Comment adapter une méthodologie d'analyse de risque CyberSécurité d'un contexte aéronautique au ferroviaire ?

Mehdi Romdhane

Comment adapter une méthodologie d'analyse de risque CyberSécurité d'un contexte aéronautique au ferroviaire ?

Mehdi ROMDHANE
APSYS
ZA Clef de Saint Pierre
1 Boulevard Jean Moulin
78990 Élancourt

Résumé

Dans le secteur industriel, où la prise de conscience des menaces cyber est récente, les méthodes classiques d'analyse de risque doivent être adaptées pour prendre en compte des contraintes liées à des systèmes complexes. Nous proposons ainsi de capitaliser sur une expérience aéronautique pour construire une méthode adaptée au ferroviaire.

Summary

In the industry, where the cyber threat awareness is quite new, classical risk analysis methods should be adapted to take into account constraints related to complex systems. We also propose to capitalize on our aeronautical experience to build a method adapted to railway.

Introduction

Dans un monde hostile, les menaces qui pèsent sur la sécurité des systèmes d'information évoluent et leur pression s'accroit. Qu'elles soient externes (hacktivisme, déstabilisation, gains financiers) ou internes (intentionnelles ou non), les attaques sont de plus en plus ciblées et les attaquants se professionnalisent à une époque où l'expertise nécessaire est de plus en plus facilement accessible. Les exemples sur les systèmes d'informations de grands comptes sont de plus en plus nombreux dans l'actualité et les systèmes industriels sont désormais également des cibles. Depuis 2009 et l'exemple Stuxnet, le nombre de vulnérabilités (failles de cyber sécurité pouvant être exploitées par une menace) connues sur le domaine des SI industriels a explosé. 80% de ces vulnérabilités ont d'ailleurs été découvertes à partir de 2011. La menace s'est ainsi totalement mondialisée, d'où la nécessité aujourd'hui d'évaluer ces risques et les mettre sous contrôle, encore plus qu'hier. Un risque sur une activité correspond à la survenance d'un évènement empêchant l'atteinte des objectifs liés à cette activité. Ce sont les analyses de risques qui vont permettre aux acteurs industriels d'orienter leur vision stratégique, de réaliser les bons choix en termes de sécurité et d'arbitrer les grands projets de transformation. L'analyse de risque est ainsi la clé de voûte du processus itératif de gestion des risques.

La norme ISO27005 propose un processus complet de gestion des risques de sécurité de l'information. Elle établit une démarche mais ne l'outille pas.

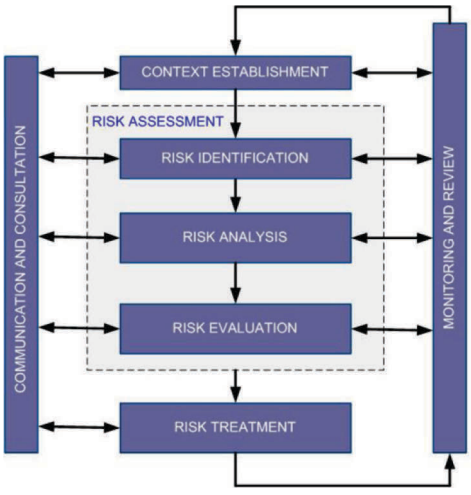

Figure 1. Analyse de risque ISO27005

Elle donne ainsi les lignes directrices du processus mais la méthodologie utilisée reste libre. Il en existe de nombreuses aujourd'hui (EBIOS, MEHARI, SECRAM, ED203…), elles décrivent toutes des principes à appliquer dans un certain contexte d'analyse pour arriver au résultat requis dans la norme ISO27005. Chacune a ses avantages et ses inconvénients et est adaptées à un contexte particulier.

	MEHARI	EBIOS	ED203	SECRAM
Adaptable à l'IT et/ou au contexte produit industriel	Les deux	Les deux	Produit	Les deux
Capacité à gérer des scénarios complexes	Faible	Faible	Oui	Faible
Capacité de justification	Moyenne	Moyenne	Haute	Moyenne

Table 1. Comparaison de méthodologies

Le contexte, justement, doit également être adapté, partagé et validé pour chaque nouvel environnement en amont de l'analyse de risque. Cela comprend les critères d'impact, les critères de vraisemblance et la matrice de risque (critères d'acceptation du risque, nombre de niveaux de vraisemblance et nombre de niveaux d'impact).

L'objectif de cette communication est de proposer une piste d'amélioration des bonnes pratiques de l'analyse de risque en CyberSécurité informatique et industrielle en présentant au travers d'un retour d'expérience les échecs observés au sein d'un grand groupe industriel ferroviaire ainsi que les axes d'améliorations retenus. Nous tenterons de démontrer comment Apsys, en capitalisant sur l'expérience aéronautique d'Airbus, a su adapter sa démarche pour mettre au point une méthodologie efficace adaptée à l'évaluation des risques « cyber » dans le domaine ferroviaire.

Contexte

Apsys a donc été sollicité par un industriel ferroviaire pour réaliser une revue critique des analyses de risque sécurité menées en interne via la méthodologie EBIOS, recommandée par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

Nous avons rapidement constaté plusieurs dysfonctionnements et manques de cohérence dus principalement à une mise en œuvre trop académique du standard EBIOS :

- Dans **l'évaluation des impacts** d'un évènement redouté : EBIOS requiert deux étapes, l'évaluation des besoins de sécurité par rapport aux échelles de Confidentialité, Intégrité et Disponibilité tout d'abord, l'évaluation des conséquences ensuite par rapport aux échelles des différents critères d'impact sélectionnés. Cela a généré des incohérences dans les évaluations avec des impacts maximum supérieurs aux besoins identifiés : les besoins de sécurité sont censés couvrir les impacts potentiels maximum. Côté Apsys, nous considérons que ces deux étapes ne sont pas obligatoires. Le référentiel Airbus est basé sur le principe d'une évaluation d'impact en une seule étape.
- Dans la **formalisation des risques et des scénarios de menace** : la construction des scénarios de risque ne permettait pas de prendre en compte les éléments d'architecture du système et donc l'origine d'un scénario de menace. Ils étaient basés uniquement sur une combinaison de la menace et du composant concerné. Les origines potentielles (interfaces sans fil, réseaux sol, connexions filaires avec d'autres systèmes…) devraient être identifiées dans une étude globale d'architecture.
- Dans le **calcul de la vraisemblance** : l'évaluation de la probabilité d'occurrence d'un risque n'était pas suffisamment justifiée. Des métriques devraient être définies, aussi bien qu'une définition claire de la formule de calcul, pour que l'analyse puisse être reproductible. Chaque critère de calcul devrait être explicitement justifié.
- Dans la **communication des résultats** : lors de la diffusion des résultats de l'analyse de risque aux différentes parties prenantes, il est important d'adapter son message pour des populations non formées à la sécurité et qui attendent des enjeux business. Plusieurs risques de niveau technique devraient être factorisés dans des groupes de plus haut niveau rassemblant des risques avec des caractéristiques communes, en rappelant les impacts sur le business (en se basant sur la table d'impact définie dans le contexte de l'analyse).

D'un point de vue plus humain que méthodologique, mais avec des conséquences au moins aussi lourdes pour la CyberSécurité du produit, nous avons aussi constaté une réelle difficulté à collecter auprès du client les impacts potentiels d'une malveillance, notamment sur un composant critique du système. L'interprétation des conséquences d'un évènement de CyberSécurité n'est pas encore imprégnée dans un secteur encore très tourné vers la sûreté de fonctionnement et la fiabilité plus que vers les menaces cyber.
Il a donc été commandité une série de sessions de formation et de workshops dans le but de faire mûrir une nouvelle méthodologie adaptée au contexte. Le point d'attention était notamment de s'assurer de ne pas être en « over-design » de sécurité et de se doter de la capacité de percevoir les impacts des mesures de sécurité sur le produit dans son ensemble afin de ne pas les multiplier sur chaque composant ou sous-composant.

Méthodologie

1 La méthode SECRAM

Apsys a d'abord cherché à capitaliser sur l'expérience aéronautique d'Airbus. Il a été décidé d'utiliser comme baseline, la méthodologie SECRAM, utilisée de façon globale côté industriel chez Airbus ainsi que dans le cadre d'activité d'audit en sécurité industrielle (dits « Site Surveys ») chez le client). Les objectifs étaient :

- D'affiner l'évaluation des impacts et sa justification au niveau du composant du scénario de menace
- De construire les scénarios de menace en identifiant l'origine du chemin d'attaque
- De prendre en compte la contribution des mesures de sécurité déjà en place dans l'évaluation de la vraisemblance
- D'assurer une répétabilité de l'analyse en définissant et justifiant plusieurs critères d vraisemblance

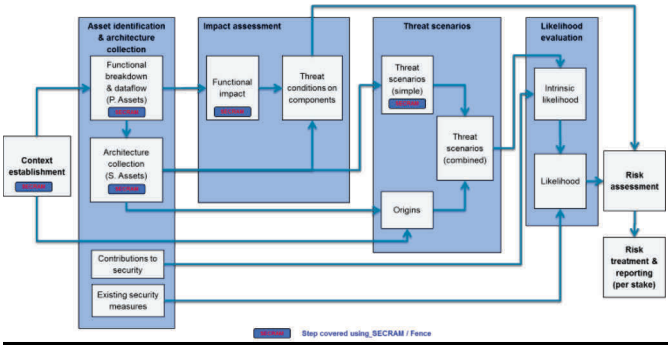

Figure 2. Vue globale de la méthode SECRAM

La méthode SECRAM a ses atouts et est déjà largement utilisée chez Airbus. D'assez haut niveau, elle permet d'identifier facilement dans un système les zones où lancer les projets de sécurisation. Il convient néanmoins de l'adapter pour remplir les objectifs cités plus hauts.

Définition du contexte de l'analyse

Au préalable de chaque analyse, le contexte de l'étude doit être défini en atelier avec les différents managers et process owners. Le contexte comprend :

- La définition des critères d'impacts : les impacts doivent être définis par le business. La définition des enjeux à prendre en compte (Image, Qualité de Service, Safety, Financier…) devrait se faire à un niveau groupe pour assurer une meilleure cohérence entre les analyses
- La définition des critères de vraisemblance : ils vont permettre de définir la probabilité d'occurrence d'un scénario de menace et doivent prendre en compte la contribution des mesures de sécurité
- La définition de la matrice de risque : elle définit les critères d'acceptation du risque en se basant sur les traitements proposés par le standard ISO27005
- Les hypothèses : afin de valider précisément le scope de l'analyse, des hypothèses doivent être formulées et validées par le management
- La taxonomie de menaces : pour définir un scope de scénarios adapté au contexte à prendre en compte, des typologies de menaces sont sélectionnées ou écartées

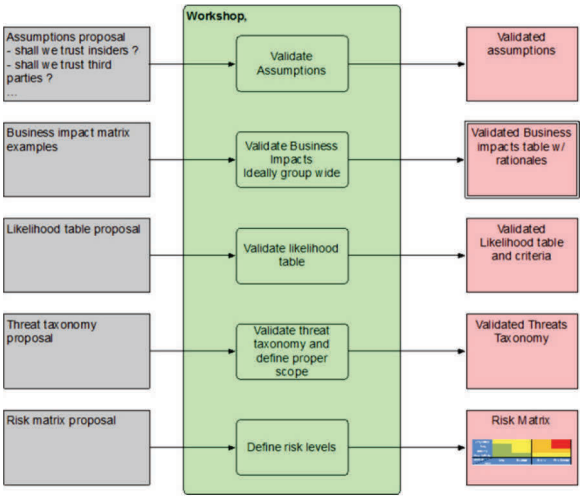

Figure 3. Définition du contexte

1.1 Critères d'impact

Dans le domaine aéronautique, des tables d'impact sont définies et sont exprimées selon les termes employés par le

référentiel de certification. Dans le cas du référentiel ED203, chapitre « Characterization of Threat Conditions and Their Effects », on définit notamment la table suivante pour le critère safety :

Impact level	Safety Consequences
VERY STRONG	CATASTROPHIC as per CS 25.1309 - Loss of the Aircraft - Single or multiple fatalities
STRONG	HAZARDOUS as per CS 25.1309 - Physical damage on the A/C - Injuries of passenger and/or flight crew - Physical distress or higher workload such that the flight crew cannot be relied upon to perform their task accurately or completely - loss of confidence of pilot in A/C control and navigation system
MEDIUM	MAJOR as per CS 25.1309 - Significant increase of flight crew workload with potential reduction of safety margins. - Significant discomfort for passengers or flight crew - loss of confidence of flight or cabin crew in A/C non-essential system
LOW	MINOR as per CS 25.1309 - Slight Increase of flight crew workload - Some inconvenience to the occupants
NO IMPACT	- No safety effect

Table 2. Table d'impact Safety ED203

Concernant le domaine ferroviaire, les analyses de risques CyberSécurité déjà réalisées et les processus de safety déjà existants nous ont amené à considérer une échelle qui soit plus adaptée à l'environnement réglementaire spécifique. Partant du principe que nous devrions avoir la possibilité de nous reposer sur des analyses safety préalables, la gravité des impacts safety est donc indexée sur le niveau de SIL (Safety Integrity Level) des composants systèmes impactés (cf. Table 3). Une autre possibilité aurait été de se reporter directement aux niveaux de conséquences identifiées dans la norme ferroviaire EN 50126, définissant un processus de développement de produits standardisé applicable à l'ensemble des acteurs du secteur.

Impact level	Safety environment
CATASTROPHIC	Fatalities and/or multiples severe injuries and/or major damage to the environment
CRITICAL	Single fatality and/or significant threat to the environment
MARGINAL	Minor injury and/or significant threat to the environment
INSIGNIFICANT	Possible minor injury

Table 3. Table d'impact Safety EN 50126

Les critères d'impact devant être adaptés au business de l'entreprise, ils ont également été repris du contexte d'une ancienne analyse de risque. Ceux retenus sont donc : la safety (potentiels impacts physiques sur les personnes), la qualité de service (interruptions de services à plus ou moins long terme), la finance (pertes financières), l'image (couverture médiatique d'ampleur d'un évènement de CyberSécurité) et légal (poursuites judiciaires suites à un évènement de CyberSécurité).

Level	Safety	Quality of Service	Finance	Image	Legal
1	No safety involvement	Service is slightly disturbed or interrupted for a very short time	No or little impact	Bad internal feedback	Warning
2	No safety impact	Service is degraded or interrupted for a short time	Project issue resolution costs	Bad feedback from passengers	Fine
3	SIL1 or SIL2 event	Service is long-term disrupted	Impact on business activities	Specialized press coverage	Moderate legal impact
4	SIL3 or SIL4 event	Service is interrupted with no putting back to service	Critical losses	Public Media coverage	Critical legal impact

Table 4. Critères d'impact

La méthode SECRAM définit 3 critères de sécurité :

- La confidentialité des données du système analysé
- L'intégrité du système
- La disponibilité du système

L'évaluation des impacts identifie l'impact business maximum possible lors de l'atteinte à un critère de sécurité, et ce pour chaque critère de sécurité.

1.2 Critères de vraisemblance

Pour assurer la justification et la répétabilité du calcul de l'occurrence d'un risque, nous avons choisi d'évaluer tout d'abord une vraisemblance intrinsèque sur la base d'une moyenne des 6 critères suivants, décrits dans les table 5 à 10 :

- L'expertise de l'attaquant (EXP)
- L'équipement nécessaire (EQU)
- La fenêtre d'opportunité (WOO)
- La connaissance de la cible (KOT)
- Le sentiment d'impunité (FOI)
- Le temps de préparation nécessaire (ETI)

Ce qui donne la formule de calcul suivante :

Vraisemblance intrinsèque = $\frac{EXP+EQU+WOO+KOT+FOI+ETI}{6}$ {1}

(Arrondie au chiffre supérieur)

Value	Expertise of the attacker	Description
1	Multiple Expert	Multiple Experts are highly skilled in several fields of expertise (including Product operation) necessary to conduct a complex attack.
2	Expert	Expert has a high and specific knowledge of an attack. The nature of the expertise depends of the type of attack.
3	Proficient	Proficient has general knowledge of information security or Product operation and is familiar with the security behavior of the target of the attack.
4	Layman	Layman has no particular expertise of information security.

Table 5. Définition de l'expertise de l'attaquant

Value	Equipment Means	Description
1	Bespoke equipment	Several specialized equipment, needing large resources and time to develop, assemble or build.
2	Specialized equipment	Equipment which cannot be readily bought even in specialized shops. Equipment may be specially produced or developed, assembled or built for the attack.
3	Specialized COTS	Equipment which can be readily bought, but which is usually not yet in the possession of an average person.
4	None/Standard equipment	No equipment or equipment (hardware or software) commonly already available and/or easy to buy (e.g. a laptop).

Table 6. Définition de l'équipement nécessaire

Value	Window of opportunity	Description
1	Short	The target is rarely accessible and/or during short period.
2	Moderate	The target is often accessible and/or during moderate period.
3	Long	The target is frequently accessible and/or during a long period.
4	Unlimited access	The target is always accessible.

Table 7. Définition de la fenêtre d'opportunité

Value	Knowledge of the target	Description
1	Critical	Information concerning the Target is tightly access controlled to few individuals on a strict need to know basis and individual undertaking.
2	Sensitive	Information concerning the Target is access controlled to limited groups of people inside the Division or project organization, e.g. knowledge that is shared between discreet teams within developer organization, access to which is constrained only to members of the specified teams.
3	Restricted	Information concerning the Target is access controlled to large group of people inside the division or project organization, e.g. knowledge that is controlled within the developer organization under a non-disclosure agreement.
4	Public	Information concerning the Target is publicly available e.g. available on the internet.

Table 8. Définition de la connaissance de la cible

Value	Elapse time	Description
1	Long	The attack is difficult to prepare - elapse time is superior to one month.
2	Moderate	The attack need moderate time of preparation - elapse time is inferior to one month.
3	Short	The attack is easy to prepare - elapse time is inferior to one week.
4	Very Short	The attack is very easy to prepare - elapse time is inferior to one day.

Table 9. Définition du temps de préparation nécessaire

Value	Feeling of impunity	Description
1	Low	Low anonymity: High possibility to be identified and punished.
2	Moderate	Moderate anonymity: Moderate possibility to be identified and punished.
3	High	High anonymity: Low possibility to be identified and punished.
4	Full	Full anonymity: No or few possibility to be identified and punished.

Table 10. Définition du sentiment d'impunité

Certaines de mesures de sécurité peuvent potentiellement être déjà en place et réduire de façon significative la vraisemblance d'un scénario de menace. Pour les prendre en compte de façon significative, nous avons choisi de calculer la vraisemblance finale sur la base de la matrice ci-dessous. Prendre en compte la contribution de mesures de sécurité dans une moyenne non pondérée comme les autres critères n'aurait pas permis de diminuer significativement la vraisemblance avec l'apport de mesures de sécurité.

		Contribution of security measures			
		1	2	3	4
Intrinsic likelihood	1	1	1	1	1
	2	2	1	1	1
	3	3	2	1	1
	4	4	3	2	1

Table 11. Calcul de la vraisemblance finale

Seules les mesures majeures sont considérées. Une contribution de sécurité majeure est une mesure qui :

- Est implémentée avec un niveau de qualité prouvé, comprenant notamment une revue de vulnérabilités pendant le développement
- Est clairement identifiée comme ayant un effet protecteur vis-à-vis du scénario de menace

Pour considérer deux mesures de sécurité pour un même scénario, elles doivent être indépendantes et ne pas avoir de vulnérabilités en commun. Selon la Table 11, chaque mesure de sécurité identifiée permet ainsi de diminuer la vraisemblance intrinsèque calculée avec la formule {1} d'un niveau pour obtenir la vraisemblance finale.

Value	Contribution of security measures	Description
4	Very High	No lack of major security measure identified / More than two major security measure contributing to mitigate the threat scenario are identified
3	High	At least two major security measure contributing to mitigate the threat scenario are identified
2	Medium	At least one major security measure contributing to mitigate the threat scenario is identified
1	Low	No major security measures contributing to mitigate the threat scenario are identified

Table 12. Contribution des mesures de sécurité

1.3 Matrice de risque

Le niveau de risque d'un évènement de CyberSécurité est la combinaison de sa vraisemblance et de l'impact de l'évènement sur les fonctions principales du systèmes en utilisant la matrice ci-dessous.

		Likelihood			
		1 - Very unlikely	2 - significant	3 - likely	4 - very likely
Impact	4 – critical	2	3	4	4
	3 – important	1	2	3	4
	2 – limited	1	2	2	3
	1 – negligible	1	1	2	2

Table 13. Définition de la matrice de risque

On définit ainsi quatre niveaux de risques : **Bas**, **Moyen**, **Haut** et **Très Haut**. En accord avec le standard ISO27005, l'ensemble des risques de niveaux Haut et Très haut seront traités et le traitement choisi et la mitigation. Les risques de niveau moyens seront arbitrés au cas par cas en considérant les enjeux business associés. Les risques de niveau bas sont automatiquement acceptés.
Pour rappel, les traitements possibles proposés par l'ISO 27005 sont les suivants : diminution du risque, évitement, partage et acceptation.

1.4 Hypothèses

Les hypothèses permettent d'expliciter de façon précise les profils d'attaquants à considérer en définissant :

- Le scope : choix de la phase de vie du produit industriel, inclusion ou non du périmètre géré directement par l'IT
- Les personnes : les employés, les sous-traitants, les clients, quelles typologies de personnes sont de confiance ?
- Les menaces : quels types de menaces sont de base écartées (ex : menaces environnementales, attaques physiques…) ?

On répond ainsi aux questions qu'est ce qui me menace et qui me menace.

2 Déroulement de l'analyse

2.1 Identification des assets

L'analyse démarre par l'identification des assets du système étudié. Les assets sont de deux niveaux :

- Les primary assets : les fonctions trains
- Les supporting assets : les éléments matériels, les réseaux, les données, les personnes, les logiciels, tous les éléments possédant les vulnérabilités qui pourront être exploitées par un scénario de menace

Ces assets sont identifiés sur la base de schémas d'architecture / documentations techniques et d'interviews avec les propriétaires de chaque asset. Le but de ces interviews est de collecter l'ensemble des informations techniques permettant d'identifier les points d'entrée, les chemins d'attaque et d'évaluer les différents critères de vraisemblance. Une documentation technique complète permettra d'identifier de façon exhaustive l'ensemble des supporting assets.

Supporting Asset Type
Fixed Hardware
Mobile Hardware
IT Peripheral
Storage Devices
Data
Software
Operating System
Firmware
Network Equipment
Network Link
Personnel
Site
Organization

Table 14. Types de supporting assets

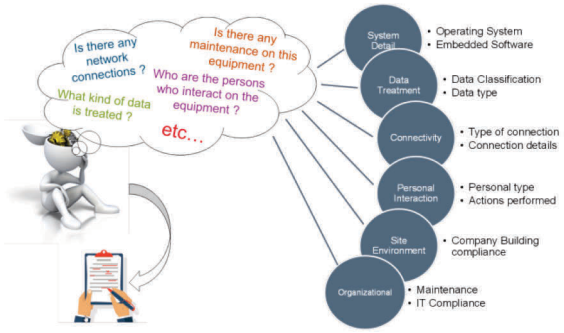

Figure 4. Informations à collecter en interviews

2.2 Evaluation des impacts

Pour l'évaluation des impacts, une nouvelle démarche est formalisée pour cibler plus efficacement les questions permettant d'évaluer les conséquences business d'un évènement « cyber » avec les différentes parties prenantes. L'évaluation des impacts doit être réalisée sur toutes les fonctions haut niveau du train, celles que l'on nomme les primary assets, mais au niveau des composants (supportings assets), en se basant sur :

- Le lien supporting asset / primary asset pour définir l'impact potentiel maximal sur la fonction train
- L'étude, au niveau composant, des conséquences d'une perte ou d'une altération d'un de ses critères de sécurité. Nous appellerons ces conséquences les Threats Conditions.

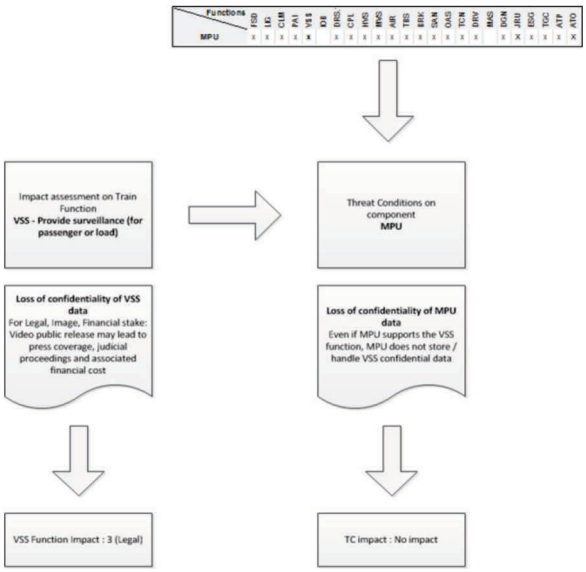

Figure 5. Exemple de Threat Condition

En affinant l'évaluation des impacts au niveau du composant et d'éviter de surévaluer la conséquence d'un scénario de menaces. En effet, un composant contribuant à une fonction train n'est pas forcément critique pour son activité. Les Threats Conditions permettent également une meilleure justification des risques.

2.3 Construction des scénarios de menace

Sur cette base, de nouveaux scénarios de menaces ont été construits de façon chainée en définissant une origine de l'attaque et un chemin d'attaque complet. Tous les scénarios doivent a minima présenter l'origine de l'attaque, que ce soit en termes d'agent de menace, que d'interface exploitée. Les scénarios applicables sont définis dans une démarche en trois étapes :

1) Les scénarios de menaces directs sont d'abord identifiés en déterminant les combinaisons menace / vulnérabilité / supporting asset applicables. Un schéma d'architecture global est d'abord produit pour représenter l'ensemble des domaines et des interfaces exposées dans le cadre de l'étude.
   Les scénarios de menace sont générés automatiquement par notre outil FENCE après avoir renseigné au préalable les primary et supporting assets.
2) Les chemins d'attaque possibles sont identifiés sur la base de cette architecture (définissant les interfaces disponibles), des hypothèses établies dans le cadre du contexte de sécurité (définissant les zones de confiance) et des interfaces exposées.
3) Les scénarios de menaces directs sont alors combinés avec un chemin d'attaque pour lister les scénarios pertinents dans le cadre de l'architecture étudiée, c'est-à-dire des scénarios permettant de visualiser l'origine d'un scénario de menace.

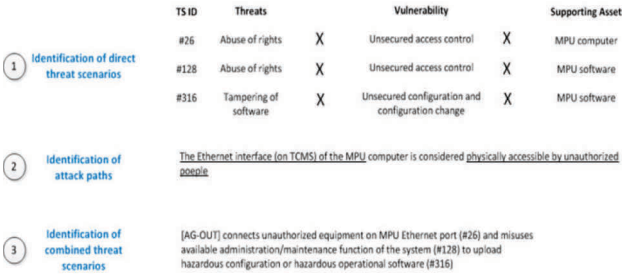

Figure 6. Exemple de construction de scénario de menace

La vraisemblance sera alors calculée sur la base de ces scénarios combinés afin de considérer l'ensemble des éventuelles mesures de sécurité présentes sur le chemin d'attaque.

Les conclusions de l'analyse sont alors présentées aux différentes parties prenantes en groupant les risques évalués par enjeu business. Les matrices de risque s'accompagnement d'un plan de traitement associé, en accord avec ce qui a été défini dans le contexte de l'analyse.

Figure 7. Exemple de restitution

Les risques évalués peuvent également être restitués à un niveau détail plus élevé :

Threat Scenario ID	Description	Origin	Threat Condition	Impact	Likelihood	Risk Level
29	[AG-OUT] connects unauthorized equipment on PTU plug and sends malicious traffic to ATC sub-systems components through the Train network CRS and ATC sub-system CRSv2, in order to perform logical intrusion on ATC.	CRS/GSE equipment - PTU plug	Loss of integrity of ATC/ATP	4	2	3
42	[AG-OUT] connects unauthorized equipment on DCU Ethernet port and misuses available function of the operating system to upload hazardous configuration or hazardous operational software	DCU computer - Ethernet interface (TCMS)	Loss of integrity of DCU	3	2	2
43	[AG-OUT] connects unauthorized equipment on DCU Ethernet port and misuses available administration/maintenance function of the system to upload hazardous configuration or hazardous operational software	DCU computer - Ethernet interface (TCMS)	Loss of integrity of DCU	3	2	2
44	[AG-OUT] connects unauthorized equipment on DCU USB port and misuses available function of the operating system to upload hazardous configuration or hazardous operational software	DCU computer - USB front face interface	Loss of integrity of DCU	3	2	2
45	[AG-OUT] connects unauthorized equipment on DCU USB port and misuses available administration/maintenance function of the system to upload hazardous configuration or hazardous operational software	DCU computer - USB front face interface	Loss of integrity of DCU	3	2	2
142	[AG-OUT] connects unauthorized equipment on ACE TCMS Ethernet port and misuses available function of the operating system to upload hazardous configuration or hazardous operational software	ACE computer - Ethernet interface (TCMS)	Loss of integrity of ACE	3	2	2
143	[AG-OUT] connects unauthorized equipment on ACE TCMS Ethernet port and misuses available administration/maintenance function of the system to upload hazardous configuration or hazardous operational software	ACE computer - Ethernet interface (TCMS)	Loss of integrity of ACE	3	2	2

Table 15. Exemple de restitution

3 Résultats

Le cheminement parcouru aux côtés de notre client et décrit ici, aura duré environ un an. Cette méthodologie a été envisagée et raffinée sur des activités d'analyse de risques pour notre client ferroviaire. Ces activités s'inscrivent dans un processus côté client de définition d'objectifs et de mesures de sécurité à intégrer dans des architectures. Nous ne sommes ni impliqués dans les phrases de définition de spécifications vers les fournisseurs, ni dans les phases de validation et de vérifications, ni dans les phases de mise à jour de l'analyse de risques suite aux développements effectifs des solutions de sécurité. Par conséquent, nous n'avons pas pu mesurer les effets concrets de notre méthodologie sur le niveau effectif de la sécurité des systèmes.

Apsys propose cependant désormais un compromis méthodologique efficace issu de la méthode SECRAM et adaptable aux contextes et aux enjeux différents de chaque client et projet. Les compromis que nous avons identifiés ont pour but d'essayer de rendre l'analyse de risques plus pertinente en maitrisant le temps nécessaire pour réaliser l'étude, pour éviter une explosion des coûts. A ce titre, les compromis dont fait état la méthodologie proposée sont les suivants :

- L'utilisation de scénarios « de bout en bout » est un élément supplémentaire par rapport à la méthodologie SECRAM, qui est basée sur une génération automatique de scénarios unitaires de type « Menace x Vulnérabilité x Supporting Asset ».Toutefois, le composition des scénarios end-to-end est réalisée sur la base des scénarios unitaires et leur composition est manuelle et laissée sous la responsabilité de l'analyste. Nous n'avons pas décidé de passer par une génération automatique de scénarios end-to-end dans le but de ne pas avoir d'étape où la combinatoire génèrerait un nombre énorme et ingérable de scénarios.
- Les vraisemblances ne sont calculées que sur les scénarios « de bout en bout », pas sur les scénarios unitaires. Ainsi, on considère l'ensemble des mesures (effectives ou théoriques) proposées par l'architecture de sécurité pour l'évaluation des risques.
- La formule de calcul de vraisemblance par le biais d'une table à double entrée (Table 11) est un moyen d'éviter une sous-pondération du critère « Contribution des Mesures de Sécurité » par rapport aux autres. Il s'agit d'un compromis entre une formule fonctionnant par moyenne (SECRAM) et une formule plus complexe, telle que définie dans le document ED203.

Conclusion

Un des points essentiels à souligner est que chaque méthodologie a ses avantages et ses inconvénients et qu'il est important d'en disposer de plusieurs. Il est utile notamment de disposer d'une méthodologie assez haut niveau pour commencer par identifier les grandes zones de projets de transformation à mener, avant d'utiliser une méthodologie plus bas niveau pour pouvoir définir les spécifications système.

Il est également important de noter que toute méthodologie doit être complétée par un outillage adapté et spécialisé permettant la réutilisabilité et l'alignement des contextes au travers des différents projets. A ce jour, Apsys dispose de l'outil d'analyse de risque sécurité Fence.

Enfin, d'un point de vue gouvernance, la clé de tout projet d'analyse de risque en sécurité informatique réside dans la capacité à faire accepter l'ensemble de la méthodologie auprès de toute la chaine de décision de l'entreprise : depuis le top management, jusqu'aux ingénieurs spécialisés.

4 Remerciements

Julien CHASTAGNIER, Operation Manager, APSYS-AIRBUS
Loïc DEJEAN, Technical Advisor Risk, APSYS-AIRBUS

5 Références

ANSSI, 2010, EBIOS, Expression des Besoins et Identification des Objectifs de Sécurité – Méthode de gestion des risques
ED 203 (AIRWORTHINESS SECURITY METHODS AND CONSIDERATIONS), 2015
ISO27001,2013
EUROCONTROL, AIRBUS, AENA, NATMIG, NORACON, SESAR ATM Risk Assessment Methodology (SecRAM)