LA RESILIENCE DES SYSTEMES : HISTORIQUE ET CADRAGE CONCEPTUEL

Gaël Morel
Maître de Conférences, Université de Bretagne Sud, Laboratoire CRPCC (EA 1285), équipe LECTIC, centre de recherche, rue saint Maudé, 56321 LORIENT, France
gmorel@univ-ubs.fr

Christine Chauvin
Maître de Conférences (HDR), Université de Bretagne Sud, Laboratoire CRPCC (EA 1285), équipe LECTIC, centre de recherche, rue saint Maudé, 56321 LORIENT, France
cchauvin@univ-ubs.fr

Résumé

Depuis les années 1930, plusieurs grandes périodes de sécurisation se sont succédées: 1. fiabilité technique ; 2. fiabilité humaine ; 3. erreurs humaines ; 4. approches systémiques. Ces dernières années, la communauté de chercheurs regroupée autour d'Hollnagel & Woods s'emploie à construire les bases d'une nouvelle approche en matière de sécurité des systèmes complexes : l'ingénierie de la résilience. Ainsi, le concept de résilience est devenu un axe de recherche important en matière de sécurité des systèmes complexes. Nombreux sont ceux qui voient la résilience comme un moyen pour atteindre l'ultra sécurisation des systèmes sociotechniques complexes. Cette communication traite par conséquent de l'articulation entre les concepts de sécurité et de résilience, autour d'un exemple d'application : le système sociotechnique des pêches maritimes.

Mots-clés: résilience, sécurité, performance, prise de décisions.

Introduction

La résilience trouve son origine première dans les sciences physiques et représente « le degré de résistance aux chocs des matériaux[1] » ou plus encore « l'aptitude d'un corps à résister aux pressions et à reprendre sa structure initiale après une déformation[2] ». Cette définition introduit d'une manière implicite la notion d'élasticité - propriété intrinsèque des matériaux autorisant la déformation et le retour à un état initial stable après un choc. Le dictionnaire anglo-saxon étend le sens de la résilience à « la capacité de recouvrer un état de santé habituel après avoir été malade » ou encore « la qualité de quelqu'un qui ne se laisse pas abattre ». En repartant de l'étymologie latine : « salire » (sauter, rebondir), le préfixe *re* indiquant la répétition, résilier c'est rebondir, aller de l'avant après une maladie (Tomkiewicz, 2000). Le terme de résilience est très certainement ancien puisque Confucius en son temps affirmait déjà que « la plus grande gloire n'est pas de ne jamais tomber, mais de se relever à chaque chute ». Des siècles plus tard, on retrouve cette même vision chez Nietzsche qui estimait que « ce qui ne tue pas rend plus fort ».

Depuis quelques années, la résilience tend à s'élargir au domaine de la gestion des risques via l'émergence du courant de l'ingénierie de la résilience impulsé par Hollnagel, Woods et Leveson (2006). Cette communication traite de cette nouvelle approche et plus particulièrement de

[1] Source : dictionnaire Larousse.
[2] Source : dictionnaire anglo-saxon Longman.

l'articulation entre les concepts de sécurité et de résilience. Elle s'appuie sur des travaux empiriques ayant porté sur le système sociotechnique des pêches maritimes (Morel, Amalberti & Chauvin, 2008, 2009) et comporte trois parties : 1. présentation de l'ancrage théorique en lien avec le courant de l'ingénierie de la résilience ; 2. articulation conceptuelle entre sécurité et résilience ; 3. discussion autour des apports de la résilience et des voies possibles de sécurisation des systèmes sociotechniques complexes.

Cadre théorique

Cette contribution s'inscrit dans le cadre théorique de l'ingénierie de la résilience (Hollnagel, Woods & Leveson, 2006). Nous traiterons dans un premier temps de l'émergence du concept de résilience. Dans un second temps, nous présenterons les différentes définitions relatives à ce concept central.

Emergence du concept de résilience

Les premiers efforts en matière de sécurité ont porté sur le développement de méthodes et outils visant à fiabiliser les composants techniques des systèmes. Leur mise en œuvre s'est traduite par une diminution très nette des accidents attribués aux défaillances techniques.

Entre 1960 et 1980, un certain nombre d'accidents industriels majeurs ont très clairement fait apparaître que l'opérateur humain constituait un facteur « d'infiabilité ». Le besoin de fiabiliser la composante humaine s'est alors imposé comme une évidence, même s'il était déjà communément admis depuis des décennies que l'homme, de par sa nature adaptative, était capable de contourner les dispositifs de sécurité, même les plus avancés (Reason, 1993). À partir des principes quantitatifs issus de la sûreté de fonctionnement, un certain nombre de méthodes de fiabilité humaine ont été élaborées, dont la plus célèbre : THERP - Technique for Human Reliability Analysis - (Swain, 1964). Cependant, d'autres accidents majeurs comme Three Miles Island (1979) ont fait prendre conscience des limites de ces méthodes de quantification des erreurs et de la nécessité de développer de nouveaux cadres de description visant à mieux appréhender la composante humaine dans sa dimension cognitive. La psychologie ergonomique a été en mesure de les apporter, notamment grâce aux travaux ayant porté sur la modélisation du fonctionnement cognitif des opérateurs (Rasmussen, 1983, 1986 ; etc…) et ceux ayant porté sur l'erreur humaine (Leplat, 1985 ; Reason, 1988 ; etc…).

Rapidement, l'objectif d'évitement total de l'erreur a été abandonné (irréaliste d'un simple point de vue théorique) et la sécurité s'est naturellement déplacée vers une perspective plus systémique (Reason, 1997 ; Rasmussen, 1997). En effet, la série d'accidents majeurs survenus entre 1985 et 1990 (Bhopal, 1984 ; Tchernobyl, 1986,…) au sein d'un éventail de technologies pourtant bien défendues, ont révélé que les causes de ces accidents pouvaient se situer au niveau des sphères managériales et organisationnelles des systèmes complexes et non pas uniquement au niveau où le travail est réalisé par les opérateurs. Ce constat a d'ailleurs été source de nombreux travaux dans le domaine de la sociologie (Turner, 1978 ; Vaughan, 1996 ; Weick, 2001, etc…).

En parallèle des approches systémiques, Hollnagel et Woods (1983) ont mis l'accent sur les conditions d'un meilleur couplage homme - machine, qui ferait considérer le risque lié aux systèmes plus par leur dynamique d'interaction que par les risques de défaillances des composantes isolées de ce système, machine d'un côté et homme de l'autre. À partir des années 1990, une importante communauté de chercheurs en psychologie ergonomique s'est inscrite dans cette mouvance, avec trois caractéristiques fortes : 1. un intérêt pour les situations dynamiques complexes ; 2. pour les études de terrain et les arbitrages de sécurité réellement opérés par les opérateurs (sécurité

écologique : Amalberti, 2001 ; Hoc & Amalberti, 2007 ; prise de décision en situation naturelle : Klein & al., 1993) ; 3. un intérêt pour limiter les pièges ou surprises des opérateurs provoquées par une automatisation mal conçue (Billings, 1997 ; Woods & al., 1994).

La multiplication récente d'accidents et de catastrophes (crashs aériens, catastrophes naturelles, etc…) a conduit cette même communauté de chercheurs à réfléchir à une autre approche de la sécurité des systèmes complexes articulée autour du concept de résilience : capacité d'une organisation à conserver ou à recouvrer rapidement un état stable, lui permettant de poursuivre ses activités durant et après un accident majeur ou bien en présence de pressions continues et importantes (Wreathall, 2006). Finalement, l'émergence du concept de résilience est la suite logique des travaux décrits précédemment.

Aujourd'hui, nombreux sont ceux qui voient la résilience comme un moyen pour atteindre l'ultra sécurisation des systèmes complexes. Nous verrons par la suite que cette hypothèse pose de nombreuses questions.

Définitions du concept de résilience

Le concept de résilience est très largement utilisé dans de nombreuses disciplines : la psychologie clinique, l'écologie, la physique, l'économie, etc. Dans le cadre de cette communication, nous nous intéressons aux définitions majeures produites au sein du courant de l'ingénierie de la résilience. Ainsi, il se dégage deux grandes classes de définitions. La première considère la résilience comme une aptitude à gérer les perturbations. Il s'agit de la capacité d'anticiper (prévenir la survenue d'une perturbation), de percevoir (empêcher l'aggravation des effets de la survenue de la perturbation) et de répondre (récupérer, survivre après la survenue de la perturbation) (Hollnagel & Woods, 2006). De nombreux accidents et/ou catastrophes récents ont révélé un manque crucial de résilience sur ces trois points. Ceci a eu pour effet de conduit à la perte de contrôle des activités au sein de ces systèmes. Un système dit résilient doit par conséquent avoir la capacité de s'adapter pour faire face aux perturbations imprévues et déstabilisantes de manière à ne pas perdre le contrôle de ses opérations. La deuxième classe de définitions est centrée sur le management des conflits entre les objectifs de performance[3] et de sécurité. Il s'agit de la capacité d'une organisation à manager de lourdes pressions et des conflits entre la sécurité et la production (Flin, 2006 ; Hale & Heijer, 2006). Cette dernière classe de définitions est intéressante dans la mesure où elle pose clairement la question de l'articulation entre deux concepts majeurs que sont la sécurité d'un côté et la résilience de l'autre. Nous proposons dans la partie suivante de discuter de cette articulation autour d'un domaine d'application : le système sociotechnique des pêches maritimes.

Articulation entre sécurité et résilience

Le concept de résilience fait l'objet de fortes préoccupations. Nombreux sont ceux qui voient en la résilience une possibilité nouvelle permettant d'améliorer les niveaux de sécurité des systèmes sociotechniques complexes. Cet espoir est compréhensible dans la mesure où les efforts en matière de sécurisation des systèmes sont continus et nécessitent l'apport de nouvelles théories et modèles. Cependant, deux articles de recherche récents (Morel, Amalberti & Chauvin, 2008, 2009) ont posé très clairement la problématique de l'articulation entre sécurité et résilience au travers de l'étude du système sociotechnique des pêches maritimes. Il a été montré que la résilience constituait une forme bien précise de sécurité reposant sur les savoirs faire, la compétence et l'autonomie des acteurs des systèmes sociotechniques complexes. L'étude du système des pêches maritimes (un modèle artisan) a démontré que la résilience constituait une propriété native des systèmes de base qui restent très

[3] Fortement en lien avec les capacités de production

peu encadrés par de la sécurité dite prescriptive. Ainsi, la résilience constitue une forme de sécurité dite gérée (Sg) qui, associée à la sécurité dite prescriptive (procédures de sécurité, réglementations, normes, règles, etc.) complète l'équation de la sécurité observée au sein des systèmes (i.e. la sécurité que l'on peut mesurer par des données objectives comme le nombre d'accidents du travail, de maladies professionnelles, etc.) : .*SécuritéObservée = [Sc + Sg]*.

Ces études ont montré que le système des pêches maritimes est très résilient[4] mais également peu sûr ; la sécurité prescriptive est par ailleurs très peu développée, ce qui peut paraître paradoxal dans la mesure où ce système est également très fortement encadré. Le point important dans ce constat est le suivant : un système résilient n'est pas un système sûr. Ceci va poser un certain nombre de questions de fond qui seront développées dans la discussion à venir.

Discussion

D'un point de vue historique, la sécurisation des systèmes sociotechniques complexes a toujours été réalisée en favorisant la sécurité prescriptive. Cela a eu pour effet de réduire considérablement la composante adaptative de ces mêmes systèmes (résilience, i.e. sécurité gérée) les rendant ainsi extrêmement rigides et par conséquent très peu adaptables à la survenue de perturbations importantes. Les réponses à ces dernières sont très souvent inadaptées ce qui engendre très souvent une perte de contrôle des opérations (à l'origine de nombreuses catastrophes et accidents majeurs qui ont nécessairement des conséquences su point de vue de la santé et sécurité des acteurs de ces systèmes). Par ailleurs, il n'est pas possible de parler de sécurisation des systèmes sans traiter de la question de la limitation des niveaux de performance de ces derniers. En effet, en sécurisant un système sociotechnique complexe il est très difficile de ne pas abaisser les niveaux de performance. Les conflits entre les objectifs de performance d'une part, et les objectifs de sécurité d'autre part, conduisent très souvent à des arbitrages qui s'opèrent au profit de la performance, donc au détriment de la sécurité (très souvent pour faire face à la compétitivité et l'agressivité des marchés). Idéalement, il faudrait trouver de nouveaux moyens de sécurisation qui permettent à la fois d'augmenter la performance des systèmes et leurs niveaux de sécurité.

Une des deux études précitées (Morel, Amalberti & Chauvin, 2009) présente plus largement cette problématique au travers d'une discussion centrée sur les différentes formes de sécurisation des systèmes. Ils défendent l'idée selon laquelle les actions de résilience dans les systèmes pourraient permettre d'augmenter les niveaux de sécurité sans contraindre systématiquement les objectifs de performance à la baisse. Introduire de la résilience dans les systèmes consisterait par conséquent : 1. à redonner de l'autonomie aux opérateurs ; 2. à développer les savoirs faire dans des situations déstabilisantes (par le biais de scénarii d'anticipation, d'actions en simulateur, de partage de compétences avec des experts, etc.) ; 3. à développer les aptitudes décisionnelles dans des situations de conflits entre les objectifs de performance et de sécurité. Bien évidemment, nous devons nous interroger sur la réelle capacité des systèmes déjà ultra sûrs (et sécurisés par la prescription) à assumer un tel changement. Le retour en arrière est-il encore possible, sachant que tout a été mis en œuvre pour limiter, voire faire disparaître la résilience au sein de ces systèmes ? D'un point de vue théorique, il manque des études visant à démontrer que toute augmentation du niveau de résilience (sécurité gérée) n'induit pas automatiquement une baisse du niveau de sécurité prescriptive (et inversement). Si tel était le cas, les gains concernant le niveau de sécurité observée (Sobs = Sc + Sg) seraient marginaux voire nuls.

Concernant les systèmes artisans (très résilients, très performants et très peu sûrs), la problématique de sécurisation est différente. Pour garder le bénéfice de cette propriété adaptative portée par la

[4] i.e. très adaptable dans des situations extrêmes. Les décisions prises s'opèrent toujours au profit de la performance économique et au détriment de la sécurité.

résilience, d'autres formes de sécurisation doivent être envisagées (et qui peuvent également l'être dans des systèmes sûrs, voire ultra sûrs) pour ne pas systématiquement avoir recours à de la sécurisation prescriptive. Actuellement, de nombreuses réflexions sont conduites autour du développement de la culture de sécurité et des systèmes de managements intégrés Qualité-Sécurité-Environnement. Les travaux de recherche futurs devront explorer ces pistes de manière à répondre aux nombreuses interrogations qui restent en suspend.

Bibliographie

Amalberti, R. (2001). The paradoxes of almost totally safe transportation systems. *Safety Science*, 37 : 109-126.

Billings, C. (1997). *Aviation automation: the search for a Human-centred approach*. Mahwah, Lawrence Erlbaum associates, Mahwah, New Jersey.

Flin, R. (2006). Erosion of Managerial Resilience : Vasa to NASA. In E. Hollnagel, D.D. Woods & N. Leveson (Eds.), *Resilience Engineering: concepts and precepts*. Ashgate publishing, Aldershot, UK, 208-219.

Hale, A., & Heijer, T. (2006). Defining resilience. In E. Hollnagel, D.D. Woods & N. Leveson (Eds.), *Resilience Engineering : concepts and precepts*. Ashgate publishing, Aldershot, UK, 31-36.

Hoc, J.M., & Amalberti, R. (2007). Cognitive control dynamics for reaching a satisficing performance in complex dynamic situations. *Journal of cognitive engineering and decision making*, 1 : 22-55.

Hollnagel, E., & Woods, D.D. (2006). Epilogue: Resilience Engineering Precepts. In E. Hollnagel, D.D. Woods & N. Leveson (Eds.), *Resilience Engineering : concepts and precepts*. Ashgate publishing, Aldershot, UK, 326-337.

Hollnagel, E., Woods, D.D, & Leveson, N. (2006). *Resilience Engineering: concepts and precepts.* Aldershot, UK: Ashgate publishing.

Hollnagel, E., & Woods, D.D. (1983). Cognitive system engineering: new wine in new bottles. *International Journal of Man-Machine Studies*, 18 : 583-600.

Klein, G., Orasanu, J., Calderwood, R., & Zsambok, C.E. (1993). *Decision Making in Action: Models and Methods*. Norwood, NJ: Ablex Publishing Co.

Leplat J (1985). *Erreur humaine, fiabilité humaine dans le travail.* A. Colin, Paris.

Morel, G., Amalberti, R., Chauvin, C. (2009). How good micro/macro ergonomics may improve resilience, but not necessarily safety. *Safety Science*, 47 (2*)* : 285-294.

Morel, G., Amalberti, R., Chauvin, C. (2008). Articulating the differences between safety and resilience: The decision-making process of professional sea fishing skippers. *Human Factors*, 50: 1-16.

Perrow, C. (1984). *Normal accidents: living with high risk technologies*. Basic Books Inc, New York.

Reason, J. (1993). New approaches to organisational safety. In B. Wilpert, T. Qvale (Eds.), *Reliability and safety in hazardous work systems*. Lawrence Erlbaum Associates, Hillsdale, NJ, England, 7-22.

Rasmussen, J. (1997). Risk management in a dynamic society, a modelling problem. *Safety Science*, 27 : 183-214.

Rasmussen, J. (1986). *Information Processing and Human-machine Interaction.* Elsevier, Amsterdam, North Holland.

Rasmussen, J. (1983). Skills, Rules and Knowledge : signals, signs and symbols and other distinctions in human performance models. *IEEE Transactions : Systems, Man & Cybernetics*, 13 : 257-267.

Reason, J. (1997). *Managing the risks of organisational accidents*. Ashgate, Aldershot, UK.

Reason, J. (1988). Modelling the Basic Error Tendencies of Human Operators. *Reliability Engineering and System Safety*, 22 : 137-153.

Swain, A.D. (1964). *THERP*. Sandia Lab., Albuquerque, New-Mexico, Report SC.R.64.1338.

Tomkiewicz, S. (2000). La résilience. *Actualités et Dossiers en Santé Publique*, 31 : 60-62.

Turner, B.A. (1978). *Man-made disasters*. Wykeham Publications, London, England.

Vaughan, D. (1996). *The challenger launch decision*. Univ. Chicago Press, Chicago.

Weick, K. (2001). *Making Sense of the organization.* BlackWell Publishing, Massachusetts.

Woods, D. D., Johannsen, L., Cook, M., & Sarter, N. (Ed.). (1994), *Behing Human Error*. Dayton OHIO : WPAFB, CERSIAC SOAR 94-01.

Wreathall, J. (2006). Properties of resilient organizations: an initial view. In E. Hollnagel, D.D. Woods & N. Leveson (Eds.), *Resilience Engineering: concepts and precepts* (pp. 258-268). Aldershot, UK: Ashgate publishing.