Processus d'interconnexions entre Safety et Cybersecurity sur des systèmes Air Defense et Air Traffic Management

Joanna Peres, Frédéric Motte

Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

Processus d'interconnexions entre Safety et Cybersecurity sur des systèmes Air Defense et Air Traffic Management

Interaction process between Safety and Cybersecurity about Air Defense and Air Traffic Management systems

PERES Joanna
THALES Land & Air Systems/SIAM Safety
Rungis
joanna.peres@thlaesgroup.com

MOTTE Frédéric
THALES Land & Air Systems/SIAM Cyber
Rungis
frederic.motte@thlaesgroup.com

Résumé — Cette démarche d'interconnexion entre les processus Safety et Cybersecurity a été élaborée dans le but de garantir un niveau de protection sécuritaire maximal des systèmes, tout en conservant les bases de chacune des disciplines ainsi que leurs processus classiques. La méthode se décompose en 9 points d'étapes : Réunion de lancement, Partage des événements redoutés, Socle commun, Vérification croisée, Solution design, Evolutions, Tests, Réunion de clôture et Suivi. Un cas pratique de mise en œuvre réelle et complète de la démarche a été réalisé sur un système de type Air Defense. Le résultat a été jugé concluant pour le projet et Thales souhaite dorénavant procéder à la généralisation de son application sur l'ensemble des systèmes Air Defense et Air Traffic Management concernés.

Mots-clefs — Safety, Cybersecurity, Processus, Interconnexions, Use case

Abstract — The aim of this interaction process between Safety and Cybersecurity is to assure a maximal protection level of systems, while keeping the basis of each discipline and their legacy processes. The method consists of 9 steps : Kick-off, Share feared events, Baseline, Cross-check, Solution design, Evolutions, Tests, Closure and Monitoring. A complete and practical case study has been performed on an Air Defense system. The results are conclusive and so Thales wants to generalise this process to the overall concerned Air Defense and Air Traffic Management systems.

Keywords — Safety, Cybersecurity, Processus, Interaction, Use case

I. INTRODUCTION ET CONTEXTE

Aujourd'hui, la Safety et la Cybersecurity sont deux disciplines indispensables à considérer durant la conception et le développement des systèmes. Elles ont des périmètres distincts (gestion d'incidents involontaires versus traitement d'actes volontaires de malveillance numérique) et des dossiers d'analyses indépendants. Cependant, des interdépendances existent entre elles et, si cette réalité n'est pas prise en compte, cela peut conduire potentiellement à des failles de Sécurité (Safety/Cyber).

Les normes et réglementations ont commencé à intégrer des solutions pour concilier ces deux disciplines comme la CLC/TS 50701 [1] dans le domaine ferroviaire, qui décrit les différentes mesures de Cybersecurity à appliquer dans le cadre du processus de cycle de vie FMDS (Fiabilité, Maintenabilité, Disponibilité, Sécurité/Safety) de la norme EN 50126-1 [2]. Le nucléaire avec la norme IEC 62859 [3] propose un cadre de travail permettant de gérer les interactions entre la Safety et la Cybersecurity pour les systèmes dans les NPP (Nuclear Power Plant), ou encore la S-CAT 12805 [4] applicable aux bâtiments de la Marine Nationale qui demande une analyse Safety et Cybersecurity conjointe. Néanmoins, l'adoption de ces nouveaux procédés nécessite la modification plus ou moins forte des pratiques actuelles pour l'une, voire les deux disciplines. Cela représente donc

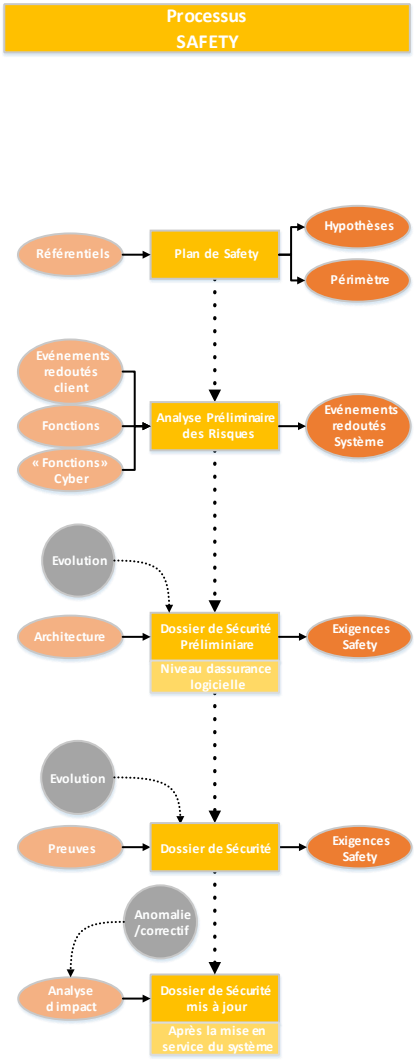
un coût non négligeable et du temps pour la mise en place, ainsi que la sensation par certains acteurs de devoir s'adapter à de nouveaux processus imposés par une autre discipline.

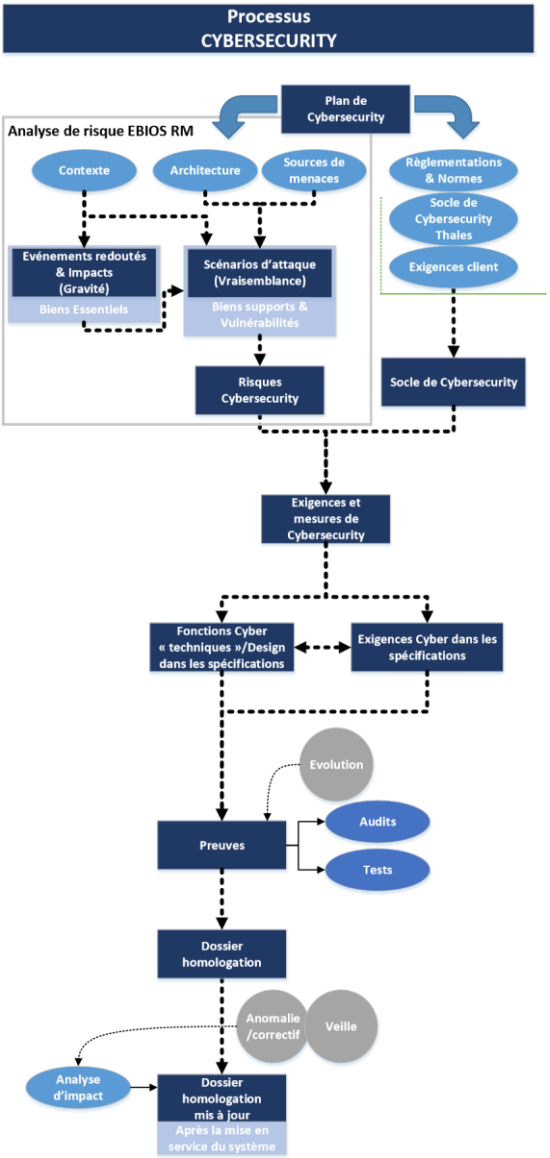
Pour ses systèmes Air Defense et Air Traffic Management, l'objectif de Thales était de définir un processus d'interconnexions entre la Cybersecurity et la Safety qui s'affranchisse de la complexité de mise en œuvre que peuvent apporter les normes. De plus, Thales avait la volonté de s'appuyer directement sur ses processus bien ancrés de Cybersecurity et Safety, dont la maturité est élevée et reconnue. Ainsi, Thales a fait le choix de mettre en place une démarche se rapprochant d'une gestion de type ERM. Cela a permis d'atteindre le niveau de souplesse souhaité et de conserver les cycles existants des deux disciplines en fixant des points de rencontre entre elles.

II. METHODOLOGIE

A. Présentation globale de la méthode

Chaque discipline possède ses propres référentiels/méthodologies (EBIOS RM [5], DIRCAM4150 [6], MIL-STD882 [7], ARP-4751 [8]…) ainsi que ses processus internes Thales, qui sont déployés et éprouvés depuis de nombreuses années. Pour bâtir une procédure sur des bases robustes et ne pas bouleverser l'ordre actuel au sein des différentes équipes, nous sommes repartis de l'existant :


Processus
SAFETY
Référentiels
Plan de Safety
Hypothèses
Périmètre
Evénements redoutés client
Fonctions
« Fonctions» Cyber
Analyse Préliminaire des Risques
Evénements redoutés Système
Evolution
Architecture
Dossier de Sécurité Préliminiare
Niveau dassurance logicielle
Exigences Safety
Evolution
Preuves
Dossier de Sécurité
Exigences Safety
Anomalie /correctif
Analyse d impact
Dossier de Sécurité mis à jour
Après la mise en service du système


Processus
CYBERSECURITY
Plan de Cybersecurity
Analyse de risque EBIOS RM
Contexte
Architecture
Sources de menaces
Règlementations & Normes
Socle de Cybersecurity Thales
Exigences client
Evénements redoutés & Impacts (Gravité)
Biens Essentiels
Scénarios d'attaque (Vraisemblance)
Biens supports & Vulnérabilités
Risques Cybersecurity
Socle de Cybersecurity
Exigences et mesures de Cybersecurity
Fonctions Cyber « techniques »/Design dans les spécifications
Exigences Cyber dans les spécifications
Evolution
Preuves
Audits
Tests
Dossier homologation
Anomalie /correctif
Veille
Analyse d'impact
Dossier homologation mis à jour
Après la mise en service du système

?

Les activités inter-disciplines nécessaires ont été identifiées puis ajoutées afin d'avoir une gestion du risque globale.

Cette démarche met ainsi en perspective neuf points d'étape nécessaires devant être mis en œuvre au minimum afin de créer des interconnexions entre la Cybersecurity et la Safety. Par ailleurs, le management des risques (liés aux malveillances ou aux défaillances du système étudié) étant le cœur de métier des acteurs des deux disciplines, la structure de leurs processus respectifs a été aisément intégrable dans un protocole de gestion des risques de type ERM :

1. Identification des risques
2. Analyse des risques
3. Traitement des risques
4. Contrôle/monitoring des risques

Son niveau d'exécution a été ajusté au plus près des besoins techniques Safety/Cyber du système étudié et a été intégré dans un processus de gestion des risques plus global/macroscopique à l'échelle du projet (intégration de l'ensemble des risques : financier, technique, juridique, écologique…).

Cette réalisation a nécessité le concours d'experts des deux disciplines, afin que le processus soit partagé et générique pour une applicabilité sur des systèmes Air Defense et Air Traffic Management :

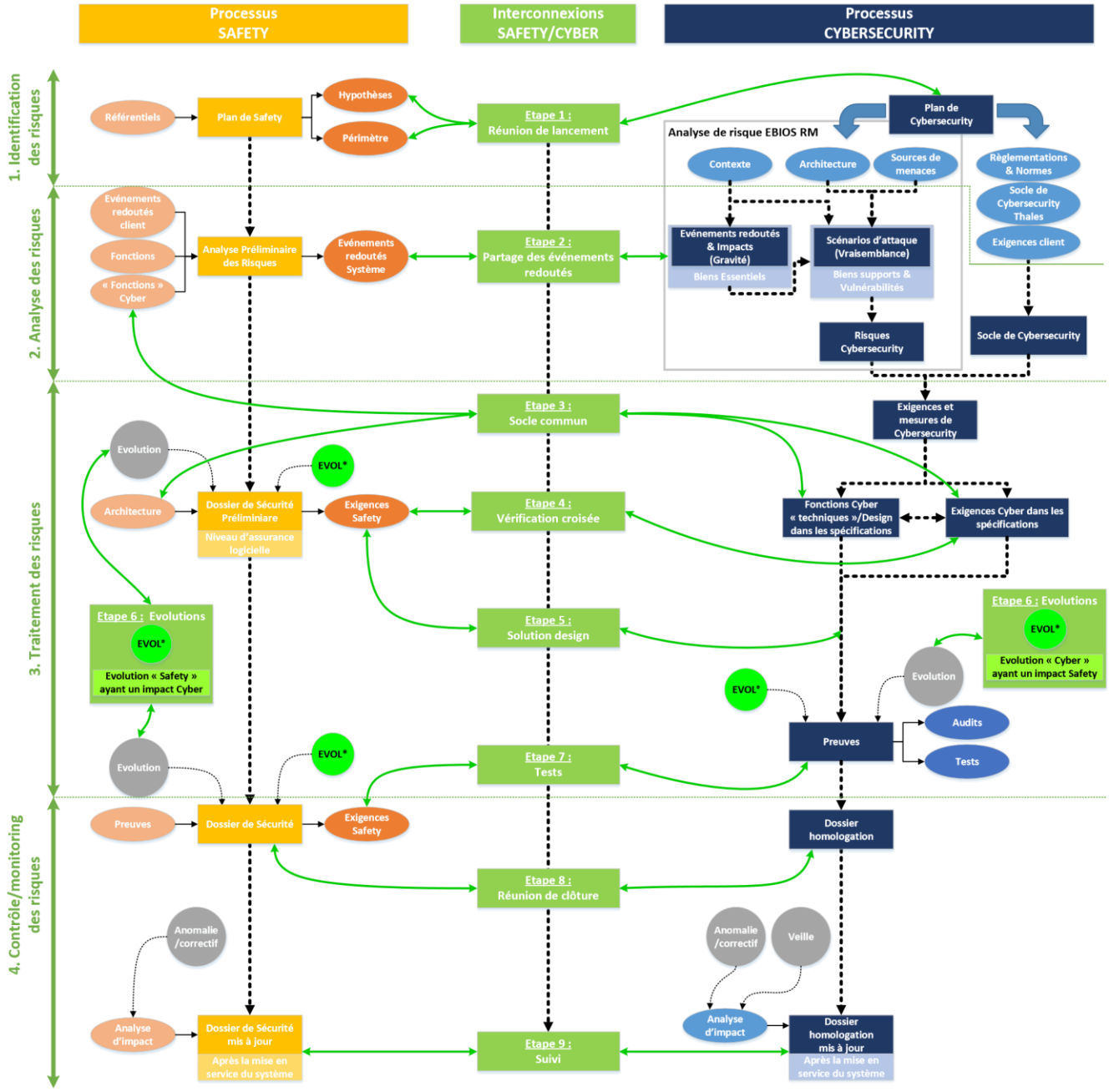


Fig. 2. Processus d'interconnexions entre la Cybersecurity et la Safety

B. Présentation détaillée de la méthode avec un cas pratique

Le fait que cette démarche d'interconnexions se base sur les activités existantes de la Cybersecurity et de la Safety, dont le déroulement correspond déjà à un processus de gestion des risques, a permis de la déployer rapidement et d'obtenir l'adhésion des différents acteurs. Un cas pratique de mise en œuvre réelle et complète de la méthode, a été réalisé sur un système Air Defense (cf. Fig. 3) afin de pouvoir évaluer concrètement les gains de ces nouvelles interactions et les axes d'améliorations. Les résultats de chaque étape sont présentés avec des exemples ciblés d'application (les résultats détaillés sont confidentiels industrie).

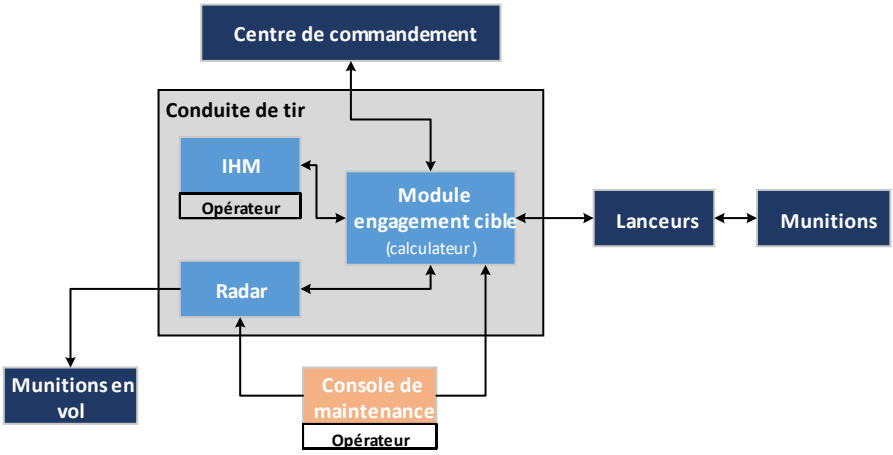


Fig. 3. Structure du système Air Defense du cas pratique

1. *Identification des risques*

Etape 1 : Réunion de lancement

Le but de cette première étape est de créer le dialogue entre les acteurs de la Cybersecurity et de la Safety en phase amont du projet. En se basant sur les stratégies décrites dans le Plan de Safety et le Plan de Cybersecurity du projet (cf. Fig. 2), chacune des disciplines présente le périmètre de ses activités sur le projet (contexte, hypothèses, limitations…), afin de définir le périmètre des analyses Safety/Cyber à mener et de s'assurer de leur bonne cohérence.

Dans le cadre de cette étude, la réunion de lancement a explicité pour les analyses Safety/Cyber :

- Le **périmètre** : Conduite de tir du système Air Defense dont les sous-systèmes sont le radar, l'IHM et le module d'engagement de la cible (cf. Fig. 3) ;
- Les **limitations/hypothèses** : Seuls les scénarios pour lesquels le système est utilisé en « temps de paix » sont étudiés (les scénarios en « temps de guerre » étant uniquement applicables pour la Cybersecurity) ;
- Les **objectifs** : ○ Obtenir une meilleure maîtrise globale des risques liés aux aspects sécuritaires (Safety et Cybersecurity) ; ○ Compléter les analyses de Safety du système Air Defense en y introduisant des compléments relatifs aux scénarios de Cybersecurity (cyberattaques, intrusions externes dans les systèmes d'informations…) ;
  - ○ Enrichir les études de Cybersecurity du système Air Defense en y intégrant les scénarios liés à la Safety (accidents résultants de défaillances fonctionnelles, matérielles ou logicielles…) ; ○ Suivre ces interconnexions Safety/Cyber durant le cycle de vie du système Air Defense ;
- Les **référentiels** applicables : ○ Cybersecurity : EBIOS RM [5] ; ○ Safety : MIL-STD882E [7] ;
- Le **pilotage** des interconnexions Safety/Cyber : Pilotage conjoint entre l'acteur référent Cybersecurity et celui Safety avec une supervision des autorités du projet.

Cette première étape a ainsi apporté une vision précise aux acteurs de chaque discipline avec une liste exhaustive des soussystèmes en commun et nécessitant une interconnexion forte.

2) Analyse des risques

Etape 2 : Partage des événements redoutés

Les études de Safety ne traitant que des actes accidentels involontaires (défaillances, agressions externes, erreurs humaines) et non d'actes volontaires, les cas d'actes de malveillance qui aboutissent à des accidents relatifs à la Safety ne sont pas traités par les analyses Safety.

Cette étape permet de pallier cette problématique en communiquant de manière systématique les événements redoutés du système (scénarios relatifs à la Safety identifiés dans l'Analyse Préliminaire des Risques de la Safety cf. Fig. 2) aux acteurs de Cybersecurity (en s'assurant de la correcte interprétation entre les différentes équipes), ainsi que l'impact et la gravité associés.

Ces événements redoutés Safety sont ensuite intégrés au processus de Cybersecurity EBIOS RM [5] et sont traités comme des risques « classiques » de Cybersecurity (cf. Fig. 2), seule leur origine est différente.

Dans le cas d'étude pour le système Air Defense, cette étape a été particulièrement importante car les événements redoutés Safety étaient trop abstraits pour être intégrés directement dans les études de Cybersecurity, qui ne possédaient pas la vue fonctionnelle et logique du système. Une phase de raffinement de ces événements redoutés Safety en événements redoutés Cyber fonctionnels a été nécessaire.

Pour réaliser le partage des événements redoutés avec les acteurs des deux disciplines (dont les exemples de résultats sont présentés dans les Tableau 1 et Tableau 2), les étapes suivantes ont été définies :

- Présenter les événements redoutés Safety ainsi que leurs gravités ;
- Décrire les fonctionnalités et flux/messages impactés ;
- Associer des actions de malveillance en lien avec chaque événements redoutés Safety ;
- Créer des événements redoutés Cybersecurity plus proche du fonctionnel et des équipements impactés ;
- Attribuer une gravité aux événements redoutés Cybersecurity fonctionnels en tenant compte du degré de menace de l'attaquant défini dans les analyses de Cybersecurity.

Evénement redouté Safety			Evénement redouté Cybersecurity	Gravité
ID	Description	Gravité		
ER_1-1	Ordre de tir impestif envoyé au lanceur	Critique	Envoi d'un ordre de tir malveillant	4
			Corruption de la communication entre le module d'engagement et le lanceur	4
…	…	…	…	…
ER_3-1	Radiation du radar dans une zone d'émission interdite	Majeure	Corruption de la zone d'émission interdite	3
			Désactivation malveillante de la zone d'émission interdite	3
			Neutralisation/corruption de la communication entre le module d'engagement et le radar	3
…	…	…	…	…

Tableau 1. Exemples de partage des événements redoutés Safety

Evénement redouté Cybersecurity	Gravité	Equipement/Liaison							
		Module engagement	Radar	IHM	Module engagement-Radar	Module engagement-Lanceur	Module engagement-Centre commandement	Module engagement-IHM	Radar-Munition en vol
Envoi d'un ordre de tir malveillant	4	X	-	-	-	X	-	-	-
Corruption de la communication entre le module d'engagement et le lanceur	4	-	-	-	-	X	-	-	-
…	…	X	X	-	X	-	X	-	-
Corruption de la zone d'émission interdite	3	X	X	-	-	-	-	-	-
Désactivation malveillante de la zone d'émission interdite	3	X	X	-	-	-	-	-	-
Neutralisation/corruption de la communication entre le module d'engagement et le radar	3	-	-	-	X	-	-	-	-
…	…	-	-	X	-	-	-	X	X

Tableau 2. Exemples de traçabilité entre des événements redoutés Cybersersecurity fonctionnels et les équipements/liaisons

Grâce à cette étape, les événements redoutés du système ont donc un traitement de la Safety ainsi que de la Cybersecurity, renforçant le niveau de protection sécuritaire garanti : chacun des 14 événements redoutés Safety est lié à au moins l'un des 29 événements redoutés Cybersecurity fonctionnels et leur traçabilité est exhaustive. Ce deuxième point d'interconnexion a ainsi permis :

- A la discipline Cybersecurity : d'effectuer une traçabilité concrète entre ses risques de malveillances et les fonctionnalités du système qu'ils impactent ;
- A la discipline Safety : de prendre conscience des menaces de Cybersecurity qui sont liées à ses événements redoutés et de la surface d'attaque associée.

3) Traitement des risques

Etape 3 : Socle commun

Les événements redoutés Safety et les risques de Cybersecurity étant partagés, le but de cette étape est de s'assurer que ces analyses ont été effectuées avec le même référentiel (spécifications, fonctionnalités…) et continueront de l'être. Sans cela, ces études inter-disciplines seront nécessairement incomplètes car basés sur une architecture erronée.

Dans le cas d'étude pour le système Air Defense, les vérifications ont été réalisées à deux niveaux :

- Confirmer que la Cybersecurity n'a pas ajouté de nouvelles fonctionnalités cyber dans les spécifications au gré des analyses de Cybersecurity, et qui n'auraient pas été analysées dans l'Analyse Préliminaire des Risques de la Safety (cf. Fig. 2). Par exemple, ce point d'étape a permis de détecter que l'implémentation d'un protocole fiable entre deux composants du système par les acteurs Cybersecurity, n'avait pas été identifié dans les spécifications. Ce protocole fiable a un impact sur les analyses Safety car il diminue la corruption et la perte de message en cas de défaillance ;
- Confirmer que la Cybersecurity n'a pas modifié le design dans les spécifications pouvant avoir un impact sur l'architecture, et qui n'aurait pas été analysé dans le Dossier de Sécurité Préliminaire de la Safety (cf. Fig. 2).

Cette interconnexion permet ainsi de valider un socle commun de travail et de s'assurer de sa correcte prise en compte par les analyses de la Safety. Le cas échéant, ces interconnexions régulières permettent de mettre en évidence les écarts suffisamment en amont du projet pour que le sujet soit appréhendé avec un impact raisonnable sur le planning.

Etape 4 : Vérification croisée

Cette étape permet de garantir une traçabilité ainsi qu'un suivi rigoureux des exigences ayant un double lien Cybersecurity et Safety via un tag. La double vérification pour notre cas d'étude se décompose en deux parties :

- L'ajout d'un tag « Safety » sur les exigences de la Cybersecurity ayant un lien avec un événement redouté Safety communiqué précédemment dans l'étape 2 : Partage des événements redoutés. Les acteurs Cybersecurity ont ainsi directement l'information du caractère Safety de leurs exigences ;

Type	SSS ME Text	Object Type	Tag
	3.4.3.1.4 Network	Heading	
CYBERSECURITY	The design of the ..... Module network shall be compliant with the ..... guide.	Requirement	
	END_REQ	END_REQ	
CYBERSECURITY	Equipment connected to a same LAN shall be separated in different logical subnets defined by criteria as a function or a level of sensibility.	Requirement	SAFETY
	END_REQ	END_REQ	
CYBERSECURITY	For the ..... , the minimal implementation shall be four partitioned subnets: • ..... • ..... • ..... •	Requirement	SAFETY

Fig. 4. Exemple d'exigences Cybersecurity ayant un tag « Safety » dans l'outil DOORS

- L'émission d'un tag « Cyber » sur les exigences Safety (issues du Dossier de Sécurité Préliminaire de la Safety cf. Fig. 2) uniquement dans les cas suivants :
  - Un événement redouté Safety est nouveau, modifié ou supprimé ;
  - Un potentiel impact sur l'architecture dû à la Safety est identifié : composant nouveau/supprimé ou interface nouvelle/supprimée ;

  Les acteurs Safety ont ainsi directement l'information du caractère Cybersecurity de leurs exigences et les communiquent systématiquement à la Cybersecurity pour une analyse d'impact plus approfondie.

Type	SSS ME Text	ObjectType	Tag
	3.4.6.1 Feared event "Inadvertent elaboration of an engagement order from the FCU"	Heading	
SAFETY	The probability of failure of the ..... leading to have the ..... in the wrong status shall be	Requirement	CYBER
SAFETY	The probability of the ME HW involved in the safety function ..... that leads to consider the wrong position of the	Requirement	
SAFETY	The probability of failure of ME HW involved in the stop the engagement sequence when	Requirement	

Fig. 5. Exemple d'une exigence Safety ayant un tag « Cyber » dans l'outil DOORS

Dans le cas d'étude pour le système Air Defense, grâce à l'outil DOORS, un tag « Safety » a été ajouté sur 65% des exigences de Cybersecurity et un tag « Cyber » a été émis sur 10% des exigences de Safety.
Peu de cas répondant aux critères tag « Cyber » listés ci-dessus se sont présentés. Una analyse avec les acteurs Cybersecurity a confirmé que ces critères correspondent au juste besoin et que, par conséquent, il n'y a pas de cas qui auraient été oubliés (les 10% sont corrects).

La suite de cette étape a consisté en l'identification des exigences Safety/Cyber en doublon (sur-spécification), antagonistes (conflit) et complémentaires (efficience : exigence Cybersecurity qui répond à un besoin de la Safety, alors que la Safety a des difficultés pour l'atteindre seule, et inversement).
Le fait d'avoir réalisé la double vérification et de l'avoir effectué via un outil, a permis de mener cette activité de comparaison plus rapidement. Par exemple dans notre cas d'étude, des exigences Safety et Cybersecurity demandaient en doublon la mise en place de procédés dans le but de garantir l'intégrité des données. Ces exigences étant séparées par de nombreux paragraphes et ayant des formulations différentes, la détection manuelle était complexe mais les tags ont permis de présenter automatiquement ce cas.

L'ensemble de cette étape a garanti le maintien d'une traçabilité des interconnexions entre les deux disciplines et un renfort sur la gestion globale des exigences sécuritaires.

Etape 5 : Solution design

Dans le cas d'étude pour le système Air Defense, ces réunions Solution design ont été déclenchées de manière systématique par les acteurs de la Cybersecurity avec ceux de la Safety, lorsque des solutions techniques Cybersecurity (architecture ou fonctionnalités) devaient être choisies, et que ces dernières pouvaient avoir un impact sur la Safety. Une analyse d'impact de cette solution technique Cybersecurity est menée par la Safety sur ses exigences et mesures de réduction de risque. Par exemple, le choix d'utilisation d'un firewall, dont le niveau d'assurance logicielle n'est pas compatible avec les besoins de la Safety (antagonisme), a fait l'objet de cette étape.

Etape 6 : Evolutions

L'objet de cette étape est de pouvoir identifier puis analyser les évolutions ayant un double impact Cybersecurity et Safety. Ce point de rencontre pour notre étude de cas se décompose en deux catégories :

- L'identification des évolutions « Cybersecurity » ayant des conséquences potentielles sur la Safety (cf. EVOL* dans la Fig. 2), c'est-à-dire possédant un lien avec les événements redoutés Safety et/ou les exigences avec un tag « Safety » identifiés lors des points de rencontre précédents. Les acteurs de la Cybersecurity doivent communiquer l'ensemble de ces EVOL* à la Safety pour que l'impact sur ses études puisse être analysé ;

- L'identification des évolutions « Safety » ayant des conséquences potentielles sur la Cybersecurity (cf. EVOL° dans la Fig. 2), c'est-à-dire ayant un tag « Cyber » et/ou répondant aux critères suivants :
  - Absence ou retrait d'une mesure de sécurité (au sens Cybersecurity) ;
  - Anomalie sur une mesure de sécurité (au sens Cybersecurity) ; o Apparition d'une vulnérabilité.

  Les acteurs de la Safety doivent communiquer l'ensemble de ces EVOL° à la Cybersecurity pour que l'impact sur ses études puisse être analysé.

Par ailleurs, les acteurs de la Cybersecurity doivent systématiquement fournir à la Safety les évolutions associées aux exigences ayant un tag « Safety », et inversement pour les tags « Cyber ».

Pour le cas d'étude du projet Air Defense, cet exercice a permis de montrer que :

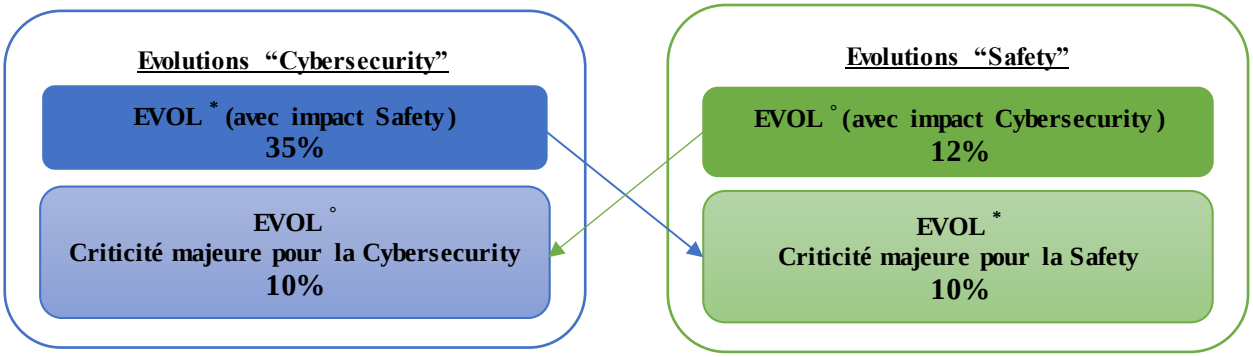


Fig. 6. Liens entre les différents types d'évolutions

Ces évolutions ont ainsi pu être traitées suffisamment en avance pour ne pas impacter le planning du projet et sans que cela nécessite une analyse dans l'urgence. Par ailleurs, la gestion des évolutions étant gérée grâce à un outil informatique pour le projet Air Defense, les échanges entre les différents acteurs. Cet échange interdisciplinaire des EVOL* et EVOL° est essentiel pour garantir un niveau de protection sécuritaire maximal au système.

Etape 7 : Tests

L'objectif de cette étape est de suivre les exigences avec un tag « Safety » ou « Cyber » pendant les phases de rédaction ainsi que de passage des tests, et donc d'avoir une traçabilité complète (phases descendante et remontante du cycle en V) de ces exigences.

Les résultats des tests ayant un double impact Safety/Cyber doivent être vérifiés de manière renforcée. Une attention particulière sera à apporter lorsque les tests ou audits sont négatifs via l'analyse des évolutions (analyses d'impact, analyses de vulnérabilités…).

Cette étape a permis de compléter les résultats de tests du Dossier de Sécurité de la Safety (cf. Fig. 2). Les acteurs Cybersecurity se sont auparavant assurés que tous les résultats des tests concernés étaient corrects et justifiés.

4) Contrôle/monitoring des risques

Etape 8 : Réunion de clôture

Avant la mise en service du système, ce point de rencontre a pour but de réunir les acteurs de la Cybersecurity et de la Safety afin de valider de manière commune que l'ensemble des analyses Safety/Cyber a été mené selon le périmètre défini lors de la réunion de lancement (Etape 1). Cette étape permet également de capitaliser les résultats obtenus pour les prochains projets.

Les événements redoutés Safety sont totalement couverts (aspects défaillances et malveillances) et documentés via le Dossier de Sécurité de la Safety et les risques de la Cybersecurity sont traités via le Dossier d'homologation (cf. Fig. 2).

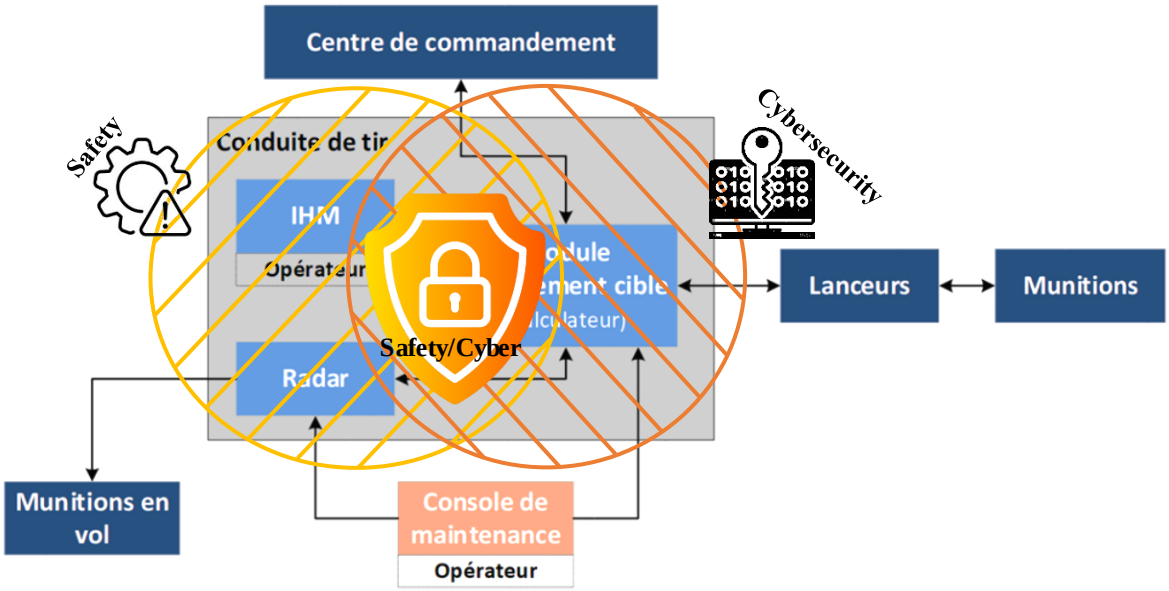


Fig. 7. Couverture sécuritaire globale Safety et Cybersecurity

Etape 9 : Suivi

Lorsque le système est en service, des analyses d'impacts sont réalisées par la Cybersecurity et la Safety suite à la découverte d'anomalies ou de nouvelles vulnérabilités. Le Dossier de Sécurité de la Safety et le Dossier d'homologation sont alors mis à jour en conséquent si nécessaire.

L'objectif de cette dernière étape Safety/Cyber est de continuer à partager entre les deux disciplines ces modifications qui auraient un double impact en utilisant les mêmes critères que ceux définis lors de l'Etape 6 : Evolutions. Ainsi, la protection globale sécuritaire du système est maintenue et garantie y compris après la mise en service.

III. DISCUSSION ET PERSPECTIVES

Suite à cette première application concrète de la démarche a été globalement jugée concluante. Les acteurs Safety et Cybersecurity ont validé le fait que l'implémentation des interconnexions ne nécessitant pas de fortes modifications dans les processus existants, la gestion des risques Safety/Cyber a pu rapidement et aisément être mis en œuvre. Ils ont constaté qu'en moyenne sur une année, la charge supplémentaire induite par ces activités équivalait à une journée par mois (réunions et analyses incluses). En contrepartie, cela a permis de maîtriser en amont des problématiques (protocole fiable, firewall, évolutions…) qui auraient été traitées dans l'urgence en impactant le planning du projet dans un processus classique (c'est-à-dire sans interconnexions). Les différents acteurs (y compris les architectes et les chefs de projet) ont conclu que cette démarche d'interconnexions Safety/Cyber a généré un gain de temps non négligeable, notamment grâce à la détection et au traitement en amont des problématiques majeures.

Cependant, cette première mise en œuvre réelle et complète de la méthode a permis de mettre en évidence certains points d'améliorations à prendre en considération. En effet, les aspects de modélisation du système n'ont pas été abordés. A ce jour, il n'est pas trivial de trouver un outil de type MBSE qui réponde à la fois aux besoins de modélisations de la Safety (représentation exhaustive des interfaces, des fonctions et des flux du système, architecture détaillée…) avec ceux de la Cybersecurity (chemins d'attaques, représentation des différentes couches logiques, gestion dynamique…). Un groupe de travail est en cours au sein des équipes Thales afin de travailler sur ce sujet.

Une autre étape qui apparaît comme étant à faire évoluer est celle concernant les tests. A l'issue de ce premier échange de résultats de tests/audits, les acteurs Cybersecurity et Safety ont constaté que des mutualisations pouvaient être effectuées (tests d'une discipline couvrant également des exigences de l'autre) et que, si la démarche était suivie, cela n'impliquait pas une surcharge de travail. Dans cette même optique, la Safety utilise des checklists ainsi que des règles de codage pour une partie de l'activité d'assurance logicielle qui pourraient également servir pour les besoins des acteurs Cybersecurity. Un autre groupe de travail Thales a débuté pour étudier la faisabilité de ces différentes activités liées aux tests.

IV. CONCLUSION

Ce processus d'interconnexions commun entre la Safety et la Cybersecurity a permis de garantir un niveau de protection sécuritaire maximal des systèmes Air Defense et Air Traffic Management, tout en conservant les bases de chacune des disciplines, et sans impliquer la mise en place de nouvelles analyses/activités complexes ou chronophages. Il existe une meilleure traçabilité entre les risques induits par la Safety et ceux de la Cybersecurity, ainsi qu'une gestion des impacts communs.

Son application concrète sur notre cas d'étude Air Defense a permis notamment d'apporter une double couverture des événements redoutés Safety et une gestion anticipée des exigences en doublon ou antagonistes entre les deux disciplines. Ce premier passage de la démarche a été bénéfique pour le projet et Thales souhaite dorénavant procéder à la généralisation de son application sur l'ensemble des systèmes Air Defense et Air Traffic Management concernés.

En parallèle, des réflexions sont en cours sur la possibilité d'intégrer les aspects de modélisation du système à ce processus, ainsi que l'amélioration des tests effectués.

V. BIBLIOGRAPHIE

[1] CLC/TS 50701, Railway applications – CyberSecurity (2023)

[2] NF EN 50126-1, Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) Partie 1 : Processus FMDS générique (2017)

[3] NF EN IEC 62859, Centrales nucléaires de puissance - Systèmes d'instrumentation et de contrôle-commande - Exigences pour coordonner sûreté et cybersécurité (2020)

[4] DGA, S-CAT 12805, Référentiel technique et réglementaire appliqué aux bâtiments de la Marine Nationale – Objectifs de sécurité, édition 1.0, 2017

[5] ANSSI, EBIOS RM, version 1.1 (2018)

[6] DSAÉ, DIRCAM4150, Processus de supervision et de réalisation des études de sécurité des prestataires de services de la navigation aérienne de la défense (2022)

[7] DoD, MIL-STD882, version E (2012)

[8] SAE, ARP4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment (1996)