Architecture Software - Cybersécurité

Eric Silva

Spring 2025 – Micro 371

Eric Silva

Plan du cours

N°	Prof	Type	Dates	Thème
1	SI	Cours	18/02/2025	Gestion de projet et Organisation du cours
2	SI	Cours	25/02/2025	Patrons de conception et styles d'architecture
3	SF	Cours	04/03/2025	DevOps: Intégration Continue (slides et exercices)
4	SF	Cours	11/03/2025	DevOps: Intégration Continue
5	ES	Cours	18/03/2025	Evaluation des risques et définitions des fonctions de sécurité
6	ES	Cours	25/03/2025	Ecriture d'exigences, du système au logiciel, spécification des tests
7	ES	TP	01/04/2025	TP1 - Spécification des exigences du projet
8	SF	TP	08/04/2025	TP2 - Mise à jour du gitlab board en fonction des exigences
9	SF	Cours	15/04/2025	DevOps: Automatisation des tests
			22/04/2025	Vacances
10	SF	TP	29/04/2025	TP3 - Spécifications et Réalisation des tests automatisés
11	ES	Cours	06/05/2025	Processus de développement et toolchain
12	ES	Cours	13/05/2025	Cybersécurité et Communication
13	ES	Cours	20/05/2025	Tests statiques de code
14	ES	TP	27/05/2025	TP4 - Tests statiques et finalisation du projet

Plan du cours d'aujourd'hui

- Introduction à la cybersécurité et aux règlements en vigueur
  - Cyber Resilience Act (CRA)
  - Radio Equipment Directive (RED)

- Threat Analysis & Risk Assessment (TARA)
  - Comprendre le système
  - Identifier les conséquences des attaques
  - Evaluer la faisabilité des attaques
  - Calculer les valeurs de risque et définir les actions à entreprendre

- Case study for self learning

Les systèmes sont des proies vulnérables

La sécurité par l'obscurité est toujours d'actualité et la sécurité elle est principalement considérée comme un centre de coûts.

Les systèmes historiques ont généralement été développés sans tenir compte de la cybersécurité.

La connectivité, l'architecture et la complexité technologique des systèmes augmentent rapidement.

- Les voitures modernes comportent environ 100 millions de lignes de code, qui devraient tripler d'ici 2030.En comparaison, un avion de ligne contient environ 15 millions de lignes de code.

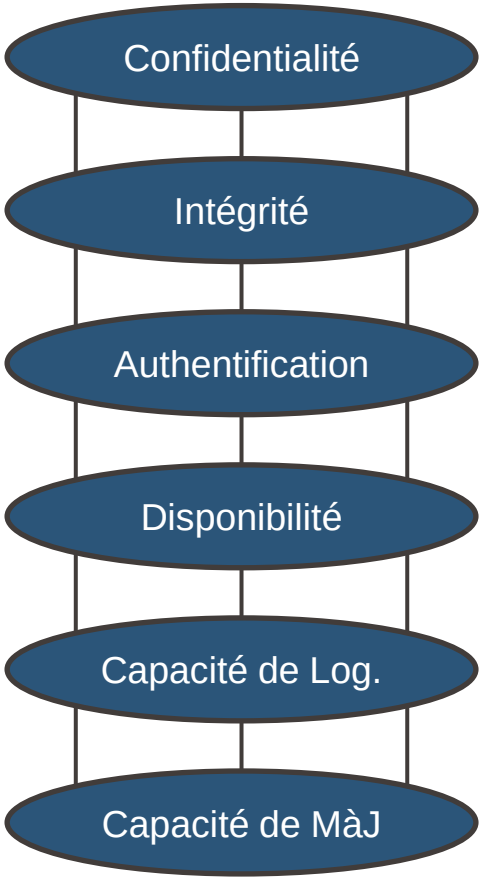
Les systèmes intègrent des fonctions d'automatisation (par exemple, les véhicules automatisés), ce qui accroît la complexité de l'identification des risques ainsi que les conséquences des attaques potentielles.

- Un véhicule connecté génère et consomme environ 20 téraoctets de données toutes les huit heures de conduite.

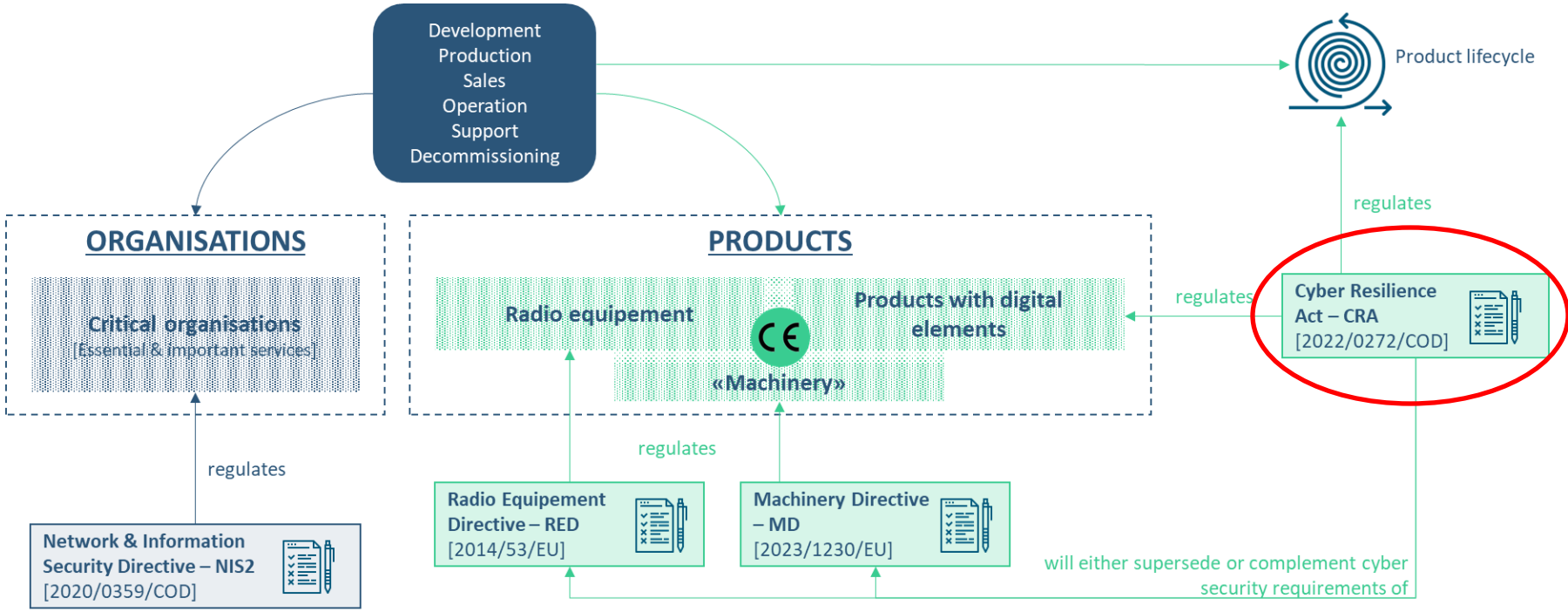
Eric Silva

Une approche pragmatique

- **Approche holistique** - Technologie, processus et personnel
- **Approche basée sur le risque -** Viser un niveau de sécurité raisonnable
- **Défense en profondeur** - Multiplier les barrières de protection
- **Sécurité par conception** - Intégrer la cybersécurité en tant que pilier fondamental de votre organisation et de vos services/produits
- **Soyez réactif ET proactif** - Évaluez et concevez, puis surveillez, réévaluez et réagissez.
- **Penser « en collaboration »** - Le partage de l'information est essentiel.



Une approche pragmatique



Cyber Resilience Act (CRA)

“This regulation applies to any products with digital elements whose intended, or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network.” – CRA [2022/0272/COD], Article 2.1

Entrée en force – 11 décembre 2027
Pénalités – Jusqu’à 15 million d’euros ou 2.5% du revenue annuel (le plus haut des deux)

Cyber Resilience Act (CRA)

“Product with digital elements’ means a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately.” – CRA [2022/0272/COD], Article 3

4 catégories de produits:

- **Produits importants de classe I ou II (voir annexe III)** - remplissant des fonctions essentielles pour la cybersécurité d'autres produits ET/OU remplissant une fonction qui comporte un risque important d'effets néfastes.
- **Produits critiques (voir article 8/annexe IV)** - fonctions d'appui d'entités importantes (NIS2 - 2020/0359/COD), ou considérés comme des éléments clés des chaînes d'approvisionnement.
- **Catégorie par défaut** - tous les autres produits contenant des éléments numériques qui répondent aux définitions générales.

Produits exclus (CRA)

Les « produits » suivants sont exclus du champ d'application du CRA:

- Les dispositifs médicaux professionnels couverts par les règlements (UE) 2017/745 et (UE) 2017/746 ;
- Les véhicules à moteur et leurs remorques, leurs systèmes, composants et unités techniques distinctes, couverts par le règlement (UE) 2019/2144.
- Les systèmes de l'aviation civile et les équipements marins, respectivement régis par les règlements (UE) 2018/1139 et 2014/90/UE.
- Les éléments numériques développés ou modifiés exclusivement à des fins de sécurité ou de défense nationale.

Qu'en est-il des logiciels libres / open-source ?

- Les logiciels libres qui ne font pas partie d'une activité commerciale ne sont pas concernés par le CRA
- **Activité commerciale** : produit ayant un prix défini, support technique, intention de monétiser, l'utilisation prolongée de données personnelles, l'acceptation de dons déraisonnables...

Deux groupes d'exigences (CRA) – Annexe I

Propriétés des produits

Exigences de sécurité liées aux propriétés des produits contenant des éléments numériques

- Approche basée sur le risque pour garantir la présence sur le marché de produits sûrs dès leur conception
- Les produits contenant des éléments numériques doivent être livrés sans vulnérabilité exploitable connue.

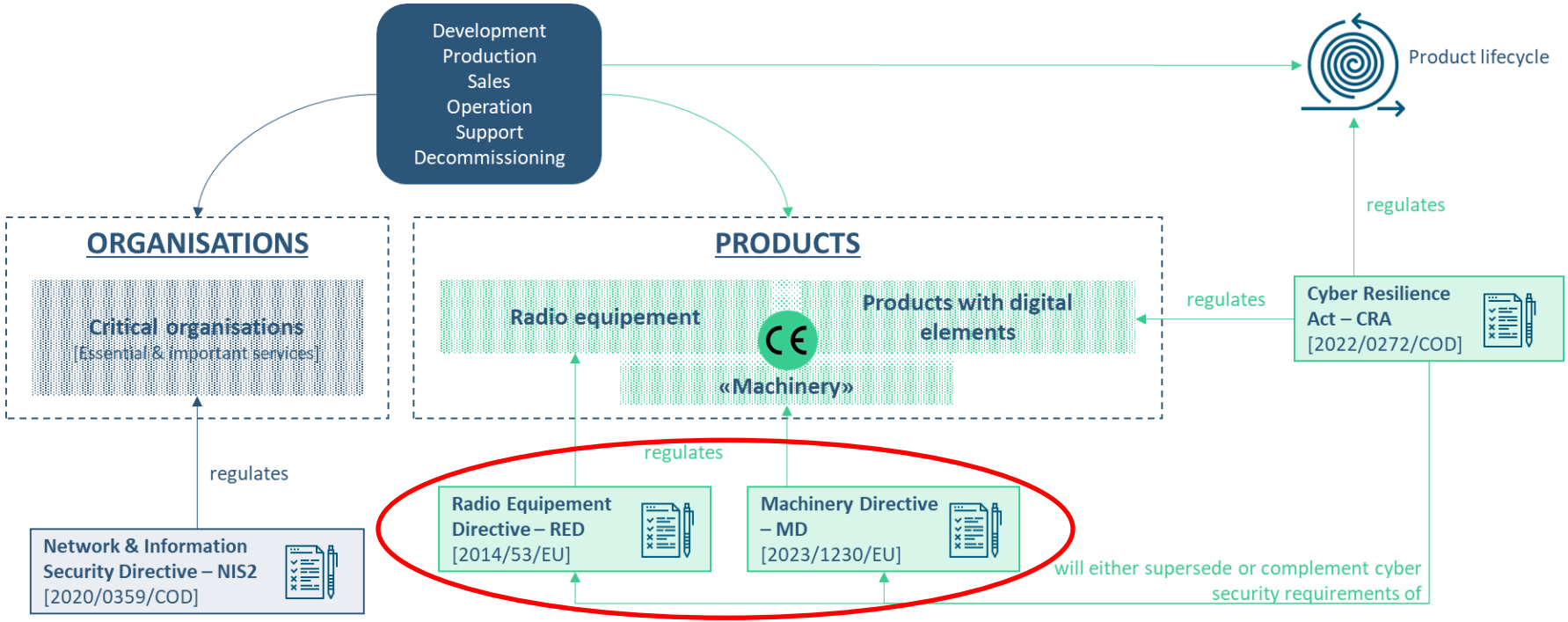
Si applicables, les éléments suivants doivent être démontrés :

- Configuration sécurisée par défaut, y compris la possibilité de réinitialiser le produit à son état d'origine
- Gestion des accès
- Minimisation des données, confidentialité et intégrité (en transit et au repos / stockées)
- Disponibilité des fonctions essentielles (y compris la résilience contre les dénis de service)
- Réduction de la surface d'attaque
- Fonctions de surveillance et de journalisation du système et du produit
- Mise à jour de la sécurité (Capacité)

Gestion des vulnérabilités

- Identifier et documenter les vulnérabilités et les composants contenus dans le produit, y compris en établissant une nomenclature des logiciels (SBOM) en fonction des risques que présentent les produits contenant des éléments numériques, traiter les vulnérabilités et y remédier sans délai, y compris en fournissant des mises à jour de sécurité
- appliquer des tests et des examens efficaces et réguliers de la sécurité du produit contenant des éléments numériques
- une fois qu'une mise à jour de sécurité a été mise à disposition, divulguer publiquement des informations sur les vulnérabilités corrigées
- prévoir des mécanismes de distribution sécurisée des mises à jour pour les produits contenant des éléments numériques afin de garantir que les vulnérabilités exploitables sont corrigées ou atténuées en temps utile
- veiller à ce que, lorsque des correctifs ou des mises à jour de sécurité sont disponibles pour remédier à des problèmes de sécurité identifiés, ils soient diffusés sans délai et gratuitement

Une approche pragmatique



RED – Radio Equipment Directive

Delegated regulation 2022/30/EU (RED) covers devices that can communicate over the internet, whether directly or via other equipment. Radio equipment that may expose sensitive personal data is also in scope

Elle entre en vigueur le 1er février 2022 et devient obligatoire le 1er août 2025, ce qui laisse aux fabricants de dispositifs une période de transition de 42 mois.

RED – Radio Equipment Directive (2)

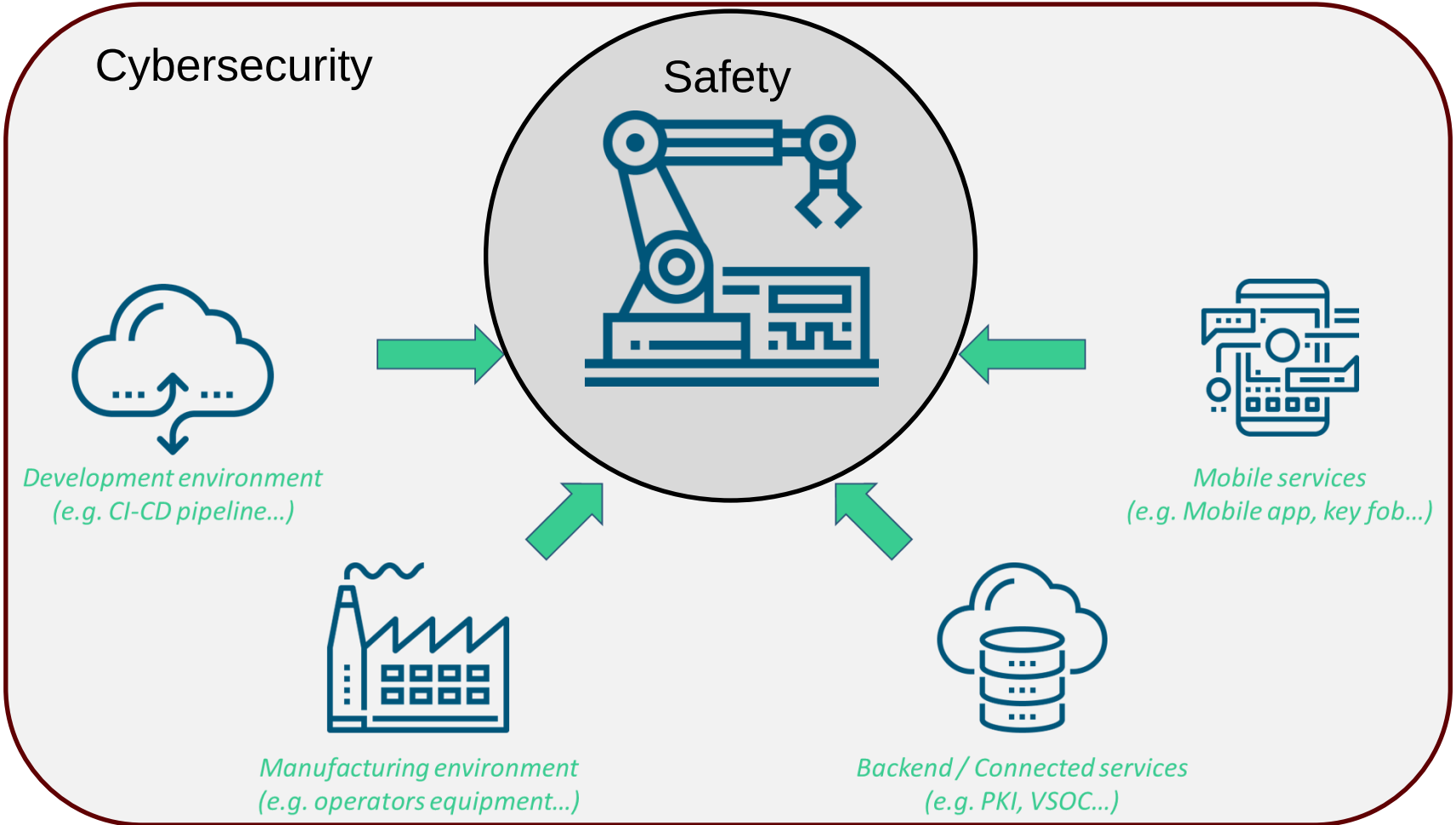
EN 18031-1 – Requirements categories

6.1 [ACM] Access control mechanism
6.2 [AUM] Authentication mechanism
6.3 [SUM] Secure update mechanism
6.4 [SSM] Secure storage mechanism
6.5 [SCM] Secure c
6.6 [RLM] Resilience mechanism
6.7 [NMM] Network monitoring mechanism
6.8 [TCM] Traffic control mechanism
6.9 [CCK] Confidential cryptographic keys
6.10 [GEC] General equipment capabilities
6.11 [CRY] Cryptography communication mechanism

RED – Radio Equipment Directive (3)

Mitigation category		Security requirement / capability / mitigation technique / design principle	S	T	R	I	D	E
Identify		Authentication mechanism (AUM)	X	X			X	
		Confidential cryptographic keys (CCK)	X	X	X			
Protect	Prevent	Access control mechanism (ACM)		X		X	X	X
		Secure storage mechanism (SSM)	X	X		X		X
		Secure communication mechanism (SCM)	X	X	X	X		X
		Encryption (CRY)		X		X		
		Up-to-date software and hardware (GEC-1)	X	X	X	X	X	X
		Configuration of optional services (GEC-3)				X	X	X
		User documentation (GEC-4)				X		
	Limit	Limit exposure (GEC-2 and GEC-5)				X		X
		Input validation (GEC-6)		X		X		
Detect		Network monitoring mechanism (NMM)	X			X	X	
Respond		Traffic control mechanism (TCM)	X	X		X	X	
Recover		Secure update mechanism (SUM)	X	X	X	X	X	X
		Resilience mechanism (RLM)					X	

Le périmètre de la cybersécurité

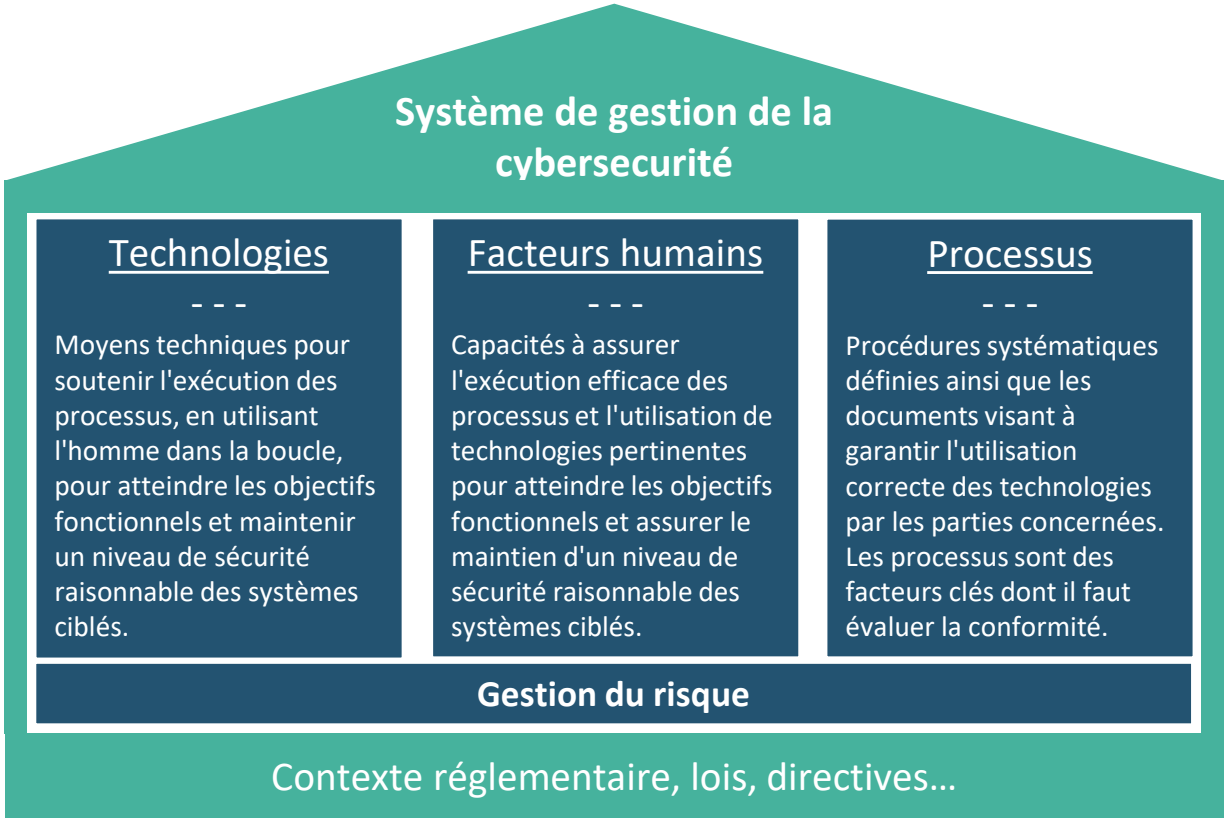


Threat Analysis & Risk Assessment (TARA)

- Quels sont mes actifs clés et quelles sont les conséquences ou les dommages potentiels ?
- Quels sont les vecteurs d'attaque contre mes actifs ?
- Comment et sur quoi investir pour atteindre un niveau de sécurité raisonnable ?
- Quelles mesures de sécurité pour quelle amélioration ?
- Que faut-il surveiller pour garantir des risques résiduels acceptables en permanence ?

... et quels sont les principes de sécurité que nous sommes prêts à suivre ?

Threat Analysis & Risk Assessment (TARA)



Principe de cybersécurité ciblé – Sécurité par défaut

Intégrer des mesures et des contrôles de cybersécurité

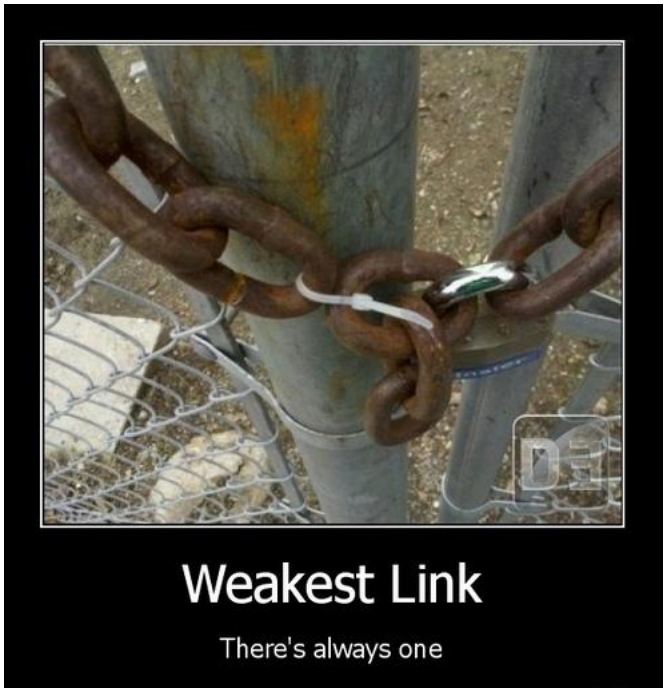
1. Dès le début du développement, fournir/utiliser des capacités de sécurité
2. Où et quand c'est le plus important, et de la manière la plus pragmatique
3. De la manière la plus efficace possible pour réduire les risques à un niveau acceptable
4. En gardant une visibilité actualisée sur l'état actuel des menaces

Eric Silva

Principe de cybersécurité ciblé – Sécuriser le lien le plus faible

En prenant en compte l'ensemble du cycle de vie des actifs

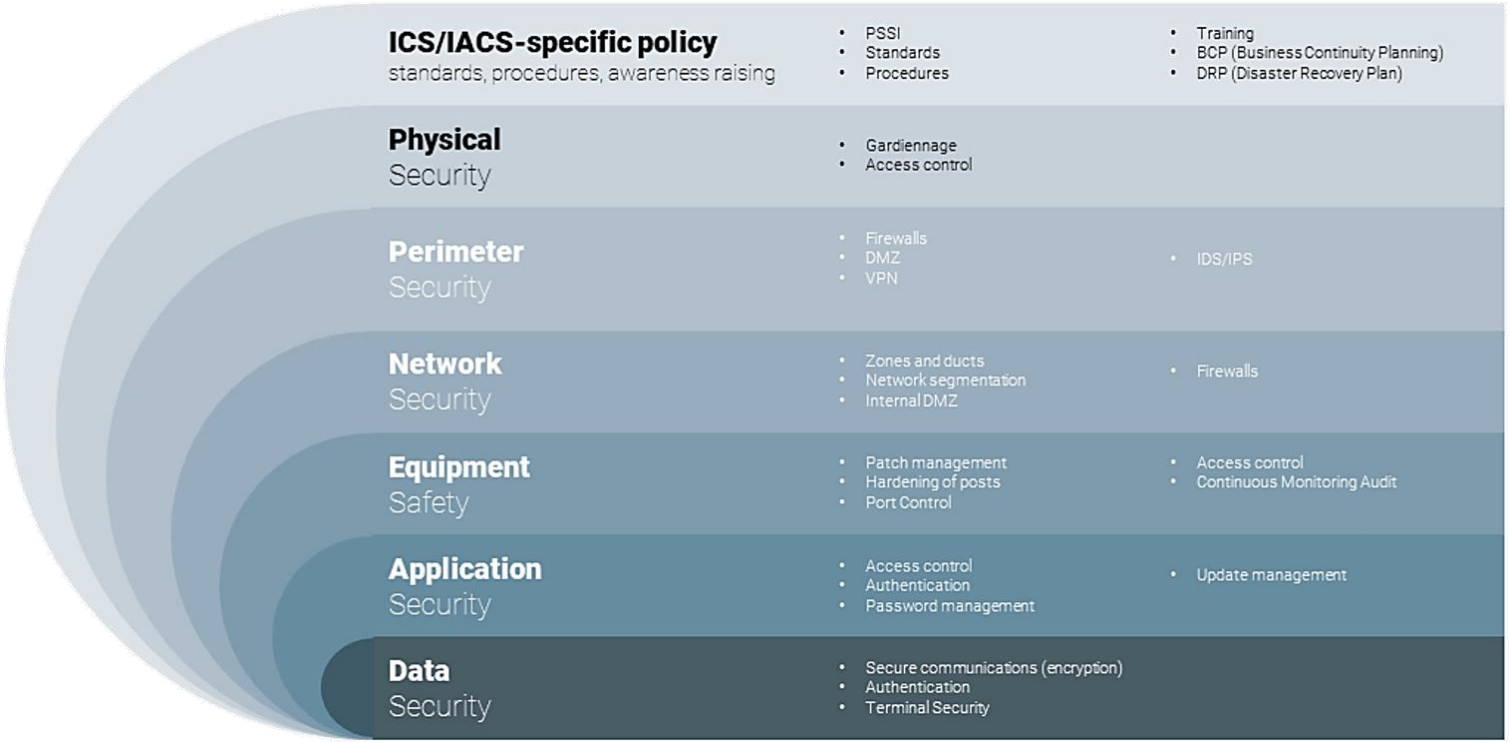
Source: https://sarasch.com/events/the-biggest-threat-to-cybersecurity-is-often-humans/



En prenant en compte l'ensemble de la chaîne d'attaque

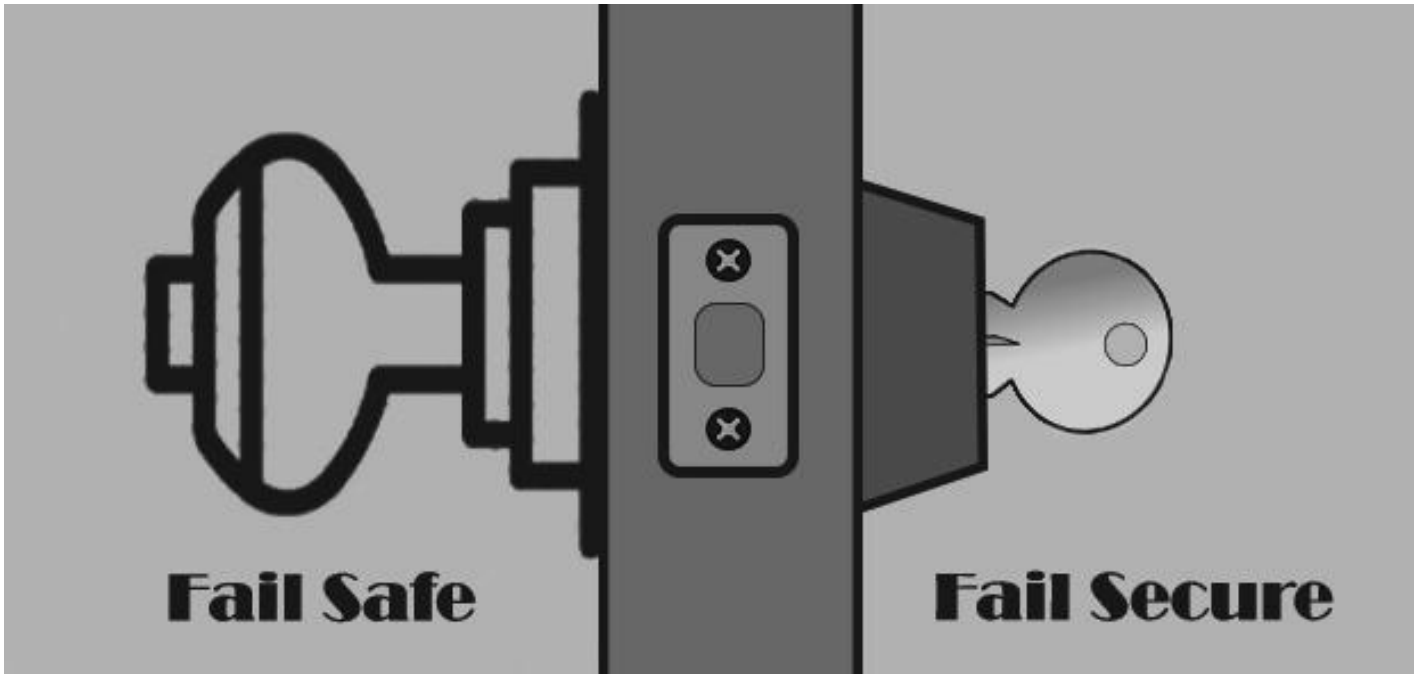
Source: https://jlou.eu/optimisez-votre-azure-2-4-la-securite/

Principe de cybersécurité ciblé – Défense en profondeur



Source: https://www.stormshield.com/news/iec-62443-the-essential-standard-for-industrial-cybersecurity

Principe de cybersécurité ciblé – Implémentation “fail secure”

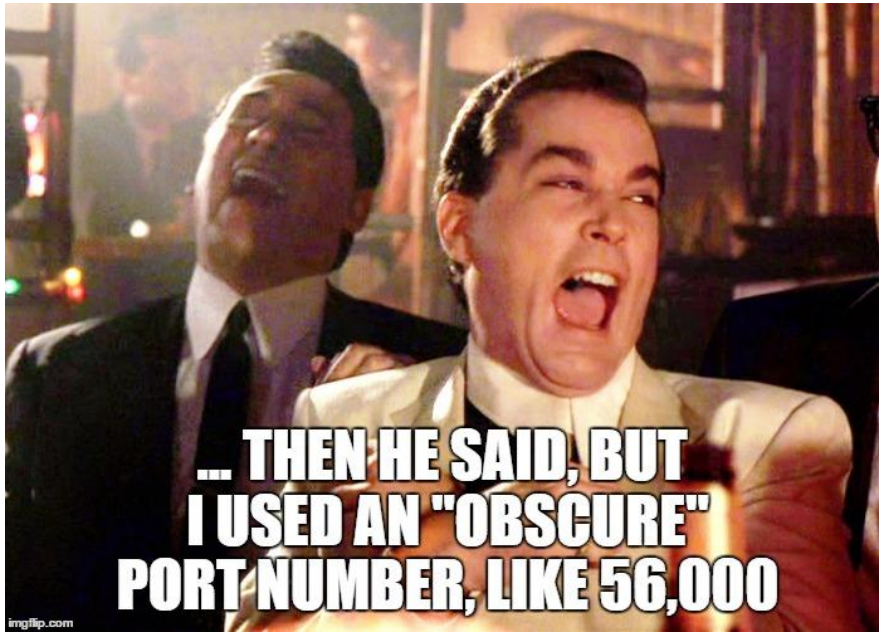


Source: https://softwareg.com.au/blogs/cybersecurity/fail-safe-defaults-fail-secure-cybersecurity

Eric Silva

Principe de cybersécurité ciblé – Toujours pessimiste

Faire au mieux en supposant le pire



Oublier les principes de sécurité par obscurité

Source: https://www.infosys.com/toons/cybersecurity.html

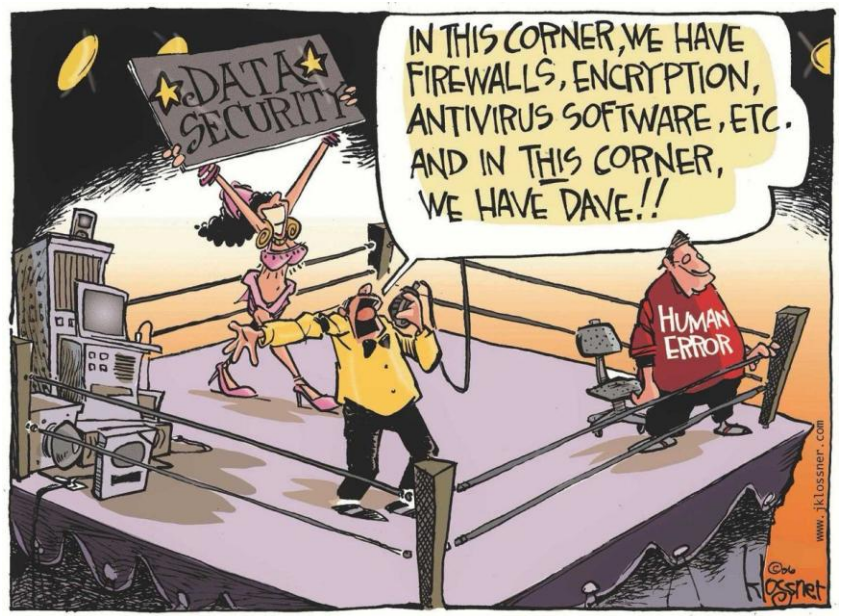
Source: https://imgflip.com/i/1jgg5c

Principe de cybersécurité ciblé – Contrôle et audit

Source: https://commitstrip.com

Source: https://www.darkreading.com/cloud-security/cartoon-c-suite-cybersecurity-

Principe de cybersécurité ciblé – Proportionnalité et précaution



Source: https://www.jklossner.com/humannature

Source: https://www.jklossner.com/humannature/vqmglje5sqm27mkm6x47bggyl7v4z1

Principes de cybersécurité – Wrap-up

1. Sécurité par défaut
2. Sécuriser le lien le plus faible
3. Défense en profondeur
4. Implémentation fail-secure
5. Toujours pessimiste
6. Contrôle et audit
7. Proportionnalité et précaution

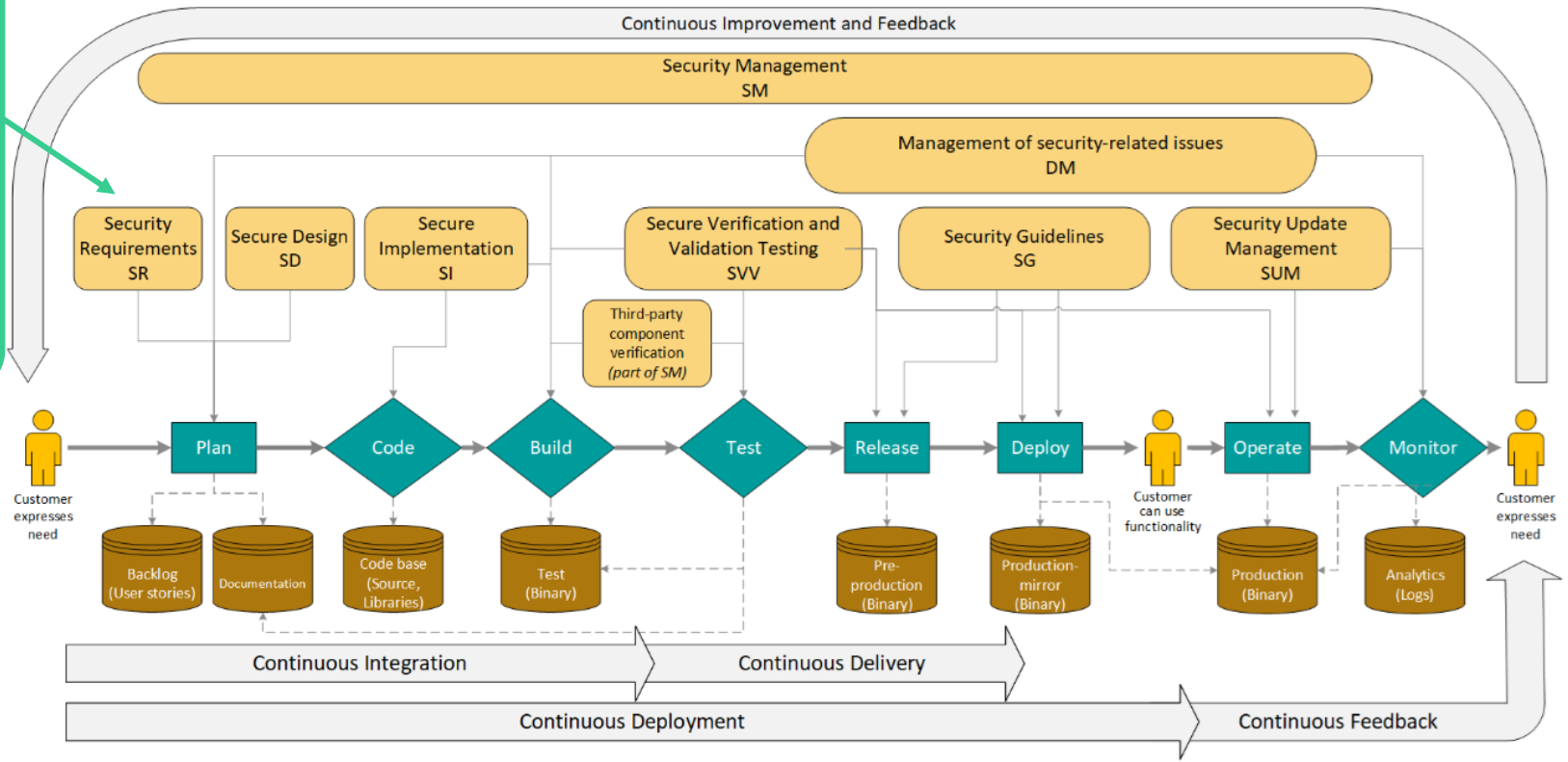
Threat Analysis & Risk Assessment (TARA)

Eric Silva

TARA

Spécifications Cyber

Exigences et revendications en matière de cybersécurité définies en exigences



Source: https://www.researchgate.net/publication/351929062_Integration_of_Security_Standards_in_DevOps_Pipelines_An_Industry_Case_Study

Threat Analysis & Risk Assessment (TARA)

Attributs des actifs & cybersécurité
Composants clés (matériel, logiciel, données) et leurs attributs de sécurité (confidentialité, intégrité, disponibilité) qui ont une valeur pour les parties prenantes du produit/système.

Exemples : confidentialité des données utilisateur, intégrité d'un nouveau package logiciel…

Scénarios de menace
Situations d'attaque réalistes et de haut niveau décrivant comment des adversaires pourraient cibler des vulnérabilités du système pour compromettre la sécurité.

Exemples : déni de service de la fonction de journalisation, usurpation GPS, données falsifiées…

Scénarios de dommages
Impact et/ou conséquences des cyberattaques réussies, incluant la sécurité, les aspects financiers, opérationnels et juridiques, parmi d'autres dimensions (jusqu'à la gestion des risques de l'entreprise).

Exemples : perte de données personnelles (PII) entraînant une amende RGPD et des dommages à la réputation…

Threat Analysis & Risk Assessment (TARA)

Mesures & contrôles de cybersécurité
Mesures techniques et organisationnelles pour réduire les risques et protéger les actifs contre les menaces cyber.

Exemples : mécanismes de démarrage sécurisé, déploiement OTA sécurisé des logiciels, SecOC sur CAN…

Vulnérabilités
Faiblesses réelles dans un produit/système qui pourraient être exploitées par un acteur malveillant, mettant en œuvre un scénario de menace.

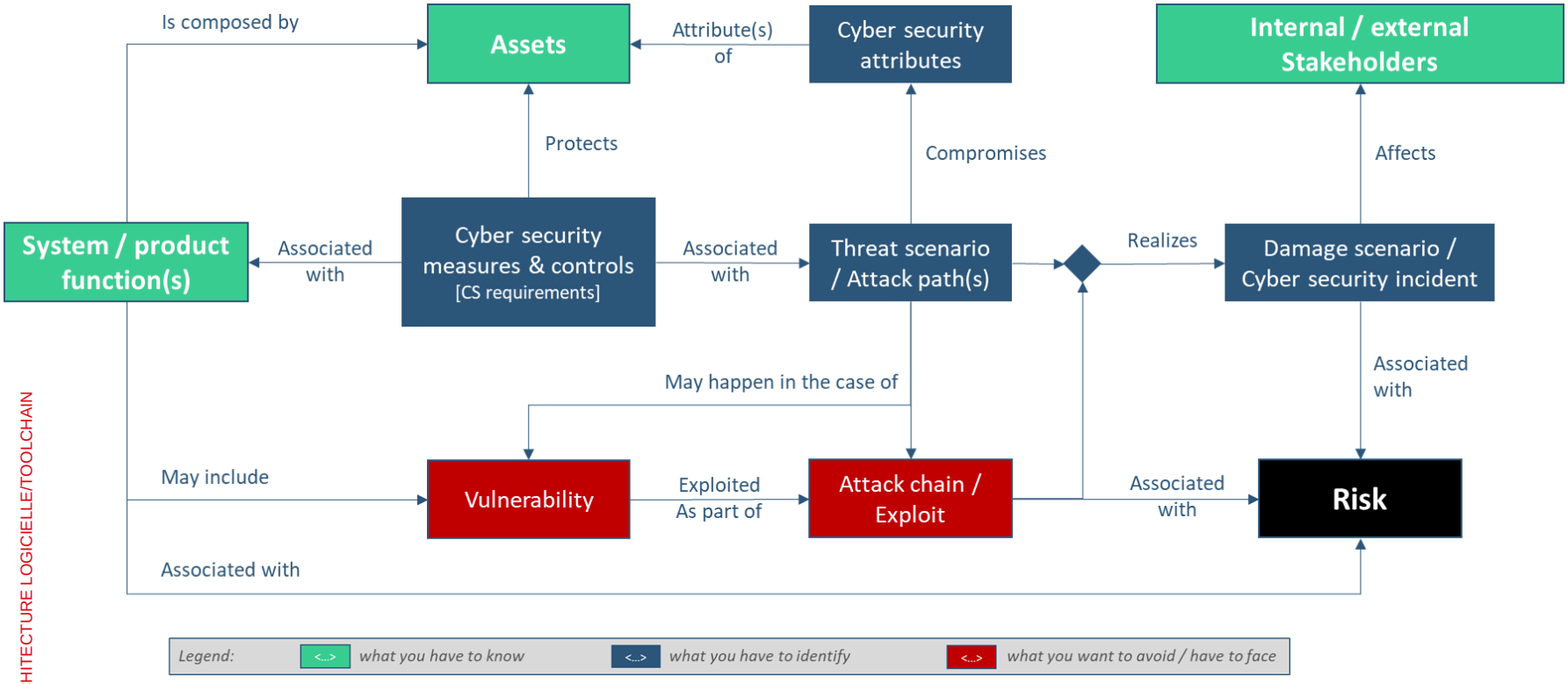
Exemples : débordements de mémoire tampon, exécution de code à distance, gestion non sécurisée des entrées…

Exploits / chaînes d'attaque
Méthodes pas-à-pas utilisées par les attaquants pour exploiter les vulnérabilités et atteindre des objectifs malveillants.

Exemples : campagne de phishing, récupération d'identifiants, usurpation de messages de communication…

Eric Silva

Threat Analysis & Risk Assessment (TARA)



Eric Silva

TARA – Walkthrough

Comment identifier les menaces pertinentes, les évaluer à l'aide de métriques raisonnables et initier l'intégration de tels principes clés de sécurité ?

En abordant le risque à l'aide d'une méthodologie systématique et holistique :

I

Comprendre votre système / produit

II

Identifier les conséquences potentielles

Identifier la faisabilité des compromissions

III

Calculer les valeurs de risque et prendre des décisions de traitement basées sur le risque

TARA – Etape 1 - définition du système

Fonction du produit / système : Quelles sont les fonctions fournies au client et à toute autre partie prenante durant toutes les phases du cycle de vie du produit ?
Exemples : mesure de capteur, activation du mode sécurisé, diagnostic du système, mise à jour logicielle, enregistrement des données…

Pertinence des actifs et attributs de cybersécurité : Qu'est-ce qui est important en cas de compromission ?
Exemples : confidentialité des données utilisateur, intégrité de la mise à jour logicielle, disponibilité de la fonction de sécurité…

Hypothèses : Quelles conditions préalables / environnementales / adverses impactent le système / produit ?
Exemples : fonctionnement dans un environnement protégé / restreint, parties prenantes formées, serveurs d'authentification centralisés fournis par l'environnement d'hébergement…

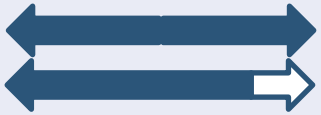
Architecture : Quelles sont les sous-parties du produit / système ?
Communications (flux de données, technologies) : Quelles informations sont échangées entre les parties du produit / système et vers des parties externes ?
Limites de confiance : Qu'est-ce qui est sous le contrôle de l'entreprise ?

TARA – Etape 1 - définition du système

Eric Silva

Diagrammes de flux de données (DFD)

Un moyen d'aider à visualiser le système faisant l'objet de la modélisation des menaces. À un niveau global, les DFD permettent de représenter les entités impliquées dans le fonctionnement du système ou du produit, la manière dont ces entités sont reliées, ainsi que les frontières de confiance supposées entre elles.

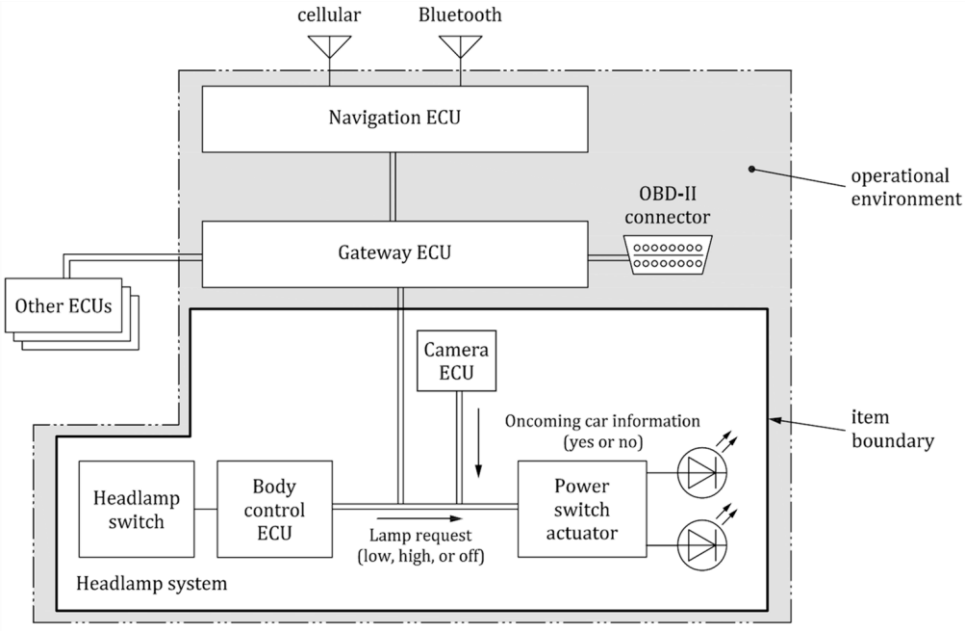
Elements	Symbol	Definitions
Entité externe		Tout ce qui est en dehors de votre contrôle. Exemples : personnes et systèmes gérés par d'autres organisations ou même d'autres divisions.
Processus		Tout code en cours d'exécution, y compris compilé, scripts, commandes shell, procédures stockées SQL…
Stockage de données		Tout endroit où les données sont stockées, y compris fichiers, bases de données, mémoire partagée, services de stockage cloud, cookies…
Flux de données		Toutes les façons dont les processus peuvent communiquer avec les stockages de données ou entre eux. Si une conversation n'est initiée que d'un seul côté, vous pouvez représenter ce côté initiateur par une flèche vide.
Limites de confiance		Un moyen de représenter différents niveaux de confiance entre des objets.

TARA – Etape 1 - définition du système

Eric Silva

Exemple de descriptions des fonctions de l'élément :
Le système de phares allume ou éteint le phare en fonction de la demande du conducteur via l'interrupteur. Si le phare est en mode grand phare, le système commute automatiquement le phare en mode feux de croisement lorsqu'un véhicule venant en sens inverse est détecté. Il remet également automatiquement le phare en mode grand phare si aucun véhicule venant en sens inverse n'est détecté.

Exemple de descriptions de l'environnement opérationnel :
L'élément (système de phares) est connecté à l'unité de contrôle passerelle (gateway ECU), et la passerelle est connectée à l'unité de contrôle navigation pour la communication de données. Hypothèse 1 : la gateway ECU dispose de contrôles de sécurité robustes, incluant une fonction pare-feu.



TARA – Etape 1 – Propriétés principales

Les scénarios de dommages sont les conséquences de compromissions des propriétés de cybersécurité des actifs.

Principales propriétés de cybersécurité

- **Authentification** : L'actif doit être lié à son auteur / éditeur tout au long de son cycle de vie.
- **Intégrité** : L'actif est exact et complet (= non altéré) pendant tout son cycle de vie.
- **Confidentialité** : L'actif n'est pas rendu accessible ou divulgué à des personnes, entités ou processus non autorisés.
- **Disponibilité** : L'actif doit être disponible lorsqu'il est nécessaire.

Une triade bien connue:

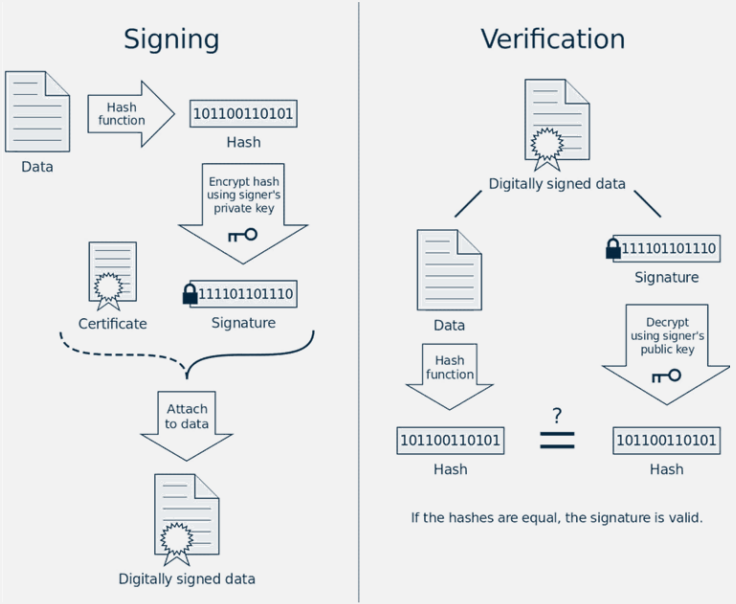
- **CIA :** Confidentialité, Intégrité et Disponibilité (Availability), un modèle conçu pour guider les politiques de sécurité de l'information au sein d'une organisation.

Eric Silva

TARA – Etape 1 – Propriétés principales

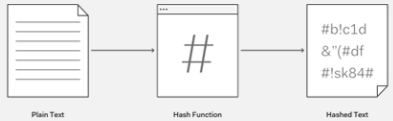
Authentication

Usually mitigated using identifiers in conjunction with integrity checks or digital signatures



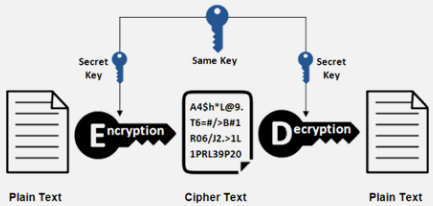
Integrity

Usually mitigated using hashing schemes and fingerprinting / signature



Confidentiality

Usually mitigated using encryption schemes (e.g. symmetric, asymmetric, hybrid)



Availability

Usually mitigated using redundant architectures, degraded mode handling and elastic capabilities

Eric Silva

TARA – Walkthrough

Comment identifier les menaces pertinentes, les évaluer à l'aide de métriques raisonnables et initier l'intégration de tels principes clés de sécurité ?

En abordant le risque à l'aide d'une méthodologie systématique et holistique :

I

Comprendre votre système / produit

II

Identifier les conséquences potentielles

Identifier la faisabilité des compromissions

III

Calculer les valeurs de risque et prendre des décisions de traitement basées sur le risque

TARA – Etape 2 – Scénarios de dommage

Eric Silva

Les scénarios de dommages doivent être évalués en fonction des conséquences négatives potentielles pour les parties prenantes, au moins selon les catégories d'impact indépendantes suivantes : sécurité, financier, opérationnel et confidentialité (privacy) ou légal.

- Impacts dits « SFOP »

Si d'autres catégories d'impact sont prises en compte au-delà de S, F, O et P, alors ces catégories doivent être documentées.

- Exemples d'autres catégories, plus spécifiques : perte de propriété intellectuelle, pertes financières pour l'entreprise, perte d'image de marque ou de réputation

La cotation de l'impact du scénario de dommage doit être déterminée comme l'une des suivantes : Sévère, Majeur, Modéré ou Négligeable.

Impact Rating	Criteria for Financial Impact Rating
Severe	The financial damage leads to catastrophic consequences which the affected stakeholder might not overcome.
Major	The financial damage leads to substantial consequences which the affected stakeholder will be able to overcome.
Moderate	The financial damage leads to inconvenient consequences which the affected stakeholder will be able to overcome with limited resources.
Negligible	The financial damage leads to no effect, negligible consequences or is irrelevant to the stakeholder.

TARA – Etape 2 – Analyse d'impact

Exemples de l'industrie automobile [ISO/SAE 21434, annex H]

Impact Rating	Criteria for Operational Impact Rating
Severe	The operational damage leads to a vehicle not working, from non-intended operation up to the vehicle being non-operational.
Major	The operational damage leads to the loss of a vehicle function.
Moderate	The operational damage leads to partial degradation of a vehicle function or performance.
Negligible	The operational damage leads to no effect or indiscernible degradation of a vehicle function or performance.

Impact Rating	Criteria for Privacy Impact Rating
Severe	The privacy damage leads to significant or even irreversible impact to the road user. In this case, the information regarding the road user is highly sensitive and easy to link to a PII principal.
Major	The privacy damage leads to serious impact to the road user. In this case, the information regarding the road user is: a) highly sensitive and difficult to link to a PII principal, or b) sensitive and easy to link to a PII principal.
Moderate	The privacy damage leads to significant inconveniences to the road user. In this case, the information regarding the road user is: a) sensitive but difficult to link to a PII principal, or b) not sensitive but easy to link to a PII principal.
Negligible	The privacy damage leads to no effect or can create few inconveniencies to the road user. In this case, the information regarding the road user is not sensitive and difficult to link to a PII principal.

Impact Rating	Criteria for Safety Impact Rating
Severe	S3: Life-threatening injuries (survival uncertain), fatal injuries
Major	S2: Severe and life-threatening injuries (survival probable)
Moderate	S1: Light and moderate injuries
Negligible	S0: No injuries

Safety impact rating criteria are taken from ISO 26262-3:2018.

Eric Silva

TARA – Walkthrough

Comment identifier les menaces pertinentes, les évaluer à l'aide de métriques raisonnables et initier l'intégration de tels principes clés de sécurité ?

En abordant le risque à l'aide d'une méthodologie systématique et holistique :

I. Comprendre votre système / produit

II. Identifier les conséquences potentielles

II. Identifier la faisabilité des compromissions

III. Calculer les valeurs de risque et prendre des décisions de traitement basées sur le risque

Eric Silva

TARA – Etape 2 – Scénarios de dommage

L'identification des scénarios de menace est une étape intermédiaire clé pour identifier les scénarios de haut niveau qu'une attaque pourrait exploiter afin de compromettre des actifs, et ainsi forcer le système / produit à aboutir à un scénario de dommage.

STRIDE est un acronyme. Il signifie :

Accr.	Menace	Propriété recherchée	Description
S	Usurpation d'identité (Spoofing)	Authenticité	Se faire passer pour quelque chose ou quelqu'un d'autre
T	Altération (Tampering)	Intégrité (C**I**A)	Modifier des données ou du code
R	Répudiation	Non-répudiation	Prétendre ne pas avoir réalisé une action
I	Divulgation d'information (Information disclosure)	Confidentialité (**C**IA)	Divulguer des informations à une personne non autorisée
D	Déni de service	Disponibilité (Availability) (CI**A**)	Refuser ou dégrader le service aux utilisateurs
E	Élévation de privilège	Autorisation	Obtenir des droits/capacités sans autorisation adéquate

TARA – Etape 2 – Scénarios de dommage

Eric Silva

Exemple de l'industrie automobile [ISO/SAE 21434, annex H]

Damage Scenario No.	Damage Scenario	Threat Scenario	Threat Scenario No.
:	:	:	:
D.x	Unintended headlamp's turn off during night driving resulting from loss of integrity of CAN signal	Spoofing of a signal leads to loss of integrity of the CAN message of "Lamp Request" signal of Power Switch Actuator ECU potentially causing unintended headlamp's turn off during night driving resulting from loss of integrity of CAN signal	T.x
		Tampering of a signal sent by Body Control ECU leads to ….	T.y
		….	…
:	:	:	:

TARA – Etape 2 – Arbres d'attaque

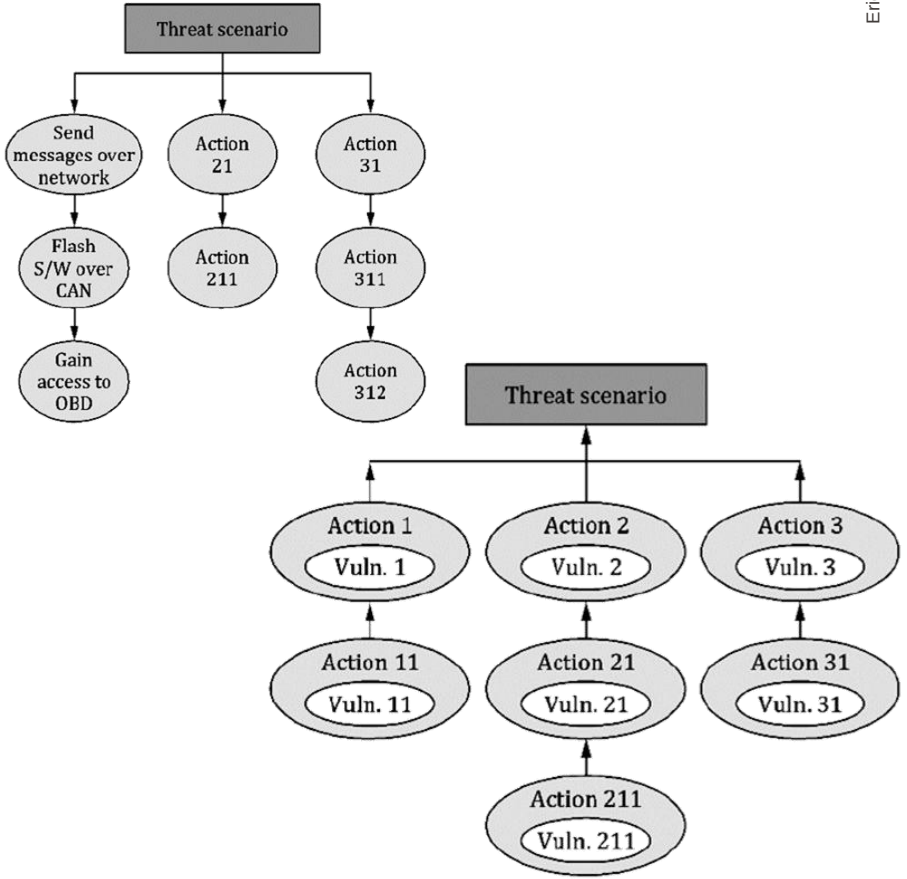
Les scénarios de menace doivent être analysés afin de décrire les chemins d'attaque possibles.

Une analyse des chemins d'attaque peut se baser sur :

- **Des approches descendantes** telles que les arbres d'attaque, les graphes d'attaque, ou les approches basées sur des taxonomies mnémoniques (par exemple, STRIDE) : elles sont utiles lors des phases de conception et de développement, lorsque l'implémentation de l'élément ou du composant n'est pas disponible, ou lorsque l'effort est dirigé vers la construction d'hypothèses d'attaque ou de modèles de chemins d'attaque.

- **Des approches ascendantes** (par exemple, issues de l'analyse de vulnérabilités) : elles sont le plus souvent utilisées lorsqu'une implémentation de l'élément ou du composant est disponible, ou lorsque des hypothèses ou des modèles d'attaque doivent être confirmés.

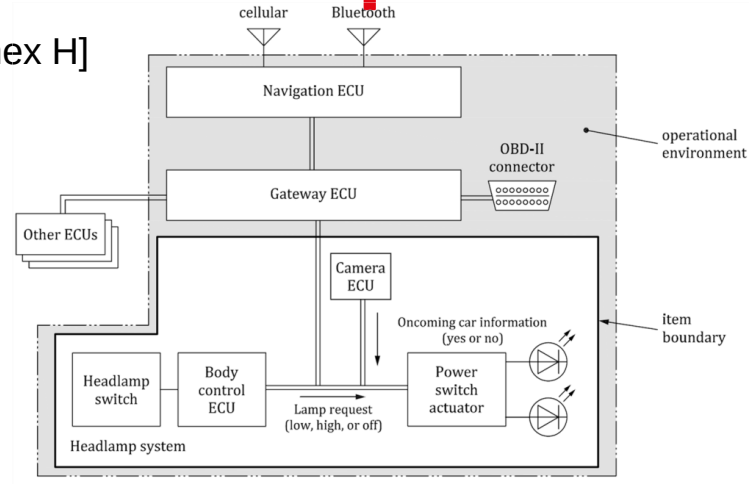
- Une combinaison des approches descendantes et ascendantes.

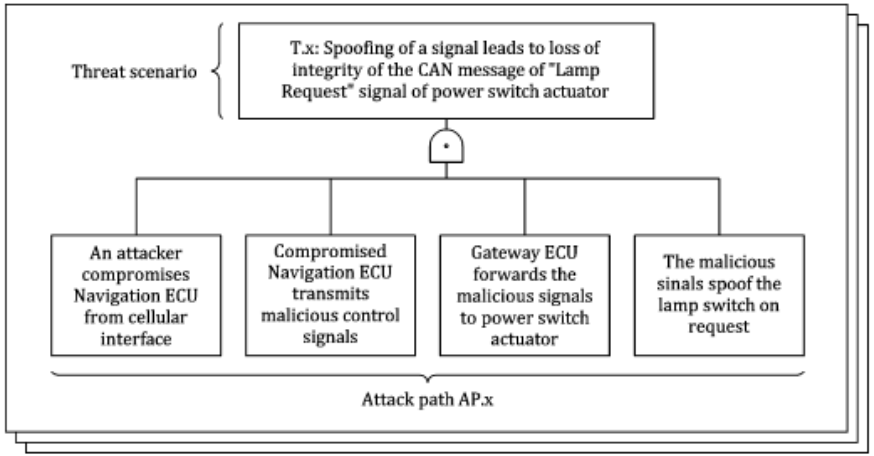


TARA – Etape 2 – Arbres d'attaque

Exemple de l'industrie automobile [ISO/SAE 21434, annex H]

Threat Scenario No.	Threat Scenario	Attack Path No.	Attack Path
T.x	Spoofing of a signal leads to loss of integrity of the CAN message of "Lamp Request" signal of Power Switch Actuator ECU	AP.x	An attacker compromise Navigation ECU from Cellular interface
			Compromised Navigation ECU transmits malicious control signals
			Gateway ECU forward the malicious signals to Power Switch Actuator
			The malicious signals spoof the lamp switch on request
		AP.y	An attacker compromise Navigation ECU from Bluetooth interface
			Compromised Navigation ECU transmits malicious control signals
			Gateway ECU forward the malicious signals to Power Switch Actuator
			The malicious signals spoof the lamp switch on request
		AP.z	An attacker sends malicious control signals from OBD2 connector
			Gateway ECU forward the malicious signals to Power Switch Actuator
			The malicious signals spoof the lamp switch on request
		:	:





TARA – Etape 2 – Faisabilité d'attaque

Pour chaque chemin d'attaque, le niveau de faisabilité de l'attaque doit être déterminé comme l'un des suivants : **élevé**, **moyen**, **faible** ou **très faible**. Plusieurs méthodes existent, selon la stratégie de l'entreprise, les informations disponibles et la maturité du développement et de la mise en œuvre du système ou du produit.

- **Approche basée sur le vecteur d'attaque** : basée sur l'évaluation du vecteur d'attaque prédominant du chemin d'attaque → approche basique mais utile pour une évaluation précoce.
- **Approche basée sur CVSSx (Common Vulnerability Scoring System)** : doit être déterminée à partir des métriques d'exploitation du groupe de base, incluant le vecteur d'attaque, la complexité de l'attaque, les privilèges requis et l'interaction avec l'utilisateur.
- **Approche basée sur le potentiel d'attaque** (voir ISO/IEC 18045 pour les facteurs) : doit être basée sur des facteurs clés tels que le temps nécessaire, l'expertise requise, la connaissance de l'élément ou du composant, la fenêtre d'opportunité et l'équipement.

TARA – Etape 2 – Faisabilité d'attaque

Eric Silva

Approche basée sur les vecteurs d'attaque (voir ISO/SAE 21434 annex G pour plus d'information)

Attack feasibility rating	Criteria
High	**Network:** Potential attack path is bound to network stack without any limitation. EXAMPLE 1 Cellular network connection making the ECU directly connected and accessible on the internet.
Medium	**Adjacent:** Potential attack path is bound to network stack; however, the connection is limited physically or logically. EXAMPLE 2 Bluetooth interface, virtual private network connection.
Low	**Local:** Potential attack path is not bound to network stack and threat agents require direct access to the item for realizing the attack path. EXAMPLE 3 Universal serial bus mass storage device, memory card.
Very low	**Physical:** Threat agents require physical access to realize the attack path.

TARA – Etape 2 – Faisabilité d'attaque

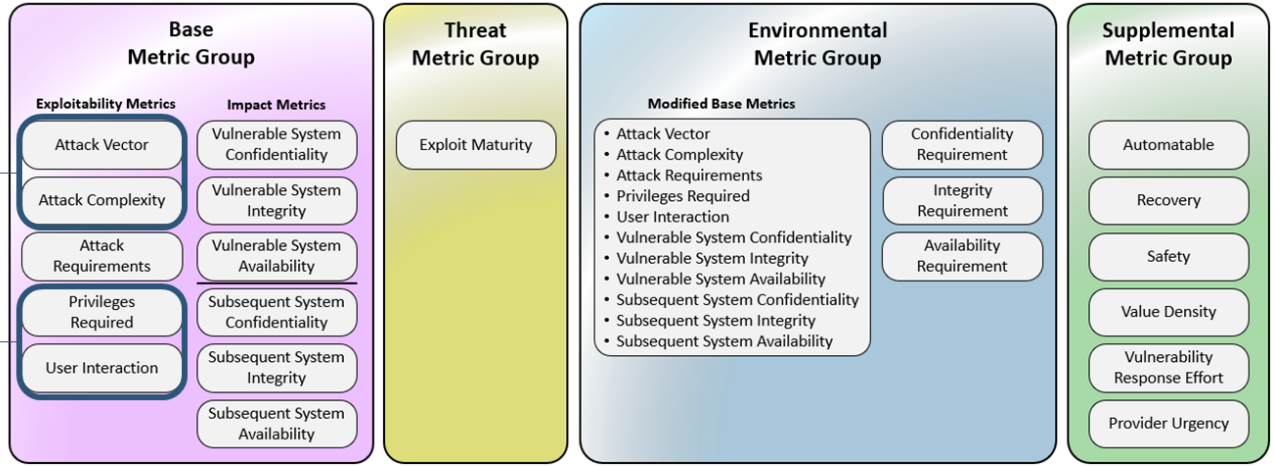
Eric Silva

Approche basée sur CVSS4 (peut fournir à la fois des informations sur l'impact et la faisabilité)

- Nécessite un niveau de maturité en cybersécurité plus élevé
- Permet une intégration fluide des considérations de vulnérabilité aux étapes ultérieures

$$E = 8{,}22 \times V \times C \times P \times U$$

Attack feasibility rating	CVSS exploitability value
High	2,96 - 3,89
Medium	2,00 - 2,95
Low	1,06 - 1,99
Very low	0,12 - 1,05



TARA – Etape 2 – Faisabilité d'attaque

Approche basée sur le potentiel d'attaque:

Elapsed time		Specialist expertise		Knowledge of the item or component		Window of opportunity		Equipment	
Enumerate	Value	Enumerate	Value	Enumerate	Value	Enumerate	Value	Enumerate	Value
≤1 day	0	Layman	0	Public	0	Unlimited	0	Standard	0
≤1 week	1	Proficient	3	Restricted	3	Easy	1	Specialized	4
≤1 month	4	Expert	6	Confidential	7	Moderate	4	Bespoke	7
≤6 months	17	Multiple experts	8	Strictly confidential	11	Difficult/ none	10	Multiple bespoke	9
>6 months	19								

Attack feasibility rating	Values
High	0 - 9
	10 - 13
Medium	14 - 19
Low	20 - 24
Very low	≥ 25

TARA – Etape 2 – Faisabilité d'attaque

Eric Silva

Exemple d'approche par vecteur d'attaque appliquée au « use-case » automobile:

Threat Scenario No.	Threat Scenario	Attack Path No.	Attack Path
T.x	Spoofing of a signal leads to loss of integrity of the CAN message of "Lamp Request" signal of Power Switch Actuator ECU	AP.x	An attacker compromise Navigation ECU from Cellular interface
			Compromised Navigation ECU transmits malicious control signals
			Gateway ECU forward the malicious signals to Power Switch Actuator
			The malicious signals spoof the lamp switch on request
		AP.y	An attacker compromise Navigation ECU from Bluetooth interface
			Compromised Navigation ECU transmits malicious control signals
			Gateway ECU forward the malicious signals to Power Switch Actuator
			The malicious signals spoof the lamp switch on request
		AP.z	An attacker sends malicious control signals from OBD2 connector
			Gateway ECU forward the malicious signals to Power Switch Actuator
			The malicious signals spoof the lamp switch on request
		:	:

TARA – Etape 2 – Faisabilité d'attaque

Exemple d'approche par vecteur d'attaque appliquée au « use-case » automobile:

Attack path	Attack feasibility rating
i. Attacker compromises navigation ECU **from cellular interface**. ii. Compromised navigation ECU transmits malicious control signals. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Malicious signals spoof the lamp request (ON).	High
i. Attacker compromises navigation ECU **from Bluetooth interface**. ii. Compromised navigation ECU transmits malicious control signals. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Malicious signals spoof the lamp request (ON).	Medium
i. Attacker sends malicious control signals **from OBD2 connector**. ii. Gateway ECU forwards the malicious signals to power switch actuator. iii. Malicious signals spoof the lamp request (ON).	Low

TARA – Etape 2 – Faisabilité d'attaque

Eric Silva

Exemple d'approche par vecteur d'attaque appliquée au « use-case » automobile:

- Approche la plus complète
- Adoptée par les principaux acteurs de nombreux secteurs, notamment l'automobile, le ferroviaire, l'automatisation, le médical, le pharmaceutique, etc

Threat scenario	Attack path	Attack feasibility assessment						
		ET	SE	KoIC	WoO	Eq	Value	Attack feasibility rating
Denial of service of oncoming car information	i. Attacker compromises navigation ECU from cellular interface. ii. Compromised navigation ECU transmits malicious control signals. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Attacker floods the communication bus with a large number of messages.	1	8	7	0	4	20	Low
	i. Attacker attaches a Bluetooth-enabled OBD dongle to OBD connector when vehicle is parking unlocked. ii. Attacker compromises driver's smartphone with Bluetooth interface. iii. Attacker sends message via smartphone and Bluetooth dongle to Gateway ECU. iv. Gateway ECU forwards malicious signals to power switch actuator. v. Attacker floods the communication bus with a large number of messages.	1	8	7	4	4	24	Low

Key
ET elapsed time
SE specialist expertise
KoIC knowledge of the item or component
WoO window of opportunity
Eq equipment

Eric Silva

TARA – Walkthrough

Comment identifier les menaces pertinentes, les évaluer à l'aide de métriques raisonnables et initier l'intégration de tels principes clés de sécurité ?

En abordant le risque à l'aide d'une méthodologie systématique et holistique :

I

Comprendre votre système / produit

II

Identifier les conséquences potentielles

Identifier la faisabilité des compromissions

III

Calculer les valeurs de risque et prendre des décisions de traitement basées sur le risque

TARA – Etape 3 – Matrices de risque

Une matrice de risques est une représentation d'une cartographie des niveaux d'impact et de faisabilité d'attaque respectivement, selon des échelles données de valeurs de risque. La détermination d'une valeur de risque peut avoir l'un des objectifs suivants :

- soutenir les critères pour les décisions sur le traitement du risque, y compris la sélection des mesures de contrôle ;
- priorisation des risques à traiter ;
- rapport aux parties prenantes ;
- suivi du risque.

		Attack feasibility rating			
		Very Low	Low	Medium	High
Impact rating	Severe	**2**	**3**	**4**	**5**
	Major	**1**	**2**	**3**	**4**
	Moderate	**1**	**2**	**2**	**3**
	Negligible	**1**	**1**	**1**	**1**

TARA – Etape 3 – Matrices de risque

Eric Silva

Threat scenario	Aggregated attack feasibility rating	Impact rating	Risk value
Spoofing of a signal leads to loss of integrity of the data communication of "Lamp Request" signal for power switch actuator ECU	**High**	**Severe**	**S: 5**
Denial of service of oncoming car information	Low	Moderate	O: 2

		Attack feasibility rating			
		Very Low	Low	Medium	High
Impact rating	Severe	**2**	**3**	**4**	**5**
	Major	**1**	**2**	**3**	**4**
	Moderate	**1**	**2**	**2**	**3**
	Negligible	**1**	**1**	**1**	**1**

Ou mathématiquement

$$R = 1 + I \times F$$

où

Impact rating	Numerical value *I* for impact
Negligible	0
Moderate	1
Major	1,5
Severe	2

Attack feasibility rating	Numerical value *F* for attack feasibility
Very low	0
Low	1
Medium	1,5
High	2

TARA – Etape 3 – Matrices de risque

Finalement, une option de traitement du risque doit être déterminée, en tenant compte des catégories d'impact, des chemins d'attaque et des résultats de la détermination du risque. Typiquement, les options de traitement du risque sont les suivantes :

- éviter le risque en supprimant les sources de risque, ou en décidant de ne pas démarrer ou poursuivre l'activité générant ce risque ;
- réduire le risque → des mesures de cybersécurité doivent être identifiées ;
- partager ou transférer le risque (par exemple, via des contrats, l'achat d'assurances) ;
- accepter ou conserver le risque.

Pour l'acceptation et le transfert du risque, les justifications correspondantes sont enregistrées sous forme de revendications de cybersécurité et font l'objet de validation, de suivi et de gestion des vulnérabilités.

Eric Silva

TARA – Wrap-up

Comment identifier les menaces pertinentes, les évaluer à l'aide de métriques raisonnables et initier l'intégration de tels principes clés de sécurité ?

En abordant le risque à l'aide d'une méthodologie systématique et holistique :

I

Comprendre votre système / produit

- Quelle fonction fournit-il ?
- Quelle partie de l'architecture avons-nous ? Quelles propriétés de sécurité sont importantes (CIA – Confidentialité, Intégrité, Disponibilité) ?
- Quelles phases du cycle de vie existent ?
- Quels sont mes acteurs internes / externes ? Quelles frontières de confiance avons-nous ?
- Quelles sont mes hypothèses concernant son environnement opérationnel ?

II

Identifier les conséquences potentielles:

- Sécurité / Financier / Operation / Légal
- Quel lois et règlements s'appliquent

Identifier la faisabilité des violations:

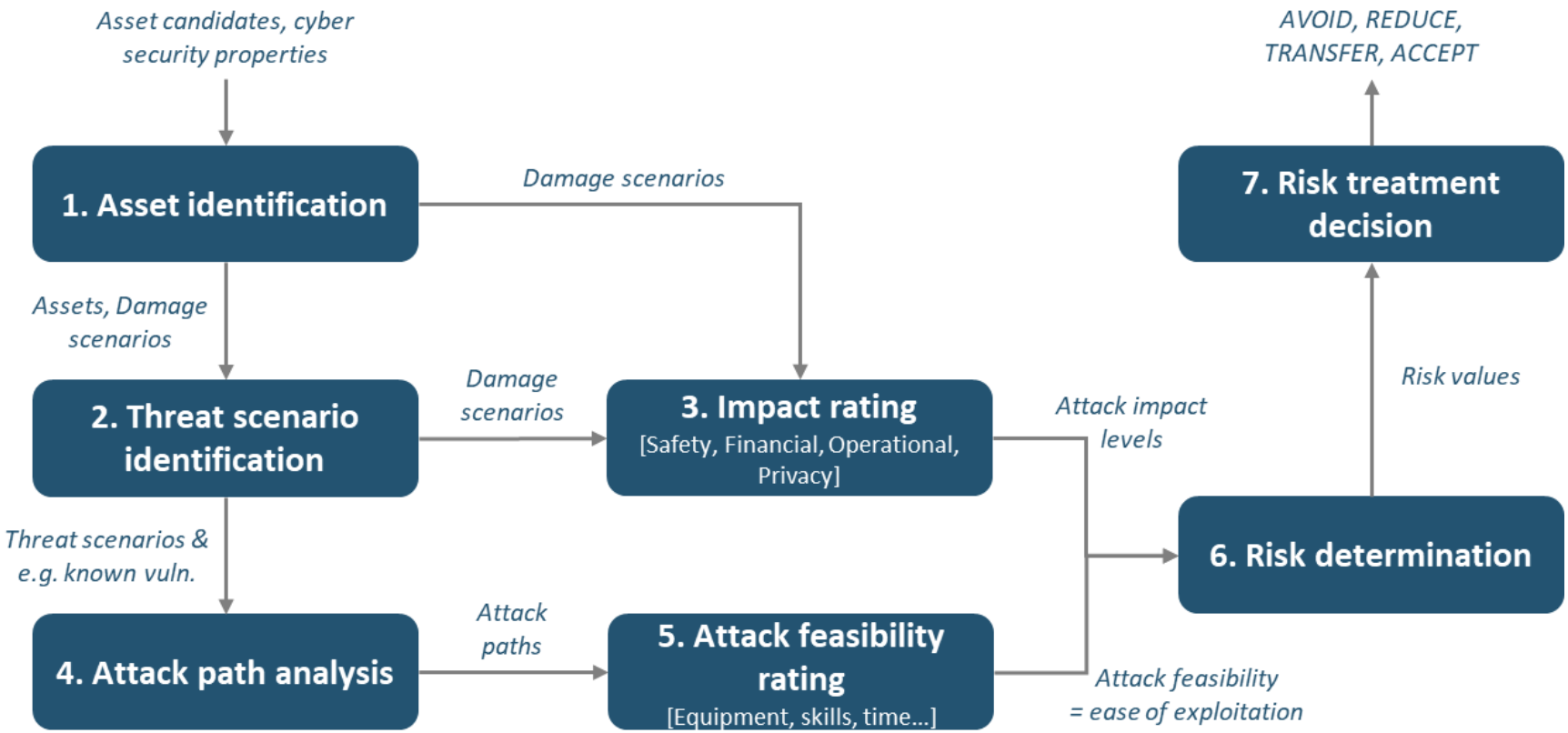
- Quels sont les vecteurs d'attaque ?
- L'attaque est faisable ou complexe?

III

Calculer les valeurs de risque et prendre des décisions de traitement basées sur le risque:

- Accepter le risque – Documenter la justification de l'acceptation
- Réduire le risque – Identifier les mesures et contrôles de sécurité à mettre en œuvre et à contrôler
- Éviter le risque – Supprimer les sources de risque | peu courant..
- Transférer le risque – Identifier le partage du risque avec d'autres parties (par ex. intégrateurs, assurances…)

TARA – Détail du processus



TARA – Vérification

Exhaustivité : Toutes les informations de l'analyse STRIDE (ou autre) sont-elles complètes ? Pour chaque aspect du modèle de menace, tous les sous-éléments sont-ils couverts ? Par exemple, les arbres d'attaque dépendent de l'aptitude et de l'expertise du modélisateur de menaces pour obtenir un ensemble suffisamment complet d'attaques que des développeurs moins expérimentés pourraient ne pas envisager. Les mesures de mitigation les plus fortes ont-elles été identifiées, et pour chaque composant ? S'il y a des lacunes, comprend-on bien pourquoi elles existent ?

Clarté : Chaque élément, chaque atténuation, etc., est-il clairement expliqué ? Est-ce compréhensible pour le public visé ? Idéalement, la clarté devrait émerger naturellement avec l'itération du modèle de menace parmi divers participants de l'organisation, mais il y aura toujours des lecteurs externes : certains aspects devront donc être explicités.

Spécificité : Chaque élément est-il suffisamment précis et au niveau de détail attendu pour le public cible ? Par exemple, donner le nom d'un protocole peut suffire dans certains cas, alors que pour d'autres, la version ou le mode de configuration seront nécessaires.

Traçabilité : Les relations entre les différents éléments du modèle de menace sont-elles facilement traçables ? Si des mesures sont utilisées, sont-elles clairement identifiées ? Y a-t-il des doublons ou des descriptions multiples pour le même concept dans le même contexte ?

Cohérence : Y a-t-il une cohérence entre la conception prévue et la mise en œuvre de l'élément analysé ? La documentation peut évoluer fréquemment, donc des incohérences peuvent apparaître si les échanges ne sont pas reflétés dans la documentation.

Rôles et responsabilités : Pour l'analyse de risque ou le modèle de menace, les rôles et responsabilités des opérateurs, des parties prenantes et des patients (le cas échéant) sont-ils clairement identifiés, notamment lors de la discussion sur le risque ?

Hypothèses : Toutes les hypothèses sont-elles clairement identifiées ? Sont-elles raisonnables ?

Justifications : Les justifications pour les décisions sont-elles incluses avec suffisamment de détails, en particulier pour les risques acceptés ou transférés ? Y a-t-il une possibilité de revenir sur les choix de mitigation, par exemple pourquoi une mitigation est sélectionnée plutôt qu'une autre ?

TARA – Challenges

Manque de compétences en cybersécurité au sein des organisations (en particulier pour l'évaluation réaliste des chemins d'attaque)

Absence de stratégie générale de cybersécurité, entraînant des incohérences

- Suppositions initiales et justifications manquantes
- Prise en compte des mesures de protection existantes biaisant l'analyse

Faible maturité des outils et du support logiciel

Nécessité d'interactions entre parties prenantes

- Interfaces avec d'autres évaluations de risques (par ex. qualité, sécurité fonctionnelle, fiabilité…)
- Interfaces entre IT-Sec, OT-Sec et Product-Sec
- RASIC [Responsable, Autorité, Soutien, Informé, Consulté]

Complexité de la maintenance

- Les risques évoluent en permanence (par ex. techniques d'attaque, outils, vulnérabilités connues…)
- Intégration des considérations de vulnérabilité pendant la phase d'exploitation

Use case : Domestic Medical Device

System definition

The Ankle Monitor Predictor of Stroke (AMPS)

AMPS is a fictional home use medical device worn at night (or when resting) by patients considered at risk for a stroke. The AMPS system gathers medical readings that can be later analyzed by a medical professional. While the system can help predict a patient's risk of experiencing a stroke, it does not alert – and is not intended to alert – if a stroke is imminent or occurring

- *Period of expected use: One to three months*
- *Medical capability: Diagnostic only*
- *Device invasiveness: Low (easily removable, like a wristwatch)*

Scenario

Alice has been informed by her doctor, based on her family history and several other risk factors, that she is at increased risk of experiencing a stroke. To gain further insight and determine a treatment plan, her doctor has instructed her to take the **AMPS system** home and wear it when she sleeps to take readings. She is also directed to install a **companion app on her phone** that will connect to the AMPS system (via Bluetooth Low Energy) and upload the readings every day to **the AMPS cloud service**, where they will be analyzed by an automated algorithm. Alice's doctor will check the results after the first week to identify any immediate causes of concern, and they will schedule a follow-up consult in two months

Use case : Domestic Medical Device

System definition

AMPS Device

AMPS is a health monitoring system worn on a patient's ankle when they are resting. It has the following specifications and capabilities:

- On/off switch
- Physical Bluetooth pairing button
- Proprietary stroke-predicting sensor.
- Heart rate monitor
- Body temperature sensor
- Bluetooth Low Energy (BLE) connectivity
- Onboard computer and flash storage that can store up to two weeks of patient data for later transmission

AMPS Cloud Service

The AMPSCS is a collection of virtual machines hosted in a cloud infrastructure. It consists of the following functionality:

- An application gateway server to inspect and limit traffic going into the AMPSCS systems
- A set of backend services that perform analysis of the patient data
- A collection of patient-facing services that communicate with the patient app, provide a web portal for patients to register their AMPS device, and authorize clinicians to view their data
- A collection of health delivery organization (HDO)-facing services that provide a web portal for clinicians to create an account and access a patient's data
    - Clinicians' access to the portal using a web browser.
    - Authentication is provided via username and password.
    - Clinician service identifiers that clinicians can provide to patients so the patients can authorize them through the app.
    - The clinicians can view a summary of the patient's raw data and the analysis performed by the AMPSCS backend algorithms.
    - The ability for clinicians to download a patient's data via an encrypted zip file.

Use case : Domestic Medical Device

System definition

AMPS Patient App

There are two different versions of the patient app, one for Apple iOS, and another for Android devices. Both apps contain the following functionality:

- It can pair with the AMPS device via Bluetooth.
- It contains an interface for a patient to create an account with the AMPS cloud services, register an AMPS device, and authorize clinicians to view their data.
- If the patient gives permission to the app, it will automatically connect to the AMPS device once a day and upload readings to the AMPSCS. If the patient does not give it permission, the app will store the data retrieved from the AMPS device until a manual upload is initiated. The amount of data transferred per upload is typically less than 1 megabyte a day.
- The app will display status information to the patient, including the last time the app synced with the AMPSCS, a log of the days the app was able to pull data from the AMPS device, and a log listing if the AMPS device was successfully collecting data.
- There is a device management screen that primarily focuses on diagnosing Bluetooth connection problems, and common issues that may prevent the AMPS device from collecting data. In addition:
  - The app can wipe patient data from the AMPS device.
  - The app can check for and update the firmware of the AMPS device with new versions.
  - The app can revert the AMPS device to factory default settings.
- If the device does not successfully sync to the cloud services once every 24 hours, an in-app notice will appear directing the patient to sync their data. After 72 hours have elapsed since a successful sync, the patient will be emailed an automatic reminder.

Rappel – Etape 1 - définition du système

Eric Silva

Diagrammes de flux de données (DFD)

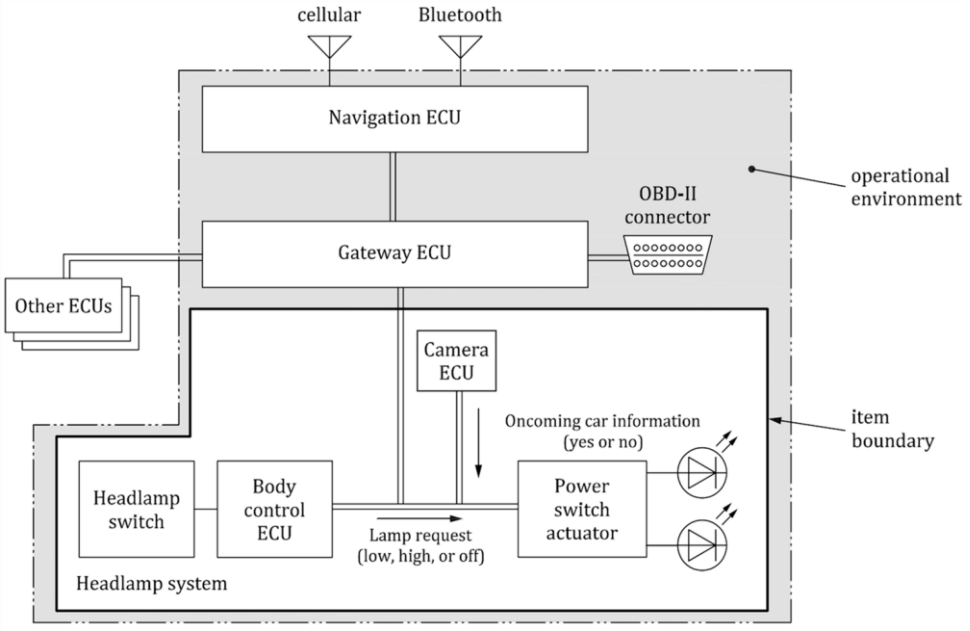
Un moyen d'aider à visualiser le système faisant l'objet de la modélisation des menaces. À un niveau global, les DFD permettent de représenter les entités impliquées dans le fonctionnement du système ou du produit, la manière dont ces entités sont reliées, ainsi que les frontières de confiance supposées entre elles.

Elements	Symbol	Definitions
Entité externe		Tout ce qui est en dehors de votre contrôle. Exemples : personnes et systèmes gérés par d'autres organisations ou même d'autres divisions.
Processus		Tout code en cours d'exécution, y compris compilé, scripts, commandes shell, procédures stockées SQL…
Stockage de données		Tout endroit où les données sont stockées, y compris fichiers, bases de données, mémoire partagée, services de stockage cloud, cookies…
Flux de données		Toutes les façons dont les processus peuvent communiquer avec les stockages de données ou entre eux. Si une conversation n'est initiée que d'un seul côté, vous pouvez représenter ce côté initiateur par une flèche vide.
Limites de confiance		Un moyen de représenter différents niveaux de confiance entre des objets.

Rappel - Etape 1 - définition du système

Exemple de descriptions des fonctions de l'élément :
Le système de phares allume ou éteint le phare en fonction de la demande du conducteur via l'interrupteur. Si le phare est en mode grand phare, le système commute automatiquement le phare en mode feux de croisement lorsqu'un véhicule venant en sens inverse est détecté. Il remet également automatiquement le phare en mode grand phare si aucun véhicule venant en sens inverse n'est détecté.

Exemple de descriptions de l'environnement opérationnel :
L'élément (système de phares) est connecté à l'unité de contrôle passerelle (gateway ECU), et la passerelle est connectée à l'unité de contrôle navigation pour la communication de données. Hypothèse 1 : la gateway ECU dispose de contrôles de sécurité robustes, incluant une fonction pare-feu.



Use case : Domestic Medical Device

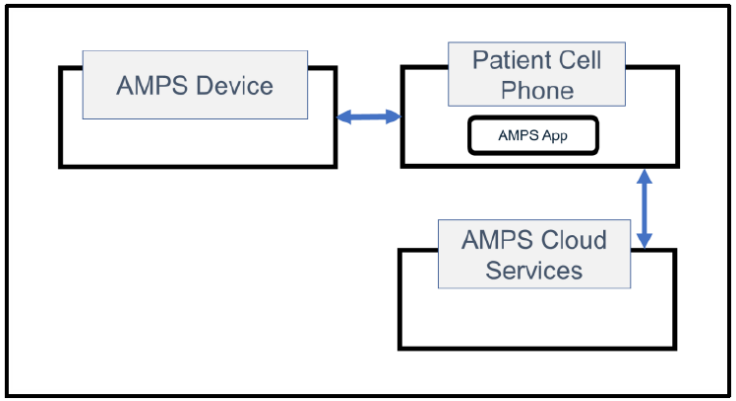
System definition

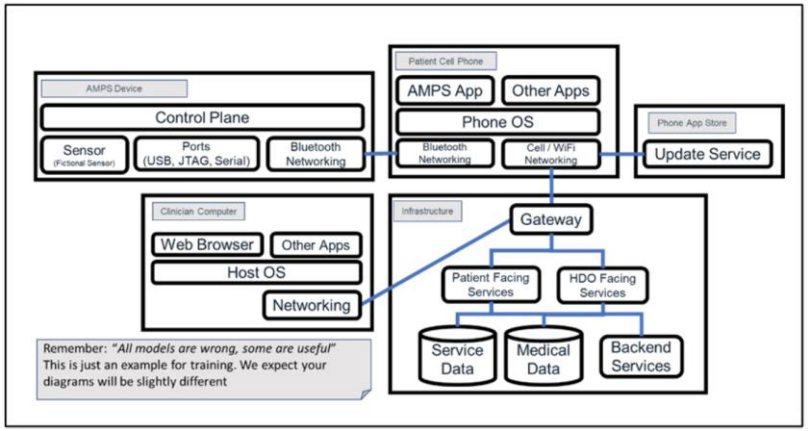
Exercice 1 – Data Flow Diagram

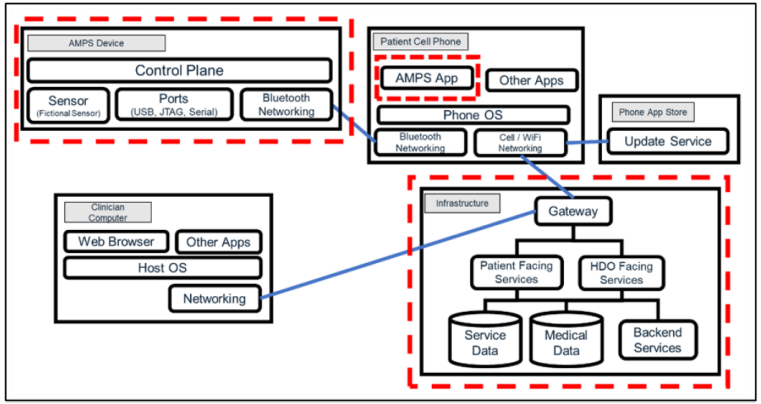
Dessinez le diagramme de flux de données du dispositif médical domestique défini dans les diapositives précédentes, y compris les parties du système, les flux de communication et les limites de confiance.

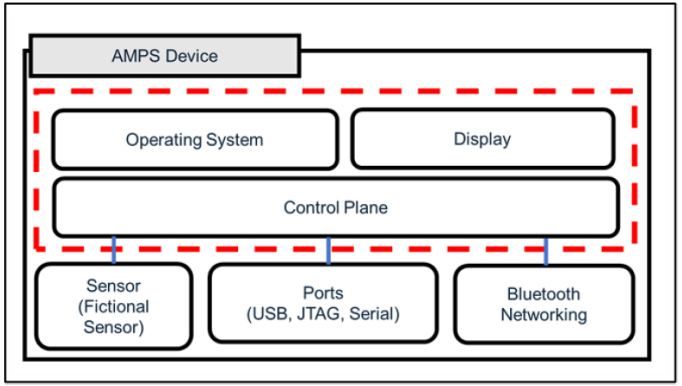
Use case : Domestic Medical Device

System definition









Use case : Domestic Medical Device

Threat Modelling

Exercice 2 – Identification des scénarios de menaces en utilisant STRIDE

Identifier les scénarios de menace pertinents à l'aide de la méthodologie STRIDE, y compris au moins un exemple par dimension de la menace

Rappel – Etape 2 – Scénarios de dommage

L'identification des scénarios de menace est une étape intermédiaire clé pour identifier les scénarios de haut niveau qu'une attaque pourrait exploiter afin de compromettre des actifs, et ainsi forcer le système / produit à aboutir à un scénario de dommage.

STRIDE est un acronyme. Il signifie :

Accr.	Menace	Propriété recherchée	Description
S	Usurpation d'identité (Spoofing)	Authenticité	Se faire passer pour quelque chose ou quelqu'un d'autre
T	Altération (Tampering)	Intégrité (C**I**A)	Modifier des données ou du code
R	Répudiation	Non-répudiation	Prétendre ne pas avoir réalisé une action
I	Divulgation d'information (Information disclosure)	Confidentialité (**C**IA)	Divulguer des informations à une personne non autorisée
D	Déni de service	Disponibilité (Availability) (CI**A**)	Refuser ou dégrader le service aux utilisateurs
E	Élévation de privilège	Autorisation	Obtenir des droits/capacités sans autorisation adéquate

Rappel – Etape 2 – Analyse d'impact

Exemples de l'industrie automobile [ISO/SAE 21434, annex H]

Impact Rating	Criteria for Operational Impact Rating
Severe	The operational damage leads to a vehicle not working, from non-intended operation up to the vehicle being non-operational.
Major	The operational damage leads to the loss of a vehicle function.
Moderate	The operational damage leads to partial degradation of a vehicle function or performance.
Negligible	The operational damage leads to no effect or indiscernible degradation of a vehicle function or performance.

Impact Rating	Criteria for Privacy Impact Rating
Severe	The privacy damage leads to significant or even irreversible impact to the road user. In this case, the information regarding the road user is highly sensitive and easy to link to a PII principal.
Major	The privacy damage leads to serious impact to the road user. In this case, the information regarding the road user is: a) highly sensitive and difficult to link to a PII principal, or b) sensitive and easy to link to a PII principal.
Moderate	The privacy damage leads to significant inconveniences to the road user. In this case, the information regarding the road user is: a) sensitive but difficult to link to a PII principal, or b) not sensitive but easy to link to a PII principal.
Negligible	The privacy damage leads to no effect or can create few inconveniencies to the road user. In this case, the information regarding the road user is not sensitive and difficult to link to a PII principal.

Impact Rating	Criteria for Safety Impact Rating
Severe	S3: Life-threatening injuries (survival uncertain), fatal injuries
Major	S2: Severe and life-threatening injuries (survival probable)
Moderate	S1: Light and moderate injuries
Negligible	S0: No injuries

Safety impact rating criteria are taken from ISO 26262-3:2018.

Use case : Domestic Medical Device

Threat Modelling

STRIDE ID	Definitions	Examples	STRIDE association			
			Ext. Entity	Proc.	Data Store	Data Flow
Spoofing	Tricking a system into believing a falsified entity is a true entity	Using stolen or borrowed credentials to log on as another nurse	X	X		
Tampering	Intentional modification of a system in an unauthorized way	Changing patient data to incorrect values		X	X	X
Repudiation	Disputing the authenticity of an action taken	Denying that a prescribed treatment has been provided to the patient	X	X	?	
Information disclosure	Exposing information intended to have restricted access levels	Health data is sent over an unencrypted Bluetooth connection		X	X	X
Denial of Service (DoS)	Blocking legitimate access or functionality of a system by malicious process(es)	A Bluetooth SpO2 sensor is flooded with bad pairing requests, preventing legitimate connections		X	X	X
Elevation of Privilege (EoP)	Gaining access to functions to which an attacker should not normally have access according to the intended security policy of the product	A patient uses a web portal vulnerability to see all patient data, rather than their own		X		

Use case : Domestic Medical Device

Threat Modelling

AMPS components	Threat types					
	S	T	R	I	D	E
Entity: AMPS Device	1	2	-	-	3,34 35	4
Entity: AMPS App	5,36	6	-	7	8	9,37
Entity: APP Store	10,38	11	-	12	13	14
Entity: AMPS Cloud Service	15,39 40	16,41	17,42 43,44	18,45	19,46 47,48	20,49 50
Entity: Clinician Computer	21,51, 52	22	-	23	24,53	25
Data Flow: Bluetooth	-	-	-	26	27,54	-
Data Flow: Cellular / Wifi	-	28	-	29	30	-
Data Flow: Clinician IT network	-	31	-	32	33	-

ID	Threat type	Threat scenario identification
1	S	An attacker could pretend to be an authorized phone app to obtain readings from the device
2	T	Control plane could be attacked and given incorrect readings
3	D	Invalid input could cause device to crash
34	D	Software could be corrupted
35	D	Battery could be drained more rapidly than normal
4	E	Device could be hacked, and software could be installed to perform other actions (such as make it part of a botnet, enable lateral movement, etc.)

Rappel – Etape 2 – Analyse d'impact

Exemples de l'industrie automobile [ISO/SAE 21434, annex H]

Impact Rating	Criteria for Operational Impact Rating
Severe	The operational damage leads to a vehicle not working, from non-intended operation up to the vehicle being non-operational.
Major	The operational damage leads to the loss of a vehicle function.
Moderate	The operational damage leads to partial degradation of a vehicle function or performance.
Negligible	The operational damage leads to no effect or indiscernible degradation of a vehicle function or performance.

Impact Rating	Criteria for Privacy Impact Rating
Severe	The privacy damage leads to significant or even irreversible impact to the road user. In this case, the information regarding the road user is highly sensitive and easy to link to a PII principal.
Major	The privacy damage leads to serious impact to the road user. In this case, the information regarding the road user is: a) highly sensitive and difficult to link to a PII principal, or b) sensitive and easy to link to a PII principal.
Moderate	The privacy damage leads to significant inconveniences to the road user. In this case, the information regarding the road user is: a) sensitive but difficult to link to a PII principal, or b) not sensitive but easy to link to a PII principal.
Negligible	The privacy damage leads to no effect or can create few inconveniencies to the road user. In this case, the information regarding the road user is not sensitive and difficult to link to a PII principal.

Impact Rating	Criteria for Safety Impact Rating
Severe	S3: Life-threatening injuries (survival uncertain), fatal injuries
Major	S2: Severe and life-threatening injuries (survival probable)
Moderate	S1: Light and moderate injuries
Negligible	S0: No injuries

Safety impact rating criteria are taken from ISO 26262-3:2018.

Use case : Domestic Medical Device

Threat Modelling

ID	Threat type	Threat scenario identification	Damage scenario [Safety, Financial, Operational, Privacy]	Worst impact
1	S	An attacker could pretend to be an authorized phone app to obtain readings from the device	Erroneous diagnostic [S-O], PII leakage [F-P]	P: Severe
2	T	Control plane could be attacked and given incorrect readings	Erroneous diagnostic [S-O]	S-O: Major
3	D	Invalid input could cause device to crash	System / function degradation [F-O]	O: Moderate
34	D	Software could be corrupted	Erroneous diagnostic [S-O], System / function unavailability or degradation [F-O], PII leakage [F-P]	P: Severe S-O: Major
35	D	Battery could be drained more rapidly than normal	System / function degradation [F-O]	O: Moderate
4	E	Device could be hacked, and software could be installed to perform other actions (such as make it part of a botnet, enable lateral movement, etc.)	Erroneous diagnostic [S-O], System / function unavailability or degradation [F-O], PII leakage [F-P]	P: Severe S-O: Major

Use case : Domestic Medical Device

Attack feasibility

Exercice 3 – Attack trees

Sur la base de l'hypothèse que vous pouvez définir, dressez la liste des étapes du chemin d'attaque ou dessinez les arbres d'attaque liés aux scénarios de menace suivants

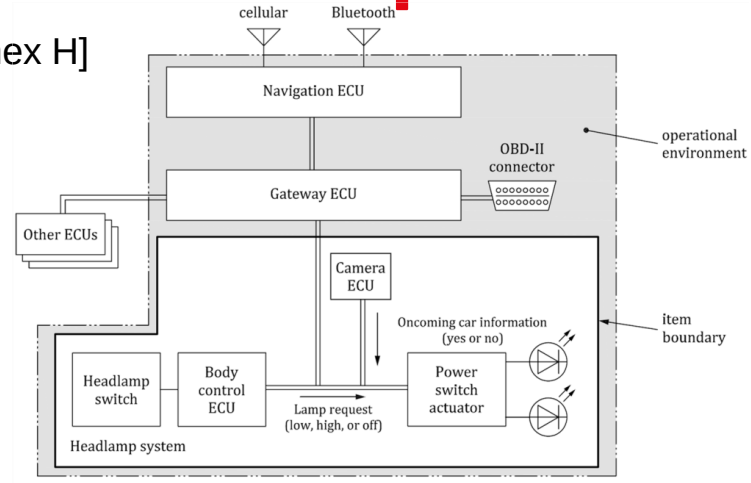
- Un attaquant pourrait se faire passer pour une application téléphonique autorisée afin d'obtenir des relevés de l'appareil.
- Une entrée invalide pourrait entraîner le plantage de l'appareil.

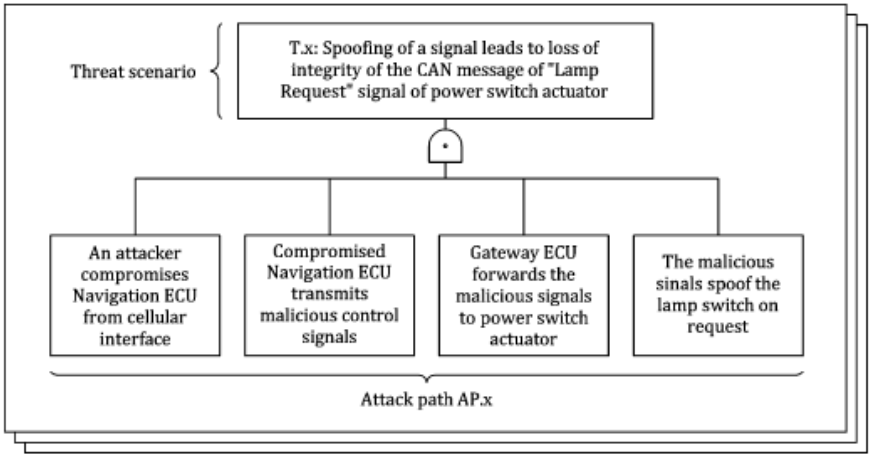
En supposant que l'évaluation de l'impact est Sévère pour (1) pour les questions de vie privée, et MODÉRÉE pour (2) pour les questions opérationnelles, calculez les valeurs de risque et proposez un traitement du risque.

Rappel – Etape 2 – Arbres d'attaque

Exemple de l'industrie automobile [ISO/SAE 21434, annex H]

Threat Scenario No.	Threat Scenario	Attack Path No.	Attack Path
T.x	Spoofing of a signal leads to loss of integrity of the CAN message of "Lamp Request" signal of Power Switch Actuator ECU	AP.x	An attacker compromise Navigation ECU from Cellular interface
			Compromised Navigation ECU transmits malicious control signals
			Gateway ECU forward the malicious signals to Power Switch Actuator
			The malicious signals spoof the lamp switch on request
		AP.y	An attacker compromise Navigation ECU from Bluetooth interface
			Compromised Navigation ECU transmits malicious control signals
			Gateway ECU forward the malicious signals to Power Switch Actuator
			The malicious signals spoof the lamp switch on request
		AP.z	An attacker sends malicious control signals from OBD2 connector
			Gateway ECU forward the malicious signals to Power Switch Actuator
			The malicious signals spoof the lamp switch on request
		:	:





Rappel – Etape 2 – Faisabilité d'attaque

Approche basée sur le potentiel d'attaque:

Elapsed time		Specialist expertise		Knowledge of the item or component		Window of opportunity		Equipment	
Enumerate	Value	Enumerate	Value	Enumerate	Value	Enumerate	Value	Enumerate	Value
≤1 day	0	Layman	0	Public	0	Unlimited	0	Standard	0
≤1 week	1	Proficient	3	Restricted	3	Easy	1	Specialized	4
≤1 month	4	Expert	6	Confidential	7	Moderate	4	Bespoke	7
≤6 months	17	Multiple experts	8	Strictly confidential	11	Difficult/ none	10	Multiple bespoke	9
>6 months	19								

Attack feasibility rating	Values
High	0 - 9
	10 - 13
Medium	14 - 19
Low	20 - 24
Very low	≥ 25

Rappel – Etape 2 – Faisabilité d'attaque

Exemple d'approche par vecteur d'attaque appliquée au « use-case » automobile:

- Approche la plus complète
- Adoptée par les principaux acteurs de nombreux secteurs, notamment l'automobile, le ferroviaire, l'automatisation, le médical, le pharmaceutique, etc

Threat scenario	Attack path	Attack feasibility assessment						
		ET	SE	KoIC	WoO	Eq	Value	Attack feasibility rating
Denial of service of oncoming car information	i. Attacker compromises navigation ECU from cellular interface. ii. Compromised navigation ECU transmits malicious control signals. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Attacker floods the communication bus with a large number of messages.	1	8	7	0	4	20	Low
	i. Attacker attaches a Bluetooth-enabled OBD dongle to OBD connector when vehicle is parking unlocked. ii. Attacker compromises driver's smartphone with Bluetooth interface. iii. Attacker sends message via smartphone and Bluetooth dongle to Gateway ECU. iv. Gateway ECU forwards malicious signals to power switch actuator. v. Attacker floods the communication bus with a large number of messages.	1	8	7	4	4	24	Low

Key
ET elapsed time
SE specialist expertise
KoIC knowledge of the item or component
WoO window of opportunity
Eq equipment

Use case : Domestic Medical Device

Attack feasibility

Attack paths	Threat types						
	ET	SE	KoIC	WoO	Eq	Value	Feas.
Threat scenario: An attacker could pretend to be an authorized phone app to obtain readings from the device **Attack path:** ➢ Attacker sniffs Bluetooth communications to identify AMPS device ➢ Attacker forge & send an email to patient / victim mimicking clinician team members to retrieve access credentials for system maintenance purposes ➢ Attacker connect to the AMPS device using credentials retrieved from victim, and get access to patient data / PII	1	3	0	4	4	12	High
Threat scenario: Invalid input could cause device to crash **Attack path:** ➢ Attacker sniffs Bluetooth communications to identify AMPS device ➢ Attacker floods / fuzzes AMPS devices using tailored pairing attempts to overload the target	0	6	3	4	4	17	Medium

ET elapsed time
SE specialist expertise
KoIC knowledge of the item or component
WoO window of opportunity
Eq equipment

Elapsed time		Specialist expertise		Knowledge of the item or component	
Enumerate	Value	Enumerate	Value	Enumerate	Value
≤1 day	0	Layman	0	Public	0
≤1 week	1	Proficient	3	Restricted	3
≤1 month	4	Expert	6	Confidential	7
≤6 months	17	Multiple experts	8	Strictly confidential	11
>6 months	19				

Window of opportunity		Equipment	
Enumerate	Value	Enumerate	Value
Unlimited	0	Standard	0
Easy	1	Specialized	4
Moderate	4	Bespoke	7
Difficult/ none	10	Multiple bespoke	9

Attack feasibility rating	Values
High	0 - 9
	10 - 13
Medium	14 - 19
Low	20 - 24
Very low	≥ 25

Use case : Domestic Medical Device

Attack feasibility

		Attack feasibility rating			
		Very Low	Low	Medium	High
Impact rating	Severe	2	3	4	5
	Major	1	2	3	4
	Moderate	1	2	2	3
	Negligible	1	1	1	1

Attack paths	Risk metrics		Risk value	Risk treatment decision
	Impact rating	Feasibility rating		
Threat scenario: An attacker could pretend to be an authorized phone app to obtain readings from the device **Attack path:** ➢ Attacker sniffs Bluetooth communications to identify AMPS device ➢ Attacker forge & send an email to patient / victim mimicking clinician team members to retrieve access credentials for system maintenance purposes ➢ Attacker connect to the AMPS device using credentials retrieved from victim, and get access to patient data / PII	Severe	High	5	**Reduce the risk** Access to AMPS device readings / data shall be authenticated using MFA
Threat scenario: Invalid input could cause device to crash **Attack path:** ➢ Attacker sniffs Bluetooth communications to identify AMPS device ➢ Attacker floods / fuzzes AMPS devices using tailored pairing attempts to overload the target	Moderate	Medium	2	**Accept the risk** Rationale: risk of AMPS device crash is communicated to the patient which has to check device status regularly (tbd), and restart if/when crashed

TARA – Etape 3 – Matrices de risque

Eric Silva

Threat scenario	Aggregated attack feasibility rating	Impact rating	Risk value
Spoofing of a signal leads to loss of integrity of the data communication of "Lamp Request" signal for power switch actuator ECU	**High**	**Severe**	**S: 5**
Denial of service of oncoming car information	Low	Moderate	O: 2

		Attack feasibility rating			
		Very Low	Low	Medium	High
Impact rating	Severe	**2**	**3**	**4**	**5**
	Major	**1**	**2**	**3**	**4**
	Moderate	**1**	**2**	**2**	**3**
	Negligible	**1**	**1**	**1**	**1**

Ou mathématiquement

$$R = 1 + I \times F$$

où

Impact rating	Numerical value *I* for impact
Negligible	0
Moderate	1
Major	1,5
Severe	2

Attack feasibility rating	Numerical value *F* for attack feasibility
Very low	0
Low	1
Medium	1,5
High	2

Use case : Domestic Medical Device

Attack feasibility

		Attack feasibility rating			
		Very Low	Low	Medium	High
Impact rating	Severe	2	3	4	5
	Major	1	2	3	4
	Moderate	1	2	2	3
	Negligible	1	1	1	1

Attack paths	Risk metrics		Risk value	Risk treatment decision
	Impact rating	Feasibility rating		
Threat scenario: An attacker could pretend to be an authorized phone app to obtain readings from the device **Attack path:** ➢ Attacker sniffs Bluetooth communications to identify AMPS device ➢ Attacker forge & send an email to patient / victim mimicking clinician team members to retrieve access credentials for system maintenance purposes ➢ Attacker connect to the AMPS device using credentials retrieved from victim, and get access to patient data / PII	Severe	High	5	**Reduce the risk** Access to AMPS device readings / data shall be authenticated using MFA
Threat scenario: Invalid input could cause device to crash **Attack path:** ➢ Attacker sniffs Bluetooth communications to identify AMPS device ➢ Attacker floods / fuzzes AMPS devices using tailored pairing attempts to overload the target	Moderate	Medium	2	**Accept the risk** Rationale: risk of AMPS device crash is communicated to the patient which has to check device status regularly (tbd), and restart if/when crashed