15 Février 2008

Presenté par

Gérard LADIER

Head of Software Methods/Quality Section

Avionics & Simulation Products

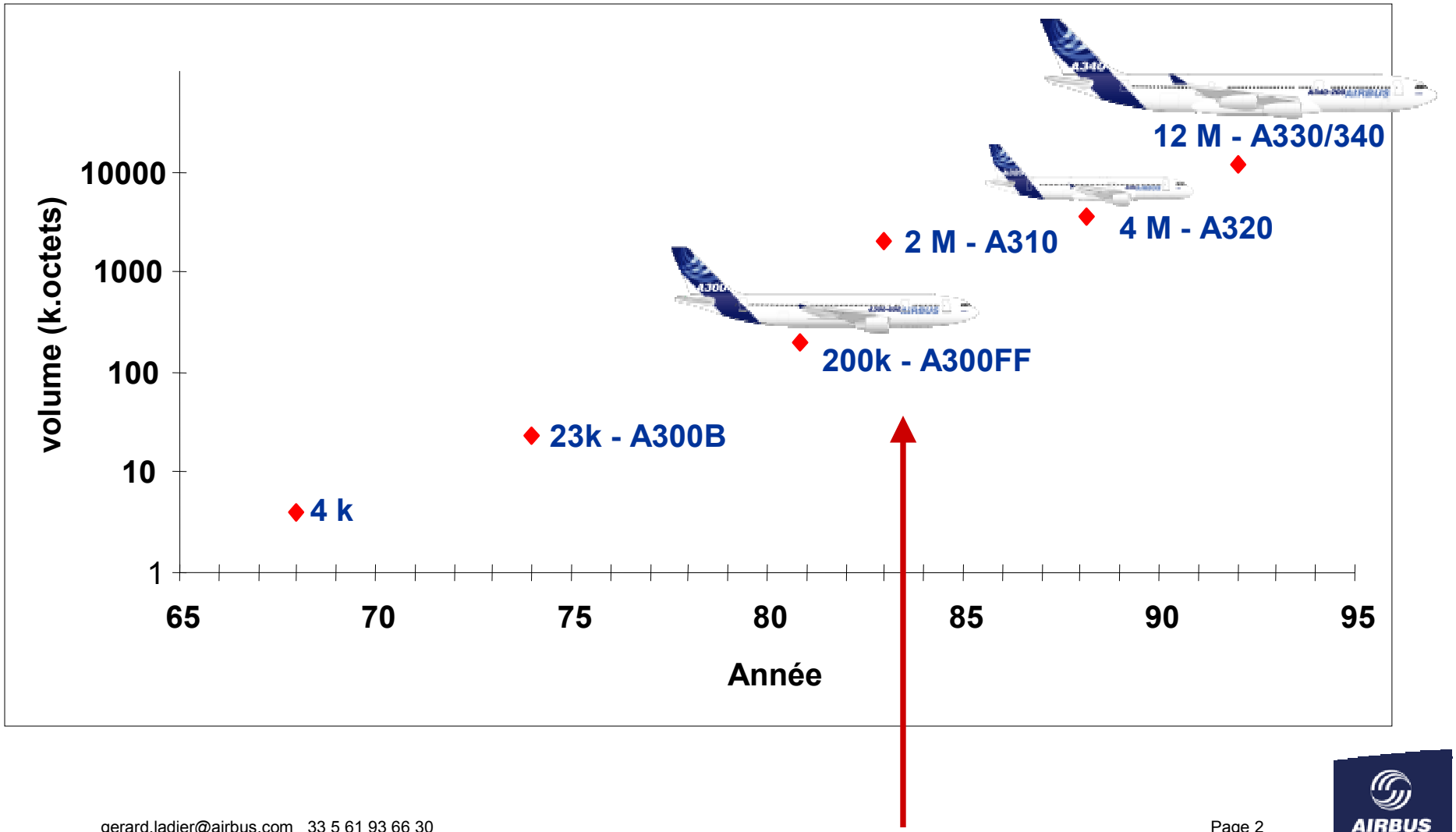
Airbus France

La certification, ou comment faire confiance au logiciel pour l'avionique critique

AIRBUS

Les débuts du logiciel embarqué

- Première utilisation à grande échelle du logiciel pour l'avionique : début des années 80



gerard.ladier@airbus.com 33 5 61 93 66 30

Les débuts du logiciel embarqué

- A cette époque, “logiciel” était quasiment synonyme de “bug” … :

Les débuts du logiciel embarqué

- A cette époque, “logiciel” était quasiment synonyme de “bug” … :

ÉQUIPEMENTS AVIONIQUE

LA COMPLEXITE DES LOGICIELS EMBARQUES MENACE LA SECURITE DES AVIONS

Nombre d'incidents survenus récemment à des Boeing 747 sont imputés à des erreurs logicielles. Des problèmes analogues dans la mise au point des C-17 et F-14D remettent une nouvelle fois en question le rôle qu'on attribue aux calculateurs embarqués.

British Airways signale 10 incidents d'origine logicielle survenus notamment sur ses 747.

PAR JEAN DUPONT

RESEARCH PAPER

CAD: COMPUTER-AIDED DISASTER

PETER MELLOR
Centre for Software Reliability, C
Northampton Square, London EC
e-mail: p.mellor@csr.city.ac.uk

Computers can kill [or have other undesirable effects]. This paper describes a number of recent disasters in which computers have been wholly or partly to blame, including the Therac-25, which overdoses of radiation to its patients,

The great disk initialization disast
In 1986 a consultant had volunte
known human rights organizatio
computer system in its head office
had just been delivered, and the
accounting package had been
disk by the software house whic
software. The office man
how to format a diskette.
his experience in using
, and approached the
The sequence of events
resultant departed after
reinstalling all the so
on's personal experienc

NEWS

COMPUTER WEEKLY AUGUST 13 1992

Boeing opposes tests on safety-critical software

Tony Collins

US AIRCRAFT manufacturer Boeing wants to dilute an already weakened aviation standard on the testing of safety-critical and other software.

In a letter to a standards-setting committee it urges

come into operation next year.

But Boeing says the checks would "go well beyond" the existing US Federal Aviation Regulations which cover software inspections and tests. The manufacturer says it is "opposed to the use of

turer could contest a rejection of its software. Also, Boeing says spot-checks by certification authorities would undermine the tests carried by its employees. "Validation of the life-cycle processes should be left to the applicant (Boeing) rather than the certification author-

nical Concepts for Aviation in Seattle, US, has already rejected calls from the British Computer Society for the mandatory independent testing of all safety-critical software used in computerised aircraft such as the Airbus A320.

However, the committee has included a provision in

=> l’industrie mondiale la plus réglementée

=> l’industrie mondiale la plus réglementée

- Dès le début : 1ère ébauche de règlement international à la conférence de Paris en 1910

=> l'industrie mondiale la plus réglementée

- Dès le début : 1ère ébauche de règlement international à la conférence de Paris en 1910
- Tout est réglementé :
  - Conception, fabrication, commercialisation, stockage, propriété, maintenance, opération, réparation des produits avioniques
  - Transport des personnes et des biens et tout autre travail aérien
  - Vols de loisir
  - Construction amateur
  - Construction, propriété, opération et utilisation des aéroports, communication aéronautique et installation de navigation, services de lutte contre l'incendie, de secours, d'approvisionnement en carburant
  - Travail des pilotes, personnels de cabine, dispatchers, I
  - Utilisation de l'espace aérien
  - Utilisation du terrain autour des aéroports
  - Bruit et émissions
  - Santé des population
  - Sécurité
  - Charges et droits
  - Fréquence et capacité des services aériens
  - Et bientôt les règles pour les vols suborbitaux…

La logique réglementaire

Federal Aviation Regulations

FAR 25 –
CS-25 Book 1

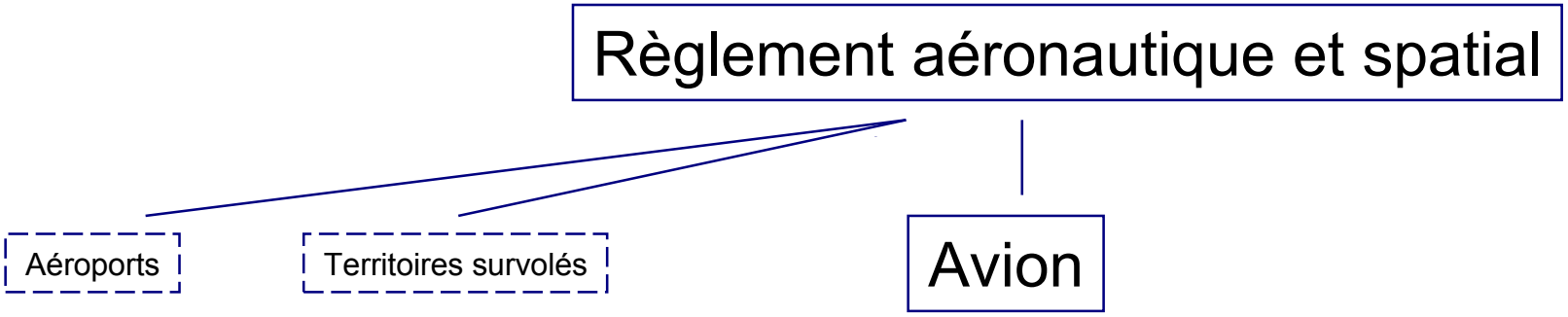
European Aviation Safety Agency

FAR/CS 25-1309

Convention on international civil aviation, Chicago, 7/12/1944

gerard.ladier@airbus.com 33 5 61 93 66 30

La logique réglementaire



Federal Aviation Regulations

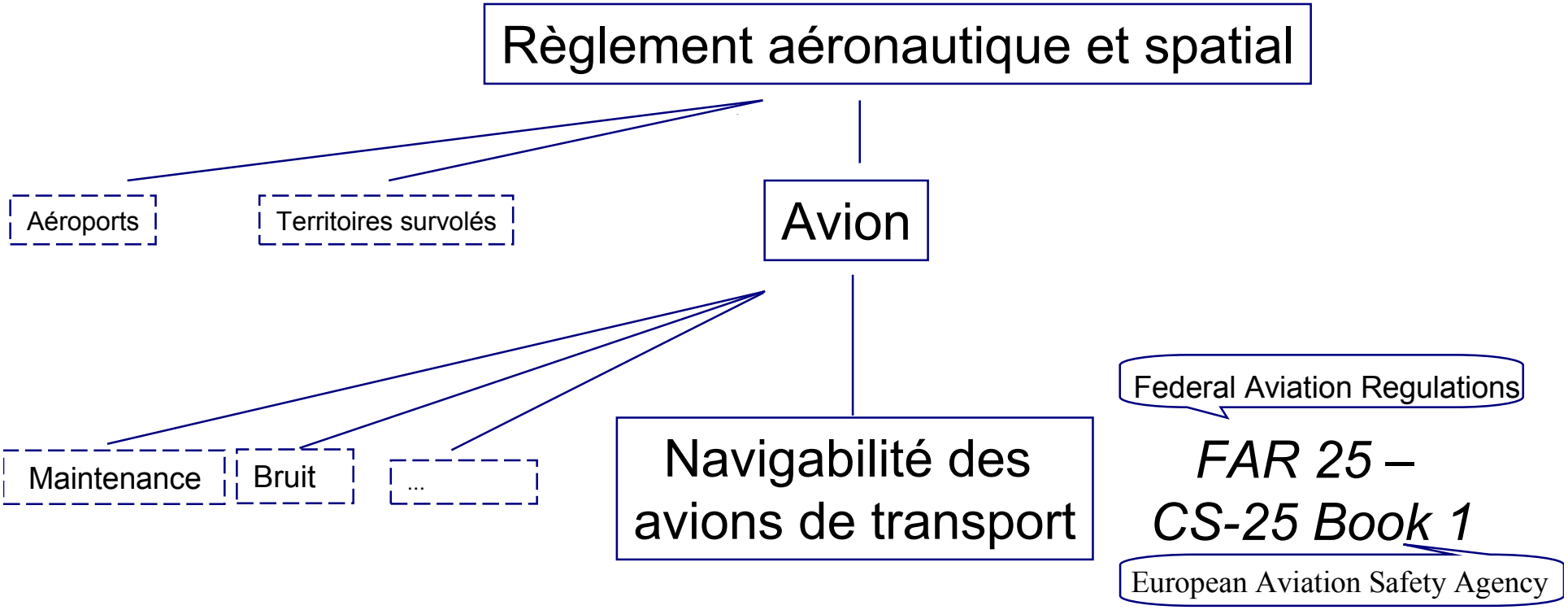
FAR 25 –
CS-25 Book 1

European Aviation Safety Agency

FAR/CS 25-1309

Convention on international civil aviation, Chicago, 7/12/1944

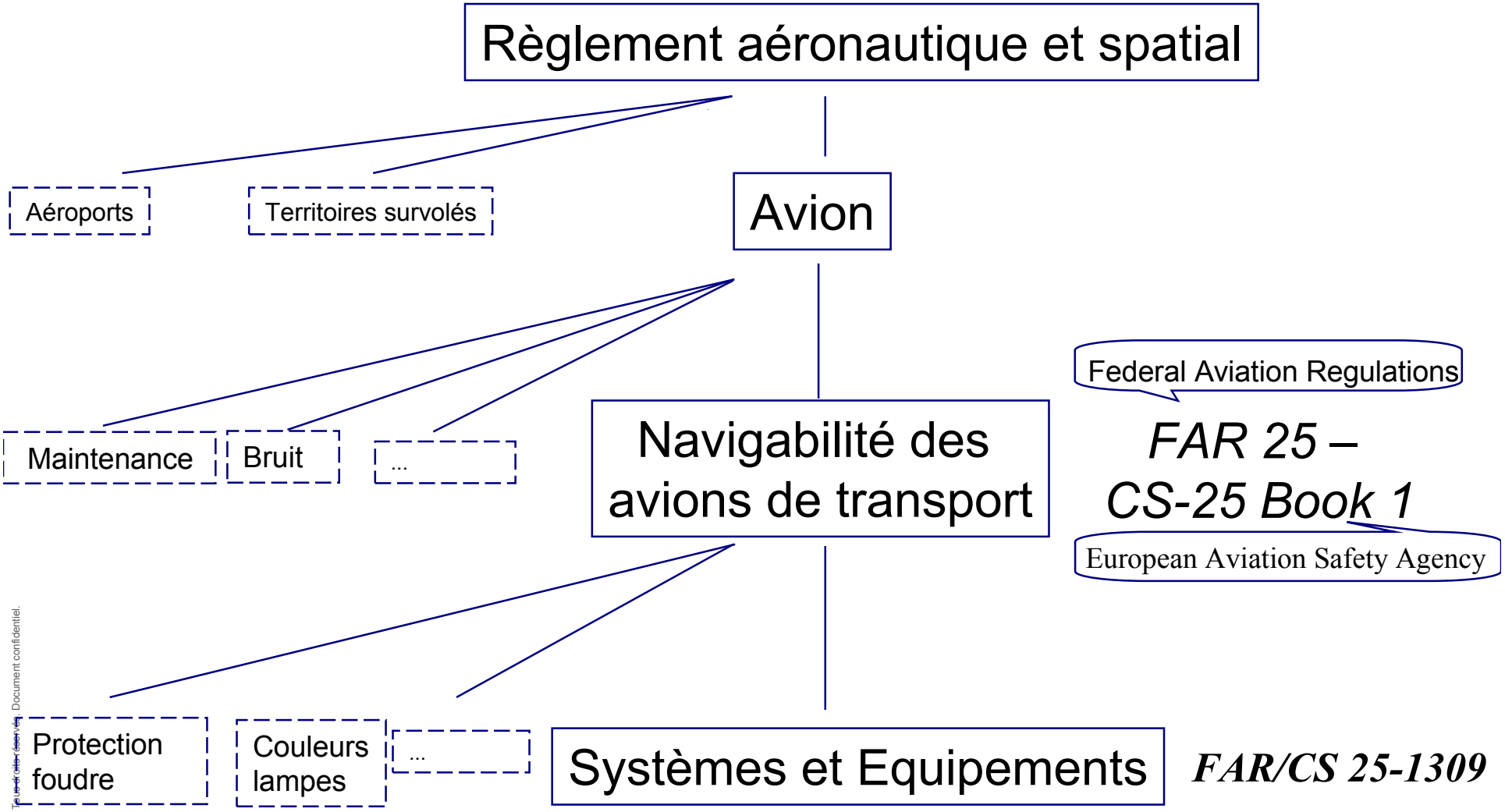
La logique réglementaire



FAR/CS 25-1309

Convention on international civil aviation, Chicago, 7/12/1944

La logique réglementaire

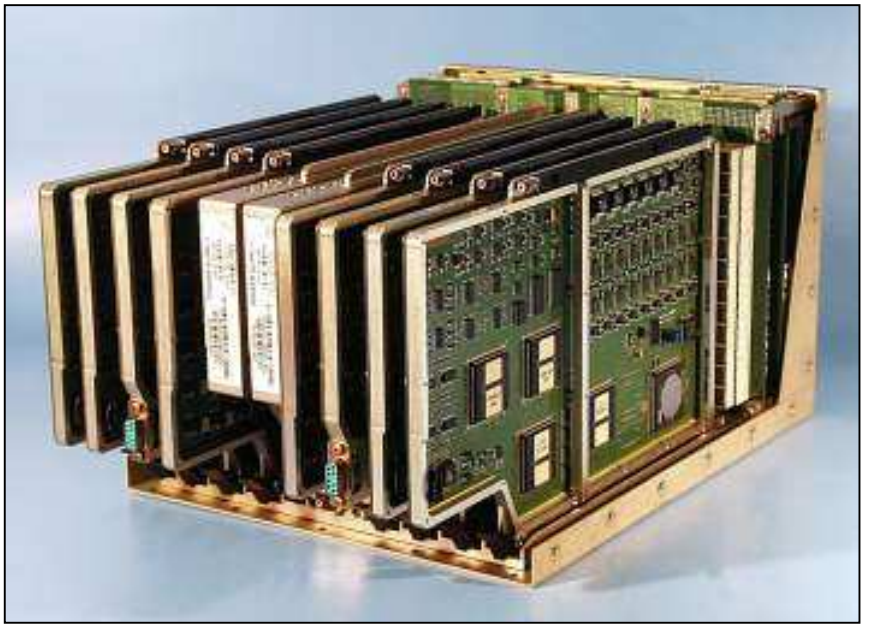


Convention on international civil aviation, Chicago, 7/12/1944

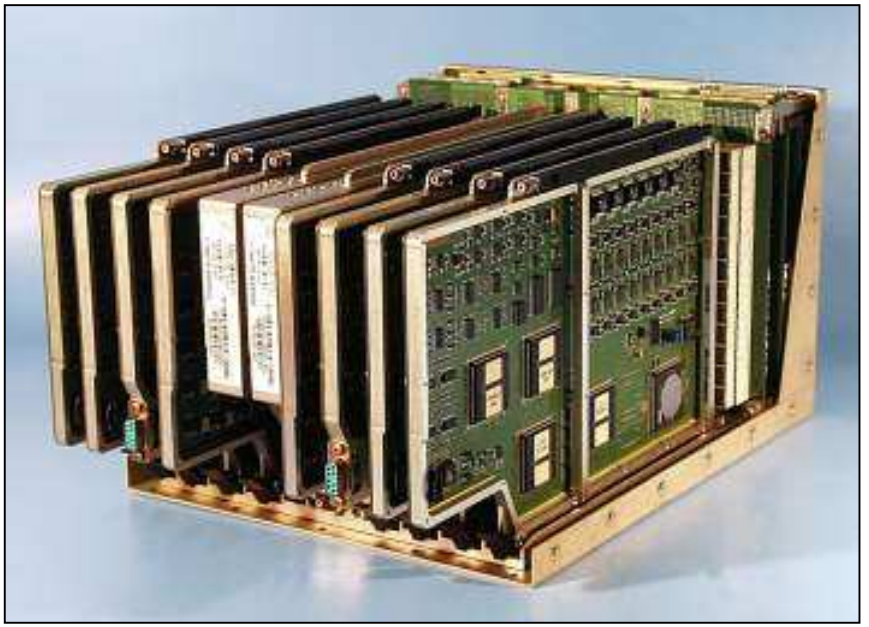
Equipement ? Système ?

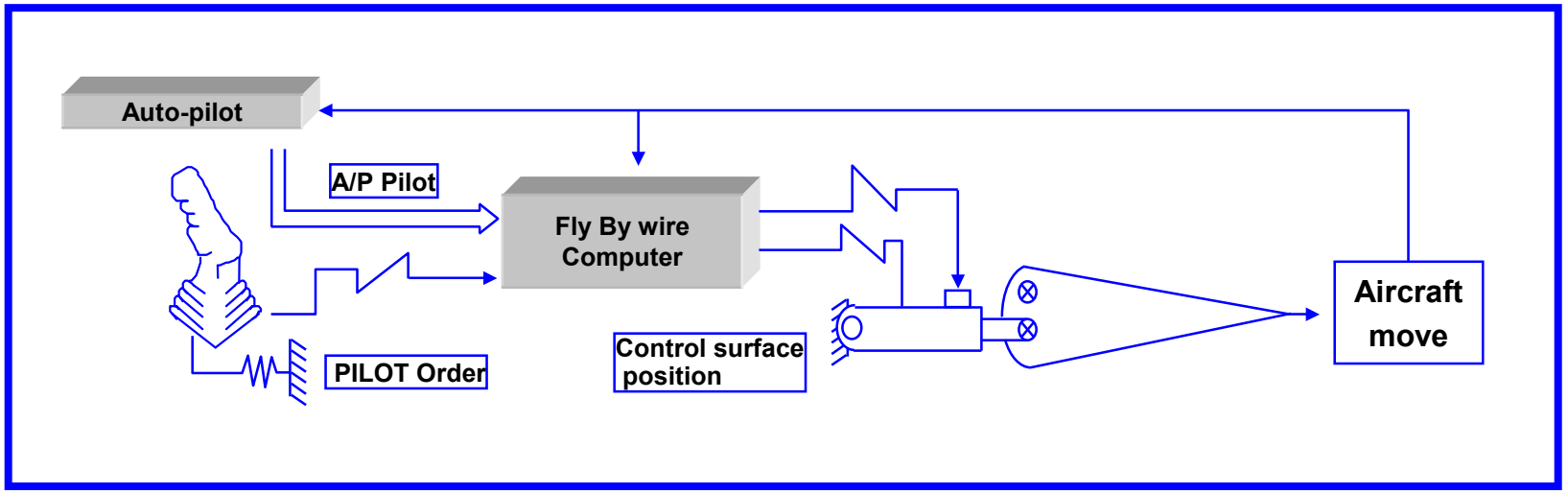
Equipement ? Système ?

Equipement ? Système ?



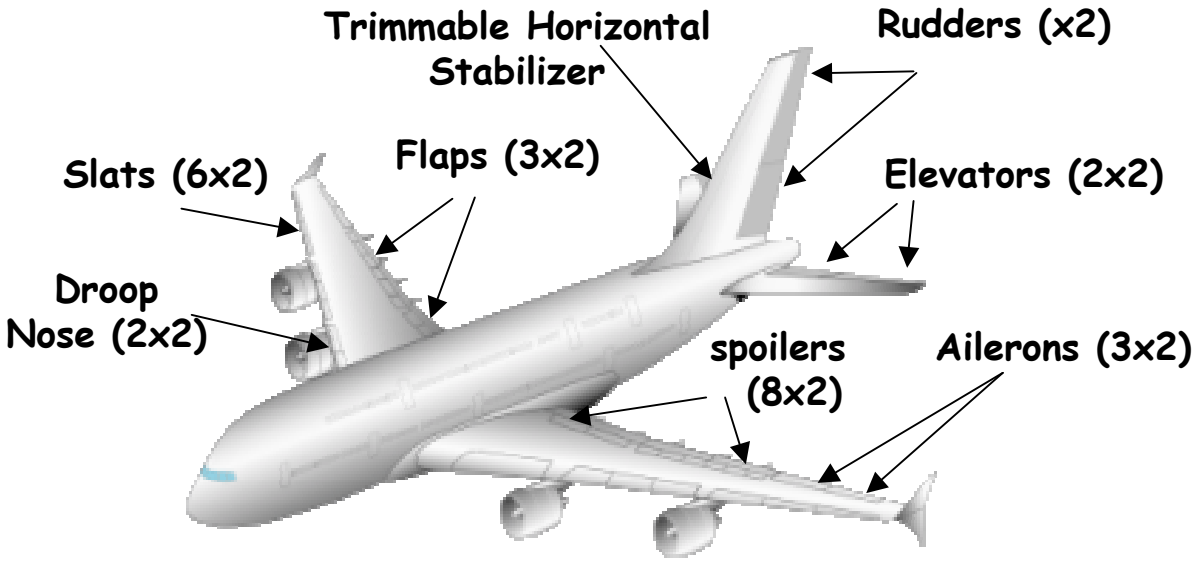
Equipement ? Système ?





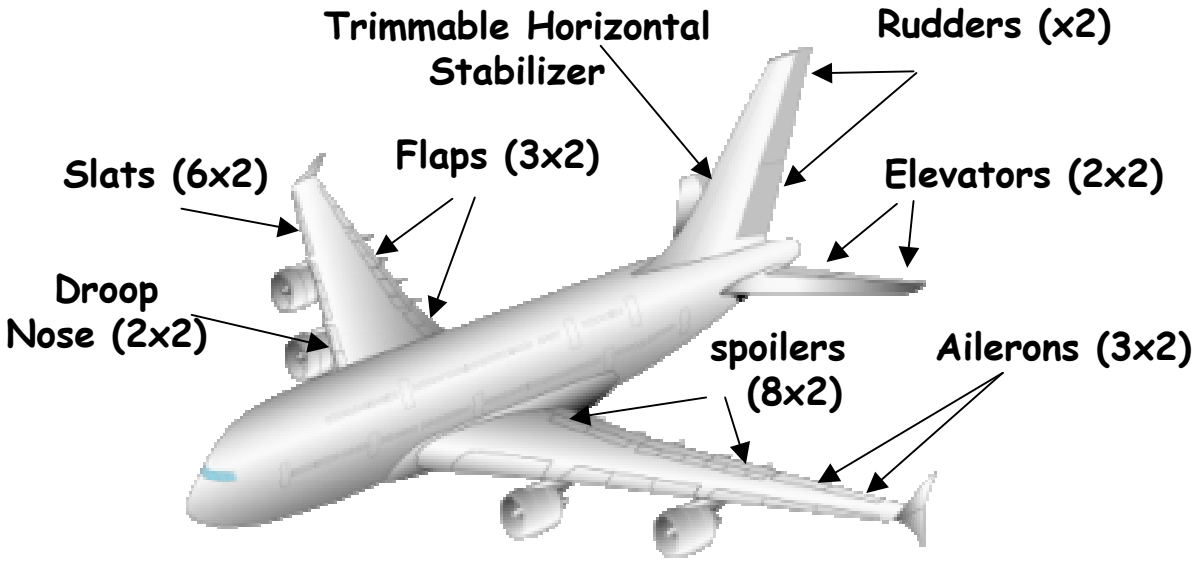
Exemple : Commandes De Vol Electriques

Objectif du système de CDVE A380 : contrôler toutes les surfaces



Exemple : Commandes De Vol Electriques

Objectif du système de CDVE A380 : contrôler toutes les surfaces



3 Primary Computer

= 6 x Flight Control & Guidance Unit

+ 3 x SEcondary Computer

Règlement et moyens de conformité

Règlement et moyens de conformité

- Les équipements "essentiels" doivent être conçus pour assurer les fonctions attendues

Règlement et moyens de conformité

- Les équipements "essentiels" doivent être conçus pour assurer les fonctions attendues
- Les systèmes et les composants, vus seuls ou interconnectés doivent être conçus de telle sorte que l'apparition

Règlement et moyens de conformité

- Les équipements "essentiels" doivent être conçus pour assurer les fonctions attendues
- Les systèmes et les composants, vus seuls ou interconnectés doivent être conçus de telle sorte que l'apparition

  - de défaillances limitant la sécurité du vol ou de l'atterrissage soit EXTREMEMENT IMPROBABLE et ne résulte pas d'une panne simple

Règlement et moyens de conformité

- Les équipements "essentiels" doivent être conçus pour assurer les fonctions attendues
- Les systèmes et les composants, vus seuls ou interconnectés doivent être conçus de telle sorte que l'apparition

  - de défaillances limitant la sécurité du vol ou de l'atterrissage soit EXTREMEMENT IMPROBABLE et ne résulte pas d'une panne simple

  - de toute autre nature de défaillance affectant l'intégrité de l'avion ou les actions de l'équipage soit IMPROBABLE

Règlement et moyens de conformité

- Les équipements "essentiels" doivent être conçus pour assurer les fonctions attendues
- Les systèmes et les composants, vus seuls ou interconnectés doivent être conçus de telle sorte que l'apparition

  - de défaillances limitant la sécurité du vol ou de l'atterrissage soit EXTREMEMENT IMPROBABLE et ne résulte pas d'une panne simple

  - de toute autre nature de défaillance affectant l'intégrité de l'avion ou les actions de l'équipage soit IMPROBABLE

  - …

Moyens de conformité à la FAR 25-CS 25 1309

Moyens de conformité à la FAR 25-CS 25 1309

Compliance with the requirements … of this paragraph must be shown by analysis, and where necessary, by appropriate ground, flight, or simulator test.

Moyens de conformité à la FAR 25-CS 25 1309

Compliance with the requirements … of this paragraph must be shown by analysis, and where necessary, by appropriate ground, flight, or simulator test.

- *Cette exigence conduit à :*
  - *effectuer une analyse rationnelle de tous les modes possibles de défaillance et de leurs conséquences (Analyse de Sécurité Système)*
  - *à classer les équipements en fonction de la sévérité des effets des modes de défaillances => 5 catégories / niveaux*

Moyens de conformité à la FAR 25-CS 25 1309

Compliance with the requirements … of this paragraph must be shown by analysis, and where necessary, by appropriate ground, flight, or simulator test.

- *Cette exigence conduit à :*
  - *effectuer une analyse rationnelle de tous les modes possibles de défaillance et de leurs conséquences (Analyse de Sécurité Système)*
  - *à classer les équipements en fonction de la sévérité des effets des modes de défaillances => 5 catégories / niveaux*

Severity Matrix		Degree of redundancy		
		0 (single Fault)	1 (double Fault)	2 (Triple Fault)
Failure Condition Classification	Catastrophic	A	B	C
	Hazardous	B	C	D
	Major	C	D	D
	Minor	D	D	D
	No safety Effect	E	E	E

Moyens de conformité pour le logiciel

gerard.ladier@airbus.com 33 5 61 93 66 30

Moyens de conformité pour le logiciel

il est invisible/intangible
il ne vieillit pas, il ne s'use pas
il n 'est pas détérioré par le test
il est fabriqué artisanalement
il n 'est pas fabriqué à partir de composants standardisés
il est facilement reproductible
il est très (trop) facile à modifier

Moyens de conformité pour le logiciel

gerard.[illegible]@[illegible].com 33 5 61 93 66 30

AIRBUS

Moyens de conformité pour le logiciel

- *It is in general not feasible to assess the number or kinds of software errors, if any, that may remain after the completion of system design, development, and test. DO-178B/ED-12B, provides acceptable means for assessing and controlling the software used to program digital-computer-based systems*"

gerard.la[illegible] 33 5 61 93 66 30

AIRBUS

Le DO-178B/ED-12B dans un ensemble complet

DO178B -ED12B
"Software considerations in airborne systems and equipment"

Le DO-178B/ED-12B dans un ensemble complet

Airworthiness Regulation Requirements

Federal Airworthiness Requirements / Joint Airworthiness Requirements (EASA)

FAR - CS 25.1309 "Equipment, Systems and Installations"

AC - AMC 25.1309 "System design and analysis »

System Level

Recommended Practices for system safety assessment

ARP4754-ED79
"Certification considerations for highly-integrated or complex aircraft systems"

ARP4761-ED135
"Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment »

Component Level

DO254-ED80
"Design assurance guidance for airborne electronic hardware"

DO178B -ED12B
"Software considerations in airborne systems and equipment"

DO160E -ED14E
"Environmental conditions and test procedures for airborne equipment"

Le DO-178B/ED-12B dans un ensemble complet

Airworthiness Regulation Requirements

Federal Airworthiness Requirements / Joint Airworthiness Requirements (EASA)

FAR - CS 25.1309 "Equipment, Systems and Installations"

AC - AMC 25.1309 "System design and analysis »

Normes de Navigabilité

Lois

System Level

Recommended Practices for system safety assessment

ARP4754-ED79
"Certification considerations for highly-integrated or complex aircraft systems"

ARP4761-ED135
"Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment »

Component Level

DO254-ED80
"Design assurance guidance for airborne electronic hardware"

DO178B -ED12B
"Software considerations in airborne systems and equipment"

DO160E -ED14E
"Environmental conditions and test procedures for airborne equipment"

Le DO-178B/ED-12B dans un ensemble complet

Airworthiness Regulation Requirements

Federal Airworthiness Requirements / Joint Airworthiness Requirements (EASA)

FAR - CS 25.1309 "Equipment, Systems and Installations"

AC - AMC 25.1309 "System design and analysis »

System Level

Recommended Practices for system safety assessment

ARP4754-ED79
"Certification considerations for highly-integrated or complex aircraft systems"

ARP4761-ED135
"Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment »

Component Level

DO254-ED80
"Design assurance guidance for airborne electronic hardware"

DO178B -ED12B
"Software considerations in airborne systems and equipment"

DO160E -ED14E
"Environmental conditions and test procedures for airborne equipment"

Normes de Navigabilité

Lois

Normes "industrielles"

Pour constuire la conformité

Guides

Premier principe

Premier principe

on ne peut avoir de l'eau propre à la sortie d'un tuyau sale

⇒

on va demander toutes les garanties sur le tuyau

gerard.ladier@airbus.com 33 5 61 93 66 30

Premier principe

Process T(q)

Define HLR's

HLR

Process T(q+1)

Define HLR(1)

HLR(1)+ Implementation detail

Process T(q+2)

Define HLR(2)

HLR(2)+ Implementation detail

Process T(x)

Produce Object Code

Object Code

on ne peut avoir de l'eau propre à la sortie d'un tuyau sale

⇒

on va demander toutes les garanties sur le tuyau

DO-178B/ED-12B : les exigences sur le tuyau …

gerard.ladier@airbus.com 33 5 61 93 66 30

AIRBUS

DO-178B/ED-12B : les exigences sur le tuyau …

- “DO-178B/ED-12B is primarily a process-oriented document”

DO-178B/ED-12B : les exigences sur le tuyau …

- "DO-178B/ED-12B is primarily a process-oriented document"

  => *Recueil d'exigences sur les processus et leurs produits*

DO-178B/ED-12B : les exigences sur le tuyau …

- “DO-178B/ED-12B is primarily a process-oriented document”

  => *Recueil d’exigences sur les processus et leurs produits*

- Rappel : «l'apparition de défaillances limitant la sûreté du vol ou de l'atterrissage soit EXTREMEMENT IMPROBABLE, etc»

DO-178B/ED-12B : les exigences sur le tuyau …

- "DO-178B/ED-12B is primarily a process-oriented document"

  => *Recueil d'exigences sur les processus et leurs produits*

- Rappel : «l'apparition de défaillances limitant la sûreté du vol ou de l'atterrissage soit EXTREMEMENT IMPROBABLE, etc»

  => *Les exigences varient donc en fonction des niveaux*

DO-178B/ED-12B : les exigences sur le tuyau …

- "DO-178B/ED-12B is primarily a process-oriented document"

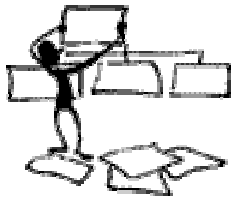
  => *Recueil d'exigences sur les processus et leurs produits*

- Rappel : «l'apparition de défaillances limitant la sûreté du vol ou de l'atterrissage soit EXTREMEMENT IMPROBABLE, etc»

  => *Les exigences varient donc en fonction des niveaux*

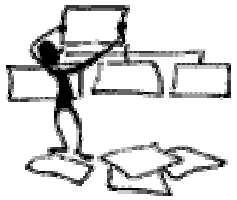
	Objectif		Applicabilité par niveau logiciel				Produit		Catégorie de contrôle par niveau logiciel			
	description	Réf	A	B	C	D	Description	Réf.	A	B	C	D
3	La couverture de test des exigences de haut niveau est assurée	6.4.4.1	●	❍	❍	❍	Résultats de Vérification du Logiciel	11.14	②	②	②	②

Cycles de vie et processus



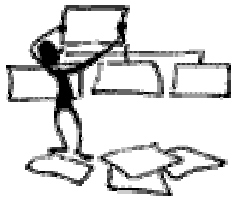
Cycles de vie et processus

- Définition des processus qui seront combinés pour décrire le cycle de vie d'un projet donné :
  - Processus de planification (organisation, plans)
  - Processus de développement (spécification, conception, codage, intégration)
  - Processus intégraux (vérification, gestion de configuration, assurance qualité, coordination pour la certification).



Cycles de vie et processus

- Définition des processus qui seront combinés pour décrire le cycle de vie d'un projet donné :
  - Processus de planification (organisation, plans)
  - Processus de développement (spécification, conception, codage, intégration)
  - Processus intégraux (vérification, gestion de configuration, assurance qualité, coordination pour la certification).



- Définition pour chaque processus (ex : conception) :
  - des objectifs d'Assurance (ex : définir l'architecture et les éléments permettant de coder)
  - des moyens de les satisfaire (ex : pas de précision)
  - des données d'entrées : (ex : Spécifications, Plan de dév., Régles de conception)
  - des activités : (ex :définir l'architecture, les exigences dérivées, etc.)
  - des produits : (ex : description de conception)
  - des critères de transition

Les exigences communes sur les processus de développement - 1

gerard.ladier@airbus.com 33 5 61 93 66 30

Les exigences communes sur les processus de développement - 1

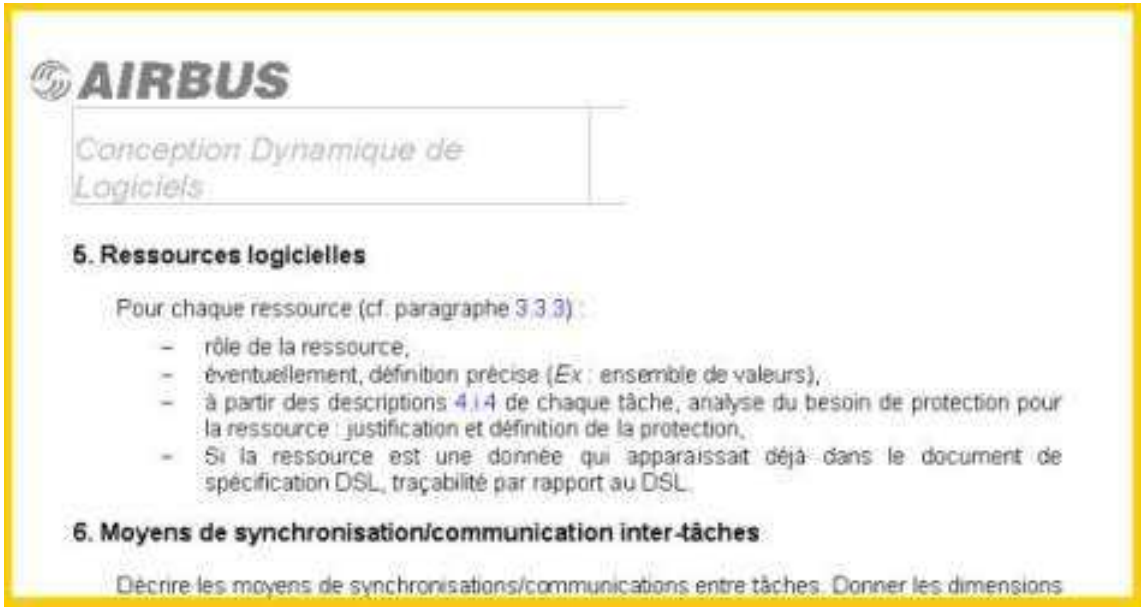
- Etablissement préalable et respect des règles

Les exigences communes sur les processus de développement - 1

- Etablissement préalable et respect des règles
- Règles ?
  - Plusieurs dizaines de documents
  - Précisent comment réaliser une activité (méthodes, moyens, contraintes à satisfaire, produits attendus, etc.)
  - Exemples :

Les exigences communes sur les processus de développement - 1

- Etablissement préalable et respect des règles
- Règles ?
  - Plusieurs dizaines de documents
  - Précisent comment réaliser une activité (méthodes, moyens, contraintes à satisfaire, produits attendus, etc.)
  - Exemples :



AIRBUS

Conception Dynamique de Logiciels

5. Ressources logicielles

Pour chaque ressource (cf. paragraphe 3.3.3) :

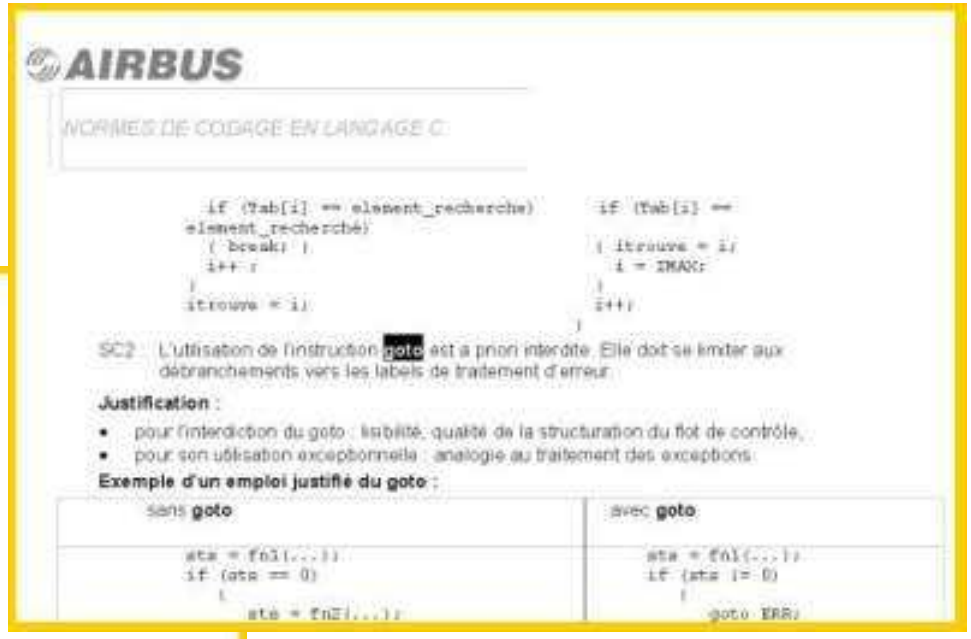
- rôle de la ressource,
- éventuellement, définition précise (*Ex* : ensemble de valeurs),
- à partir des descriptions 4.i.4 de chaque tâche, analyse du besoin de protection pour la ressource : justification et définition de la protection,
- Si la ressource est une donnée qui apparaissait déjà dans le document de spécification DSL, traçabilité par rapport au DSL.

6. Moyens de synchronisation/communication inter-tâches

Décrire les moyens de synchronisations/communications entre tâches. Donner les dimensions

Les exigences communes sur les processus de développement - 1

- Etablissement préalable et respect des règles
- Règles ?
  - Plusieurs dizaines de documents
  - Précisent comment réaliser une activité (méthodes, moyens, contraintes à satisfaire, produits attendus, etc.)
  - Exemples :


AIRBUS

NORMES DE CODAGE EN LANGAGE C

```
  if (Tab[i] == element_recherche)
element_recherché)
  { break; }
  i++ ;
}
itrouve = i;
```

```
if (Tab[i] ==
{ itrouve = i;
  i = IMAX;
}
i++;
}
```

SC2 : L'utilisation de l'instruction goto est à priori interdite. Elle doit se limiter aux débranchements vers les labels de traitement d'erreur.

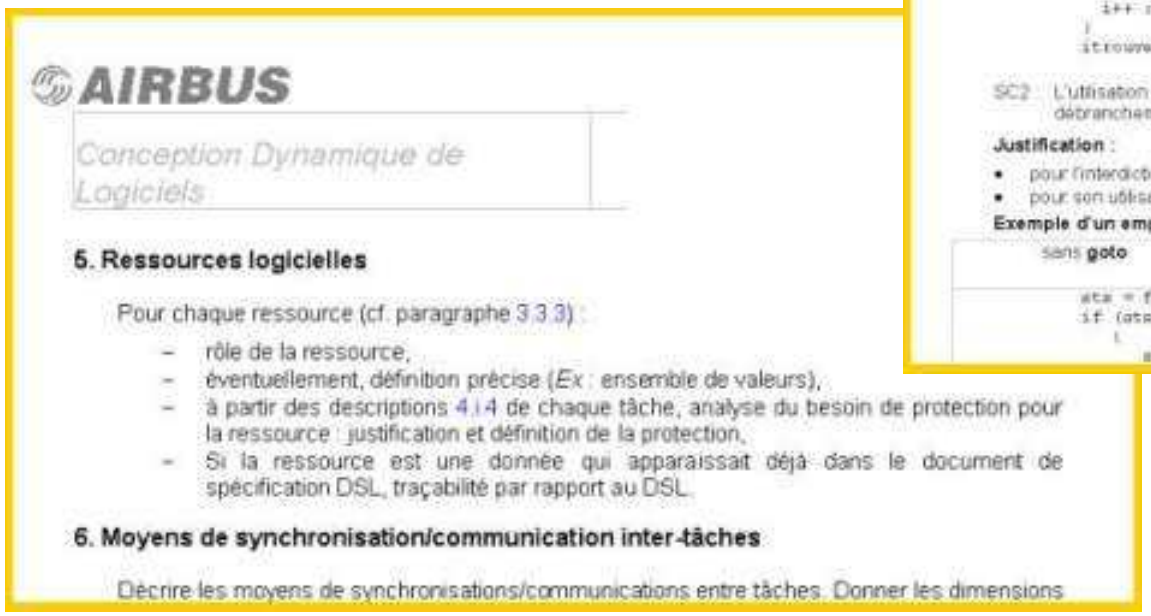
Justification :

- pour l'interdiction du goto : lisibilité, qualité de la structuration du flot de contrôle,
- pour son utilisation exceptionnelle : analogie au traitement des exceptions

Exemple d'un emploi justifié du goto :

sans **goto**	avec **goto**

`sta = fn1(...);`
`if (sta == 0)`
`{`
`  sta = fn2(...);`
	`sta = fn1(...);`
	`if (sta != 0)`
	`{`
	`  goto ERR;`


AIRBUS

Conception Dynamique de Logiciels

5. Ressources logicielles

Pour chaque ressource (cf. paragraphe 3.3.3) :

- rôle de la ressource,
- éventuellement, définition précise (*Ex* : ensemble de valeurs),
- à partir des descriptions 4.i.4 de chaque tâche, analyse du besoin de protection pour la ressource : justification et définition de la protection,
- Si la ressource est une donnée qui apparaissait déjà dans le document de spécification DSL, traçabilité par rapport au DSL.

6. Moyens de synchronisation/communication inter-tâches

Décrire les moyens de synchronisations/communications entre tâches. Donner les dimensions

Les exigences communes sur les processus de développement - 2

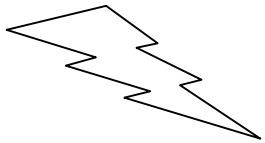
gerard.ladier@airbus.com 33 5 61 93 66 30

Les exigences communes sur les processus de développement - 2

Chaque élément
de spécification
ou de conception
doit être

Les exigences communes sur les processus de développement - 2

précis

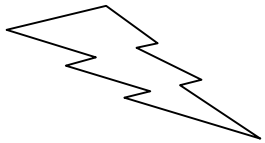


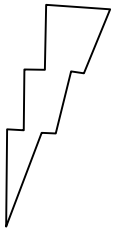
Chaque élément
de spécification
ou de conception
doit être

Les exigences communes sur les processus de développement - 2

cohérent

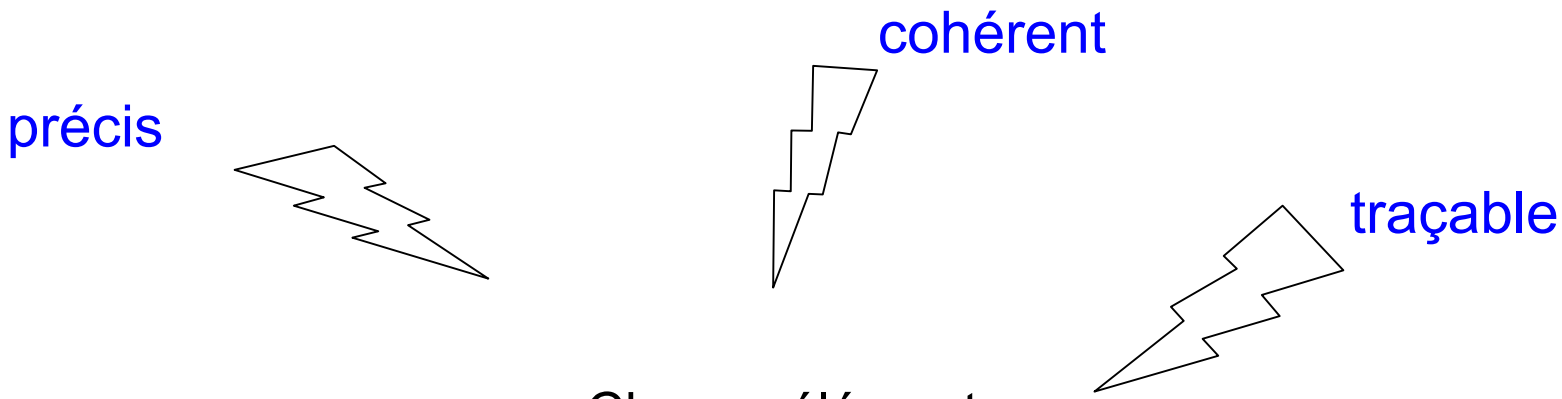
précis



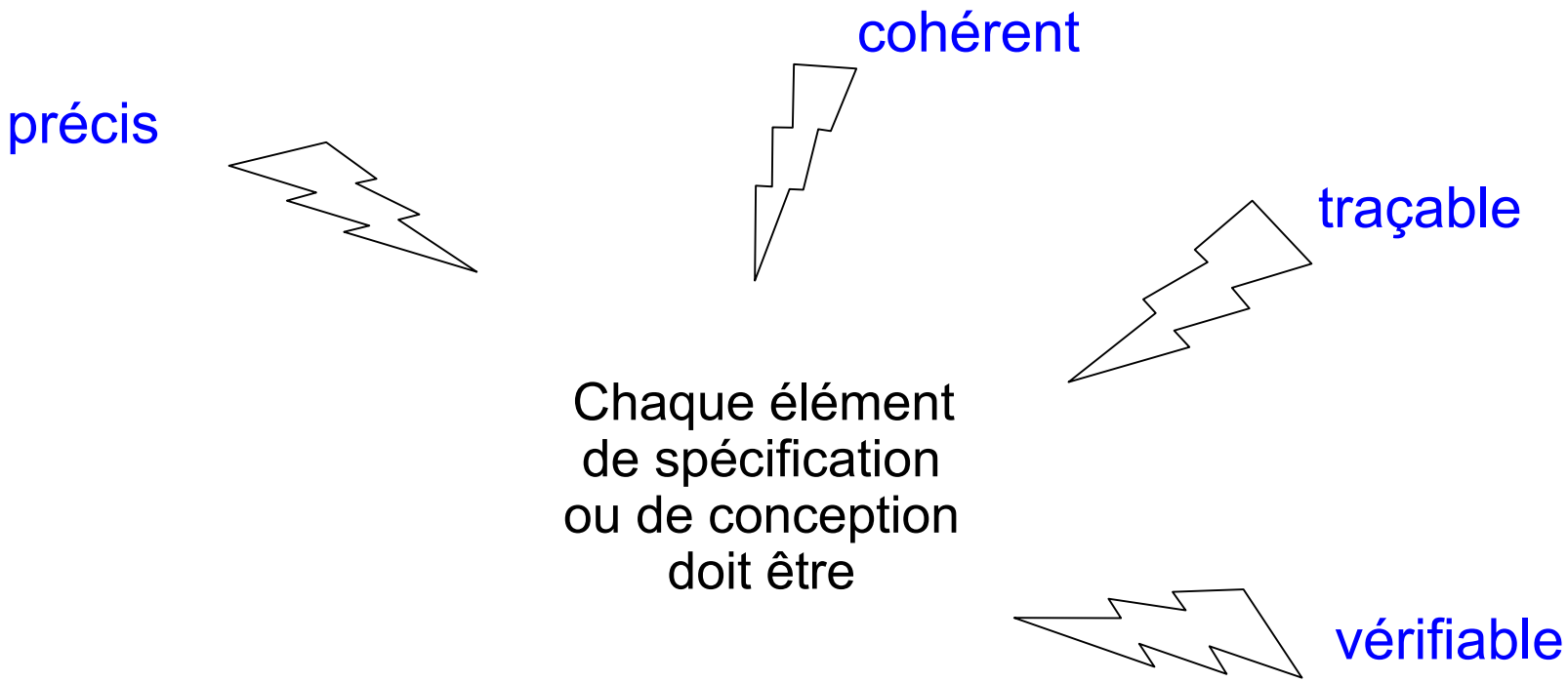


Chaque élément
de spécification
ou de conception
doit être

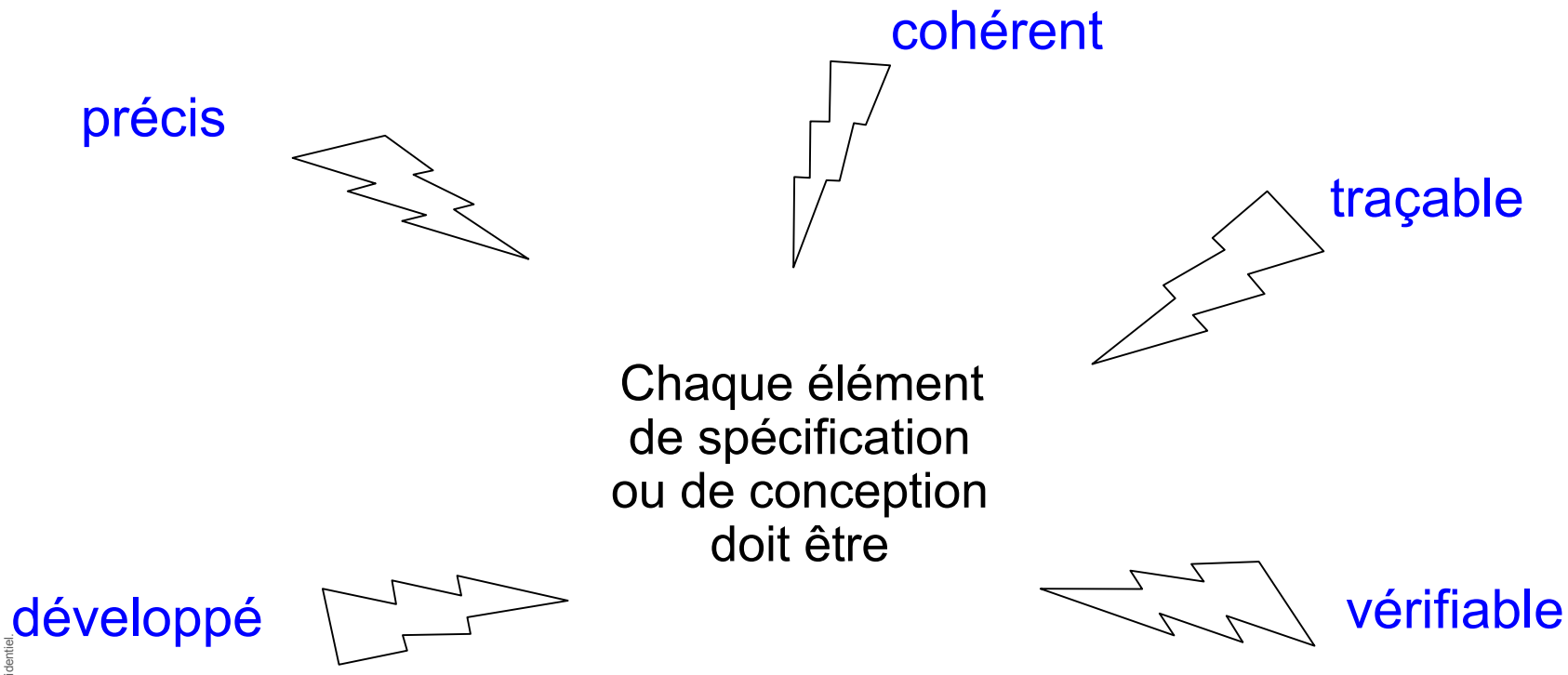
Les exigences communes sur les processus de développement - 2



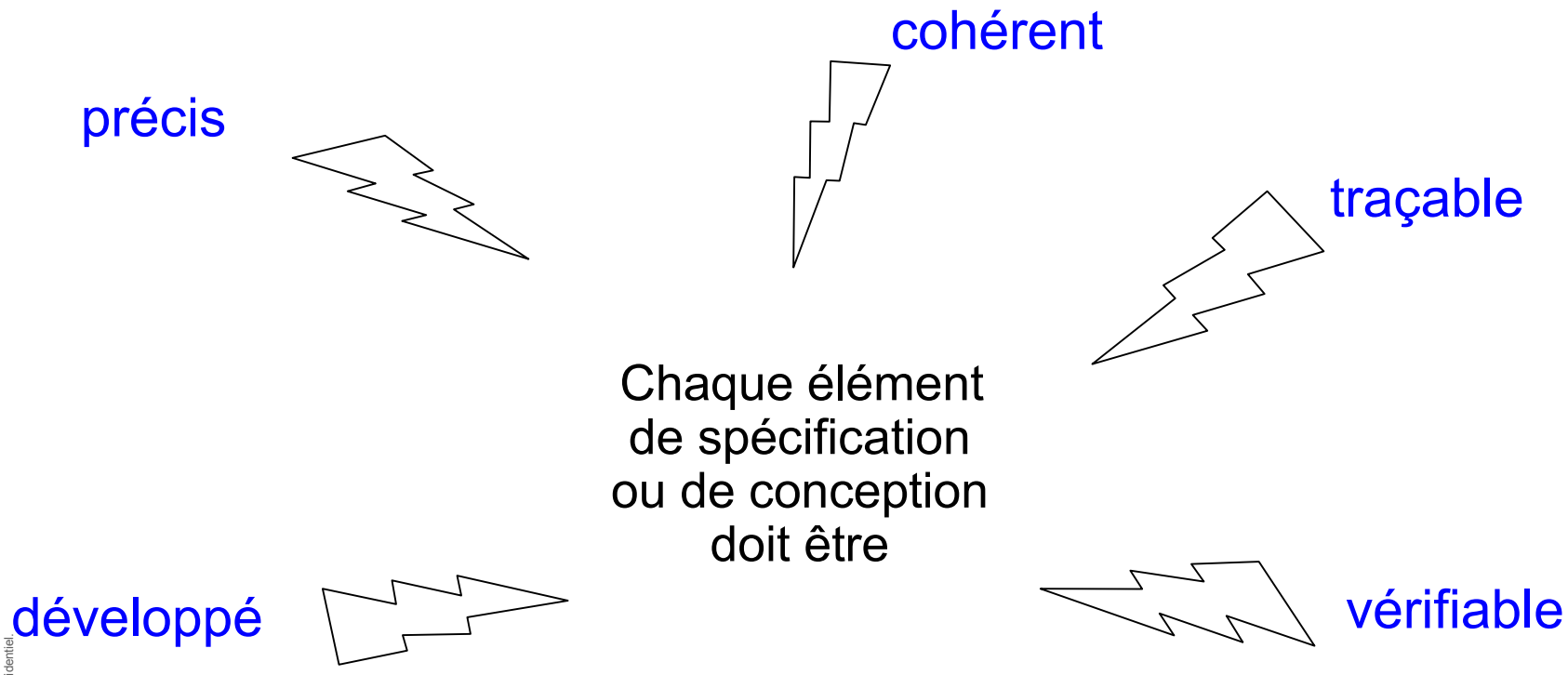
Les exigences communes sur les processus de développement - 2



Les exigences communes sur les processus de développement - 2

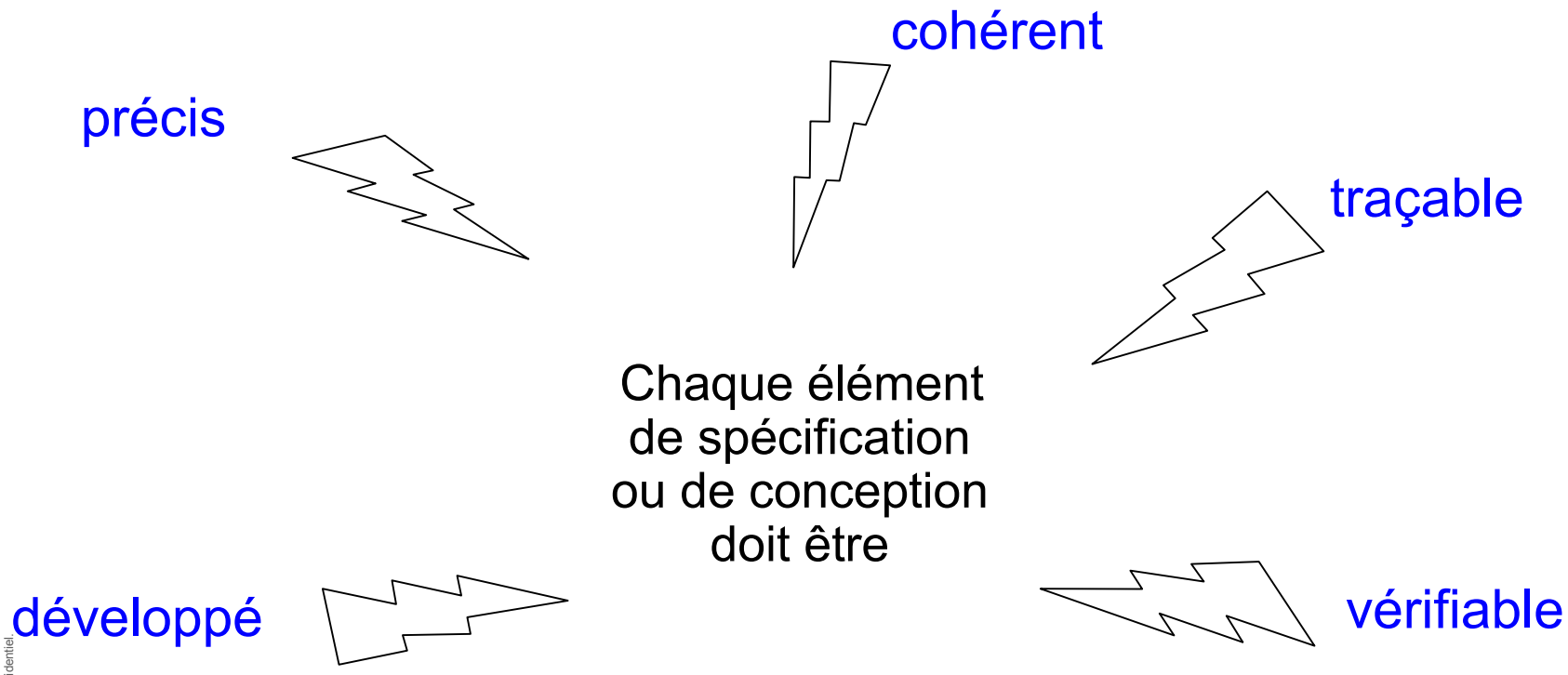


Les exigences communes sur les processus de développement - 2



- Retour vers les processus amont en cas de découvertes de problèmes pouvant les impacter

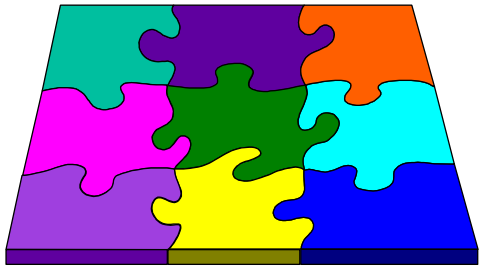
Les exigences communes sur les processus de développement - 2



- Retour vers les processus amont en cas de découvertes de problèmes pouvant les impacter
- Interdiction de "patches" post-certification

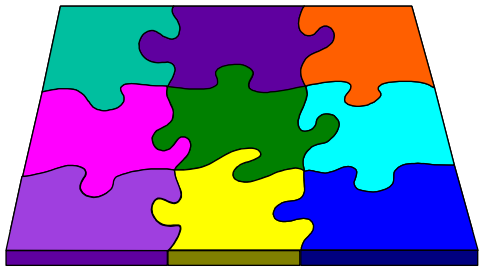
Gestion de configuration et Assurance qualité

Gestion de configuration et Assurance qualité



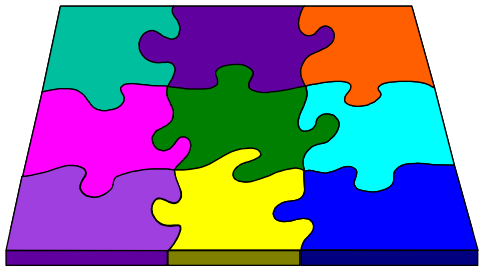
Gestion de configuration et Assurance qualité

- Exigences détaillées pour permettre de satisfaire les objectifs généraux par :
  - la maîtrise de la configuration
  - une bonne gestion des problèmes et des modifications
  - des moyens d'archivage/restauration
  - la traçabilité
  - le contrôle de l'environnement de développement



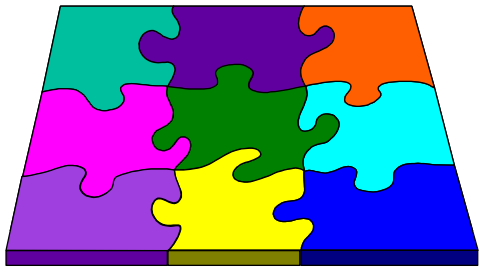
Gestion de configuration et Assurance qualité

- Exigences détaillées pour permettre de satisfaire les objectifs généraux par :
  - la maîtrise de la configuration
  - une bonne gestion des problèmes et des modifications
  - des moyens d'archivage/restauration
  - la traçabilité
  - le contrôle de l'environnement de développement



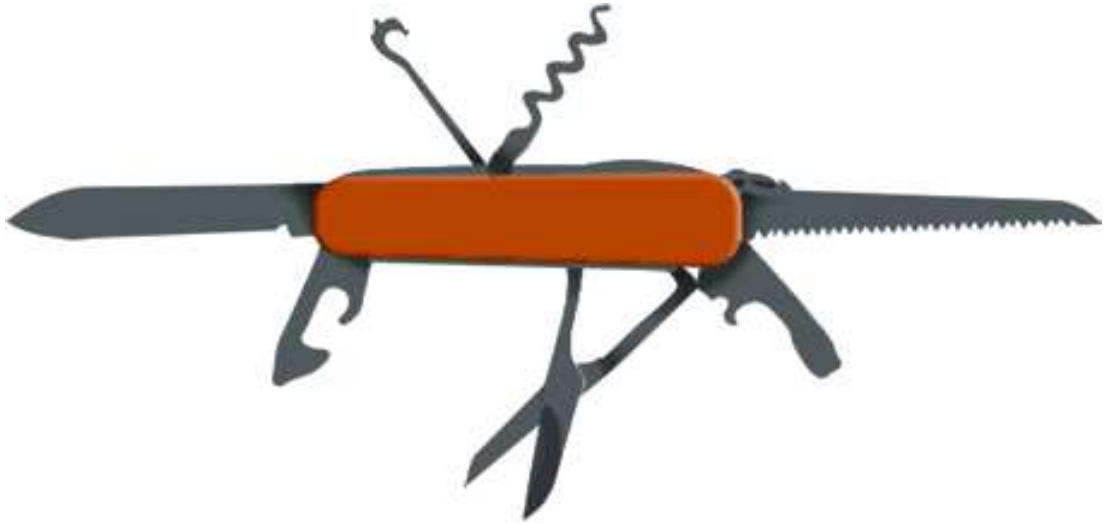
Gestion de configuration et Assurance qualité

- Exigences détaillées pour permettre de satisfaire les objectifs généraux par :
  - la maîtrise de la configuration
  - une bonne gestion des problèmes et des modifications
  - des moyens d'archivage/restauration
  - la traçabilité
  - le contrôle de l'environnement de développement

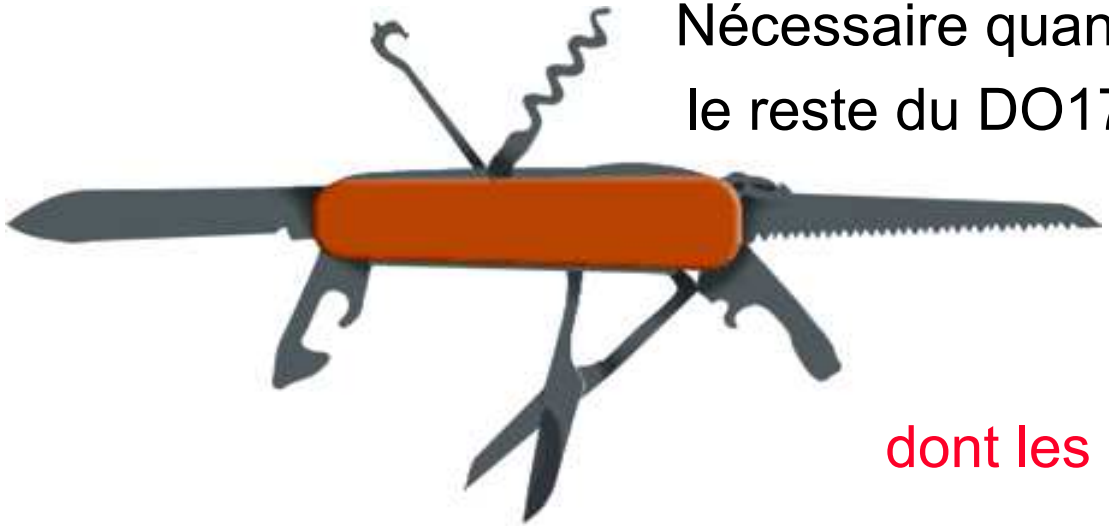


- Objectif :
  - Obtenir l'assurance que la réalité du développement est conforme à ce qui était prévu
- Caractéristiques majeures :
  - indépendance
  - rôle actif dans les activités du cycle de vie.

Qualification des outils



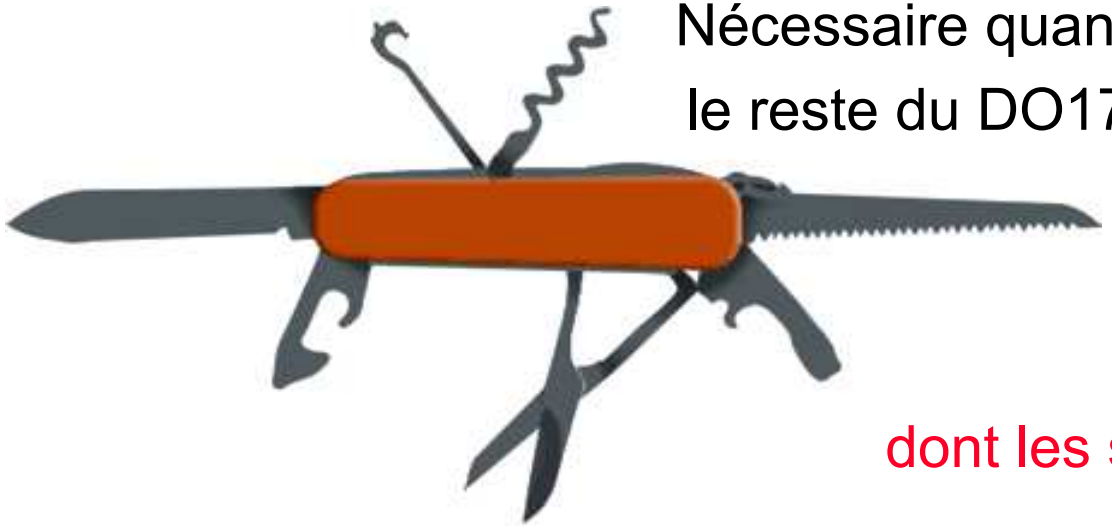
Qualification des outils



Nécessaire quand des processus requis par le reste du DO178B sont éliminés, réduits, ou automatisés par l'utilisation d'un outil (déterministe)

dont les sorties ne sont pas vérifiées

Qualification des outils

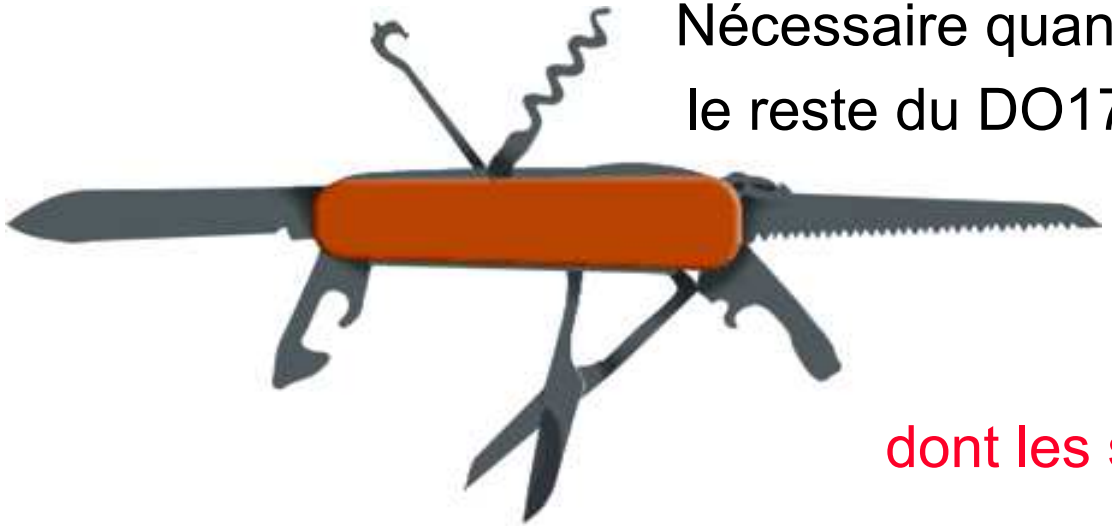


Nécessaire quand des processus requis par le reste du DO178B sont éliminés, réduits, ou automatisés par l'utilisation d'un outil (déterministe)

dont les sorties ne sont pas vérifiées

- outils de développement (ex : générateur de code)

Qualification des outils



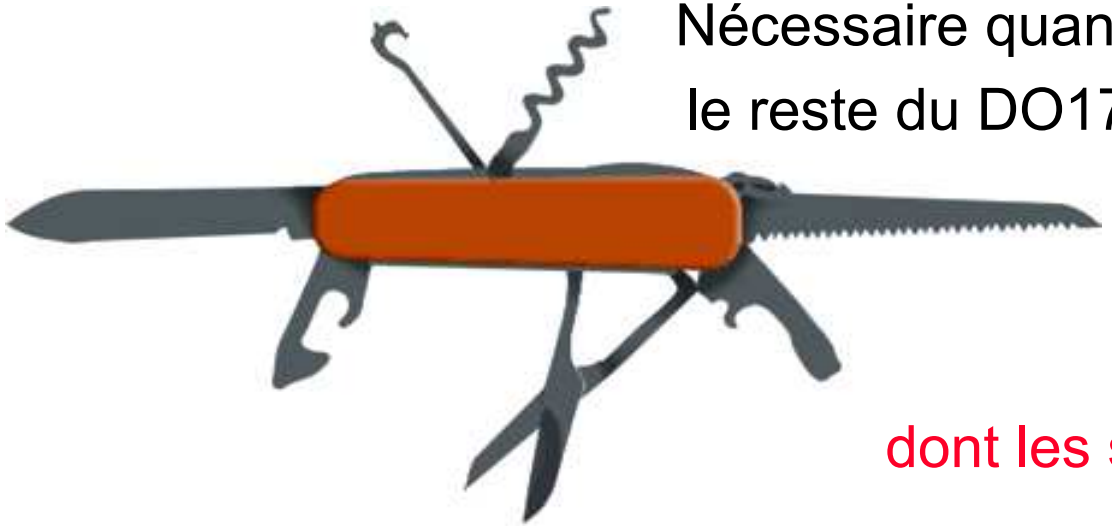
Nécessaire quand des processus requis par le reste du DO178B sont éliminés, réduits, ou automatisés par l'utilisation d'un outil (déterministe)

dont les sorties ne sont pas vérifiées

- outils de développement (ex : générateur de code)

Exigences équivalentes à celles du niveau du logiciel généré

Qualification des outils



Nécessaire quand des processus requis par le reste du DO178B sont éliminés, réduits, ou automatisés par l'utilisation d'un outil (déterministe)

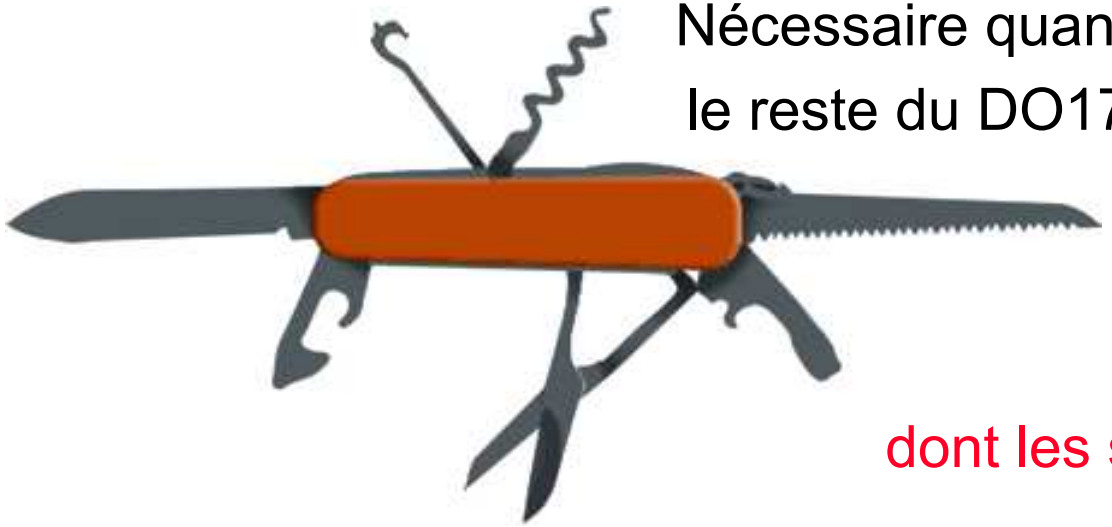
dont les sorties ne sont pas vérifiées

- outils de développement (ex : générateur de code)

  Exigences équivalentes à celles du niveau du logiciel généré

- outils de vérification (ex : émulateurs, simulateurs)

Qualification des outils



Nécessaire quand des processus requis par le reste du DO178B sont éliminés, réduits, ou automatisés par l'utilisation d'un outil (déterministe)

dont les sorties ne sont pas vérifiées

- outils de développement (ex : générateur de code)

  Exigences équivalentes à celles du niveau du logiciel généré

- outils de vérification (ex : émulateurs, simulateurs)

  Exigences réduites, limitées à la validation de l'outil.

Deuxième principe

Deuxième principe

… un tuyau propre ne donne pas nécessairement de l'eau propre

⇒

on superpose les filtres pour détecter et éliminer les impuretés

La vérification

La vérification

- Le chapitre le plus important du DO-178B/ED-12B
  - en volume : 13 pages de description (~ 5 pages pour les autres)
  - en charge de travail induite (A380 : 4 lignes de test pour 1 ligne de code embarqué…)

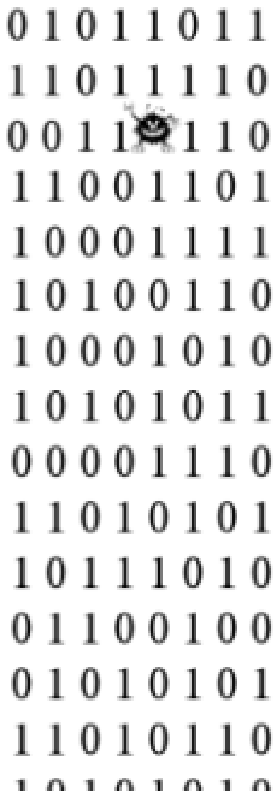
La vérification

- Le chapitre le plus important du DO-178B/ED-12B
  - en volume : 13 pages de description (~ 5 pages pour les autres)
  - en charge de travail induite (A380 : 4 lignes de test pour 1 ligne de code embarqué…)
- Principes de base :
  - processus transverse => s'applique à tous les autres processus
  - combinaison de
    - revues,
    - analyses
    - tests

    pour détecter et rendre compte des erreurs introduites au cours du développement

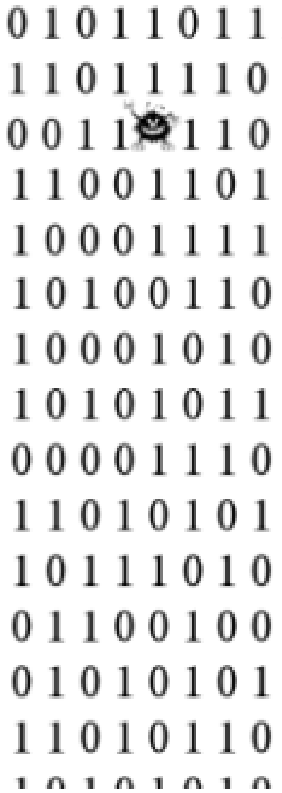
Revues ? Analyses ? Tests ?

- Trois outils majeurs de la chasse aux bugs :



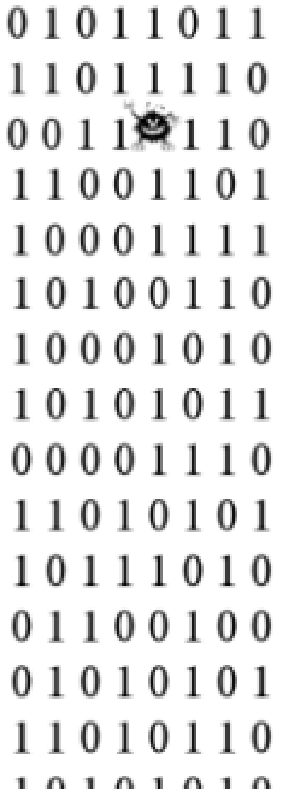
Revues ? Analyses ? Tests ?

- Trois outils majeurs de la chasse aux bugs :
  - Revue : inspection d'un produit par une personne indépendante (niv A) ; *évaluation qualitative*



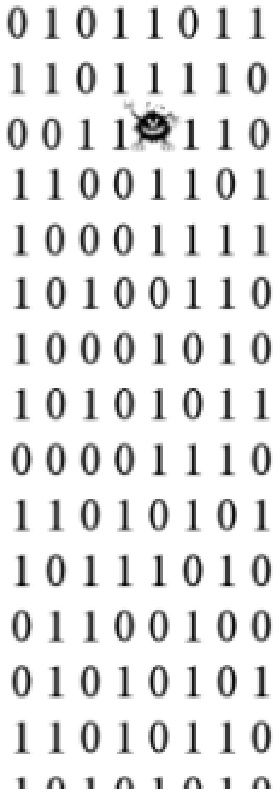
Revues ? Analyses ? Tests ?

- Trois outils majeurs de la chasse aux bugs :
  - Revue : inspection d'un produit par une personne indépendante (niv A) ; *évaluation qualitative*
  - Analyse : examen détaillé d'un produit, éventuellement effectué par un outil ; *évaluation quantitative*



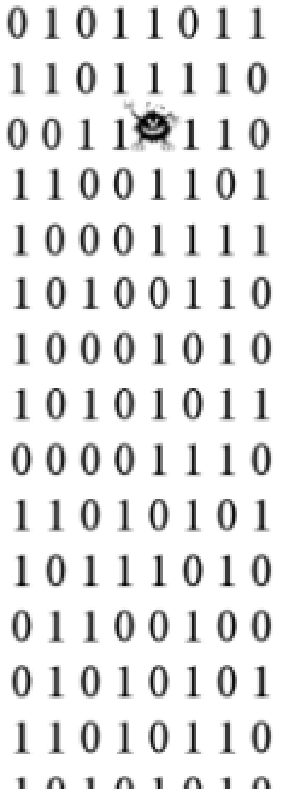
Revues ? Analyses ? Tests ?

- Trois outils majeurs de la chasse aux bugs :
  - Revue : inspection d'un produit par une personne indépendante (niv A) ; *évaluation qualitative*
  - Analyse : examen détaillé d'un produit, éventuellement effectué par un outil ; *évaluation quantitative*
  - Test : exécution d'un logiciel pour comparer les résultats obtenus avec les résultats attendus



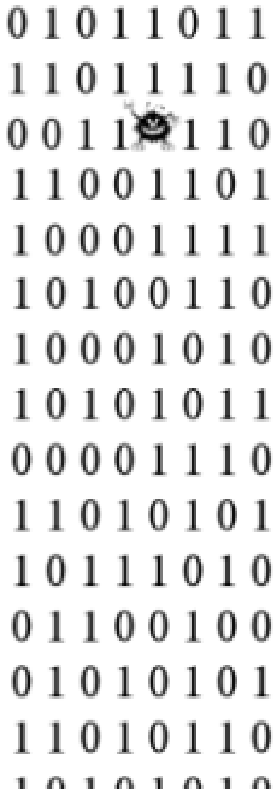
Revues ? Analyses ? Tests ?

- Trois outils majeurs de la chasse aux bugs :
  - Revue : inspection d'un produit par une personne indépendante (niv A) ; *évaluation qualitative*
  - Analyse : examen détaillé d'un produit, éventuellement effectué par un outil ; *évaluation quantitative*
  - Test : exécution d'un logiciel pour comparer les résultats obtenus avec les résultats attendus
    - Test fonctionnel



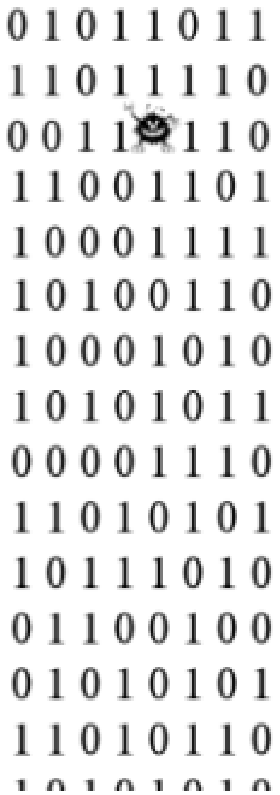
Revues ? Analyses ? Tests ?

- Trois outils majeurs de la chasse aux bugs :
  - Revue : inspection d'un produit par une personne indépendante (niv A) ; *évaluation qualitative*
  - Analyse : examen détaillé d'un produit, éventuellement effectué par un outil ; *évaluation quantitative*
  - Test : exécution d'un logiciel pour comparer les résultats obtenus avec les résultats attendus
    - Test fonctionnel
    - PAS DE TEST FONDE SUR LA STRUCTURE DU CODE

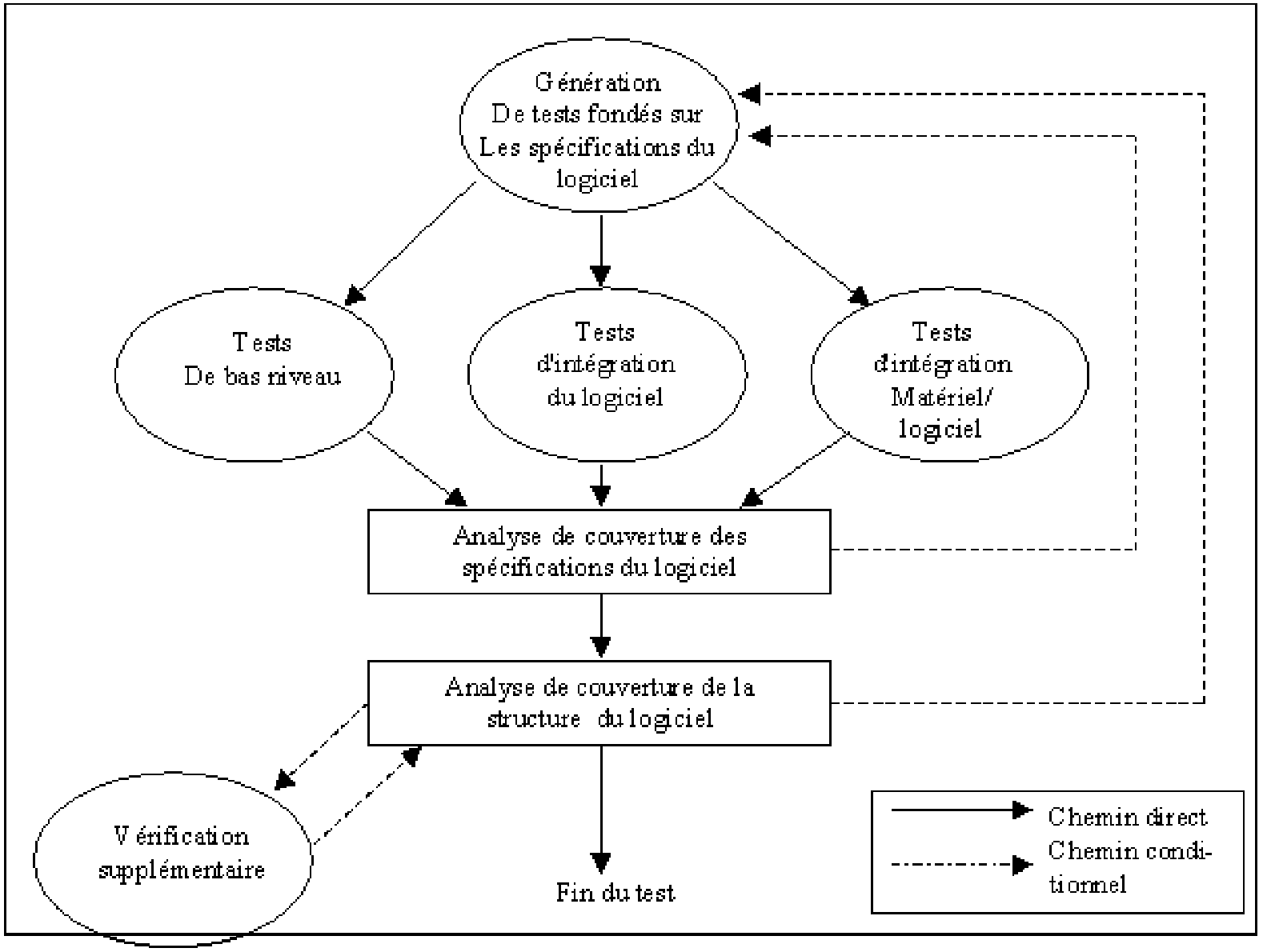


Revues ? Analyses ? Tests ?

- Trois outils majeurs de la chasse aux bugs :
  - Revue : inspection d'un produit par une personne indépendante (niv A) ; *évaluation qualitative*
  - Analyse : examen détaillé d'un produit, éventuellement effectué par un outil ; *évaluation quantitative*
  - Test : exécution d'un logiciel pour comparer les résultats obtenus avec les résultats attendus
    - Test fonctionnel
    - PAS DE TEST FONDE SUR LA STRUCTURE DU CODE
    - analyses de couverture "fonctionnelle" et "structurelle"



La logique de test



Troisième principe

Troisième principe

beaucoup d'intérêts potentiellement contradictoires sont en jeu

⇒

il faut une autorité indépendante pour évaluer le respect des objectifs

Les acteurs de la navigabilité

gerard.ladier@airbus.com 33 5 61 93 66 30

Les acteurs de la navigabilité

- La chaîne de la navigabilité est composée essentiellement :
  - Des autorités
  - Des fabricants d'avions et de moteurs
  - Des compagnies aériennes
  - Des gestionnaires du trafic aérien

Transports Canada Transport Canada

gerard.ladier@airbus.com 33 5 61 93 66 30

AIRBUS

Les acteurs de la navigabilité

- La chaîne de la navigabilité est composée essentiellement :
  - Des autorités
  - Des fabricants d'avions et de moteurs
  - Des compagnies aériennes
  - Des gestionnaires du trafic aérien
- Les autorités :

Transports Canada Transport Canada

gerard.ladier@airbus.com 33 5 61 93 66 30

AIRBUS

Les acteurs de la navigabilité

- La chaîne de la navigabilité est composée essentiellement :
  - Des autorités
  - Des fabricants d'avions et de moteurs
  - Des compagnies aériennes
  - Des gestionnaires du trafic aérien
- Les autorités :
  - FAA aux USA,
    Transport Canada, etc.

Transports Canada Transport Canada

gerard.ladier@airbus.com 33 5 61 93 66 30

AIRBUS

Les acteurs de la navigabilité

- La chaîne de la navigabilité est composée essentiellement :
  - Des autorités
  - Des fabricants d'avions et de moteurs
  - Des compagnies aériennes
  - Des gestionnaires du trafic aérien
- Les autorités :

Transports Canada Transport Canada

  - FAA aux USA, Transport Canada, etc.
  - En Europe, JAA hier et aujourd'hui :
    - Créée en 1970
    - Association des autorités nationales de 38 Etats européens (DGAC,…)

gerard.ladier@airbus.com 33 5 61 93 66 30

AIRBUS

Les acteurs de la navigabilité

- La chaîne de la navigabilité est composée essentiellement :
  - Des autorités
  - Des fabricants d'avions et de moteurs
  - Des compagnies aériennes
  - Des gestionnaires du trafic aérien
- Les autorités :

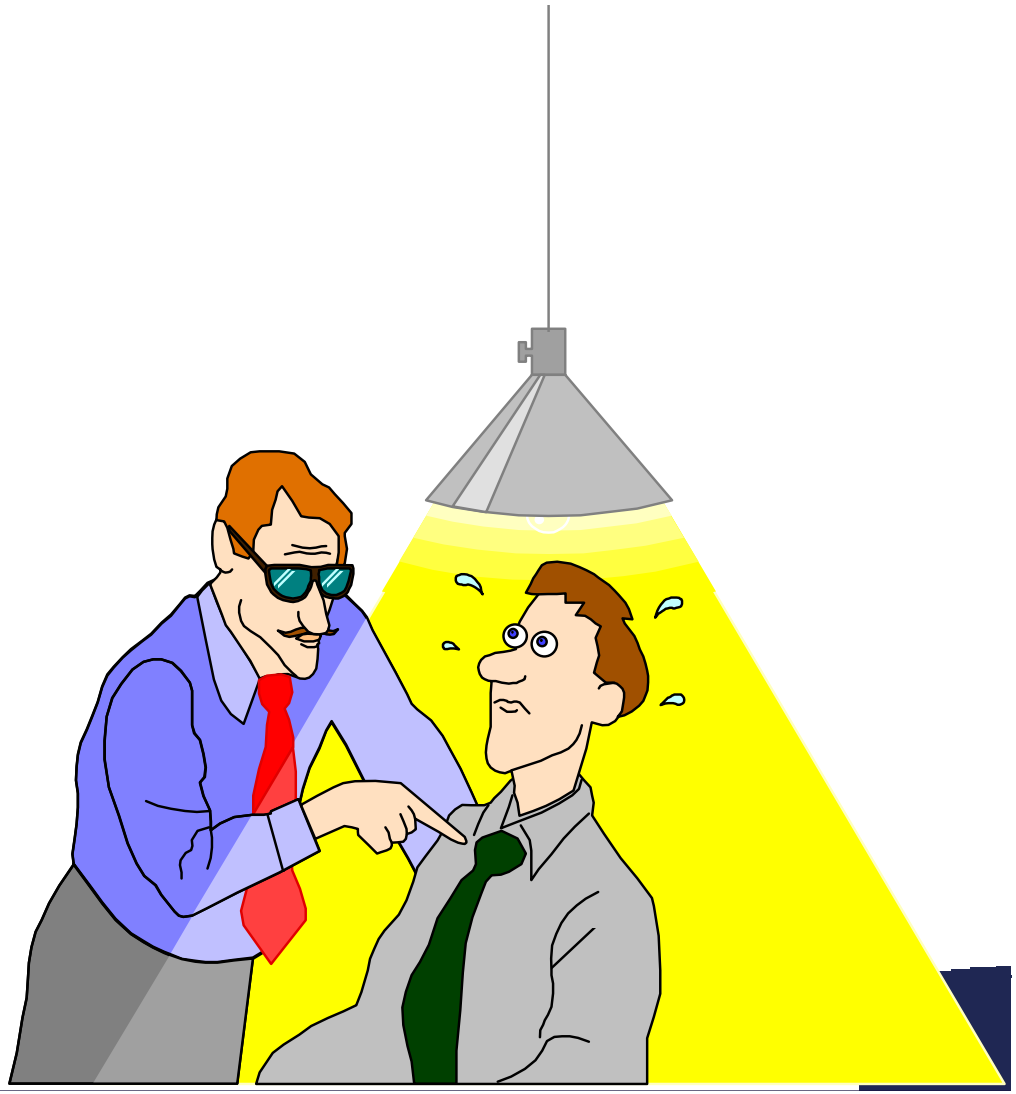
Transports Canada Transport Canada

  - FAA aux USA, Transport Canada, etc.
  - En Europe, JAA hier et aujourd'hui :
    - Créée en 1970
    - Association des autorités nationales de 38 Etats européens (DGAC,…)
  - En Europe, EASA aujourd'hui et demain :
    - European Aviation Safety Agency
    - Créée le 28/09/2003

gerard.ladier@airbus.com 33 5 61 93 66 30

AIRBUS

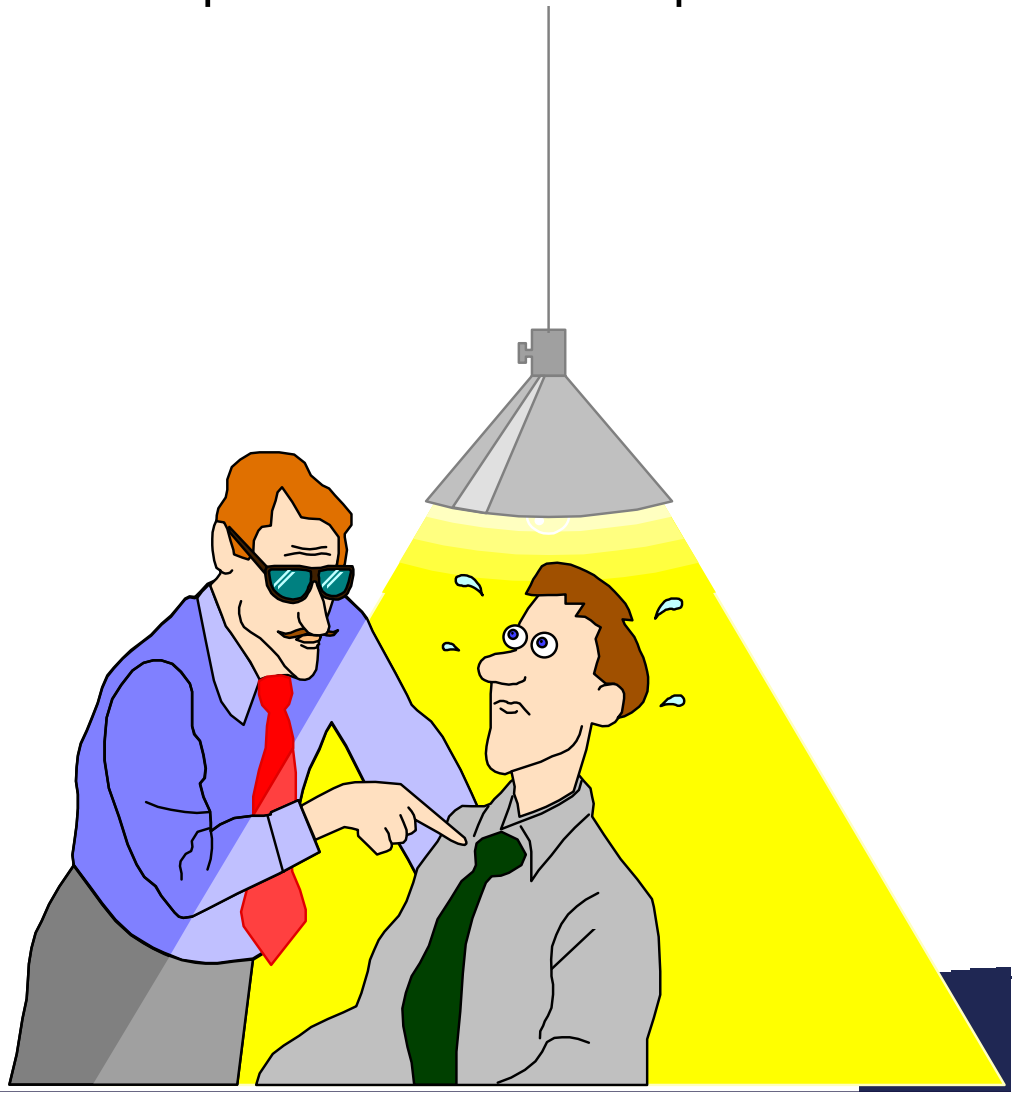
DO-178B/ED-12B : Coordination pour la certification



gerard.ladier@airbus.com 33 5 61 93 66 30

DO-178B/ED-12B : Coordination pour la certification

- Objectif :
  - garantir une bonne communication/compréhension entre le postulant et l'autorité de certification



gerard.ladier@airbus.com 33 5 61 93 66 30

DO-178B/ED-12B : Coordination pour la certification

- Objectif :
  - garantir une bonne communication/compréhension entre le postulant et l'autorité de certification

- Moyens principaux :
  - Le Plan des Aspects Logiciels de la Certification, communiqué le plus tôt possible aux autorités
  - Des revues, menées par les spécialistes "logiciel" des autorités de certification à leur discrétion.

gerard.ladier@airbus.com 33 5 61 93 66 30

DO-178B/ED-12B : Coordination pour la certification

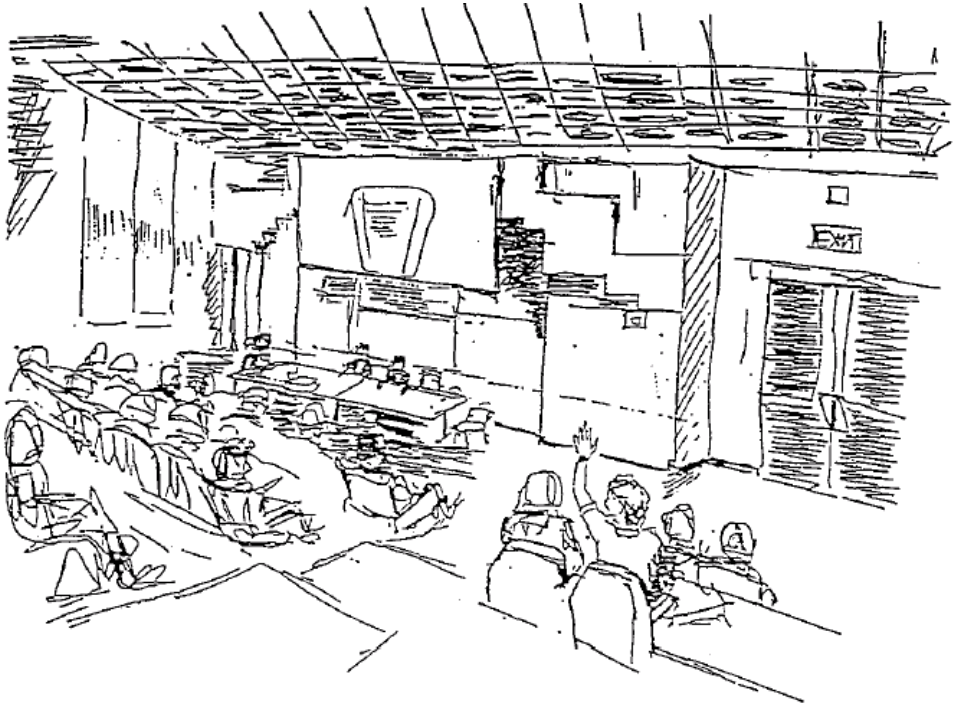
- Objectif :
  - garantir une bonne communication/compréhension entre le postulant et l'autorité de certification

- Moyens principaux :
  - Le Plan des Aspects Logiciels de la Certification, communiqué le plus tôt possible aux autorités
  - Des revues, menées par les spécialistes "logiciel" des autorités de certification à leur discrétion.

> Organisation industrielle interne spécifique, indépendante

gerard.ladier@airbus.com 33 5 61 93 66 30

Quatrième principe



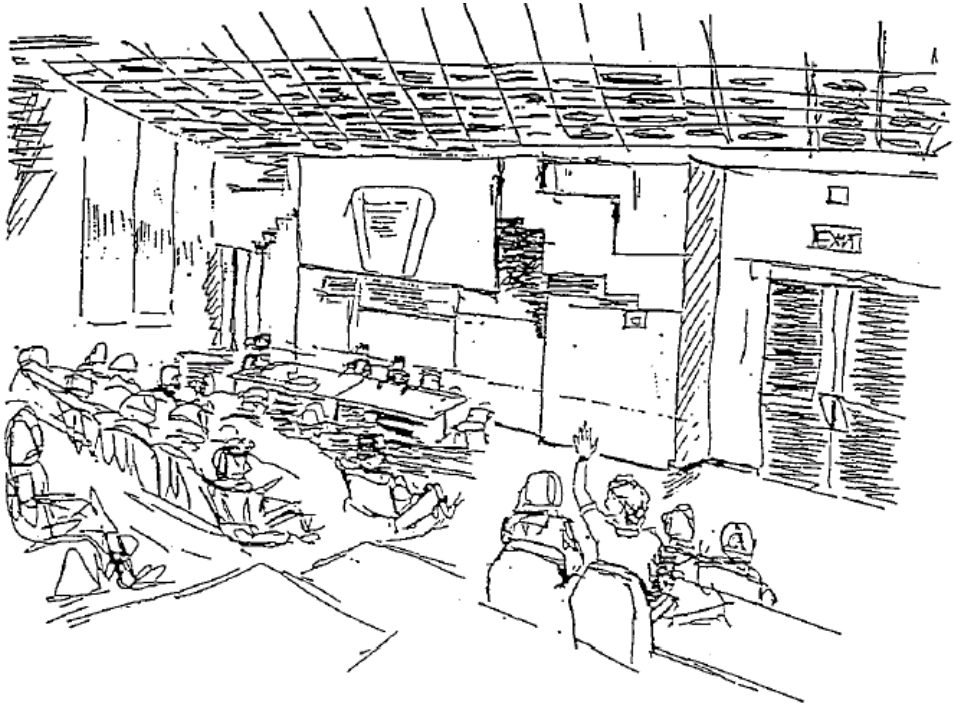
Consensus n. Collective opinion or concord; general agreement or accord. [Latin, from *consentire*, to agree]

Quatrième principe

Tous les intérêts doivent être pris en compte pour établir une norme reconnue de tous

⇒

Le recueil d'exigences est créé et modifié par tous les spécialistes et acteurs impliqués



Consensus n. Collective opinion or concord; general agreement or accord. [Latin, from *consentire*, to agree]

Consensus sur les exigences

Consensus sur les exigences

- Réunions conjointes entre 2 groupes RTCA SC-205 EUROCAE WG-71

Consensus sur les exigences

- Réunions conjointes entre 2 groupes RTCA SC-205 EUROCAE WG-71
- Ouverture, consensus :
  - plus de 1000 personnes inscrites sur le site WEB
  - plus de 120 acteurs par réunion ; avionneurs, motoristes, équipementiers, autorités, scientifiques et consultants spécialisés
  - Le texte final doit être agréé par TOUS les participants

Consensus sur les exigences

- Réunions conjointes entre 2 groupes RTCA SC-205 EUROCAE WG-71
- Ouverture, consensus :
  - plus de 1000 personnes inscrites sur le site WEB
  - plus de 120 acteurs par réunion ; avionneurs, motoristes, équipementiers, autorités, scientifiques et consultants spécialisés
  - Le texte final doit être agréé par TOUS les participants

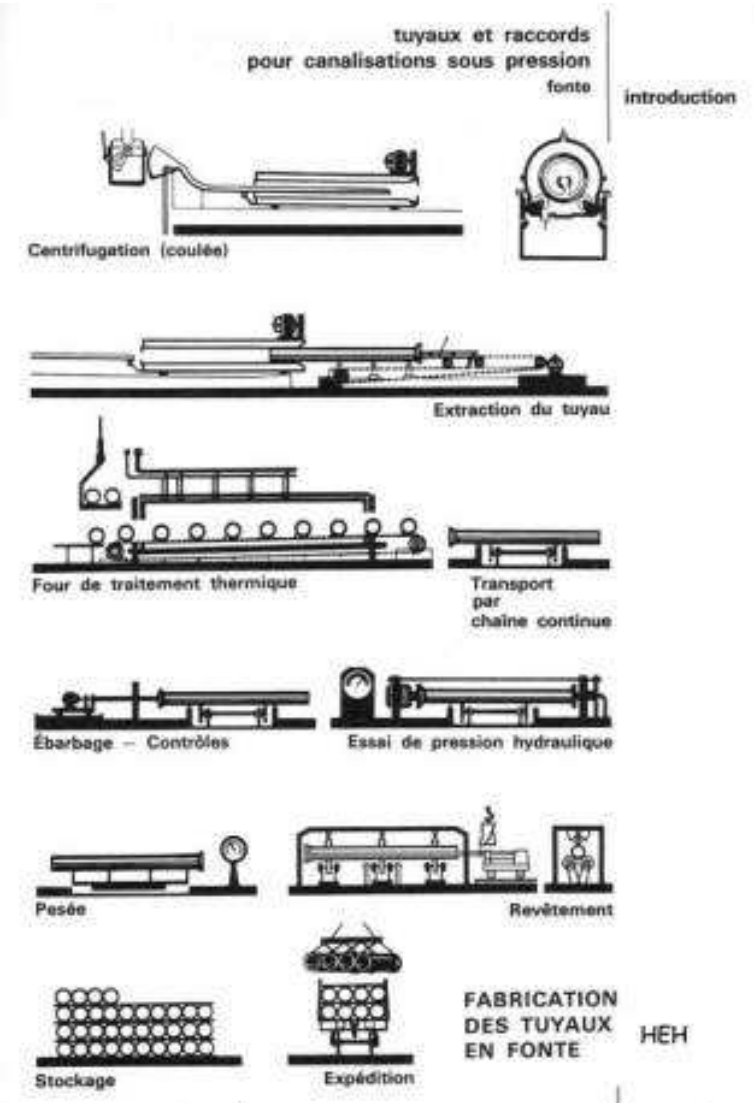
Consensus sur les exigences

- Réunions conjointes entre 2 groupes RTCA SC-205 EUROCAE WG-71
- Ouverture, consensus :
  - plus de 1000 personnes inscrites sur le site WEB
  - plus de 120 acteurs par réunion ; avionneurs, motoristes, équipementiers, autorités, scientifiques et consultants spécialisés
  - Le texte final doit être agréé par TOUS les participants
- Principaux thèmes discutés :
  - Qualification des outils,
  - Développement basé sur les modèles
  - Technologie Orientée Objet
  - Méthodes Formelles
  - Harmonisation bord / sol

Consensus sur les exigences

- Réunions conjointes entre 2 groupes RTCA SC-205 EUROCAE WG-71
- Ouverture, consensus :
  - plus de 1000 personnes inscrites sur le site WEB
  - plus de 120 acteurs par réunion ; avionneurs, motoristes, équipementiers, autorités, scientifiques et consultants spécialisés
  - Le texte final doit être agréé par TOUS les participants
- Principaux thèmes discutés :
  - Qualification des outils,
  - Développement basé sur les modèles
  - Technologie Orientée Objet
  - Méthodes Formelles
  - Harmonisation bord / sol
- Durée :
  - de Mars 2005
  - à Fin 2009

Cinquième principe

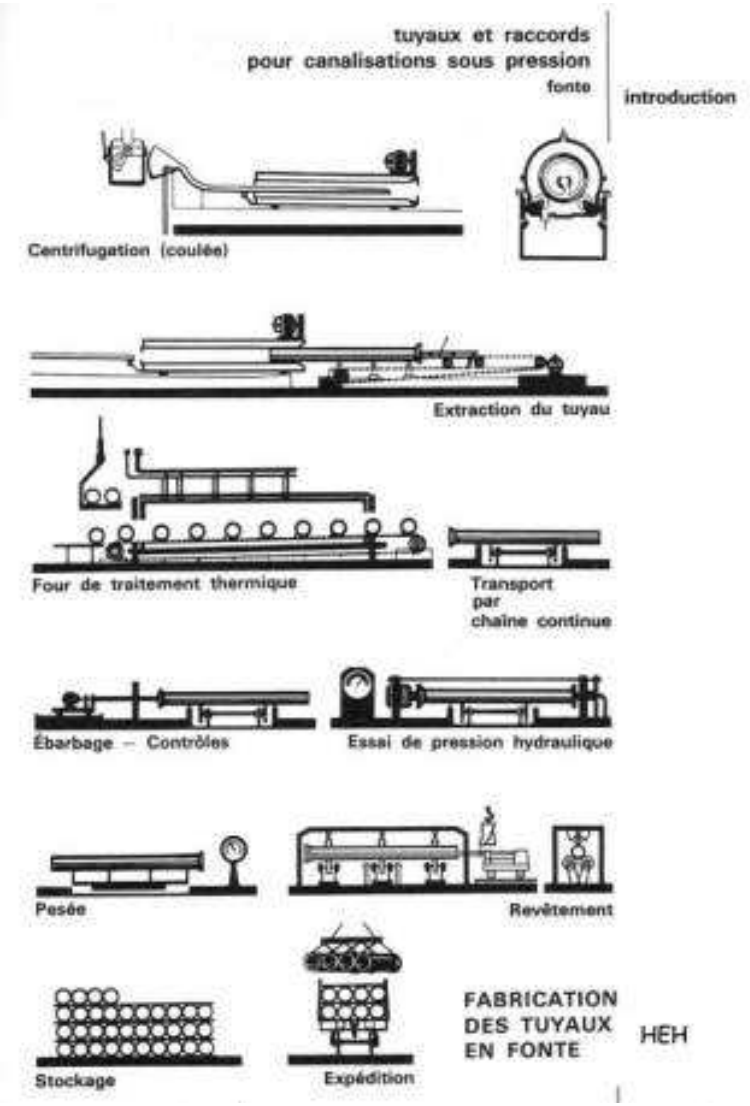


Cinquième principe

seules les exigences sont imposées, pas les moyens

⇒

la fabrication du « tuyau » est l'affaire des industriels



D’une approche traditionnelle…

… vers une grande automatisation des processus

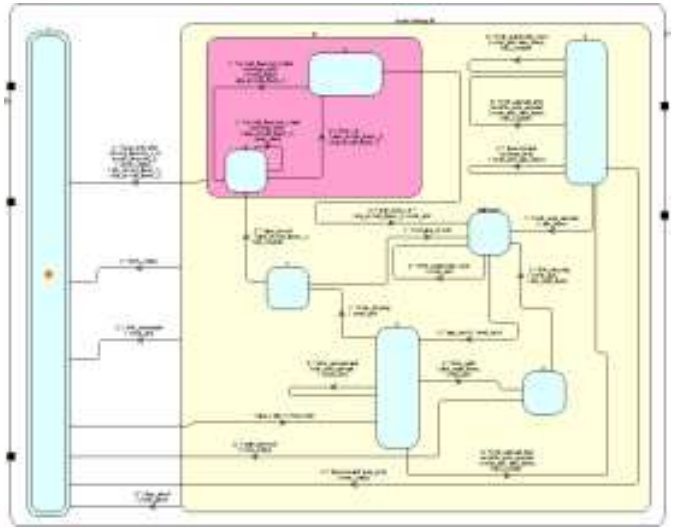
… Pour allier sécurité et efficacité

gerard.ladier@airbus.com 33 5 61 93 66 30

AIRBUS

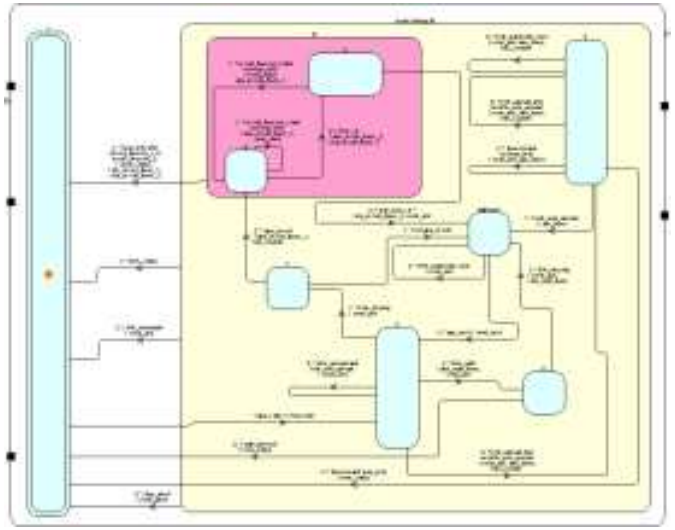
… vers une grande automatisation des processus

… Pour allier sécurité et efficacité



… vers une grande automatisation des processus

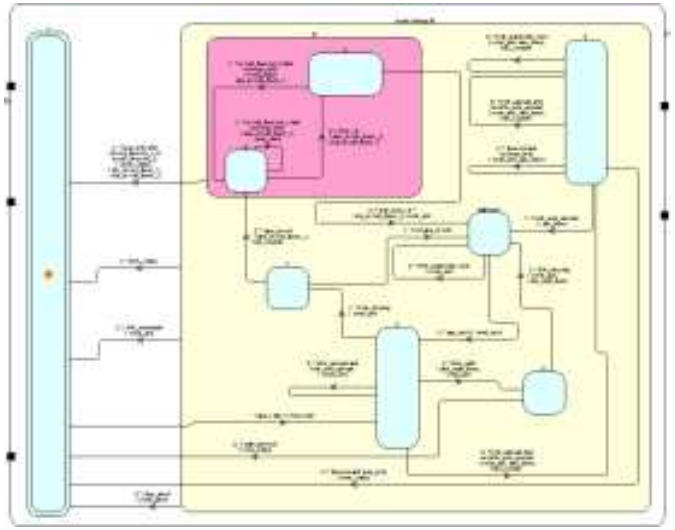
… Pour allier sécurité et efficacité



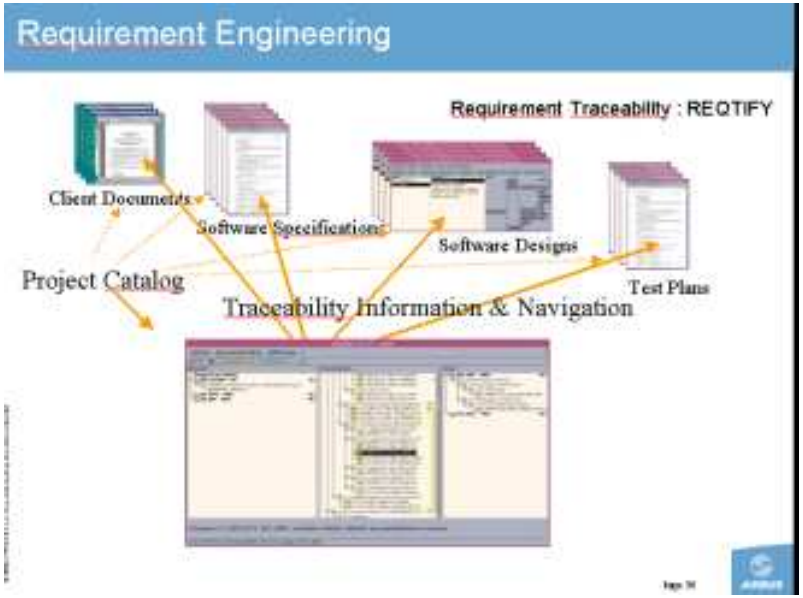
SCADE SUITE™

… vers une grande automatisation des processus

… Pour allier sécurité et efficacité

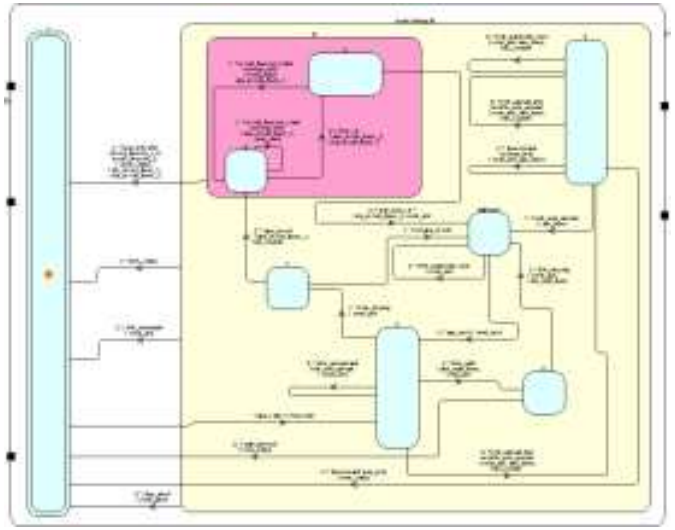


SCADE SUITE™

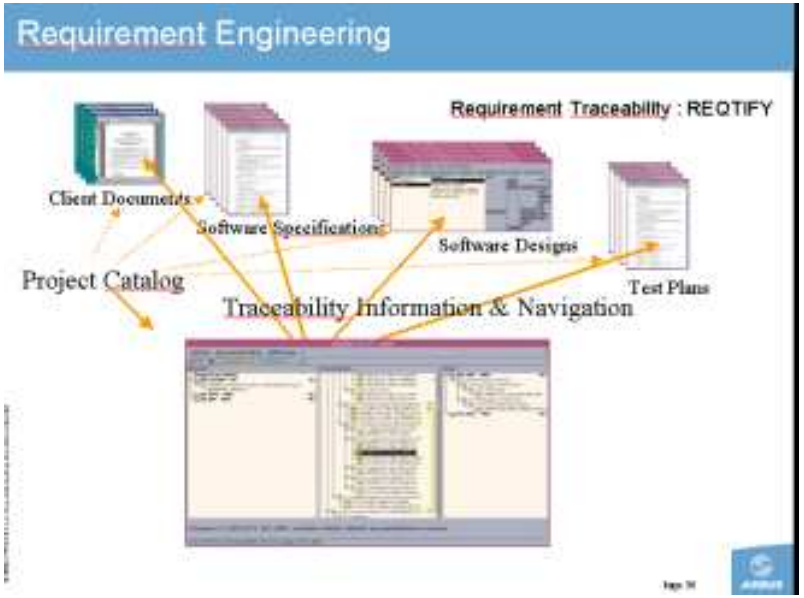


… vers une grande automatisation des processus

… Pour allier sécurité et efficacité

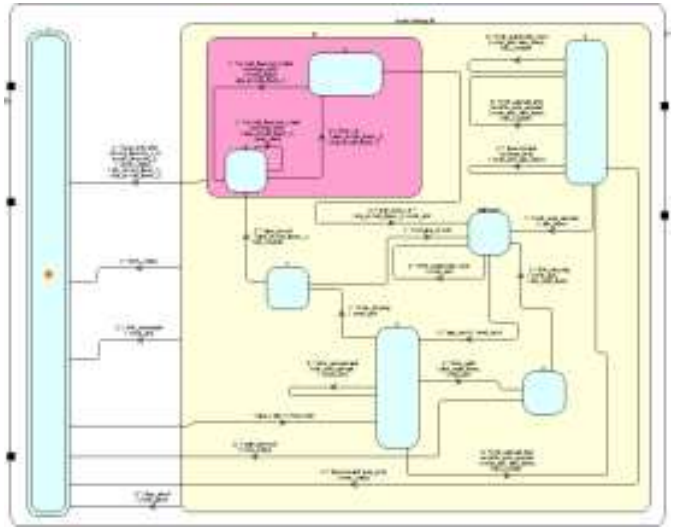


SCADE SUITE™

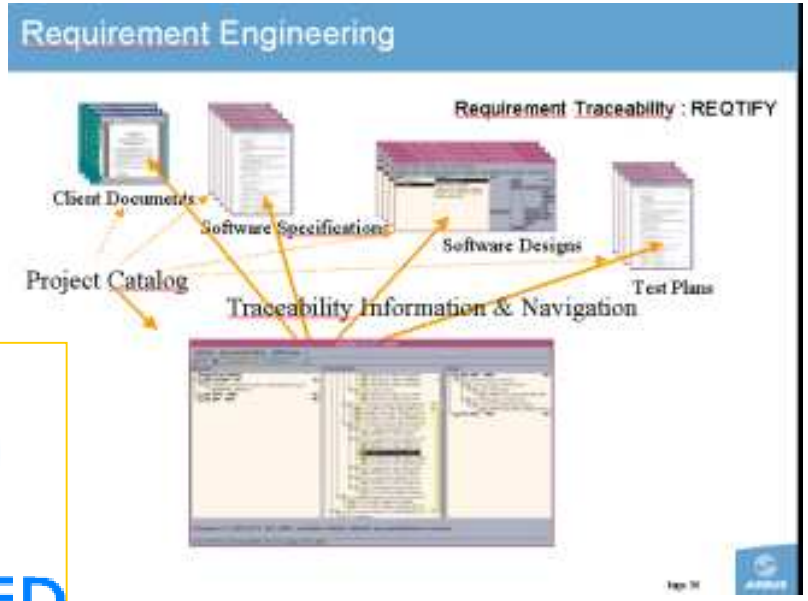


… vers une grande automatisation des processus

… Pour allier sécurité et efficacité



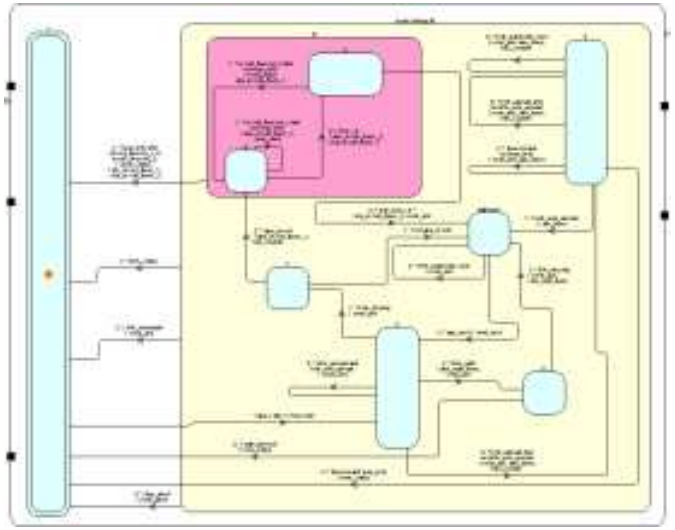
SCADE SUITE™



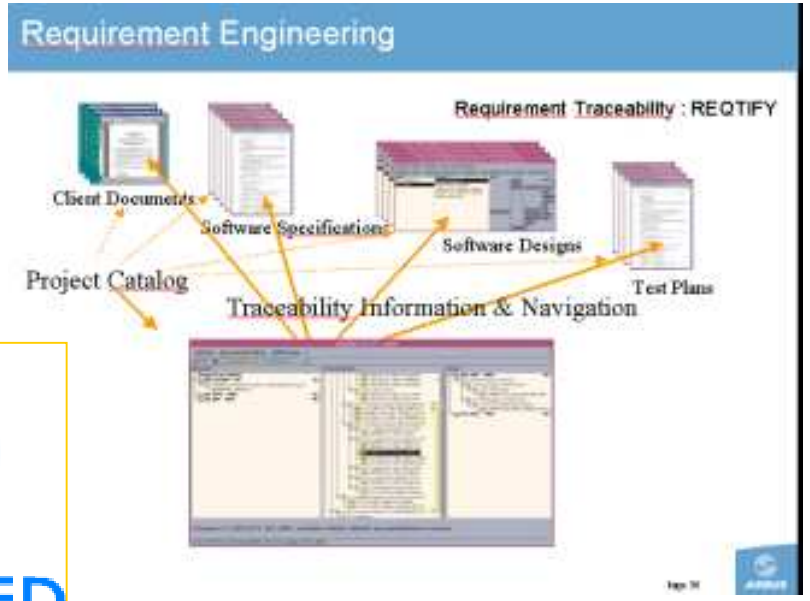
TOPCASED
The Open Source toolkit for critical systems

… vers une grande automatisation des processus

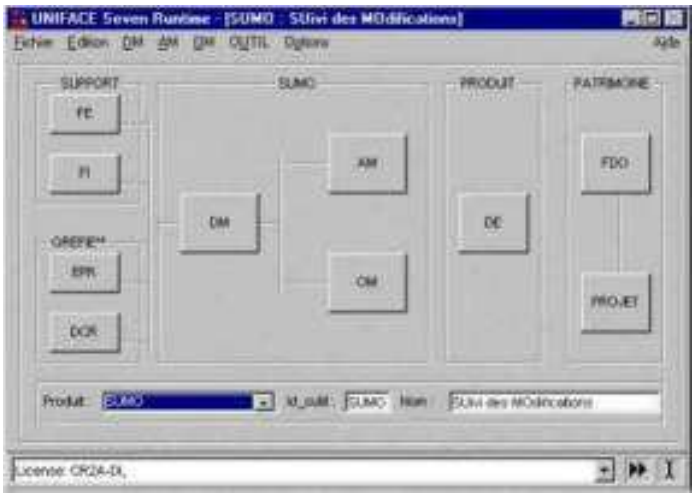
… Pour allier sécurité et efficacité



SCADE SUITE™



TOPCASED
The Open Source toolkit for critical systems



	Nb SLOC Manuel	Nb SLOC Auto
C1	219 316	
C2	150 100	1 087 555
C3	221 969	
C4	114 498	262 007
C5	130 000	276 220
C6	104 634	3 044 515
C7	99 361	
C8	32 836	1 347 293
C9	18 684	129 120
C10	13 571	85 784
Total	**1 104 969**	**6 232 494**
	7 337 463	

gerard.ladier@airbus.com 33 5 61 93 66 30

AIRBUS

En résumé, une ligne de code avionique est …

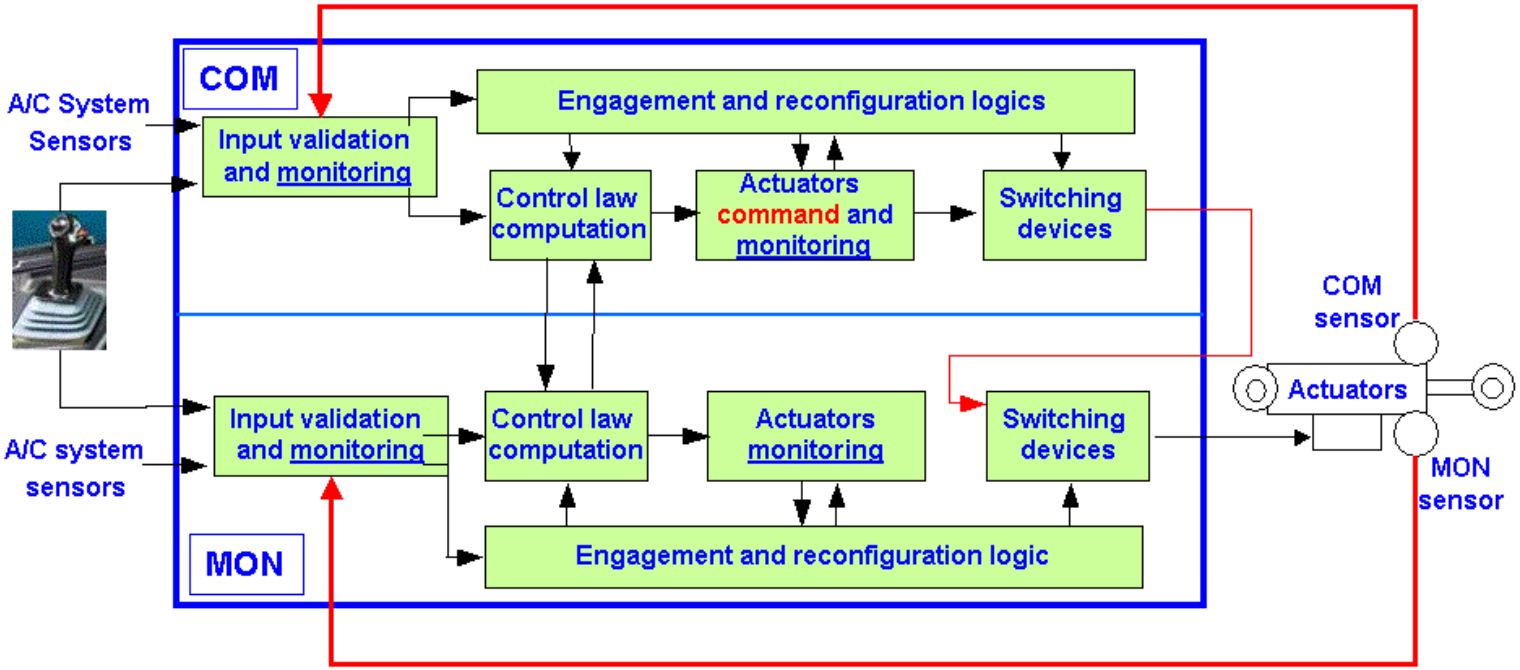
- Intégrée
  - Avec les autres lignes et avec le matériel
  - En garantissant l'absence de code mort
  - En vérifiant par revue cette intégration (complétude, correction)
- Testée par des jeux de tests
  - Établis en respectant des règles définies par des experts
    - approuvées par les équipes qualité/méthodes du développeur
    - contrôlées par les équipes qualité du constructeur
    - validées par les autorités de certification
  - Fondés sur les exigences
  - Couvrant toute la fonctionnalité
  - Avec des données dans et hors les plages de variation prévues
  - Vérifiés (analyse de couverture structurelle obtenue) avec indépendance
- Gérée en configuration/modification
  - En suivant des règles définies par des experts
    - approuvées par les équipes qualité/méthodes du développeur
    - contrôlées par les équipes qualité du constructeur
    - validées par les autorités de certification
  - En analysant les anomalies éventuelles pour améliorer les processus
- Développée avec des outils qualifiés
  - respectant eux-mêmes les exigences ci-dessus…

En résumé, une ligne de code avionique est …

- Spécifiée par une/des exigences
  - Allouées au logiciel par les spécifications du système
  - Établies en respectant des règles définies par des experts
    - approuvées par les équipes qualité/méthodes du développeur
    - contrôlées par les équipes qualité du constructeur
    - validées par les autorités de certification
  - Revues (conformité, cohérence, précision, compatibilité, vérifiabilité) avec indépendance
- Conçue par une/des exigences de conception
  - Tracée vers une/ou des exigences de spécification
  - Établies en respectant des règles définies par des experts
    - approuvées par les équipes qualité/méthodes du développeur
    - contrôlées par les équipes qualité du constructeur
    - validées par les autorités de certification
  - Revues (conformité, cohérence, précision, compatibilité, vérifiabilité) avec indépendance
- Codée
  - Pour réaliser les exigences de conception
  - en respectant des règles définies par des experts
    - approuvées par les équipes qualité/méthodes du développeur
    - contrôlées par les équipes qualité du constructeur
    - validées par les autorités de certification
- Revue (conformité, cohérence, précision, compatibilité, vérifiabilité) avec indépendance

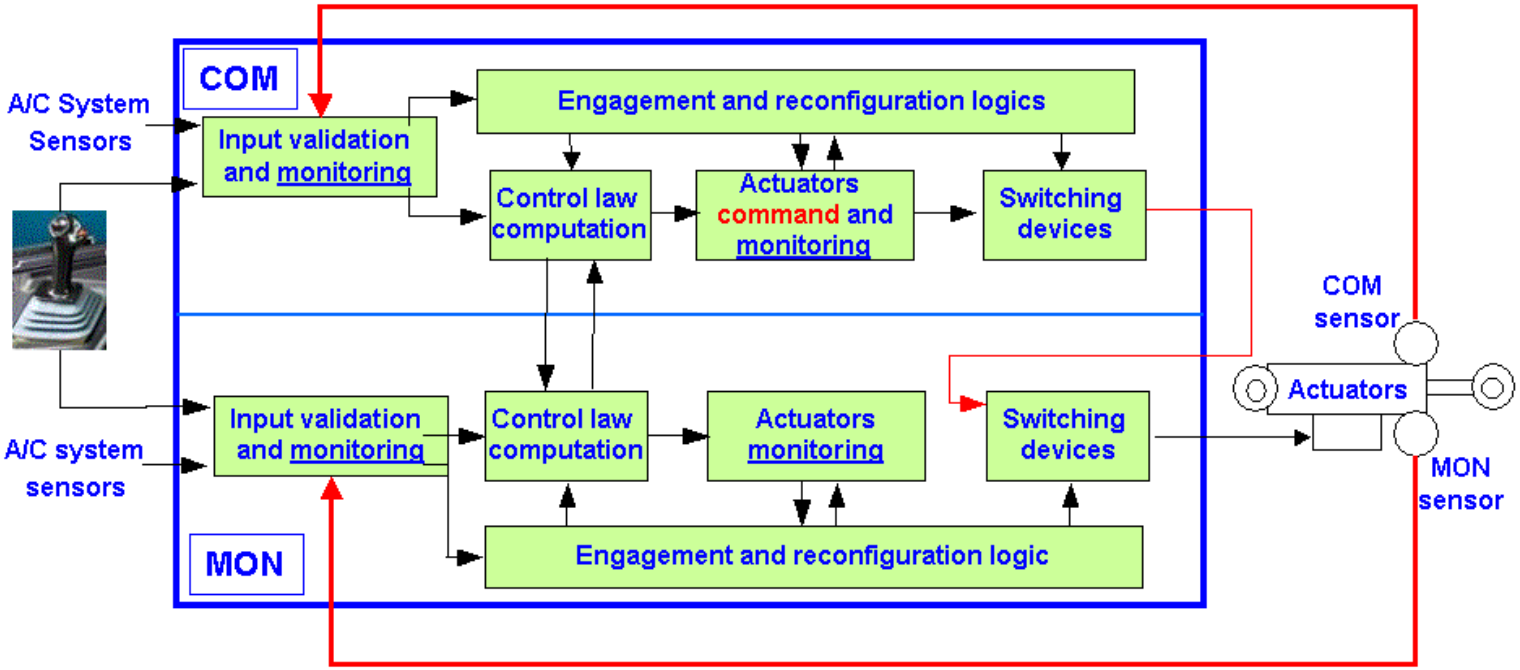
- Intégrée
  - Avec les autres lignes et avec le matériel
  - En garantissant l'absence de code mort
  - En vérifiant par revue cette intégration (complétude, correction)
- Testée par des jeux de tests
  - Établis en respectant des règles définies par des experts
    - approuvées par les équipes qualité/méthodes du développeur
    - contrôlées par les équipes qualité du constructeur
    - validées par les autorités de certification
  - Fondés sur les exigences
  - Couvrant toute la fonctionnalité
  - Avec des données dans et hors les plages de variation prévues
  - Vérifiés (analyse de couverture structurelle obtenue) avec indépendance
- Gérée en configuration/modification
  - En suivant des règles définies par des experts
    - approuvées par les équipes qualité/méthodes du développeur
    - contrôlées par les équipes qualité du constructeur
    - validées par les autorités de certification
  - En analysant les anomalies éventuelles pour améliorer les processus
- Développée avec des outils qualifiés
  - respectant eux-mêmes les exigences ci-dessus…

Mais en plus …



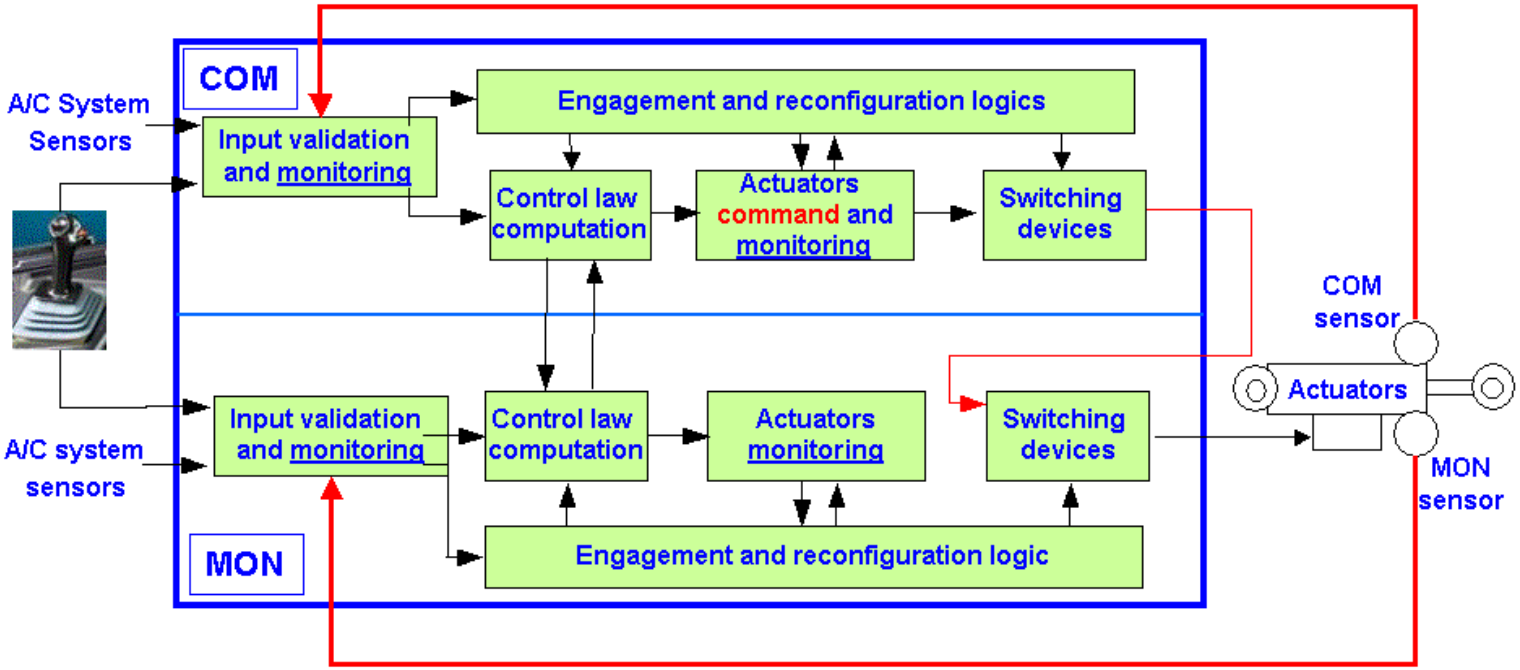
Mais en plus …

- On est très prudent au niveau des systèmes les plus critiques …



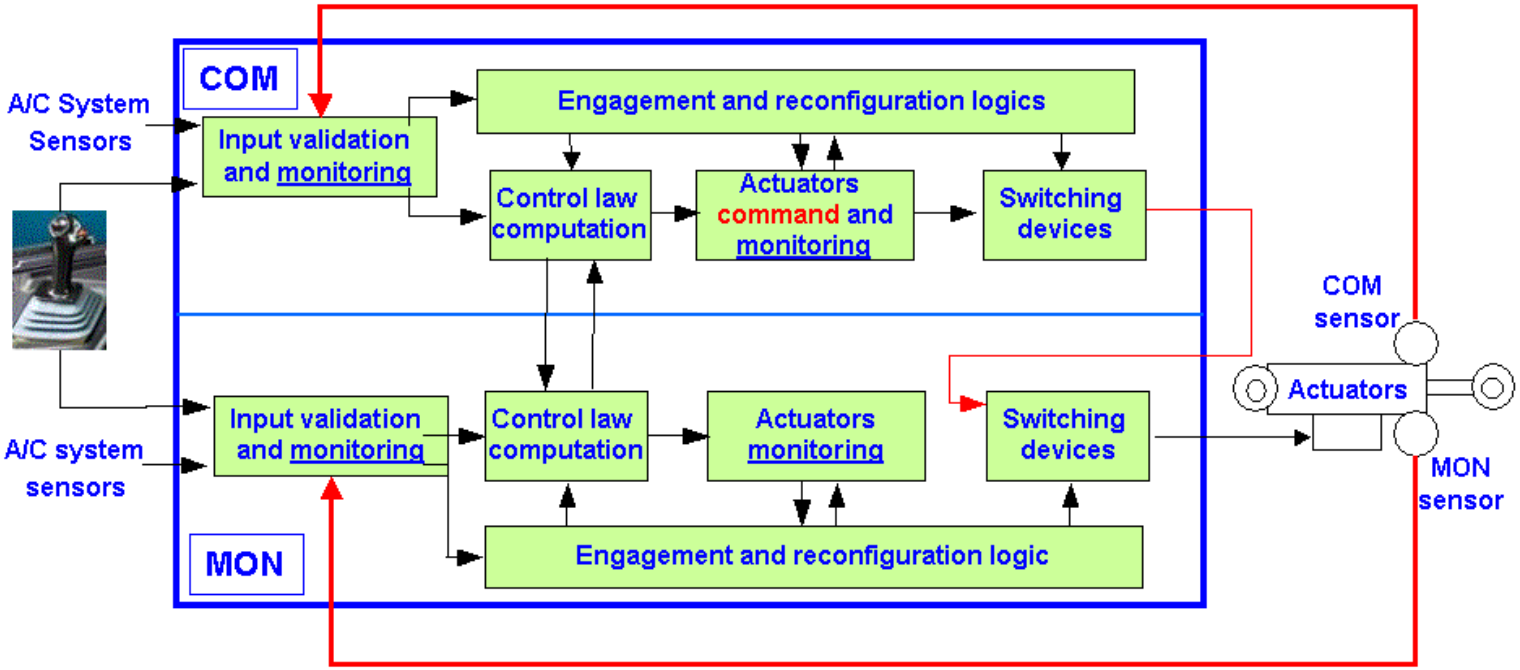
Mais en plus …

- On est très prudent au niveau des systèmes les plus critiques …
  - Logiciels et Matériels de niveau A



Mais en plus …

- On est très prudent au niveau des systèmes les plus critiques …
  - Logiciels et Matériels de niveau A
  - Architecture redondante



Et encore plus ….

Et encore plus ….

- Pour diminuer le risque d'une panne de mode commun, réalisation dissymétrique des calculateurs de CDVE d'Airbus :

Et encore plus ….

- Pour diminuer le risque d'une panne de mode commun, réalisation dissymétrique des calculateurs de CDVE d'Airbus :
  - Hardware :
    - Principe et conception
    - Composants (microprocesseurs, capacités, FPGA, résistances, …)

Et encore plus ….

- Pour diminuer le risque d'une panne de mode commun, réalisation dissymétrique des calculateurs de CDVE d'Airbus :
  - Hardware :
    - Principe et conception
    - Composants (microprocesseurs, capacités, FPGA, résistances, …)
  - Software
    - Générateurs de code
    - Compilateurs
    - Séquencement des tâches
    - Etc.

Et encore plus ….

- Pour diminuer le risque d'une panne de mode commun, réalisation dissymétrique des calculateurs de CDVE d'Airbus :
  - Hardware :
    - Principe et conception
    - Composants (microprocesseurs, capacités, FPGA, résistances, …)
  - Software
    - Générateurs de code
    - Compilateurs
    - Séquencement des tâches
    - Etc.
  - Processus de fabrication

Le résultat …. sur le cycle de développement

gerard.ladier@airbus.com 33 5 61 93 66 30

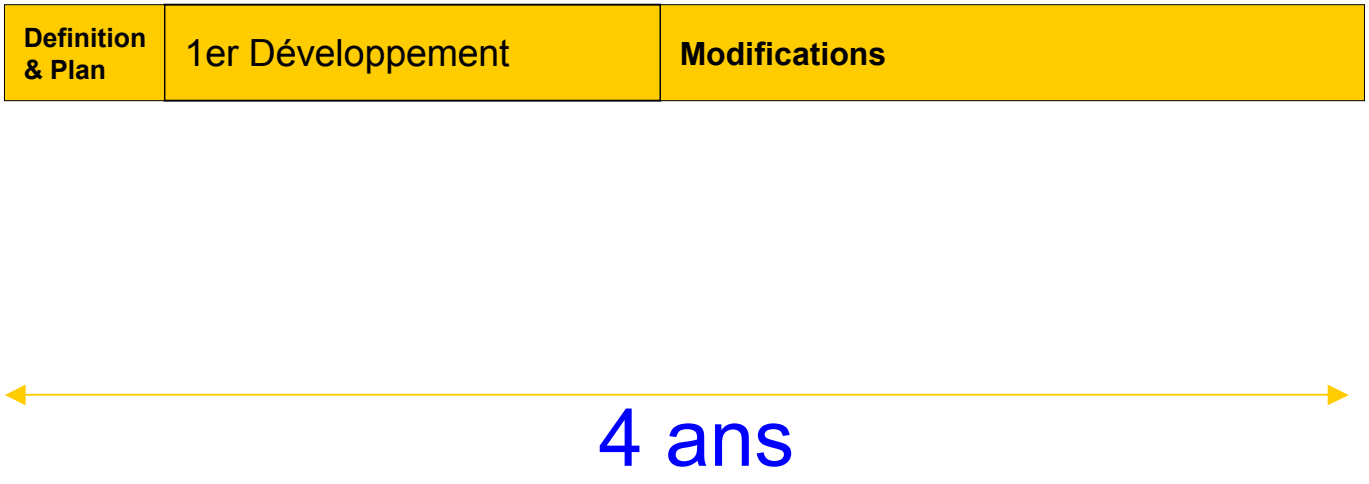
Le résultat …. sur le cycle de développement

Definition & Plan	1er Développement	Modifications

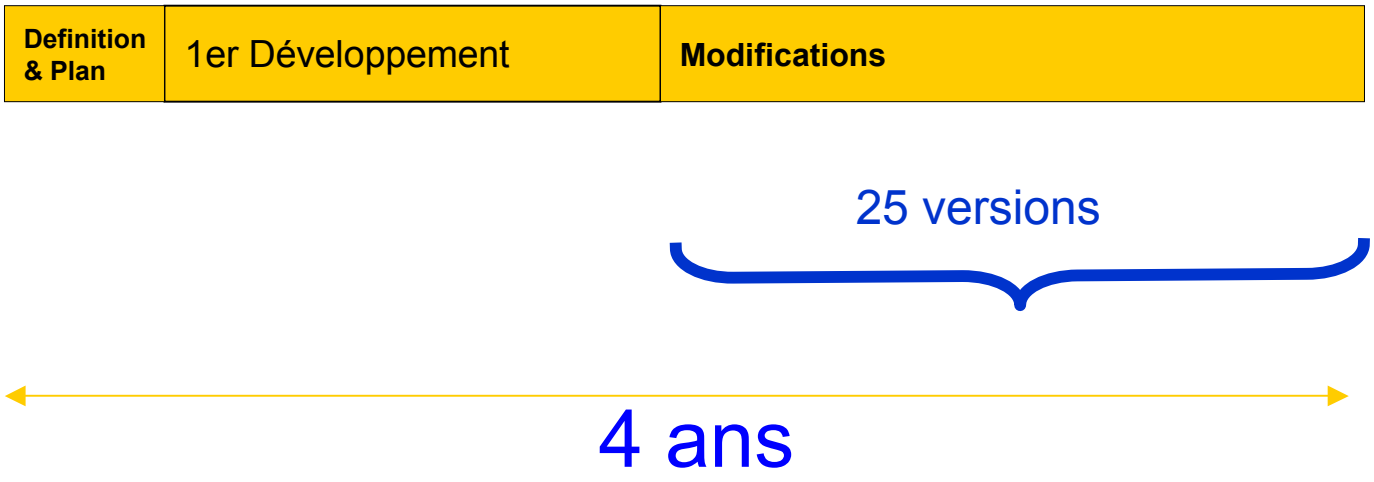
gerard.ladier@airbus.com 33 5 61 93 66 30

AIRBUS

Le résultat …. sur le cycle de développement



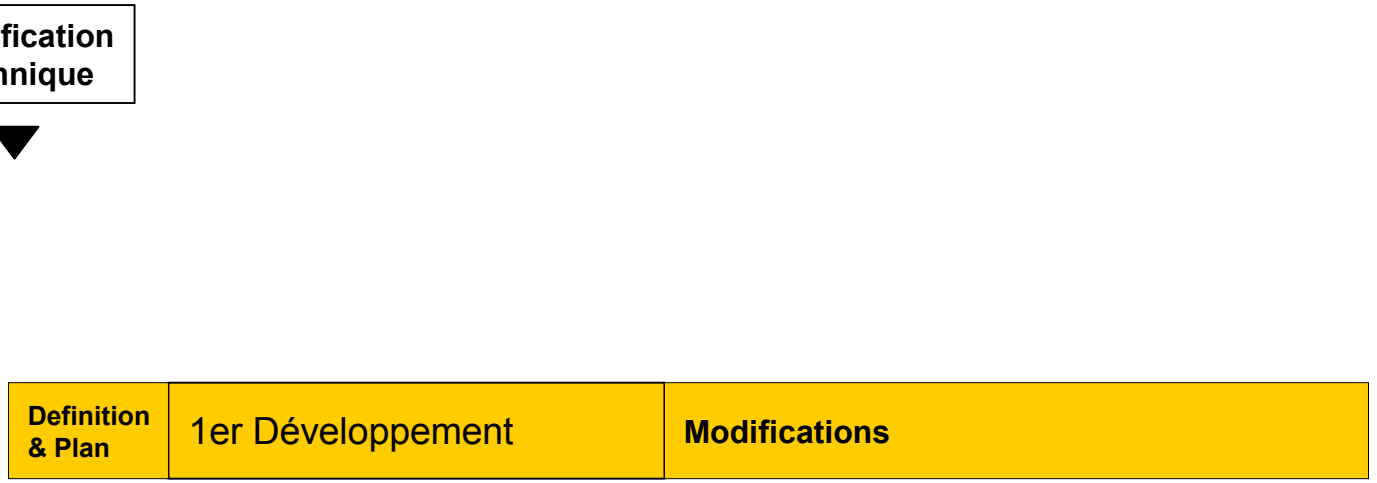
Le résultat …. sur le cycle de développement



Le résultat …. sur le cycle de développement

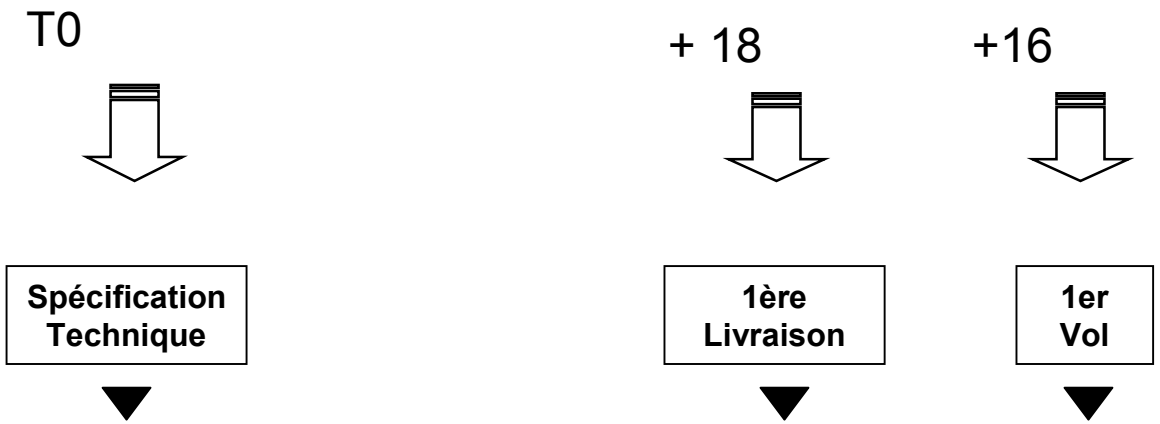
T0

Spécification Technique

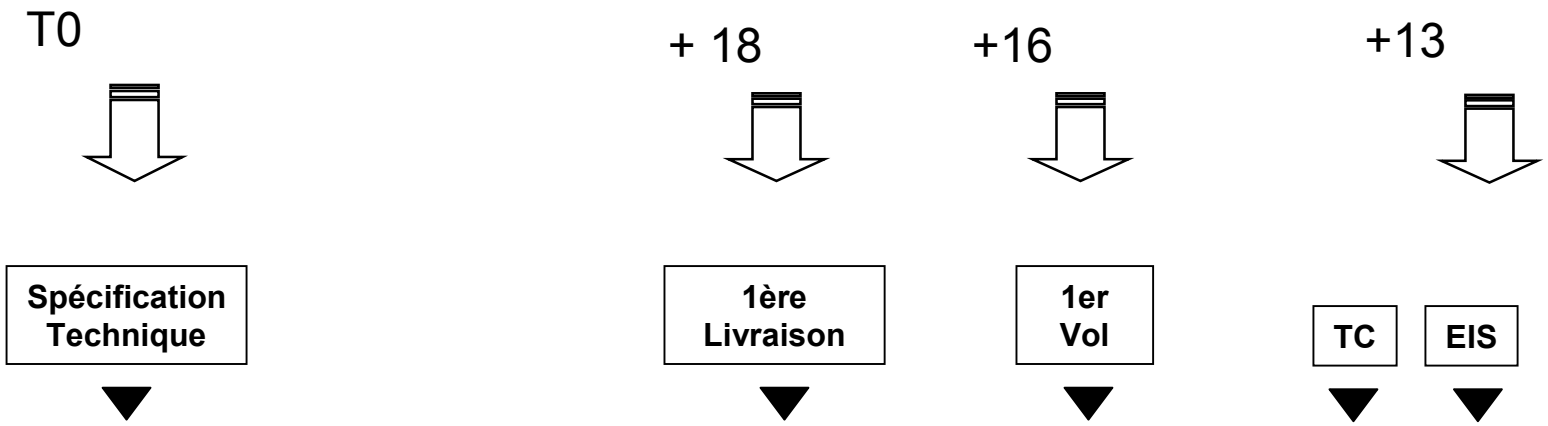


Le résultat …. sur le cycle de développement

Le résultat …. sur le cycle de développement



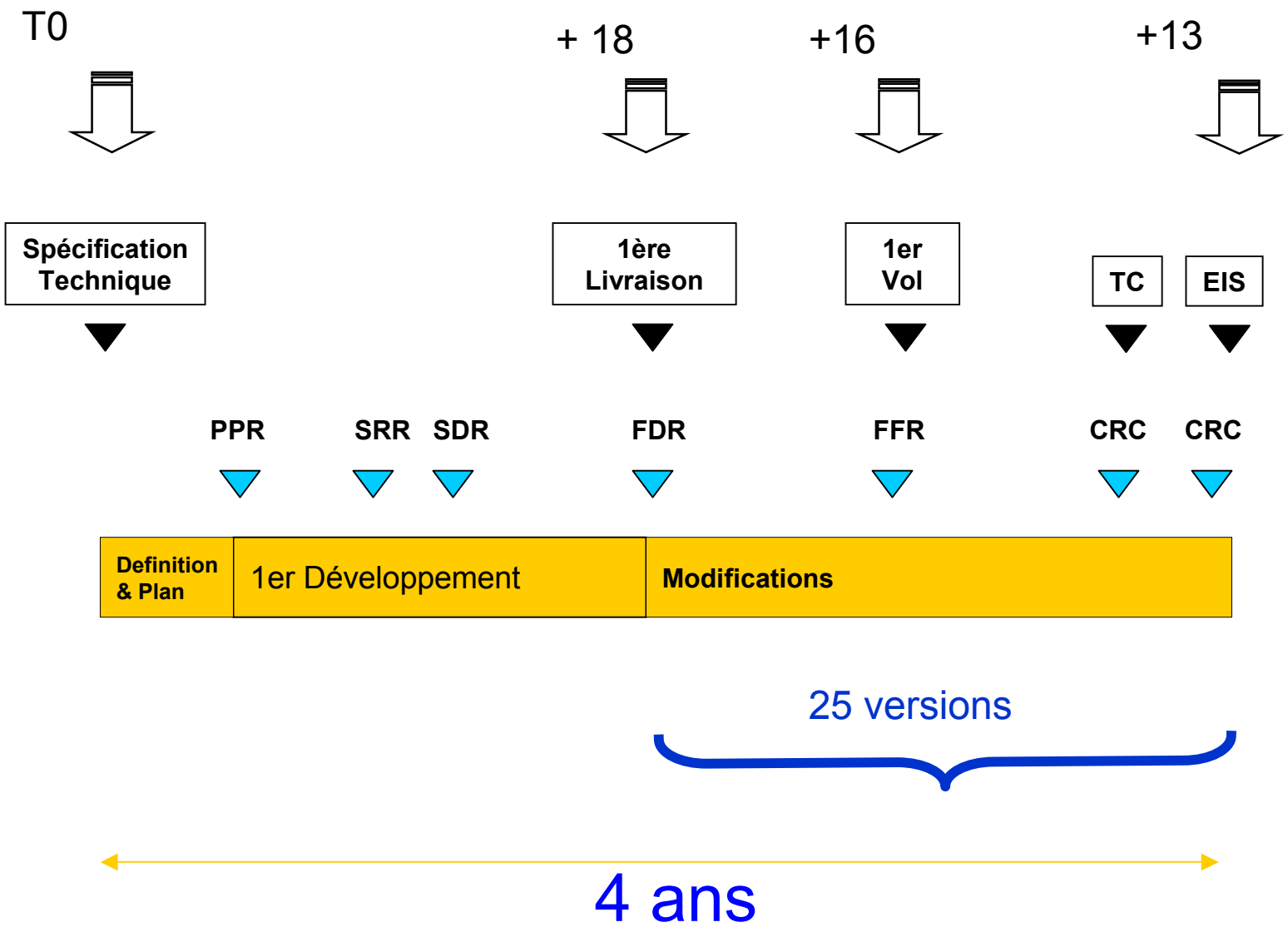
Le résultat …. sur le cycle de développement



25 versions

4 ans

Le résultat …. sur le cycle de développement



Le résultat …. sur la sécurité

Le résultat …. sur la sécurité

En général :

Le résultat …. sur la sécurité

En général :

Le résultat …. sur la sécurité

En général :

- En particulier : SEC famille A320

Le résultat …. sur la sécurité

En général :

- En particulier : SEC famille A320

Le résultat …. sur la sécurité

- En particulier : SEC famille A320
  - 1 er vol : 22 Février 1987

Le résultat …. sur la sécurité

- En particulier : SEC famille A320
  - 1 er vol : 22 Février 1987
  - 3333 avions en opération

Le résultat …. sur la sécurité

En général :

- En particulier : SEC famille A320
  - 1 er vol : 22 Février 1987
  - 3333 avions en opération
  - 50 000 000 + heures de vol

Le résultat …. sur la sécurité

- En particulier : SEC famille A320
  - 1 er vol : 22 Février 1987
  - 3333 avions en opération
  - 50 000 000 + heures de vol
  - ~ 100. 000 lignes de code

Le résultat …. sur la sécurité

- En particulier : SEC famille A320
  - 1 er vol : 22 Février 1987
  - 3333 avions en opération
  - 50 000 000 + heures de vol
  - ~ 100. 000 lignes de code
  - 0 bug détecté en vol

Et après ?

Et après ?

Et après ?

- Réglementation :

Et après ?

- Réglementation :
  - DO-178C/ED-12C à partir de 2010

Et après ?

- Réglementation :
  - DO-178C/ED-12C à partir de 2010
  - Introduction plus simple d'approches nouvelles

Et après ?

- Réglementation :
  - DO-178C/ED-12C à partir de 2010
  - Introduction plus simple d'approches nouvelles
  - Homogénéisation progressive des règlements bord / sol

Et après ?

- Réglementation :
  - DO-178C/ED-12C à partir de 2010
  - Introduction plus simple d'approches nouvelles
  - Homogénéisation progressive des règlements bord / sol
- Approches de développement :

Et après ?

- Réglementation :
  - DO-178C/ED-12C à partir de 2010
  - Introduction plus simple d'approches nouvelles
  - Homogénéisation progressive des règlements bord / sol
- Approches de développement :
  - Généralisation d'une ingénierie "basée sur le calcul" :
    - Génération automatique de code
    - Vérification automatisée de modèles
    - Preuves mathématiques (formelles)

Et après ?

- Réglementation :
  - DO-178C/ED-12C à partir de 2010
  - Introduction plus simple d'approches nouvelles
  - Homogénéisation progressive des règlements bord / sol

- Approches de développement :
  - Généralisation d'une ingénierie "basée sur le calcul" :
    - Génération automatique de code
    - Vérification automatisée de modèles
    - Preuves mathématiques (formelles)
  - Permettant un passage progressif vers une assurance « basée produit »