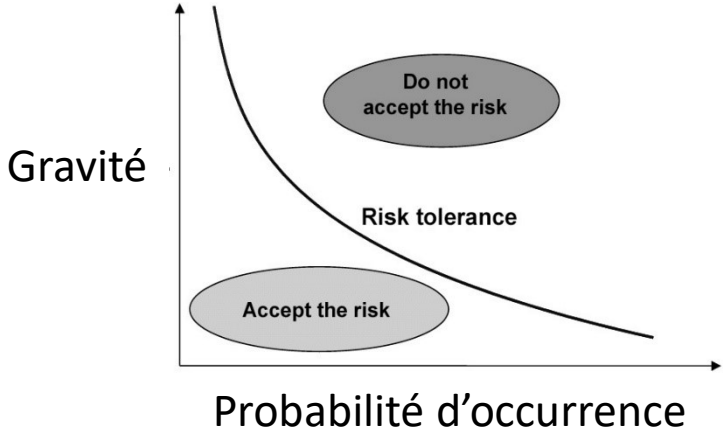
3.3 Risk analysis and evaluation

Attack Difficulty | Impact

Analyse et évaluation

- Décider quels risques doivent être traités avec quelles propriétés
- Analogie avec la sûreté de fonctionnement
- Donner la décision basée sur deux éléments: probabilité de risque et gravité de l'impact
- Gravité de l'impact : retour d'expérience

→Problème : pas de retour expérience pour l'analyse probabiliste



La question n'est pas seulement la probabilité d'être victime d'une attaque.
La question est que l'on veut se protéger d'une attaque considérée comme suffisamment probable, pour laquelle nous nous intéresserons à la difficulté d'attaque

Overview

1. Problematics and vocabulary
2. Dependability, safety, functional safety, security (RAMSS)
3. Risk analysis
4. Some considerations on networks, Safety networks
5. Dependability of networks and networked control systems
6. Cyber-security
7. Applications to cyber-physical systems
8. Discussions & Conclusions

Approaches: Modelling and Evaluation

- Complexity
- Methods and tools, graph-type
  * Automata
  * Queues
  * Petri Nets (MocaRP, DesignCPN,…) and extensions (colored, stochastic, timed, aging tokens…)
    Study of marking or occurrence graphs
    Detection of catastrophic states
    Study of scenarios leading to these states
  * Stochastic Activity Networks (Möbius)
  * Network simulators (OpNet, Network Simulator NS3)
- Probabilist approaches
  * Markov Chains, graphs
  * Distributed Dynamic Bayesian Networks

Approaches: Modelling and Evaluation

True-Time

- Co-design approaches
- Hybrid systems simulation (soft co-simulation)
- BUT, Simplified model of the network

Monte-Carlo Simulation

Co-simulation

- Soft co-simulation, SITL (Software in the Loop)
  (interaction between software, ex: OpNet & Matlab)
- Hard co-simulation, HITL (Hardware in the Loop)
  (interaction with hardware devices)

Conclusion

- Dependability and safety (SIL level)
- Dependability of dynamic systems
- Components (hardware and software)
- Network
  - Independent communication links
  - Actual network
- Physical Architecture (topology)
- Functional architecture (Common Cause Failures)
- Intelligent-based architecture
  - Complexity
  - Integration of diagnosis and/or security devices
- Cyber-security issues for critical applications

Conclusion

Evaluation of the dependability of a networked control system
- Multi time-scale and hybrid
- Transient « failures »

State of the system, dynamic aspects

Critical information

Integration of approaches
- SITL
- HITL

No magic formula

Give priority to formal approaches, whenever possible

Still some scientific deadlocks with societal implications…

ANSSI

Conclusions on Cyber-security of CPS

- New issues
- Integration of the IT and ICS worlds (convergence)
- Double culture (computer science/engineering and automation)
- Behaviour of the system
- Security of the Communication/Information system => Safety of the networked control system
- Implementation of cryptography
- In-depth security

References

- J. Arlat – Composants logiciels et sûreté de fonctionnement, intégration de COTS – Hermes, 2000.
- JF Aubry, N. Brinzei – Systems Dependability Assessment – Wiley, 2015
- M. A. Azgomi & A. Movaghar – Definition and analysis of cloured stochastic activity networks – Technical report, Dept. Of Computer Engineering, Sharif University of Technology, Tehran, Iran, 2004.
- P. Barger – Evaluation et validation de la fiabilité et de la disponibilité des systèmes d'automatisation à intelligence distribuée, en phase dynamique – thèse de l'Université Henri Poincaré Nancy 1, 15 décembre 2003.
- M. Bayart – *Instrumentation intelligents, systèmes automatisés de production à intelligence distribuée* – Habilitation à Diriger des Recherches, USTL, Lille, 21 décembre 1994.
- A. Carneas & al. – Secure control: towards survivable cyber-physical systems – 28th International Conference on Distributed Computing Systems Workhop – 2008.
- A. Cervin, D. Henriksson, B. Lincoln, J. Eker, K.E. Årzén – How does control timing affect performance? – IEEE Control Systems Magazine, JUne 2003, Vol. 23, N.3
- Groupe CIAME – Réseaux de terrain, description et critères de choix – Hermes, Paris, 1999.B. Conrard – Contribution à l'évaluation quantitative de la sûreté de fonctionnement des systèmes d'automatisation en phase de conception – thèse de l'Université Henri Poincaré Nancy 1, 24 septembre 1999.
- Blaise Conrard, Jean-Marc Thiriet, Michel Robert – Problems of precision for control loops implanted on Distributed Automation System – CESA'98 (Computational Engineering in Systems Applications)/IMACS/IEEE, Hammamet/Nabeul (Tunisie), avril 1998, pp. 180-185, vol. 1.
- M. Conti, S. Giordano – Multihop ad hoc networking: the theory – IEEE Communications, Vol 45, n°4, p.78, avril 2007.
- R. David, H. Alla – Discrete, continuous, and hybrid Petri Nets – Springer, 2010 .
- M. Diaz – Les réseaux de Petri, modèles fondamentaux – Hermes, Paris, 2001.
- JP Georges – Systèmes contrôlés en réseau : évaluation de performances d'architectures ethernet commutées – thèse UHP-CRAN, Nancy, 2005.
- F. Hohlbaum, M. Braendle, F. Alvarez – Practical considerations for implementing IEC 62351 – ABB, 2009
- W. Hu, D. Willkomm, G. Vlantis, M. Gerla, A. Wolisz – Dynamic frequency hopping communities for efficient IEEE 802.22 operation – IEEE communications, vol 45, n° 5, mai 2007, p. 80
- K. Jensen – Coloured Petri Nets. Basic Concepts, Analysis Methods and Practical Use – Monographs in Theoretical Computer Science, Springer-Verlag, 2nd corrected printing 1997.
- Guy Juanole – Réseaux de communication et automatique – *Journées "Automatique et Communication"*, 13-14 mars 2001.
- G. Juanole, I. Blum – Quality of service of real time networks and performances of distributed applications – LAAS report 99166, avril 1999.

References

- F. Jumel, J.M. Thiriet, J.F. Aubry, O. Malasse - "Towards an information-based approach for the dependability evaluation of distributed control systems" - 20th IEEE Instrumentation and Measurement Technology Conference (IEEE/IMTC2003), Vail (Colorado, United States), 20-22nd May 2003, pp. 270-275.
- P. Kleinschmidt, F. Schmidt - How many sensors does a car need ? - Eurosensors V, Roma, 2 October 1991, pp.1-13.
- P.R. Kumar – New technological vistas for systels and control – IEEE Control Magazine, February 2001
- M.J. Lee, J. Zhang & al. – A new taxonomy of routing algorithms for wireless mobile ad hoc networks: the component approach – IEEE p. Communications, Vol. 44, N° 11, novembre 2006, 116
- K. Lu, Y. Qian – A secure and service-oriented network control framework for WIMAX network – IEEE Communications, Vol 45, N° 5, p. 124, mai 2007
- Stéphane Mocanu – Cours de réseaux, ENSIEG, 2005
- R. M. Murray, K.J. Åström, S. P. Boyd, R. W. Brockett, G. Stein – Future directions in control in an information-rich world, IEEE Control Magazine, April 2003, Vol. 23, n. 2
- Natale, O.R.; Sename, O.; Canudas-de-Wit, C.; - Inverted pendulum stabilization through the Ethernet network, performance analysis - American Control Conference, 2004. Proceedings of the 2004 - Volume 6, 30 June-2 July 2004 Page(s):4909 - 4914 vol.6
- Q. Ni, A. Vinel, Y. Xiao, A. Turlikov, T. Jiang – Investigation of bandwidth request mechanisms under point-to-multipoint mode of Wimax networks – IEEE Communications, Vol 45, N° 5, p. 132, mai 2007
- S.I. Niculescu – Systèmes à retard, aspects qualitatifs sur la stabilité et la stabilisation – Diderot éditeur, Paris, 1997.
- D. Niyato, E. Hossain – Integration of WImax and Wifi: optimal pricing for nadwidth sharing – IEEE Communications, Vol 45, N° 5, p. 140, mai 2007.
- L. Ondrej, M. Mlanic, T. Vollmer – Improving cyber-security of amrt grids systems via anomay detection and linguistic domain knowledge – 2012.
- L. Pelusi, A. Passarella, M. Conti – Opportunistic networking: data forwarding in disconnected mobile ad hoc network, IEEE Communications, Vol. 44, N° 11, novembre 2006.
- S.A. Reinemo, T. Skeie, T. Sodring, O. Lysne, O. Torudbakken – An overview of QoS capabilities in InfiniBand, Advanced Switching Interconnect, and Ethernet – IEEECommunications, Vol 44, n° 7, juillet 2006, page 32
- M. Robert, M. Marchandiaux, M. Porte – *Capteurs Intelligents et Méthodologie d'Evaluation* – Hermès, 1993.
- D. J. Smith & K. G. Simpson – Functional safety (second edition) a straightforward guide to applying IEC 61508 and related standards – Elsevier, 2004.
- Y. Q. Song – performance analysis and improvement of zig-bee routing protocol – Fet, 2007, Toulouse.
- Stouffer, K. A., Falco, J. A., and Scarfone, K. A. (2011). Sp 800-82. guide to industrial control systems (ics) security: Supervisory control and data acquisition (scada) systems, distributed control systems (dcs), and other control system configurations such as programmable logic controllers (plc). Technical report, Gaithersburg, MD, United States.

References

- J.M. Thiriet - Habilitation à Diriger des Recherches de l'Université Henri Poincaré Nancy 1 en Automatique : "Sûreté de fonctionnement de Systèmes d'Automatisation à Intelligence Distribuée" - CRAN-UHP, Nancy, 16 décembre 2004.
- Törngren M. – Fundamentals of implementing real-time control applications in distributed computer systems, Real-Time Systems Journal, Volume 14, Number 3, May 1998.
- V. Volovoi – Modeling multiphased missions using stochastic Petri nets with aging tokens – RAMS'04, Annual Reliability and Maintainability Symposium, Los Angeles, janvier 2004.
- G.C. Walsh, H. Ye – Scheduling of networked control systems – IEEE control Magazine, février 2001.
- Witrant, E.; Canudas-De-Wit, C.; Georges, D.; Alamir, M.; - Remote stabilization via time-varying communication network delays: application to TCP networks - Control Applications, 2004. Proceedings of the 2004 IEEE International Conference on - Volume 1, 2-4 Sept. 2004 Page(s):474 - 479 Vol.1
- J. Zaytoon – Systèmes dynamiques hybrides – traité ic2 série systèmes automatisés, Hermes, 2002.
- W. Zhang, M.S. Branicky, S.M. Philips – Stability of networked control systems – IEEE control Magazine, février 2001.
- Zhou, C., Huang, S., Xiong, N., Yang, S.-h., Li, H., Qin, Y., and Li, X. (2015). Design and Analysis of Multimodel-Based Anomaly Intrusion Detection Systems in Industrial Process Automation. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 45(10):1345–1360
- 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-Hélié – *Sécurité informatique et réseaux* – Dunod, 2005.
- C. Davis, M. Schiller, K. Wheeler - *IT Auditing: using control to protect assets* – 2007, Mc Graw Hill
- D. Vergnaud – *Exercices et problèmes de cryptographie* – 2ème édition, 2015, Dunod

References

[1] Andrew J. Kerns, Daniel P. Shepard, Jahshan A. Bhatti, and Todd E. Humphreys. 2014. Unmanned Aircraft Capture and Control Via GPS Spoofing. J. Field Robot. 31, 4 (July 2014), 617-636
[2] L. He, W. Li, C. Guo and R. Niu, "Civilian Unmanned Aerial Vehicle Vulnerability to GPS Spoofing Attacks," *2014 Seventh International Symposium on Computational Intelligence and Design*, Hangzhou, 2014, pp. 212-215
[3] Z. Feng *et al*., "Efficient drone hijacking detection using onboard motion sensors," *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017*, Lausanne, 2017, pp. 1414-1419.
[4] Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park, Juhwan Noh, Kibum Choi, Jungwoo Choi, and Yongdae Kim. 2015. Rocking drones with intentional sound noise on gyroscopic sensors. In Proceedings of the 24th USENIX Conference on Security Symposium (SEC'15)
[5] D. Davidson, H. Wu, R. Jellinek, V. Singh, and T. Ristenpart, "Controlling uavs with sensor input spoofing attacks," in 10th USENIX Workshop on Offensive Technologies (WOOT 16), (Austin, TX), USENIX Association,2016.
[6] E. Vattapparamban, İ. Güvenç, A. İ. Yurekli, K. Akkaya và S. Uluağaç, "Drones for smart cities: Issues in cybersecurity, privacy, and public safety," trong *Wireless Communications and Mobile Computing Conference (IWCMC), 2016 International*, Paphos, Cyprus, 2016
[7] Guillaume Fournier, Paul Audren de Kerdrel, Pascal Cotret, Valérie Viet Triem Tong. DroneJack: Kiss your drones goodbye!. SSTIC 2017 - Symposium sur la sécurité des technologies de l'information et des communications, Jun 2017, Rennes, France. pp.1-8. 〈hal-01635125〉
[8] M. Heiges, R. Bever and K. Carnahan, "How to Safely Flight Test a UAV Subject to Cyber-Attacks," Systems Engineering Research Center, 2014.
[10] A. Y. Javaid, W. Sun, V. K. Devabhaktuni và M. Alam, "Cyber security threat analysis and modeling of an unmanned aerial vehicle system," trong Homeland Security (HST), 2012 IEEE Conference on Technologies for, Waltham, MA, USA, 2013
[11] "ISO/IEC 27005:2011 Information technology - Security technique - information security[managment," ISO/IEC, 2011.
[12] "MEHARI-Overview," Clusif, Paris, 2010.
[13] AIRWORTHINESS SECURITY PROCESS SPECIFICATION ED-202 / DO-326. [Performance]. EUROCARE/RTCA, 2014.
[14] EVITA, "D2.3 Security requirements for automotive on-board networks based on dark-side scenarios," EVITA, 2009
[15] JARUS guidelines on Specific Operations Risk Assessment (SORA), 2017
[16] Livre "System engineering fundamental", Defense Acquisition University, Virginal, 2011
[17]B. Schneier, "Modeling security threats," Dr. Dobb's Journal, 12 1999.
[18] Eric J. Byres, Matthew Franz , Darrin Miller, "The use of attack trees in assessing vulnerabilities in SCADA systems," in IEEE Conf. International Infrastructure Survivability Workshop, 2004.
[19] S. Gil-Casals, Thèse "Risk assessment and Intrusion detection for airbone networks," Hal, Toulouse, 2014.
[20] Dr. Barry Horowitz et al, "System Aware Cyber Security for an Autonomous Surveillance System On Board an Unmanned Arial Vehicle"
[21] Silvia Gil-Casals. Risk Assesment and Intrusion Detection for Airborne Networks. Networking and Internet Architecture [cs.NI]. INSA
[22]T J. Xu, K. K. Venkatasubramanian and V. Sfyrla, "A methodology for systematic attack trees generation for interoperable medical devices," 2016 Annual IEEE Systems Conference (SysCon), Orlando, FL, 2016, oulouse, 2014. English

References

- "Stuxnet", in L'Informaticien, Nov. 2010.
- L. Bloch, C. Wolfhugel, A. Kokos, G. Billois, A. Soullié, A. Anzala-Yamakajo, T. Debize, Sécurité informatique, pour les DSI, RSSI et administrateurs, 5ème edition, Eyrolles, 2016.
- M. Cislo, Virus and industrial processes, WINS/CNMS Bachelor memoir, Univ. Grenoble Alpes, Grenoble, 2015.
- N Falliere, L. O. Murchu, and E. Chien. W32.stuxnet dossier. https://www.symantec.com/content/en/us/enterprise/media/security_response/ whitepapers/w32_stuxnet_dossier.pdf, 2011. [Online, acc. : March-2018].
- US-CERT. Crashoverride. https://www.us-cert.gov/ncas/alerts/TA17-163A, 2017. [Online, acc. : March-2018]
- Dragos. Crashoverride: Analysis of the threat to electric grid operations. lhttps://dragos.com/blog/crashoverride/, 2017. [Online, acc. : July-2018]
- O. Koucham, Détection d'intrusions pour les systèmes de contrôle industriels, thèse de Doctorat, Univ. Grenoble Alpes, 2018.
- A. Mkhida, Contribution à l'évaluation de la sûreté de fonctionnement des Systèmes Instrumentés de Sécurité intégrant de l'Intelligence, thèse de Doctorat, Univ. de Lorraine, 2008.
- J. C. Laprie, Sûreté de fonctionnement et tolérance aux fautes : concepts de base, rapport LAAS n°88.287, paru dans les techniques de l'ingénieur, 1988.
- R. Ghostine, Influence des fautes transitoires sur la fiabilité d'un système commandé en réseau, thèse de Doctorat, Univ. de Lorraine, 2008.
- CEI 61508. Sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables relatifs à la sécurité. Commission Electrotechnique Internationale, Genève, Suisse, 2000.
- G. Moncelet. Application des réseaux de Petri à l'évaluation de la sûreté de fonctionnement des systèmes mécatroniques du monde automobile, Thèse de Doctorat, N°3076, Université Paul Sabatier, Toulouse, 9 octobre (1998).
- P.J. Portugal, and A. Carvalho. A Stochastic Petri Net Framework for Dependability Evaluation of Fieldbus Networks – A Controller Area Network (CAN) Example. International IEEE Conference in Mechatronics and Robotics, MECROB, 2004.
- Navet, N., Y. Song and F. Simonot. Worst-Case Deadline Probability in Real-Time Applications Distributed over Controller Area Network. In: Journal of systems Architecture. Vol (46), No. 1, p: 607-617, 2000.
- J. Galdun, JM Thiriet, J. Liguš, Study of different load dependencies among shared redundant systems, International Workshop on Real Time Software RTS'2008 within International Multiconference on Computer Science and Information Technology IMCSIT'2008, October 20–22, Wisla, Poland, pp. 609 – 615, ISSN 1896-7094, 2008.
- R. Ghostine, JM Thiriet JF Aubry, M. Robert, A Framework for the Reliability Evaluation of Networked Control Systems, 17th IFAC World Congress, July 6-11, pp. 6833-6838, 2008.
- P. Barger, JM Thiriet, M. Robert, Dependablity study in distributed control systems integrating smart devices, Low Cost 2004, Ottawa (Canada), pp. 79-84, 2004.
- J. Tixier, G. Dusserre, O. Salvi, D. Gaston, 'Review of 62 risk analysis methodologies of industrial plants', Journal of Loss Prevention in the process industries 15, pp. 291–303. 2002.
- C. Davis, M. Schiller, K. Wheeler, IT Auditing: using control to protect assets, Mc Graw Hill, 2007.
- E. Cole, R. Krutz, JW Conley, Network security bible, Wiley, 2005.
- D. Diallo, M. Feuillet, Détection d'intrusion dans les systèmes industriels : Suricata et le cas de Modbus, CAESAR 2014, website of ANSSI, [Online, acc. : October-2018].
- S. Cheung and K. Skinner. Using Model-based Intrusion Detection for SCADA Networks. In Proc. SCADA Security Scientific Symposium, pages 127–134, 2007.
- H. Lin, A. Slagell, C. Di Martino, et al. Adapting Bro into SCADA: building a specification-based intrusion detection system for the DNP3 protocol. In Proc. CSIIRW '13, pages 1–4, 2013.

References

- N. Goldenberg and A. Wool. Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems. International Journal of Critical Infrastructure Protection, 6(2):63–75, 2013.
- A. Kleinmann and A. Wool. Accurate modeling of the siemens s7 scada protocol for intrusion detection and digital forensics. Journal of Digital Forensics, Security and Law, 9(2), 2014.
- R. Barbosa, R. Sadre, and A. Pras. Flow whitelisting in SCADA networks. Int. Journal of Critical Infrastructure Protection, 6(3-4):150–158, December 2013.
- H. Hadeli, R. Schierholz, M. Braendle, and C. Tuduce. Leveraging determinism in industrial control systems for advanced anomaly detection and reliable security configuration. In IEEE Conference on Emerging Technologies and Factory Automation ETFA 2009, pages 1–8, 2009.
- S. Ponomarev and T. Atkison. Industrial Control System Network Intrusion Detection by Telemetry Analysis. IEEE Transactions on Dependable and Secure Computing, 5971(c):1–1, 2015.
- D. Yang, A. Usynin, and J. Hines. Anomaly-based intrusion detection for SCADA systems. In 5th Intl. Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies (NPIC&HMIT 05), pages 12–16, 2005.
- R. Ramos, R. Barbosa, R. Sadre, and A. Pras. Difficulties in Modeling SCADA Traffic : A Comparative Analysis. In Proceedings of the 13th international conference on Passive and Active Measurement (PAM '12), pages 126–135, 2012.
- O. Linda, T. Vollmer, and M. Manic. Neural Network based Intrusion Detection System for critical infrastructures. 2009 International Joint Conference on Neural Networks, pages 1827–1834, 2009.
- C. Zimmer, B. Bhat, et al. Time-based intrusion detection in cyber-physical systems. In Proc. First ACM/IEEE Int. Conf. on CPS, pages 109–118, 2010.
- J. Rrushi and K.-D. Kang. Detecting Anomalies in Process Control Networks. IFIP Advances in Information and Communication Technology, 311:151–165, 2009.
- J. Reeves, A. Ramaswamy, M. Locasto, S. Bratus, and S. Smith. Intrusion detection for resource-constrained embedded control systems in the power grid. International Journal of Critical Infrastructure Protection, 5(2):74–83, 2012.
- C. Bellettini and J. L. Rrushi. A product machine model for anomaly detection of interposition attacks on cyber-physical systems. IFIP International Federation for Information Processing, 278:285–299, 2008.
- D. Hadziosmanovic, R. Sommer, and E. Zambon. Through the Eye of the PLC: Towards Semantic Security Monitoring for Industrial Control Systems. In Proc. ACSAC 14, 2014.
- N. Erez and A. Wool. Control variable classification, modeling and anomaly detection in Modbus/TCP SCADA systems. International Journal of Critical Infrastructure Protection, 10:59–70, 2015.
- A. Carcano, I.N. Fovino, M. Masera, and A. Trombetta. Statebased network intrusion detection systems for SCADA protocols: A proof of concept. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6027 LNCS:138–150, 2010.
- I. N. Fovino, A. Carcano, T. D. L. Murel, A. Trombetta, and M. Masera. Modbus/ dnp3 state-based intrusion detection system. In Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on, pages 729–736, April 2010.
- R. Mitchell and I.-R. Chen. Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems. Dependable and Secure Computing, IEEE Transactions on, 12(1):16–30, Jan 2015.
- S. Pan, T. Morris, U. Adhikari, Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems. IEEE Transactions on Smart Grid, 6(6):3104–3113, 2015.
- R. Berthier, W.H. Sanders, and H. Khurana. Intrusion Detection for Advanced Metering Infrastructures: Requirements and Architectural Directions. Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, 2010.
- M. Parvania, G. Koutsandria, V. Muthukumary, S. Peisert, C. McParland, and A. Scaglione. Hybrid control network intrusion detection systems for automated power distribution systems. In Dependable Systems and Networks (DSN), 2014 44th Annual IEEE/IFIP International Conference on, pages 774–779, June 2014.

References

- C. Zhou, S. Huang, N. Xiong, et al. Design and analysis of multimodel-based anomaly intrusion detection systems in industrial process automation. IEEE Trans. Systems, Man, and Cybernetics: Systems, 45(10):1345–1360, 2015.
- J. Galdun, Dependability Analysis of Networked Control Systems with Consideration of Shared Redundant Subsystems, PhD Kosice-Grenoble, 2008.
- J. Ligušová, JM Thiriet, J. Liguš, P., Barger, Effect of Element Initialization in Synchronous Networked control System to Control Quality, Reliability and Maintainability Annual Symposium, RAMS, p. 135-140, January 2004.
- F-L. Lian, JR Moyne, DM Tilbury, Performance evaluation of control networks: Ethernet, ControlNet,and DeviceNet", IEEE Control Systems Magazine, Vol. 21, p. 66 – 83, February 2001.
- D. Paret, Le Bus CAN Aplications CAN, CANopen, DeviceNet, OSEK, SDS..." (in French), ISBN: 2 10 0003659 9, Dunod, Paris, 1999.
- J. Galdun, R. Ghostine, JM Thiriet, J. Liguš, J. Sarnovský,Definition and modelling of the communication architecture for the control of a helicopter-drone, 8th IFAC Symposium on Cost Oriented Automation, Cuba, February 2007
- A. Tanwani, J. Galdun, JM Thiriet, S. Lesecq, S. Gentil, Experimental Networked Embedded Mini Drone - Part I. Consideration of Faults, European Control Conference 2007, Kos, Greece, p.: 4332-4337, ISBN: 978-960-89028-5-5, July 2007.
- L.-B. Fredriksson, A CAN Kingdom – Rev 3.01, KVASER AB, Kinnahult, Sweden, 1995.
- Y. Fourastier, L. Pietre-Cambaceded, Cybersécurité des systèmes industriels, Cepadues, 2015.
- M. Kabir-Querrec, Cyber security of the smart grid control systems: intrusion detection in IEC 61850 communication networks, thèse de Doctorat, Univ. Grenoble Alpes, 2017.
- ISO/IEC 27002:2013, Information technology -- Security techniques -- Code of practice for information security controls, IEC 2013
- ISO/IEC 27005:2018, Information technology -- Security techniques -- Information security risk management, IEC 2018.
- Caselli, M., Zambon, E., and Kargl, F. (2015). Sequence-aware Intrusion Detection in Industrial Control Systems. In *Proc. 1st ACM Workshop CPSS*, pages 13–24.
- Dwyer, M. B., Avrunin, G. S., and Corbett, J. C. (1999). Patterns in property specifications for finite-state verification. In *Proc. ICSE'99*.
- Foulard, C., Flaus, J.-M., and Jacomino, M. *Automatique pour les classes préparatoires : cours et exercices*.
- Lemieux, C., Park, D., and Beschastnikh, I. (2015). General LTL specification mining. In *Proc. ASE'15*, pages 81–92.
- Mitchell, R. and Chen, I.-R. (2014). Behavior Rule Specification-based Intrusion Detection for Safety Critical Medical Cyber Physical Systems. *IEEE Tran. on Depend. and Sec. Comp.*, 12(1) :16–30.

References

- Trung Duc TRAN, Jean-Marc THIRIET, Nicolas MARCHAND, Amin El MRABTI. A Cybersecurity Risk Framework for Unmanned Aircraft Systems under Specific Category, Journal of Intelligent and Robotic Systems, Springer Verlag, 2022, 104, pp.4. ⟨10.1007/s10846-021-01512-0⟩
- Stéphane MOCANU, Jean-Marc THIRIET - Real-time performance and security of IEC 61850 process bus communications. Journal of Cyber Security and Mobility, River Publishers, 2021, ⟨10.13052/jcsm2245-1439.1021⟩. ⟨hal-03192264⟩
- Jean-Marc THIRIET, Denis GENON-CATALOT, Stéphane MOCANU, Hamed YAHOUI. Industry 4.0: Educational platforms disseminations in South-East Asia in the field of Automation - EAEEIE 2021 - 30th Annual Conference of the European Association for Education in Electrical and Information Engineering (EAEEIE), Sep 2021, Prague, Czech Republic. ⟨10.1109/EAEEIE50507.2021.9530861⟩
- Karem HAFSI, Denis GENON-CATALOT, Jean-Marc THIRIET, Olivier LEFEVRE. DC building management system with IEEE 802.3bt standard, HSPR 2021 IEEE International Conference on High Performance Switching and Routing (HSPR), Jun 2021, Paris, France. pp.1-8, ⟨10.1109/HPSR52026.2021.9481806⟩
- Trung Duc TRAN, Jean-Marc THIRIET, Nicolas MARCHAND, Amin EL MRABTI - Toward Cybersecurity of Unmanned Aircraft System operations under “Specific” category - ICUAS, Athens, 2020, September 1-4, 2020, hal-03108301.
- Stéphane MOCANU, Jean-Marc THIRIET - Experimental study of performance and vulnerabilities of IEC 61850 process bus communications on HSR networks - 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Sep 2020, Genoa, Italy, hal-02921495.
- Jean-Marc THIRIET, Stéphane MOCANU - A course in cyber-security, with orientations towards cyber-physical systems. EAEEIE 2019 - 29th Annual Conference of the European Association for Education in Electrical and Information Engineering, Sep 2019, Ruse, Bulgaria. ⟨hal-02283490⟩
- Trung Duc TRAN, Jean-Marc THIRIET, Nicolas MARCHAND, Amin EL MRABTI, Gabriele LUCULLI - Methodology for risk management related to cyber-security of Unmanned Aircraft Systems - 24th IEEE Conference on Emerging Technologies and Factory Automation (ETFA2019), IEEE Industrial Electronics Society (IES), Sep 2019, Zaragoza, Spain. ⟨hal-02308354⟩
- Jean-Marc THIRIET, Stéphane MOCANU - Some Considerations on Dependability Issues and Cyber-Security of Cyber-Physical Systems - The 7th IEEE International Conference on Smart Communications in Network Technologies (SACONET’18), Oct 2018, El Oued, Algeria, France. ⟨hal-01909025⟩
- Oualid KOUCHAM, Stéphane MOCANU, Guillaume HIET, Jean-Marc THIRIET, Frédéric MAJORCZYK - Efficient Mining of Temporal Safety Properties for Intrusion Detection in Industrial Control Systems - 10th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes (SAFEPROCESS'18), Aug 2018, Warsaw, Poland. pp.1-8. ⟨hal-01877109⟩
- Abdelhak MKHIDA, Jean-Marc THIRIET, Jean-François AUBRY - Integration of intelligent sensors in Safety Instrumented Systems (SIS) - Process Safety and Environmental Protection, 92 (2014) 142–149, Elsevier, Elsevier, 2014, 92 (2), pp.142-149 (JCR).
- Faiza CHARFI, Walid LABIDI, Jean Marc THIRIET - Performance Study of a New CSMA/CA Access Method with QoS Based on 802.11b and Comparison with

References

- Zeashan H. KHAN, Jean Marc THIRIET, Denis GENON-CATALOT - Drive-by-Wireless Teleoperation with Network QoS Adaptation – International Journal of Advanced Engineering Sciences and Technologies - ISSN: 2230-7818, Volume 2 Issue 2, février 2011, pp. 160-169.
- Rony GHOSTINE, Jean-Marc THIRIET, Jean-François AUBRY - Variable delays and message losses: influence on the reliability of a control loop - Reliability Engineering & System Safety - RESS-D-09-00489R1, doi:10.1016, Vol 96, Issue 1 (2011) pp. 160-171 (JCR).
- Faiza CHARFI, Oumsaad SLAMA, Jean-Marc THIRIET, Suzanne LESECQ - Improving the control performance in Wireless Network Controlled Systems, using the beacon mode - Journal of telecommunications, Volume 3, Issue 1, June 2010, pp.72-78. ISSN 2042-8839.
- J. M. THIRIET, F. MERIAUDEAU, J. C. BURGUILLO, H. FREMONT, H. YAHOUI, P. de FOOZ - Toward an International Curricula Network for exchanges and LifeLong Learning - Electronics and Electrical Engineering, No. 10 (106), December 2010, pp. 147-150, ISSN 1392-1215.
- J. GALDUN, J.-M. THIRIET, J. LIGUS – Study of different load dependencies among shared redundant systems - Scalable Computing: Practice and Experience, Volume 10, no. 3 (September 2009), Special Issue: Real-Time Distributed Systems and Networks, pp. 241-252, ISSN 1895-1767.
- Zeashan H. KHAN, Denis GENON-CATALOT and J.M. THIRIET - Wireless Network Architecture for Diagnosis and Monitoring Applications - MJC, MASAUM Journal of Computing (ISSN 2076-0833), Volume: 1 Issue: 2, September 2009, pp. 318-325.
- Insaf SASSI, Alexia GOUIN, Jean-Marc THIRIET - Wireless Network Performance Evaluation for Networked Robots - 22nd IEEE International Conference on Emerging Technologies And Factory Automation - ETFA 2017, Sep 2017, Limassol, Cyprus. ⟨hal-01665237⟩
- Insaf SASSI, Alexia GOUIN, Jean-Marc THIRIET - Distributed to Embedded Bayesian Network for Diagnosis of a Networked Robot - IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA 2017), Jun 2017, Annecy, France. ⟨hal-01558499⟩
- Insaf SASSI, Alexia GOUIN, Jean-Marc THIRIET - Diagnosis architecture reconfiguration for a networked mobile robot - 27th European Safety and Reliability Conference (ESREL 2017), Jun 2017, Portorož, Slovenia. ⟨ 10.1201/9781315210469-373 ⟩. ⟨hal-01558498⟩
- Oualid KOUCHAM, Stéphane MOCANU, Guillaume HIET, Jean-Marc THIRIET, Frédéric MAJORCZYK - Detecting Process-Aware Attacks in Sequential Control System - 21st Nordic Conference on Secure IT Systems (NordSec 2016), pp.20-36, Nov 2016, Oulu, Finland. <http://nordsec.oulu.fi>. <hal-01361081>

References

- Ahmed ALTAHER, Stéphane MOCANU, Jean-Marc THIRIET - Dependability Optimization of Process-level Protection in an IEC-61850-Based Substation Walls, Revie & Bedford - 26th European Safety and Reliability Conference, Sep 2016, Glasgow, United Kingdom. Tayor & Francis Group, Risk, Reliability and Safety: Innovation Theory and Practices - ESREL 2016, pp.284, 2016. <http://esrel2016.org/>. <hal-01380261>
- Insaf SASSI, Alexia GOUIN, Jean-Marc THIRIET - A Bayesian network for diagnosis of networked mobile robots - European Safety and Reliability Conference 2016, Sep 2016, Glasgow, United Kingdom. <http://esrel2016.org/>. <hal-01375924>
- Maëlle KABIR-QUERREC, Stéphane MOCANU, Jean-Marc THIRIET, Eric SAVARY - A Test bed dedicated to the Study of Vulnerabilities in IEC 61850 Power Utility Automation Networks - Proceedings of IEEE 21th Conference on Emerging Technologies & Factory Automation (ETFA 2016), Berlin, Germany, September 2016, 2016, <http://www.etfa2016.org/index.php>. <hal-01366270>
- Ahmed ALTAHER, Stéphane MOCANU, Jean-Marc THIRIET - Evaluation of Time-Critical Communications for IEC 61850-Substation Network Architecture - Surveillance 8 International Conference, Oct 2015, Roanne, France. Proceeding of Surveillance 8 2015, <http://surveillance8.sciencesconf.org/>
- Ayoub SOURY, Melek CHARFI, Denis GENON-CATALOT, Jean-Marc THIRIET - Performance analysis of Ethernet Powerlink protocol: Application to a new lift system generation - 20th IEEE International Conference on Emerging Technologies and Factory Automation, ETFA'2015, IEEE, 8-11/9/2015, <10.1109/ETFA.2015.7301492>. <hal-01233841>
- Maëlle KABIR-QUERREC, Stéphane MOCANU, Jean-Marc THIRIET, Eric SAVARY - Power Utility Automation Cybersecurity: IEC 61850 Specification of an Intrusion Detection Function - ESREL 2015, Zurich, 7-10 Septembre 2015.
- Ayoub SOURY, Denis GENON-CATALOT, Jean-Marc THIRIET - New lift safety architecture to meet PESSRAL requirements - 2nd World Symposium on Web Applications and Networking (WSWAN), IEEE Computer Society, 21st to 23rd March 20152015, IEEE, 2015, <10.1109/WSWAN.2015.7210314>. <hal-01233766>

Many Thanks !

- A. Altaher (Gipsa-lab, Grenoble)
- C. Aubrun (CRAN, Nancy)
- JF Aubry (CRAN, Nancy)
- P. Barger (Heudyasic., UTC, Compiègne)
- M. Bayart (Cristal, Lille)
- C. Berbra (Gipsa-lab, Grenoble)
- L. Cauffriez (LAMIH, Valenciennes)
- P. Charpentier (INRS, Nancy)
- J. Ciccotelli (INRS, Nancy)
- B. Conrard (Cristal, Lille)
- A. El-Mrabti (Sogilis, Grenoble)
- J. Galdun (Rockwell, Prague)
- D. Genon-Catalot (LCIS, Valence)
- S. Gentil (Gipsa-lab, Grenoble)
- R. Ghostine (Thales, London)
- A. Gouin (Gipsa-lab, Grenoble)
- M. Haffar (Saudi Oger, S.A.)
- G. Hiet (Supelec, Rennes)
- M. Kabir-Querrec (ABB, Zürich)
- Z. Khan (Riphah Int. Univ., Pakistan)
- O. Koucham (Sentryo, Lyon)
- S. Lesecq (CEA, Grenoble)
- J. Ligus (Univ. Kosice, Slovaquie)
- N. Marchand (Gipsa-lab, Grenoble)
- A. Mechraoui (Mediane Systèmes, Paris)
- A. Mkhida (ENSAM, Meknes)
- S. Mocanu (Gipsa-lab, Grenoble)
- M. Robert (CRAN, Nancy)
- E. Rondeau (CRAN, Nancy)
- I. Sassi (Post-doc, IFFSTAR, Lille)
- C. Simon (CRAN, Nancy)
- Đ. T. Trung (Gipsa-lab, Grenoble)
- M. Wahl (INRETS, Villeneuve d'Ascq)
- P. Weber (CRAN, Nancy)

FACTORI 4.0
Erasmus +

UGA
Université Grenoble Alpes

ស‌ូមអរគុណចំពោះការយកចិត្តទុកដាក់របស់អ្នក។ (KH)

ຂອບໃຈຫຼາຍໆ ສຳ ລັບຄວາມສົນໃຈຂອງທ່ານ (LAO)

ขอบคุณมากสำหรับความสนใจของคุณ (TH)

Merci pour votre attention

Thank you for your attention

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