

Le retour d'expérience : principes, échecs et perspectives

Elodie Gigout
i3-CRG École polytechnique CNRS Paris-Saclay

Le REX (retour d'expérience) est reconnu aujourd'hui comme étant un des piliers de la gestion des risques. Cependant, malgré sa mise en place, des catastrophes perdurent et, bien souvent, dans les analyses post-événements, on se rend compte que la catastrophe aurait pu être évitée si un certain nombre de signaux avaient été pris en compte. Nous commencerons donc par expliquer ce qu'est le REX puis nous détaillerons l'analyse de ces échecs en nous basant essentiellement sur la communication de Dechy & Dien (2007)¹ et nous aborderons enfin les perspectives pour améliorer le REX.

Qu'est-ce que le REX ?

Pendant très longtemps, afin de faire perdurer les connaissances, le système du biseau était mis en place, à savoir un dédoublement temporaire des postes afin de faire du transfert de connaissance. Cependant, cette démarche est limitée dans son efficacité notamment par le fait que toutes les situations qui produisent de la connaissance ne se produisent pas au moment de la mise en place du biseau (Bès, 1998). Selon cet auteur, les connaissances sont une ressource de l'entreprise indissociable de l'action et en perpétuel renouvellement. Le REX est né d'un besoin de capitalisation des connaissances. Historiquement, le secteur nucléaire (CEA et EDF) est le premier à se lancer dans le REX, le besoin de capitalisation des connaissances étant rendu possible par les avancées technologiques de l'informatique. Le CEA, en particulier, se doit de garder ses connaissances actives à cause notamment de l'arrêt des projets Phénix et Superphénix et du défi du stockage des déchets à long terme. Ce besoin de capitalisation des connaissances est renforcé par l'obligation de conservation des compétences imposée par le législateur au domaine nucléaire (Bès, 1998). Alors que nous faisons tous du REX sans le savoir – nous apprenons de nos erreurs afin de ne pas les reproduire –, dans une organisation complexe, « *la mémorisation des connaissances et leur réappropriation ne sont des processus ni naturels ni automatiques* » et « *la difficulté essentielle des actions de capitalisation et de repêchage des technologies porte sur la préservation du contexte d'élaboration* ».

Initialement, le REX était centré sur la sûreté de fonctionnement. Par la suite, il a progressivement étendu son domaine aux Facteurs Organisationnels et Humains (FOH). Ainsi, il peut être vu comme une mémoire de la connaissance acquise au sein de l'entreprise. Mais il peut également être la source même de cette connaissance dans la mesure où l'analyse de l'accident, de l'incident ou du signal faible, peuvent créer cette connaissance (Dechy & Dien, 2007).

L'IMdR (INSTITUT
DU MANAGEMENT
DES RISQUES),
ORGANISE LE
CONGRÈS LAMBDA
MU (λμ) TOUS LES
DEUX ANS. EN
OCTOBRE 2014, LA
XIX^{ÈME} ÉDITION
S'EST DÉROULÉE À
DIJON AVEC POUR
THÈME : « DÉCIDER
DANS UN MONDE
INCERTAIN : ENJEU
MAJEUR DE LA
MAÎTRISE DES
RISQUES »

1. Les références bibliographiques présentes dans cet article sont essentiellement basées sur les actes des communications de différents congrès de l'IMdR.

Dans leur article, Dechy & Dien identifient différentes étapes du REX :

Le processus global de REX qui est partie prenante dans l'apprentissage organisationnel, comporte plusieurs étapes :

- la définition de la politique de REX (type d'événement à traiter, ressources allouées, relations entre les entités impliquées dans le REX, ...) ;
- la détection de l'événement ;
- la collecte des données ;
- l'analyse de(s) l'événement(s) ;
- la définition des mesures correctives ;
- la mise en œuvre des mesures correctives ;
- l'évaluation, à terme, de l'efficacité des mesures ;
- l'archivage de l'événement, de ses enseignements et de son traitement ;
- la communication des enseignements aux parties prenantes ou potentiellement intéressées.

Les auteurs font l'hypothèse que si l'une des étapes du processus est défaillante, le processus REX est affecté dans sa globalité. Grâce à une analyse des échecs du REX dans leurs dimensions verticales, transversales, historiques et communicationnelles, ils identifient des défaillances majeures des processus REX que nous reprendrons ci-dessous et auxquelles nous ajouterons les pistes explorées par des chercheurs ayant présenté leurs travaux lors du congrès µ19.

Les échecs de l'analyse du REX : causes et perspectives

La collecte des données

Le REX se base sur des données. Une des premières questions à se poser est donc : quelles sont celles que l'on va collecter et quels sont les moyens que l'on va affecter à ce recueil ? Le choix des données recueillies repose sur une vision des causes que l'on cherche à identifier : « *la stratégie générale et la culture d'entreprise déterminent directement la place des expériences et des expertises dans le management de projets* » (Bès, 1998).

Cependant, pour que les données recueillies auprès des différents acteurs soient de qualité, il convient d'instaurer un climat de confiance et de non punitivité afin que la parole soit libérée et non pas auto-censurée (ces deux conditions ont été exprimées lors de l'atelier sur le REX du congrès µ19). En effet, une des premières choses qui peut poser problème est la crainte de parler des difficultés rencontrées de peur d'une mise en cause personnelle. Si elle est nécessaire, l'évaluation suite à un événement est difficile à mener puisque se pose la question des conséquences pour la personne. Souvent les personnes peuvent tenter de combler l'écart entre le réel et le prescrit (Bourrier, 1999) afin que rien ne puisse leur être reproché.

Alors que, sur le long terme, privilégier le risque d'être mis en cause juridiquement plutôt que la sécurité ou sûreté n'est pas bénéfique puisque de plus graves incidents peuvent survenir, Dechy & Dien (2007) indiquent que cette prise de conscience est difficile à faire naître quand le *turn over* est important. Le gain que représente dans un service le fait de ne pas avoir de problème est favorisé par la dilution de la responsabilité. En externe, la communication sur les incidents peut être bloquée par la crainte de sanctions. En interne, si ces incidents font partie des indicateurs, une logique concurrentielle peut amener les personnes à éviter la diffusion de l'information.

Enfin, les auteurs précisent que « *la collecte de données est rarement menée au niveau de l'analyse du travail, au niveau des facteurs humains, organisationnels, culturels et sociétaux.* » (Dechy & Dien, 2007).

L'importance des causes profondes organisationnelles et culturelles

En se basant sur l'analyse d'un certain nombre d'événements, Dechy & Dien (2007) montrent que l'analyse porte trop peu souvent sur les causes profondes, notamment les « *Facteurs Organisationnels Pathogènes* ». Un accident est trop souvent résumé par l'erreur humaine ou la faiblesse technique, et il y a trop peu de descriptions du travail des cadres et de points de vue des acteurs directs.

Périnet et Garandel (2014) partent de ce même constat :

Par exemple, à la suite de la catastrophe de Tchernobyl (1986), les premiers éléments fournis par les responsables russes faisaient peser tout le poids de l'accident sur les opérateurs en insistant sur les non-respects de règles de conduite. L'analyse des causes profondes de l'accident a révélé que ces règles n'étaient ni claires ni comprises et que les principales causes de la catastrophe étaient en réalité liées à la conception de l'installation, à la pauvreté des études de sécurité ainsi qu'à la faiblesse des spécifications techniques d'exploitation et de la formation qui en résultait

et ajoutent :

L'erreur humaine est le symptôme de dysfonctionnements plus profonds et doit être considérée non comme l'aboutissement mais comme le point de départ de l'analyse.

En partant du principe que l'on ne trouve que ce que l'on cherche et que, de fait, la collecte de données est influencée, le Groupe de Travail et de Réflexion « Organisation et maîtrise des risques » de l'IMdR, indique qu'il faut adopter une posture moins normative et plus naïve pour laisser de la place à la surprise. L'objectif du groupe était de fournir un outil qui permette de prendre en compte la complexité des systèmes et ceci notamment en multipliant les points de vue pris en compte lors de l'analyse d'un incident, en se basant sur le principe de variété requise des HRO (High Reliability Organisations). Une marguerite a ainsi été créée, dont les pétales représentent des thèmes. Une première version de la marguerite est proposée aux participants avec des thèmes prédéfinis et on leur demande d'indiquer le degré d'implication des thèmes dans l'événement. Puis une seconde marguerite, avec des thèmes élargis, notamment organisationnels, leur est proposée. Ensuite, les participants sont amenés à ajouter des thèmes dont ils pensent qu'ils ont eu un impact sur l'événement. Les participants sont volontairement des acteurs de différents domaines liés de près ou de loin à l'incident. Ainsi, la marguerite s'étoffe progressivement et permet d'ouvrir le débat entre des personnes issues de domaines très différents. Cet outil permet de prendre en compte aussi bien les causes directes que les « facteurs d'influence », dont le lien de causalité avec l'événement ne peut pas être prouvé. La vocation de l'outil n'est pas de « *remplacer les techniques classiques telles que l'arbre des causes, mais de les compléter en ouvrant des axes supplémentaires* ».

Pendant longtemps, le REX a consisté en une analyse des événements après coup. Progressivement, il tend vers une anticipation visant à prendre en compte les événements précurseurs. Ceux-ci peuvent alors être analysés et identifiés correctement, ainsi que le risque encouru. Le REX prend donc deux formes : un REX réactif qui, une fois



Gris bleu, Serge Poliakoff (1962)

un événement intervenu va essayer d'en retrouver les causes, et un REX proactif essayant de repérer les signes précurseurs d'incidents (Dechy & Dien, 2007).

La traque des signaux faibles

Le REX proactif prend notamment la forme de la traque et du repérage du signal faible que Vaughan (2001) définit comme « un signal difficile à décoder, ou un signal qui, après analyse, paraît si improbable que les opérateurs considèrent qu'il a peu de chances de se reproduire ».

Détecter un signal faible n'est pas chose aisée puisque nous ne sommes pas conscients de ne pas savoir. La représentation du monde acceptée doit être remise en cause afin que puisse apparaître l'inadéquation entre cette représentation et le risque qui menace. La difficulté peut être amplifiée si le risque lié au signal faible a été préalablement associé à d'autres signaux, devenus routiniers. Dans un tel cas de figure, la menace est attribuée à cette cause bien identifiée, et il est dès lors encore plus difficile de repérer des signaux faibles liés à elle. Un autre cas peut se présenter : celui dans lequel des informations contradictoires empêchent le repérage des signaux faibles. Un exemple est donné par l'incident de la centrale de Millstone qui avait pourtant des résultats exemplaires en matière de sécurité comparés à ceux de la centrale de Milgrim (Dechy & Dien, 2007).

Dès lors, comment opérationnaliser l'exploitation des signaux faibles *a priori* ?

Dechy, Jouniaux & Hadida (2014) posent une définition du signal faible en termes de relation :

Données de source formelle ou informelle qu'une organisation saurait positionner dans un scénario de défaillance ou d'affaiblissement vis-à-vis de la maîtrise des risques critiques (fort du savoir scientifique, technique et professionnel).

Cette nouvelle définition influence leur approche du « traitement » des signaux faibles. Elle mêle analyse des données et expertise au cours des trois étapes définies ci-dessous, en se basant sur des facteurs organisationnels et humains et des statistiques de sûreté de fonctionnement :

- La détection est l'étape qui « associe des démarches expertes et de traitement des données pour trouver le lien entre les données REX et un scénario de sensibilisation au risque » ;
- L'évaluation de la pertinence de la relation entre le risque et les données vient ensuite ;
- L'amplification consiste à ré-interroger le modèle de défaillance après la prise en compte du nouveau risque, en le confrontant à ce qu'il était auparavant. Cette étape crée de la connaissance et va permettre de prendre en compte la relation, notamment au travers d'indicateurs de suivi.

Une telle démarche nécessite des préalables, à savoir :

- Une implication de la direction mais aussi des personnels dans la démarche de sécurité/sûreté ;
- La mise en place d'un processus efficace de remontée d'informations, de données objectivables mais aussi de données de contexte, notamment via des éléments de textes libres (questions ouvertes, par exemple) ;
- La connaissance du risque organisationnel qui doit permettre de créer des barrières efficaces.

Escande, Le Coze & Proust (2014) proposent également de tenter de trouver de nouveaux scénarios accidentels. Selon eux, la méthode ne doit pas être uniquement rationnelle, mais doit s'appuyer sur l'abduction² qui, « au vu d'une observation

2. Sur la notion d'abduction, voir Dumez (2012).

surprenante conduit à émettre une hypothèse plausible » dans une « *démarche qui associe “hasard et sagacité” : la sérendipité* ». La démarche est celle employée par les détectives – on pense à Sherlock Holmes – qui, à partir d’un savoir hétéroclite et d’une bonne capacité d’observation, formulent une hypothèse en partant d’un indice. Ici, il s’agit de formuler un scénario à partir de signaux faibles, puis de tenter de le valider grâce à de nouvelles observations. Sur le terrain, c’est de cette manière que fonctionnent les experts. Tirant parti du hasard, une telle démarche n’est pas programmable, mais elle peut être favorisée par la constitution de bases de données factuelles importantes mêlant de l’opérationnel et de l’organisationnel et l’utilisation d’un outil permettant de repérer les analogies et les similarités.

Selon Dien (2014), une amélioration de la détection des signaux faibles peut être envisagée *via* une meilleure écoute des lanceurs d’alerte, ces derniers pouvant être vus comme des relayeurs de signaux faibles. Il rappelle quelques caractéristiques du signal faible :

- « *Il est qualitatif, intuitif et subjectif* »
- « *Il est porteur d’une information fragmentaire* »
- « *Sa signification est ambiguë* »
- « *Il ne répond pas au canon du positivisme scientifique qui demande des faits vérifiés ; ainsi, lorsque les ingénieurs de Morton Thiokol firent part de leur souci la veille du vol fatal de la navette Challenger, des responsables de la NASA leur demandèrent de “prouver” le risque, de “quantifier leurs inquiétudes”* »

Or, Turner (1978) définit la sécurité comme un ensemble de croyances partagées par l’organisation ; dès lors, si quelque chose ou quelqu’un vient contredire ces croyances, il est fréquent qu’un déni se produise : celui qui lance une alerte est souvent catalogué comme un éternel mécontent. Pourtant, selon Dien (2014), la traque des signaux faibles peut être améliorée par l’écoute des lanceurs d’alerte et, pour ce faire, des débats doivent être engagés sur la sécurité sans « *phénomène de censure ou d’autocensure* ». Ces débats ne peuvent être que bénéfiques car ils donnent une place centrale à la question de la sécurité.

Les mesures correctives comme partie intégrante du processus REX

Suite à la détection et à l’analyse de nouveaux risques, des mesures correctives devraient être prises. Mais la mise en œuvre de ces mesures peut se heurter à des arbitrages défavorables liés à des enjeux autres que celui de la sécurité. Dans l’accident de la raffinerie Avon de Tosco qui, en 1999, coûta la vie à quatre ouvriers ayant essayé de colmater une fuite dans une conduite, le problème de corrosion était reconnu mais rien n’avait été fait pour y remédier. Pour éviter que les mesures nécessaires soient négligées, une des solutions est que les autorités se saisissent du problème en changeant la réglementation (Dechy & Dien, 2007). Mais il s’agit là d’une solution à long terme. Dans l’action, s’opposent deux impératifs : prendre des mesures correctives le plus rapidement possible pour pouvoir « relancer la machine » et prendre le temps nécessaire pour mettre en place des mesures correctives issues d’une analyse digne de ce nom. Périnet et Garandel (2014) attirent par ailleurs l’attention sur le fait que la fiabilité humaine n’est pas uniquement faite de procédures et de formation. Ces deux mesures peuvent même se révéler contre-productives. L’outil que les auteurs ont mis au point, la marguerite dont nous avons parlé plus haut, dans la mesure où elle permet de prendre en compte différents points de vue, ouvre le champ des possibilités en termes de leviers d’action, et donc de mesures correctives. Il faut, de plus, faire très attention au phénomène de leurre identifié par Turner (1978).

Un problème mal défini est souvent associé au phénomène de « leurre », c'est-à-dire que les précautions prises pour faire face au(x) risque(s) supposé(s) distraient l'attention du ou des risques qui seront finalement avérés. La mauvaise définition du risque [...] entraîne une « cécité organisationnelle » vis-à-vis de la sécurité de l'installation. (cité in Dien, 2014)

Bulot et Sfez (2014) évoquent le problème de mesures correctives difficilement applicables dans un service de radiothérapie. Ces chercheurs ont alors développé une méthode (utilisation d'un outil d'analyse *a priori* – APR Analyse Préliminaire des Risques – pour mener une analyse *a posteriori*) qui permet de mettre en place des actions correctives adaptées à la maille des services et décidées collectivement, donc mieux connectées à la réalité. Cet exemple montre que le processus REX n'est pas terminé tant qu'il n'y a pas eu preuve d'une amélioration. En effet, une mesure corrective peut se révéler contre-productive et déstabilisante. Le suivi de sa mise en place est donc nécessaire, et il devrait être partie intégrante du REX, ce qui est rarement le cas (Dechy & Dien, 2007).

Les apports de l'informatique : Le traitement automatique des langues (TAL)

Les capacités de stockage de l'information ne cessent d'augmenter et les bases de données sont de plus en plus importantes. Au début, le REX ne comportait que des données techniques. Au fil du temps, le volume d'information s'est étoffé, avec notamment des données contextuelles. Du coup, il s'est enrichi de textes non structurés ou semi structurés, dont l'analyse est particulièrement laborieuse du fait de leur nature et de leur volume.

Blatter et Raynal (2014) se sont penchés sur l'apport du Traitement Automatique des Langues (TAL) pour le traitement des bases de données REX. Ils notent que *« le retour d'expérience est considéré comme un processus de signalisation, de stockage et d'analyse des événements (écarts, défaillances, incidents) dans une entreprise, mais également comme un objet textuel qui va, par là-même, être l'objet du TAL »*. L'objectif du TAL est alors de *« mettre en évidence des causes, retrouver des situations similaires, catégoriser des faits »*.

Le TAL peut intervenir à différentes étapes du REX :

- Aide à la rédaction ;
- Catégorisation automatique ;
- Vérification de la cohérence intra-document ;
- Vérification de la cohérence inter-documents ;
- Recherche d'information ;
- Calcul de similarité ;
- Fouille de texte ;
- Clustering ;
- Application de modèles linguistiques pour mettre en évidence des relations spécifiques (causalité, temporalité, subjectivité etc.) ;
- Constitution de ressources langagières, pour améliorer les traitements futurs sur les données textuelles.

Après avoir testé différents outils de TAL sur plusieurs jeux de données issus de REX réels, les auteurs tirent quelques constats d'ordre général sur la relation TAL/REX :

- Les outils sont pertinents, efficaces et performants par rapport à la demande initiale ;
- Ils nécessitent un fort investissement en temps, ceci étant lié aux différentes attentes des organisations en fonction du type de REX à leur disposition ;

- La demande doit être précise ;
- Chaque configuration besoin/outil est particulière et implique des contraintes.

Les acteurs du REX doivent alors être formés au TAL et un réseau pour promouvoir l'utilisation du TAL pour traiter les REX est en formation.

Million-Rousseau et Tassan (2014) ont utilisé le TAL sur un point précis : l'apport du traitement sémantique sur une base de REX. Pour ce faire, la construction d'une ontologie (structuration des concepts d'un domaine) et d'une terminologie de l'organisation constitue une étape préliminaire. Pour l'analyse d'une base de 40 000 descriptions d'accidents ou d'incidents (ARIA), qui comportent une partie en texte libre qui jusque-là n'a pas été traitée, les auteurs s'appuient sur la méthode Os Way d'Ontologos corp qui « *est une méthodologie outillée de construction et de maintenance des référentiels qui exploite les documents de l'organisation et implique les experts* ». Cette méthode de création d'une ontologie comporte plusieurs étapes résumées ci-dessous :

- Générer un lexique de mots et d'expressions couramment utilisées (grâce à la combinaison de catégories grammaticales) ;
- Créer le support de l'ontologie à partir des termes apparaissant plus de deux fois ;
- Enrichir la terminologie en traitant les synonymes.

Par la suite, le logiciel OS Doc se servira de cette terminologie pour classer tout nouvel accident dans l'ontologie, ce qui permettra l'obtention d'une cartographie sémantique. Lors de l'interrogation de la base de données, la requête est analysée du point de vue de l'ontologie afin de pouvoir renvoyer les résultats les plus pertinents. Le couplage de l'analyse sémantique avec d'autres techniques engendre une forte valeur ajoutée. Dans un exemple, les auteurs montrent comment, grâce à l'ontologie, il est possible de trouver une typologie causes/événement/conséquences avec les fréquences associées : les configurations les moins fréquentes peuvent permettre de détecter un signal faible.

Conclusion : d'un REX réactif vers un REX proactif

Le REX est un processus complexe comprenant de nombreuses étapes, dont chacune peut avoir des faiblesses. Il est un pilier de la gestion des risques, et progressivement il tend à devenir de plus en plus proactif, notamment grâce à la traque des signaux faibles, en prenant en compte la complexité des systèmes observés. Alors que des quantités d'informations toujours plus grandes sont stockées dans les bases de données, les progrès des traitements informatiques, et notamment du TAL, permettent d'analyser des documents écrits non structurés et riches de sens, et ce de plus en plus finement. Se passer d'une analyse humaine n'est évidemment pas imaginable mais ces outils pourraient se révéler dans le futur de véritables supports pour les experts.

Les risques majeurs sont des risques à faible probabilité, donc avec une période de retour longue (tous les cents ans). Il convient de ne pas interpréter l'absence d'accidents majeurs ou la faible occurrence d'événements mineurs comme un REX positif. Le partage de REX (entre unités, sites, groupes, industries) est un bon moyen d'améliorer le référentiel de risque en « bénéficiant » de l'apprentissage des événements des « voisins ». Le REX externe est donc un bon levier d'amélioration, pour le moment trop peu usité (Dechy & Dien, 2007). Le secteur nucléaire, qui a été le premier à se rendre compte de l'importance du REX, est aujourd'hui également en avance sur ce type de partage de données REX au travers de WANO (la World Association of Nuclear Operators) ■

Références

- Bès Marie-Pierre (1998) “La capitalisation active des connaissances Principes, contextes et obstacles”, *Gérer et Comprendre*, n° 54 (décembre), pp. 38-51.
- Blatter Christian & Raynal Céline (2014) Méthodes d’analyse textuelle pour l’interprétation des REX humains, organisationnels et techniques, Congrès λμ19 (IMdR) “Décider dans un monde incertain : enjeu majeur de la maîtrise des risques”, Dijon, 21-23 octobre.
- Bourrier Mathilde (1999) *Le nucléaire à l’épreuve de l’organisation*, Paris, Presses Universitaires de France.
- Bulot Mireille & Sfez Michel (2014) Améliorer l’efficacité des analyses d’événements en radiothérapie, Congrès λμ19 (IMdR) “Décider dans un monde incertain : enjeu majeur de la maîtrise des risques”, Dijon, 21-23 octobre.
- Dechy Nicolas & Dien Yves (2007) Les échecs du retour d’expérience dans l’industrie : problème de verticalité et/ou de transversalité, Les entretiens du Risques (IMdR) “Maîtrise des malveillances et conception des systèmes d’information face aux risques”, Paris, 13-14 décembre.
- Dechy Nicolas, Jouniaux Pierre & Hadida David (2014) Détection, pertinence et amplification des signaux faibles dans le traitement du retour d’expérience, Congrès λμ19 (IMdR) “Décider dans un monde incertain : enjeu majeur de la maîtrise des risques”, Dijon, 21-23 octobre.
- Dien Yves (2014) Les signaux faibles à l’aune des lanceurs d’alerte, Congrès λμ19 (IMdR) “Décider dans un monde incertain : enjeu majeur de la maîtrise des risques”, Dijon, 21-23 octobre.
- Dumez Hervé (2012) “Qu’est-ce que l’abduction, et en quoi peut-elle avoir un rapport avec la recherche qualitative ?”, *Le Libellio d’Aegis*, vol. 8, n° 3, pp. 3-9.
- Escande Jean, Le Coze Jean Christophe, & Proust Christophe (2014) Les signaux faibles : dépasser le problème de l’impossible prédictibilité, Congrès λμ19 (IMdR) “Décider dans un monde incertain : enjeu majeur de la maîtrise des risques”, Dijon, 21-23 octobre.
- Million-Rousseau Cécile & Tassan Yannick (2014) Retour d’expérience sur la gestion sémantique de la base ARIA, Congrès λμ19 (IMdR) “Décider dans un monde incertain : enjeu majeur de la maîtrise des risques”, Dijon, 21-23 octobre.
- Périnet Romuald & Garandel Sylvie (2014) Elargir l’horizon des possibles en multipliant les points de vue, Congrès λμ19 (IMdR) “Décider dans un monde incertain : enjeu majeur de la maîtrise des risques”, Dijon, 21-23 octobre.
- Turner Barry A. (1978) *Man-made disasters*, London, Wykeham Publications.
- Vaughan Diane (2001) “La normalisation de la déviance : une approche d’action située” in Bourrier Mathilde [ed] *Organiser la fiabilité*, Paris, L’Harmattan, pp. 201-234.



Sans titre, Serge Poliakoff (1967)