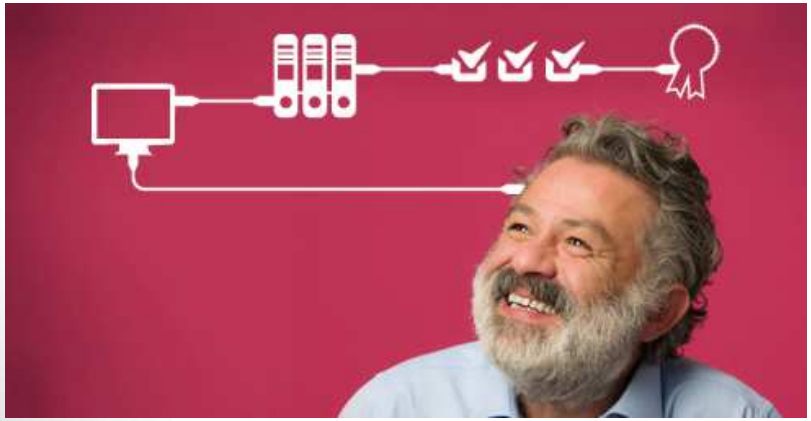
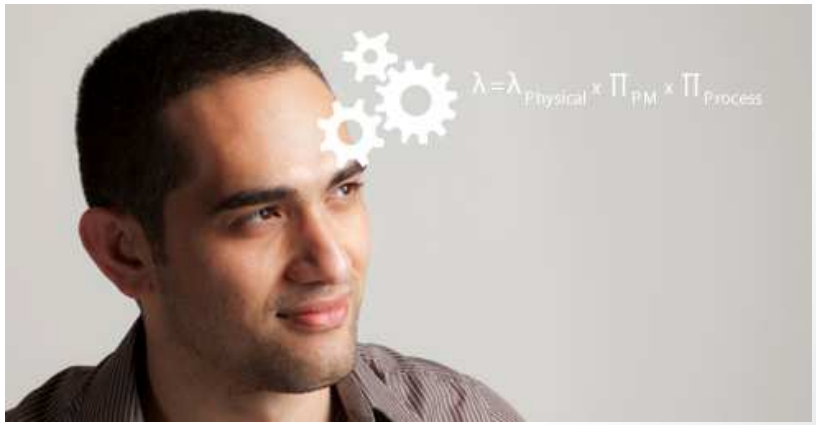
ERASM

EXPERTISE EN MAÎTRISE DES RISQUES

christophe.barnier@erasm.fr
julien.munerot@erasm.fr
Tel: 04 84 47 00 03





ERASM
EXPERTISE EN MAÎTRISE DES RISQUES

Développement et Intégration de systèmes critiques

ERASM
EXPERTISE EN MAÎTRISE DES RISQUES

Développement de systèmes critiques

- Un développement c'est:
  - La mise en œuvre de processus
  - Dans un cadre spécifique projet
  - Dans un contexte défini
    - Cahier des Charges / spécification client ou Exigences Clients
    - (Normes)

- Un développement de système critique c'est:
  - La mise en œuvre formalisée de processus
  - Dans un cadre spécifique projet
  - Dans un contexte défini
    - Cahier des Charges / spécification client ou Exigences Clients
    - Normes
    - Normes relatives aux systèmes critiques

se conformer à un référentiel

ERASM
EXPERTISE EN MAÎTRISE DES RISQUES

Développement de systèmes critiques

- Les différents Processus:
  - Processus de Développement
    - Processus de définition
    - Processus de conception
    - Processus de réalisation
    - Processus d'intégration
  - Processus Intégraux
    - Processus de Vérification
    - Processus de Gestion de configuration
    - Processus d'assurance qualité
  - Planification

ERASM
EXPERTISE EN MAÎTRISE DES RISQUES

Développement de systèmes critiques

- Comment avoir l'assurance que le développement est maîtrisé?
  - En demandant à l'industriel de décrire comment il va travailler
    - → rédaction de plans:
      - → Plan de développement
      - → Plan de Vérification
      - → Plan Qualité….
    - → Il ne faut pas recopier les normes mais dire ce que l'on va faire et faire ce que l'on a dit.
  - En structurant et formalisant l'ensemble du développement
    - Documents Types
    - Règles de conception
    - Règles de réalisation
  - En détaillant par un processus itératif les exigences que doit réaliser l'équipement

ERASM
EXPERTISE EN MAÎTRISE DES RISQUES

Développement de systèmes critiques

- Est-ce suffisant? Non, car l'erreur est humaine et le stress toujours présent
  - On va effectuer des tests sur ce qui est développé
    - Tests Fonctionnels
    - Tests Environnementaux
    - ….
- Est-ce suffisant? Non – car on a pu faire quelque chose de façon erronée
  - On va vérifier que tout ce que l'on devait faire a été fait correctement
    - Vérification des éléments techniques, documentaires, inspections...
- Est-ce suffisant? Non
  - Pour les niveaux de criticité important DAL A, DAL B on va demander que certaines taches de vérification soient effectuées une personne différente.

ERASM
EXPERTISE EN MAÎTRISE DES RISQUES

Développement de systèmes critiques

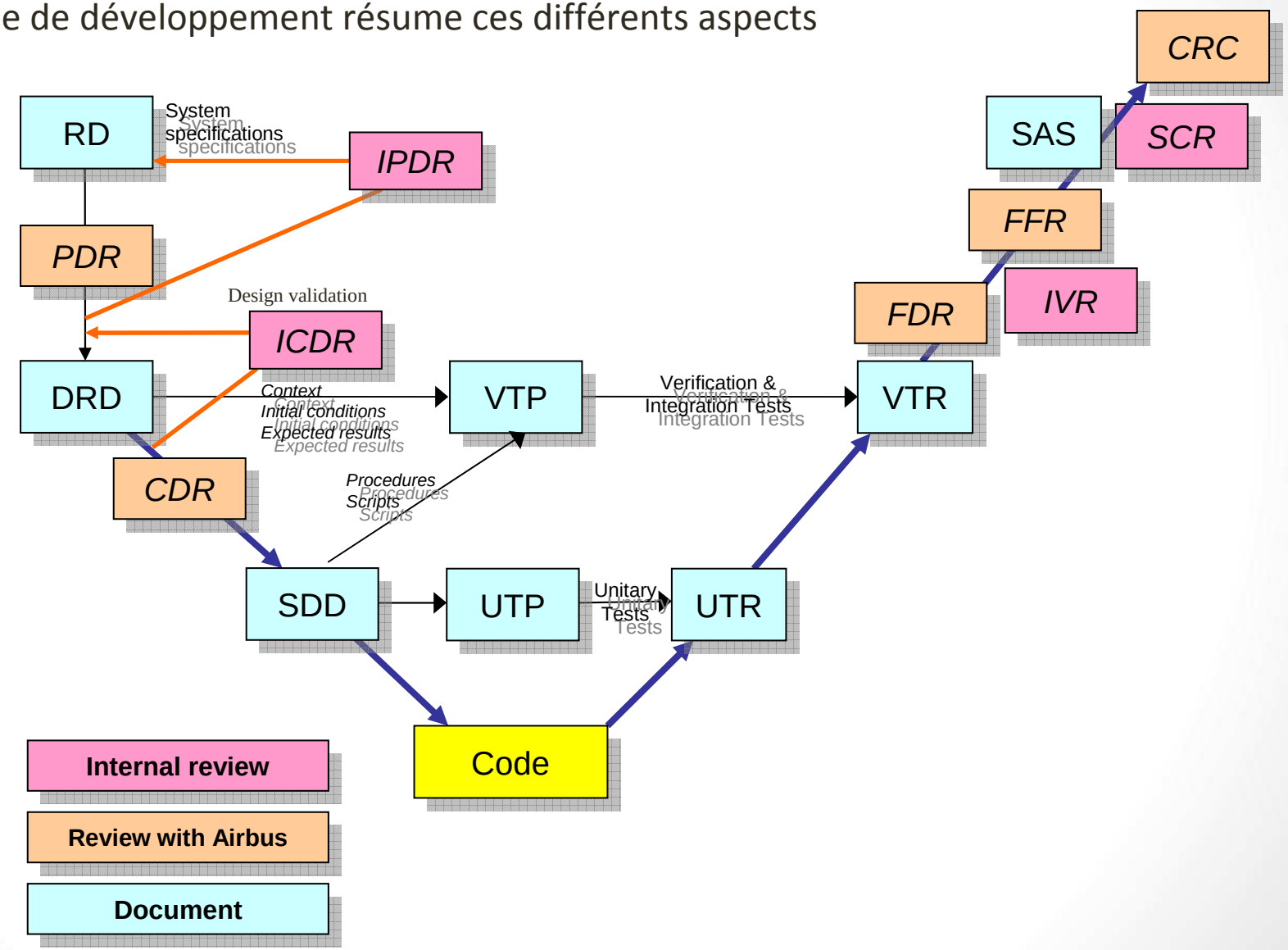
- La formalisation de la progression de l'avancement au cours du projet se fait par la tenue de revues:
  - Revue de planification
    S'assurer que les plan ont été correctement rédigé et qu'ils répondent aux besoins.
  - PDR : Preliminary Design Review
    S'assurer que la conception de l'objet peut répondre aux exigences. Est-ce faisable? sous quelles conditions?
  - CDR : Critical Design Review
    S'assurer que la conception de l'objet répond aux exigences?
  - QR : Qualification Review
    S'assurer que l'équipement répond aux contraintes d'environnements
  - FDR: First Article Design Review
  - FFR/CRC
  - Passage de jalons significatifs de la progression du développement

Revue Interne / Revue Externe !

ERASM
EXPERTISE EN MAÎTRISE DES RISQUES

Développement de systèmes critiques

Le Cycle de développement résume ces différents aspects



ERASM
EXPERTISE EN MAÎTRISE DES RISQUES

Développement de systèmes critiques

- Le Processus de sécurité repose sur les normes suivantes :
  - ARP4754: Certification Considerations for Highly-Integrated or Complex Aircraft Systems
  - ARP4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

- Le Processus de développement repose sur les normes suivantes :
  - DO178: Software considerations in airborne systems and equipment certification
  - DO254: Design assurance guidance for airborne electronic hardware

- Le Processus de qualification environnement repose sur :
  - DO-160: Environmental Conditions and Test Procedures

ERASM
EXPERTISE EN MAÎTRISE DES RISQUES

Développement de systèmes critiques

- Allocation du niveau de DAL

  - Résulte des études de sécurité amont
    - FHA: Functional Hazard Analysis
    - PSSA: Preliminary System Safety Assessment

  - Etudes de sécurité → les conséquences sur la sécurité du vol et la charge de travail des pilotes

  - Les études de sécurité se prononcent sur la perte ou le fonctionnement erronée de fonctions
    - Functional Failure Paths.

  - Elles aboutissent au classement de fonctions incorporant des constituants matériel et logiciel et donc au classement de ces matériels et logiciels

ERASM
EXPERTISE EN MAÎTRISE DES RISQUES

Développement de systèmes critiques

- La stratégie de sécurité (redondance,…) va déterminer le processus de développement
  - Development Assurance Level → DAL A/B/C/D/E
- Le développement écrit des exigences / La sécurité classe des fonctions auxquelles on associe des équipements et des logiciels
- Il existe une difficulté certaine à classer des exigences suivants un niveau de sécurité au travers des analyses de sécurité
- C'est la vérification qui va effectuer le travail de vérification de la consistance et de la complétude des exigences

  La vérification est un aspect très important dans l'aéronautique

ERASM
EXPERTISE EN MAÎTRISE DES RISQUES

L'intégration de systèmes critiques

ERASM
EXPERTISE EN MAÎTRISE DES RISQUES

Intégration de systèmes critiques

- L'intégration de systèmes critiques peut s'effectuer à différents niveaux.
  - Equipements / Equipements
  - Equipement (hardware) / logiciel
  - Logiciel / Logiciel

ERASM
EXPERTISE EN MAÎTRISE DES RISQUES

Intégration de systèmes critiques

- Les éléments descriptifs (documents/tests/…) doivent être présent pour les 2 constituants à intégrer.
- Il est nécessaire de développer un ensemble de vérification pour l'intégration des 2 constituants
  - Tests bas niveau/Test haut niveau/Qualification…
- Il est très délicat de faire reposer le développement d'un des constituants sur le retour d'expérience.
  - Combien de constituants fonctionnent?
  - Comment ils ont été testés?
  - Comment les erreurs sont analysées et corrigées?
  - …
- On va donc rechercher un équipement avec un dossier équivalent au niveau souhaité → pour les COTS on évoque « pack de certif »

ERASM
EXPERTISE EN MAÎTRISE DES RISQUES

Intégration de systèmes critiques

- L'intégration d'équipements de niveau critique:
  - Level A + Level A → Level A
  - Level A + Level B → Level B ou Level A sous certaines conditions de conception (cf. ARP4754 table 4)
  - Level A + Level C → Level C ou =< Level C sous certaines conditions de conception (cf. ARP4754 table 4)
  - Level B + Level D → Level D ou =< Level D <A sous certaines conditions de conception (cf. ARP4754 table 4)