



Ateliers de la SATW de la plate-forme thématique «Risque»

## Gestion du risque – Anciens et nouveaux défis

La **notion de risque** continue de faire l'objet d'une interprétation plus ou moins large, en fonction de la communauté, soit en la limitant aux conséquences d'événements indésirables, c'est-à-dire en se limitant au risque, soit en y incluant les aspects positifs et les chances. Il n'existe pas de définition universelle; les éléments essentiels du risque, en particulier la «probabilité» et sa conjonction avec d'autres éléments se heurtent souvent à l'incompréhension. Les incertitudes résiduelles qui peuvent résulter du manque de connaissances ou du caractère fortuit inhérent à l'événement – pensons par exemple à un tremblement de terre – nous laissent souvent perplexes, tout comme la gestion du **risque résiduel**. Le simple **concept de risque**, avec la relation multiplicative de sa fréquence et de ses conséquences, est souvent considéré comme inadéquat dans le cas d'événements induisant un préjudice extrême malgré la rareté qui les caractérise – comme c'est souvent le cas dans le domaine nucléaire.

Par ailleurs, étant donné l'intégration croissante et les interdépendances dans le domaine d'infrastructures vitales, un **«système de systèmes»** complexe a vu le jour. Dans son fonctionnement, ce dernier dépend fortement de l'environnement opératoire et organisationnel et présente des modèles de perturbation, y compris des effets de cascade, que nous comprenons pour le moment difficilement et que nous pouvons moins encore prévoir. Les méthodes classiques quasi statiques comme les arbres de défaillance et d'événements ne suffisent pas à cet effet. Dans de nombreux domaines, les **événements extrêmes** se produisent plus souvent et se déroulent autrement que prévu: ils se situent en dehors des fonctions de distribution courantes. Certains les considèrent, même en présence de ce que l'on appelle des «heavy tails», comme des valeurs aberrantes émergentes; pour d'autres, ils ne sont absolument pas prévisibles, en d'autres termes il s'agit de ce que l'on appelle des «cygnes noirs».

La «résilience» s'impose comme un **nouveau paradigme** qui étend le concept de risque orienté jusqu'à présent sur l'augmentation de la capacité de résistance à la restauration de la fonctionnalité en passant par le comportement d'un système après des événements perturbateurs. La **gestion du risque** devrait par exemple être intégrée géographiquement, être développée dans le sens d'une **«gouvernance»** en cas de problématiques d'une portée considérable et impliquer les acteurs principaux en cas d'incertitudes et d'ambiguïtés importantes.

Un atelier a été organisé en novembre 2013 abordant ces défis, tantôt anciens, tantôt nouveaux, et des possibilités avancées. Ce document de réflexion a pour but de résumer une sélection de contributions et de les communiquer aux personnes intéressées.

Des versions plus complètes des différentes contributions peuvent être téléchargées (en anglais) en format PDF sur le site Internet [www.satw.ch/risiko](http://www.satw.ch/risiko).

## Modules de risque, méthodes traditionnelles d'analyse de risque

Wolfgang Kröger, ETH Zurich

Différentes sources d'**incertitudes** jouent un rôle important dans l'évaluation du risque. Généralement, les **éléments du risque**, c'est-à-dire la fréquence et les conséquences d'un événement indésirable sont multipliés et, s'il y a plusieurs événements, les résultats obtenus sont ensuite additionnés.

Le **risque résiduel** est utilisé soit comme une notion descriptive et résume le risque subsistant après la mise en œuvre de toutes les mesures de sécurité prévues ou soit comme une notion normative afin de désigner le risque admissible après l'évaluation postulée de l'acceptation.

Le **risque systémique** inscrit les risques dans un contexte plus large de conséquences sociales, financières et économiques et d'interdépendances plus étroites. La notion de **sécurité** peut faire l'objet d'une définition absolue (absence de danger), relative (risque relativement faible ou acceptable, gestion des exigences normatives) ou être considérée comme sécurité perçue.

De préférence, les estimations des risques devraient se baser sur des données disponibles, utilisables directement, et des expériences d'événements similaires. Souvent, la base d'une telle **évaluation statistique du risque** n'est pas établie et il faut utiliser des modèles prévisionnels d'événements et de scénarios de défaillance rares, encore jamais observés, qui utilisent les données empiriques existantes au niveau des composants.

En partant de l'hypothèse que les événements, ainsi que leur probabilité d'occurrence, peuvent être identifiés préalablement, la méthodologie globale et systématique de l'analyse de sécurité probabiliste (ASP) a été développée et utilisée principalement pour les centrales nucléaires. Les **évaluations prévisionnelles des risques** en résultant ont été utilisées comme plate-forme spécifique aux installations pour l'échange de questions en matière de sécurité. Il existe trois niveaux superposés d'ASP. En Suisse, comme dans de nombreux pays, les niveaux 1 (détermination de la fréquence de fusion du cœur) et 2 (détermination de la fréquence d'un dégagement important de substances radioactives) sont utilisés pour contrôler si les mesures de sécurité prises sont suffisamment fiables et équilibrées et si les valeurs-cibles en matière de sécurité sont respectées. Ils ne sont pas destinés à la détermination de risques sociétaux effectifs qui résultent de l'exploitation de centrales nucléaires. À cet effet, des méthodes et approches traditionnelles devraient être étendues et les lacunes affectant les connaissances devraient être comblées.

---

# Résilience et gestion intégrative du risque

---

Hans R. Heinimann, ETH Zurich

---

Les associations croissantes et la diminution de l'hétérogénéité à l'intérieur et entre les systèmes socio-techniques ont conduit à des modèles comportementaux d'un nouveau genre qui nécessitent de nouvelles approches de l'évaluation du risque. Deux concepts émergents ont été proposés, leur application promettant une meilleure gestion des perturbations dans un «système de systèmes».

**La gestion intégrative du risque (IRM)** est un concept qui vise à maintenir simultanément un portefeuille de risques naturels, techniques, économiques et sociaux pour une région géographique déterminée. En aspirant à une réduction des risques, il recherche un équilibre optimal entre les coûts et les profits, en initiant une série d'actions de co-acteurs publics et privés et en franchissant à cette occasion les limites traditionnelles des disciplines et communautés impliquées. L'IRM exige des efforts com-

muns et une nouvelle conscience, et doit réunir différentes disciplines de l'ingénierie, de l'économie et des sciences sociales.

Au cours des 10 dernières années, le **concept dit de résilience** a pris beaucoup d'importance et s'est imposé dans le domaine des systèmes techniques. La résilience se définit comme la «faculté d'un système d'absorber les perturbations (chocs) et de se réorganiser/reconfigurer afin de retrouver en substance sa structure et sa fonctionnalité d'origine». C'est donc un nouveau paradigme par opposition à l'approche classique de l'ingénieur qui vise à augmenter la capacité de résistance d'un système par son «durcissement».

---

# Rois dragons: appréhender la nature des événements extrêmes

---

Spencer Wheatley et Didier Sornette, ETH Zurich

---

Les événements extrêmes dominent la qualité durable et l'organisation des principaux systèmes naturels et sociaux: les deux plus grands accidents de centrale nucléaire ont occasionné cinq fois plus de dommages et les cinq plus grandes épidémies depuis 1900 ont fait 20 fois plus de morts que tous les autres accidents historiques du même type considérés conjointement. Les distributions statistiques correspondantes se caractérisent par des «queues» marquées (heavy tails); les pires événements constituent des résultats aberrants.

Ce rapport évoque un type particulier d'événements extrêmes: ce que l'on appelle les **rois dragons**. Cette double métaphore désigne un événement qui – par opposition à d'autres événements du même système – est extrême par son ampleur et son action (un «roi») et est produit à partir d'un processus unique en son genre

(un «dragon»). Dans un large spectre de systèmes physiques, de nombreux événements extrêmes sont prévisibles jusqu'à un certain degré à condition que l'on puisse développer et représenter une compréhension suffisamment profonde de la structure et de la dynamique du système cible et que l'on puisse également la contrôler. C'est en cela que la théorie des rois dragons se distingue fondamentalement de ce que l'on appelle les «cygnes noirs» qui sont considérés comme imprévisibles. De nombreux événements tels que la crise financière de 2008 ou le tremblement de terre de 2011 au Japon sont à première vue des «cygnes noirs»; cependant, une analyse plus précise révèle qu'il s'agit d'exemples typiques de rois dragons.

---

# Compréhension de systèmes socio-techniques complexes

---

Giovanni Sansavini, ETH Zurich

---

Des intégrations de système et des changements de stratégie ainsi que des investissements insuffisants au cours des dernières années ont eu pour effet que des réseaux étendus de haute technicité dépendent de plus en plus les uns des autres et sont exploités aux limites de leurs capacités. «L'homme», à la fois exploitant et utilisateur, en augmente de ce fait globalement la complexité. Un exemple typique d'un tel réseau est le système de distribution d'électricité. Les «systèmes de systèmes» obtenus tendent vers des comportements imprévisibles avec des effets de cascade et des conséquences considérables dont la compréhension et la caractérisation sont déterminantes de l'analyse approfondie de leur fiabilité et de leur vulnérabilité.

Afin d'apprécier les conséquences d'événements perturbateurs de gravité variable, il convient de faire appel à des modèles et simulations qui vont au-delà des approches standard actuelles en exploitant des observations généralement peu empiriques. La **Théorie du réseau complexe (CNT)**, entre-temps omniprésente pour la recherche de propriétés structurales/topologiques de systèmes socio-techniques complexes, a également été utilisée pour le réseau suisse de distribution d'électricité. Il a conduit à une série de résultats et de conclusions surprenants sur le plan de l'extension de l'effet de cascade. Par exemple, des effets de cascade considérables peuvent se briser lorsque les systèmes opèrent dans des conditions de stress et à la limite des marges de sécurité. Dans ce cas, un degré d'interconnexion inférieur a d'abord un effet positif mais, lorsque la charge critique est atteinte, la cascade de défaillances s'étend par à-coups et ne peut plus être modérée que difficilement. Inversement, les réseaux au maillage très dense sont certes plus vulnérables à une extension en cascade mais la charge critique est plus élevée.

---

# Le concept de «Risk Governance»

---

Ortwin Renn, Université de Stuttgart

---

La notion de «Risk Governance» se rapporte à la manière différente dont plusieurs acteurs, personnes individuelles et institutions, publiques et privées, gèrent ou devraient gérer la complexité et l'ambivalence des risques dans un environnement d'incertitude. L'un des concepts correspondants a été développé par l'International Risk Governance Council (IRGC). Ce cadre adaptatif promet un soutien sous forme de fil conducteur lors de l'élaboration de stratégies globales pour l'évaluation et la gestion des risques; il intègre des aspects scientifiques, économiques, sociaux et culturels et prévoit des phases imbriquées, ayant pour mission centrale une communication efficace.

Le concept de «Risk Governance» est, d'une part, utilisé dans un sens descriptif de la façon dont les décisions sont prises et, d'autre part, dans un sens normatif afin d'améliorer les structures et processus pour les décisions politiques. La «Risk Governance» attire l'attention sur le fait que de nombreux risques, en particulier pour de grands systèmes techniques, ne sont pas simples à gérer. Une simple opération multiplicative de la fréquence et des conséquences des événements indésirables ne suffit pas. De nombreux risques font l'objet de considérations complexes des coûts et profits qui doivent être dûment intégrés pour des décisions socialement pertinentes en impliquant les principaux acteurs.

---

# Perspectives

À l'avenir, et peut-être dans une mesure croissante, nous nous verrons également confrontés à des développements et interrogations qui représentent pour la société des risques réellement importants auxquels il ne sera cependant plus possible de faire face et de répondre par les méthodes et procédures éprouvées compte tenu des risques possibles. Ces développements et problématiques comprennent, d'une part, l'intégration de systèmes ainsi que la commande par des systèmes d'information et de communication numérique jusqu'à l'«Internet of Everything» et la mobilité autonome et, d'autre part, les systèmes de distribution d'énergie ou des concepts de circulation et de construction «intelligents et tournés vers l'avenir».

Étant donné la complexité de la conception du système et de ses attributions qui en découle généralement, nos aptitudes de compréhension, de simulation et d'évaluation préalables trouvent leurs limites. De nouvelles méthodes et approches s'avèrent nécessaires.

Des suggestions riches en perspectives cohabitent avec des doutes persistants quant à nos chances d'y parvenir. Les contributions des auteurs montrent des approches qui peuvent éventuellement aboutir à des méthodes viables.

La voie la plus prometteuse pour une conception plus robuste et plus résiliente de nos systèmes et processus passe souvent par leur simplification, notamment par le biais du découplage et de la décentralisation, par exemple dans le domaine de la distribution d'électricité. L'avenir montrera à quel point cette approche est possible, faisable et souhaitée.

Il faut prêter une attention de rigueur aux nouveaux risques, surtout induits par la cybercriminalité, car notre faculté de nous représenter les dangers qui peuvent émaner de manipulations malveillantes des systèmes est encore limitée.

Des efforts constants s'imposent pour savoir comment parvenir à une «bonne» gestion des risques. Pour les risques élevés d'une importance sociale qui se caractérisent par des incertitudes et ambiguïtés élevées, l'application du concept de «Risk-Governance» mérite certainement d'être essayée. La réponse à l'«éternelle» question de savoir «How safe is safe enough?» et, en particulier, jusqu'à quel niveau les dommages sont tolérables, doit finalement décider la société et la convaincre qu'il n'existe pas de «risque zéro». La science peut tout au plus fournir la base d'évaluation.

Auteurs: Wolfgang Kröger (ETH Zurich) et autres (voir pages suivantes)  
© SATW | décembre 2016

Exemple d'un événement extrême: une grande partie de La Nouvelle-Orléans se trouve sous les eaux après le passage de l'ouragan Katrina. Les dégâts causés par l'ouragan se sont élevés à plus de 100 milliards de dollars US.

Source: AP Photo/U.S. Coast Guard, Petty Officer 2nd Class Kyle Niemi (29.8.2005)

**satw** it's all about  
technology

Académie suisse des sciences techniques SATW  
Gerbergasse 5 | 8001 Zurich | 044 226 50 11 | info@satw.ch | www.satw.ch

