A Formal Framework for Modeling and Prediction of Aircraft Operability using SysML

Sagar Shenoy Manikar, Pierre De Saqui-Sannes, Joël Jézégou, Philippe Asseman, Emmanuel Bénard

A FORMAL FRAMEWORK FOR MODELING AND PREDICTION OF AIRCRAFT OPERABILITY USING SYSML

Sagar Shenoy Manikar
Airbus
ISAE-SUPAERO
Université de Toulouse
Toulouse, France
sagar-shenoy.manikar@isae-supaero.fr

Pierre de Saqui-Sannes
Joël Jézégou
Emmanuel Bénard
ISAE-SUPAERO
Université de Toulouse
Toulouse, France
pdss@isae-supaero.fr
joel.jezegou@isae-supaero.fr
emmanuel.benard@isae-supaero.fr

Philippe Asseman
Aircraft Operability
Airbus
Toulouse, France
philippe.asseman@airbus.com

KEYWORDS
Aircraft Operability, Airline Operations, SysML, MBSE, Simulation, Model Checking.

ABSTRACT

Aircraft operability characterizes the ability of an aircraft to meet operational requirements in terms of reliability, availability, risks and costs. Any operational interruption such as a delay of flight can have significant impact on airline flight schedule and operating cost. Aircraft operability is therefore considered a major requirement by each airline. Prediction of aircraft operability during the development stages of an aircraft can yield valuable feedback to the designers. The subject reaches a complexity level that deserves investigations in a Model-Based System Engineering (MBSE) approach enabling abstractions, as well as simulation and formal verification of models. In this paper, aircraft operability is modeled using Finite State Machines (FSM) supported by SysML. Simulation and model checking techniques are used to evaluate the impact of an event on airline operations using operability Key Performance Indicators (KPIs) such as reliability, availability and cost. The modeling framework is demonstrated on a case study of air-conditioning pack.

INTRODUCTION

Each aircraft is an asset whose objective is to safely achieve its missions through on-time departures and arrivals, without imposing extensive operating costs to airlines. Aircraft operations can be interrupted by scheduled events, *e.g.* scheduled maintenance, and unscheduled events, *e.g.* due to a system failure or a structural damage detected during operations, both requiring actions to ensure airworthy status for the aircraft and its components. These events can lead to significant operational interruptions either right after their occurrence, *e.g.* if it impacts the aircraft airworthiness, or when the related maintenance action makes the aircraft unavailable for continuous operations. Furthermore they are usually associated with expenditures, for example to cover maintenance actions or passengers' compensations, thus impacting aircraft direct operating costs.

The ability of an aircraft to meet its operational requirements is a key driver in airline aircraft selection process and profitability, and is monitored through performance metrics that can possibly be guaranteed in purchase or support contracts. Therefore, it is important for the aircraft manufacturer to develop aircraft that deliver high operational performance on top of the safety regulations mandated by certification agencies. During the aircraft development stages, if the operational performance of an aircraft can be predicted based upon the way that it is going to be utilized in airline operations, valuable insights can be provided to the designers for improving the system of interest.

In this context, this paper proposes an innovative methodological contribution towards evaluation and prediction of the operability Key Performance Indicators (KPIs) of individual aircraft and aircraft fleet. To achieve relevancy and completeness of metrics, it explores the operability problematic through an overall approach aiming at integrating all the influencing factors such as aircraft mission, operational environment and context, along with technical events related to aircraft and systems reliability.

Characterized by uncertainty, heterogeneity and multidisciplinary nature inherent to this kind of operations, aircraft operability reaches a complexity level that deserves investigating modeling techniques to capture and help mastering that complexity. To address and formalize this problem, in a context of aircraft development, the question of using a MBSE approach is raised in this paper with a first research contribution in applying FSMs (Finite State Machines). For this purpose, the proposed approach is to clarify the need for modeling operability, to model it in the form of FSMs, to implement a formal verification process (model checking) and

to run simulations with operability KPIs evaluation.

To make contributions amenable to a broad audience, this paper uses finite state machines of the Systems Modeling Language (SysML), and more precisely the form of finite state machines supported by free software TTool (Apvrille et al. 2020). These state machines handle data, communication, time intervals, and probabilities. TTool's simulator randomly explores the state space of the SysML model. Conversely the model checker relies on mathematics rather than simulation sampling to verify a SysML model against its expected properties.

BACKGROUND

Aircraft Operability

Aircraft operability characterizes the ability of an aircraft to meet its operational requirements in terms of availability, reliability and operating costs within a given operational environment.In this paper, an aircraft mission is defined as a series of commercial air transport flights with regular turn-around time before an extended stop for aircraft restoration and clearance of deferred maintenance tasks. As per regulation, any aircraft performing a flight shall be in an airworthy status, that includes accomplishment of maintenance in accordance with a maintenance program and rectification of any defect and damage affecting its safe operation.

The turn-around time (TAT) is defined as the time between the moment the aircraft stops at the gate after a flight until the moment it leaves the gate for the next flight. Maintenance actions to rectify defects and damages can or have to be performed during this time so that the aircraft is airworthy for next flight. Undesirable extension of turnaround time may be needed to perform those actions. Aircraft operational unavailability, defined by the International Air Transport Association (IATA) measures the unavailability of an aircraft for flight due to maintenance from the *operations point of view*. It covers non-operating time of an aircraft due to scheduled and unscheduled maintenance actions for technical reasons which affect airline operations. It can be influenced by aircraft manufacturer and design. Minimizing unavailability increases aircraft operating time and is essential to optimize profitability.

An Operational Interruption is the interruption of a flight caused by a technical malfunction of the aircraft, its systems and components, by related checking and necessary corrective actions. Those interruptions can occur on ground or in flight, and can lead to delays, cancellations, in-flight turn-backs or diversions, thus contributing to operational unavailability. In this paper, an event is defined as any technical occurrence that generates a maintenance demand considering the given mission and operational context, *e.g.* failure of a component, detection of a structural impact during pre-flight check. It can potentially lead to aircraft operational unavailability or an operational interruption if not resolved within the natural downtime of the aircraft.

Maintenance

The aircraft maintenance program is an approved living document describing the maintenance tasks that have to be performed within specified intervals to ensure continuing airworthiness of the aircraft. It therefore formalizes the maintenance demand to be considered throughout the life cycle of the aircraft and consequently influences aircraft unavailability, airline maintenance policy and organization, required workforce and direct operating costs. A significant part of the program is prescribed by aircraft manufacturer and components suppliers through the initial scheduled maintenance program. A collection of manuals describe the details of execution of routine maintenance, malfunction troubleshooting and corrective maintenance tasks.

The Master Minimum Equipment List (MMEL) is an approved operational document established by the manufacturer that provides the conditions to fly an aircraft in airworthy conditions. It identifies individual equipment that may be inoperative at the commencement of a flight. Each MMEL item is assigned with one of the following status: 'GO' when continued operation is permitted for a limited period of time, a limited number of flights or flight hours without any operational restrictions, 'GO-IF' when continued operation is permitted for a limited period of time, a limited number of flights or flight hours with operational restrictions, 'NO-GO' when continued operation is not permitted and corrective maintenance action must be performed before the aircraft can continue operations. The limited period of time is defined by a Rectification Interval, which is the allowable interval for rectification of the malfunction. If at the end of this interval, malfunction is not rectified the aircraft is not in an airworthy status; therefore improper management of MMEL items by airlines can lead to aircraft unavailability. The MMEL can alleviate the impact of malfunctions and avoid costly disruptions to operations by providing the airline with the opportunity to schedule the necessary maintenance actions at the next suitable opportunity.

Operability KPIs

Operational Availability (OA) is one of the key metrics to evaluate the technical and financial performance of an aircraft and its corresponding maintenance system. It basically represents the time where the aircraft is not unavailable from the *operations point of view*. It is computed as the total operating time of an aircraft minus the operational unavailability time. Maintenance Unavailability (MU) represents all the time that the aircraft is grounded due to maintenance without making a distinction of whether it affects operations or not. Operational Reliability (OR) represents the ability of the

aircraft to take-off and land on-time, and is computed as the percentage of flights that do not incur an operational disruption. Any delay greater than 15 minutes of scheduled departure is considered as an operational disruption. Direct Operating Costs (DOC) are all the costs supported by an airline related to aircraft flying operations. They include aircraft ownership, fuel, crew expenses, maintenance, expenses due to delays and cancellations. Direct Maintenance Costs (DMC) are the costs of the labor and materials directly expended in performing all maintenance actions of aircraft and its components, either on-aircraft or in maintenance shops. DOC and DMC are influenced by aircraft operability.

SysML and TTool

To address aircraft operability problems in the form of finite state machine depictions, this paper reuses the syntax of SysML, the Systems Modeling Language standardized by OMG and supported by free software TTool (Apvrille et al. 2020). The following SysML diagrams are used in this paper:

- The block diagram that usually models the architecture of the system under design.
- The state machine diagrams that model the inner workings of the blocks defined in the block diagram.

In brief, a block diagram encompasses a set of blocks interconnected by channels (see Figure 3). Each block contains one state machine describing how the block handles its attributes, its input/output signals and its timers. Figure 1 depicts the syntax of state machines. The latter handle data, time intervals, signals emission/reception, and probabilities.

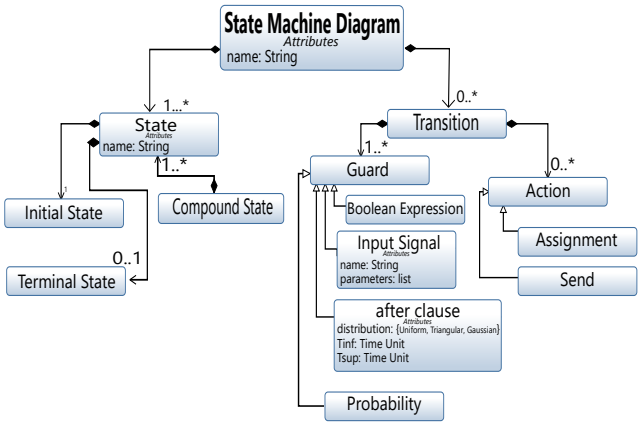

Figure 1: State Machine Diagrams - Syntax

Giving block diagrams and finite state machines a formal semantic makes them executable by the simulation engine of TTool and ready to be verified against their expected properties using a model checker.

MODELING FORMALISMS

There are different modeling formalisms used in conventional reliability and availability engineering which can be categorized broadly into non-state-space models like reliability block diagrams, fault trees, *etc.* and state-space models like Markov chains, Petri-nets, *etc.* Non-state-space methods possess high analytical tractability but low modeling power compared to state-space methods as dependencies are not captured (Trivedi and Bobbio 2017). Some of these techniques have been used to model aspects of aircraft operability such as operational reliability and maintenance downtime. SysML has also been deployed in diverse domains like production, aerospace, automotive, *etc.* for different activities of the product life cycle (Wolny et al. 2020).

Aircraft Operability Models

Markov processes have been used to model aircraft operational reliability in (Hugues and Charpentier 2002), in which flight and stopover phases have been modeled using constant transition rates. But this study only predicts operational reliability. Further, the Markov processes use the same parametric model for modeling all the equipment of the aircraft, which does not allow incorporating system specific properties such as complex redundancies. A mathematical framework using bound algorithms has been used to model aircraft reliability in (Saintis et al. 2009). The algorithms allow estimating the bounds of the operational interruption rate indicators for different events. It is shown that these algorithms outperform the Markov methods in terms of computation time while maintaining a satisfactory level of accuracy. The computation time becomes an important factor while dealing with complex models such as an aircraft fleet since there are usually several combinations of parameters that have to be simultaneously evaluated to obtain operability results.

A dependability assessment framework for online assessment of the aircraft which can be used for mission planning and adjustment of maintenance activities has been investigated in (Tiassou et al. 2013). A stochastic dependability-model based on a meta-model is integrated with up-to date operational data to make the live assessment. A state-space based formalism has been used for modeling and the paper evaluates the use of AltaRica (Arnold et al. 1999) for qualitative analysis and Stochastic Activity Networks (SAN) for quantitative analyses.

Other techniques such as discrete event simulation have been investigated in (Warrington et al. 2002) for modeling aircraft reliability and maintenance. A framework called Ultra Reliable Aircraft Model (URAM) based on discrete event simulation is presented to address Maintenance Free Operating Periods (MFOP) for aircraft.

SysML models and State machines

SysML has been used for reliability modeling in (David et al. 2010) and has been connected to a conventional reliability modeling language such as AltaRica. A way to automatically perform Failure Modes and Effects Analysis (FMEA) studies from the functional design models in SysML has been presented.

State machines have been used in aerospace applications before but have mainly focused on the development of aircraft control systems and software (Krause and Holzapfel 2018, Spagnolo et al. 2018, Kügler and Holzapfel 2017). Probabilistic finite state machines have been used to model aircraft landing sequencing behavior for their ability to deal with stochastic systems (Tang and Abbass 2014).

Model checking

Model checking is defined as the method by which a desired behavioral property of a reactive system is verified through exhaustive enumeration (explicit or implicit) of all the states reachable by the system and the behaviors that traverse through them (Fisman and Pnueli 2001). There have been several advances in the field of model checking especially with the advent of Statistical Model Checking (SMC) techniques which involves sampling and simulation. SMC techniques are better suited than numerical techniques for complex problems and those with large state spaces (Legay et al. 2019). Over the last two decades, there have been many applications of SMC in the fields of computer networking, security and systems biology (Agha and Palmskog 2018). In this paper, the in-built model checker of TTool explores the state space of the SysML model and relies on model checking techniques to check SysML models against safety and liveness properties.

Hence, SysML and State machines have been successfully applied in different domains. Aircraft Operability has also been modeled using different approaches but as per authors' knowledge, state machines have not been used previously to represent aircraft operability. Therefore, this paper investigates a novel method of applying SysML state machines to model and simulate aircraft operations.

CASE STUDY

There are different kinds of events that affect aircraft operations like a system failure, structural damage, abnormal operation, *etc.* A malfunctioning or inoperative system due to a part failure is one kind of event considered in this study and is presented hereafter through a part failure case study of an air-conditioning pack.

An air-conditioning pack (ATA 21-52-01), is part of the Environmental Control System (ECS) of an aircraft that is included in the MMEL of Airbus A320. The ECS is primarily responsible for the pressurization, ventilation and temperature control of the cabin and flight deck along with the cooling of electrical equipment. Since commercial aircraft usually fly at high altitudes where outside pressure and temperature are very hostile, ECS is necessary to ensure the safety and comfort of the passengers and crew by conditioning the air and pressure inside the cabin (Bender 2017).

The case study in this paper considers the failure of an air-conditioning pack, which produces a GO-IF situation at the aircraft level and has a rectification interval of 10 days as per the MMEL. The parameters used to characterize a part failure are 'Mean Time To Failure' (the average time before which a part fails), 'Rectification interval', 'MMEL time' (time to perform maintenance activities defined in MMEL) and 'Repair time' (time to restore functionality). Some of these parameters are expressed as probabilistic distributions in reliability studies. Maintenance tasks and repair actions are usually expressed using triangular or log-normal distributions. The objective of the case-study is to evaluate the impact of air-conditioning pack failure on the operability of the aircraft in terms of OR, OA, MU and DMC summarized in Figure 2.

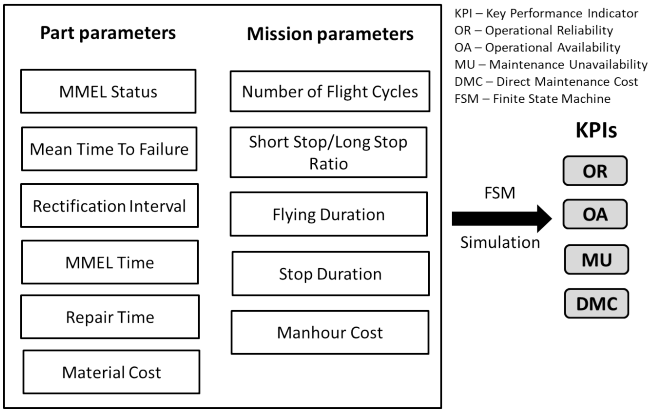

Figure 2: Parameters and KPIs of the case study

MODELING THE CASE STUDY

Rationale

During aircraft development, it is key to understand how the aircraft will be operated by airlines in order to reduce the operating cost and improve aircraft availability, thereby increasing the profitability of airlines. Hence, developing a modeling framework for airline operations will allow to project the potential impact of an aircraft design early during the development stages. This will help compare different system designs in terms of operability performance to make trade-off studies between the different alternatives.

Aircraft operational behavior can exhibit non-

determinism when representing it using a generic model because each airline has a different way of operating its fleet of aircraft. Hence, a stochastic modeling approach was deemed necessary to adequately address the probabilistic nature of airline operations.

An aircraft can be assumed to be present in one of the different operational states during regular operations by an airline. For example, an aircraft during flight can be represented by the state 'Flying' whereas an aircraft on ground which is in preparation for the next flight can be represented by a state called 'Stop'. Along with the existence of different operational states, aircraft operational behavior can be characterized by a notion of time duration associated to each state. Depending on the type of state, there can be a nominal or minimum amount of time spent by the aircraft in that state before transitioning to the next one. For example, an aircraft spends a minimum amount of time in a turn-around before the next flight. Hence, modeling this kind of aircraft behavior helps in capturing the amount of time spent by the aircraft in different states.

Each operational state is also associated with certain properties and actions that are performed when the aircraft enters that state. Therefore, in order to capture the states, probabilities, time and data associated with aircraft operational behavior, a state machine paradigm supported by SysML language was employed. This allowed simulating random sequences of events and evaluating the impact of an event on aircraft operability.

Modeling aircraft operations using Finite State Machines helps in calculating an initial distribution of the time spent in different states when the aircraft operation is simulated for a large number of flight cycles. A distribution refers to the average percentage of time spent in different states when the aircraft operations is simulated over a long period of time. When an event is introduced in the aircraft operations (*e.g.* a part failure), the time distribution of states changes because the aircraft undergoes some maintenance actions as a consequence of the event. Hence, when a set of events is input to aircraft operations and the state machine is simulated for a certain number of flight cycles, a new distribution of the time spent in different states is achieved. The difference in the initial and final time distributions helps in evaluating the impact of the set of events on the different Operability KPIs. These results help to make trade-off decisions while evaluating the potential candidates for a system during aircraft development.

Modeling Aircraft Operations

The operational states of an aircraft can be modeled at different levels of granularity depending on the purpose of evaluation. For the case study considered in the paper, a high-level abstraction was used to identify the five main states shown in Table 1. The aircraft can be either flying or in a stop. Stops are further classified into 'Short stop' or 'Long stop' depending on the duration of the stop. A short stop is essentially the turnaround time in between two flights required for the disembarkation and boarding of passengers, refuelling, *etc.* A long stop occurs usually at the end of the mission when the aircraft remains on ground for a much longer duration than the turnaround time to carry out some deferred maintenance tasks or scheduled maintenance tasks. A long stop such as a 'night stop' for short haul flights can also occur due to regulations in certain countries which ban flights from taking-off or landing during certain hours in the night.

Maintenance activities can be performed both during short stops and long stops. In case the duration of the maintenance activity exceeds the allotted stop duration, it causes a disruption of aircraft operations in the form of delays, cancellations, *etc.* In such situations, the aircraft enters the state 'Short stop with disruption' or 'Long stop with disruption' depending on its preceding state.

Table 1: Operational States of Aircraft

State	**Description**
Flying	all aircraft phases from Taxi-out to Taxi-in
Short stop	when the aircraft is in a turnaround
Long stop	when the aircraft is in an extended stop at the end of the mission
Short stop with disruption	when the aircraft is in a Short stop and the maintenance activity exceeds the Short stop duration by more than 15 minutes, causing an operational disruption
Long stop with disruption	when the aircraft is in a Long stop and the maintenance activity exceeds the Long stop duration by more than 15 minutes, causing an operational disruption

The health of a part can be represented using states 'Healthy' or 'Failed' state corresponding to whether the part is operative or inoperative respectively. Depending on the type of part, different kinds of maintenance actions may be required to restore the functionality of the failed part. When the state of a failed part changes back to healthy, it does not necessarily imply that the same part serial number was repaired. It rather refers to the restoring of the part functionality in the aircraft.

Certain assumptions were made during the modeling of aircraft operations and part failures. The duration of the flights, short stops and long stops were assumed to follow triangular probability distributions as these time durations cannot go below a certain minimum value due to operational constraints. The repair and MMEL action times were also assumed to follow a triangular distribution. For GO and GO-IF kind of part failures, the repair of the part was assumed to be always carried out in a long stop unless there was an aircraft NO-GO situation caused due to expiration of the rectification interval of a part. The planned maintenance events and the as-

sociated 'Out of Service' states are not covered in the scope of this study. For the sake of simplicity, the replacement of a part before its failure is not considered, which can be the case in planned and predictive maintenance. Also when considering the time to failure, No Fault Found (NFF) rate is not taken into account.

Block diagram

The architecture of the aircraft operations system was modeled using a block diagram as shown in Figure 3. A block diagram includes a set of blocks (rectangles) interconnected via channels that link pairs of ports (black squares). Different blocks communicate with each other through signals which are connected through channels of the type synchronous, asynchronous, broadcast, *etc.* On Figure 3, block `PartsHealth` embeds `Part1`, `Part2`, and `Part3` and broadcasts to all of them.

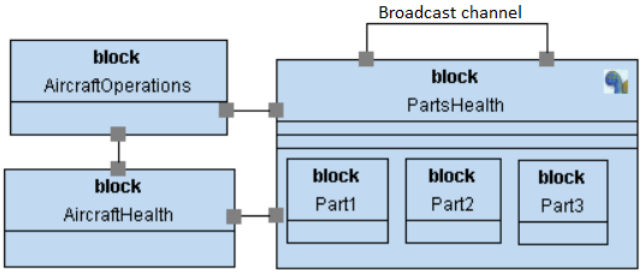

Figure 3: Blocks containing the State Machines

Each block on Figure 3 contains a Finite State Machine. These blocks play the following roles:

- `AircraftOperations` : models the operations of the aircraft in terms of different operational states identified in Table 1.
- `AircraftHealth` : models the overall airworthiness status of the aircraft which determines whether the aircraft is fit for flying or not.
- `PartsHealth` : models the composition of different parts that are considered for operability analysis. It acts as a communication channel between the block 'AircraftHealth' and individual parts.
- `Part1`, `Part2`, `Part3, etc` : model the health status of individual parts (Healthy/ Failed).

For the case study, just a single part (`Part 1`) was sufficient as the failure of the air-conditioning pack at the system level was considered. For analysis comprising of component-level failures, multiple parts can be defined in the `PartsHealth` block to represent each component. The modular approach adopted in the modeling framework allows to define as many parts as required.

State machine diagrams

The behavior of each block defined in Figure 3 is described using a state machine diagram. A part of the 'AircraftOperations' state machine is shown in Figure 4. The states 'Short Stop' and 'Long Stop' contain several sub-states which model the different activities during a stop. A detailed view of 'Short Stop' and 'Short Stop with disruption' states is presented in Figure 5. When the delay is greater than 15 minutes of scheduled departure, the aircraft enters a disruption state.

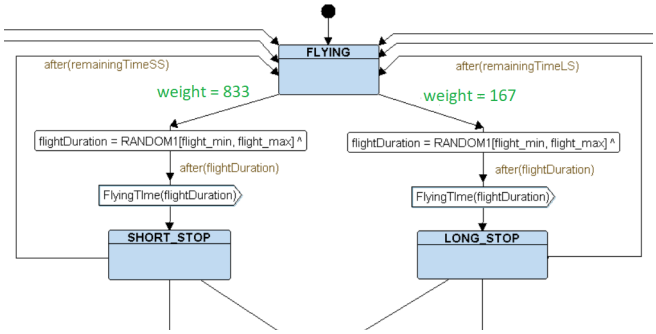

Figure 4: A part of the high-level view of State Machine diagram of 'Aircraft Operations' block in TTool

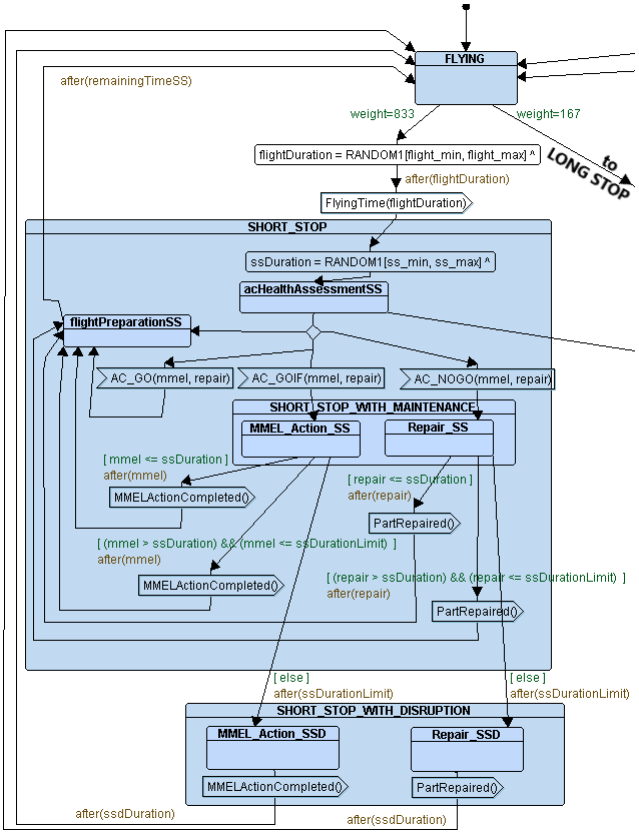

Figure 5: A detailed view of 'Short Stop' and 'Short Stop with Disruption' states

Random variables were employed to model the underlying uncertainty with respect to flight duration, stop duration, type of stop, *etc.* in the stochastic model. The transition from 'Flying' to 'Short Stop' or 'Long Stop' was based on probabilities that can be assigned to transitions. A transition can be assigned a probability (expressed as `weights` in the model) from 0 to 1000. As seen in Figure 4, the transition to Short Stop was assigned a weight of 833 while the transition to Long Stop was assigned a weight of 167 as per the *Short Stop/ Long Stop ratio* defined for the case-study in Table 2 .

Similarly, the state machines for other blocks were also defined. The state machine of `Parts` consists of two main states: 'Healthy' and 'Failed'. Signals were used to communicate the state of a part to `AcHealth` block through `PartsHealth` block. The different parameters of the case study defined in Table 3 were modeled using corresponding probabilistic distributions.

Model Simulation

The SysML state machine diagrams were simulated using the simulation feature of TTool. The model was initialised with the values of mission and part parameters as shown in Tables 2 and 3. It was simulated for 15,000 flight cycles which is close to 7 years of operation for a single-aisle aircraft. The parameters used in this paper are not representative of real systems, but instead are sample values used for illustrative purposes only.

Table 2: Mission Parameters for Simulation in TTool

Input: Mission Parameters				
Number of flight cycles	15,000			
Short Stop / Long Stop ratio	83.3/ 16.7			
Man-hour cost ($/hour)	75			
State	**Distribution**	**Time (mins)**		
		Min	**Mode**	**Max**
Flying	Triangular	105	120	145
Short Stop	Triangular	50	60	90
Long Stop	Triangular	360	420	540

It is possible to observe the simulation results regarding the visited states on both the SysML diagrams as well as the simulation dialog box in TTool. Additional user-defined variables were also used to keep track of the time spent in different states which were continuously updated during the simulation. The final values of these variables were then used to compute the distribution of time spent by the aircraft in different states as shown in Table 4. It is seen that the aircraft spends roughly half the time flying and half the time in stops.

Table 3: Part Parameters for Simulation on TTool

Input: Part Parameters (Air-conditioning pack)				
MMEL Status	GO-IF			
Mean Time to Failure (hours)	10,000			
Rectification Interval (days)	10			
Material cost ($)	15,000			
	Distribution	**Time (mins)**		
		Min	**Mode**	**Max**
MMEL time	Triangular	30	45	120
Repair time	Triangular	360	450	900

Simulation results show that the part failed three times during 15,000 flight cycles out of which it caused one delay and one disruption.

Table 4: Distribution of Time spent in Different States.

Output: Simulation results	
Number of failures	3
Number of disruptions	1
Number of delays	1
State	**Total Time (%)**
Flying	49.228
Short Stop	22.098
Long Stop	28.670
Short Stop with Disruption	0
Long Stop with Disruption	0.004
Total	**100**

The simulation results were post-processed to compute the different Operability KPIs. Operational Reliability (OR) is computed as the percentage ratio of number of disruptions to the total number of take-offs. Maintenance Unavailability (MU) is computed as the total time that the aircraft is on ground due to maintenance. It is measured in the units of days per year per aircraft. Operational Availability (OA) is deduced by subtracting Operational Unavailability (OU) from the total time. Operational Unavailability is computed as the time that the aircraft is on ground due to maintenance that affects the airline operations. The Direct Maintenance Cost (DMC) is computed as the sum of the material cost of the replaced part and the labour cost for carrying out the associated maintenance tasks. It is measured in units of cost per flight hour ($/FH). The corresponding results on Operability KPIs for the case study are presented in Table 5.

Table 5: Operability KPIs for the Case Study

Output: Operability KPIs results		
Operability KPI	**unit**	**Value**
Operational Reliability (OR)	%	99.993
Maintenance Unavailability (MU)	days/year	0.146
Operational Availability (OA)	%	99.999
Direct Maintenance Cost (DMC)	$/FH	1.525

From Table 5, it can be seen that the Operational Reliability is very high (99.993%) for the air-conditioning pack as it produced just one operational disruption during the entire mission. The time spent in this *disruption* state was just 163 minutes leading to very small aircraft operational unavailability. As a result, the operational availability is also close to 100%. The maintenance action required to repair the part three times led to a maintenance unavailability of 0.146 days per year. The resulting cost (DMC) expressed as a cost per flight hour was 1.525 $ per flight hour for the air-conditioning pack. It has to be noted that the results obtained in this study pertain to the analysis of a single part. At the aircraft level, these KPIs are calculated as an overall impact from the different parts comprising an aircraft.

Model Checking

A model checker is catered with a model of the system and a formal expression of the properties to be verified. The model checker processes the model and the properties, and outputs a yes/no answer stating whether the property holds or not. The model checker also traces execution paths that leads to property violations.

For the SysML model of aircraft operability introduced by previous section, the properties to be verified are as follows:

- `Property 1.` A failed GO-IF part that is dispatched under MMEL will be subsequently repaired in a Long stop.
- `Property 2.` It should never occur that the aircraft is flying and the aircraft health is in a NO-GO condition *i.e.* when the aircraft is not airworthy.
- `Property 3.` The maximum delay in a nominal stop is 15 minutes after which an operational disruption is caused.

The above properties can be expressed in the form of safety pragmas included in the SysML model. The safety pragmas are not part of the OMG SysML standard, but are instead an extension supported by TTool for model checking. Each line in a safety pragma expresses a logic property. The syntax of the query language used in this paper is explained below using two expressions `p` and `q` which can be states or attributes:

- `p --> q` : Whenever p is true, q will be eventually true in that path.
- `E <> p` : There exists at least one path in which p will be true eventually.
- `A [] p` : The property p is globally true for all the paths.

Further, the following notation is used: `B` '.' `S` to denote a state S belonging to the state machine embedded by block B.

Using the syntax presented above, the three properties defined in this section are expressed as safety pragmas in the TTool model as follows:

1. *AircraftOperations.mmelActionSS* `-->` *AircraftOperations.RepairLS* : Whenever AircraftOperations.mmelActionSS state is encountered, the AircraftOperations.RepairLS state will also be encountered subsequently.
2. `E <>` *AircraftOperations.FLYING* && *AcHealth.NOGO* : There exists a path in which there is at least one instance where the states AircraftOperations.FLYING and AcHealth.NOGO are encountered together.
3. `A []` *AircraftOperations.delayDuration* `<=` *15* : The value of the AircraftOperations.delayDuration variable is always lesser than or equal to 15.

Figure 6 shows the safety pragmas when model checking is completed. Properties preceded with a 'tick mark'(green) hold whilst properties preceded by 'X'(red) do not. `Property 2` is also verified as the model checker proves that it is not possible to have the 'aircraft flying' and 'aircraft health in NO-GO condition' together during any time during the operations.

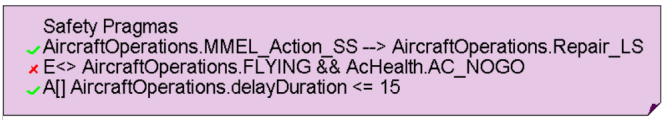

Figure 6: Verified Safety Pragmas in TTool

It is also possible to quickly check whether a given part has the potential to cause an operational disruption using formal verification. Hence, for a set of parameters and an operational context, it can be checked whether it is possible to reach the states causing disruption *i.e.* 'Short Stop with Disruption' and 'Long Stop with Disruption'. If the states cannot be reached, it essentially means that the part failure will not cause a disruption during operations. For the case study, there was one instance where aircraft entered 'Long Stop with Disruption'.

CONCLUSION

Aircraft operability has so far been addressed by engineering methods that do not satisfactorily cope with the complexity of the problems associated with the discipline. The advent of MBSE has opened new avenues to master that complexity and little work has been published on the subject.

This paper synthesizes first results in developing a MBSE approach to address aircraft operability. Problems were expressed in the form of finite state machines by reusing the syntax of SysML. TTool enabled simulation and model checking of SysML state machines. The developed modeling framework could analyse the impact of all three kinds of part failures (GO, GO-IF and NO-GO) on aircraft operability. The effectiveness of this framework in evaluating operability was demonstrated on a case study of air-conditioning pack. The simulation of SysML state machines allowed to evaluate the operability performance of the system. It was possible to incorporate stochastic behavior observed in actual airline operations into the SysML models by using appropriate probabilistic distributions. A large number of flight cycles could be quickly simulated due to the good simulation speed offered by the simulation kernel of TTool. Another main advantage of this framework is the ability to formally verify the correctness of the created models by checking against certain properties. For instance, it was verified that the aircraft always flew in an airworthy condition in the model.

Currently, the framework takes into account only the unscheduled maintenance for operability performance evaluation. Part failures which are one of the main kind of events are addressed in this paper. In the future work, the study will be extended to the analysis of redundant systems. It is also planned to incorporate scheduled maintenance activities in the model along with managing other kinds of events which impact operations, such as structural damage and abnormal operations.

ACKNOWLEDGEMENT

The first author acknowledges support from Association Nationale de la Recherche et de la Technologie (ANRT), France. We thank Ludovic Apvrille (Professor, Télécom Paris, Sophia-Antipolis, France) for adding new probability distribution laws to TTool and for his valuable support to the community of TTool's users.

REFERENCES

Agha G. and Palmskog K., 2018. "A Survey of Statistical Model Checking". *ACM Transactions on Modeling and Computer Simulation*, 28, no. 1, 6:1–6:39.

Apvrille L.; de Saqui-Sannes P.; and Vingerhoeds R., 2020. "An Educational Case Study of Using SysML and TTool for Unmanned Aerial Vehicles Design". *IEEE Journal on Miniaturization for Air and Space Systems*, 1, no. 2, 117–129.

Arnold A.; Point G.; Griffault A.; and Rauzy A., 1999. "The AltaRica Formalism for Describing Concurrent Systems.". *Fundam Inform*, 40, 109–124.

Bender D., 2017. "Integration of exergy analysis into model-based design and evaluation of aircraft environmental control systems". *Energy*, 137, 739–751.

David P.; Idasiak V.; and Kratz F., 2010. "Reliability study of complex physical systems using SysML". *Reliability Engineering & System Safety*, 95, no. 4, 431–450.

Fisman D. and Pnueli A., 2001. "Beyond regular model checking". *21st conference on Foundations of Software Technology and Theoretical Computer Science*, LNCS 2245, 156, 170.

Hugues E. and Charpentier E., 2002. "Application of Markov processes to predict aircraft operational reliability". In *3rd European Systems Engineering Conference (EUSEC)*. Toulouse, 231–235.

Krause C. and Holzapfel F., 2018. "Implementing a multi-level finite state machine with MATLAB Simulink and Stateflow in the environment of high-integrity aircraft controller software". In *2018 4th International Conference on Control, Automation and Robotics (ICCAR)*. 147–151.

Kügler M.E. and Holzapfel F., 2017. "Autoland for a novel UAV as a state-machine-based extension to a modular automatic flight guidance and control system". In *2017 American Control Conference (ACC)*. 2231–2236.

Legay A.; Lukina A.; Traonouez L.M.; Yang J.; Smolka S.A.; and Grosu R., 2019. "Statistical Model Checking". In B. Steffen and G. Woeginger (Eds.), *Computing and Software Science: State of the Art and Perspectives*, Springer International Publishing, Cham, Lecture Notes in Computer Science. 478–504.

Saintis L.; Hugues E.; Bes C.; and Mongeau M., 2009. "Computing In-Service Aircraft Reliability". *International Journal of Reliability, Quality and Safety Engineering*, 16, no. 02, 91–116.

Spagnolo C.; Sumsurooah S.; Hill C.I.; and Bozhko S., 2018. "Finite state machine control for aircraft electrical distribution system". *The Journal of Engineering*, 2018, no. 13, 506–511.

Tang J. and Abbass H.A., 2014. "Behavioral learning of aircraft landing sequencing using a society of Probabilistic Finite state Machines". In *2014 IEEE Congress on Evolutionary Computation (CEC)*. 610–617. ISSN: 1941-0026.

Tiassou K.; Kanoun K.; Kaâniche M.; Seguin C.; and Papadopoulos C., 2013. "Aircraft operational reliability—A model-based approach and a case study". *Reliability Engineering & System Safety*, 120, 163–176.

Trivedi K.S. and Bobbio A., 2017. *"Reliability and Availability Engineering: Modeling, Analysis, and Applications"*. Cambridge University Press, Cambridge.

Warrington L.; Jones J.; and Davis N., 2002. "Modelling of maintenance, within discrete event simulation". In *Annual Reliability and Maintainability Symposium. 2002 Proceedings (Cat. No.02CH37318)*. 260–265.

Wolny S.; Mazak A.; Carpella C.; Geist V.; and Wimmer M., 2020. "Thirteen years of SysML: a systematic mapping study". *Software and Systems Modeling*, 19, no. 1, 111–169.