# DE LA SURETE DE FONCTIONNEMENT A LA RESILIENCE DES SYSTEMES
# FROM DEPENDABILITY & SAFETY TO SYSTEMS RESILIENCE


Jean-François GAJEWSKI

ASTRIUM
31 Avenue des Cosmonautes
31402 Toulouse
Tél. 05 62 19 66 27
jean-francois.gajewski@astrium.eads.net

Christine BEZARD

AIRBUS France
316 rte de Bayonne 31060 Toulouse
Tél. 05 61 18 76 42
christine.bezard@airbus.com

André Cabarbaye

CNES / CAB INNOVATION
18, avenue Edouard Belin - 31401 Toulouse /
3 rue de la Coquille – 31500 Toulouse
Tél. 05 61 54 68 08
andre.cabarbaye@cnes.fr /
andre.cabarbaye@cabinnovation.fr

Outre les auteurs mentionnés, cette communication est présentée par l'ensemble des membres du Groupe de Travail «Résilience des Systèmes » de l'Association Française d'Ingénierie Système (AFIS).



## Résumé

Emanant du groupe de travail « Résilience des Systèmes » de l'Association Française d'Ingénierie Système (AFIS), cette communication tente de préciser le concept de résilience, en émergence dans le domaine de la Maîtrise des Risques. Elle le définit comme la capacité à survivre non seulement à des événements prévisibles mais également totalement imprévus, en allant ainsi au delà de la Sûreté de Fonctionnement traditionnelle. Après une brève présentation de systèmes plus ou moins résilients en opération, elle propose une première démarche de construction de la résilience ainsi que l'amorce d'un retour d'expérience sur le sujet. Elle est illustrée de divers exemples, issus notamment des domaines aéronautique et spatial.

## Summary

Presented by the working group « Systems Resilience » of the French Association of System Engineering (AFIS), this communication aims at defining the concept of resilience, emerging in the field of Risks Control. The resilience is considered as the ability to survive not only to foreseeable but also totally unexpected events, beyond the scope of Dependability & Safety. After a brief presentation of systems more or less resilient in operation, it offers a first step in resilience building as well as the beginnings of a corporate knowledge on the subject. It is illustrated with some examples from aeronautics and space fields.


## Introduction

Désignant en métallurgie, son domaine d'origine, la capacité d'un matériau à retrouver son état initial à la suite d'un choc ou d'une contrainte particulière, la résilience est un concept nomade qui tient à la fois de l'élasticité et de la fragilité.
Selon l'étymologie, la résilience est la notion de re-sauter, par extension de rebondir. Pour l'écologiste, elle recouvre la capacité de récupération ou de régénération d'un organisme et l'aptitude d'un écosystème à se remettre plus ou moins vite d'une perturbation telle que la reconstitution d'une forêt après un incendie. En psychologie, elle exprime l'aptitude d'un individu à supporter un traumatisme et à « vivre avec ». Les premières publications dans ce domaine datent de 1939-1945 à Hawaï et portent sur l'observation par E. Werner [1] de la « force mystérieuse » qui a permis à des enfants sans structure ni famille, a priori condamnés, de s'en sortir. A partir de 1990, l'éthologue Boris Cyrulnik [2] a développé ce concept en France en le définissant comme « l'art de naviguer dans les torrents ».

Aussi n'est-il pas surprenant de voir ce concept polysémique émerger aujourd'hui dans notre communauté de la Maîtrise des Risques pour dépasser les frontières traditionnelles de la Sûreté de Fonctionnement et s'intéresser à la capacité à « survivre » tant aux événements prévus qu'imprévus [3]&[4].

Mais pour l'esprit cartésien qui caractérise le fiabiliste, vouloir maîtriser l'imprévisible a-t-il du sens ?

C'est pour tenter de répondre à cette question que s'est créé le groupe de travail « Résilience des Systèmes » au sein de l'Association Française d'Ingénierie Système (AFIS). Rassemblant des industriels, organismes publics, universitaires et sociétés de services intervenant dans des domaines divers, celui-ci est aujourd'hui convaincu de l'intérêt de ce concept en ingénierie qu'il définit comme la "Capacité d'un système (incluant son utilisation) dans son environnement (au sens large) à assurer ses missions à un niveau acceptable et sûr (à définir au cas par cas selon le système considéré) en maîtrisant/s'adaptant à des situations/événements prévus et/ou non prévus."

Le but de cette communication est de faire partager cette conviction et de présenter les premiers résultats des travaux du groupe «Résilience des Systèmes » qui s'est donné comme objectifs de :

- capitaliser les connaissances et retour d'expérience en matière de résilience des systèmes,
- élaborer des concepts, processus, méthodes et outils permettant de prendre en compte la résilience des systèmes,
- promouvoir et disséminer les connaissances et pratiques contribuant à la résilience des systèmes.

Un groupe similaire à celui-ci, le "Resilient Systems Working Group », oeuvre de l'autre côté de l'atlantique au sein de l'International Council on Systems Engineering (INCOSE), dont l'AFIS est un membre affilié.

Mais avant de vouloir améliorer les pratiques, faut-il d'abord s'interroger sur l'existant. Les systèmes actuels sont-ils résilients par essence ?

## 1. L'observation sur le terrain

Le Retour d'Expérience sur les incidents passés montre que certains systèmes résistent à des agressions totalement imprévues lors de leur conception alors que d'autres s'effondrent dès la sortie de leurs conditions nominales.
Un avion civil n'est ainsi pas conçu pour résister à un impact de missile, les équipages civils ne sont pas non plus entraînés à réagir à ce genre d'agression. Cependant, les règles et les marges de conception ont permis à un AIRBUS A300B4 de rester structurellement « apte à voler », après un tel événement. De plus, bien que ses commandes de vol ne soient plus opérationnelles, l'équipage a su s'adapter à la situation en tirant le meilleur parti des moyens de contrôle encore disponibles (poussée moteur) pour faire atterrir l'avion en configuration très dégradée. Le système Avion + Equipage a démontré, à cette occasion, une résilience certaine [5].
Les tours du World Trade Center, quant à elles, n'ont pas été dimensionnées pour tenir très longtemps au stress extrême qu'elles ont subi le 11 septembre 2001. Mais leur effondrement soudain, engendré notamment par la dégradation des matériaux à haute température (800°C environ) quelques dizaines de minutes après l'impact de deux avions BOEING 767, ainsi que les difficultés d'évacuation occasionnées n'ont pas permis de sauver un grand nombre de personnes (2595 morts dont 403 membres des personnels de secours). Ne pouvait-on pas imaginer lors de leur construction qu'une quelconque catastrophe de grande ampleur puisse arriver dans les étages d'un immeuble de cette taille, au delà du simple départ de feu « standardisé » et préconiser des moyens d'évacuation d'urgence rapides et diversifiés ? Auparavant il avait déjà fallu plusieurs heures pour venir à bout d'un incendie qui se déclencha au onzième étage de la tour Nord le 13 février 1975 et l'explosion d'un camion chargé de 680 kg d'explosif au nitrate dans l'un de ses parkings souterrains, le 26 février 1993, démontrait, tant sans faut, la crédibilité de la menace terroriste à l'encontre d'un bâtiment symbole de l'Amérique. Ces événements précurseurs avaient toutefois conduit à des améliorations de la signalétique et des exercices d'évacuation, sans lesquelles le bilan aurait été probablement plus lourd.

Mais s'il est facile de tirer des leçons d'accidents et d'incidents après coup, peut-on caractériser a priori la résilience d'un système ou du moins tenter de concevoir celui-ci afin qu'il soit robuste ?

## 2. Prémices d'une démarche

La démarche d'appréhension et de construction de la résilience des systèmes, qui reste encore largement à développer, est évidemment plurielle. Parmi les pistes envisagées, l'identification des limites des méthodes et outils traditionnels de la Sûreté de Fonctionnement apparaît riche d'enseignements.

Considérons un système conçu selon l'état de l'art et donc robuste aux situations et événements prévisibles telles que les défaillances (et propagations de panne), les conditions aux limites (toutes combinées entre elles), ou les erreurs humaines générées par des défauts de procédure ou d'ergonomie des postes de travail. L'imprévu portera alors sur des évènements, des modes d'utilisation ou d'exploitation, ou des environnements difficiles, voire impossibles, à imaginer a priori. Mais comment s'en prémunir ? Outre le fait qu'une conception parfaitement sûre, selon les règles de la « Sûreté de Fonctionnement », se révèle « une vue de l'esprit » dès que l'on atteint une certaine complexité et que la chasse aux erreurs, qui remplissent nos divers bêtisiers de Retour d'Expérience, constituera toujours la priorité, trois approches viennent immédiatement à l'esprit :

- tenter d'améliorer notre connaissance de l'aléa et restreindre ses effets lors de la conception
- débusquer en exploitation tous les événements imprévus, et notamment leurs signes avant-coureurs, et prendre au fur et à mesure les actions appropriées pour les maîtriser,
- confiner les entités potentiellement dangereuses et définir des états de sauvegarde permettant de pallier l'aléa, quel qu'il soit, le temps que l'on puisse comprendre la situation et intervenir sur le système, si nécessaire.

### 2.1 Traitement de l'aléa en conception

Parmi les actions d'amélioration entrant dans cette première catégorie, nous pouvons par exemple citer :

- La simple réflexion sur l'imbrication et l'interdépendance des systèmes (ou organisations) dont on peut imaginer la perte de certains constituants, quelle qu'en soit la raison. Les « systèmes de systèmes » présenteront par exemple une fragilité intrinsèque si certaines ressources partagées peuvent subir des pics de sollicitations à l'occurrence d'événements singuliers (saturation des lignes de communications, des moyens de transport, des sources d'énergie, etc.). En terme de solution, une conception modulaire décentralisée peut permettre d'accroître les possibilités de reprise en cas de perte de certaines ressources. Ainsi l'un des ancêtres du réseau Internet a été développé par la DARPA (Defense Advanced Research Projects Agency) pour répondre au besoin de l'armée américaine de rendre ses systèmes de communication robustes à des attaques massives survenant en de multiples endroits…encore qu'il ne s'agissait pas à l'époque d'attaque de virus informatique qui remettent à nouveau en cause les concepts existants. On notera ici l'importance toute particulière du concept de résilience pour les armées dont le rôle est de répondre à tous les types de menace, même après que celle-ci ait engendré d'éventuelles destructions.

- La lutte contre les pannes de modes communs qui peut conduire à la différentiation de la conception et/ou des approvisionnements de certains constituants critiques, sans avoir une connaissance précise des possibles scénarios de défaillance. Une alimentation de secours par batterie, groupe électrogène, ou source locale d'énergie renouvelable s'avéra, par exemple, plus robuste que la duplication des lignes sur le réseau électrique, même si l'amélioration de fiabilité qu'elle procure est parfois difficile à quantifier.

- La bonne gestion des marges vérifiées à travers les analyses pires cas, qui combinent les conditions extrêmes d'utilisation du produit jusqu'à sa fin de vie prévue, et les analyses des contraintes, qui permettent de s'assurer que des marges ont été prises sur les caractéristiques intrinsèques des composants électriques (analyse de Derating) ou mécaniques vis-à-vis de leurs conditions d'utilisation.

- Les choix de conception robuste (spécification de modes de fonctionnement nominal et dégradés, critères quantitatifs et qualitatifs, implantation de barrières de sécurité, concept fail Operational et/ou fail safe, surveillance macroscopique des fonctions critiques pour s'affranchir des combinaisons de panne, etc.)

- L'implantation de ségrégations significatives entre éléments et chemins en redondance ou entre fonctions et protections associées, même si la capacité d'intégration toujours croissante des composants s'offre à certains concepteurs comme une « tentation du diable ». Comment peut-on démontrer l'absence de risque de propagation de panne au sein d'un même composant ou d'un espace restreint ?

- La conception robuste des interfaces aux sollicitations extérieures de toute nature. On veillera notamment à ce que des systèmes supportant des conditions extrêmes (crue du siècle, tempête, foudre, radiation…), que l'on suppose correctement estimées, ne s'effondre pas en cas de répétition ou de prolongement de celles-ci, notamment en fin de vie, par des phénomènes de fatigue ou par saturation des moyens de protection (un calculateur à bord d'un satellite, par exemple, dont les divers mécanismes de détection et protection succomberont les uns après les autres par la répétition de pannes fugitives engendrées par des radiations durant un pic d'irruption solaire). Cette robustesse à la sollicitation peut également concerner des événements relativement anodins dont seule la multiplication est source de danger.

- L'identification et la suppression de causes favorisant les comportements humains imprévus. Outre la rationalité individuelle qui restera toujours en partie mystérieuse malgré tous nos efforts (de sélection, formation, entraînement, suivi, etc.), certains choix organisationnels conduisent à l'ambiguïté voire immanquablement à la transgression.

Sur ce dernier point, il n'est pas inutile de rappeler que le travail collaboratif s'exerce entre des acteurs contingents motivés par des intérêts de circonstance. Ainsi, un partage de tâches entre des organisations plus ou moins concurrentes, davantage motivé par des considérations contractuelles ou de politique industrielle que techniques, peut engendrer une complexité organisationnelle et un climat peu propice à l'échange et la coopération nécessaire à la maîtrise des risques. Cette ambiance de travail collaboratif, qui prévalaient sur des programmes probatoires comme les projets Apollo (premier homme sur la Lune) aux Etats-Unis, ou SPOT (satellite d'observation de la terre) en France, a tendance à se déliter quelque peu quand chacun doit protéger son territoire par une multiplication de clauses de confidentialité et que toute information sur d'éventuelles faiblesses peut se retourner contre son auteur. Les schémas et analyses de défaillance détaillées sont ainsi pratiquement tous devenus confidentiels dans le domaine spatial, de même que les rapports d'incidents.

De même, certains choix organisationnels favorisent le non-respect des consignes en exploitation. Comment un pilote de ligne choisit-il sa trajectoire quand il doit arbitrer entre la sécurité des personnes et la durée du vol, sachant que le raccourcissement de cette dernière peut engendrer le versement de primes, dans certaines compagnies ? Comment ne pas privilégier le fonctionnement d'un hélicoptère sur sa maintenance quand on est payé à l'heure de vol [6] ? Issus d'un domaine aéronautique tout particulièrement soucieux des aspects sécuritaires, ces deux exemples illustrent un phénomène bien connu des psychologues que l'on peut associer à la « communication paradoxale » ou aux messages contradictoires que l'on retrouve à la source de multiples « erreurs humaines ». L'anthropologue G. Bateson, inspirateur de l'Ecole de Palo Alto qui a abordé la communication d'un point de vue systémique, a notamment expliqué le caractère perturbant de messages paradoxaux émis simultanément par une même source qu'il qualifiait par l'expression « double bind » (double contrainte).

## 2.2 Traitement de l'aléa en exploitation

Le retour d'expérience en exploitation est évidemment la manière la plus naturelle de débusquer l'imprévu, ou du moins ses signes annonciateurs. Encore faut-il les détecter, ce qui suppose de consacrer des ressources adéquates pour observer et traiter l'information en continu, maintenir un lien entre concepteur et exploitant pendant toute la durée de la vie du système et initier des modifications le cas échéant avec le recul nécessaire.
Par ailleurs, les plans et procédures préétablis ont leurs limites dans un environnement dynamique. A l'origine de certaines défaillances, ce changement incessant est parfois difficile à anticiper ; ce qui oblige à laisser une certaine marge de manœuvre et d'initiative à l'opérateur pour gérer l'imprévu, en misant sur ses capacités d'intelligence et d'expérience, malgré les erreurs qu'il est susceptible de commettre.

## 2.3 Survie et confinement

En identifiant à un niveau macroscopique les fonctions « vitales » d'un système ou d'un « système de systèmes » quel qu'il soit, il apparaît souvent possible de bâtir des stratégies de surveillance et de préservation de ces fonctions pendant une durée suffisante pour que l'on puisse analyser la situation et mener des actions correctives. Dans le domaine spatial, par exemple, les satellites sont généralement dotés d'un mode de survie qui assure les conditions thermique et énergétique minimales indispensables à la préservation de leur intégrité dès que cette dernière semble menacée. Un logiciel spécifique, ou du moins de taille limitée pour être testé de manière quasi exhaustive en développement, se contente alors d'assurer la bonne orientation des panneaux solaires et le réchauffage des quelques équipements les plus fragiles, à l'exception de toute autre fonctionnalité, le temps que les opérateurs auscultent le satellite au travers de télémesures et interviennent du sol au moyen de télécommandes. Combien de satellites ont-ils ainsi survécu à l'imprévu, de nature humaine, environnementale, technologique, ou autre, grâce à leur mode de survie ?
A contrario, qu'en est-il de nos villes dont l'évacuation immédiate en cas d'urgence se transformerait immanquablement en thrombose généralisée, au regard des schémas routiers adoptés ? Le cyclone à la Nouvelle-Orléans, l'explosion de l'usine AZF de Toulouse (heureusement sans dégagement de phosgène) ou les récents actes terroristes à Londres ou à Madrid sembleraient pourtant montrer qu'une catastrophe urbaine de grande ampleur est un événement « imprévisible » à classer plutôt dans le domaine du « probable».

De même peut-on identifier dans un système la présence de matériaux intrinsèquement dangereux et assurer leur confinement même si leur diffusion semble a priori impossible. Une enceinte bétonnée sur la centrale Tchernobyl aurait probablement permis de mieux se protéger des répercussions d'une incroyable succession d'erreurs humaines. Outre les éléments radioactifs, ce confinement peut également concerner des matériaux chimiques ou biologiques indésirables (agents pathogènes, germes infectieux, etc.) pour lesquels des mesures peuvent être prises pour éviter leur dispersion dans l'environnement (barrières physiques, système auto destructif, local en dépression constante, etc.).

Par ailleurs, la réflexion sur les événements prévus ou imprévus conduit inexorablement à s'interroger sur la qualité de l'expertise. Comment le risque est-il identifié puis évalué ? Quelles sont les erreurs commises ? Quelles sont les conditions du débat technique ? Comment se prend la décision sécuritaire ? Un regard tourné sur les dernières grandes affaires de santé publique en France (nuage radioactif, sang contaminé, amiante, etc.) montre que les collèges d'experts, même les plus éminents, sont également faillibles. Qu'en est-il de la résilience écologique à certains Organismes Génétiquement Modifiés (OGM) qui fait actuellement débat ?

# 3. Amorce de capitalisation des connaissances

L'un des objectifs du groupe de l'AFIS est de capitaliser les connaissances et le retour d'expérience en matière de résilience des systèmes. Aussi l'une de ses premières actions a consisté à rechercher les « travaux pertinents » et les « véritables experts », dans une nébuleuse qui gravite autour de ce concept en émergence, qui intéressent l'ingénierie des systèmes.

Accessible sur le site de l'AFIS à l'adresses : www.afis.fr/nav/gt/rds/rds.html, cette capitalisation se présente aujourd'hui sous la forme de diverses listes concernant :

- les experts reconnus,

- les différents réseaux,
- les sites Internet
- les colloques et congrès,
- la bibliographie (livres, articles),

traitant du concept de résilience appliqué à l'ingénierie des systèmes.

## Conclusion

Si maîtriser l'imprévisible semble évidemment utopique, il nous apparaît quelque peu imprudent de ne considérer que le "probable" ou le "certain" dans la conception des systèmes à risques.

Déjà parmi les événements envisageables, la quantification probabiliste est souvent restreinte par l'absence de modèles ou de données statistiques représentatives, notamment dans le cas d'événements rares.

De plus, le possible ne se cantonne pas toujours au domaine bien connu. En termes d'événements redoutés, notre connaissance atteint d'autant plus ses limites que les systèmes mis en œuvre sont sophistiqués et leur durée de vie élevée dans des conditions d'utilisation incertaines (ex : GPS, initialement utilisé par les militaires, puis par l'aéronautique civile et maintenant par tout à chacun dans ses déplacements).

Enfin, tel un vaccin ou un antibiotique, certaines précautions présentent un large spectre qui recouvre en partie l'imprévu. Des exigences de robustesse, telles que les concepts d'indépendance, de ségrégation ou de bonne gestion des marges, peuvent être classées dans cette catégorie même si dans un environnement évolutif, ces précautions peuvent perdre de leur efficacité au cours du temps.

Et de son côté, la menace évolue…

Sur la base de ce premier constat, penser en terme de résilience, nous semble porteur d'améliorations des systèmes à concevoir.

On notera cependant que la résilience peut également devenir problématique quand la désactivation de certaines fonctionnalités en devient difficile, à l'image de l'ordinateur HAL 9000 du film culte de Stanley Kubrick « 2001 : l'odyssée de l'espace ». C'est le cas, par exemple, des échanges non maîtrisés sur Internet dont on ne peut pas se débarrasser totalement.

**Références**

[1] - Werner, E.E., & Smith, R.S. (1989). Vulnerable, but invincible: A longitudinal study of resilient children and youth. New York, NY: Adams, Bannister, Cox.
[2] - Boris Cyrulnik. Un Merveilleux Malheur, Odile Jacob, 1999.
[3] - Erik Hollnagel, David D. Woods and Nancy Leveson, Resilience Engineering : Concepts and precepts , Ashgate, 2006
[4] - Scott Jackson. Resilient Systems en draft sur le site de l'INCOSE
[5] - Y. Malinge, A300B4 Loss of all hydraulics Baghdad - A remarkable example of airmanship, ISASI, 2004
[6] - Woods D.D., Gomes J.O., and al, Application of Resilience Engineering on Safety in Offshore Helicopter Transportation, SIEDS'06, Charlottesville, USA, 28/04/06