

# **Rex: Déploiement de la ToIP sur Lyon-Saint Exupéry**

**Mercredi 16 Décembre 2009**

**Dominique MACHU (RSSI)**

[dominique.machu@lyonaeroports.com](mailto:dominique.machu@lyonaeroports.com)



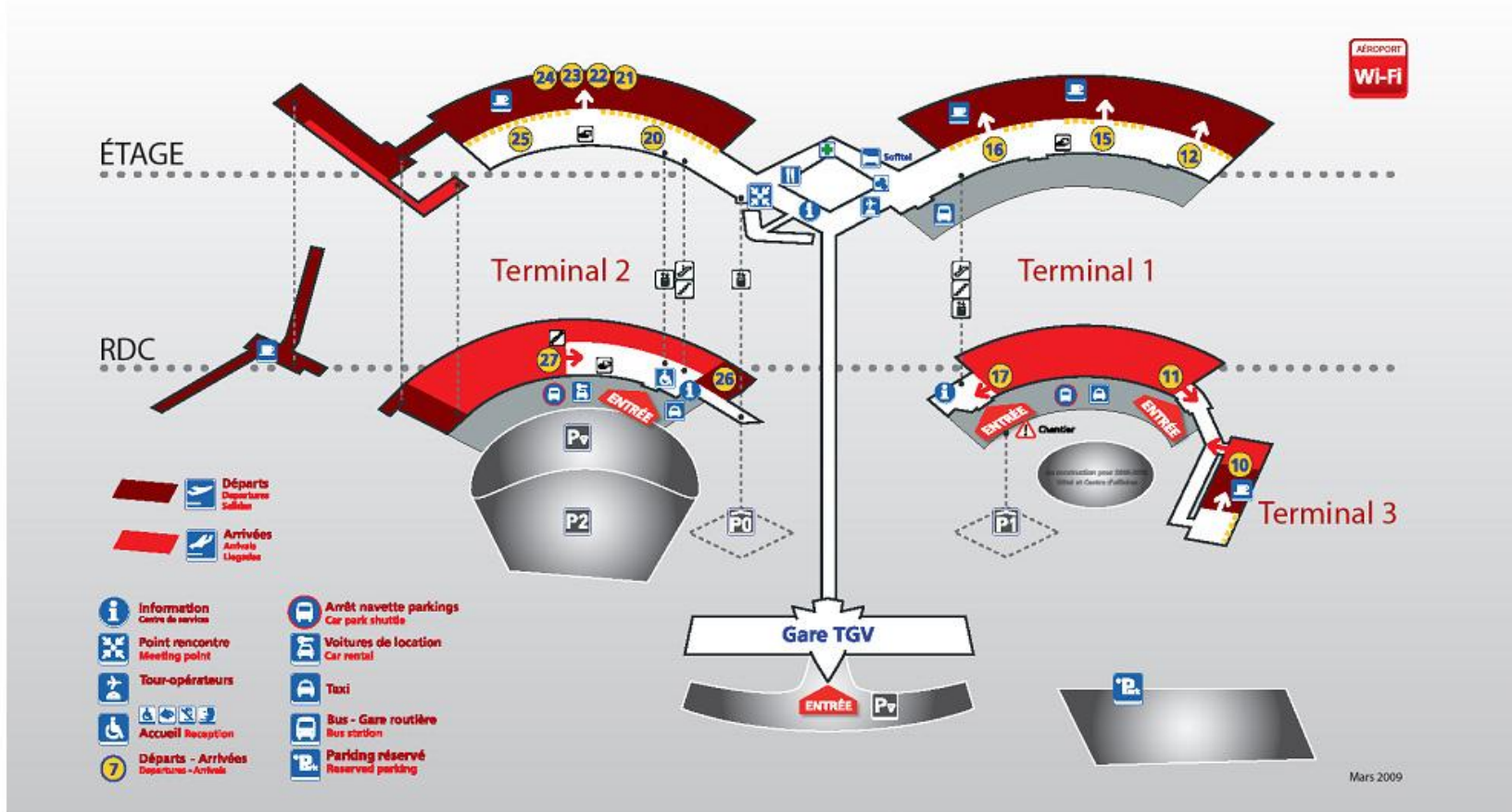
## Infrastructure une des plus modernes d'Europe



- Deux Pistes
  - Piste A: 4 000m
  - Piste B: 2 670m
- Capacité : 52 mouvements / heure
- Terminaux passagers :
  - 3 terminaux pour passagers
  - 1 plate-forme pour le Fret
- 37 postes connectés directement aux terminaux (incluant 16 passerelles)
- Plus de 16 000 places de parking
- 2 000 hectares, dont 900 de réserve foncière pour de futurs développements



## 3 terminaux passagers



## ↘ **Trafic – Chiffres clés (1)**

**62% International**

**7 924 000 passagers**

**jusqu'à 31 000 passagers  
par jour**

**52 mouvements / heure**

**Fret Aérien  
138 000 tonnes**

**plus de 50 compagnies**

**52% affaires  
48% loisirs**

**7 200 mouvements  
en aviation d'affaires**

"Avec 8,2% de croissance en 2008, Aéroports de Lyon affiche la meilleure performance de tous les aéroports français et se positionne largement au dessus de la moyenne européenne".

**plus de 80 routes en vol régulier**





## Projets (2)

Objectif : 12 à 15 millions de passagers en 2020



# Projet de déploiement de la ToIP

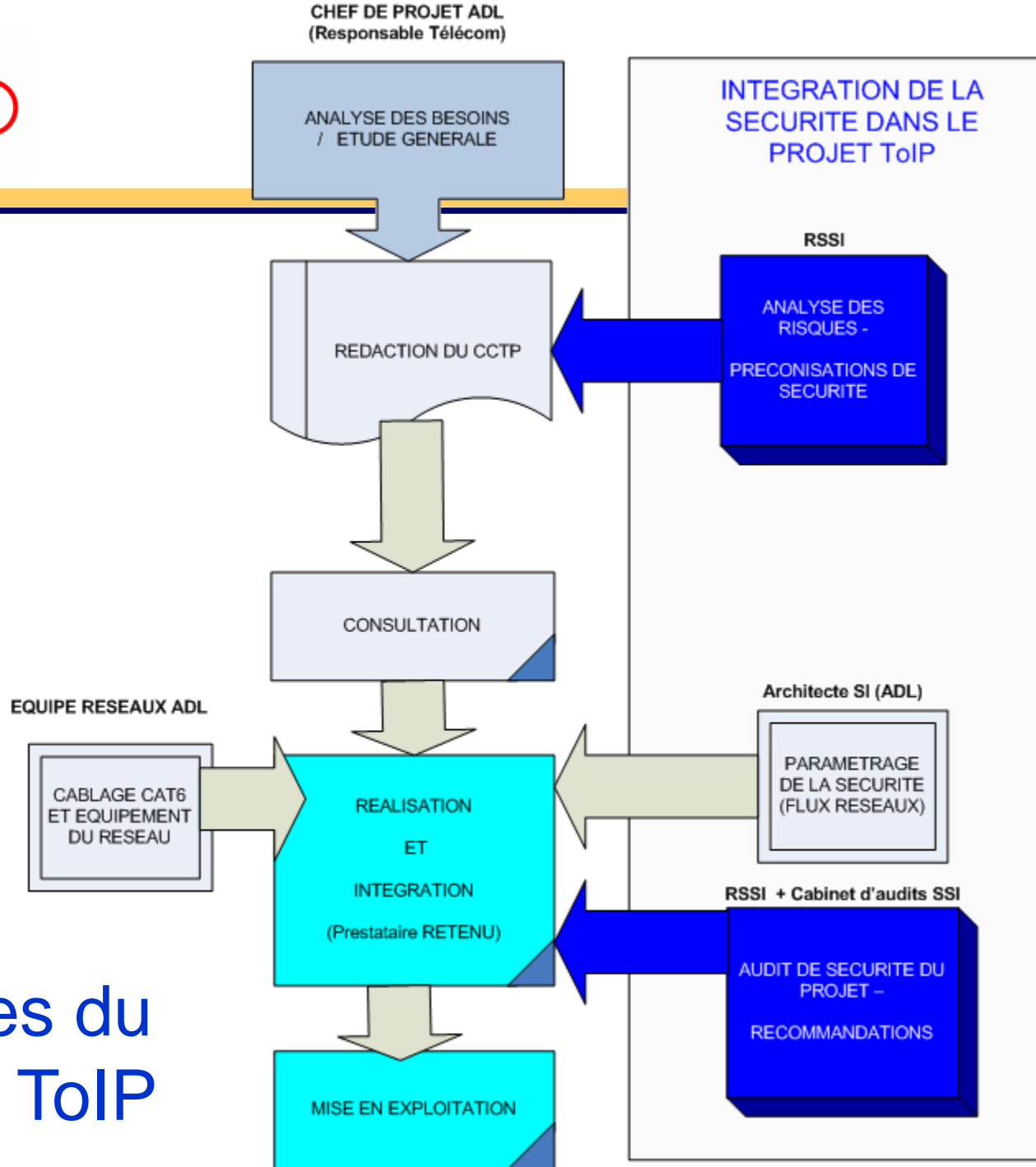
## Contexte du projet de ToIP

- la société Orange Business Services fournit aux Aéroports de Lyon et à la plupart des occupants de la plateforme de Lyon-Saint Exupéry l'ensemble de leurs lignes téléphoniques. Pour cela, Orange Business Services fournit et exploite trois autocommutateurs Alcatel 4400 répartis sur le site.
- Dans ce cadre, les Aéroports de Lyon ont actuellement un contrat pour 1106 lignes, avec 446 lignes administratives, et 660 lignes aéroportuaires.

- Disposer d'un système téléphonique fiable et évolutif,
- Effectuer une avancée technologique en mettant en œuvre la téléphonie sur IP sur l'aéroport Lyon-Saint Exupéry,
- Optimiser ses coûts de fonctionnement en choisissant les meilleures offres correspondant aux besoins. **Cout annuel : 300 K€ --> 180 K€**
- Profiter des nouvelles technologies pour apporter de nouveaux usages aux utilisateurs.

- Evolution du câblage réseau : conjointement au projet évolution du câblage existant (cat 2 et 3 ) non adapté au déploiement de la ToIP par un câblage en CAT 6 ( on garde le câblage en CAT 5)
- Assurer une forte disponibilité du service ToIP
  - Le fonctionnement d'un Aéroport sans téléphones est impensable (660 téléphones métiers) .
- Les téléphones ToIP seront hébergés sur un VLAN dédié sur le réseau des aéroports (10 Gbits redondants)

# Phases du projet de ToIP



# Phases du Projet ToIP

# Intégration de la SSI dans le projet de ToIP

## Etape 1 : analyse des risques - préconisations

## Analyse des Risques (D.I.C.T. \*) :

\*Disponibilité - Intégrité - Confidentialité - Traçabilité

La notion de risque en téléphonie sur IP ne diffère pas de celle en informatique : les risques sont de même nature :

- l'indisponibilité des fonctions téléphonie,
- la confidentialité et intégrité des communications téléphoniques.

**Le niveau de sécurisation sera donc le même que tout autre Système d'information** et l'on devra aussi se prémunir de nouveaux risques spécifiques à la TOIP:

- écoutes téléphoniques , consultation illicites des boites vocales
- appels illicites au frais de l'entreprise
- Déni de services (DOS)
- Attaques spécifiques...

## PREVERSER LA DISPONIBILITE

Impact	1	2	3	4
4	2	3	4	4
3	2	3	3	4
2	1	2	2	3
1	1	1	1	2
Potentialité	1	2	3	4

1 : gravité faible
2 : gravité moyenne
3 : gravité forte
4 : gravité intolérable

Classification des risques

- **Se prémunir des défaillances de l'environnement technique** (climatisation, énergie) et des accidents ( incendie.. ) les équipements actifs du Système ToIP seront hébergés dans les 2 salles serveurs qui sont bien protégés de ces risques
- **La criticité de l'infrastructure de ToIP sur l'aéroport (H24- 660 postes métiers) exige une forte disponibilité et/ou un rétablissement rapide en cas de panne.** Les équipements critiques seront donc dupliqués et des mécanismes de redondance automatique ou par répartition de charge mis en œuvre. Les postes téléphoniques clients devront indifféremment pouvoir se connecter sur l'infrastructure principale ou celle de secours. Idem pour les infrastructures assurant le trafic entrant et sortant.
- **Des tests réguliers doivent en outre être conduits** pour contrôler les procédures de basculement et le bon fonctionnement des systèmes ainsi que des liens redondants (réseau et flux E/S).

## PRESERVER LA CONFIDENTIALITE ET L'INTEGRITE

Impact				
4	2	3	4	4
3	2	3	3	4
2	1	2	2	3
1	1	1	1	2
	1	2	3	4
	Potentialité			

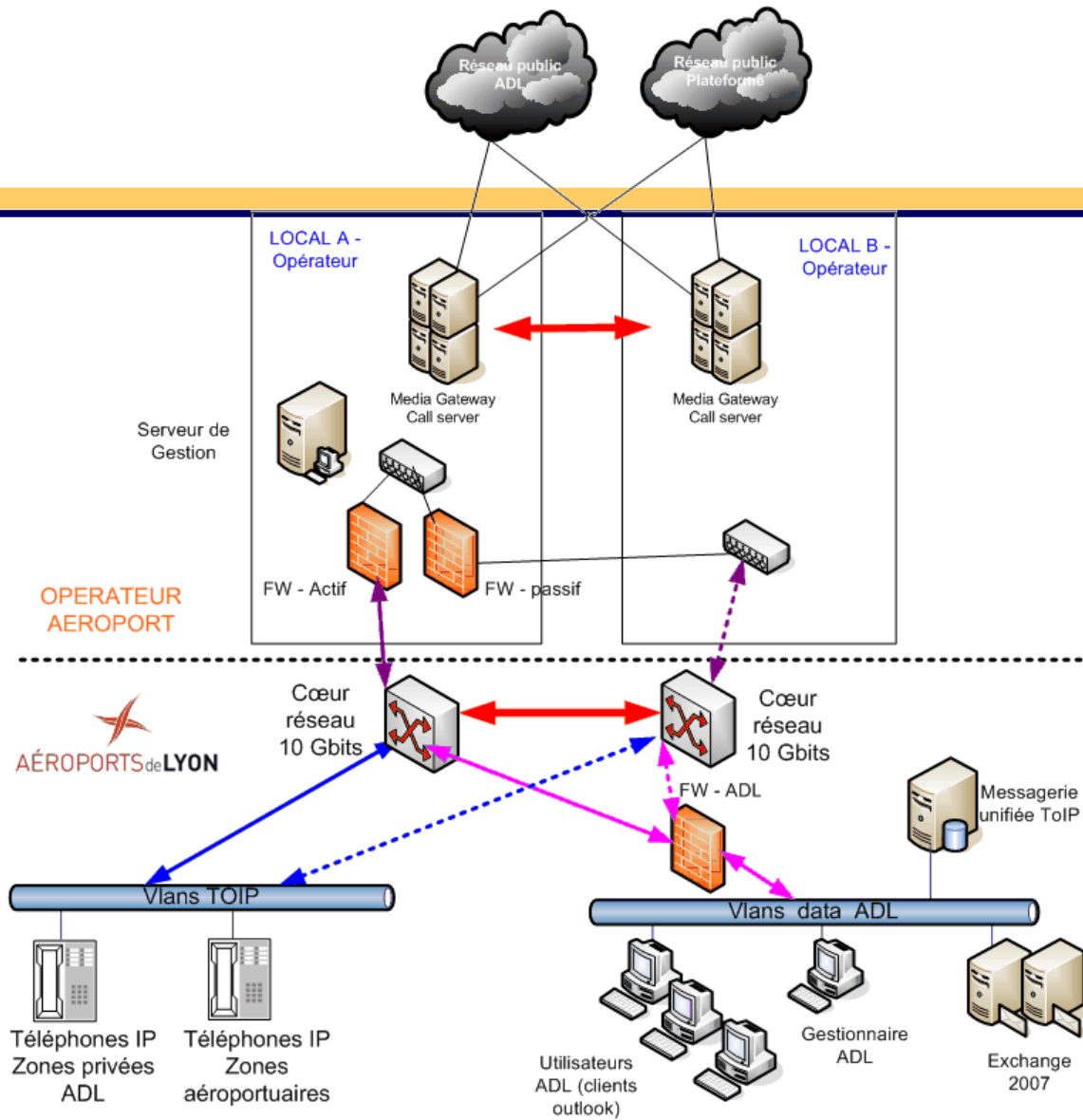
1 : gravité faible
2 : gravité moyenne
3 : gravité forte
4 : gravité intolérable

Classification des risques

- **L'accès à l'infrastructure ToIP sera restreint et contrôlé**
- **Les serveurs et bases de données seront sécurisés selon les règles de l'art** (Mots de passe système et base de données robustes, abolition des mots de passe constructeurs, désactivation des services et ports non actifs..).
- Pour préserver la confidentialité, **les flux de signalisation** (chargés de mettre en relation l'appelant et l'appelé) **et média** (transport de l'information) **seront chiffrés**.  
→ nota : la plupart des 660 téléphones métiers se trouvent dans des « zones publiques »
- **Le réseau ToIP sera implémenté sur un segment séparé** et les flux protégés par les pare-feux de l'infrastructure réseau mis à disposition par les ADL pour le déploiement de la ToIP.
- **Les systèmes seront mis à jour pour corriger les vulnérabilités**, des permissions et droits d'accès seront appliqués, **protection antivirale des serveurs**.
- **L'administration du système s'appuiera sur l'utilisation de protocoles sécurisés** (SSH, SSL, HTTPS .. ;) depuis un poste protégé sur le plan logique et physique (login/PW, antivirus à jour..).

# Intégration de la SSI dans le projet de ToIP

## Etape 2 : Intégration avec « l'opérateur Aéroport »



## Intégration avec « l'opérateur aéroport »

# Intégration de la SSI dans le projet de ToIP

## Etape 3 : Audit Sécurité du projet

- **Vérifier les préconisations de sécurité définies dans le cahier des charges de fourniture d'une solution de ToIP**
- **Vérifier que les équipements actifs et infrastructures réseaux ne présentent pas de vulnérabilités pouvant compromettre les services attendus ou la sécurité de la téléphonie sur IP.**
- **Vérifier que les risques liés à l'usage de la ToIP soient pris en compte et réduits par des mesures de protection de la confidentialité, la disponibilité et l'intégrité.**
- **vérifier le niveau de sécurité par rapport aux menaces et actes de malveillances par connexion illicite sur le réseau ou depuis un poste de travail.**
- **Contrôle de la qualité de service de la fonction ToIP (QoS)**

## DISPONIBILITE

**Taux annoncé : 99.95% (soit une indisponibilité de 4h par an)**

- **Scepticisme sur la capacité à respecter les engagements de disponibilité du service en cas de sinistre majeur sur le local « A » de l'opérateur**
    - **Architecture partiellement distribuée entre les deux locaux**
- **Une indisponibilité de la ToIP est intolérable (analyse de risque) sur les postes métiers et opérationnels de l'aéroport. Pour l'instant le projet à été limité aux téléphones « administratifs »**

## **CONFIDENTIALITE et INTEGRITE**

### **Conversations téléphoniques:**

- **Les flux voix et signalisation ne sont pas chiffrés et peuvent être interceptés**
- **Ce risque est accepté par la direction (diminution du cout du projet par absence de modules de chiffrement). Si la ToIP est déployée dans les zones publiques ce point est à revoir.**
- **Recommandation : désactiver la sortie PC (non utilisée) sur les téléphones IP**

### **Réseaux:**

#### **Les bonnes pratiques sont été mises en œuvre**

- Cloisonnement des réseaux
- Ports inutiles fermés sur l'ensemble des équipements testés

## **CONFIDENTIALITE et INTEGRITE (suite)**

### **Serveur de messagerie unifiée:**

- Les mots de passes par défaut non pas été modifiés
  - Accès aux Bal et « messagerie vocale » de l'ensemble de l'entreprise
  - Pas de protection anti-virus
  - Pas de patches de sécurité déployés
- **Ce serveur peut devenir le « talon d'Achille » au niveau sécurité de votre S.I. !**

### **Recommandations :**

- Revoir politique des mots de passes
- Sécuriser le « Système d'exploitation » (AV et patches de sécurité)
- Utilisation de l'authentification AD\_(application des politiques SSI de l'entreprise)
- Sécurisation des Flux Web (Portail du serveur)

# Intégration de la SSI dans un projet de ToIP

## **CONCLUSION**

■ **La ToIP est génératrice d'avantages :**

- **Diminution du cout de fonctionnement de la téléphonie (Cout abonnement, maintenance, câblage banalisé, configuration..)**
- **Apport de nouveaux service aux utilisateurs (messagerie unifiée et intégration dans le client de messagerie de l'entreprise)**
- ...

**Mais :**

- **La ToIP doit être considérée comme un système d'information à part entière et doit être sécurisée au même titre que tout S.I. de l'entreprise (D.I.C.T.) au risque de le mettre en péril.**

**2 actions sont à mettre en œuvre dans un projet de ToIP :**

- **Bien évaluer les risques induits en amont du projet (analyse de risque et préconisations de sécurité )**
- **S'assurer de l'application des règles et politiques de SSI de l'entreprise (réalisation d'un audit)**