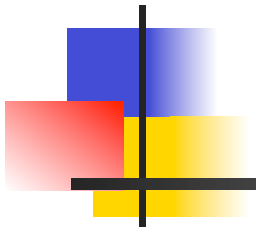
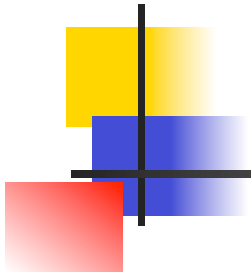


Integrated Modular Avionic

Laurent Pautet

Laurent.Pautet@enst.fr

Version 1.1



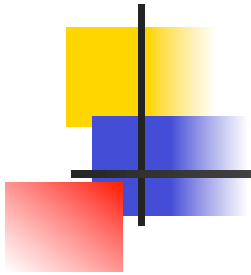
Systèmes avioniques

Ensemble de fonctions permettant à un aéronef civil ou militaire d'exécuter sa mission de vol.

- Cabine
- Cockpit
- Navigation
- Energie
- Moteurs
- Contrôle en vol
- Communications

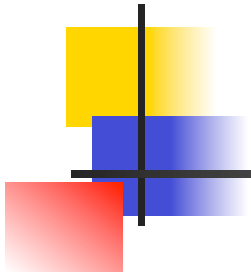
Fonctions de la cabine

- Smoke Detection Function
- Fire Protection System
- Cabin Oxygen
- Crew Oxygen
- Cabin intercommunication data system
- Cabin Communication systems
- Cockpit Door Locking System
- Doors and Slide Control System
- In flight entertainment



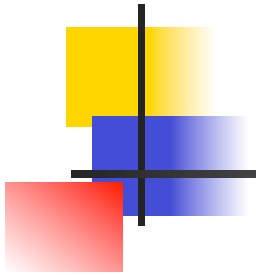
Fonctions du cockpit

- External And Taxiing Camera System
- Audio Control
- Flight Warnings System
- Control and Display System
- Electronic Centralized Aircraft Monitoring
- Head-Up Display
- Concentrator and Multiplexer for Video
- Digital Flight Data Recording System
- Tail Strike Indication System



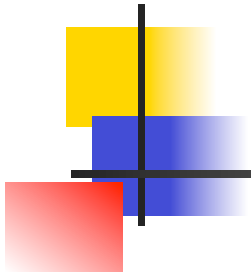
Fonctions pour l'énergie

- Electrical Load Management
- AC and DC Generation Control System
- Primary and Secondary Power Distribution Management
- Emergency Power Generation & Distribution
- Windows Heat Controller
- Exterior and Internal Lights (cockpit and cabin)
- Auxiliary Power Unit
- Circuit Breaker Monitoring
- Ice Detection
- Engine Control system



Fonctions de contrôle de vol

- Flight Management
- Flight Envelope
- Automatic Flight Guidance
- Weight and Balance Back-Up Computation
- Flight Controls unit
- Flight Control Data Concentrator

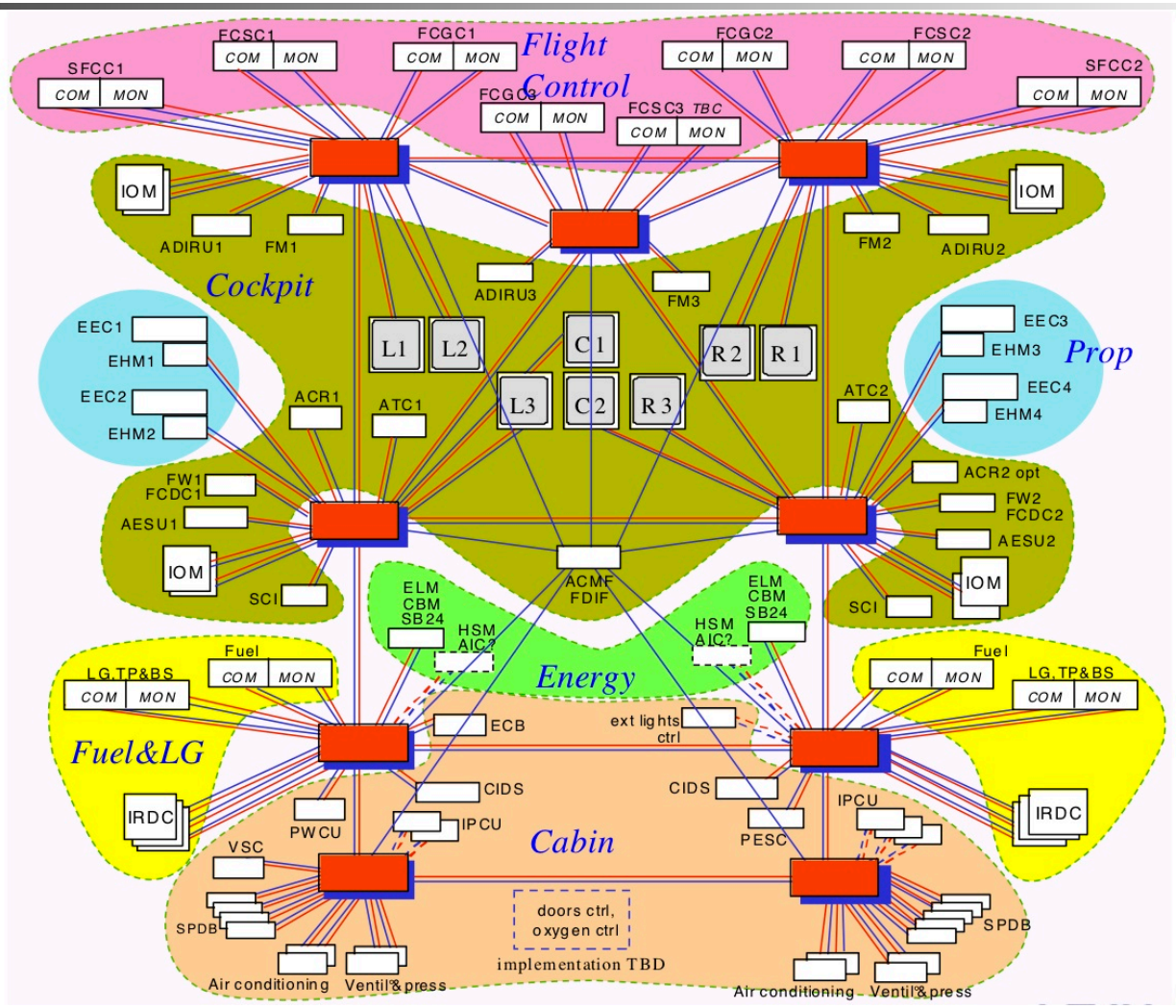


Fonctions de navigation

- Automatic Direction Finder
- VHF Omni directional Range (VOR)
- Distance Measuring Equipment
- Air Data Reference
- Multi Mode Receiver
- Onboard Airport Navigation System
- Radio Altimeter
- Weather Radar
- Traffic Collision Avoidance System
- Traffic Awareness and Warning System

Architectures avioniques

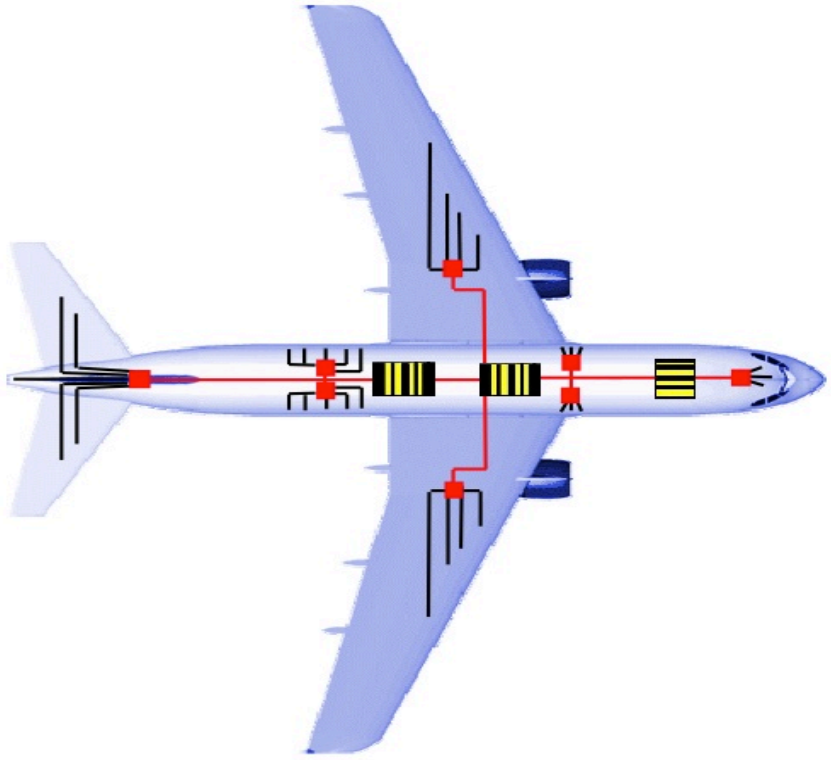
Avionics Data Communication Network

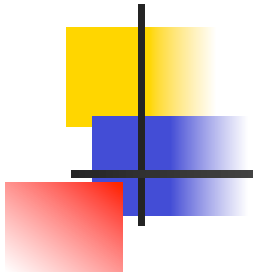


Architecture dite Fédérée

Federated Architecture

- Line Replaceable Unit (LRU)
  - une fonction,
  - un logiciel, un matériel,
  - un confinement,
  - un fournisseur
- Dédié à un avion particulier
- Assemblage des différents LRU au travers d'un réseau de câbles
- Acteurs et Capteurs près du calculateur
- +100 kms de câbles
- 20-30 calculateurs





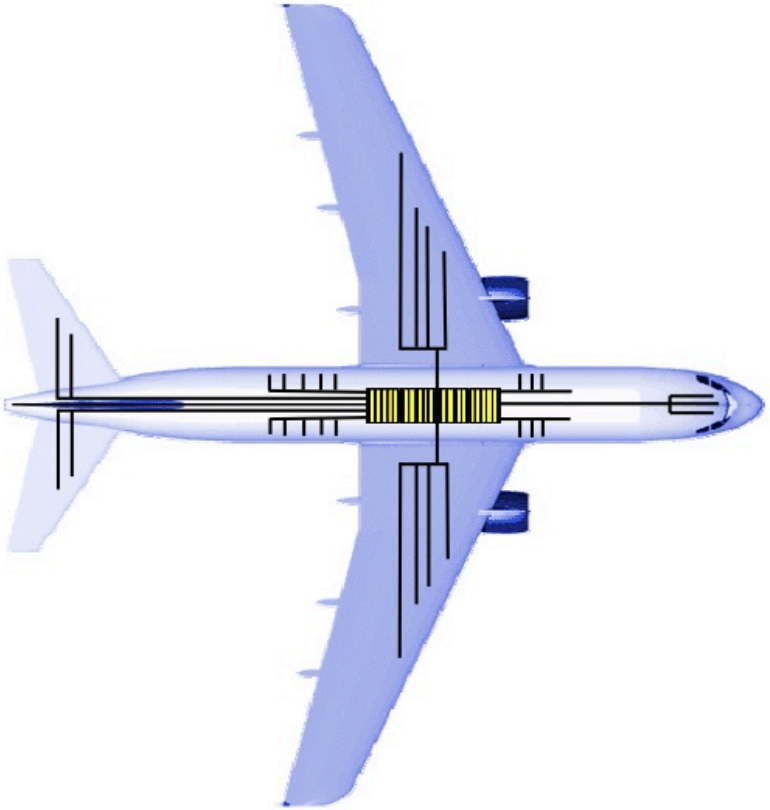
Objectifs
Integrated Modular Architecture

- Réduire l'impact du matériel
  - Lors de la conception du logiciel et de l'exécution sur la plate-forme
- Banaliser le matériel, réduire les coûts
  - Pour une utilisation de matériel grand public
- Réduire la dépendance vis à vis d'un fournisseur
- Améliorer la portabilité et la modularité
- Augmenter le nombre de fonctions
  - Lors des 10 ans de conception de l'avion, les besoins évoluent
- Réduire le poids, le volume et l'énergie
- Réduire les coûts de conception et de certification
- Réduire les coûts de maintenance et d'évolution au sol

Architecture dite Intégrée

Integrated Modular Architecture

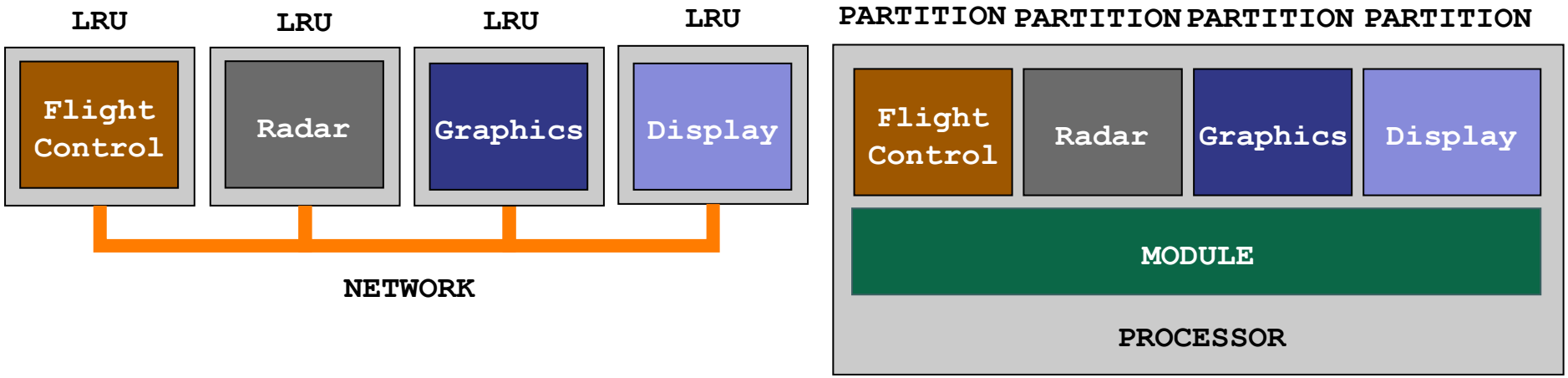
- Plusieurs fonctions, un calculateur
- Le fournisseur produit une fonction
- L'intégrateur alloue une partie des ressources au fournisseur pour cette fonction
- 6 à 8 calculateurs banalisés
- Moindre en poids, volume et énergie
- Ajout de nouvelles fonctions ainsi facilitée



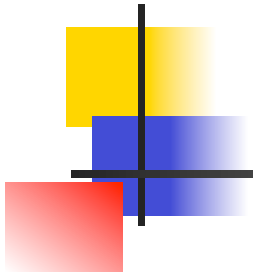
Mises en œuvre classiques

- Architecture Fédérée
- Unité : LRU
- Intégration: réseau

- Architecture Intégrée
- Unité : module
- Intégration: partition



Fédérée vs Intégrée



Architecture Fédérée

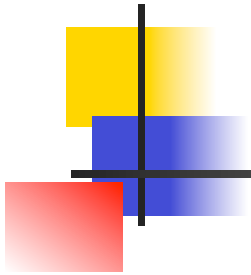
- Une fonction, un matériel
- Méthodologie bien maitrisée
- Conception assez facile
- Certification assez facile

- Forte consommation en volume/poids/énergie
  - Matériels et câbles
- Bande passante limitée
  - 30-40 fonctions max par bus
- Faible réutilisation / portabilité
- Lié aux fournisseurs

Architecture Intégrée

- Plusieurs fonctions, un matériel
- Moindre consommation en volume/poids/énergie
- Forte réutilisation
- Forte portabilité
- Ajout facilité de fonctions

- Méthodologie moins maitrisée
  - Les fonctions communiquant fortement sur un même module
- Intégration plus complexe
- Certification plus complexe

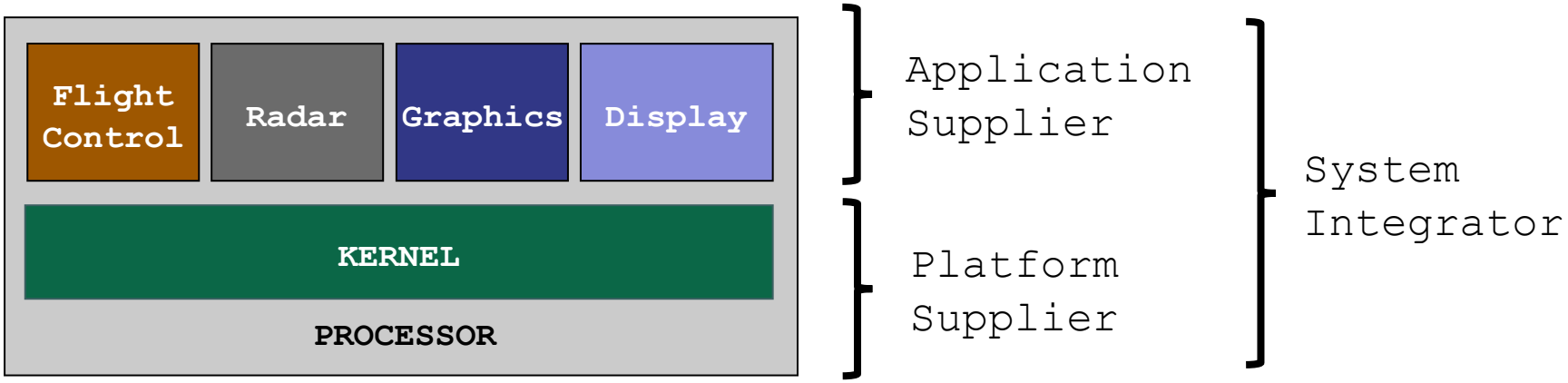


Processus

- Un système avionique doit procurer une bonne fiabilité et donc le respect d'un ensemble d'exigences
- Une agence de certification s'assure du respect de standards garantissant le respect d'exigences comme FAA (USA) ou EASA (EU)
- RTCA produit des standards pour la certification
  - DO-297 pour la gestion du cycle de développement
  - DO-178 pour les logiciels
  - DO-254 pour les matériels
  - DO-278 pour la gestion du trafic aérien

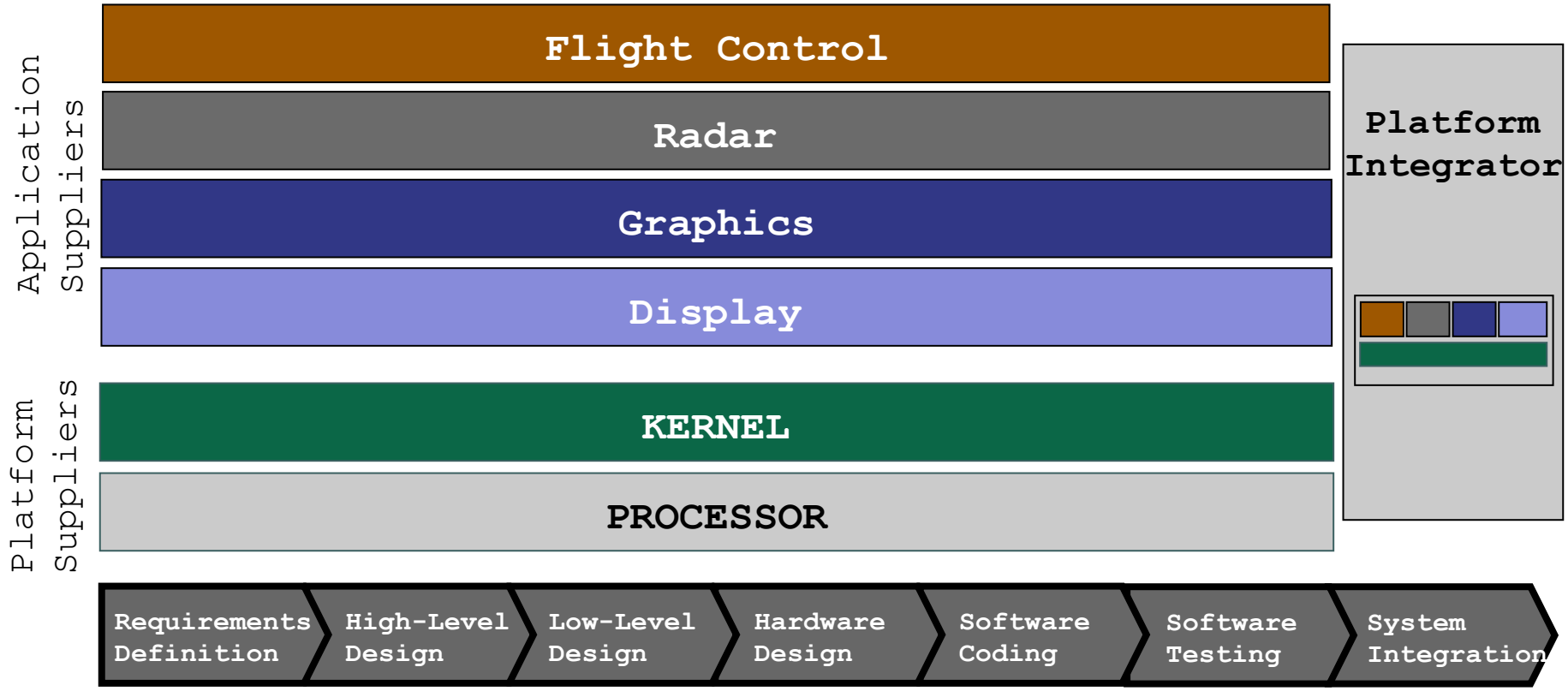
Standard DO-297 (1/2)

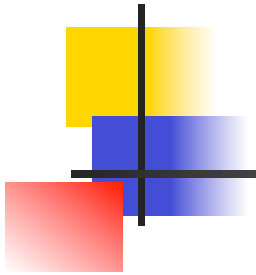
- Développement organisé autour de 3 rôles
  - Platform Supplier (matériel + logiciel de base comme noyau)
  - Application Supplier (logiciel des fonctions)
  - System Integrator



Standard DO-297 (2/2)

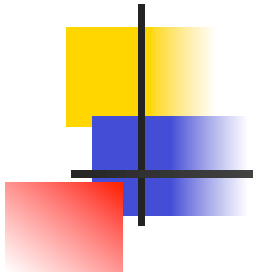
- Conception et certification parallèles et indépendantes





DO-178

- DO-178 propose des règles pour assurer la fiabilité du logiciel (fonctions, noyau, intégration, …)
- Une fonction se voit attribuer un niveau de criticité en fonction de la gravité de sa défaillance
- Le niveau de criticité détermine la probabilité acceptable d'occurrences de fautes (en nombre par heure)
- Il détermine les règles de développement à appliquer en fonction du niveau de criticité
- Ces règles portent sur l'ensemble du développement (planning, requirement, design, coding, testing…)
- Comment certifier le code sans vérification formelle ?

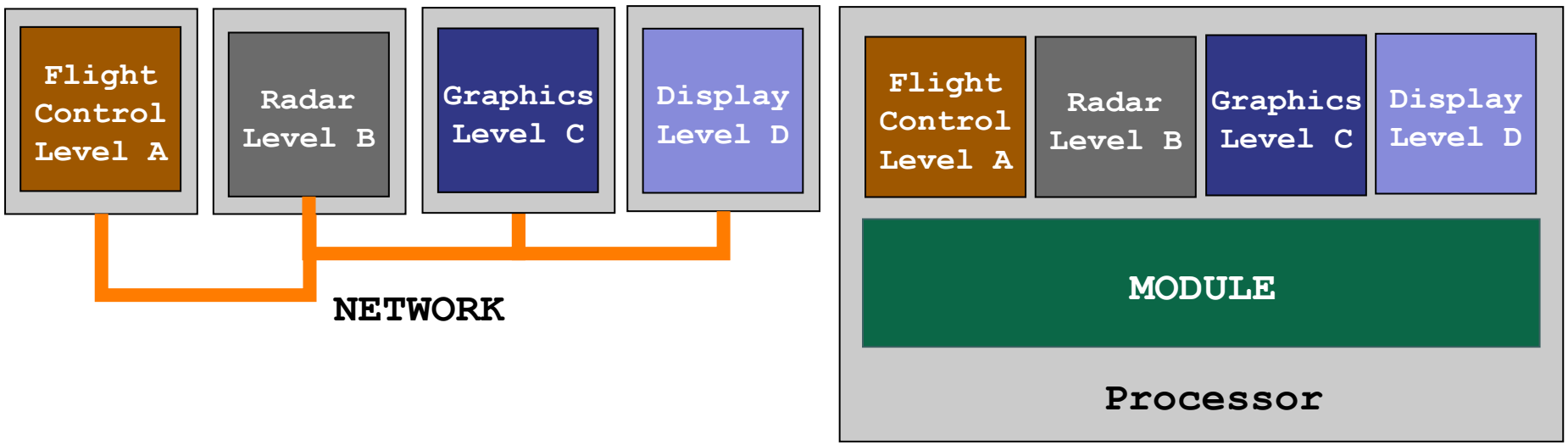


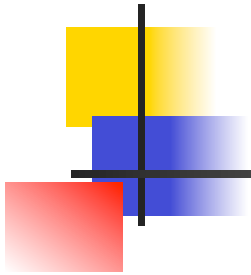
Niveaux de criticité

Niveau de criticité	Règles à vérifier	Pourcentage de fonctions	Conséquence	Occurrences maximum
E	0	5%	Aucune	
D	28	10%	Mineure	10^{-3}/h
C	57	20%	Majeure	10^{-5}/h
B	65	30%	Dangereuse	10^{-7}/h
A	66	35%	Catastrophique	10^{-9}/h

Architectures et Criticités

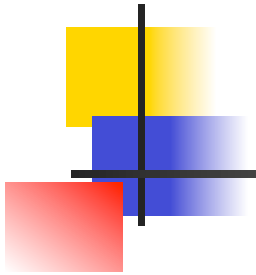
- Architecture Fédérée
- Architecture Intégrée
  - Différents niveaux de criticité sur un même calculateur





Problématiques

- Assurer le confinement des erreurs que l'architecture soit fédérée ou intégrée
- Assurer qu'une fonction de criticité donnée ne perturbe pas une fonction de criticité supérieure
- Dès lors, dans le cas de l'architecture intégrée
  - Isoler les fonctions spatialement (mémoire) et temporellement (CPU)
  - Interdire à une fonction de criticité donnée de transmettre (IO) à une fonction de criticité supérieure (éventuellement sur le même calculateur)

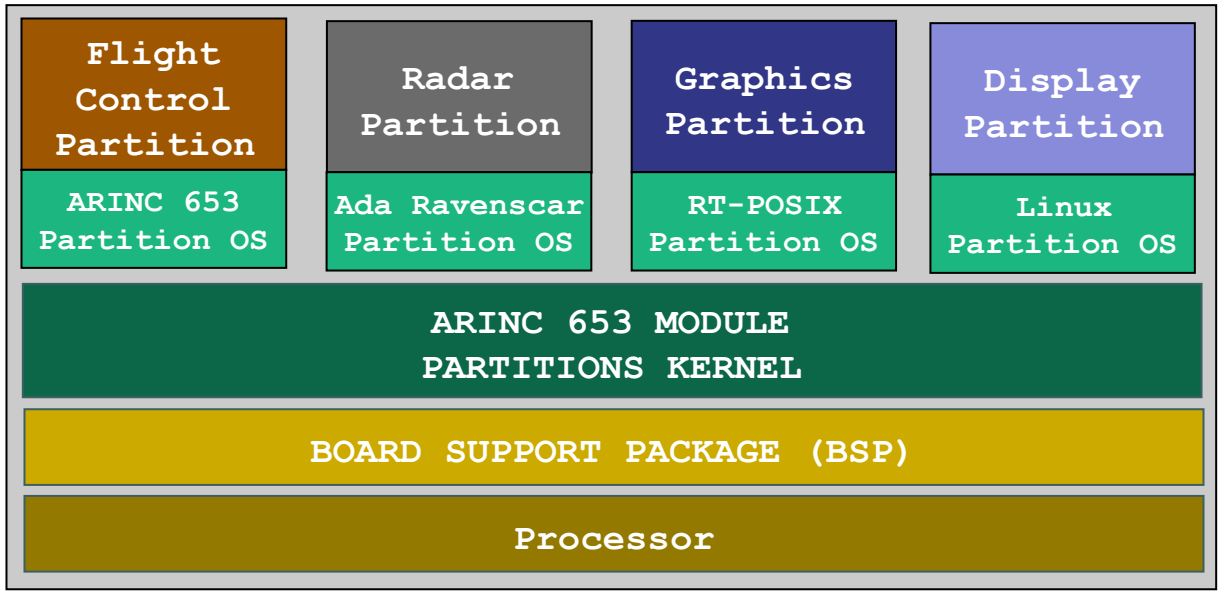


ARINC 653

- ARINC 653 fournit une spécification pour réaliser une architecture intégrée au dessus d'un noyau sur un processeur
- Le noyau ARINC 653 est certifié de sorte que si les fonctions sont certifiées (indépendamment), l'ensemble devient certifié
- Le noyau ARINC 653 doit assurer l'isolation spatiale et temporelle et garantir les contraintes de criticités lors des communications
- APEX, API d'ARINC 653, fournit 7 services : Partition, Process, Time, Memory, Inter et Intra Partition Communication, Health Monitor
- ARINC 653 permet de s'affranchir de dépendances sur le matériel

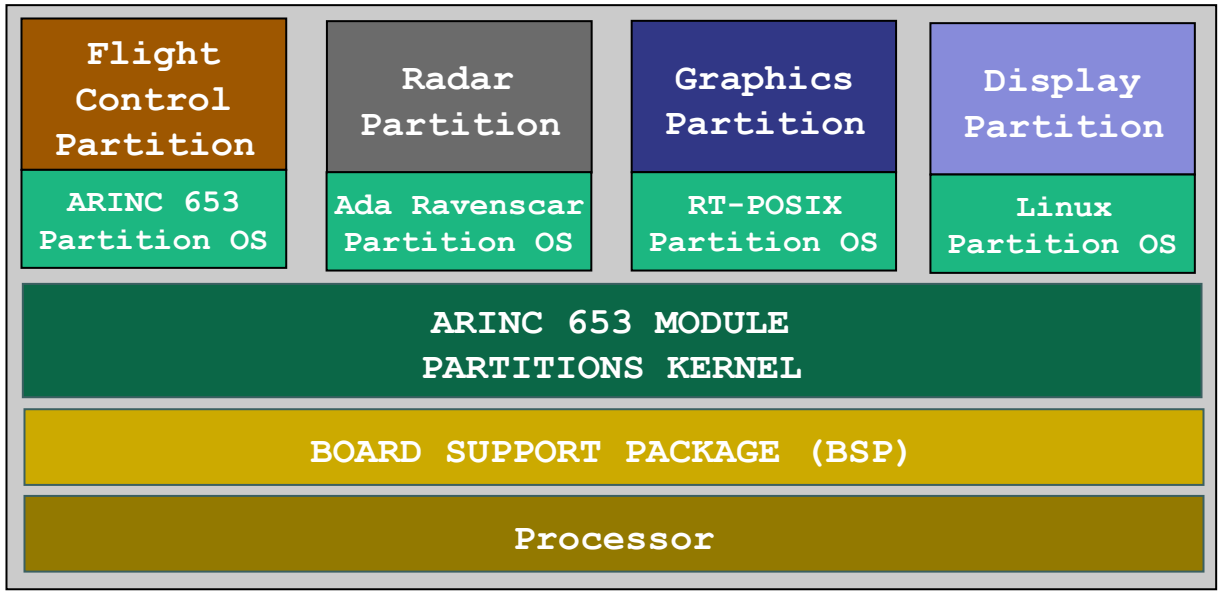
ARINC 653 – APEX
Partition

- L'isolation spatiale et temporelle est assurée en préallouant
  - Zones de calcul disjointes de taille fixe dont le noyau prévient tout débordement
  - Zones de mémoire de taille fixe qu'un mécanisme de MMU protège
- Un exécutif au sein d'une partition peut fournir du multi-tâches
- Un fichier XML permet au démarrage de configurer ces zones

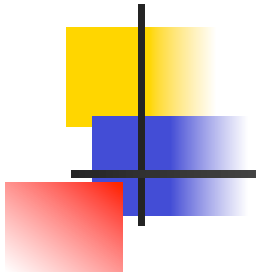


ARINC 653 – APEX
Partition

- L'isolation spatiale et temporelle est assurée en préallouant
  - Zones de calcul disjointes de taille fixe dont le noyau prévient tout débordement
  - Zones de mémoire de taille fixe qu'un mécanisme de MMU protège
- Un exécutif au sein d'une partition peut fournir du multi-tâches
- Un fichier XML permet au démarrage de configurer ces zones



ARINC 653 – APEX
Isolation temporelle



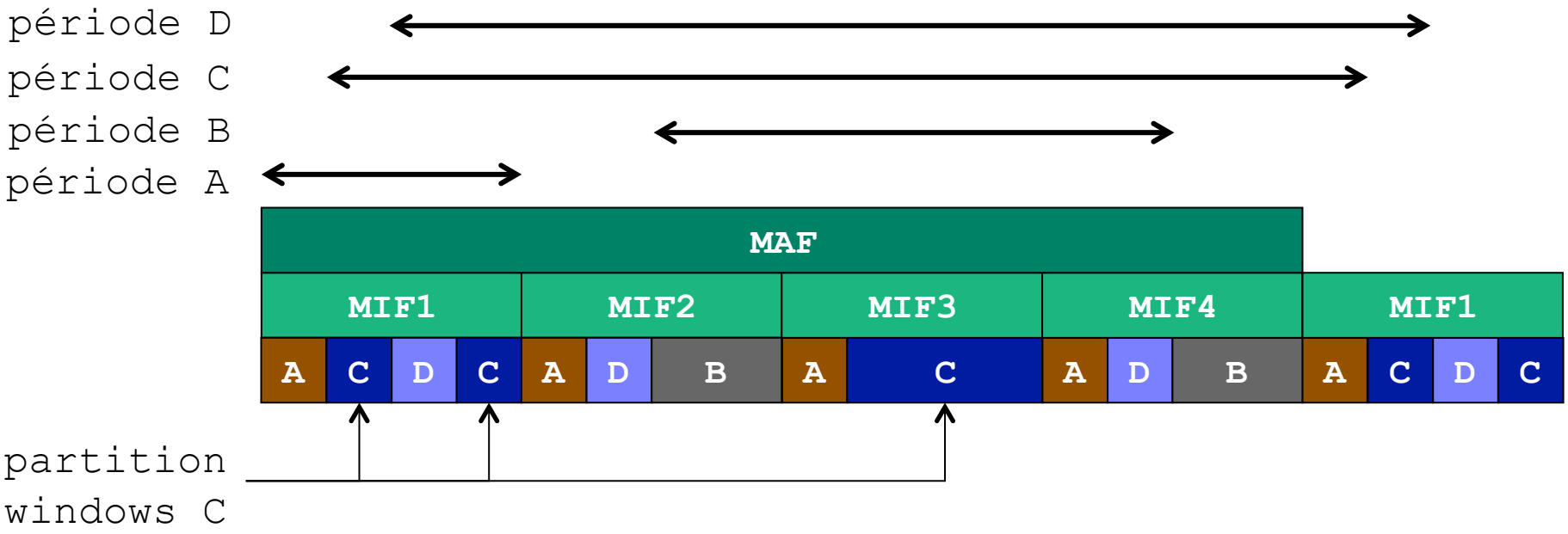
- Le temps se découpe en MAjor Frame périodiques (MAF)
  - Souvent le PPCM de périodes de partitions harmoniques
- Une MAF se découpe en plusieurs MInor Frames (MIF)
  - Souvent le PGCD des périodes de partitions harmoniques
- Sur sa période chaque partition se décompose en plusieurs tranches de temps appelées Partition Windows
- Chaque MIF se compose de Partition Windows de plusieurs partitions
- L'intégrateur attribue les Partition Windows de sorte que chaque partition s'exécute en respectant son échéance
- Le noyau vérifie que chaque partition ne déborde pas temporellement de la Partition Window allouée

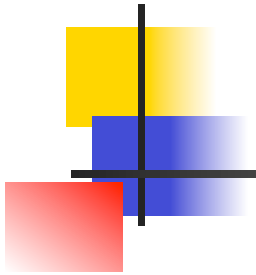
ARINC 653 – APEX

Isolation temporelle

Partition	A	B	C	D
Période	10ms	20ms	40ms	40ms

MAF	MIF
40ms	10ms

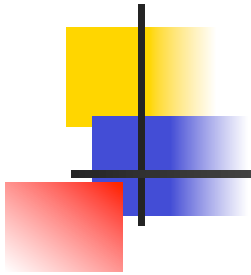




ARINC 653 – APEX
Isolation spatiale

- Chaque partition dispose d'une zone mémoire protégée par le noyau lorsque la partition n'est pas active
- Le noyau utilise les mécanismes fournis par le Memory Management Unit disponible dans le processeur
- Une partition active ne peut donc pas écrire dans les zones les autres partitions
- Les zones de mémoire pour les communications entre partitions sont également protégées par le noyau

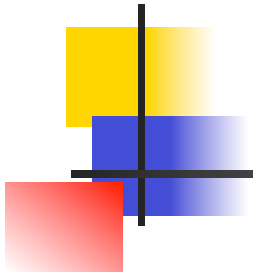
ARINC 653 – APEX
Process et Temps



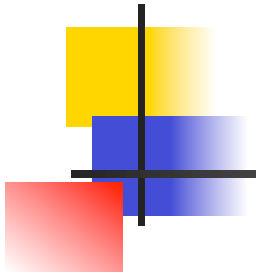
- Se rapproche fortement d'un thread
- S'exécute dans une partition (au moins un processs)
- Dispose d'attributs tels que priorité, période, capacité …
- Respecte un ordonnancement préemptif à priorité fixe

- Un process d'initialisation démarre la partition
- Un process peut attendre pendant un temps donné
- Un process peut attendre jusqu'à sa prochaine activation
- Un process peut obtenir l'heure courante

ARINC 653 – APEX
Sémaphore et Evénement

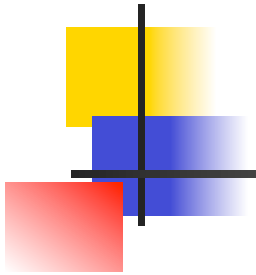


- Deux mécanismes sont disponibles pour synchroniser les process d'une même partition entre eux :
- Semaphore permet d'obtenir le mécanisme classique de sémaphore. Les politiques de PIP et PCP sont disponibles.
- Event permet d'attendre qu'un événement soit vrai et de bloquer dans le cas contraire.



ARINC 653 – APEX
Communication intra-partition

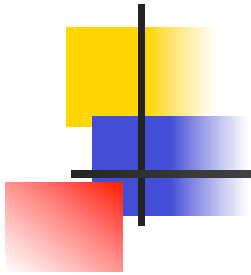
- Deux mécanismes sont disponibles pour communiquer entre process d'une même partition :
- Blackboard parmet d'écraser la valeur précédente d'une donnée par une nouvelle valeur et de la lire autant de fois que nécessaire. Il dispose d'une donnée initiale.
- Buffer permet également d'écrire plusieurs valeurs d'une donnée mais ne les écrase et les conserve dans une zone de mémoire suivant un ordre soit FIFO soit par priorité. Il permet également de les lire en bloquant si aucune valeur n'est disponible.



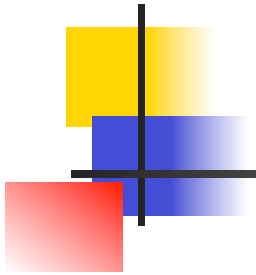
ARINC 653 – APEX
Communication inter-partition

- Deux mécanismes sont disponibles pour communiquer entre partitions d'un même calculateur. Ces mécanismes sont similaires à Blackboard et Buffer.
- Sampling port permet d'écraser la valeur précédente d'une donnée par une nouvelle valeur et de la lire autant de fois que nécessaire. Il dispose d'une donnée initiale.
- Queuing port permet également d'écrire plusieurs valeurs d'une donnée mais ne les écrase et les conserve dans une zone de mémoire suivant un ordre soit FIFO soit par priorité. Il permet également de les lire en bloquant si aucune valeur n'est disponible.

ARINC 653 – APEX
Health Monitor

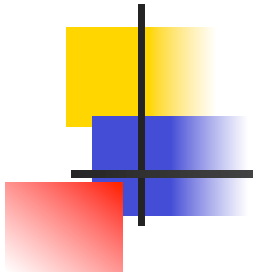


- Le Health Monitoring permet de traiter les erreurs :
  - Identifie et signale les erreurs
  - Associe des traitements aux erreurs
- … de manière hiérarchique :
  - Au niveau processus pour l'Application Supplier
  - Au niveau partition pour le System Integrator
  - Au niveau module pour le Platform Supplier
- Le système doit garantir qu'une erreur levée à un niveau (partition) sera traitée à ce niveau ou plus bas (partition ou module)
- Le traitement peut impliquer un redémarrage
  - Cold restart (code et données sont réalloués et réinitialisés)
  - Warm restart (opération identique à Cold Restart mais moins complète)



ARINC 664
AFDX – réseau pour ARINC 653

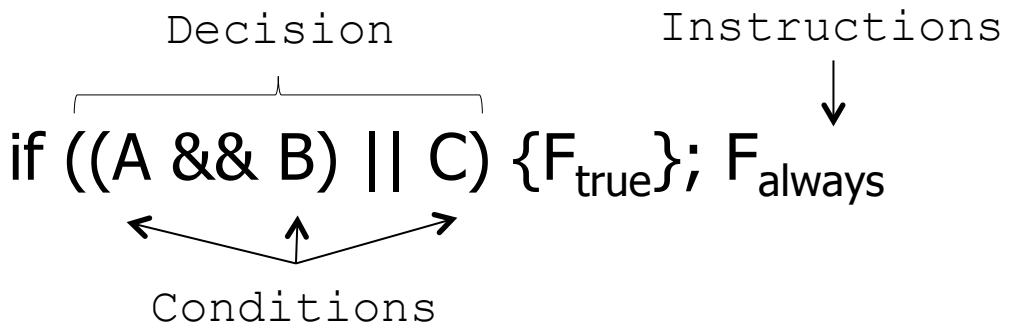
- ARINC 664 définit des moyens déterministes de communication (ARINC 653 pour le réseau)
- L'AFDX (Avionic Full DupleX) s'appuie sur
  - du matériel classique souvent redondant
  - les principes d'un réseau commuté de type Ethernet
  - la réservation de bande passante
- Ainsi des virtual links contrôlent émissions et réceptions afin d'éviter collisions et réémissions
- L'AFDX s'appuie sur des standards connus et profite du caractère fermé du système pour garantir des bornes sur les latences



Couverture de code

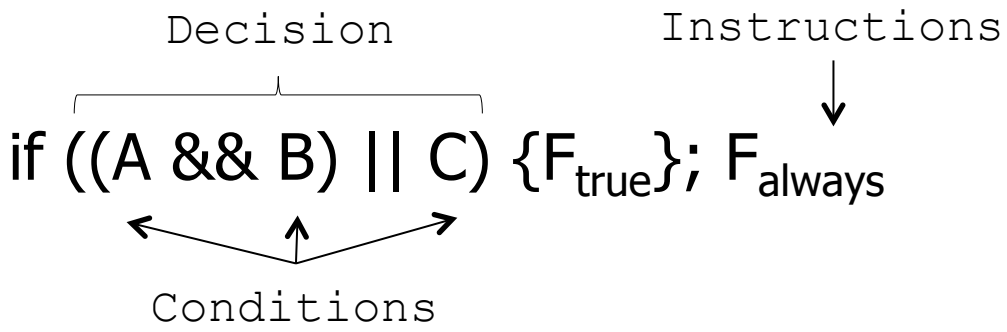
- DO-178 demande que suffisamment de tests soient appliqués pour parcourir toutes les zones de code : il s'agit de couverture de code
- La couverture de code peut aller plus ou moins loin
- Il existe 3 sortes d'exigence de couverture
  - Modified Condition/Decision Coverage pour niveau A
  - Decision Coverage pour niveau B
  - Statement Coverage pour niveau C
  - Les niveaux D et E ne sont pas concernés

Couverture de code
Statement Coverage – Decision Coverage



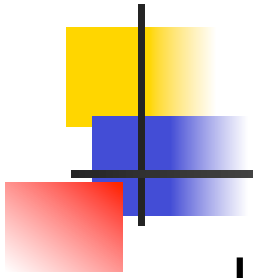
- Statement Coverage: exécuter au moins une fois toutes les instructions du code
  - Exécuter F_{true}+F_{always} ; 1 test avec la décision valant true
- Decision Coverage: passer au moins une fois dans chaque branche de décision
  - Exécuter F_{true}+F_{always} et F_{always} seule ; 2 tests avec la décision valant true et false

Couverture de code
Modified Condition / Decision Coverage



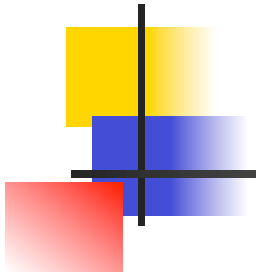
- MC/DC: Decision Coverage + chaque condition influe indépendamment sur le résultat de la décision
- Pour N conditions, il faut au moins N+1 tests. Pour cette décision, une possible campagne de tests :

A	B	C	D
T	T	F	T
F	T	F	F
F	T	T	T
T	F	F	F



Couverture de code
Niveau de criticité

- Le niveau de criticité implique le degré de couverture
  - Niveau A : Modified Condition / Decision Coverage
  - Niveau B : Decision Coverage
  - Niveau C : Statement Coverage
- La couverture de code source n'est pas équivalente à la couverture de code objet
  - Comme on ne vérifie pas l'indépendance des conditions, la couverture de code objet se rapproche de Decision Coverage



Conclusions
Importance et Généralisation

- Rien n'empêche d'appliquer l'IMA au ferroviaire, à l'automobile, à la radio logicielle, etc.
- Ces industries ont prétendu que l'approche avionique n'était pas transposable ailleurs
  - Nombre réduit d'avions très coûteux
  - Nombre important de fonctions d'un avion
  - Exigences critiques d'un avion (on ne peut pas s'arrêter)
- Les différences tendent à s'estomper de sorte que d'autres industries s'intéressent à l'IMA
- Les standards du ferroviaire (CENELEC 50128), de l'automobile (ISO26262) ou du spatial (ECSS-E40A) vont tendre à se rapprocher de DO-178 et de l'IMA.