Aircraft Operational Reliability - A Model-based Approach

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

Project: @Most

Formal Methods Forum, January 26, 2016
Context

☞ Growing interest in air transportation

☞ Competitiveness

☞ Enhance service delivery and minimize operation and maintenance costs

Contribution: Reinforce the role of dependability assessment in aircraft operation
Aircraft Dependability Modeling & Assessment

Common practice: during system design and development

Safety and availability oriented models ➞ Support for System architecture definition

Long-term objectives

Future: usable during system operation - in addition -

Models for assessment in operation ➞ Adjust aircraft operation according to the current operational conditions and changes

Short-term objectives
Objectives: Dependability Assessment in Operation

Whenever necessary

Assessment to support mission definition

Mission planning

Mission start

Re-assessment

\[\rightarrow\] Continue
\[\rightarrow\] Plan maintenance
\[\rightarrow\] Mission interruption

Unforeseen event:
- Failure
- Mission re-definition

Mission end

To avoid as much as possible disruptions/interruptions

Delay, Cancellation, In-flight turn back, Diversion

\[\Rightarrow\] Evaluate the probability to operate without operational disruption/interruption until a given time or location
Means

☞ Develop a model-based dependability assessment framework usable in operation

☞ Forecast operational reliability with regard to disruptions caused by failures and maintenance issues

Operational Dependability Measures

- **System Reliability, \( SR(t) \):** Probability to meet minimum requirements related to the system, during flight duration

- **Mission Reliability, \( MR(t) \):** Probability to achieve a specific mission without interruption
Dependability Modeling

- Model calibration & analysis
- Measure

Model Content definition

During the design phase
- M0

Modeling Specialist and System Builders

In Operation
- M1

Operators and Maintainers

Event / Change
- M2
To Achieve the Objectives

☞ Identification of relevant information for the model construction

☞ Modeling basis that facilitates:
  • Model construction
  • Model update in operation

☞ Validation on case studies
Outline

① Relevant Information Identification

② Modeling Approach: Meta Model and Stochastic Model

③ Stochastic Modeling in the Context of @Most

④ Case Study
  • Stochastic Model
  • Results
Mission & Mission Dispatch

Flight achievement

Mission = sequence of flights

Ground phase  Flight phase

Mission Dispatch Decision

Dispatch ?  Dispatch ?  .....
Next Flight Dispatch Decision

- **All Ok**
- **Failure**
- **Dispatch status**

**Go**

- **Goif-o**
  - Operational Limitation
- **Goif-m**
  - Maintenance Procedures

**NoGo**

- **Corrective Actions**
  - Delay or Cancellation

Acceptable? Feasible?
Relevant Information - 1

- **Failure**
  - Dispatch status:
    - **Go**
      - **Goif-o** Operational Limitation
    - **NoGo**
      - Maintenance Procedures

- **All Ok**
  - **Goif**
    - Acceptable?
      - Feasible?

- **System component state**
  - Requirements
  - Corrective Actions
  - Delay or Cancellation
Relevant Information - 2

Core Information

① Relevant Information Identification
Outline

① Relevant Information Identification
② Modeling Approach: Meta Model and Stochastic Model
③ Stochastic Modeling in the Context of @Most
④ Case Study
  • Stochastic Model
  • Results
Changes and modeling constraints

☞ Changes to be Taken into Account

- Changes in the states of the system components
  - Failure, Maintenance activities
- Failure distributions of the components
- Mission profile

☞ Modeling constraints

- Model construction during the design and development phase
- Model update in operation by non-modeling specialist
Implementation

Diagnosis & Prognosis

Mission profile & maintenance data

Assessment manager

Model update interface

Model Processing

Processing Module

Configuration data

Stochastic Model
Petri Net, AltaRica, SAN

Operational dependability model

Modeling Approach: Meta Model and Stochastic Model
Model Construction and Update Process

Modeling Approach: Meta Model and Stochastic Model
Benefits of the Meta-model

☞ Abstracts and structures model content

☞ Aircraft families

Model generation
Example of Meta-model: System Components

Modeling Approach: Meta Model and Stochastic Model
From Meta-model to Stochastic Model

☞ Dynamic models – state-based models

Modeling Approach: Meta Model and Stochastic Model
Outline

① Relevant Information Identification

② Modeling Approach: Meta Model and Stochastic Model

③ Stochastic Modeling in the Context of @Most

④ Case Study
  • Stochastic Model
  • Results

◎ Conclusion and Perspectives
AltaRica and SAN

Basic Component

```
node Component
flow
stateOk : bool : out ;
power: bool : in;
state
status : {ok,failed} ;
event
failure,
init
status := ok ;
trans
status=ok and power | failure
  -> status:=failed;
assert
stateOk=(status=ok);
extern
law <event failure> = exponential(2.0E-4);
edon

AltaRica model
```

```
C.power

Status=ok
and power

failure \( \lambda \) = 2.10^{-4}

status=failed

stateOk=Status

C.StateOK

SAN model

Predicate: \( (status->Mark() =1) \)
&& power->Mark()

Function: status ->Mark() =0;

Exponential: \( \lambda = 2.10^{-4} \)

status
IGFailure
Assert_update

power

predicate

Predicate:
\( (stateOk->Mark()) != (status->Mark()=1) \)

Function:
stateOk->Mark() = (status->Mark()=1);
```

③ Stochastic Modeling in the Context of @Most
Case Study: The Rudder Control Subsystem

Initially: PL1, PL2, PL3 activated

After failures of P1, P2 and P3: activation of S1

After failures of P1, P2, P3 and S1: activation of BCM, BPS_B, BPS_Y

Min_Sys_R = (PL2 =ok ∧ BCL =ok ∧
(PL1 =ok ∨ (PL3 =ok ∧ SL =ok)) ∧
(PL3 =ok ∨ (PL1 =ok ∧ SL =ok)) ∧
(SL =ok ∨ (PL1 =ok ∧ PL3 =ok))

Case Study: The Rudder Control Subsystem
Global Model Structure

Min_Sys_R = (PL2 =ok ∧ BCL =ok ∧
(PL1 =ok ∨ (PL3 =ok ∧ SL =ok)) ∧
(PL3 =ok ∨ (PL1 =ok ∧ SL =ok)) ∧
(SL =ok ∨ (PL1 =ok ∧ PL3 =ok))
Case Study

To air

In Flight

Flying

Landing

Taxing to Takeoff

Abort

Abort Condition

Back To Ramp

Diversion

Diversion Condition

Diverted

To ground

Abort Condition

Back To Ramp

Diversion Condition

Diverted

To ground

Abort

Abort Condition

Back To Ramp

Diversion

Diversion Condition

Diverted

To ground

Flight Phases

Departure

Ready

Next flight preparation

Pending Departure

Estimated duration

Max tolerated time

Delay or cancellation

Ground preparation

Next flight

Landed

Prof

MProg

Ground Period

SM_Time

Inhibit M

CP_M

Set M

Scheduled maintenance

Dispatch condition

Dispatchability

Allow

No Dispatch

Require maintenance

Unscheduled maintenance

Min Sys R

Loop
The Core Model

Control line PL1 sub-model
Assessment

☞ Parameter setting of model in operation

☞ All system components considered initially operational

☞ Exponential distribution for the failure events
  - Failure rates between $10^{-6}/FH$ and $10^{-4}/FH$

☞ Deterministic durations for flight phases and ground activities
Initial assessment & re-assessment after major changes

- Failure - Maintenance
- Distribution change
- Mission profile changes
Initial Assessment

MR(t) evaluated before the start of the mission
Mission: 7 days, 4 flights/day, 3 hours each

Minimum Mission Reliability Requirement

MMRR
Failure of P1 after 4 days
Case Study

Failure of P1 after 4 days
Failure of P1 after 2 days

Re-assessment

MMRR

Case Study
Maintenance Planning

Failure in day 2, repair end of day 3

Re-assessment
Maintenance Planning

Failure in day 2, repair end of day 4
Failure in day 2, repair end of day 5

MMRR
Conclusion

- Aircraft Operational dependability modeling for an assessment while in service:
  - Feasible
  - Relevant

- Modeling approach coherent with Airbus processes

- Probabilistic dispatch decision integrating multiple flights

- Optimization of maintenance cost