apsys
SIMPLIFYING COMPLEXITY

Les points clés et les évolutions de la certification avionique

Atelier ARP4761

FABRE Pascal – Project Manager - 18 Septembre 2013

Les points clés et les évolutions de la certification avionique

Atelier ARP4761

Guidelines and Methods for conducting the safety assessment process on civil airborne systems and equipment

SOMMAIRE

- **Partie A - Les points clés de l'ARP4761**
- **Partie B - Les évolutions vers l'ARP4761A**

Les points clés et les évolutions de la certification avionique

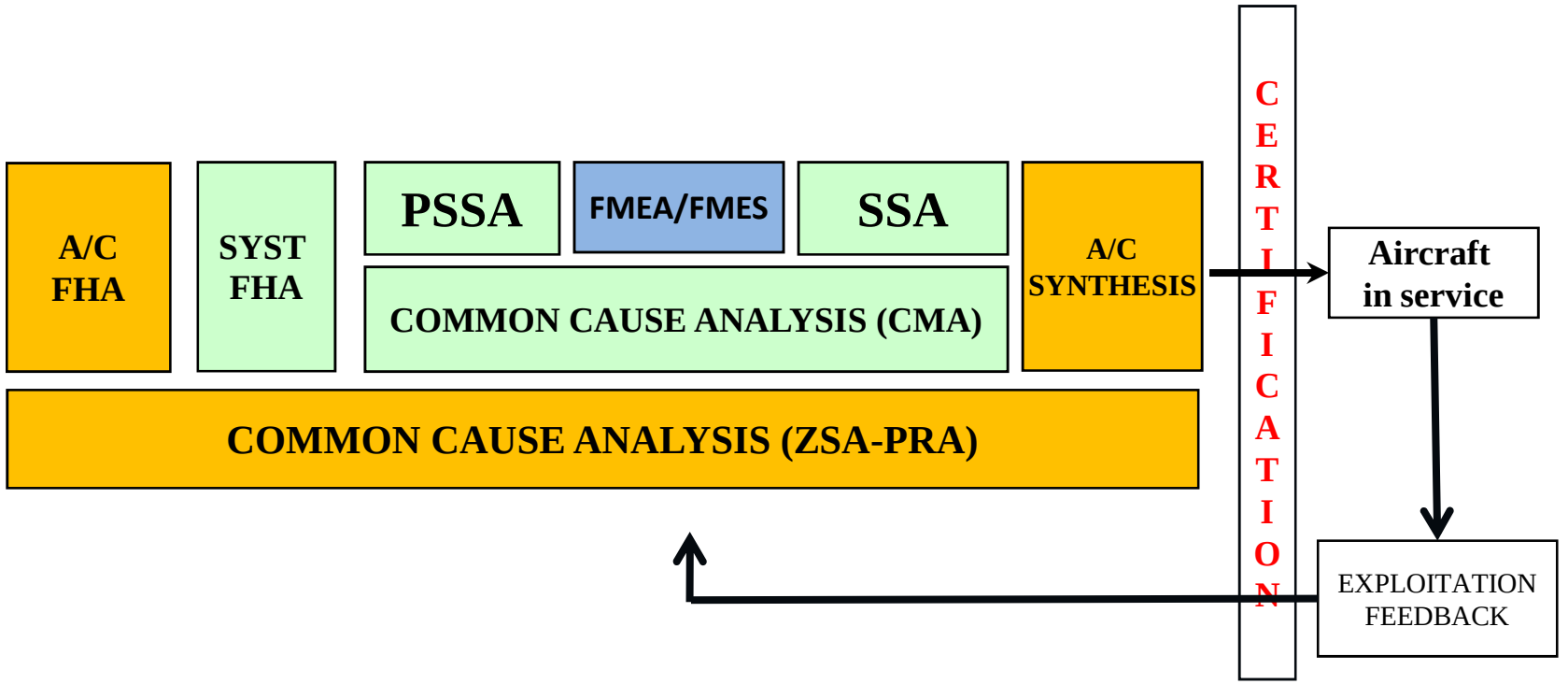
Atelier ARP4761

Partie A : Les points clés de l'ARP4761

ARP 4761

- **FHA** : Functional Hazard Assessment
- **PSSA** : Preliminary System Safety Assessment
- **SSA** : System Safety Assessment
- **CCA** : Common Cause Analysis
  - ZSA - Zonal Safety Analysis
  - PRA - Particular Risks Analysis
  - CMA - Common Mode Analysis
- **FTA/DD/MA** : Fault Tree Analysis / Dependence Diagram / Markov Analysis
- **FMEA** : Failure Modes and Effects Analysis
- **FMES** : Failure Modes and Effects Summary

PROCESS SAFETY – ARP4761



ARP 4761 – Vision très simplifiée

- **FHA** : Identification/caractérisation des Failure Conditions (FC)
- **PSSA** : Conformité préliminaire + Allocation objectifs
- **SSA** : Justification de conformité finale

- **FTA/DD/MA** : Evaluer les probabilités d'occurrence des FC

- **FMEA** : Identification exhaustive des défaillances
- **FMES** : Synthèse FMEA

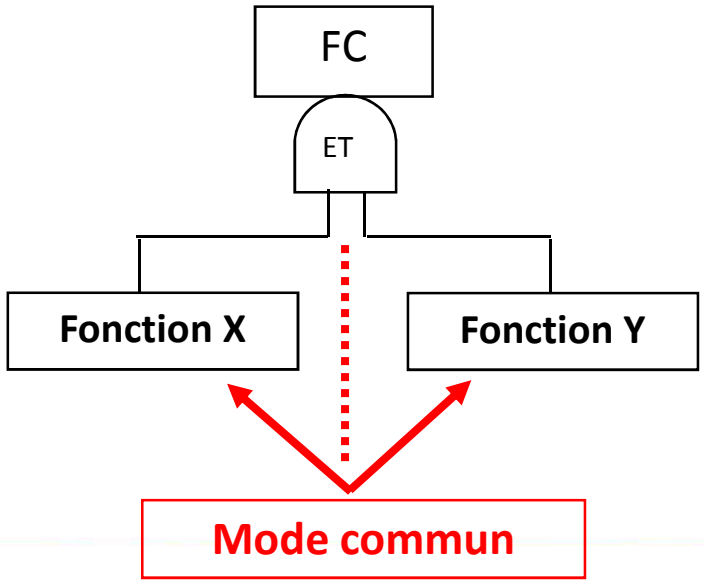
ARP 4761

➢**CCA** : « Maîtriser » l'impact des modes communs potentiels

ZSA - Zonal Safety Analysis

PRA - Particular Risks Analysis

CMA - Common Mode Analysis



ARP4761 **=> <u>Guidelines and Methods</u>** for conducting the safety assessment process on civil airborne systems and equipment

=> Présentation de l'approche globale de sécurité en réponse à la réglementation

L'approche globale de sécurité

Diverses Causes d'accident/d'incident:

- **Causes techniques (Hw/Sw) -> défaillance, erreurs de conception**
- **Risques internes A/C (Feu, UERF, pneu éclaté /accu., etc)**
- **Risques externes A/C (Impact d'oiseau, foudre, …)**
- **Environnement (Mauvais temps, vent, givre, circulation, …)**
- **Causes organisationnelles (procédures, formation,…)**
- **Facteurs humain (charge de travail, erreurs humaine,…)**

Ces causes peuvent être regroupées en 3 causes racines:

- **Défaillance aléatoire (Random failure)**

  Ex : Court circuit d'un composant → Fiabilité, FMEA …

- **Erreur (Error)**

  Erreur humaine → Analyse facteur Humain

  Erreur développement → Concept de DAL

- **Evénement (Event)**

  Evénement environnementaux/météo

  Flight Operation

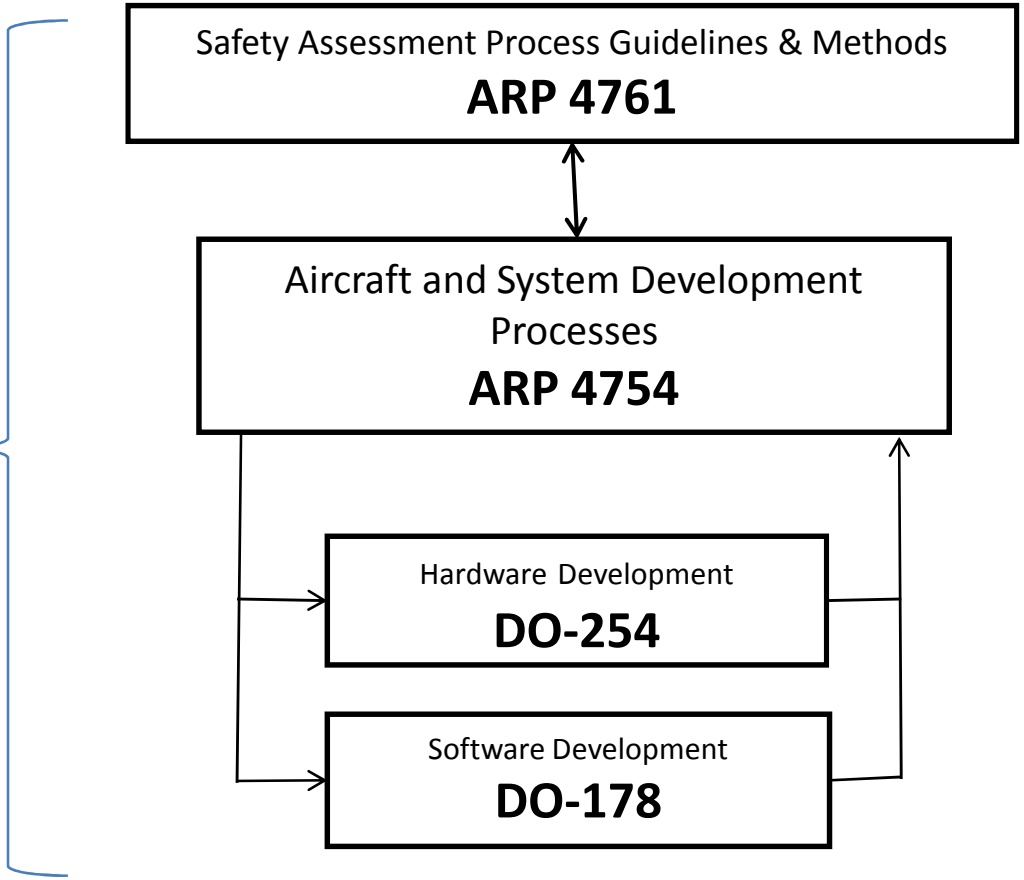
  Fire / smoke event

  Bird impact

  → Pris en compte dans les analyses FHA, SSA, FTA …

Point Clé du Process Safety

L'approche globale des analyses de sécurité



Point Clé du Process Safety

⇒Implication très forte lors des phases préliminaires (RFP, PR et PDR) :

⇒ Définition de l'architecture en conformité avec les exigences safety : DAL, Probabilités, Fail safe, SEU, MTBF …

⇒ Apporter un niveau de confiance élevé sur la future conformité de l'architecture

⇒ En phase RFP : Impact financier et sécurisation de la certification

Les points clés et les évolutions de la certification avionique

Atelier ARP4761

Partie B : Les évolutions vers l'ARP4761A

ARP4761 actuelle => publiée en 1996

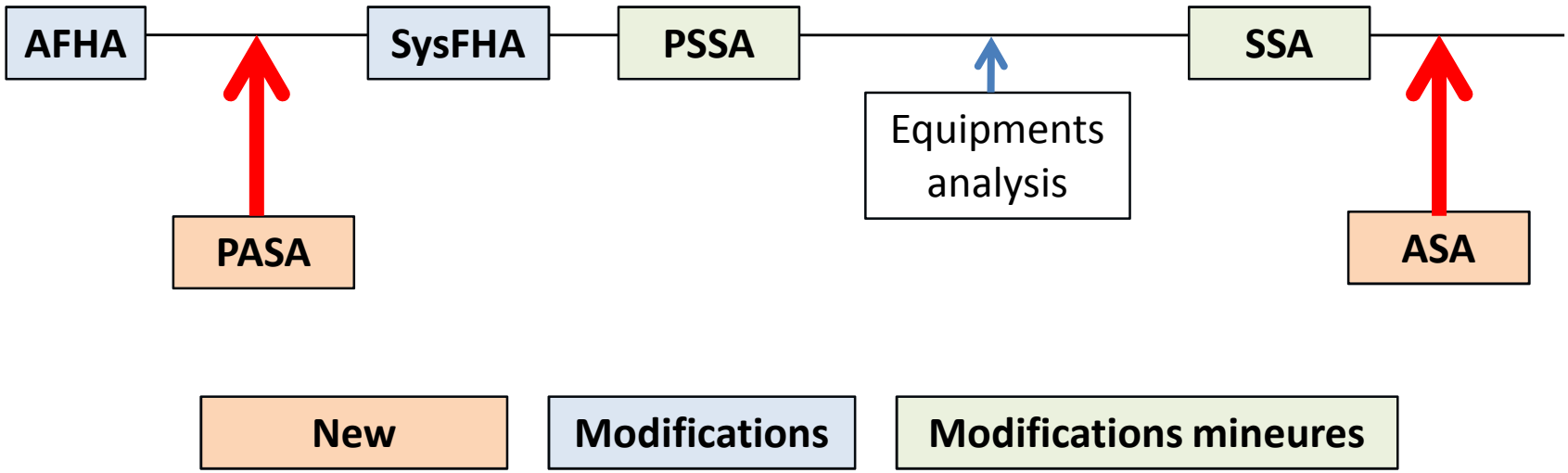
ARP4761a => prévue pour Avril 2015 avec prise en compte de :

- **Evolution des pratiques depuis 1996**
- **Compatibilité avec l'ARP4754a**
- **Meilleure description du process safety au niveau a/c**

<u>Evolution majeure</u> => Evolution du Process d'analyse safety

⇒ **Intégration des analyses**

- ⇒ **PASA : Preliminary Aircraft Safety Assessment**
- ⇒ **ASA : Aircraft Safety Assessment**



PASA et ASA => Aircraft Safety Assessment

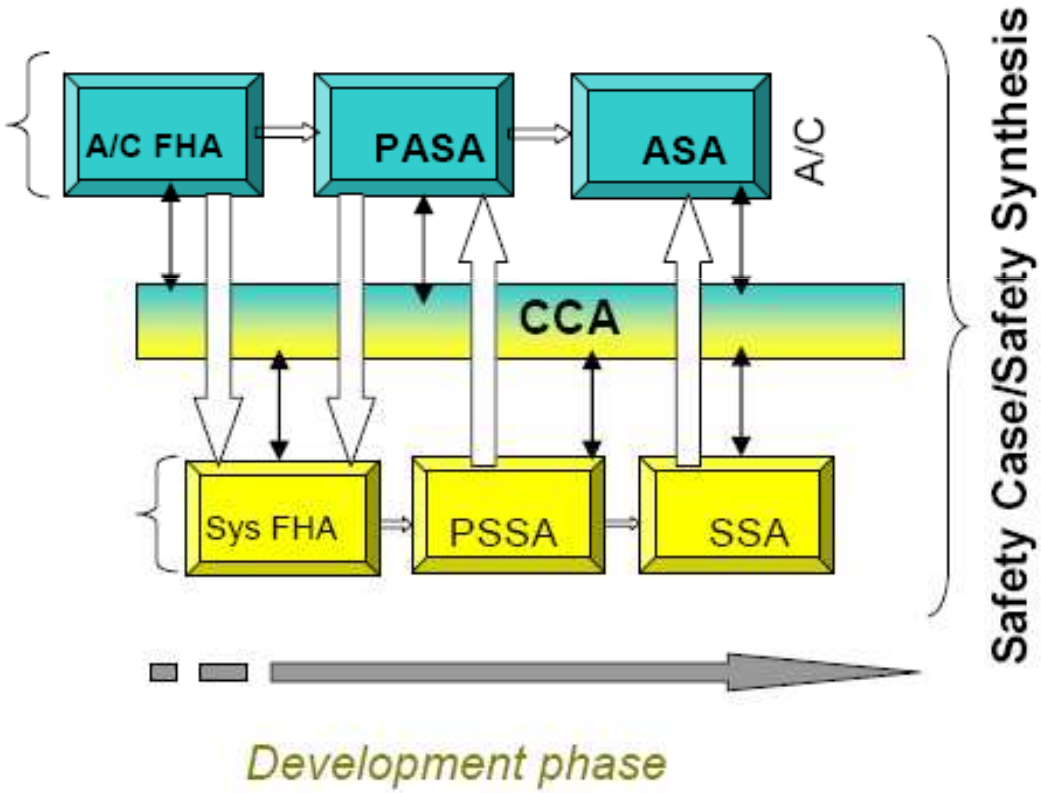
A partir des FCs identifiées par l'AFHA, la PASA à pour objectif :

1/ Identifier les FCs à traiter au niveau A/C :
FC multi-système (ex : Perte du freinage)
FC liée aux ressources avion (ex : Perte barre électrique)

2/ Analyser les architectures afin d'allouer les exigences safety aux différents systèmes impliqués (FDAL, indépendance, probabilité)

3/ Analyser les FCs (ASA)

PASA et ASA => Aircraft Safety Assessment



AFHA - SFHA

⇒ **Séparation des 2 méthodes d'analyse dans l'ARP4761a**

⇒ **Intégration des pratiques industrielles pour l'AFHA**

⇒ **Très peu de modification pour SFHA**

CMA => Adaptation de la checklist CMA dans l'ARP4761a

PSSA/SSA => Modifications mineures

Autres analyses (FTA/FMEA/FMES/MA) => Pas de changement

Model Based Safety Assessment (MBSA)

⇒ **Ajout dans l'ARP4761a d'une annexe relative au MBSA**

- **L'évaluation des performances « safety » par des méthodes de modélisation fonctionnelle et dysfonctionnelle sera reconnue au niveau de l'ARP4761a au même titre que les méthodes FTA/DD/MA**

- **Evolution possible des pratiques (et des outils) …**

<u>Projet AIR6219</u> - Aerospace Information Report :

Development of atmospheric neutron single event effects analysis for use in safety assessment

⇒ **Clarifier et formaliser les méthodes d'analyses SEU/MBU afin de les intégrer dans le process d'analyse safety (ARP4761a)**

- **A ce jour, difficulté de convergence sur ce sujet entre industriel et SAE/EUROCAE (cf CTIC-WG63)**
- **EASA/FAA => Certification Memo en préparation**

Merci pour votre attention

Pascal FABRE – EADS APSYS