R5.cy.12-Norme Normes, standards et analyse de risque

Année 2024-25

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

2. Analyse de risque

Année 2024-25

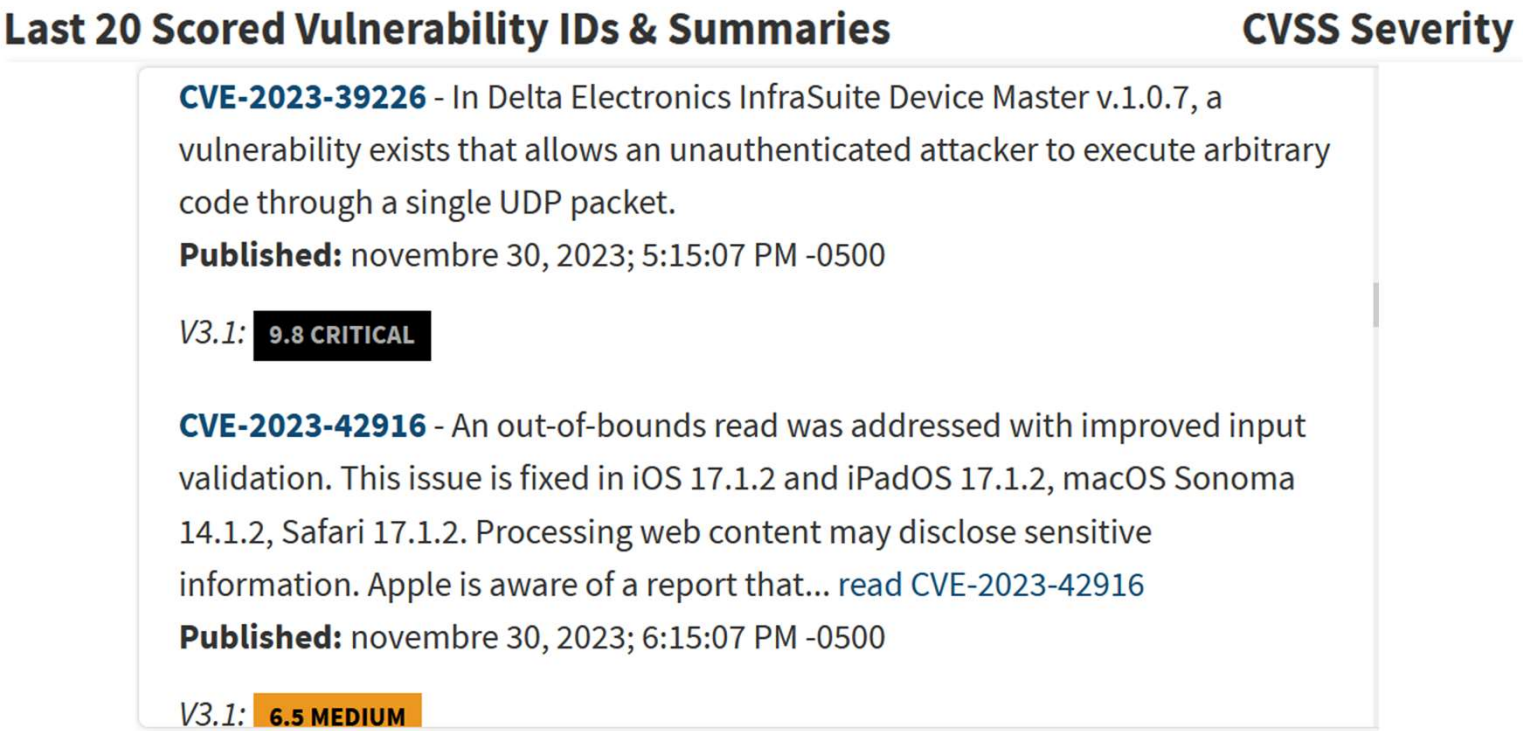
jean-marc.thiriet@univ-grenoble-alpes.fr

Contexte : types de cibles

- Cible opportune
  - Au hasard : détecté par les pirates à la recherche de machines ou serveurs peu protégés
  - Que faire : mettre à jour l'infrastructure avec les correctifs des systèmes
  - Tester son système (essayer de trouver des failles)
- Cible de choix
  - Cible précise : intérêt stratégique de l'entreprise pour des tiers…

Informations sur les vulnérabilités

- Les risques en termes de sécurité autour des réseaux et des systèmes d'information
- https://nvd.nist.gov/



ALERTES DE SÉCURI

Informations sur les vunérabilités:
https://www.cert.ssi.gouv.fr/

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

23 octobre 2023	CERTFR-2023-ALE-012	[MàJ] Vulnérabilité dans Citrix NetScaler ADC et NetScaler Gateway	Alerte en cours	
17 octobre 2023	CERTFR-2023-ALE-011	[MàJ] Multiples vulnérabilités dans Cisco IOS XE	Alerte en cours	
2 octobre 2023	CERTFR-2023-ALE-010	Multiples vulnérabilités dans Exim	Alerte en cours	
17 juillet 2023	CERTFR-2023-ALE-007	[MàJ] Vulnérabilité dans Zimbra Collaboration Suite	Alerte en cours	
19 juillet 2023	CERTFR-2023-ALE-008	[MàJ] Vulnérabilité dans Citrix NetScaler ADC et NetScaler Gateway	Alerte en cours	

VOIR TOUTES LES ALERTES »

En cas d'incident, les bons réflexes en cas d'intrusion sur un système d'information sont à retrouver ici.

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

26 octobre 2023	CERTFR-2023-CTI-009	Campagnes d'attaques du mode opératoire APT28 depuis 2021
23 octobre 2023	CERTFR-2023-CTI-008	Synthèse de la menace ciblant les collectivités territoriales
18 septembre 2023	CERTFR-2023-CTI-007	FIN 12 : Un groupe cybercriminel aux multiples rançongiciels
18 septembre 2023	CERTFR-2023-CTI-006	Démantèlement du botnet Qakbot
30 août 2023	CERTFR-2023-CTI-005	Grands évènements sportifs – Évaluation de la menace 2023

Informations sur les vunérabilités:
https://www.cert.ssi.gouv.fr/

AVIS DE SÉCURITÉ

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

6 décembre 2023	CERTFR-2023-AVI-1001	Vulnérabilité dans Atlassian Confluence
6 décembre 2023	CERTFR-2023-AVI-1000	Multiples vulnérabilités dans Progress MOVEit Transfer
6 décembre 2023	CERTFR-2023-AVI-0999	Vulnérabilité dans ElasticSearch pour Hadoop
6 décembre 2023	CERTFR-2023-AVI-0998	Multiples vulnérabilités dans Google Chrome
6 décembre 2023	CERTFR-2023-AVI-0997	Vulnérabilité dans SolarWinds Serv-U
5 décembre 2023	CERTFR-2023-AVI-0996	Vulnérabilité dans TheGreenBow VPN Client
5 décembre 2023	CERTFR-2023-AVI-0995	Multiples vulnérabilités dans Google Android
5 décembre 2023	CERTFR-2023-AVI-0994	Multiples vulnérabilités dans SonicWall SMA

VOIR TOUS LES AVIS »

INDICATEURS DE COMPROMISSION

Les indicateurs de compromission, qualifiés ou non par l'ANSSI, sont partagés à des fins de préventions

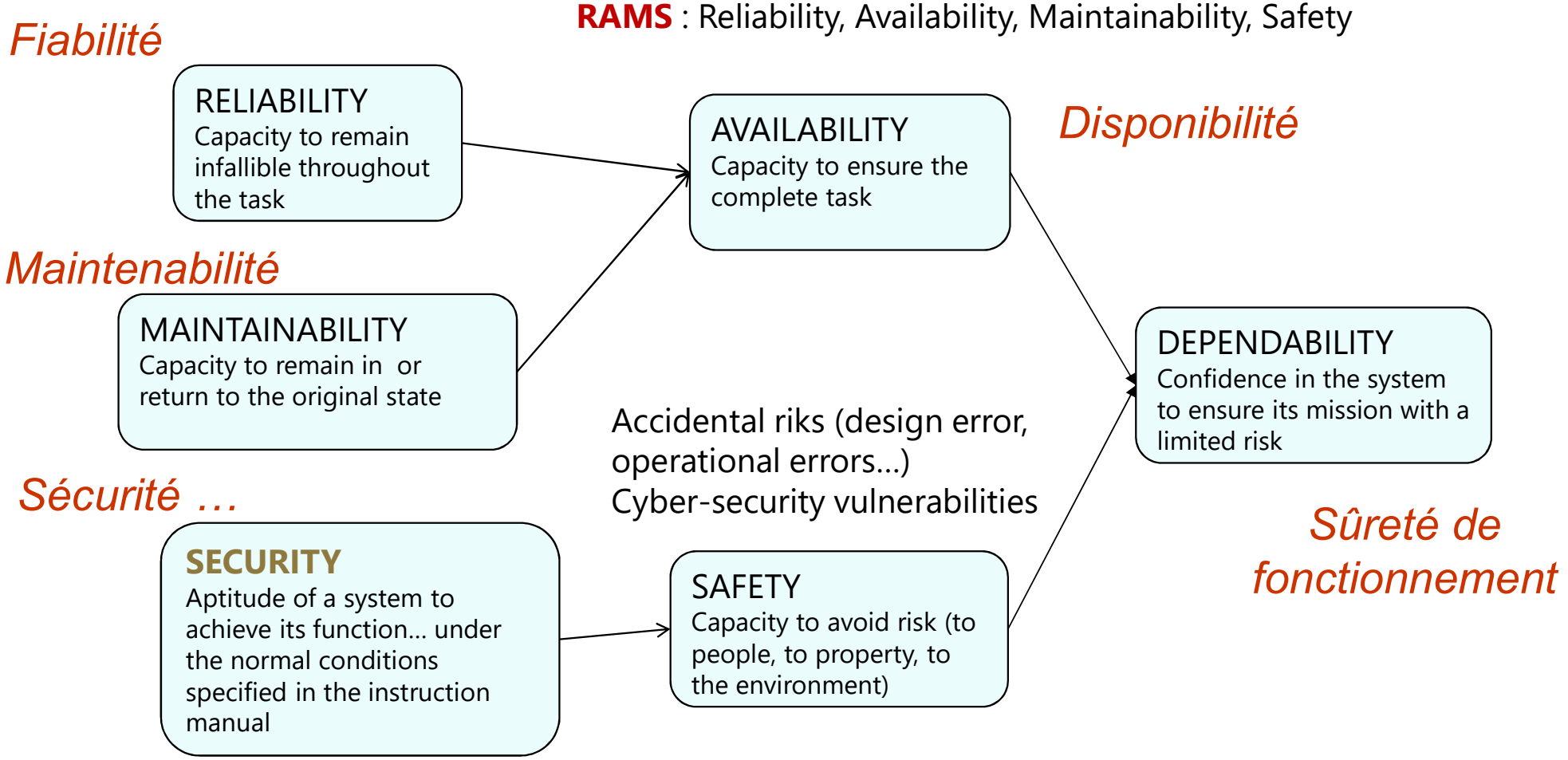
18 septembre 2023	CERTFR-2023-IOC-001	FIN 12 : Un groupe cybercriminel aux multiples rançongiciels
12 juillet 2022	CERTFR-2022-IOC-001	Feed MISP public
6 décembre 2021	CERTFR-2021-IOC-005	Campagnes d'hameçonnage du mode opératoire d'attaquants Nobelium
3 novembre 2021	CERTFR-2021-IOC-004	Identification d'un nouveau groupe cybercriminel : Lockean

Introduction à la sûreté de fonctionnement, principes de sécurité

- Sûreté de fonctionnement
- La Sécurité : définition
- Principes de sécurité

Dependability

RAMS : Reliability, Availability, Maintainability, Safety



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*.

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

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 ≤ à un certain %age d'une valeur de référence
    - ex 2 : la perte, ou la destruction irrémédiable de données stratégiques pour l'entreprise

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

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

Eléments 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.).

Eléments 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 1/3
    - 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: 70% * 1/3 = 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)

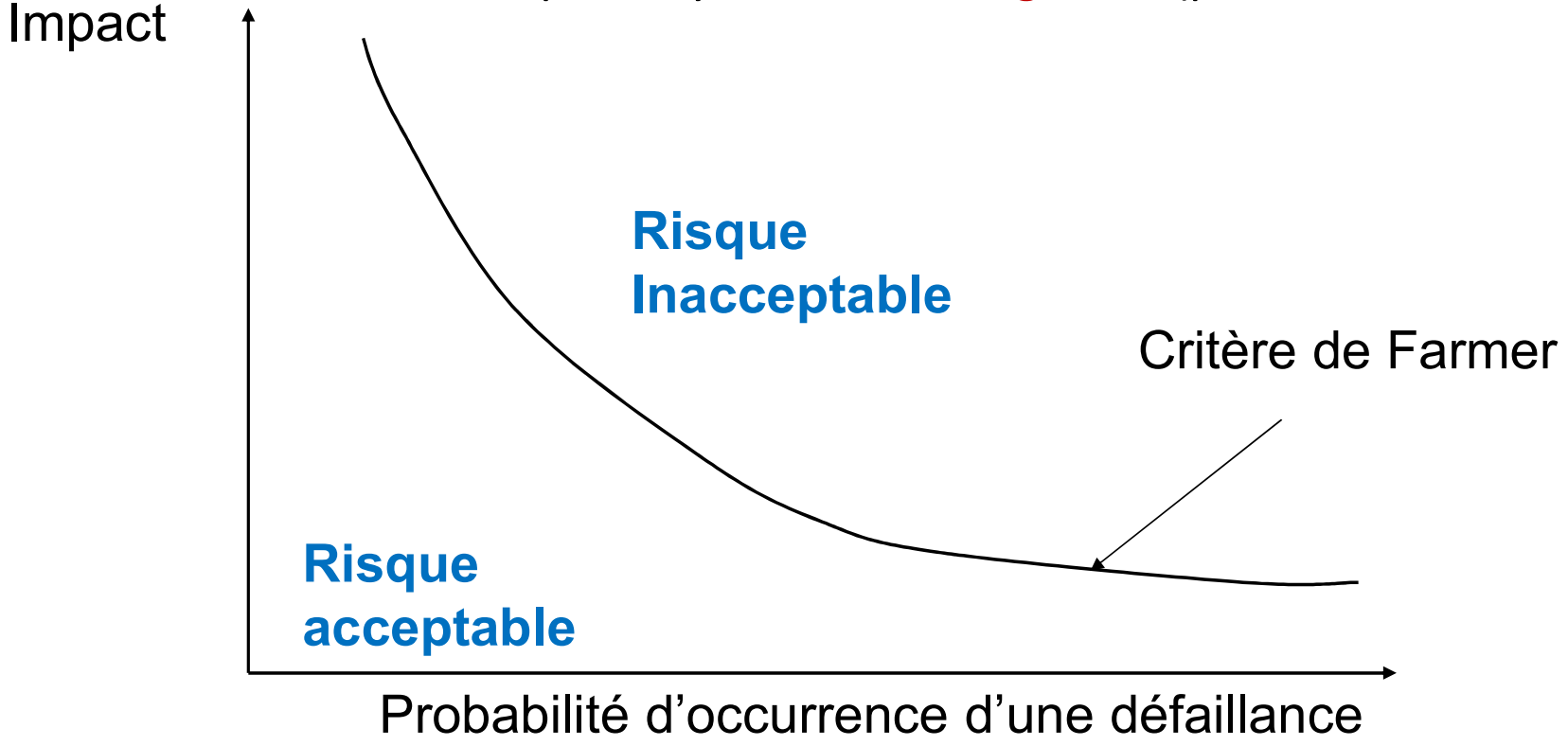
  - La plupart du temps, plusieurs contrôles sont utilisés pour protéger un actif.
  - Ex: si la menace est qu'un employé puisse voler des secrets commerciaux et les vendre à la concurrence
  - Pour contrer cette menace, nous pouvons :
    - mettre en œuvre une politique de classification des informations,
    - surveiller le courrier électronique sortant,
    - interdire l'utilisation de dispositifs de stockage portables

Origines des risques

- Risques accidentels
  - Risques matériels accidentels (incendie, explosion, chocs, collision, inondation …)
  - Vol et sabotage
  - Panne et dysfonctionnement de matériel ou de logiciel de base
- Risques d'erreur
  - Erreur de saisie, de transmission
  - Erreur d'exploitation
  - Erreur de conception et de réalisation
- Risques de malveillance
  - Fraude, sabotage immatériel
  - Indiscrétion (jusqu'à l'espionnage industriel ou commercial), détournement d'informations
  - Détournement de logiciels (piratage)
  - Grève, départ de personnel stratégique

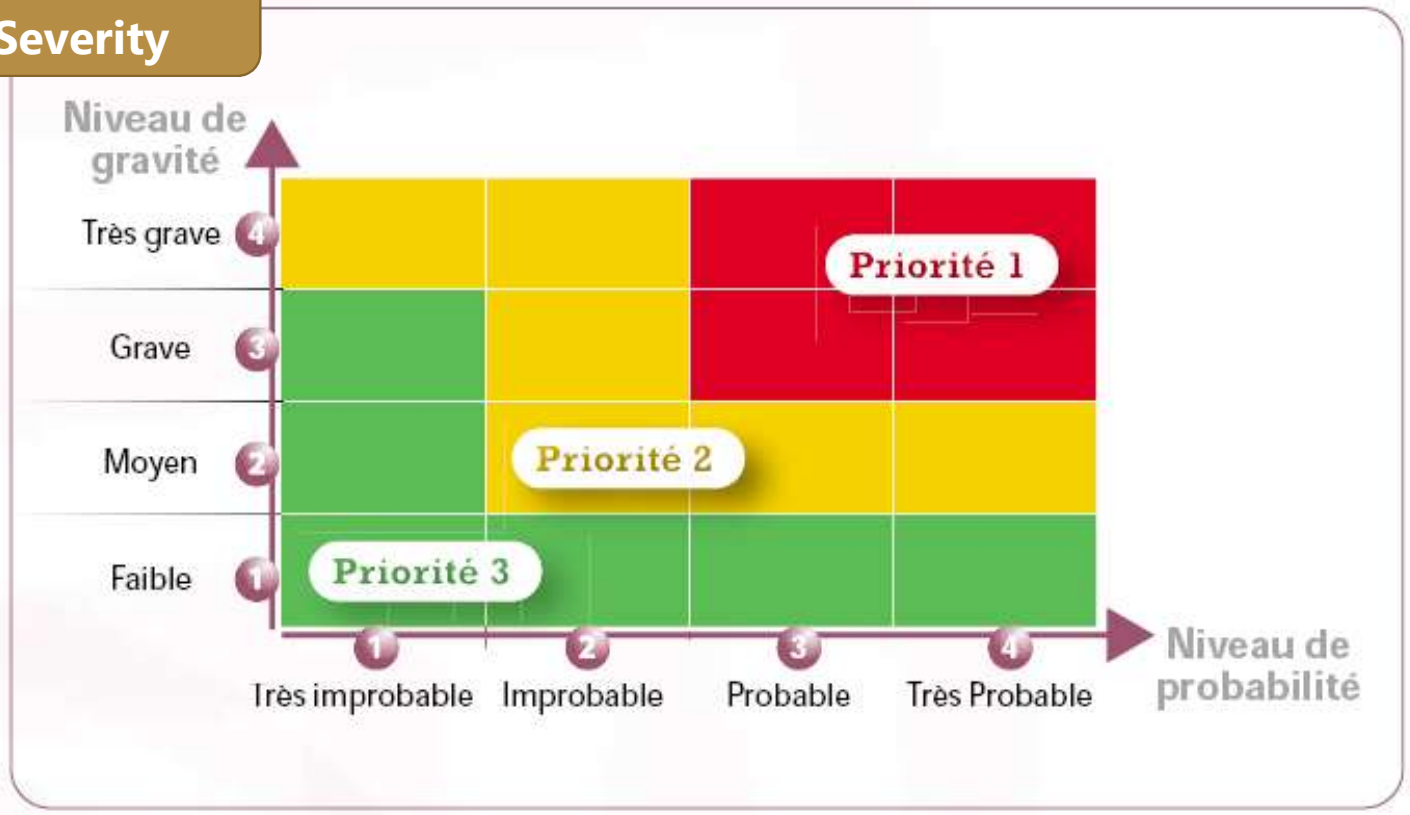
Loi Gravité-Probabilité

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



Evaluation des risques, évaluation de la gravité

Gravité = Severity



Exemple

Danger (cause)	Situation dangereuse	Evénement dangereux	Risque de …	Conséquence	Gravité	Probabilité	Priorités	Observations
Eclatement d'un pneu								

Exemple

Danger (cause)	Situation dangereuse	Evénement dangereux	Risque de …	Conséquence	Gravité	Probabilité	Priorités	Observations
Eclatement d'un pneu	Dérapage du véhicule	Une vis dans le pneu	Accident	Mort des passagers	4 (haut)	1 (bas)	2 (int.)	Avoir une roue de secours

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

Les principes de sécurité

- Sécurité physique
- Sécurité de l'exploitation
- Sécurité logique
- Sécurité applicative
- => Checklist !

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…)

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

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…)

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

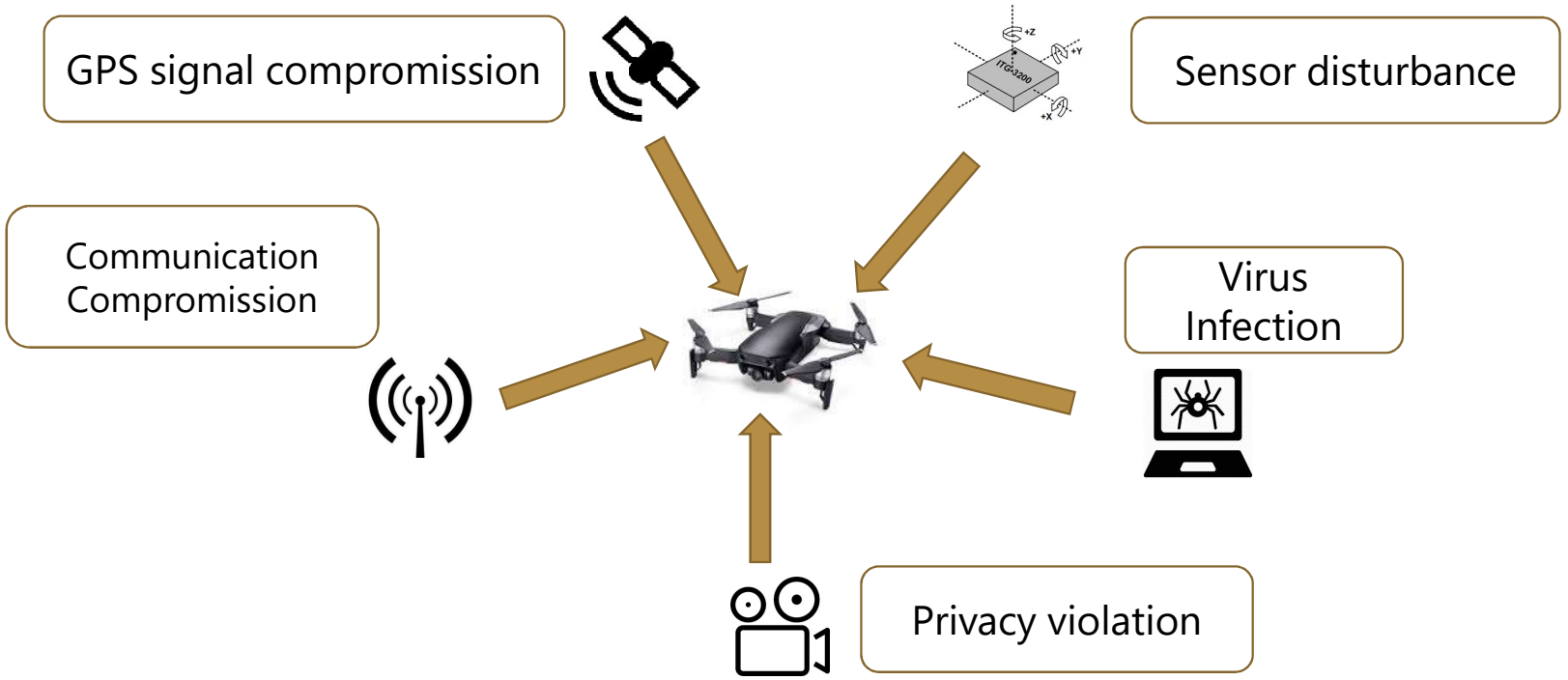
1. Systèmes d'Exploitation
   - Windows W. Server, Linux, Mac OS (ordinateurs, serveurs)
   - Android, iOS (OS de téléphones portables)
   - Real Time OS (IoT, systèmes embarqués)
2. Applications classiques
   - Office software (Open Office, Microsoft Office)
   - Matlab
3. Applications métier
   - TIA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

Cyber-security of flying drones

Vulnerability of the drone:



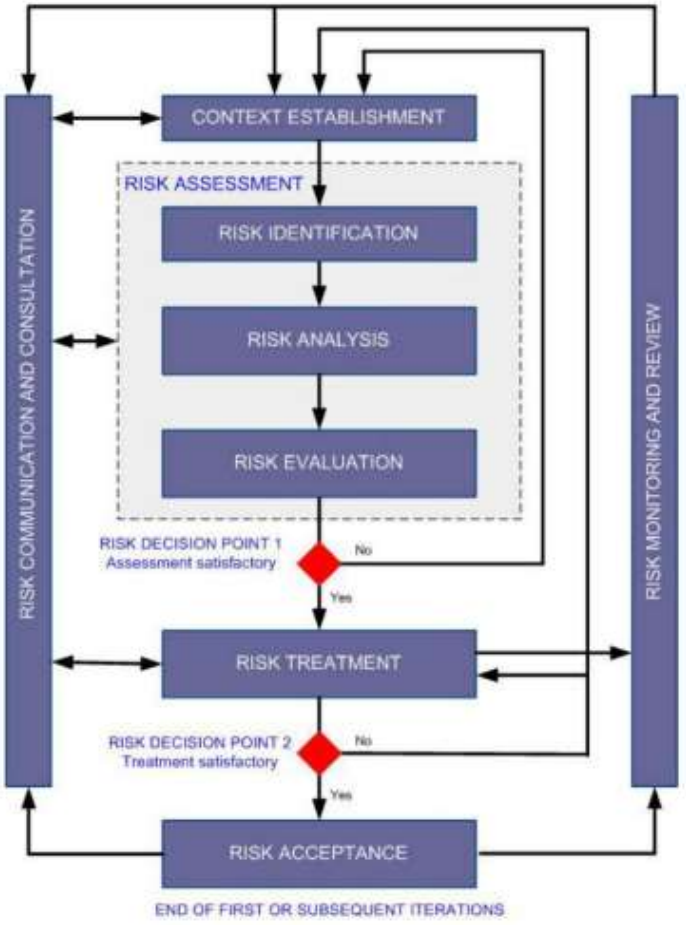
Need of a methodology to get a cartography of the drone security in a systematic way and to ensure completude

Ex: methodologies in the industrial domain

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

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

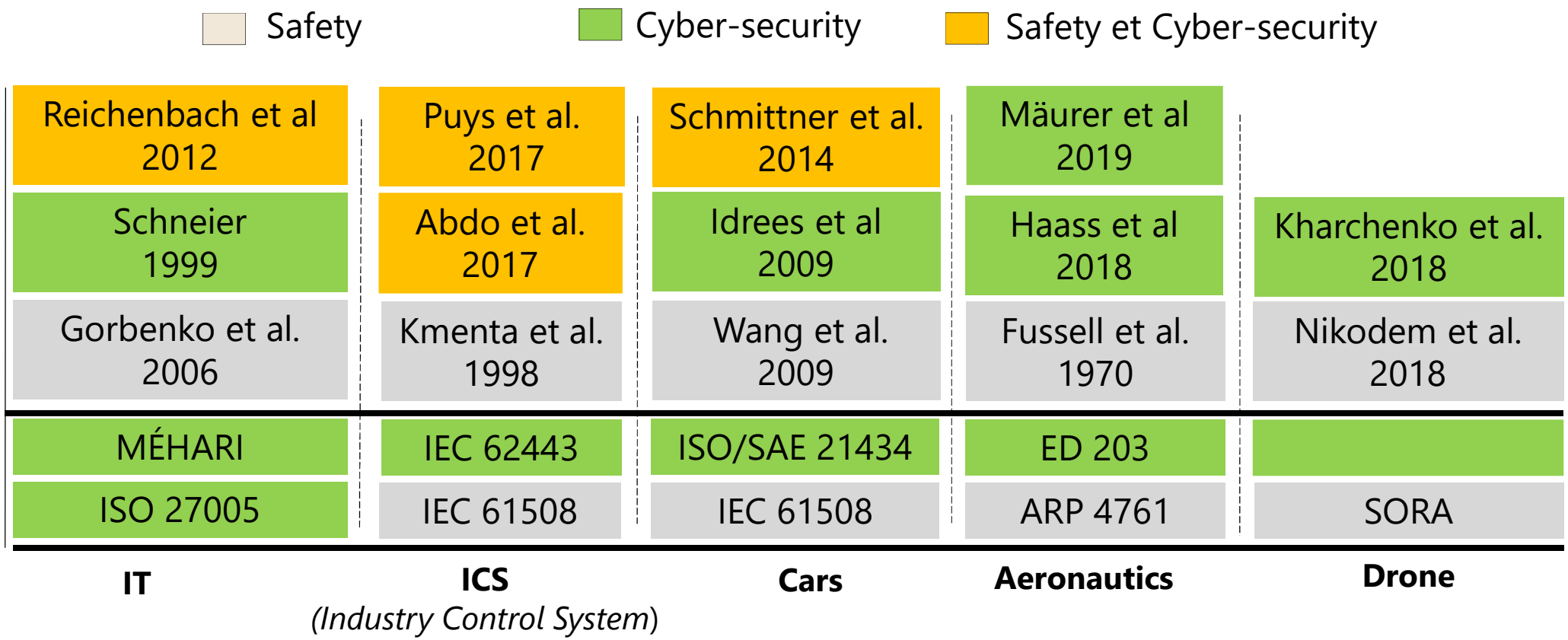
- **ED202A/DO326A Standard:**
  - Avionics security
  - During the processus of aircraft development



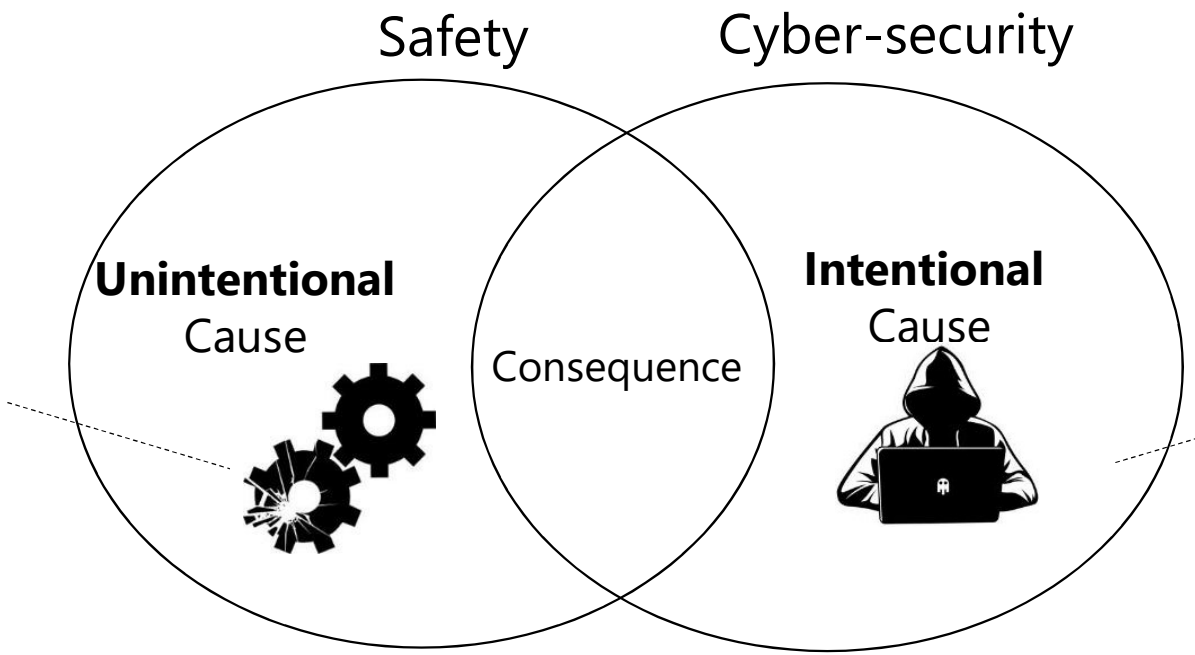
Generic cyber-security approach

Specific security standards

Risk Assessment: Safety and Cyber-security



Safety and Cyber-security



No one wants the "consequences" to happen

Someone wants the "consequences" to happen

Different **causes**, same **consequences**

Différences entre sûreté et sécurité

« Sûreté » et « Sécurité » ont des significations différentes en fonction du contexte. L'interprétation de ces expressions peuvent varier en fonction de la sensibilité de chacun ou des contextes normatifs.

Sûreté

Protection contre les dysfonctionnements et accidents involontaires

Exemple de risque : saturation d'un point d'accès, panne d'un disque, erreur d'exécution, etc.

Quantifiable statistiquement (ex. : la durée de vie moyenne d'un disque est de X milliers d'heures)

Parades : sauvegarde, dimensionnement, redondance des équipements…

Sécurité

Protection contre les actions malveillantes volontaires

Exemple de risque : blocage d'un service, modification d'informations, vol d'information

Non quantifiable statistiquement, mais il est possible d'évaluer en amont le niveau du risque et les impacts

Parades : contrôle d'accès, veille sécurité, correctifs, configuration renforcée, filtrage…

Références

- S. Ghernaouti – Cyberssicurité : Analyser les risques, Mettre en œuvre les solutions
- J.F. Aubry, Nicolae Brinzei – Systems Dependability Assessment, Modeling with Graphs and Finite State Automata, Wiley, Fév. 2015.
- J.C. Laprie & al. – Guide de la sûreté de fonctionnement – Cépaduès, 1995.
- A. Villemeur – *Sûreté de fonctionnement des systèmes industriels* – Editions Eyrolles, Paris, 1988.
- C. Davis, M. Schiller, K. Wheeler - *IT Auditing: using control to protect assets* – 2007, Mc Graw Hill
- Cours Stéphane Mocanu, ENSE3, Industrial Communication Labs, 2016
- Cours Emmanuel Simeu, Polytech Grenoble, Supervision
- Patrick Monassier, cours CESI 2009, Informatique industrielle.
- Pierre Bonnet, cours Université de Lille, Introduction à la supervision, 2010
- EPFL, Industrial Automation course
- P_RAYMOND_BTS_MAI_Les_API
- Cours de C. Bulfone
- Cours de F. Lombardi
- Transmissions et réseaux, S. Lohier & D. Présent, Dunod, Paris, 2003.
- Cours Stéphane Mocanu, ENSE3, Industrial Communication Labs, 2016
- Cours Emmanuel Simeu, Polytech Grenoble, Supervision
- Cours de Blaise Conrard, Polytech Lille.
- Patrick Monassier, cours CESI 2009, Informatique industrielle.
- Pierre Bonnet, cours Université de Lille, Introduction à la supervision, 2010
- G. Boujat et P. Annaya, Automatique industrielle en 20 fiches, Dunod, 2007
- W. Bolton, Automates programmables industriels, Dunod, 2015.
- Duc Tran Trung , Cybersecurity risk assessment for Unmanned Aircraft System, PhD, Univ. Grenoble Alpes
- 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
- Cybersecurity risk assessment for Unmanned Aircraft Systems, TRAN Trung Duc, Thèse UGA, 2021.

Références

https://www.technologuepro.com/cours-automate-programmable-industriel/Les-automates-programmables-industriels-API.htm

http://www.est-usmba.ac.ma/coursenligne/GE-S2-M8.1-Automatismes%20logiques%20Industriels-CRS-El%20Hammoumi.pdf

http://colasapoil.free.fr/HEI/HEI5%20TC/Maintenance/h5_tc_maintenance_coursv2_coursv2_1783.pdf

https://www.cours-gratuit.com/cours-divers/cours-sur-les-definitions-methodes-et-operations-de-la-maintenance

https://www.manager-go.com/logistique/organisation-de-la-logistique.htm

https://www.lecoindesentrepreneurs.fr/logistique-entreprise/
https://d1n7iqsz6ob2ad.cloudfront.net/document/pdf/5346e085efe6e.pdf

https://www.icours.com/cours/economie/la-production

https://perso.imt-mines-albi.fr/~fontanil/THESE/5_Partie1_p13_43.pdf

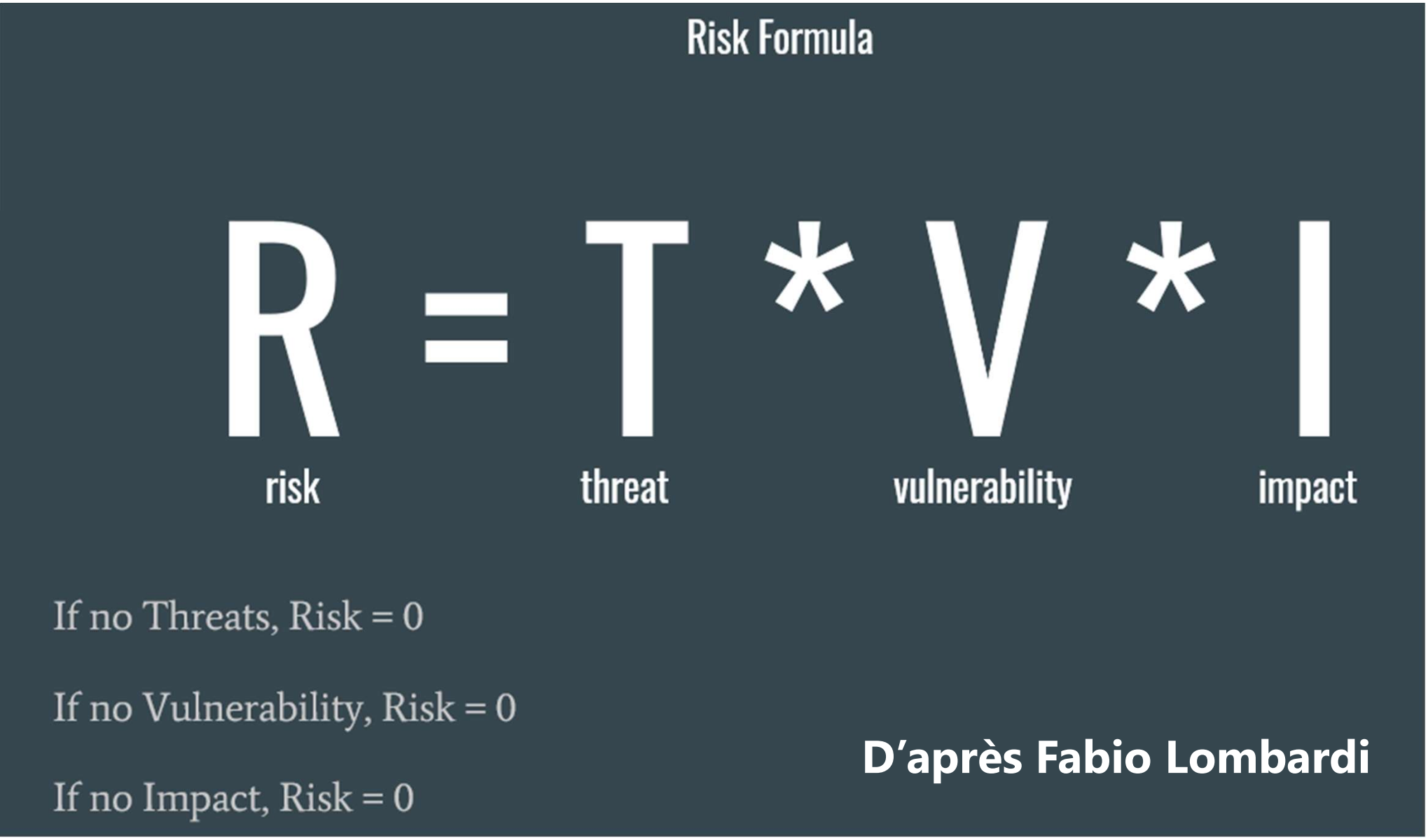
jean-marc.thiriet@univ-grenoble-alpes.fr

Merci pour votre attention

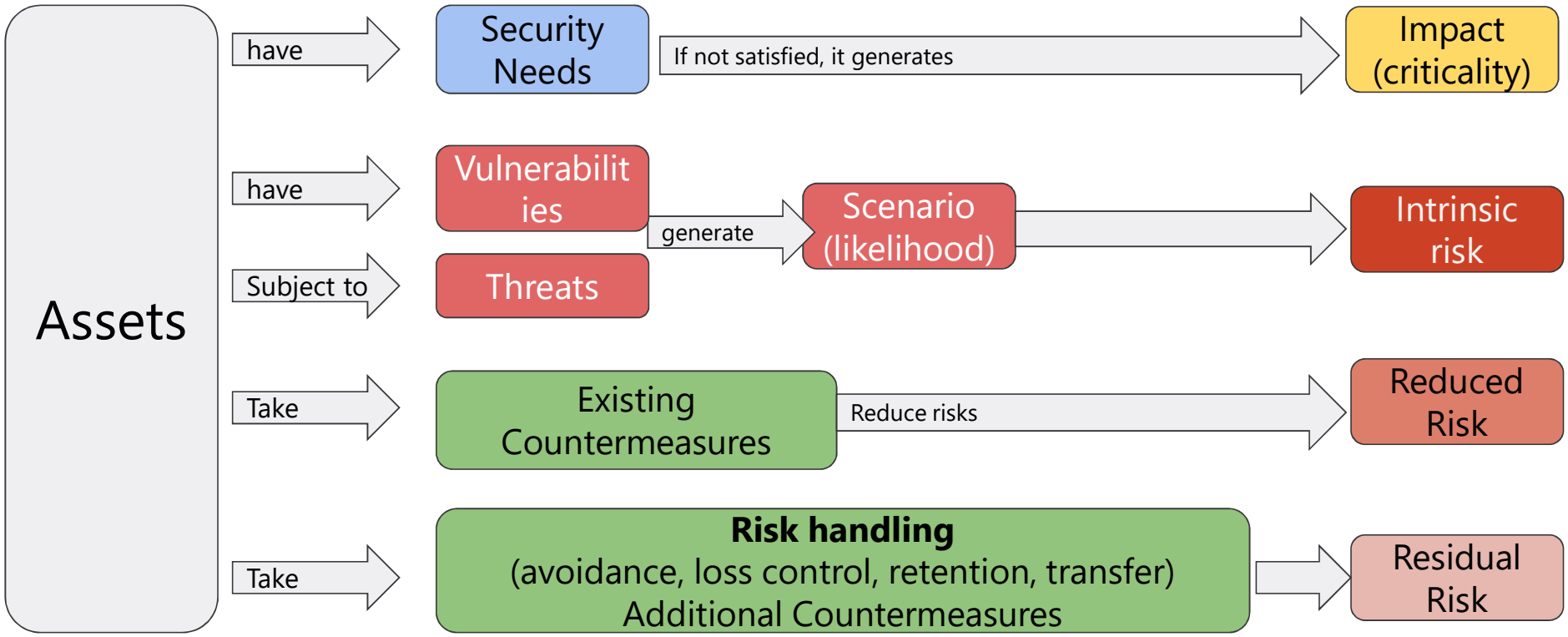
Merci pour votre attention

Université Grenoble Alpes

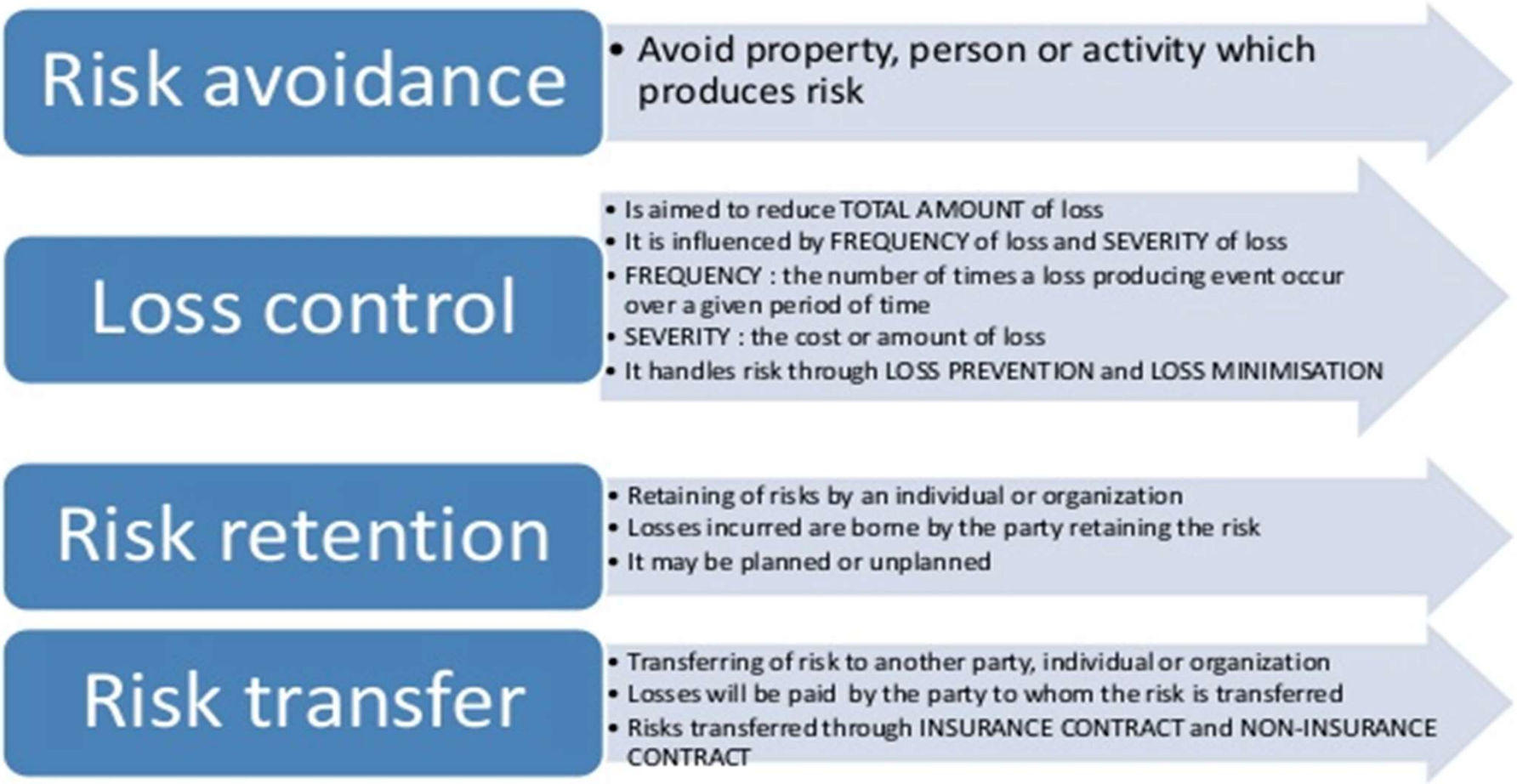
Merci pour votre attention


Risk Formula
R = T * V * I
risk
threat
vulnerability
impact
If no Threats, Risk = 0
If no Vulnerability, Risk = 0
If no Impact, Risk = 0
D'après Fabio Lombardi

Risk evaluation and handling

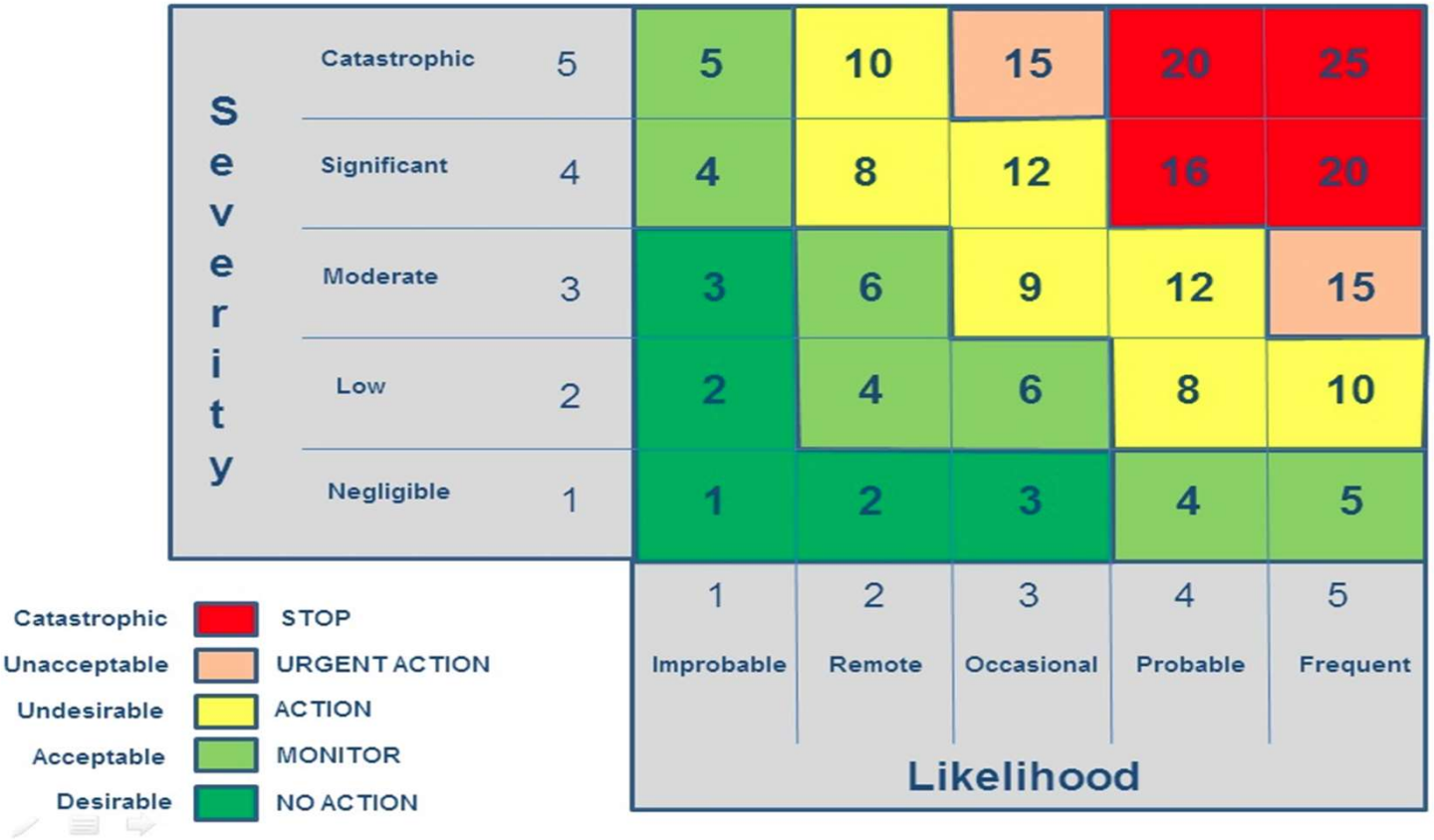


Risk handling methods



Risk Mapping

Risk Rating = Likelihood x Severity



Risk Mapping

IMPACT	Risk Management Actions		
Significant • Financial Loss > $5MM • Stakeholder faith impacted and lasts > 18 months • Isolated or Multiple Loss of Life • Multiple events of fine, fraud or legal action • Complete system crash with loss of critical data • Inability to recruit, retain staff to operate • Labour disruption that impacts graduation	Considerable Management Required	Must manage and monitor risks	Extensive management essential
Moderate • Financial Loss < $5 MM • Stakeholder faith impacted and lasts 6-12 months • Significant injury to one or more • Isolate incidents of fine, fraud, or legal action • System crash during a peak period • Difficulties in recruiting and retaining staff • Labour disruption that impacts operations of any duration	Risks may be worth accepting with monitoring	Management effort worthwhile	Management effort required
Minor • Financial Loss < $500,000 • Stakeholder faith impacted and lasts < 6 months • Isolated injury • Civil or criminal action threatened • System off-line periodically during non-peak periods	Accept risks	Accept but monitor risks	Manage and monitor risks
	Low > 36 months	**Medium** 18 to 36 months	**High** 12 to 18 months
	LIKELIHOOD		

TD Analyse de risques

- Par groupe de 4, prendre un exemple d'entreprise
  - Société accueillant un alternant
  - Société où vous allez/avez effectuer/ée votre stage
- Effectuer une analyse des risques informatiques
  - Confidentialité
  - Intégrité
  - …
- Faire des hypothèses pour chacun de ces risques
  - Fréquence d'occurrence
  - Conséquences (gravité)
- Définir une priorité d'actions à mener (priorités)

Rendu attendu

- Presentation (as slides) to be achieved next class: 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