ANALYSE DE RISQUES DANS LE CADRE D'UNE INGENIERIE SYSTEME RELATIVISEE

RISKS STUDY IN RELATIVISED SYSTEM ENGINEERING

H. BOULOUET et V. BRINDEJONC
Membres Fondateurs d'AdMCR
PSA Peugeot Citroën
57, avenue du Général Leclerc
25600 SOCHAUX
henri.boulouet@mpsa.com

Mme M. MUGUR-SCHÄCHTER
Présidente de l'Association pour le Développement de la Méthode de Conceptualisation Relativisée (AdMCR)
Ancien Professeur de Physique Théorique à l'Université de Reims et Directeur du Laboratoire de Mécanique Quantique et Structures de l'Information de Reims. Présidente du CeSEF

Résumé
L'Ingénierie Système Relativisée (ISR) est fondée sur la Méthode de Conceptualisation Relativisée (MCR). Cet article expose la démarche analytique propre aux études de risques qui accompagnent la création de nouveaux produits aboutissant à de nouveaux artefacts physiques. Elle apporte une réponse tout à la fois formelle et concrète à cette problématique, tant au niveau de la prise en compte du « vécu » utilisateur porté par le produit, que de la robustesse de la solution technique proposée analysée comme le moyen de mettre le produit au niveau de service et de qualité souhaité. Elle répond aux problématiques posées par des normes comme l'ISO CD 26262.

Summary
Relativised System Engineering (ISR in French) stems from the Method of Relativised Conceptualization (MCR in French). It is a tooled and a pragmatic approach to system engineering and risk analysis. This article focuses on the analytic process involved in the creation of new products or/and physical artefacts. ISR bridges the gap between product marketing, psychological approach and technical object design. It stresses a comprehensive approach to hazard and safety analysis. ISR focuses on the way the average end user is supposed to master the product within a certain context and what the technical solution must be, how reliable it must be to bring up the product to the targeted level. It fits ISO CD 26262 requirements.

Contexte

Les industriels sont poussés à une diversification et à une complexité croissante des prestations de par les attentes de leurs clients tant en termes de confort que de sécurité. Dans le même temps, les exigences d'optimisation technico-économiques requièrent une factorisation des solutions autour d'architectures standard modulables. Ces dernières deviennent de plus en plus complexes et diversifiées. Exprimer un besoin par rapport à une utilisation pressentie, porté par des ressources partagées, et vérifier qu'il est effectivement satisfait de façon sûre de fonctionnement, devient une véritable gageure en même temps qu'un enjeu technique, industriel et commercial de tout premier plan. Ce besoin appelle une vision relativisée de la conception et des risques à laquelle ne répondent pas les approches fondées, telle l'approche fonctionnelle, sur un point de vue « unique », « absolu », « complet », d'un « tout » à connotation ontologique.
Cet exposé a pour objectif de présenter la démarche ISR d'analyse de risques qui accompagne tout processus de conception.
Sa spécificité est de structurer la représentation du nouveau, de l'inconnu à créer, sous la forme de la conjonction d'une part d'un modèle de contexte, exprimant une connaissance foncièrement statistique et, d'autre part, d'un modèle déterministe exprimant le niveau de maîtrise que l'on souhaite se donner sur l'artefact émergent.

Fondements de la solution proposée

ISR a pour ambition de satisfaire aux trois conditions qui permettent une méthode générale et appliquée traitant des « entités physiques » :

- Démontrer une efficacité réelle sur des cas concrets : l'efficacité des solutions proposées est testée incrémentalement au travers de cas pilotes
- S'appuyer sur des processus structurés par un langage et reposant sur des outils qui la mettent en œuvre, dans le cadre d'une solution viable techniquement, humainement et économiquement : ISR formalise l'ensemble de ses concepts au travers d'un métalangage, d'un profil UML 2 associé, servant de base à l'élaboration d'environnements utilisateurs d'édition, de simulation et de génération de cas de test.

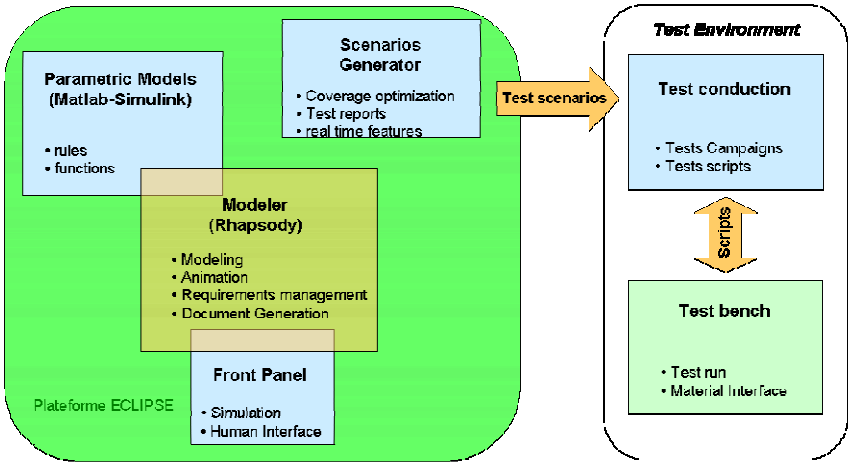

Figure 1: Solution outillée.

- Fonder la méthode sur une théorie de la connaissance permettant d'établir un lien formel entre les éléments du langage utilisé et la factualité physique : ISR est fondée sur MCR, élaborée par Mme Mugur-Schächter [1], et applique pratiquement cette théorie de la connaissance à l'ingénierie système.

Ce dernier point, fondateur, nécessité d'évoquer les postulats fondamentaux de MCR même si cet enracinement d'ISR dans MCR ne peut être décrit dans le périmètre limité de cet article :

- MCR est fondée sur le concept de description relativisée qui peut être représentée par le symbole *D(G, œ$_G$,V)* ou *G* désigne une "opération de génération" (physique et/ou abstraite) de l'entité à décrire dénotée *œ$_G$*, et *V* désigne un ensemble de une ou plusieurs vues-aspects *V$_g$* représentées globalement par la vue *V*. *(G, V)* définissent un référentiel épistémique spécifique de *D*.
- Par postulat méthodologique, afin de bannir toute présupposition absolue à connotation ontologique qui dépasseraient le cadre purement factuel dans le cas particulier d'une entité-à-décrire encore non conceptualisée auparavant du point de vue souhaité, toute répétition de *G* est conçue générer la "même" entité *œ$_G$* (le mot "identique" tout court est banni, car il pointe vers un "faux absolu" dépourvu de sens : toute identité définissable est relative à quelque vue-aspect ou vue spécifiée). Ce postulat méthodologique est essentiel pour la reconstruction MCR du concept de probabilité, qu'ISR implémente.
- Toutes vue qualifiante V désigne un ensemble structuré de vues-aspects *V$_g$*. Chacune vue-aspect *V$_g$* introduit une dimension sémantique *g* (couleur, poids, …) qui sous-tend un ensemble correspondant fini de qualifications dénommées "valeurs" *gk* de *g*. La définition d'une dimension sémantique g comporte nécessairement la spécification des examens-g – avec les procédures et les éventuels appareils que ceux-ci impliquent – à accomplir sur une entité-à-décrire *œ$_G$* afin de la qualifier par *g*. La valeur *gk* produite par un acte donné d'examen-g est déterminée via un codage bien spécifié de tout ensemble de résultats observables de l'examen, en termes d'une valeur *gk* et une seule.
- La définition du concept d'existence mutuelle pose qu'une entité *œ$_G$* et une vue-aspect *V$_g$* n'existent mutuellement que si la réalisation d'un examen-g sur un exemplaire de l'entité *œ$_G$* générée par G, permet d'observer un résultat (effet) qui, selon la définition de *V$_g$*, code pour une valeur *gk* de *g*. En outre, ce résultat *gk*, même s'il est obtenu, ne peut être considéré définitivement comme qualifiant l'entité à décrire, que si la répétition N fois de cet examen-g sur un exemplaire de *œ$_G$* produit, soit N fois la même valeur *gk* (cas de N-stabilité individuelle) soit une distribution statistique de valeurs *gk* dont les fréquences relatives convergent vers une "mesure de probabilité".
- Le principe-cadre d'espace-temps pose – notamment – que toute entité à décrire physique existe par rapport à au moins une vue (référentiel) d'espace-temps *V(ET).*
- Le *principe de séparation* pose que lorsque toutes les qualifications d'une entité œ$_G$ donnée, que l'on peut réaliser par une vue V donnée, i.e. à l'intérieur d'un *référentiel épistémique (G, V),* ont été obtenues, ce référentiel a épuisé ses capacités de description et la recherche – si on veut la continuer – exige l'introduction d'un nouveau référentiel épistémique.
- Le principe de séparation organise les descriptions relativisées en *chaînes* de *cellules* de description qui se méta-relient de manière *hiérarchisée*. Pour chaque chaîne il existe un niveau *primordial* absolu dénoté 0 : c'est le niveau où sont recueillis des effets *physiques*, observables et codés en termes de valeur *gk* d'une grandeur *g* "de transfert" (sur les enregistreurs d'un appareil physique), effets produits par un acte d'interaction *physique* "de mesure" entre une entité à décrire physique qui n'a jamais encore été conceptualisée auparavant *du point de vue souhaité* (entité-boîte-noire face à ce point de vue là), et un appareil de transfert. La numérotation des niveaux de conceptualisation subséquents – modélisants – est variable, donc conventionnelle.
- Toute connaissance communicable sans restriction et consensuelle est une description relativisée.

Plusieurs avantages découlent du choix de se placer dans le cadre de MCR.

- La cohérence et la généralité de l'ensemble constitué par les postulats, principes, définitions, preuves (au total 21 formulations) ;
- La construction de cette représentation de *l'ensemble* des processus de conceptualisation *normés uniformément*, en : ***(a)*** partant de la représentation de descriptions physiques d'entités physiques accomplies par des interactions physiques, mais qui d'emblée impliquent foncièrement et explicitement aussi des actions *psychiques* de choix et d'organisation conceptuelle de la part de l'observateur-concepteur ; ***(b)*** incluant progressivement tout processus de conceptualisation ; et ***(c)*** touchant finalement la limite qui sépare le connu rationnel, du métaphysique.
- L'exclusion – par construction – des ambiguïtés et faux problèmes innombrables issus de la confusion entre des référentiels épistémiques distincts ;
- La mise en évidence des degrés de liberté subjectifs liés à toute conceptualisation, en même temps que la formalisation des choix réalisés.

Introduction aux concepts de produit et objet technique

L'objet de l'ingénierie système, d'un point de vue industriel, est d'organiser la conception d'artefact(s) physique(s) nouveau(x) procurant une réelle valeur ajoutée à l'utilisateur au travers d'un système cohérent de services offerts : « le produit ».

L'artefact physique est le support matériel qui va rendre possible le produit. Il va procurer à l'utilisateur une nouvelle façon de percevoir et d'agir sur son environnement dans la mesure où l'utilisateur est capable de l'intégrer, en extension, dans son propre schéma corporel (réflexes d'un conducteur aguerri utilisant sa voiture).

L'ingénierie système se doit de représenter les liens de dépendance entre la réalité vécue définissant le produit, objet de validation, et l'objet technique, entité physique à soumettre à des vérifications. A ce dédoublement du projet en produit et objet technique répond un dédoublement de l'analyse des risques en termes d'une évaluation des dangers liée à l'usage du produit et de la sûreté de fonctionnement liée au fonctionnement de l'objet technique. Notons que selon MCR les descriptions du produit et de l'objet technique sont foncièrement distinctes car elles introduisent deux référentiels mutuellement exclusifs.

Considérons l'exemple suivant :
Un utilisateur acquiert un « produit-voiture-haut-de-gamme ». Ce produit comporte un système de navigation permettant à l'utilisateur de définir un itinéraire et d'être guidé. Si la localisation est impossible, il souhaite en être averti.

« L'objet technique-voiture-haut-de-gamme » désigne la voiture « concrète» qui sort des chaînes de montage. Cet objet doit être conforme à son modèle et répondre, conjointement avec son environnement, aux exigences définies pour le « produit-voiture-haut-de-gamme ».
A cette fin, « l'objet technique-voiture-haut-de-gamme » intègre un calculateur et une Interface Homme Machine permettant de mettre en œuvre le système de navigation. Ce système est conçu pour exploiter les informations GPS.

Un dysfonctionnement du produit peut ou non être lié à une défaillance de l'objet technique. Si la localisation de l'utilisateur s'avère impossible, le « produit-voiture-haut-de-gamme » avertira le conducteur, qu'il s'agisse:

- d'une défaillance de « l'objet technique-voiture-haut-de-gamme » : par exemple calculateur défaillant,
- d'une modification dans l'environnement de « l'objet technique-voiture-haut-de-gamme » qui ne correspond pas à un contexte connu ou un contexte anticipé mais dans lequel il n'a pas été prévu de rendre ce service: passage dans un tunnel, destruction des satellites…

Points de vue relatifs sur le produit et l'objet technique : concept de domaine d'étude

De multiples réseaux d'exigences et de contraintes convergent vers les deux concepts de produit et d'objet technique :

- vers le produit: ensemble des critères affectant l'usage et les dangers liés, la facilité de mise en œuvre, la fiabilité, la maintenabilité, la perception du client potentiel, y compris le prix relatif, la comparaison avec d'autres produits du marché, l'insertion dans l'environnement, le processus de fabrication (tel qu'il est vécu) etc.,
- vers l'objet technique: exigences relatives aux différents aspects techniques et de Sûreté de Fonctionnement : électrique, mécanique, aérodynamique, niveaux de performance, réglementation en vigueur, contraintes physiques environnementales, techniques, humaines, etc.

Ces réseaux de contraintes ne sont pas indépendants : le système d'exigences et de contraintes pesant sur l'objet technique est justifié par le système d'exigences et de contraintes spécifiant le produit. Chaque réseau d'exigence et de contrainte implique la définition de d'une procédure de comparaison entre les configurations factuellement observables (physiquement dans le cas d'objet technique, consensuellement dans le cadre des descriptions spécifiques au produit) et les configurations « a observer » générées par les modèles.
Ces systèmes d'exigences impliquent des points de vue multiples sur une même « réalité » à venir, simplement désignée au départ par un nom et un ensemble d'idées, d'a priori, d'expériences de nature très différentes, point de départ commun du processus de conception: le « pré –modèle ».

Chaque partie prenante au processus de réalisation, ou agent, est porteuse d'un certain point de vue sur le produit et, comme résultante, d'un certain système d'exigences et de contraintes sur l'objet technique. Un agent est la représentation d'un fonctionnement psychique capable de générer ses propres cadres descriptifs.

Un produit « réussi » est celui qui a su tenir compte de l'ensemble de ces points de vue, de la satisfaction du client**,** à l'équation économique de l'entreprise ; du positionnement du produit sur son marché**,** à la prise en compte des contraintes de fabrication de sécurité et d'après - vente, à son intégration dans son environnement.

Dans ISR, chaque point de vue, ici sur le couple produit-objet(s) technique(s), est caractérisé génétiquement par ses propres finalités et dispositifs d'évaluation.
L'élaboration de règles de correspondance entre vécu et factualité observable, la hiérarchisation des niveaux de conceptualisation, définissent un horizon d'analyse et de conception circonscrit (pour paraphraser Michel Bitbol [2]) par une réponse satisfaisante données à la question « comment ? », autrement dit par un certain niveau de connaissance.
Cette question donne le cadre d'une étude de risques spécifique comprise comme une étude de danger relative au produit et autant d'études de sûreté de fonctionnement que nécessaire en fonction de la structuration de la conception.

Toute la difficulté est dès lors de définir une articulation satisfaisante entre ces différents points de vue, articulation qui, forcément, doit s'organiser in fine autour d'entités "partagées", points d'ancrage autour desquels peuvent s'organiser compromis et consensus, à un méta niveau. C'est face à ces entités qui répondent à la question « comment? » que se superposent les différentes systèmes explicatifs et peut se construire un système de convainquant de réponses. « Si nous commençons à croire à quelque chose, ce n'est pas une proposition isolée mais un système entier de propositions » [3]): Ces points d'ancrage sont matérialisés par le concept d'article final ISR.

Représentation du produit

Il s'agit de décrire la façon dont un utilisateur va percevoir et agir sur son environnement au travers de l'usage d'un nouveau média: l'objet technique en devenir.
Il n'est pas réaliste de penser maîtriser la chaîne, qui, partant du constat de l'interaction physique, aboutit au fait psychique: il faudrait décrire le système nerveux, le cerveau humain et l'ensemble de la réalité psychique.
Il faut donc admettre que le fait psychique encapsule l'interaction physique sans qu'une description formelle en soit établie. Cet usage est caractérisé par tout un très riche ensemble de points de vue finalisées et relativisés, sur le produit. Ces points de vue se construisent au travers de scenarii exprimant une analyse finalisée du cycle de vie du produit, cycle de vie structurée en « phases-type ».
Exemple : On décondamne un véhicule, on s'installe au poste de conduite, on sécurise ses enfants, on démarre… A chaque phase finalisée correspond une étude de danger spécifique (que se passe-t-il si l'on démarre en croyant avoir activé une sécurité enfant et que ce n'est pas le cas ?) représentant le vécu d'un individu type dans le cadre de son usage du produit.
ISR généralise l'analyse de ces cycles en type d'usage propre au produit au travers du concept de prestation dont la définition est irréductiblement arbitraire. Elle reflète la structure d'analyse du marketing, le sens et le degré d'innovation que l'on souhaite apporter (par opposition à invention, qui relève de l'objet technique), détermine les options que l'on va proposer à l'utilisateur.
Le vécu est individuel. Une telle représentation suppose la description d'utilisateur type en tant qu'agent confronté à des contextes type. La validité de la description suppose un accord intersubjectif entre responsables produits, ergonomes, impliqués tant dans la conception du produit que dans les analyses de danger, etc.. Cet accord aboutit aux exigences produit.
Il est supposé atteint quand il y a convergence des appréciations quant à la représentativité de la description et des échelles qualitatives qui la sous-tendent.
Il n'est rendu possible que dans la mesure ou statistiquement, par retour d'expérience ou par opération de l'esprit, construite sur la base de paradigmes comportementaux, il correspond à des schémas type partagés consensuellement (règles ergonomique, etc.).
Cet accord est validé à la lumière de la convergence des évaluations constatées sur le produit fini, sur le fondement du système descriptif formel mis en place pour évaluer les prestations et les exigences qualitatives qui y sont liées.

Représentation d'un système

Un système est la description d'une entité physique qui matérialise un point de spécification, de conception et de vérification, mais non de réalisation.
Tout point de vue finalisé sur le produit (toute prestation) a vocation à se traduire par un certain regard porté sur l'entité physique considérée ("réalité physique" s'utilise pour *toute* la réalité physique, globalement), fut-elle à l'état de simple projet.
Le terme d'entité physique doit être compris dans sa définition MCR : il s'agit de désigner une chose *qualifiable* quelconque, de porter son regard sur une certaine "élément de réalité" concret *ou abstrait*, avec une finalité, consciente ou non, implicite ou explicite ; quelque chose que l'on peut *décrire*, notamment sur le fondement d'interactions physiques recueillies lors de tests préalables à toute tentative de conceptualisation (exemple : banc de test).

Rendre possible le produit par la création de nouveaux artefacts physiques nécessite de les examiner selon les approches jugées nécessaires pour arriver au résultat : celles du mécanicien, de l'électronicien, etc. Cette nécessité se traduit par autant de cadres descriptifs différents, de système différents, sur une réalité physique en devenir et sur les contextes dans lesquels elle doit évoluer. (Modèles aérodynamique, électromagnétique, mécanique, climatique…).

Chaque cadre descriptif va structurer la « réalité physique », en affectant un certain rôle à différents périmètres physiques ; objet de *spécification (représentation de l'attendu en « boite noire »)* et de *conception* (*rôle de ressources rendant possible cet attendu*), définissant ainsi un ***système particulier***. L'ensemble ordonnancé dans le temps et dans l'espace des interactions physiques constatées lors des tests doit transcender (rendre relativement « objective ») une telle représentation, spécification ou conception, la valider en tant que description structurale.
Une *spécification* est une description d'une entité qui fait abstraction des ressources matérielles utilisées: elle définit la forme permettant d'exprimer l'ensemble des attendus vis-à-vis de cette réalité~~s~~ physique (définit une enveloppe particulière d'exigences et de contraintes physiques à laquelle devra se conformer globalement *l'assemblage* des objets techniques, tel que spécifié dans la conception de cette entité).

Une *conception* est la description de cette même entité sous la forme d'une méta description finalisée d'un ensemble de ressources, les objets techniques, auxquels elle affecte un rôle particulier).

Un système est considéré comme défini lorsque le méta cadre descriptif permettant de *comparer* spécification et conception, est satisfaisant. Ceci implique l'utilisation d'une "méta vue de comparaison" exigée par le fait que la combinaison des enveloppes d'exigences et contraintes allouées aux différents objets techniques (allocations de responsabilités) rentre dans l'enveloppe des exigences et contraintes définie par la spécification. (ISR permet d'automatiser cet aspect).

Exemple : la modélisation de l'ensemble constitué du moteur, de la tringlerie, de la vitre et des joints d'une porte de voiture, du point de vue de l'ouverture et de la fermeture de la vitre, doit exprimer les contraintes physiques dont le respect doit être vérifié lors des tests techniques sur cet ensemble. Elle contribue à rendre possible la prestation « condamner le véhicule » mais aussi la prestation « piloter l'ouverture de sa fenêtre ».

L'analyse de sûreté de fonctionnement va épouser cette structure descriptive. Elle va se focaliser, d'une part, au niveau des spécifications, sur les relations entre le périmètre considéré, appréhendé comme un tout et son contexte et, d'autre part, au niveau de la conception, sur la responsabilité particulière affectée à telle ou telle ressource, du point de vue finalisé porté par le système.
Exemple : Le défaut constaté sur le « système de fermeture de la vitre » dû à une rupture mécanique de la tringlerie, à une casse moteur etc.

Cette analyse constitue le premier axe de couplage entre Sûreté de Fonctionnement et ingénierie système. Une approche complémentaire est nécessaire.

Pour satisfaire, en effet, la nécessité de vérifier l'obtenu par rapport au voulu, les systèmes de contraintes correspondants doivent être vérifiables « objectivement » au travers de caractéristiques physiques mesurables: vitesse, énergie, etc. Ces "vues de vérité" dont le principe est établi dans MCR, impliquent de gérer le lien entre factualité foisonnante et description du rôle spécifique affecté à une entité. Cette mise en correspondance n'est possible qu'au travers d'un empilement de niveaux de conceptualisation. ISR a choisi d'organiser ces niveaux aux travers de quatre méta-niveaux hiérarchisés. Sans entrer dans les détails, soulignons simplement que l'information ne parcourt pas systématiquement ces différents niveaux (un conditionnement actif ou passif par exemple ne dépasse pas la méta couche présentation)(cf. table ci après) ;

Méta-Niveau de conceptualisation	***Description***
Applicatif	Niveaux sémantiques qui expriment les finalités du cadre descriptif
Sens	Production de sens tenant de compte de phénomène sensibilisation, habituation, conditionnement… également domaine du reflexe conditionné.
Témoignage	Description relativisée de l'information portée par un événement témoignage, Filtre par première algèbre d'événement propre a chaque point de vue
Transfert	Codage et extraction de l'information (à partir du codage) de l'interaction physique

La répétition d'une même expérience, d'un même test ne donne que rarement plusieurs fois exactement le même résultat. Autrement dit, il s'agit d'analyser les résultats obtenus au travers de classes d'équivalence permettant de faire le lien entre une factualité caractérisée par une diversité potentiellement infinie et une représentation par essence généralisante et réductrice puisqu'elle utilise des structures de description et des domaines de définition finis. Les enjeux, du point de vue de l'analyse de risque, passent par la définition de seuils significatifs autorisant l'analyse.

Exemple : Une défaillance est un événement qui émerge d'une qualification d'une interaction recueillie en un point pendant un certain temps. Ainsi, la réception sur une broche de connecteur d'un niveau de tension inférieur à un seuil de 4 V pendant plus de x ms est assimilé à un signal erroné issu d'un capteur défaillant..

La gestion des différents niveaux de conceptualisation impliqués va permettre de déployer l'analyse de sûreté de fonctionnement « en profondeur » dans une vision orthogonale et complémentaire à celle évoquée au niveau du processus de spécification et de conception système. Ce déploiement va permettre de mettre en évidence la chaîne explicative qui va de l'interaction physique à l'information qui "fait sens" d'un point de vue donné et, grâce à une structure en « chaînes hiérarchisées de cellules descriptionnelles », d'éviter de mélanger des informations de niveaux différents.

Exemple : Dans l'exemple des lève-vitres, la rupture mécanique de la tringlerie empêchant la fermeture de la fenêtre peut-être expliqué par une succession d'efforts supérieurs à l'attendu (caractérisé en Newton) sur un certain laps de temps (phénomènes d'échauffement).

Cette analyse constitue le second axe de couplage entre Sûreté de Fonctionnement et ingénierie de système.

La réalité physique dépasse cependant ***fondamentalement*** *TOUTE* représentation car:

- la portée d'une description est par essence limitée à des capacités descriptives finies liées à un certain niveau de conceptualisation alors que la réalité physique d'où elle tire in fine fondamentalement sa légitimité est, elle, inépuisable. Par exemple : le concepteur

électronique devra considérer la défaillance d'une résistance comme un aléa, qu'un autre cadre descriptif (celui du fondeur de composant) imputera à l'impureté de l'alliage, et un physicien pourrait l'analyser, lui, au travers de la structure atomique…

- la variabilité de l'environnement dans lequel est plongé l'objet de l'étude est, elle aussi, inépuisable. Par exemple la variation de la température, etc.

Il est donc nécessaire, pour « coller » à la réalité, d'introduire autour de la représentation, des caractéristiques attendues de la part d'une certaine réalité physique, un modèle de contexte (et non pas seulement d'environnement), tenant compte de ces deux types d'éléments dans la mesure où ils jouent un rôle dans l'horizon que le concepteur se donne, interviennent dans les tests qu'il réalise, *même s'ils ne sont pas décrits, expliqués, mais expriment le « possible » au travers d'une entité :le modèle du contexte.*
D'un point de vue probabiliste un modèle de contexte décrit la procédure de tirage aléatoire et d'examen des résultats permettant de révéler la forme spatio-temporelle qui globalise l'ensemble des attendus relatifs à une entité (prestation, système, objet technique), dans le cadre spatial et temporel défini par le domaine d'étude. Un domaine d'étude ISR est définie par la conjonction d'un modèle de contexte et d'un modèle de l'entité objet d'étude exprimant le niveau de maîtrise recherché d'une certaine réalité.

Représentation de l'objet technique
La conception des différents systèmes doit in fine se ramener à des ressources, les objets techniques *déjà connus, notamment du point de vue de leur Sûreté de Fonctionnement*. Ce processus nécessite généralement l'empilement de plusieurs horizons de spécification/ conception et se caractérise par une démarche allant du plus particulier/spécifique au plus général/réutilisable. Il implique la création, à des niveaux intermédiaires, de nouveaux couples (produit, objet(s) technique(s)), appréhendés en tant que *ressources* par les systèmes qui les utilisent. Toute la difficulté est dès lors, dans le cadre d'une organisation, de définir une articulation satisfaisante entre les différents points de vue portés par les ressources qui définissent l'horizon de conception et la responsabilité d'une entité organisationnelle donnée.
Cette articulation doit nécessairement se traduire par la création d'objets techniques "partagés", points d'ancrage autour desquels peuvent s'organiser compromis et consensus entre contraintes et exigences issues du processus de conception de différents systèmes. C'est au niveau des ces entités posées consensuellement, que se superposent les différents rôles affectés par chacun des systèmes à une ressource donnée et se construit un ensemble cohérent de propositions décrivant la ressource à créer ou utiliser.
Ces objets techniques qui marquent l'articulation entre différents horizons de conception, systémiers et équipementiers par exemple, **constituent, pour l'analyse de risque, les points de rencontre entre caractéristiques demandées et caractéristiques offertes, en incluant la sûreté de fonctionnement**.

Les principes exposés ci-avant et le choix d'inscription dans le cadre MCR permettent d'aborder la problématique du test et du verdict sous trois angles complémentaires qui doivent être dimensionnés en fonction des exigences de sûreté de fonctionnement, justifiés par les analyses de danger :

- Les incontournables : scénarii de test aboutissant à des ER (Evénements redoutés) mettant en cause les personnes et/ou le matériel ;
- La génération automatique de vecteurs de tests correspondant à différents type d'ordonnancement d'événements ***possibles***, possibles gérés dans une entité spécifique de chaque modèle de contexte ISR : le contrôleur ; qui *animent* les différents agents ;
- Le calcul d'un niveau de confiance que l'on peut avoir dans le fait qu'un périmètre physique donné soit effectivement conforme à un certain point de vue finalisé.

Cette liaison formelle entre spécification et tests laisse présager des avantages conséquents d'un point de vue industriel, qu'il s'agisse d'estimer une conformité ou de passer des test imposés et/ou générés. Ces travaux font l'objet du projet VETESS [4], labellisé par le pôle de recherche « Véhicule du futur », retenu dans le cadre des appels d'offres FUI (Fonds Unique Interministériel).

Synthèse des structures de modélisation
ISR est articulé autour de la représentation de chaque point de vue sous la forme d'un domaine d'étude ayant une double fonction prédictive et explicative.

Les choix des structures de représentations, notamment des méta descriptions de satisfaction/comparaison répondent à deux objectifs fondamentaux :

- Maitriser les dépendances entre produit et objet technique, c'est-à-dire être capable d'estimer les conséquences en terme de dangers (risques ou événements craints liés à l'usage du produit) de défaillances redoutées en matière de sûreté de fonctionnement (objet technique) et, réciproquement, adopter des recommandations en matière de conception technique qui répondent à des dangers inacceptables identifiés au niveau du produit
- Ramener toute situation, qu'il s'agisse d'étude de danger ou d'étude de sûreté de fonctionnement à :
  - Un contexte statistiquement maîtrisé : le modèle contextuel (les possibles), au sens ISR défini ci-avant
  - Un modèle « explicatif » et « prédictif », donc déterministe, permettant de décrire le lien logique entre les données contextuelles (dont les événements redoutés) et les qualifications réalisées sur l'entité générée, objet de l'étude.

Un contexte est la représentation « de ce qui peut arriver » à un moment donné et en un endroit donné du cadre spatio-temporel du domaine d'étude sous la forme d'événements ayant une certaine propension à survenir. Cette propension peut être approximée de façon différente en fonction du type d'événement:

- événements pour lesquels la loi de distribution statistique approxime un ensemble de faits effectivement constatés : retour d'expérience.

  Exemple : données climatiques
- événements, qui peuvent faire l'objet de schémas explicatifs dans un autre cadre épistémique, non pertinent par rapport à la finalité et au cadre de l'étude. La loi de distribution est dans ce cas approximée à partir de formes « explicatives » et du contexte qui leur est associé.

  Exemple : le taux de défaillance d'une résistance suffit lorsqu'il s'agit d'étudier un calculateur, mais ce taux résulte d'un modèle approximé dans le cadre de l'étude fondé sur des infra-modèles physiques.
- Evénement résultants d'opérations de l'esprit réalisées par analogie, induction, par référence à des paradigmes formalisés ou non, par similarité avec des situations jugées analogues ou simplement ressemblantes, etc.
-

  Exemple : le comportement d'un enfant dans une voiture

Exemple commenté d'étude de danger (cadre descriptif d'une prestation d'un produit)
L'exemple qui suit est un modèle fictif extrapolé d'une étude réelle traitant d'une prestation de type « sécurité enfant » relatif à un produit «Véhicule-automobile ». Cette prestation a pour objet d'empêcher un enfant d'ouvrir une vitre ou une porte arrière et de tomber sur la chaussée. Dans cet exemple seule la vision analyse de danger est présentée. Elle s'intègre dans le cadre d'une Ingénierie Système conduite selon les canons d'ISR.

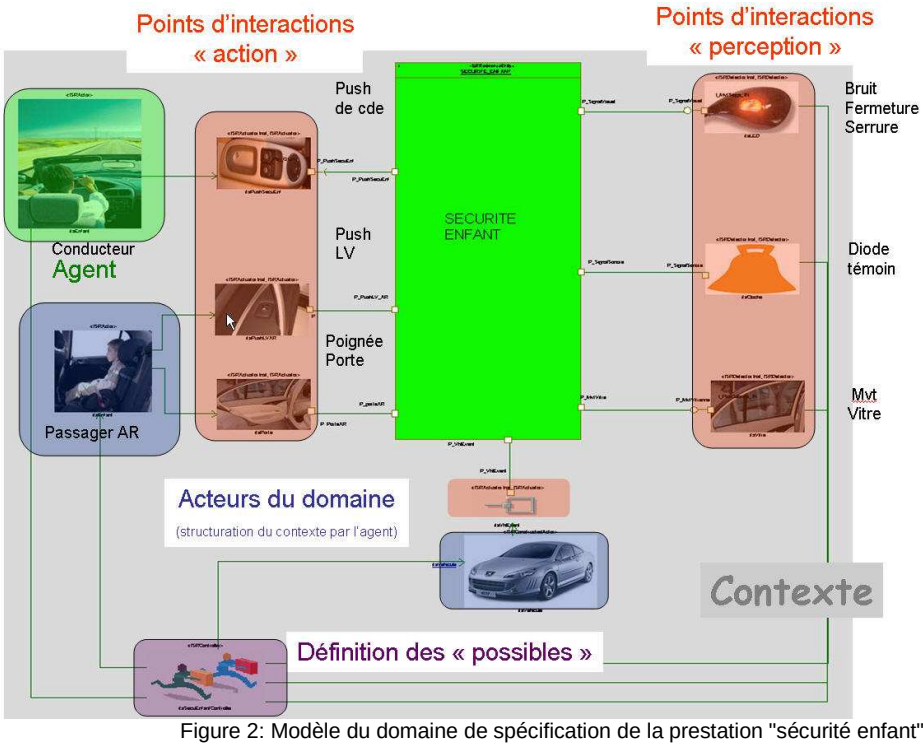

Figure 2: Modèle du domaine de spécification de la prestation "sécurité enfant"

Au méta niveau descriptif où l'on se situe, l'utilisateur est représenté comme agent (« Conducteur »). Le cas considéré, relativement simple, ne nécessite qu'une faible structuration du contexte. On remarque la « voiture » désignant, du point de vue de l'utilisateur un acteur, source d'un certain nombre d'événements qui échappent à son contrôle direct (par exemple, une défaillance ou le fait d'allumer et d'éteindre un voyant en dehors de toute action). Le « Passager AR » représente l'image qu'élabore le conducteur de son enfant assis sur la banquette arrière et des actions qu'il peut réaliser.
Dans ce contexte, les études de danger vont porter sur les distorsions entre cette image construite que ***devrait avoir l'utilisateur***, image qui correspond à l'entité relativement déterminée, et l'image qui lui est effectivement suggéré, via ses interactions avec le produit, déterminant les « possibles ».
Les concepts ISR d'actuateur et de détecteur matérialisent ces points d'interaction, tels qu'un utilisateur type se les figure. Ils ne référencent en aucun cas des objets physiques. L'actuateur « PUSH LV » dans le diagramme ci-avant ne désigne nullement le PUSH physique mais le fait que l'utilisateur a intégré dans son psychisme qu'il pouvait effectivement contrôler le mouvement voulu d'une vitre via une interaction avec le produit, extension de son corps propre, en un point symbolique, le PUSH. Il en est de même pour les détecteurs qui permettent de gérer la correspondance entre le contexte qui devrait être perçu par l'utilisateur et le contexte qu'on suppose qu'il perçoit effectivement.
Les événements redoutés sont issus de dysfonctionnements affectant ces deux aspects. « Ce que l'utilisateur devrait percevoir ou pouvoir faire et qu'il est effectivement amené à percevoir et pouvoir faire». Ils expriment un dysfonctionnement lié à une distorsion dans la perception du contexte et/ou une incapacité d'agir (perte de contrôlabilité) par rapport à la description des possibilités offertes par le produit, telles qu'elles doivent être intériorisées.
L'analyse de dangers est construite sur le fondement d'une Analyse Préliminaire exprimée sous forme de scenarii issus d'une analyse finalisée du cycle de vie. Elle intègre éventuellement plusieurs prestations afin d'étudier les effets induits par les distorsions ; exemple : condamnation automatique du véhicule entraînant un bruit de verrouillage assimilé à l'activation de la sécurité enfant.
L'analyse de danger dans ISR représente formellement les événements qui caractérisent l'exposition au risque, les périodes critiques, des événements craints et leur sémantique qui vont déterminer la sévérité et la contrôlabilité.
Cette structure d'analyse est synthétisée dans le schéma ci-après :

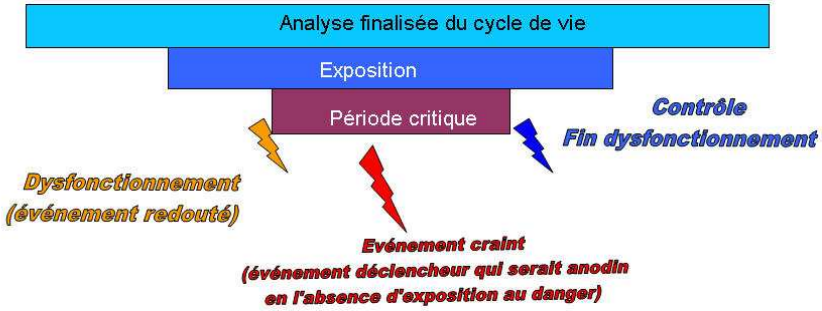

Figure 3: Exposition au danger

La structure de représentation des distorsions possibles (envisagées, vraisemblable ou non) distingue les événements contribuant à leur apparition (concept ISR d'événements contributifs), les événements redoutés rendant possibles la survenue effective d'événements craints, du point de vue d'un ou plusieurs enjeux classifiés selon les grilles de gravité qualitatives (Gravités d'ER). Dans un cadre ISO CD 26262 [5], l'***exposition*** au danger est définie par un certain contexte définie dans le cadre des enjeux permettant d'estimer la ***Sévérité***. La contrôlabilité

est déterminée par la capacité du conducteur à mettre fin à la période critique avant la mise en cause des enjeux de sécurité. Dans notre exemple l'exposition est estimée à 100% du temps de roulage.

Réf	Fonction ->UC	Séquence de référence ou état de référence	événement initiateur du sous cas d'utilisation	Mode de défaillance	Déroulement scénario	Evénement Redouté	Situation aggravante
Situation de vie : vie utile y compris crash							
UC2 Inhiber la sécurité enfant			**Préco: Contact ON: sécurité enfant activée**				
ER11	**désinhiber la sécurité enfant**	**Cas nominal**	**P_PSEC_InfoSecuEnfInactive**	Perte info	**Cas d'une détection de sécu enfant passive (position bouton) et non active (LED).** La sécurité enfant n'est plus active bien que le bouton apparaisse bien comme enfoncé. Le conducteur est conforté dans cette croyance par le buit que font les serrures lors de la condamnation centralisée automatique.	Sécurité enfant désactivée perçue activée	Roulage

Figure 4: Exemple partiel de grille d'analyse de danger

Le scenario aboutissant à l'émergence d'un événement craint peut être généré à partir d'un cadre descriptif spécifique à l'étude de la prestation, dérivé du cadre descriptif objet de l'étude. On est généralement conduit à introduire des acteurs supplémentaires. Comme dans le cas donné en exemple, le fait de faire figurer la prestation « condamnation du véhicule » afin d'identifier des effets de bord entre deux cadres finalisés distincts. Dans le cas présent, le bruit d'un verrouillage des serrures à un sens dans deux cadres différents, ce qui conduit à la nécessité soit de générer un bruit différent, soit de mettre en place un moyen de perception complémentaire (une diode témoin par exemple).

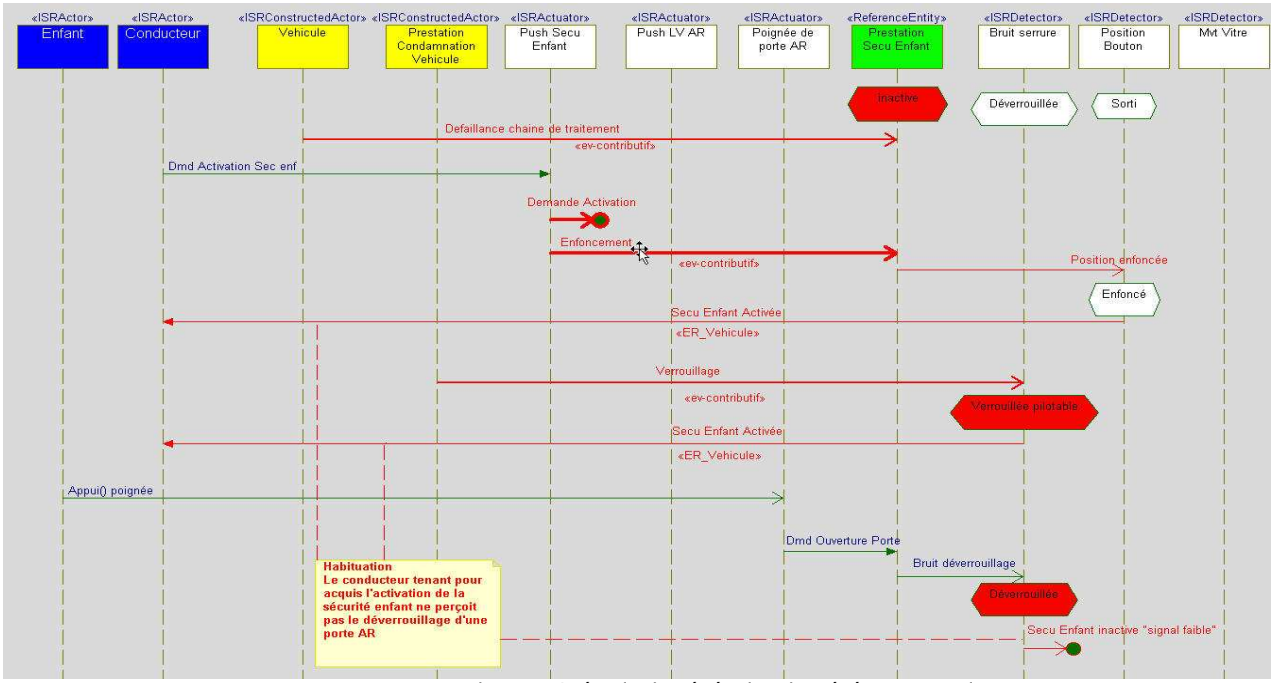

Figure 5: Scénario de génération d'un événement craint.

De l'analyse de danger à la sûreté de fonctionnement

Etant donné l'ampleur du sujet, le traitement de la sûreté de fonctionnement dans le cadre conceptuel définie par ISR sur fondement MCR ne peut être ici qu'évoquer.

A la différence des études de dangers qui portent sur le produit, les études de sûreté de fonctionnement portent sur l'objet technique. Elles se déploient dans ISR selon deux dimensions complémentaires orthogonales, la première analyse la responsabilité des ressources dans le respect de la responsabilité globale du tout qui les utilisent (processus d'analyse spécification/conception système), le second analyse la chaîne de conceptualisation qui va du recueil de l'interaction physique jusqu'à l'expression de la sémantique.

Il convient après ces rappels d'insister sur deux caractéristiques majeures :

1) L'articulation entre produit et objet technique est réalisée de façon biunivoque dans le cadre d'un processus itératif, par l'intermédiaire d'un triple questionnement portant sur

- La complétude : tout événement défini au niveau prestation peut-il être interprété comme le résultat d'un ou plusieurs événements représenté au niveau technique ? Autrement dit, a-t-on tout concrétisé ?
- La Consistance : peut-il y avoir ambigüité d'interprétation d'un certain événement « lorsqu'un même événement qui relève de la conception technique se voit octroyer plusieurs sémantiques au niveau des prestations ?
  Exemple : bruit de la serrure de porte liée à la fois à la condamnation du véhicule et à la sécurité enfant.
- La suffisance : Tout événement représenté au niveau technique peut-il être justifié par rapport au cadre défini par la prestation via la conception de la solution technique?

Exemple (extrait d'une problématique de lève-vitre)

Prestation	Applicatif	Transfert	commentaire
Appui-court (vitre en position haute)	Demande de descente automatique (moteur inactif :qualification préalable)	Tension >4V et <6V entre 50 et 200ms sur E1	Deux impulsions en moins de 500ms sont considérés comme exprimant la même demande (pas d'arrêt ou de reprise du mouvement)
		Temporisation de 500ms	
Appui-court (vitre en descente)	Demande de descente automatique (moteur actif :qualification préalable)	Tension >4V et <6V entre 50 et 200ms sur E1	
		Temporisation de 500ms	

2) Classiquement la Sûreté de Fonctionnement distingue les origines internes et externes d'une défaillance.
Le concept ISR de domaine d'étude représenté comme l'interaction d''un contexte et d'une entité relativement déterministe va modifier cette structure d'analyse comme le présente la figure suivante :

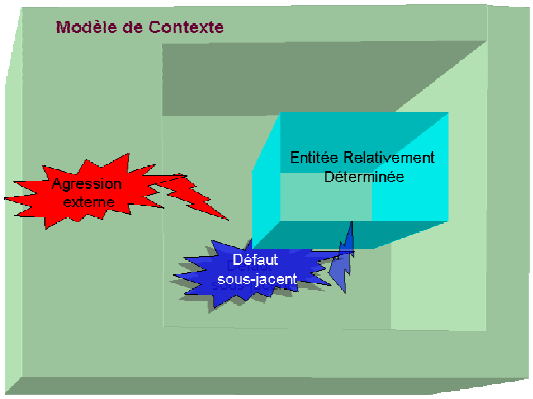

Figure 6: Domaine d'étude – contexte : environnement et niveau sous-jacent.

Une structure spécifique, l'entité relativement déterminée, va représenter le niveau de maîtrise technique minimal que l'on ***veut*** se donner d'une certaine réalité physique afin de garantir un certain niveau de qualité du point de vue des prestations qu'il supporte.
Cette modification n'est pas anodine, elle réconcilie *structurellement* ingénierie système et sûreté de fonctionnement.
A partir du moment où sont excluent du domaine maîtrisé – déterministe – les défauts « sous-jacents » pour être inclus dans le modèle de contexte, une séparation claire est opéré entre statistiques, déterminisme et lois de probabilité. Par essence, le modèle contextuel repose sur une base statistique estimée suffisamment maîtrisée eu égard aux enjeux (par exemple on accepte qu'il y ait une chance sur 10000 pour qu'un certain type de défaillance intervienne dans le cadre temporel défini par le domaine d'étude). La procédure qui consiste à générer un évènement (via le contrôleur) à partir de ce modèle tient lieu de procédure de tirage aléatoire permettant de découvrir une ***forme spatio - temporelle,*** celle du modèle déterministe exprimant le domaine de maîtrise.
Les rétroactions de cette forme vers son contexte, recueillies via les « *detector* » ISR spatialement référencés, tiennent compte de l'historicité des évènements l'ayant ***générée,*** telle qu'elle est, **à partir d'une référence initiale, d'un générateur racine de l'arbre des probabilités factuelles MCR.** C'est donc par analyse de cette forme que la loi de probabilité factuelle peut être calculée et la fréquence des événements redoutés estimés.

Conclusion

ISR, fondé sur MCR, se propose d'élaborer une approche structurée et rigoureusement fondée de l'ingénierie système dont la portée est loin de se réduire au seul domaine industriel. Cette approche intègre ***génétiquement*** la problématique de l'analyse de risques. ISR poursuit aujourd'hui son développement, structuré par les trois niveaux d'exigences qu'elle s'est donnée: une fondation conceptuelle irréfutable sur la base de MCR, une efficacité pragmatique constatée sur la base de l'enchaînement de projets pilotes aux ambitions accrues (aujourd'hui VETESS), la création d'environnements utilisateur adaptés.

Références

[1] Mioara Mugur Schächter - Sur le tissage des Connaissances » (Lavoisier)
- Foundation of Science – volume 7 – Nos:1-2, 2002 Quantum Mechanics, Mathematics Cognition and Action
- Proposals for a Formalized Epistemology (KLUWER ACADEMIC PUBLISHERS)
- http://www.mugur-schachter.net/ (textes téléchargeables)
[2] Michel Bitbol : Mécanique Quantique : une introduction philosophique (Flammarion 1999)
[3] Wittgenstein 'De la certitude" Gallimard 1969
[4] VETESS - http://www.adira.com/blog/2008/03/10/Deux-projets-du-Pole-Vehicule-du-Futur-selectionnes-lors-d-un-appel-a-projets-interministeriel.html
[5] ISO CD 26262 – Road Vehicle – Functional Safety - 2008