Ecole Nationale de l'Aviation Civile

La référence aéronautique

TLS-SEC

Sûreté/Security et Sécurité/Safety

Ladislas HAJNAL

2020

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Objectifs

At the end of the presentation the student will

- Discuss the differences and similarities between safety and security
- Acknowledge the need for optimisation
- Explain the standards and documentations dealing with these issues
- Describe the solutions adopted in civil aviation

www.enac.fr

The French Civil Aviation University

Plan

Security et safety

Security ou Safety ?
Security vs Safety ?
Similitudes et différences
Conflits
Contributions
Optimisation
Contexte aviation civile
Conclusion

Ecole Nationale de l'Aviation Civile
La référence aéronautique

Security et safety

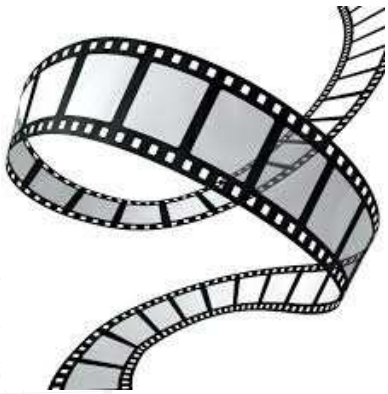
Security ou Safety ?
Security vs Safety ? (and vice versa)
Similarities and differences
Conflicts
Conributions
Optimization
Civil Aviation Context
Conclusion

www.enac.fr
The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Safety or Security ?



www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Safety ou Security ?

2 angles pour les to distinguer:

- ✓ intentionnalité
- ✓ séparation système/environnement

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Safety ou Security ?
2 angles pour les to distinguer

✓ intentionnalité

- Safety: prévention/détection/réaction à des dommages dus à des actions non-intentionnellement nuisibles par des acteurs bienveillants
- Security: prévention/détection/reaction à des dommages dus à des actions intentionnelles par des acteurs malveillants

✓ séparation système/environnement

- Safety: Capacité du système à ne pas affecter négativement/endommager son environnement
- Security: capacité de l'environnement à ne pas affecter négativement/endommager le système mais la distinction malveillant ou "accidentel" est toujours requise.

Mais est-ce la bonne approche ?

www.enac.fr

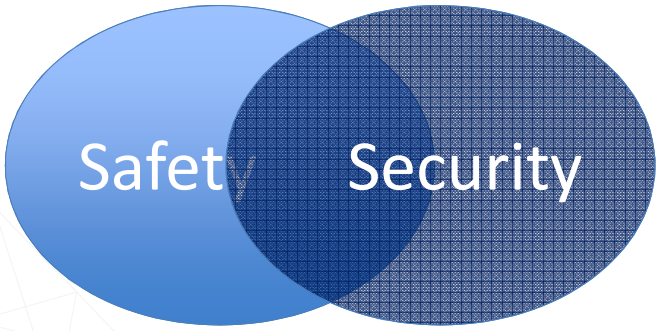
The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Une intersection dans les faits

Différentes intentions



Mêmes conséquences

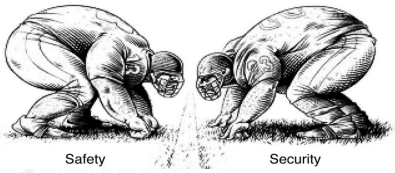
www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Security et safety



Security or Safety ?

Security vs Safety ? (et vice versa)

Similarities and differences

Conflicts

Contributions

Optimization

Civil Aviation Context

Conclusion

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

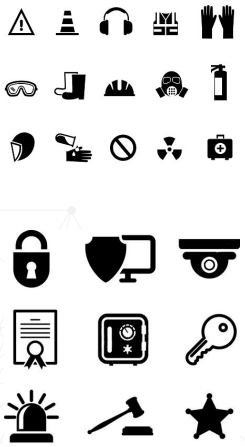
Problèmes potentiellement conflictuels

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique



Security et safety

Security or Safety ?

Security vs Safety ? (and vice versa)

Similitudes et différences

Conflicts

Contributions

Optimization

Civil Aviation Context

Conclusion

www.enac.fr

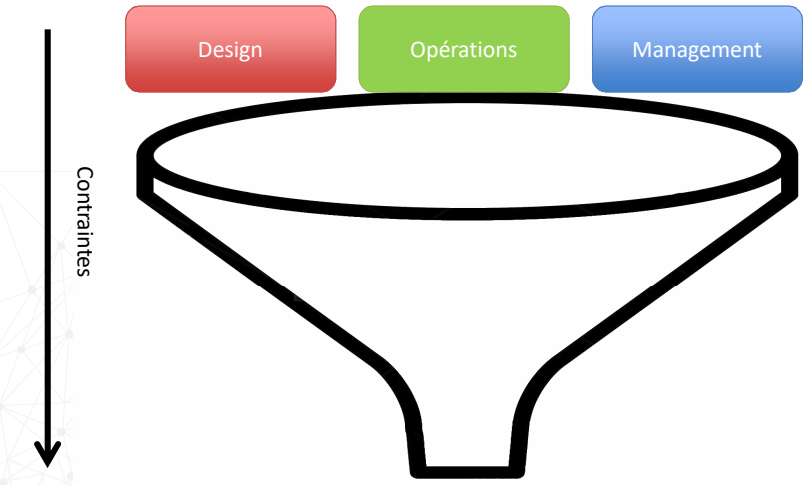
The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Safety et Security - Modèle

À partir de rien



Système déjà en place

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Safety - Security

Différences

Similitudes

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Safety - Security

Différences

Similitudes

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Safety and Security - Differences

	Safety	Security
Design D/O	Non intentionnel	Intentionnel
Design D/O		
Design M		
Design D		
Operations D		
Operations D/O/M		
Operations D/O		
Management D		
Management D		

www.enac.fr

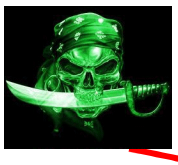
The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

A fundamental distinction

Reason diagram



Artificial alignment of all faults used to form the path of failure
⇔
"Intentional" risk scenario

"accidental" Risk Scenario
⇔
Natural Alignment of all faults used to Form the path of failure

Accident scenario schematization consecutively to latent errors and dangerous actions

***Reason, J. (1990)**. Human Error. Cambridge Univ. Press, in CROW (2009). Road Safety Manual. CROW Record 26*

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Safety et Security - Différences

Design

Operations

Management

	Safety	Security
D	La question est : Va-t-il y avoir des incidents?	La question est: Quand va-t-il y avoir des incidents ?
D		
D		

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Safety and Security - Différences

Design

Operations

Management

	Safety	Security
D	Vérification et validation	Vérification , validation et évaluation
D	Modèle déterministe et probabiliste Crisp set : Yes or no	Non déterministe, non probabiliste Fuzzy set : Between 0 and 1

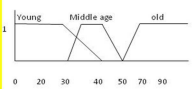
CRISP SET

Defines either value is 0 or 1

YES or NO

FUZZY SET

Defines value between 0 or 1



www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Safety - Security

Vérification :

- ✓ l'évaluation de la mise en œuvre des exigences afin de déterminer si elles ont été respectées.
- ✓ Avons-nous construit l'avion / le système / la fonction / l'article correctement?

Validation:

- ✓ la détermination que les exigences pour un produit sont correctes et complètes.
- ✓ Construisons-nous le bon avion / système / fonction / article?

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Safety - Security

La validation n'est pas évidente en sûreté (security):

- ✓ Pas de contrôle complet et absolu de la zone de menace
  - ✓ De nouveaux vecteurs de menaces
  - ✓ Nouveau chemin de menace
  - ✓ Humain impliqué
  - ✓ Imprévisibilité (par exemple, occurrence passée non pertinente…)
  - ✓ Fuzzy set
- ✓ Pas de guarantie que le système couvre tout
- ✓ L'évaluation apporte une solution

www.enac.fr

The French Civil Aviation University

Safety and Security - Différences

Différences Sémantiques

AVAILABILITY

- Security usage: Ensuring authorized users have access to information and associated assets when required [Source: ISO 17799]
- Safety Usage: Qualitative or quantitative attribute that a system or item is in a functioning state at a given point in time. It is sometimes expressed in terms of the probability of the system (item) not providing its output(s) (i.e. unavailability). [Source: ED-79A / ARP 4754A]

INTEGRITY

- Security usage: The property of protecting the accuracy and completeness of assets. [Source: ISO 27000, 2012]
- Safety Usage: Qualitative or quantitative attribute of a system or an item indicating that it can be relied upon to work correctly. It is sometimes expressed in terms of the probability of not meeting the work correctly criteria. [Source: ED-79A / ARP 4754A]

Ecole Nationale de l'Aviation Civile
La référence aéronautique

Safety and Security - Différences and similitudes

Différences Sémantiques

	safety		security
does	hazard	=	threat ?
does	.....	=	Vulnerability ?
does	failure condition	=	threat condition ?
does	likelihood	=	likelihood ?
does	Feared event	=	..... ?
does	Fault tolerance	=	Intrusion tolerance ?
does	resilience	=	resilience ?
does	.....	=	..... ?

www.enac.fr
The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Safety - Security

Similitudes

Differences

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Safety and Security - similarities

Design

Operations

Management

Safety	Security
D/O/M	Les deux traites des risques
D/O/M	
D/M	
D	
D	
D	
M	

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Security and safety

Security or Safety ?
Security vs Safety ?
Similarities and differences
Conflits
Contributions
Optimization
Civil Aviation Context
Conclusion

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Conflits
Safety VS Security

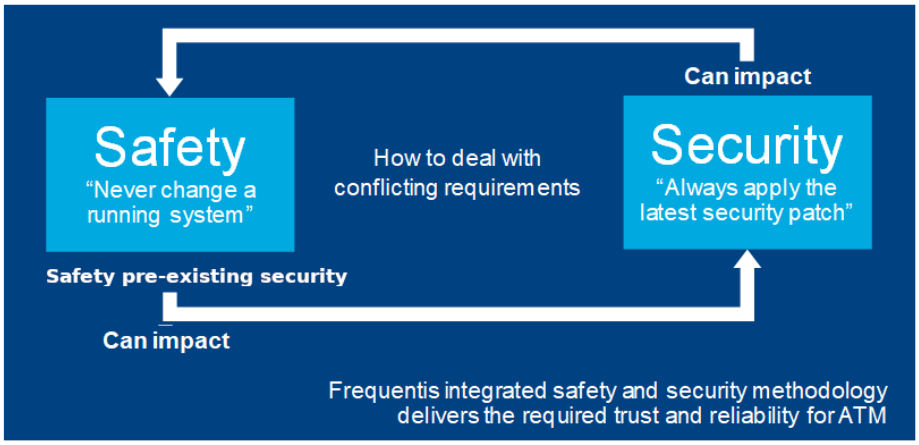
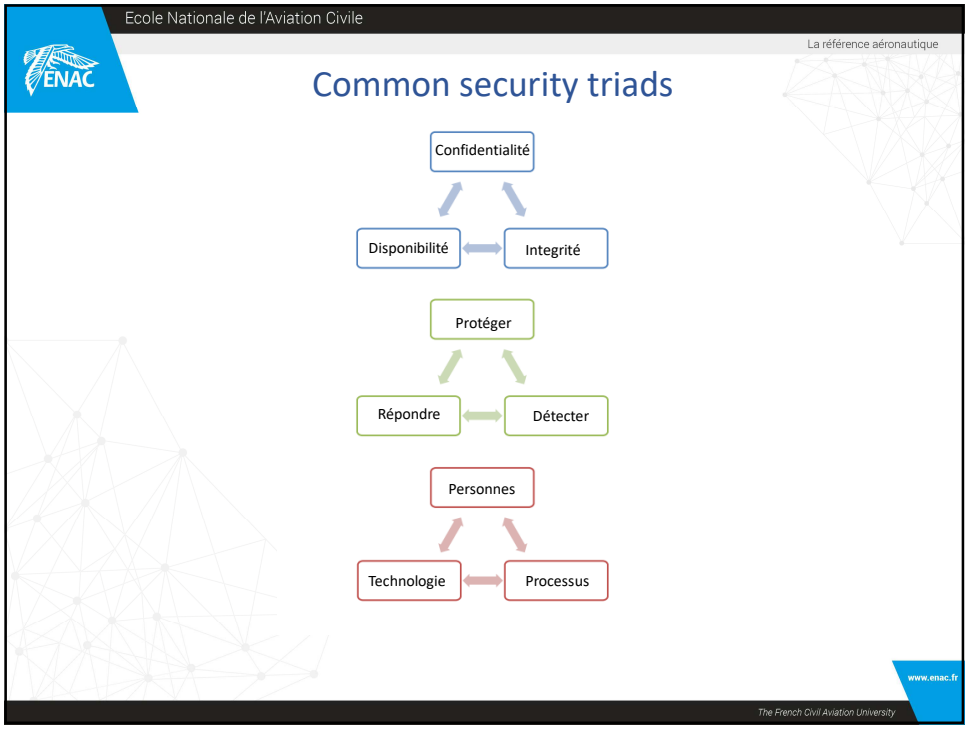


Figure 1 : Conflict of safety and security

www.enac.fr
The French Civil Aviation University


Ecole Nationale de l'Aviation Civile
La référence aéronautique
Common security triads
Confidentialité
Disponibilité
Integrité
Protéger
Répondre
Détecter
Personnes
Technologie
Processus
www.enac.fr
The French Civil Aviation University


Ecole Nationale de l'Aviation Civile
La référence aéronautique
Conflicts
Safety triad
SAFETY
Disponibilité
Fiabilité
www.enac.fr
The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Conflits
Safety VS Security

La relation avec la sécurité (safety) s'amplifie à mesure que l'on progresse vers les niveaux de contrôle et de processus,

- La sûreté (security) devra être réévaluée sur des échelles de temps différentes de la sécurité (safety)
  - ✓ les attaques et l'évolutions des menaces, les nouvelles vulnérabilités et les exploits potentiels entraîneront le lancement du cycle d'évaluation de la sûreté à un rythme plus élevé que les incidents ou les pannes qui relancent le cycle d'évaluation de la sécurité.

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Conflits
Safety VS Security

- Bien que l'analyse de la sécurité (safety) et de la sûreté (security) commence par l'étude de l'environnement,
- La cyberdéfense s'appuie sur une approche basée sur les menaces, de préférence à la gestion des vulnérabilités

- Usabilité des mesures de sûreté (security):
  - le contrôle d'accès est une fonction de sécurité typique qui peut restreindre l'utilisabilité du point de vue de la sécurité.
  - L'absence de principes d'authentification multi-facteurs éprouvés peut entraîner des faiblesses de sûreté potentiellement inacceptables.

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Conflits
Safety VS Security

- Les Décisions prises en safety ne doivent ppas créer des nouvelles vulnérabilités de security/sûreté
- De la même façon, les décisions prises en security/sûreté ne doivent pas compromettre la sécurité/safety.

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Un problème multi-dimensionnel

www.enac.fr
The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Un problème multidimensionnel

Sûreté --- > menaces

Concepts

Historique

Profils Expert

Organisations

Le + souvent entités séparées

Gouvernance

Rapprochement souhaitable dans une même entité: SMI

Methodes & strategies

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Security and safety

Security or Safety ?

Security vs Safety ?

Similarities and differences

Conflicts

Contributions de la safety à la security

From security to safety

Optimization

Civil Aviation Context

Conclusion

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Safety Contributions to security
Tolérance à l'Intrusion

La tolérance à l'intrusion est transposée à partir de la tolérance aux pannes.

la complexité et la nature de plus en plus distribuée des systèmes et l'imprévisibilité des attaquants rendent les intrusions et les attaques réussies inévitables;

les systèmes doivent également être conçus pour tolérer les cyberattaques

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Safety Contributions to security
Assurance sûreté and Effectivité

Security **Effectivité**
Capacité d'une mesure de sureté de prévenir, d'atténuer, de détecter, de réagir ou de récupérer après des attaques réussies sur des actifs, tout en permettant et en préservant l'utilisation prévue des actifs.
Security **Assurance**
Les actions planifiées et systématiques nécessaires pour fournir une confiance et des preuves suffisantes qu'un produit ou un processus satisfait les objectifs de sûreté et les exigences de sûreté donnés.

Exemples:
• Security Effectiveness requirement: *"L'architecture doit être conçue de manière à ne pas pouvoir être altérée ou contournée."*
• Security Assurance objective: *"L'architecture de sécurité est définie et conforme aux exigences de sécurité de niveau supérieur et est conçue pour empêcher le contournement et l'altération des mesures de sécurité."*
• Security Assurance action: *"Évaluez l'architecture pour s'assurer qu'elle est conçue de manière à ne pas être altérée ou contournée"*

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Safety Contributions to security
Assurance de sûreté d'après les critères Communs

L'assurance détermine le degré de confiance qu'un produit informatique répond à ses objectifs de sûreté. L'assurance peut être dérivée de la référence à des sources telles que des affirmations sans fondement, une expérience pertinente antérieure ou expérience spécifique.

Cependant, les CC fournissent une assurance grâce à une enquête active. Une investigation active est une évaluation du produit informatique afin de déterminer son propriétés de sûreté

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Safety Contributions to security
Security levels

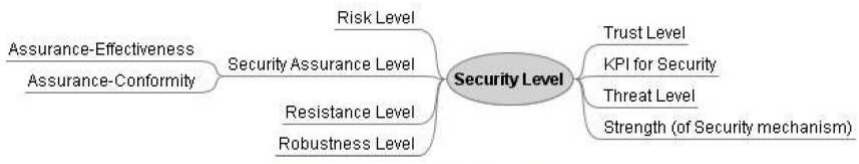


Figure 1: Elements of a Security Level

www.enac.fr

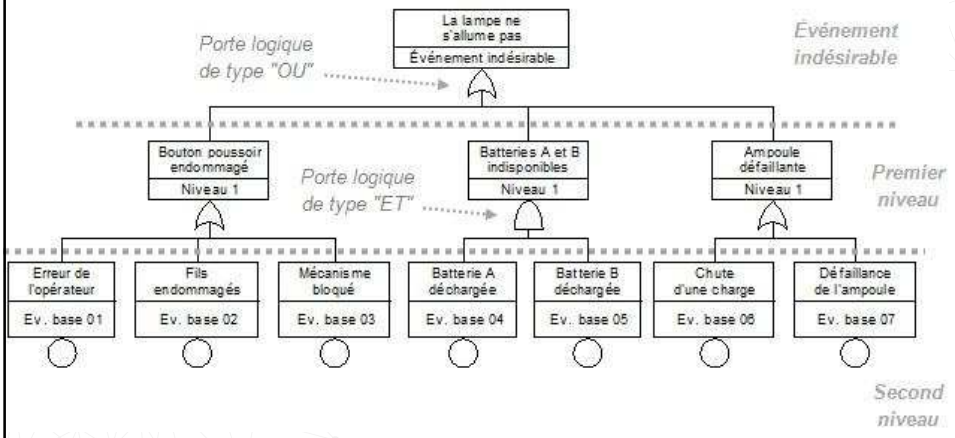
The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Safety Contributions to security

Modeling: Fault Tree & Attack tree



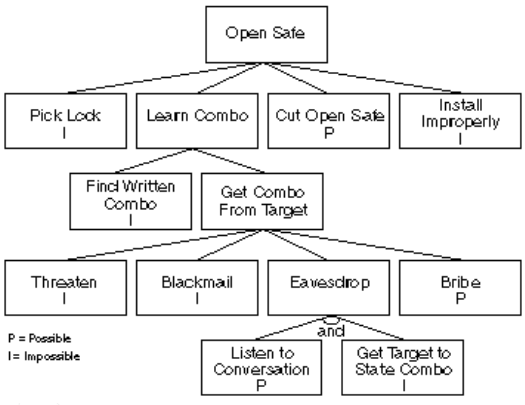
Fault Tree

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Safety Contributions to security

Modeling: Fault Tree & Attack tree



Attack Tree

www.enac.fr
The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Safety Contributions to security
et aussi

Défense en Profondeur
Analyse de risque structurée
Injection de pannes

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Security and safety

Security or Safety ?
Security vs Safety ?
Similarities and differences
Conflicts
Contributions
- From safety to security
- de la security à la safety

Optimization
ATM Context
Conclusion

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

security contributions to safety

Notion of safety kernel

- ✓ kernel-based architectural approaches for safety software

Détournements d'utilisation (misuse cases) et diagrammes de détournements de misuse sequence diagrams) en safety

Modèles de Security utilisésen injection de défaillances de safety.

- ✓ Propriétés de Non-interference

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

security contributions to safety
Resilience engineering

Plans de continuité d'activité et de reprise d'activité

La resilience en sécurité n'est pas seulement une question de conception mais se traite également au niveau operational.

Par conséquent, l'ingénierie de Résilience utilise les informations issues de la recherche sur les défaillances de systèmes complexes, y compris les contributeurs organisationnels au risque, et les facteurs qui affectent la performance humaine pour fournir des outils d'ingénierie des systèmes pour gérer les risques de manière proactive »(Woods, 2003).

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

security contributions to safety
Resilience engineering

Le concept de résilience est généralement lié à des termes de conception tels que robuste,stable, élastique et flexible.

Il peut être conçu comme «une caractéristique de certains systèmes qui leur permet de répondre à une perturbation imprévue pouvant entraîner une défaillance, puis de reprendre rapidement les opérations normales et avec une diminution minimale de leurs performances» (Fairbanks et al., 2014).

Ainsi, l'ingénierie de la résilience peut être préconisée en tant que discipline visant à fournir aux systèmes des moyens de concrétiser ces caractéristiques en réponse à des perturbations externes et internes (Hollnagel, 2006, Woods, 2006).

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

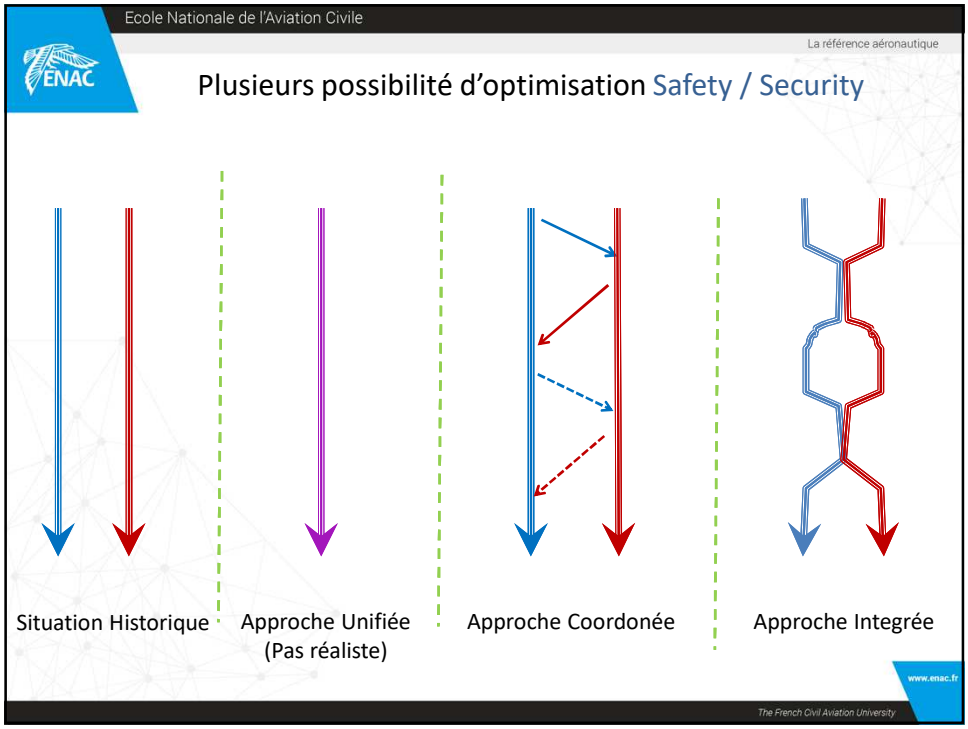
La référence aéronautique

Security and safety

Security or Safety ?
Security vs Safety ?
Similarities and differences
Conflicts
Contributions
Optimisation
Civils Aviation Context
Conclusion

www.enac.fr

The French Civil Aviation University



Security and Safety Integration
Airworthiness (ed-202A)

Aircraft safety-security interface

Few standards detail the interface
• Alignment with ED-79A / ARP 4754A

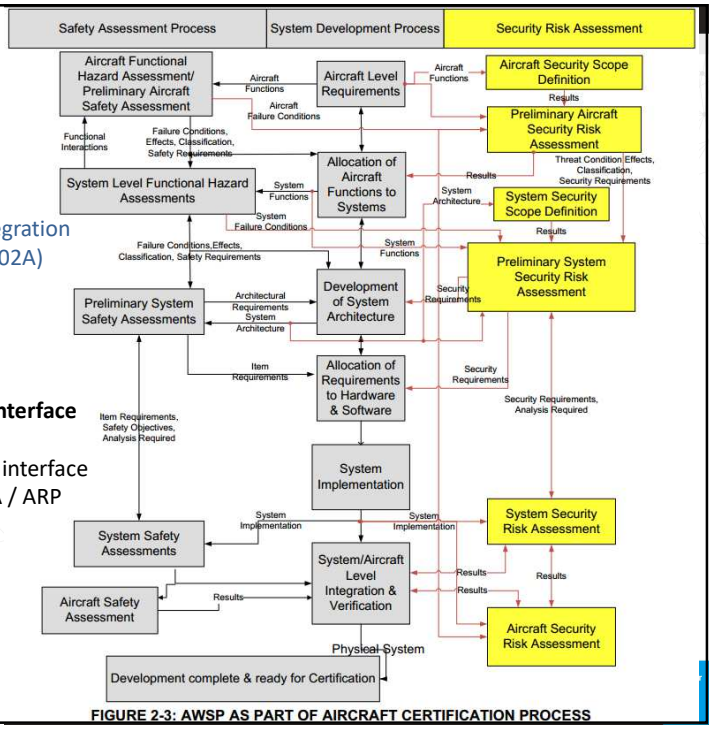


FIGURE 2-3: AWSP AS PART OF AIRCRAFT CERTIFICATION PROCESS

Ecole Nationale de l'Aviation Civile

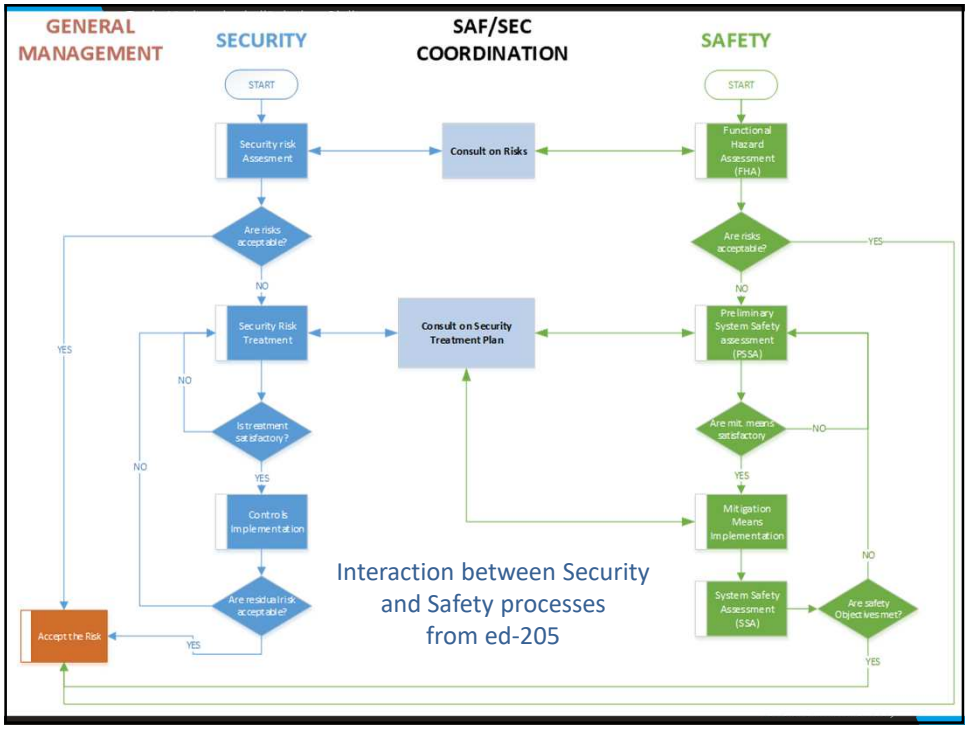
La référence aéronautique

Security and Safety Relationship in ATM
ed-205

- Il ne peut pas y avoir de danger de sécurité (safety) direct consécutif après une attaque de sûreté (secutity) réussie.
- L'intention pourrait être un discriminateur entre un événement conduisant à un incident de sûreté et un événement qui crée un danger pour la sécurité
  - Sec concentrer sur les incidents qui affectent la safety
- Il n'y a pas de modèle d'intention quantifiable.
- L'utilisation de distributions de probabilité n'est pas une méthodologie appropriée pour la sûreté.
- Il est probable que la sûreté devra être réévaluée plus fréquemment que la sécurité.
- Les décisions prises en matière de sûreté ne doivent pas compromettre la sécurité et vice-versa.

www.enac.fr

The French Civil Aviation University



Interaction between Security and Safety processes from ed-205

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Security and safety

Security or Safety ?
Security vs Safety ?
Similarities and differences
Conflicts
Contributions
Optimization
Security for Safety
Le contexte aviation Civile
Conclusion

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

Safety vs Security 1/2

SAFETY	SECURITY
• Etablissement des Evènements Redoutés, réduction de gravité par correction, réduction d'occurrence par prévention	• Etablissement des risques, réduction du niveau de risque sur vraisemblance d'occurrence principalement
• Objectif de probabilité d'occurrence max	• Risques résiduels à accepter si inférieur à niveau de risque particulier
• Régulé par l'Europe, repris sous forme de Regulations par Comission Européenne)	• Régulé par procédure interne, et depuis peu ANSSI, et dans un futur proche EASA

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

Safety vs Security 2/2

De part leur nature, les deux démarches peuvent s'opposer dans leurs mise en œuvre. Quelques exemples:

SECURITY

- système verrouillé (contrôle d'accès notamment)
- Contrôle d'exécution du code (notamment antivirus), par nature non prédictif
- Strates de protection « en profondeur » (chiffrement, monitoring, contrôle d'accès)
- Patch patch patch patch !!!!

SAFETY

- système facilement manipulable en opération (pas de contrôle d'accès)
- système temps réel (problèmes de performances)
- Simplicité du système (relative, les redondances étant sources de complexité)

SAFETY WINS!

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

SECURITY FOR SAFETY (JUDO SPIRIT)

1. Pilotage par la gestion de risque
2. Complément de la démarche safety
3. Adaptation et appui à/sur l'existant
4. Intégration précoce dans les nouveaux systèmes

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

PILOTAGE PAR LA GESTION DE RISQUE

La sûreté dogmatique ne fonctionne pas ici, à cause de l'environnement et des contraintes

Nécessité de mettre en œuvre une appréciation de risque, pour créer des moyens de réduction adaptés:

- Réduction d'impact
- Réduction de vraisemblance

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

COMPLÉMENT DE LA DÉMARCHE SAFETY

La démarche safety couvre les menaces accidentelles, la sûreté vise la malveillance, elles sont donc complémentaires

La démarche sûreté s'appuie sur les résultats des études sécurité pour affiner la gravité des risques sûreté

www.enac.fr

The French Civil Aviation University

ADAPTATION À L'EXISTANT

Prise en compte des équipements hérités (legacy) dans la stratégie sûreté

- Protection des entrées sorties (firewalling)
- Filtrage des données en entrée (avec vérification syntaxique)

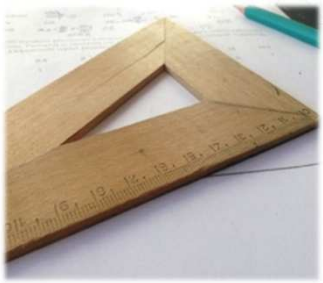
Forte composante physique dans la protection du SI

- Gestion des accès des personnes
- Règles de protection unifiées sur tous les sites

INTÉGRATION PRÉCOCE DANS LES NOUVEAUX SYSTÈMES

Intégration d'un corpus de « règles d'infrastructure » en cours de standardisation à la DTI

- Issu de contraintes externes (ANSSI)
- Comprenant les nouveaux moyens mis en œuvre à la (gestion des évènements/incidents par exemple)



Intégration des moyens de réduction de risques issus de l'analyse sûreté du changement

Le tout peut s'apparenter à la défense en profondeur

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Security and safety

Security or Safety ?
Security vs Safety ?
Similarities and differences
Conflicts
Contributions
Optimisation
Civil aviation Context
Conclusion

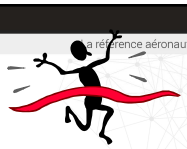
www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

La référence aéronautique

Conclusion



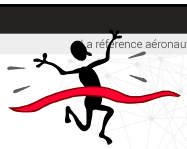
- La sécurité était de loin la principale préoccupation du transport de l'aviation civile mais de nos jours, les risques pour la sûreté des systèmes d'information doivent être pris en compte
- La sûreté et la sécurité ont des exigences contradictoires, mais convergent de plus en plus
- Les décisions prises en matière de sécurité ne doivent pas créer de nouvelles failles de sécurité (et vice versa)

www.enac.fr

The French Civil Aviation University

Ecole Nationale de l'Aviation Civile

Conclusion

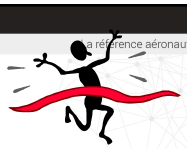


Équipes distinctes
Méthodologies différentes
standards différents

→ Vrai défi pour la creation de standards

Ecole Nationale de l'Aviation Civile

Conclusion

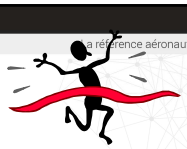


- Attention à ne pas cloisonner, à la fois en matière de sécurité et de sûreté, mais aussi de conception, d'exploitation et de gestion.
- les équipes de sécurité, de qualité et d'environnement doivent travailler ensemble,
- L'optimisation est requise

Ecole Nationale de l'Aviation Civile

la référence aéronautique

Conclusion



- Nécessité réelle d'adaptation, approche unifiée/fusion(?), Révision des normes
- L'approche unifiée des risques n'est pas pour aujourd'hui

www.enac.fr

The French Civil Aviation University