

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

1. Sécurité des systèmes d'information

Jean-Marc THIRIET

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



CV succinct

- Docteur Université Nancy 1993
- Maître de Conférences Nancy-IUT de Nancy-Brabois Dépt. Réseaux & Télécoms 1993-2005
- Habilitation à Diriger des Recherches Nancy en 2004
- Professeur à l'UGA, IUT1 de Grenoble 2005
 - Enseignement en Réseaux, sécurité des réseaux, réseaux industriels, traitement du signal, automates programmables (DUT, licence, master)
 - Responsable Licence Professionnelle « réseau sans fil et sécurité » de 2007 à 2011 (programme international jusqu'en 2016)
 - Actuellement responsables des relations internationales, IUT1
- Recherche en sûreté de fonctionnement des systèmes automatisés intégrant des réseaux de communication
- Directeur du Laboratoire de Recherche GIPSA-Lab (Automatique, Traitement du Signal) de 2011 à 2015
- Responsable d'un projet européen EIE-Surveyor www.eie-surveyor.org traitant de l'évolution des formations universitaires dans nos disciplines en Europe (110 universités partenaires)

Introduction : contexte

Industrie 4.0

From Industry 1.0 to Industry 4.0...

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

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

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

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



From Industry 1.0 to Industry 4.0...

Purposes: Production, minimal cost

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

Industry 4.0

- 1. Challenges: Safety & Cyber-security**
- 2. Maintenance**
- 3. Logistics & Organisation**
- 4. Production**
- 5. Supervision**
- 6. Robotics in Industry**

- ENQUÊTE - Les cyberattaques contre les systèmes de contrôle industriel ont augmenté de 40% dans le monde au 1er semestre 2018. L'énergie et les transports sont les plus ciblés.
- Voici un an, une raffinerie de la société Aramco en Arabie saoudite subissait une cyberattaque qui a sonné l'alarme dans le monde industriel. Elle a été victime de Triton, premier virus créé spécifiquement pour corrompre une infrastructure industrielle. La catastrophe a été évitée de justesse. Les deux premiers dispositifs de sécurité chargés de bloquer la circulation des flux de pétrole ont été paralysés par les hackers, mais le troisième, déconnecté des autres, a tenu bon.
- [Le Figaro, 12/12/2018]
- STUXNET

Convergence between IT and cyber-physical systems



US Black-out, 2003

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

INFRASTRUCTURE

Industrial
Control
Systems (ICS)

Smart grids

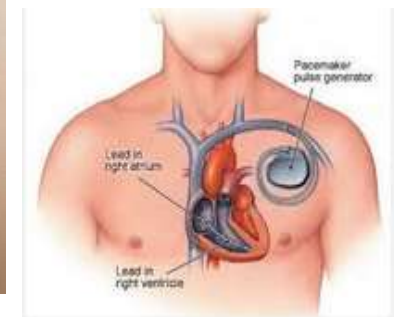


Cyber attack ukrainian power network,
Dec. 2015



EMBEDDED SYSTEMS

Drones
Autonomous vehicles
Connected objects



Context

Methodology, standards

Science

Applications

Societal

1. **Dependability** : Confidence in the system to ensure its mission without risk (or with a risk management)
 - => Co-design approach (Network QoS $\Leftrightarrow$ 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 61508]
3. **Cyber-security**: Cyber security is the protection of systems, networks and data in cyberspace [www.itgovernance.co.uk, www.ssi.gouv.fr]
4. **Networked Control Systems**: Control System closed through a **network**
5. **Complex systems**, infrastructure, distributed systems
6. **Embedded system**, autonomous system, connected objects
7. **ICS** : Industrial Control Systems
8. **IoT**: Internet of Things, **IloT**: Industrial Internet of Things
9. **Cyber-physical systems (CPS)**: Marrying physicality and computation [persyval-lab.org]
10. 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

Cyber-security

- **Cybernetics** from Greec κυβερνήτης (*kubernêtês*) => Used 19th and 20 century => ideas of control and communication
- **Cyber** : Greek *kubernân*, to govern
- Today used for everything relative to the « digital » world (internet, web...)
- **Cyber-security:**
 - Cyber security comprises technologies, processes and controls that are designed to protect systems, networks and data from cyber attacks. Effective cyber security reduces the risk of cyber attacks, and protects organisations and individuals from the unauthorised exploitation of systems, networks and technologies (<https://www.itgovernance.co.uk/what-is-cybersecurity>)
 - État recherché pour un système d'information lui permettant de résister à des événements issus du cyberspace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense. (ANSSI, <https://www.ssi.gouv.fr/entreprise/glossaire/c/>)

Introduction à la sécurité des réseaux

Sécurité en profondeur – In-depth security

- La sécurité devient de plus en plus cruciale dans les télécommunications
 - Les réseaux sont passés d'un modèle relativement fermé à un modèle ouvert (réseau IP partagé)
 - IP VPN
 - Intranet
 - Extranet
 - IPSec
 - Wi-Fi
- L'usage d'Internet dans les entreprises s'est généralisé

Types d'applications

Accès au web

Messagerie

Accès Internet

Commerce électronique

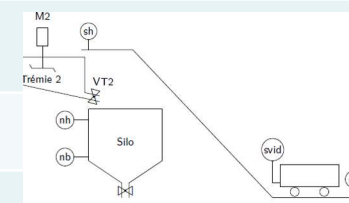
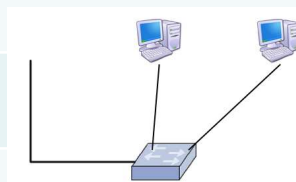
Brainstorming

- Les risques en termes de sécurité autour des réseaux et des systèmes d'information

- 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
- Sécurité en profondeur / *In-depth security*

Comparison between IT (Information Technology) and OT (Operational Technology, ex: ICS)

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



Brainstorming

- Les risques en termes de sécurité autour des réseaux et des systèmes d'information
- <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.

Approches pour la sécurité

- Approche théorique (cryptologie, virologie)
- Approche organisationnelle (politique de sécurité, aspects humains, plan de sauvegarde, stratégie de recouvrement, gestion des utilisateurs)
- Approche méthodologique (configuration de pare-feu, stratégies d'attaques et de défense...)
- Approche technologique (réseau, topologie, serveurs, pare-feu matériels et logiciels, protocoles de sécurité)
- Approche qualité (vérifications, tests, audits ...)

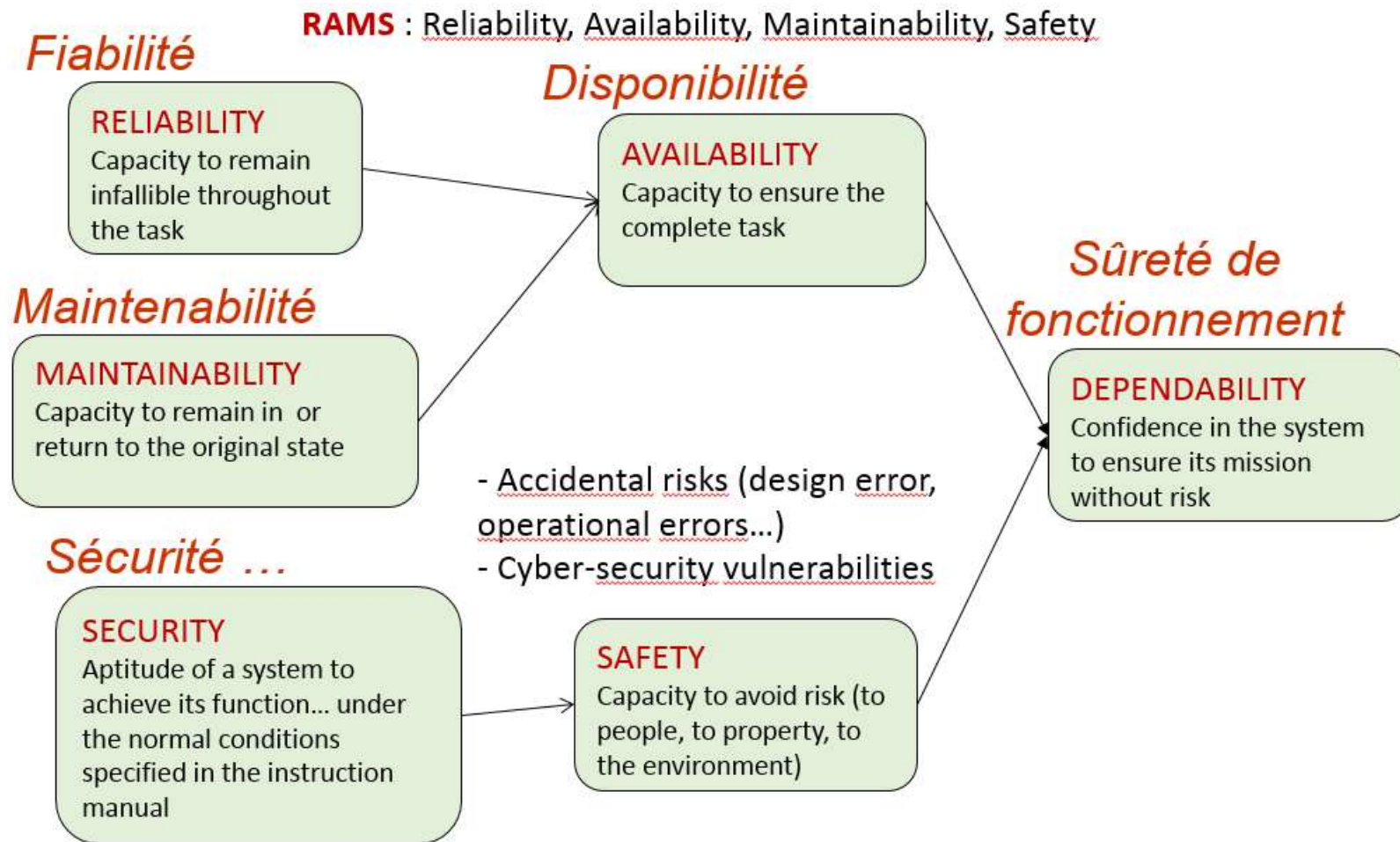
1. Introduction à la sûreté de fonctionnement, principes de sécurité

1.1 Sûreté de fonctionnement

1.2 La Sécurité : définition

1.3 Principes de sécurité

Sûreté de fonctionnement



Paramètres de Sûreté de fonctionnement

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

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

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

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

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

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

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

Sûreté de fonctionnement = science des défaillances

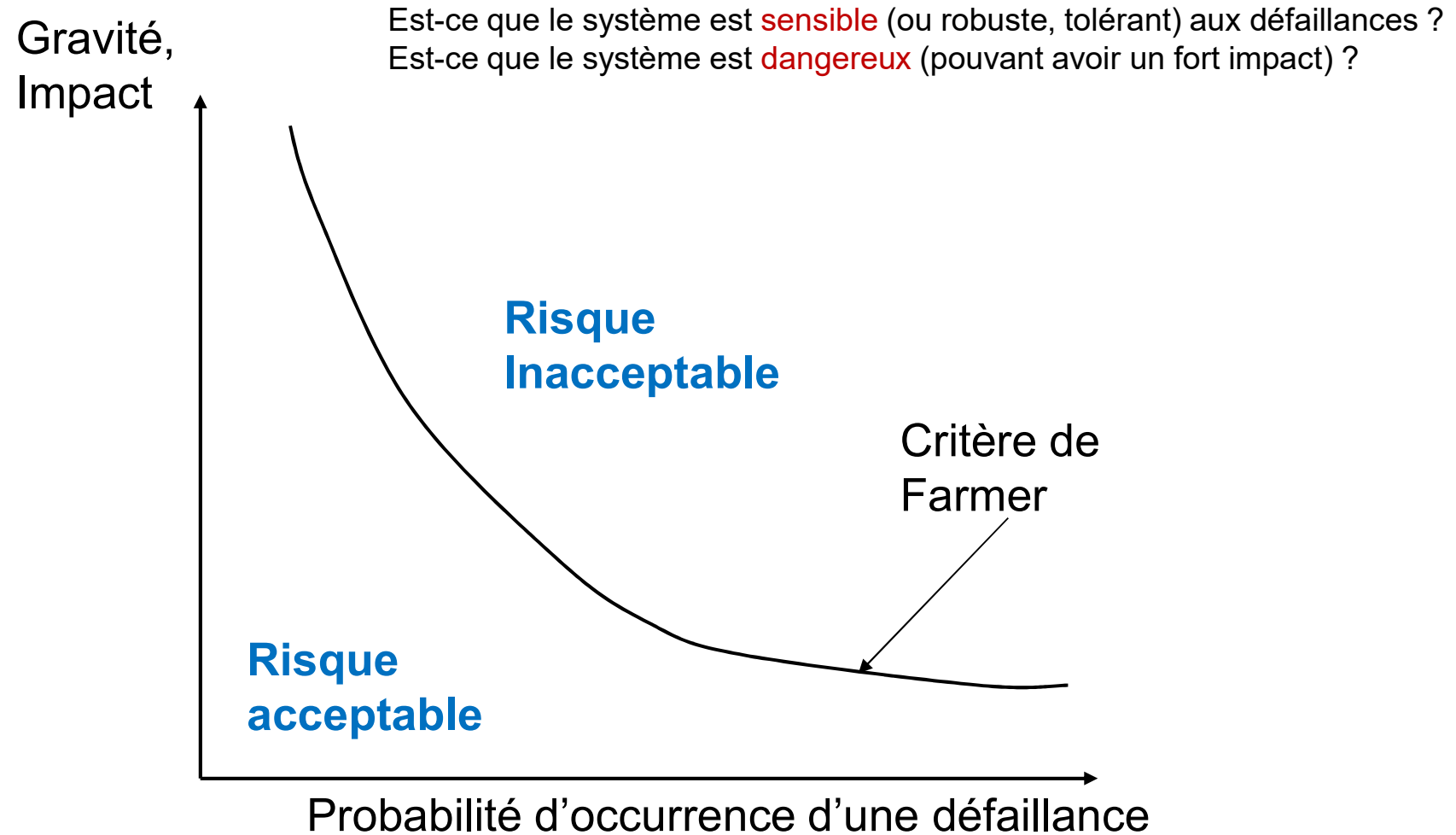
- Défaillance : cessation de l'aptitude d'une entité à accomplir une fonction requise
 - Il faut définir la fonction concernée
 - ex 1 : assurer la communication entre deux sites
 - ex 2 : **assurer la mise à disposition des données informatiques**
(en local et à distance)
 - Il faut préciser le critère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

Sûreté de fonctionnement

= ANALYSE DE RISQUE => Maîtrise des risques

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

Loi Gravité-Probabilité



Éléments de risque (Actif)

- Asset (*actif*)
 - Représenté par une valeur monétaire
 - Tout objet de valeur pouvant être endommagé, compromis ou détruit par une action accidentelle ou délibérée
 - La valeur d'un actif est généralement bien supérieure aux simples coûts de remplacement (image, questions juridiques, etc.).

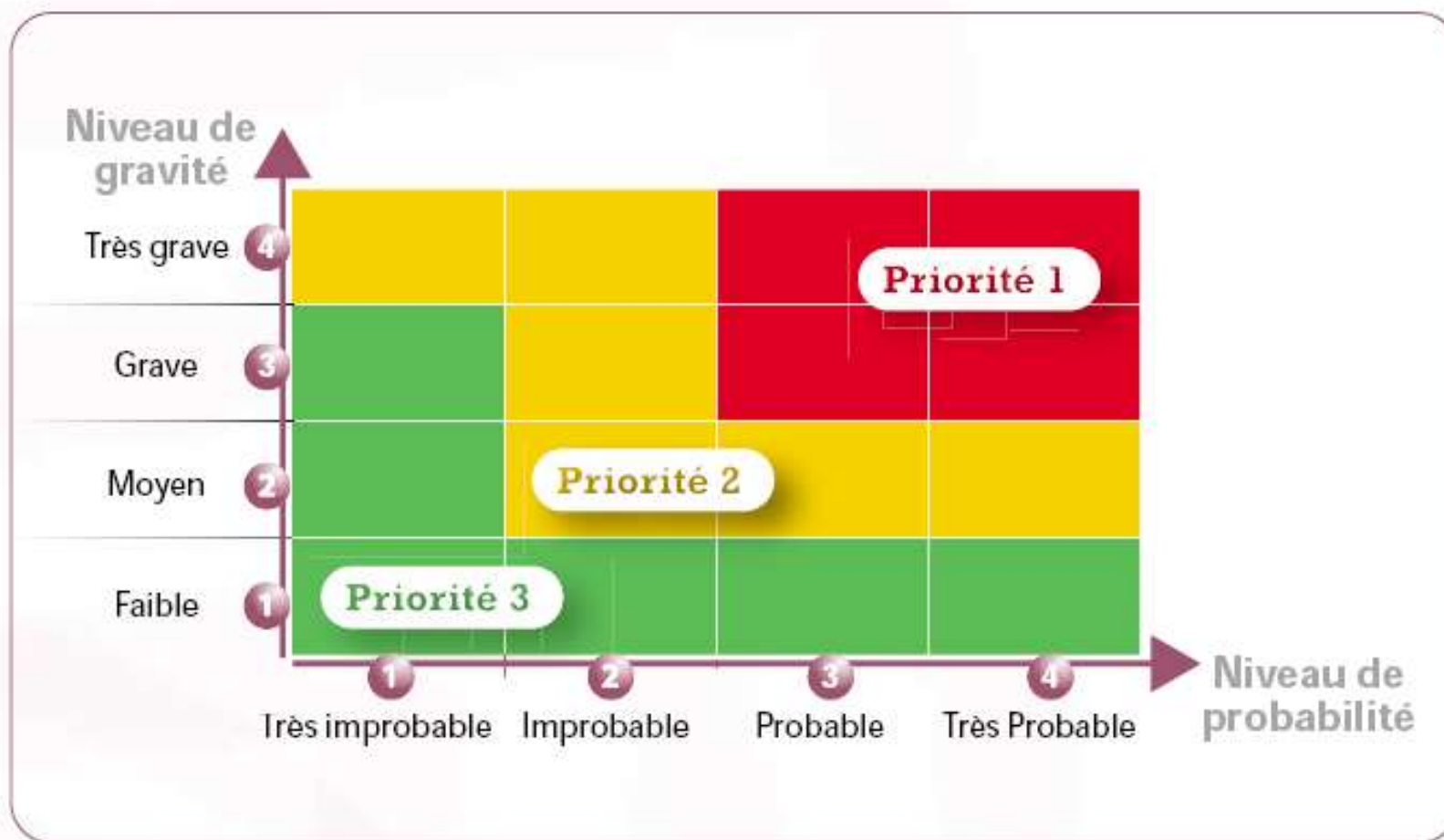
Éléments de risque (Menace)

- Threat (*menace*)
 - Événement potentiel qui, s'il était réalisé, causerait un impact non désiré
 - Deux facteurs peuvent avoir une conséquence sur la gravité d'une menace: le degré de perte et la probabilité d'occurrence
 - Taux d'occurrence annuel: probabilité qu'une menace donnée soit réalisée en une seule année en cas d'absence totale de contrôle - ex: si nous estimons qu'un incendie se produira tous les trois ans, le taux d'occurrence annuel sera de 33 % ou 0,33
 - Facteur d'exposition: degré de perte (pourcentage de la perte d'actifs en cas de menace) - ex: si nous estimons qu'un incendie entraînera une perte de 70% de la valeur des actifs, le facteur d'exposition est de 70% ou 0,7
 - => Une menace peut être calculée en pourcentage en multipliant le facteur d'exposition par le taux d'occurrence annuel. Ex: $0,7 * 0,33 = 0,231$ ou 23,1%

Eléments de risque (Vulnérabilité)

- Vulnerability (*vulnérabilité*)
 - Absence ou faiblesse de la protection des contrôles « cumulatifs » pour un actif particulier
 - Estimé en pourcentage exprimant la faiblesse du niveau de contrôle
 - Le déficit de contrôle (Control Deficiency CD) est calculé en soustrayant l'efficacité du contrôle de 100% - ex: si nous estimons que nos contrôles d'espionnage industriel sont efficaces à 70%, alors $100\% - 70\% = 30\%$ (CD)
 - La plupart du temps, plusieurs contrôles sont utilisés pour protéger un actif.
 - Ex: si la menace est qu'un employé puisse voler des secrets commerciaux et les vendre à la concurrence
 - Pour contrer cette menace, nous pouvons :
 - mettre en œuvre une politique de classification des informations,
 - surveiller le courrier électronique sortant,
 - interdire l'utilisation de dispositifs de stockage portables

Evaluation des risques, évaluation de la gravité



Exemple

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

Prescriptions, Méthodes pour l'analyse de risques

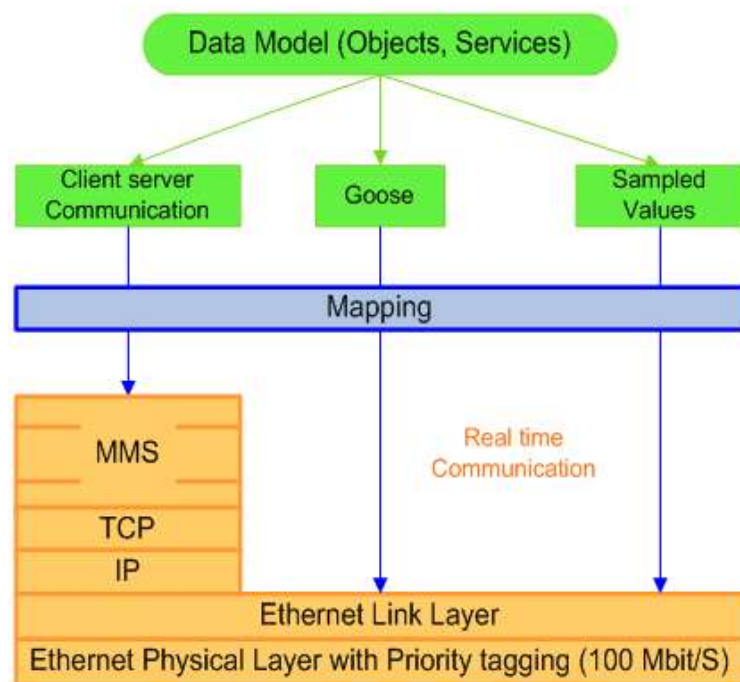
- **Méthodes**

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

- **Prescriptions**

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

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 application 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

1.2 La Sécurité : définition

- Sécurité : Définition (d'après norme EN 292)
 - Aptitude d'un système à accomplir sa fonction ... dans les conditions normales spécifiées dans la notice d'instruction...
- Sécurité-innocuité (safety)
 - Aptitude d'une entité à éviter de faire apparaître des événements critiques ou catastrophiques => pouvant affecter les personnes, les équipements, l'environnement
- **Confidentialité & intégrité**
 - Aptitude d'une entité à la préservation de la **confidentialité** et de **l'intégrité** des informations

1.2 Définitions de termes liés à la sûreté de fonctionnement et la sécurité pour des applications de type informatique-réseaux (1/2)

Propriétés propres à la sécurité

- Confidentialité : prévenir la visualisation d'information par des personnes non autorisées
- Intégrité : prévenir la non détection de modifications de l'information par des personnes non autorisées
- Authentification : permettre la vérification de l'identité des utilisateurs

Propriété liée à la sécurité

- Disponibilité : prévenir que des personnes non autorisées ne vont pas empêcher l'accès ou l'utilisation par des utilisateurs autorisés

1.2 Définitions de termes liés à la sûreté de fonctionnement et la sécurité pour des applications de type informatique-réseaux (2/2)

- Autorisation : prévenir de l'accès au système par des personnes non autorisées
- "Auditabilité" : possibilité de reconstruire l'histoire complète du comportement du système à partir d'enregistrements d'historiques
- Non "répudiabilité" : être capable de fournir une preuve irréfutable de qui est à l'origine de certaines actions sur le système
- Protection des tierces personnes : prévenir des dommages conséquents au fait que le système ait pu être attaqué (piraté) par des tiers.

1.3 Principes de sécurité

Les principes de sécurité

- 1.3.1 Sécurité physique
- 1.3.2 Sécurité de l'exploitation
- 1.3.3 Sécurité logique
- 1.3.4 Sécurité applicative
- => Checklist !

1.3.1 Sécurité physique

- Protection des sources énergétiques (alimentation...)
- Protection de l'environnement (incendie, température, humidité...)
- Protection des accès
 - Protection physique des équipements
 - Locaux de répartition
 - Tableaux de connexion, infrastructure câblée,
 - Traçabilité des accès dans les locaux
- Sûreté de fonctionnement et fiabilité des matériels
- Redondance physique
- Marquage des matériels
- Plans de maintenance préventive (tests...) et corrective (pièces de rechange...)

1.3.2 Sécurité de l'exploitation

- = bon fonctionnement du système
- Plan de sauvegarde
- Plan de secours
- Plan de continuité
- Plan de tests
- Inventaires réguliers et si possible dynamiques
- Gestion du parc informatique
- Gestion des configurations et des mises à jour
- Gestion des incidents et suivis jusqu'à leur résolution
- Automatisation, contrôle et suivi de l'exploitation
- Analyse des fichiers de journalisation et de comptabilité
- Gestion des contrats de maintenance
- Séparation des environnements de développement, d'industrialisation et de production des applicatifs
- Connectivité fiable et de qualité
- Infrastructure réseau sécurisée

1.3.3 Sécurité logique

- Mécanismes de sécurité par logiciel
 - Identification
 - Authentification
 - Autorisation
- Dispositifs mis en place pour garantir la confidentialité et l'intégrité
 - Cryptographie
 - Gestion efficace des mots de passe
 - Antivirus
 - Sauvegarde des informations sensibles
- Classification des données
 - Degré de sensibilité (normale, confidentielle...)

1.3.4 Sécurité applicative

- Méthodologie de développement (respect des normes de développement propres à la technologie employée)
- Robustesse des applications
- Contrôles programmés, tests
- Sécurité des progiciels (choix des fournisseurs, interface de sécurité)
- Contrats avec les sous-traitants (clauses d'engagement de responsabilité)
- Plan de migration des applications critiques
- Validation et audit des programmes
- Qualité et pertinence des données
- Plan d'assurance sécurité

Type d'Applications

1. Systèmes d'Exploitation
 - Windows W. Server, Linux, Mac OS (ordinateurs, serveurs)
 - Android, iOS (OS de téléphones portables)
 - Real Time OS (IoT, systèmes embarqués)
2. Applications classiques
 - Office software (Open Office, Microsoft Office)
 - Matlab
3. Applications métier
 - Unity, TIA Portal...
4. Logiciels « Faits-maison »
 - ???

Exemple

- La Direction d'une entreprise demande pour objectifs que soit assurées :
 - La disponibilité des moyens de communication du siège situé à Paris
 - La disponibilité des moyens de communication de l'usine à Grenoble
 - La disponibilité des moyens de communication avec le sous-traitant ABC
 - La disponibilité de la messagerie
 - La production
 - Le confidentialité et l'intégrité des secrets de fabrication
 - La mise à jour du programme de production

Déontologie

- Etudiants
=> signer une charte informatique
- Administrateur Réseau/Systèmes
=> responsabilité
- L'utilisation des méthodes
décrites dans ce cours engage la
responsabilité des utilisateurs !

TD Analyse de risques

- Par groupe de 4, prendre un exemple d'entreprise
 - Société accueillant un alternant
 - Société où vous allez effectuer votre stage
- Effectuer une analyse des risques informatiques
 - Confidentialité
 - Intégrité
 - ...
- Faire des hypothèses pour chacun de ces risques
 - Fréquence d'occurrence
 - Conséquences (gravité)
- Essayer de mettre un coût face à ces risques

Références bibliographiques

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