IMdR Info
Lettre d'information
de l'Institut pour la Maîtrise des Risques
Sûreté de fonctionnement - Management - Cindyniques
n°40
1er trimestre 2019

sommaire

Edito

Lambda Mu 21 « Maîtrise des Risques et transformation numérique : opportunités et menaces »

Ce cru champenois 2019 de notre congrès Lambda Mu 21 était clairement inscrit sous le signe stratégique des mutations numériques profondes que connaissent nos industries et plus généralement l'ensemble de nos sociétés civiles, et ce pour le plus grand bonheur de tous… mais attention ! Si l'explosion des technologies qui en résultent démultiplie les opportunités, bénéfices et apports fonctionnels vis-à-vis des utilisateurs finaux que nous sommes, « la part d'ombre » qui se développe dans le même temps véhicule son lot de menaces que nos différents métiers se doivent de contrecarrer ou du moins vis-à-vis desquelles ils doivent nous protéger !

Le programme Lambda Mu 21 a traité largement des deux aspects avec réalisme et transparence, et non sans une certaine ambition théorique et méthodologique, sans sacrifier pour autant les disciplines historiques… Bien sûr notre congrès a fait la part belle aux systèmes autonomes et connectés dont le déploiement opérationnel ne cesse de marquer notre environnement : véhicules ou trains autonomes, drones, usines connectées concentrent différents types d'innovations technologiques que nos méthodes se doivent d'appréhender, d'autant plus que leur exploitation opérationnelle est associée à de nouveaux facteurs de complexité : ces systèmes sont désormais plongés dans des environnements totalement ouverts, l'homme, le plus souvent, n'est plus dans la boucle, et de nouveaux algorithmes embarqués, relevant des techniques d'Intelligence Artificielle se doivent de détecter et interpréter à tout moment les situations se présentant, et de décider du comportement ou de la trajectoire à adopter…

Ces nouvelles thématiques, fers de lance des éco systèmes d'innovation qui imprègnent désormais notre tissu industriel à tous les niveaux, à savoir « Intelligence Artificielle », « Big Data », « Block Chain », « Traitement Automatique des Langues » ont clairement été adressés lors de cette semaine, et jurons qu'elles figureront bientôt en tête de liste du Vade Mecum du Parfait Fiabiliste…

L'autre volet à propos duquel le contrat a été bien rempli, concerne les multiples apports de ces innovations, cette fois non pas à l'adresse des industriels ou des sociétés civiles, mais visant à enrichir la « boîte à outils » des acteurs de la Sûreté de Fonctionnement et de l'Assurance des Performances que nous sommes: « Health and Usage Management System », « Maintenance Prédictive » (ou prévisionnelle…), « Suivi des Facteurs Organisationnels et Humains » grâce au TAL (Traitement Automatique des Langues) ont été largement traités dans le cadre de sessions spécifiques, mais il en est de même des disciplines MBSA/MBSE en support des activités de validation par virtualisation et simulation…

Enfin, « last but not least », une journée entière a été consacrée à la « Cyber sécurité » dans un lieu emblématique, l'amphithéâtre « Clovis », et pour la première fois, des robots ont participé à notre table ronde, ce qui montre que notre institution, tout en assumant 40 ans d'histoire fructueuse et pluridisciplinaire, se projette sans hésitation dans un avenir technologique à la fois riche en innovation et porteur de nouveaux champs de complexité !

Emmanuel ARBARETIER, APSYS
Président du jury des λμ d'or

Les tutoriels

La journée des tutoriels est le traditionnel précurseur du congrès λμ. Un bien subtil mélange entre des jeunes qui souhaitent découvrir le domaine de la maîtrise des risques, et des moins jeunes animés par une curiosité sans cesse renouvelée. Chacun y trouve un intérêt selon sa sensibilité, d'autant que tout est fait au travers de l'organisation toujours millimétrée, pour le susciter. Si les libellés des thèmes qui structurent cette journée ne surprennent plus la plupart des participants historiques que sont nos très chers fiabilistes, leur contenu s'adapte toujours aux problématiques et techniques actuelles.

Parmi ces thèmes, on retrouve bien sûr « ***L'historique*** » Méthodes de sûreté de fonctionnement (SdF). Alors, pas de révolution sur les méthodes de la SdF…Guy Planchette, le Président d'honneur de l'IMdR nous montrait d'ailleurs à l'occasion du bilan du congrès, une Analyse des Modes de Défaillances de leurs Effets et de leur Criticité (AMDEC) de plus de 40 ans et force est de constater qu'elle ne nous a pas dépaysés. Non, pas de révolution mais bien une adaptation à de nouvelles installations industrielles, à de nouveaux risques qu'il faut quantifier, et à l'apparition de nouveaux logiciels notamment.

Il y a également, « ***L'habitué*** » Facteurs humains et organisationnels (FOH) – cindyniques, dans lequel il n'est jamais superflu de rappeler les concepts cindyniques. D'ailleurs que signifie le terme Cindynique ? Pour les personnes qui liraient ces quelques lignes et qui n'auraient pas la réponse à cette question, une séance de rattrapage est programmée en 2020… Au cœur de ce thème, signalons le Retour d'Expérience FOH qui doit se tailler la part du lion centrée sur la technique. On constate également que les FOH peuvent être accompagnés d'outils de modélisation…oui, de modélisation.

L'enjeu auquel sont confrontées les organisations consiste à tendre vers des performances optimales, dans un contexte où les informations sont incomplètes, les ressources financières limitées et où les défaillances peuvent avoir des conséquences critiques. Aussi, « ***L'incontournable*** » Management des risques et analyse de la décision, donne des clés précieuses et rassurantes sur la prise de décision dans un monde incertain.

Enfin, le 4ème et dernier thème est également celui du congrès : Maîtrise des risques et transformations numériques ». Il met en exergue de réelles opportunités, au travers du Traitement Automatique du Langage Naturel qui offre un nouvel angle d'exploitation des REX ou encore du Prognostics and Health Management utile pour de la maintenance prédictive. Par ailleurs, comment ne pas aborder la cybersécurité, avec des systèmes de plus en plus ouverts et soumis à des menaces nouvelles : cyberattaques, prises de contrôle à distance, intrusions etc.

N'oublions pas les témoignages de jeunes ingénieurs qui ont jalonné cette journée. Les participants ont pu découvrir, au travers de regards neufs, la sécurité industrielle des infrastructures gazières avec Maëlle (GRTgaz), la cybersécurité avec Nanding (EDF), le suivi et l'analyse du REX ferroviaire avec Camille (RATP), les études de sûreté de fonctionnement avec Elodie (Air Liquide) et enfin, les études de sûreté avec Arthur (SECTOR). Bonne chance à eux pour leur carrière professionnelle, qu'on espère longue sur la route de la maîtrise des risques.

Arnaud BERLATIER, GRTgaz
Animateur des tutoriels du Lambda Mu 21

les ateliers de l'IMdR

Les Groupes de Travail et de Réflexion (GTR) de l'IMdR, lieux d'échanges et de rencontres, permettent d'approfondir certains sujets et d'apporter des réponses concrètes aux préoccupations de maîtrise des risques et de sûreté de fonctionnement. Ils permettent de croiser les approches et les réflexions des industriels, universitaires et autres représentants de sociétés membres. Portant sur des sujets variés (domaine technique, facteur humain, facteur organisationnel, aspects économiques, ...), les groupes se fixent leur calendrier de travail et leurs objectifs et peuvent être amenés à publier leurs travaux. Le congrès Lambda Mu est l'occasion, pour un certain nombre de ces groupes, de se faire mieux connaître. Pour cela, des ateliers sont inscrits au programme. Nous remercions ici les animateurs des ateliers qui ont bien voulu rédiger quelques lignes sur leurs travaux.

Atelier 1 : Maîtrise de la complexité des systèmes et innovations de rupture transversales

Cet atelier a identifié dans des domaines applicatifs non technologiques ou industriels les différences de représentation et de traitement de la complexité pour décision ou adaptation comportementale. L'état de l'art des méthodes innovantes et de leurs insuffisances a montré des pistes de développement de méthodes traitant des systèmes complexes.

Après trois focus rapides sur l'Analyse Intégrée des Risques, les véhicules autonomes, et les organismes vivants, les participants ont notamment souligné la difficulté de comprendre et de rendre compte du phénomène d'émergence. Il a beaucoup été question des enjeux de modélisation, de la difficulté de gérer le niveau de détail, et de choisir les langages pertinents pour ne pas trahir la complexité des systèmes. Il a enfin été souligné que la nécessité de maîtriser tous les axes d'évolutions d'un système et de son environnement à travers l'ensemble de son cycle de vie contribue à accroître et diversifier cette notion de complexité.

Reste que les systèmes vivants demeurent à l'unanimité « le summum » de complexité jamais présentée par aucun autre type de système, puisqu'en perpétuel échange avec l'environnement, mais aussi apprentissage, adaptation, voire évolution, à travers une gestion dynamique de mécanismes d'auto-organisation…

Atelier 2 : Actualité du GTR « maintien de la méthodologie FIDES »

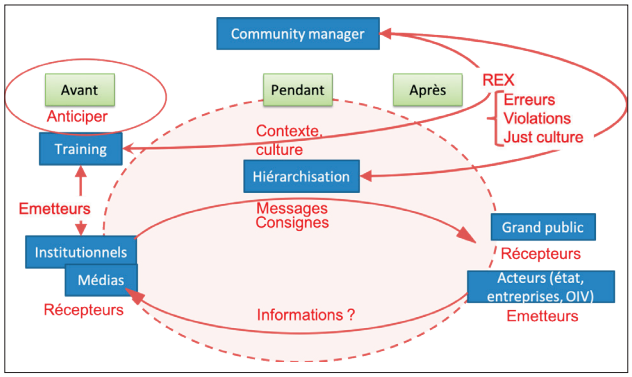
À partir des travaux du GTR FIDES, cet atelier a présenté : le modèle de fiabilité FIDES (projet IMdR) pour les condensateurs film, des nouveaux guides méthodologiques, les travaux du nouveau sous-groupe d'application au domaine spatial, l'état des travaux sur la normalisation IEC de FIDES (IEC 63142), ainsi qu'un point global sur l'avancement de la méthodologie FIDES.

Les échanges ont été nombreux. Des possibilités de nouveaux traitements à partir de la modélisation FIDES ont notamment été abordées, comme par exemple l'utilisation de FIDES pour définir des programmes d'essais accélérés. Rendez-vous a été pris en 2020 pour un nouvel atelier FIDES lors du Lambda Mu 22.

Atelier 3 : Une vision à partager de la gestion de crise

Cet atelier a débattu des travaux du GTR « Gestion de crise » en ciblant sur l'une des thématiques qu'il se propose de travailler en lien avec la thématique du congrès : la place de l'innovation dans la gestion de crise : intelligence artificielle, intégration des médias sociaux…

Les participants de l'atelier se sont structurés en deux sous-groupes de travail, le premier traitant successivement de l'innovation technologique (outils numériques, de communications et réseaux sociaux), puis de l'innovation méthodologique (REX, compétences non techniques…) et enfin de l'innovation organisationnelle tant en préparation d'exercices qu'en résilience de l'organisation de crise sur le terrain (menaces sur le site de gestion de crise, compositions d'équipe hétérogènes, complexité relative des exercices et de la crise réelle). Le second sous-groupe s'est focalisé sur le besoin de communiquer en situation de crise et sur l'arrivée du community manager dans les dispositifs de crise. Un des schémas produits au cours de l'atelier est reproduit ci-dessous.



Le retour de cet atelier vers les travaux de fond du GTR Gestion de crise a été particulièrement rapide puisqu'une journée IMdR et un retour vers le GTR Normalisation sont déjà programmés. La création d'un sous-groupe portant sur « Innovation et gestion de crise » est par ailleurs imminente (IMdR/ARMIR), avec pour premier

objectif la production de fiches portant un regard critique sur les innovations et leur intégration dans l'existant.

Atelier 4 : Gestion des risques et transformation numérique : comment faire coexister sûreté de fonctionnement et cybersécurité ?

Cet atelier a présenté les enjeux émergents de la cybersécurité dans les études de sûreté de fonctionnement et les questions de coexistence efficace des approches technique et culturelle des deux domaines. La nature du risque, les aspects normatifs et méthodologiques, les exigences de conception, la coexistence sûreté / cybersécurité ont été discutés.

Il est apparu que ce dernier point trouve un écho important dans la communauté IMdR. La réflexion, le retour d'expérience et l'élaboration de bonnes pratiques concernant la gestion en parallèle de la sûreté de fonctionnement et de la cybersécurité feront donc l'objet des travaux à venir du GTR Cybersécurité des installations industrielles et Internet Industriel des Objets (IIoT).

Atelier 5 : La fiabilité des structures dans l'univers des risques

L'Analyse de la Fiabilité des Structures (AFS) évalue les risques de défaillance de structures industrielles ou de génie civil. Cet atelier, proposé par le GTR « Sécurité et Sûreté des Structures » de l'IMdR, a replacé l'AFS dans l'analyse des risques et souligné sa capacité à évaluer la probabilité de défaillances rares. Cette capacité repose sur la disponibilité de modèles de comportement de la structure, de données et connaissances sur les incertitudes affectant leurs paramètres d'entrée et de méthodes numériques, parfois avancées, nécessaires à l'estimation de la probabilité ou à l'analyse de sensibilité à un coût computationnel industriellement acceptable.
Concernant les données, les participants ont apprécié l'apport des nouvelles technologies de surveillance des ouvrages pour valider les prévisions des modèles (cf. l'exposé sur les mesures par système de satellites (GPS, GNSS) en temps réel des déplacements de ponts (écartement des pylônes par suite de la dilatation thermique)). Dans d'autres cas néanmoins, il est vain d'espérer un accroissement sensible des données disponibles (coût des essais expérimentaux de structures de génie civil).

Concernant les modèles de comportement, les échanges ont montré que de nombreux phénomènes sont connus mais qu'un effort de modélisation reste à poursuivre dans certains cas (phénomènes d'impact, risque rocheux).
Concernant les méthodes numériques, des développements restent nécessaires, notamment pour faire face à la complexité grandissante des modèles physiques. Parfois, les méthodes sont en avance sur certains besoins industriels, dont l'évolution potentielle n'est donc pas problématique (cf. fiabilité dépendant du temps).

Enfin, l'atelier a montré comment ces évaluations de fiabilité pouvaient, pour finir, trouver une utilisation directe dans le processus de décision industriel relatif à l'intégrité des structures (cas des conduites forcées des centrales hydro-électriques).

Atelier 6 : Propagation d'incertitudes ➠ de l'élément aux systèmes !

Cet atelier s'est penché sur le passage des méthodes de propagation des incertitudes élémentaires à l'échelle des systèmes et des systèmes complexes. La propagation d'incertitudes de modélisation, après une décennie de progrès, commence à traiter correctement et simplement la modélisation de systèmes complexes.

Atelier 7 : L'importance des ressources linguistiques pour le TAL

Cet atelier a permis d'échanger autour d'expériences d'utilisation d'outils de Traitement Automatique des Langues (TAL). Le cœur du TAL réside dans l'analyse automatique des textes. Le contenu de ceux-ci et la langue utilisée étant propres à chaque métier, des ressources linguistiques adaptées peuvent contribuer à l'amélioration des traitements proposés.

Les différents types de ressources, leurs avantages et inconvénients ont été présentés et discutés. Un intérêt certain ressort pour ces problématiques et l'idée d'un nouveau GTR de l'IMdR dédié au TAL a été proposée.

Atelier 8 : Maîtrise de la transition entre les exigences de sécurité au niveau système et les exigences de sécurité du logiciel et du matériel électronique

Cet atelier s'est penché sur la déclinaison des exigences de sécurité jusqu'au système ou au boîtier pour définir le juste niveau de barrières de sécurité, ainsi que le niveau de détail nécessaire au développement d'un logiciel ou du matériel contenant des fonctions de sécurité.

Les discussions ont permis de mettre en évidence que cette déclinaison avait une variabilité importante d'un secteur à l'autre mais que les difficultés liées à ces sujets de déclinaison des exigences de sécurité « au bon niveau » sont partagées. D'autre part, l'importance de la co-ingénierie et du rôle des architectes dans la déclinaison des exigences de sûreté de fonctionnement aux bons niveaux a été soulevée par les participants, ainsi que le rôle primordial d'un processus d'intégration pour porter la réponse à ces exigences.

Jean-Marc CAVEDON, IMdR
Président des GTR

➠ *En savoir plus sur les groupes de travail et de réflexion (GTR) sur le site web de l'IMdR* ***www.imdr.eu****.*

λμ d'or et prix

Les prix λμ d'or récompensant les quatre meilleures communications conférences et interactives ont été remis par M. Emmanuel Arbaretier (Apsys), Président du jury, comme suit :

• **λμ d'Or** «Transformation Numérique : opportunités et menaces» à Jean Caire (RATP) et Sylvain Conchon (CONIX) pour *« Influence 2.0 – comprendre les opérations d'influence dans un monde hyperconnecté »*

• **λμ d'Or** «Méthode et Industrie» à Emilie Miranda, Michel Broniatowski (Université Pierre et Marie Curie) et Maëva Biret (SAFRAN) pour *« Stratégie de planification d'essais pour la caractérisation de contrainte admissible en fatigue des matériaux »*

• **λμ d'Or** «Méthode et Industrie» à Suber Rangra (IRT SystemX), Mohamed Sallak, Walter Schön (Université de Technologie de Compiègne) et Fabien Belmonte (Alstom) pour *« Risk and safety analysis of mainline autonomous train operation: context challenges and solutions »*

• **λμ d'Or** du «public» à Céline Vinuesa, Cyrille Folleau (SATODEV), Stéphane Collas (TOTAL) et Frédéric Doux (LGM) pour *« Nouvel outil d'évaluation des fréquences d'occurrence pour les études de risque »*

Les prix « Recherche & Industrie » récompensant les travaux de thèse réalisés en collaboration avec l'industrie ont été remis par M. Olivier Delabroy (Air Liquide) et M. Pierre-Etienne Labeau (Ecole Polytechnique de Bruxelles) qui sponsorisaient ces prix à hauteur de 1 000€ chacun à :

• L-R. LAGADEC (SNCF RÉSEAU), I. BRAUD, P. BREIL (IRSTEA), B. CHAZELLE, L. MOULIN (SNCF RÉSEAU) pour *« Présentation et évaluation d'une méthode de cartographie du ruissellement pour améliorer la gestion des risques liés à l'eau sur les voies ferrées »*

• P. LAKOMICKI, Y. TOURBIER (RENAULT), B. CASTANIER (Université d'Angers), A. GRALL (UTT) pour *« Encadrement de la fiabilité du véhicule autonome pour guider les tests de validation »*

« C'était ma première participation au congrès Lambda Mu et j'en garde une excellente impression, beaucoup de rencontres, de temps d'échange et des présentations de grande qualité. Le palais des congrès de Reims était un peu intimidant pour présenter les résultats de mon travail de thèse mais l'auditoire était très réceptif et bienveillant. Je me réjouis d'avoir noué de nombreux liens bien que ma thématique de recherche sur les risques naturels liés à l'eau soit plutôt modestement représentée. J'ai également eu l'honneur de recevoir le prix Recherche et Industrie, c'est un immense plaisir, une grande satisfaction pour mon travail de thèse et un bon coup de pouce pour la poursuite de notre projet à l'intérieur et à l'extérieur de l'entreprise. Je tiens à remercier l'IMdR pour ce travail de fédération d'acteurs qui partagent des problématiques et des intérêts communs malgré des environnements de travail très variés. Ces évènements donnent un joli tour d'horizon du domaine de la maîtrise des risques. »

Lilly-Rose LAGADEC
lauréate du prix recherche et industrie

Table ronde

« Stratégie des entreprises et transformation numérique »

La table ronde consacrée à la stratégie des entreprises face à la transformation numérique a réuni trois représentants de grands groupes : Monsieur Olivier DELABROY, Vice-Président Group Digital Transformation à AIR LIQUIDE, Monsieur François DIONIS, chef de plusieurs projets de transition numérique à la Direction de la Production Nucléaire et Thermique d'EDF et Monsieur Michel EYMARD, Directeur Technique de SAFRAN.

Après s'être présentés dans un premier tour de table, les intervenants ont d'abord examiné les opportunités offertes par la transformation numérique pour la stratégie de leurs entreprises.

François DIONIS a d'abord indiqué que la transition numérique a commencé à EDF par l'équipement des rondiers chargés de la conduite d'installations avec des applications mobiles partageant des données et pouvant être démarrées, interrompues puis reprises. EDF s'est lancé dans le *big data* avec la collecte d'informations venus des systèmes d'information et des processus. Un gros travail est réalisé pour installer des capteurs et les connecter au système d'information et la CAO. L'objectif est d'abord de pouvoir tirer le maximum de données des équipements (vibrations, températures, pressions...) afin d'anticiper des défaillances et pouvoir faire de la maintenance prédictive à partir de cet *e-monitoring*. Il faut aussi que l'opérateur de terrain ait un retour d'un superviseur des informations qui lui sont nécessaires (une position de vanne, un cadenas intelligent de consignation...). Dans les faits, les objets connectés sont difficiles à mettre en œuvre dans un contexte industriel lourd tel qu'une centrale nucléaire et obtenir un maximum d'efficience des objets connectés et de la mobilité. Une expérience pilote est menée à la centrale du Blayais pour amener du réseau en tout point de la centrale et a vocation à être généralisée.

Pour Olivier DELABROY, les opportunités de création de valeur par le digital sont multiples. La finalité est d'avoir des clients et des collaborateurs satisfaits. Il utilise l'acronyme ACE (A pour Actifs, C comme Clients, E comme Ecosystèmes ou Employés).Concernant les Actifs, AIR LIQUIDE a la chance de pouvoir disposer déjà de 15 ans de données issues des SCADA des différentes usines. Il est possible désormais d'apprendre du passé et connaitre les réglages optimaux. AIR LIQUIDE a centralisé à Saint-Priest, près de Lyon, le pilotage de la vingtaine d'usines de France. Après un an d'expérience, un tel centre de pilotage va être installé à Shanghai pour les usines de Chine et à Kuala Lumpur pour celles du Sud-Est asiatique. Les mêmes solutions de maintenance prédictive vont pouvoir être déployées partout. Les changements de pièces peuvent être programmés pendant les campagnes de maintenance des clients. C'est un enjeu d'efficacité mais aussi d'expérience client. Les Clients disposent désormais d'un portail leur permettant d'effectuer leurs commandes en ligne et d'obtenir des informations sans avoir à téléphoner à un *back office* : factures, nombre de bouteilles installées... Cette pratique venue en France depuis les Etats-Unis suite au rachat d'Airgas est en cours de déploiement de manière accélérée sur l'Europe et l'Asie. Concernant l'écosystème des collaborateurs, l'enjeu est de changer les documents en données accessibles à tout moment. Cela passe par l'élaboration et le partage de documents collaboratifs, par l'analyse sémantique des multiples écrits réalisés dans les usines ou la consultation pear to pear par un opérateur débutant d'une vidéo filmée dans une autre usine par un opérateur expérimenté lors d'une opération particulière, de maintenance par exemple.

Michel EYMARD a indiqué qu'on retrouve les mêmes préoccupations chez SAFRAN avec le double objectif d'améliorer la performance de l'entreprise et apporter de la valeur aux clients. Pour ce qui concerne l'administratif, l'objectif est de diviser par 6 le nombre des 60 000 procédures en usage actuellement. Le digital n'est pas la seule solution mais est *le booster* pour revisiter les pratiques et simplifier les processus. Une tendance lourde du futur est l'augmentation du trafic aérien (on prévoit un doublement d'ici 2040) tout en devant réduire l'impact environnemental. Il faut respecter les objectifs de la COP 21 et réduire les émissions de CO_2 et de NOx ainsi que le bruit autour des zones aéroportuaires. On peut prévoir une pénurie de pilotes et un objectif prioritaire est de développer des avions pouvant être pilotés, dans un premier temps, avec un seul pilote avant d'envisager des avions sans pilote. On commencera tout d'abord par le fret aérien. La première étape est donc de disposer des données avec des capteurs de différentes natures pour des systèmes d'avionique avancés qui permettront d'atteindre cet objectif. Beaucoup de données sont créées tous les jours (54 000 décollages et atterrissages par jour avec des produits SAFRAN) et seulement une faible proportion, quelques pour cents, sont exploitées. L'enjeu est d'exploiter et d'intégrer toutes les données. Les ruptures technologiques à venir concernent l'hybridation propulsive, le stockage avec de l'hydrogène, l'avion électrique. La fabrication additive fait l'objet d'un investissement important : un projet notamment est en cours pour permettre de remplacer 250 pièces par une seule. Il est très important d'assurer la continuité digitale depuis la conception, la production, le support et les services. Une industrie 4.0 a été mise en place, s'appuyant sur trois piliers : l'ingénierie 4.0, l'usine 4.0 et les services 4.0. Un jumeau numérique (digital twin) accompagnera chaque produit depuis sa conception jusqu'à son exploitation. Lors de celle-ci, les données recueillies permettront d'effectuer les maintenances en concertation avec les compagnies aériennes. Au-delà des moyens, la transformation numérique amène à changer la manière de travailler avec plus de collaboratif, plus de transfert d'information, plus d'agilité, plus de transversalité dans le management. De nouvelles compétences sont nécessaires notamment des *data scientists*. Mais cette

transformation doit être réalisée en respectant l'exigence de non-régression de l'opérationnel.

Les intervenants de la table ronde ont ensuite présenté les menaces qui accompagnent la transformation numérique.

Pour François DIONIS, la première menace est la fuite des données. Il est hors de question de laisser sortir des données d'exploitation de centrales nucléaires. Tout projet est audité et fait l'objet de corrections s'il ne respecte pas des règles drastiques de cybersécurité. Toutes les composantes (mobilité, *data lake*, système d'information, objets connectés) passent au crible de la cybersécurité. Il s'agit de maîtriser les informations, les connaissances. EDF a décidé de passer du monde de la publication habituelle (word, pdf) au monde des données structurées. Mais les données qui doivent pouvoir être partagées avec les opérateurs sur le terrain ne doivent pas fuiter. Il faut aussi tenir compte du facteur humain. Dans les projets de transformation numérique, un risque est de « faire briller les yeux trop vite » et de décevoir. Il faut que les utilisateurs de systèmes qui ne sont pas parfaits du premier coup puissent avoir un retour rapide des modifications qu'ils ont demandées. Cela nécessite une gestion de projet en mode agile. L'accompagnement des utilisateurs est fondamental. Pour un développement donné, une ou deux centrales pilotes sont choisies ; elles interagissent rapidement de façon que, quand on généralise, il y ait moins de souci. Il y a un risque à ne pas faire la transition numérique, c'est celui de laisser certains avec des logiciels isolés et de ne pas donner à tous l'accès à la connaissance. Le progrès ne vaut que s'il est partagé par tous. Mais quand on souhaite partager des données avec une entreprise extérieure, surviennent des problèmes de partage de la propriété intellectuelle, des problèmes de modélisation commune des données, des problèmes de signature. Par exemple, si l'on veut permettre qu'un membre d'une entreprise extérieure puisse signer l'exécution d'une tâche sur une procédure numérique de l'entreprise, cela nécessite, au-delà du développement technologique, une entente juridique de propriété intellectuelle. Il faut réfléchir à tous ces problèmes rapidement faute de quoi la transformation visée ne pourra pas se faire.

Pour Olivier DELABROY, le premier risque auquel tout le monde pense est la cybersécurité. Le développement de toute application doit intégrer deux exigences : *safe by design* et *privacy by design* (protection des données personnelles). La plus grande vulnérabilité est l'*operation technology*. La première action est d'effectuer un recensement exhaustif de tous les ordinateurs et automates. Se préparer, c'est aussi faire des scénarios de crise et faire des tests d'intrusion. Mais Olivier DELABROY voudrait insister sur d'autres catégories de menaces et de risques. Le premier est de se jeter tout de suite sur la solution. On peut concevoir un très beau produit qui ne sera jamais utilisé : c'est le plus grand danger de la transformation numérique. Le risque existe d'être une usine à preuves de concept et de ne jamais passer à l'échelle. Il faut mettre l'humain avant la technologie. Outre la gestion de projet en mode agile, comme mentionné par François DIONIS, de nouvelles compétences sont requises comme, par exemple, des ethnologues pour comprendre comment le client d'une application (qui peut être un collaborateur de l'entreprise) va réagir. Il faut absolument prendre le luxe de comprendre et de prendre le temps pour cela. Le président d'Air Liquide prend une semaine dans son agenda chaque année pour, en petit comité, parcourir le monde pour comprendre le tsunami qui arrive sur l'entreprise et ses clients. L'intelligence artificielle, en particulier, va changer tous les métiers dans les 5 ou 10 ans qui viennent.

Michel EYMARD, parmi les risques externes à l'entreprise, est revenu sur la cybersécurité. Le *design* s'efforce de couvrir toutes les menaces mais ne peut les couvrir toutes malheureusement. Il faut donc tester et prendre tous les cas possibles qui peuvent arriver. Le problème est d'autant plus critique que, pour être compétitif, on utilise des *operating systems* et des *commercial off-the-shelf*. On utilise des systèmes dans nos systèmes. Cela exige de revoir la conception de nos systèmes qui utilisent ces logiciels et ces composants en créant des barrières pour éviter que nos systèmes soient pénétrés par des personnes malveillantes. Mais des risques internes existent aussi. Il faut faire évoluer les métiers et vite. Un premier risque est de ne pas disposer des compétences nécessitées par la transformation numérique. Trouver un data scientist et le payer au prix du marché est difficile. Mais il faut aussi préparer à la transformation des collaborateurs qui ont une culture de de plusieurs années dans la conception ou la production. Dans les 4 ans qui viennent, 21 000 personnes vont partir à la retraite. C'est une menace mais c'est aussi une opportunité pour introduire le digital dans les processus et recruter des personnes bien positionnées. Par exemple, on va pouvoir remplacer des opérateurs en connectant des machines et en créant des postes de superviseurs de 15 ou 20 machines dans les usines. L'intelligence artificielle va s'insérer dans tous les processus. On ne connait pas encore son impact mais il sera énorme. La connaissance peut être capitalisée et il va falloir repenser le rôle des experts. Il faut être capable de gérer cette transformation. Et une menace supplémentaire réside dans la rapidité d'exécution nécessaire : on dispose de peu de temps pour réussir cette transformation. Car d'autres acteurs peuvent intervenir, certains étant des partenaires d'aujourd'hui, clients et fournisseurs. Dans le cadre de l'entreprise étendue, des fournisseurs travaillent « chez nous » et capte notre connaissance. Comme l'a évoqué François DIONIS, le risque existe concernant la propriété intellectuelle. Il faut être rapide pour se positionner sur les marchés futurs. On dit que changer une culture demande 10 ans. On ne dispose que de quelques mois, un an, deux ans peut-être. Il faut embarquer le comité exécutif mais aussi tous les collaborateurs. Il y a le risque de ne pas capter ce qui se passe actuellement. Par exemple, dans le domaine de la fabrication additive, il y a une nouvelle information disponible chaque semaine concernant les machines, l'approvisionnement en poudres... Il ne faut pas sur-réagir car il y a des effets de mode mais il faut être agile en étant stable sur le cap, garder en tête les objectifs et le sens de ce qu'on fait.

L'échange avec les auditeurs de la table ronde avec l'exercice des questions et des réponses a permis de préciser et approfondir quelques points.

Concernant l'adaptation à la rapidité de la transformation numérique, il y a une certaine lourdeur dans les grandes entreprises qui ont une organisation, des processus, des usines qui doivent continuer à produire. Les intervenants s'accordent sur la nécessité de commencer à bâtir des fondations solides et de procéder par étapes. Olivier DELABROY parle de *transformation journey*. Parmi les fondations, on trouve les modèles de données qui seront utilisées dans toutes les applications : l'entreprise va devoir manager ses données comme elle manage ses processus. Avec des données structurées, il est facile de changer d'outils logiciels et transférer les données. La maintenance prédictive est aussi un basique parce qu'elle ne remet pas en cause la chaine de valeurs. C'est aussi un sujet sur lequel l'analyse coût/bénéfice peut être faite : les gains sont mesurables. Le challenge, c'est d'assurer les basiques et de travailler, sur le plus long terme, sur la culture pour que l'entreprise soit *transformation ready*, qu'elle soit capable de se transformer toute seule. Car l'enjeu n'est pas seulement la transformation numérique, c'est la transformation tout court. Le climat va aussi transformer les clients et les chaines de valeurs.

Concernant l'agilité devenue nécessaire, Michel EYMARD rappelle que l'agilité consiste à vérifier que l'on est toujours bien centré sur les objectifs, que l'on prend en compte une exigence nouvelle d'un client, qu'on intègre tous les événements pouvant se produire dans les produits et les processus. François DIONIS indique qu'il faut pouvoir associer le processus achat dans la transformation. Chez AIR LIQUIDE, des équipes produits plutôt que des équipes projets sont mises en place pour un projet de transformation numérique : une maquette est montée, les commentaires sont pris et à chaque étape, on mesure. A la fin, le produit sera utilisé et aura coûté moins cher qu'avec un cycle en V traditionnel.

Michel EYMARD est revenu sur le sujet de la propriété intellectuelle. Récemment, un de ses clients a fabriqué une pièce de SAFRAN avec les plans de SAFRAN en utilisant la fabrication additive. La propriété intellectuelle devient un outil stratégique et SAFRAN a revu récemment son organisation en la matière : il faut d'une part éviter les copies, en mettant par exemple des traceurs dans les pièces, et pouvoir déployer des technologies sans barrière.

Philippe LE POAC
Président de l'IMdR

Visite des caves Nicolas Feuillatte

Cette visite technique a commencé par un transfert en car suivant une agréable route traversant la campagne champenoise. Celle-ci, grâce aux charmes de l'automne, était parfois embrumée, parfois ensoleillée et parsemée de domaines de Champagne aux noms évocateurs.

À notre arrivée, nous avons été accueillis et présentés à notre sympathique et compétente guide qui fut à l'écoute de nos questions tout au long de cette visite de près de deux heures.

Nicolas Feuillatte est la plus jeune des maisons de Champagne, elle regroupe 84 coopératives qui rassemblent plus de 4500 vignerons. La guide nous a présenté les différentes étapes d'élaboration du Champagne, et installations associées, de l'arrivée des raisins jusqu'à la mise en carton.

Ces installations industrielles, sont largement mises en valeur par un circuit attractif et optimisé pour les visites. Nous avons été particulièrement impressionnés par la taille imposante des cuves en inox, l'éclairage jaune spécifique ambiant, l'automatisation et la propreté des installations, ainsi que la modernité de l'architecture des lieux. Le seul regret fut par rapport à la faible activité de l'usine due à cette période de l'année.

Cette visite enrichissante nous a permis de bien comprendre le processus de fabrication du champagne et restera associée au tout égal bon cru que fut le Lambda Mu 21.

Michel GIRAUDEAU
IMdR

Bilan du congrès lambda MU 21

Cette 21ème édition du congrès Lambda Mu a permis de traiter un sujet qui bouscule les métiers de la Maîtrise des Risques et de la Sûreté de Fonctionnement : la transformation numérique. 440 personnes sont ainsi venues partager leurs expériences et échanger sur leurs réflexions. Le congrès a laissé une large part aux thématiques classiques :

- **la fiabilité et la maintenance, les méthodes de sûreté de fonctionnement**, des thèmes qui ont montré leur capacité d'adaptation face aux enjeux et aux défis de la transformation numérique.

- **les facteurs humains et organisationnels** qui sont maintenant une composante incontournable des congrès Lambda Mu.

- ou encore **la maîtrise des risques** avec ses différentes composantes : projet, entreprise, santé, environnement.

D'autre part, ce congrès a permis de consacrer une session dédiée à la transformation numérique sur les trois jours de conférence.

Trois axes se dégagent en particulier sur cette thématique : la **cyber sécurité**, la fiabilité des **véhicules autonomes** et des objets connectés et enfin l'apport des techniques de **Traitement Automatique des Langues** (TAL) et d'**Intelligence Artificielle** pour l'exploitation du retour d'expérience.

Le thème du congrès était également bien présent dans les sessions dédiées à la maintenance notamment au travers de communications qui traitent de la **maintenance prédictive**. On peut citer en particulier la communication qui présente les résultats du projet IMdR « **HUMS – Health & Usage Monitoring System** – état de l'art et opportunités ». La cyber sécurité, les conséquences d'un monde hyper connecté et l'impact des médias dans la gestion de crise furent abordés avec le prisme des sciences humaines et sociales. Enfin, de nombreuses communications montrent l'apport du numérique pour la modélisation des systèmes et leur simulation.

Par ailleurs, on peut noter de nombreuses communications qui présentent des travaux sur l'ingénierie des modèles, la normalisation et l'aide à la décision.

Quatre temps forts ont jalonné ce congrès et ont contribué à enrichir les échanges :

• **L'allocution d'ouverture** a été l'occasion dans un premier temps pour Christian GALIVEL (directeur général adjoint à la RATP), Président du Congrès, de rappeler les enjeux de la maîtrise des risques pour nos entreprises et en particulier dans ce contexte de la transformation numérique. La présentation préparée par Guy PLANCHETTE et André LANNOY a permis par la suite de retracer l'histoire de la maîtrise des risques et la sûreté de fonctionnement, de l'IMdR et des congrès Lambda Mu à l'occasion de ce 40ème anniversaire du congrès. Ils ont également proposé des axes de réflexion face aux enjeux actuels et futurs.

• **Les ateliers de l'IMdR** ont été l'occasion de présenter les travaux et les réflexions de plusieurs GTR de l'IMdR, d'autres étaient dédiés au thème du congrès. Au-delà du temps de partage et d'échange, des actions et orientations concrètes ont été identifiées suite à ces ateliers. On peut notamment citer la volonté de créer un GTR dédié au TAL ou encore la mise en place d'un sous-groupe pour poursuivre la réflexion sur l'apport de l'innovation (technologique, méthodologique et organisationnelle) pour la gestion de crise.

• **La table ronde** qui a réuni des représentants d'AIR LIQUIDE, EDF et SAFRAN autour de « **la stratégie des entreprises et la transformation numérique** » a été l'occasion de partager les enjeux, les opportunités et les menaces. Les participants ont notamment rappelé la place centrale de l'homme dans cette transformation et donc la nécessité de partager et de garder le sens des actions et des orientations prises. Ils ont également rappelé les enjeux en termes de cyber sécurité et de **gouvernance de la donnée** et d'intégration des **compétences digitales** dans les entreprises. Ils ont finalement insisté sur la nécessité de développer une certaine **agilité** dans l'organisation, de lui permettre d'être **transverse et inclusive** pour qu'elle puisse s'adapter au rythme des changements de plus en plus rapides.

• **L'allocution de clôture** a été l'occasion d'écouter Marc de FOUCHÉCOUR qui nous a permis de prendre de la hauteur et de questionner la place de l'homme dans ce monde digitalisé.

Les défis et chantiers de demain

Plusieurs axes de réflexions se dégagent et pour lesquels il faudra apporter des réponses dans les années à venir :

- Adapter nos métiers et tirer profit de la transformation numérique.

- Proposer et promouvoir des approches qui permettent de garder le sens physique, la compréhension des phénomènes et l'expertise au cœur de nos processus de décision.

- Questionner la place de l'Homme et l'impact de la transformation numérique sur le travail et sur les interactions entre les acteurs.

- Questionner nos organisations et nos modes de management dans cette période changement pour garantir la maîtrise des risques.

Alors rendez-vous au Lambda Mu 22 pour aller encore plus loin et relever de nouveaux défis indispensables dans ce monde en pleine transformation.

Leïla MARLE, GRTgaz
Présidente du comité de programme du Lambda Mu 21

La vie de l'institut

Nos journées et formations 2019

Date	Titre	Lieux
31 janvier	Journée sécurité fonctionnelle : partage des bonnes pratiques autour de la norme CEI 61508 et de ses dérivées	GRTgaz, Saint-Denis
15 mars	Journée « Jeunes Ingénieurs et Jeunes Chercheurs »	École Centrale d'Électronique (ECE), Paris
11 avril	Formation « Sensibilisation aux concepts cindyniques »	École Spéciale des Travaux Publics (ESTP), Cachan
6 juin	Assemblée Générale	EDF, Palaiseau
27 juin	Journée Inter-GTR : vers une vision systémique de la maîtrise des risques	Carré des sciences, Paris
3 et 4 décembre	Les Entretiens du Risque	Carré des sciences, Paris

Nos projets

L'IMdR propose aux entreprises qui le souhaitent de mutualiser leurs ressources humaines et financières au sein de « **projets** ». Les entreprises souscrivent aux sujets qui les intéressent (co-financement) et pilotent les travaux menés par la société de conseil ou le laboratoire universitaire choisi par appel d'offres. Le «groupe projet» est ainsi composé d'un chef de projet (le pilote), des représentants des sociétés souscriptrices et des ingénieurs des sociétés de conseil en charge de l'étude. Un projet est généralement mené sur douze à quinze mois. Actuellement, dix projets sont ouverts à souscription :

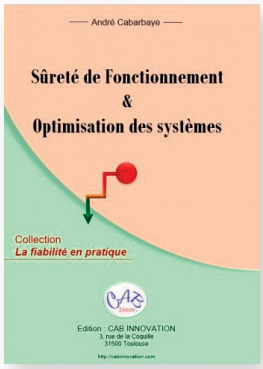
- Impact des facteurs humains et organisationnels sur les défaillances de structures industrielles ou de génie civil
- Guide pratique d'orientation pour l'application des normes actuelles de management des risques et de sûreté de fonctionnement
- Méthodes statistiques de traitement et d'interprétation d'un retour d'expérience en langage naturel
- Méthodes de caractérisation et de quantification de la résilience – Etat de l'art
- Identification des différences de traitement des événements internes, agressions internes et agressions naturelles extrêmes, lors de l'évaluation du niveau de risque d'une installation industrielle
- Comparaison de logiciels de traitement des incertitudes
- Recherches sur le concept de vulnérabilité relatif aux systèmes et ouvrages socio-techniques
- Création d'un modèle FIDES pour les composants de type «Condensateur céramique de la gamme automobile dit «Fail-safe »
- Représenter et propager l'incertitude à l'aide de réseaux
- Création d'un modèle FIDES pour les composants de type « Potentiomètres » (potentiomètre de recopie)

Retrouvez toutes les fiches synthèses des projets à souscriptions sur le site web de l'IMdR dans l'onglet « activés »
www.imdr.eu

Nous avons lu

«Sûreté de Fonctionnement & Optimisation des systèmes»

Cabarbaye André, Collection La fiabilité en pratique, Edition CAB Innovation
Février 2017, 241 pages



L'auteur, expert dans le domaine spatial, est bien connu des milieux de l'analyse de risque et de la sûreté de fonctionnement. Il publie un état de l'art des connaissances actuelles sur les principales méthodes utilisées en sûreté de fonctionnement. Cet ouvrage se veut une actualisation d'ouvrages précédents rédigés il y a plusieurs années par Jean-Claude Ligeron ou Patrick Lyonnet, et nous le considérons comme un vade-mecum de notre domaine, permettant à un jeune ingénieur comme à un ingénieur expérimenté d'accéder à des méthodes et pratiques adaptées. L'auteur les a manifestement développées et utilisées. L'ouvrage se présente plus comme un répertoire de méthodes et de pratiques que comme une étude ou une structuration de processus (par exemple de conception, ou de maintenance, ou d'analyse de risque, ou de retour d'expérience).

Les méthodes y sont décrites, avec leurs hypothèses, de nombreuses figures explicatives, avec des applications pratiques (principalement issues du secteur spatial) et de nombreux conseils. Peut-être peut-on regretter, souvent, l'absence de références à des ouvrages de la documentation technique, qui permettraient d'aller plus loin.

Nous ne sommes pas en accord avec tous les arguments déployés dans ce livre, nous l'avons cependant beaucoup apprécié pour différentes raisons.

En premier lieu nous avons fait des découvertes de méthodes que nous ne connaissons pas, par exemple la méthode HSIA (*Hardware / Software Interaction Analysis*) page 52, les méthodes D-Optimalité et Caboum page 139…

Dans un second temps nous avons apprécié la démarche et l'accent mis par l'auteur sur certaines méthodes :

- En premier lieu l'analyse fonctionnelle, on n'engage pas une étude de sûreté de fonctionnement sans avoir procédé à une analyse fonctionnelle (page 33),

- Page 46, l'auteur présente le diagramme d'Ishikawa, encore utilisé en qualité, mais qui a laissé sa place à l'arbre des causes, plus compliqué pourtant,

- Page 51 où la méthode HAZOP, de notre point de vue insuffisamment utilisée en France (si ce n'est dans les secteurs chimie et *oil &gas*), est présentée ; rappelons que cette méthode est reliée à la compréhension physique des phénomènes et à la connaissance de l'exploitant, ce qui est un argument majeur en analyse de risque,

- Page 68, l'auteur évoque les ambigüités liées à l'utilisation des termes sécurité – sûreté ; ne faudrait-il pas revenir à l'étymologie latine ?

- Page 104, l'auteur fait à juste raison la promotion de l'estimateur de Kaplan-Meier, si peu utilisé dans le monde industriel, malgré des atouts importants : pas d'incertitude de modèle, prise en compte des censures, maximisation de la vraisemblance,

- La page 121 attire l'attention du lecteur sur la modélisation des dégradations (les processus gamma et de Wiener) ; il s'agit d'un sujet important où des efforts importants devraient être menés à court terme compte tenu de l'arrivée des systèmes HUMS,

- La page 146 permet d'actualiser tous les recueils de données de fiabilité ; cette approche Bayésienne, initiée dans le nucléaire, est maintenant largement utilisée dans de nombreux secteurs industriels,

- Page 201, notre regard s'est porté sur les processus d'allocations ; l'ouvrage explicite les méthodes existantes ; les allocations sont utilisées dans tous les processus de conception, le lecteur peut être surpris par le faible nombre de méthodes et leur rusticité.

À plusieurs endroits du texte, pages 54, 129, 197 et suivantes, l'auteur aborde l'analyse pire cas (*Worst Case Analysis*). De notre point de vue les méthodes contraintes-résistance sont les candidates les mieux placées. Sur la base d'équations physiques, prenant en compte les incertitudes des données d'entrée sous la forme de fonctions de distributions de

probabilités, il est possible de déterminer le pire cas (l'évènement « imprévisible ») et d'estimer sa probabilité d'occurrence (d'évènement rare). Prendre les valeurs enveloppes ou pessimistes avec une estimation déterministe pour déterminer un coefficient de sécurité ne nous parait pas une bonne solution, car cette estimation, considérée à tort pessimiste, ne peut pas nous garantir l'examen de toutes les situations, et donc la sûreté.

Ce livre d'André Cabarbaye nous parait une aubaine. Son aspect pratique permet à l'ingénieur d'identifier rapidement la méthode disponible la mieux adaptée à la solution de son problème, de peser les difficultés, d'apprécier les tâches à réaliser et les données à rassembler. Son intérêt pour les ingénieurs, les chefs de projet, les analystes de risque, les experts, mais aussi pour les étudiants et leurs enseignants est manifeste.

André LANNOY
IMdR

Adhésion 2019

Adhérez à l'IMdR ou renouvelez votre adhésion afin de permettre à l'association en tant que société savante de rassembler le plus grand nombre possible d'entreprises, universitaires et individuels intéressés par l'amélioration des connaissances dans le vaste domaine « des risques ». Plus nous serons nombreux, mieux nous pourrons faire partager les expériences, mutualiser les savoirs et approfondir les méthodes.

Adhérez à l'IMdR c'est, intégrer un réseau, participer à des groupes de travail et de réflexion, pouvoir consulter le Centre d'Orientation, de Documentation et d'Information Technique conservant des ouvrages aussi anciens que modernes, rester informé des dernières actualités, mais aussi profiter de tarifs préférentiels d'entrée aux journées mensuelles, aux formations, au congrès Lambda Mu et aux «Entretiens du risque».

Utilisez le formulaire d'adhésion en ligne sur notre site : **www.imdr.eu**

IMdR - 12 avenue Raspail - 94250 Gentilly
Tél. : 01 45 36 42 10 • Fax : 01 45 36 42 14 • E-mail : secretariat@imdr.eu - www.imdr.eu
Directeur de la Publication : Philippe Le Poac - Directeur de la Communication : Denis Marty
Délégué Général : Clément Judek - Community Manager et Webmaster : Manon Raguenet
Réalisation - Impression : Imprimerie ANQUETIL
N° ISSN 1639-9706
L'Institut pour la Maîtrise des Risques (IMdR)
est une association Loi 1901 à but non lucratif, émanant de l'Institut Sûreté de Fonctionnement (ISdF) - Siret 443 923 719 00027