Generic characterization of diagnosis and prognosis for complex heterogeneous systems

Pauline Ribot[1], Yannick Pencolé[2], and Michel Combacau[3]

[1,3] *Université Paul Sabatier, University of Toulouse, France*

[1,2,3] *LAAS-CNRS, Toulouse, France*
pauline.ribot@laas.fr
yannick.pencole@laas.fr
michel.combacau@laas.fr

ABSTRACT

Maintenance efficiency of complex industrial systems is an important economical and business issue. Main difficulties come from the choice of maintenance actions. A wrong choice can lead to maintenance costs that are not acceptable. In this paper, we propose a generic health monitoring system that integrates some diagnostic and prognostic capabilities to determine the current and future state of a large and complex system such as an aircraft. The diagnostic function aims at identifying faulty components that may cause global system failures. The prognostic function estimates the remaining time until the next global system failure. A formal and generic modeling framework for a complex system encapsulating the knowledge required to get the consistent coordination of the diagnostic and prognostic functions is presented. We propose in this framework to take into account component redundancies which is common in systems like aircrafts. Moreover, an original coupling of diagnosis and prognosis is established based on the characterization of the system operational modes and on a decentralized architecture of the monitoring system.

1. INTRODUCTION

Maintenance efficiency of industrial systems, like aircrafts or cars, is an economical and business issue. It is a way to improve reliability, security, safety and reduce the final cost of systems. The main difficulties come from the choice of maintenance actions. A maintenance action consists in replacing a component of the system which is not able to perform its set of functions any more. A wrong choice of maintenance action can lead to the system unavailability and implies unacceptable costs. That is the reason why automated diagnostic capabilities are required to efficiently detect and isolate the faults throughout the system. Moreover, in order to reduce the system unavailability, it is necessary to perform preventive maintenance, that is to replace components before they get faulty and propagate failures in the system and then to reduce the number of replacements after the occurrence of a fault. Generally preventive maintenance only relies on reliability analyses and does not take the real solicitations of the system into account.

Nowadays, with help of new technologies and sensors, it is still possible to improve the maintenance capabilities of a complex system by deploying a complete on-board health monitoring system with two capabilities: on-line diagnosis and on-line prognosis. By analyzing the flow of observations (measurements), diagnosis aims at precisely determining online the present set of faulty components that cause the system failures and which have to be replaced (Hamscher, Console, & De Kleer, 1992; Isermann, 2005). As opposed to reliability analyses, prognosis aims at evaluating/updating the system remaining useful life (RUL for short) (Kirkland, Pombo, Nelson, & Berghout, 2004; Wilkinson, Humphrey, Vermeire, & Houston, 2004) by taking into account the real solicitations (temperature, humidity, vibrations, voltage, or any other stress factor) of the system at operating time. Indeed, solicitations at operating time may accelerate or slow down the system degradation and the on-line analysis of these solicitations can optimize the cost of preventive maintenance by a more accurate RUL estimation (Engel, Gilmartin, Bongort, & Hess, 2000). In particular, faulty components may induce abnormal solicitations on the other components of the system and could modify the overall system RUL (Kacprzynsk, Sarlashkar, Roemer, Hess, & Hardman, 2004).

The main contribution of this paper is a formal characteriza-

tion of a generic on-line health monitoring system (HMS for short) for the maintenance of complex system like an aircraft that embeds diagnosis and prognosis capabilities.

This contribution relies on a detailed analysis of a real industrial HMS that is developed by our aeronautical partner AIRBUS. This analysis has been done thanks to a strong collaboration with the AIRBUS maintenance department.[1]

Our characterization is formal and modular and defines the requirements that local diagnosis/prognosis methods should implement to guarantee the global health monitoring function. This characterization is motivated by a set of challenges and difficulties that any realistic HMS should deal with (see Section 2 for details). The second contribution of this paper is the formal characterization of an original coupling between diagnosis and prognosis that shows how diagnosis can assist prognosis. Introduced concepts are finally illustrated on a complete example and a scenario.

The paper is organized as follows. We first present the motivations and the challenges of this work in Section 2. The generic modeling framework of a complex system is presented in Section 3. The characterization of the diagnostic and prognosis functions is then described in Section 4 as well as their coupling. Section 5 illustrates this framework on an example inspired from the PHM literature. Related Work is presented in Section 6.

2. MOTIVATIONS AND CHALLENGES

Optimising the maintenance cost of a system is a very difficult problem as the maintenance process can fail or be delayed for many reasons and its global cost can explode. To ensure a successful maintenance process, one crucial part is the use of a HMS that maintainers can *trust*.

An HMS that can be trusted must be able to always provide a *complete* and *consistent* understanding of the current health of the system (for emergency repair) and an estimate about the remaining time before the system globally fails (for preventive maintenance). Completeness is obviously necessary as any replaceable part of the system can fail. Consistency is also necessary to avoid wrong maintenance actions: if the health monitoring system only suspects healthy components instead of the faulty ones, maintenance actions derived from this wrong statement are obviously unnecessary and the global cost for troubleshooting and maintenance can dramatically increase due to the use of off-line testing methods to really isolate the problem and fix it. To develop and deploy a HMS that is complete and consistent, the first step is thus its *formal characterization*. With a formal characterization, it is then possible:

1. to define how the different parts of the HMS will communicate to provide a *consistent*, *accurate* and *complete* estimate of the system health state,
2. to select the modeling and engineering tools and/or the formal language to develop one part of the HMS in particular; as long as any developed part of the HMS fulfills the formal characterization, it is then easier to guarantee the global consistency of the HMS.

The second challenge before developing a HMS is to deal with the fact that a real system (like an aircraft) is a large assembling of components whose nature can be very different (mechanical, hydraulic, electrical, software, etc). This reality has two consequences. The first and most obvious one is that the HMS must be *modular*: it requires the development of different diagnosis/prognosis techniques (a technique depending on the type of component) that are able to communicate together. The second consequence is that components may be designed by different companies and confidentiality issues raise. The developer of the system may not have the right to know how a component really works internally: the HMS must then be *decentralized*, some sub-parts are designed by the owners of the components and the system owner is in charge of developing the communication between these parts to reach global consistency.

The third challenge we are dealing with when developing a modern HMS is about the redundancy in the system. In critical systems, there exist several set of resources/components that can perform the same set of functions to avoid that if a failure occurs on one set, the system functions are not lost because the system can switch on the redundant components to operate (this is typical in an aircraft). From a maintenance point of view, redundancy implies that a system can work properly even if it contains faulty components, maintenance actions may not be immediately required, the diagnosis of the current health of the system should be able to take redundancy into account.

Last but not least, modern HMSes must provide two types of information, one for normal maintenance (what is the current health of the system?) and another one for preventive maintenance (what is the prediction for the time of the next fault occurrence?). It implies that an HMS must implement *diagnosis* processes and *prognosis* processes. Prognosis methods now can benefit of aging sensors, health indicators to estimate the current aging of a component and then predicts its RUL. Moreover, prognosis and diagnosis are not independent in the sense that the result of the diagnosis can be useful to improve the performance of the prognosis by providing other estimates of the current aging of a component.

3. MODELING FRAMEWORK FOR MONITORING A COMPLEX SYSTEM

To characterize a HMS on a complex system, it is required to find an abstracted but common formal framework based on

[1]This work is partly supported by the ARCHISTIC project in collaboration with Airbus France and National Engineering School of Tarbes, France.

which the different maintenance functions (monitoring, diagnosis, prognosis, troubleshooting,...) can be defined and then implemented. This section is about such a formal framework.

3.1. Preliminaries

Definition 1 (Parameter)**.** *A* parameter *is a variable that represents a quantity or a property in a model.*

A parameter may have a continuous domain (for instance a temperature, a pressure, a speed,...), a discrete domain (for instance a boolean signal, a counter). In this framework, for the sake of generality, any time-variant quantity is a parameter. Any subset of the domain of a parameter p is called a *range* and is denoted $r(p)$, the domain of p being the biggest range $r_{max}(p)$. Let $\mathcal{P} = \{p_1, \ldots, p_n\}$ denotes the set of parameters of the system and $r_{max}(\mathcal{P}) = r_{max}(p_1) \times \cdots \times r_{max}(p_n)$, a *trajectory* τ from time t_0 to time t_1 is thus a subset of the space $r_{max}(\mathcal{P}) \times [t_0, t_1]$ such that for any $t \in [t_0, t_1]$, there exists one and only one $(v_1, \ldots, v_n) \in r_{max}(\mathcal{P})$, v_i is called the value of p_i at time t in this trajectory τ. The set of possible trajectories of the system between t_0 and t_1 is denoted $\mathcal{T}(t_0, t_1)$. The principle of modeling a system that evolves from time t_0 to t_1 is thus to design a set of *relations* $\mathcal{R}$ over $r_{max}(\mathcal{P}) \times [t_0, t_1]$ such that

$$\tau \in \mathcal{T}(t_0, t_1) \equiv \forall t \in [t_0, t_1], (v_1, \ldots, v_n, t) \in \tau \wedge \mathcal{R}(v_1, \ldots, v_n, t) \text{ holds.} \quad (1)$$

Depending on the type of system, there are many ways to define $\mathcal{R}$. For continuous systems, $\mathcal{R}$ is usually written as a set of differential equations, for instance a linear time invariant system is modelled by $\dot{x} = Ax + Bu, y = Cx + Du$, where x is called the state of the system, u the inputs, y the outputs and A, B, C, D are constant matrices. In our framework, x, u and y gather the set of parameters $\mathcal{P}$. Similarly, for discrete systems, $\mathcal{R}$ comes usually from equations like $x_{k+1} = Ax_k + Bu_k, y_k = Cx_k + Du_k$ where k is the number of samples over time that can be equivalently represented by automata, Petri nets, etc. For hybrid systems, it is a mix of both representations. And finally, for logical systems, behaviour models are represented with logics, especially first-order logic with statement like $\neg abnormal(x) \wedge adder(x) \wedge input(x, u1) \wedge input(x, u2) \wedge sum(u1, u2, y) \Rightarrow woutput(x, y)$ which represents the nomimal behaviour of an digital adder (Reiter, 1987), here also $\mathcal{P} = \{abnormal(x) \in \{true, false\}, u1 \in \mathbb{N}, u_2 \in \mathbb{N}, y \in \mathbb{N}\}$.

3.2. System and components

Following the preliminaries and for the sake of generality, a *system* is defined as follows.

Definition 2 (System)**.** *A complex system Σ is defined by a pair $\Sigma = \langle \mathcal{P}, \mathcal{R} \rangle$ where:*

- *$\mathcal{P}$ is the set of system parameters,*
- *$\mathcal{R}$ is the set of relations over $r_{max}(\mathcal{P}) \times \mathbb{R}^+$ such that Equation (1) holds.*

Modeling a system usually requires a compositional approach that models a set of N interacting components $Comps = \{C^1, \ldots, C^N\}$. A component C^i is modeled as a part of the system and contains a subset of parameters and a subset of relations (Ribot, Pencolé, & Combacau, 2009a) and is a system on its own.

Definition 3 (Component)**.** *A component $C^i \in Comps$ is defined by a pair $C^i = \langle \mathcal{P}^i, \mathcal{R}^i \rangle$ where:*

- *$\mathcal{P}^i \subseteq \mathcal{P}$ is the set of component parameters,*
- *$\mathcal{R}^i \subseteq \mathcal{P}$ is a set of relations between parameters of $\mathcal{P}^i$ modeling the set of trajectories of C^i.*

In the compositional modeling approach, the model of the system is obtained by composing the component models with help of a *structural model* (Chitttaro, Guida, Tasso, & Toppano, 1993).

3.3. Structural model

Structural models describe the possible set of interactions between components. Usually, interactions are modeled with ports (also called terminals) (Pencolé & Cordier, 2005) which can exchange data, data flow corresponding to a physical flow (like voltage, intensity, pressure, etc.) in the system. Here, ports are parameters.

Definition 4 (Structural model)**.** *The* structural model *of the system is the partial function $St : \mathcal{P} \xrightarrow{St} 2^{\mathcal{P}}$ that represents a flow of information coming from the parameter op and going to the set of parameters $St(op)$.*

As St represents a flow of information, it is assumed that $\{op\} \cap St(op) = \varnothing$. From the structural model follow the underlying relations H_{Struct} about the structural interactions:

$$H_{Struct} : St(op) \ni ip \Rightarrow \ \forall t \in \mathbb{R}^+ \ \ op(t) = ip(t). \quad (2)$$

Intuitively speaking, if op is structurally linked with ip, it means that for any trajectory of the system and at any time, op and ip share the same value. The structural model induces some new notions.

Definition 5 (Output/Input system parameters)**.** *The* output parameters *$\mathcal{OP}$ is the subset of $\mathcal{P}$ where St is defined. The* input parameters *$\mathcal{IP}$ is $\mathcal{IP} = \{ip \in \mathcal{P}, \exists op \in \mathcal{OP}, St(op) \ni ip\}$.*

Any input parameter of $\mathcal{IP}$ is involved in only one connection, which means that $\forall op, op' \in \mathcal{OP}, op \neq op' \Rightarrow St(op) \cap St(op') = \emptyset$.

Definition 6 (Output/Input/Private component parameters)**.** *Let $C^i \in Comps$ denote a component:*

- *$\mathcal{OP}^i = \mathcal{P}^i \cap \mathcal{OP}$ is the set of* output parameters *of C^i;*
- *$\mathcal{IP}^i = \mathcal{P}^i \cap \mathcal{IP}$ is its set of* input parameters*;*
- *$\mathcal{PP}^i = \mathcal{P}^i \setminus (\mathcal{OP}^i \cup \mathcal{IP}^i)$ is its set of* private parameters*.*

Intuitively, the value of an input parameter in $\mathcal{IP}^i$ is determined by H_{Struct} conditions. Mechanisms and internal resources of component C^i cannot modify the value of an input parameter. The value of an output parameter in $\mathcal{OP}^i$ results from the internal resources and the mechanisms implemented by C^i and its input parameters. A private parameter represents an internal characteristic, specific to a component like a physical property, an internal state and more importantly, as described in Section 3.5, a fault in a diagnosis/prognosis problem.

Figure 1 represents a component C^1 with three input parameters $ip^{1,1}$, $ip^{1,2}$, $ip^{1,3}$, two output parameters $op^{1,1}$, $op^{1,2}$ and two private parameters $pp^{1,1}$, $pp^{1,2}$. $ar^{1,1}$ and $ar^{1,2}$ are relations involving this set of parameters.

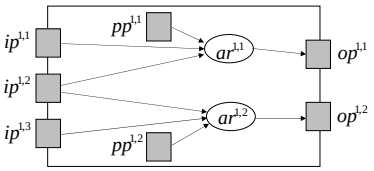

Figure 1. Component and parameters

Finally, the compositional modeling is obtained as follows: for any *subsystem* $\Sigma' = \langle \mathcal{P}', \mathcal{R}' \rangle$ composed of the family of components $\{C^i\}_{i \in I \subset \{1,\ldots,N\}, I \neq \varnothing}$:

$$\Sigma' = \langle \bigcup_{i \in I} \mathcal{P}^i, \{H_{struct}\} \cup \bigcup_{i \in I} \mathcal{R}^i \rangle. \tag{3}$$

The compositional modeling of the whole system is the one of the subsystem defined by $I = \{1, \ldots, N\}$.

Figure 2 shows such a sub-system of 4 components $\{C^1, C^2, C^3, C^4\}$ with $St(op^{1,1}) = \{ip^{2,1}\}$, $St(op^{1,2}) = \{ip^{4,1}\}$, $St(op^{3,1}) = \{ip^{4,2}\}$, $St(op^{4,1}) = \{ip^{2,2}\}$ represented by the four oriented connectors.

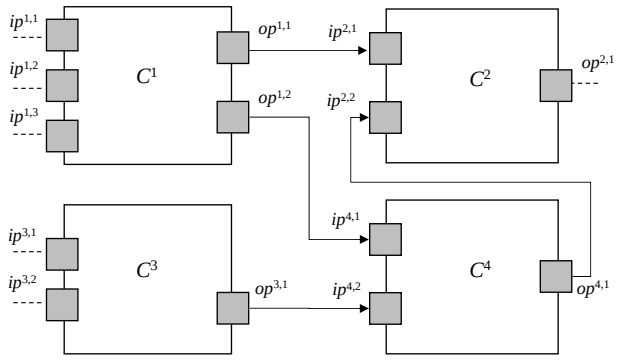

Figure 2. Components and structure

3.4. Functional modeling

A system is usually designed in order to provide a set of functions $\mathcal{FU}$. Among these functions are the goal functions $\mathcal{FU}_g$ (Chitttaro et al., 1993). To perform the goal functions, the components have to implement a set of basic functions $\mathcal{FU}_b \subset \mathcal{FU}$. The set of basic functions implemented by a component C^i is denoted $\mathcal{FU}^i$, thus $\mathcal{FU}_b = \bigcup_{i=1}^{N} \mathcal{FU}^i$. These basic functions rely on the component behavior and are modeled as functional conditions that fully determine an output parameter op^i_j of C^i with respect to its input parameters and its private parameters.

Definition 7 (Functional condition)**.** *The functional condition associated to a basic function of $\mathcal{FU}^i$ is a relation $rel \in \mathcal{R}^i$ such that there exists at least an output parameter $op^i_j \in \mathcal{OP}^i$ so that for any time t, if $(v^i_1, \ldots, v^i_{j-1}, v^i_j, v^i_{j+1}, \ldots, v^i_{n_i}, t) \in rel$ then for any other value $\tilde{v}^i_j \neq v^i_j$, $(v^i_1, \ldots, v^i_{j-1}, \tilde{v}^i_j, v^i_{j+1}, \ldots, v^i_{n_i}, t) \notin rel$.*

A basic function is said to be *available* on a component if its associated functional condition is satisfied. The relations $ar^{1,1}$, $ar^{1,2}$ in Figure 1 model conditions of two basic functions implemented by C^1, they respectively determine $op^{1,1}$ and $op^{1,2}$ (see also Section 5.1.2). Depending on the nature of the system, functional conditions can be written in different forms. For instance, for continuous system, a functional condition is a relation like $y = Cx + Du$. For logical systems, a functional condition in a logical property that determines the output with respect to its input. The logical formula presented in section 3.1 is typically a functional condition as it determines the output y as the sum of u_1 and u_2 and represents the *adding* function.

The functional model of a complex system defines the set of basic functions implemented by components and describes how they are combined in order to perform the goal functions. The composition of basic functions relies on functional dependencies that can be described as follows. The mapping $Pred$ defines the predecessors of functions in $\mathcal{FU}$:

$$\begin{cases} \mathcal{FU} & \stackrel{Pred}{\longrightarrow} & P(\mathcal{FU}) \\ Fu_j & \stackrel{Pred}{\longrightarrow} & Pred(Fu_j) = \{Fu_k, \ldots, Fu_l\}. \end{cases} \tag{4}$$

If $Fu_k \in Pred(Fu_j)$, the function Fu_k is called a predecessor of Fu_j, and the function Fu_j is available if Fu_k is available. $Pred$ can be used to formalize the concepts of basic and goal function.

- Basic function: $Fu \in \mathcal{FU}_b \Leftrightarrow Pred(Fu) = \emptyset$.
- Goal function: $Fu \in \mathcal{FU}_g \Leftrightarrow \forall Fu' \in \mathcal{FU},\ Fu \notin Pred(Fu')$.

The mapping $Pred$ can be graphically represented as a tree structure, called a function tree in Rausand and Hoyland (2004). The definition of the mapping $Pred$ is not accurate enough in the case where a function Fu_j has several predecessors i.e. $||Pred(Fu_j)|| \geq 2$. Indeed, in case of functional

redundancies, the availability of Fu_j may only require the availability of a subset of $Pred(Fu_j)$. The mapping n/m is used for this purpose:

$$\begin{cases} \mathcal{X} \xrightarrow{n/m} P(\mathcal{X}) \\ X \xrightarrow{n/m} \{Y \subseteq X\} \text{ with } n = ||Y|| \text{ and } m = ||X||. \end{cases} \quad (5)$$

Each $Y \in n/m[Pred(Fu_j)]$ is a subset of n predecessors of Fu_j whose availability is a sufficient condition for the availability of Fu_j. It must be noticed that the mapping n/m is a generalization of the classical AND and OR logical operators:

$$\begin{cases} AND & \leftrightarrow & m/m \\ OR & \leftrightarrow & 1/m. \end{cases}$$

These mappings can be used to express redundancies in an functional tree.

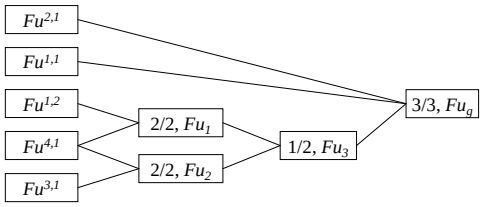

Figure 3. Functional model : composition and redundancies

Figure 3 represents the functional model of the system illustrated in Figure 2. The components C^1, C^2, C^3 and C^4 implement five basic functions $Fu^{1,1}$, $Fu^{1,2}$, $Fu^{2,1}$, $Fu^{3,1}$ and $Fu^{4,1}$ that are composed in order to perform some intermediate functions and then to realize the system goal function Fu_g. The intermediate functions Fu_1 and Fu_2 rely on the implementation of $Fu^{1,2}$, $Fu^{3,1}$ and $Fu^{4,1}$ and are modeled by:

$$\begin{array}{l} 2/2[Pred(Fu_1)] = \{\{Fu^{1,2}, Fu^{4,1}\}\} \\ 2/2[Pred(Fu_2)] = \{\{Fu^{3,1}, Fu^{4,1}\}\}. \end{array} \quad (6)$$

The intermediate function Fu_3 is correctly performed if at least one of the intermediate functions Fu_1 or Fu_2 is correctly performed:

$$1/2[Pred(Fu_3)] = \{\{Fu_1\}\{Fu_2\}\}. \quad (7)$$

This expression describes a functional redundancy. To realize the goal function Fu_g, all function predecessors in $Pred(Fu_g)$ must be available:

$$3/3[Pred(Fu_g)] = \{\{Fu^{2,1}, Fu^{1,1}, Fu_3\}\}. \quad (8)$$

The sets $Comps$, $\mathcal{FU}$ and the mapping $Pred$ derive from the knowledge available at the design stage.

3.5. Modes

As written in Section 3.1, any trajectory $\tau \in \mathcal{T}(t_0, t_1)$ of the system is a time-continuous subset of elements from $r_{max}(\mathcal{P}) \times [t_0, t_1]$ from time t_0 till time t_1. All along this trajectory, the system is going through a set of modes. Generally speaking, a mode is a subset of $r_{max}(\mathcal{P})$. The interest of defining a mode is that it is always characterizing a property that the supervisor wants to detect/isolate by observing the system. Typical properties are failures, faults, degradations...
Definition 8 (Mode)**.** *A* mode m *of the system* $\Sigma = \langle \mathcal{P}, \mathcal{R} \rangle$ *is a subset of* $r_{max}(\mathcal{P})$.

3.5.1. Component modes

Straightforwardly from the definition of functional conditions, one can characterize a set of *functional modes* on a component: considering a functional condition with its relation rel, the functional mode associated to this functional condition is the projection on $r_{max}(\mathcal{P})$ of the set $rel \cap (r_{max}(\mathcal{P}) \times \mathbb{R}^+)$. And then we can say that the component is in such a functional mode iff the associated basic functions are available at this time. The problem is that the definition of *functional modes* is not sufficient. Detecting that a component is failing (i.e. it is out of at least one of the functional modes) is not sufficient to know whether the component must be replaced as the failure may be due to a *fault* in another component, component that must be replaced (failure propagation due to a fault). That is the reason why, in the context of maintenance, the purpose is to detect/isolate/predict *fault modes* that can explain the loss of *functional modes*.

A fault f in a component C is an internal property of the component usually representing a physical problem in the component. In Automatic Control, a fault is usually represented as an input (exogenous) perturbation from the environment. In our framework, it is represented as a private parameter $p_f \in \mathcal{PP}$. The fault f is said to be present at time t iff $p_f \in r_f(p_f) \subset r_{max}(p_f)$. The absence of f is then represented by $p_f \in r_n(p_f) = r_{max}(p_f) \setminus r_f(p_f)$.

The fact that the fault f is represented as a private parameter (endogenous) is crucial, as written before, fault represents physical problems and physical problems may be due to degradation, aging. By representing a fault by a private parameter, we allow to model degradation that *cause* the fault and thus to introduce degradation models for prognosis (see Section 4.3). It is now time to define the classes of operational modes. Operational modes describe fault propagation in the system that induces failures (loss of functions).
Definition 9 (Nominal mode)**.** *The nominal mode* m_n^i *of the component* $C^i = \langle \mathcal{P}^i, \mathcal{R}^i \rangle$ *is characterized by:*

- *for all fault parameter* $p_f^i \in \mathcal{PP}^i$*, its value is in* $r_n(p_f^i)$*;*
- *for all basic function* $Fu^{i,k} \in \mathcal{FU}^i$*, the function condition of* $Fu^{i,k}$ *holds.*

The nominal mode is unique by definition. No fault is present and all the basic functions are available. From the nominal mode, we can derive the nominal range of each parameter $p \in r_n(p)$ as the projection of the nominal mode to $r_{max}(p)$.

The knowledge about the nominal mode m_n^i usually comes from the specification/design stage of the component C^i.

Definition 10 (Fault mode)**.** *The fault mode m_f^i of the component $C^i = \langle \mathcal{P}^i, \mathcal{R}^i \rangle$ is characterized by:*

- *the value of the fault parameter $p_f^i \in \mathcal{PP}^i$ is in $r_f(p_f^i)$.*

A fault mode always induces a loss of function (at least one of the function condition does not hold in a fault mode). A failure will occur as soon as the lost function is utilized. A fault mode of a component C^i is an operational mode with an explicit model (i.e. the relations that rule the mode are known). This means that the fault is perfectly known at the design stage (Hamscher et al., 1992). It is also possible to define multiple fault modes as long as knowledge about how the component behaves under several faults is available (Pencolé & Cordier, 2005).

Definition 11 (Abnormal mode)**.** *An abnormal mode m_a^i of the component $C^i = \langle \mathcal{P}^i, \mathcal{R}^i \rangle$ is characterized by:*

- *an input parameter $p^i \in \mathcal{IP}^i$ is such that $p^i \notin r_n(p^i)$.*

An abnormal mode always induces a loss of function (at least one of the function condition does not hold in an abnormal mode). This loss is due to the fact that an input is out of range and violates at least one functional condition. An abnormal mode may not be represented with explicit relations like fault modes but just characterized by an input parameter out of its range. Finally, for the sake of completeness, we can also cite the so-called *unknown mode* defined as the complement of the set of known modes in $r_{max}(\mathcal{P})$.[2]

3.5.2. Mode of components and system

According to the previous definitions, a set of operational modes is associated to a component C^i; let $\mathcal{M}^i$ be this set[3]. At a given time t, a component C^i is in one mode only that is either the nominal mode (m_n^i) or a mode that can be faulty, abnormal or both.

Definition 12 (Component mode)**.**

$$\begin{cases} Comps \times time \xrightarrow{Mode^C} \bigcup_i \mathcal{M}^i \\ (C^i, t) \longrightarrow Mode^C(C^i, t) = m_x^i \in \mathcal{M}^i. \end{cases}$$

For a complex system Σ with N components $\langle C^1 \dots C^N \rangle$ a *system mode* can also be defined from the knowledge of each component mode. A system mode x is noted m_x^Σ and is formalized by the mapping $Mode^\Sigma$.

Definition 13 (System mode)**.**

$$\begin{cases} time \xrightarrow{Mode^\Sigma} \mathcal{M}^1 \times \ldots \times \mathcal{M}^N \\ Mode^\Sigma(t) = m_x^\Sigma = \langle Mode^C(C^1, t) \dots Mode^C(C^N, t) \rangle \\ \textit{so that in } \ m_x^\Sigma \quad H_{Struct} \textit{ is verified.} \end{cases}$$

[2]The unknown mode is useful when the model is incomplete. The hypothesis of model incompleteness is not in the scope of this paper. So in the following, we do not consider the unknown mode.

[3]As stated previously, a mode is defined as a set of relations so the set of modes fully depends on the available knowledge about the component.

The definitions of nominal, fault and abnormal mode can be extended to the system mode as follows:

- nominal mode m_n^Σ: all components are in nominal mode;
- fault mode m_f^Σ: at least one component is in a fault mode;
- abnormal mode m_a^Σ: at least a component is in an abnormal mode.

Fault propagation is fully represented by an operational system mode. In Figure 2, if C^1 is in a fault mode, C^2, C^3 are in the nominal mode and C^4 is in an abnormal but non-faulty mode, it means that a fault has occurred in C^1 that propagates through $op^{1,2}$ (but not through $op^{1,1}$) and implies failures on C^4. Note that here it also implies that the goal function is failing (see Figure 3) and from a maintenance viewpoint, C^1 must be replaced. If in the tree of Figure 3, $Fu^{4,1}$ and $Fu^{3,1}$ were interchanged, the goal function would be still available because of the redundancy, C^1 could be replaced later.

3.5.3. Sequence of modes

During the system operation, from t_0 till t, the mode of the component C^i changes each time a fault or an abnormal solicitation occurs on it. So, along the operation time of the system, the component C^i follows a sequence of modes $(m_0^i\, m_1^i\, \ldots\, m_j^i)$. This sequence named *the component mode trajectory* is defined at time t by $T^C(C^i, t)$ with

$$\begin{cases} Comps \times time \xrightarrow{T^C} [\mathcal{M}^i]^{j+1} \\ T^C(C^i, t) = (m_0^i\, m_1^i\, \ldots\, m_j^i) \\ T^C(C^i, t) = (Mode^C(C^i, t_0) \dots Mode^C(C^i, t_j)) \\ \text{with } \forall h \in \{0, \ldots, j-1\}, \forall t' \in [t_h, t_{h+1}[, \\ \qquad Mode^C(C^i, t_h) = Mode^C(C^i, t') \\ \text{and } \forall t' \in [t_j, t], Mode^C(C^i, t_j) = Mode^C(C^i, t'). \end{cases}$$

At time t, a sequence of system modes m_x^Σ is named *a system mode trajectory*, is noted T^Σ and is defined by the mapping

$$\begin{cases} time \xrightarrow{T^\Sigma} [\mathcal{M}^1 \times \ldots \times \mathcal{M}^N]^{j+1} \\ T^\Sigma(t) = (m_0^\Sigma\, m_1^\Sigma\, \ldots\, m_j^\Sigma) \\ T^\Sigma(t) = (Mode^\Sigma(t_0) \dots Mode^\Sigma(t_j)) \\ \text{with } \forall h \in \{0, \ldots, j-1\}, \forall t' \in [t_h, t_{h+1}] \\ \qquad Mode^\Sigma(t') = Mode^\Sigma(t_h) \\ \text{and } \forall t' \in [t_j, t], Mode^\Sigma(t_j) = Mode^\Sigma(t'). \end{cases}$$

This definition implicitly defines that the system mode m_j^Σ holds between time t_j and time t_{j+1} as shown in Figure 4. This convention will be used in the sequel of the paper.

Very often, at time t_0, the system is in its nominal mode m_n^Σ. A complete trajectory always ends with a *failure mode* m_p^Σ

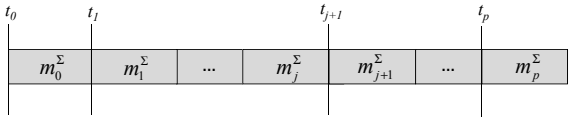

Figure 4. Mode trajectory of the system

in which a goal function is not available any more and thus the system is considered to be non-operational, maintenance is then required (see the example described above).

3.6. Aging modeling

As stated in Section 3.5, a fault is represented by a private parameter that deviated and is out of nominal range, this deviation represents a *degradation* of the component. Knowledge about degradation comes from security analyses of the system components and is contained in *aging models* (also called degradation models or life consumption models in Wilkinson et al. (2004)). An aging model can be a statistical model established by reliability analyses (Kaufman, Grouchko, & Cruon, 1975) or a physical model involving parameters that represent the solicitations on the component (humidity, pressure, vibrations, normal and abnormal inputs, etc.).

Still for the sake of generality in this framework, an aging model is characterized as follows:

Definition 14 (Aging model)**.** *An aging model $ag^{i,k}$ is a relation in $\mathcal{R}^i$ associated to a private parameter $pp^{i,k}$ of the component C^i.*

Aging model $ag^{i,k}$ is the means for predicting the value $\widehat{pp}^{i,k}(t)$ of the parameter $pp^{i,k}$ over the time t. An aging model relies on health indicators describing environmental conditions and faults that are represented as input and private parameters of the component (Ribot, Pencolé, & Combacau, 2009b).

4. FROM DIAGNOSIS TO PROGNOSIS

Section 3 describes the formal characterization of the models that are necessary to perform health monitoring of a complex system. With the notion of mode, the evolution of the system can be abstracted as a trajectory (sequence of modes) that is the sufficient piece of information to provide at the maintenance agent. From a maintenance point of view, two questions must now be answered.

1. What is the current global mode? In other words, are there faulty components that must be replaced immediately?
2. When does a global mode implying a system failure occur in the future? In other words, what is the maximal time before replacing a component that will avoid the next system failure?

The aim of diagnosis and prognosis is to respectively answer questions 1 and 2.

4.1. Observations and mode compatibility

Within this framework, the goal of diagnosis is to determine, at time t, the current mode of the system from which it is possible to determine which components have to be replaced. The diagnosis process involves the measured values of a subset of parameters called the *observations*. Some parameter values are recorded by available sensors within the system, these measurements are called observations. So the set of observations is directly linked to the system monitoring capability. Sensors record values of physical quantities that are represented as input, output or private parameters. A local observation, on a component C^i, at time t is then a measure of the value of a parameter. Such a local observation is denoted $Obs(p^{i,k}, t)$ for the parameter $p^{i,k}$. For a component C^i, the set of parameters is partitioned at time t into the subset of *observed* parameters $\mathcal{P}^i_{Obs}(t)$ (i.e. the set of parameters whose value can be measured at time t) and the subset of *non observed* parameters $\mathcal{P}^i_{\neg Obs}(t)$. Let us note $\{Obs(p^{i,k}, t)\}$ the set of values of the observed parameters at time t.

Definition 15 (Compatibility between a component mode and a set of observations)**.** *At time t, a mode m^i_x of component C^i is said to be compatible with the set of local observations $\{Obs(p^{i,k}, t)\}$ iff :*

$$\begin{cases} \forall p^{i,k} \in \mathcal{P}^i_{Obs}(t),\ Obs(p^{i,k}, t) \in r_x(p^{i,k}); \\ \forall p^{i,j} \in \mathcal{P}^i_{\neg Obs}(t),\ \exists p^{i,j}(t) \in r_x(p^{i,j}) | \mathcal{R}^i \text{ holds}. \end{cases}$$

Definition 15 typically characterizes consistency-based diagnosis. In the logical framework (Reiter, 1987), this notion of compatibility is implemented as checking satisfiability of the diagnosis problem $(SD(C^i), \{Obs(p^{i,k}, t)\}, m^i_x)$ where $SD(C^i)$ is a first-order logic representation of the relations $\mathcal{R}^i$: in other words, is the theory $SD(C^i) \wedge \bigwedge Obs(p^{i,k}, t) \wedge m^i_x)$ satisfiable or not? In the FDI community, compatibility is usually expressed as a set of residuals resulting from the observations $\{Obs(p^{i,k}, t)\}$ that are below a threshold (Isermann, 2005).

Definition 16 (Compatibility between a system mode and a set of observations)**.** *At time t, a system mode $m^\Sigma_x = \langle m^1_{x1}, \ldots, m^N_{xN} \rangle$ is said to be compatible with the set of observations $\bigcup_i \{Obs(p^{i,k}, t)\}$ iff:*

(a) $\forall i \in [1..N], m^i_{xi}$ is compatible with $\{Obs(p^{i,k}, t)\}$

(b) H_{Struct} is verified.

Definition 16 characterizes the decentralized diagnosis problem (Pencolé & Cordier, 2005). Indeed a mode m^i of a component C^i may not be consistent with a mode $m^j, j \neq i$ of a component C^j as m^i and m^j imply inconsistent constraints on a set of parameters (it is the case when m^i asserts that a given parameter p is a range R_i whereas m^j asserts p is a range R_j but the structural model H_{struct} asserts that

$R_i \cap R_j = \varnothing$). Definition 16 ensures the global consistency checking of component modes.

Using Reiter (1987) again, the global consistency checking consists in checking whether the theory $\bigwedge_{i=1}^{N} SD(C^i) \wedge \bigwedge_{i=1}^{N} Obs(p^{i,k}, t) \wedge \bigwedge_{i=1}^{N} m_{xi}^i) \wedge H_{Struct}$ is satisfiable or not. In the context of discrete event systems (Pencolé & Cordier, 2005), this is implemented by the synchronization of shared events defined by H_{struct}. In continuous system, finally, a way to implement this checking between component modes that rely on shared parameters can be found in Indra, Travé-Massuyès, and Chanthery (2011).

4.2. Diagnosis characterization

For complex systems, it is very difficult to think globally in order to directly obtain a diagnosis of the whole system. That is why a set of diagnostic modules is deployed in order to compute *local diagnoses* at the component level and then provide a *global diagnosis* for the whole system (Pencolé & Cordier, 2005).

Definition 17 (Local diagnosis)**.** *The local diagnosis of component C^i at time t is*

$$\Delta^i(t) = \{Mode^C(C^i, t) \textit{ compatible with } \{Obs(p^{i,k}, t)\}\}.$$

Note that the presented definition is the consistency-based diagnosis (see Definition 15): this is the most generic one. Depending on the type of knowledge available in the $\mathcal{R}^i$, it is obviously possible to implement diagnosis methods that can be more accurate/less ambiguous (that is they compute only a subset of modes of $\Delta^i(t)$ using abductive reasoning as defined in the spectrum of diagnosis definitions in Console and Torasso (1991)). The use of abductive reasoning on a component is typical if an FMEA is available as a model of the given component.

Finally, a system diagnosis at time t is built from the knowledge of local diagnosis at time t. Any system mode of the global diagnosis is the assignment of a component mode for any component of the system so that the result is compatible with the whole set of observations (see Definition 16).

Definition 18 (System diagnosis)**.** *A system diagnosis, at time t, $\Delta^\Sigma(t)$ is the subset of system modes formally defined as follows:*

$$\Delta^\Sigma(t) = \{\langle m_{x1}^1, \ldots, m_{xN}^N \rangle\}$$

with

$$\begin{cases} \langle m_{x1}^1, \ldots, m_{xN}^N \rangle \in (\Delta^1(t) \times \ldots \times \Delta^N(t)) \\ \langle m_{x1}^1, \ldots, m_{xN}^N \rangle \textit{ compatible with } \bigcup_i \{Obs(p^{i,k}, t)\}. \end{cases}$$

4.3. Prognosis characterization

As the diagnosis of the system at time t consists in determining the trajectory of past modes of the system from t_0, the prognosis consists in calculating at time t, the trajectory of future fault modes of the system until t_p, the time of the system failure (failure mode). This coupling is illustrated by Figure 5.

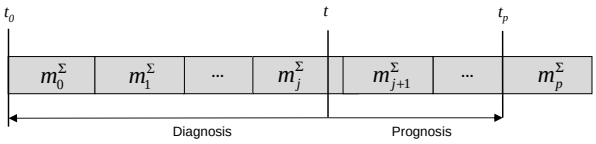

Figure 5. Diagnosis and prognosis of a system Σ

It will never be possible to determine the real trajectory of future modes because the prognosed trajectory has not happened yet. The prognosis at time t consists in estimating the next mode changes based on an evaluation of the system health status.

4.3.1. What can diagnosis offer to prognosis?

Diagnostics and Prognostics are different problems. On one hand, Diagnostics relies on structural, functional and behavioural models to explain the observations by a set of faults that occurred in the system and generate failures throughout the system (see Section 4.2). On the other hand, Prognostics mainly relies on structural and aging models to predict when next faults will occur and generate the same system failures, as it will be formally defined later in Section 4.3.2 and Section 4.3.3. The success of Prognostics requires to solve two sub-problems: the acquisition of the aging models (M. Roemer, Byington, Kacprzynski, & Vachtsevanos, 2005; Ferreiro & Arnaiz, 2008), the acquisition of on-line health indicators. Diagnostics can assist to solve the latter problem. As stated in Section 3.6, the prognosis function relies its computation on the aging model $ag^{i,k}$ available for the component C^i and associated to the parameter $pp^{i,k}$ to predict the value $\widehat{pp}^{i,k}(t')$ for a given time $t' > t$. This computation relies on values of health indicators about C^i that can be directly observed (measured by sensors). However, such health indicators can also be estimated by the current diagnosis $\Delta^i(t)$ issued from the system diagnosis $\Delta^\Sigma(t)$ (in other words we only retain in $\Delta^i(t)$ the set of modes of C^i that appear at least once in $\Delta^\Sigma(t)$). Formally, the prognosis function of C^i will base its computation on the following values of health indicators $\{p^{i,j}\}$:

- direct observation: if $p^{i,j} \in \mathcal{P}^i_{Obs}(t)$, then $p^{i,j}(t) = Obs(p^{i,j}, t)$;
- diagnosis-based estimation $m_x^i \in \Delta^i(t)$: if $p^{i,j} \in \mathcal{P}^i_{\neg Obs}(t)$, it is possible to assign at least one value $v^{i,j} \in r_x(p^{i,j})$.

4.3.2. Local prognosis

The local prognostic function aims at predicting at time t the next mode changes for each component C^i. For this purpose the date t_d of each possible fault occurrence on the components must be computed. At time t, the remaining time until a private parameter $pp^{i,k}$ becomes faulty is denoted $rtf(pp^{i,k}, t)$ (rtf for remaining time to fault):

$$rtf(pp^{i,k}, t) = \min(t_d - t) \text{ s.t. } \widehat{pp}^{i,k}(t_d) \notin r_n(pp^{i,k}) \tag{9}$$

The estimated date t^i_{j+1} of the next fault mode of the component C^i is then computed with

$$t^i_{j+1} = t + \min(rtf(pp^{i,k}, t) \mid pp^{i,k} \in \mathcal{PP}^i). \tag{10}$$

The next fault occurrence corresponds to the private parameter pp^f with the shortest rtf, the next fault mode can thus be evaluated as follows: let m^i_j be the current mode of component C^i at time t,

Definition 19 (Next fault mode for a component)**.** *The set of possible* next fault modes $NFM(m^i_j, t)$ *of a component* C^i *is*

$$\begin{aligned} NFM(m^i_j, t) = \{m \in \mathcal{M}^i \mid \widehat{pp}^f(t^i_{j+1}) \in r_m(pp^f) \wedge \\ \forall pp \in \mathcal{PP}^i \setminus \{pp^f\}, \widehat{pp}(t^i_{j+1}) \in r_m(pp) \cap r_{m^i_j}(pp)\}. \end{aligned} \tag{11}$$

Informally, the mode m is possible if the faulty parameter pp^f is estimated to be in the range of m at time t^i_{j+1} and the estimation of the other private parameters belong to both range of m^i_j and m. In the case where the same rtf is computed for several private parameters of the component, there are several hypotheses about the next fault mode of the component.

Definition 20 (Local prognosis)**.** *A local prognosis* $\Pi^i(t)$ *for a component* C^i *at time* t *is the set of next fault modes which match with a local diagnostic candidate of* $\Delta^i(t)$*:*

$$\Pi^i(t) = \{\widehat{m}^i_{j+1} \in NFM(m^i_j, t) \mid m^i_j \in \Delta^i(t)\}. \tag{12}$$

If the local diagnosis contains more than one local diagnostic candidate $\Delta^i(t) = \{m^i_j\}$, the date t^i_{j+1} of the next mode change is determined from each local diagnostic candidate. As opposed to classical definitions of prognosis, this one does not rely on the component RUL but is more detailed. As soon as a private parameter is faulty, the component cannot implement all the set of basic functions which follows that the RUL of a component C^i is:

$$RUL(C^i, t) = \min(rtf(pp^{i,k}, t) \mid pp^{i,k} \in \mathcal{PP}^i). \tag{13}$$

4.3.3. Global prognosis

A next system mode $\widehat{m}^\Sigma_{j+1}$ is obtained by first determining the date t_{j+1} of the next mode change through the system, that is: $t_{j+1} = min_{i \in \{1,\dots,n\}}(t^i_{j+1})$. Let min denote the index of the component C^{min} where the next fault should occur (i.e. $t_{j+1} = t^{min}_{j+1}$), the next system mode is then composed of a mode m^{min} from the local prognosis $\Pi^{min}(t)$. Obviously this local prediction has global consequences. Firstly, the system mode $\widehat{m}^\Sigma_{j+1}$ predicted to change at time t_{j+1} must respect the structural condition H_{Struct}. Secondly, the predicted mode m^{min} may change the conditions on some output parameter op^{min} of C^{min} and generate abnormal solicitations on a parameter ip^i of a component C^i such that $ip^i \in St(op^{min})$. In this case, it is possible that at time t_{j+1}, the component C^i also switches to an abnormal mode m^i but it is not a new fault mode (as the local prediction states that only C^{min} switches on a new fault mode at time t_{j+1}).

The following definition formally summarizes how a next system mode is built. Using an abuse of language, let $St : Comps \rightarrow 2^{Comps}$ denote the function such that $St(C)$ is the set of components C' which have an input parameter ip' such that $St(op) \ni ip'$ where op is an output parameter of C. Let also $St^* : Comps \rightarrow 2^{Comps}$ be the transitive closure: $St^*(C) = \{C\} \cup St(C) \cup \bigcup_{C' \in St(C)} St^*(C')$, $St^*(C)$ denotes then the set of components that may have a mode change at time t_{j+1}.

Definition 21 (Next system mode)**.** *The set of possible* next system modes $NSM(m^\Sigma_j, t)$ *is:*

$$\begin{aligned} NSM(m^\Sigma_j, t) = \{m = \langle m^1, ..., m^{min}, ..., m^N \rangle \wedge H_{Struct} \wedge \\ m^{min} \in \Pi^{min}(t) \wedge \forall i \in \{1, \dots, N\}, \\ (C^i \notin St^*(C^{min}) \Rightarrow m^i = m^i_j) \wedge \\ (C^i \in St^*(C^{min}) \setminus \{C^{min}\} \Rightarrow \\ (\forall pp \in \mathcal{PP}^i, \widehat{pp}(t) \in r_n(pp) \Rightarrow \widehat{pp}(t_{j+1}) \in r_n(pp)))\} \end{aligned} \tag{14}$$

Once a date t_{j+1} and its corresponding system mode $\widehat{m}^\Sigma_{j+1}$ are estimated, it is then possible to reiterate the procedure in order to estimate a date t_{j+2} and a mode $\widehat{m}^\Sigma_{j+2}$ and so on. For each component C^i switching in abnormal mode at time t_{j+1} because of an abnormal solicitation on an input parameter ip^i, a new value $v^i \in r_a(ip^i)$ has to be assigned to the parameter ip^i at time t_{j+1}. If this parameter is involved in the aging model $ag^{i,k}$ of the component C^i, that modifies the estimation of private parameter $\widehat{pp}^{i,k}$ that is required to compute the date t_{j+2}. These predictions in future values of input parameters represents fault propagation in components of the system. A global prognostic candidate for a complex system Σ at t is then a system mode trajectory $\widehat{m}^\Sigma_{j+1}. \dots . \widehat{m}^\Sigma_p$ such that $\widehat{m}^\Sigma_p$ is a failure mode.

Definition 22 (Global prognosis)**.** *The global prognosis* $\Pi^\Sigma_s(t)$ *for a system* Σ *at time* t *is the set of next system mode trajectories* $\{\widehat{m}^\Sigma_{j+1} \dots \widehat{m}^\Sigma_p\}$ *that match the current diagnosis* $\Delta^\Sigma(t)$*:*

$$\begin{aligned} m^\Sigma_j \in \Delta^\Sigma(t) \wedge \widehat{m}^\Sigma_{j+1} \in NSM(m^\Sigma_j, t) \wedge \\ \forall h \in \{j+1, \dots, p-1\}, \widehat{m}^\Sigma_{h+1} \in NSM(\widehat{m}^\Sigma_h, t_h). \end{aligned} \tag{15}$$

As stated above, the global prognostic procedure is recursive and stops when a failure mode $\widehat{m}^\Sigma_p$ is estimated at time t_p

which means that at every step of the mode estimation, it is necessary to determine whether the estimated mode is a failure mode. In the following, we suppose that the procedure is at step h and we try to figure out whether $\widehat{m}^{\Sigma}_{h+1}$ is a failure mode or not, that is $p = h + 1$. When a failure mode occurs at the date t_p, the system cannot correctly ensure the whole set of goal functions $\mathcal{FU}_g$. Goal functions are obtained by the composition of basic functions described by the functional model of the system (see Section 3.4). A basic function $Fu^{i,j}$ fails only if one of the private parameters $PP(Fu^{i,j}))$ of C^i involved in the functional condition $Fu^{i,j}$ is faulty. The *estimated time to failure* ($ettf$ for short) of a basic function $Fu^{i,j}$ is then evaluated at time t_h as follows:

$$ettf(Fu^{i,j}, t_h) = \min(rtf(pp^{i,k}, t_h) \mid pp^{i,k} \in PP(Fu^{i,j})). \tag{16}$$

In complex systems, basic functions are often implemented by redundant components. When a redundant component is faulty, the function may still be available on the second one. For this reason, the global prognosis must take the system functional aspect into account like in Voisin, Levrat, Cocheteux, and Iung (2010) or Dragomir, Gouriveau, Zerhouni, and Dragomir (2007) to estimate the $ettf$ of any non-basic function Fu_i. The $ettf$ of a non-basic function Fu_i derives from the $ettf$ of the functions that belong to $Pred(Fu_i)$ that can be either basic functions or non-basic functions. From the functional dependencies defined in Section 3.4, it follows that:

$$ettf(Fu_i, t_h) = \max_{Y \in n/m[Pred(Fu_i)]} \left[\min_{Fu_j \in Y} ettf(Fu_j, t_h) \right], \tag{17}$$

where $\|Y\| = n$ and $\|Pred(Fu_i)\| = m$. We can then check whether $\widehat{m}^{\Sigma}_{h+1}$ is a failure mode or not if there exists a goal function Fu^i_g such that:

$$ettf(Fu^i_g, t_h) = t_p - t_h = t_{h+1} - t_h. \tag{18}$$

Finally, the global RUL of a complex system Σ corresponds to the remaining time until the system cannot perform one of the goal functions (Goebel & Eklund, 2007). At time t, the RUL is:

$$RUL(\Sigma, t) = t_p - t. \tag{19}$$

4.4. Discussion

Section 4 proposes a complete characterization of what is required to develop a decentralized architecture for an HMS that embeds diagnosis and prognosis functions. Deliberately, the proposed framework is deterministic in the sense that the diagnosis result is the complete set of system modes that are compatible with the observations. One could argue that it is unrealistic and this set can be very large so stochastic methods could be used to only compute a subset of candidates (the most likely ones) for example. Such stochastic approaches come with a price in a decentralized architecture, the loss of consistency due to the difficulty to mix local/global probabilities distribution if the hypothesis of event independence does not hold. It may happen that most likely local diagnoses are globally inconsistent so that the HMS is unable to return any global candidate. We claim that the use of probability is interesting to rank or prefer diagnoses and then rank and prefer prognosis and not for filtering and/or pruning candidates that would affect the correctness of the whole HMS. Using probability or any ranking system on our framework simply consists in adding a weight function of the local/global diagnosis to rank/prefer the component/system modes. Another way to minimize the ambiguity relies on diagnosability analysis which consists in determining the source of ambiguity at design time and add new sensors in the system for a better observation of it by the HMS and therefore a better discrimination of the ambiguity.

5. ILLUSTRATIVE EXAMPLE

In this section, we show how the presented generic formalism can be used to model a fuel distribution system. This studied application is composed of common heterogeneous elements (pumps and valve) that can be found in in (Roychoudhury & Daigle, 2011). This example points out how the system heterogeneity and the functional redundancies are taken into account.

5.1. Modeling

The studied Distribution System (DS) receives liquid delivered by two pumps P_1 and P_2. The liquid is stored in a tank T before being distributed to user systems through a valve V_3. The components of the system are illustrated in Figure 6. An intelligent sensor I_3 is added to build indicator in order to monitor the valve V_3. The distribution system is then composed of five components that interact with each other: $Comps = \{P_1, P_2, T, V_3, I_3\}$.

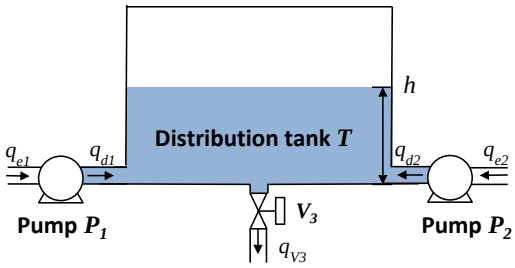

Figure 6. Distribution System

5.1.1. Structural modeling

Figure 7 depicts the interactions between the DS components. For both pumps P_1 and P_2, input parameters are control signals equivalent to a flow reference and output parameters are

the actual delivered outflow:

$$P_1 : \begin{cases} \mathcal{IP}^{P_1} = \{q_{e1}\} \\ \mathcal{OP}^{P_1} = \{q_{d1}\} \\ \mathcal{PP}^{P_1} = \{A_1\} \end{cases} \quad P_2 : \begin{cases} \mathcal{IP}^{P_2} = \{q_{e2}\} \\ \mathcal{OP}^{P_2} = \{q_{d2}\} \\ \mathcal{PP}^{P_2} = \{A_2\}. \end{cases} \tag{20}$$

The private parameters A_1 and A_2 are introduced for diagnosis and prognosis purpose. They are wear parameters used to represent the component degradation leading to the pump failure.

For the valve V_3, input parameters are the liquid level h in the tank and a control signal u_3 to open or close the valve:

$$V_3 : \begin{cases} \mathcal{IP}^{V_3} = \{h, u_3\} \\ \mathcal{OP}^{V_3} = \{q_{V_3}, i_{wV3}\} \\ \mathcal{PP}^{V_3} = \{w_{V_3}\}. \end{cases} \tag{21}$$

The private parameter w_{V_3} is a wear parameter used to represent the valve fault modes, stuck open or stuck closed. The valve output parameter is the outflow and i_{wV3} represents an image of the valve private parameter to interact with the sensor component I_3.

The intelligent sensor I_3 provides a fault indicator value a_{V_3} that is built from the following input parameters:

$$I_3 : \begin{cases} \mathcal{IP}^{I_3} = \{i_{wV3}, u_3, q_{V_3}\} \\ \mathcal{OP}^{V_3} = \{a_{V_3}\}. \end{cases} \tag{22}$$

Here the sensor is supposed to be reliable and non faulty.

Fluid delivered by pumps is then stored in a tank T. The input parameters of this component are the flows delivered by pumps and the output parameter is the fluid level h in the tank:

$$T : \begin{cases} \mathcal{IP}^{V_3} = \{q_{d1}, q_{d2}, q_{V_3}\} \\ \mathcal{OP}^{T} = \{h\}. \end{cases} \tag{23}$$

For the sake of simplicity, the tank is assumed to be perfect with no degradation.

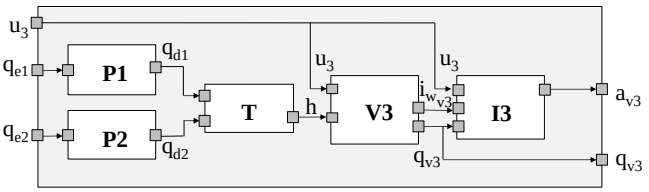

Figure 7. DS structural model

5.1.2. Functional modeling

The DS components implement some basic functions in order to realize the system goal function Fu_g that is to store and distribute fuel to consumer systems. The pump function is to deliver pressurized fuel consistently to the control signal:

$$\begin{array}{l} Fu^{P_1} \equiv (q_{d1} = ar^{P_1}(q_{e1}, A_1)) \\ Fu^{P_2} \equiv (q_{d2} = ar^{P_2}(q_{e2}, A_2)). \end{array} \tag{24}$$

For more detail about equations describing the pump behavior, we can refer to (Roychoudhury & Daigle, 2011). The pump P_1 is default used to fill the tank. The flow control q_{e1} describes a square signal : it is equal to 600 for 5 hours and is null for the next 5 hours. The pump P_2 is started only if a problem is detected with P_1. At start P_1 is assumed to be nominal, so the control signal q_{e2} is null.

The basic function of the tank T is to store fluid provided by the pumps P_1 and P_2. The water level h in the tank is computed through the following mass balance equation:

$$\begin{array}{lcl} Fu^T & \equiv & (h = ar^T(q_{d1}, q_{d2}, q_{V_3})) \\ ar^T & : & (\dot{h} = (q_{V_1} + q_{V_2} - q_{V_3}/S)), \end{array} \tag{25}$$

where S is the tank sectional area. The relation ar^T is represented by a differential equation. The output parameter value h is obtained by integrating it. The tank is assumed to be perfect without leak faults, so its function is always available in the system.

The basic function of the valve V_3 is to distribute liquid contained by the tank to consumer systems consistently to the control signal u_3. The flows through the valve is computed from the Torricelli law:

$$\begin{array}{lcl} Fu^{V_3} & \equiv & (q_{V_3} = ar^{V_3}(h, u_3, w_{V_3})) \\ & \equiv & (q_{V_3} = |u_3 - w_{V_3}| A_3 \sqrt{2gh}) \\ & & \wedge\ (w_{V_3} = 0), \end{array} \tag{26}$$

where A_3 is the valve cross-sectional area and g is the gravity constant. The command signal u_3 is equal to zero to close the valve or equal to one to open it. This basic function is correctly performed when the wear parameter w_{V_3} is null.

The basic function of the intelligent sensor I_3 is to built a fault indicator a_{V_3} for the valve V_3 from its control signal u_3 and its outflow q_{V_3}:

$$\begin{array}{lcl} Fu^{I_3} & \equiv a_{V_3} = ar^{I_3}(i_{wV3}) \\ & \equiv a_{V_3} = i_{wV3}. \end{array} \tag{27}$$

This sensor verifies the inputs u_3 and q_{V_3} to assign a value to a_{V3}. For example, $a_{V3} = 1$ indicates a fault ($w_{V_3} = 1$) for the valve when the following conditions on input parameters hold:

$$(u_3 = 1 \wedge q_{V_3} = 0) \vee (u_3 = 0 \wedge q_{V_3} \neq 0). \tag{28}$$

As said before, the component is assumed to be non faulty, so, this function is always available.

The basic functions are composed in order to realize a set of intermediate functions on which relies the realization of the DS goal function:

$$Fu_g = 3/3(Fu_1, Fu^T, Fu^{V_3}) \tag{29}$$

where,

- Fu_1 is to provide fuel (this intermediate function is built from pump functional redundancy Fu^{P_1} and Fu^{P_2}),

- Fu^T is to store fuel delivered by pumps,
- Fu^{V_3} is to distribute fuel through a controlled valve.

This composition can be represented as a functional tree and is represented in Figure 8. The sensor function does not participate to the realization of the system goal function, that is why it is not represented in the functional tree.

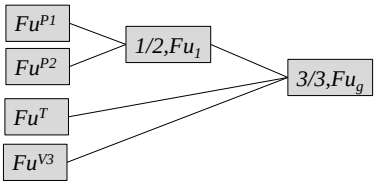

Figure 8. DS functional model

5.1.3. Aging modeling

A reliability data-based model is established from failure history for the valve V_3 and gives the fault probability of valve V_3 at any operating time. The exponential distribution is used in the model to describe the random fault phenomenon with a constant failure rate λ that is relative to the component use. The valve aging model for V_3 is

$$\begin{aligned} w_{V_3} &= ag^{w_{V_3}}(t) \\ &= \begin{cases} 0 & \text{if} \quad 1-\exp(-\lambda_3 t) < p_{max} \\ 1 & \text{otherwise.} \end{cases} \end{aligned} \tag{30}$$

with $\lambda_3 = 2,25.10^{-5}$ and p_{max} is a non accepted probability threshold fixed a priori. $w_{V_3} \neq 0$ means a fault has occurred on the valve V_3 and the component is either stuck open or stuck closed. Reliability data-based models do not consider component real solicitations, then they do not depend on component input parameters.

A stress-based model can be used for pumps. A physical analytical law is identified from series of real experiments (like accelerated life testing) and determines a degradation level to evaluate the wear parameter value like in Gorjian, Ma, Mittinty, Yarlagadda, and Sun (2009). In Roychoudhury and Daigle (2011), two degradations are studied for the pump, the bearing wear and the impellar wear. The bearing wear provokes an increase in the pump friction coefficient and the impellar wear appears as a decrease of the impellar area due to erosion of the rotating element in contact with fluid. Here, we choose to represent only the impellar wear with the following equation that depends on the control signal q_{ei} of the pump P_i:

$$\begin{aligned} A_i &= ag^{A_i}(q_{ei}(t)) \\ \dot{A}_i &= \begin{cases} -w_A q_{ei}(t)^2 & \text{if} \quad q_{ei}(t) > 0 \\ -5.10^4 w_A & \text{otherwise} \end{cases} \end{aligned} \tag{31}$$

where $w_A = 3.10^{-8}$ for both pumps and the initial value of the impellar area is $A_i(t_0) = 60$. The value of A_i is then computed by integrated the differential equation explained for relation ar^{P_i}. When the pump is degraded the impellar A_i decreases and as a consequence q_{di} also decreases. The minimal value $A_i = 55$ was identified from tests for a non faulty pump.

5.1.4. Operational modes

Some fault modes have been identified for the components P_1, P_2 and V_3 by defining private parameters. The following tables express for each component the parameter ranges according to the component operational mode. There exist as many abnormal modes as combinations of input parameters for each component but for the sake of simplicity, they are not described here. We recall that the components T and I_3 are assumed to be always nominal.

P_1 Modes	$m_n^{P_1}$	$m_f^{P_1}$
$r(q_{e1})$	$\{0, 600\}$	$\{0, 600\}$
$r(q_{d1})$	$\{0, 600\}$	$[0, 600[$
$r(A_1)$	$[55, 60]$	$[0, 55[$

Table 1. P_1 operational modes

Table 1 represents operational modes for the pump P_1. In nominal mode, the control signal q_{e1} is either equal to 600 or null and the delivered flow is then also equal to 600 or null. The private parameter that represents the impellar area is initially equal to 60. In fault mode, while input parameter q_{e1} remains in the same range, the delivered flow is inferior to 600 and the impellar area is inferior to 55 the minimal accepted value. The basic function of P_1 is not available. The component fails to provide liquid consistently to the command signal q_{e1}. Table 2 represents operational modes for the pump P_2 that is similar to the ones explained for P_1. Table 3 represents operational modes for valve V_3. The range of control signal u_3 is either closed or open and represented by the value set $\{0, 1\}$.

P_2 Modes	$m_n^{P_2}$	$m_f^{P_2}$
$r(q_{e2})$	$\{0, 600\}$	$\{0, 600\}$
$r(q_{d2})$	$\{0, 600\}$	$[0, 600[$
$r(A_2)$	$[55, 60]$	$[0, 55[$

Table 2. P_2 operational modes

V_3 Modes	$m_n^{V_3}$	$m_f^{V_3}$
$r(u_3)$	$\{0, 1\}$	$\{0, 1\}$
$r(h)$	$[3, 20]$	$[0, 3]$
$r(q_{V_3})$	$[0, 20]$	$[0, 20]$
$r(w_{V_3})$	0	1

Table 3. V_3 operational modes

5.2. Scenarios

The proposed characterization is illustrated with a scenario in two steps. At the operating start $t_0 = 0$, the health monitoring system identifies the current system mode and predict the RUL. Then, a fault for the pump P_1 is injected at time $t_1 = 30\,000$.

5.2.1. Scenario at time $t_0 = 0$

Diagnosis Diagnosis aims at determining the current mode of components at time t_0 which is consistent with the component models and the available observations. Sensors measure the flow delivered by pumps P_1 and P_2, another sensor measures the liquid level h in the tank and the intelligent sensor provides the indicator a_{V3}. The acquired measures, the pump and valve controls are observable. Then, we assume that the set of observed parameter is invariant :

$$\{q_{e1}, q_{d1}, q_{e2}, q_{d2}, h, u_3, a_{V_3}\}. \tag{32}$$

At t_0, the values of observed parameters are :

$$\{600, 600, 0, 0, 10, 0, 0\} \tag{33}$$

Every local observation is in nominal range. The system is in nominal mode at the operating start then all functions are available on the components.

Prognosis The prognostic function aims at determining the future mode for the system which is consistent with the diagnosis and the aging models of component parameters. The aging models $\{ag^{i,k}\}$ are used to estimate the value of private parameters $\{\widehat{pp}^{i,k}\}$ and compute the fault date t_d at which the private parameters are out of the nominal ranges defined in Section 5.1.4.

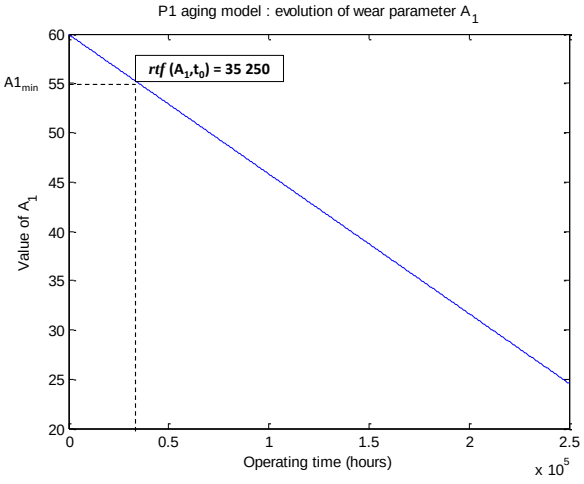

Figure 9. P_1 aging model : evolution of wear parameter A_1

Figures 9, 10 and 11 represent the evolution of private parameters of components P_1, P_2 and V_3 according to aging models

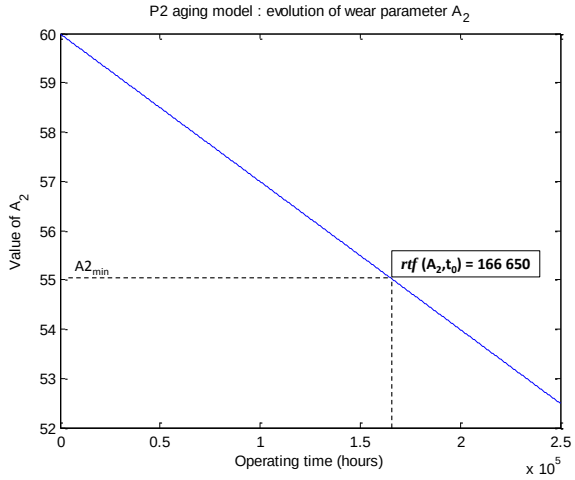

Figure 10. P_2 aging model : evolution of wear parameter A_2

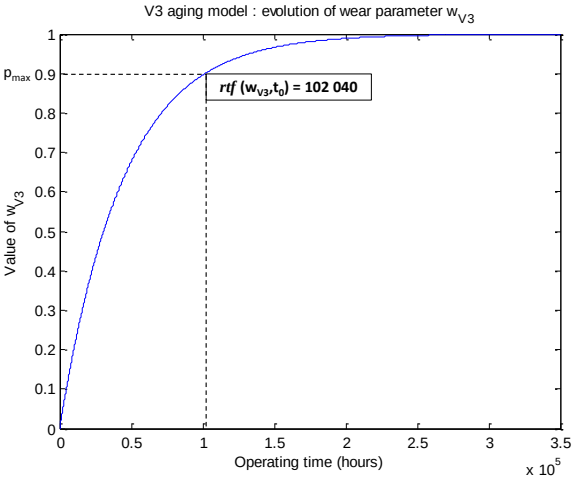

Figure 11. V_3 aging model : evolution of wear parameter w_{v_3}

explained in Section 5.1.3. For the pump P_1, this evolution takes future inputs for q_{ei} into account from the definition of the square control signal. We recall that the components T and I_3 are supposed to be perfect, not degrading and thus no prognosis is performed on them.

The rtf of components that define the remaining time until a fault occurrence are computed from these aging models (see Equation 9 in Section 4.3.2):

$$\begin{aligned} rtf(P_1, t_0) &= 35\,250 \\ rtf(P_2, t_0) &= 166\,650 \\ rtf(V_3, t_0) &= 102\,040 \end{aligned} \tag{34}$$

Local prognoses at time t_0 give the component next modes

and can be formally defined as follows (see Definition 20):

$$\begin{cases} \Pi^{P_1}(t_0) = \widehat{m}^{P_1}_{+1} = m^{P_1}_f \text{ with } t^{P_1}_{+1} = 35\ 250 \\ \Pi^{P_2}(t_0) = \widehat{m}^{P_2}_{+1} = m^{P_2}_f \text{ with } t^{P_2}_{+1} = 166\ 650 \\ \Pi^{V_3}(t_0) = \widehat{m}^{V_3}_{+1} = m^{V_3}_f \text{ with } t^{V_3}_{+1} = 102\ 040 \end{cases} \tag{35}$$

As only one private parameter is defined in this illustration for each component, the RUL of components is equivalent to the rtf. These numerical values show P_1 is predicted to be the next faulty component. Its RUL is shorter than the one for P_2 because P_1 is the default pump. Then the second component predicted to be faulty is V_3.

As stated by Definition 21 in Section 4.3.3, the next system mode $\widehat{m}^{\Sigma}_{+1}$ is determined from $m^{min} \in \Pi^{min}(t_0)$, the next mode of the component C^i with a minimal t^i_{+1}. As $t^{min}_{+1} = t^{P_1}_{+1}$, the next fault mode for the system is

$$\widehat{m}^{\Sigma}_{+1} = \langle m^{P_1}_f, m^{P_2}_n, m^{V_3}_n, m^{I_3}, m^T_n \rangle. \tag{36}$$

In order to compute the system RUL, the date t_p of the system failure mode m^{Σ}_p must be computed. For this purpose, the availability of basic and intermediate functions implemented by components have to be evaluated at time $t^{min}_{+1} = 35\ 250$. As the components have only one private parameter, the $ettf$ of basic functions can be directly evaluated to the rtf of their private parameters (see Equation 16).

As described by the functional model in Figure 8, the intermediate function Fu_1 is available as long as Fu^{P_1} or Fu^{P_2} is available. It expresses the redundancy of pumps. The $ettf$ of Fu_3 is then computed using Equation 17 as follows:

$$\begin{aligned} ettf(Fu_1, t_0) &= \max(ettf(Fu^{P_1}, t_0), ettf(Fu^{P_2}, t_0)) \\ &= \max(35\ 250, 166\ 650) = 166\ 650. \end{aligned} \tag{37}$$

The function Fu_1 and Fu^{V_3} are required to perform the system goal function Fu_g, then

$$\begin{aligned} ettf(Fu_g, t_0) &= \min(ettf(Fu_1, t_0), ettf(Fu^V_3, t_0) \\ &= \min(166\ 650, 102\ 040) = 102\ 040. \end{aligned} \tag{38}$$

The RUL of the system corresponds to the remaining time until it cannot correctly perform its goal function Fu_g, then $RUL(\Sigma, t_0) = t_p - t_0 = 102\ 040$.

5.2.2. Scenario at time $t_1 = 30000$

In this scenario, all the components are in nominal mode between t_0 and t_1 and degrade normally according to the aging model. At time t_1, a fault is injected in the component P_1. Diagnosis result is the same as the one in t_0 between these two dates and prognosis is currently updated by evaluating the rtf of private parameters, the $ettf$ of functions and the system RUL according to the current operating time, in particular at t_1

$$RUL(\Sigma, t_1) = t_p - t_1 = 72\ 040. \tag{39}$$

Diagnosis At $t_1 = 30\ 000$, the values of observed parameters are:

$$\{q_{e1}, q_{d1}, q_{e2}, q_{d2}, h, u_3, a_{V_3}\} = \{600, 550, 0, 0, 5, 0, 0\} \tag{40}$$

For each component, the local diagnosis is computed by checking the compatibility between local observations and the modes (see Definition 15 in Section 4.1): $Obs(q_{e1}, t_1) = 600$ and $Obs(q_{d1}, t_1) = 550$ are compatible with one mode of P_1:

$$\Delta^{P_1}(t) = \{m^{P_1}_f\}. \tag{41}$$

$Obs(q_{e2}, t_1) = 0$ and $Obs(d_{e1}, t_1) = 0$ is compatible with two modes of P_2 but as the component is supposed to be nominal at operating start and P_2 has not started yet, only the nominal mode is considered:

$$\Delta^{P_2}(t) = \{m^{P_2}_n\}. \tag{42}$$

$Obs(q_{V_3}, t_1) = 0$ and $Obs(u_3, t_1) = 0$ are compatible with two modes of V_3:

$$\Delta^{V_3}(t) = \{m^{V_3}_n, m^{V_3}_f\}. \tag{43}$$

The local diagnosis of V_3 is ambiguous. From local observations, it cannot be disambiguised.

The system mode at $t_1 = 30\ 000$ is obtained by merging local diagnostic candidates and excluding the system modes that do not satisfy the H_{struct} hypothesis (see Definition 16 in Section 4.1). By merging local diagnoses, we obtain two global system mode

$$\begin{aligned} &(\Delta^{P_1}(t_1) \times \Delta^{P_2}(t_1) \times \Delta^T(t_1) \times \Delta^{V_3}(t_1) \times \Delta^{I_3}(t_1)) \\ &= \{\langle m^{P_1}_f, m^{P_2}_n, m^T_n, m^{V_3}_n, m^{I_3}_n \rangle, \\ &\langle m^{P_1}_f, m^{P_2}_n, m^T_n, m^{V_3}_f, m^{I_3}_n \rangle\}. \end{aligned} \tag{44}$$

These system modes need to be compatible with all observations. The fault indicator $Obs(a_{V_3}, t_1) = 0$ means that V_3 cannot be faulty then the second system mode is not compatible with observations and is removed from global diagnosis:

$$\Delta^{\Sigma}(t_1) = \langle m^{P_1}_f, m^{P_2}_n, m^T_n, m^{V_3}_n, m^{I_3}_n \rangle. \tag{45}$$

Prognosis At $t_1 = 30.000$, the component P_1 is diagnosed faulty, the component P_2 is then started with the same square control signal as P_1 previously. This naturally modifies the degradation of the component P_2 according to new solicitations as illustrated in Figure 12.

As for the scenario at time t_0, the fault date t_d associated to each private parameter of components is computed from aging models and nominal ranges defined in operational modes. Then the rtf of components are updated :

$$\begin{aligned} rtf(P_2, t_1) &= 58\ 850 \\ rtf(V_3, t_1) &= 102\ 040. \end{aligned} \tag{46}$$

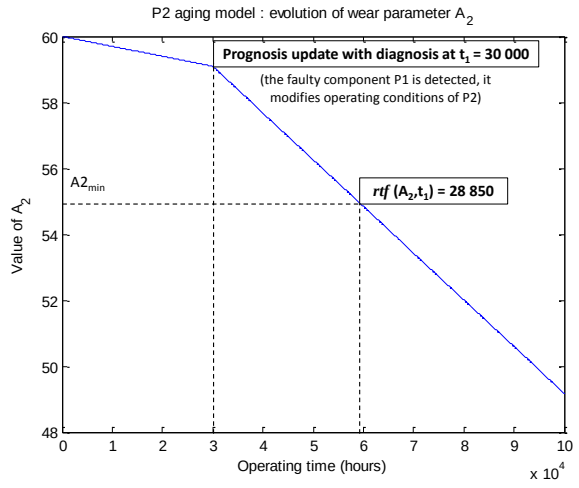

Figure 12. P_2 aging model : evolution of wear parameter A_f according to diagnosis result

P_1 is already faulty and T and I_3 always assumed to be nominal. New local prognosis at time $t_1 = 30.000$ are then computed for non faulty components:

$$\begin{cases} \Pi^{P_2}(t_1) = \widehat{m}^{P_2}_{+1} = m^{P_2}_f \text{ with } t^{P_2}_{+1} = 58\,850 \\ \Pi^{V_3}(t_1) = \widehat{m}^{V_3}_{+1} = m^{V_3}_f \text{ with } t^{V_3}_{+1} = 102\,040 \end{cases} \tag{47}$$

The next faulty component P_2 is predicted to fail at $t^{P_2}_{+1} = 58\,850$. Then at $t^{min}_{+1} = t^{P_2}_{+1}$, the next system mode is

$$\widehat{m}^{\Sigma}_{+1} = \langle m^{P_1}_f, m^{P_2}_f, m^{T}_n, m^{V_3}_n, m^{I_3}_n \rangle. \tag{48}$$

The RUL of the pump P_2 has decreased because of its new solicitations and it modifies consequently the system RUL. In order to compute the system RUL, the $ettf$ of the intermediate functions and the goal functions have to be evaluated:

$$\begin{aligned} ettf(Fu_1, t_1) &= \max(ettf(Fu^{P_1}, t_1), ettf(Fu^{P_2}, t_1)) \\ &= \max(0, 28\,850) = 28\,850 \\ ettf(Fu_g, t_1) &= \min(ettf(Fu_1, t_1), ettf(Fu^{V_3}, t_1)) \\ &= \min(28\,850, 72\,040) = 28\,850. \end{aligned} \tag{49}$$

We recall that the rtf and the $ettf$ values represent durations from time $t_1 = 30\,000$ and not a fault or a failure date. The RUL of the system at time t_1 is now $RUL(\Sigma, t_1) = t_p - t_1 = 28\,850$. If the pump P_1 had correctly worked until predicted rtf, P_2 would have been solicited much later and the system RUL would have been longer.

This example illustrates each part of our generic modeling framework for the diagnosis and the prognosis of a heterogeneous complex system. It also points out the need of diagnosis to update predictions for prognosis.

6. RELATED WORK

Fault diagnosis has become a mature problem and a lot of research works are now considered as references in this field (Hamscher et al., 1992; Isermann, 2005; Lamperti & Zanella, 2003). It aims at identifying faults occurring on components that may cause a system failure. In the diagnosis community, a fault represents a deviation of one component characteristic or property. Diagnostic methods rely on the monitoring capabilities and a knowledge of the system behavior. This knowledge can be represented as an experience (Buchanan & Shortliffe, 1984; Jackson, 1998), a known qualitative or quantitative model in DX/FDI communities (Gertler, 1998; Hamscher et al., 1992) or an estimated model obtained by learning and classification methods (Fouladirad & Nikiforov, 2005; Takagi & Sugeno, 1985).

As opposed to diagnosis, prognosis is quite a new field of interests. In the more recent literature, a lot of definitions can be found for prognosis (Goh, Tjahjono, Baines, & Subramaniam, 2006). In Brotherton et al. (2002), prognosis is defined as the ability to assess the current health of a component or to predict the next time to failure. For Engel et al. (2000) it is the capability to provide early detection of incipient fault condition and to have the means to manage and predict the progression of this fault condition to the component failure. For both definitions, prognosis consists in predicting the remaining time until the system cannot perform successfully its function anymore and must be replaced, i.e. the time to failure. Whereas this prediction can be done all over the system operation in the first definition, it is performed only after a fault occurrence in the second definition. In our case, the preventive maintenance objective is ultimately to replace the component before a fault occurs on it which means that the prognosis process starts as soon as the system starts operating, and it continuously updates the prediction of the remaining time before the system failure. Moreover, faults may result in change in the solicitations of the neighboring subsystems (Abbas & Vachtsevanos, 2009) even if failures have not happened yet (latent faults for instance). These subsystems could deteriorate quickly. This temporal prediction relies on a knowledge about the health state of the system (Dasgupta & Pecht, 1991; Gorjian et al., 2009). In the literature, there already exist several prognostic approaches which rely on different models (Ghelam et al., 2006; Heng, Zhang, Tan, & Mathew, 2009; M. Roemer et al., 2005; Schwabacher & Goebel, 2007). In M. J. Roemer and Byington (2007), a spall initiation model is used to evaluate the current health of bearings and a progression model of crack length is used to obtain the RUL. Abbas and Vachtsevanos (2009) defines the fault progression as the evolution of a fault in a subsystem under given operational condition and the fault propagation as the effect of a fault on another fault both in the same system. In our framework, the fault progression is represented as an aging model and the fault propagation relies on a structural function that defines component interactions.

Finally, prognosis requires some health indicators of the system that can obviously be delivered by diagnosis techniques.

Very few works exist on this topic. Lebold and Thurston (2001) and Sheppard, Kaufman, and Wilmering (2008) defines standard architectures for PHM. They combine diagnostics and prognostics modules but no formalization of both problems is given and the link between both modules diagnostics-prognostics is not really explicit. In Daigle and Goebel (2011), the authors proposed a Model-Based Prognostics Approach to predict the end of life and the RUL of a pneumatic valve. This approach proposes an architecture with a fault detection, isolation and identification module that injects information to the prognostic module (damage estimation and prediction). This work presents a diagnostic/prognostic methodology by choosing specific models and method that does not aim at being generic. The prognostic method proposed in Daigle and Goebel (2011) could be a potential candidate to implement the local diagnosis and the local prognosis for a component like the proposed pneumatic valve. In Roychoudhury and Daigle (2011), a more detailed version of the diagnosis part of the previous architecture is introduced and is implemented by a classical observer technique based on residuals (Isermann, 2005) and qualitative reasoning (Mosterman & Biswas, 1999).

To the best of our knowledge, no research paper addresses the formal characterization of an embedded and decentralized diagnosis/prognosis HMS in charge of the monitoring of a complex system such as an aircraft.

7. CONCLUSION

A formal characterization of a modern on-line HMS has been presented in this paper. The objective of this characterization was to be as generic as possible in order to provide formal but consistent requirements for the development and the deployment of any HMS on a complex system like an aircraft. The characterization is modular, it introduces a decentralized architecture for diagnosis and prognosis (local/global) that is consistent. Within this framework, we also introduce the notion of mode trajectory which is an abstraction of the underlying evolution of the system that is sufficient for the maintenance decision. Both diagnosis and prognosis rely on this abstraction to provide results: diagnosis is in charge of determining the current mode of the system whereas prognosis is in charge of predicting the date of the next mode changes till the prediction of the occurrence of system failure. Consistency of the diagnosis, that is critical in a HMS, is based on the structural model. Moreover, our framework proposed that diagnosis takes into account the redundancy in the system by the use of a functional model that represents the minimal requirements for a global function to work properly even if some components are faulty. The prognosis process takes into account direct measurements or parameter estimates from the diagnosis part to tune the available aging models and performs the prognosis. Here also, prognosis takes into account redundancy to estimate when a system failure will occur.

This characterization extends the framework that was initiated to model an HMS on a sub-part of the aeronautical system called the Engine Bleed Air System within the ARCHISTIC projet in collaboration with the AIRBUS maintenance department. Recent works on more specific problems started with help of this characterization. Vinson, Ribot, Prado, and Combacau (2013) uses the functional and aging modeling framework to model the functional behavior and health evolution through time of permanent magnet synchronous machines. In Chanthery and Ribot (2013), the integration of diagnosis and prognosis is investigated to develop a monolithic HMS on hybrid systems based on the characterization presented here.

One of our main perspectives is to fully deploy and integrate a set of specific techniques for the diagnosis/prognosis as the ones cited above to implement an HMS on a large assembling of components whose nature is different (continuous, discrete, hybrid systems). This HMS would have the guarantee that the global result is consistent. Another perspective is to provide generic algorithmic tools for the developed HMS to scale up, especially, we would like to investigate different ranking/preference methods (see Section 4.4) to sort the diagnoses/prognoses provided by the HMS for better maintenance decisions. Finally, we also would like to investigate whether the prognostic outputs provided by the HMS would not be relevant for improving the accuracy of the diagnosis part, in other words, can the diagnosability of a system be improved by prognosis?

REFERENCES

Abbas, M., & Vachtsevanos, G. J. (2009, September 27 October 1). A System-Level Approach to Fault Progression Analysis in Complex Engineering Systems. In *the Annual Conference of the Prognostics and Health Management Society 2009.* Sans Diego, CA.

Brotherton, T., Grabill, P., Wroblewski, D., Friend, R., Sotomayer, B., & Berry, J. (2002, March 9-16). A testbed for data fusion for engine diagnostics and prognostics. In *Proceedings of the IEEE Aerospace Conference* (Vol. 6, p. 3029-3042). Big Sky, Montana.

Buchanan, B., & Shortliffe, E. (1984). *Rule Based Expert Systems: The Mycin Experiments of the Stanford Heuristic Programming Project*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc.

Chanthery, E., & Ribot, P. (2013, March). An Integrated Framework for Diagnosis and Prognosis of Hybrid Systems. In *the 3rd Workshop on Hybrid Autonomous System (HAS).* Roma, Italy.

Chitttaro, L., Guida, G., Tasso, C., & Toppano, E. (1993).

Functional and Teleological Knowledge in the Multi-modeling Approach for Reasoning about Physical Systems: A Case Study in Diagnosis. *IEEE Transactions on Systems, Man and Cybernetics*, *23*, 1718–1751.

Console, L., & Torasso, P. (1991). A spectrum of logical definitions of model-based diagnosis. *Computational intelligence*, *7*(3), 133–141.

Daigle, M. J., & Goebel, K. (2011, August). A Model-Based Prognostics Approach Applied to Pneumatic Valves. *International Journal of Prognostics and Health Management*, *2*.

Dasgupta, A., & Pecht, M. (1991, December). Material Failure Mechanisms and Damage Models. *IEEE Transactions on Reliability*, *40*(5), 531–536.

Dragomir, O., Gouriveau, R., Zerhouni, N., & Dragomir, F. (2007). Framework for a distributed and hybrid prognostic system. In *the 4th IFAC Conference Management and Control of Production and Logistics* (pp. 431–436). Romania.

Engel, S., Gilmartin, B., Bongort, K., & Hess, A. (2000, March). Prognostics, The Real Issues Involved With Predicting Life Remaining. In *IEEE Aerospace Conference* (Vol. 6, p. 457-469). USA.

Ferreiro, S., & Arnaiz, A. (2008). Prognosis Based on Probabilistic Models and Reliability Analysis to improve aircraft maintenance. In *International Conference on Prognostics and Health Management.* Denver, USA.

Fouladirad, M., & Nikiforov, I. (2005, July). Optimal statistical fault detection with nuisance parameters. *Automatica*, *41*(7), 1157–1171.

Gertler, J. (1998). *Fault Detection and Diagnosis in Engineering Systems*. Marcel Deker.

Ghelam, S., Simeu-Abazi, Z., Derain, J.-P., Feuillebois, C., Vallet, S., & Glade, M. (2006). Integration of Health Monitoring in the Avionics Maintenance System. In *6th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Process* (p. 1519-1524). China.

Goebel, K., & Eklund, N. (2007, 7-10 May). Prognostic Fusion for Uncertainty Reduction. In *AIAA Infotech@ Aerospace Conference and Exhibit.* Rohnert Park, California.

Goh, K., Tjahjono, B., Baines, T., & Subramaniam, S. (2006). A Review of Research in Manufacturing Prognostics. In *Proceedings of the IEEE International Conference on Industrial Informatics* (p. 417-422). New York.

Gorjian, N., Ma, L., Mittinty, M., Yarlagadda, P., & Sun, Y. (2009, September 28-30). A review on degradation models in reliability analysis. In *the 4th World Congress on Engineering Asset Management.* Athens, Greece.

Hamscher, W., Console, L., & De Kleer, J. (1992). *Readings in model-based diagnosis*. Morgan Kaufmann Publishers Inc.

Heng, A., Zhang, S., Tan, A., & Mathew, J. (2009). Rotating machinery prognostics: Stateoftheart, challenges and opportunities. *Mechanical Systems and Signal Processing*, *23*, 724–739.

Indra, S., Travé-Massuyès, L., & Chanthery, E. (2011). A decentralized FDI scheme for spacecraft: Bridging the gap between model based FDI research and practice. In *EUCASS.*

Isermann, R. (2005). Model-based fault-detection and diagnosis – status and applications. *Annual Reviews in Control*, *29*, 71–85.

Jackson, P. (1998). *Introduction to Expert Systems*. Boston, USA: Addison-Wesley Longman Publishing Co., Inc.

Kacprzynsk, G. J., Sarlashkar, A., Roemer, M. J., Hess, A., & Hardman, W. (2004). Predicting Remaining Life by Fusing the Physics of Failure Modeling with Diagnostics. *Journal of the Minerals, Metals and Material Society*, *56*, 29–35.

Kaufman, A., Grouchko, D., & Cruon, R. (1975). *Modèles mathématiques pour l'étude de la fiabilité des systèmes* (Masson, Ed.).

Kirkland, L., Pombo, T., Nelson, K., & Berghout, F. (2004, March 6-13). Avionics Health Management: Searching for the Prognostics Grail. In *IEEE Aerospace Conference* (Vol. 5, p. 3448-3454).

Lamperti, G., & Zanella, M. (2003). *Diagnosis of active systems*. Kluwer Academic Publishers.

Lebold, M., & Thurston, M. (2001). Open Standards for Condition-Based Maintenance and Prognostic Systems. In *5th Annual Maintenance and Reliability Conference (MARCON 2001).* Gatlinburg, USA.

Mosterman, P. J., & Biswas, G. (1999, November). Diagnosis of continuous valued systems in transient operating regions. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, *29*(6), 554–565.

Pencolé, Y., & Cordier, M.-O. (2005, May). A formal frame-

work for the decentralised diagnosis of large scale discrete event systems and its application to telecommunication networks. *Artificial Intelligence*, *164*, 121–170.

Rausand, M., & Hoyland, A. (2004). *System reliability theory: models, statistical methods and applications*. Wiley.

Reiter, R. (1987). A theory of diagnostic from first principles. *Artificial Intelligence*, *32*, 57–95.

Ribot, P., Pencolé, Y., & Combacau, M. (2009a, October 11-14). Diagnosis and prognosis for the maintenance of complex systems. In *IEEE International Conference on Systems, Man, and Cybernetics* (p. 4146 - 4151). San Antonio, USA.

Ribot, P., Pencolé, Y., & Combacau, M. (2009b, July 1-3). Functional prognostic architecture for the maintenance of complex systems. In *the 7th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes (SafeProcess'09).* Barcelona, Spain.

Roemer, M., Byington, C., Kacprzynski, G., & Vachtsevanos, G. (2005). An Overview of Selected Prognostic Technologies with Reference to an Integrated PHM Architecture. In *the 1st International Forum on Integrated System Health Engineering and Management in Aerospace.*

Roemer, M. J., & Byington, C. S. (2007, May 14-17). Prognostics and Health Management Software for Gas Turbine Engine Bearings. In *Proceedings of GT2007 ASME Turbo Expo 2007 : Power for Land, Sea, and Air* (p. 795-802). Montreal, Canada.

Roychoudhury, I., & Daigle, M. (2011, October 4-7). An Integrated Model-Based Diagnostic and Prognostic Framework. In *22nd International Workshop on Principle of Diagnosis.* Murnau, Germany.

Schwabacher, M., & Goebel, K. (2007). A survey of Artificial Intelligence for Prognostics. In *AAAI Fall Symposium.* Arkington VA, USA.

Sheppard, J., Kaufman, M., & Wilmering, T. (2008). IEEE Standards for prognostics and health management. In *Proc. IEEE AUTOTESTCON* (pp. 97–103).

Takagi, T., & Sugeno, M. (1985). Fuzzy identification of systems and its applications to modeling and control. In *IEEE International Conference on Systems, Man and Cybernetics* (Vol. 15, pp. 116–132).

Vinson, G., Ribot, P., Prado, T., & Combacau, M. (2013, June 2-5). A Generic Diagnosis and Prognosis Framework: Application to Permanent Magnets Synchronous Machines. In *11th International Conference on Chemical and Process Engineering.* Milan, Italy.

Voisin, A., Levrat, E., Cocheteux, P., & Iung, B. (2010, Accepted article). Generic prognosis model for proactive maintenance decision support: application to pre-industrial e-maintenance test bed. *Journal of Intelligent Manufacturing*, *21*(2), 177-193.

Wilkinson, C., Humphrey, D., Vermeire, B., & Houston, J. (2004, March). Prognostic and Health Management for Avionics. *IEEE Aerospace Conference Proceedings*, *5*, 3435-3446.