



**HAL**  
open science

# VERS UN SYSTEME D'INFORMATION ANTIFRAGILE? UNE RECHERCHE EN COURS

Cécile Godé

► **To cite this version:**

Cécile Godé. VERS UN SYSTEME D'INFORMATION ANTIFRAGILE? UNE RECHERCHE EN COURS. Management & Data Science, 2024, 10.36863/mds.a.27266 . hal-04445660

**HAL Id: hal-04445660**

**<https://hal.science/hal-04445660v1>**

Submitted on 12 Feb 2024

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

## VERS UN SI ANTIFRAGILE ? UNE RECHERCHE EN COURS

Cécile Godé

Professeure agrégée des universités

Aix Marseille Univ, CERGAM, Aix-en-Provence, France

Site Pauliane-MEGA

424, chemin du Viaduc

13080 Aix-en-Provence

[cecile.gode@univ-amu.fr](mailto:cecile.gode@univ-amu.fr)

### Résumé

Un Système d'Information (SI) résilient est conçu dans une optique de préservation des processus et fonctionnalités clés en cas de choc, puis de retour à la normale. Mais un SI résilient peut-il évoluer vers un SI antifragile, surpassant l'objectif de « rebond résilient » pour se renforcer et s'améliorer dans l'imprévu ? A partir d'une perspective socio-technique, cette recherche en cours présente la version bêta d'une grille de diagnostic d'un SI antifragile articulant résilience et antifragilité.

### Introduction

Quand Netflix lance l'application Chaos Monkey en 2011, la finalité est d'introduire « *un singe sauvage lâché dans un datacenter ou un cloud qui, avec une arme, mettrait aléatoirement hors d'état des instances et sectionnerait des câbles, l'objectif étant de continuer à servir ses clients sans interruption* » ([Netflix TechBlog, 2019](#)). Chaos Monkey est le premier des nombreux soldats de l'Armée Simienne de Netflix, qui oblige à une vigilance de tous les instants pour garantir le service de streaming parmi le plus efficace au monde. Cet exemple illustre en partie ce qu'un Système d'Information (SI) antifragile peut être.

Un SI antifragile se renforce dans l'adversité : plus il est confronté à la nature dynamique non linéaire des « cygnes noirs » – événements à forts impacts, difficiles à prédire ([Taleb, 2011](#)) – plus son exposition aux pertes est limitée et son potentiel de gain augmente ([Taleb et West, 2023](#)). C'est toute la philosophie sous-tendant l'ingénierie du chaos mise en action par Netflix. L'imprévu, le choc, le stress sont considérés comme autant d'opportunités d'amélioration du SI.

Malgré ces promesses encourageantes, peu nombreuses sont les organisations qui développent des SI antifragiles. Les principes de conception dominants les conduisent plutôt à construire des SI résilients, préservant leurs processus et fonctionnalités clés pendant la perturbation pour rebondir à l'issue et retrouver leur fonctionnement normal ([Abbas et Munoz, 2021](#)). Mais un SI résilient peut-il évoluer vers un SI antifragile ?

La littérature en management des SI (MSI) et informatique traite de façon différenciée résilience et antifragilité, sans véritablement interroger les potentielles continuité et articulation entre les deux approches de conception. Adoptant une perspective socio-technique du SI et s'inscrivant dans la méthode du *Design Science Research* (voir l'annexe méthodologique produite en fin d'article), cet article de recherche en cours réconcilie ces deux visions et propose les résultats de la première boucle de conception réalisée : la version bêta d'une grille de diagnostic d'un SI antifragile.

## **Le SI socio-technique**

Initiée par le *Tavistock Institute of Human Relations* et notamment rendue célèbre par les travaux séminaux de Emery et Trist (1974), la perspective socio-technique considère l'organisation comme un système ouvert constitué de deux sous-systèmes – social et technique – interconnectés et interdépendants. Dès le début des années 90, le MSI s'empare de cette approche dans son appréhension des technologies et trajectoires d'appropriation (par ex., [Orlikowski, 1992](#) ; [Desanctis et Poole, 1994](#) ; [Godé, 2008](#)). Le SI est compris dans sa double dimension technique, portant sur « *les processus, tâches et technologies nécessaires pour transformer des inputs en outputs* » et sociale, renvoyant aux « *attributs des personnes (par ex., attitudes, compétences, valeurs), à leurs relations, aux systèmes de récompenses et aux structures d'autorité* » du SI ([Bostrom et Heinen, 1977](#), p. 17). En contournant le piège du déterminisme (technologique et social) pour considérer la complexité du réel, l'approche socio-technique met l'accent sur les imbrications entre organisation et technologie. Elle conduit ainsi à intégrer les dimensions humaines et matérielles du SI, très tôt dans le processus de conception.

## **Principes de conception d'un SI résilient**

A quelques rares exceptions près ([Gorgeon, 2015](#) ; [Abbas et Munoz, 2021](#) ; [Godé et al., 2023](#)), le MSI ne s'intéresse pas à la conception de SI antifrangibles. La vision dominante, dans les mondes à la fois académiques et professionnels, incite plutôt à la conception de SI résilients. Les approches incrémentales reposent alors sur l'identification des risques connus – le plus souvent par le biais de cas d'usage types – puis le développement d'une architecture, de processus et de fonctionnalités à même de les gérer et les limiter (par exemple, [Liu et al., 2010](#) ; [Zhang et Lin, 2010](#) ; [Arlat et al., 2006](#)). La finalité recherchée est le maintien des opérations cœur de l'organisation sans interruption majeure lors du choc, puis le rebond vers un fonctionnement courant. L'analyse de la littérature académique et professionnelle spécialisée, en MSI principalement, permet de produire le tableau 1 ci-dessous. Deux précautions importantes à la lecture de ce tableau : d'une part, il est nécessaire de l'aborder comme toujours en cours d'élaboration, en particulier concernant les attributs du système social. Ces derniers donnent à voir à ce stade des dimensions principalement « métiers » qui ne sauraient à eux seuls satisfaire aux attentes de la perspective socio-technique ; une attention accrue devra être portée aux structures organisationnelles, usages et trajectoires d'appropriation lors de la prochaine boucle de conception. D'autre part, certains principes de conception apparaissent en bleu ; nous verrons dans la grille de diagnostique qu'ils correspondent à une phase de transition vers un SI antifrangible.

SI RESILIENT Principes de conception (par ordre alphabétique)	SI socio-technique	
	Sous-système technique	Sous-système social
<b>Adaptabilité</b>	Architecture flexible capable de s'adapter à l'évolution des sources d'informations et des besoins métiers et clients. Par ex., intégration de composants et d'interfaces logiciels « hérités » (ERP, CRM) et nouveaux (API, RPA SaaS)	Prise en compte de l'expérience utilisateur
<b>Compartmentation</b>	Segmenter le SI pour favoriser l'autonomie des composants fonctionnels pris isolément et se protéger des défaillances locales	Expertises en développement, intégration et exploitation des infrastructures du SI; développement de stratégies back-up
<b>Contrôle continu</b>	Capteurs dédiés à la surveillance temporelle et spatiale du bon fonctionnement du SI	Expertises en exploitation, surveillance et maintenance du SI
<b>Fiabilité</b>	Transmission, intégrité, conformité et consolidation des données stockées (automatisation)	Expertises en développement, intégration et exploitation des infrastructures du SI
<b>Prédiction</b>	Capacités prédictives pour anticiper les vulnérabilités (internes) et les menaces (externes) vis-à-vis du SI	
<b>Apprentissage par l'erreur</b>	Tolérance à la faute pour prendre en compte les risques résultant d'une potentielle défaillance du SI en étant capable de diagnostiquer les erreurs (fautes de développement, d'IHM, malveillance), de les traiter et de rétablir le système	Expertises en exploitation et maintenance (corrective) du SI, management de la transformation numérique. Importance de la tolérance aux fautes de la part de l'utilisateur et des dispositifs d'apprentissage à mettre en œuvre pour les éviter; importance de prendre en compte les rôles et profils des utilisateurs.
<b>Redondance des données</b>	Copie et stockage des ensembles de données dans différents endroits (serveurs sur site, hors site, cloud) afin de faciliter leur récupération en cas d'événements imprévus (par ex., panne, cyberattaque, catastrophe naturelle)	Expertises en développement, l'intégration et l'exploitation des infrastructures du SI
<b>Sécurité</b>	Le SI dispose de mesures robustes pour se protéger contre les cyberattaques, les violations de données ou toutes autres menaces de sécurité	Gouvernance dédiée au management de la sécurité du SI couvrant les aspects humains et organisationnels: développer et mettre en œuvre la politique de sécurité, identifier les investissements clés, agir sur les compétences nécessaires et le système d'incitation vis-à-vis des utilisateurs des SI

Tableau 1. Les principes socio-techniques de conception d'un SI résilient

### Principes de conception d'un SI antifragile

Pour identifier précisément les principes de conception clés d'un SI antifragile, c'est vers l'informatique qu'il est alors nécessaire de se tourner. Depuis une quinzaine d'année, la discipline produit en effet des travaux dédiés, s'intéressant notamment à la conception et au développement de logiciels et architectures antifragiles (voir par exemple, [Hole, 2016](#) ; [O'Reilly, 2019](#) ; [Simonette et al., 2019](#)). Etant impossible d'éviter les cygnes noirs, il convient d'en tirer avantage pour se renforcer. Les auteurs spécialisés s'attachent ainsi à développer des systèmes adaptatifs complexes capables d'absorber et d'apprendre de petits chocs inévitables, tout en se protégeant des grands risques, porteurs de trop fortes menaces pour le système ([Godé et al., 2023](#)). L'analyse de la littérature académique et professionnelle spécialisée, en informatique principalement, permet de produire le tableau 2. Les précautions de lecture précisées ci-dessus s'appliquent à nouveau.

SI ANTIFRAGILE Principes de conception (par ordre alphabétique)	SI socio-technique	
	Sous-système technique	Sous-système social
Diversité des modules	Les modules dupliqués sont conçus et/ou implémentés différemment, tout en fournissant (presque) les mêmes fonctionnalités (le but est d'éviter de se retrouver confronté à la même défaillance ou au même défaut que le module original).	
Liens faibles	Les connexions entrantes vers un module défaillant sont interrompues de façon à ce que les modules dépendants subissent le moins de dégâts possible, limitant ainsi les dommages au seul module concerné	Expertises en développement, intégration et exploitation des infrastructures du SI; développement de stratégies back-up
Modularité	Le SI est composé de modules logiciels et matériels faiblement interconnectés (en cas de panne, de défaut ou de problème local détecté sur un module, la connexion aux autres est interrompue pour éviter la propagation à l'ensemble du système)	
Apprentissage par l'erreur	De petits chocs (pannes, défauts) sont intentionnellement introduits dans le système pour favoriser l'apprentissage par l'erreur et transformer le SI afin de limiter l'impact des incidents futurs	Soutenues par l'organisation, des pratiques de retour d'expérience sont développées par les utilisateurs pour favoriser un apprentissage individuel et collectif continu
Redondance des modules	Duplication des modules logiciels et matériels	Expertises en développement, l'intégration et l'exploitation des infrastructures du SI
Sécurité	Le SI dispose de mesures robustes pour se protéger contre les cyberattaques, les violations de données ou toutes autres menaces de sécurité	Gouvernance dédiée au management de la sécurité du SI couvrant les aspects humains et organisationnels: développer et mettre en œuvre la politique de sécurité, identifier les investissements clés, agir sur les compétences nécessaires et le système d'incitation vis-à-vis des utilisateurs des SI

Tableau 2. Les principes socio-techniques de conception d'un SI antifragile

### Proposition d'une grille de diagnostic (première boucle de conception – version Bêta)

Les deux premiers tableaux révèlent l'existence de principes de conception homogènes qui permettent d'articuler SI résilient et SI antifragile : l'apprentissage par l'erreur, la redondance des données et des modules, et la sécurité. Ainsi, une lecture intéressante pourrait-elle être de considérer la continuité entre d'une part, le développement et le déploiement d'un SI résilient basés sur l'analyse et la gestion des risques, et d'autre part sa transformation progressive en SI antifragile se soumettant volontairement aux perturbations et chocs (maîtrisés).

La grille de diagnostic du SI antifragile présentée dans le tableau 3 repose sur cette vision. Dans le contexte actuel, caractérisé par une accélération du processus de transformation digitale (Varenne et Godé, 2021) et une forte instabilité politico-économique, l'importance pour les organisations de se doter d'un outil de diagnostic capable d'évaluer, à un instant donné, le stade de développement d'un SI antifragile est critique.

		SI RESILIENT					SI RESILIENT/ANTIFRAGILE				SI ANTIFRAGILE		
		Adaptabilité	Compartmentation	Contrôle continu	Fiabilité	Prédiction	Redondance des données	Apprentissage par l'erreur	Sécurité	Redondance des modules	Diversité des modules	Liens faibles	Modularité
SI socio-technique	Sous-système technique												
	Sous-système social												

Tableau 3. Version bêta de la grille de diagnostic d'un SI antifragile

### Bibliographie

- Abbas, R. et Munoz, A. (2021). Designing Antifragile Social-Technical Information Systems in an Era of Big Data. *Information Technology & People*, 34(6), 1639-1663. <https://doi.org/10.1108/ITP-09-2020-0673>
- Arlat, J., Crouzet, Y., Deswarte, Y., Fabre, J. C., Laprie, J. C. et Powell, D. (2006). Tolérance aux fautes. Dans J., Akoka et I., Comyn-Wattiau (dir.), *Encyclopédie de l'informatique et des systèmes d'information* (Partie I., p. 240-269). Vuibert.
- Bostrom, R. P. et Heinen, J. S. (1977). MIS Problems and Failures: A Socio-Technical Perspective. Part I: The Causes. *MIS Quarterly*, 1(3), 17-32. <https://doi.org/10.2307/248710>

- Desanctis, G. et Poole, M.S. (1994). Capturing the Complexity in Advanced Technology Use: Adaptive Structuration Theory. *Organization Science*, 5(2), 121-146. <https://doi.org/10.1287/orsc.5.2.121>
- Emery, F.E. et Trist, E.L. (1974). Socio-Technical Systems. Dans M. Argyle (ed.), *Social Encounters: Contributions to Social Interaction*. Routledge.
- Godé, C., Lebraty, J.-F. et Barbaroux, P. (2023). D'un système d'information résilient à un système d'information anti-fragile ? Illustrations à partir des organisations militaires. *Les Cahiers Risques et Résilience*, 5, 83-96.
- Godé, C. (2008). Les TIC comme leviers du changement : une analyse du cas des Armées américaines en Afghanistan. *Systèmes d'Information et Management*, 13(1), 7-30. <https://doi.org/10.3917/sim.081.0007>
- Gorgeon, A. (2015). *Anti-fragile information systems*. The 36th International Conference on Information Systems (ICIS), Proceedings. 6. <https://aisel.aisnet.org/icis2015/proceedings/BreakoutIdeas/6>
- Hole, K. J. (2016). *Anti-fragile ICT systems*. Simula SpringerBriefs on Computing, Springer.
- Liu, D., Deters, R. et Zhang W. J. (2010). Architectural Design for Resilience. *Enterprise Information Systems*, 4(2), 137-152. <https://doi.org/10.1080/17517570903067751>
- O'Reilly, B. (2019). No More Snake Oil: Architecting Agility through Antifragility. *Procedia Computer Science*, 151, 884-890. <https://doi.org/10.1016/j.procs.2019.04.122>
- Orlikowski, W. J. (1992). The Duality of Technology: Rethinking the Concept of Technology in Organizations. *Organization Science*, 3(3), 398-427. <https://doi.org/10.1287/orsc.3.3.398>
- Simonette, M., Magalhães, M., Bertassi, E. et Spina, E. (2019). *Beyond Resilience in Sociotechnical Systems*. The International Symposium on Systems Engineering (ISSE), Proceedings, 1-4. <https://doi.org/10.1109/ISSE46696.2019.8984570>
- Taleb, N. N. (2011). *Le Cygne noir : la puissance de l'imprévisible*. Les Belles Lettres.
- Taleb, N. N. et West, J. (2023). Working with Convex Responses: Antifragility from Finance to Oncology. *Entropy*, 25(2), 1-21. <https://doi.org/10.3390/e25020343>
- Varenne, P. et Godé, C. (2021). Transformation digitale : vers un Business Model Digital Dynamique (BMD2). *Management et Data Science*, 5(3), <https://doi.org/10.36863/mds.a.16269>
- Shipitsyn, V., Adler, M., Egyed, Z. et Blankinship, P. (2020). Design for Resilience. Dans H., Adkins, B., Beyer, P., Blankinship, P., Lewandowski, A. Oprea et A., Stubblefield (dir.), *Building Secure and Reliable Systems* (Chapter 8, p. 143-181). O'Reilly Media, Inc.
- Zhang, W. J. et Lin, Y. (2010). On the Principle of Design of Resilient Systems: Application to Enterprise Information Systems. *Enterprise Information Systems*, 4(2), 99-110. <https://doi.org/10.1080/17517571003763380>

## Annexe méthodologique

Le DSR travaille à rapprocher les mondes de la recherche et professionnel en adoptant « *un nouveau mode pour penser et exécuter la recherche scientifique, [...] dans lequel la conception d'un artefact est centrale pour résoudre le problème initial auquel la recherche tente de répondre* » (Pascal, 2012, p. 8). En tant que méthode scientifique, le DSR vise ainsi à développer des connaissances sur les artefacts et leur processus de conception dans une optique de résolution de problèmes (Simon, 1969, 3<sup>ième</sup> édition 1996). Appliqué au management des systèmes d'information (MSI), le DSR permet de concevoir, développer et évaluer des artefacts technologiques – dans une perspective socio-technique selon Carlsson (2007) – afin de produire des connaissances actionnables. L'une des méthodes la plus connue et employée en MSI est celle de Hevner et al. (2004), qui repose sur sept critères de mise en œuvre (voir Pascal, 2012, pour une analyse critique approfondie des apports de Hevner et al, 2004) : la conception de l'artefact (construit, modèle, méthode, etc.), la pertinence (identification du problème initial et cohérence de la solution proposée), l'évaluation (observation expérimentation, étude de terrain, etc.), les contributions (apports de la recherche aux mondes académique et professionnel), la rigueur (démarche scientifique), le processus (mise en œuvre de plusieurs boucles de conception) et la communication (des résultats de la recherche aux professionnels confrontés au problème initial). Ces critères se combinent au sein de boucles de conception itératives qui permettent au chercheur d'apprendre et d'améliorer progressivement l'artefact, offrant au final des éléments de solution au problème identifié initialement.

Dans notre recherche en cours, nous retenons la méthode DSR pour concevoir la première version de notre grille de diagnostique (artefact) d'un SI antifragile. L'article produit pour *Management & Data Science* repose sur la réalisation d'une première boucle de conception en respect des sept critères décrits ci-dessus (tableau 1) :

BOUCLE DE CONCEPTION N°1	
CRITERES (Hevner et al, 2004)	APPLICATION DES CRITERES
<b>La conception</b>	Un outil (grille) de diagnostic permettant d'évaluer, à un instant donné, le stade de développement d'un SI antifragile. Au cœur de la conception est la volonté de réconcilier résilience et antifragilité : si les architectures et processus SI sont à l'origine conçus pour être résilients, certains des principes de conception rejoignent ceux de l'antifragilité et peuvent évoluer vers un SI antifragile.,
<b>La pertinence</b>	Les « cygnes noirs », telles que les cyber-attaques et les catastrophes naturelles et sanitaires, surviennent fréquemment et ont des impacts négatifs croissants sur les SI. La capacité des organisations à tirer profit de ces événements perturbateurs peut déterminer le succès des projets SI, voire garantir leur propre survie.
<b>L'évaluation</b>	Présentation (3) et recueil de retours critiques autour de la grille de diagnostique auprès de : <ul style="list-style-type: none"> <li>– Chercheurs en management (pour certains spécialisés en MSI) français (avril 2023) et américains (nord et sud, mai 2023)</li> <li>– Professionnels (acteurs militaires et d'une entreprise de la BITD français) fréquemment confrontés aux risques de perturbations et d'attaques de leurs SI opérationnels et de gestion (juin 2023)</li> </ul> Echanges mails (8) avec deux des professionnels ci-dessus pour discuter de points d'amélioration spécifiques de la grille
<b>Les contributions</b>	La notion de SI antifragile, très peu abordée en MSI dans sa dimension conception ; la grille de diagnostique à destination des professionnels (Direction des SI, par exemple)

<b>La rigueur</b>	Base de connaissance disponible pour entamer la conception de la grille (revue de littérature en MSI et informatique ; littérature professionnelle spécialisée) ; cohérence des objectifs de la recherche avec le DSR et la méthode de Hevner et al. (2004)
<b>Le processus</b>	La recherche est en cours. Les résultats reposent sur une première boucle de conception et donc une version Bêta de l'artefact, qui ne permet pas encore de répondre au problème initial. Il est essentiel de poursuivre la revue de littérature autour des dimensions du sous-système technique, et plus encore social, de la grille.
<b>La communication</b>	Outre la volonté de recueillir des critiques constructives, les présentations qui ont été faites aux chercheurs académiques et aux professionnels (voir critère évaluation) poursuivaient également une finalité de communication des travaux.

Tableau 4. Application des critères DSR de Hevner et al. (2004)

### Bibliographie

- Carlsson, S. A. (2007). Developing Knowledge through IS Design Science Research. *Scandinavian Journal of Information Systems*, 19(2), 75-86. <https://www.proquest.com/scholarly-journals/developing-knowledge-through-is-design-science/docview/2632320926/se-2?accountid=162151b>
- Hevner, A. R., March, S. T., Park, J. et Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, 28(1), 75-106. <https://doi.org/10.2307/25148625>
- Pascal, A. (2012). Le design science dans le domaine des systèmes d'information : mise en débat et perspectives. *Systèmes d'Information et Management*, 17(3), 7-31. <https://doi.org/10.3917/sim.123.0007>
- Simon, H. (1996). *The Sciences of the Artificial*. 3rd ed., MIT Press.