Online model adaptation for aircraft operational reliability assessment

Kossi Tiassou[1, 2], Karama Kanoun[1, 2], Mohamed Kaâniche [1, 2], Christel Seguin[3],
Chris Papadopoulos[4],
[1] CNRS; LAAS; 7 Avenue du Colonel Roche, F-31077 Toulouse Cedex 4, France
[2] Université de Toulouse; UPS, INSA, INP, ISAE; UT1, UTM, LAAS; F-31077 Toulouse Cedex 4, France
{*firstname.lastname*}@laas.fr
[3] ONERA/DCSD/CD, 2 Avenue Edouard Belin, 31055 Toulouse Cedex 4, France
christel.seguin@onera.fr
[4]AIRBUS Operations Ltd., New Filton House, Golf Course Lane, Filton, Bristol, BS99 7AR, United Kingdom
Chris.Papadopoulos@Airbus.com

ABSTRACT
This paper addresses the reliability modeling of an aircraft considering the aircraft operational state and its missions. It presents an assessment approach that one can use for the initial assignment of aircraft missions and possible adjustment and adaptation in case of unpredicted events during the mission. The developed model captures the current operational states of the aircraft with regards to its mission in order to assess the aircrafts ability to achieve the mission. A formal description of the model is presented together with the parameters that may have to be changed in order to adapt the model to online situations.

Keywords
Reliability, online evaluation, mission planning, aircraft, operability.

1. INTRODUCTION

All along its mission achievement, an aircraft has to fulfill operational requirements involving the current online situation. In particular, before each flight, some conditions called dispatch requirements, must be met otherwise the aircraft is not allowed to fly or its mission has to be adapted to fit the current aircraft configurations capability. The dispatch requirements concern principally the current operational state of the aircraft's equipment, the intended mission and the ability to conveniently achieve maintenance activities. It is worth mentioning that aircraft mission profiles are not identical and maintenance facilities are not the same at all airports. Usually, there are more facilities at the aircraft operator's base than at the other airports. Additionally, while a given equipment failure may not allow dispatch for some mission profile, it may require only some simple adjustments like deactivating the equipment solicitation in other cases.

An aircraft mission consists of a sequence of flights and stops. Not meeting the operational requirements before or during a flight can cause significant disruptions that may lead to heavy economic loss [5] due, for instance, to inoperability and compensation given to passengers. Therefore, special attention must be continuously paid to the aircraft operational capability. The missions and maintenance activities must be adjusted regularly. One can base the assignment of a suitable mission to a given situation and maintenance activities planning on operational reliability assessment using models. The model should be able to capture and to adapt to the various situations that may be encountered during missions' achievements.

Our work aims at developing an assessment approach, based on dependability modeling, that makes it possible to continuously assess the ability of an aircraft to keep operating up to a given time or location. Our approach is based on developing a generic stochastic dependability model that can be dynamically updated to represent the current state of the aircraft, with regards to the planned/ intended mission. The model is structured in such a way that different kinds of measure can be done, considering a mission profile or not, maintenance activities or not. The global objective is to assess the operational reliability of the aircraft with regards to operational interruptions. In this paper, an interruption corresponds to a delay, a flight cancellation, an in-flight turn back or a diversion from the initial plan.

The work does not address safety, which is dealt with in previous published work (see e.g., [1]). It is mainly dedicated to aircraft operability and more specifically to model adaptation online, during the aircraft mission. To the best of our knowledge, there are almost no publications related to aircraft operability modeling for online assessment. The studies related to aircraft operability are about dispatch reliability and are carried out for design enhancement [2, 7]. In [5], the operational risks of aircraft systems failures were studied using event tree analysis, but the work did not deal with the operability assessment during the aircraft mission.

This paper presents the modeling approach, together with its online adaptation management. Section 2 provides a description of a typical aircraft's mission. Section 3 outlines the role that the model-based reliability assessment can play in an aircraft's operability improvement. Section 4 presents the modeling and update approach. Section 5 presents a formal description of the model and identifies the changes that may affect it during missions' achievement. Section 6 is devoted to the conclusion and future work.

2. MISSION DESCRIPTION

An aircraft mission consists in performing a predefined set of flights under some 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.
At each stop, the aircraft is inspected and the discrepancies that are 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 refers to an approved document called *Minimum Equipment List* (MEL) 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:

- **Go-if-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.
- **Go-if-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.

Figure 1 summarizes the possible outcomes of the dispatch status.

Dispatch is allowed if i) there is no "No Go" and ii) all "Go If" conditions are acceptable.

When dispatch is allowed, the flight can be aborted or diverted if the aircraft capability is degraded. Procedures stated in the Flight Crew Operating Manual (FCOM) are used to determine whether the flight must be diverted (or aborted depending on the location) or not.

Adverse situations while operating an aircraft lead to operational interruptions such as, flight delays, cancellations, in flight turn-back and diversions [2, 5]. Our work mainly deals with operational interruptions caused by systems failures and the inability to maintain within an acceptable time.

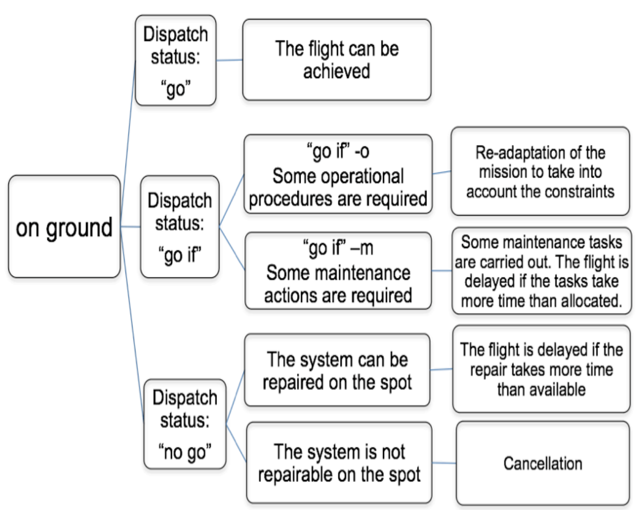

Figure 1 Dispatch status outcomes

3. ROLE OF MODEL-BASED RELIABILITY ASSESSMENT

The problem is to assess, during the aircraft's operations, its ability to satisfy the operational requirements, in the presence of unforeseen events, and initiate an adapted corrective action to prevent adverse situations. There is a need to have good control on the aircraft's behavior while in service, and to be able to predict, with a good level of precision, the events that may be encountered. This includes an ability to cope with random events and a capacity to ensure that the solutions adopted are suitable. Model-based dependability assessment is well suited to support this process.

In our approach the model is essentially used to evaluate the probability to continue operating until a given period of time, known as reliability measure, and the estimated probability will determine whether a corrective action must be initiated or not.

The model can be used while planning the missions and during their achievement. To plan the mission, the model can be used to estimate the period of time during which the aircraft system can be operated without reaching an adverse state. This allows us to determine the mission profile to be assigned to the aircraft. Once a mission is assigned to the aircraft, the model can be 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, and readapt it if necessary. The following describes how the model can be used during the mission.

3.1 On ground

The dispatch decision process takes into consideration the ability to achieve the upcoming flight. Using the model, this dispatch decision may take into account the ability to continue until the next airport where there are enough facilities to fix the problems that may be encountered. To do so, the model is updated with the current state of the aircraft, the failure distributions of the system components, the considered mission profile and maintenance activities.

3.2 During the flight

During the flight, the model can be updated, after the occurrence of major events that may affect the operability, to provide an indication on the reliability of the remaining part of the mission. The result may help in selecting the most appropriate maintenance or operations planning actions in order to improve the ability to achieve the whole mission. When a major event happens, the model is updated and run to assess the aircraft ability to continue the mission. The outcome may be used to support the decision, by the operations control centre, to continue the flight or revise the planned mission. In case of a decision to divert the flight, the model can also be used to determine a convenient diversion airport. In case of emergency (due for example, to problems that may affect safety), the model can be used once a diversion airport is selected, to re-assess the operational reliability.

3.3 Maintenance planning

Assessing the success of a mission is a means for evaluating the concordance of a maintenance program with the mission. Different maintenance strategies can be compared considering various alternatives and priorities for performing component repairs. The best strategy can be determined based on the estimated probability of mission accomplishment without operational interruption.

4. THE MODELING APPROACH

As stated in Section 2, the aircraft has to fulfill a set of operational requirements from the MEL (dispatch requirements) before flying and operational requirements from the FCOM (in-flight requirements) during the flight. We distinguish:

The minimal requirements (Min_Sys_Req): from the MEL, independent of the mission profile and which must be fulfilled to operate the aircraft whatever the mission profile.

The mission profile requirements (M_Prof_Req), which are specific to the mission profile.

The evaluations will be based on the fulfillment of both of these requirements.

4.1 Quantitative measure

The objective is to evaluate the probability of occurrence of an adverse event that may lead to an operational interruption. We distinguish two cases of evaluation:

- While planning a mission: the aircraft **system reliability (SR)** is evaluated with regard to Min_Sys_Req in order to determine the maximum number of flight hours that can be achieved, without maintenance. This is used to determine the length of the mission or to plan maintenance activities.
- Once a mission is assigned to the aircraft and during its achievement: the probability to achieve the mission without an operational interruption, referred to as **Mission Reliability (MR)**. MR is evaluated with regard to Min_Sys_Req and M_Prof_Req in order to determine whether a preventive action (change in the mission profile or maintenance actions) must be initiated or not.

4.2 Structure of the model

Assessing the aircraft operational reliability based on dependability models is clearly convenient to suitably manage its mission. However, the assessment will be useful only with an adequate modeling approach. The model must not only represent efficiently the aircraft and its missions but also be easily updatable to be adapted efficiently to i) the current real state of the aircraft, ii) to changes in the initial mission, and iii) to changes in the maintenance facilities at the next airports. The model must be thus designed in such a way so as to facilitate the updates.

Figure 2 shows the overall structure of the model. In this paper, we focus on the main philosophy for structuring and describing the model rather than on a specific modeling formalism. For the sake of separation of concerns and in order to make the model flexible, the relevant elements of the global problem that need to be captured appear explicitly. Four levels are distinguished.

Operational level: It describes the succession of periods during which the aircraft is either flying or on ground (i. e., the mission profile). A distribution is specified to define the duration of each period.

Requirements level: It corresponds to the aggregation of the operational requirements Min_Sys_Req and M_Prof_Req, expressed as a function of the states of the aircraft components and the mission profile. These requirements are formulated as Boolean expressions, representing the different combinations that do not lead to an operational interruption.

System: It describes the aircraft system behavior. The system is decomposed into subsystems and atomic components according to its design logic or its functions. This level describes the components failure scenarios.

Maintenance level: It describes the maintenance possibilities at the various airports involved in the mission. It is intended to represent the predefined maintenance facilities available at the airports. This has an impact on the repair time of the system components at a given stop. The maintenance activity itself is modeled at the system level.

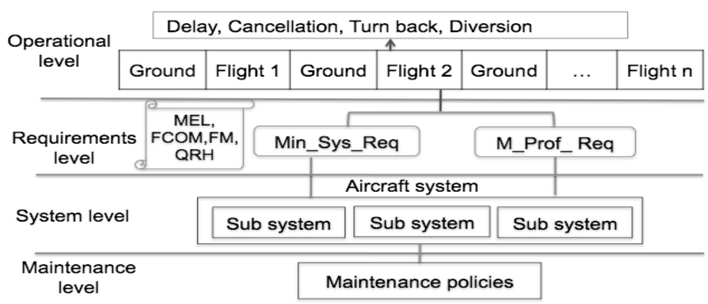

Figure 2 Overall structure of the dependability model

The above structure of the model is of great help for model updating. The model can be easily adapted when changes occur in a given level. For instance, when a component, which must be maintained at a main maintenance base airport, fails, the system level sub model should be updated with this new state and the new failure distributions of the other components. The operational level sub model should also be updated with the remaining parts of the mission. Therefore, the global model construction process must be designed in such a way so as to cope with these issues and facilitate the update. The model construction and update are presented in the following.

4.3 Model construction and update

The model construction is based on a dynamic model building process, taking into account the different categories of updates that may generally happen. The global model building consists in an initial basic modeling work and the establishment of instructions that can be used for the updates online. The different kinds of updates that may generally affect the model are identified in the following.

4.3.1 Overview of the dependability model's kinds of update

Three kinds of updates may take place.

Update of the initial state of the model: this corresponds to the case where for example some system components have failed and/or the aircraft is at a new step of the achievement of the mission. The reliability is evaluated to assess the impact of the new state on the mission's achievement. In this case, only the states of the components are updated; the events distributions and the mission profile may remain the same.

Update of parameters or event distributions: this corresponds to the case where i) new failure distributions have been prognosticated for the system components, or ii) the mission's flights durations have changed or iii) the maintenance facilities at the next airports have changed, affecting the mean time to repair the components. The update can concern the parameters of the distribution laws or the laws themselves. It can have an impact also on the model processing techniques. Analytical methods always require some restrictions on the events distributions laws used in the model, e.g. some formalisms do not allow non-exponential laws to be managed. In this case, simulation techniques are used to process the models.

The update affecting the structure of the model: this corresponds to the case where the mission profile has changed. For example while considering various alternatives of mission profile. Changing the mission profile may imply also changes in maintenance scenarios (the maintenance activities take place at the airports included in the mission profile) and M_Prof_Req (each mission profile has its specific requirements). Therefore, different operational, requirements and maintenance levels sub models corresponding to each alternative, have to be considered.

Due to the need of reconstruction implied by these possible changes, the method to obtain the global model must be clearly established.

4.3.2 Construction of the model

We consider the following dynamic model building methods:

Dynamic Composition of pre-developed sub-models: In order to build the global model online, one may use pre-developed sub-models corresponding to pre-identified and analyzed situations. The sub-models are built with coherent linking interface that can be used to compose them. The sub models can be gathered in a library and the construction of the global model consists just in the composition of some selected ones. The drawback of this technique for an online model construction is that all the possible scenarios must be identified and modeled once and for all.

Completion of a model: One may have an initial model, which can be completed in order to create a global model corresponding to a more general situation. To do so, the initial model provides a "public" interface that is used to develop and integrate the additional sub-models. The "public" interface is a set of identifiable variables provided by the initial model. These variables are used by the additional sub-model to depict its behavior.

For our case, there will be an initial construction that can be completed by sub-models whether specified online or retrieved from a library. The construction of the global model consists then of two steps: the construction of an initial model, done once and for all, and its completion by the mission profile information online. The initial model describes the static part of the model and provides an interface for the initialization of its variables. The interface also provides the information regarding the composition with the additional models.

4.3.3 Model update management

The approach to manage the model update consists in using some configuration files that can be updated with the current states of the components and the mission profile. The parameters that are set in the configuration files will be used to update and complete the model before the (re-)evaluations. Moreover, the update of the configuration files will be notified to an evaluation manager, which will determine its relevance in order to initiate the processing of the model.

The evaluation manager can correspond to a human operator or to an automatic algorithm that determines when the identified changes in the mission profile, or the system state should lead to an update of the model, or most probably a mix of both. Figure 3 shows the update scenario.

It is expected that the system update will rely on diagnosis and prognosis modules (that are run and updated at runtime either automatically by diagnosis and prognosis online mechanisms embedded in the control systems or by the crew) to parameterize the system level sub model. Data from the flight plans will be used to configure the operational level sub model.

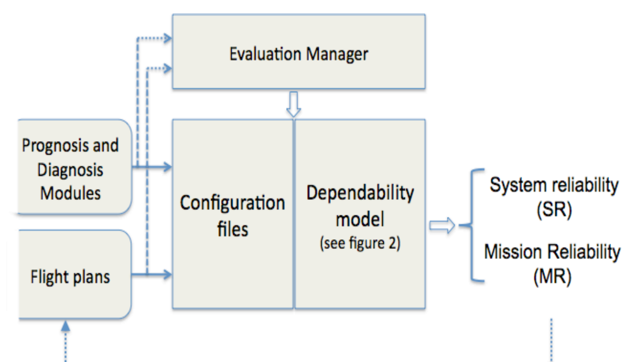

Figure 3 Update of the model

As stated in section 3, the evaluation can be done either at the operator's request or automatically in order to notify the operator of changes that may affect the ability to continue the mission.

The aim is to make the data exchange, between the evaluation manager and the model, independent of the modeling formalism used for building and processing the dependability model. The update is possible by someone who is aware that there are changes requiring a model update, and who can easily enter the changes. Some kinds of update are automatically done by other runtime processes.

Additionally, updating and processing the model can be performed either online or on ground while the aircraft is still in flight, without waiting for the aircraft landing, in order to obtain as early as possible the new assessment results (i. e., the updated system reliability and/or the updated mission reliability).

A formal description of the underlying dependability model is given in the following, together with the update specification and integration.

5. FORMAL DESCRIPTION, POSSIBLE CHANGES AND BUILDING THE MODEL

The formal description of the model helps us in identifying more clearly the major variables affected by changes in the model. The description of the scenarios to specify the changes deals with the data exchange while updating the model.

5.1 Formal description

We formally present in the following the different components of the model by detailing the information involved in each level. To facilitate the comprehension, an UML-like graphical representation of the different elements is given in figure 4.

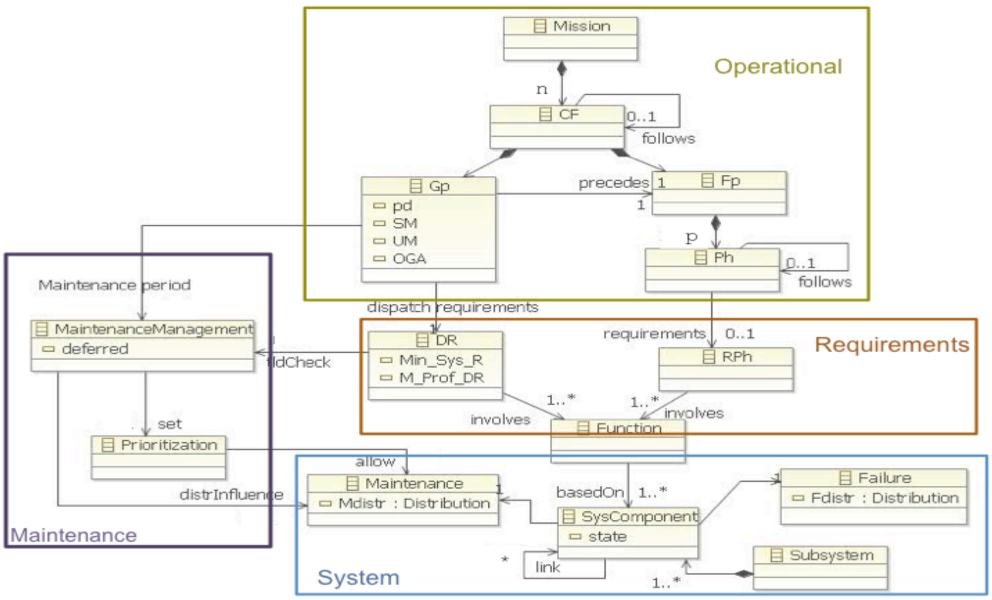

Figure 4 General description of the model

5.1.1 Operational level

A mission is composed of a sequence of flights, which are actually achieved considering a preflight period on ground (named "ground period" in this paper) to get ready, and the flight period itself. Let *Gp* denote a preflight period on ground and *Fp* a flight period. The couple *CF =(Fp, Gp)* or *CF= Fp•Gp* represents the complete flight achievement process, from the flight preparation activities to the flight end. In the remainder of this paper, the operator "•" symbolizes a succession of activities or periods.

A mission *M* composed of *n* flights is then formulated as follows: $M = \bullet_{i=1..n} CF_i = \bullet_{i=1..n} (Gp_i, Fp_i)$.

Each flight period can be decomposed into phases that are distinguished by the system functionalities required for their success. Assuming that a given number *p* of phases can be identified for each flight, we have $Fp = Ph_1 \bullet Ph_2 \bullet \dots Ph_p$. The order of the phases in this notation is important in the sense that the phases are achieved successively. Each phase Ph_j has a duration determined by a distribution law DPh_j that may be deterministic.

Let *I* denote the occurrence of an interruption during the mission. *I* might occur during a flight period or a ground period.

The interruption of a flight is defined as the interruption of one of its phases. A phase interruption is defined as the loss of its requirements fulfillment when the phase is ongoing. At this level, the requirements fulfillment of a phase Ph_i is represented by a Boolean variable RPh_i, which indicates whether the requirements are fulfilled or not. These requirements are defined at the requirements level.

At each ground period, it should be ensured that the aircraft meets the requirements to achieve the next flight and some activities should complete before departure time; otherwise an interruption occurs. A ground period can consist of: i) scheduled maintenance (SM) activities and other ground activities (OGA) or ii) scheduled maintenance activities extended by unscheduled maintenance (UM) activities, followed by the other ground activities.

Accordingly, each ground period can be represented by the succession of the corresponding activities: $Gp=SM \bullet UM \bullet OGA$. SM and OGA have an associated duration determined by a distribution law, which depends on the considered location. The extension of an SM activity with an UM activity depends on the operational state of the system and the maintenance facilities. An UM activity generally takes place when the dispatch requirements (denoted *DR*) are not met. It is generally dedicated to the repair of the critical system components that are needed to perform the flight. These are explicitly identified in *DR*.

A ground period has a deterministic planned duration *pd(Gp)*, which indicates the maximum time beyond which an interruption of the flight occurs.

From the above representation, it appears that the definition of the operational level requires the knowledge of the number *n* of flights composing the mission, the phases composing each flight and their durations, as well as the ground period activities durations, and the sequencing of the flights and ground periods. The planned duration of the ground period activities, beyond which the flight is interrupted, should also be defined.

5.1.2 Requirements level

This level describes the requirements to be satisfied for the successful achievement of the mission defined at the operational level, taking into account the decomposition of the mission into successive flight and ground periods.

The successful accomplishment of the phases Ph_j of a flight is conditioned by the availability of a group of functions $f_1\, f_2 \ldots f_{nj}$ delivered by the aircraft system. Thus, the availability of these functions corresponds to the requirements to be satisfied during each phase to ensure the successful evolution of the flight. These requirements, denoted as RPh_i, can be defined by a Boolean expression identifying the combination of functions that need to be available for achieving the corresponding phase. Alternatively, these requirements can be defined through the identification of the combination of function losses that would lead to the interruption of the flight phase.

The dispatch requirements DR_i to be fulfilled by the system during a ground phase Gp_i can be defined in a similar way. These requirements, defined by a Boolean expression, are determined by: i) the availability of some required functionalities $f_1, f_2, \ldots f_{nf}$ and ii) the possibility of performing some maintenance activities (*Ma*) within the planned duration $pd(Gp_i)$: $DR_i = f\,(f_1, f_2, \ldots f_{nf}, Ma)$.

It is noteworthy that the duration of an unscheduled maintenance period UM correspond to the time needed to perform the unscheduled maintenance actions.

To summarize, a requirement is a combination of functions needed at the operational level, to allow dispatch or the successful accomplishment of a flight phase. The requirements associated to a given mission composed of *n* flight cycles result from the aggregation of the requirements associated to each flight cycle of the mission. For a given flight CF_i, DR_i and $RPh_{j=1..p}$ are the requirements related to ground and flight phases. For dispatch requirement DR_i, the required functions are almost the same whatever the flight to be achieved. Therefore, we gathered the required combinations of functions needed by every flight in a requirement called *Min_Sys_R*eq. We denote by $M\_Prof\_DR_i$ the additional requirements that are specific to the mission profile under investigation. These mission profile specific requirements can be related to the availability of some functions or to the achievement of the maintenance activities required to dispatch the flight, if any.

Accordingly, $DR_i = Min\_Sys\_R \wedge M\_Prof\_DR_i$. $M\_Prof\_DR_i$ is by default true.

The requirements are represented using Boolean expressions, based on the availability of system functions. The availability of each function is derived from the analysis of the availability of the system components contributing to its implementation. The mapping between system function states and system components states is achieved at the system level of the modeling approach. Concretely a function is characterized by its state, which is defined by a conditional function based on the system components state. In the following, we use the notation:

$f_{k=1,2,..} = g\ (C_1S,\ C_2S,\ \ldots\ C_{nk}S)$; $C_1S,\ C_2S,\ \ldots\ C_{nk}S$ are the variables representing the state information of the components involved in the accomplishment of f_k, *g* is a function formulating the relation between the components states and the function f_k.

5.1.3 System level

The system can be seen as a set of components C_l with possible dependencies among them. It is represented using stochastic state space techniques. Each system component is subject to failures events and maintenance activities. More generally, the state of a component C_l, represented by C_lS, may take different values identified as its domain C_lSD. C_lSD can be decomposed into two domains C_lSD = Operational (C_lSO) ∪ Failed (C_lSF). Usually, at least two distinct states are associated to each component: $C_lSD = \{ok,\ ko\}$. Failure events and maintenance activities are then defined as change of the state variable value respectively from C_lSO to C_lSF, and from C_lSF to C_lSO. The specification should also include the definition of the probability distributions describing the occurrence of failures events (denoted as *Fdistr*$_i$), and maintenance activities durations (denoted as *Mdistr*$_i$). Generally, exponential distributions are assumed for these events, characterized respectively by instantaneous failure rates $\lambda(t)$, and repair rate $\mu(t)$. Usually, these rates are assumed to be time independent. A maintenance strategy should also be defined with priority level is associated to each component in order to determine the order of the maintenance activities when several components are failed.

It appears from this description that the relevant characteristics that define a system component are its state, its failure distribution law, and its maintenance duration distribution law.

As maintenance activities depend on the facilities available, the repair rate may depend on the considered location.

5.1.4 Maintenance level

Maintenance activities at each ground period are characterized by the resources available such as spares and technicians. Considering a nominal maintenance distribution for each system component C_l, we consider an impact function MI_{Gp} which is used to determine the additional delay that the ability to have the facilities necessary for the maintenance tasks at the considered ground period Gp, may add on the nominal maintenance duration. A similar approach is proposed in [9].

It is at this level that the deferred maintenance activities are managed together with the global maintenance program.

When several components are failed, there may be a prioritization in the maintenance activities, inducing an order in the components maintenance. The management of the priorities is done at this level. It is done by allowing the maintenance activities by priority level. The maintenance of two or more failed components of the same priority level is non deterministic.

The parameters specifying maintenance duration in the different ground periods included in the mission profile are the parameters that can change at this level.

5.1.5 Interface between the levels

The interface between the operational level and the requirements level corresponds to the list of requirements $((RPh_1, \ldots RPh_p)_i, DR_i)_{i=1..n}$ corresponding to the flight phases and ground periods.

The interface between the requirements level and the system level is the list of functions (f_1, f_2, … f_{nf}) provided by the system, on which is based the specification of the requirements.

The interface between the system level and the maintenance level is the maintenance facilities impact on the system components maintenance (MI_{Gp}).

The interface between maintenance level and the operational level is the information about the current ground period and whether it is ongoing or not.

5.2 Changes in the model and specification update

The changes concern essentially the mission profile, the system components and the maintenance policies. The changes that may occur are described together with how they can be reported to the model in the following.

5.2.1 Changes in the different levels

Operational level: The changes concern the definition of the number n of flights, the parameters of each flight, and the ground period parameters. The parameters of a flight are the duration distribution laws of the phases Ph_1, Ph_2, … Ph_p. For a ground period, the parameters concern the total duration allocated to the ground activities, the estimation of scheduled maintenance activities *(SM)* and the other activities ***(****OGA)* durations. These durations are specified using estimated values given whether by an operator, or based on historical data.

Requirements level: When the mission profile changes, the functions required for the achievement of the flights in the new mission profile may change. That is for each flight Fp_i in the new profile, the required functions allowing it and those required for each of its phases have to be indicated. The specification of the requirements consists in defining combinations of predefined functionalities. The requirements can be specified by selection of predefined ones or combination established by the operator, based on known functionalities. However, it will be hardly necessary to change the requirements expressed in the initial model.

System level: The changes concerning the system components are their initial state and their failure and maintenance distribution law. For the state of the components, it consists in changing its current value to another value of its domain. The impact on the global model is just the change of its initial configuration. For failure and maintenance distributions, it consists in considering new distribution function or new values for the distribution function parameters, in order to have a better fitting of the event occurrence distribution.

Maintenance level: The parameters that must be updated at the maintenance level are the maintenance influence function MI_{Gp} related to the ground periods involved in the mission profile. These are defined whether by maintenance crew via the specification of facilities available, or based on historical maintenance data related to the ground periods.

5.2.2 Model specification update

From an external viewpoint, the changes will be considered as mission profile change, component state change, failure prognosis, and maintenance duration estimation. The mission profile change will most likely involve changes in several levels of the model. It may concern the operational level, the requirements level and the maintenance level. The state change and failure prognosis concern the system level. The integration of the changes to the model will be done considering specification from external actors/processes. The scenarios to specify the changes that must be integrated are described in the following.

Mission profile:

The specification of a new mission profile is based on the flights to achieve. To simplify the task, it may be possible to use predefined objects. All the flight and ground periods that need to be taken into account must be specified following the order of their achievement. The specification of a mission profile will be done based on the following operations.

- Specification of a flight:
  - Indication of a predefined flight if the flight profile has been already defined, or
  - Definition of a new flight profile:
    - Specification of the additional dispatch requirements (M_Prof_DR).
    - Specification of the phases Ph_1, Ph_2, … Ph_p . For each phase:
      - Its duration DPh_i: the external actor/process provides an estimated deterministic duration and, in case it is not deterministic, specifies the probability distribution function characterizing DPh_i.
      - Its requirements stated as Boolean combination of functions

For the specification of requirements, the user may select requirements related to a predefined flight or define them by combining listed functionalities using "and", "or" and "not" operators. This task is adapted to our targeted users, who are aircraft operators, as they are familiar with the functionalities and only basic logical operators are used.

- Specification of a ground period:
  - Indication of its planned duration.
  - Specification of scheduled maintenance (SM) duration: similar to a flight phase duration specification.
  - Definition of the other activities duration.
- Specification of maintenance policies: Indication of the list (MI_{Gp1}, MI_{Gp2} … MI_{Gpn}) corresponding to the ground periods included in the mission profile.

The maintenance impact function cannot be given directly by maintenance crew. They should be determined based on basic information that can be provided by maintenance crew. The estimation can be based on information like the technician availability and the time to repair some typical components.

Component state

The indication of a new value for a component state. This can be done either by a diagnosis process, which assesses the component state and provides the information concerning the current state, or via a human machine interface where an operator indicates the new state value.

Prediction of component failure and maintenance activity duration

They concern the specification of an event distribution. New failure distribution and maintenance duration distributions can be specified either by a human actor or a process. In case of a human actor, the distribution is specified by giving values like the estimation of the time to the event occurrence, which can be used as parameters for a predetermined distribution function. The distribution function can also be given directly by an external process (a prognosis module). The possible distribution functions must be identified and standardized for all the interacting modules.

5.3 The model building

As stated in the modeling approach, the global model building consists in an initial model that must be completed online based on the update scenario.

5.3.1 Initial construction of the model

The initial model consists essentially of the system level model. Only the components whose structure will not change are represented. The system level model is constructed and all the functions that may be used at the requirements level are defined. As Min_Sys_Req are common to all the missions and independent of missions' profile, they are also represented at the requirements level in the initial model.

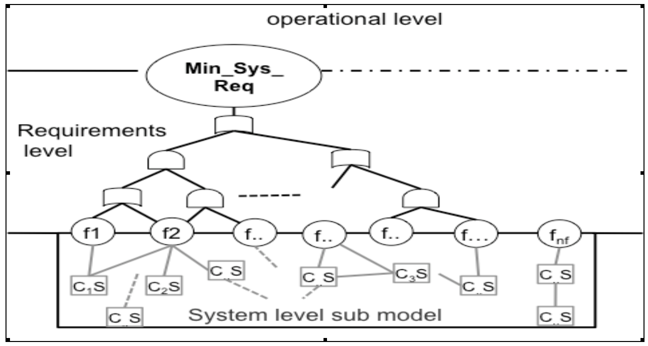

Figure 5 The initial model's content

Figure 5 shows the initial content of the model. The system level sub model is constructed leaving the state of the basic system components and events distributions as parameters to be instantiated in the global model.

The system level sub model provides as output the state of the functions that are needed by the requirements expression. Min_Sys_Req is to be combined with the additional requirements of the mission profile, which will be specified, based on the functions $f_{k=1,\dots}$, when considering the operational level.

This initial model, parameterized with the initial states and failure distribution information, corresponds to the model that will be used to evaluate the system reliability measure, which is the probability to meet Min_Sys_Req for a given duration.

5.3.2 Construction of the global model

The completion of the previous model, taking into account the mission profile, forms the global model. Figure 6 shows the elements that must be added to the initial model in order to obtain the global model in the case of a single flight period *Fp* composed of three phases, preceded by a ground period *Gp*. One has specify the expected duration of each phase (Ph1, Ph2, Ph3), and the requirements corresponding to each of them. The expected duration of ground period activities must also be specified, together with M_Prof_DR, which completes Min_Sys_Req in the condition to allow the upcoming flight.

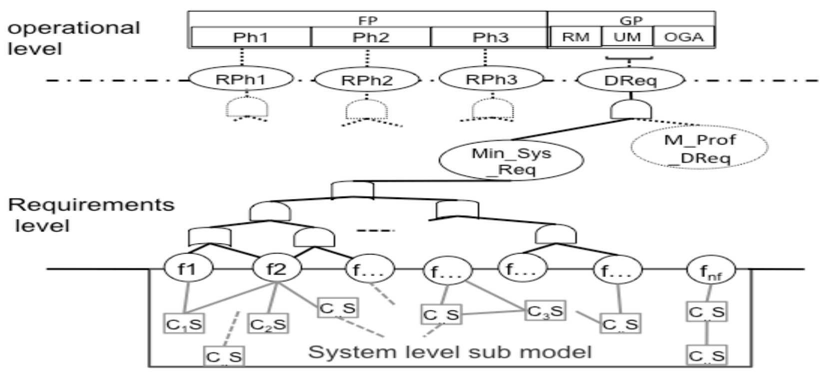

Figure 6 The global model realization

The dynamics of a flight period is that, when a phase is ongoing, its requirements must remain fulfilled up to the end of its duration. The phases take place successively indicating the requirements that must be fulfilled at each time point of the flight profile. A flight period interruption occurs when the requirements of the phase that is ongoing are not met.

6. CONCLUSION AND FUTURE WORK

The objective of the work is to develop a model that helps improve the operability of an aircraft all along its mission. A modeling approach has been developed distinguishing the main components involved in the global problem. The model is adaptable, based on an update method, in order to represent correctly the situations for which it will be used.

In this paper, we concentrated on the approach to develop the dependability model, especially its formal description, and on how it can be updated online in order to adapt to changes in the current situation of the aircraft. The aim is to re-assess the mission operability as soon as some changes take place. The current description has been made independent of the formalism that must be used to build the model. For a concrete implementation, one has to choose an appropriate formalism. We have considered AltaRica and SANs as formalisms for the implementation. AltaRica was used for the purpose of safety study (see e.g., [3]), to model a number of aircraft subsystems on which the work is based. SAN is an extension of Petri nets. SAN and the associated Möbius tool [4] provide compositional operators that are convenient to master the complexity of the model.

The corresponding AltaRica and SAN models [6] [8] were developed using a subsystem of an aircraft. The model updates have been achieved manually.

Future work will consider concrete implementations of the model dynamic construction, taking as examples the major changes that may happen.

7. REFERENCES

[1] D. Prescott and J. Andrews, “Aircraft safety modeling for time-limited dispatch,” in Annual Reliability and Maintainability Symposium, 2005. Proceedings, pp. 139-145.

[2] L. Saintis et. al, “Computing in-service aircraft reliability,” International Journal of Reliability, Quality and Safety Engineering, vol. 16, n°. 02, pp. 91, 2009.

[3] P. Bieber et al, “Safety Assessment with AltaRica - Lessons learnt based on two aircraft system studies” 18th IFIP World Computer Congress, Topical Day on New Methods for Avionics Certification, August 26th, 2004, Toulouse (France), LNCS series (copyright Springer-Verlag): 505-510.

[4] D. Daly et. al, “Möbius: An extensible tool for performance and dependability modeling,” In 11th International Conference, TOOLS 2000, vol. Lecture Notes in Computer Science, pp. 332-336, Schaumnurg, IL B.R. Haverkort, H. C. Bohnenkamp, and C. U. Smith (Eds.), 2000.

[5] A. Ahmadi and P. Soderholm, “Assessment of Operational Consequences of Aircraft Failures: Using Event Tree Analysis,” in 2008 IEEE Aerospace Conference, pp. 1-14, 2008.

[6] K. Tiassou, M. Kaâniche, K. Kanoun and C. Seguin, “DIANA Operational Reliability — Modelling the Rudder System Using AltaRica and Stochastic Activity Networks,” LAAS report No 11001.

[7] M. Bineid and J. P. Fielding, “Development of an aircraft systems dispatch reliability design methodology, the aeronautical journal,” 2006, vol. 110, no1108, pp. 345-352.

[8] K. Tiassou, K. Kanoun, M. Kaâniche, C. Seguin, and C. Papadopoulos, “Modeling Operational Reliability, the 30th International Conference on Computer Safety,” Reliability, and Security (SAFECOMP-2011), Naples, Italy, 2011, pp. 157-170.

[9] U Disnesh Kumar et al, “Reliability, Maintenance and Logistic Support: A Life Cycle Approach,” Kluwer, 2000, ISBN 0-412-84240-8, pp. 250-259