Impact of Operational Reliability Re-assessment during Aircraft Missions

Kossi Tiassou, Karama Kanoun, Mohamed Kaâniche, Christel Seguin, Chris Papadopoulos

Impact of Operational Reliability re-Assessment during Aircraft Missions

Kossi Tiassou
Karama Kanoun
Mohamed Kaâniche
LAAS-CNRS
7, Avenue du Colonel Roche
31077 Toulouse Cedex 4, France
{firstname.lastname}@laas.fr

Christel Seguin
ONERA
2 Avenue Edouard Belin
31055 Toulouse Cedex 4, France
christel.seguin@onera.fr

Chris Papadopoulos
AIRBUS Operations Ltd.
New Filton House
Golf Course Lane, Filton, Bristol, BS99 7AR, United Kingdom
Chris.Papadopoulos@Airbus.com

Abstract— Dependability assessment, by system manufacturer, during aircraft design, based on stochastic modeling, is common practice, but model based operational dependability assessment in the way described in this paper and in real-time is seldom done. Usually, the stochastic assessment addresses aircraft or mission safety, and does not specifically tackle aircraft maintenance during its operation. This paper will address an aircraft mission operational reliability as resulting from component failures, environment changes, and maintenance facilities offered at the various stops involved in the mission. We will show how the on-line assessment of operational reliability will help adjust an aircraft mission, in case of major changes during the mission. The assessment is made possible thanks to the building and validation of a generic dependability model that is easily i) processed for the assignment of an initial mission, and ii) updated during mission accomplishment, following the occurrence of some specific major events. The generic model can be built as early as the design phase, by engineers who are specialist in dependability assessment, based on stochastic processes. Model update and processing, during aircraft operation, can be achieved by operators who are not necessarily familiar with stochastic processes in the way that they are being applied in this research. We will present examples of results that show the valuable role of operational dependability re-assessment during aircraft mission

Keywords: *Aircraft mission reliability, stochastic assessment, dependabity modeling, maintenance, mission planning*

I. INTRODUCTION

Dependability assessment, by systems manufacturers, during aircraft design, based on stochastic modeling, is of common practice. It is very useful for defining an appropriate architecture satisfying the dependability requirements set for a given system. However, currently, during aircraft utilization, the airline companies do not rely on model based dependability assessment approaches such as those described in this paper in a real-time setting. They use pre-defined, deterministic, rules to make decisions concerning aircraft dispatch and mission re-assignment. The aim of our work is to support airline companies to use dependability assessment before and during an aircraft mission, in addition to current means, to assign an aircraft mission or to optimize maintenance operations during an aircraft mission. To this end, we have developed a modeling approach. The preliminary principles and main steps of this approach have been published in [1], [2]. However the results presented in this experience report presenting different examples that illustrate the impact of on-the-fly operational reliability re-assessment on aircraft missions are new and have never been published. This practical experience report is aimed at showing that, even for short-time missions, of the order of one week, integrating new information related to the current system component's states, in the operational reliability model, leads to better updated results, and can help for maintenance decision. The motivation is to use onboard reliability data obtained during flights to obtain updated reliability measures for making mission and reliability decisions. The motivation is to use onboard reliability data observed during flights, or notified by prognosis teams, to obtain updated reliability measures for making mission and reliability decisions. For example, if the reliability measure from an updated model is below a threshold, then the problem (e. g., failed components) must be fixed at one of the next destination airports, before the end of the mission.

It is worth stressing that safety is addressed first. If a single safety requirement is not met or if a safety requirement may be at risk, immediate repair will be obligatory. Maintenance is addressed only when all safety requirements are satisfied and are not at risk.

To the best of our knowledge, aircraft operational reliability assessment on-the-fly has been seldom addressed in the literature. A considerable amount of research efforts have been devoted to modeling operational-phase aircraft or spacecraft dependability and performability, and performability-driven maintenance decisions, without addressing on the-fly dependability assessment (see e.g., [3–6]. Also, several previous studies concentrated on safety aspects (see [7–9] for instance), and most published work on operational reliability addressed design enhancement purpose [10], [11]. In [12], the issues of delays in airline maintenance and safety are investigated. A probabilistic risk analysis model is developed in order to quantify the effect of airlines maintenance policies on their aircrafts operability. A decision support approach to maintenance planning is

presented in [13]. It proposes a method to schedule the repairs taking into account some optimization criteria: cost, remaining useful life and operational risks. The approach proposed does not assess reliability measures, but it uses the reliability as input. In [14], the operational consequences of system failures are studied using event tree analysis. The paper discusses the possible consequences of failures taking into account the flight phase during which they have occurred. A modeling approach based on fault trees of the aircraft is presented in [11], considering only dispatch events without addressing in-flight operational consequences.

[15], [16] address phase mission systems dependability modeling using deterministic duration for the phases. [16] shows that, under some given conditions, the model can be processed using an analytical method. Chew et al. [15] address the problem using the concept of maintenance-free operating periods; the system evolves through a series of phases with no possible maintenance. The developed model is solved by simulation.

Of all the above-mentioned work, none is aimed directly at modeling aircraft operability during mission achievement. The closest works [11], [14] are carried out for long-term operational dependability analysis and are based on event trees and fault trees. Moreover, as far as we are aware, our work is the only one giving re-assessment results.

This experience report addresses aircraft operational reliability using stochastic state-based models. The model is essentially used to evaluate the probability to continue operating until a given period of time, taking into account recent events. The estimated probability will determine whether a corrective action must be initiated or not before the next flights of a mission.

The modeling approach is briefly presented in Section 3, after the presentation of the assessment context and objectives in Section 2. Section 4 illustrates the kind of models that can be built for a subsystem of the aircraft and Section 5 gives examples of assessment results together with their use in real time for this subsystem.

II. ASSESSMENT CONTEXT AND OBJECTIVES

An aircraft mission consists in performing a predefined set of flights under some operating and maintenance conditions. The achievement of the mission is such that each flight is followed by a stop where the aircraft is prepared for the next flight. Adverse situations while operating an aircraft lead to mission (or operational) interruptions resulting in flight delays, flight cancellation, or in-flight turn-back and diversions [11], [14]. Our work is mainly related to operational interruptions caused by system failures and to the inability to perform corrective maintenance within an acceptable time.

At each stop, the aircraft is inspected and the anomalies reported during the previous flight are checked. If a component is found inoperative, a dispatch decision is taken based on the requirements of the next flight. The flight captain and maintainer refer to an approved document (called Minimum Equipment List) where the components are listed with the status Go, Goif or Nogo.

The **Go** status is the case where the aircraft can fly with the component inoperative. It is worth noting that even in this case, attention must be paid to the future behavior of the aircraft since a subsequent failure may prevent dispatch.

For the **Goif** status, the flight can be achieved provided that other equipment are operative and/or some technical (operational or maintenance) procedures are feasible:

- **Goif-o:** Some operational procedures must be carried out or feasible to allow the dispatch. It concerns essentially a limitation in the functionalities that will be available during the flight.
- **Goif-m:** Some maintenance procedures must be carried out. These include time limited dispatch requirements and have an impact on the planned maintenance activities, e.g., the failed component must be repaired within a period of ten days.

The **Nogo** status prevents the aircraft from flying. In this case, the component must be repaired before any flight.

The dispatch is allowed if there is no "Nogo" and if all "Goif" conditions are acceptable. When it is allowed, the flight can be aborted or diverted if the aircraft capability is degraded. Procedures stated in the Flight Crew Operating Manual are used to determine whether the flight must be diverted (or aborted depending on the location) or not.

A. Role of dependability assessment

The aim is to assess, during the aircraft's operations, its ability to satisfy the operational requirements, in the presence of unforeseen events, and initiate corrective action to prevent adverse situations. The assessment is to be used for planning a mission and during its achievement.

To plan a mission, the assessment is used to estimate the period of time during which the aircraft can be operated without reaching an adverse state. This will allow us to determine the kind of mission profile to be assigned.

Once a mission is assigned to the aircraft, the assessment is used during its achievement, both on ground and while in flight, to assess the ability to succeed in continuing on the remaining part of the mission, or re-adapt it if necessary, in case of occurrence of major changes. To do so, the assessment model is updated with the new states of the aircraft and of the environment and is processed again.

During the flight (or on-ground during aircraft inspection), the operational assessment is performed, after the occurrence of (or the detection of) major events that may affect the operability, to provide an indication on the reliability of the remaining part of the mission. The outcome may be used to support the decision, by the operations control centre, to continue the mission or to revise the planned mission.

In case of a decision to divert the flight, the assessment can be used to help determine which of the candidate diversion airports has sufficient facilities to return the aircraft to a dispatch-able state. In case of emergency (due for example, to problems that may affect safety), the assessment can be used once a diversion airport is selected, to re-assess the operational reliability.

Finally, the result may help in selecting the most appropriate maintenance or operation planning actions in order to improve the ability to achieve the whole mission. Hence, different maintenance strategies can be compared considering various alternatives for performing component repairs. The best strategy is then selected based on the estimated probability of mission accomplishment without operational interruption.

B. Major changes to be accounted for

As the system will be continuously monitored, diagnosis and prognosis information will be notifying major changes in the system components' functional state, their failure rates and distributions. For instance, the failure distribution of a computer may be initially following the exponential law and prognosis may denote, during the mission achievement, an increasing likelihood of failure, suggesting a failure distribution that is following a Weibull law. As these changes may affect the predicted mission reliability, the model must be updated with the new failure distribution in order to reevaluate the reliability. We have identified three kinds of major changes that may take place during the achievement of an aircraft mission, summarized hereafter.

C1: Changes in the state of system components: this corresponds to the case where for example a system component has failed during the achievement of the mission (we assume that this failure does not impact safety, otherwise the mission is interrupted). Even though such an event is included in the stochastic model, undertaking new flights may impact the aircraft operability.

C2: Changes in components' failure rates: this mainly concerns the case where new failure rates or distributions have been prognosticated for the system components, during the duration of the mission.

C3: Changes in mission profile. A mission is characterized by the number of flights per day, the number of days, and the duration of each flight. Due to external events such as weather conditions or failures in other aircrafts, the number of flights and flight destinations may change. This may impact the number and duration of flights. Changing the mission profile also implies changes in maintenance facilities available at the various stops (or destinations), as well as in the mean time to repair the failed components or the repair time distribution itself.

Changes of types C1 and C2 are provided by diagnosis and prognostic facilities, while C3 changes are governed by the operational teams of the airline company.

III. MODELING APPROACH

To sum up, our aim is to make possible the assessment of the operational reliability during aircraft missions. Before a mission start, the model will help assign a mission that is in accordance with the states of the aircraft components and with other impacting conditions. After the occurrence of one of the above changes, the operational reliability is re-evaluated to assess the impact of the new conditions on the mission's achievement. In practice, a change results in dependability model update. The global dependability model should thus allow for an easy and efficient model tuning, update and processing. Moreover, as the model is to be used at run-time, the tuning and update of the model should not require the presence of modeling specialists. It should be possible to tune or update the model from outside, without necessitating a deep knowledge of the model.

As a consequence, our approach consists in building and validating a generic dependability model for which the essential operational information can be entered and checked through a dedicated interface. Additionally, model tuning and update should not require the knowledge of the underlying modeling technique and formalism used. Indeed, the generic model, including detailed information about the system components and functions, their interactions, and their stochastic behavior, can only be built by the Original Equipment Manufacturer (OEM), and the Maintenance, repair, and operations (MRO's) , who will not necessarily be involved in model tuning and update in operation.

Our work has thus two complementary, non independent, facets, related respectively to i) the generic dependability model construction by the Original Equipment Manufacturer or the Maintenance, repair, and operations, and to ii) the tuning and update of this generic model by the airlines and the Maintenance, repair, and operations, to adapt it to the current operational conditions. The first facet is dedicated to the definition of a modeling approach, based on stochastic processes, in which some parameters should be tunable from outside. The second facet is more concerned by how to use this model at run-time and how to obtain useful results.

In this experience report we put emphasis on the second facet and show how to use the assessment results during an aircraft mission to manage the mission and its associated maintenance activities.

The approach to tune or update the model consists in setting some configuration files to be updated with the current states of the mission before the processing of the updated model. An Assessment Manager, that is composed of a human operator, assisted by an automatic algorithm to check for consistency, updates the configuration files and initiates model processing after consistency checks. The generic model is then transformed into the operational dependability model, after integration of the information provided in the configuration files. Processing of the operational dependability model provides the Mission Reliability measure. Figure 1 shows the update scenario.

To update the configuration files, the assessment manager relies on i) diagnosis and prognosis modules, that are run and updated at runtime either automatically by mechanisms embedded in the aircraft control systems or by the crew, and on ii) flight plans.

It is worth to mention that updating and processing the model can be performed while the aircraft is still in flight, without waiting for the aircraft to land, in order to obtain as early as possible the new assessment results.

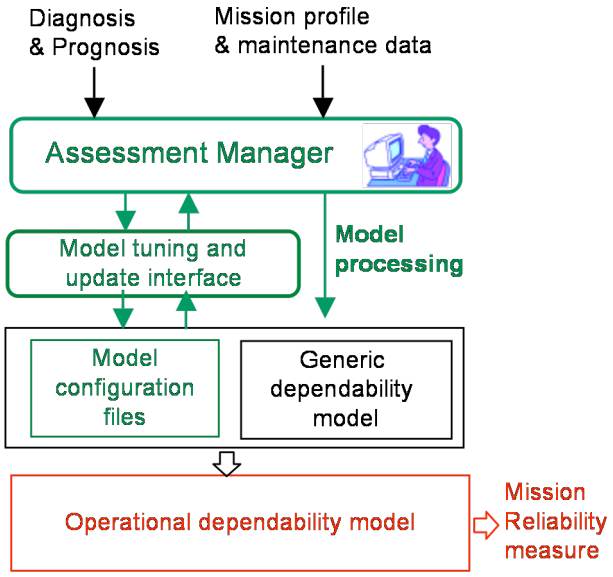

Figure 1: Update of the model

Finally, the model tuning and update interface, should be user-friendly and should not depend on the underlying modeling formalism used in the modeling approach.

It is noteworthy that the rate at which the model should be updated will tightly depend on the operational context and on the rate at which a significant variation of the model parameters is observed. The decision can be taken automatically e.g., when a predefined variation threshold of some model parameters is observed, or at a regular basis (e.g., at the end of each day).

A. Modeling formalism

The generic dependability model can be built using classical dependability modeling formalisms such as Petri Nets and their off-springs, Stochastic Activity Networks (SANs) or AltaRica. The only requirement is that, once the model is built, it can be easily tuned from outside and processed efficiently. For the final usage, the generic and operation reliability models will be based on the AltaRica language [7], [17], [18], and the optimized model-processing module, that is under development, is proprietary. The algorithm for the assessment manager and the model interface are also proprietary and are still under development.

To obtain quick results allowing us to check the validity of the approach, before the end of the implementation of all the proprietary modules, we have used existing tools to build and process the models. The dependability measure assessed is Mission Reliability defined in the next section. We have used on one hand AltaRica and on the other hand the SANs to build and validate the models. It is worth to mention that the two formalisms are equally expressive. The model presented in Section 4 is based on SANs. It has been processed by the Möbius tool [19].

B. Mission Reliability

The aircraft has to fulfill specific dispatch and in-flight requirements to be allowed to fly.

We distinguish:

- the *minimal system requirements* (Min_Sys_Req) that are independent of the mission profile and that must be fulfilled to operate the aircraft whatever the mission.
- the *mission profile requirements* (Mission_Req) that are specific to the mission profile.

The evaluation is based on the fulfillment of these requirements. The objective is to evaluate the probability of occurrence of the adverse events that may lead to an operational interruption. **Operational interruptions** correspond to flight delays, cancellations, in-flight turn-back and diversions. Delays and cancellations occur on ground, while turn-back and diversion occur in flight.

In this paper, we concentrate on **Mission Reliability measure, *MR***, defined as the probability to achieve the mission without an operational interruption. It is evaluated with regard to Min_Sys_Req and Mission_Req in order to determine whether a preventive action is to be initiated or not.

It is worth to mention that model tuning and update concern only Mission_Req. The Min_Sys_Req are taken into account in the generic dependability model.

C. The generic dependability model

In order to facilitate model update, the generic model is structured into two major levels, corresponding respectively to i) the system level (composed of the models of the sub-systems and the Min_Sys_Req), and ii) the mission level (including the description of a mission, with its maintenance facilities at each stop, and the Mission_Req). This is illustrated in the next section.

IV. EXAMPLES OF SUB-SYSTEMS AND OF MODELS

In order to illustrate the results, we have selected an aircraft subsystem, the rudder. It is composed (see Figure 2) of three primary computers (P1, P2, P3), a secondary computer S1, three servo-controls (ServoCtrl_G, ServoCtrl_B and ServoCtrl_Y), a backup control module (BCM) and two backup power supplies (BPS_B and BPS_Y).

The computers are connected to the servo-controls, which move the surface. S1 and P1 are connected to ServoCtrl_G, P2 to ServoCtrl_B, and P3 to ServoCtrl_Y. The connection between a computer and a servo-control forms a control line that can act on the surface. It has four control lines:

- P1 control line (PL1): P1 and ServoCtrl_G
- P2 control line (PL2): P2 and ServoCtrl_B
- P3 control line (PL3): P3 and ServoCtrl_Y
- S1 control line (SL): S1 and ServoCtrl_G.

We have also a Backup control line (BCL), based on BCM, BPS_B, BPS_Y, ServoCtrl_Y and ServoCtrl_B.

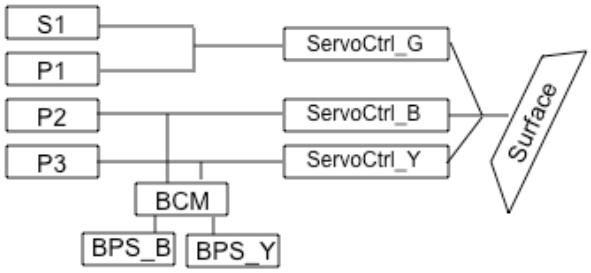

Figure 2: The subsystem structure

Initially S1, the backup control module BCM and the backup power supplies BPS_B and BPS_Y are inhibited, and the surface is controlled by the three primary control lines (PL1, PL2, PL3). When the three primary control lines fail, S1 is activated and the system switches to SL. If the latter also fails, BCM, BPS_B and BPS_Y are activated enabling the backup control line, BCL.

Related Operational Requirements: According to [20] [1], the failure of P2, ServoCtrl_G, ServoCtrl_Y, ServoCtrl_B, BCM, BPS_B or BPS_Y leads to "Nogo" status. P1, P3 and S1 are "Goif" items with "Goif" conditions stated respectively at sections MMEL 27-93-01-1, MMEL 27-93-01-3 and MMEL 27-94-01-1 of the document. The dispatch conditions resulting from these sections are respectively[2]:

- (P1=ok) ∨ (S1=ok ∧ P3=ok);
- (P3=ok) ∨ (S1=ok ∧ P1=ok);
- (S1=ok) ∨ (P1=ok ∧ P2=ok ∧ P3 =ok).

In the three cases, the component must be repaired before 10 days. These conditions form the rudder Min_Sys_Req.

A. Mission and Sub-system modeling

Figure 3 gives a high-level view of the dependability model that is built based on the SAN formalism. We only describe the mission level model and its connection with the system level model. The connection is achieved through the modeling of the minimal system requirements Min-Sys-Req based on the states of PL1, PL2, PL3, SL1 and BCL control lines described in the corresponding submodels. The marking of *Min-Sys-Req fulfillment* place is updated by the firing of the instantaneous activities *Fulfilled* and *Not fulfilled* as a result of a change of the subsystems states. The corresponding conditions are encoded in the input gates *IGN* and *IGFul*. It is noteworthy that in this example, we do not consider specific mission profile requirements that could be associated to each flight.

Considering the mission level sub model, it is composed of two parts. The upper part represents a flight and the lower part represents the activities on ground at a stop. A flight is represented by three phases *Taxing_to_Takeoff*, *In_Flight* and *Landing*. During the *Taxing_to_ Takeoff* the flight can be aborted and it can be diverted during the *In_Flight* phase. The *AbortCondition* and *DiversionCondition* input gates define the conditions for these interruptions to occur.

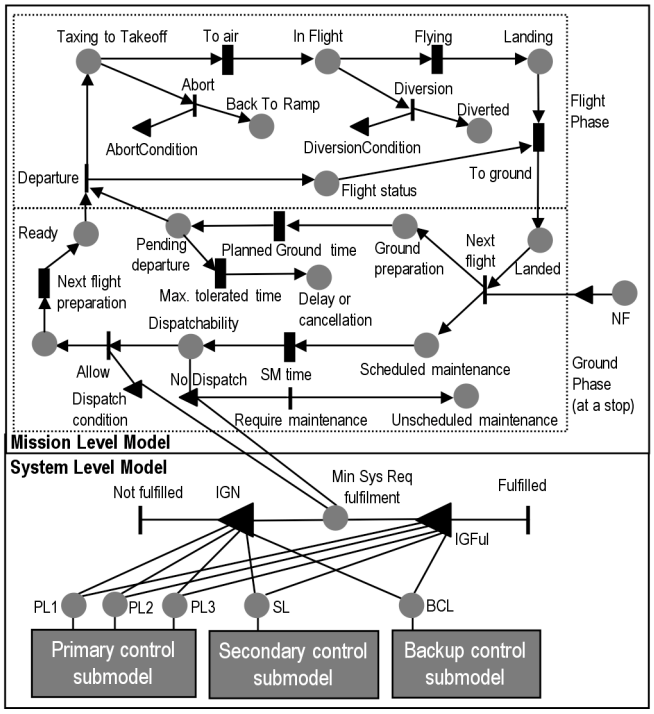

Figure 3: Dependability model overview

The ground period sub model describes the preparation of the next flight and the readiness for departure on time. The start of the preparation for the next flight is represented by the marking of places *Ground_Preparation* and *Scheduled_Maintenance* (routine checks for instance) [3]. When the scheduled maintenance is finished (activity *SM_Time* fires), the place *Dispatchability* is marked. The

[1] [8] is actually a Master MEL (MMEL). MELs result from the completion of MMELs with airline specific policies and are not public documents. MMELs are established by the aircraft's manufacturer.

[2] We only consider the conditions related to the components involved in the subsystem considered.

[3] These tasks are aimed at detecting failures, and not to repair any failed component.

instantaneous activity *Allow* can fire if the dispatch requirements, stated in the *Dispatch_Condition*, are fulfilled. Otherwise the instantaneous activity *Require Maintenance* fires if the corrective action requires maintenance tasks (stated by the *No_Dispatch* condition). Place *Dispatchability* remains marked until the corrective action succeeds (predicate of *Dispatch_Condition* becomes true) and the flight is allowed. In the current illustration, the fulfillment of dispatch requirements consists of testing the marking of Min_Sys_Req place. Until then, the scheduled ground duration may have elapsed (firing of activity *Planned Ground Time* moving the token to place *Pending Departure*) and the maximum tolerable delay (*Max tolerated time*) may be running out. A delay or cancellation occurs if the tolerated time to dispatch is exceeded. The timed transition *Next flight preparation* represents the other activities (passengers and baggage processing …) that may consume time, causing delay. Place *NF* (at right) is an extended place representing the list of flights to be achieved. The input gate linked to this place indicates whether there is a next flight to achieve or not (end of the mission or not). It is noteworthy that different distributions can be specified for different flights when considering the timed activities defined in the mission level model.

V. ASSESSMENT RESULTS

In order to show the impact of the changes introduced in Section 2, we have defined a typical initial mission composed of four identical flights per day during one week, and assessed the mission reliability, *MR*, as a function of calendar time *t*. We assume that, as long as *MR* is larger than a threshold, referred to as Minimal *MR* Requirement (*MMRR*), the mission can be continued. *MMRR* is set by the airline company, in agreement with the aircraft manufacturer. For the sake of illustration, we have considered *MMRR* = 0.975. It is worth to mention that, in order to preserve the industrial confidentiality, the set of values used in this section have been selected to form a consistent set, without disclosing the industrial property.

We will first consider the impact of a failure occurrence during the mission, and show how the assessment results will help to determine when to repair this component. Then we will show the impact of a failure distribution change before analyzing the impact of mission profile changes.

A. Component failure occurrence

The single failures of P1 or S1 do not affect safety and do not prevent mission achievement. However, the failures of both components lead to a mission interruption.

Failure of primary computer P1

Curve 0 of Figure 4-a shows the mission reliability, *MR*, as assessed before mission beginning, assuming that all components are OK at the starting of the mission. It can be seen that at the end of the mission, *MR* is above *MMRR*.

Curve 1 of Figure 4-b corresponds to the case where P1 has been diagnosed as inoperative at the end of day 4. *MR* is thus re-assessed, considering i) as initial time (t=0) day 5, and ii) P1 is inoperative at t=0. *MR* is thus equal to 1 for each re-assessment, as the system is in an operative global state at the time the model execution is performed. It can be seen that the new assessed measure is still above MMRR at the end of the whole planned mission. The mission can be continued without maintenance until its end, unless a new event occurs, in which case a new re-assessment will be needed.

Curve 2 of Figure 4-c corresponds to the case where P1 has been diagnosed as inoperative at the end of day 2. As for the previous case, *MR* is re-assessed, considering i) as initial time the next day (i. e., day 3), and ii) P1 is inoperative at t=0. It can be seen that *MR* is below *MMRR* from day 5. This result shows that P1 has to be repaired no later than day 5 to satisfy the MMRR requirement.

Of course, the earlier P1 is repaired the earlier the remaining mission reliability will be improved. However, spares are not available at all destinations, and one has to find the right time to repair P1, according to resource availability, while ensuring an *MR* above *MMRR*. Three situations are possible at this stage, considered below:

- S3: P1 is repaired at the end of day 3,
- S4: P1 is repaired at the end of day 4,
- S5: P1 is repaired at the end of day 5.

Figures 4-d, 4-e and 4-f correspond respectively to the three above situations. Curve X, X = {3, 4, 5}, is related to situation SX. It corresponds to the result of *MR* re-assessment, at end of day 2, assuming that P1 will be repaired at the end of day X. It can be seen that for S3 and S4, *MR* is above *MMRR* for the whole mission, while S5 leads to an *MR* below *MMRR*, in day 7. S5 improves *MR* but not enough to avoid an *MR* below the threshold. This means that P1 should be repaired either in day 3 or day 4, depending where and when the maintenance can take place.

It can be seen that curves 1 and 2 have the same slope but shifted in time, which is not surprising, as they have been obtained from the same model, with the same initial states of the components and the same exponential distributions.

Indeed, we have assumed exponential distributions for all components to show that the operational changes will induce perceptible changes in the results. With the modeling approach used and the available tools, it is possible to consider other distributions and to take into account the age of the other components involved in the analysis. However, aging is a long-term variation process, the granularity of changes is much larger than one day or one week (the duration of a mission). In addition, very small variation of the failure rates of the components during a mission induces a non-perceptible variation in the reliability curves. However, we will see in the next section that changes in components' distributions can have a significant impact.

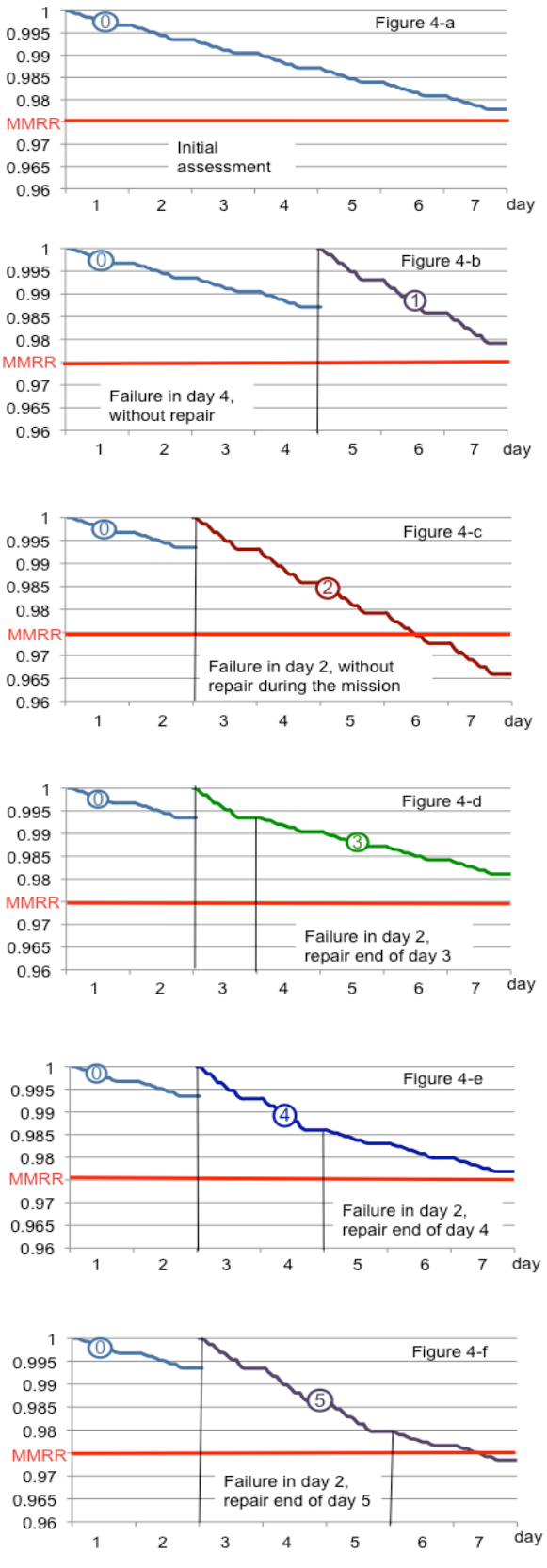

Figure 4: Impact of P1 failure during mission achievement

Failure of secondary computer S1

Curves 6 and 7 of Figure 5 show the re-assessment of *MR* after the secondary computer S1 failure, respectively during day 4 and day 2. These curves are to be compared to curves 1 and 2 of Figure 4-b and 4-c. Curve 0 is the same for all figures.

Curve 6 is below curve 1 and Curve 7 is below curve 2. This means that S1 has a more negative impact on the remaining mission reliability than P1. This is due to the fact that P1 failure rate is greater than S1 failure rate. The requirements are that one of computers P1 and S1 must be operative in order to achieve the mission. Therefore the risk of interrupting the mission is higher when S1 is inoperative than when P1 is inoperative.

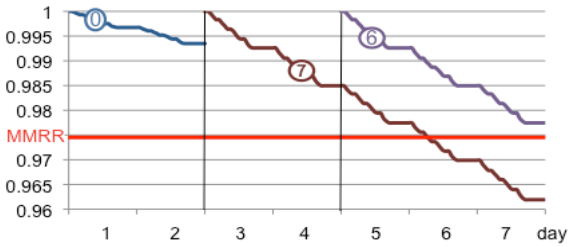

Figure 5: Impact of S1 failure during mission achievement

B. *Changes in failure distribution*

The prognostic is based on long-term observations of specific parameters during the whole life of multiple aircrafts of the same family. It is based on statistics as well as on other approaches that provide an acceptable confidence (this cannot be detailed more, not to disclose the idea). Prognostic results are usually made available from time to time (that can be of the order of magnitude of few months to few years), without any synchronization with mission achievements.

The aim of this analysis is to check if it is important to integrate the new information, as soon as it is available, or to wait the next mission to adjust the distribution. Again, this does not mean that the distribution has suddenly changed during the mission. This corresponds to the case where the notification of the distribution change takes place during the mission.

The impact of the primary computer P2 failure on mission reliability is larger than the impact of P1 or S1 failures, because the failure of P2 leads directly to an inoperative state. Let us assume that, based on the various observation means used by the prognostic process:

- P2 failure has been first identified as following an exponential distribution, with a mean time to failure, MTTF0 = 5000 flight hours.
- during day 2, a new distribution is notified.

For purpose of illustration, and based on observed phenomena, we consider two possible distributions for the failure rate of P2, D1 and D2:

- D1: is a conditional Weibull distribution with shape parameter α=2.5 (α>1 represents an increasing failure rate), scale parameter β=5635 and elapsed time T_e=5000.
- D2: is also an exponential distribution, with a mean time to failure, MTTF1 = MTTF0 / 2 (on average 4 failures per year instead of 2 failures per year).

Figure 6 shows the impact of the distribution change from exponential (curve 0) to Weibull (curve 8). Curve 8 corresponds to a prognostic issued at day 2 of the mission. The rapid reliability decrease of curve 8 compared to curve 0 results from the increasing failure rate of computer P2.

Curve 8 shows in particular that with a Weibull distribution, *MR* is almost equal to *MMRR* at the end of the mission.

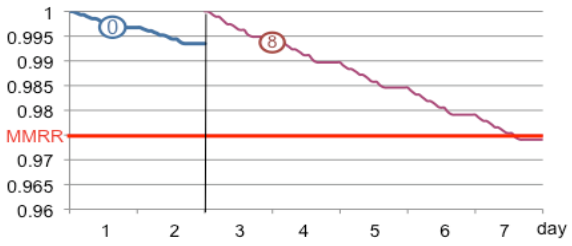

Figure 6: Failure distribution change, notified and integrated at day 2

The curve corresponding to distribution D2 is very similar to curve 8. It is slightly below this curve from day 5, due to the fact that the failure rate of D2 is on average higher than that of D1. It is in particular below MMRR for day 7. As a result, the mission should be modified, most probably shortened, to satisfy the MMRR condition.

It is worth to mention that comparable distribution changes for P1 and S1 lead to non-significant changes in mission reliability.

These results show that for some impacting parameters, taking into account the newly identified distribution, as soon as it is notified, is very important, while it is less important for some other parameters. Such analyses should be performed during the building of the model to identify the most sensitive parameters for which mission reliability re-assessment is recommended as soon as a new distribution is notified.

C. *Change in the Mission Profile*

Aircraft operations depend on various external factors. In particular, some unforeseen events, that do not necessarily affect directly the aircraft itself, may lead to change the initial mission. For example, an aircraft may be assigned new flights with different durations, or additional flights that were initially assigned for another aircraft that should undergo a repair. Such changes require the re-assessment of the mission reliability.

To illustrate the impact of changes in mission profile, we have considered four profiles, presented in Figure 7:

PR0: the initial assignment, 4 flights per day during 7 days, the duration of each flight is 3 hours. PR0 corresponds to the case considered for the previous assessments.

PR1: 5 flights per day from day 2 (corresponds to a mission change after day 1), same durations of flights.

PR2: 2 flights per day from day 2, the duration of each flight is 9 hours.

PR3: 2 flights per day from day 2 to day 4, the duration of each flight is 9 hours, then again 4 flights per day, 3 hours each, from day 5.

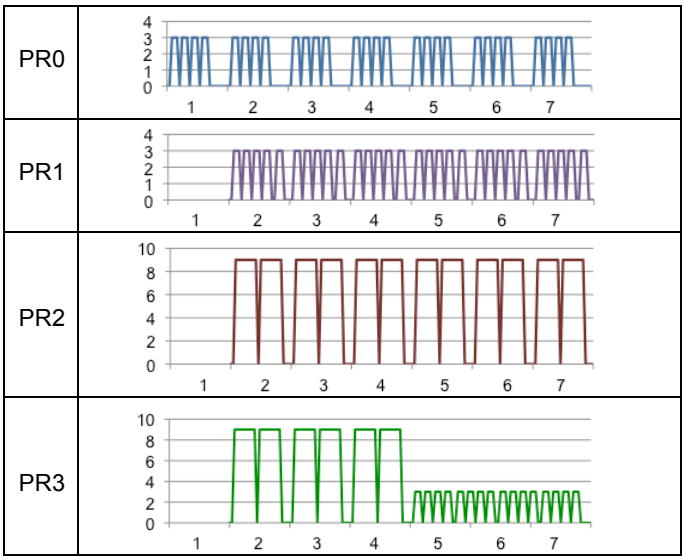

Figure 7: Mission profiles (number and duration of flights per day)

Figure 8 gives *MR* for PR0 and PR1. One can see that the reliability values for PR1 is lower than the values for PR0 after 6 days. However, the minimal mission reliability requirement (*MMRR* = 0.975) is still satisfied.

Figure 9 gives *MR* for PR0, PR2 and PR3. For PR2, *MR* becomes lower than *MMRR*. One can consider adjusting this new profile in order to improve the mission reliability. A possible mission adjustment could correspond to PR3. The mission reliability with the adjusted profile PR3 becomes approximately the same as the initial one, and the *MMRR* is again satisfied.

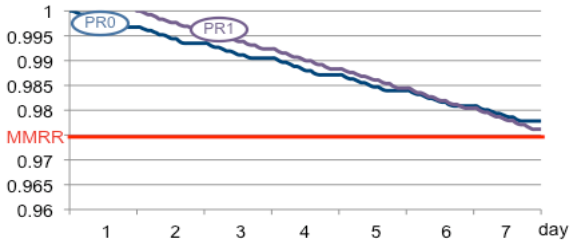

Figure 8: Mission changes from PR0 to PR1

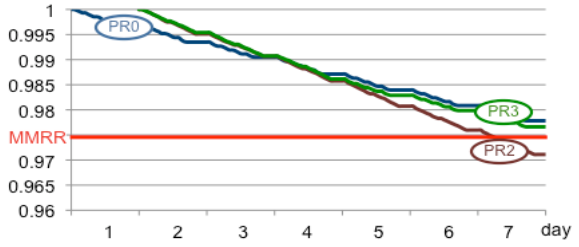

Figure 9: Mission adjustment from PR2 to PR3

VI. CONCLUSION

This experience report presented a modelling approach and numerical examples illustrating how stochastic dependability models can be used: i) to assess aircraft operational reliability during their mission and ii) to adjust the assessments on-the-fly when significant changes affecting the aircraft component states, the environment or the mission profile occur. A prototype tool implementing the proposed approach is currently under development. The human interaction with the tool will mainly consist in the specification of updated parameters characterizing the mission profile (number of flights, duration of flight and ground periods for each flight, maintenance strategies, etc.). The model parameters related to components failure and repair times will be updated based on the information provided by diagnostic and prognostic modules that monitor the state of the aircraft in real-time, together with maintenance information.

The results provided by the tool, that are illustrated though the numerical examples presented in the paper, are aimed at giving insights about the impact of reported changes on the aircraft operational reliability for the remaining mission time, that should be useful to adjust the mission if needed. As far as we are aware, there is no similar existing tool providing such information.

Finally, we stress again that safety is addressed first. If a single safety requirement is not met or if a safety requirement may be at risk, immediate repair will be obligatory. Maintenance is addressed only when all safety requirements are satisfied and are not at risk.

REFERENCES

[1] K. Tiassou, K. Kanoun, M. Kaâniche, C. Seguin, and C. Papadopoulos, "Online model adaptation for aircraft operational reliability assessment," presented at the 6th European Congress on Embedded Real Time Software and Systems (ERTS2 2012), Toulouse, 2012.

[2] K. Tiassou, K. Kanoun, M. Kaâniche, C. Seguin, and C. Papadopoulos, "Modeling aircraft operational reliability," in *Proceedings of the 30th international conference on Computer safety, reliability, and security*, Naples, Italy, 2011, pp. 157–170.

[3] Meyer, Furchtgott, and Wu, "Performability Evaluation of the SIFT Computer," *IEEE Transactions on Computers*, vol. C-29, no. 6, pp. 501–509, Jun. 1980.

[4] A. T. Tai, L. Alkalai, and S. N. Chau, "On-board preventive maintenance: a design-oriented analytic study for long-life applications," *Performance Evaluation*, vol. 35, no. 3,Äì4, pp. 215 – 232, 1999.

[5] I. Mura and A. Bondavalli, "Markov regenerative stochastic petri nets to model and evaluate phased mission systems dependability," *IEEE Trans. Comput.*, vol. 50, no. 12, pp. 1337–1351, Dec. 2001.

[6] H. Sun, D. Tang, and R. Wood, "Optimizing Service Strategy for Systems with Deferred Repair," in *Proceedings of the 11th Pacific Rim International Symposium on Dependable Computing*, Washington, DC, USA, 2005, pp. 269–274.

[7] C. Kehren, C. Seguin, P. Bieber, C. Castel, C. Bougnol, J.-P. Heckmann, and S. Metge, "Advanced simulation capabilities for Multi-systems with Altarica," in *Proceedings of the 22nd International System Safety Conference*, 2004, pp. 489–498.

[8] D. R. Prescott and J. D. Andrews, "Aircraft safety modeling for time-limited dispatch," in *Proceedings of the Annual Reliability and Maintainability Symposium*, Alexandria, VA, USA, 2005, pp. 139–145.

[9] A. Ramesh, D. Twigg, and T. Sharma, "Advanced methodologies for average probability calculation for aerospace systems," presented at the 26th international congress of the aeronautical sciences, 2008.

[10] M. Bineid and J. P. Fielding, "Development of an aircraft systems dispatch reliability design methodology," *The Aeronautical journal*, vol. 110, no. 1108, pp. 345–352, 2006.

[11] L. Saintis, E. Hugues, C. Bes, and M. Mongeau, "Computing in-service aircraft reliability," *Int. J. Rel. Qual. Saf. Eng.*, vol. 16, no. 02, p. 91, 2009.

[12] M. Sachon and E. Paté-Cornell, "Delays and safety in airline maintenance," *Reliability Engineering & System Safety*, vol. 67, no. 3, pp. 301–309, Mar. 2000.

[13] N. Papakostas, P. Papachatzakis, V. Xanthakis, D. Mourtzis, and G. Chryssolouris, "An approach to operational aircraft maintenance planning," *Decision Support Systems*, vol. 48, no. 4, pp. 604–612, Mar. 2010.

[14] A. Ahmadi and P. Soderholm, "Assessment of Operational Consequences of Aircraft Failures: Using Event Tree Analysis," in *2008 IEEE Aerospace Conference*, Big Sky, MT, USA, 2008, pp. 1–14.

[15] S. P. Chew, S. J. Dunnett, and J. D. Andrews, “Phased mission modelling of systems with maintenance-free operating periods using simulated Petri nets,” *Reliability Engineering & System Safety*, vol. 93, no. 7, pp. 980 – 994, 2008.

[16] I. Mura, A. Bondavalli, X. Zang, and K. S. Trivedi, “Dependability Modeling and Evaluation of Phased Mission Systems: A DSPN Approach,” in *Proceedings of the conference on Dependable Computing for Critical Applications*, Washington, DC, USA, 1999, pp. 319–337.

[17] A. Arnold, G. Point, A. Griffault, and A. Rauzy, “The AltaRica formalism for describing concurrent systems,” *Fundamenta Informaticae*, vol. 40, no. 2–3, pp. 109–124, Nov. 1999.

[18] M. Boiteau, Y. Dutuit, A. Rauzy, and J.-P. Signoret, “The AltaRica Data-Flow Language in Use: Assessment of Production Availability of a MultiStates System,” *Reliability Engineering and System Safety*, vol. 91, pp. 747–755, 2006.

[19] D. Daly, D. D. Deavours, J. M. Doyle, P. G. Webster, and W. H. Sanders, “Möbius: An Extensible Tool for Performance and Dependability Modeling,” in *Proceedings of the 11th International Conference on Computer Performance Evaluation: Modelling Techniques and Tools*, London, UK, 2000, pp. 332–336.

[20] Master Minimum Equipment List - AIRBUS A-340-200/300, http://fsims.faa.gov/wdocs/mmel/a340-200-300 original 05-30-08.pdf.