astrium

Justification de sûreté de fonctionnement des logiciels spatiaux, évolution vers la certification

Jean-Paul Blanquart, Jean-François Muller

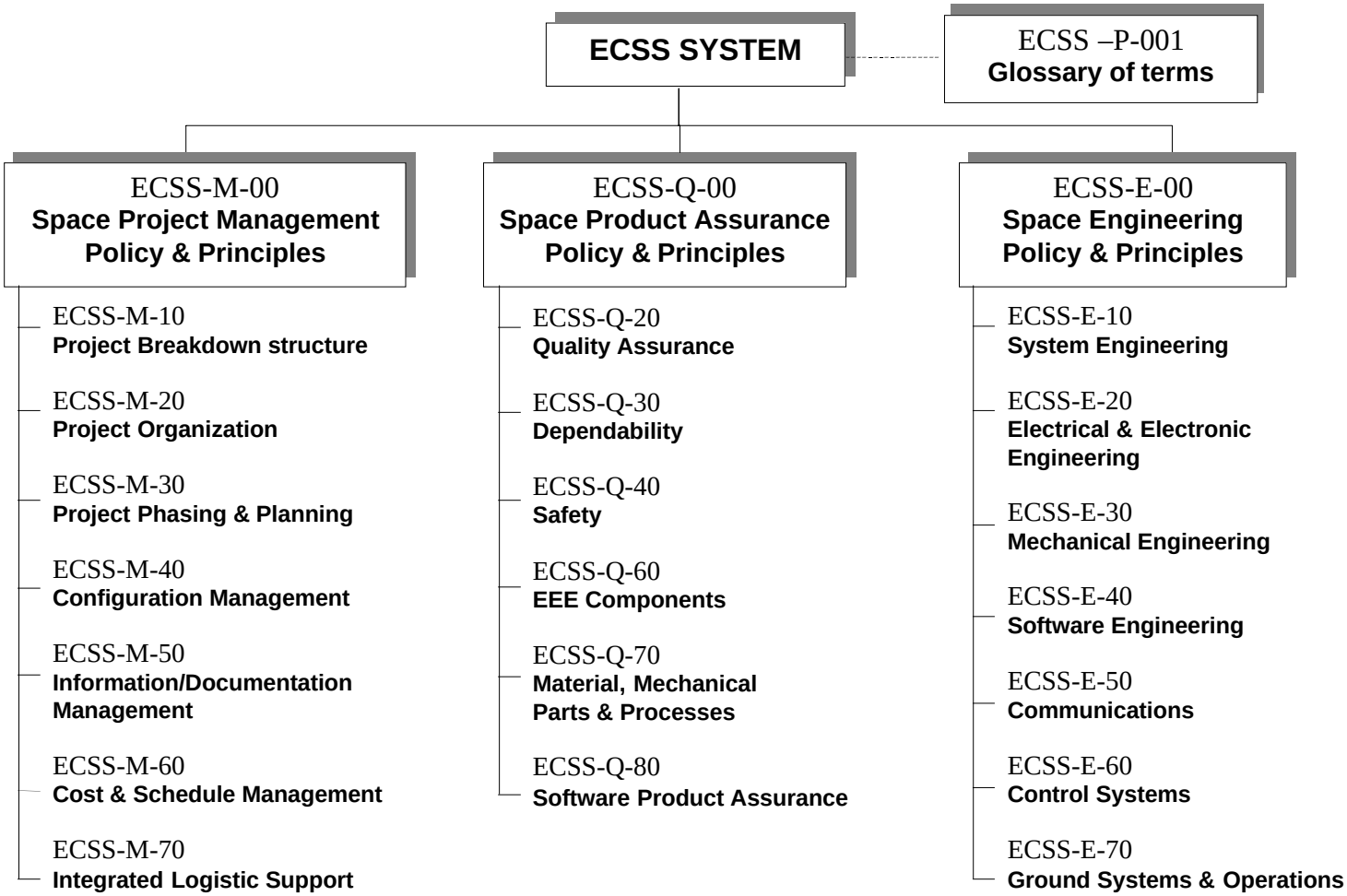
Toulouse, 18 mars 2003

5ème atelier « Justification de la sûreté de fonctionnement: approches industrielles, méthodes de construction et structure ».
Réseau d'Ingénierie de la Sûreté de fonctionnement

Logiciel spatial: justification de sûreté

- **Cadre réglementaire: les « ECSS » (European Cooperation for Space Standardization)**
- **Relation bi-partite client-fournisseur**
- **Cadre général:**
  - Adaptations négociées par projet
  - Evolutions:
    - Discussions
    - Etudes
    - Groupes de travail
    - Revues

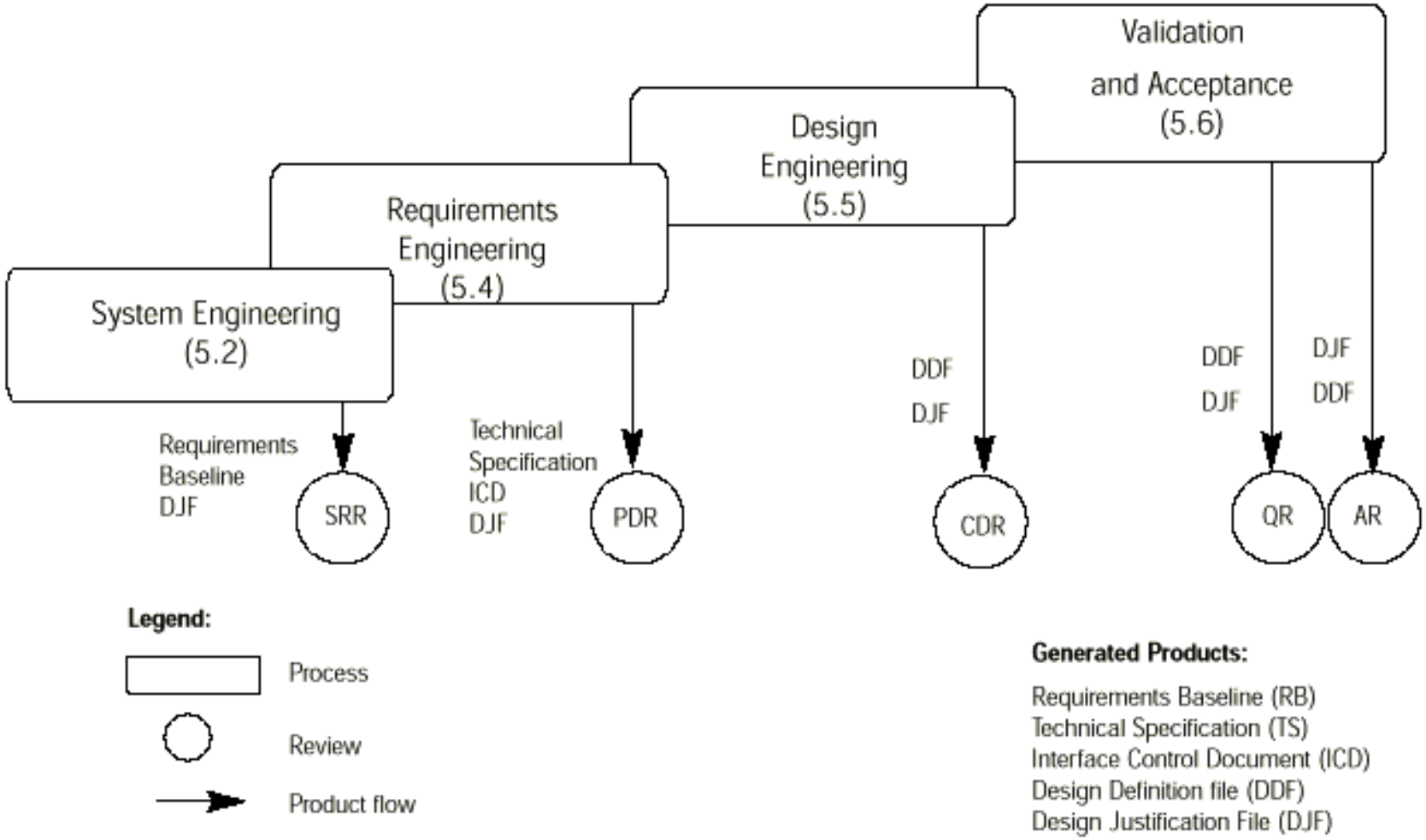
Standards pour l'espace: ECSS



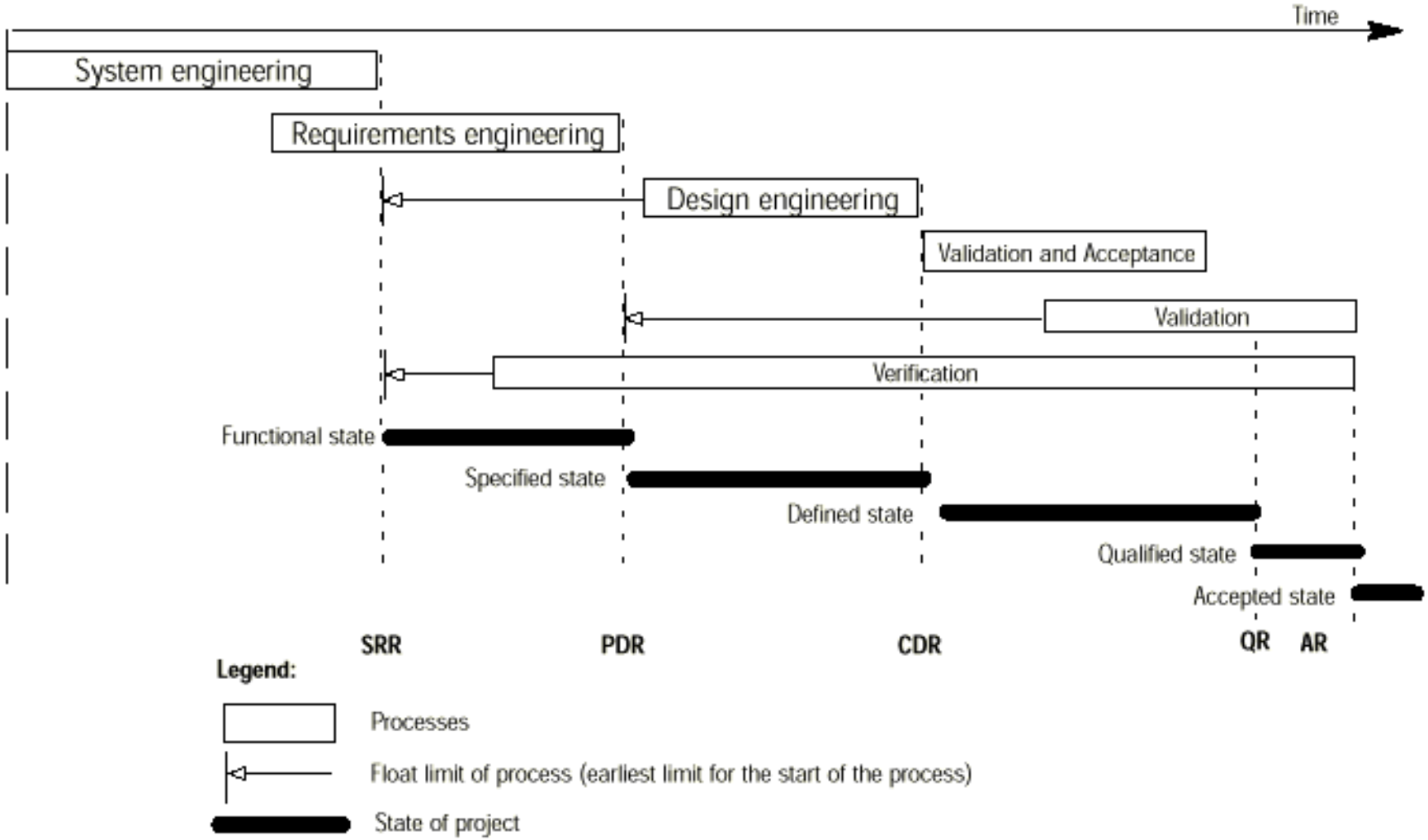
Principes généraux

- **Hiérarchie**
- **Processus**
  - Primaires
    - Acquisition, fourniture, développement, opération, maintenance
  - Support
    - Documentation, gestion de configuration, assurance qualité, vérification, validation
  - Organisation
    - Gestion, infrastructure, amélioration, formation
- **Points clés, revues**
- **Documentation**
- **Méthodes**

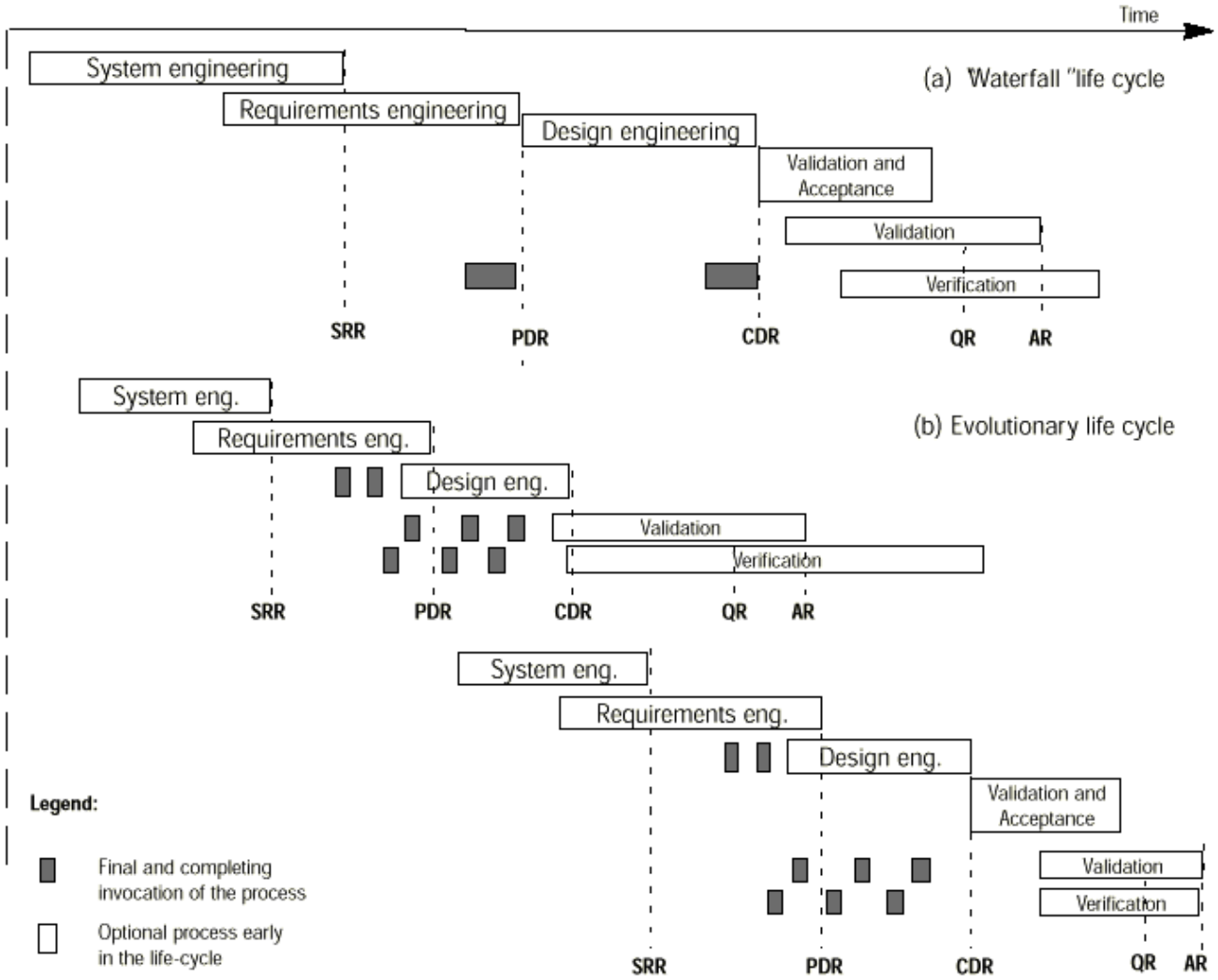
Processus du développement et revues



Les contraintes sur le cycle de vie



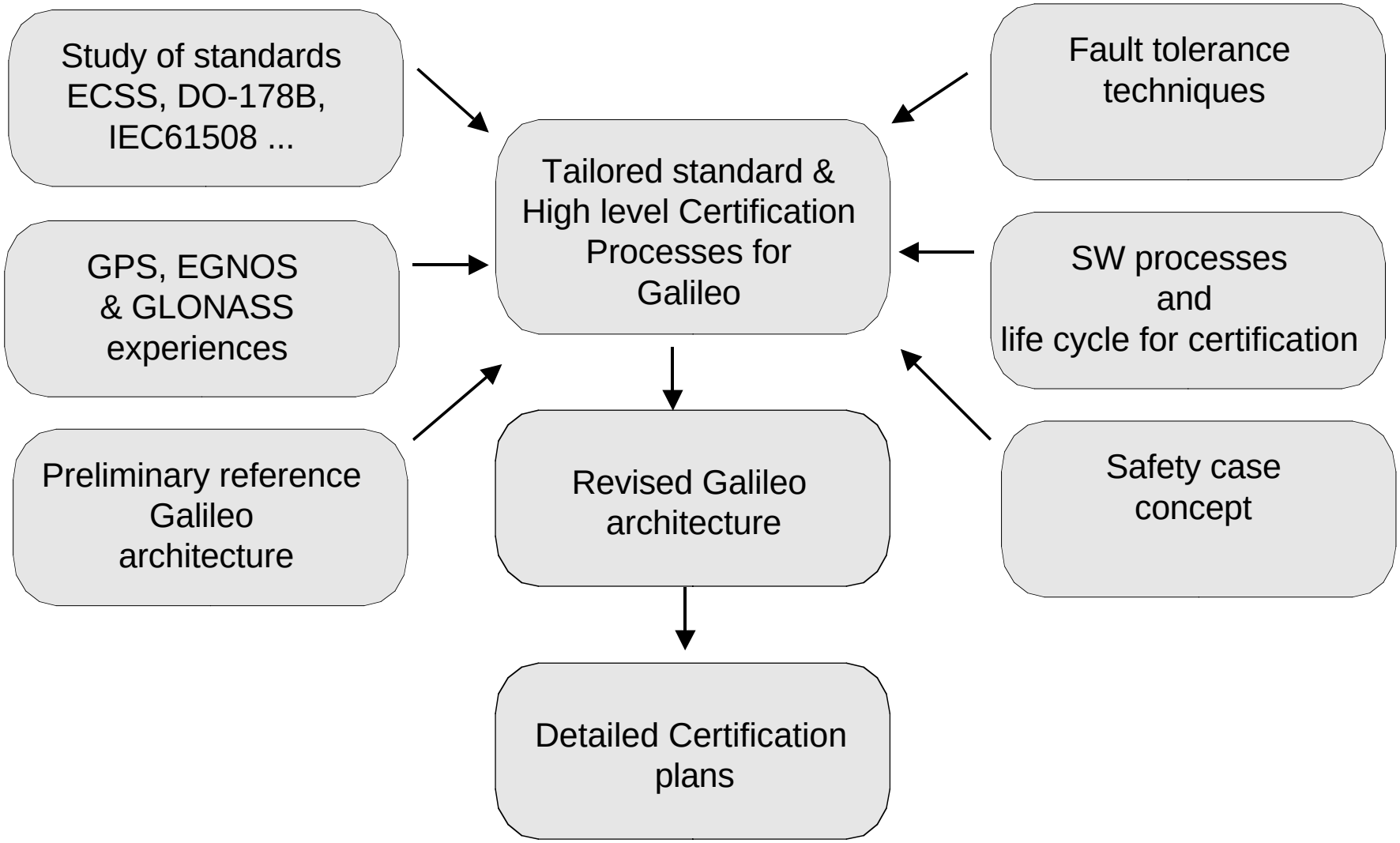
Plusieurs cycles possibles



Logiciels spatiaux et certification: GNSS

- **Un service basé sur un système spatial (positionnement)**
- **Pour des applications critiques:**
  - Exemple: support à l'aviation civile
- **Certification vis à vis d'une autorité tierce, existante**
- **Aspects logiciels**
- **Etude « GNSS-2/Galileo System Software Certification »**
  - Etude ESA (ESTEC)
  - DNV, Astrium, Airbus, CSI, Isoscope, LAAS-CNRS
  - 2000-2001

Logique de l’étude



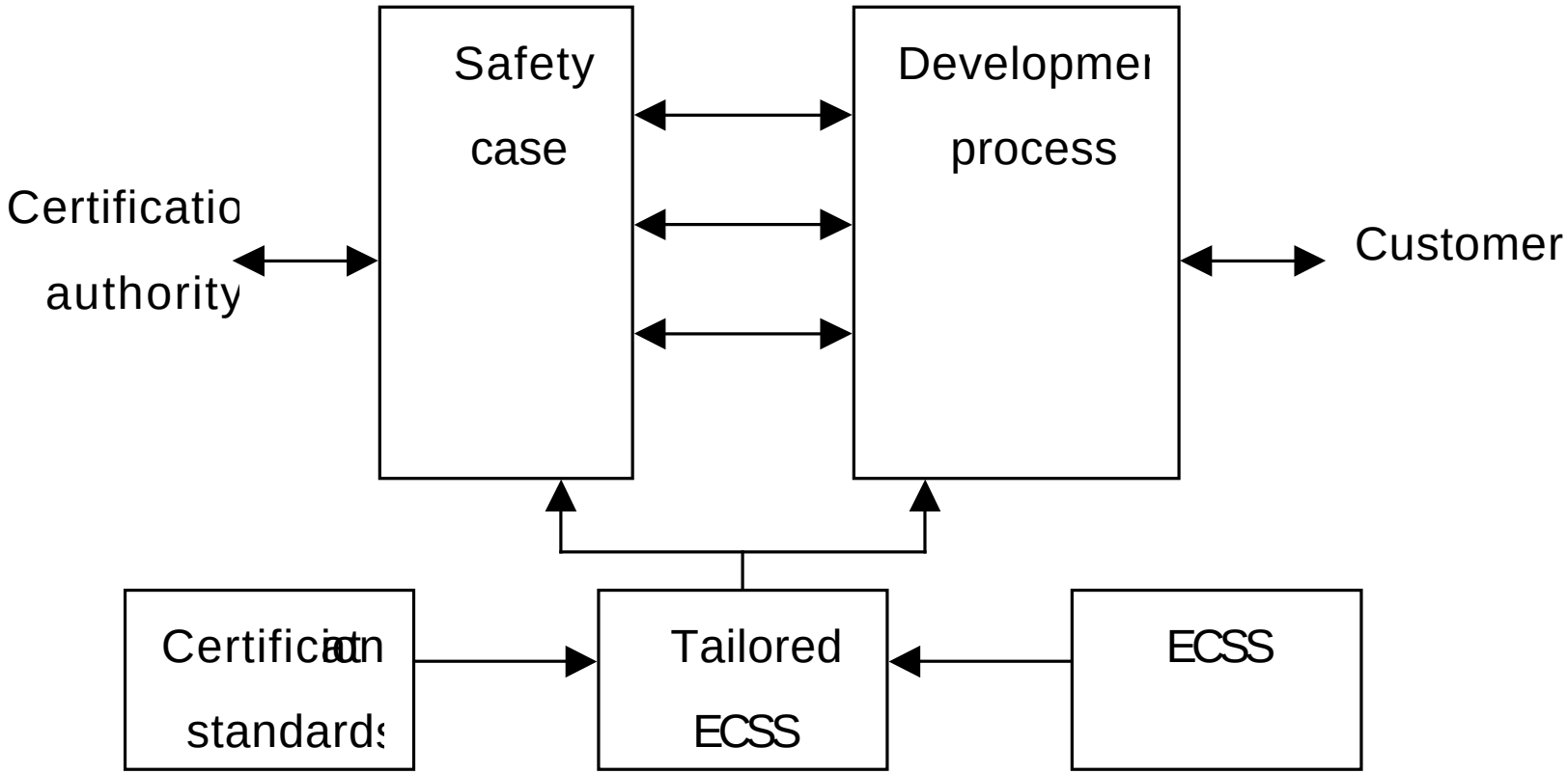
Adaptations spécifiques du standard

Normative requirements	Software types / Software Classes	All	1		2			3		4		5		6		7	
			B	C	A	B	C	B	C	C	D	B	C	B	C	D	E
…																	
5.1.6 Software Safety Case Manager																	
5.1.6.N1																	
One person shall be appointed as Software Safety Case Manager for the project.			X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
The Software Safety Case Manager shall be different from the software product assurance manager			X		X	X		X				X		X			
The software product assurance manager may be appointed as Software Safety Case Manager.				X			X		X	X	X		X		X	X	X
…																	
5.3.3 Audits																	
ECSS-Q-20 clause 2.6 is applicable.																	
5.3.3.N1																	
The Software Safety Case Manager shall perform software safety audits to verify compliance of the project with safety requirements and policies. Audits may lead to identify safety related issues or errors that were not uncovered through normal product assurance or verification and validation activities.			X	X	X	X	X	X	X	X		X	X	X	X		
5.3.3.N2																	
Synthesis of audit results may be included by the Software Safety Case Manager for integration to the Software Safety Case.			X	X	X	X	X	X	X	X		X	X	X	X		
…																	

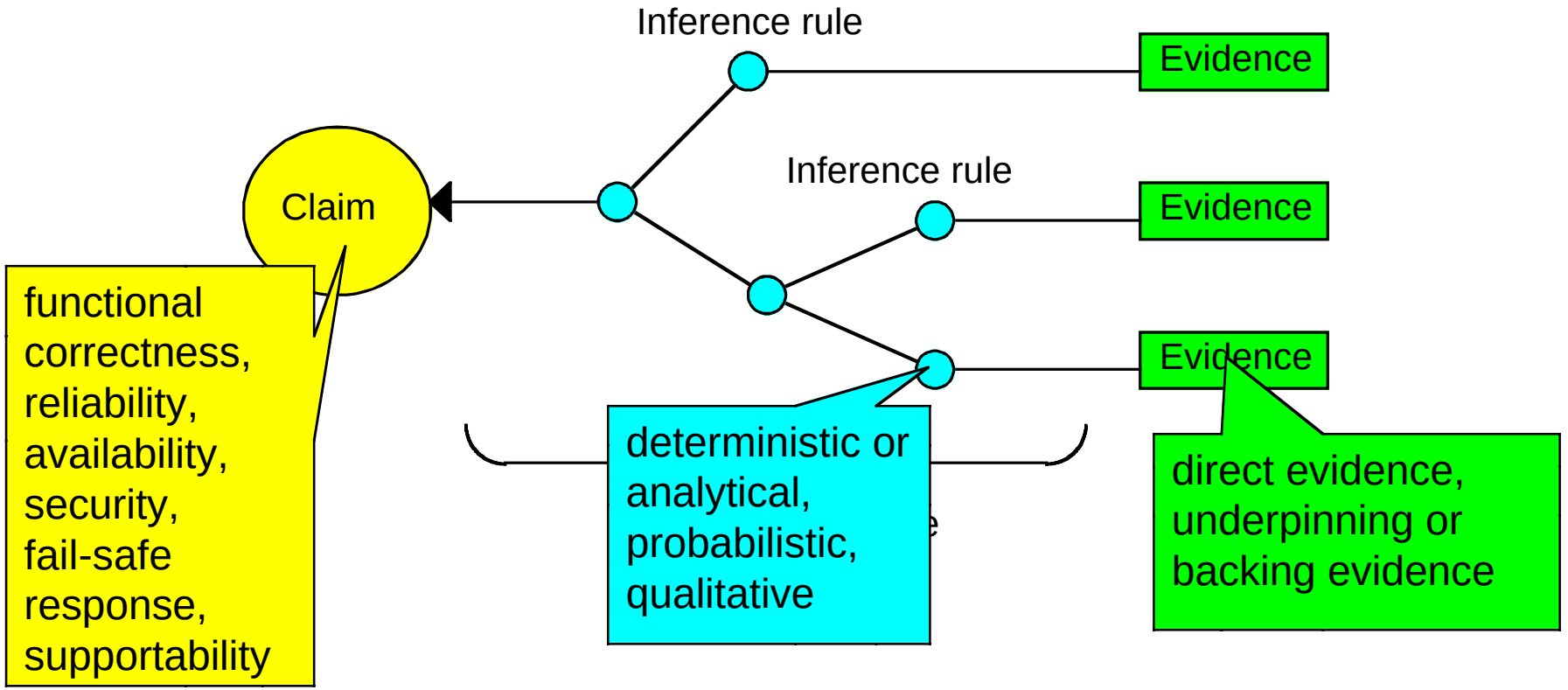
L’étude CARES

- **« Certification Assessment Requirements for ESA Software »**
- **Approche générale**
  - Domaines
  - Services
  - Systèmes
- **Processus et méthodes pour logiciels de systèmes spatiaux critiques**
- **Accréditation d’organismes**
- **Etude ESA (ESTEC), Astrium-Adelard-Airbus-Critical SW-DNV, 2001-2003**

CARES



Approche « Safety Case »



Analyse des standards

- DO 178B / ED12B
- IEC 61508
- MoD 00/55, 00/56
- CENELEC 50126/8/9
- …

- ECSS: Analyse des écarts

- Propositions

Méthodes de sûreté de fonctionnement (logiciel)

- **Pratiques industrielles**
- **Standards**
- **Etudes précédentes**

- **34 (groupes de) méthodes analysées, ADF, AMDEC, tolérance aux fautes, modélisation, test, etc.**

- **Principe:**
  - moyens suggérés (recommandés?) pour atteindre un objectif
  - Guides de « bonne » utilisation

Quelques pistes

- **Utilisation, Justification de la tolérance aux fautes**
- **Les approches orientées objet**
  - Le test
  - Les métriques
    - Support au développement
    - Evaluation du produit
- **Logiciels sur étagère, logiciels libres**
- **Co-ingénierie**
- **Modélisation, génération automatique**
- **Firmware**