M33-1-Security of information systems

In-depth security
Sécurité en profondeur

Jean-Marc THIRIET

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

Organisation course M33

- 1. Risk analysis (JMT)
- 2. Cyber-Attacks (CB)
- 3. C. threat, responses 1 (CB)
- 4. C. threat, responses 2 : IDS (JMT)
- 5. Strategy, Audit (JMT)
- 2 Labs (DL + En cours)
- Exam M25:
- & M33:

Introduction to Network and Systems Security

- Security is nowadays important in Networks and Telecommunications
  - Today's networks are open rather than closed
    - IP VPN
    - Intranet
    - Extranet
    - IPSec
    - Wi-Fi

Types of applications

Web access

Mailing

Internet access

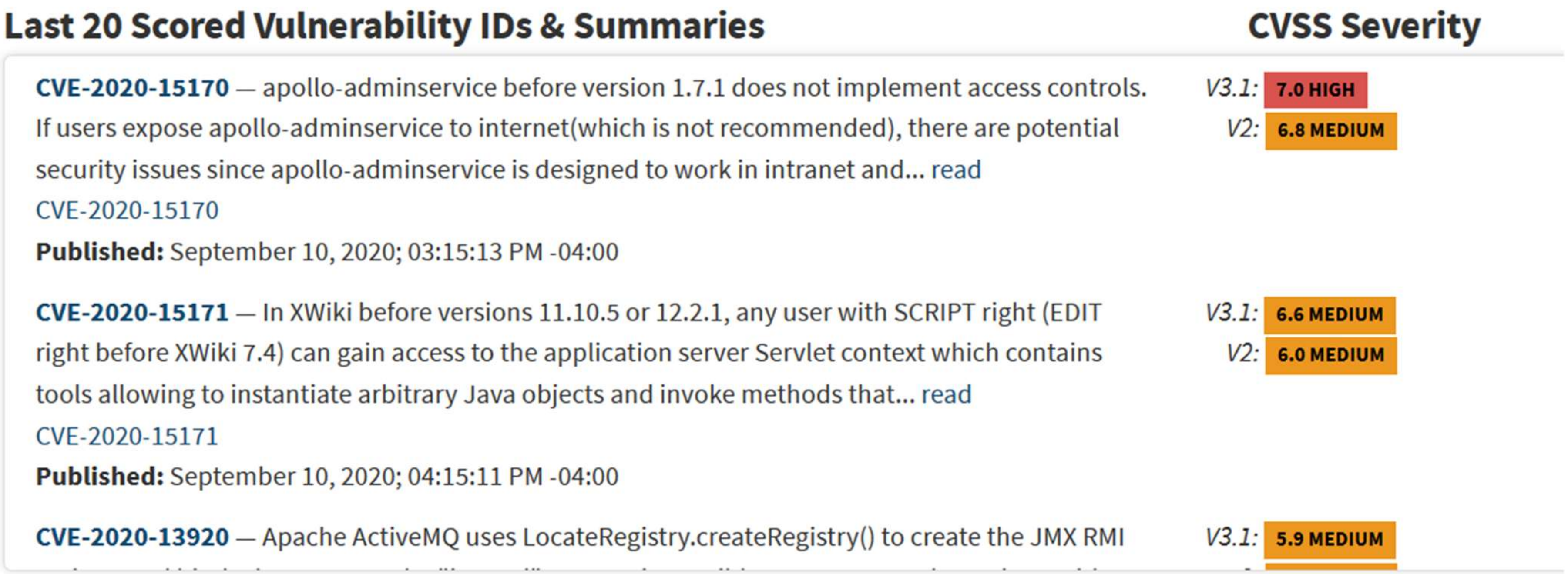
E-commerce

The use of the Internet in companies is widespread

- Opportune target : *cible opportune*
  - Hackers looking for opportune targets
  - Ddos attacks, zombie machines army
- Chosen target : *cible choisie*
  - You are the actual victim
  - Hacker is interested by you, your activity, your data

Brainstorming

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



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

CVE-2020-15170 — apollo-adminservice before version 1.7.1 does not implement access controls. If users expose apollo-adminservice to internet(which is not recommended), there are potential security issues since apollo-adminservice is designed to work in intranet and... read CVE-2020-15170

Published: September 10, 2020; 03:15:13 PM -04:00

V3.1: 7.0 HIGH
V2: 6.8 MEDIUM

CVE-2020-15171 — In XWiki before versions 11.10.5 or 12.2.1, any user with SCRIPT right (EDIT right before XWiki 7.4) can gain access to the application server Servlet context which contains tools allowing to instantiate arbitrary Java objects and invoke methods that... read CVE-2020-15171

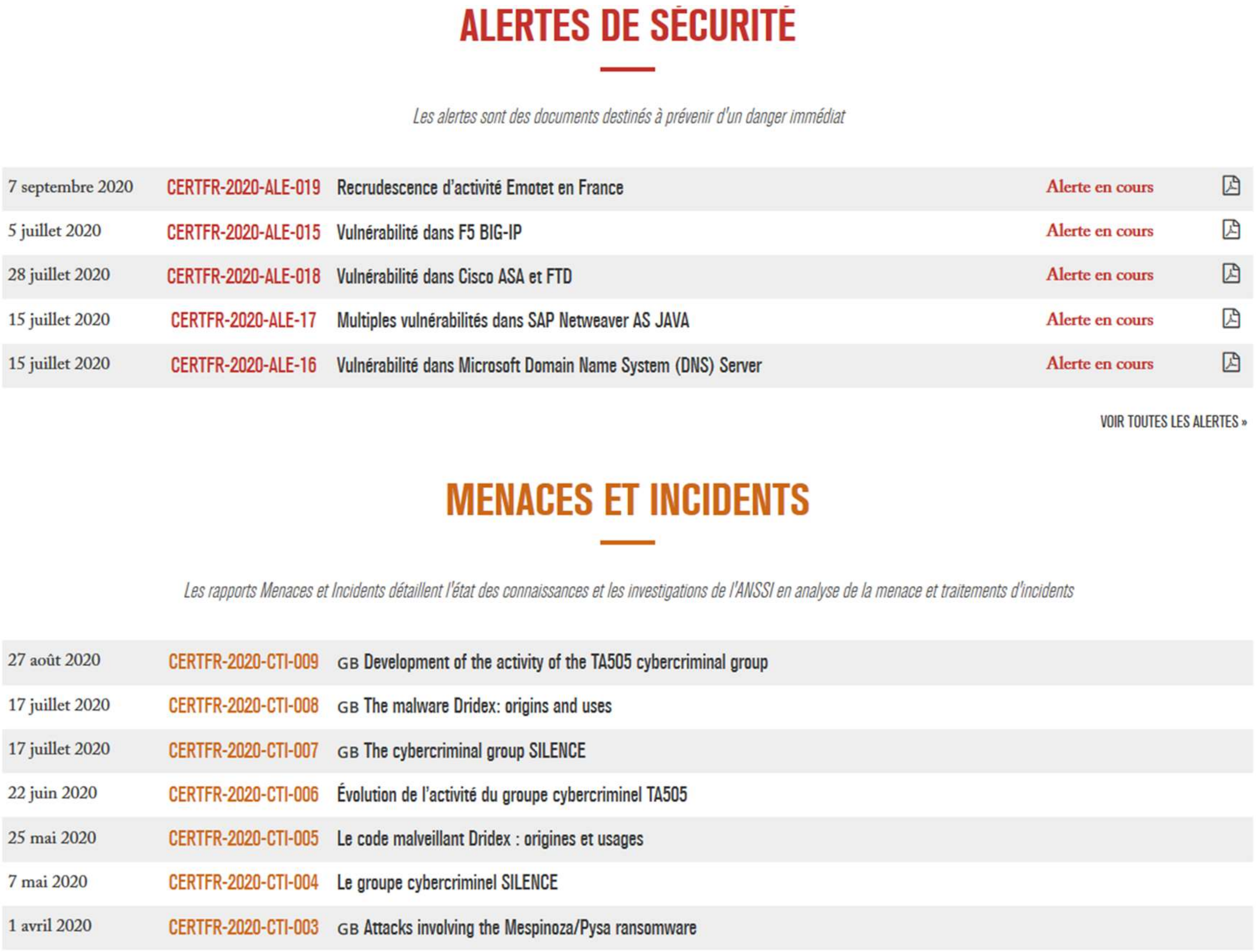
Published: September 10, 2020; 04:15:11 PM -04:00

V3.1: 6.6 MEDIUM
V2: 6.0 MEDIUM

CVE-2020-13920 — Apache ActiveMQ uses LocateRegistry.createRegistry() to create the JMX RMI

V3.1: 5.9 MEDIUM

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



ALERTES DE SÉCURITÉ

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

7 septembre 2020	CERTFR-2020-ALE-019	Recrudescence d'activité Emotet en France	Alerte en cours
5 juillet 2020	CERTFR-2020-ALE-015	Vulnérabilité dans F5 BIG-IP	Alerte en cours
28 juillet 2020	CERTFR-2020-ALE-018	Vulnérabilité dans Cisco ASA et FTD	Alerte en cours
15 juillet 2020	CERTFR-2020-ALE-17	Multiples vulnérabilités dans SAP Netweaver AS JAVA	Alerte en cours
15 juillet 2020	CERTFR-2020-ALE-16	Vulnérabilité dans Microsoft Domain Name System (DNS) Server	Alerte en cours

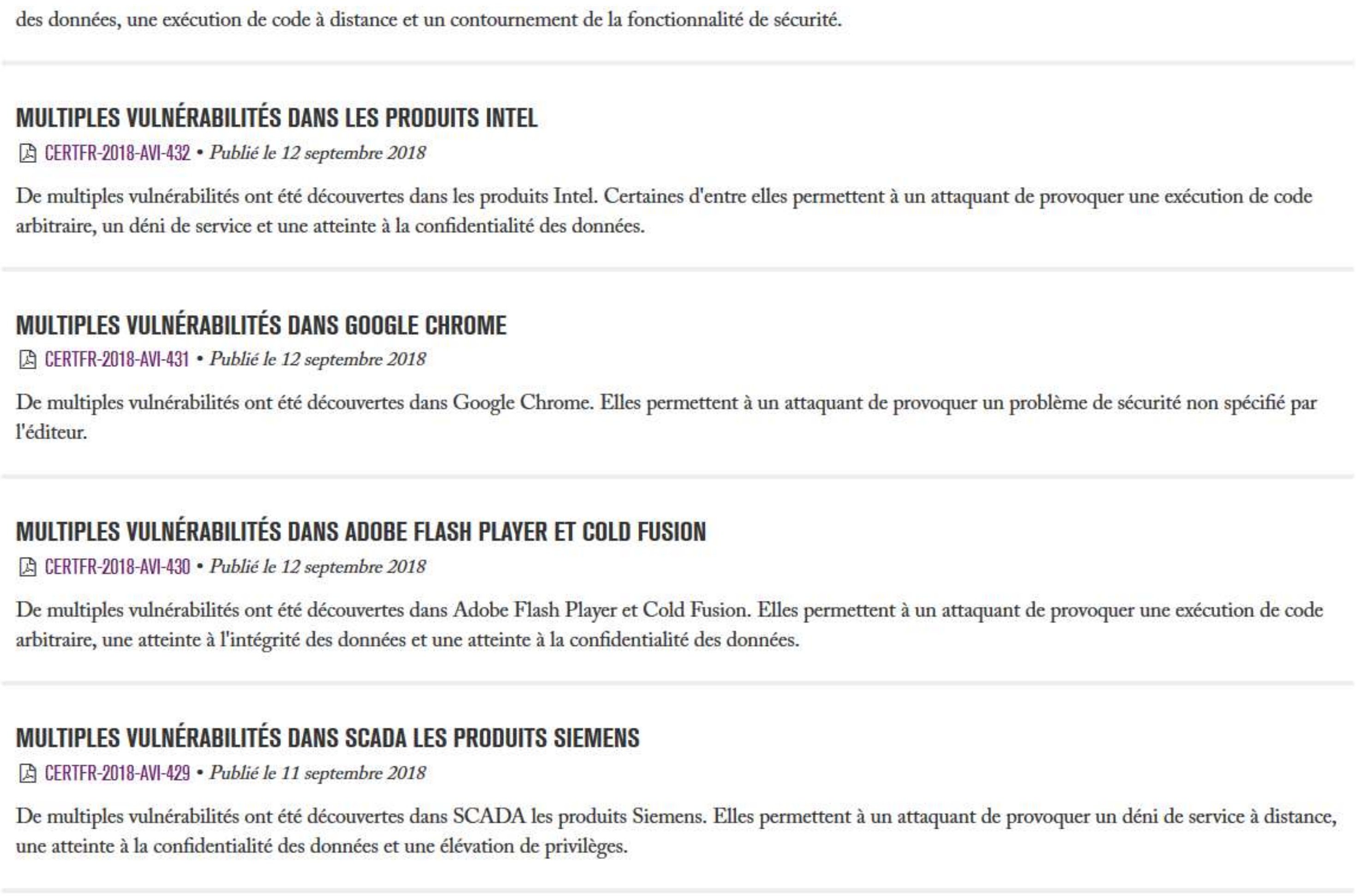
VOIR TOUTES LES ALERTES »

MENACES ET INCIDENTS

Les rapports Menaces et Incidents détaillent l'état des connaissances et les investigations de l'ANSSI en analyse de la menace et traitements d'incidents

27 août 2020	CERTFR-2020-CTI-009	GB Development of the activity of the TA505 cybercriminal group
17 juillet 2020	CERTFR-2020-CTI-008	GB The malware Dridex: origins and uses
17 juillet 2020	CERTFR-2020-CTI-007	GB The cybercriminal group SILENCE
22 juin 2020	CERTFR-2020-CTI-006	Évolution de l'activité du groupe cybercriminel TA505
25 mai 2020	CERTFR-2020-CTI-005	Le code malveillant Dridex : origines et usages
7 mai 2020	CERTFR-2020-CTI-004	Le groupe cybercriminel SILENCE
1 avril 2020	CERTFR-2020-CTI-003	GB Attacks involving the Mespinoza/Pysa ransomware

Also Industrial systems…



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

MULTIPLES VULNÉRABILITÉS DANS LES PRODUITS INTEL

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

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

MULTIPLES VULNÉRABILITÉS DANS GOOGLE CHROME

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

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

MULTIPLES VULNÉRABILITÉS DANS ADOBE FLASH PLAYER ET COLD FUSION

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

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

MULTIPLES VULNÉRABILITÉS DANS SCADA LES PRODUITS SIEMENS

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

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

Approaches for security

- Theoretic approach (cryptology, virology)
- Organisational approach (security policy, human aspects, saving policy & recovery, management of users)
- Methodological approach (firewall configuration, attacks strategies and defense…)
- Technological approach (network, topology, servers, hardware and software firewalls, security protocols)
- Testing (quality, ISO 9001 => formalization, documentation, be able to prove…) approach (checking, testing, audit…)

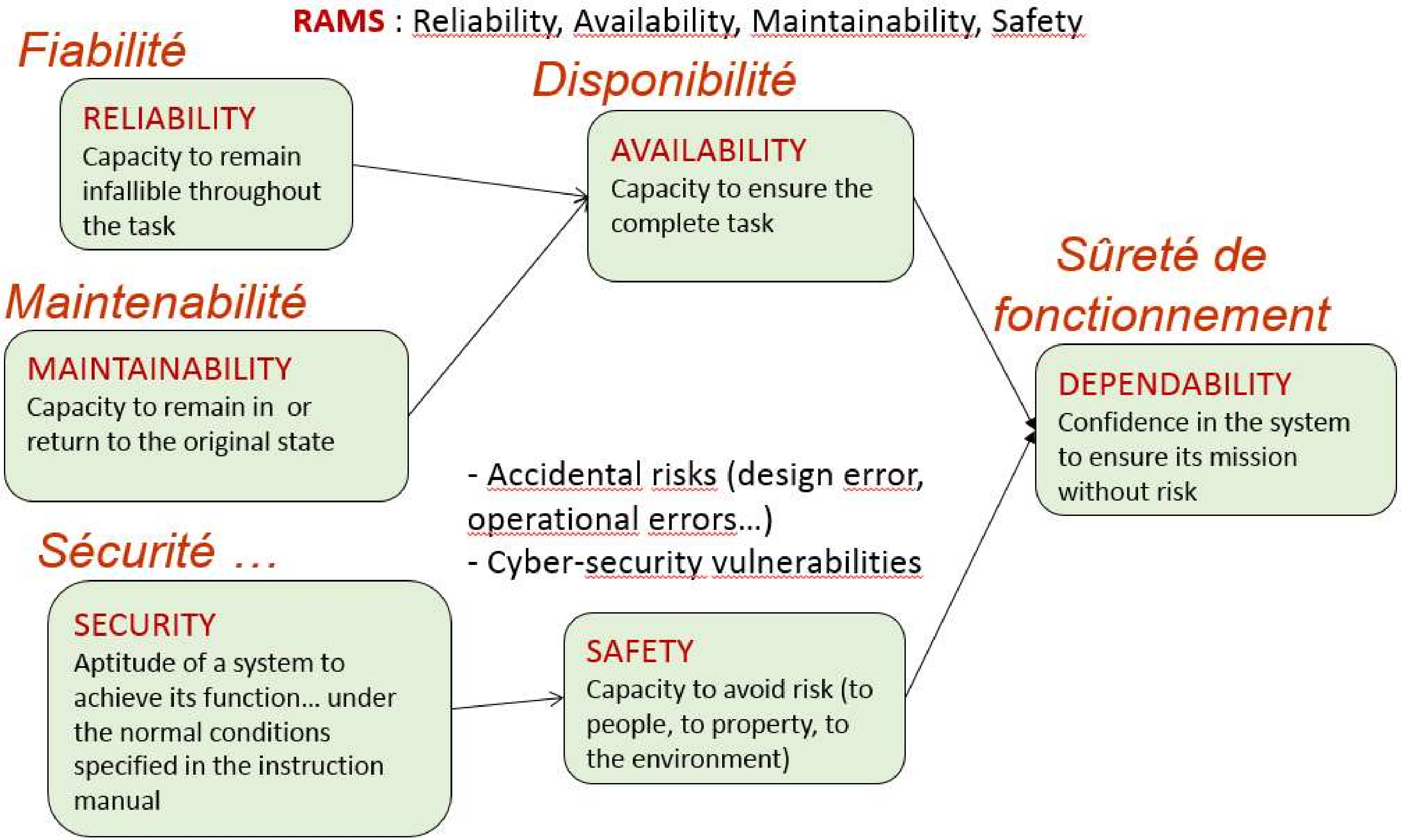
1. Introduction to dependability, security principles

1.1 Dependability

1.2 Safety and security: definition

1.3 Safety and security principles

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)

1.1 Safety
= the Science of Failures

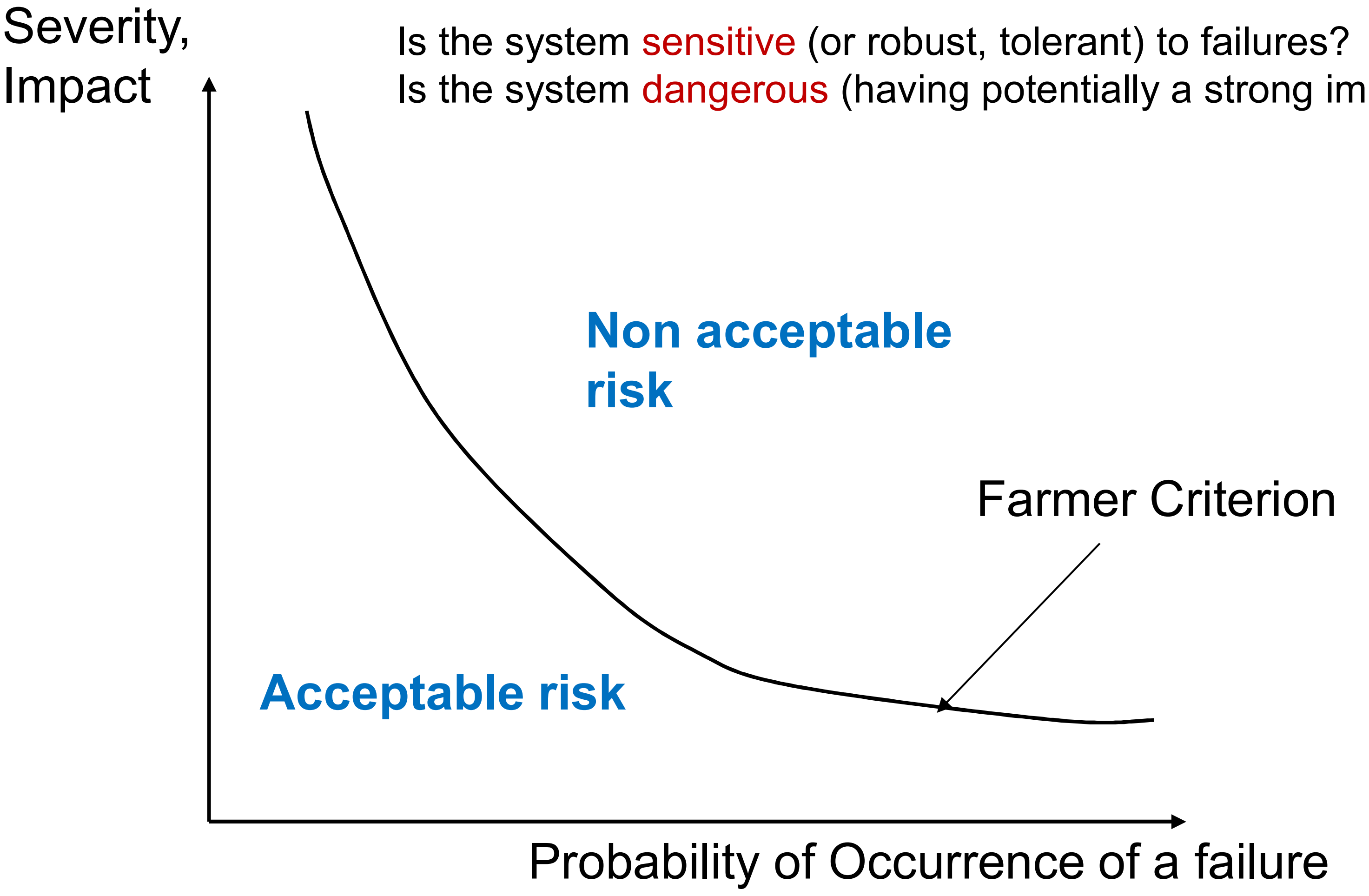
- Failure (*défaillance*): interruption of the capacity of an entity to carry out a necessary function
  - The function concerned should be defined
    - ex 1: to ensure communication between two sites
    - ex 2: **to ensure the accessibility of data** (locally and remotely)
  - the criterion of interruption 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

1.1 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 (gravity)** 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/resilience
  - -Protection

1.1 Severity-probability

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



Elements of risks (Asset)

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

Elements of risks (Threat)

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

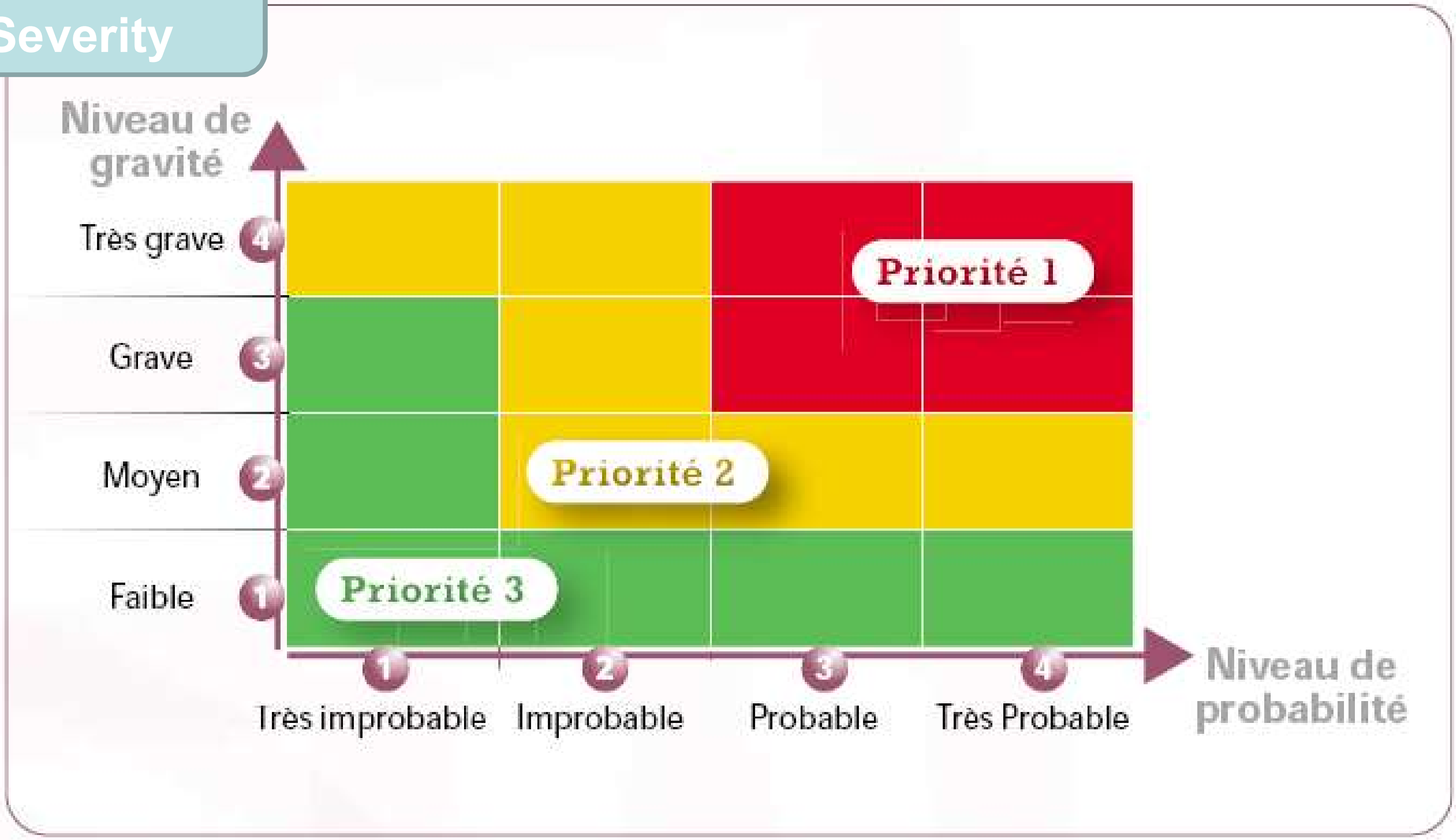
Elements of risks (Vulnerability)

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

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

Risks evaluation, evaluation of the severity

Gravité = Severity



Example

Danger (cause)	Dangerous situation	Dangerous event	Risk of…	Consequence	Severity	Probability	Priorities	Observations
Explosion of a tyre	Car sliding	Screw in the tyre	Accident	Killing people in the car	4 (high)	1 (low)	2 (int.)	Having a 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 grid 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

1.2 Safety and security: definition

- 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

1.2 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

1.2 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.

1.3 Security principles

Security principles

- 1.3.1 Physical security
- 1.3.2 Operational security
- 1.3.3 Logical security
- 1.3.4 Applicative security
- => Checklist!

1.3.1 Physical security

- Protection of energy sources (electricity (power supplies)…)
- Environmental protection (fire, temperature, moisture/fungi/fungus (humidity)…)
- Protection of access
  - Physical protection of the equipment
  - Distribution premises
  - Plugboards (electrical connections boards), cabled infrastructure,
  - Traceability of access on the premises
- Operational reliability and materials reliability
- Physical redundancy
- Marking (census) of the materials
- Preventive (tests…) and corrective (spare parts…), maintenance plans

1.3.2 Operational security

- = correct operation of the system
- Back up plan
- Emergency help plan
- Continuity plan
- Test plan
- Regular and if possible dynamic inventories
- Management of the computer park
- Management of the configurations and the updates
- Management of the incidents and follow-ups until resolution
- Automation, control and follow-up of the exploitation
- Analysis of accountancy and logging files
- Management of the maintenance contracts
- Separation of the environments of development, industrialization and production of add-ons
- Reliable and quality connectivity
- Protected infrastructure network

1.3.3 Logical security

- Mechanisms of security by software
  - Identification
  - Authentication
  - Authorization
- Devices set up to guarantee confidentiality and integrity
  - Cryptography
  - Effective password management
  - Antivirus
  - Backup of sensitive data
- Classification of data
  - Degree of sensitivity (normal, confidential…)

1.3.4 Applicative security

- Development Methodology (respect of the development standards suited to the technology employed)
- Robustness of the applications
- 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
- Quality and relevance of data
- Security Insurance Plan

Type of Applications

1. Operating Systems
   - Windows W. Server, Linux, Mac OS (computers, servers)
   - Android, iOS (Smart phones OS)
   - Real Time OS (IoT, embedded systems)
2. Classical Applications
   - Office software (Open Office, Microsoft Office)
   - Matlab
3. Specialised applications/Business applications
   - Unity, TIA Portal…
4. « Home-made » software
   - ???

Example

- The management team of a company requires the following objectives
  - Availability of the communication media of the Headquarters situated in Paris
  - Availability of the communication media for the Grenoble plant
  - Availability of the communication media with the suppliers or sub-contractors ABC
  - Availability of the mailing system
  - Production
  - Confidentiality and integrity of the company production « secrets »
  - Updates of the production programme

Deontology

- Students

  => signing of a computer (informatics) charter

- Administrator Network/Systems

  => responsibility

- The use of the methods described in this course engages the responsibility of the users!

Exercise: Risk analysis (1/4) (Presentation Date: 4th January 2023)

- Per teams of 4-5 people (International teams), take an example of a company
  - Company in which you will spend your training period, for example
- Achieve an analysis of computer risks
  - Confidentiality
  - Integrity
  - …
- Do some assumptions for each of theses risks
  - Occurrence frequency
  - Consequences (severity)
- Try to give a cost for each of these risks
- Make a presentation next class

Exercise: Risk analysis (2/4) Steps and deadlines

- This is a group work
- Each group: 1 Leader (to manage the group), 1 Rapporteur (to give the feedback at the end of the process) => Deadline for the groups composition: As soon as possible
- Each group : To choose/define an example of applications (like hospital, airport, shop, government facilities, embedded system (autonomous car, pacemaker…)) => Deadline: As soon as possible

Exercise: Risk analysis (3/4) Steps and deadlines

- Based on the application chosen
  - – Make a risk analysis (3 situations)
  - – Try to give some indicators
  - – Prepare an action plan

Exercise: Risk analysis (4/4) Expected result

- Presentation (as slides) to be achieved next class 4/1/23: done by the **rapporteur**: 4 slides for a 5-minute presentation
  - 1. Composition of the group, roles, choice of the « application »
  - 2. Risk analysis (3 situations max)
  - 3. Action plan (priorities for the setting of actions to resolve (or decrease) the risks) on the identified situations
  - 4. Explaination of how the group worked
- Slides to be sent to me 3/1/23, 8pm, at last

References

- J.F. Aubry – Cours de Sûreté de Fonctionnement, INPL Lorraine, 2005.
- J.C. Laprie & al. – Guide de la sûreté de fonctionnement – Cépaduès, 1995.
- A. Villemeur – *Sûreté de fonctionnement des systèmes industriels* – Editions Eyrolles, Paris, 1988.
- S. Ghernaouti-Helie – *Sécurité informatique et réseaux, 4ème édition* – Dunod, 2013
- C. Davis, M. Schiller, K. Wheeler - *IT Auditing: using control to protect assets* – 2007, Mc Graw Hill