DIRIS : utilisation des diagrammes d'influence (réseaux bayésiens) dans l'analyse des risques pour les installations industrielles

{ R. Farret , J.-C. Le Coze }

Le programme de recherche DIRIS, mené en collaboration avec EDF R&D (Département maîtrise des risques industriels), a pour objectif principal de permettre une analyse de risques dite « transverse » d'un système industriel en incluant son environnement humain et organisationnel, en plus des facteurs techniques, via un « réseau bayésien ». Également appelés « diagrammes d'influence », les réseaux bayésiens sont des outils très intéressants à exploiter dans le cadre de l'analyse des risques, car ils peuvent représenter les relations de dépendance entre différents éléments ainsi que les probabilités associées, le tout via un support graphique. Ils permettent d'élargir la notion « d'arbre des défaillances » et d'estimer la probabilité d'occurrence de différents scénarios d'accidents tout en intégrant la complexité de l'ensemble du système industriel.
L'objet de notre programme de recherche est de prendre en compte des facteurs humains et organisationnels comme la gestion du REX (retour d'expérience), les stratégies de maintenance, la gestion des procédures. Les résultats obtenus sont d'une part la structuration conceptuelle du modèle, d'autre part l'application de l'outil bayésien sur un cas industriel.

Modèle conceptuel

Nous avons proposé un modèle générique structuré en trois niveaux principaux (illustration en figure 1, partie de gauche) :
• le niveau 1 est focalisé sur les éléments techniques, il s'agit d'un premier réseau bayésien élaboré comme un diagramme en forme de « nœud papillon », représentant les scénarios accidentels possibles : un « arbre de défaillances » mène à un Événement redouté central (ERC), qui entraîne à son tour un « arbre d'événements » ;
• au niveau 2, les décisions et actions individuelles, dont l'efficacité produit des effets sur les événements au niveau 1, par exemple l'application d'une procédure d'urgence, ou une action de maintenance, qui auront une influence directe ou indirecte sur le bon fonctionnement d'une barrière de sécurité ;
• au niveau 3, les facteurs managériaux et organisationnels : ceux-ci traitent des processus relatifs à l'organisation, aux moyens qu'elle met en place ou aux contraintes qu'elle génère (exemple : formation, pression de production).

Sur la figure 1, dans la partie droite, au niveau 1 du modèle, les variables ou nœuds figurent les événements que l'on retrouve classiquement dans un nœud papillon : événements initiateurs (telles les défaillances techniques), et résultats des actions dues aux barrières de sécurité.
Au niveau 2, les Facteurs d'Efficacité des Actions Particulières (FEAP) regroupent l'ensemble des déterminants de l'efficacité d'une action humaine (ex : compétence des opérateurs, qualité des outils et aides disponibles, etc.). Ils sont spécifiques du « petit collectif de travail » : une équipe, ou un ensemble d'opérateurs agissant sur un

équipement précis. Ces FEAP sont en phase avec les récents développements au sein d'autres programmes à EDF comme à l'INERIS (MIRIAM/ATOS, référentiel Oméga 20).
Au niveau 3, les facteurs managériaux et organisationnels sont modélisés à l'aide de sept facteurs organisationnels pathogènes (FOP) proposés par EDF [Y. Dien, S. Pierlot], par exemple : la culture organisationnelle de sûreté, ou la pression de production. Ce seront les nœuds amont du réseau bayésien. Chaque FOP est « présent » ou « absent », avec une certaine probabilité de répartition entre ces deux états.
Lors de la déclinaison sous forme de réseau bayésien, le principe de base est la « dégradation » des probabilités au sein du réseau : lorsqu'une variable amont est à l'état négatif (ex. : facteur FOP « pression de production » présent) cela vient dégrader la probabilité de succès de la variable aval (ex. : niveau de formation satisfaisant), donc la probabilité de réussite de l'action sous-jacente (ex. : maintenance d'un capteur). L'INERIS a proposé des « coefficients de dégradation » génériques, en approfondissant le travail de la thèse de Aurélie Léger portant sur ce sujet et sur la formalisation unifiée des connaissances - thèse encadrée par le CRAN, Centre de Recherche en Automatique de Nancy, UMR 7039. Cela correspond au principe habituel de « décote » semi-quantifiée dans les études de dangers, mais en l'adaptant au réseau bayésien ainsi qu'aux actions humaines.

Étude de terrain et modélisation sous réseau bayésien

Une étude de terrain a été menée chez un industriel, en complément d'une étude de sécurité existante, sur un site de fabrication de matières plastiques (événement redouté : atmosphère explosive dans un silo de stockage). Elle a permis de légitimer la démarche en montrant sa faisabilité, de valider le protocole de terrain, et d'assurer le lien entre l'approche générique présentée plus haut et l'approche clinique au « cas par cas ».
Plusieurs séries d'entretiens ont été menées, par binôme regroupant un expert en sciences organisationnelles et un expert en analyse des risques techniques. La figure 2 présente un extrait du modèle.
Le niveau de sécurité sur le site est globalement élevé, cependant le diagnostic organisationnel a décelé *l'absence de réexamen des hypothèses de conception* comme facteur organisationnel pathogène (FOP) possible ; or, cela est en concordance avec un autre constat sur un plan purement tech-

RÉFÉRENCES

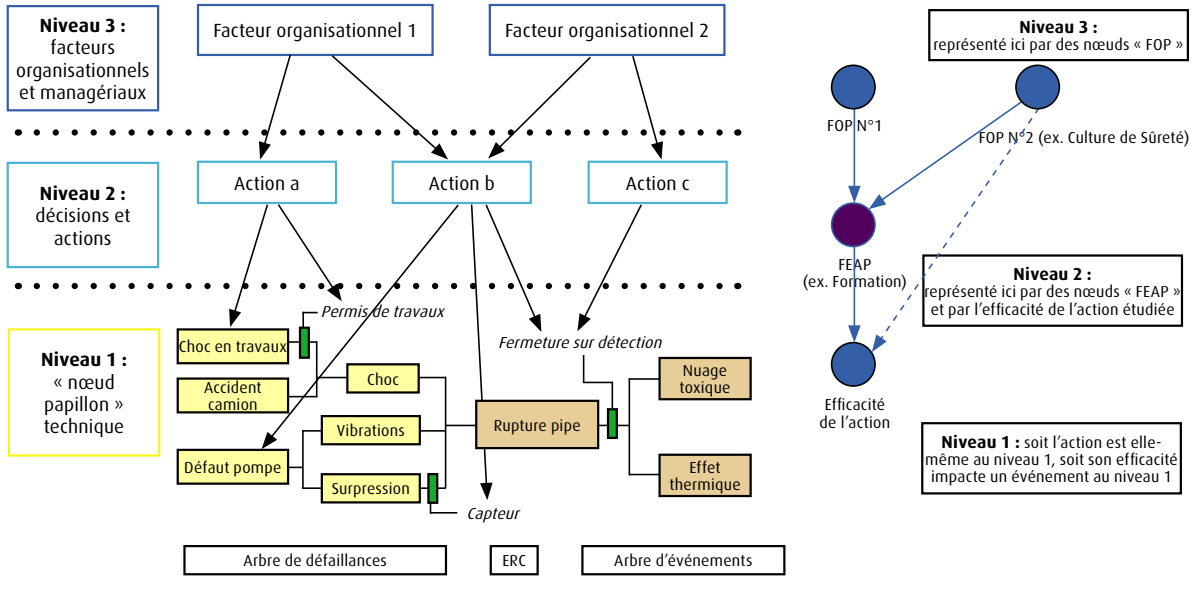
Farret R., Le Coze J-C., Merad M., Léger A., Duval C., 2006. Epistemological perspective of the modelling process of a system with technical and organisational dimensions, SRA Conference, Ljubljana, Slovénie.

Duval C., Léger A., Farret R., Weber Ph., 2007. Méthodologie d'analyse de risques pour les systèmes socio-techniques complexes et application à un cas industriel, Congrès lambda-mu 16 (IMdR).

Duval C., Léger A., Farret R., 2007. Choice of a risk analysis method for complex socio-technical systems. ESREL Conference 2007, Stavanger, Norvège.

Léger A., Levrat E., Weber Ph., Iung B., Duval C., Farret R., 2008. Methodology for a Probabilistic Risk Analysis of Socio-Technical Systems, INSIGHT Vol.11 Issue 3 (revue de l'INCOSE, International Counsil on Systems Engineering).

Léger A., Weber Ph., Levrat E., Duval C., Farret R., Lung B., Methodological developments for probabilistic risk analyses of socio-technical systems, *soumis en novembre 2008 au* Journal of Risk and Reliability *(Proceedings of the Institution of Mechanical Engineers, Part O),* accepté en juin 2009.



Modèle conceptuel en trois niveaux (à gauche) et variables correspondantes dans le réseau bayésien (à droite).
ERC : événement redouté central.
FOP : facteurs d'organisation pathogène.
FEAP : facteurs d'efficacité des actions particulières.

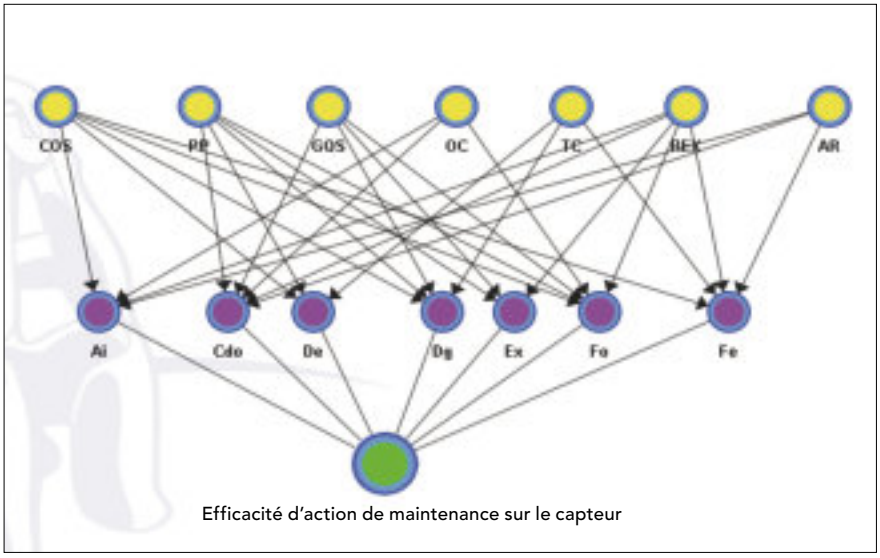
#1

Modèle sous réseau bayésien pour le cas d'un accident sur un silo industriel : zoom sur une action de maintenance et son influence sur une barrière, les facteurs influents (FOP et FEAP) sont en amont, les variables influencées en aval.

FOP : facteurs d'organisation pathogène.
FEAP : facteurs d'efficacité des actions particulières.

Parmi les FOP :
COS : Culture Organisationnelle de Sûreté.
PP : Pression de production.
AR : Absence de Réexamen des hypothèses de conception.
Parmi les FEAP :
Fo : Formation et compétence des opérateurs.
Ai : Qualité des outils et aides disponibles.
Cdo : Contrôle des actions et définition des objectifs.

#2



Efficacité d'action de maintenance sur le capteur

nique : la fiabilité de la barrière basée sur le capteur d'oxygène pourrait être augmentée, car bien que la redondance de la fonction de détection soit très bien assurée, la redondance du traitement des informations ne l'est pas. Enfin, en montrant en termes probabilistes l'influence des FOP, le modèle a montré les facteurs sur lesquels l'industriel peut agir, tel le besoin de maintenir le contrôle des actions par un tiers (service HSE).

Signalons enfin que l'étape « d'approbation » par l'industriel est importante avant de passer à l'étape de quantification. Une validation par rapport à la réalité serait ici impossible puisqu'on étudie des événements rares. Mais il s'agit de s'assurer que le système est bien compris et que le modèle est jugé adapté à l'objectif recherché.

ABSTRACT

Any industrial system is constrained by regular human interventions conditioned by organizational decisions, which must be taken into account by the risk analysis. The research led in the DIRIS project aims at developing a methodology, a tool and a «risk model» that can be adapted to case studies. Our work considers a probabilistic frame and focuses on the modeling of safety barriers, that are key elements including human and organizational influences. The «bayesian network» was chosen, because it combines the calculation of probabilities with event trees represented in a graphic manner. It integrates all the probabilistic links within the network, and deterministic links can be introduced. We defined a generic «risk model» composed of three levels: a technical level, a level of human actions, and an organizational level. The last one is represented through 7 «pathogenic organizational factors» (POFs), such as «weakness of control» or «production pressure». This model is then applied to a real industrial site, with the study of the explosion of a vessel. The probabilistic links between the variables are modified by quantitative degradation coefficients that take into account upstream influences. This industrial application offered the opportunity to develop bayesian networks as replicable tools, and proved the feasibility of the whole method.