



LA LETTRE DES CINDYNIQUES

EDITORIAL

UN MANDAT CLAIR

Le récent colloque « Activités à risques et démocratie : vers de nouvelles formes de gouvernance » organisé par l'Institut en partenariat avec l'Office Parlementaire a rencontré un vif succès auprès des divers participants et a eu le mérite de faire prendre conscience de l'efficacité des approches cindyniques, en particulier parmi les personnalités politiques présentes.

Dans la Lettre des Cindyniques d'avril 2003, le Président, Claude FRANTZEN, nous appelait à tirer « la quintessence » de ce colloque.

Aujourd'hui, l'interpellation me paraît encore plus d'actualité !

En effet, notre assemblée générale du 26 juin dernier, marquée par un très faible taux de participation, a pourtant été décisive.

Interrogeons nous d'abord sur la participation. Etait-ce la date non propice, l'horaire mal adapté, l'insuffisance de disponibilité des adhérents, ou encore le désintérêt pour une réflexion de fond sur l'avenir de l'IEC ? Vous seuls détenez les vraies réponses. Mais ne pensez vous pas important de nous les faire connaître afin de faire progresser notre réflexion.

Dans son rapport moral, le président FRANTZEN, proposait un rapprochement fort avec le nouvel « Institut pour la maîtrise des risques », héritier de l'« Institut de Sécurité de Fonctionnement » afin de constituer un « lieu d'échange en matière de maîtrise des risques, depuis la vision politique et stratégique, jusqu'aux outils scientifiques concrets et quotidiens ».

Par son vote favorable, l'AG a entériné la constitution d'un nouveau conseil d'administration auquel elle a confié un mandat clair : **la mission de conduire en un an le rapprochement des deux associations.**

La réunion du conseil, qui a suivi immédiatement l'AG, a désigné les membres du bureau :

Président	: Guy PLANCHETTE ,
Vice-Président	: Claude FRANTZEN,
Secrétaire Général	: Jean-François RAFFOUX,
Trésorier	: Gérard BOUGET,
Délégué Communication	: Patrick RUBISE
Contrôleur	: Angela Minzoni Derocho

J'aurai donc la lourde responsabilité de vous rendre compte de notre mission dans le courant du mois de juin 2004.

En conséquence je compte sur vous tous qui êtes attachés au développement des cindyniques. Consacrez quelques minutes de votre temps à nous faire connaître vos idées pour que la vision politique et stratégique de la maîtrise des risques connaisse la place qu'elle mérite. Rappelons-nous les écrits prémonitoires de Claude FRANTZEN ¹: « Dans ce grand chambardement, les cindyniques restent une valeur sûre, surtout si elles prennent bien leur distance par rapport au positivisme si prégnant dans la culture des élites techniques, pour intégrer toute la richesse des sciences de la complexité ».

Guy PLANCHETTE
Président

¹La lettre des Cindyniques n° 36 – Mars 2002

Danger center in the human brain

Cet article est écrit par un nouvel adhérent à l'Institut, le Professeur Konstantin Trinus de l'Université de Kiev, qui a conduit, avec des experts internationaux de la société de neurootologie et d'équilibrimétrie, une enquête sur les incidences neurologiques dues à Tchernobyl¹. Il nous livre une synthèse en anglais.

Definitions

Damage might be regarded as a destruction of the body or its parts. Damage might be total or partial, in the latter case the percentage of the damage might be considered. Damaging factors might be classified as mechanical, physical, chemical and biological. In human beings we can also speak about psychogenic damage.

Danger might be defined as high probability of the damage. Subjective expectation of danger is called Anxiety.

Human perception of the danger

For prediction of the dangerous situations the body has sensory systems. Mechanical damages are perceived with somatosensory system. Some of the physical damages : heat, very low temperatures are also perceived with the somatosensory (hot and cold) receptors located in the skin.

Other possible mechanical damages (ruining the rock and mountains, approaching the storm, hurricanes, etc) might be predicted from the information perceived with vision and hearing.

Earthquakes are perceived with vestibular system. Many animals feel anxious at the approaching earthquake.

Many discussions are held around the problem of the magnetic sensor in the human brain. Two structures are possible candidates :

- One is the vestibular system
- The others are the bones of the ethmoidal sinuses.

Chemical substances are altering metabolism in the body. These changes are resulted in the changes of the red-ox potential. Specific sensor of it is hair cell of the vestibular system. In such a manner vestibular system might be named the sensor of the chemical damages,

¹Chornobyl Vertigo; 10 years of monitoring publié en 1996, in neurootology newsletter et disponible à l'IEC.

including also biochemical: viral, bacterial/fungal and protozoic toxins.

Taste and smell also help us to discriminate which substances to be consumed or avoided. Smell is also important in emotional formation, including sexual and aggressive behavior.

Arousal level of danger center - anxiety

There might be possible at least two polar situations : high level and low level of danger. In first occasion the expectation of danger does exist, and it means preparation either to fight or to escape. The opposite situation is absence of danger. If there is no anticipation of damage, sexual, eating, drinking, intellectual behavior is dominating. So, we can speak about the level of danger and also about the level of danger evaluation. So, we are speaking about the arousal level of the danger center. The question is about the correlation of the danger evaluation to the level of the danger. The level of the danger might be evaluated correctly or incorrectly. If incorrectly it might be either underestimated or overestimated. Both situations might be normal or pathological. In normal situation incorrect estimation of danger level might be because of many reasons : lack of information, unusual environment, etc.

Pathological situation depends of the mental condition of the subject.

Under estimation of the danger might cause technogenic catastrophe.

Overestimation of the danger cause psychogenic anxiety, which is regarded as illness. Special occasion is psychogenic public panic, for example in the cinema somebody cried about fire and the audience rushed to the exit traumatizing each other.

The question is how to differentiate the people who underestimate the danger? What are the criteria of the people who are very susceptible or, from the other side stable to the panic situation. Another problem is training of the correct danger estimation.

Outputs of danger center

Final reaction to danger might depend from at least three important inputs :

- Genetics,
- Tradition,
- Individual experience.

The reactions might be classified into aggressive and escaping types.

Aggressiveness is possible when we can destroy the damaging factor, for example kill the mosquito. If the rock is falling, it is better to step aside. Intermediate profiles are multiple and the percentage of aggressiveness might be sometimes difficult to be established exactly.

Danger escape satisfaction from it

Danger is not stable, it is dynamic feature. We stepped aside from the place of falling rock and there is no danger for us any longer. We feel satisfaction because of the danger passed by. Satisfaction sensation vary individually. Some people have low level of this reaction, others -highintensive. In some of them the level of the reaction is adequate to the risk level. There are the people, who have exaggerated satisfaction after danger or even in the dangerous situation. From this point of view the extreme sports are becoming understandable. From all the above mentioned the whole behavior might be regarded as balancing between danger and satisfaction.

The speculations presented pose many problems about the individual attitude to the risk situations of different individuals, development of the diagnostic methods evaluation of the stuff possibilities and training the adequate danger evaluation.

K. Trinus

trinus@ukrpack.net

RISQUE ET ETHIQUE

Le 22 mai, en partenariat avec le GROUPE SNPE, le Centre National des Risques Industriels (CNRI) a organisé un colloque à l'ENSI de Bourges, sur le sujet « Risques et Ethique ». Deux thèmes ont sous-tendu les exposés et débats tout au long de cette journée :

- L'évolution de la relation de l'entreprise à la société dans « l'après AZF » et l'importance de restaurer la confiance par des règles et des comportements nouveaux.

- Le choix d'une législation et de contrôles renforcés ou l'alternative qui consiste à s'inscrire dans une démarche participative et consensuelle qui permette une approche partagée et durable des risques industriels et technologiques.

Quelques 220 personnes (dirigeants d'entreprises, responsables de collectivités, élus, enseignants, chercheurs, experts dans le domaine des risques industriels, directeurs des ressources humaines, responsables de services de prévention des risques, syndicalistes, étudiants, etc...) ont participé à cette journée où des intervenants aussi prestigieux que C. Lepage, C. Fiterman, Ph. Essig, E. Braine, etc, ont apporté leur avis d'expert, mais aussi leur sensibilité de citoyen, ceci contribuant largement à donner une dimension nationale à cette manifestation.

Cette journée a également été le moment choisi par le CNRI pour faire connaître plus précisément sa stratégie

(formation, recherche, développement économique) et ses priorités d'actions. Les intervenants, les participants, mais également les médias présents, ont pu découvrir la plaquette institutionnelle du Centre National des Risques Industriels, rendue publique à cette occasion (1).

À l'issue du colloque, le Centre National des Risques Industriels a annoncé le second colloque qu'il organise cette année avec le Cérés (Collectif d'Echanges et de Recherches Interdisciplinaires en Sciences humaines et sociales). Celui-ci aura lieu les 16 et 17 octobre prochains dans les locaux de l'ENSI et aura pour thème « les risques industriels et technologiques : enjeux internes et effets externes ».

G. Hayotte

(1) Vous pouvez vous procurer cette plaquette auprès du CNRI

Point de Vue sur le Colloque « Risques et Ethique »

Ce colloque, organisé par le Centre National des Risques Industriels (CNRI) en partenariat avec le Groupe SNPE s'est tenu le 22 mai 2003 à l'ENSI de Bourges.

Des intervenants prestigieux et respectueux du temps de parole et de réaction, un animateur précis dans son questionnement et un auditoire participatif, s'accordant sur le principe de réalité que le risque zéro n'existe pas, ont mis en lumière les principaux éléments qui entrent en jeu dans la compréhension, dans la gestion et dans l'évaluation des risques par des personnes qui, de plus en plus nombreuses, se sentent concernées par les situations à risque tout en ayant des formations, des profils, des logiques et des intérêts très divers, parfois contradictoires. C'est dans ce contexte, où la peur – qui n'est pas déraison – est très présente, que l'éthique apparaît comme un support à la fois fédérateur et rassurant. C'est la pratique d'un comportement éthique qui, au niveau individuel et collectif, légitime les décisions prises ; mais ce comportement va-t-il de soi ? comment l'acquérir, comment le transmettre, le communiquer, le rendre concret à travers les actes et les réseaux d'information ? est-il possible de mesurer le comportement éthique, d'en faire des normes ?

Trouver la réponse à ces questions contribue à préparer le futur - futur qui a été présenté à plusieurs reprises comme étant en crise- puisque c'est la pratique d'un comportement éthique qui :

- permet de communiquer les émotions d'une manière constructive : celle du scientifique qui cherche à

expliquer les causes et les effets, celle du responsable d'atelier qui est directement touché par l'accident, celle de l'opérateur qui, l'espace d'une seconde, a tourné la clé qu'il ne fallait pas, celle du maire qui a hérité d'une agglomération urbaine là où il n'était pas prévu qu'il y en ait une, celle de la victime qui ignorait même l'existence d'une source de danger jusqu'au jour où elle est frappée de plein fouet ...

- aide les dirigeants industriels et politiques, les concepteurs des systèmes complexes sur qui reposent fiabilité, sécurité et disponibilité des installations mais aussi des organisations et des circuits de décision, à faire preuve d'humilité,

- facilite l'engagement dans la durée car si juste après un accident la mobilisation de tous est forte, elle le devient moins avec le temps au point, par exemple, de mettre en péril des lieux d'information pour les collectivités qui finissent par être désertés et donc perdre leur utilité.

Dans ce contexte, est-il possible et souhaitable de voir naître, en France, un « bureau des valeurs et de l'éthique » qui, sur le modèle Canadien, serait chargé de construire une culture capable de faire évoluer les perceptions du risque (car le seul débat, par proche qu'il se veuille des citoyens ou des salariés n'est pas en soi une solution), de diffuser les bonnes pratiques en la matière, d'harmoniser les politiques ?

D'un point de vue cindynique, le colloque a mis en évidence et rappelé plusieurs déficits relatifs, notamment, aux modèles et aux règles plus qu'aux faits, objectifs ou valeurs. Parmi ces déficits figurent :

- la réponse, presque toujours réglementaire, en aval des accidents plutôt que la réflexion amont sur les risques que l'on crée,

- le décalage des rythmes de ceux qui se posent l'objectif de la réduction des risques : industriels, investisseurs, politiques au niveau européen, national, régional, local, citoyens au niveau des riverains mais aussi au niveau national voire européen ou international,

- l'essoufflement des méthodes et des modèles qui prennent appui sur l'élaboration de scénarios majorants donnant ainsi l'impression de maîtrise du risque à priori,

- l'écart entre la « culture du secret » et la « culture du dialogue ». Comment repenser l'acceptation du risque car elle dépend non seulement de plusieurs facteurs mais de facteurs conjoncturels et instables dans le temps ? Que signifie concrètement « organiser le débat au plus proche des citoyens » ? tout en sachant qu'il n'y a pas de lien direct de cause à effet entre le débat (ou l'information) et l'acceptation d'un risque par une collectivité. D'autant plus que, dans le cas des risques industriels, ce n'est pas le seul individu qui choisit de prendre le risque ni la durée pour laquelle il s'expose ni le moment où il arrêtera de le prendre comme cela est le cas pour la consommation de tabac

ou la pratique de certains sports.

L'élément qui est apparu comme étant en frontière entre le risque et l'éthique et, donc, clé d'une possible évolution en France a été celui de l'acceptabilité. Pour utiliser cette notion, il faut évoluer vers des modèles probabilistes, résoudre ce qui est encore présenté comme une contradiction entre risque « réel » et risque « perçu », se doter de moyens pour mesurer l'acceptabilité afin qu'elle devienne un paramètre des calculs probabilistes. Ce schéma semble prendre appui sur une double représentation du risque : le risque « individuel », dont un exemple serait lorsqu'un opérateur meurt dans un accident et le risque « sociétal », plus large et moins probable, comme par exemple, le nucléaire. Toutefois, quelle est la part de l'organisation du travail dans la mort d'un opérateur ? pouvons-nous dire qu'il s'agit d'un risque individuel seulement parce que la victime est un seul opérateur ? Ne sommes-nous pas en face d'un risque tout aussi « sociétal » même si le périmètre géographique est plus restreint ? Et puis, par quels mécanismes, à quel prix l'acceptabilité deviendrait-elle un facteur clé de la réduction de risques ?

Le prochain colloque du CNRI « Les risques industriels et technologiques : enjeux internes et effets externes » qui se tiendra à Bourges les 16 et 17 octobre prochains sera la meilleure occasion pour approfondir la question de l'acceptable dans ses dimensions techniques, politiques, économiques et culturelles.

Angela Minzoni-Déroche

Conseil de Synthèse. Administratrice et Membre du Conseil Scientifique de l'Institut Européen de Cindyniques (IEC)



**L'hyperespace du danger
et son application aux risques logiciels**

Bernard Homès M. Sc., membre (Belge) de l'IEC est consultant, conférencier international et spécialiste reconnu en tests de logiciels. Il est aussi membre du bureau Français de l'IEEE (Assistant VP), et du Comité Aviseur de conférences sur la qualité logicielle, et participe au groupe de travail de mise à jour de la norme IEEE Std 1074-1997 (Standard for Developing

Software Life Cycle Processes).

L'Hyper-Espace du danger a démontré son utilité dans l'analyse et la recherche des dysfonctionnements et catastrophes, industrielles ou non. Son application aux risques logiciels permet de démontrer que de tels risques peuvent être traités de la même manière systémique.

Résumé

Après avoir proposé des exemples d'application des Déficits Structurels Cindynogènes (DSC) dans le monde des SSII (sociétés de services et d'ingénierie informatique), nous verrons comment ces DSC peuvent s'adapter à l'hyperespace du danger. Ensuite nous verrons comment la réduction des risques et l'amélioration de la qualité des logiciels peuvent bénéficier de méthodes, normes et techniques utilisées dans les tests de logiciels. En conclusion nous proposons diverses méthodes pour implémenter ces techniques sur le marché, en prenant en compte les impératifs économiques des sociétés.

Introduction

L'informatique est souvent considérée par les profanes comme le fut l'alchimie il y a plusieurs siècles : une science opaque pratiquée dans des endroits reculés de l'entreprise par des (pseudo) savants utilisant des termes totalement inconnus des non-initiés (sgbd, java, bluetooth, interface, ...). Promettant beaucoup les réalisations n'étaient généralement pas à la hauteur des investissements consentis. La recherche de la pierre philosophale n'est pas différente de la frénésie s'étant emparée de beaucoup de nos concitoyens lors de la période de la bulle Internet.

A une époque où la rentabilité des investissements d'une entreprise devient primordiale, l'atteinte des objectifs fixés dans le respect des coûts et des délais est une priorité. Tout ce qui peut avoir un impact sur ces aspects devient un risque qui ne peut plus être considéré comme mineur.

Les méthodes cindyniques ont montré leur applicabilité dans divers domaines de détection des risques industriels, leur application est aussi possible dans le domaine des risques logiciels.

Définition des risques informatiques

Un projet informatique est un ensemble de tâches administratives et techniques dont la finalité est l'atteinte d'un objectif défini par la hiérarchie. Pour être considéré comme un projet informatique, les tâches techniques doivent – partiellement ou totalement – s'appuyer sur les techniques informatiques telles programmation et/ou développement de logiciels. Un risque sur le projet est toute action qui a un impact sur la réalisation du projet, que ce soit en augmentant la durée et/ou le coût de réalisation de ce projet. Donc tout retard ou toute augmentation du coût du projet est considéré comme un risque, même s'il ne s'applique pas directement à des tâches techniques.

De la même façon nous pouvons étendre le panorama d'application pour inclure l'utilisation des produits logiciels développés. Il est en effet évident qu'un produit logiciel a une fonction de production tout comme un tour ou un moteur. Le mauvais fonctionnement du logiciel est à évaluer au même titre que le mauvais fonctionnement d'un moteur est aussi à évaluer.

Nous nous trouvons donc avec un paradigme où l'utilisation de l'outil informatique de même que sa conception définissent le périmètre des risques logiciels : Un projet qui prend plus de temps ou de ressources que prévu pour être terminé est un projet qui a subi un risque ; si ce projet est un projet de réalisation d'un logiciel ou met en œuvre des outils logiciels il sera donc considéré comme un projet informatique et à ce titre le risque est un risque informatique.

Séparation des risques

Dans le paradigme il est nécessaire de séparer les deux aspects du problème :

- L'utilisation d'un outil informatique pour la réalisation d'une tâche,
- La réalisation d'une application informatique.

Le premier cas n'est pas foncièrement différent de l'utilisation d'un outil pour exécuter une tâche : il faut que l'outil soit adapté à la tâche. La difficulté vient de ce que les tâches à exécuter sont plus complexes et que la spécification d'un outil pour les réaliser est de ce fait plus ardue. L'absence de normes de conception et de définition de spécifications ne rend pas la tâche plus facile. L'outil logiciel est généralement conçu de manière à ce que tous les utilisateurs de cet outil, quelle que soit leur tâche, soient connectés au même outil, un peu comme si tous les outils d'un garage étaient regroupés en un seul, utilisable simultanément par tous les mécaniciens. Il est évident qu'en cas de mauvais fonctionnement, tous sont affectés, ce qui n'est pas le cas si différentes tailles (et/ou marques) de tournevis (par exemple) sont utilisés : en cas de défaillance (bris, perte, ...) d'un tournevis, un autre peut être utilisé en remplacement.

Le second cas est similaire à la conception d'un ouvrage d'art (bâtiment, port, échangeur autoroutier, ...) faisant intervenir plusieurs corps de métier. Il ne viendrait à l'idée de personne de construire une maison sans en faire les plans, les architectes et les ingénieurs de constructions connaissent les standards minimaux pour l'inclinaison des canalisations, des normes existent concernant le nombre et la taille des issues de secours pour les établissements recevant du public. Actuellement, la conception de logiciels est traitée comme un art¹ plutôt que comme une science². Les standards, normes et méthodes sont appliqués de manière non systématique et leur interprétation varie selon les praticiens. Les risques informatique dans ce cas sont donc des risques de fonctionnement

incorrect ou non satisfaisant générant une application insatisfaisante, et des risques de dépassement des délais et budgets pour atteindre un fonctionnement correct.

Illustration par des exemples

Afin de mieux appréhender l'utilisation des dix Déficients Structurels Cindynogènes (DSC) et les mettre en rapport avec des cas concrets de risques informatiques, prenons quelques exemples, associés à chacun des DSC. Les exemples proposés sont tirés, pour la plupart, d'expériences vécues au sein de SSII françaises :

DSC1 : Culture d'infaillibilité :

Pour convaincre un prospect, le commercial ou le directeur de projet annonce que leur SSII est tout à fait capable de résoudre le problème du client, qu'ils ont déjà fait cela pour d'autres clients (montrent une liste de clients grand comptes pour convaincre le prospect). Bien sûr « nous avons les spécialistes et les experts adéquats ». De retour dans leur SSII, il est décidé de former sur le tas un ou plusieurs ingénieurs pour les faire paraître « expert » ou « spécialiste » aux yeux du client. Comme s'il était possible de former un spécialiste en quelques jours...

DSC2 : Culture du simplisme :

Explication souvent entendue dans la bouche de divers responsables : « c'est simple, on fait un prototype puis on l'adapte ». En fait cela revient à simuler un traitement mono-utilisateur et mono-poste puis à augmenter la taille des bases de données et le nombre des utilisateurs. C'est à ce moment que l'on se rend compte des problèmes d'accès concurrent au même enregistrement (faut-il prévenir qu'un autre utilisateur utilise l'enregistrement ?; qui a priorité en cas de sauvegarde ?), des problèmes de backups (on ne peut pas effectuer le backup s'il reste un utilisateur connecté, mais ils sont répartis dans tout le pays), de problèmes de sécurité etc qui n'ont pas été prévus initialement.

DSC3 : Culture de la non-communication :

Dans le cadre d'un projet impliquant de multiples systèmes et donc de multiples équipes de conception (internes et sous-traitants), il est arrivé de nombreuses fois que les équipes ne communiquent pas entre elles, résultant en un échange de données dans des formats incompatibles (ASCII³ vs EBCDIC⁴).

¹ Art : aptitude, habileté à faire qqch. (source : dictionnaire Larousse).

² Science : ensemble cohérent de connaissances relatives à certaines catégories de faits, d'objets ou de phénomènes obéissant à des lois et vérifiés par des méthodes expérimentales. (source : dictionnaire Larousse).

³ American Standard Code for Information Interchange, codage des caractères sur 7 bits préconisé par l'ANSI.

⁴ Extended Binary Coded Decimal Interchange Code, codage des caractères sur 8 bits préconisé par IBM.

DSC4 : Culture du nombrilisme :

Dans un projet de la NASA (sonde d'exploration de Mars), les programmes de guidance étaient développés d'une part en Europe (avec une mesure en Km/sec.) et d'autre part aux USA (avec une mesure en Mille/sec.). Ni l'une ni l'autre des deux équipes ne se sont préoccupées de la possibilité de différence d'unité de mesure, chacune prenant l'unité de mesure qui leur était habituelle.

DSC5 : Subordination des risques à la production :

Beaucoup de SSII fournissent ou mettent sur le marché, sciemment et en connaissance de cause, des applications dont la qualité est médiocre. Ceci uniquement pour satisfaire des dates de livraison associées à des pénalités de retard. Comme le niveau de qualité n'est pas spécifié, ils fournissent ensuite des patches⁵ et autres corrections jusqu'à atteindre le niveau de qualité souhaité ou le montant total des investissements que le client peut se permettre.

DSC6 : Dilution des responsabilités :

La multiplicité des intervenants et la différence de compétences techniques entre les intervenants mène souvent à une dilution des responsabilités : les techniciens rejetant la faute à d'autres techniciens, ou à de mauvaises spécifications, voire à des sous-traitants (ou co-traitants), quand ce n'est pas à des produits qu'ils auraient eux-même proposé (cf projet Socrate à la SNCF).

DSC7 : Absence de retour d'expérience :

Dans la conception d'applications logicielles, il est rare qu'une SSII conçoive plusieurs fois le même logiciel. Le retour d'expérience est donc restreint. De plus le taux de renouvellement des équipes (de l'ordre de 30%) implique que les effectifs sont quasi totalement renouvelés après 3 ans, ce qui ne facilite pas le retour d'expérience. L'analyse des expériences des autres acteurs de la profession est rendu malaisé par un manque de communications et de statistiques.

DSC8 : Absence de méthode cindynique :

Dans la majorité des SSII, l'absence de préconisations écrites de la direction et/ou de l'encadrement laisse libre court à la créativité (ou l'absence de créativité) de chacun des intervenants. En ce qui concerne la sécurité des données informatiques, cet aspect est généralement traité une fois que l'aspect fonctionnel de l'application a été traité correctement. Les risques d'effets de bords entre deux applications ne sont généralement pas traités et n'apparaissent que lors des retours

(plaintes) de la part des utilisateurs.

Dans une banque, le mauvais fonctionnement d'un programme de reprise de données de nuit détruit les informations sur les supports de sauvegarde. Les opérateurs, suivant la procédure en cas de non fonctionnement, reprennent les supports de la journée précédente (même souci) puis des journées antérieures (même souci). Quand ils demandent l'accès au coffre pour prendre la dernière des sauvegardes disponibles, le responsable de l'accès au coffre demande l'autorisation au responsable informatique qui, au vu des informations disponibles, interdit la mise à disposition et sauvegarde ainsi les données comptables concernant plusieurs centaines de milliers de clients.

DSC9 : Absence de formations aux risques :

La formation aux risques des ingénieurs et techniciens informatiques est totalement absente des cursus de formation, ou n'est mentionnée qu'à titre connexe dans certains cas. Ceci est du partiellement à l'absence de statistiques fiables et détaillées sur les causes des dysfonctionnements des applications.

DSC10 : Absence de planification des situations de crise :

Lors d'une anomalie majeure remettant en question le projet, seuls quelques décideurs (commerciaux et directeurs) se réunissent afin de déterminer la meilleure stratégie. La crise n'est traitée que sous son aspect économique et en fonction de l'impact que cela peut avoir sur la comptabilité de l'entreprise ou la poursuite de ses relations commerciales avec son client.

Une nouvelle approche ?

L'analyse des causes des retards ou des dépassements de budget des projets informatiques a fait l'objet de nombreuses études, tant en Europe qu'en Amérique du nord. Les arguments avancés par leurs auteurs varient, mais peuvent se regrouper en trois axes :

- La préconisation de méthodes formelles procédurales ;
- La mise en place de techniques plus ou moins bien adaptées ;
- L'utilisation de normes et standards.

Le niveau de pénétration de ces solutions est variable selon les cultures, important dans les cultures germaniques et anglo-saxonnes, faible dans les pays de culture latine. Il suffit pour se convaincre de ce fait de comparer le nombre de livres publiés sur les tests de logiciels en anglais et en français.

Dans un monde où les échanges et les techniques sont à la base de la réussite économique des structures (états, sociétés, individus), la réduction des risques sur

⁵ Littéralement : emplâtre. Modification appliquée à un logiciel pour effectuer une correction de celui-ci.

les projets est une priorité. L'approche par les DSC et l'hyperespace du danger fourni une approche nouvelle et prometteuse.

Adaptation des DSC à l'Hyperespace du danger

L'hyperespace du danger (voir page 4) permet de regrouper de façon graphique les différentes causes de risques. Nous fournissons ci-dessous une proposition d'adaptation des DSC aux diverses dimensions de l'hyperespace,

1. Axe Statistique : Dimension des faits de mémoire de l'histoire et des statistiques, DSC : 7
2. Axe Epistémique : Dimension des représentations et modèles élaborés à partir des faits DSC : 1, 3, 8
3. Axe des Finalités : Dimension des objectifs et finalités (traduction sociale de l'entreprise) DSC : 2, 3, 4, 5
4. Axe Déontologique : Dimension des lois, normes, règles et standards, obligatoires ou libres DSC : 3, 6, 8
5. Axe Axiologique : Dimension des systèmes de valeur des référents DSC 5, 6, 9, 10



Figure 1 : Hyperespace du Danger

Réduction des risques et amélioration de la qualité des logiciels

Plusieurs méthodes et techniques sont utilisées dans le but d'améliorer la qualité des logiciels :

- Méthodes de détection des anomalies présentes
Ces méthodes ont pour but de détecter des anomalies qui auraient été introduites dans les logiciels. Ce sont donc des méthodes qui se situent en aval du codage et potentiellement sur le chemin critique de la livraison (mise sur le marché).
 - o Tests fonctionnels (automatisés ou non)
 - o Tests de performances (généralement automatisés)
 - o Tests d'acceptation (généralement manuels),
 - o Tests boîte noire ou boîte blanche,
 - o Tests de régression, tests de couverture
- Méthodes de réduction des anomalies futures
Ces méthodes et techniques ont pour but de prévenir des anomalies futures, soit en se basant sur les anomalies existantes (FMEA, gestion de configuration

et d'anomalies), soit en recherchant les incohérences dans les spécifications ou dans le code, préalablement à leur utilisation (V&V, Revues de code et de documents)

- o FMEA (Failure Mode and Effect Analysis)
- o V&V (Verification & Validation)
- o Revues de codes et revues de documents
- o Gestion de configuration
- o Gestion d'anomalies
- Normes

Diverses normes ont pour but de formaliser les développements logiciels et de fournir une documentation servant de référence pour le codage. Ces normes, méthodes et standards peuvent être utilisées dans le cadre de développements logiciels de manière à réduire les risques logiciels. S'il est certain que l'utilisation de ces normes et standards auront dans un premier temps un effet de ralentissement de la production informatique, dans un second temps – généralement assez rapidement – des résultats positifs se font sentir.

Pour l'exemple voici différentes normes pouvant s'appliquer à certains aspects de la qualité des logiciels :

- o ISO⁶ 9126 : Standard pour l'évaluation de produits logiciels
- o ISO/IEC 14598 : évaluation de produits logiciels
- o IEEE⁷ 829 : standard pour la documentation de tests
- o IEEE 730 : assurance qualité des logiciels
- o IEEE 1058 : Standard for Software Project Management Plans
- o IEEE 1059 : guide pour les plans de V&V de logiciels
- o ANSI⁸/IEEE 1042 : guide de gestion de configuration des logiciels
- o SW-CMM : Capability Maturity Model pour les logiciels (CMU/SEI⁹)

Toute politique d'amélioration de la qualité des logiciels produits doit être implémentée en prenant en compte les DSC.

Dimension statistique :

Diverses études, majoritairement nord américaines, démontrent l'impact de la non qualité au cours de l'évolution d'un logiciel. En général le coût d'une correction est 200 fois plus élevé si elle intervient au moment de la livraison du système qu'au moment de la conception de ce système¹⁰. 75% des projets ne se terminent pas dans les délais ni dans les coûts initialement estimés¹¹.

⁶ International Standard Organisation

⁷ Institute of Electrical and Electronical Engineers

⁸ American National Standard Institute

⁹ Carnegie Mellon University / Software Engineering Institute

¹⁰ Source : IBM Research

¹¹ Source : IDC

L'absence de statistiques en France ne doit pas servir de prétexte pour penser que les concepteurs de logiciels nationaux sont meilleurs ; aucune raison ne laisse penser cela, surtout si l'on se rapporte à l'absence de percée sur le marché mondial des logiciels français.

Dimension épistémique :

Certains modèles existent permettant de déterminer un taux d'anomalies par milliers de ligne de code ; d'autres modèles mathématiques sont disponibles pour déterminer la charge de développement (et de tests) nécessaire pour réaliser un logiciel. L'utilisation de ces modèles est généralement repoussée au profit de l'estimation empirique de tel ou tel ingénieur, réduite par le commercial pour tenir dans les budgets du client.

Dimension des finalités :

Le nombre important d'acteurs impliqués dans la définition des finalités en rend la définition risquée. D'une part nous avons les utilisateurs d'un produit informatique, d'autre part les aspects économiques dans le cadre de la conception d'applications informatiques par les SSII. La finalité pour les utilisateurs d'une application informatique est que l'application facilite leurs tâches. La finalité pour les SSII est que le client paye les prestations qui lui sont fournies. Les objectifs sont donc totalement différents, quasiment opposés. Pour l'aspect économique la finalité est de produire l'application au moindre coût et dans les délais les plus courts. Pour l'aspect utilisation, le bon fonctionnement de l'application est primordial.

Dimension déontologique :

Nous avons vu qu'un nombre important de règles et de normes ont été produites par des organismes de normalisation reconnus (IEEE, ISO, ANSI), cependant leur utilisation très réduite. Leur enseignement est plus que confidentiel et leur percée dans la profession est extrêmement faible. Il est donc compréhensible que leur utilisation reste confidentielle.

Outre les normes mentionnées ci-avant, il existe un certain nombre de règles, écrites ou non, déterminant le mode de fonctionnement des composants logiciels visibles par l'utilisateur : un bouton a par défaut telle forme et tel mode de fonctionnement (variant selon le système PC ou Mac), ceci est aussi applicable pour les autres composants d'un écran ou d'une page web.

Dimension axiologique :

Le système de valeur dans le cadre des applications logicielles est difficile à déterminer. Il peut être déterminé par la valeur ajoutée fournie à l'exécution des tâches des utilisateurs (réduction du temps, augmentation de la productivité), il peut être

déterminé par le coût du logiciel, ou par la valeur que met l'utilisateur à des données fiables. Pour un même coût de logiciel, la valeur peut être différente s'il s'agit d'un logiciel de suivi des patients dans une salle de soins intensifs, d'un logiciel d'achat/vente d'actions dans une salle de marchés, ou un logiciel de jeu vidéo.

Implémentation de la réduction des risques

L'implémentation peut venir de deux sources majeures :

- Elle peut être imposée,
 - o soit par des décrets, qu'ils soient rendus obligatoires par le législateur (cf obligation de faire certifier les logiciels du MSSS¹³ par le CRIM¹⁴ au Québec),
 - o soit par des impératifs économiques (cf obligation de faire certifier le logiciel pour obtenir le logo « compatible Microsoft »)
 - o soit imposés par la direction des entreprises
 - o soit par les clients eux-mêmes.
- Elle peut devenir une pratique courante dans le futur en étant enseignée aux futures générations d'informaticiens et de managers.

Si la profession de testeur de logiciels a connu un essor important outre-Atlantique, c'est peut-être suite aux poursuites en dommages et intérêt engagées par de nombreux clients à l'encontre de sociétés développant des logiciels et suite à la mise en place de normes strictes par l'organisme de régulation (FDA¹⁵ et DoD¹⁶ par exemple). Un autre aspect non négligeable outre-Atlantique est la position dominante et militante de certaines associations d'ingénieurs (cf IEEE) dans la diffusion et l'utilisation de normes et de méthodes d'amélioration de la qualité.

Sans une volonté forte de la part des gouvernants, des dirigeants économiques et des clients, y compris des consommateurs, une augmentation nette de la qualité des applications logicielles ne verra pas le jour.

Les méthodes d'amélioration existent, elles doivent devenir d'un usage courant dans la profession.

Propositions

L'approche de la réduction des risques doit se faire par plusieurs canaux :

- La sensibilisation des dirigeants et des responsables, tant au niveau des SSII que des clients
- La formation des futurs cadres et techniciens, et la remise à niveau des ingénieurs
- La mise en place par le législateur d'un niveau de certification rendant obligatoire la mise en place de pratiques cindyniques pour certaines applications telles celles relevant de la santé, des échanges bancaires et/ou des informations à caractère personnel.

La sensibilisation des managers et responsables informatiques est un mode de diffusion de

¹² méthodes des Points de Fonctions (function points), méthodes COCOMO et COCOMO II entre autres

l'information, mais ne doit pas être le seul, surtout que ces interlocuteurs sont confrontés à des impératifs économiques et des sollicitations de toutes parts.

La formation des futurs techniciens et ingénieurs informaticiens, (et des futurs managers) devrait affecter une partie non négligeable du cursus aux aspects de sécurité et de gestion des risques, en mettant l'accent sur les problèmes de responsabilité personnelle des intervenants. Ceci permettra d'obtenir des résultats dans les années à venir. La remise à niveau des informaticiens (par le biais du 1% patronal par exemple) n'est pas une mesure qui donnera des résultats à court terme.

La mise en place par le législateur, (initialement dans des domaines spécifiques tel la santé, la finance, les assurances et/ou pour tout traitement utilisant des données personnelles) d'un niveau minimal de certification, de façon à rendre obligatoire une démarche cindynique permettrait de vérifier l'impact de ces méthodes sur un secteur de l'économie. Cela pourra servir de base de référence pour une extension de ces normes aux autres domaines de l'économie.

Le Canada a déjà déterminé des obligations de certifications pour les logiciels utilisant le Réseau des Télécommunications Socio-Sanitaires (RTSS) ; les Etats Unis, par le biais de la FDA et du DoD ont défini des normes et des méthodes d'amélioration de la qualité des logiciels ; d'autres pays ont, ou vont commencer, ce type de démarches. L'IEC¹⁷, en tant qu'organisme indépendant et impartial, pourrait (devrait ?) se trouver à la pointe de ces efforts, d'une part en proposant des réunions de sensibilisation pour les managers et les dirigeants, d'autre part en étant force de proposition auprès des législateurs, et auprès des organismes d'éducation pour former les informaticiens du 21^e siècle.

Bernard Homès

¹³ Ministère de la Santé et des Services Sociaux (province du Québec)

¹⁴ CRIM : Centre de Recherche Informatique de Montréal (Québec)

¹⁵ Food and Drug Administration

¹⁶ Departement of Defence : ministère de la défense des USA.

¹⁷ Institut Européen de Cindyniques

Tableau des Déficités Systémiques Cindynogènes

Vous trouverez ci-dessous un tableau récapitulatif de dix Déficités Systémiques Cindynogènes.

	Num	Désignation	Symptômes classiques	Application aux logiciels
C U L T U R E , O R G A N I S M E	DSC 1	Culture d'infailibilité	Nous sommes sûrs du succès. Ce système est garanti contre toute défaillance.	Vous aurez votre logiciel dans 3 jours. Nous avons les experts. Il correspondra à vos besoins
	DSC 2	Culture de simplisme	Notre affaire n'est pas complexe, Nous rejetons l'idée de système, Ça marche sans méthodes complexes.	La solution proposée est la plus simple et nous avons de l'expérience avec ce type d'applications.
	DSC 3	Culture de non communication	On ne peut vivre en remettant en question certaines vérités évidentes de notre métier, La hiérarchie de notre entreprise supporte mal la remise en question des pratiques techniques. On discute peu entre nous des opérations pratiques. Le personnel parle Hindi, l'équipage le portugais, les passagers le norvégien.	Notre méthodologie a fait ses preuves dans de nombreux cas. Les évolutions techniques sont suivies et mises en place : nos développeurs sont utilisés en fonction des besoins (pas de coordination ?)
	DSC 4	Culture nombriliste	Nous sommes les leaders et nous économisons pas mal de temps du fait que nous n'allons pas voir ailleurs ce qui se passe. Nous avons toujours été les premiers à percevoir les problèmes de notre profession. Nous sommes certains du retard de nos concurrents en matière de sécurité.	Nous sommes expérimentés et nous n'avons pas besoin de normes pour nous dire comment travailler. « Nous avons une expérience reconnue [...] dans les principaux secteurs qui sont les nôtres [et] une connaissance approfondie des métiers et des défis économiques de nos clients »
O R G A N I S A T I O N	DSC 5	Subordination des fonctions de gestion du risque aux fonctions de production ou à d'autres fonctions de gestion créatrices de risques	Le responsable de la sécurité n'est qu'un collaborateur parmi d'autres du responsable de production. On ne va tout de même pas réduire les prérogatives du chef de production ou lui compliquer la tâche. On crève sous les fonctionnels, ce n'est pas le moment d'inventer un autre. D'accord, il y a des risques, mais ce n'est pas pour semer le désordre dans nos structures.	Nous incluons les aspects sécurité après avoir développé les aspects fonctionnels. La sécurité sera constituée d'un mot de passe, ... (rien n'indique ce qui doit se passer en cas de mot de passe erroné, ni comment les données seront sécurisées si elles sont accessibles par base de données, ni comment les échanges seront sécurisés, ...)
	DSC 6	Dilution des responsabilités Non explicitation des tâches de gestion des risques. Non affectation des tâches à des responsables désignés.	Nous avons rejeté tout formalisme dans notre organisation, chacun peut s'exprimer avec spontanéité. Les gens sont adultes et savent parfaitement ce qu'ils doivent faire sans qu'il soit utile de le leur rappeler.	Dans la définition du lien entre deux applications, aucun des interlocuteurs ne divulgue les risques liés à la perte d'informations au cas où le lien tombe (perte de données, pas de point de reprise, duplication des informations..)

M E T H O D E D E G E S T I O N	DSC 7	Absence d'un système de retour d'expérience.	Maintien de pratiques considérées comme dangereuses dans d'autres établissements ou organisations. Pas d'attention aux signes précurseurs apparaissant dans la même profession. Pas d'exploitation systématique des faits concernant les dysfonctionnements survenus mondialement dans le même domaine technique.	La veille technologique, quand elle est présente dans les ssii est tournée vers les nouveautés et non vers la recherche de dysfonctionnements survenus dans le même domaine. De plus les dysfonctionnements ne sont généralement ni publiés ni discutés par peur de détériorer l'image de marque.
	DSC8	Absence d'une méthode cindynique dans l'organisation.	Dans ce secteur, il faut reconnaître qu'il n'y avait pas de manuel ou d'instruction écrite de la direction.	Nombre de sociétés ne possèdent pas de méthodes de réduction ou d'analyse des risques logiciels.
	DSC 9	Absence d'un programme de formation aux cindyniques adapté à chaque catégorie de personnel.	Les gens des ateliers ont été pris au dépourvu et ont commis des erreurs qui ont aggravé les choses.	Les procédures mises en place sont souvent peu claires et amènent à des situations aggravant les risques.
	DSC 10	Absence de planification des situations de crise.	Quand on a entendu ce bruit épouvantable, tout le monde s'est mis à courir dans toutes les directions.	Les seuls points pris en compte comme situation de crise sont les aspects de perte de données. On a vu cependant lors des événements du 11 septembre 2001, que les risques ne se limitent pas aux données, mais incluent aussi les aspects matériels, humains et fonctionnels, y compris pour les sociétés clientes des sociétés touchées dans les tours jumelles du WTC.



**INSTITUT EUROPEEN DE
CINDYNIQUES
COMPTE-RENDU
DE L'ASSEMBLEE GENERALE
DU 26 juin 2003**

1ère Partie :

L'Assemblée Générale de l'IEC s'est tenue le jeudi 26 juin 2003 dans les locaux de l'Ecole Supérieure des Travaux Publics à Paris. Une quinzaine de membres de l'institut étaient présents mais de nombreux mails d'excuses de membres prouvaient leur intérêt à cette assemblée mais leur impossibilité à être présents à la date envisagée.

Elle a débuté à 17 h 30 par une conférence-débat de Monsieur Chris Lajtha, Risk Manager chez Schlumberger, qui a traité de la notion de risque dans les entreprises multinationales ayant des intérêts dans les pays les plus variés.

Cette présentation a démontré l'usage fait des "politiques" (policies papers) à appliquer dans toutes les opérations affectant le fonctionnement de cette multinationale.

La particularité de Schlumberger est de travailler sur un créneau qui n'est plus la seule recherche-exploration pétrolière, au service des entreprises mondiales du secteur, mais bel et bien le créneau large de la gestion d'information.

Monsieur Lajtha a insisté sur son rôle d'animateur-coordonnateur (par opposition à «manager») pour faire passer les messages. Il a longuement souligné le fait que chacun était responsable de l'application de ces politiques à son niveau, la méconnaissance ou la non application des recommandations étant considérée comme une faute inexorable par l'entreprise.

A la tête d'une équipe de six personnes il pratique une veille en matière de risque sur l'ensemble du monde et en informe l'ensemble des acteurs de la société sur un site intranet, de telle sorte que les informations données deviennent des connaissances communes pour tous les acteurs concernés du Groupe, coordonnant ainsi efficacement leurs actions.

Une synthèse de la présentation sera présentée sur le site internet de l'IEC dès que l'orateur la transmettra à l'Institut

2ème Partie :

Elle a continué par l'Assemblée Générale proprement dite qui a commencé vers 19 heures.

Le Président Frantzen a lu le rapport moral qui suit :

Rapport moral sur l'exercice 2002 et le début de 2003

Tout d'abord nous aurons une pensée émue pour notre ami Francis Delobea qui est décédé le 10 juin 2003. J'ai exprimé, avec retard, à Madame Delobea la tristesse que nous éprouvons tous.

La Lettre des Cindyniques rappellera à tous nos membres tout ce que Francis Delobea a apporté à notre Institut.

1. La démission, pour raison de santé, de notre Secrétaire Général, Bruno Folléa, conduit à ce que ce rapport moral soit présenté par le Président. Cela me paraît encore plus approprié compte tenu du fait que, comme on va le voir, la situation impose la prise de décisions importantes pour l'avenir de l'Institut et de ses membres.
2. L'activité de l'institut s'est peu à peu limitée à :
 - la parution de " La lettre des Cindyniques ", pour la quelle

Patrick Rubise s'épuise à obtenir des contributions ; il obtient néanmoins des résultats qui paraissent appréciés de nos lecteurs ; en 2002 trois lettres ont été produites et diffusées par courriel et par courrier ;

- le site internet, totalement l'œuvre de Gérard Bouget, qui est un franc succès si on regarde la courbe toujours ascendante des consultations (les véritables consultations) ;
- un seul groupe de travail, certes double, (" facteur humain et responsabilité pénale " et " risque et opinion publique ") animé à Lyon par Roger Grollier Baron et qui rassemble des ingénieurs et des magistrats,
- le colloque " risque et démocratie, vers de nouvelles formes de gouvernance ? ", sur lequel je reviens plus loin,
- Tous les autres groupes ont disparu, quelles que soient les intentions toujours optimistes mais jamais concrétisées,
- Les contacts avec l'Institut Méditerranéen de Cindyniques se sont poursuivis et de nouveaux contacts ont été établis avec le C.N.R.I. de Bourges et avec l'Ecole d'Administration Pénitentiaire.
- Le trésorier vous présente par ailleurs les comptes de l'exercice 2002.

3-Le colloque s'est construit dans une situation très délicate :

- faute de temps disponible, la " chasse aux sponsors ", toujours difficile en ces temps de rigueur, encore plus difficile par la réticence de nombreuses entreprises à s'engager sur un thème pouvant déranger leur communication courante en matière de risques, n'a pu réunir que des ressources très limitées ; les seuls sponsors ont été Total, qui soutient depuis longtemps notre institut, EDF et GDF amenés par le Président, deux PME amies de notre trésorier qui ont fourni des prestations à prix cassé, l'ADEME sensibilisée au travers du comité de programme. Hors de ce réseau de relations très étroit rien n'a été fait, enfin l'INERIS qui a fourni une secrétaire à mi-temps pendant trois mois,
- Gilles Hériard-Dubreuil (Mutadis) a réuni un comité de programme très efficace sur le plan scientifique, mais qui, à l'exception de l'ADEME, a toujours voulu ignorer les difficultés provoquées par ce défaut de financement et donc pour l'organisation matérielle,
- le CEPN, dont le directeur était membre du comité de programme, et qui avait déjà organisé très efficacement des manifestations comparables, a proposé son aide pour l'organisation matérielle et la communication ; mais les moyens très limités qu'il pouvait consacrer à ces tâches et la faiblesse encore plus critique de l'Institut (1 seul administrateur consacrait un peu de temps à l'organisation matérielle et en disposant d'un budget insuffisant) n'ont pas permis que se noue une véritable coopération ;
- le contenu scientifique du colloque a été très apprécié et tous ceux qui y ont contribué doivent en être remerciés ; l'organisation matérielle a bien fonctionné (merci à Gérard Bouget qui l'a entièrement prise sur ses épaules) ; mais l'annonce médiatique du colloque ayant été inexistante, les participants ne sont venus que par bouche à oreille (avec l'Email entre les deux...) ; on n'a donc pas fait le plein de participants payants à la limite de capacité des salles ; or comme ce sont les derniers payants qui rendent la marge financière positive, les résultats du colloque sont décevants, probablement juste équilibrés, le résultat définitif n'étant toujours pas parvenu, et certaines factures n'ayant pas encore été reçues ;
- très globalement je dirai que ce colloque a eu un effet modéré sur la notoriété intellectuelle de l'institut, un effet nul sur les ressources et enfin qu'il a mis en pleine lumière le fait que celui-ci n'existe que par trois personnes !

4-La fraction du conseil d'administration qui consacre à

l'Institut au moins le temps de ses réunions a examiné cette situation et en a conclu qu'une réflexion en profondeur sur l'avenir de l'institut s'imposait. Pour la favoriser, le conseil, lors de sa dernière réunion, a décidé de démissionner collectivement.

5-Pour ma part je ne vois d'avenir pour un cadre associatif de promotion de concepts « cindyniques » que dans un rapprochement fort avec le nouvel « Institut pour la Maîtrise des Risques et la Sécurité De Fonctionnement », héritier de l' « Institut de Sécurité de Fonctionnement » de feu le « M.F.Q. ». Un seul « guichet » permettrait aux entreprises, sans lesquelles le cadre associatif est totalement inefficace, d'y trouver le lieu d'échange en matière de maîtrise des risques, depuis la vision politique et stratégique, jusqu'aux outils scientifiques concrets et quotidiens.

6-Aussi je propose à vos suffrages la désignation d'un nouveau conseil d'administration composé de celles et ceux qui ont démontré pratiquement et encore récemment qu'ils pouvaient amener à l'institut des apports très concrets (du temps, des sponsors, des animateurs qui eux même amènent...), plus Guy Planchette, Président de l'I.M.R. ; ce nouveau conseil aurait comme mission de conduire en un an le rapprochement des deux associations. Dans mon esprit ce rapprochement devrait aller jusqu'à la fusion. Si telle était la conclusion de l'année de travail du nouveau conseil, alors notre prochaine assemblée générale devrait être une assemblée extraordinaire prenant les décisions appropriées.

7- Dans cette perspective, je propose de maintenir pour l'instant le montant des cotisations pour 2004 au niveau qui avait été fixé pour 2003.

Claude Frantzen

Présentation des comptes par le Trésorier

Le Trésorier, Gérard Bouget, a présenté les comptes de l'Institut :

- Comptes de l'IEC :

	Budget 2002 réalisé		
	DEBIT	CREDIT	
Fouritures	1695,35	5625,36	Adhérents
Loyer	6705,04	9292,45	Sponsors
Assurances	443,48		
Site Web	5294,91		
Publications	3812,17	470,04	Vente
Missions,			
Réceptions	5604,00		
Poste	165,04		
Téléphone, Fax	749,82	22866,45	Sp colloque
Σ TFSE	24 469,81	Euros	
Salaires et charges			
Partage Secrétaire	5 945,52		
Σ «Salaires»	5 945,52		
Total Débit	30 415,33	Total Crédit : 38 254,3	

Résultat 2002 positif mais lié aux entrées de capitaux du colloque

	Budget 2003 prévisions		
	Débits	Crédits	
TFSE	20 000	8 800	Adhérents
Secrétariat	10 000	24 000	Sponsors
		1 000	Publications
Total Débit	30 000	33 800	Total Crédit

- Comptes du Colloque

Liste des frais

	Budget	Réalisé
Secrétariat	8970	8970,00
Plaquette	5604	5945,52
Frais Comité de programme	6000	2852,35
2eme plaquette	5000	5001,43
Tirages divers (programmes, ...)	500	1680,00
Salle UIC (*)	9614	9937,41
Mercure avec 25 chambres (*)	17250	17515,00
Hilton (*)	21100	20090,00
Transport	4000	5231,76
Service sécurité/hôtesse	2600	0,00
Badges	3000	1500,00
Frais divers	5000	1337,49
Assurance spécifique	1500	1215,00
Réserve (environ 10%)	10000	
Total général	10 0138	81 275,96

Résultat financier

Total des dépenses : 81 275,96

Payants IEC	7 600,00	20
Payants non IEC	17 200,00	40
Part. réduite	400,00	4
Invités		75
Sponsors	44 111,45	

Total des entrées : 69 311,45

Attente ADEME	10 000,00
Total prévu :	79 311,45
Perte	1 964,51

Mais attente réglements...

Présentation du Conseil d'Administration proposé par ordre alphabétique :

- Gérard Bouget,
- Claude Floret,
- Claude Frantzen,
- Didier Gaston,
- Claude Janvier,
- Angela Minzoni-Deroche,
- Bertrand Munier,
- Guy Planchette,
- Jean-François Raffoux,
- Patrick Rubise,
- Olivier Sorba.

Les votes :

	OUI	NON	Abstentions
1° - Approbation des comptes 2002	73%	-	27%
2° - Quitus gestion 2002	87%	-	13%
3° - Election d'un nouveau CA	80%	1%	19%
4° - Cotisation 2004 identique à 2003	87%	-	13%

Immédiatement après, le Conseil d'Administration
nouvellement élu a défini les responsabilités attribuées :

Guy Planchette	- Président
Claude Frantzen	- Vice Président
Jean-François Raffoux	- Secrétaire Général
Patrick Rubise	- Délégué Communication
Gérard Bouget	- Trésorier
Angela Minzoni Deroche	- Contrôleur

Petites nouvelles

Le GRID, laboratoire de recherche CNRS créé à l'ENS de Cachan il y a une dizaine d'années (et qui avait été présenté dans ces colonnes) partage désormais son rattachement institutionnel entre le CNRS et l'ENSAM, à laquelle l'ESTP est rattachée depuis 1999. Il reste l'UMR 8534 du CNRS et continue à conduire, à côté d'interventions en gestion des risques au profit des entreprises et des organisations publiques, des recherches fondamentales sur la modélisation et le traitement du risque et de la décision en avenir risqué et incertain.

Nouvelles coordonnées : GRID, Maison de la Recherche de l'ESTP, 30, avenue Wilson, 94230 Cachan.

Mail : grid.ensam@estp.fr

Site web: www.grid.ensam.estp.fr

Les formations à la recherche et par la recherche (DEA Sciences de la Décision et Microéconomie des Risques) et de type professionnel (Mastère Spécialisé des Grandes Ecoles en Management Global des Risques) sont répertoriées sur le site de l'IEC, www.cindynics.org et décrites en détail sur le site web du GRID. Souhaitons que le nouveau cours que le laboratoire va connaître dans cette configuration originale soit à l'origine de techniques nouvelles et de savoirs renouvelés en matière de gestion des risques industriels.

INSTITUT EUROPEEN DE CINDYNIQUES

Adresse :

9 rue de Rocroy - 75010 PARIS

Tél. : 01 48 78 46 59

Fax : 01 48 78 47 90

E-mail : secretariat@cindynics.org

Pour connaître l'I.E.C., consulter le contenu d'articles ou de lettres anciennes, un site WEB est à la disposition du public (plus de 6 000 consultations par mois actuellement) :

www.cindynics.org

« LA LETTRE DES CINDYNIQUES »

Directeur de la publication : Guy Planchette

Directeur de la Communication : Patrick Rubise

La reproduction totale ou partielle des articles figurant dans La Lettre des Cindyniques est interdite, sauf accord préalable de la rédaction.