Définition d'une architecture de sécurité adaptative pour les communications aéronautiques

Mohamed-Slim Ben Mahmoud, Nicolas Larrieu, Alain Pirovano

11e Congrés des Doctorants 2010
EDSYS (École Doctorale Systèmes)
6 et 7 mai, Toulouse

Définition d'une architecture de sécurité adaptative pour les communications aéronautiques

Mohamed Slim Ben Mahmoud (slim.ben.mahmoud@recherche.enac.fr)
LEOPART (Laboratoire d'Etude et d'OPtimisation des Architectures des Réseaux de Télécommunication), Toulouse
ENAC (Ecole Nationale de l'Aviation Civile), Toulouse

Thèse encadrée par : Alain Pirovano et Nicolas Larrieu (LEOPART/ENAC–département CNS)

Résumé *Cet article présente une infrastructure de sécurité adaptée au contexte aéronautique. Différentes spécificités propres aux communications aéronautiques sont prises en compte comme l'hétérogénéité du trafic, la priorité entre les flux gérés ainsi que l'évolution des ressources réseaux disponibles. La politique de sécurité proposée est ainsi dynamique et optimisée.*

Ce travail s'inscrit pour partie dans le cadre d'un projet industriel intitulé FAST[1](Fiber-like Aircraft Satellite Telecommunications) qui vise à proposer une infrastructure de communication aéronautique par satellite haut débit. L'architecture de sécurité proposée dans cet article sera développée sous forme de maquette puis testée et validée pour les besoins du projet.

A. INTRODUCTION

Les communications aéronautiques sont appelées à évoluer dans les années à venir. Actuellement, la voix analogique reste le moyen principal pour communiquer entre l'avion et le sol dans des bandes de fréquences réservées. Néanmoins, plusieurs organismes internationaux prédisent une migration imminente vers des communications numériques dans un futur proche. Par exemple, EUROCONTROL (Organisation européenne pour la sécurité de la navigation aérienne) et la FAA (Federal Aviation Administration - USA) ont rédigé en partenariat le COCR (Communications Operating Concept and Requirements for the Future Radio System) qui est un document technique recensant, entre autres, les nouveaux services cockpit (ATS - Air Traffic Services) et compagnie (AOC - Aeronautical Operational Control Services) [EF07].

Ces services basés sur des communications de données devraient remplacer les communications voix progressivement dans les années à venir. De plus, les compagnies aériennes seront certainement amenées à déployer de nouveaux services passagers (APC - Aeronautical Passenger Communication Services), comme l'Internet cabine par exemple, mais aussi des services AOC "nouvelle génération" comme la télé-médecine[2] ou la télé-surveillance[3].

Avec une telle diversité des flux, le trafic air-sol devient de plus en plus dense et hétérogène. Il apparaît donc opportun de mixer ces flux afin d'offrir une meilleure utilisation des ressources. Dans la perspective de faciliter l'interopérabilité entre les différents réseaux concernés, le déploiement d'un réseau de communications aéronautiques tout-IP (Internet Protocol) devient une évidence pour le futur de l'ATM (Air Traffic Management). Afin de faciliter cette interconnexion entre le réseau ATN (Aeronautical Telecommunications Network) et les autres réseaux terrestres basés sur IP, l'OACI (Organisation de l'Aviation Civile Internationale) a permis l'utilisation d'ATN avec la suite protocolaire IPS (Internet Protocol Suite)[ICA02]. L'implémentation de l'ATN/IPS permettra non seulement une meilleure adéquation entre les réseaux de communications terrestres et aéronautiques, mais aussi l'utilisation de protocoles et de standards matures et bien connus de la communauté industrielle (COTS - Commercial-Off-The-Shelf).

[1]Le projet est financé par la DGCIS (Direction Générale de la Compétitivité, de l'Industrie et des Services) et le FUI (Fonds Unique Interministériel) et réunit plusieurs partenaires (ENAC, ISAE, LAAS-CNRS, Telecom Bretagne, EADS Astrium, Axess Europe, Vodea et Medes).

[2]Système permettant de prodiguer des soins médicaux à distance et l'échange d'informations médicales.

[3]Système de surveillance à distance.

A long terme, les communications aéronautiques numériques présentent donc un potentiel considérable. Leur utilisation systématique permet d'envisager des gains importants en fiabilité, en coût, et en qualité de transmission. Elles permettent également des échanges plus riches et plus fréquents entres les systèmes informatiques sol et les systèmes avioniques embarqués.

B. CONTEXTE ET PROBLÉMATIQUE

Inévitablement, l'industrie devra tôt ou tard faire face aux conséquences directes d'une telle mutation. La sécurité des communications devient une priorité à gérer dans un contexte aussi critique : une attaque pourra non seulement compromettre les données échangées entre l'avion et le sol, mais aussi mettre en danger la vie des personnes à bord (suite à une attaque de déni de service qui empêcherait le pilote de communiquer avec le contrôleur aérien par exemple). Une architecture de sécurité devra donc être rigoureusement définie afin d'assurer confidentialité, intégrité et authentification des données échangées.

Cette architecture devra aussi tenir compte d'autres contraintes propres aux communications aéronautiques. En effet, dans un environnement aussi imprévisible, l'état du réseau reste très fluctuant et dépend de plusieurs paramètres exogènes tels que les performances intrinsèques de certaines technologies utilisées pour communiquer de l'avion vers le sol (comme le débit par exemple). De plus, la politique de sécurité appliquée devra aussi gérer les priorités qui existent entre des flux relatifs à la sûreté du vol (ATS) et le reste des communications. Dans un système aux conditions aussi variables, une politique de sécurité statique sera coûteuse et inadéquate au contexte et aux contraintes qu'impose cet environnement complexe.

Auparavant, quelques solutions pour sécuriser les échanges air-sol ont été proposées, comme l'AMS (ACARS Message Security) pour l'ACARS[4] (Aicraft Communications Addressing and Reporting System). Un état de l'art des mécanismes de sécurité utilisés pour les communications aéronautiques a été fourni dans [BMLP09] ainsi qu'une taxonomie permettant de classer les menaces et les attaques pouvant surgir sur une communication air-sol. Néanmoins, ces solutions ne prennent pas en compte les contraintes liées à l'interopérabilité entre réseaux hétérogènes, la priorité entre domaines, et les ressources réseaux limitées.

Afin de pallier ce manque, une architecture de sécurité adaptative pour les communications aéronautiques par satellite est présentée dans cet article. La diversité ainsi que la priorité entre les différents services seront prises en compte à travers la mise en place d'une politique de sécurité dynamique. Les mécanismes de sécurité appliqués varient en fonction des niveaux de sécurité minimums requis par chaque application, mais aussi en fonction de l'évolution des ressources réseaux disponibles. Cette architecture prend en compte le lien satellitaire haut débit du projet FAST à travers des mécanismes de gestion de la qualité de service (QoS - Quality of Service) et des considérations d'interconnexion entre le terminal satellite et le reste des composants de l'architecture embarquée.

C. ARCHITECTURE SYSTÈME ET QUALITÉ DE SERVICE

L'architecture globale du système retenue est illustrée dans la figure 1. Au niveau du sol, une Gateway (GW) est connectée à deux routeurs : un routeur ATN pour le réseau aéronautique, et un routeur Internet pour les services APC destinés aux passagers. Pour le réseau à bord, deux routeurs sont connectés au terminal satellite : un routeur ATN/IPS pour l'ATS et un routeur NG (Next Generation) pour les services AOC et APC. Les normes DVB (DVB-S2 pour le lien aller et DVB-RCS pour le lien retour) ont été retenues comme méthodes d'accès pour le lien satellitaire du projet FAST [ETS05b, ETS05a].

Au niveau du domaine APC, plusieurs points d'accès WIFI seront dispatchés à travers l'avion afin d'assurer une disponibilité continue du service Internet cabine et télé-médecine, qui requiert une mobilité absolue. Une connexion multi-SSID (Service Set IDentifier) permet de séparer les deux types de trafics pour des raisons évidente de sécurité (chaque application aura sa propre clé pour se connecter) et de disponibilité des ressources, surtout quand une application aussi critique que la télé-médecine veut se connecter à un des points d'accès de l'avion.

Au niveau du routeur NG, un premier niveau de QoS IP est mise en oeuvre avec Diffserv[5] (Differentiated services) en associant chaque domaine connecté au routeur NG à une file d'attente donnée (télé-médecine, télé-surveillance, services AOC "standards" et Internet cabine).

Au niveau du terminal satellite, deux ports physiques sont considérés pour connecter le routeur ATN/IPS (flux ATS) et le routeur NG. Ainsi, la séparation entre les services cockpit ATS et le reste du trafic est assurée conformément aux normes et pratiques recommandées par l'OACI [ICA02]. L'architecture retenue est basée sur la norme DVB-RCS comme décrit dans l'architecture de référence BSM (Broadband System Multimedia) [ETS06] de l'ETSI (European Telecommunications Standards

[4]Système de communication entre l'avion et le sol par liaison radio de très haute fréquence ou satellite.
[5]Architecture réseau qui spécifie un mécanisme pour classer et contrôler le trafic tout en fournissant un qualité de service.

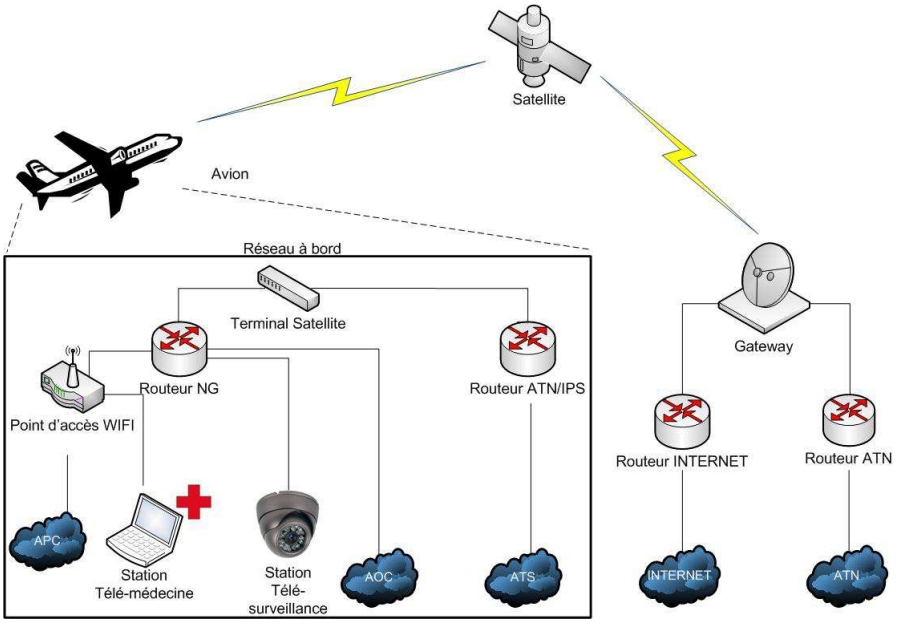

Figure 1. *Architecture globale du système satellite en environnement non sécurisé.*

Institute).

A l'entrée du terminal satellite, un classifier IP est mis en place afin de différencier les flux IP provenants des deux routeurs. Une phase de "mapping" est ainsi réalisée afin de gérer les priorités entre les flux grâce à plusieurs niveaux de priorité PID (Priority ID), assignés à chaque classe de service et envoyés vers la file d'attente correspondante identifiée grâce à un QID (Queuing ID). De cette façon, la séparation entre les couches dites "satellite dépendant" (SD) et "satellite indépendant" (SI) est assurée conformément au modèle BSM de référence.

Dans la suite, une seconde version de l'architecture système à bord sera présentée, cette fois-ci en environnement sécurisé grâce au module de gestion de la sécurité (SecMan) L'interconnexion des différents composants sera décrite et les principes de fonctionnement y sont introduits.

D. ARCHITECTURE DE GESTION ADAPTATIVE DE LA SÉCURITÉ

L'architecture sécurisée embarquée à bord est présentée dans la figure 2. Deux relais sécurité (SMP - SecMan Proxy) sont considérés et connectés respectivement au routeur ATN et au routeur NG. Chaque proxy est isolé dans une zone démilitarisée DMZ (Demilitarized Zone) grâce à des fonctions de pare-feu (Firewalling) implantées au niveau des routeurs.

Les pare-feux retenus sont de type Stateful Inspection, réputés assez robustes et efficaces contre les attaques de déni de services (DoS - Denial of Service), contrairement aux pare-feux Stateless, reposants sur des règles et des listes d'accès trop simples pour éviter des tentatives d'intrusions évoluées. Les pare-feux applicatifs (niveau 7) peuvent être une alternative intéressante, mais le traitement et le calcul qu'ils engendrent ralentissent considérablement les échanges, ce qui va à l'encontre d'une politique de sécurité adaptative et visant justement à améliorer les performances réseaux.

D'autres part, afin d'avoir une politique de sécurité flexible, SecMan est capable de fonctionner en deux modes :

1)*Mode Intra-classe* : ce mode est utilisé quand les flux appartiennent à la même classe. Par conséquent, la priorité entre les flux n'est pas prise en compte et la politique de sécurité s'adaptera en fonction des ressources réseaux disponibles. SecMan fonctionnera en mode Intra-classe sur le proxy sécurité connecté au routeur ATN/IPS car seul le trafic ATS est considéré (SMP en DMZ_1),

2)*Mode Inter-classe* : ce mode est utilisé quand les flux appartiennent à plusieurs classes de trafic. La politique de sécurité d'adaptera donc en fonction des ressources réseaux et des priorités entre flux issus de domaines différents. SecMan fonctionnera en mode Inter-classe sur le proxy sécurité connecté au routeur NG (SMP en DMZ_2).

De plus, plusieurs modes de sécurisation peuvent être appliqués en adaptant la politique de sécurité au besoin, quelque soit le mode de fonctionnement de SecMan(Inter-classe ou Intra-classe) :

1) *Mode transparent non sécurisé* : les paquets qui transitent sur les routeurs sont simplement routés sans aucun mécanisme de sécurité (tout en respectant les contraintes de QoS),

2) *Mode transparent sécurisé* : il sécurise les paquets échangés à l'aide d'un mécanisme tel que IPSec (IP Security)[KSre] et est transparent pour

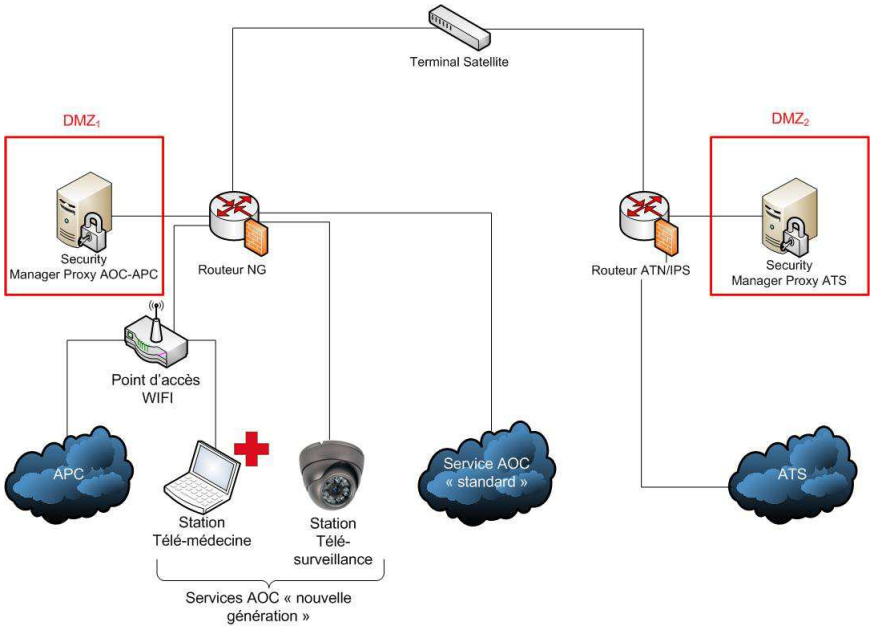

Figure 2. *Architecture à bord sécurisée.*

l'utilisateur,

3) *Relais au niveau transport* : SMP sécurise les connexions de bout en bout (HTTPS par exemple),

4) *Relais applicatif* : SMP se comporte dans ce mode comme un proxy applicatif "classique" (proxy http ou ftp par exemple).

1. Principe de fonctionnement de SecMan

La figure 3 illustre le fonctionnement de SecMan. Comme il a été décrit précédemment, compte tenu des services à sécuriser et de l'intérêt de converger vers un réseau aéronautique tout-IP, il apparaît pertinent de porter l'étude sur un réseau IP. Il est à noter que le module gère les mécanismes de sécurité des couches hautes de la pile TCP/IP, au-dessus de la limite FRS (Future Radio System) définie dans le COCR. Le module est informé de l'évolution constante des ressources réseaux disponibles à travers un mécanisme cross-layer[6]. Il prend également en compte les besoins de sécurité exprimés en amont à travers une phase d'évaluation des risques pour les différents flux en entrée de SMP. Plusieurs routines d'activation des mécanismes de sécurité sont aussi créées au travers de primitives telles que *Change-Cipher* pour modifier l'algorithme de chiffrement ou *ByPass* pour ne pas activer un mécanisme de sécurité donné.

2. Algorithme d'aide à la décision multi-critères

Un des composants les plus importants de SecMan est sans doute le décideur. Le décideur est l'algorithme qui va permettre la prise de décision vis à vis de la politique de sécurité à appliquer. A cette fin, les algorithmes d'aide à la décision multi-critères (MCDMA - Multi Criteria Decision Making Algorithm) sont adaptés surtout dans un système aussi riche et complexe[FGE05]. Il s'agit de méthodes et de calculs permettant de choisir la solution optimale parmi tout un ensemble de solutions en essayant de prendre en compte les exigences des acteurs et leur comportement à la fois dans un cadre de processus de décision "humain" et dans un cadre de processus de décision "automatique".

ANP (Analytic Network Process) fait partie des méthodes MCDMA les plus efficaces et les plus appréciées notamment grâce à sa manière simple et structurée de résoudre le problème (un but, des critères de décision, et des alternatives). Une étape de comparaison par paires, permettant de pondérer les poids d'importances entre les critères, précède une suite de calcul matriciel qui aboutit finalement à un classement des alternatives listées. La méthode est présentée en détail dans [Saa00].

Afin d'adapter la méthode au contexte particulier des mécanismes de sécurité, une liste non exhaustive de métriques pouvant servir à la comparaison a été établie. Ces critères sont des caractéristiques inhérentes aux différents algorithmes constituants les protocoles de sécurité (taille de la clé, taille de l'empreinte, nombre de rondes).

Ces protocoles ont été au préalable négocié entre l'avion et l'entité sol grâce à une phase de négociation sécurisée. Au terme de la négociation,

[6]Mécanisme d'optimisation des échanges inter-couches afin d'améliorer le débit et de réduire la latence.

une table des mécanismes supportés est stockée dans une base de donnée embarquée appelée SSPD (Supported Security Protocol Database).

Ainsi, les protocoles de sécurité seront évalués selon leur robustesse et leur impact en terme de ressources systèmes et réseaux.

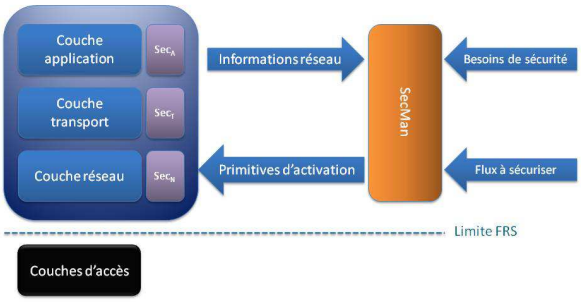

Figure 3. *Principes de fonctionnement de SecMan*

3. Avantages

Cette architecture de sécurité présente plusieurs avantages :

1) *Consommation des ressources réseaux optimisée* : l'optimisation du niveau de sécurité permet de diminuer le surplus induit par les mécanismes de sécurité et de fait, la consommation des ressources réseaux est mieux gérée,

2) *Gestion des priorités* : la priorité entre les différents services relatifs à l'ATS, AOC et APC est gérée,

3) *Politique de sécurité sélective et multi-couches* : SecMan est capable d'activer plusieurs mécanismes de sécurité opérants sur une ou plusieurs couches de la pile protocolaire TCP/IP en fonction des besoins identifiés afin de maximiser la robustesse offerte,

4) *Compatibilité et interopérabilité accrues* : SecMan est tout à fait compatible avec n'importe quel réseau IP utilisant une technologie autre que le satellite au niveau des couches d'accès réseaux car les mécanismes de sécurité sont gérés au-dessus de la limite FRS du COCR. Il est aussi notable que les concepts d'interconnexion du système présenté peuvent être appliqués hors contexte aéronautique.

E. CONCLUSION

Dans cet article, une architecture de sécurité adaptée au contexte des communications aéronautiques a été présentée. Les problématiques de priorités entre les flux, de gestion de la qualité de service et des ressources réseaux ont été détaillées et prises en compte dans la définition de la politique de sécurité. Les principes de fonctionnement du module de gestion de la sécurité ainsi que son interconnexion avec le reste des composants a été décrite.

Néanmoins, certains points relatifs à la sécurité des communications aéronautiques restent à résoudre. Tout d'abord, le contexte aéronautique nécessite de considérer les problématiques de mise à l'échelle pour ce qui est de la gestion des échanges en environnement sécurisé. A titre d'exemple, dans le ciel français, le nombre d'avion à un instant t peut atteindre les **500** avec plusieurs services (passager et/ou compagnie) pouvant opérer en même temps dans chaque avion.

Le nombre élevé des échanges qui en résultent nécessite de proposer une infrastructure à clés publiques (PKI - Public Key Infrastructure) permettant d'optimiser la gestion des clés et des certificats entre les usagers. L'accent sera mis sur les procédures de vérification/révocation des certificats à travers le protocole OCSP (Online Certificate Status Protocol) [MAM+99]. Cette PKI permettra aussi de sécuriser les échanges induits par la phase de négociation des mécanismes de sécurité supportés (SSPD).

A long terme, les considérations d'implémentation seront aussi traitées. Pour les besoins du projet FAST, un démonstrateur sera mis en place dans les mois à venir à travers une plateforme utilisant un noyau Linux, un émulateur de lien satellitaire, et les sources de trafic spécifiques au projet (ATS, AOC, APC, télé-médecine, télé-surveillance). Toutefois, afin de proposer cette architecture de sécurité aux professionnels de l'aviation civile et l'utiliser dans un environnement réel, plusieurs contraintes d'implémentation doivent être respectées. En effet, n'importe quel logiciel embarqué à bord d'un système avionique doit être rigoureusement vérifié et certifié comme décrit dans [RTC92].

A cette fin, une architecture MILS (Multiple Independant Layer Security/Safety) [Jac04] sera utilisée. MILS est une approche assez récente permettant d'implémenter des systèmes sécurisés et vérifiables à travers une séparation des différents processus issus de parties disjointes du système global, ainsi qu'un contrôle rigoureux des flux d'information gérés au sein de ce système.

RÉFÉRENCES

[BMLP09] M.Slim. Ben Mahmoud, N. Larrieu, and A. Pirovano. An aeronautical data link security overview. pages 4.A.4–1 –4.A.4–14, octobre 2009.

[EF07] Eurocontrol and FAA. Communications operating concept and requirements for the future radio system. Technical report, Mai 2007.

[ETS05a] ETSI. Digital video broadcasting (dvb) ; interaction channel for satellite distribution systems. Technical report, Septembre 2005.

[ETS05b] ETSI. Digital video broadcasting (dvb) ; second generation framing structure, channel coding and modulation systems for broadcasting, interactive services, news gathering and other broaband satellite applications. Technical report, Mars 2005.

[ETS06] ETSI. Satellite earth stations and systems (ses) ; broadband satellite multimedia (bsm) services and architectures : Qos functional architecture. Technical report, Janvier 2006.

[FGE05] J. Figueira, S. Greco, and M. Ehrgott. *Multiple Criteria Decision Analysis : State of the Art Surveys*. Springer Verlag, Boston, Dordrecht, London, 2005.

[ICA02] ICAO. *Manual of Technical Provisions for The ATN, Doc 9705, Ed 3*, 2002.

[Jac04] J.M. Jacob. High assurance security and safety for digital avionics. In *Digital Avionics Systems Conference, 2004. DASC 04. The 23rd*, volume 2, pages 8.E.4–8.1–9 Vol.2, Octobre 2004.

[KSre] S. Kent and K. Seo. Security Architecture for the Internet Protocol. RFC 4301 (Proposed Standard), Juin Décembre.

[MAM+99] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. RFC 2560 (Proposed Standard), June 1999.

[RTC92] RTCA. Software considerations in airborne systems and equipment certification. Technical report, Décembre 1992.

[Saa00] Thomas.L. Saaty. *Fundamentals of the Analytic Hierarchy Process*. RWS Publications, 4922 Ellsworth Avenue, Pittsburgh, PA 15413, 2000.