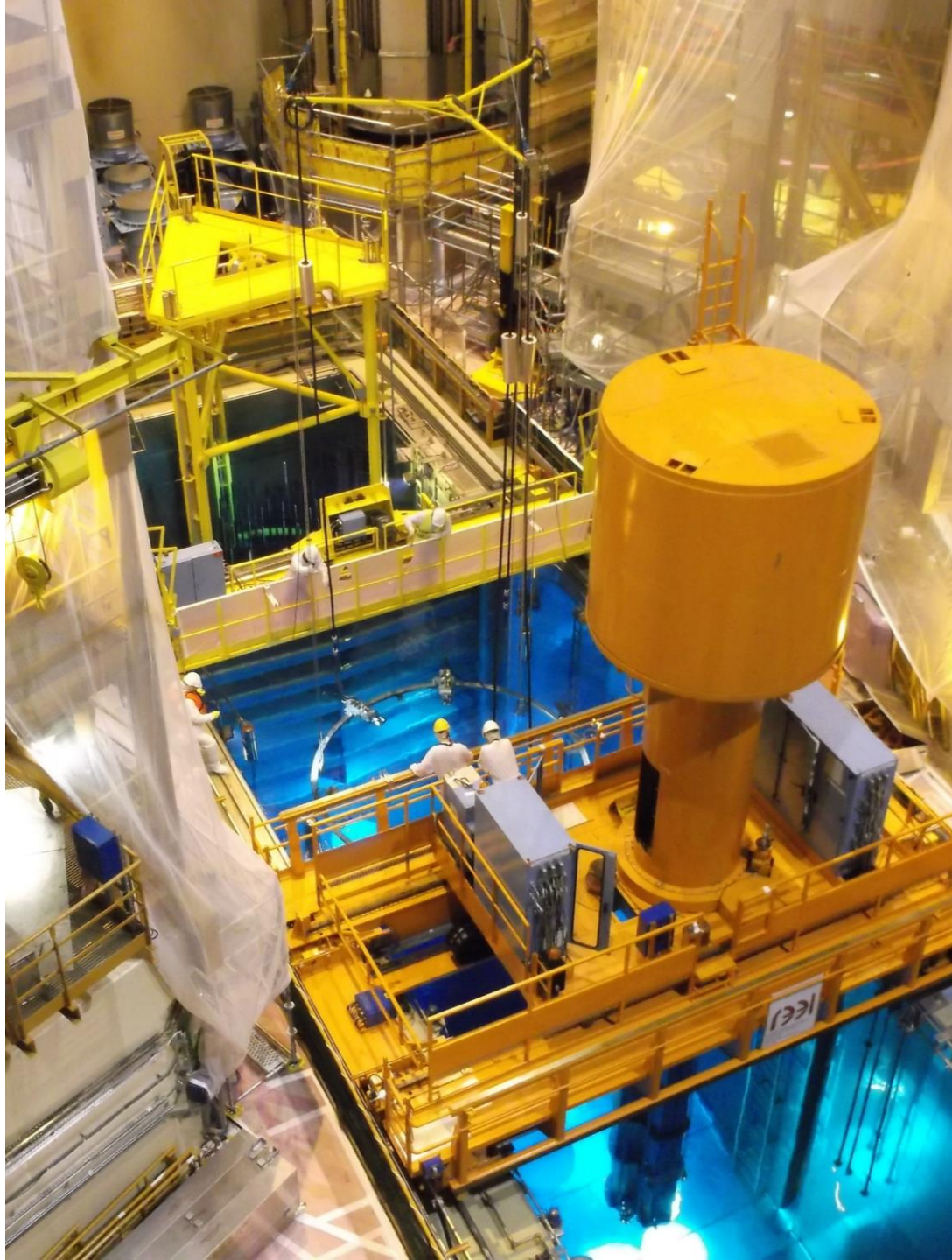
CQPM Automaticien 2024/2025

MODULE R1 – Exigences du secteur nucléaire

Sommaire

Rappel des enjeux



Sûreté Nucléaire

La **sûreté nucléaire** est l'ensemble des activités qui assurent le maintien de l'intégrité des mécanismes, processus, outils ou instruments mettant en œuvre de la matière radioactive, permettant de garantir l'absence d'effets dommageables sur les populations et l'environnement.

Fonctions fondamentales de sûreté :

- Le confinement des particules radioactives
- l'évacuation de la chaleur et de la puissance résiduelle (refroidissement)
- La maîtrise de la réactivité

Les équipements classés Importants pour la sureté (EIPS) peuvent comporter un système de contrôle commande classé de sureté , pouvant assurer des fonctions de sureté.

La spécification, le développement et les tests des logiciels peuvent contribuer à la sûreté nucléaire de l'installation nucléaire.

Sûreté Nucléaire

Les 3 fonctions :

- Maitriser la réactivité
- Confiner les matières radioactives
- Assurer le refroidissement

Evènements redoutés type :

- Chute de charge
- Perte d'intégrité de l'engin
- Collision avec structures environnantes EIPS
- Dommage sur le colis

Evènements initiateurs (potentiellement combinés) :

Interne au système (défaillance composant, dimensionnement; agression interne)

Externe au système - Agression (Séisme, incendie, conditions climatiques, CEM, interface avec un autre système…)

Erreur humaine, Malveillance (cyber)

Sécurité des personnes

Les machines peuvent être dangereuses pour les personnes

Phénomènes dangereux :

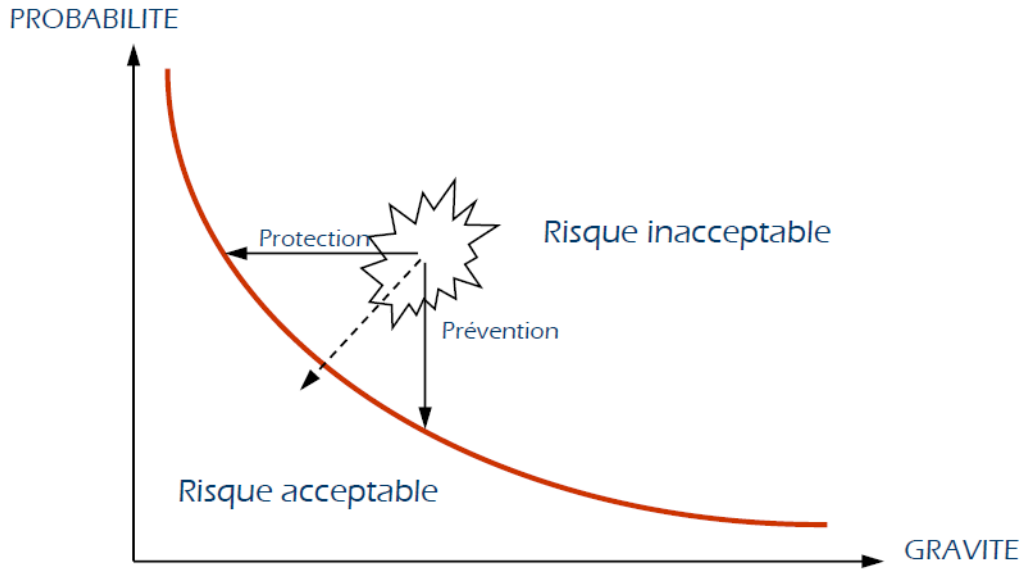
1) Machines en mouvements : risque de collision, écrasement
2) Electricité
3) Hauteur
4) Radioactivité
5) Etc…

Ces phénomènes dangereux peuvent induire des risques qui se doivent d'être traités pour réduire leur criticité et le rendre **acceptable**. (parades techniques et organisationnelles – de prévention et de protection)

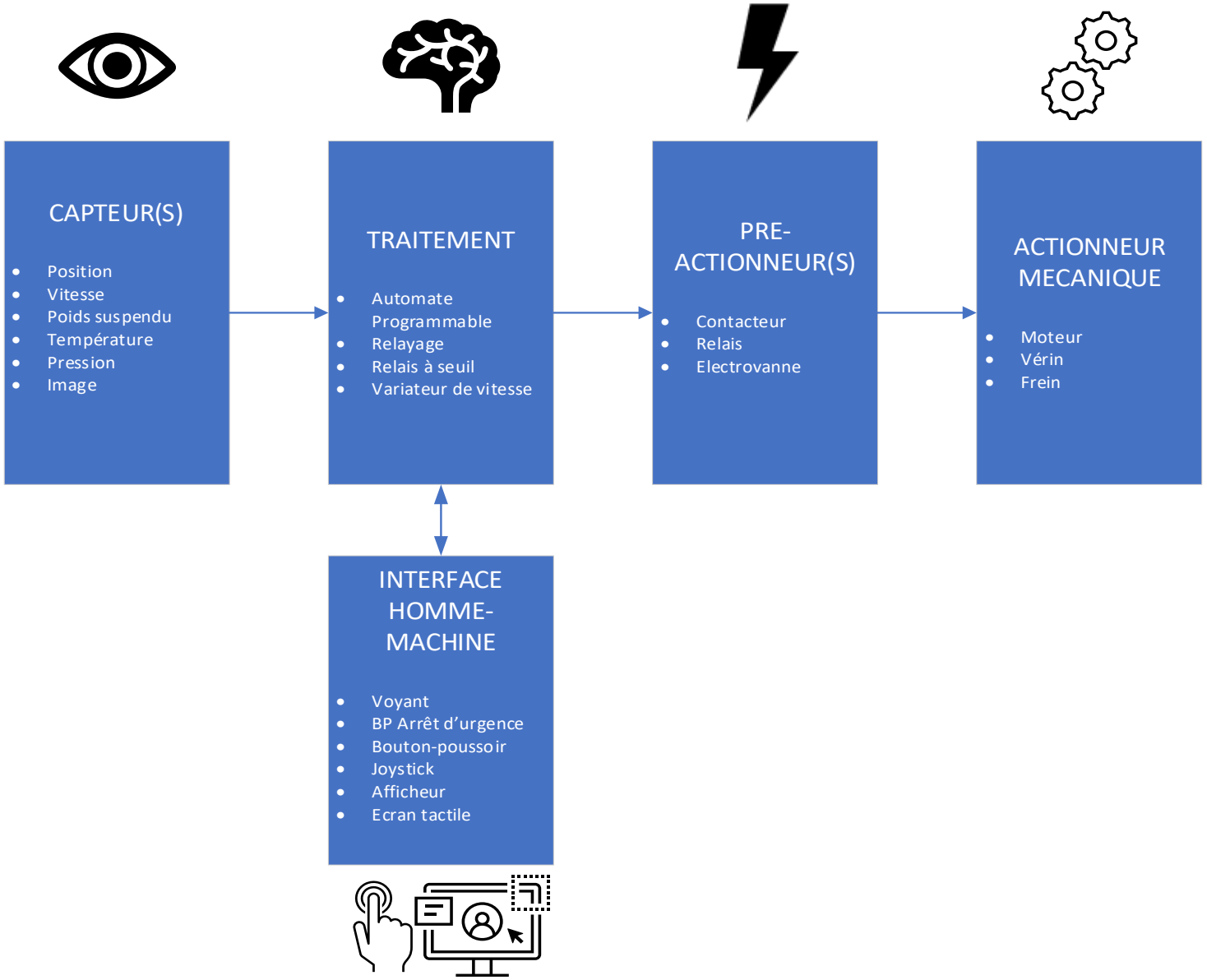
cf. Module Analyse de Risque

La spécification, le développement et les tests des logiciels peuvent contribuer à la sécurité des personnes

Exemple : système anticollision



Système de contrôle commande



Un système de CC peut remplir plusieurs fonctions.

Typiquement, trois types de fonctions à remplir :

- Les fonctions opérationnelles (exemple : gestion des trajectoires)
- Les fonctions de prévention (exemple : régulation de vitesse)
- Les fonctions de détection d'anomalie (exemple : détection de survitesse)

La fiabilité et la qualité

FIABILITE

Probabilité d'un système ou d'un composant à remplir ses fonctions exigées dans des conditions déterminées pour une période de temps déterminé dans des conditions définies.

Pour du matériel : approche quantitative. Mesurable. (SIL, PL, MTBF…)

Pour du logiciel : approche qualitative. Pas mesurable.

QUALITE

C'est l'ensemble des propriétés et caractéristiques d'un produit, processus ou service qui lui confèrent son aptitude à satisfaire les besoins exprimés ou implicites.

« Dire ce qu'on fait - Faire ce qu'on dit » - Et en apporter la preuve !

-> On documente

Référentiels

ISO 9001 : pour tous les logiciels !

NF EN ISO 9001 – Système de management de la qualité – Exigences

Cette norme définit des exigences pour la mise en place d'un système de management de la qualité pour les organismes souhaitant améliorer en permanence la satisfaction de leurs clients et fournir des produits et services conformes

ISO/IEC 90003
Ingénierie du logiciel — Lignes directrices pour l'application de l'ISO 9001 aux logiciels informatiques

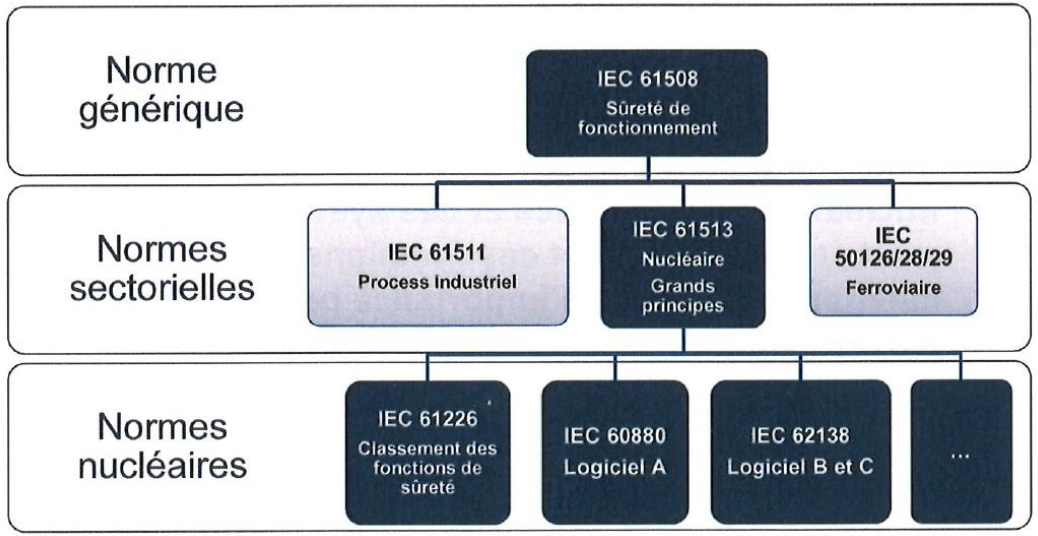
Elle identifie les éléments qu'il convient de traiter, de façon indépendante de la technologie, des modèles de cycle de vie, des processus de développement, de l'enchaînement des activités et de la structure organisationnelle de l'organisme.

Série IEC 61508 : pour les fonctions de sécurité

IEC 61513 - Centrales nucléaires de puissance - Instrumentation et contrôle-commande importants pour la sûreté - Exigences générales pour les systèmes

APPROCHE **DETERMINISTE** (contrairement à la 61508 , qui est une approche PROBABILISTE)

IEC 62138 - Centrales nucléaires – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B ou C



Fonctions classées de sureté.

Catégorie A :

Fonctions qui tiennent un rôle **principal** dans l'obtention ou le maintien de la sureté de la centrale pour empêcher que les événements ne conduisent à des conséquences inacceptables.

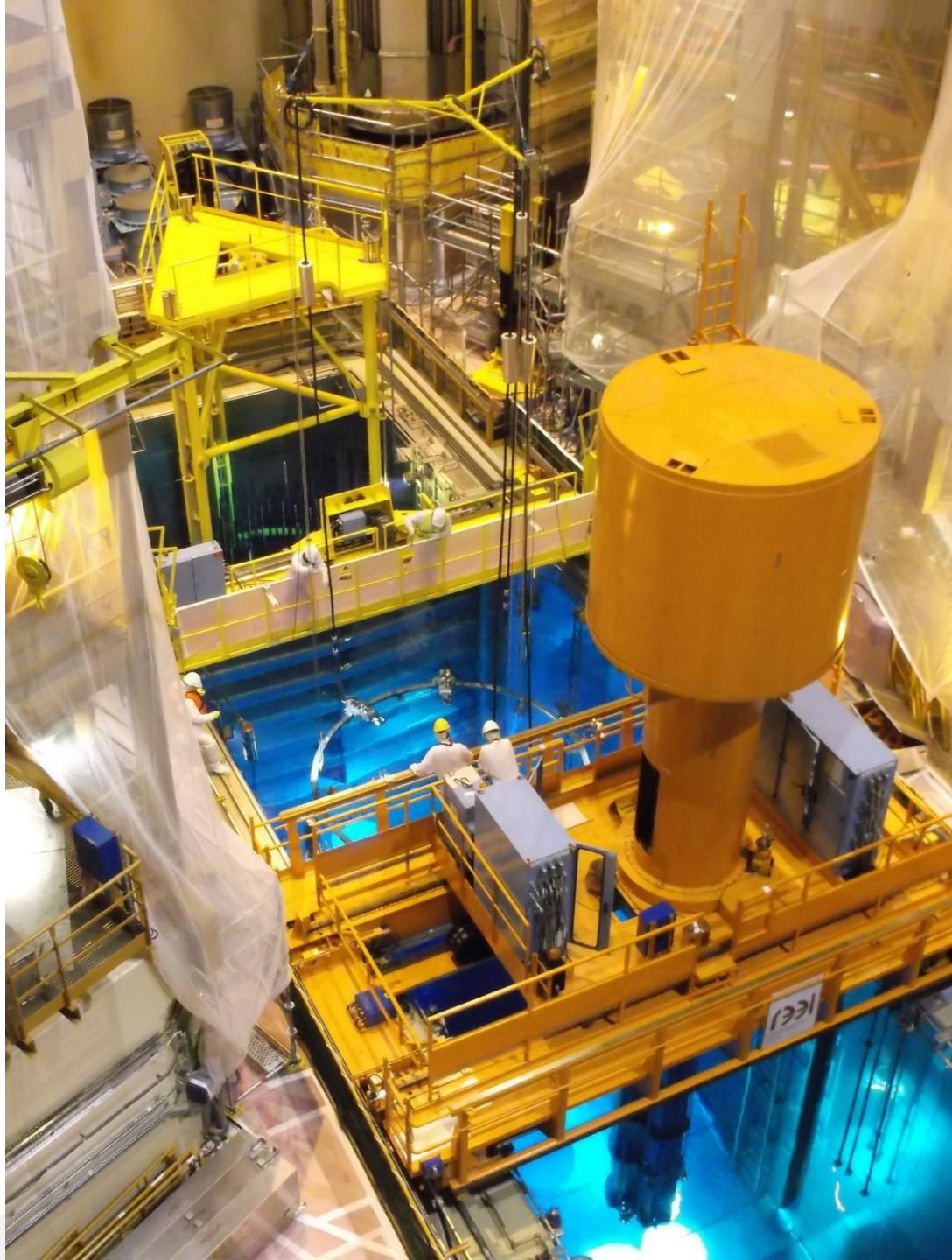
Catégorie B :

Fonctions qui tiennent un rôle **complémentaire** par rapport aux fonctions de catégorie A . La mise en œuvre d'une fonction de catégorie B peut éviter le déclenchement d'une fonction de catégorie A.

Catégorie C :

Fonctions qui tiennent un rôle **auxiliaire ou indirect** .

Impact pour les architectures



Architecture

Une architecture est la structure organisant un système de CC.
Une architecture est faite de choix technologiques et doit répondre à des fonctions.
La conception de l'architecture du CC est dépendante de nombreux facteurs interdépendants et parfois antagonistes :

Exigences sur l'architecture

Approche déterministe – Gradation des exigences selon la catégorie.

- **Séparation** des systèmes (physique et électrique)
- **Indépendance** des systèmes (isolation électrique, séparation physique, communications)
- **Diversité** (physique, fonctionnelle) (classe 1)
- **Redondance** des systèmes (classe 1 et classe 2)
- Qualification environnementale des composants
- Démonstration de fiabilité (calcul probabiliste de défaillance)
- Qualification / robustesse des logiciels système et applicatifs
- Traçabilité des exigences
- Testabilité des fonctions
- Autosurveillance (panne dormante)

Ces systèmes peuvent donc être très complexes et parfois contradictoire avec les objectifs tels que :

- La simplicité des systèmes de sécurité (limiter le nombre de défaillances potentielles)
- Les fonctions et la disponibilité de l'engin
- La faisabilité technique (intégrable)
- L'opérabilité
- La fabricabilité
- La maintenabilité
- Le coût

Qualité logiciel

Définition de la qualité d'un logiciel :

« Appréciation globale d'un logiciel associé à des indicateurs »

Qualité fonctionnelle :

Requis→ Fonction→ Conformité

Qualité structurelle :

- Modularité
- Testabilité
- Fiabilité
- Performance
- Maintenabilité
- Facilité d'utilisation

Qualité logiciel

Définition de la qualité d'un logiciel :

« Appréciation globale d'un logiciel associé à des indicateurs »

Qualité fonctionnelle :

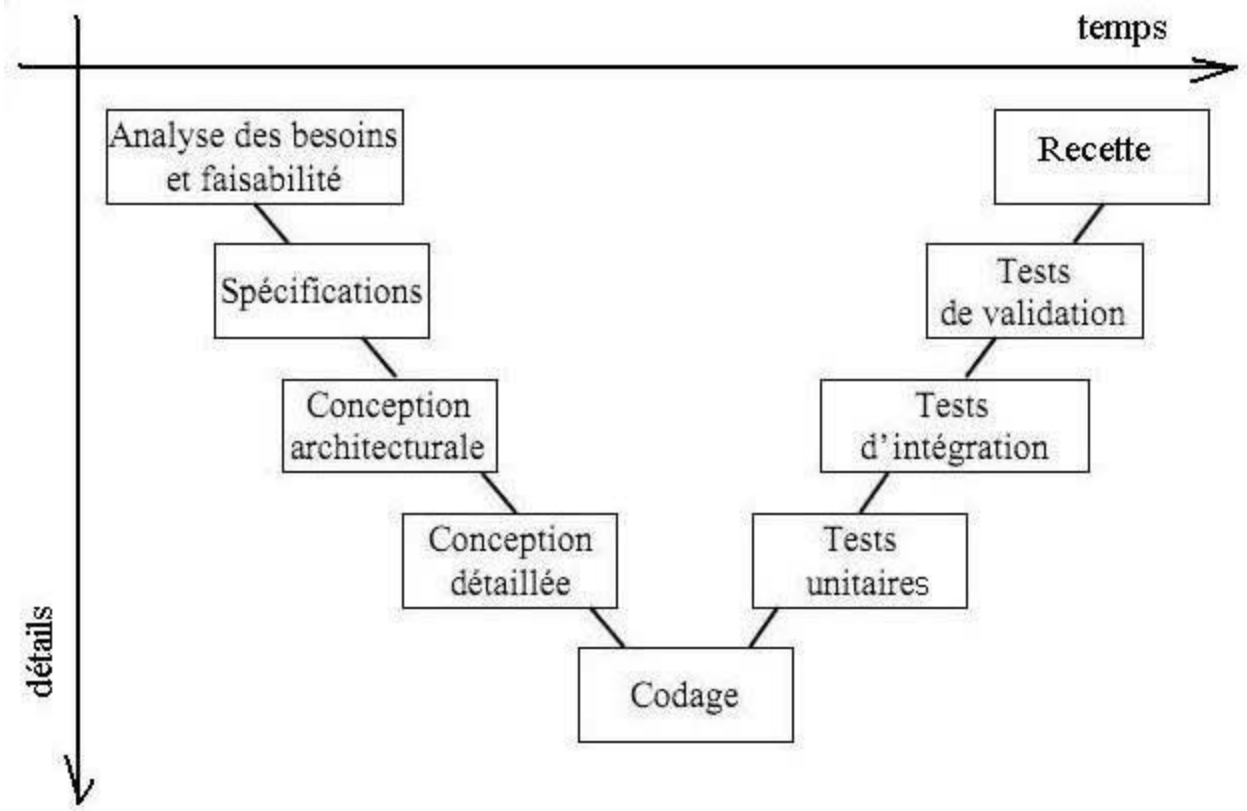
Requis -> Fonction -> Conformité

Qualité structurelle :

Code source et architecture influencent :

- Facilité d'utilisation
- Fiabilité
- Performance
- Maintenabilité
- Portabilité

Cycle en V :



Phase analyse des besoins

Analyse des besoins du clients

Cette partie est décisive, car les analyses et les conceptions ultérieures dépendent de cette étape.

Compréhension des attentes et exigences.

Phase de convergence avec le client.

Spécification fonctionnelle

Il s'agit d'identifier de façon claire et précise l'ensemble des fonctionnalités répondant aux besoins du client exprimés dans le cahier des charges.

L'analyse fonctionnelle :

- Liste les fonctions du système
- Définit une architecture qui doit répondre aux exigences avec les différents composants nécessaires
- Expose les exigences sur le matériel, et les performances.
- Expose le choix de la plateforme supportant le logiciel
- Définit les interfaces

Spécification logicielle

La spécification logicielle doit être une référence pour la conception et la validation du logiciel, ainsi que pour les modifications éventuelles.

- Montre la correspondance entre fonction logicielle et fonction système.
- Liste et spécifie les fonctions devant être assurées par le logiciel
- Etablit les exigences fonctionnelles, de performance, de niveau de sécurité, d'interface
- Etablit le plan de test du logiciel,
- Spécifie les modes de fonctionnement du logiciel requis en cas de détection d'erreur ou de défaillance.

Phase Conception

- Décrit la structure et le fonctionnement du logiciel (vue d'ensemble)
- Liste les modules
- Montre la correspondance entre fonction du logiciel et module
- Liste les exigences de développement (testabilité, complexité, niveau de documentation incorporée, indépendances logicielle et matériel)
- les langages de programmation à utiliser

La conception décrit également, le cas échéant, les moyens particuliers mis en œuvre prévus pour la réalisation des tests

Phase Codage

L’objectif du codage est de réaliser les modules sous la forme de briques logicielles, dans le respect des :

- Règles de programmation applicables,
- Objectifs de réalisation des tests,
- Métriques de qualification.

Documentation (exemple)

La documentation est réalisée pendant les phases du cycle de vie du logiciel.

Le tableau suivant montre la relation entre phase et document produit :

Phase		Documents d'entrée	Document produit	Condition
Analyse fonctionnelle		- Documents applicables du client - Plan Qualité Logiciel	- Analyse fonctionnelle - Plan des tests (niveau fonctionnel)	- Revue de l'analyse fonctionnelle suivant instruction **INS-05-01** - Validation des documents par le client
Conception		- Analyse fonctionnelle	- Document de conception - Plan des tests (niveau modules)	Validation des documents de conception par le RTE
Codage		- Documents de conceptions et plans de test - Normes de codage - Plan de questionnement logiciel		Revue de relecture (*) RTE + RQL
Tests plateforme	Tests unitaire	- Code et fonctions de test	Rapport de tests	Jeu de tests concluant
	Tests d'intégration 1	- Code, fonctions de test, moyens particuliers	Rapport de tests	- Jeu de tests concluant - Revue des tests plateforme (*) RTE + RQL
Tests usine	Tests d'intégration 2	- Code, fonctions de tests, équipement final - Plan de questionnement logiciel **D806**	- Rapport de tests - Fiches de suivi	- Jeu de tests concluants - Identification du logiciel §7.1
	Tests fonctionnels	- Plan des tests fonctionnels	- Rapport des tests fonctionnels - FNC	Acceptation par le client

Merci de votre attention

François LE TIEC : fletiec@reel.fr

www.reelinternational.com