IMdR Info
Lettre d'information
de l'Institut pour la Maîtrise des Risques
Sûreté de fonctionnement - Management - Cindyniques
n°35
2ème trimestre 2017

sommaire

Edito

Amiante, pesticides, perturbateurs endocriniens,… la liste serait trop longue à énumérer de cas de dossiers dont nous avons tous, plus ou moins pris connaissance, et ayant, depuis, fait la une des médias. Ces dossiers sont à l'évidence assez symptomatiques d'un refus de reconnaître l'ampleur de conséquences potentielles sur les personnes, sur les biens et sur l'environnement.

Ce refus, voire ce déni des risques dont les ramifications sont construites cognitivement, de manière organisationnelle et culturelle, est souvent analysé sous l'angle de la stratégie consciente et volontaire de groupes d'acteurs ayant intérêt à nier les évidences. Ou sous l'angle sociétal, pointant la montée du cynisme au sein de certains domaines d'activité, voire plus largement au sein de la société. Le septième Art s'en est d'ailleurs amplement fait l'écho avec des films emblématiques tels que « Margin Call » de Jeffrey C. Chandor (2011), « Les Marches du pouvoir » de George Clooney (2011),… et plus récemment « La Fille de Brest » d'Emmanuelle Bercot (2016) ou « Miss Sloane » de John Madden (2016).

Or, si ceci peut recouvrir une partie de l'explication des mécanismes de déni des risques, il demeure nécessaire de reconnaître l'existence de plusieurs autres mécanismes explicatifs. La fabrique du poids des évidences et de moments de bifurcation, les biais de perception des risques, l'équilibre entre la prise de risque et l'innovation, l'autocensure, … sont autant d'aspects à considérer lors de l'analyse des ramifications profondes de la construction individuelle ou collective d'un déni des risques.

Les 14 et 15 novembre 2017, les « Entretiens du Risque » organisés par l'IMdR apporteront un éclairage nouveau sur ce thème en conjuguant un savant partage entre témoignages issus de la pratique du terrain et résultats de recherche pluridisciplinaires. Les mécanismes de déni des risques individuels et collectifs, en situations usuelles, extrêmes, voire en contextes d'innovation seront décrits et analysés par les orateurs. Tout au long de ces deux journées, la démarche cindynique servira de fil rouge permettant de rendre compte de l'influence des modèles, des règles, de la construction des objectifs, du poids des faits et des données, ainsi que des valeurs individuelles et collectives sur la fabrique, le maintien et la reconstruction du déni des risques au sein de nos organisations et de nos territoires. Notez d'ores et déjà ces dates sur votre agenda et participez aux présentations et aux nombreux échanges sur le thème **« Le déni du risque : de l'attitude individuelle à la gouvernance des organisations »** !

Myriam MERAD, CNRS
Présidente du comité de programme des « Entretiens du risque 2017

les congrès λμ

Après notre lettre d'information du 1er trimestre qui a consacré huit de ses douze pages au 20ème congrès de maîtrise des risques et de sûreté de fonctionnement de Saint-Malo (dont un article consacré à l'atelier « Sécurité pratique : état des lieux et perspectives »), nous remercions MM. Emmanuel Ardillon (EDF Lab Chatou), Alaa Chateauneuf (Université Blaise Pascal, Clermont-Ferrand) et Thierry Yalamas (PHIMECA Engineering, Clermont-Ferrand & Paris) pour les informations qu'ils nous livrent ici sur l'atelier n°8 ***« Fiabilité et Robustesse »*** *qu'ils ont animé lors du congrès.*

L'atelier « Fiabilité et Robustesse » était organisé sur proposition du GTR (groupe de travail et de réflexion) conjoint IMdR / AFM « Sûreté et Sécurité des Structures ». Il a réuni une quarantaine de participants, répartis de manière équilibrée entre industriels et universitaires.

Après une introduction générale (E. Ardillon) rappelant brièvement l'organisation et les objectifs de l'atelier, les animateurs intervenaient par un exposé d'une dizaine de minutes chacun, fournissant un éclairage particulier sur la thématique « Fiabilité et Robustesse » :

- Fiabilité et Robustesse en conception : exigences contradictoires ou complémentaires (A. Chateauneuf)
- Fiabilité / Robustesse : quelles mesures ? (T. Yalamas)
- Fiabilité, Robustesse, Décision : apports de l'approche *info-gap* (E. Ardillon).

Ensuite venait le temps des discussions avec l'assistance, structurées autour de trois thèmes principaux :

- Les contextes faisant appel à la robustesse : conception, décision, modélisation, projet, construction, composant ou système
- L'évaluation quantitative de la robustesse : existe-t-il des mesures de robustesse ? quels sont les problèmes numériques que l'on peut rencontrer ? (Point détaillé pour la solution *info-gap*)
- Les liens entre fiabilité et robustesse.

Tout d'abord, sur ce dernier sujet, on constate que la **fiabilité** est appréhendée de manière diverse selon les branches industrielles. Ainsi, dans l'industrie automobile, la fiabilité est garantie par l'application de règles de l'art, mais on cherche à éviter des évaluations de fiabilité trop poussées, à la différence parfois du domaine de la production d'électricité : on se ramène généralement à des grandeurs indirectes qui garantissent la fiabilité. L'analyse de sensibilité permet de déterminer les variables les plus influentes. Elle permet aussi d'éviter un effet domino, une petite déviation pouvant engendrer de gros problèmes.

Par ailleurs, la **robustesse** est généralement associée à une insensibilité aux incertitudes (invariance en présence d'incertitudes), parfois même aux incertitudes non imaginées (cf. redondance en génie civil, manque d'information en modélisation). La robustesse impose de se préoccuper des dispersions de fabrication et d'usage par le retour d'expérience. La solution la plus robuste n'est pas nécessairement la plus performante (i.e. la plus fiable dans notre contexte), et ce constat général - qui peut être quantifié grâce à la théorie *info-gap* (approche non probabiliste de la robustesse dans un contexte de forte incertitude) - est commun à divers domaines, dont les stratégies de maintenance. Il résulte aussi de l'optimisation robuste, qui montre que l'optimum global peut ne pas être un optimum robuste. Il apparaît au final que les notions de fiabilité et de robustesse sont complémentaires, mais peuvent être parfois contradictoires.

Enfin tous les participants s'accordent sur le fait qu'il faut une tolérance au dommage.

Accès aux communications des congrès λμ

Les communications des congrès de maîtrise des risques et de sûreté de fonctionnement sont répertoriées dans les bases du CNRS / INIST (Institut de l'information scientifique et technique) depuis le congrès d'octobre 2014. Toutes les communications de nos congrès sont désormais consultables **six mois** après chacun d'eux, sur www.irevues.inist.fr ou sur le site www.imdr.eu. Les communications du congrès de Saint-Malo sont donc ouvertes à tous sur l'un ou l'autre de ces sites.

Le 21ème congrès λμ se déroulera du 16 au 18 octobre 2018 au Palais des congrès de Reims, précédé d'une journée de tutoriels le 15.
L'appel à communications sera diffusé dans le courant du mois de juin et vous disposerez alors de six mois pour proposer une (ou plusieurs) communications. Ne manquez pas cet évènement !

« Pourquoi et comment élaborer un Plan de Continuité d'Activité (PCA) » ?

Journée d'études du 19 janvier

Cette journée a été réalisée en partenariat avec l'IESF (Ingénieurs et Scientifiques de France), le CCA (Club de la Continuité d'Activité) et l'IMdR (Institut pour la Maîtrise des Risques). Elle a été le fruit de l'expérience de divers responsables réunis au sein du comité « Maîtrise des Risques Opérationnels » de l'IESF.

Partis du constat qu'aucune entreprise ne peut ni ne doit se considérer comme infaillible, ils ont cherché à les aider - et plus particulièrement les PME – à se protéger des risques de cessation partielle ou importante d'activités. Car au-delà d'une certaine durée d'arrêt, toute entreprise pourrait supporter d'importantes pertes financières et d'image, une défaillance dans la confiance de ses clients, et pourrait même disparaître.

Les objectifs essentiels de cette journée consistaient donc à :

- montrer que l'existence d'un PCA permet, soit de réduire le temps d'arrêt probable de l'activité, soit d'en minimiser les conséquences,
- préciser la démarche d'élaboration d'un PCA.

Pour préciser l'intérêt de disposer d'un PCA, les intervenants ont appelé l'attention des participants sur les difficultés rencontrées par certaines entreprises qui n'ont pas préparé de PCA, comparativement à celles qui en disposent.

Quant au processus d'élaboration d'un PCA, ils ont conseillé de se focaliser sur les risques (internes ou externes) qui conduiraient à l'impossibilité de continuer à produire, la réussite de la démarche passant par un ensemble de questions, de clarifications et d'actions. Les questions seront relatives à la nature et à la durée de l'interruption des processus critiques - comment se protéger pour qu'ils soient poursuivis – et à l'impact sur les ressources, celles uniques irremplaçables et celles critiques, dont aussi les ressources humaines. Les clarifications expliciteront la définition des rôles et des niveaux de responsabilités en cas de pilotage d'une crise. Quant aux actions, elles consisteront en la mise en place des dispositions retenues, à la formation des personnels associés au fonctionnement d'un PCA et à la sensibilisation des autres grâce à une large communication interne sur la politique de continuité de l'entreprise. En dernier lieu, il sera indispensable de tester le PCA, le contenu du test pouvant aller de la simple *check-list* des processus mis en place à l'expérience d'un arrêt total ou partiel permettant de vérifier la pertinence des politiques choisies afin de les infléchir ou de les améliorer. Bien entendu, les tests ne doivent pas mettre en péril l'activité.

Tout au long de cette journée, les intervenants ont insisté sur les points importants en étayant les aspects budgétaires et en commentant l'ensemble des dispositions à prendre pour se lancer dans la démarche et la faire vivre. Vu l'ampleur des actions à mener, il a été conseillé d'adopter une démarche pragmatique de bon sens sans tomber dans le contexte « d'une usine à gaz ».

En conclusion, il a été montré que l'étude et la mise en place d'un PCA, au lieu d'être considérées comme des coûts inabordables, sont au contraire l'occasion de mieux connaître son entreprise, de saisir l'opportunité de simplifier certains processus, d'accroître la confiance de tous ses partenaires, enfin, d'être un investissement utile en cas de crise.

Cette journée a été l'occasion de faire comprendre la nécessité de disposer d'un PCA, d'en avoir une vision d'ensemble pour en clarifier les aspects, d'en peser les avantages et de savoir utiliser la norme ISO 22301 : 2012 « Vers le management de la continuité » comme guide. Elle fût riche d'enseignements et d'intérêts caractérisés par le nombre très important de questions des participants qui ont permis, entre autres, de lever l'ambiguïté qui pouvait exister entre les rôles respectifs du manager des risques et du responsable du plan de continuité.

Guy PLANCHETTE

Journée « Jeunes chercheurs et jeunes ingénieurs » 2017

La 9ème édition de cette journée annuelle IMdR s'est tenue le 16 mars, en partenariat avec et sur le campus de l'Ecole Spéciale des Travaux Publics (ESTP) / Institut de Recherche en Constructibilité (IRC). Cette journée ouverte par Madame Florence Darmon, Directrice générale de l'ESTP et Monsieur Philippe LE POAC, Président de l'IMdR a été extrêmement riche en présentations. Elle a permis de faire le point sur les préoccupations industrielles et académiques actuelles en matière de recherche dans le domaine des risques. Pour la première fois, un espace dédié aux sociétés industrielles et de service qui le souhaitaient a été ouvert pendant toute la durée de la journée, permettant d'établir de nombreux contacts entre étudiants et sociétés, notamment en matière de stages, voire d'informations sur les carrières. Un prochain numéro reviendra plus en détail sur cette journée.

« From Risk to Resilience : Methodology and Case Studies »

Séminaire AFPCN - IMdR du 11 avril

Ce séminaire d'une demi-journée a été organisé par le GTR conjoint « Incertitudes et décisions» de l'AFPCN (Association Française pour la Prévention des Catastrophes Naturelles) et de l'IMdR. Il a été animé par Myriam Merad (CNRS). La conférence a été présentée par le Dr Igor Linkov, *Risk and Decision Science Team, US Army Engineer Research and Development Center*, Boston. Elle a été très intéressante et très suivie, si l'on prend en compte les très nombreuses questions et discussions engagées par les participants.

Le conférencier a d'abord clarifié la notion de résilience (du mot latin *resilire*). Plusieurs réflexions, plusieurs définitions ont été proposées et nous préférons celle-ci: *the ability to anticipate, to prepare for and adapt to changing conditions and withstand, respond to and recover rapidly from disruption*s. Il manque peut-être, par rapport à la définition latine, le fait qu'il ne faut point hésiter à se retirer, à se replier, à sauter en arrière avant de repartir.

L'auteur a ensuite comparé l'analyse de risque à l'analyse de résilience. L'analyse de risque (qui est une approche *bottom/up*) exige une quantification déterminant la contribution de chaque élément (composant, système …) au risque. On pourra alors en déduire toutes les options de prévention ou de protection nécessaires pour réduire le risque. On ne peut pas se contenter de la matrice de criticité, incapable de prendre en compte les évènements extrêmes et les évolutions des menaces et des valeurs sociales. La robustesse est une composante de l'analyse de risque, elle est une propriété du composant - système - … étudié.

Il n'est cependant guère réaliste de croire qu'il est possible de prévoir tous les évènements de très faible probabilité et de fortes conséquences. Il convient donc de se préparer à cette éventualité d'occurrence d'un évènement extrême. Dans ces conditions, il faut effectuer une analyse de résilience (qui est une approche *top/down* prenant en compte les interactions) permettant de quantifier la résilience. Les données démographiques sont déjà de bons indicateurs de vulnérabilité. Des méthodes qualitatives existent mais ne donnent pas satisfaction car elles oublient l'incertitude. L'auteur propose la construction de la matrice de résilience dont les lignes représentent les points de vue (*physical, information, cognitive, social)* et les colonnes représentent les étapes de la résilience (*prepare, absorb, recover, adapt*). Chaque case est quantifiée, ce qui nécessite le recours au retour d'expérience, à l'élicitation d'expertise, aux résultats de l'analyse de risque en utilisant les méthodes de gestion de l'incertain comme les réseaux probabilistes. Cette quantification de la résilience va permettre d'estimer les coûts et bénéfices des différentes options potentielles. Les choix seront faits, ensuite, par des méthodes multicritères d'aide à la décision.

On peut regretter que l'auteur n'ait pas eu le temps de développer ces deux aspects de modélisation et de montrer une application détaillée sur un cas pratique. Quelques exemples ont été rapidement présentés : la circulation automobile dans la région de San Francisco, l'impact d'une onde de submersion marine en Jamaïque…

La quantification de la résilience, la préparation qu'elle oblige semblent bien adaptées au problème du traitement de l'évènement extrême. Se préparer pourrait peut-être adoucir les critères probabilistes d'acceptation, mais cela reste à vérifier. L'harmonisation des efforts, les actions de R&D concernent principalement l'utilisation des réseaux probabilistes et le développement de la résilience au niveau des systèmes.

André LANNOY

Nos autres formations et journées (1er semestre 2017)

4 mai Formation aux concepts cindyniques.

4 mai Formation : « Sensibilisation à la démarche probabiliste en conception, exploitation et maintenance des structures industrielles et de génie civil».

16 mai «Des méthodes aux applications du traitement automatique des langues (TAL) dans le retour d'expérience».

20 juin «La catastrophe de Bhopal : une tragédie en trois actes et ses enseignements».

Notez également

13 juin L'assemblée générale annuelle IMdR sera accueillie par Engie, sur le site du CRIGEN (Centre de recherche et innovation gaz et énergies nouvelles) à La Plaine Saint-Denis. La matinée sera mise à profit pour présenter un projet, un GTR et une commission IMdR. De très intéressantes visites de laboratoires seront proposées l'après-midi.

Le planning des activités du 2ème semestre sera communiqué dans le courant de l'été, mais vous pouvez d'ores et déjà inscrire sur vos agendas les rencontres des **14 et 15 novembre** baptisées « Entretiens du risque ». Elles se dérouleront au carré des Sciences du ministère de l'Education nationale, de l'Enseignement supérieur et de la Recherche (Paris Vème) sur le thème **« Le déni du risque : de l'attitude individuelle à la gouvernance des organisations »**. Les inscriptions seront ouvertes dès le mois de juin.

Informations sur www.imdr.eu.

Nos GTR

L'IMdR vous informe de la création d'un nouveau groupe sur ***« Gestion intégrée des risques et de la complexité : architecture des systèmes, pilotage des résultats de l'entreprise et apprentissage ».*** *Pour toute information ou pour participer aux travaux, prenez contact avec Francis Claude, à l'origine de cette initiative et animateur du groupe.*

Combien de professionnels disposent d'indicateurs clés de risques (KRI) et de la complexité (KCI) qui intègrent leurs objectifs afin de leur permettre de gérer au plus juste les écarts par rapport aux attentes à l'échéance et au quotidien ? Des difficultés scientifiques et techniques semblent exister pour établir ce type d'indicateurs.

Ce GTR transverse souhaite donc avoir une démarche générale comme celle proposée par le ministère de la Recherche pour identifier des activités de R&D de conception innovante et faire émerger de nouveaux produits, procédés ou services adaptés et innovants : ici pour une gestion intégrée des risques et de la complexité permettant une meilleure réconciliation des visions techniques, économiques, financières (incertaines) avec les attentes comptables et un meilleur apprentissage collectif.

Le programme de travail et de réflexion de ce groupe (PTR) propose de s'orienter sur les difficultés scientifiques et techniques rencontrées au niveau de l'architecture des produits complexes (systèmes à faire), des projets et portefeuille de projets complexes (système pour faire) ainsi que celle du management intégré des risques de l'entreprise.

La richesse des courants présents au sein de l'IMdR ou des systèmes formels qui la composent - comme la sûreté de fonctionnement, la maîtrise des risques, les cindyniques, le management des risques - sera nécessaire à l'identification des difficultés et à la réalisation d'états de l'art qui pourront être accompagnés d'expertises dans les domaines de l'assurance, la banque, la finance, l'informatique, les mathématiques ou autres, en fonction de la finalité qui devra être adaptée à des groupes, des ETI et des PME importantes.

Francis CLAUDE
ESTP / IRC

Nous avons lu

Collectif sous la direction de Yannick FOURASTIER & Ludovic PIETRE-CAMBACEDES

Cépaduès Editions, 2015, 530 pages, 55€ ISBN : 9782364931688

Ce livre sur la malveillance numérique a été écrit par de nombreux spécialistes sous la direction de Yannick FOURASTIER (Airbus Group) et Ludovic PIETRE-CAMBACEDES (EDF) et est très complet (4 parties et 16 chapitres). Il est préfacé par Guillaume POUPARD, Directeur Général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Tout d'abord, précisons que, dans cet ouvrage, la sécurité concerne les risques exogènes, provenant de l'environnement et dont les conséquences potentielles concernent le système considéré. La sûreté concerne réciproquement les risques endogènes, provenant du système et dont les conséquences potentielles concernent l'environnement. Ainsi, les risques d'origine malveillante relèvent de la sécurité, alors que les risques accidentels, c'est à dire d'origine non intentionnelle, relèvent de la sûreté. Ce point de vue rejoint le nôtre même s'il n'est pas toujours partagé.

Les mythes et réalités de la cybersécurité ainsi que l'historique de la menace sont présentés. La presse a beaucoup parlé en 2010 du virus STUXNET, sciemment créé par des services spéciaux étatiques pour prendre le contrôle des installations de centrifugation iraniennes et les mettre hors d'usage. Cet évènement a mis sur la place publique la vulnérabilité des systèmes numériques industriels (SNI) et notamment des logiciels de pilotage et d'acquisition de données (SCADA en anglais pour *Supervisory Control And Data Acquisition*).

Des chapitres traitent des aspects électroniques et informatiques et l'offre technologique est présentée. Ces chapitres ont dépassé notre propre compétence mais seront très utiles aux spécialistes. Il est clair que la sécurité des systèmes industriels nécessite de maîtriser les protocoles et la configuration des équipements. La recommandation de base de la cybersécurité est évidemment d'établir et de maintenir à jour l'inventaire des matériels et des configurations. Il est aussi fondamental de disposer d'un système de détection d'intrusion (IDS pour *Intrusion Detection System*). Il est également recommandé de challenger régulièrement sa posture cybersécurité (sans compromettre la production habituelle du système) par des tests d'intrusion en environnement industriel (*pen-tests*).

Yannick FOURASTIER et Jean-Claude JABOT (Apsys) traitent de l'analyse des risques et soulignent que, pour être correcte et complète, l'appréciation des risques des installations industrielles doit aborder à la fois les aspects sûreté de fonctionnement et cybersécurité, ce qui n'est pas sans poser de problèmes dans la pratique : les cultures sûreté de fonctionnement et cybersécurité sont différentes, ainsi que les échelles de temps. Les auteurs rappellent que la norme ISO 31000 propose une méthodologie d'analyse des risques très comparable dans sa philosophie à celle de l'ISO/IEC 27005. L'évaluation du risque doit permettre la recherche et la description des causes des défaillances aléatoires ou des défauts de développement (sûreté de fonctionnement) et l'identification et la caractérisation des vulnérabilités potentielles ou réelles susceptibles d'être exploitées par des menaces et leurs descriptions (cybersécurité).

Ludovic PIETRE-CAMBACEDES et Marc BOUISSOU (EDF et Ecole Centrale Paris) approfondissent la problématique : « Mieux intégrer sûreté et sécurité : problématique, enjeux et perspectives ». Ils définissent quatre grandes familles d'interdépendance entre sûreté et sécurité : la dépendance conditionnelle (le respect d'exigences de sûreté conditionne le niveau de sécurité ou réciproquement) ; le renforcement mutuel (des mesures prises à des fins de sûreté contribuent également à la sécurité ou réciproquement) ; l'antagonisme (les exigences ou mesures de sûreté et de sécurité mènent, considérées conjointement, à des situations conflictuelles) ; l'indépendance (pas d'interaction). Les auteurs citent quelques travaux industriels en pointe et des recherches académiques concernant la sûreté visant à leur extension au monde de la sécurité.

La dernière partie de l'ouvrage traite des normes et des référentiels. Un zoom très détaillé est fait par Pierre KOBES (Siemens) sur la norme internationale IEC 62443 qui est dédiée à la sécurité informatique des IACS (*Industrial Automation and Control Systems*) et qui définit quatre niveaux de sécurité (*Security Levels*, SL) et sept exigences fondamentales (*Foundational Requirements*, FRs). Frédéric GUOMARD (EDF) et Stéphane MEYNET (ANSSI) présentent le panorama des certifications de cybersécurité et en discutent l'intérêt et les limites. Ils concluent qu'en attendant la convergence indispensable entre la sûreté de fonctionnement et la cybersécurité, il est important de pouvoir rapidement renforcer le niveau de cybersécurité des systèmes numériques industriels en s'appuyant sur des schémas pragmatiques issus du monde de l'informatique de gestion, mais adaptés aux systèmes numériques industriels.

Philippe LE POAC
Président de l'IMdR

Yann POLLET

Ellipses, décembre 2016, 432 pages, 41€ ISBN : 978234001486

Au-delà de son titre très ciblé sur SysML, l'auteur nous présente un état des pratiques et des principes généraux applicables à la définition, la spécification, l'architecture d'un système et plus particulièrement d'un système informatique.

Après avoir défini les notions de systèmes et d'ingénierie et/ou d'intégration système, notions largement utilisées dans le langage courant mais souvent dans des sens assez différents, il aborde à la fois les problématiques organisationnelles (et la répartition des rôles entre maîtrise d'ouvrage et maîtrise d'œuvre), fonctionnelles (élicitation des exigences), architecturales (impact des choix architecturaux), ainsi que les différentes manières de représenter ces différents volets de la description d'un système en s'appuyant sur des exemples concrets pour mieux faire passer ces messages. L'ingénierie système (pour les phases descendantes du cycle en V) est analysée et décrite de manière détaillée à la fois dans sa dimension fonctionnelle et dans sa dimension technique. Différents principes de l'ingénierie système sont abordés : séparation entre problème et solution ; spécification des besoins, choix d'une architecture ; décomposition du système ; gestion des exigences ; modélisation du système ; construction du projet sur la base de processus.

De cette manière, les différents aspects d'un système sont passés en revue avec, à chaque fois, une description détaillée des enjeux et contraintes qu'il est nécessaire de bien maîtriser pour permettre de poursuivre la démarche d'ingénierie :

- enjeux liés à la détermination des besoins et à l'ingénierie des exigences,
- enjeux des choix (et représentations associées) des architectures selon les différents styles architecturaux (hiérarchique, flot de données, distribuée ….),
- ingénierie guidée par les modèles avec un zoom particulier sur la modélisation d'un système en utilisant le langage SysML (dont une description détaillée est présentée dans l'ouvrage).

Ces éléments sont présentés de manière didactique. Les aspects test ne sont pas abordés, et les notions liées à la sûreté de fonctionnement sont traitées comme des attributs du système comme les autres.

Chacune des notions abordées est illustrée de manière indépendante. Un exemple en fin d'ouvrage permet d'avoir une vision intégrée de l'ensemble des concepts et de la démarche d'ingénierie système qui peut alors justifier pleinement l'expression « intégration des systèmes ».

Ce livre peut intéresser à la fois les personnes qui veulent soit avoir une vue d'ensemble de l'ingénierie système et celles qui, ayant une connaissance ou une expérience des systèmes au sens classique du terme, se trouvent confrontées à de nouvelles problématiques telles que la prise en compte du logiciel ou des architectures complexes.

En conclusion, Yann POLLET met son expérience et la formation qu'il dispense au Conservatoire National des Arts et Métiers (chaire d'intégration des systèmes) dans un ouvrage qui n'a pas actuellement de réel équivalent.

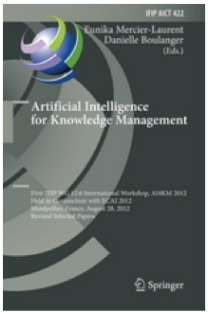
Patrice KAHN
KSdF Conseil

Ouvrages : notre sélection

Artificial Intelligence for Knowledge Management

Eunika MERCIER-LAURENT & Danielle BOULANGER

Editions Springer, juin 2014, 189 pages ISBN : 978-3642548963



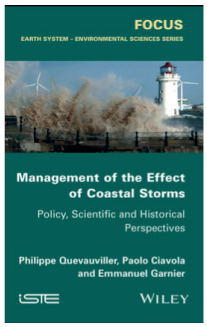
The IFIP AICT series publishes state-of-the-art results from the fields of information and communication technology. The scope of the series includes: foundations of computer science; software theory and practice; education; computer applications in technology; communication systems; systems modeling and optimization; information systems; ICT and society; computer systems technology; security and privacy protection in information processing systems; artificial intelligence; human-computer interaction and entertainment computing.

Proceedings of refereed international conferences focusing on the information and communication sciences and interdisciplinary fields are featured in the IFIP AICT series. The papers presented in these proceedings often precede journal publication and represent the most current research results in a particular area of ITC. The principal aim of the IFIP AICT series is to encourage education and the dissemination and exchange of research results on all aspects of information and communication technology. **This book features a selection of papers presented at the First IFIP WG 12.6 International Workshop on Artificial Intelligence for Knowledge Management, AI4KM 2012, held in Montpellier, France, in August 2012, in conjunction with the 20th European Conference on Artificial Intelligence, ECAI 2012. The 11 revised and extended papers were carefully reviewed and selected for inclusion in this volume. They present new research and innovative aspects in the field of knowledge management.**

Management of the Effect of Coastal Storms – Policy, Scientific and Historical Perspectives

Philippe QUEVAUVILLER, Paolo CIAVOLA et Emmanuel GARNIER

Wiley ISTE, March 2017, 188 pages, 115,20€ ISBN : 978-1-84821-762-1



A large part of the world's coastlines consists of sandy beaches and dunes that may undergo dramatic changes during storms. Extreme storm events in some cases dominate the erosion history of the coastline and may have dramatic impacts on densely populated coastal areas. Policy, research and historical background are essential elements that need to be interconnected for effective coastal planning and management.

This book discusses this framework, with Chapter 1 providing an insight into policy settings and science-policy interactions in the area of coastal risks related to storms and flooding, and integrated coastal zone management. This is followed by a review of the current understanding of the processes generating extreme coastal events, the morphological evolution of coastlines during and after the events, and the methods for monitoring the process as it occurs or for post-event appraisal. The final chapter discusses the importance of historical approaches regarding coastal threats, taking the Xynthia storm as an example.

IMdR - 12 avenue Raspail - 94250 Gentilly (RER : Gentilly)

Tél. : 01 45 36 42 10 • Fax : 01 45 36 42 14 • E-mail : secretariat@imdr.eu • N° ISSN 1639-9706

CODIT - Centre d'Orientation, de Documentation et d'Information Technique :
Espace convivial où des animateurs vous renseignent et vous conseillent. Prenez RDV au 01 45 36 42 10

Directeur de la Publication : Philippe Le Poac - Directeur de la Communication : Denis Marty - Délégué Général : Jean-Pierre Petit
Conception et réalisation : Imprimerie ANQUETIL - www.imdr.eu - Webmaster : John Obama

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