dgac

STAC

Journée Technique 2009

Gestion de la sécurité logicielle

Céline Pelletier

STAC – Sûreté de Fonctionnement

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Écologie, de l'Énergie, du Développement durable et de l'Aménagement du territoire

Ressources, territoires et habitats
Énergie et climat
Développement durable
Prévention des risques
Infrastructures, transports et mer

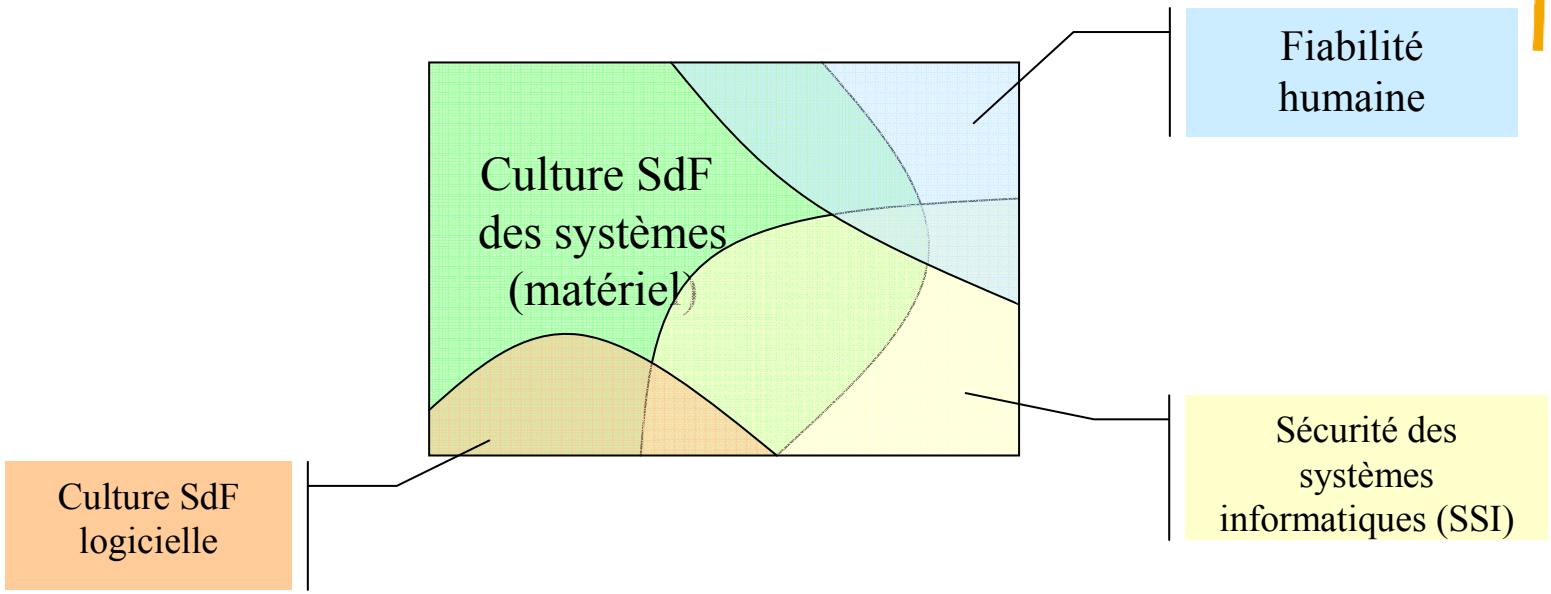
Présent pour l'avenir

Qu'est-ce qu'un logiciel?

- Tout ce qui n'est pas purement matériel ou électronique est du logiciel (Définition du règlement CE 482/2008)
- Programmes informatiques et données de configuration correspondantes
- Différentes catégories de logiciels:
  - Applications développées spécifiquement
  - COTS, applications réutilisées

Sûreté de fonctionnement

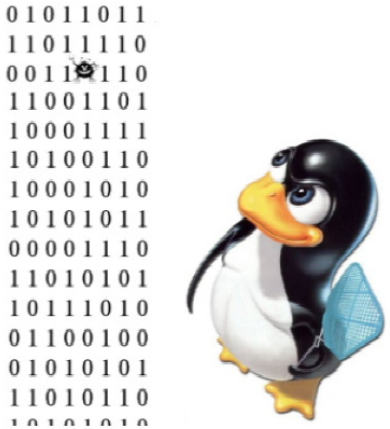
- Qualité du service délivré par un système, qualité telle que les utilisateurs de ce service puissent placer une confiance justifiée dans le système qui le délivre



La Sûreté de fonctionnement logicielle

- Lorsqu'un logiciel est soumis à une contrainte donnée le résultat est toujours le même
- Les défaillances logicielles relèvent uniquement de fautes de développement et de réalisation

- 4 leviers d'action
  - Évitement des fautes
  - Tolérance aux fautes
  - Élimination des fautes
  - Prévision des fautes



Taux de défaillance vs Assurance logicielle

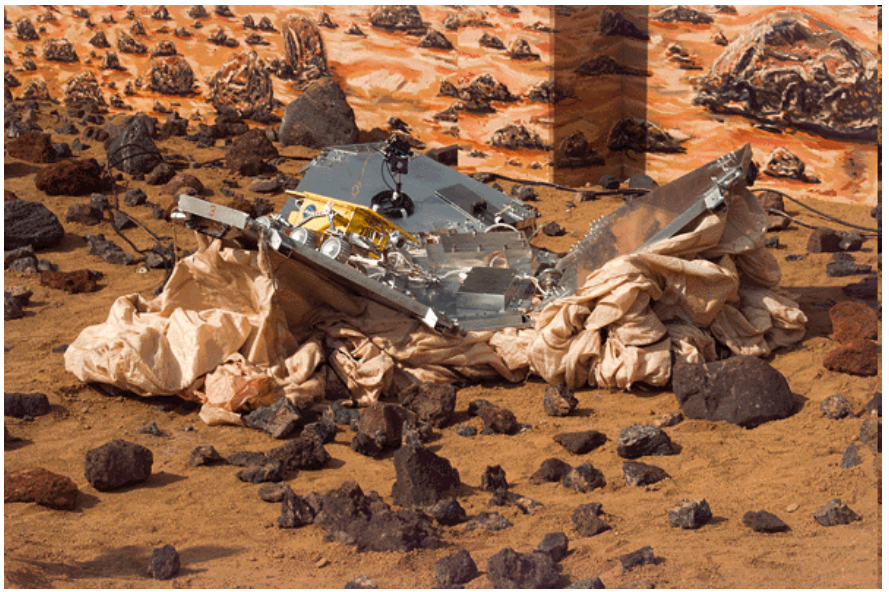
- Pour les matériels utilisation de taux de défaillance MTBF…

  ⇨Pas de taux de défaillance pour les logiciels !

- L'état de l'art, dans tous les domaines (nucléaire, spatial, avionique, etc.) consiste à substituer à la notion de « taux de défaillance » la notion d'assurance logicielle

Taux de défaillance vs Assurance logicielle

- Assurance logicielle = Niveau de confiance que:
  - Les spécifications du logiciel sont valides
  - Le logiciel est conforme à ses spécifications
- Niveau de confiance: AL,SIL, SWAL



Le règlement CE 482/2008

- Paru le 1/05/2008

- Objectif:
  - Mise en œuvre d'un système d'assurance de la sécurité des logiciels afin de réduire à un niveau tolérable les risques associés à l'utilisation des logiciels ATM sol.

- Applicable dès
  - le 1er janvier 2009 aux nouveaux logiciels
  - Le 1er juillet 2010 aux modifications

SWAL: Software assurance level

- Le SWAL met en rapport la rigueur des assurances logicielles et la criticité d'un logiciel.

- On distingue:
  - SWAL requis
  - SWAL atteint

- Un logiciel n'a pas de SWAL dans l'absolu.

Exigences fondamentales du règlement

- Le prestataire doit mettre en place un **Système d'Assurance de la Sécurité des Logiciels.**

- Le SASL doit permettre de donner un niveau de confiance suffisant vis-à-vis de :
  - la **validité** des exigences logicielles (spécifications)
  - la **vérification** des logiciels
  - la **gestion** de la **configuration**
  - la **traçabilité** des exigences
  - L'absence de fonction nuisant à la sécurité

Les travaux du STAC

- Participation à la mise en place de la réglementation et à son interprétation.

- Action en tant qu'expert auprès de l'ANS sur l'interprétation et l'application du règlement.

- Réalisation d'études.

Merci de votre attention

Céline PELLETIER
STAC/SINA/Navigation Aérienne/
Sûreté de fonctionnement
celine.pelletier@aviation-civile.gouv.fr
01 49 56 83 66