

ONZIÈME CONFÉRENCE DE NAVIGATION AÉRIENNE

Montréal, 22 septembre – 3 octobre 2003

- Point 2 :** La sécurité et la sûreté dans la gestion du trafic aérien (ATM)
2.5 : Sécurité et sûreté de l'infrastructure ATM

SÛRETÉ DANS LES COMMUNICATIONS ATM

(Note présentée par l'Italie)

SOMMAIRE

Le transport aérien doit être considéré comme une «infrastructure nationale cruciale (CNI)» et, de ce fait, les moyens de communication ATM, à savoir les sous-réseaux mobiles et fixes, doivent être regardés comme des «infrastructures cruciales d'information (CII)». La présente note décrit certains aspects propres aux systèmes CNI-CII ayant trait à la sûreté, tels que le cryptage, la connectivité et la qualité de service, entre autres.

L'Italie propose de faire appel aux initiatives stratégiques d'EUROCONTROL et de définir des lignes directrices pour l'amélioration de la sûreté des communications de gestion du trafic aérien.

La suite à donner par la Conférence figure au paragraphe 4.

1. INTRODUCTION

1.1 De nos jours, les États et les organismes supranationaux fondent leur croissance et leur organisation interne sur des systèmes d'infrastructure de complexité grandissante et de portée toujours plus vaste, par exemple pour la distribution de l'énergie électrique, les transports, les communications publiques, etc. Il existe donc une forte corrélation entre, d'une part, la sûreté et la vulnérabilité de ces infrastructures et, d'autre part, l'efficacité du système dans son ensemble.

1.2 Depuis les attaques du 11 septembre, les organismes qui jouent un rôle crucial, tant sur la scène nationale que sur la scène internationale, doivent revoir leur approche à l'égard de la sûreté et de la survivabilité des infrastructures.

1.3 Les infrastructures de ce type ont été définies comme étant des infrastructures nationales cruciales (CNI) — et la «défense» essentielle est devenue urgente.

1.4 Le transport aérien doit être considéré comme un élément important des CNI, et les réseaux de télécommunication et d'information fixes et mobiles utilisés dans le cadre de la gestion du trafic aérien (ATM) doivent être considérés comme une CNI ou, plus précisément, comme ce qu'il est convenu d'appeler une infrastructure cruciale d'information (CII).

1.5 Dans le cadre ci-dessus, l'Italie propose de faire appel aux initiatives stratégiques d'EUROCONTROL et a élaboré une série d'actions coordonnées centrées sur la manière dont la sûreté des communications de gestion du trafic aérien pourrait être améliorée.

2. CII FIXES ET MOBILES

2.1 Communications fixes

2.1.1 Les principales caractéristiques essentielles à une CII offrant de bonnes conditions de sûreté sont les suivantes :

- a) **Redondance de la topologie :** La CII devrait être planifiée de manière que la connectivité soit élevée entre les nœuds de cœur (un degré minimal de 3 est recommandé) et entre les nœuds d'accès et les nœuds de cœur (là où un «double rattachement» est recommandé);
- b) **Circuits porteurs pour transmission de haute qualité :** Une CII devrait garantir un flux informationnel exact et sans retard dans toutes les circonstances, tant dans les situations régulières que dans les situations d'urgence. Les utilisateurs devraient se voir attribuer la largeur de bande exigée et la qualité de service (QS) convenue. C'est pourquoi des liaisons à grande capacité et des nœuds de commutation intelligents devraient être utilisés. Pour satisfaire au besoin de redondance, les liaisons devraient être de différents types, notamment des liaisons radio à grande capacité (en visibilité directe [LOS] et par satellite [SAT] et par câbles à fibres optiques [FOC]). Pour une gestion efficace de la largeur de bande, les liaisons devraient appartenir à la CII proprement dite et, éventuellement, être séparées des lignes publiques;
- c) **Répartition de l'intelligence du réseau :** La CII devrait être en mesure de fournir des services voix et données de la qualité requise. Elle devrait optimiser, d'une manière dynamique, l'affectation des ressources d'ensemble du réseau, en trouvant le trajet le moins congestionné et, le cas échéant, en exploitant la redondance dans les types de ligne et dans la topologie du réseau. En outre, la CII devrait pouvoir traiter des flux de trafic de priorités différentes, selon différentes catégories de service, et doit être capable d'interrompre les connexions de priorité moindre en cas d'urgence ou de réduction de la largeur de bande disponible. La technologie du mode de transfert asynchrone qui, de par sa nature, offre presque toutes ces caractéristiques, est jugée comme étant le meilleur choix pour l'infrastructure de transmission et le plan de commande de la gestion du réseau;
- d) **Caractéristiques de sûreté :** La CII achemine des données cruciales pour les CNI; elle doit donc être protégée contre les intrusions matérielles, tout comme les données doivent être protégées contre les visualisations ou les modifications sans autorisation. Le problème devrait être résolu par le cryptage et les barrières de sécurité. Des barrières de sécurité devraient être mises en place aux limites des domaines locaux et être configurées de manière appropriée. Elles sont particulièrement importantes dans

le cas des accès à distance aux postes de commande et pourraient inclure de solides mécanismes d'authentification, adéquatement réglés pour différents niveaux d'accès (selon le principe d'origine militaire du *besoin de connaître*). Par ailleurs, il est fortement recommandé que le trafic crucial (comme les mots de passe ou les clés d'authentification, ainsi que les données de commande ou les données système) soit acheminé dans le réseau sous forme cryptée pour éviter toute détection externe de la topologie interne des CNI et de l'emplacement des ressources cruciales par l'analyse du trafic;

- e) **Capacités d'interopérabilité et d'intégration efficaces :** La CII devrait être conçue pour être compatible, dans la mesure du possible, avec les normes d'intercommunication et devrait s'intégrer aux systèmes mobiles et fixes.

2.2 Communications mobiles

2.2.1 Les principales caractéristiques essentielles à un élément air-sol d'une CII offrant de bonnes conditions de sûreté sont les suivantes :

- a) **Interdiction des visualisations non autorisées :** les communications air-sol peuvent être visualisées facilement au moyen d'un récepteur disponible sur le marché. Le problème devrait être résolu par le cryptage et l'authentification de la source de l'information ou par d'autres solutions appropriées;
- b) **Capacité de fonctionner en présence de signaux brouilleurs :** les communications air-sol peuvent être brouillées facilement au moyen d'un récepteur disponible sur le marché. Le problème devrait être résolu par les transmissions par sauts de fréquence ou avec étalement du spectre, ou par d'autres solutions appropriées;
- c) **Capacité de fonctionner en présence de leurrage :** les communications air-sol peuvent facilement faire l'objet d'un leurrage provenant d'un récepteur disponible sur le marché. Le problème devrait être résolu par l'authentification des messages; les sauts de fréquence ou l'étalement du spectre devraient aussi être utiles;
- d) **Intégrité des données :** un haut niveau d'intégrité d'une CII mobile pour ce qui concerne les informations cruciales et sensibles devrait être assuré par la présence d'une liaison de communication air-sol de remplacement (par exemple une liaison de communication par satellite);
- e) **Séparation physique :** pour garantir une gestion efficace des communications, les communications ATM dans le sens air-sol devraient être séparées éventuellement des autres services air-sol, notamment l'Internet, le courrier électronique, les communications publiques, la télévision par câble et les communications d'entreprise (système embarqué de communications, d'adressage et de compte rendu [ACARS] et contrôle d'exploitation aéronautique [AOC]).

3. INITIATIVE STRATÉGIQUE PROPOSÉE

3.1 Il est proposé d'élaborer et de valider, y compris en fonction du rapport coûts-avantages, les lignes directrices sur la sûreté qui vont définir les besoins minimaux en ce qui concerne les aspects liés à la sécurité pour les communications ATM fixes et mobiles, tels que l'architecture au sol et de bord, la

redondance, la connectivité, la protection de l'information, l'interopérabilité, l'intégrité des données et le brouillage/leurage.

4. SUITE À DONNER PAR LA CONFÉRENCE

4.1 La Conférence est invitée à :

- a) reconnaître que les réseaux fixes et mobiles prenant en charge les communications ATM sont des «infrastructures cruciales d'information» et doivent, par conséquent, offrir les garanties de sûreté appropriées;
- b) demander à l'OACI d'élaborer et de valider des lignes directrices applicables aux communications ATM fixes et mobiles sûres prises en charge par les CNI-CII, lignes directrices qui prendront aussi en compte les aspects coûts-avantages.

— FIN —