Vers des systèmes de systèmes robustes

Towards resilient systems-of-systems

Ilyas Ed-daoui[1,3], Mhamed Itmi[2], Abdelkhalak El Hami[3], Nabil Hmina[1], Tomader Mazri[4]

[1] Laboratoire Génie des Systèmes (LGS), ENSA-Kénitra, Université Ibn Tofail, Maroc, ilyas.eddaoui@insa-rouen.fr, hmina@univ-ibntofail.ac.ma
[2] Laboratoire d'Informatique, de Traitement de l'Information et des Systèmes (LITIS), INSA-Rouen-Normandie, France, mhamed.itmi@insa-rouen.fr
[3] Laboratoire d'Optimisation et Fiabilité en Mécanique des Structures (LOFIMS), INSA-Rouen-Normandie, France, abdelkhalak.elhami@insa-rouen.fr
[4] Laboratoire Génie Électrique et Système de Télécommunication, ENSA-Kénitra, Université Ibn Tofail, Maroc, tomader20@gmail.com

RÉSUMÉ. Les échecs, les erreurs et bien d'autres irrégularités représentent les menaces principales aux systèmes de systèmes. Nous présentons deux scénarios qui déclenchent ces menaces. Le premier scénario est lorsqu'une perturbation désorganise une partie du système voire le système tout entier (dans certains cas) et le deuxième scénario est lorsqu'une exploitation d'une vulnérabilité ait lieu.
Dans cet article, on représente notre approche pour la gestion de ces menaces ciblant les systèmes de systèmes. On s'appuie sur l'exploitation de tableau de bord pour la supervision des perturbations potentielles aux systèmes de systèmes. Des recommandations pour la gestion des vulnérabilités et la résolution de ces problèmes sont également citées dans la dernière section de l'article.
ABSTRACT. Failures, errors and many other irregularities represent the main threats to systems-of-systems. We present two scenarios that trigger these threats. The first scenario is when a disruption disorganizes a part of the system or even the entire system and the second scenario is when an exploitation of a vulnerability occurs.
In this article, we present our approach to managing the triggers of threats targeting the systems-of-systems. It is based on the use of dashboards to monitor potential disruptions of systems-of-systems. Recommendations for the management of vulnerabilities and resolution of these problems are also mentioned in the last section of the article.
MOTS-CLÉS. Systèmes de systèmes, Résilience, Tableau de bord, Perturbation, Vulnérabilité.
KEYWORDS. Systems-of-Systems, Resilience, Dashboard, Disturbance, Vulnerability.

1. Introduction

Les systèmes de systèmes sont des systèmes complexes composés d'entités multi-physiques, distinctes, hétérogènes, autonomes et qui sont mis en communication pour atteindre un objectif commun. La mesure des incidents, des défaillances et des dysfonctionnements, dans ce contexte, est extrêmement essentielle comme une défaillance d'un système peut provoquer une altération complète du processus ou même endommager l'ensemble du système dans certains cas.

Dans le contexte des systèmes de systèmes, le concept de la résilience n'est pas facile à interpréter. Elle est définie comme la capacité du système à résister une perturbation tout en gardant les paramètres de dégradation de performance acceptable pour le système ainsi que la possibilité de se remettre à l'état normal dans un délai acceptable et avec des coûts raisonnables [AVE 11].

Dans ce papier, la résilience, ou la robustesse, concerne les conséquences en cas de perturbations et d'incertitudes associées. Nous disons que le système est résilient si le système peut faire face à des perturbations et revenir rapidement au comportement normal.

Il existe plusieurs méthodes pour aborder la résilience : nous pouvons considérer la résilience comme une quantité fixe pour le système. Cette approche est limitative parce que dans le contexte des systèmes de systèmes, nous ne parlons pas d'un système fixe avec des attributs fixes (nous sous-entendons ici les composants du système, les services...), au contraire on parle souvent d'un système multi-physique muni d'une

architecture flexible et modifiable. Par contre, la seconde approche la considère comme une variable aléatoire, en particulier pour les systèmes modifiant leur architecture, leur environnement et leur composition.

Dans cet article, on aborde le problème de la robustesse des systèmes de systèmes en essayant de le contrôler de sa source. Cette source peut être externe ou interne, ici on parle des perturbations ou des vulnérabilités qui peuvent mettre le système en péril. Et pour gérer leurs éventuelles conséquences, on propose d'établir une stratégie de minimisation du taux d'échec du système et l'élaboration d'une politique du rétablissement du système après chaque défaillance.

2. Travaux connexes

La méthodologie présentée apporte une contribution à la supervision de la fiabilité des systèmes hétérogènes et complexes en général et la supervision de la résilience des systèmes de systèmes en particulier. Elle fournit une méthode basée sur l'utilisation de tableau de bord pour la supervision de la performance de ces systèmes.

Dans ce cadre, certaines approches ont été proposées. L'une d'entre elles s'articule autour d'un modèle d'analyse de résilience [FIL 14]. Ce modèle est conçu pour dériver des quantités structurelles et dynamiques afin de fournir une image complète du système étudié.

Les auteurs de [FIL 14] proposent une méthodologie de l'analyse de la résilience des systèmes de systèmes qui consiste à faire, premièrement, une étude de l'infrastructure fondée sur les dépendances fonctionnelles entre les systèmes est adoptée, ensuite, une analyse des propriétés structurelles et dynamiques inhérentes du système de systèmes.

Le modèle théorique proposé dans [BUK 16] est basé sur la méthodologie de l'ingénierie des services et il est étroitement lié à l'idée de l'entreprise résiliente ainsi que le concept de la tolérance des perturbations. Un concept pour la description de la qualité opérationnelle et basée sur le temps est aussi proposé. Le concept est baptisé 'dependability'.

L'auteur de [BUK 16] propose trois perspectives pour la définition du concept proposé qui sont :

- Une approche probabiliste liée aux disponibilités,
- Une approche probabiliste déterministe liée à la disponibilité et la crédibilité,
- Une approche liée au risque.

Dans ce qui suit, on propose une méthodologie dédiée à l'établissement d'une stratégie de minimisation du taux d'échec du système ainsi qu'à l'élaboration d'une politique de rétablissement du système après une défaillance.

3. Notre modèle proposé

L'architecture distribuée et changeable des systèmes de systèmes complique souvent la conception d'une infrastructure robuste et fiable. Ce qui nous pousse à aborder le problème de la fiabilité des systèmes de systèmes par le contrôle des vulnérabilités et les perturbations internes et externes. Comme la montre la figure ci-dessous, notre vision vis-à-vis de la robustesse des systèmes de systèmes s'appuie sur plusieurs parties prenantes pour finalement cerner le concept de la fiabilité.

Dans notre étude, on se concentre sur l'exploitation des vulnérabilités ainsi que les perturbations internes et externes. De plus, pour améliorer la résilience des systèmes de systèmes, il faut faire appel à deux éléments primordiaux : la définition d'une stratégie de minimisation du taux d'échec pour chaque groupe de systèmes et l'élaboration d'une politique du rétablissement du système de systèmes après chaque défaillance.

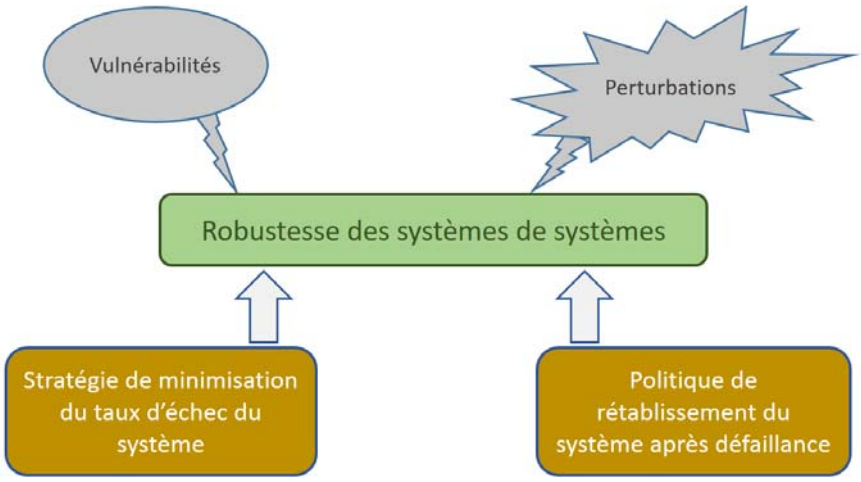

Figure 3. *Notre modèle pour l'amélioration de la robustesse*

3.1. *Que signifient les perturbations et les vulnérabilités dans le contexte des systèmes de systèmes ?*

Les perturbations, comme la nomination l'indique, représentent les éléments, phénomènes, actions ou comportements pouvant inciter des nuisances au déroulement normal du système de systèmes, elles peuvent être classées selon deux catégories :

– ***Perturbations internes :*** elles sont des anomalies ou des désordres provenus d'une entité au sein du système de systèmes. Elles peuvent être des entités physiques ou des programmes logiques (des bugs, des inondations de trafic, etc.).

– ***Perturbations externes :*** elles sont incitées soit suite à une intervention humaine soit à un phénomène naturel.

Les vulnérabilités, par contre, représentent les failles du système qui peuvent faire l'objet d'éventuelles exploitations et, par conséquent, mettre le système en péril. Elles sont aussi classées selon deux catégories :

– ***Vulnérabilités physiques :*** liées à l'architecture physique du système, c'est-à-dire les entités et les liaisons utilisés.

– ***Vulnérabilités logiques :*** liées à la partie logicielle du système.

3.2. *Comment peut-on contrôler les vulnérabilités et les perturbations ?*

Pour faire face aux problèmes liés aux vulnérabilités et à ceux causés par des perturbations, on propose un outil de supervision basé sur un tableau de bord. Ce tableau de bord illustre des indicateurs quantitatifs en temps réel permettant d'évaluer à chaque instant l'état des systèmes par rapport aux perturbations.

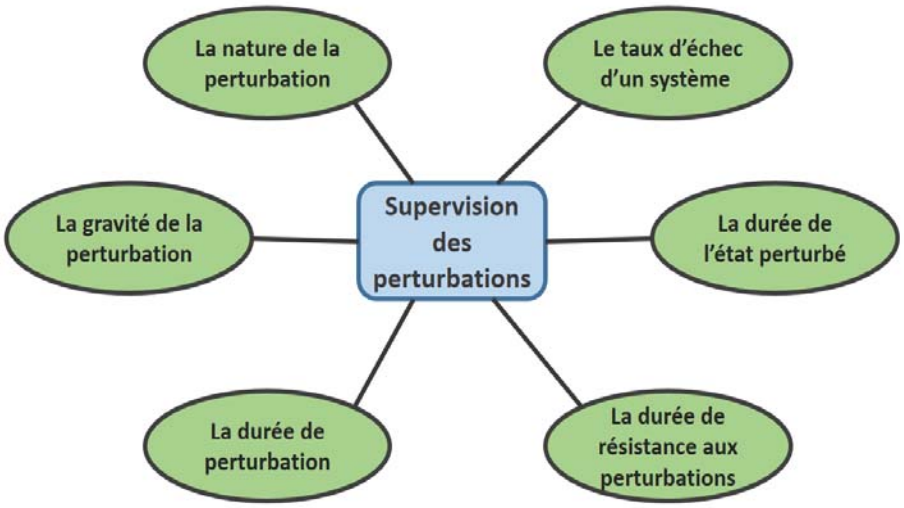

Figure 3. *Les éléments du tableau de bord pour la supervision des perturbations*

Les éléments de ce tableau de bord ne sont pas exhaustifs, ils peuvent varier selon le contexte. Voici la définition de chacun des éléments présentés sur figure 3 :

La nature de la perturbation : permet de définir la source existentielle de la perturbation en question (environnementale, humaine, technique, etc.)

La gravité de la perturbation : représente à quel point la perturbation en question peut nuire au système. Ce point de contrôle nous permet de classifier les perturbations selon leurs degrés de nuisance au système qui les subit. Ce degré de perturbation peut être classifié selon la norme de classification ci-dessous :

a) Une perturbation est baptisée *perturbation de 1er degré* si elle est courte, très faible et ne parvient pas à créer des nuisances au fonctionnement du système.

b) Une perturbation est baptisée *perturbation de 2ème degré* si elle reste faible mais parvient à altérer légèrement le fonctionnement du système pour une durée qui reste courte avant que le système reprenne son état initial.

c) Une perturbation est appelée *perturbation de 3ème* degré si elle arrive à désorganiser significativement le fonctionnement normal du système.

d) Une perturbation est dénommée *perturbation de 4ème* degré si elle cause une interruption au fonctionnement du système et il devient difficile pour lui de revenir à son état initial.

e) Une perturbation est appelée *perturbation de 5ème degré* si elle peut causer une rupture au fonctionnement du système qui lui devient impossible de regagner son état initial.

La durée de perturbation (D_{per}) : la durée globale d'un système pour résister à une perturbation. Ce point de contrôle varie selon le degré de la perturbation et l'état du système :

Pour chaque Perturbation P on associe un intervalle $[T_{min} ; T_{max}]$, avec :

- T_{min}**:** la durée minimale pour un système pour supporter une perturbation.
- T_{max}**:** la durée maximale pour un système pour supporter une perturbation.

La durée de l'état perturbé (T_{DDS}) : la période durant laquelle le système sort de son état initial (cela dépend du degré de la perturbation et de sa durée). Dans certains cas, le T_{DDS} peut-être significativement plus grand que la durée de la perturbation, et cela peut être dû à plusieurs facteurs notamment le degré de la perturbation et la criticité des systèmes subissant cet ébranlement.

Le taux d'échec d'un système : il représente le taux des groupes défaillants au sein du système de systèmes après une perturbation.

FR (%) = N_{NFR}/N_{Total} *** 100 ,** avec :

- N_{NFR} : le nombre des systèmes qui continuent à rester dans leurs états perturbés.
- N_{Total}: le nombre total des systèmes au sein du groupe.

La durée de résistance aux perturbations (D_{RF}) : elle représente la période durant laquelle le système peut résister la perturbation en question. Une perturbation avec un degré élevé et une durée plus grande que la durée D_{RF}, peut provoquer la défaillance d'une partie de système.

Par contre il sera difficile de gérer les vulnérabilités comme les perturbations, car il s'agit de deux éléments différents. Les perturbations sont de nature aléatoire, et pour les gérer, il faut d'abord les identifier, classer, voir le comportement inhérent du système, et finalement, prendre une décision pour protéger le système.

Par contre, les vulnérabilités existent depuis la mise en place du système. Comme certaines d'eux peuvent être prévues dès la phase de la conception, ce qui permet de les corriger avant de construire le système, d'autres peuvent être imprévisible, et ne deviennent identifiables qu'après sa mise en place. Ce qui nécessite un entretien fréquent de l'infrastructure, des entités, des liaisons, des programmes et logiciels du système.

3.3. *Quelle est la contribution de la minimisation du taux d'échec du système et la politique du rétablissement du système après une défaillance dans la protection du système ?*

Le taux d'échec d'un système, comme précédemment défini, représente le nombre des systèmes qui ne peuvent plus revenir à leurs états initiaux et qui peuvent, par conséquent, altérer le comportement normal du système.

Quant à la politique de rétablissement du système, elle consiste à définir des procédures de gestion de défaillance à l'avance, et à préparer des instructions précises pour remédier aux éventuelles défaillances.

Principalement, ces deux aspects sont extrêmement liés et leur contrôle occasionne implicitement la gestion des ressources physiques, ainsi que l'arbitrage de la fiabilité du rendement globale du système.

Pratiquement, cela peut être résolu avec la prolifération des dépendances entre les différentes entités du système, par exemple. L'application de cette théorie permet aux entités du système de multiplier leurs chances de rester en communication même si une ou plusieurs liaisons tombent en panne et de contourner les échecs inhérents des opérations.

Une autre méthode consiste à favoriser la redondance des systèmes. Lorsqu'une entité sorte de son état initial et trouve du mal à se comporter comme prévu, une autre entité dédiée prend le relai, et se met dans l'état initial du système en panne et continue ce que la première est censée faire.

4. Conclusion

Cet article a présenté une méthodologie pour l'analyse de la fiabilité des systèmes de systèmes et le contrôle de la résilience. Comme on l'a expliqué auparavant, notre approche s'appuie sur la gestion des perturbations et les vulnérabilités, sur la définition d'une stratégie de minimisation du taux d'échec du système et sur l'élaboration d'une politique du rétablissement du système après chaque défaillance.

De plus, il a de bonnes chances d'être étendu pour résoudre les problèmes découlant de l'intégration de nouveaux systèmes et de l'élimination des systèmes existants. Comme il est fréquent aux systèmes de systèmes d'être hétérogènes et de supporter l'intégration et le retrait de ses entités tout en gardant un fonctionnement normal.

Bibliographie

[AVE 11] AVEN T., « On Some Recent Definitions and Analysis Frameworks for Risk, Vulnerability, and Resilience », *Risk Analysis*, 31(4), p. 515-522, 15 November 2010.

[FIL 14] FILIPPINI R., SILVAA., « A modeling framework for the resilience analysis of networked systems-of-systems based on functional dependencies », *Reliability Engineering & System Safety*, vol. 125, p. 82-91, 2014

[BUK 16] BUKOWSKI L., « System of systems dependability- Theoretical models and applications examples », *Reliability Engineering and System Safety*, 151, 76–92, 2016.

[EDD 16] Ed-daoui I., Mazri T., Hmina N., « Security Enhancement Architectural Model for IMS based Networks », *Indian Journal of Science and Technology*, Vol 9(46), December 2016.

[KOT 97] Kotov V., « Systems-of-Systems as communicating structures », *Hewlett Packard Computer Systems Laboratory Paper*, HPL-97-124, 1997.

[FIL 15] Filippini R., Silva A., « IRML : An Infrastructure Resilience-Oriented Modeling Language ». IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 45, no 1, p. 157-169, 2015.

[GUA 13] Guariniello C., DeLaurentis D., « Dependency Analysis of System-of-Systems Operational and Development Networks », Procedia Computer Science, 16, 265–274, 2013.

[AOU 15] Aoues Y., Makhloufi A., El Hami A., « A. Optimizing Reliability of Electronic Systems », vol. 2, p. 181-215, 2015.

[EMH 16] Ed-daoui I., Mazri T., Hmina N., « Unveiling Confidentiality-Related Vulnerabilities in an IMS-Based Environment », 5th International Conference on Multimedia Computing and Systems (ICMCS) IEEE, 2016.

[KOE 04] Kharmanda G., Olhoff N., El Hami A., « Optimum Values of Structural Safety Factors for a Predefined Reliability Level with Extension to Multiple Limit States », Structural and Multidisciplinary Optimization, vol. 27, p. 421–434, 2004.

[IED 17] Ed-daoui I., Mazri T., Hmina N., « Towards Reliable IMS-based Networks », LAP LAMBERT Academic Publishing, Germany, 2017.

[CAR 16] Cardon A., Itmi M., « Les Nouveaux Systèmes Autonomes », ISTE Editions, 2016.