A unified failure/damage approach to battle damage regeneration : application to ground military systems

Maxime Monnin, Olivier Sénéchal, Benoît Iung, Pascal Lelan, Michel Garrivet

A UNIFIED FAILURE/DAMAGE APPROACH TO BATTLE DAMAGE REGENERATION : APPLICATION TO GROUND MILITARY SYSTEMS

Maxime Monnin * **Olivier Sénéchal** * **Benoit Iung** **
Pascal Lelan *** **Michel Garrivet** ****

* *University of Valenciennes and Hainaut Cambrésis, LAMIH (UMR 8530), 59313 Valenciennes Cedex 9, France. olivier.senechal@univ-valenciennes.fr maxime.monnin@cran.uhp-nancy.fr*
** *University Henri Poincaré, CRAN (UMR 7039), 54506 Vandoeuvre lès Nancy, France. benoit.iung@cran.uhp-nancy.fr*
*** *DGA, pascal.lelan@dga.defense.gouv.fr*
**** *Giat Industries, m.garrivet@giat-industries.fr*

Abstract: Availability is a determining factor in systems characterization. Because they must act in a hostile environment, military systems are particularly vulnerable in situations of non-availability. Military weapon systems availability can be affected by system failures or by damage to the system, and in either case, system regeneration is needed. However, very few availability studies take battlefield damage into account in their more general dependability studies. This paper takes a look at the issues and trends related to the study of battlefield damage, specifically those related to the modeling of such damage and it proposes a unified approach to regeneration engineering that exploits the parallelism between failure and damage in order to manage system failure and damage to the system.

Keywords: Dependability, Damage, Battlefield Repair, Regeneration Engineering

1. INTRODUCTION

Nowadays, controlling system availability is a determining factor in industry, making dependability an important issue. However, the conditions in which many systems are exploited have become increasingly hostile, with system availability becoming more and more subject to external factors, such as intentional threats, aggressions and/or damage. Applications have already been designed in variety of domains to deal with such external factors (Argirov, 1998; Liu *et al.*, 2004; Papanikolaou and Boulougouris, 1998) and recent dependability studies have begun to emphasize new elements (i.e., vulnerability, survivability and regenerability) in order to take such factors and causes into account (Tarvainen, 2004; Perrin *et al.*, 2001; Levetin and Lisinanski, 2000). It appears that most systems are affected by these new dependability study elements.

Certain systems - like those developed by our industrial partner *Giat Industries* - are more affected than others since they operate in battlefield

conditions [1]. These systems need to be quickly repaired in a hostile environment. Such repairs are referred to as system regeneration (Perrin *et al.*, 2001). Guaranteeing both the level of system availability and the level of system regenerability represents new challenge for system designer and developers. Clearly, taking external threats, system survivability and system regenerability into consideration during the systems dependability analysis brings to light a number of issues. These issues must be handled in the design phase, because they will have a global impact on both the main system and the Logistic Support in the operation phase due to the integrated engineering framework. The most important issues are listed below :

a) To enhance survivability (decrease vulnerability) and to increase accessibility for Logistic Support, the system design must specify a spatially distributed architecture for the equipment (topological aspect).
b) To facilitate regeneration (i.e. Logistic Support supply and decrease system vulnerability) different technologies must be chosen for the assorted equipment (technological aspect).
c) To ensure portability and compensation, the same functions must be performed by different equipment (functional aspect).
d) To validate system design, availability and regenerability assessments must be performed.

Though research specifically on regeneration is scarce, several elements in the list above have been mentioned in previous studies. (Levetin and Lisinanski, 2000) have examined bridge topology as way to enhance system survivability and (Liu *et al.*, 2004) have studied process migration in Information System survivability. (Papanikolaou and Boulougouris, 1998) have proposed a global design framework intended to enhance survivability. However, most of these researches are related to a specific application and does not deal with failure and damage in a unified way as part of overall system dependability. Thus, this paper proposes a modeling methodology allowing the system regenerability assessment in the dependability framework.
This short introduction highlights the motivating factors behind our study. The rest of the paper is organized as follows. In Section 2, the concept of regeneration is defined and placed within the concept of dependability. In turn, Regeneration Engineering is placed within the context of systems engineering. Section 3 describes our unified approach based on the parallel between failure and damage, which leads to a new type of system modeling. In Section 4, an experimental methodology for system modeling is presented using a qualitative example. Section 5 offers our conclusions and provides prospectives for further work.

2. REGENERATION ENGINEERING

2.1 Dependability, Survivability and Regeneration

System survivability has become a widely-studied system property. Thus, it is first necessary to understand the concept of regeneration in terms of system dependability and survivability. (Perrin *et al.*, 2001) defines regeneration as *Battle Damage Repair (BDR)* :

Essential repair, which may be improvised, carried out rapidly in a battle environment in order to return damaged or disabled equipment to temporary service [2].

From this definition it appears that the goal of regeneration is to give the system at least the temporary capacity to fulfill its mission. A system's regenerability refers to its ability to be regenerated. Exactly what capacities will be restored is not specified. However, the key point of the definition is the reference to battle conditions. Regeneration is carried out during the mission under battle conditions. Regeneration thus deals with the consequences of battle damage, and so must be considered in terms of survivability. Though it is still being debated in the literature, one definition of survivability appears to be generally accepted (Tarvainen, 2004) :

Survivability is the ability of a system to fulfill its mission in a timely manner, in the presence of attacks, failures or accidents.

Though there is no one single definition for survivability, as there is for reliability or availability, system survivability is almost always considered to be a component of dependability. In addition, vulnerability and susceptibility which are often associated with survivability, can be considered as a part of survivability. For industrial applications as described in (Levetin and Lisinanski, 2000) and (Papanikolaou and Boulougouris, 1998), survivability analysis leads to design requirements that enhance system survivability. In these applications, survivability is not connected to the Logistic Support or to the maintenance of the system. In IT systems communities, actions that permit a system to recover capacities (i.e. process migration or software patching), are considered to be a part of survivability (Liu *et al.*, 2004). In addition to achieve survivable architectural designs,

[1] Giat Industries develops systems and equipment to meet the needs of French and foreign armed forces. The group designs, develops and manufactures armored vehicles, weapon systems, and medium-to-large calibre munitions. http://www.giat-industries.fr

[2] (DoD, NATO, STANAG 2418), http://www.dtic.mil/doctrine/jel/doddict/data/b/00694.html

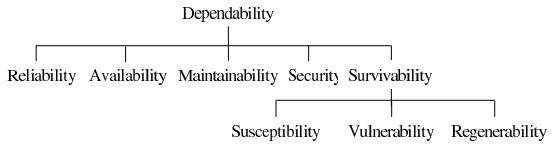

Fig. 1. The concepts of dependability.

IT systems are equipped to perform processes during or after an aggression that will enable them to fulfill their mission. Given such studies, and in light of definition of the regeneration, it would seem that regenerability is a constituent of survivability, and thus of dependability, as illustrated in Figure 1. However, the features of survivability have not yet been well formalized, due to the heterogeneous contribution dedicated to different applications. Obviously, survivability and regenerability contribute to the overall availability and maintainability of a system (Figure 1). To enhance system availability and regenerability, tools and methods must be used in the design phase not only to create a survivable architecture, but also to give the system the ability to be regenerated (the ability to be returned to temporary service). These tools and methods have to be used within the context of system engineering and moreover have to belong to a Regeneration Engineering.

2.2 Regeneration Engineering

Regeneration Engineering (RE) is used to estimate a system's capacity to regain operational capabilities following damage and/or failure. In the context of integrated systems engineering (http://www.incose.org.uk/), RE must be part of the process that defines the main system and must be integrated into the Logistic Support analysis (see Figure 2). The goal of Logistic Support anal-

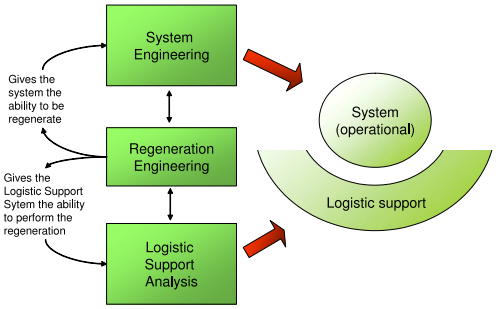

Fig. 2. Regeneration engineering as part of an integrated systems engineering approach.

ysis is to make it possible to maintain the main system in operational condition. Considering the notion of regeneration during the system design phase has a direct impact on Logistic Support. In fact, the results of the regeneration process will not only have repercussions on system design (e.g. technological and architectural choices), but also will on affect the Logistic Support Analysis in terms of supplies, tools, equipment, organization or training. For example, if the regeneration analysis recommends that a component should be located in a specific spot in order to enhance survivability, that recommendation necessarily implies special constraints for Logistic Support (i.e., accessibility). In the same way, if a component must be changed with another more reliable, the supply chain must be reconsidered. Identifying and defining the links that exist between the main system's engineering and the Logistic Support analysis is the goal of regeneration engineering. Within the context of system engineering, RE should become a part of dependability studies in a wide range of domains, particularly for military systems. Given the links that exist between failure, damage, regeneration and maintenance, RE should be defined through a unified approach based on the parallel between failure and damage.

3. A UNIFIED APPROACH FOR THE FAILURE/DAMAGE MODELING

The starting point of this study is the parallel between failure and damage discussed by (Perrin *et al.*, 2001). This parallel summarized in Figure 3 permits a unified approach to handling system regeneration. Damage to the system can be compared to system failure at many points. Thus, system survivability can be analyzed using methods similar to those used for the dependability attributes studies. This unified view of damage and failure is, moreover, quite natural since the two notions are close, even interdependent :

- *close* because both failure analysis and damage analysis can prevent malfunctions and can provide solutions for minimizing unavailability, and
- *interdependent* because the two interact, with system failure sometimes causing damage and damage sometimes leading to system failure.

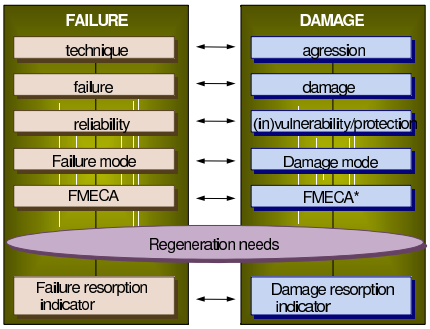

Fig. 3. The Failure/Damage Parallel (Perrin *et al.*, 2001)

3.1 Damage Specificities

Before considering the specificity of damage, two additional definitions are needed to clarify the relationship between damage, aggression and threats. Damage is the result of an aggression against the system, and aggression is the result of a threat. But what constitutes an aggression and what constitutes a threat ? The definitions are given from a compilation of different sources (Perrin *et al.*, 2001; Guzie, 2000; Abbott, 2002) :

A threat is the intentional use of equipment or techniques to prevent a system from accomplishing its intended mission.

An aggression is one expression of a threat which relays the potential effects of the threat. (i.e. aggression = threat/action/impact point/ direction; e.g. :missile/pierce/frame/from the front)

Thus, the main difference between failure and damage comes from the cause of the malfunction. Damage can be *hidden* and *widespread*. It means that components performing different functions but located in the same place in the system can be **simultaneously** affected by an aggression. This phenomenon can be compared with the occurrence of n simultaneous failures, without functional link between the failed components. Therefore, the consequences of damage are difficult to assess due to propagation mode of damage and to the numerous dependencies existing in a system. Few work in the literature are related to this kind of consideration. Furthermore, damage can lead to situations not foreseen within the framework of dependability studies (i.e. destruction of an equipment due to an aggression or in the case of nuclear or bacteriologic attacks which can affect both the system and its Logistic Support). This highlights the difference between an equipment's failed and damaged state, since the loss of equipment due to a technical failure will not have the same consequence in terms of regeneration as that equipment's destruction. Thus, assessing these consequences requires new aspects in the modeling process in which both a structural and functional analysis of the system is needed. Then, damage can have an impact on both the system and its Logistic Support. In order to address the problems raised by these conclusions, the regeneration engineering described above employs a unified approach based on the parallel between failure and damage.

3.2 The Failure/Damage Unified Approach

The relationship between failure and damage shown in Figure 3 led to the unified approach that typifies definition of regeneration engineering. This approach is unified along three different points :

- First of all, our approach to regeneration engineering supports a methodology that allows both failure and damage to be modeled, starting from unified dependability studies. That means a unified view of availability and maintainability that takes both failure and damage into account through an evaluation of survivability.
- Second, it acknowledges the connections between systems engineering, Logistic Support analysis and regeneration engineering.
- Third, it produces results that can be used throughout the system's life cycle. In fact, regeneration engineering is an ongoing process, which begins during system design and continues through system exploitation.

Clearly, considering both damage and failures during system engineering can have a wide impact. To facilitate this integration, we chose to use a modeling approach that combines different models.

4. DAMAGE AND REGENERATION MODELING

The goal of our work is to allow the specificity of damage to be taken into account during system dependability analysis in order to coherently assess the impact of system failure and damage on system availability. As shown above, the specificity of damage implies taking the structural aspects of the system into account. However, the major existing dependability modeling methods do not allow either system structure or damage dynamics to be taken into account and do not assess the impact on Logistic Support. A brief overview of the existing methods is provided below. Two types of dependability analysis methods are generally identified in the literature, (Muppala *et al.*, 2000) :

- the combinatorial methods, whose most current tools are Fault Trees and Reliability Diagrams, and
- the state/space methods that use tools such as Petri Nets, Markov Graphs and Bayesian Networks.

These various dependability analyses have some limitations with respect to the needs of regeneration engineering. Combinatorials methods for instance cannot easily handle complex situations (Sathaye *et al.*, 2000) (e.g. failure/repair dependencies and shared repair facilities). Moreover they do not allow to consider time dependencies (Dutuit *et al.*, 1997). The state/space methods seem more adapted for damage-regeneration modeling since they allow many points of view and time dependencies to be taken into account. In the following, we propose an approach to sys-

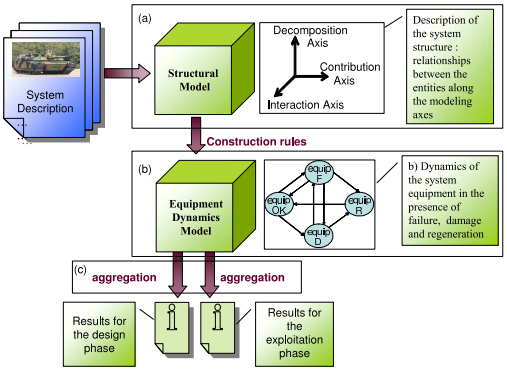

Fig. 4. The modeling approach.

tems modeling able to take the specificity of damage and regeneration into account. This approach combines systemic, state/space and aggregation rules methods to create a model that is appropriate for damage and regeneration assessment.

4.1 An Approach to Damage and Regeneration Modeling : A Behavioral Model

Our approach to regeneration analysis falls within the framework of regeneration engineering and is based on a behavioral model, like many quantitative dependability studies (Rouvroye and van den Bliek, 2002). This model has been designed to allow system availability and regenerability to be evaluated in an operational context that includes failure, damage and regeneration. The model describes the behavior of the system in the face of failure, damage and regeneration. The process follows three steps, and the behavioral model is based on a combination of models (Figure 4) in order to resolve the issues highlighted in the introduction. The first model based on a systemic approach (Donnadieu and Karsky, 2002), is called the *Structural Model*. It provides the structure of the system in terms of the system's topological, functional and technological aspects (cf issues (a) and (b) in the introduction). Moreover, it allows the dependencies linked to availability and regenerability performance to be described in terms of the Logistic Support of the system. From this system description, the construction rules extract information from the Structural Model in order to build the second model, called the *Equipment Dynamics Model*. This second model represents the dynamics of the system equipment using a state/space method. Finally, a set of *Aggregation Rules* combines the Equipment Dynamics Model to the Structural Model to allow the model to move from the equipment level to the system level.

(a) The *Structural Model* is inspired by Tomala's product model (Tomala, 2002). Each primary function of the system is decomposed into different entities : *subfunctions, topological sets, components, characteristic performances (availability, regenerability)*. Each entity is then described according to the different modeling axes : the decomposition axis, the contribution axis and the interaction axis (see Figure 4-a).
These axes define the relationships between entities in order to define the structure of the system (Braesch and Haurat, 1995). For instance, for the mobility function of a ground military system, the relationship between the equipment, "gearbox", and the subfunction, "propel the vehicle", on the contribution axis might be expressed as :

$$\text{"}gearbox\text{"} \in \text{"}propel\ the\ vehicle\text{"}\ with\ 30\% \quad (1)$$

Thus, the structural model provides a static description of the system taking into account functional, technical, topological dependencies.

(b) The *Equipment Dynamics Model* is needed (Figure 4-b) to assess damage and regeneration. Because it is based on the state/space methods, this model has access to their modeling power. Used to describe system behavior at the equipment level, it must take failures, damage and regeneration into account in a unified way. The relationships formalized in the previous model define the Equipment Dynamics Model inputs. Figure 5 represents the principle of a state/space model that take damage, failure and regeneration into account. This model has to adopt new states from common dependability modeling : a damaged state and a regenerated state for taking the difference between failure and damage into account. Moreover, the transitions between these different states must also be reconsidered since the dynamic of damage and regeneration is quite different from failure/maintenance dynamic. Consequently, traditional (λ/μ) transition characterization has to be reconsidered too (since that the equipment dynamic that simultaneously takes failure and damage into account has not yet been defined, the transitions in figure 5 are not labeled).

(c) The *Aggregation Rules* are used to complete the modeling. This model moves the analysis from the equipment level (given by the equipment dynamics model) to the system level, which allows the overall impact on the system availability and regenerability of damage and failure to be estimated. To obtain an evaluation at the system level, the structural model is combined with the dynamic model and with the aggregation rules to provide a *behavioral model* of the system.In other words, the system state is provided by an aggregation of the equipment state, which takes

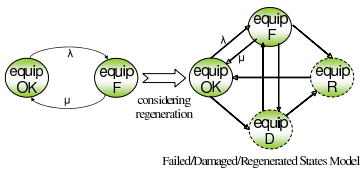

Fig. 5. The Equipment Dynamics Model

into account the different dependencies defined in the structural model (Figure 4-c).
Finally, the behavioral model allows specific missions to be simulated, starting from the definition of a scenario. During the mission, failure and damage are randomly injected into the system, which allows both system availability and regenerability to be assessed in light of the system's failed and/or damaged state. If the level of availability and regenerability do not meet the system requirements, the parameters of the model can be changed to assess another system architecture or regeneration alternative.

5. CONCLUSION

This paper discusses the problem of assessing operational availability in the particular context of military systems. Based on industrial needs, we have defined a regeneration engineering approach that will provide tools for assessing availability and regenerability. We focus on forward-looking modeling damage and regeneration, based on a unified failure/damage approach that allows failure, damage and regeneration to be taken into account simultaneously in the modeling process. Our modeling approach combines a structural model, an equipment dynamics model and aggregation rules to represent the system behavior according to the deployment mechanism of the damage. Ongoing research is related to formalizing the relationships defined in the structural model. At present, the $Unified\ Modeling\ Language^{TM}$ - UML - is investigated in order to support the Structural Model. We plan to investigate state/space methods in terms of the damage/regeneration dynamic at the equipment level. Furthermore, multicriteria analysis will be investigated for the development of the aggregation rules.
Finally, our method, which will be supported by a tool (investigation in progress of market tools), will be applied during the design phase to a weapon system developed by Giat Industries in order to study the feasibility and to improve our approach; results should be obtained in the following two years.

REFERENCES

Abbott, D. et al. (2002). Development and evaluation of sensor concepts for ageless aerospace vehicles. Technical report. NASA, Langley Research Center.

Argirov, J. (1998). Assessment of fire vulnerability for nuclear power plant safety systems by combining fault-and success-oriented logic with physical models. *Reliability Engineering and System Safety* **59**(2), 201–216.

Braesch, C. and A. Haurat (1995). *Systemic modeling in companies.* (in French), Paris : Hermès.

Donnadieu, G. and M. Karsky (2002). *Systemic means Thinking and Acting interms of complexity.* (in French), Editions Liaisons.

Dutuit, Y., E. Chatelet, J-P. Signoret and P. Thomas (1997). Dependability modeling and evaluation by using stochastic petri nets : application to two cases. *Reliability Engineering and System Safety* **55**(2), 117–124.

Guzie, G. (2000). Vulnerability risk assessment. Technical Report ARL-TR-1045. Army Research Laboratory.

Levetin, G. and A. Lisinanski (2000). Survivability maximization for vulnerable multi-state systems with bridge topology. *Reliability engineering and System Safety* **70**(2), 125–140.

Liu, Y., V. B. Mendiratta and Kishor S. Trivedi (2004). Survivability analysis of telephone access network. In: *Proceedings of the 15th IEEE Internationnal Symposium on Software Engineering (ISSRE'04).* Saint Malo, Bretagne, FRANCE.

Muppala, J., R. Fricks and K. S. Trivedi (2000). *Computational Probability.* Chap. Techniques for System Dependability Evaluation, pp. 445–480. Kluwer Academic Publishers.

Papanikolaou, A. and A. Boulougouris (1998). Design aspetcs of survivability of surface naval and merchant ships. In: *Proceedings of the 4th Workshop on Ship Stability.* Memorial Univ. of Newfoundland, St. John's, CANADA.

Perrin, J., P. Esteve and X. Le Vern (2001). Materials battlefield regeneration. Technico-operational prospective study. General Delegation for Armament, (in French, DGA : Délégation Générale pour l'Armement).

Rouvroye, J. L. and E.G. van den Bliek (2002). Comparating safety analysis techniques. *Reliability Engineering and System Safety* **75**(3), 289–294.

Sathaye, A., S. Ramani and K.S. Trivedi (2000). Availability models in practice. In: *Proceeding of Int. Workshop on Fault-Tolerant Control and Computing (FTCC-I).* Seoul, KOREA.

Tarvainen, P. (2004). Survey of the survivability of IT systems. In: *Proceedings of the Ninth Nordic Workshop on Secure IT Systems.* Helsinki, University of Technology. pp. 15–20.

Tomala, F. (2002). Proposition of models and methods for performance evaluation-aid of an innovation from its conception. PhD thesis. (in French), University of Valenciennes and Hainaut Cambrésis (UVHC). Valenciennes, FRANCE.