Outils de spécification 1 (parties 1& 2)

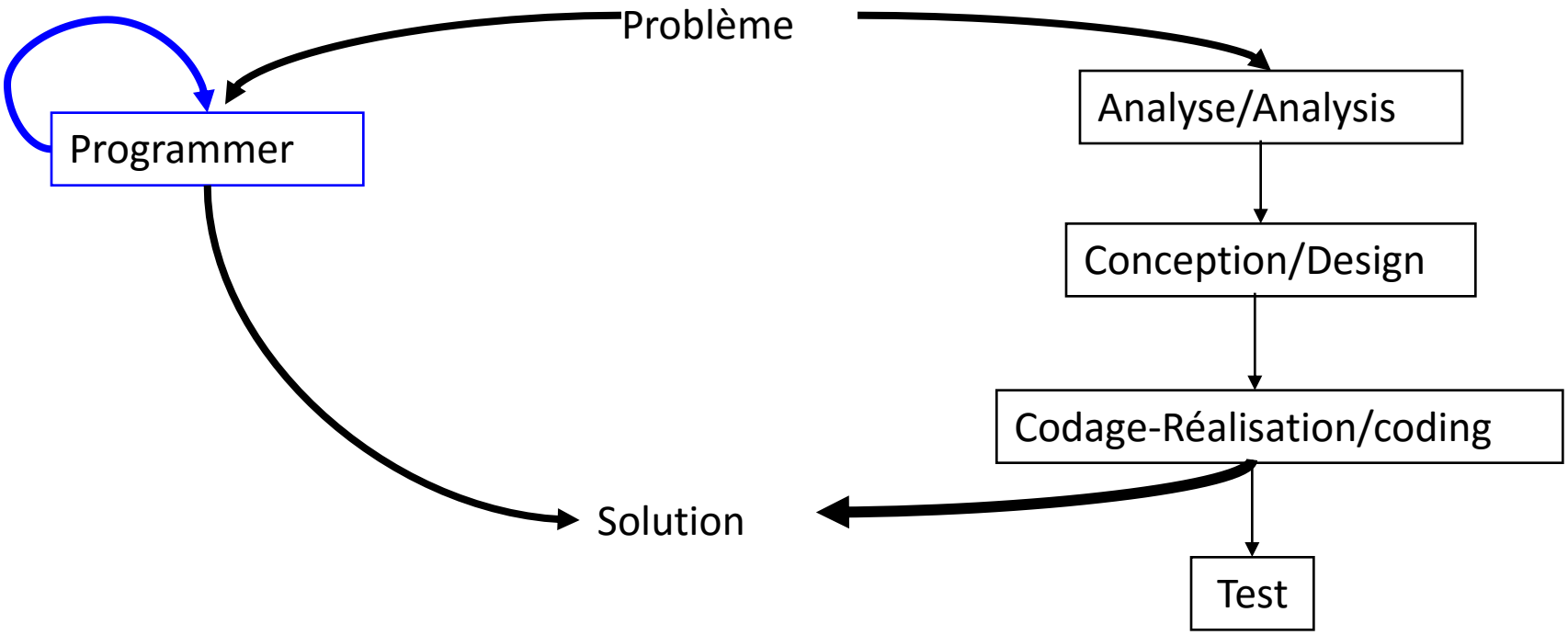
Cours de Master: M1 GLSD
2016-2017

Plan

- **Partie 1: Introduction (Systèmes critique, bogues célèbres, Langages formels, Spécification, Vérification);**
- **Partie 2: Modélisation du système (Aspects à modéliser dans un système, modèles pour la dynamique, systèmes à événement discrets, formalismes des systèmes à événement discrets)**
- Partie 3: Systèmes états-transitions
- Partie 4: Automates des systèmes infinis
- Partie 5: Logique Temporelle

But d’un développeur

- Trouver des solutions à des problème
- Développer des systèmes



Exemples de Systèmes

1. Systèmes répartis: réseaux, télécommunications . . .

2. Systèmes embarqués: téléphones mobiles, avions, fusées, automobiles

3. Systèmes domestiques: un magnétoscope, une machine à laver . . .

Systèmes critiques

- de plus en plus performants, de plus en plus miniaturisés et donc **de plus en plus complexes**

- systèmes critiques →**fiabilité indispensable**

Quelques bogues célèbres

Télécom: 1990

- un **patch non vérifié** dans le système d'exploitation
- une erreur dans un **switch** (en C)
- le réseau téléphonique de la côte Est des États-Unis a **été bloqué pendant 9h** !

Energie: 2003

• Panne d'électricité aux USA & Canada, General Electric. Cause. A nouveau : mauvaise gestion d'accès concurrents aux ressources dans un programme de surveillance.

Quelques bogues célèbres

Aéronautique:

- 1962: Perte d'itinéraire de la sonde Mariner 1 (NASA) au lancement.
  Cause. Erreur de transcription de copie papier vers code Fortran.

- 1996: Auto-destruction d'Ariane 5 (1er vol), 37 secondes après décollage. Cause: Conversion flottant 64 bits trop grand, vers entier 16 bits.

- 2004: Blocage du robot Mars River. Cause: Trop de fichiers ouverts en mémoire flash.

Medecine:

- 85–87: 5 morts par irradiations massives dues a la machine Therac-25.
  Cause: Conflit d'accès aux ressources entre 2 parties logicielles.

Quelques bogues célèbres

Informatique

06–08: Clés générées par OpenSSL et données cryptées non sures, impactant les applications l'utilisant (comme ssh). (http://linuxfr.org/news/d%C3%A9couverte-dune-faille-de-s%C3%A9curit%C3%A9-critique-dans-openssl-de-deb)
Cause. Générateur de nombres aléatoires d'OpenSSL casse.

1994: Bug du Pentium FDIV sur opérations en nombres flottants.
Cause. Algorithme de division erroné (découvert par Th. Nicely). 470 millions de $

78–95: Faille dans le protocole d'authentification de Needham-Schroeder.
Cause. Attaque « man in the middle » détectée par G. Lowe.

Bogues Quotidiens

- Ordinateur **perd un fichier**,
- **l'installation d'un nouveau logiciel** en rend un autre inutilisable
- certaines **options d'impression** refusent de fonctionner

Pourquoi ces bogues?

- La rédaction du **cahier des charges**:

  langage naturel peut être a source d'erreurs :

  1) les descriptions écrites peuvent être **ambigües**

  2) **mal interprétées** par les développeurs chargés de mettre en œuvre des solutions.

- La conception : une source potentielle d'erreurs:

  1) la complexité croissante des systèmes,
  2) Interactions avec d'autres systèmes,
  3) ou avec des parties du système

Solutions Possibles:

- Description claire du système = Méthode Formelle
- Spécification & Vérification du système