A methodology for weapon system availability assessment, incorporating failure, damage and regeneration

Maxime Monnin, Benoît Iung, Olivier Sénéchal

A Methodology for Weapon System Availability Assessment, incorporating Failure, Damage and Regeneration

Maxime Monnin [a] Benoit Iung [b] Olivier Sénéchal [a]

[a] *Université de Valenciennes, LAMIH (UMR 8530), 59313 Valenciennes Cedex 9, France. olivier.senechal@univ-valenciennes.fr*

[b] *Nancy Université, CRAN (UMR 7039), 54506 Vandoeuvre lès Nancy, France. maxime.monnin, benoit.iung@cran.uhp-nancy.fr*

Abstract

Availability is a determining factor in systems characterization. Because military systems must act in a hostile environment, they are particularly vulnerable in situations of unavailability. Military weapon systems can become unavailable due to system failures or damage to the system; in both cases, system regeneration is needed to restore availability. However, very few of the general dependability studies, or even the more specific availability studies take battlefield damage into account. This paper aims to define principles for weapon systems modeling that integrate both system failure and system damage, as well as the possibility of regeneration, into operational availability assessment. This modeling method uses a unified failure/damage approach based on state-space modeling.

Key words: Damage, failure, regeneration, availability assessment, Stochastic Activity Networks, Monte Carlo Simulation.

1 Introduction

Nowadays, controlling system availability is a key factor in industry, making dependability important as well. Many systems performing critical missions have to function in hostile environments (Liu *et al.*, 2004), where operational availability can be affected by internal system failures and external factors, such as damage. This is increasingly the case for weapon systems that operate in a battle context (Levitin and Lisnianski, 2003). Accomplishing the mission is thus directly linked to system reliability, vulnerability and regenerability. The last, system regenerability, is defined as the capacity of a system

to recover operational capabilities after failure or damage, and has become a requirement in weapon system design (Campbell and Starbuck, 2005). Traditionally, system dependability has focused on internal causes (i.e., failures), while system survivability has focused on external factors, such as damage to the system, and these two types of studies tend to be considered separately. However, working on system regeneration in order to improve system availability implies assessing the impact of both failure and damage to the system. Research considering both failure and damage is scarce, and as Campbell and Starbuck have mentioned (Campbell and Starbuck, 2005), there are currently no modeling and/or simulation methods that allow the impact of regeneration actions to be assessed dynamically.
To deal with this problem, we previously proposed a unified multi-step failure/damage modeling approach (Monnin *et al.*, 2006), developed in partnership with NEXTER Group, a French weapons systems manufacturer, who must guarantee a certain level of regenerability in all the systems they sell (e.g., Leclerc Main Battle Tanks or the VBCI, a wheeled armored infantry fighting vehicle). According to the System Engineering process, the regenerability potential of new systems must be assessed in the design phase during dependability studies, but tools and methods are still needed for both the modeling and evaluation processes. The originality of our contribution is due to the following aspects :

- The method extends the notion of dependability studies to allow failure, damage and regeneration to be taken into account in a unified way.
- These extended dependability studies are formalized using a static model called *Structural Model*, which provides a structured description of the system based on both reliability and vulnerability analysis, in accordance with the system's mission.
- In order to assess operational availability, a dynamic model is built using the construction rules derived from the Structural Model. This model, based on state-space modeling, is used to define a generic modeling atom representing the dynamic behavior of the component, with aggregation rules allowing movement from the component level to the system level. This dynamic model is then used in simulations to assess system availability.

The first 2 aspects have been already explained in detail in a previous paper (Monnin *et al.*, 2006); the present paper focuses on the third aspect, the dynamic model, which uses simulations based on Stochastic Activity Networks (SAN) modeling. The rest of this paper is structured as follows. Section 2 presents related research in the field of dependability/survivability. Section 3 introduces the principles of our modeling method, which allow failure, damage and regeneration to be taken into account. Finally, in section 4, a example is given in order to show how the modeling process can be supported by stochastic activity networks, and section 5 offers our conclusions and our propositions for future research.

2 Related work

Considering system regeneration in order to improve system availability implies assessing the impact to the system of both failure and damage. In the context of dependability studies, availability depends on system reliability and maintainability. Most dependability studies are based on a probabilistic approach to dependability, which aims to describe system behavior using state-space methods that allow complex behavior to be represented. Typical approaches to modeling availability of systems use Markov chains, (Trivedi *et al.*, 2006) or Petri nets (e.g., the Fault/Error Handling Model (FEHM) - (Trivedi *et al.*, 1987), the Fault/Repair Model (FRM) - (Hein and Goswami, 1996), (Dutuit *et al.*, 1997)) which allow failure/repair behavior to be modeled. More recently, the degradation dynamic in systems that are subject to wear has been more precisely examined in order to assess system dependability when optimizing maintenance operation (Muller *et al.*, 2006). However, these approaches are all based on system reliability and do not consider external factors. External factors can also be taken into account, at least according to the common cause failure concept (*Dependent failure analysis - Special Issue*, 1991). Thought numerous models have been introduced to analyze dependent failures, these studies all consider identical elements (k-out-of-n formulation) and do not account for repair processes. Availability models for weapon systems have been developed by Upadhya and Srinivasan (Upadhya and Srinivasan, 2005), in which battle damage is considered as a serie of specific random events modeled as a discrete probability distribution. Since damage can destroy systems, the physical impact of damage is to some extent taken into account. In fact, the damage that does not destroy the system can be repaired much like a failure. Considering damage as an event that leads to failure means that repair processes, whether in response to failure or damage, are the same. The cause of a component's failure does not change the reality of maintenance activities. In the above scenario, system maintainability is not considered. However, the physical impact of damage on the components makes it essential to consider maintainability criteria (e.g., accessibility, assembly, disassembly, interchangeability, standardization). System survivability measures the impact of both internal causes (i.e., failures) and external factors (Levitin and Lisnianski, 2003; Liu *et al.*, 2004; Campbell and Starbuck, 2005). However, it appears that when the physical impact of damage is introduced into the model (e.g., through component vulnerability), the survivability assessment never suggests repairs (Levitin and Lisnianski, 2003). Repairs (e.g., system recovery) appear to be introduced into the model only when damage is considered as leading to failure (Liu *et al.*, 2004). Though Campbell and Starbuck (Campbell and Starbuck, 2005) do introduce recovery from damage into the survivability assessment in order to ensure the fulfillment of the system's mission, they propose design requirements to enhance system survivability rather than a quantitative assessment. Based on this brief review of the literature,

it would seem that no modeling method currently exists that allows both the functional and physical impact of damage, as well as repair/reconfiguration actions, to be considered in order to ensure that the system's mission is accomplished.
In response to this lack, we propose a modeling method for weapon system availability assessment that considers failure (related to the system reliability) and damage (related to the system vulnerability) jointly in a unified way in order to define regeneration actions. "Technical functions" (related to maintainability criteria) for the system components are introduced to account for the physical impact of damage. Regeneration is defined in terms of the functional/physical impact of failure and damage, with the goal being to allow the system to restore functional capacities in order to fulfill its mission.

3 The Failure, Damage and Regeneration Modeling Atom

The proposed modeling approach is presented in figure 1, (Monnin *et al.*, 2006). The dynamic model is based on a dependability model created using state-space methods. Since this model was designed to allow system behavior to be simulated, the model has to represent the dynamics of the system components as failure, damage and/or regeneration occur. Consequently, the system is described hierarchically as a set of operational functions supported by a components set. Each component in the set also has technical functions related to the possible regeneration actions. The model is based on the assumption that failure only affects operational functions, while damage can affect either operational functions or technical functions or both. Failure and damage are considered as random events that condition the component be-

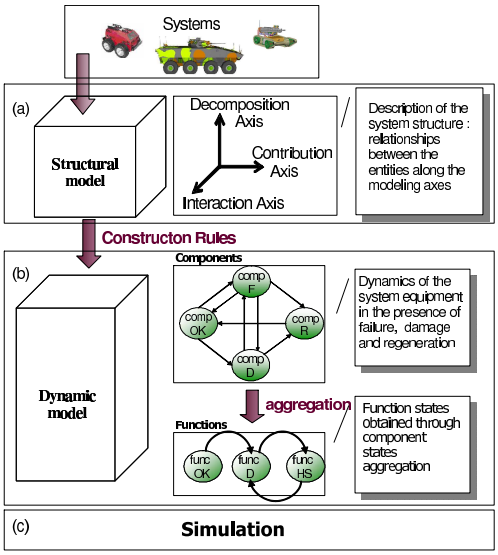

Fig. 1. Modeling approach for the regeneration

havior implying a change of state. Weapon system performance is assessed in terms of its operational functions -namely mobility, fire capability, protection, communication, observation- with each function earning one of 4 state-based performance ratings based on their state : OK, degraded, rescued and failed. Functions are deemed available if they earn an "OK" or "Degraded" rating.

3.1 Impact of failure

Due to the duration of a weapon system mission with respect to the degradation process of most components, we assume that the components can have only 2 states : "OK" or "failed". The "failed" state represents the loss of the operational function. (Remember, a failure does not affect technical functions) The transition between these 2 states is conditioned by the component's failure rate λ which may depend on the system's mission. The failure rate allows the instant of component failure to be calculated, where failure is assumed to follow an exponential law with a constant rate.

3.2 Impact of damage

The dynamic model allows both the functional and the physical impact of damage to be taken into account through operational and technical functions. According to the damage classification proposed in (Guzie, 2000), we assume that 3 kinds of damage can occur. These damages are : (a) damage that affect technical functions, (b) damage that destroy components and (c) damage that affect operational functions. In order to take into account the different ways a component can be damaged, we introduce new states related to the occurrence of damage. A "deteriorated" state linked to the first kind of damage and a "destroyed" state related to the second kind of damage. For the third kind of damage, the "failed" state is equivalent. 3 new random events have to be defined in order to represent the occurrence of damage. Since damage result from an aggression, 3 kinds of aggression are defined : 1. minor aggressions leading to the "deteriorated" state , 2. major aggression leading to the state "destroyed" and 3. *functional* aggression leading to the state "failed". The damage occurrence is calculated according to two probabilities, as explained by (Perrin *et al.*, 2001). An occurrence probability (PA) is first assigned to each class of aggression for a given mission. Then, for each component, an occurrence probability is defined for the 3 kinds of damage. For example, a given mission could be assigned a probability PA = 0.02 of a sniper aggression occurring, and if this aggression did occur, there would be a 0.3 probability that a given component (e.g., episcope) would fall into a "deteriorated" state (i.e., minor aggression) and a 0.7 probability that it would be "destroyed"

(i.e., major aggression).

3.3 Regeneration

In the army, the maintenance function is divided into 3 technical levels, depending on the personnel and equipment involved in the maintenance action. Regeneration takes place on the first level, which corresponds to on-line maintenance of the material. We assume that three kinds of regeneration actions can be performed at this first technical level.
A - Reconfiguration : this process is a response to error during an operating phase and consists of reorganizing both the material structure and its control to allow the system to continue its mission after an error occurs (Toguyéni *et al.*, 2003). This definition can be extended to apply to either failure or damage. The reconfiguration process uses at least 2 components : a component that is in an "OK" state and a component that has been affected by failure or damage. The goal of reconfiguration is to automatically replace the failed component by the "OK" component, which is able to function correctly, in order to restore the operational function affected by the damage or failure. Components that are reconfigurable are able to perform both the operational function for which the component was designed and a reconfigured function, or they are able to perform just one or the other function (i.e., operational or reconfigured).
B - Reparation : this process corresponds to the palliative maintenance activities that permit a temporary return to service, though in a degraded state. Reparation implies being able to access to the component and depends on the current state of the component. In other words, repairs can only be done after damage or failure has provoked a "failed" or "deteriorated" state. A component that has been "destroyed" is assumed to be inaccessible from the maintainability point of view. After being repaired, the component enters into a new state, called "regenerated".
C - Replacement : in this process, the component is replaced with component from an on-board stock or from a logistical support team. From the point of view of maintainability, this regeneration action requires disassembly and reassembly. A replacement cannot be effected when a component is in a "deteriorated" or "destroyed" state because the technical functions of the

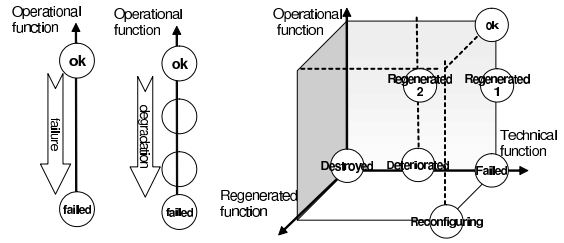

Fig. 2. Towards a damage and regeneration modeling

component have been affected. The regeneration action of replacement allows the component to move from a "failed" state to an "OK" state.
Thus, as shown in figure 2, this unified approach, with its parallel consideration of failure and damage, allows traditional dependability models to be extended by integrating new damage and regeneration states into the model. The different states related to component behavior are represented along 3 functional axes : axis 1 corresponds to the component's operational function, axis 2 corresponds to the component's technical functions, and axis 3 corresponds to the regenerated function (in the case of reconfiguration).

4 Stochastic Activity Network modeling

4.1 System modeling

We use Stochastic Activity Networks (SAN) (Sanders and Meyer, 2001) in our modeling approach. SAN models are a stochastic generalization of Petri Nets and are more flexible than most other stochastic Petri Nets extensions, including Stochastic Petri Nets (SPNs) and Generalized Stochastic Petri Nets (GSPNs) (Azgomi and Movaghar, 2005). Structurally, SAN are composed of activities, places, input gates and output gates. Input gates are used to enable the activities, allowing complex dependent behavior to be modeled. Our models were developed with Möbius (Deavours *et al.*, 2002), which supports the use

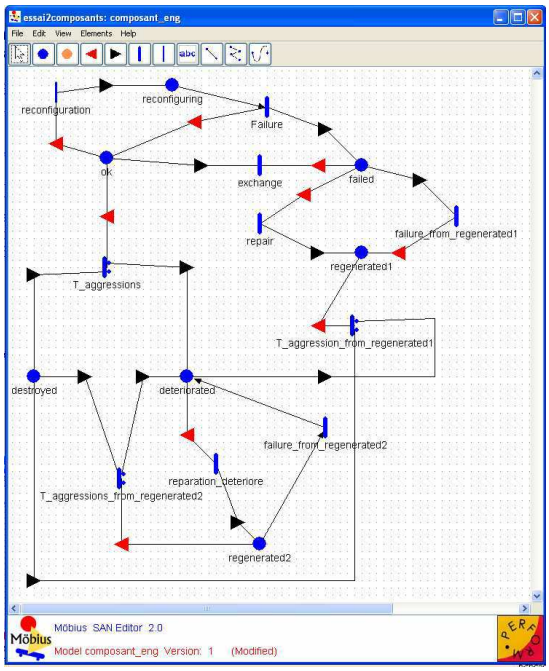

Fig. 3. A SAN model of a component.

of SAN. Möbius integrates the *Joins construct* technique that provides a hierarchical method of combining submodels to form a larger, composed model that is appropriate for describing the system hierarchically. In addition, in order to deal with the non-Markovian nature of the model, simulations are provided from which statistics can be obtained. An example of a SAN model of a component is shown in figure 3. An activity related to the damaged state is detailed to illustrate the damage mechanism. The occurrence of the aggression and the consequences of the damage (i.e., a "deteriorated" or "destroyed" state) are randomly defined as follows :

- The class of aggression that will occur, given a uniform random instance of enemy fire, is determined. This firing action is compared to the probability PA defined for each aggression class in the mission description.
- The occurrence time of the aggression ($T - occurrence - AG$) is calculated as the product of the mission length times multiplied by a random number, according to a uniform distribution. It represents the deterministic delay related to the timed activity corresponding the aggression.
- The Möbius tool allows the probability of an activity conflict to be defined, which allows the probability of the aggression consequence defined in the DMEA (cf. 3.2) to be set.

Transitions related to the regeneration actions are defined as deterministic delays, which means that, for instance, different logistical delays can be considered. Depending on the component set that support an operational function, the corresponding generic behavioral component models (figure 3) can be composed to describe the behavior of the operational function in terms of the 4 operational states: "OK", "degraded", "rescued" and "failed". The state of the function depends on the components that support it. Thus, in order to deal with the question of aggregation, we defined aggregation rules to describe the state of the operational function, given the state of each component that supports the function. For each state of the function, a combinatorial equation (figure 4) using *and* and *or* operators is written and used to compute a performance variable related to the sojourn time in the function state. This performance variable is a reward rate that permits the sojourn time to be

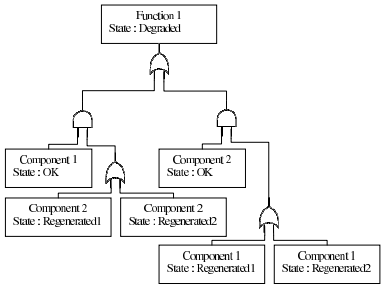

Fig. 4. Example of aggregation rule (i.e., a combinatorial equation defining the function state - "Degraded")

Table 1
Simulation results.

State	Sojourn Time	
	with regeneration	without regeneration
OK	1.3895625430E02	1.5495570331E02
Degraded	1.2931114761E02	0.0000000000E00
Rescued	9.1122106818E01	0.0000000000E00
Failed	1.4061049127E02	3.4504429669E02

evaluated.

4.2 Results

Two simulations were completed in order to show the effects of regeneration on the availability function for a simple case. The regenerated component states allow the function to be moved from the "failed" state to the "rescued" or "degraded" state.
The first simulation was designed to enable regeneration. To this end, repair activities were enabled for all "failed" and "deteriorated" component states. Another simulation was designed to disable regeneration by disabling repair activities. The different sojourn times for the function states are reported in the table 1 for a 500 time units (TU) simulation. From these results, operational function availability in case with no regeneration is about 30% of the mission length (500 TU). In cases in which regeneration is possible, the "degraded" and "rescued" state are attainable. Since the "degraded" state is considered as a functional state, the related operational availability function is about 53% of the mission length. The results obtained with this model show how regeneration can improve the operational availability function by allowing the function to move from a failed state to a functional state. As this research is still in progress, reconfiguration actions, which are the most interesting for System of Systems, were not implemented during these simulations. The 2-component model represents a first step towards a complete model of a system of systems (SoS) with about 10 systems (50 operational functions supported by 200 components). The final SoS model will allow us to assess the impact on availability of both regeneration (related to the system design) and SoS architecture (related to the system operation).

5 Conclusion

This paper discusses the problem of assessing operational availability in the particular context of military systems, where availability is affected by both failure and damage, and regeneration is needed to improve mission accomplishment rates. We have shown how a unified consideration of damage and failure can be used to represent component behavior in a modeling approach that considers failure and damage as random events. This model also permits regeneration to be taken into account. This approach defines new states and uses aggregation rules to define the operational function's performance according to its state. The SAN formalism was chosen for the actual model, both because of its modeling power and the fact that it permits simulations of complex systems and realistic component behaviors. The feasibility of the approach was demonstrated through the use of the Möbius tool, with which encouraging results were obtained. Further models are still under development. Since our partner, the NEXTER group, has already developed reliability and availability models using the STATEMATE® tool, we are currently developing a benchmark in order to validate our simulation results for "OK/failed" behavior. Moreover, to demonstrate the advantages of regeneration for future military SoS architectures, a demonstrator must be developed for NEXTER (the system designer and manufacturer) and the DGA (the system user) since they represent the end-user of our approach.

Acknowledgements

This research is supported by a grant from the French Military Procurement Agency (DGA).

References

Azgomi, A. and A. Movaghar (2005). Hierarchical stochastic activity networks :formal definitions and behavior. *International Journal of Simulation Systems, Science & Technology* **6**(1-2), 56–66.

Campbell, C. B. and D. W. Starbuck (2005). Methodology for predicting recoverability. In: *ASNE Reconfiguration and Survivability Symposium 2005 (RS 2005)*. Jacksonville/Mayport Area.

Deavours, D.D., G. Clark, T. Courtney, D. Dalys, S. Derisavi, J.M. Doyle, W.H. Sanders and P.g. Webster (2002). The möbius framework and its implementation. *IEEE Trans. On Soft. Eng.* **28**(10), 956–969.

Dependent failure analysis - Special Issue (1991). *Reliability Engineering and System Safety*.

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.

Hein, A. and KK Goswami (1996). Conjoint simulation-a technique for the combined performance anddependability analysis of large-scale computer systems. In: *Proc. of IEEE International Computer Performance and Dependability Symposium*. pp. 68–77.

Levitin, G. and A. Lisnianski (2003). Optimizing survivability of vulnerable series-parallel multi-state systems. *Reliability engineering and System Safety* **79**(3), 329–331.

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

Monnin, M., O. Senechal, B. Iung, P. Lelan and M. Garrivet (2006). A unified failure/damage approach to battle damage regeneration : Application to ground military systems. In: *Proc. of the 6th IFAC SAFEPROCESS 2006*. IFAC. Beijing, P R. CHINA. pp. 379 – 384.

Muller, Alexandre, Marie-Christine Suhner and Benoît Iung (2006). Formalisation of a new prognosis model for supporting proactive maintenance implementation on industrial system. *Reliability Engineering & System Safety*.

Perrin, J., P. Esteve and X. Le Vern (2001). Régénération des matériels au combat. Etude technico-opérationnelle. Délégation Générale pour l'Armemant (DGA).

Sanders, W.H. and J.F. Meyer (2001). Stochastic Activity Networks: Formal Definitions and Concepts. *Lecture Notes in Computer Science* **2090**, 315–343.

Toguyéni, A., P. Berruet and E. Craye (2003). Models and algorithms for failure diagnosis and recovery in fmss. *The International Journal of Flexible Manufacturing Systems* **15**, 57–85.

Trivedi, K. S., R. Vasireddy, D. Trindade, S. Nathan and Rick Castro (2006). Modeling high availability systems. In: *Pacific Rim Dependability Conference, PRDC*.

Trivedi, K.S., S. Bavuso, J.B. Dugan, R. Rothmann and W.E. Smith (1987). Analysis of fault-tolerant architectures using harp. *IEEE Transactions on Rliability* **36**(2), 176–185.

Upadhya, K. S. and N. K. Srinivasan (2005). System simulation for availability of weapon systems under various missions. *Systems Engineering* **8**(4), 309–322.