# Aircraft Preventive Diagnosis Based on Failure Conditions Graphs

Vincent Chérière

*Airbus Operations SAS, Toulouse, 31060, France*
*vincent.cheriere@airbus.com*

## ABSTRACT

Modern aircraft are designed to be fault-tolerant. Current maintenance systems provide diagnosis of existing faults, capabilities to do trend monitoring, but no information about the real-time remaining tolerance margin knowing the existing faults, and regarding next incoming MMEL (Master Minimum Equipment List) items that impact aircraft dispatch capabilities.
This paper presents a new concept of aircraft preventive diagnosis based on failure conditions graphs with the associated logical framework. The complete method was successfully applied by Airbus on A380 use cases. The first part of the present paper gives the formal logical definitions for the aircraft preventive diagnosis and remaining margin, distance, risk rate. The second part gives an application example based on the landing gear system of an aircraft and also the lessons learnt from Airbus on A380. Finally, the last section provides a logical integration of preventive diagnosis with prognosis that opens new perspectives.

## 1. INTRODUCTION

Aircraft manufacturers design modern aircraft to be fault-tolerant. Historically, the first reason for that came from *safety* considerations. *Availability* is the second reason.

Aircraft are designed with high reliability equipment and with system redundancies. Nonetheless, failures can still occur, and flight delays or cancellations lead to higher operating costs for airlines. For an aircraft, the MEL (Minimum Equipment List) is a document certified by airworthiness authorities enabling the pilot-in-command to determine whether a flight may be commenced or continued from any intermediate stop, should any instrument, equipment or systems become inoperative. "Experience has proved that some unserviceability can be accepted in the short term when the remaining operative systems and equipment provide for continued safe operations" (refer to Attachment G to ICAO Annex 6). The primary objective of the MEL is to, therefore, reconcile an acceptable level of safety with aircraft profitability, while operating an aircraft with inoperative equipment. The MMEL (Master Minimum Equipment List) is an operational document, based on the JAR OPS-1. It is an approved deviation of the aircraft Type Certificate.



Aircraft manufacturers took benefit from last technologies and last interdependent systems architectures in order to make the aircraft able to fly under MMEL conditions, although some faults without impacting effect may remain present. This has been possible thanks to more and more cooperative aircraft systems, that are more and more interconnected, sharing modular avionics, exchanging hydraulic power, electrical power, mechanical forces. On the one hand, this gives the possibility to define alternative system's functioning modes in case of fault and then a more fault-tolerant aircraft, but, on the other hand, this makes aircraft diagnosis more difficult. Indeed, it is much more complex to isolate failures when failures propagate and even more when faults accumulate.

## 2. BACKGROUND

It is undesirable for aircraft to be dispatched with inoperative equipment and such operations are permitted only as a result of careful analysis of each item to ensure that the acceptable level of safety, as intended in the applicable JAR, is maintained. A fundamental consideration is that the continued operation of an aircraft in this condition should be minimized. Therefore, the airline operators need help from aircraft diagnostic systems in order to isolate failures, identify faults and manage the fault-tolerance remaining margins on the aircraft.

The last on-board maintenance systems provide some information enabling preventive maintenance. On Airbus A380 aircraft, the centralized maintenance system provides the list of pending items to fix before they combine with next failures and lead to MMEL items impacting aircraft dispatch. The aircraft condition monitoring system generates

preventive reports that include aircraft parameters enabling the airline to do trend monitoring on some parameters, so that preventive maintenance can be done upon preventive conditions. Ground tools like Airbus AIRMAN provide statistical functions enabling analysis of the history of aircraft maintenance messages over the aircraft fleet. These statistical indicators can be used to trigger preventive maintenance actions.

Nevertheless, none of these systems provide information about the real-time remaining tolerance margin before the occurrence of the next impacting MMEL item, in terms of additional remaining failures of line replaceable units, failure combination, and quantified risk. This status about the remaining margins is very important for the preparation of an optimized preventive maintenance planning and the associated maintenance job orders.

## 3. NEED FOR AN INTEGRATED LOGICAL FRAMEWORK AND RELATED WORK

To answer these expectations, it is needed to find a framework that:

- Enables to reason on failure combinations and propagation in the aircraft,
- Enables to abduce remaining tolerance margins that are possible thanks to remaining healthy equipment in the aircraft,
- Can be extended to Prognostics so that aircraft diagnostic and prognostic reasoning are integrated, ensuring logical consistency, and taking benefit from integrated and common aircraft knowledge,
- Enables to quantify risk with respect to future aircraft dispatch, integrating information from Diagnostics and Prognostics.

The main contribution of this paper is to define a logical framework that answers these needs.

The logical framework defined in the rest of this paper is based on the theory of model-based diagnosis defined by Reiter et al. (1992) that settled fundamental concepts of consistency-based diagnosis, worked on and improved by the DX' research community for more than 20 years.

Many research works have been done on Diagnostics, on the one hand, and on Prognostics on the other hand. Few of them propose to integrate Diagnostics reasoning with Prognostics reasoning, for instance in (P. Ribot, Y. Pencolé, M. Combacau, 2008, 2009), (N. Belard, Y. Pencolé, M. Combacau, 2011), or (I. Roychoudhury & M. Daigle, 2011). But, to the best of our knowledge, very few enable to reason on multiple failures combining with multiple degradations propagating in a fault-tolerant system, and to quantify remaining risks as it is needed there.

## 4. LOGICAL FRAMEWORK

### 4.1. Definition 1. (Aircraft)

An aircraft is a triple (SP, AO, DM) where:

- SP, the aircraft system pattern, is a finite set of first-order sentences
- AO, the accusable objects, is a finite set of constants
- DM, the detection mapping, is a finite set of first-order sentences

### 4.2. Definition 2. (Accusable Object)

An accusable object is a logical constant designating an object that can be suspected by the diagnostic function. Accusable objects are organized according to the following groups:

- Hardware Fault Candidates, including the line replaceable units handled by line maintainers
- Software Fault Candidates, including the software that can be loaded by line maintainers
- Wiring Fault Candidates
- Regular Inoperative Conditions

  Example: System safety test in progress.
- Environmental Conditions

  Example: Icing conditions.
- Operational Conditions

  Example: Overspeed.
- On-going Maintenance Conditions

  Example: Circuit-breaker open and locked.

### 4.3. Definition 3. (Predicate Ab(.))

We adopt Reiter et al. convention that Ab(a) is a literal which holds when Accusable Object a is behaving abnormally.

Ab(.) is a unary predicate. Semantically, Ab(.) represents the abnormality of an Accusable Object; while ¬Ab(.) represents its normality.

### 4.4. Definition 4. (Failure Condition)

A Failure Condition is a logical constant that designates a condition having an effect on the airplane and/or its occupants, either direct or consequential, which is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions, or external events.

### 4.5. Definition 5. (Dispatch Condition)

A Dispatch Condition is a logical constant that designates the set of conditions to be fulfilled as specified by MMEL, in order to allow aircraft operation with a specific inoperative item.

Example of dispatch condition: *Cargo Door Inoperative In Closed Position*.

A Dispatch Condition may have one Dispatch Status that can be:

- no dispatch (also denoted "NO GO")
- dispatch under conditions (maintenance (m) or operational (o), it is also denoted "GO IF"),
- dispatch (also denoted "GO").

### 4.6. Definition 6. (Observation)

An observation is a logical constant.

Observations are of two main types: automatic reported observations (e.g. ECAM messages on Airbus A380) and human observations (e.g. check done during the pre-flight inspection).

Examples of observations:

- ECAM Message *APU FAULT*
- Human inspection reporting an *Hydraulic leakage in brake circuit*
- First-order assertion of the Aircraft Condition Monitoring System: *Command Voltage > 5V*
- Built-In Test Software Fault Report Code reported by a sub-system of the aircraft: *3231F542*.

### 4.7. Definition 7. (Predicate Reported(.))

The logical predicate $Reported(.)$ applies on Observations and is defined as follows: $Reported(o)$ is a literal which holds when Observation *o* is reported.

### 4.8. Definition 8. (Detection Mapping)

A Detection Mapping is a finite set of first-order sentences $\{DM_i\}_i$ complying with the following production rules:

*Let* $O_i$ *be an Observation and* $FC_i$ *be a Failure Condition*

$$DM_i = (FC_i \vDash Reported(O_i)) \qquad (1)$$

$$DM_i = (\neg FC_i \vDash Reported(O_i)) \qquad (2)$$

### 4.9. Definition 9. (System Pattern)

A System Pattern is a finite set of first-order sentences $\{SP_i\}_i$ complying with the following production rules:

*Let* $AO_i$ *be some Accusable Objects. Let* $FC_i, FC_j, FC_k$ *be some Failure Conditions. Let* $DC_p, DC_q, DC_r$ *be some Dispatch Conditions.*

$$SP_i = \left(Ab(AO_i) \vDash FC_j\right) \qquad (3)$$

$$SP_i = \left(FC_i \vDash FC_j\right) \qquad (4)$$

$$SP_i = \left(FC_i \wedge FC_j \vDash FC_k\right) \qquad (5)$$

$$SP_i = \left(\neg FC_i \wedge FC_j \vDash FC_k\right) \qquad (6)$$

$$SP_i = \left(FC_i \vDash DC_n\right) \qquad (7)$$

$$SP_i = \left(DC_p \vDash DC_q\right) \qquad (8)$$

$$SP_i = \left(DC_p \wedge DC_q \vDash DC_r\right) \qquad (9)$$

## 5. FROM FAULT TOLERANCE TO MARGIN VERSUS EFFECTS

### 5.1. Definition 10. (Aircraft Diagnosis)

Let $R$ be a set of reported Observations.

$$R = \{Reported(o_i)/o_i \text{ is an } Observation\}$$

A diagnosis $\Delta$ for an aircraft $(SP, AO, DM)$ with given reported Observations R, is a set of Accusable Objects such that:

$$SP \cup DM \cup \left\{\bigwedge_{f \in \Delta_F} Ab(f)\right\} \cup \left\{\bigwedge_{h \in \Delta_H} \neg Ab(h)\right\} \vDash R \qquad (10)$$

$$\Delta = \Delta_F \cup \Delta_H$$

$$\Delta_F \cap \Delta_H = \emptyset$$

$\Delta_F$ is called the set of *faulty* Accusable Objects, $\Delta_H$ is called the set of *healthy* Accusable Objects.

### 5.2. Definition 11. (Aircraft Preventive Diagnosis)

Let $DC$ be a set of Dispatch Conditions.

Let $R$ be a set of reported Observations.

$R = \{Reported(o_i)/o_i \text{ is an } Observation\}$.

A preventive diagnosis $\Delta_P$ preventing from $DC$ for an aircraft $(SP, AO, DM)$ with given reported Observations R, is a set of Accusable Objects such that:

$$SP \cup DM \cup \left\{\bigwedge_{f \in \Delta_{PF}} Ab(f)\right\} \cup \left\{\bigwedge_{h \in \Delta_{PH}} \neg Ab(h)\right\} \vDash R \cup DC \qquad (11)$$

$$\Delta_P = \Delta_{PF} \cup \Delta_{PH}$$

$$\Delta_{PF} \cap \Delta_{PH} = \emptyset$$

$\Delta_{PF}$ is called the set of *preventive faulty* Accusable Objects, $\Delta_{PH}$ is called the set of *preventive healthy* Accusable Objects.

### 5.3. Solving Aircraft Diagnosis or Aircraft Preventive Diagnosis

A possible solving process for Aircraft Diagnosis or Aircraft Preventive Diagnosis can be the General Diagnostic Engine (GDE, J. de Kleer and B. C. Williams, 1987), as proven in (N. Belard, 2012).

### 5.4. Definition 12. (Remaining Margin)

Let $DC$ be a set of Dispatch Conditions.

Let $R$ be a set of reported Observations.

Let $A_c$ be an aircraft $(SP, AO, DM)$.

Let $D$ be the set of all Aircraft Diagnosis for $A_c$ with given reported $R$.

Let $P$ be the set of all Aircraft Preventive Diagnosis preventing from $DC$ for $A_c$ with given reported $R$.

For a given $\Delta_P$ in P, a Remaining Margin $\mu$ is a set of Accusable Objects in $AO$ such that:

$$\mu = \{o \epsilon AO\}$$

$$\exists \Delta_P \epsilon P \; such \; that \; \forall o \in \mu, o \epsilon \Delta_P \; and \; Ab(o) \qquad (12)$$

$$\nexists \Delta \in D \; such \; that \; \forall o \in \mu, o \in \Delta \qquad (13)$$

In other words, all objects *o* are suspected within an aircraft preventive diagnosis but the objects *o* are not suspected in any aircraft diagnosis.

### 5.5. Definition 13. (Remaining Distance)

The Remaining Distance $d_\mu$ of a Remaining Margin $\mu$ is defined as the cardinality of $\mu$:

$$d_\mu = |\mu| \qquad (14)$$

### 5.6. Definition 14. (Remaining Risk Rate)

Let suppose that a failure rate is attributed to every Accusable Object in the aircraft.

$$o \epsilon AO \rightarrow \lambda(o) \epsilon ]0,1[$$

The Remaining Risk Rate $\rho_\mu$ of a Remaining Margin $\mu$ is the scalar product of the failure rates of all Accusable Objects in the Remaining Margin:

$$\rho_\mu = \prod_{o \epsilon \mu} \lambda(o) \qquad (15)$$

## 6. REPRESENTATION BASED ON ORIENTED GRAPHS

For a more intuitive representation that is easier to handle by aircraft systems engineers, we use oriented graphs to represent the logical model defined by a given aircraft with reported observations.

The industrial method to build the oriented graphs was defined by Airbus and is available in (Cheriere et al, 2010, 2012).

### 6.1. Oriented Graph of an Aircraft

Let $A_c$ be an Aircraft (SP, AO, DM).

The oriented graph for the aircraft $A_c$ is composed such that the nodes are defined by:

- Ab(A) where A is any Accusable Object,
- Failure Conditions,
- Dispatch Conditions,
- Reported(o) where o is any Observation,
- Logical connector AND
- Logical connector OR
- Logical NOT

And the oriented edges are defined by the entailments given in the System Pattern and the System Mapping, knowing that the logical connectors "AND", "OR", and "NOT" are treated as logic gates.

NB: Other Gates like "XOR" (exclusive OR), ≥N (N true at least) can be obtained thanks to the usual basic logic gates.

### 6.2. Interface Failure Condition

Any Failure Condition node in the Aircraft Graph that has no successor is named *Interface Failure Condition*.

Indeed, the Aircraft Graph may cover only a part of all aircraft systems and these nodes stand for the interfaces with external systems.

### 6.3. Example

#### 6.3.1. Introduction

Let's base the example on an aircraft landing gear system. The Figure 1 depicts an example of landing gear system of the Airbus A380.

Figure 1. A380 body and wing landing gears.
Source: Wikipedia, Florian Lindner, March 2014

The position of a landing gear door is sensed thanks to proximity sensors. The Figure 2 shows the principle of a proximity sensor.

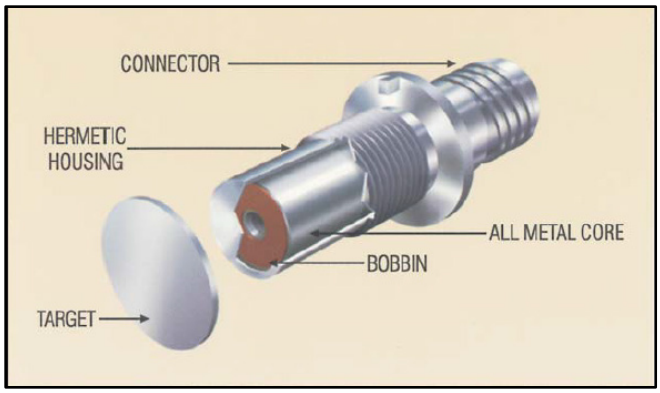


Figure 2. Principle of Proximity Switch Sensor.
Source: Crane Aerospace and Electronics, March 2014.
www.craneaerospace.com

The Proximity Switch Sensor is connected to a remote data concentrator that is an avionics unit providing the sensor with electrical power. The sensor gives a different current if the target (fixed on aircraft body) is close or not to the sensor (fixed on the actuated door). This information is used within the control loop of the door by the corresponding side of the landing gear control system.

For a same position, there are two redundant proximity switch sensors that are reporting to two redundant remote data concentrators.

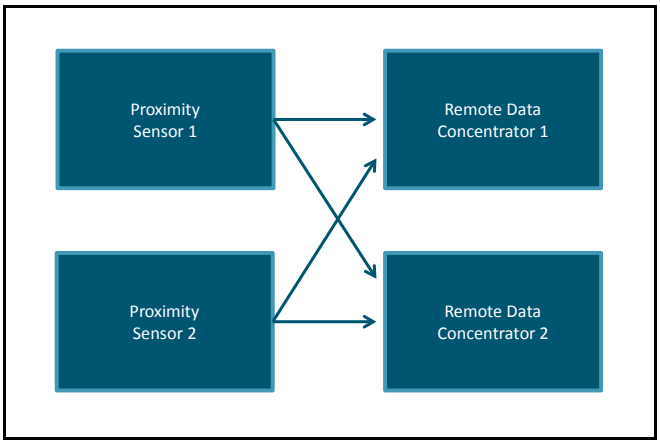


Figure 3. Redundancy Principle for the Feedback of Proximity Sensors

As soon as the door position is lost from one redundant side of the system, the pilot will be informed of this failure by a dedicated ECAM message displayed in the cockpit.

The aircraft dispatch with no landing gear available control is not allowed by the Minimum Equipment List.

It means that it is not allowed to dispatch the aircraft with the ECAM message "LOSS OF LANDING GEAR CONTROL 1+2".

### 6.3.2. Accusable objects

If we limit our Aircraft to the objects at stake in Figure 3, the list of accusable objects is:

- $AO_{11}$: Hardware Proximity Sensor 1
- $AO_{21}$: Hardware Remote Data Concentrator 1
- $AO_{31}$: Software hosted on Remote Data Concentrator 1
- $AO_{41}$: Wiring from Proximity Sensor 1 to Remote Data Concentrator 1
- $AO_{51}$: Wiring from Proximity Sensor 1 to Remote Data Concentrator 2
- $AO_{61}$: On-going Maintenance Condition: Remote Data Concentrator 1 initiated test in progress

The objects are symmetrical for the side 1 and the side 2. The side 2 will give the symmetrical set of accusable objects.

- $AO_{12}$: Hardware Proximity Sensor 2
- $AO_{22}$: Hardware Remote Data Concentrator 2
- $AO_{32}$: Software hosted on Remote Data Concentrator 2
- $AO_{42}$: Wiring from Proximity Sensor 2 to Remote Data Concentrator 1
- $AO_{52}$: Wiring from Proximity Sensor 2 to Remote Data Concentrator 2

- $AO_{62}$: On-going Maintenance Condition: Remote Data Concentrator 2 initiated test in progress

#### 6.3.3. Failure Conditions

In the example, the failure conditions that would be considered are:

- $FC_{11}$: Inconsistent current from Proximity Sensor 1
- $FC_{21}$: Current provided by Proximity Sensor 1 is not processed by Remote Data Concentrator 1
- $FC_{31}$ : Current provided by Proximity Sensor 1 is incorrectly acquired by Remote Data Concentrator 1
- $FC_{41}$: Loss of electrical continuity between Proximity Sensor 1 and Remote Data Concentrator 1
- $FC_{51}$: Loss of electrical continuity between Proximity Sensor 1 and Remote Data Concentrator 2
- $FC_{61}$ : Position information provided by Proximity Sensor 1 is incorrectly processed by Remote Data Concentrator 1
- $FC_{71}$: Feedback of door position on side 1 does not correspond to real door position
- $FC_{80}$ : Door position information are inconsistent between Side 1 and Side 2

The side 2 will bring symmetrical failure conditions (replace 1 by 2).

- $FC_{12}$: Inconsistent current from Proximity Sensor 2
- $FC_{22}$: Current provided by Proximity Sensor 2 is not processed by Remote Data Concentrator 2
- $FC_{32}$ : Current provided by Proximity Sensor 2 is incorrectly acquired by Remote Data Concentrator 2
- $FC_{42}$: Loss of electrical continuity between Proximity Sensor 2 and Remote Data Concentrator 1
- $FC_{52}$: Loss of electrical continuity between Proximity Sensor 2 and Remote Data Concentrator 2
- $FC_{62}$ : Position information provided by Proximity Sensor 2 is incorrectly processed by Remote Data Concentrator 2
- $FC_{72}$: Feedback of door position on side 2 does not correspond to real door position

#### 6.3.4. Dispatch Conditions

In the example, let's consider the dispatch conditions:

- $DC_{10}$: The landing gear system cannot determine the real door position on side 1.
- $DC_{20}$: The landing gear system cannot determine the real door position on side 2.
- $DC_{30}$: The landing gear system cannot determine the real door position on side 2.

From the Minimum Equipment List, the dispatch condition $DC_{30}$ has a NO DISPATCH status, i.e. the airline is not authorized to fly the aircraft with this condition.

#### 6.3.5. Observations

In the example, the possible observations are:

- $OBS_{11}$: LOSS OF LANDING GEAR CONTROL 1 (ECAM Message)
- $OBS_{21}$: Conversion of Proximity Sensor 1 current by Remote Data Concentrator 1 is not plausible. (Built-In Test Report From Side 1)
- $OBS_{31}$: The Proximity Sensor 1 is disconnected from Remote Data Concentrator 1 (Human Observation)
- $OBS_{41}$: The Proximity Sensor 1 is disconnected from Remote Data Concentrator 2 (Human Observation)
- $OBS_{12}$: LOSS OF LANDING GEAR CONTROL 2 (ECAM Message)
- $OBS_{22}$: Conversion of Proximity Sensor 2 current by Remote Data Concentrator 2 is not plausible. (Built-In Test Report From Side 2)
- $OBS_{32}$: The Proximity Sensor 2 is disconnected from Remote Data Concentrator 1 (Human Observation)
- $OBS_{42}$: The Proximity Sensor 2 is disconnected from Remote Data Concentrator 2 (Human Observation)
- $OBS_{50}$ : ACMF Parameter LG_CTL_1=FAILED and ACMF Parameter LG_CTL_2=FAILED
- $OBS_{60}$: LOSS OF LANDING GEAR CONTROL 1+2 (ECAM Message)

#### 6.3.6. Oriented Graph of the Aircraft

The corresponding oriented graph for the example is given on Figure 4.

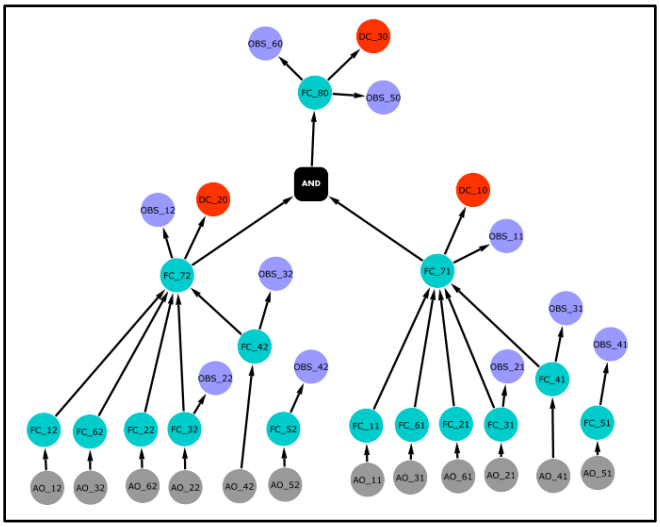


Figure 4. Oriented Graph of the Example

### 6.3.7. Aircraft Diagnosis

On the example, let's assume that R is the set of following reported Observations:

$$R = \{Reported(OBS_{21}), Reported(OBS_{11})\}$$

Then the diagnosis Δ for the aircraft $(SP, AO, DM)$ with given reported Observations R, is:

$$\Delta = \{Ab(AO_{21})\}$$

The Figure 5 illustrates the propagation path that stands for all entailments from $Ab(AO_{21})$ to $Reported(OBS_{11})$ and $Reported(OBS_{21})$.

This figure illustrates that the graphical representation is an easy way to understand and follow how failure can propagate. When engineers design new aircraft, it is a powerful mean to share knowledge and to brainstorm on failure scenarios.

For diagnostic tool, it is a convenient representation to display details in deep troubleshooting mode. Indeed, graph is a familiar way to figure out the path from one point to another point.

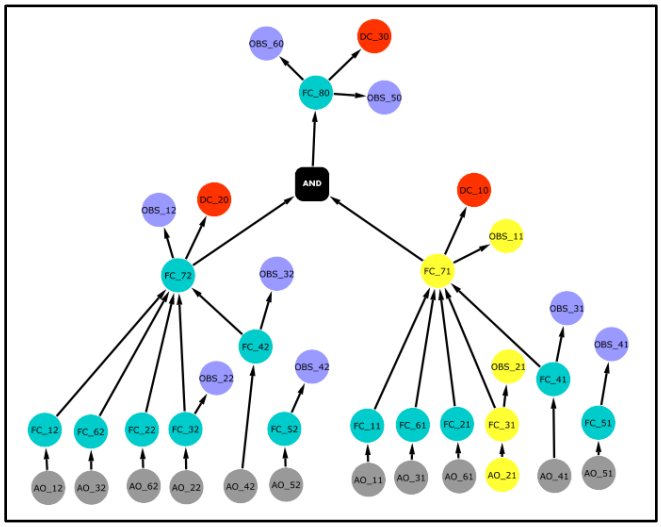


Figure 5. Nodes involved in the propagation path (highlighted in yellow)

### 6.3.8. Aircraft Preventive Diagnosis

On the example, let consider the Dispatch Condition $DC_{30}$ that has a NO DISPATCH status. The Aircraft Preventive Diagnoses preventing from $DC_{30}$ for the aircraft $(SP, AO, DM)$ with given reported Observations R are:

- $\Delta_P^1 = \{Ab(AO_{21}) \wedge Ab(AO_{12})\}$
- $\Delta_P^2 = \{Ab(AO_{21}) \wedge Ab(AO_{32})\}$
- $\Delta_P^3 = \{Ab(AO_{21}) \wedge Ab(AO_{62})\}$
- $\Delta_P^4 = \{Ab(AO_{21}) \wedge Ab(AO_{22})\}$
- $\Delta_P^5 = \{Ab(AO_{21}) \wedge Ab(AO_{42})\}$

### 6.3.9. Remaining Margins and Distances

From the Aircraft Diagnoses and Preventive Aircraft Diagnoses previously determined, let's give the corresponding remaining margins and distances:

- For $\Delta_P^1$, the Remaining Margin is $\mu_P^1 = \{AO_{12}\}$ and $d_{\mu_P^1} = 1$.
- For $\Delta_P^2$, the Remaining Margin is $\mu_P^2 = \{AO_{32}\}$ and $d_{\mu_P^2} = 1$.
- For $\Delta_P^3$, the Remaining Margin is $\mu_P^3 = \{AO_{62}\}$ and $d_{\mu_P^3} = 1$.
- For $\Delta_P^4$, the Remaining Margin is $\mu_P^4 = \{AO_{22}\}$ and $d_{\mu_P^4} = 1$.
- For $\Delta_P^5$, the Remaining Margin is $\mu_P^5 = \{AO_{42}\}$ and $d_{\mu_P^5} = 1$.

### 6.3.10. Remaining Risk Rate

If we suppose that each accusable object $AO_i$ is attached with a respective failure rate $\lambda_i$, then the remaining risk rates for the remaining margins in the example are respectively:

- Let $\lambda_{12}$ be the failure rate of $AO_{12}$. Given the remaining margin $\mu_P^1$, let's apply the equation (15) of the Definition 14. (Remaining Risk Rate). It yields to: $\rho_{\mu_P^1} = \lambda_{12}$

Likewise, we get the other remaining risk rates:

- $\rho_{\mu_P^2} = \lambda_{32}$
- $\rho_{\mu_P^3} = \lambda_{62}$
- $\rho_{\mu_P^4} = \lambda_{22}$
- $\rho_{\mu_P^5} = \lambda_{42}$

This enables to assess the risk that $DC_{30}$ occurs in the next flights, and to decide to do preventive maintenance on $AO_{21}$, in order to keep an acceptable risk rate.

By this way, the risk of NO DISPATCH can be managed optimally according to the operational conditions of the airline.

For instance, let's suppose that:

$$\max(\lambda_{12}, \lambda_{32}, \lambda_{62}, \lambda_{22}, \lambda_{42}) > R$$

where $R$ is the maximum threshold accepted by the airline before triggering preventive maintenance. Then it is worth to repair the accusable object $AO_{21}$ in order to gain tolerance margins against the dispatch condition $DC_{30}$.

The aircraft will continue its flight operations, being allowed to fly without any operational interruption, complying with airline (and passengers) expectations.

## 7. APPLICATION ON A380 AND LESSONS LEARNT

This approach was applied on Airbus A380 aircraft to model several systems and a real-time diagnostic algorithm enables to compute the Aircraft Diagnosis and Aircraft Preventive Diagnosis based on the aircraft model and the real-time observations collected from aircraft in real-time.

The Figure 6 depicts the principle of this real-time application.

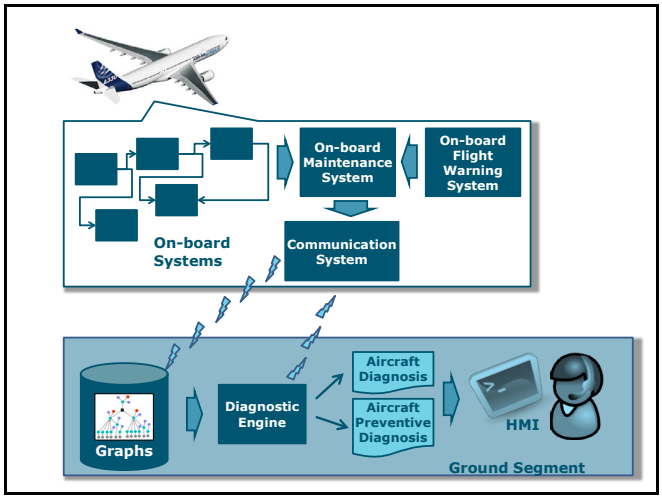


Figure 6. Principle of the real-time processing applied on A380

The integrated aircraft graph includes more than 170,000 nodes.

Observations are automatically downloaded from aircraft to Airbus ground segment, even if the aircraft is still in-flight. These observations are the ones automatically detected by on-board systems: Continuous Built-In Tests reports, Flight Warning ECAM (Electronic Centralized Aircraft Monitor) messages, but also Aircraft Condition Monitoring Parameters that can be requested from Aircraft upon demand by the Human Operator. The Aircraft Diagnosis and the associated Aircraft Preventive Diagnosis are computed by a Diagnostic Engine reasoning on the oriented graph model.

This experience enabled to identify the following lessons learnt:

- This approach enables to get a very accurate diagnosis taking benefit from in-service experience. Indeed, the graph model can be updated on ground segment according to best in-service feedbacks.
- This Preventive Diagnosis enables to identify the risky upcoming Dispatch Conditions, so that Airbus is able to advice the airline about the best preventive maintenance to perform in order to avoid any delay, flight cancellation or high unscheduled maintenance costs.
- Nevertheless, the experience showed that Preventive Diagnosis results need to be handled by Airbus Operators with very good overall knowledge of the aircraft and very high knowledge of the in-service experience, in order them to trigger the advice to Airline at the best time.

The fundamental problem is about predicting the time of next Dispatch Condition occurrence.

That is why it is needed to take benefit from Prognostics in order to provide indication about remaining lifetime before the Dispatch Condition occurs. This remaining lifetime can be used to organize the preventive maintenance from logistics (spare procurement, tools...) to operations (in the best conditions when the aircraft is back at its main base for instance).

## 8. INTEGRATION WITH PROGNOSIS

A way to solve this problem is to integrate the present preventive diagnosis approach with Prognostics that brings the capability to determine the remaining useful life before the occurrence of faults on accusable objects that are in the Remaining Margin.

For this, let's introduce additional logics.

### 8.1. Definition 15. (Degradation Condition)

A Degradation Condition is a logical constant that designates a condition that is an intermediate step on the way to a Failure Condition.

### 8.2. Definition 16. (Additional Production Rules in the Detection Mapping)

Let's extend the Detection Mapping defined in paragraph 4.8 with the following production rules:

*Let $O_i$ be an Observation and $DeC_i$ be a Degradation Condition*

$$DM_i = (DeC_i \vDash Reported(O_i)) \quad (16)$$

$$DM_i = (\neg DeC_i \vDash Reported(O_i)) \quad (17)$$

### 8.3. Definition 17. (Additional Production Rules in the System Pattern)

Let's extend the System Pattern defined in paragraph 4.9 with the following production rules.

*Let $AO_i$ be some Accusable Objects. Let $DeC_i, DeC_j, DeC_k$ be some Degradation Conditions.*

$$SP_i = \left(Ab(AO_i) \vDash DeC_j\right) \quad (18)$$

$$SP_i = \left(DeC_i \vDash DeC_j\right) \quad (19)$$

$$SP_i = \left(DeC_i \wedge DeC_j \vDash DeC_k\right) \quad (20)$$

$$SP_i = \left(\neg DeC_i \wedge DeC_j \vDash DeC_k\right) \quad (21)$$

### 8.4. Definition 18. (Remaining Useful Life Before Failure Condition)

Let's define the following logical relation between Degradation Condition and Failure Condition using modal S5 logics (where ◊ means possibility).

Let's extend production rules of the System Pattern defined in paragraph 4.9 with the following one:

*Let $DeC_i$ be a Degradation Condition and $FC_n$ be a Failure Condition.*

$$SP_i = \Diamond(DeC_i \vDash FC_n)_{RUL} \qquad (22)$$

Meaning that it is possible that the Degradation Condition $DeC_i$ entails the Failure Condition $FC_n$ after the time duration RUL (Remaining Useful Life) has elapsed.

Then we can use the set of Kripke S5-structures where all *possible* worlds *after* RUL time has elapsed are such that

$$(DeC_i \vDash FC_n) \qquad (23)$$

These worlds are accessible by worlds modeled by Eq. (22) before RUL time has elapsed.

Depending on the amount of different RULs expressed in the System Pattern, the number of accessible worlds increases. In other words, Prognostics enables to identify the future accessible worlds that model the aircraft.

### 8.5. Definition 19. (Remaining Useful Life Before Dispatch Condition)

Let $DC$ be a set of Dispatch Conditions.

Let $R$ be a set of reported Observations.

$R = \{Reported(o_i)/o_i\ is\ an\ Observation\}$.

Let's consider a preventive diagnosis $\Delta_P$ preventing from $DC$ for an aircraft $(SP, AO, DM)$ with given reported Observations R, as defined in paragraph 5.2.

Let's $\mu$ be a Remaining Margin for $\Delta_P$, as defined in paragraph 5.4.

Let's $O$ be an accusable object included in $\mu$.

From the System Pattern, let $D_O$ be the set of Dispatch Conditions such that:

$$D_O = \left\{ \begin{matrix} DeC\ such\ that: \\ \forall DC_i \in DC, (Ab(O) \vDash DeC) \text{and} \left(\Diamond(DeC \vDash DC_i)_{RUL_i}\right) \end{matrix} \right\}$$

$D_O$ may be empty.

If $D_O$ is not empty, it enables to point out a subset of $\{RUL_i\}$.

The Remaining Useful Life Before Dispatch Condition is defined as:

$$\begin{matrix} Undefined\ if\ D_O = \emptyset \\ Min(RUL_i), \forall i, otherwise \end{matrix} \qquad (24)$$

### 8.6. Graph representation

The Oriented Graph will be extended with new nodes standing for Degradation Conditions and new edges representing the entailments and possibilities added in paragraphs 8.2, 8.3, and 8.4.

### 8.7. Illustration of RUL on the example

Let's take the landing gear example again.

And let enrich the System Pattern with the Degradation Condition:

- $DeC_1$: Degraded Contact between Proximity Sensor 2 and its target

And with the following knowledge:

- $Ab(AO_{12}) \vDash DeC_1$
- $\Diamond(DeC_1 \vDash FC_{12})_{RUL_1}$

The Figure 7 presents the enriched graph.

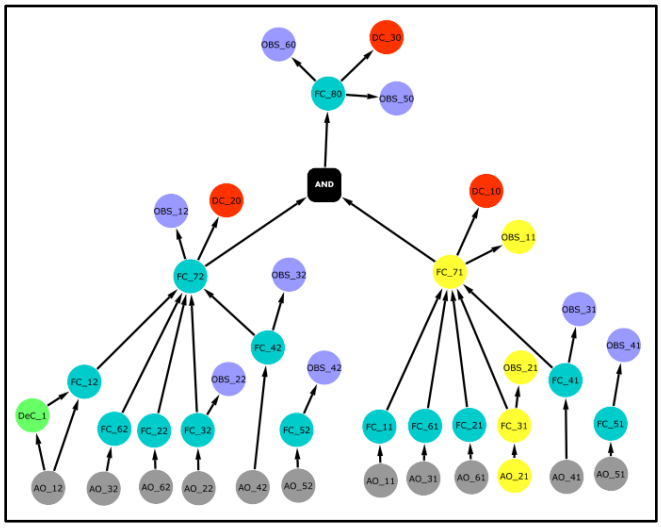


Figure 7. Oriented Graph of the Example, with the Degradation Condition $DeC_1$
(*in green bottom left on* Figure 7)

Taking the same hypotheses as paragraph 6.3.8, the Aircraft Preventive Diagnosis preventing from $DC_{30}$ for the aircraft $(SP, AO, DM)$ with given reported Observations R will be:

- $\Delta_P^1 = \{Ab(AO_{21}) \wedge Ab(AO_{12})\}$
- $\Delta_P^2 = \{Ab(AO_{21}) \wedge Ab(AO_{32})\}$
- $\Delta_P^3 = \{Ab(AO_{21}) \wedge Ab(AO_{62})\}$
- $\Delta_P^4 = \{Ab(AO_{21}) \wedge Ab(AO_{22})\}$
- $\Delta_P^5 = \{Ab(AO_{21}) \wedge Ab(AO_{42})\}$

As well for $\Delta_P^1$, the Remaining Margin is $\mu_P^1 = \{AO_{12}\}$ and $d_{\mu_P^1} = 1$.

And it yields to $D_{AO_{12}} = \{RUL_1\}$.

The Remaining Useful Life Before Dispatch Condition is equal to $RUL_1$. This enables to project the remaining time that is available to do preventive maintenance.

## 9. CONCLUSION AND PERSPECTIVES

Starting from a logical framework to formalize the problem of preventive diagnosis for airlines, the present paper proposed to define the Aircraft Diagnosis and Aircraft Preventive Diagnosis. Then the useful concepts of Remaining Margin, Remaining Distance and Remaining Risk Rate were defined. This paper proposed a graph representation of the logical aircraft model. These concepts were applied by Airbus on A380 aircraft successfully. The experience enabled to identify the need of integrating Aircraft Diagnosis, Aircraft Preventive Diagnosis with information coming from Prognostics. To do this, the logical framework was extended with concepts enabling to introduce the concept of Remaining Useful Life and to do an integrated and consistent logical reasoning with it.

This work could be followed by an extension to concepts of confidence depending on the uncertainty attached with the RUL value that is up to interest for the human decision to order preventive maintenance. Indeed, Modal Logics and validity could help to define a confident diagnosis that would be a true diagnosis in all possible worlds identified by Prognostics.

Moreover, the Graph theory and its applications in Neuroscience and Biology could help to figure out further concepts and algorithms for preventing from future Dispatch Conditions. Indeed, shall we imagine that an Aircraft System Pattern is in fact a very big molecule (of nodes) and that Degradations are in fact chemical reactions changing the composition of this big molecule in time?

## REFERENCES


R. Reiter (1987). A Theory of Diagnosis from First Principles, Artificial Intelligence, 32:57-95, 1987.

J. de Kleer and A. K. Mackworth and R. Reiter(1992). Characterizing Diagnoses and Systems. *Artificial Intelligence*, 56:197–222, 1992.

J. de Kleer and B. C. Williams. (1987) Diagnosing Multiple Faults. *Artificial Intelligence*,32, 1987.

K. D. Forbus and J. de Kleer. (1993) *Building Problem Solvers*, M.I.T. University, Press, 1993.

Y. Shoham (1988) *Reasoning about Change: Time and Causation from the Standpoint of Artificial Intelligence*, Cambridge, Massachussets, The MIT Press.

P. Ribot, Y. Pencolé, M. Combacau. (2008) Prognostics for the maintenance of distributed systems, *PHM'08*, *International Conference on Prognostics and Health Management*, October 6-10, 2008, Denver, USA, 2008.

P. Ribot, Y. Pencolé, M. Combacau. (2009) Diagnosis and prognosis for the maintenance of complex systems. In Proceedings of the *IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. San Antonio, USA. Doi: 10.1109/ICSMC.2009.5346718.

N. Belard (2012) *Reasoning about Models: Detecting and Isolating Abnormalities in Diagnostic Systems*, PhD Thesis, Toulouse, France, 2012.

N. Belard, Y. Pencolé, M. Combacau. (2011) A Theory of Meta-Diagnosis: Reasoning about Diagnostic Systems, *Twenty-Second International Joint Conference on Artificial Intelligence*, 2011.

I. Roychoudhury & M. Daigle (2011): An Integrated Model-Based Diagnostic and Prognostic Framework. *22nd International Workshop on Principle of Diagnosis*, Murnau, Germany.

W. Hodges (2001) *Classical Logic I: First-Order Logic, in Guide to Philosophical Logic*, ed. Louis Goble, Blackwell, Malden Mass. 2001.

J-C. Laprie (1995) Dependable Computing: Concepts, Limits, Challenges, Invited paper to FTCS-25, the *25th IEEE International Symposium on Fault-Tolerant Computing*, Pasadena, California, USA, June 27-30, 1995, Special Issue, pp. 42-54.

J. de Kleer, J. Kurien (2003) Fundamentals of model-based diagnosis, *5th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*, 2003.

V. Chérière, C. Abelin, J. Roger, L. Vilalta-Estrada (2010) *Procédé, dispositif et programme d'ordinateur d'aide au diagnostic d'un système d'un aéronef, utilisant des graphes d'événements redoutés*, Institut National de la Propriété Industrielle, Brevet 2966616, Enregistrement 1004161.

V. Chérière, J. Roger, V. Debray, B. Fabre, P. Chantal (2012) *Procédé, dispositif et programme d'ordinateur d'aide au diagnostic préventif d'un système d'un aéronef, utilisant des graphes d'événements redoutés*, Institut National de la Propriété Industrielle, Brevet 2989499, Enregistrement 1253383.

V. Chérière, J. Roger, L. Vilalta-Estrada, I. Geanta (2012) *Procédé, dispositif et programme d'ordinateur d'aide à l'analyse de la tolérance aux pannes d'un système d'un aéronef, utilisant des graphes d'événements redoutés*, Institut National de la Propriété Industrielle, Brevet 2989500, Enregistrement 1253384.


## BIOGRAPHIES

**Vincent Chérière** received his M.S. degree in Aeronautics and Space from ISAE SUPAERO Toulouse, France, in 2002. He worked for some years in the Automotive Industry for Engine Control Design and especially the On-Board Diagnosis of Diesel Engines at Peugeot Citroën Automobiles. Next, he joined Airbus to work on Research Projects relating to Aircraft Diagnostics, Prognostics, and Data Integration.