Diagnostic of the avionic equipment based on dynamic fault tree

Arnaud Lefebvre, Zineb Simeu-Abazi, Jean-Pierre Derain, Mathieu Glade

DIAGNOSTIC OF THE AVIONIC EQUIPMENT BASED ON DYNAMIC FAULT TREE

Arnaud Lefebvre‡, Zineb SIMEU-ABAZI, Jean-Pierre DERAIN‡, Mathieu GLADE‡*

‡ EUROCOPTER
E-mail : arnaud.lefebvre@eurocopter.com,
jean-pierre.derain@eurocopter.com
mathieu.glade@eurocopter.com
*Laboratoire G-SCOP CNRS-INPG/UJF
(Grenoble- Sciences pour la Conception, l'Optimisation et la Production)
E-mail : Zineb.Simeu-Abazi@g-scop.inpg.fr

Abstract

The diagnostic of avionic equipment on aircraft is based on the messages recorded during the flight. For a diagnostic establishment to a maintenance team, these messages are correlated with each others, thanks to specific rules. For example if message A and message B have been registered during the flight, then there are a failure, located on the equipment "n". Most of time, these rules are static, and do not integrate the dynamics of the failure and its implication on time relationship between recorded messages.

Our study is based on the improvement of these rules by integrating the time dependencies between failure messages. The rules have been implemented, thanks to the formalism of dynamic fault tree. Nowadays dynamic fault trees are mostly used to evaluate the reliability of a complex system. Static gates as AND, OR, K-of-M... gates and dynamic gates as PAND, SEQ, FDEP, CSP, HSP, WSP… are used for reliability analysis. Our study is based on the use of dynamic fault tree to isolate all faults occurring on avionic systems. In the proposed approach, three new classes of dynamic gates are defined and an extension of fault tree analysis is developed. These gates are called “temporal sequences”, “duration gates” and “counter gates”.

Key-words

Diagnostic, Avionic, Dynamic Fault Tree, dynamic gates

1. Introduction

In the aeronautical field, maintenance represents the most expensive task in the cycle of life of an aircraft [GLA05]. Then, the outline is the improvement of the availability of the equipment and the optimization of the costs related to their maintenance during all the life cycle. Currently, the avionics part was equipped with self-tests (BIT: Built In Test). The function of these BIT are

present on practically all the electronic parts and enable to deliver an alarm as soon as discordance is observed. The diagnosis of these alarms is treated only when the aircraft is on the ground. There remains then, problems of an ambiguity of localization which gives an additional delay of the maintenance actions and leads to useless maintenance actions such as false disassembling, or needs a long procedures of test to isolate the failure.

To improve the operations of localization, it is thus suitable to add-on the existing system by a part which analyzes on line the results of self-tests. Indeed, when an alarm appears, it must be detected as soon as possible, located and the cause identified. The classical stages of observation and monitoring must be completed by a deductive stage which corresponds to the investigation of the cause: the diagnosis.

The methods of diagnosis used in the various industrial sectors are very varied and take into account the specificity of the materials which constitute their industrial processes [MD98].

The operation of diagnosis is defined as being the identification of the probable failure cause by using a logical reasoning founded on a whole of information given by, an inspection or a control or a test of maintenance (standard AFNOR).

For many simple processes, the relations between the causes and their effects are bi-univocal and the diagnosis by opposite reasoning is simple. On the other hand, for more complex processes [LS01], as for the avionics systems, the diagnosis is possible only by proposing effective techniques which require particular developments. The only way to improve the fault isolation is to take into account the time occurrence of events by a dynamic model. A dynamic model based on fault tree is proposed in this paper. Our study is based on the dynamic fault tree to isolate all faults occurring on avionic systems. In the proposed approach, three new classes of dynamic gates are defined and an extension of fault tree analysis is developed. These gates are called “temporal sequences”, “duration gates” and “counter gates”.

In this paper, we will present at first the problem of diagnosis of avionic equipments. Then, we present at first the principle of dynamic fault tree and we focus on the new proposed gates used in the dynamic fault tree model. Note that, the dynamic gates proposed in section 3 with the extension given in section 4 can be used for any application. A case study by using this new dynamic model will be analyzed in section 5. Finally, results are summarized and conclusions presented.

2. The diagnostic in the aeronautic field

Avionic parts of aircraft are tested thanks to built in test (BIT) embedded on electronic equipments. When a failure occurs, the built in test generate failure messages. These messages are recorded all along the flight in the non volatile memory of the maintenance computer see figure 1.

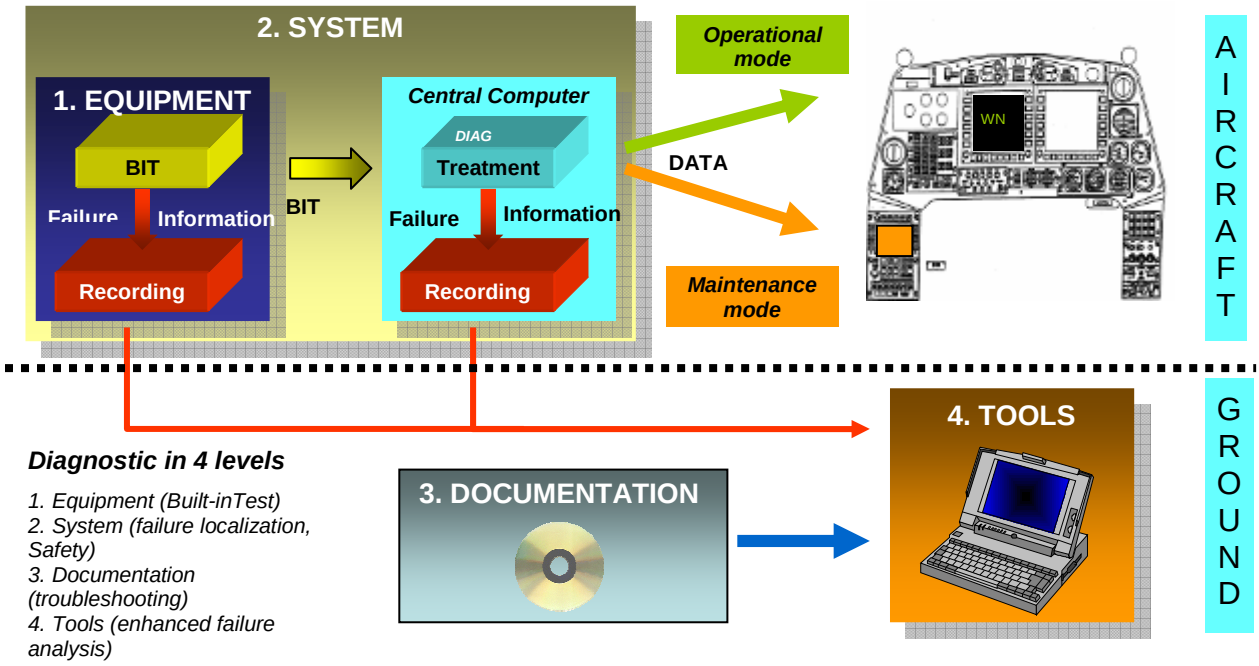

Figure 1 - Current Test and diagnostic concept for avionic failures on a helicopter

The avionic diagnostic consists in interpreting failure messages to provide relevant information:

- In flight, the operational diagnostic is performed to inform the pilot on the state of the functions
- On ground, the maintenance diagnostic is performed to provide information to maintenance team to isolate the failed parts of the aircraft.

These 2 diagnostics do not have exactly the same goals.

The aim of operational diagnostic is to identify the failed function or functional chain. The pilot does not need to know if the failure is located on a LRU but needs to know which function is degraded or failed.

On the other hand, the aim of maintenance diagnostic is to identify the failed equipment. There may be many functions hosted by the same equipment, but the useful information for maintenance

operators is the failed replaceable unit, and not the failed function. When the failed equipment is located then the equipment is replaced. This is called first level of maintenance intervention.
We are interested by the maintenance diagnostic and the isolation of failure on the equipment, called also Line Replace Unit (LRU). Failure treatment is done after the flight, all the data have been acquired during the flight. In this study we are not interested in identifying the relevant parameters to perform a good diagnosis but only in the way to interpret the registered data.
Currently diagnostic algorithm is very different and depends on the helicopter. In order to have diagnostic configuration independent diagnosis, generic rules are established. These rules are generic but inefficiency in isolation performances. Specific rules present better isolation performances but cannot take into account optional and cannot be exported to other helicopters. That's involving a redevelopment of the algorithm for each helicopter version.
The objective of this study is to propose a flexible algorithm based on generic rules or an expert construction of the diagnostic with high-performances in failure detection and localisation gates. In this study we implement temporal dependencies between failure messages, in order to improve failure isolation rates. Thus, we formalise diagnostic rules thanks to dynamic fault tree.
Dynamic fault tree is today used for the reliability analysis linking high level failures to elementary degradations trough static and dynamic gates.

3. Dynamic Fault tree definition

Nowadays dynamic fault trees are mostly used to evaluate the reliability of a complex system [MD98]. Dynamic fault trees integrates static gates as AND gates, OR gates, K-of-M gates and it integrates also dynamic gates as SEQ gates, FDEP gates, PAND gates, and spares gates as CSP, HSP and WSP [MD99]. The use of dynamic gates allows the user to integrate the notion of temporal dependencies between the failures of element and to obtain the reliability of the aircraft.

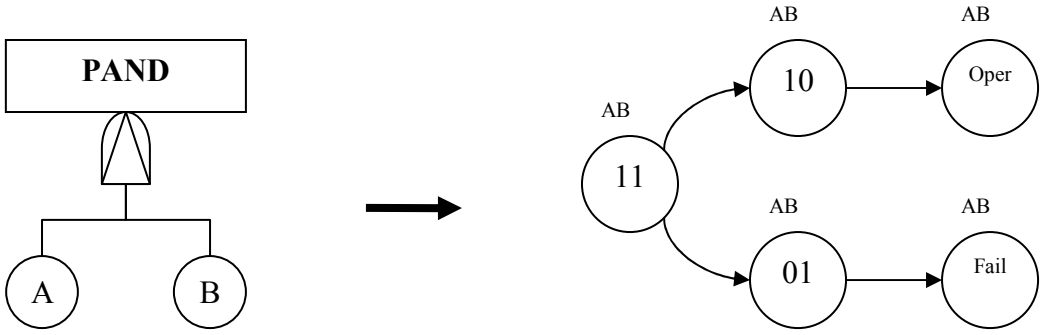

Figure 2: PAND to Markov Chain Translation

PAND gate: It is specified to "Fail" if its inputs fail in left to right order. If they do not fail in order, the subsystem represented by the gate is not "Failed". This behaviour is formalized with the

Markov diagram in Figure 2. We had to distinguish between Failed and Absorbing states. The states marked “Oper” and “Fail” are both absorbing, but in only one is the PAND “Failed”.

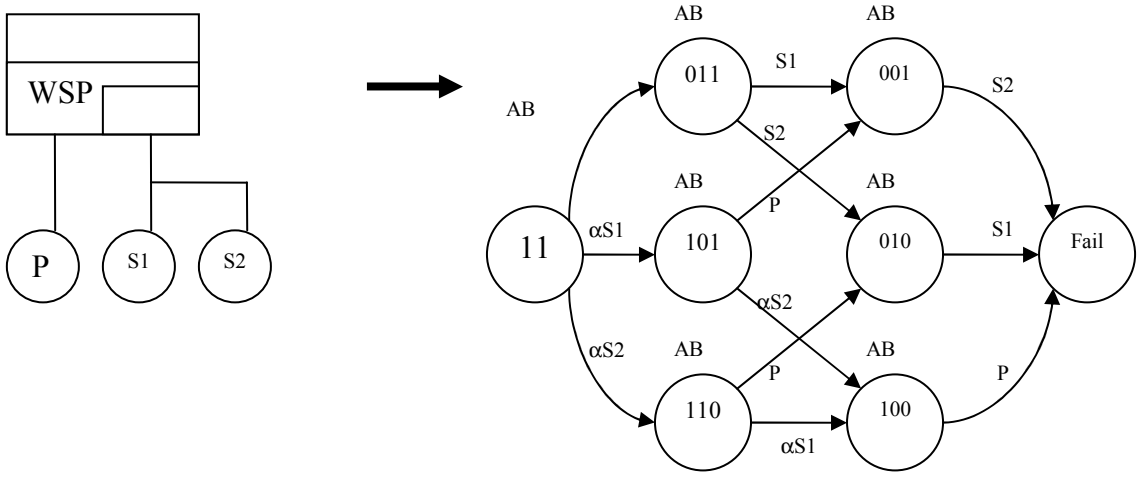

Figure 3: Accounting for Dormancy Factor in Warm Spares

warm spare gates fail at a rate lower than that specified by the rate parameter of the basic event. The attenuation is given by a dormancy factor associated with the basic event. In Figure 3, the dormancy factors for the spare basic events S1 and S2 are marked by α.

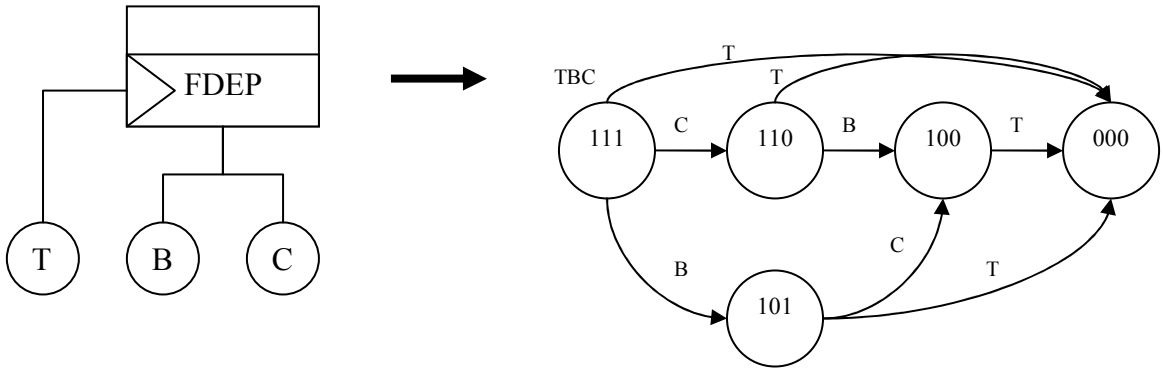

Figure 4: Accounting for Dormancy Factor in Warm Spares

Functional Dependency gates can cause simultaneous failures. This is illustrated in Figure 4 by transitions from states with more than one operational component to the state marked “000”.

A **SEQ** gate asserts that component failures can occur only in the specified order by its inputs.

All these gates have been defined in order to model the dynamic between failure messages [YM99]. In our case, we need to introduce additional gates in order to treat the failure information.

4. Dynamic gates definition extension

The diagnostic problematic in avionic is very specific for the following reasons:

- We are working at system level, and failure messages can be generated by many equipment independent
- Propagation of failure effect can occur, and a failure can generate many failure messages in different equipments.
- Post flight treatment is dependant of data acquired during the flight.

For our example, we are going to consider the following hypothesis:

- If no failure warnings have been recorded, then no failures have occurred on the aircraft.
- If one or more failure warnings have been recorded, then one or more failure may have been occurred on the aircraft.
- A failure message is linked to a begin time and an end time, that is to say, failure messages can disappear during the flight.
- The same failure messages can be generated many time in the same flight, that is to say, failure messages can have an intermittent comportment.
- Every recorded failure messages are timed, and contains intrinsic failure localisation.

From the previous hypothesis, we can conclude that a failure can have the following properties:

- It could be steady or intermittent
- It could be link to a special configuration of the aircraft
- It could be dependent of a flight phase of the aircraft

The relationship between recorded failure messages have to be done in order to give an efficient diagnostic if the intrinsic failure isolation contains a localisation ambiguity or if many failures are generated by a single failure. Hypothesis established have been done in order to propose a model as close as the helicopter functioning.

For these different cases of functioning modes it is necessary to propose new gates. Four specific gates have been developed to take into account diagnostic aspects:

- The Timed PAND denoted by: **t-PAND**
- Duration gate denoted by: **Dur**
- Counter gate denoted by: **Count**
- Occurrence gate denoted by: **Occ**

Timed PAND "t-PAND": This gates as the same functioning than a normal PAND gate but introduce a time dependency between failures in order to do the diagnostic. The first gate is specified to "Fail" if its inputs fail in left to right order and if the time between the failure of A and the failure of B is greater than "t" units of time.

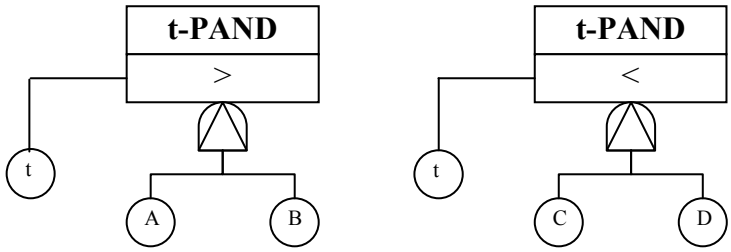

Figure 5: timed-PAND

Duration gate "Dur": In order to take into account the transient failures, the duration gate compares the "duration time of the failure" to a threshold, if it is greater or lower than the specified time, then the transition is valid.

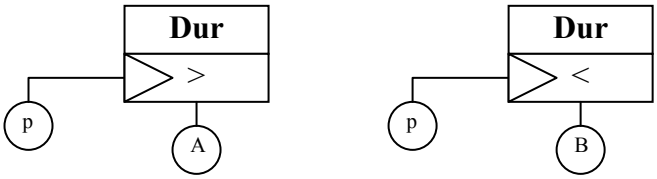

Figure 6: Duration gate

As shown in figure 6, the first gate is specified to "Fail" if its input is considered as failed during a time greater than "p" seconds.

Counter gate "Count": In order to take into account the intermittent failures, the occurrence gate compares the "number of occurrence of the failure message" to a threshold, if it is greater or lower than the specified occurrence number, then the transition is valid.

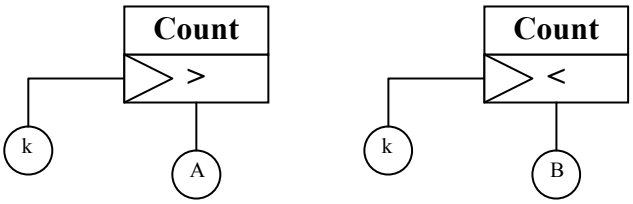

Figure 7: counter gate

As shown in figure 7, the first gate is specified to "Fail" if its input is considered as failed more than "k" times. In order to compare 2 failure messages occurrence, it is necessary to introduce a variant of the counter gate. This gate is specified to "fail" if the occurrence number of the left state is greater, lower or equal to the right state, as shown in figure 8.

Figure 8: Counter gate variant

Occurrence gate "Occ": In order to treat a specific occurrence of the failure, it is necessary to introduce a variant of the occurrence gate named count gate. This is not truly a gate, but it is introduce to treat a specific occurrence of a failure message.

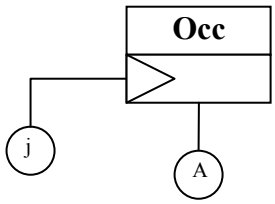

Figure 9: occurrence gate

The occurrence gate allows treating the occurrence "j" of a message A.

5. Application to the diagnostic

Failure propagation phenomenons are typical phenomenon, when a failure occurs it can trigger many integrated tests. One of the major goal of the diagnostic is to correlate the different failure messages and to propose an interpretation of all the registered parameters to the maintenance team.

Typical parameters registered on avionic equipment are built in test messages and parameters coming from the usage of the aircraft and other contextual parameters.

All these messages have to be correlated in order to propose the diagnostic of the aircraft to the maintenance operator.

Today rules established do not take into account the temporal dependency between failure messages, that is to say a failure message generated in the beginning of the flight can be correlate to a failure message generate at the end of the flight. Or the time dependency between failure messages can be a fixed time established a priori.

The goal is to mix static dependency between failure messages and dynamic dependency between failure messages.

A failure can have the following properties:

-It can be dependant of the configuration of the aircraft

-It can be dependant of the flight phase of the aircraft

-It can be permanent, intermittent or transient

To discriminate real failure from spurious one, rules can be established taken into account, the duration of the failure, the number of apparition of the failure message during the flight, the time dependency between failure messages.

Dynamic fault tree allows user to have a clear and rapid comprehension of the algorithm, but the difficulty is on the explosion of use-case that can occur on the algorithm. All the difficulty consists in representing the different cases and to propose simple gates to summarise all the other cases that can occur.

Complementary new-gates:

C-t-PAND is the complementary gate of the timed PAND gate, as illustrated on figure 10.

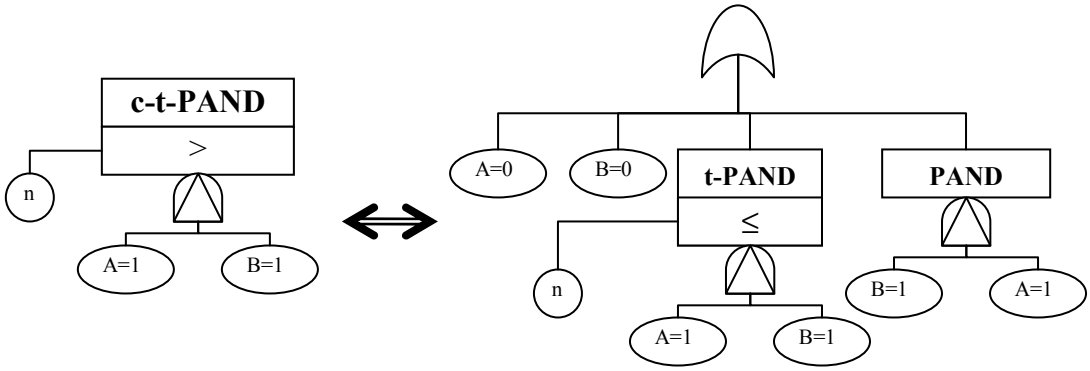

Figure 10: Complementary timed PAND gate

C-Dur is the complementary gate of the duration gate, as illustrated on figure 11.

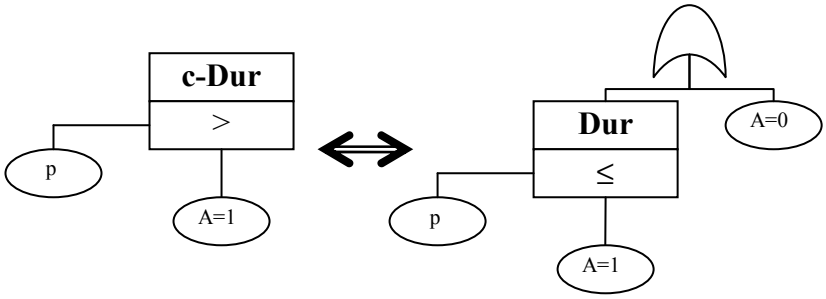

Figure 11: Complementary duration gate

C-count is the complementary gate of the counter gate, as illustrated on figure 12.

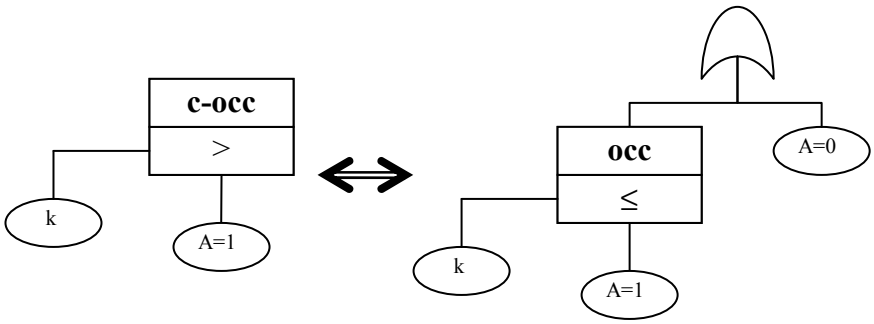

Figure 12: Complementary duration gate

Diagnostic example:

In order to illustrate the diagnostic done, thanks to the dynamic fault tree, an example is proposed on a very simple aircraft.

This aircraft has:

- 2 Configurations named “conf1” and “conf2”
- 2 Flight phases named “ground” and “flight”
- 2 Failure messages named “M1” and “M2”
- 3 Different failures named “failure1”, “failure2”, “failure3”

Failure rules apparition:

Failure1 occurred if failure message M1 appeared during at least 10 seconds, and then failure message M2 appeared during at least 20 seconds. Failure message M2 has to appear before 15 seconds after the message M1 appeared.

Failure2 occurred if the aircraft is in configuration conf1 and message m1 did not appear and message m2 occurred intermittently at least 5 times.

Failure3 occurred if the aircraft is on ground and if failure message m1 appeared or failure message m2 appeared 4 times at the most.

Other cases as considered as spurious failures.

The difficulty to translate the failure rules apparition could be easily solved thanks to the modelling of failure occurrence through dynamic fault tree, as presented on figure 13.

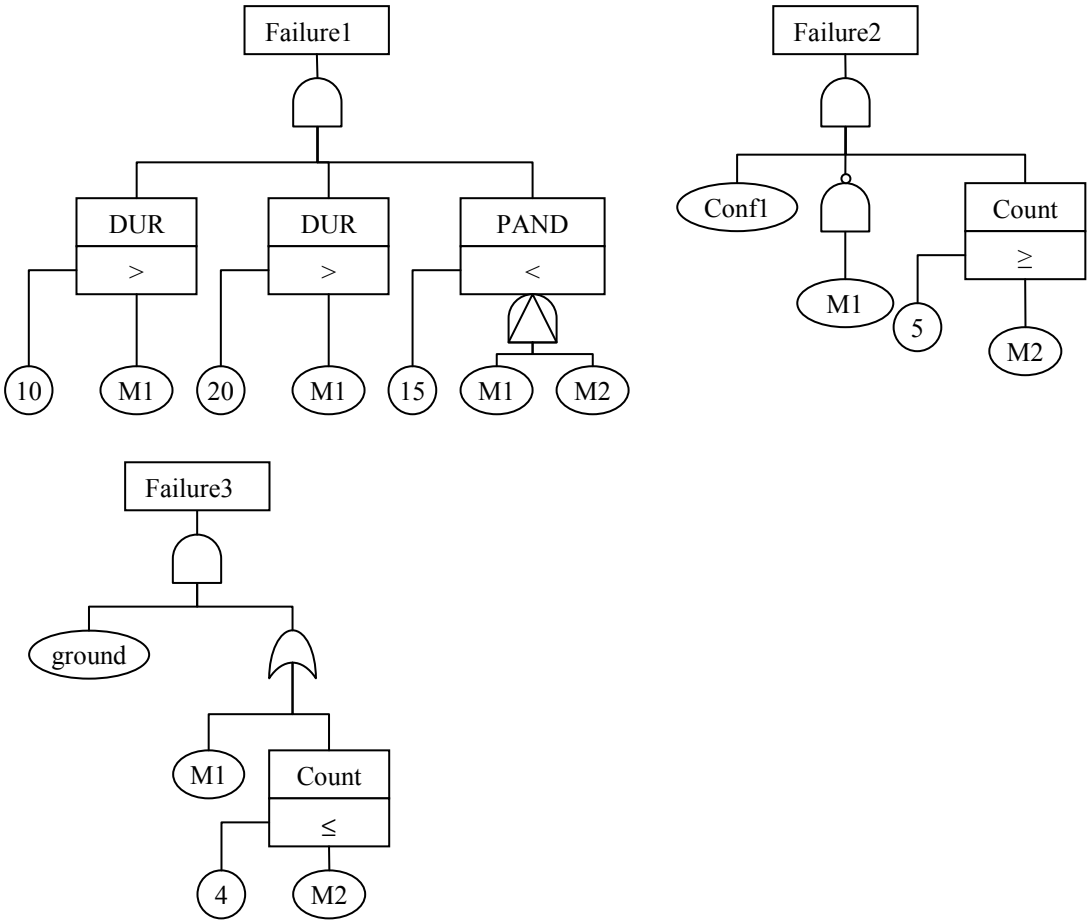

Figure 13: Example of diagnostic thanks to dynamic fault tree

From this example, we can deduce that there are ambiguities in failures in some cases, for example if the failure1 conditions are valid, and the aircraft is on ground and if failure message m2 appeared less than 5 times, then there is an ambiguity between failure1 and failure3.

In some cases, it is impossible to discriminate failure signatures, whether it is acceptable, and the maintenance operator will have an ambiguity of failure localisation or whether it is unacceptable and the failure rules have to be improved by the addition of other conditions.

6. Conclusion

Diagnostic problematic of aircraft avionic is a complicated problematic. In order to improve detection rate, we have introduce the time dependency between failure messages. To represent the dependence between failure messages, it is necessary to use dynamic fault tree as defined in this paper. Hence, to model our problematic, the only way is to define new gates which treat specific failure occurrences. These gates allow modelling almost all required dependencies to establish a robust diagnostic. Nevertheless we are confronted to two problems, the first one is the explosion of diagnostic states, and the second one is to propose a model able to evolve and to take into account experience feedback.

References

[GLA05] Glade M., « Modélisation des coûts de cycle de vie : prévision des coûts de maintenance et de la fiabilité. Application à l'aéronautique ». Thesis, 2005.

[LS01] J. Lunze, J. Schröder, and P. Supavatanakul. *Diagnosis of discrete event systems: the method and an example.* In Proceedings of the Workshop on Principles of Diagnosis, DX'01, pages 111–118, ViaLattea, Italy, 2001.

[MD98] R. Manian, D.W. Coppit, K.J. Sullivan, J.B. Dugan, *Combining Various Solution Techniques for Dynamic Fault Tree Analysis of Computer Systems, 1998*

[MD99] R. Manian, D.W. Coppit, K.J. Sullivan, J.B. Dugan, *Bridging the gap between Fault Tree Analysis Modeling Tools and the system being Modeled*, IEEE 1999 proceedings Annual reliability and maintainability symposium

[YM99] Yao Yiping, Cheng Minghua, *The application on dynamic fault tree analysis for dissimilar fault-tolerant flight control system*, IEEE, 1999