Dynamic model for assessing impact of regeneration actions on system availability: application to weapon systems

Maxime Monnin, Benoît Iung, Olivier Sénéchal, Pascal Lelan

Dynamic Model for Assessing Impact of Regeneration Actions on System Availability: Application to Weapon Systems

Maxime Monnin, LAMIH, University of Valenciennes
Benoit Iung, PhD, CRAN, Nancy University
Olivier Sénéchal, PhD, LAMIH, University of Valenciennes
Pascal Lelan, PhD, DGA (French Procurement Agency)

Key Words: failure, damage, regeneration, availability assessment, stochastic activity networks, Monte Carlo simulations

SUMMARY & CONCLUSIONS

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.

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 [1], 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 [2]. 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 [3]. 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 [3], 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 [4], 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 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 introduces the principles of our modeling method, which allow failure, damage and regeneration to be taken into account. In section 3 an example is given in order to show how the modeling process can be supported by stochastic activity networks. Finally in section 4 results of simulations are presented and section 5 offers our conclusions and our propositions for future research.

Nomenclature

CDF	Cumulative Distribution Function
DGA	French Military Procurement Agency (Délégation Générale pour l'Armement)
SAN	Stochastic Activity Network
SoS	System of Systems
UML	Unified Modeling Language
λ (h^{-1})	Mean Failure rate
P(hit)	For a given aggression, probability for a component of being hit
P(destroyed)	For a given aggression, probability for a component of being destroyed if it is hit
P(deteriorated)	For a given aggression, probability for a component of being destroyed if it is hit

2 MODELING METHOD FOR THE REGENERATION ENGINEERING

The proposed modeling approach is presented in Figure 1 [4].

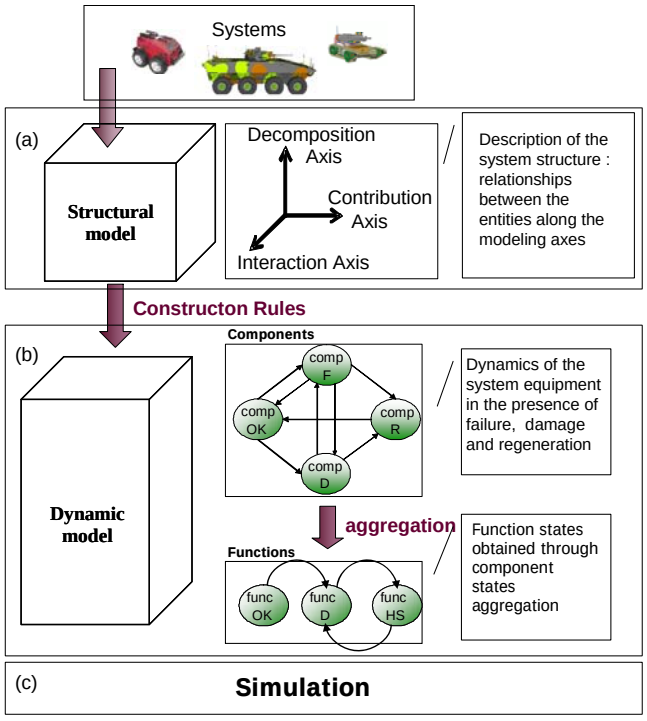

Figure 1 - Modeling approach for the regeneration

The global method is based upon 3 modeling steps. First, we define a structural model that relies on System Engineering principles (Figure 1 – a). The system is viewed as a global entity composed of component that support the system functions and these system's functions are designed in order to fulfill the system's mission. To formalize this knowledge 3 modeling axis allow defining relationships between the component, the function and the mission. Each entity (i.e. component, function, mission), is first described according to the decomposition axis. The interaction axis is related to the system dependencies, for instance, topological relationships between the components are defined in order to formalize the component location that is mandatory for the damage propagation modeling. The contribution axis formalizes relationships between the entities:

- Components that support the functions,
- Functions that ensure the mission
- Mission that impact component.

For instance the contribution relationships of the mission to the components allow accounting for the system vulnerabilities. In each component is linked to the mission according to its vulnerability probabilities for a particular threat. UML class diagrams are used to support the structural model. Figure 2 gives a conceptual representation of the structural model. From this conceptual model, class diagrams are refined in order to represent each relationship for a database generation.

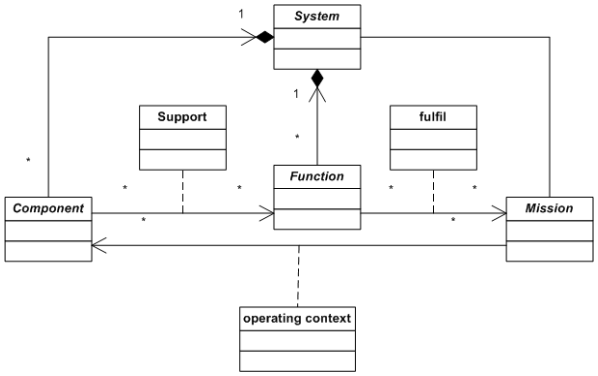

Figure 2 – UML Class diagram of the conceptual view of the structural model

The second step is devoted to the construction of the dynamic model (Figure 1 - b). This model allows system behavior to be simulated by representing the dynamics of the system components as failure, damage and/or regeneration occur. The model is based on the assumption that failure only affects operational functions (functions that the component was designed for), while damage can affect either operational functions or technical functions or both. Technical functions are related to the component maintainability criteria such as accessibility, disassembly, that allow considering the physical impact of damage for the system regeneration. Classical availability models had been extended by incorporating damage mechanism. In addition to failure event that leads to the failed state, we consider that aggressions lead to damaged states. In accordance with theses assumptions, a generic modeling atom for the component behavior as been proposed and justified in previous work [5]. This atom allows accounting for:

- Component failure (failed state)
- Component damage (deteriorated - destroyed states)
- Component regeneration (reconfiguring - regenerated1 - regenerated2 states).
    - From a conceptual point of view, the modeling atom is represented by a state graph where the set of nodes *e* correspond to the different states: *e* = {ok, failed, deteriorated, destroyed, reconfiguring, regenerated1,

regenerated2}, and the arcs represent events implying changes of states (such as failure, aggression or regeneration actions).

- As the mission fulfillment relies on the system operational performances, a generic modeling atom for the system operational function has also been discussed in [5].

Each function earning one of 4 performance ratings based on their state: {ok, degraded, rescued, failed}. Functions are deemed available for the mission if they earn an "ok" or "degraded" rating. Finally, to deal with the hierarchical description of the system, aggregation rules are defined to account for the contribution relationships between components and functions. Moreover these aggregation rules are used to determine the current state of the function according to the current state of each of the components that support it. In other words, each function state corresponds to a particular combinatorial equation of the component states.

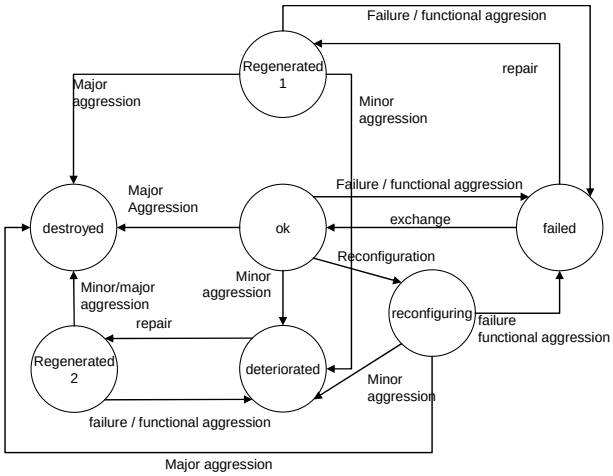

Figure 3 – Conceptual component modeling atom

According to the event tree formalism an example of aggregation rule is given in Figure 4. In this example the "degraded" state of a function supporter by 2 components is specified.

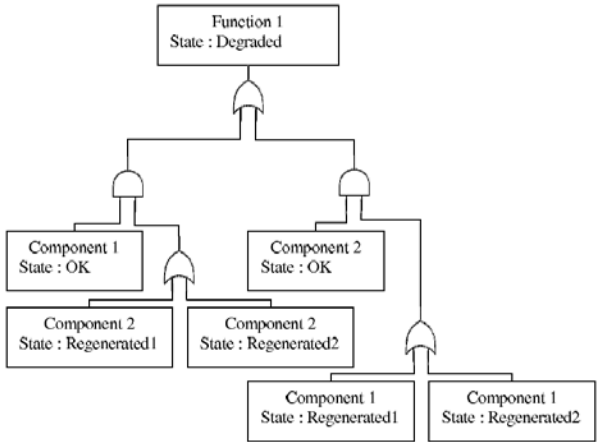

Figure 4 – Example of aggregation rule

Failure and damage are considered as random events while regeneration actions are modeled by deterministic delays. Failures follow an exponential law with a constant rate λ and discrete probability distributions are used to model damage and aggressions [6]. To deal with the non-markovian nature of the model [5], simulations are used to support the model evaluation phase of the method (Figure 1 - c).

3 *STOCHASTIC ACTIVITY NETWORK MODELING FOR THE REGENERATION ENGINEERING*

We use Stochastic Activity Networks (SAN) [7] 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 and Generalized Stochastic Petri Nets. Structurally, SAN are composed of activities, places, input gates and output gates (Figure 5).

Input gates are used to enable the activities, allowing complex dependent behavior to be modeled. Our models were developed with Möbius [8], which supports the use of SAN. Mobius integrates a *Joins construct* technique that provides a hierarchical method for combining submodels to form a larger, composed model well-suited to the hierarchical description of the system. In addition, in order to deal with the non-Markovian nature of the model, simulations are provided from which statistics can be obtained. The SAN modeling of weapon system of systems architecture for the regeneration engineering is presented in the rest of the paper along with an application case.

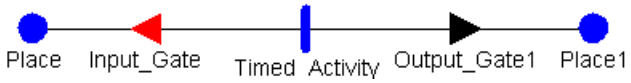

Figure 5 – SAN primitives: place, input gate, output gate, activity

3.1 *Application case*

The modeling approach proposed in this paper had been develop to support the regeneration engineering. To demonstrate the feasibility of this approach it has been applied to a weapon system of systems architecture defined by the French Procurement Agency (DGA) in partnership with NEXTER group. The process followed is presented Figure 6.

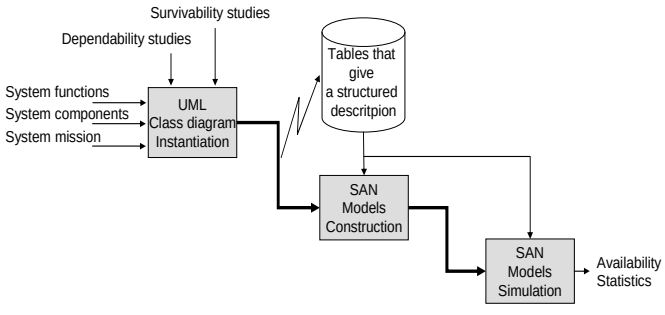

Figure 6 –Application of the modeling method

This architecture is built around an *investigation operational*

scenario. The goal of this mission is to identify a particular enemy position. The architecture is given in Figure 7.

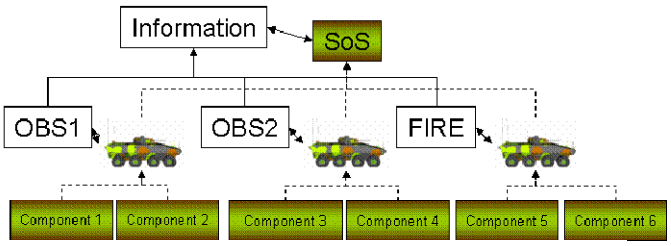

Figure 7 – System of Systems Architecture

Each plat-form has its own operational function, namely Observation1 (OBS1), Observation2 (OBS2), Fire Capacity1 (FIRE). This set of operational is designed to ensure the Information (INF) global function. Equation (1) gives the equivalent and/or equation related to the Reliability Block Diagram of the Information function.

$$INF = OBS1 \wedge OBS2 \wedge FIRE \quad (1)$$

For the purpose of this example, the mission is supposed of 24 hours length. According to the original scenario given by NEXTER Group; only one aggression is supposed to occur with an occurrence probability of 0.8. For each plat-form, the operational function is supported by 2 components. The mission assessment is based on the following assumptions:

- Each operation function is available for the Information function if they earn an "ok" or "degraded" state.
- The mission is successfully accomplished if the information function is available during a minimum of 95% of the mission length (22.8 hours).

The corresponding dynamic model relies on 6 component atomic models and 3 function atomic models.

Regeneration actions as defined in [5] can be exchange, repair or reconfiguration, depending of the current state of the component (e.g. a destroyed component cannot be repair or exchanged due to the physical impact of damage). For this example we define a reconfiguration as regeneration action. The component 5 reconfigure component 4 in case of failure or destruction. This action enables the OBS2 function to move from "failed" to "degraded" state while FIRE function move from "ok" to "degraded" state. The reconfiguration is supposed taking 15 minutes. This duration - as all the numeric values used in this example - is realistic with regard to the mission but does not correspond to real data due to confidentiality.

	λ (h^{-1})	P(hit)	P(deteriorated)	P(destroyed)
1	2.0E-5	0.12	0.2	0.8
2	5.0E-5	0.12	1	0
3	5.0E-5	0.12	0.2	0.8
4	2.0E-5	0.52	1	0
5	1.0E-6	0.06	0.2	0.8
6	2.0E-6	0.06	0.2	0.8

Table 1 – System reliability and vulnerability data

The Table 1 gives the reliability and vulnerability data for the 6 components of the architecture. The contribution relationship between the mission and the component defined by the "operating context" class in the structural model (Figure 2) gives the structure of this table In that way, the structural model gives a framework for the description of the system. This step facilitates the construction of the dynamic model by identifying all the significant parameters for the availability assessment.

3.2 *SAN modeling of the architecture*

According to the use of Möbius, tool and as highlighted by Beaudet [7], the SAN modeling process follow 3 steps that will be applied to our example:

- Construction of SAN atomic models
- Definition of reward variables
- Analysis of the model

For each component of the architecture a SAN atomic model is built according to the conceptual component modeling atom presented in Figure 3. 3 SAN atomic models are defined for the functions. In the function model, copies of the places of the corresponding component models are introduced. These places allow defining the aggregation rules in the different input gates of the function model in order to detail the function behavior. These aggregation rules correspond to a combinatorial equation of the component places marking.

In Figure 8, the OBS1 function model is presented. To finish with the construction of the models we define a composed model (Figure 9) that represents the architecture of the system.

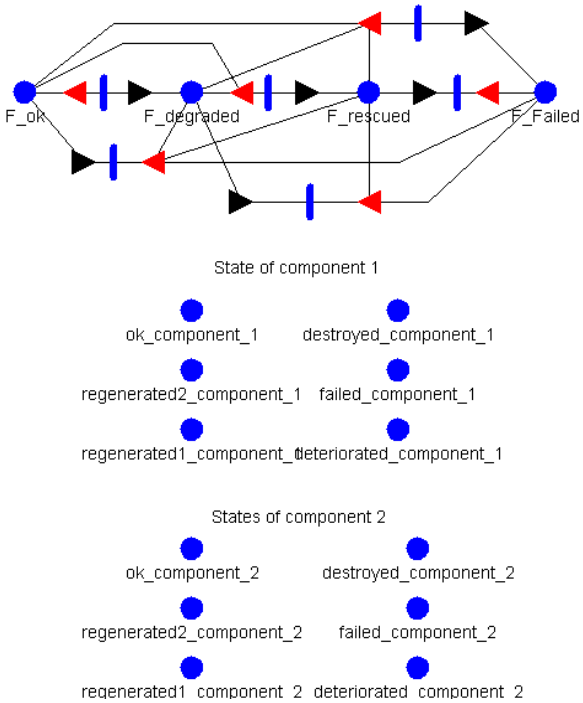

Figure 8 – SAN function model

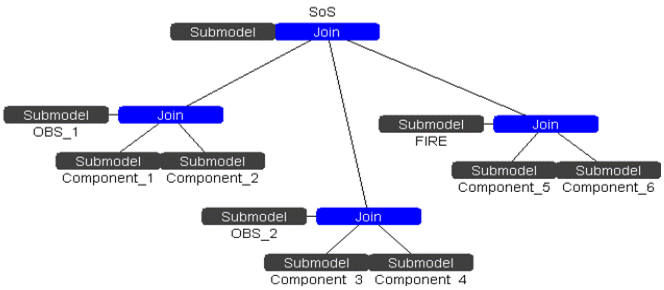

Figure 9 – SAN composed model

This model allows sharing state variables. According to this sharing process the component model places that are copied in the function take the same marking with the component model places. In that way changes of state in the component models rely on the simulated stochastic processes (failure, damage mechanisms) and changes of states in the function model rely on the aggregation rule. The second step of the modeling process aims at defining reward variables. Rewards variables allow computing performance variables from the models, such as availability. They are based on functions that compute a numerical value based on the state of the system. Rewards can be measured at specified time points, over a period of time, or when the system reaches steady state. The specifications for the reward variable definition are defined in the system description. Thus, according to our application case we define a reward variable based on equation 1. This variable will be measured over a 24 time unit period of time according to the mission duration. The corresponding function is presented in Figure 10.

```
if
((OBS_1->F_ok->Mark()==1 ||OBS_1->F_degraded->Mark()==1)
&&
(OBS_2->F_ok->Mark()==1||OBS_2->F_degraded->Mark()==1 )
&&
(FIRE->F_ok->Mark()==1 || FEU->F_degraded>Mark()==1))
return 1;
```

Figure 10 – Availability Reward Variable

4 SIMULATIONS & RESULTS

The final step in the modeling process is to analyze the SAN model in order to evaluate the reward variables and determine the availability performance. Due to the non-markovian nature of the model, Monte Carlo simulations are used to produce statistical estimates of the reward variables. During simulation, the SAN model is repeatedly executed and a new random number sequence is used for each execution to compute a different path through the system with each execution. The reward variables are evaluated for each execution of the system. These reward variable observations are then used to produce the statistical estimates. Simulation is used to produce estimates for the mean and distribution of the expected availability over an interval of time. Three cases have been defined. In the first case, the aggression and the regeneration action were disabled. To show the impact of the aggression, in the second case aggression were enabled. Finally to illustrate regeneration, the third case enables aggression and regeneration to occur.

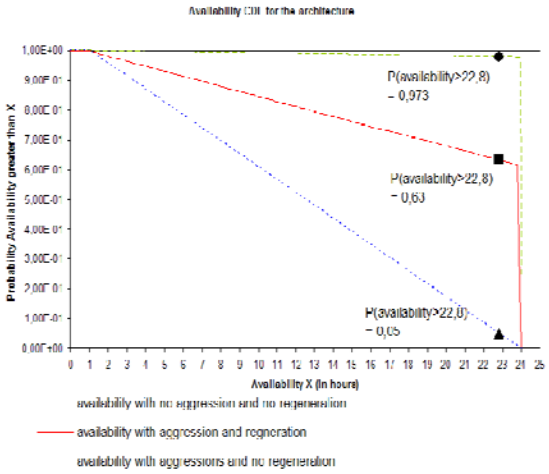

Figure 11 – Availability CDF of the architecture

A plot of cumulative distribution function (CDF) of availability (Figure 11) is used to facilitate the understanding of the availability of the deployed architecture. For each case, the CDF in Figure 11 allows the system producer to evaluate the probability of mission accomplishment according to the corresponding availability. In the example, we can see that there is a 5% probability of achieving the mission in case of no regeneration. Compared with results with no aggression and no regeneration, impact of aggression on system availability can be highlighted. The probability increases to 63 % when regeneration is enabled.

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. The SAN formalism was chosen for the actual models, both because of its modeling power and because simulations of complex systems and realistic component behaviors are allowed. 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 the DGA (the system user) since

they represent the end-user of our approach.

6 ACKNOWLEDGMENT

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

REFERENCES

1. Y. Liu, V. B. Mendiratta, K. S. Trivedi, “Survivability analysis of telephone access network”. In: *Proc. of the 15th IEEE ISSRE'04*, 2004, Saint Malo, Bretagne, FRANCE.
2. G. Levitin, A. Lisnianski, “Optimizing survivability of vulnerable series-parallel multi-state systems”. *Reliability engineering and System Safety*, 79(3), 2003, pp 329-331.
3. C. B. Campbell, D. W. Starbuck, “Methodology for predicting recoverability”. In: *ASNE Reconfiguration and Survivability Symposium 2005*. Mayport Area.
4. M. Monnin, O. Senechal, B. Iung, P. Lelan, M. Garrivet, “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. 2006, pp. 379 - 384.
5. M. Monnin, O. Senechal, B. Iung, “A methodology for weapon system availability assessment, incorporating failure, damage and regeneration” In: Proc. of the *1st IFAC Workshop on Dependable Control of Discrete-event Systems DCDS*, 2007, June 13 – 15, Cachan, FRANCE.
6. K. S. Upadhya, N. K. Srinivasan, “System simulation for availability of weapon systems under various missions”. *Systems Engineering* **8**(4), 2005, pp 309-322.
7. S. T. Beaudet, T. Courtney, W. H. Sanders, “A Behavior-Based Process for Evaluating Availability Achievement Risk Using Stochastic Activity Networks.” *Proceedings of the 52nd Annual Reliability and Maintainability Symposium (RAMS 2006)*, Newport Beach, California, January 23-26, 2006.
8. D.D. Deavours, G. Clark, T. Courtney, D. Dalys, S. Derisavi, J.M. Doyle, W.H. Sanders, P. G. Webster, “The möbius framework and its implementation”. *IEEE Trans. Soft. Eng.* **28**(10), 2002, pp 956-969.

BIOGRAPHIES

Maxime Monnin, PhD student,
LAMIH,
University of Valenciennes,
Le Mont Houy, 59313 Valenciennes Cedex 9, FRANCE

e-mail: maxime.monnin@cran.uhp-nancy.fr

Maxime Monnin received his Master degree in Industrial Automation from the University of Franche-Comté in 2004. Thanks to a grant of the French procurement agency, he starts a Ph. D in the Production System Team at the University of Valenciennes under the supervision of Professor Olivier SENECHAL and Professor Benoît IUNG from the University Henri Poincaré in Nancy. His research interests are modeling issues related to the consideration of failure and damage in a unified way in dependability studies.

Prof. Benoit Iung,
CRAN,
Nancy University,
Vandoeuvre les Nancy BP 239, FRANCE

e-mail: benoit.iung@cran.uhp-nancy.fr

Benoît IUNG is full Professor at the University Henri Poincaré - Nancy I where he is assuming the responsibility of the “Production and Sustainability Engineering” field within the master on “System Engineering”. Since 1988, he has been a researcher at the Nancy Research Centre for Automatic Control (CRAN) where he manages today a research team on Maintenance Decision Making for optimising Productivity and Dependability of Industrial Systems. His research and teaching interests are related to dependability, maintenance and e-maintenance. In relation to this topic, from 1996, he took scientific responsibility for the participation of CRAN in European and International Projects. Benoît Iung has authored more than 65 scientific papers, 15 of them in international journals. Pr. Benoît Iung was elected as French member representative in IFAC TC 4.4. on Low Cost Automation.

Prof. Olivier Sénéchal,
LAMIH,
University of Valenciennes
Le Mont Houy, 59313 Valenciennes Cedex 9, France

e-mail: olivier.senechal@univ-valenciennes.fr

Olivier Sénéchal is a full professor at the University of Valenciennes, where he is in charge of educational programs. He received successively at this same University, his Ph. D. in Production Engineering (1996) and an accreditation to be research supervisor in 2004. He is now a researcher at the LAMIH where his research and teaching interests are related to the impact of dependability on the global performances of manufacturing systems. He is involved in several national projects and groups in relation to dependability area such as the CNRS MACOD working group. Olivier Sénéchal has authored more than 40 scientific papers, 10 of them in international journals.

Pascal Lelan, PhD,
DGA/ETAS
ETAS Route de Laval BP 60036 Montreuil Juigné, 49245 Avrille Cedex, France

e-mail : Pascal.LELAN@dga.defense.gouv.fr

Pascal Lelan is a R&D project manager at the Technical Establishment of Angers ETAS. ETAS is the French organism affiliated to the French Procurement Agency. ETAS is in charge of assessment and experiment of the ground military systems for the French army. The issues handled at the ETAS are related to the mobility, the ergonomics and the dependability of weapons systems.