Éléments de correction du partiel de SYS2

Dans la suite de ce document, nous vous proposons une correction possible du sujet qui vous a été proposé. Le barème a été élaboré en gardant en tête que vous aviez à disposition tous les cours et toutes vos notes personnelles. Cette correction est à lire de la façon suivante :

Pour les questions de cours, notées chacune sur 2 points :

- Pour avoir les 2 points, il faut que votre réponse contienne une référence à chacune des notions en gras, et que votre réponse soit compréhensible.
- S'il vous manque une seule des notions en gras, ou que votre réponse est difficilement compréhensible, vous obtenez 1 point.
- Si vous n'en avez aucune, 0 point.

Pour les questions d'ouverture, notées chacune sur 10 points :

- 5 points seront attribués si toutes les notions en gras sont présentes dans votre réponse. Nous appliquerons un barème dégressif sur ces 5 points en fonction des éléments manquants.
- 3 points seront laissés à la discrétion du correcteur pour valoriser votre capacité à nous proposer une réponse complète, développée, illustrée d'exemples ou d'éléments issus de vos propres réflexions basés sur la compréhension que vous avez eu de ce cours.
- Enfin, 2 points viendront récompenser le caractère compréhensible, synthétique et sans faute d'orthographe de votre réponse.

Pour rappel, synthétique ne veut pas forcément dire court.

Si vous avez des questions sur cette correction ou sur la note que vous obtiendrez, je vous invite à prendre contact par mail avec votre enseignant.

Bonne continuation à tous !

L'équipe enseignante du cours SYS 2

Questions de cours

1. Qu'est-ce que la sureté de fonctionnement et comment l'intégrez-vous à la démarche d'IS?

La sûreté de fonctionnement est **l'aptitude** d'un système à **remplir une ou plusieurs fonctions requises dans des conditions données**. Elle englobe entre autres composantes la **fiabilité**, la **maintenabilité**, la **disponibilité** et la **sécurité**.

La **connaissance des aptitudes du système** permet aux utilisateurs du système de placer une **confiance justifiée** dans les services fournis.

C'est une activité transverse notamment présente à la descente du cycle en V, des spécifications jusqu'à la conception détaillée (e.g.: analyses de sécurité.)

2. Expliquez les enjeux d'une élaboration rigoureuse des interfaces, en illustrant vos propos des éléments vus en cours.

Élaborer les interfaces entre système, c'est **définir formellement leurs échanges**, qu'ils soient de nature fonctionnels, physiques ou logiques. Les interfaces fonctionnelles permettent de formaliser les **besoins d'échanges** d'informations entre les fonctions, tandis que les interfaces physiques et logiques définissent la **solution** mise en œuvre.

Il est fondamental d'être **rigoureux** (techniquement, et en gestion de configuration), car ces éléments **formels** seront utilisés au cours de la **totalité du cycle de vie** du system par différents intervenants, tels que (liste non exhaustive): MOA, MOE, autorités de certification, industriels et partenaires, services de maintenance, marketing, ...

3. Qu'est-ce que la gestion de configuration et comment s'applique t'elle pour les phases de validation du cycle en V?

La Gestion de configuration est **une composante de la Gestion de Projet**.

Gérer un produit en configuration consiste en :

- **L'identification de tous les éléments** qui le constituent (articles de configuration) et de leur état de maturité dans le développement (version)

- **L'identification et l'enregistrement des ensembles d'états cohérents** (Baseline, Standard)
- **La maitrise des évolutions et des corrections et de leurs impacts**
-

La gestion de configuration s'applique sur

- **Les matériels** (cartes, faisceaux, etc.)
- **Les logiciels**
- **La documentation** (spécifications, documents utilisateurs, doc de montage, formations, etc.)

En particulier, dans le contexte de la validation (ou IVV ou remontée du V) la gestion de configuration intervient

- En amont, car elle permet de **cadrer les activités de validation à mener**. La gestion de configuration permet de connaitre l'état des sous-systèmes, de configurer les moyens d'essais (modèles, bancs, etc.), d'identifier les essais qui sont pertinents (disponibilités des fonctionnalités, compatibilités entre sous-systèmes, recherche de régression, etc.)
- En aval, car **l'identification de défauts pendant les activités de validation vont conduire à des reprises du système** qui peuvent aller jusqu'au plus haut niveau de la définition. En effet, les défauts identifiés peuvent conduire à :
    - une reprise de l'implémentation → modification du software, du hardware, des câblages et donc des spécifications associées et des plans de tests unitaires, ce qui induit pour ces articles de configuration un nouveau versionnement ;
    - une reprise de la définition détaillée (et donc de l'implémentation) → modification de la définition des interfaces, des spécifications, des architectures et des plans de validation système, ce qui induit pour ces articles de configuration un nouveau versionnement ;
    - une reprise du besoin client (et donc de la définition et de l'implémentation). En effet, les essais peuvent mettre en évidence que les fonctions, telles qu'elles sont implémentées, ne sont pas faciles à mettre en œuvre selon l'utilisation qui en sera faite → modification des spécifications de besoin, voire du cahier des charges et donc des plans validation fonctionnels ce qui induit pour ces articles de configuration un nouveau versionnement.

Grâce à ces activités de gestion de configuration, les parties prenantes sont en mesure d'identifier, à chaque étape du développement, les ensembles cohérents de matériels et logiciels qui arrivent en validation, ainsi que la documentation applicable pour ces matériels et logiciels. Cette identification permettra de faire évoluer le développement pour atteindre le niveau correspondant à la demande du client.

4. Peut-on appliquer partiellement l'IS et ses outils? Illustrez votre réponse d'exemples pertinents.

L'IS est une **démarche méthodologique générale**, applicable à **l'ensemble du cycle en V**, qui englobe l'ensemble des activités adéquates pour concevoir, faire évoluer et vérifier un système apportant

une solution économique et performante aux besoins d'un client tout en satisfaisant l'ensemble des parties prenantes. L'IS permet d'obtenir, du fait des interactions entre constituants, les comportements synergiques recherchés tout en maîtrisant les comportements non intentionnels.

Il est **possible d'appliquer partiellement l'IS** et ses outils en fonction de la nature du projet :

- Par exemple, si on se limite au développement d'une simulation amont, **sans industrialisation** et **sans sous-traitance à des fournisseurs**, on peut se limiter à l'ingénierie du besoin et à l'analyse fonctionnelle.
- Ou lorsque le projet en lui-même **se limite à l'étape d'ingénierie du besoin** (exemple : négociation des objectifs techniques d'un standard d'avion de combat, ingénierie du besoin qui peut durer un an).

Dans le cas général, pour concevoir, développer et qualifier un système complet tel qu'un avion, il est déconseillé de faire l'impasse sur certaines activités de l'IS. Sinon, c'est prendre le risque de concevoir un produit:

- Qui ne répond pas au besoin du client si on fait l'impasse ou si on bâcle **l'ingénierie du besoin**.
- Qui introduira des besoins non requis, ou qui oubliera certains besoins du client, si on fait l'impasse ou si on bâcle **l'analyse fonctionnelle FAST**.
- Qui échouera à répondre aux **exigences de performance** / temps de traversée, si on omet de réaliser les **logigrammes fonctionnels**
- - Qui présente des erreurs de conception qu'il faudra reprendre. Par exemple, des erreurs de dimensionnement si on omet de réaliser les **analyses de dimensionnement** charge calcul, mémoire et bus, des erreurs de conception affectant la sûreté de fonctionnement ou la fiabilité / disponibilité de mission si on omet d'analyser les **arbres de défaillance du système**.

5. Faire et défaire, c'est parfois mieux refaire. Vu de l'IS, en quoi est-ce vrai et comment est-ce que ça s'applique?

Cette question aborde la thématique de **l'évolution**, et de la **traçabilité** entre les différentes évolutions, et donc standards, du système.

Vu de l'IS, il faut mettre en œuvre les **mécanismes de gestion de configuration** adéquats (fiche de modification par exemple) pour pouvoir: i**dentifier, justifier, effectuer des analyses d'impact, de coûts**, ... et ce afin de permettre une rigoureuse **définition de l'évolution** et traçabilité des impacts sur le système, et pour les différentes parties prenantes.

Questions d'ouverture

1. Dites-nous en quoi "fabriquer un avion" est une activité complexe qui nécessite la mise en place d'une démarche d'ingénierie des systèmes. Illustrez votre propos en vous appuyant sur tout ce qui vous a été dit par vos intervenants durant les cours.

Un avion est constitué de **très nombreux systèmes complexes** interagissant entre eux et l'environnement pour fournir de nombreuses fonctions aux pilotes et passagers.

Les activités de conception développement fabrication font appel à des **métiers/compétences très variés à coordonner**.

Le **nombre d'intervenants/parties prenantes est élevé**: ingénieurs, techniciens, ouvriers, fonctions support de l'avionneur mais aussi les fournisseurs, les autorités de certification, les clients...

La **période** de conception/développement/fabrication s'étend sur **5 années au minimum,** impliquant une **maîtrise du projet dans le temps**. (L'exploitation est bien plus longue, s'étalant sur des dizaines d'années).

Ces éléments font qu'une **organisation, des process / méthodologies / outils adaptés (=IS) sont nécessaires** pour aboutir à un **produit respectant le cahier des charges** initial du/des client(s).

La réussite du projet nait notamment de la **maîtrise des interactions :**

- **Humaines :** à l'intérieur de la société "mère" mais aussi avec les intervenants extérieurs)
- **Entre systèmes/équipements/composants** pour ce qui constitue "matériellement" l'avion.

Sur ce dernier point : la maîtrise des comportements recherchés mais aussi des comportements non-intentionnels est essentielle. Des interactions néfastes involontaires/émergentes entre systèmes peuvent dégrader les performances de l'avion, voire mener à un accident. Exemples du flutter de commandes de vol, du shimmy de train, du pompage moteur.

Comme vu en TD, les outils de l'IS nous permettent notamment :

- D'assurer la traduction du cahier des charges en énoncés clairs, précis, quantifiables…
- De s'assurer de la bonne déclinaison des spécifications en fonctions : **analyses fonctionnelles externes** (FAST, logigrammes) **puis internes** (projection sur les équipements),
- de "bien" **dimensionner** les systèmes (ex : bus numérique),
- de **maîtriser les interfaces**
- d'assurer les objectifs de **sureté de fonctionnement**.

2. Conception et validation: comment définiriez-vous ces disciplines, et en quoi sont-elles liées?

Conception et validation font toutes deux partie de la **démarche d'ingénierie système**.

La conception d'un système regroupe les activités nécessaires à **l'ingénierie du produit**, permettant de concevoir et développer un produit conforme aux besoins identifiés par **l'ingénierie du besoin**.

La validation d'un système regroupe les activités **d'intégration, vérification, validation et qualification** d'un système.

À première vue, conception et validation pourraient être vues comme étant respectivement les activités descendantes et remontantes du **cycle en V**.

S'il est vrai que les activités d'intégration, vérification, validation et qualification jouent un rôle primordial dans la partie remontante du cycle en V, en réalité la validation intervient également dans la partie descendante du V.

Ces disciplines sont étroitement liées, car **à chaque niveau de conception caractérisé par des exigences**, **correspond un niveau de validation consistant à s'assurer que les exigences sont satisfaites**. Sachant que le niveau ultime de validation est la qualification du système qui sanctionne la satisfaction du besoin client, l'utilisabilité du système entre les mains de ses utilisateurs, ainsi que la certification du système c'est-à-dire pour un avion la satisfaction de la réglementation qui l'autorise à voler ou non. Pour parvenir à ce niveau ultime, il est nécessaire de valider à différents **niveaux de granularité** du système et à **différents moments du cycle en V**.

En effet, plus un problème est détecté tard dans le cycle en V et plus il est coûteux et long à corriger. De ce fait, les industriels et notamment les avionneurs tels que DASSAULT AVIATION, améliorent leurs processus d'IS pour réaliser autant que possible des étapes de « **vérification en amont** », c'est-à-dire dès les activités de conception. Cela est rendu possible par exemple, grâce à l'utilisation d'outils d'ingénierie et de moyens d'expression de **spécifications formelles qui sont testables**. Par exemple, des outils tels que Matlab, Simulink ou SCADE permettent d'écrire une spécification sous forme de modèles formels qu'il est possible de tester. Par ailleurs, les **cas de tests utilisés lors de la conception sont bien souvent réutilisables pour les étapes ultérieures du cycle en** V, par exemple pour repasser ces mêmes cas tests aux bornes du constituant réalisé à partir de la spécification.

Par ailleurs, rappelons-nous que l'IS est une démarche « fractale » en ce sens que la démarche complète est appliquée par les fournisseurs aux bornes des constituants spécifiés par l'avionneur. Ainsi, lorsque l'on spécifie un constituant (un logiciel ou un matériel, ou les deux) à un fournisseur il faut impérativement **penser aux moyens de valider les constituants spécifiés**. Prévoir les moyens et protocoles de validation des constituants du système est donc une préoccupation à avoir pendant la conception. On ne peut pas intégrer dans un avion un constituant dont on ne sait pas valider la conformité à ses spécifications. C'est d'autant plus primordial lorsque l'on parle de **sûreté de fonctionnement**.

Pour conclure, si l'on considère un système complexe tel qu'un avion, il n'est pas envisageable de le concevoir dans une démarche de « tunnel » qui consisterait à attendre d'avoir tous les constituants

du système pour les assembler et commencer à valider seulement à ce moment. **Les activités d'intégration, vérification, validation doivent donc être conçues, planifiées et menées dès que possible pendant l'application de la démarche d'IS sur le cycle en V**.

A ce titre, il existe des démarches de conception et validation dites « **agiles** », issues du monde du développement logiciel/web, qui ont fait leur apparition dans le monde de l'industrie des systèmes aéronautiques. Ces méthodes visent à **raccourcir les cycles conception / validation des systèmes**. Ces itérations plus courtes permettent de détecter et corriger les problèmes très rapidement. Elles permettent même d'itérer au niveau ingénierie du besoin pour recaler les exigences client pendant la conception suite aux résultats de validation. Toutefois, si ces méthodes sont appliquées sur des constituants particuliers, leur applicabilité aux bornes d'un système complexe et certifié tel qu'un avion n'est pas envisageable, du moins avec l'état de l'art actuel, du fait des impacts considérables d'une évolution d'exigence client sur l'ingénierie du produit, les coûts et les délais de réalisation d'un avion.

3. Quelle est la différence entre un chef de projet et un responsable technique en charge de la mise en place de la démarche d'ingénierie des Systèmes? Vous préciserez notamment de quelle manière les 2 rôles coexistent au sein d'un projet, et quelles sont leurs prérogatives respectives.

Le chef de projet applique la gestion de projet au sens où il pilote le déroulement des activités dans le but de tenir des objectifs de qualité, de cout et de délai. Dans ce pilotage figurent en particulier la gestion du planning, la gestion du budget, la gestion des couts et la gestion des risques.

Le responsable technique applique l'ingénierie des systèmes pour s'assurer que le développement du système soit développé conformément aux besoins et contraintes exprimés par les parties prenantes, et que la solution soit conçu de manière à répondre à ces besoins/contraintes. Les éléments qui constituent cette solution doivent être correctement conçus, c'est-à-dire :

- qu'ils interagissent de façon maitrisée,
- que les comportements non intentionnels soient atténués (voire supprimés)
- que la synergie recherchée soient effectivement atteinte.

Pour cela le responsable technique s'assurera que

- l'analyse de besoin aura été menée et le contenu,
- que les étapes de définition, d'analyses de dimensionnement, de sureté de fonctionnement ont bien été menées
- que le contenu des spécifications et le résultat des analyses sont conformes aux requis,
- que l'implémentation est conforme à chacun des niveaux de définition au moyen d'essais, de simulations, analyses,
- que les plans de validation sont réalistes du besoin,
- que les essais sont représentatifs
- que les résultats font l'objet de compte rendu et que le nombre de défauts résiduels est acceptable.

Pour mener ces activités, **l'interaction entre le chef de projet et le responsable technique doit être continue**.

Le suivi du planning et du budget se feront par le chef de projet sur les remontées du responsable technique.

Les activités de gestion de configuration peuvent **mener le chef de projet à solliciter le responsable technique** pour évaluer les activités associées à une demande de modification, en particulier pour identifier la faisabilité et les risques d'une évolution, les impacts sur son système, les documents à faire évoluer, les matériels à faire évoluer, les impacts sur les moyens d'essais, les délais pour mener l'évolution, les couts récurrents et non récurrents, etc.

D’autre part **le responsable technique peut au cours du développement identifier des besoins de modification et donc solliciter le chef de projet pour déclencher le processus de gestion de configuration associé**, par exemple sur les résultats d’une analyse de dimensionnement ou de sureté de fonctionnement, on peut identifier les défauts d’une architecture et être contraint de faire une fiche de modification pour modifier l’architecture (cf. TD)

De même dans le contexte de la gestion des risques, le chef de projet peut être mener à décliner au niveau du responsable technique des risques qui ont été identifiés au niveau programme et qui devront être pris en compte dans le développement (ajouter des contraintes, demander des compléments d’études, dé-risquer par la réalisation de prototypes ou par des essais complémentaires).

D’autres part au cours du développement le responsable technique sera mené à identifier des risques dont les conséquences peuvent atteindre la totalité du programme et doit alors remonter ces risques au chef de projet pour identifier des plans de gestion des risques pertinents sur le plan technique mais aussi dans le contexte budgétaire et temporel existant.