Assistance Publique
Hôpitaux de Marseille

SECURISER LES EQUIPEMENTS TECHNIQES HOSPITALIERS

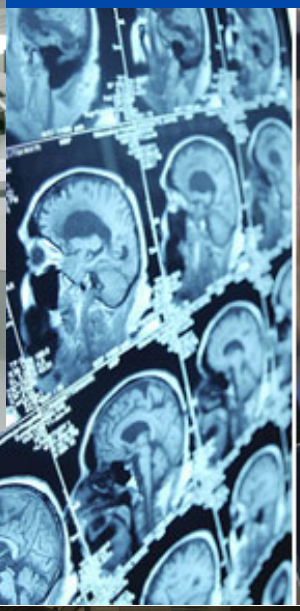
- **Sécuriser Dispositifs Biomédicaux et équipements Techniques pourquoi ?**
  - Des équipements Biomédicaux de plus en plus informatisé : *logiciel = Dispositif Médical*
  - Des équipements techniques de plus en plus tournés vers le numérique et le réseau : GTC, Pilotage ….

- Evolutions des systèmes d'information et des technologies (IT):

  Des architectures en mutation :

  – D'isolées à : connectées, hébergées (interne /externe), virtualisées, « cloudisées », …

- Impacts, réalité et projection « fiction »:
  – Une carte défaillante de sécurité incendie peut amener à fermer des locaux et arrêter les services associés ;
  – La perte d'un service du 'cloud' pourrait-il amener à dégrader/arrêter l'activité d'un établissement de santé ?



B
I
O
M
E
D

Grande diversité des composants

Exemple d'Evolution d'un DM : Réseau EEG

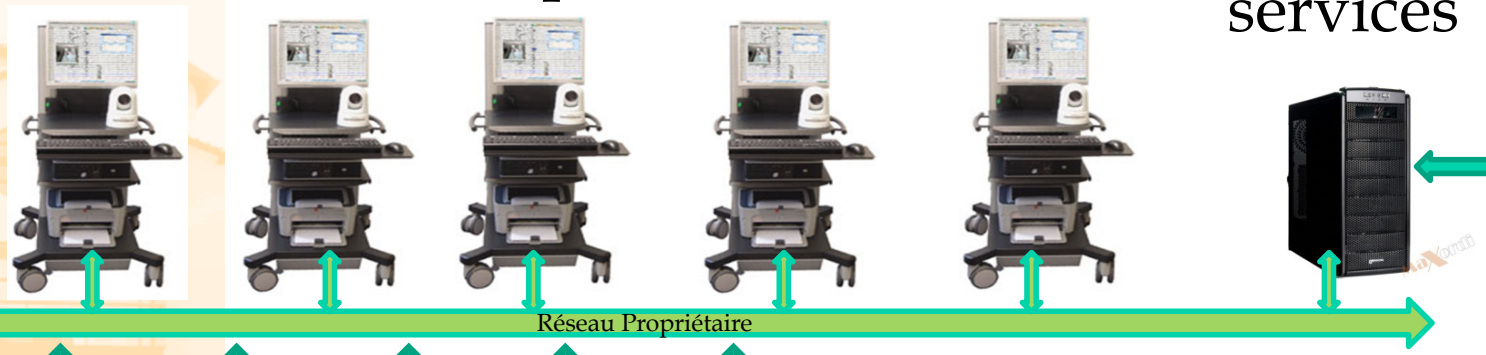
Configuration initiale (- 17 ans)

Autonomes, aucune connexion, Impossibilité de transmettre <u>RAPIDEMENT</u> des résultats.

Configuration 1

1 Serveur de données par services

Postes d'acquisition



Postes de relecture

Réseau ETBS

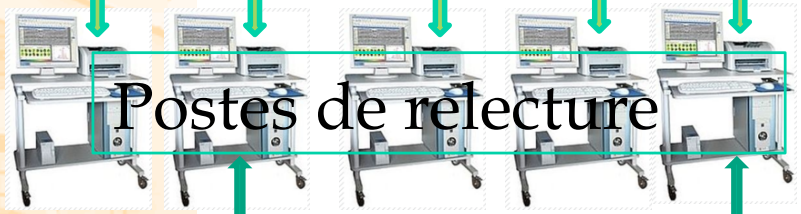
Configuration 2 : site par site

Postes d'acquisition

1 Serveur de données par services

Réseau Propriétaire

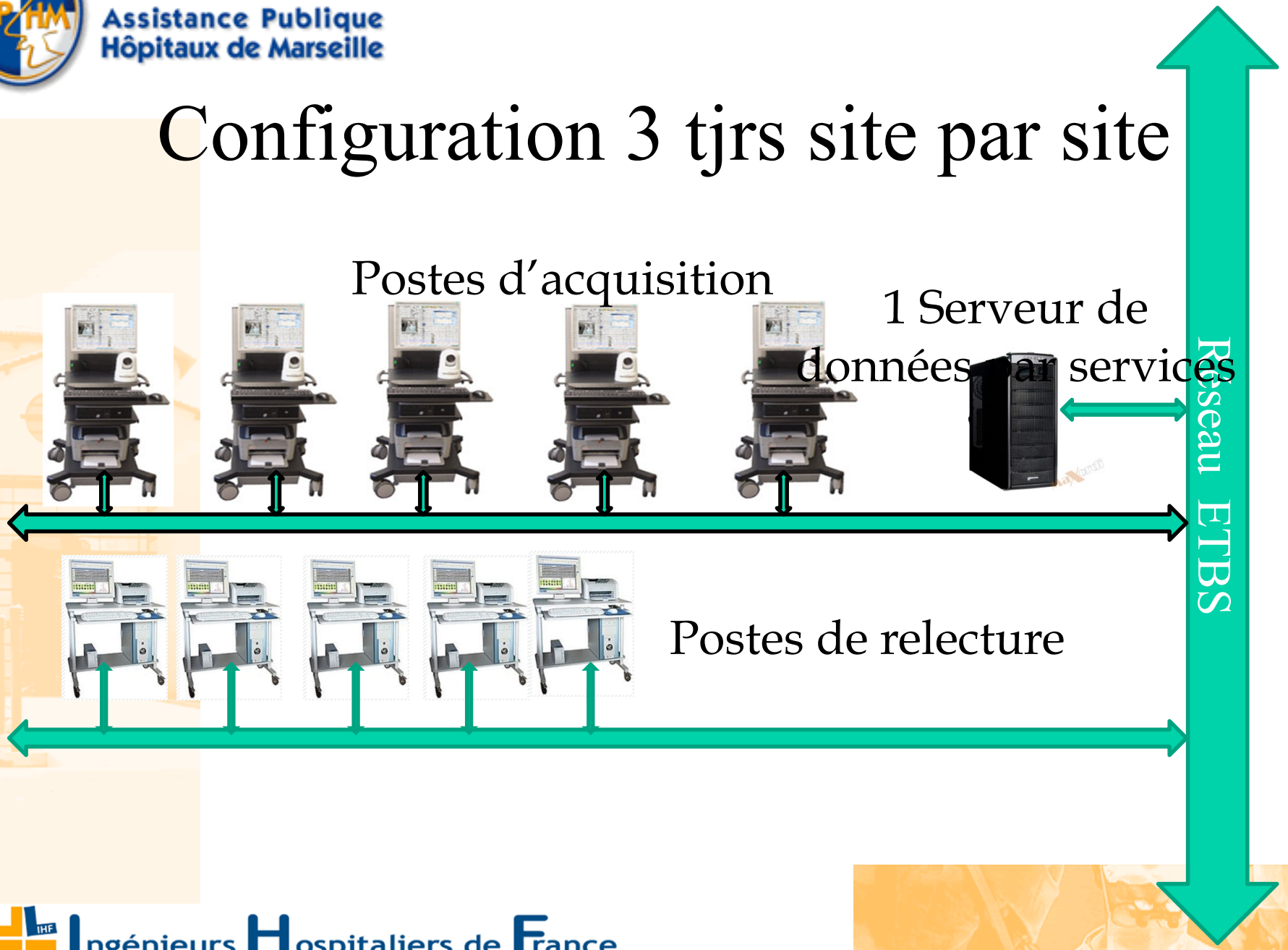
Postes de relecture



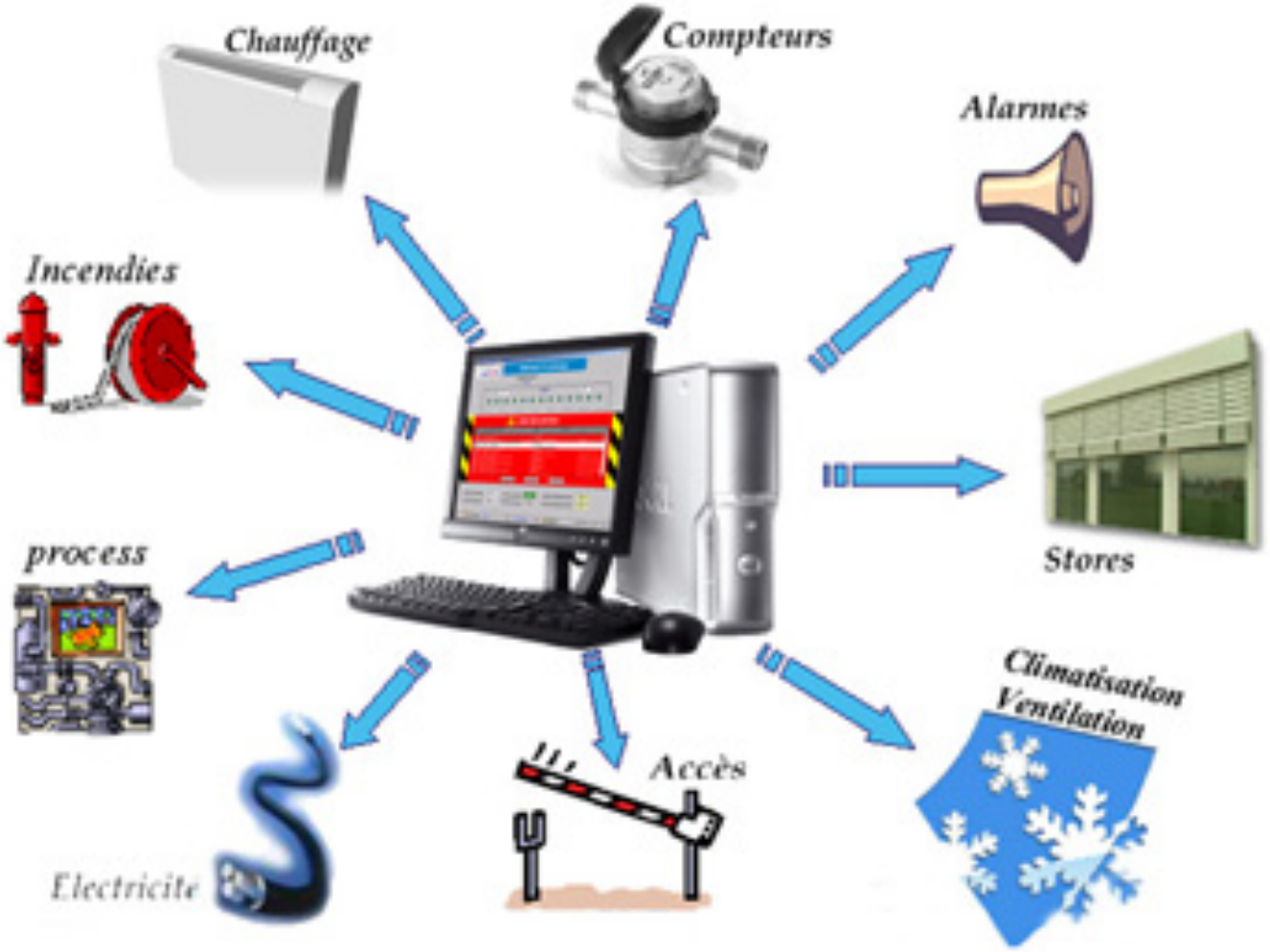
Réseau ETBS

Maintenance sur site

Configuration 3 tjrs site par site



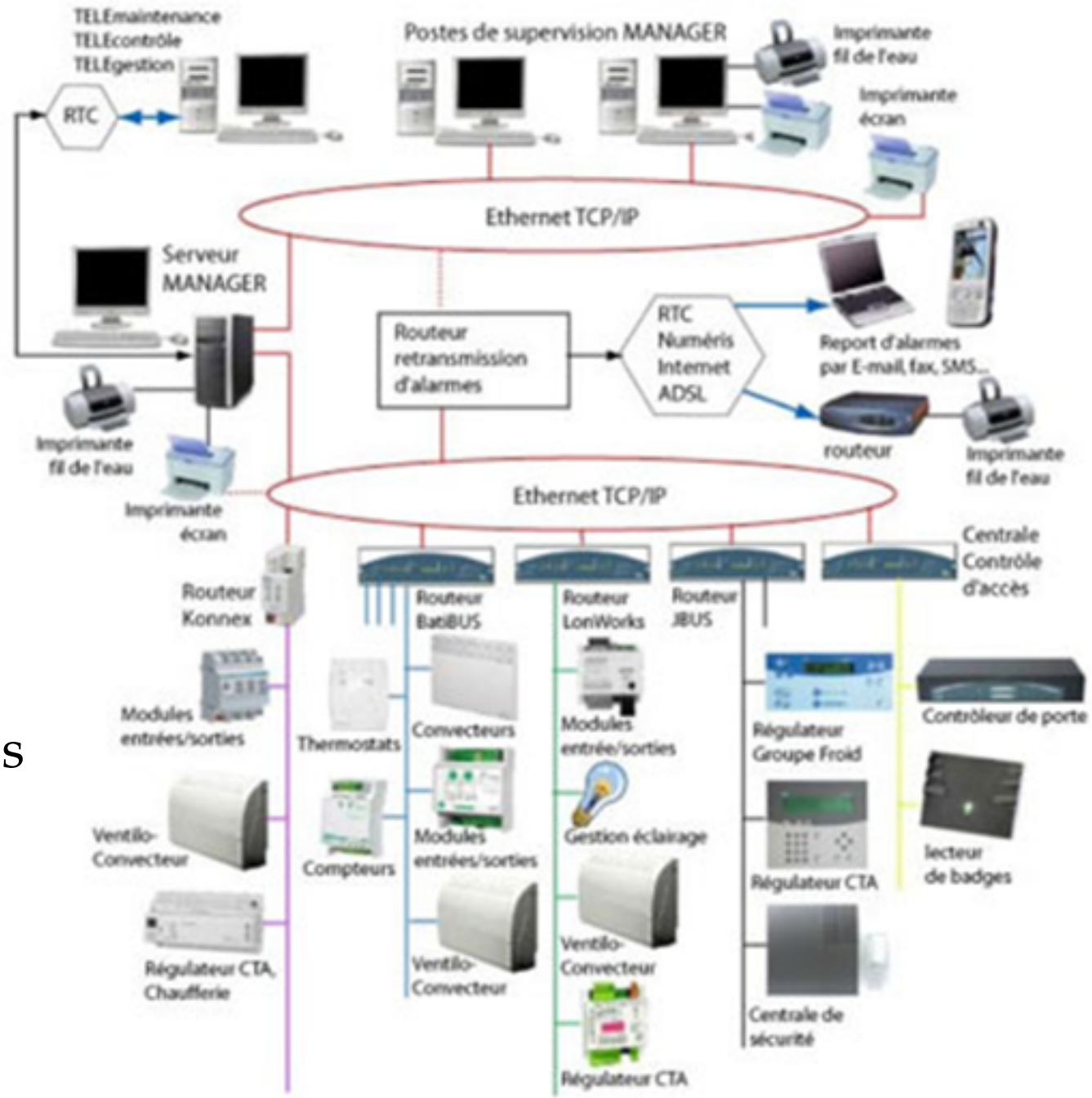
Quant aux Equipements de Gestion Technique …



Assistance Hôpitaux de

GTC

Des architectures complexes, voire « floues »



Le Cadre de référence

- Les normes de sécurité ISO 2700x
- Le Référentiel Général de Sécurité créé par l'article 9 de l'ordonnance n° 2005-1516 du 8 décembre 2005 (décret 2010-112 du 2 fév. 2010, arrêté 6 mai 2010)
- La Loi n° 78-17 du 6 janvier 1978 (CNIL)
- Les alertes issus du Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques – CERTA
- PMSSI et la PGSSI (en cours de finalisation)

et pour les Dispositifs Médicaux :

- La Directive européenne 2007/47 sur les dispositifs médicaux (ordonnance de transposition du 12 mars 2010),
- Le Décret n° 2001-1154 du 5 décembre 2001 relatif à l'obligation de maintenance

Quelle approche pour améliorer la sécurité ?

- *L'Approche* ***Empirique***
  - Par quelle recette commencer ?

OU

- *L'Approche par les* ***Risques***
  - Prioriser les actions et les systèmes et ré évaluer

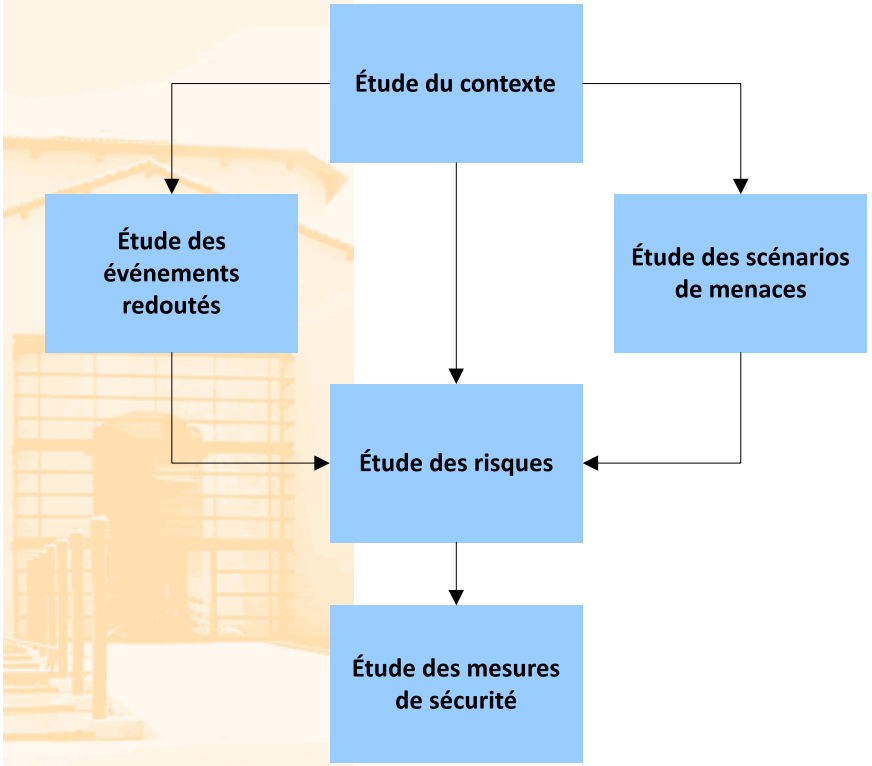
\+ difficulté/effort de mise en œuvre liés aux contraintes techniques et organisationnelles (internes et externes)

Gérer les risques

- Un cadre ISO :
  - 27001 (*mangement*) ,
  - 27005 (*démarche d'analyse de risque*),
  - 27002 (*catalogue de mesures*)
- La méthode EBIOS (*gouvernementale et conforme à l'ISO*)

EBIOS

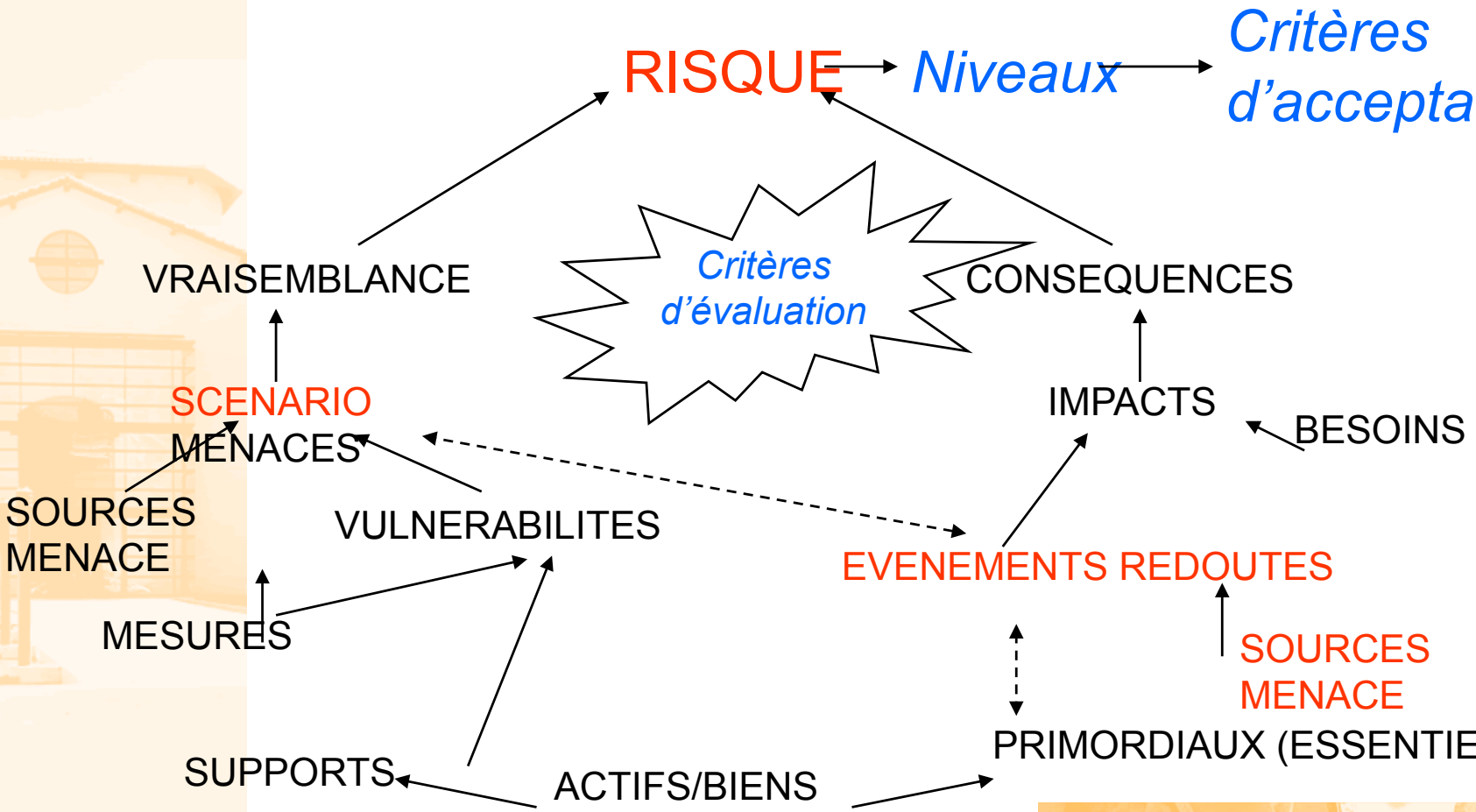
'5 modules en synthèse'



1. Étude du contexte	Pourquoi et comment va-t-on gérer les risques ? Quel est le sujet de l'étude ?
2. Étude des événements redoutés	Quels sont les événements craints par les métiers ? Quels seraient les plus graves ?
3. Étude des scénarios de menaces	Quels sont tous les scénarios possibles ? Quels sont les plus vraisemblables ?
4. Étude des risques	Quelle est la cartographie des risques ? Comment choisit-on de les traiter ?
5. Étude des mesures de sécurité	Quelles mesures devrait-on appliquer ? Les risques résiduels sont-ils acceptables ?

Une guide et une base de connaissances : ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), www.ssi.gouv.fr

Le risque selon l'ISO 27005 et EBIOS 2010



LA CARTOGRAPHIE DES COMPOSANTS DU RISQUE selon EBIOS 2010

Evènements redoutés	Communs	Scénarios de menaces
	Sources de menaces	
Biens essentiels	← Supportent	Biens supports
	Critères (D,I,C, …)	
Besoins de sécurité (GRAVITE)		Menaces
Impacts		Vulnérabilités (VRAISEMBLANCE)

Niveau de Risque brut = f(**G**ravité,**V**raisemblance)

Niveau de Risque net = f(**G**ravité,**V**raisemblance) – g(Mesures existantes)

Exemple 1 de décomposition du risque

Risque 1 : **La perte ou l'indisponibilité prolongée des données de recherche médicale** (patrimoine de recherche composé de données difficilement reproductibles (vidéos, photos, documents numériques) : par exemple des cas cliniques rares et servant à réaliser des recherches à postériori), **peut empêcher de répondre à des appels d'offre pour des contrats de recherche. L'impact peut être financier et d'image/renommée.**

Composants du risque

Bien essentiel	Patrimoine d'expérimentation
Besoin de sécurité	Non perte ou indisponibilité qq jours maximum
Impact	Perte du patrimoine, arrêt de l'activité, perte financière, Image de marque
Source de menace	Humaine Interne accidentelle ou evt interne . Humaine externe volontaire (pour source de menace avec intérêt pour les matériels)
Critère de sécurité	Disponibilité
Bien support	Ensemble du SYStème supportant le stockage incluant : exploitant de la chaîne informatique [PER], serveurs, baies de stockage, DVD [MAT]…)
Menace	Coupure électrique (avec dommages), panne serveur[MAT-DEP], détérioration [MAT-DET], départ ou erreurs de l'exploitant, vol [MAT-PTE]
Vulnérabilité	Par défaut toutes celle de ce type de [SYS]tème/dispo

Exemple 2 de décomposition du risque

Risque 2 : **Une diffusion de la maladie « sensible » d'un patient peut entrainer une condamnation suite à plainte et atteindre à l'image de l'établissement voire entrainer l'arrêt de l'activité de suivi médical associé.**

Composants du risque

Bien essentiel	Données patient confiées sur la base du volontariat
Besoin de sécurité	confidentialité
Impact	Arrêt de l'activité (perte de confiance des patients), plainte des patients (condamnation), perte d'Image, …
Source de menace	humaine interne
Critère de sécurité	Confidentialité
Bien support	Application xxxx [LOG] (et ensemble du SYStème le supportant : administrateurs métier, exploitant de la chaîne informatique [PERS], serveurs, stockage, réseau… [MAT] [RSX])
Menace	Menaces sur la confidentialité : usurpation de droits, manque protection du logiciel [LOG-], absence de sensibilisation des usagers [PER-USG/DET] , …
Vulnérabilité	Par défaut toutes celles de ce type de SYStème associées aux menaces pour le critère de confidentialité

Assistance Publique
Hôpitaux de Marseille

EBIOS*
par la pratique

**Expression des Besoins et Identification des Objectifs de Sécurité.*
Marque déposée par le SGDN

Les productions

Tableau des événements redoutés
(Bdc Ebios sources de menaces/impacts)

Tableau des scénarios de menaces
(Bdc Ebios menaces/ vulnérabilités)

Tableau des risques

Choix de traitement

PSSI

Mesures ***(Bdc Ebios mesures : ISO 27002, RGS)***

Tableau de bord SSI

Assistance Publique
Hôpitaux de Marseille

Tableau des risques (*exemple*)

Événement redouté	Besoin de sécurité	Impacts	Scénario de menaces et menaces	Sources de menaces	Vraisemblance	Gravité
ER1. Compromission de pièces jointes	4. Privé (variable)	**Impacts** Perte d'un marché Pertes financières	SM6. Compromission par une menace sur un employé Départ d'une personne Espionnage d'une personne à distance Influence sur une personne	**Sources de menaces** Concurrent avide Employé peu sérieux	3. Importante	3. Forte

Extrait étude de cas ANSSI : compromission de mel

Un cas pratique à réaliser

- **Dérouler un raisonnement EBIOS :**
- **Objectif :**
  - **Identifier et hiérarchiser les risques majeurs**
  - **Proposer une mesure par risque**

- **Périmètre : Disponibilité de la gestion (aiguillage des SMUR) des appels au Samu**

P. Tourron / Tous droits réservés

Le contexte

- Les biens essentiels

P. Tourron / Tous droits réservés

Le contexte simplifié

- Les biens essentiels
  - Recevoir un appel au 15
  - Aiguiller des secours
  - …

Le contexte simplifié

- Les biens supports

Le contexte simplifié

- Les biens supports
  - Téléphonie
  - Postes de régulation
  - Réseau local
  - Application métier
  - Autres applications et systèmes
  - Radio (communication)
  - …

Le contexte simplifié

- Liens biens essentiels / supports
  - Recevoir un appel au 15
    - Téléphonie
    - Locaux techniques
  - Aiguiller des secours
    - Réseau local
    - Application métier
    - Autres applications et systèmes
    - Radio
    - Locaux techniques
    - Serveurs / data center

Mesures existantes exemples

- PRA (plan de reprise d'activité)
- Antivirus
- Maintenances
- Procédures (manuelles)
- Charte utilisateur
- Astreintes
- …

Sources de menaces

P. Tourron / Tous droits réservés

Evénements redoutés

P. Tourron / Tous droits réservés

Evénements redoutés

- Perte du 15
- Perte du service applicatif (suivi des appels)

- Gravité

P. Tourron / Tous droits réservés

Scénarios de menaces

P. Tourron / Tous droits réservés

Scénarios de menaces

- Sur les biens supports :
  - Téléphonie
  - Postes de régulation
  - Réseau
  - « système » applicatif

Vulnérabilités/sources

Vraisemblance

P. Tourron / Tous droits réservés

Composition des risques

P. Tourron / Tous droits réservés

Assistance Publique
Hôpitaux de Marseille

Tableau des risques (*exemple*)

Événement redouté	Besoin de sécurité	Impacts	Scénario de menaces et menaces	Sources de menaces	Vraisemblance	Gravité

P. Tourron / Tous droits réservés

Composition des risques

- Perte du 15 (critère D)
- Vital
- Défaut de batterie autocom
- Vraisemblance (liée au niveau d'entretien)

P. Tourron / Tous droits réservés

Composition des risques

- Perte du service applicatif (critère D)
- Vital
- Attaque viral / déni de service pour accès au serveur distant
- Vraisemblance (liée au niveau d'entretien)

P. Tourron / Tous droits réservés

Traitement des risques : mesures

- Mise en Sécurité des locaux
- Suivi / révision des maintenances
- Politiques antivirales spécifiques
- Résilience réseau local renforcée
- Formation personnels d'Astreintes
- Formation/sensibilisation utilisateurs
- …

P. Tourron / Tous droits réservés

Synthèse du processus EBIOS

- *Scénariser (événements redoutés, menaces, risques)*
- *Choisir le traitement des scénarios de risques*
- *Proposer des mesures de traitement*
- *Arriver aux objectifs métiers*

Transposition au périmètre Biomédical (ex : EEG)

P. Tourron / Tous droits réservés

Objectif

Postes d'acquisition

Postes de relecture

Postes d'acquisition

Postes de relecture

Réseau ETBS

Mainteneur
à distance

1 seul Serveur
hébergé DSI

Scénario :

- Lors d'une visite de maintenance sur des postes non SIH connectés au réseau, un employé du prestataire utilise sa clef USB pour effectuer une mise à jour et 'infecte' par un virus les machines maintenues puis celles du réseau qui ne sont pas protégées soit par omission, soit pour des raisons techniques. Les machines infectées ne permettent plus de produire les résultats nécessaires aux soins des patients. Les chances de soins aux patients peuvent être diminuées.

Le contexte simplifié

Les enjeux :

Fiabiliser les fonctionnements (et garantir un accès contrôlé aux informations et aux process).

Prise en compte

- De **la disponibilité (intégrité)** des données patient;
- De l'**Interpénétration** des SI (composites) ;
- Du **Passage d'un mode isolé à un mode communiquant et mutualisé**

Le Processus médical :

Exploration fonctionnelle. Informations « gérées » par ces dispositifs sont très diverses :

Données patients : avec comme objectif de sécurité une confidentialité et intégrité importantes ainsi que la disponibilité (phase d'urgence) ;

Données techniques : avec comme objectif de sécurité une disponibilité et une intégrité importantes des éléments relatifs aux configurations, résultats …

P. Tourron / Tous droits réservés

Le contexte simplifié

- **Les Sources de menaces**

d'Origines Humaines : les Techniciens de maintenance externes (erreurs de configuration, transfert de virus lors de mise à jour par clef usb, …)

- Les biens supports
  - Les postes (acquisition, lecture)
  - Le serveur
  - Le réseau
  - Les mainteneurs

P. Tourron / Tous droits réservés

Le contexte simplifié

- Liens biens essentiels / supports
  - Relire un résultat
    - Serveur, réseau, postes de relecture
    - Locaux techniques
    - Les mainteneurs
  - Acquisition
    - Serveur, réseau, postes d'acquisition
    - Locaux techniques
    - Les mainteneurs

Mesures existantes exemples

- Maintenances
- Procédures (manuelles, reprises, dégradées)
- Antivirus ? À jour ?
- …

Sources de menaces

(extrait base de connaissaces Ebios 2010)

Evénements redoutés

Evénements redoutés

- Perte du « service » d'acquisition Gravité 2 (je peux m'en passer pendant x heures) ER1
- Perte du « service » de relecture Gravité 2 (je peux m'en passer pendant x heures) ER2
- Perte des données Gravité 4 ER3

Gravité 0 à 4

Scénarios de menaces

Scénarios de menaces

- Sur les biens supports :
  - Composant (**relecteur**) sans antivirus (ou pas à jour)
  - Composant mis à jour par clef usb
  - Par propagation tout composant non/mal protégé peut être impacté

  SM1 vraisemblance 4
  - Vulnérabilités/sources de menace
  - Par un **mainteneur** peu sensibilisé à la sécurité

Vraisemblance 0 à 4

P. Tourron / Tous droits réservés

Scénario de menace selon base de connaissance Ebios 2010

- **M11. LOG-MOD – Modification d'un logiciel**

Le logiciel est modifié. Il peut ainsi dysfonctionner ou ne plus fonctionner (substitution ou ajout de fonctionnalités).

piégeage logiciel :(keylogger, ***contagion par un code malveillant****, substitution d'un composant par un autre…).*

- Critère(s) de sécurité concerné(s) : **Disponibilité Intégrité Confidentialité**
- Principales vulnérabilités exploitables :

Maîtrise insuffisante par les développeurs ou les mainteneurs (spécifications incomplètes, peu de compétences internes…)

-

Composition des risques

Assistance Publique
Hôpitaux de Marseille

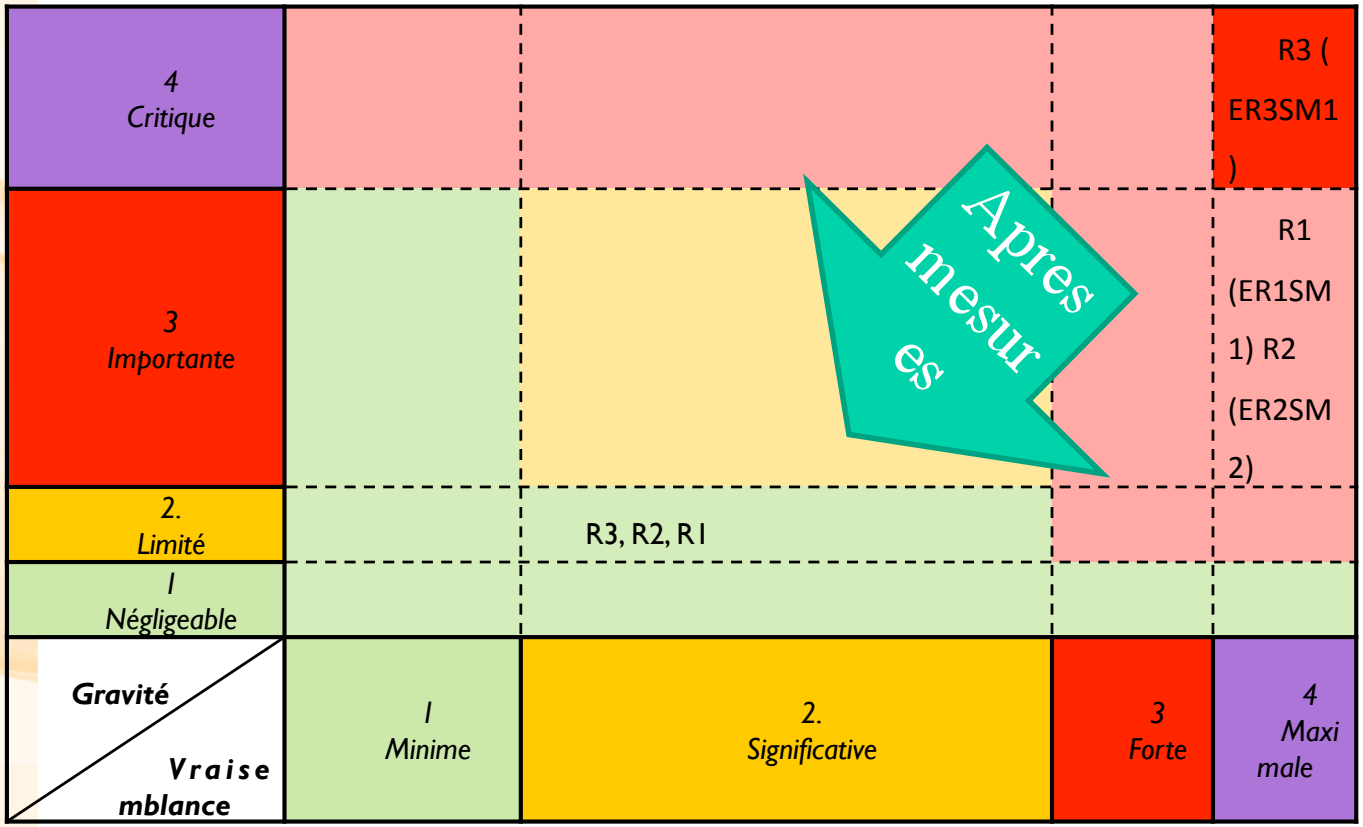
Tableau des risques (*exemple*)

Événement redouté	Besoin de sécurité	Impacts	Scénario de menaces et menaces	Sources de menaces	Vraisemblance	Gravité
Perte des données	4	• Perturbation du fonctionnement • Perte de chance	Introduction d'une clef usb avec virus [M11]	maintenueur	4	4

Composition des risques

- Lors d'une visite de **maintenance** sur des postes non SIH connectés au réseau **[relecteur EEG]**, un employé du **prestataire** utilise sa **clef USB** pour effectuer une mise à jour et 'infecte' par un **virus** les machines pas protégées soit par omission, soit pour des raisons techniques puis celles du réseau qui ne sont maintenues. Les machines infectées ne permettent **plus de produire** les résultats nécessaires aux soins des patients. Les **chances de soins** aux patients peuvent être diminuées.

Représentation des risques



Traitement des risques : réduction par des mesures (évitement, transfert, prise)

- Politiques antivirales spécifiques
- Cloisonnement réseau et filtrage de zones pour éviter la propagation
- Formation/sensibilisation des mainteneurs et personnels encadrant les maintenances
- Affichage de consigne de sécurité sur les postes
- Analyse préalable des clefs usb de mainteneurs (transfert sur un clef fiable à partir d'un poste dédié, adapté et sécurisé)
- …

P. Tourron / Tous droits réservés

Périmètres de sécurité

- Conformité légale (CNIL, archivage)
- Responsabilité et sensibilisation des intervenants
- Maintenance à distance : engagements des mainteneurs (contenu et usage)
- Remonté d'information à l'extérieur de l'établissement : engagements des mainteneurs (contenu et usage)
- Auditabilité : compte d'audit (RSSI)
- Réversibilité : restitution des données par clause du marché
- Architecture : vlan, filtrage selon niveau d'intégration
- Serveur (configuration et administration sécurisés : correctifs de sécurité, antivirus, services et comptes maîtrisés)
- Poste (configuration et administration sécurisés : correctifs de sécurité, antivirus, services et comptes maîtrisés)
- Administration des parcs: authentification(comptes/Carte), mode d'acces et d'intégration (domaine)

Les axes de sécurisation : les outils

- Fiche FASSI (analyse de sécurité simplifiée)
- Questionnaire d'évaluation de la sécurité (capacité et niveaux d'intégration : du gold à la boîte noire) : pour marché et existant
- Engagement de confidentialité
- Procédure d'acces distant
- Mise à disposition de moyens de mise en conformité (OS , antivirus)
- Fiche CIL
- Rapport type d'intervention

Les axes de sécurisation : organisation

- Analyser les marchés conjointement Biomedical/RSSI/DSI
- Un système de management de la SSI intégrant le biomedical :
  - Correspondants SSI du biomedical
  - intégrés au Comité Opérationnel SSI (analyser les risques, identifier les mesures, les difficultés d'application, amélioration suite aux incidents, …)
  - Intégrés à la cellule de crise SSI (entrainement et réalité)

Approche par niveau d'intégration / niveau de risque

- A un niveau de conformité sécurité
- Une réponse d'intégration

Les niveaux d'intégration au SI (questionnaire Marché et existant)

Grille de niveau d'intégration	
PREMIUM	SSI = SIH / DSIO
GOLD	SSI partielle (les basics)
SILVER	Minima accepté
Isolé et filtré	Non interconnecté au réseau standard APHM soit interconnecté avec filtrage des protocoles et des sources de destination préalablement identifiés et validés

Questions		Réponse *Cocher la case*
6	**Si vous ne gérez pas les mises à jour Windows et un antivirus, êtes-vous d'accord pour que :**	
	Les mises à jour Windows soient installées automatiquement dans le processus de l'AP-HM	A ☐
	Les mises à jour Windows soient automatiquement proposées, mais installées par les soins de votre technicien ou d'un personnel biomédical	B ☐
	L'antivirus de l'AP-HM soit installé (xxxxxxx) et tenu à jour automatiquement	C ☐

Réponses	PREMIUM	GOLD	SILVER	Isolé et filtré
1				
	A ☐	A ☐	A ☐	
				B ☐
2				
			A ☐	A ☐
	B ☐	B ☐		
3				
	A ☐			
		B ☐		
			C ☐	
				D ☐
4				
			A ☐	
	B ☐			
		C ☐		
5				
	A ☐	A ☐	A ☐	
	B ☐	B ☐		
			C ☐	
				D ☐
				E ☐
6				
	A ☐	A ☐	A ☐	
			B ☐	
	C ☐	C ☐		
7				
		A ☐		
			B ☐	
	C ☐			
8				
	A ☐			
		B ☐	B ☐	
			C ☐	
			D ☐	
	E ☐			
Niveau Attribué				

Bilan et perspectives

Comment sécuriser sans bloquer ? : une trajectoire par étape

- Mixer les cultures et les hommes (une organisation transverse ou structurelle)
- Parler vrai, parler couts et budgets d'intégration
- Etre ensemble sur le pont : gestion de crise
- Commencer par les nouveaux systèmes
- Déployer des architectures techniques d'intégration : réseau , système
- Faire progresser ensemble les éditeurs (liste blanche, …)

A vous de jouer

Assistance Publique
Hôpitaux de Marseille

MERCI DE VOTRE ATTENTION

Ingénieurs Hospitaliers de France