Performance and Reliability Assessment of a Mecatronic Sensor System in Wireless Sensor Networks

Amina MERBAH
CE/RITM
University Hassan II /ENSEM
Casablanca,Morroco

Hicham BELHADAOUI
CE/RITM
University Hassan II/ESTC
Casablanca,Morroco

Mohamed OUZZIF
CE/RITM
University Hassan II/ESTC
Casablanca,Morroco

Olaf MALASSÉ
A3SI
Arts et Métiers ParisTech
Metz,France

Abstract
From a functional point of view, the (mecatronic) system consists of various parts: a sensitive head, an analogical part of signal conditioning, and a digital part of information processing. In this paper, we will attempt to show our proposal for complete system modeling while associating the analogical part (amplifier, stabilized power supply, adaptation of impedance…) with the digital one. Thanks to the same approach based on information flow, we have modelled these various analogical components, through several levels of abstraction to make sure that the final information is generated as characteristics lists without any losses. The same approach can also allow the tracking of information till processor, and to propose a model including both analogical and digital parts. According to a qualitative study, we quote the types of failure that may be encountered in the analogical part. The inclusion of these types of failure is a necessary step in the construction of scenarios and combinations of possible errors. To make the system more efficient in a wireless sensor network, we have proposed a communication process, develop algorithms to ensure the proper functioning of this process and increase its reliability.

Key words
Mecatronic Sensor, Dependability, Reliability, information flow, mixed-signal(Analog, Digital), WSN.

I. INTRODUCTION:

One of the main problems pertaining to complex industrial systems in their reliability studies is taking realistically into account the dynamic interactions between the physical parameters (such as pressure, temperature, the flow of a liquid, etc ...) and the nominal behaviour or dysfunctional components [1]. However, we can add the problem of complexity related to the presence of a software layer that runs on the hardware architecture, resulting in the hardware / software interactions.

Our mecatronic system is hybrid by nature, its description will take into consideration both the continuous and the discrete aspects. The continuous dynamics is represented by continuous variables, discrete dynamics is represented by its various states and their change related to the occurrence of events. These two aspects make the hybrid modeling essential.

A mechatronic system with reference to automation is a dynamic system since the failure of a component may not yield over time the same result. It can also be seen as a hybrid problem since the failure of the system depends on its continuous state. Any approach to study the dependability of such systems must consider these two aspects (hybrid dynamics).

Overall the study of the hybrid systems is carried out through two approaches:

The integrated approach taking into account within the same formalism, continuous and discrete aspects. The integrated approach combines continuous models such as switching Bond Graph [2] and those resulting from models based on discrete events, like the hybrid Petri networks [3].

A Separate approach which cooperates two different models: one for continuous aspects and the other for the discrete ones. The separate approach gathers the models containing hybrid Automates, hybrid statecharts, mixed Petri or Differential -Predicate-Transition Petri nets [3] and [4].

In this context, various approaches dealing with the issue of the assessment of dynamic reliability are proposed [5] and [6].

The article is organized in the following way. Section II presents a study failure of the architecture of a mechatronic sensor. Section III describes the preliminary analysis of all the failure modes of such sensor. Section IV presents and explains the approach of quantitative indicators of reliability. Section V shows the utility of the results to improve the reliability of the proposed architecture in a wireless sensor network. And finally section VI concluded the proposed work and then suggests several ideas for future work.

II. RELIABILITY STUDY OF SENSOR ARCHITECTURE:

A. Influence of faults and criterion of performance:

The goal of our study is to analyze the influence of the transient and permanent faults on our intelligent sensor

Manuscript received August 5, 2011
Manuscript revised August 20, 2011

system, in particular the influence of the analogical part with continuous signals and the effects of its faults (transient and permanent) on the reliability of measurements. It seems appropriate first to focus on the influence of transient faults and quantify their probability and, second on permanent faults. Sensor fault refers to any event able to induce an "error" on measurements. Since measurement is the delivery of information representative of a physical size at a given moment, we can distinguish three categories of faults leading to the absence of information, to its alteration and to its delay.

The quality of a sensor system is defined by characterizing the set of allowable behaviours of this system(evolution of information representative of various sizes in case of failure, or response to a disturbance), thus, a system is said balanced when there is no more variation of the data which it delivers other than those related to the physical sizes. The quality of the system can be expressed by its ability to achieve balance. More precisely, in the case of size change, it is a question of quantifying the ability to achieve the desired balance (permanent mode) after a finite time. Usually three parameters are important for a sensor: overshooting time, response time to an input step, and stability. Hence, it is a question of designing a sensor with minimal overshoot and response time as short as possible and prove that the system remains stable.

B. Failure modes of the analogical part of the sensor:

Failures in value: in this case, the sensor sends incorrect data. For example, a temperature sensor may, owing to a manufacturing defect, issue a fixed value independent of the value of physical size. It is also conceivable that temperature measurement is temporarily modified by an electromagnetic disturbance in the case of a digital sensor.

Temporal failures: In this case, the sensor sends data outside of the prescribed temporal limits. It can occur in each request, but often randomly.

Failures by stopping: the sensors stop sending data (silence) or a constant value all the times equal to the last valid value.

Incoherent failures or Byzantine failures: if the sensor is connected with two controllers, sensor failures can be perceived differently by regulators. It is possible, for example, that the sensor sends two different values for both regulators [8].

It is also possible that combinations of these different failures modes occur, eg: the values of a sensor can be both erroneous and offset value over time.

If we define the mission of the sensor system as the measure of a physical quantity with quality of service (or quality control) defined by a number of factors: exceeding bounded, minimum response time, and the tend to stability, this system must be able to detect an error on the measured value and able to resolve this error. Then any behavior of the system outside of these specifications should be considered thereof as failure.

Sources of failures that we have considered as probabilistics, the system failure reveals therefore a probabilistic aspect that may be likened to the concept of reliability. Failure is defined by criterion as being the probability that a criterion is not checked, for example failure by exceeding will occur if at a given moment the output exceeds the specified set of differential. The failure of the entire system will be held if at least a failure in one of the criteria is presented. It would be ideal to identify the relation between system reliability and failure probability of the multiple causes of failures mentioned.

C. Failure by exceeding:

The failure by the exceeding of a sensor is to set a maximum deviation between measured data and the ideal response of this sensor for physical size. If at a given time the exceeding in the presence of transient faults goes beyond the variation considered, a failure is detected by exceeding. We can justify this choice physically because in many industrial applications the exceeding of certain, even transitory, variables can be temporarily dangerous. One example is the electric current in an electronic power component (avalanche phenomenon), the electric tension at the boundaries of a load (electric arc), etc… [9].

D. Failure by accuracy and response time:

The failure per response time is studied with the same approach as to the failure by exceeding: we fix a maximum change Tresponse between the response time in the presence of disturbances and the ideal response time of the system. If at a given time the variation in the presence of transient faults exceeds Tresponse, we detect failure by the response time. We can justify this choice, since response time characterizes the duration of the transient phenomenon which in many cases is a source of energy loss. Such losses must be systematically prevented when they are likely to dangerously reduce the energy autonomy of a system, an issue not covered in the work done by [Rony et al., 2008].

In the general case, a previous study must precede the evaluation phase of this probability to decide about the number of unacceptable measurements, this parameter depends on the context of the application. In this study we have assumed that this parameter is a data for the study of dependability.

III. PRELIMINARY STUDY AND ANALYSIS OF FAILURE MODES:

A. Determination of constraints:

For the components that have been used, there should be an analysis of possible failure modes for each of them. These modes have been determined.
For parts of electric use, the constraints are related to tension, to power, to temperature, etc …, to which they are normally subjected, for mechanical parts, these are forces, vibrations, shocks, friction and temperature.
We will then determine a constraint index as compared to normal constraints envisaged by the manufacturers and by the corresponding reliability data, (it is obvious that if the constraints change during normal usage, we will calculate several indices of constraints).

B. Determination of failure rates

1) Calculation of failure rate or reliability of the blocks and systems:

Having obtained, at least partially, the failure rate or the predicted reliability of the components of various blocks (sub-functional unit), we will then calculate the failure rate of each block, taking into account any redundancy if available.
For each block, we take note carefully of utilization rates adopted for the prediction to be taken into account in calculating reliability of the system.
The calculation of predicted reliability of the system completes the task of forecasting reliability, depending on the complexity and configuration of the system, utilization rates of different components, etc..., we can either make a calculation of the overall failure rate, hence the Mean time between failures M.T.B.F follows immediately, or in cases of redundancy or failure variable rates, calculating a sufficient number of values of reliability in different periods to obtain a determination of the M.T.B.F by integration (graphical or digital)of the function reliability.
We must consider the redundancy to predict the reliability of a system, that is to say, to predict the probability of system failure. On the other hand, if we are interested in the number of failures expected to quantify the costs of corrective maintenance, we should not take into account the level of redundancy in sub systems.

C. Sources of available information:

There is a number of data sources on default rates, especially in electronics, most important of which include the MIL-HDBK-217 prepared by R.C.A on a contract of the U.S. Air Force and the A.R.I.N.C report No. 203-1-344. The data from the MIL-HDBK-217 have been taken through the center of reliability at C.E.N.T, and published in the journal "Reliability". However, the data must be handled with care and it is recommended to divide the failure rates indicated in this work into two when applied to digital circuits.

Additional information has been published more recently, corresponding to the components of digital electronic calculators in a laboratory environment or normal operation by the GEC Ltd.

IV. MODELING APPROACH BY INFORMATION FLOW:

In this paragraph, we modeled both the two sides of the sensor: analogical section consists of the pattern of Figure.1. Given the radical difference between the continuous analogical information and discrete digital information (bits) it was necessary to answer certain questions required by an appropriate model (approach to information flow) in order to unify these two different information.

A. Sources of failure:

According to experts, the main sources of errors in integrated electronics are short circuits, open circuits, external disturbances and aging of individual components.
Short circuits and open circuits are the result of the phenomenon of electro-migration, that is to say, the displacement of material (metal interconnection tracks) induced by the flow of electrical charges. This can be avoided by following some simple rules of track designing based on the maximum current they have to bear.
The electromagnetic disturbances (EMD) and the disturbances generated by the ionizing particles can cause the appearance of parasitic signals that are hardly indistinguishable from the useful signal. Their effects on the analogical circuits can be attenuated through the use of techniques on signal treatment at the level of the system (filtering). As far as the digital circuits are concerned, these are primarily sensitive to ionizing particles which are generally responsible for the unexpected modification of the value of information (bit) stored in a memory (rockers, RAM, etc…).
The aging of transistors as a result of hot carriers has consequences on the performance of analogical circuits. Indeed, their essential properties (gain, bandwidth, offset, etc...) Drift slowly over time.
Due to the nature of information carried by an analogical system, the safety of such devices can not be optimized using the same methods as those used for digital systems. Drift over time of characteristics of an analogical circuit results in errors about the information, which is inherently difficult to estimate. However, we can define intervals for the different parameters of an analogical circuit and we consider as the functionality of this circuit is correct as these parameters remain in these intervals (e.g.: minimum

and maximum gain for an amplifier). To maximize the lifetime of an analogical circuit, it is thus necessary to minimize the drifts of the important parameters, so that they remain more possible for a long time in the definite intervals.

The ageing of MOS transistors as a result of hot carriers is the main cause of drift parameters of analogical circuits. Based on modeling of the drift characteristics of transistors that rely on physical laws [10], we have developed a method allowing the designer to estimate the effects of ageing on the behaviour of transistors of the complete circuit. Using this model, the designer can then evaluate the lifetime of a given circuit or even integrating the constraints of operational safety of the circuit design to maximize the duration of life .

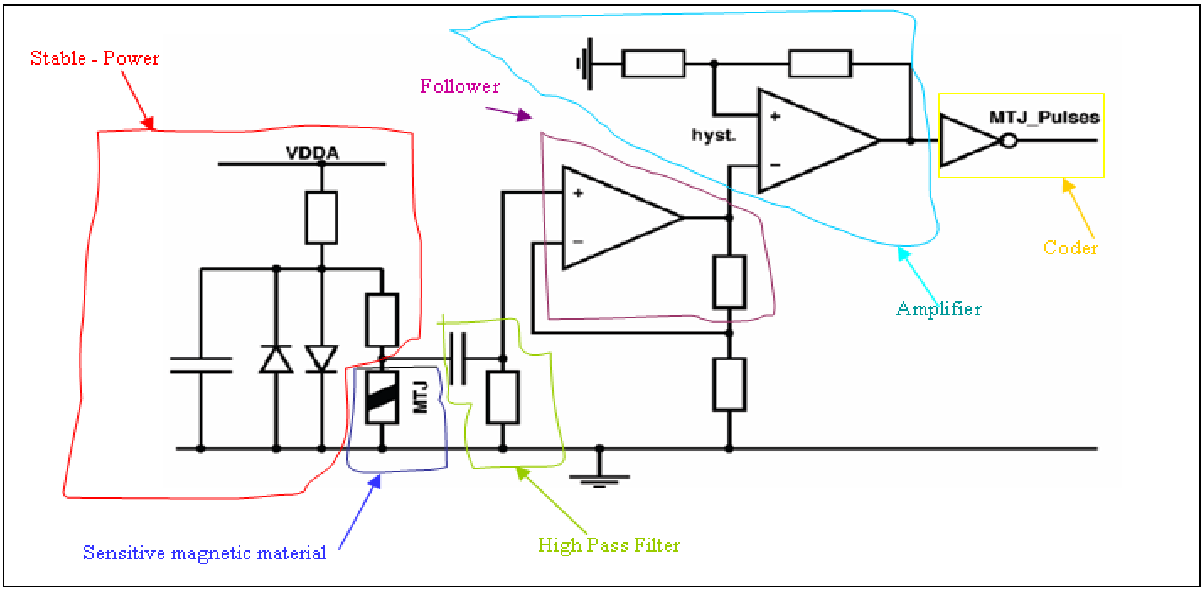

Figure 1: Electronic diagram of the analogical part of the sensor.

We have begun our study on reliability by a qualitative study as a preliminary analysis of risk, reflected in failure modes and effects analysis F.M.E.A table. The detailed analysis of the previous study (FMEA) of the circuit used to classify the most common problems that we can not deny, some of these problems are linked to the analogical part of the analogical sensor, as shown above (figure 1):

- Power Block: the failure of one of the diodes of this block may not provide the requested power.
- MTJ block: we exploit the physical property of magneto-resistance of materials in order to vary a duty cycle depending on the field. To ensure the proper response of the MTJ, we must imagine a check in the
- form of periodic testing of its response before starting measurements.
- The filtering stage consists of a first order filter. In this part, at any moment we can lose the accuracy of the bandwidth.
- Both follower and amplifier stages are carried out on integrated circuits which can not ensure their impedance matching a 100%

In the same context we can quote some essential failure mechanisms in the world of analogical components, some of which are quoted in table 1:

Failure mechanism	Failure mode	Affected areas
electrostatic Discharge	Short circuit, open circuit	Interconnection, MOS, bipolar
Breakdown of the gate oxide	Leakage current, short circuit	MOS
Effect of hot carrier	Offset of the threshold voltage, reducing the current gain	MOS, bipolar
Electromigration	Short circuit, open circuit	Interconnection
corrosion	Open circuit	Interconnection
Latchup	open circuit	CMOS
Radiation	Soft errors	memoirs

Table 1**:** Mechanisms and their modes of analogical failure.

These are microscopic failure mechanisms at the origin of macroscopic failure of the components and then of the system failure itself.

B. Modeling of a simple instruction:

The first phase to be dealt with in this study is the translations of each component of the hardware architecture by a functional entity as appropriate for the approach information flow, including:

- Signal Transformation (**TF**)
- Storage of the signal (**SB**) (for example, the modeling, of internal and temporal registers)
- Decision (**IP**) (for example, modeling the Multiplexer and UAL)
- Flow control (**CT**) (for example, modeling, internal buses)
- Online Test (**ST**) (modeling traffic control)

According to the previously defined under-functional entities and through the application of information flow approach on the overall architecture of our sensor (analogical part over numerical one), we obtain a highly-levelled global model for simulating the addition of two measurements.

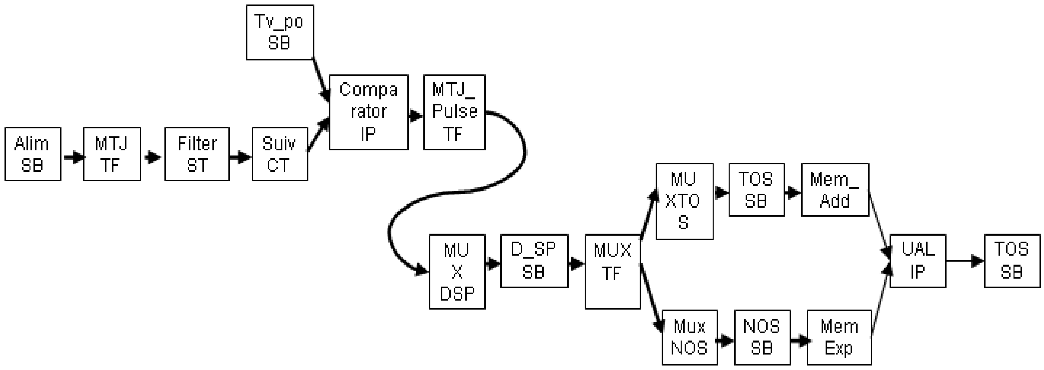

Figure 2: High level model of the architecture of the sensor in the case of an ADD instruction.

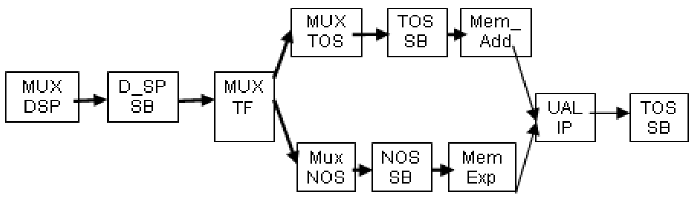

Figure 3: High level model in the absence of the analogical part.

Naturally, the next step of modeling according to the information flow approach requires passage through the low-level model in the form of finite state automaton. The problem is the interconnection between the two worlds, the automaton that represents the analogical part (continuous information) and the other representing the digital architecture of the processor (discrete information).

To better understand this problem in the analogical part, we encounter types of failures that differ from those in the digital part. In the analogical part we find three final states, namely:

- Failure in value or in accuracy.
- time Failure:
  - either through time excess.
  - or response time.
- Failure through stopping or loss of measurement.

However in the digital part, each time we would characterize and classify our architecture into six operating modes, namely:

- **Mode 1:** correct measurement, no failure detected.
- **Mode 2:** measurement error, failure detected but tolerated (search for availability).
- **Mode 3:** measurement error, failure detected but not tolerated (security research).
- **Mode 4:** measurement error, undetected failure (dangerous mode).
- **Mode 5:** correct measurement and failure detected (dirty shutdown).

- **Mode 6:** absence of measurement (stop of the system).

In this logic, it is obvious to say that the types of failure in the analogical part can cause failure of the digital part. Indeed there will be a continuation of the spread of information (information flow) between the two parties. The three analogical final states are the origin of one of the six methods above.
Subsequently we consider the concatenation and aggregation of both parties for automata (analogical and digital) to build a global model.
In Figure 4, we find several automata in cascade, each upstream automaton supplies a downstream one through information spread. The first six automata are the different components of the analogical part. As an example we consider the PLC power supply 'Alim', it consists of the following input and output:

- State of nominal operation where there is no anomaly **E-N**
- State of default value (may be a non-specific value) **E-D-V**
- State of time failure **D-E-T**
- State of information loss. **E-D-P**

The transition from one these states to another can be done through statements that represent failure modes causing the change of information, these states to the automaton in question are:

- State electrostatic discharge **D-Elc**
- State of electromigration **Elcmi**
- State of corrosion **Corro**

When the nominal information (no failure) at the component level 'Alim' passes through one of these intermediate states, this information goes to one of the states of fails listed above as shown in the block highlighted in yellow (Figure 4).
The other automata behave in the same way except that they comprise only two intermediate states:

- State of electrostatic discharge failure **D-Elc**
- State of failure by the effect of hot carriers. **D-P-CH**

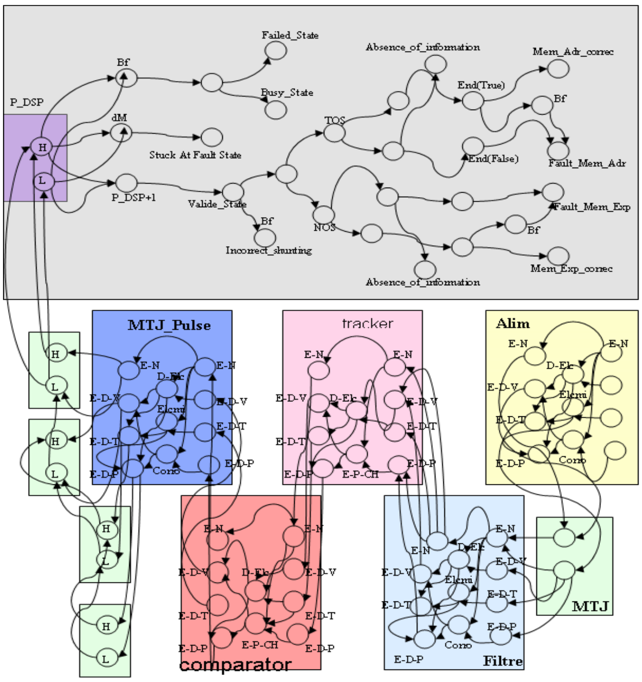

Figure 4: Model corresponds to a low level assembler instruction.

We combine the two worlds of automata, the digital part (top, mauve colour), and the analogical part (below with other colours). The result of this unification is to have the opportunity to generate global lists containing both information, both on the analogical and the digital parts for each instruction when running on the proposed architecture of the sensor.The monitoring of information begins with the first component of the analogical part to the last element of the digital architecture. The failure of information may be due to the failure of various parts or components. The global lists generated are able to locate the defaulting party and the effect of this part of the rest of the architecture.

We find the numerical values listed in Table 2 below:

Mode of operation / Instruction	Mode 1	Mode 2	Mode 3	Mode 4	Mode 5	Mode 6
ADD (Without analogical part)	$3.3\ 10^{-2}$	$0.7\ 10^{-2}$	$2.9\ 10^{-4}$	$1.1\ 10^{-5}$	$0.99\ 10^{-9}$	$1.11\ 10^{-11}$
ADD (With analogical part)	$72\ 10^{-5}$	$32\ 10^{-3}$	$893\ 10^{-3}$	$87\ 10^{-4}$	$4.99\ 10^{-4}$	$45.7\ 10^{-3}$

Table 2: Results for an ADD instruction.

The difference between these results and the results in the model about Figure 5 is the incorporation of the analogical part, the effect of which relies on increasing the probability of shutdown (mode 3), and decrease the probability of the nominal mode (mode 1).
The results at this level are related to a single assembly instruction, keeping in mind that our goal is to evaluate the program functions, knowing that each function consists of several instructions.

Probability of operating modes ADD instruction

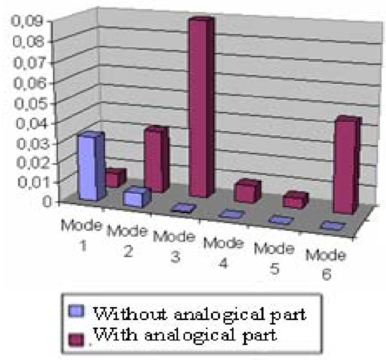

Figure 5: Graphical representation of results in Table 2

C. Case study: Program Sorting:

From the functional point of view of a digital system hierarchy, the software is designed to perform functions that the digital system performs at the level 0.
The software consists of modules. These software modules perform their tasks at the level 1 through a combination of instruction sets provided by the microprocessor part of the hardware components of the Level 3 (processor parts such as memory) are used for the treatment of an instruction level 2. So that the digital system supplements its required function, the software determines the correct order in which the resources of the material should be used. The failure of the system, thus, occurs when the software can not properly organize the sequence of material resources used, or when one or more used hardware resources have defects whereas the software has determined the correct sequences of material resources.

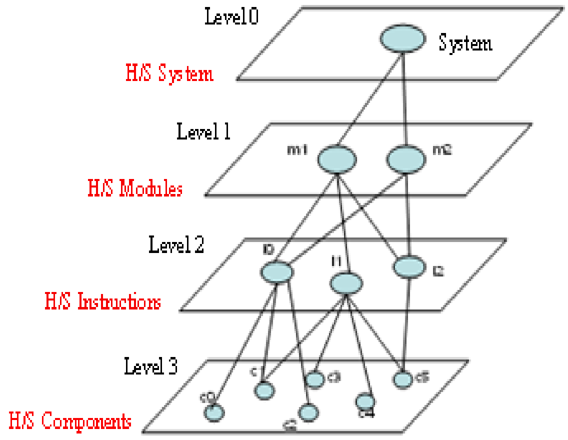

Figure 6: Hierarchical model of a software application.

In this work, we study a combinatorial model to estimate the reliability of embedded digital system using a multi-functional description. This model considers not only the handling of errors attributed to the digital part, but also the interaction between software and hardware with the examination of operating profile of the software.
The operational profile of the software determines the frequency of use of each of the software modules that control the frequency of use of the hardware components.
The operational profile of the software is modeled by the adaptation of multifunctional software flow control.
The functional model (dysfunctional) low-level shown in Figure 4, can generate all the lists on the level 3 (H / O components) in Figure 6.This package back in level 2 (H / O instructions) to give an idea about running an assembler instruction.

LInstruction=LAlim.LMTJ.LFiltre.Ltracker.LComparator.LMTJPULSE.LProcessor

LAlim: List characteristics of bloc power.
LMTJ: List characteristics of the sensitive head.
LFilter: list characteristics of filter block.
LTracker: tracker block list characteristics.
LComparator: comparator block list characteristics.
LMTJ-PULSE : Block List characteristics MTJ-PULSE.

LProcessor: List characteristic of the cell processor part,

Lfunction = LInstruction1, LInstruction2, LInstruction3, LInstruction4…. LInstruction i
Lmodule = LFunction1, LFunction2, LFunction3, LFunction4…. LFunction i….

Lapplication = Lmodule1, Lmodule2, Lmodule3, Lmodule4, Lmodule5 … Lmodule i

Using the method of calculation and quantification of each mode, we came up with the numerical results cited in the following table 3.
The numerical results show how the addition of the analogical part reduces overall system reliability. We note the decrease in the reliability indices measured in the table (six modes).
The analogical part witnesses some specific failure modes such as information drift that is the direct consequence of the aging phenomenon.

	Mode 1	Mode 2	Mode 3	Mode 4	Mode 5	Mode 6
Program_sort (Without considering the analogical part)	**$6.32\ 10^{-2}$**	**$1.57\ 10^{-2}$**	**$2.39\ 10^{-4}$**	**$55.8\ 10^{-5}$**	**$73\ 10^{-9}$**	**$45.91\ 10^{-11}$**
Program_sort (Taking into account the analogical part without tolerance)	**$5.22\ 10^{-4}$**	**$1.1\ 10^{-3}$**	**$5.5\ 10^{-4}$**	**$67.3\ 10^{-3}$**	**$12.2\ 10^{-6}$**	**$45.2\ 10^{-9}$**
Program_sort (Taking into account the analogical part and with tolerance)	**$11.49\ 10^{-2}$**	**$1.2\ 10^{-2}$**	**$9.67\ 10^{-4}$**	**$99.3\ 10^{-5}$**	**$27.8\ 10^{-9}$**	**$98.61\ 10^{-11}$**

Table 3: Effect of analogical part on the reliability assessment of the sensor .

V. OPERATING RESULTS TO IMPROVE RELIABILITY

After the connection has been established, the devices (sensors) of our system start to exchange, communicate and acquire information. In this case several problems have occured, we can mention the following ones as example: loss of information, problem of checking up messages, so as to eliminate the duplicated ones ,and the resolution helps to conserve battery power of each device. After identifying major deficiencies which reduce the reliability of this system, we will develop an algorithm, specifically with the aim of remedying the problem of aberrant values, and that will eventually give a degree of confidence of the exchanged values.

A. Communication process in the proposed architecture:

The peers (sensors, aggregators, etc...) are represented by components. Indeed, in a distributed system, a component is often represented by a set of software modules [11]. Communication between these components is provided by interfaces as events (Figure.7).
To exchange the information, the communication interfaces of each component must respect the following events:

-*Request:* Events used by a component to request another component in the system.
-*Confirmation:* Used by the same component to confirm the completion of a request.
-*Indication:* Used by the component to deliver information to another component in order to ensure the corresponding reliability guarantee.

All communication that passes through the peers must respect the events listed above.

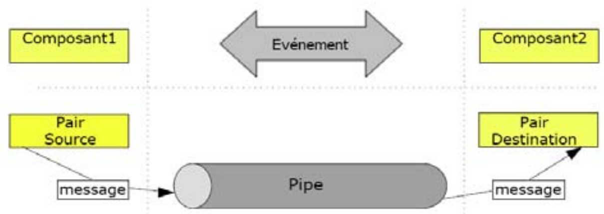

Figure.7: Process of message exchanging in the network

B - Definition some modules of the network:
We opted for the logic of interfaces that will be defined as abstract models [11].

1) Aberrant values detection:
Based on statistical measures stored in the database of our wireless sensors network (WSN), we can notice that exact values are repeated in relation to a specific location for a specific application of a WSN. This statement allows us to check the measurements before validation and aggregation. To achieve this process, we propose the following analogy of verification:
Example: Temperature measurements in a location E.
After a given time t according to monitoring and statistics, the temperature value (V_{te}) varies between two exact values:

$$I: [E_x: V_{min} - \varepsilon \le V_{te} \le V_{max} + \varepsilon] \quad (1)$$

$V_{min:}$ Value of the maximum temperature.
$V_{max:}$ Value of the minimum temperature.

Such as ε varies according to the location E_x.

Module 1: *Interface and properties of aberrant values detection.*

Name: *Aberrant Values Detection* (*avd*).

Events:

Request: (*avdSent* | *dest*, *v*): Used to request transmission of the message *v* to the destination *dest*.

Indication: (*avdReception* | *src*, *v*): Used to deliver the message *v* sent by the source *src*.

Properties:

Pr1: *avdVerificationTemp*: Let c_i any component that sends a value *v* to a component c_j. If the value of *v satisfies the condition (1).* Then c_j receives the value *v*.

Pr2 : *avdAlerte* : The system triggers a dysfunction when the transmitted value does not belong to the interval I.

To implement the various events and the achievement of the Module.1 properties, we propose the algorithm .2.

```
Begin
    ε := π ;
    Set Vmin: =init (Vmin);
    Set Vmax: =init (Vmax);
        Call (avdSent | dest, v);
        If [v Є [Vmin, Vmax]] then
            (avdReception | src, v) ;
          Else
            Call avdAlerte ();
        End if;
End;
```

Algorithm2: Triggering failures

2) Loss and duplication of messages:

In a WSN it is possible that messages are lost during their transmission. This may cause severe problems if the message is intended to convey pertinent information. the loss of information is still probable due to the sudden dysfunctioning of the network devices. The solution is to detect at the right time if a message has failed in order to know the source of failure. A secondary problem of message transfer in WSNs is related to the large number of duplicated messages; this generates a loss of battery power for the sensors.Module.2 is an implementation of interfaces and properties used in this context. We have implemented a fusion of the verification of sending messages and the verification of its duplication in this module.

Module 2: *Interface and properties of verification Loss and duplication of messages*

Name: Loss Duplication (*ld*).

Events:

Indication1: Used to obtain confirmation of reception of the message v, either, *Ok* or *No.*

Indication2: (*ldadd*| *Tablemsg*, *v*): Used to add the values those have not circulated in the network.

Indication3: (pdDraw |msg, *v*): Used to format the messages to display.

Indication4: ldAlarm (): Used to trigger the loss of a sensor value.

Properties:

Pr1: *NoLoss :* If a message is not reached its destination, the system triggers the loss.

Pr2: *NoDuplication:* each value can be sent by a sensor only once.

The procedure for eliminating duplicated messages, safeguarding the values that were never collected by a sensor, and the detection of lost messages, are implemented in the algorithm3.

```
Begin
// we call the Module.1 to use its events.
    Use Module1;
//Tablemsg: Is a volatile storage unit of the messages already sent by a sensor.
    Tablemsg: = init (Table);
    Status: = Nok;
        If (v Є Tablemsg) then
          Call (ldDraw |" duplicated message", v);
          Exit (1);
        Else
            Call (ldSent | dest, v);
            Call (ldStatus | reqid, statuts);
            // Storing sent messages
            Call (ldadd| Tablemsg, v);
        Endif;
        If (status = ok) then
          Call (ldReception | src, v);
           Else
              Call ldAlarm ();
        Endif;
End;
```

Algorithm3 : NoLoss & NoDuplication

VI. CONCLUSION

Reliability predictions do not contribute substantially to the reliability of a system, but must be an element of trial to assess the actions needed to improve it and they must also be used to assess the current state of reliability of system with respect to the objectives that were set. The main objectives of these predictions are: assessing the feasibility of this system, comparison of competitive solutions and methods, determining the required objectives, highlighting the problems of reliability, searching for numerical data insufficient study of compromises with other cost elements in the system, appreciation of progress and predicting the maintenance of this system. All of these points are summarized as follows:

- Assessment of options: check the compatibility of the operating principles to the objectives of reliability which have been proposed.
- Comparison of competitive solutions and methods: state of the art.
- Highlighting the problem of reliability.
- Operating reliability data: during the analysis required by the prediction phase we will highlight the points for which reliability data are not entirely suitable, because of different operating conditions or following a change for a component that differs from the initial component.
- Progress follow-up : checking the situation of the project with respect to the targeted objectives
- Predicted maintenance: Finally, the estimated reliability allow for the assessment of maintenance and repairing costs in order to deal with random failures of the system.

In this paper, the study of the analog part shows that the failure modes are radically different from the digital part, taking into account the nature of the information (continuous signal). We have shown the effect of the components age that impacts on reliability. Fortunately, the informational approach flow is valid and has allowed us to evaluate the two parts of the sensor (processor, analogical part) together in a model which unifies both.

The presence of the analogical part has obviously changed the probability values, in this case the sensor tends to be in state 3 and 4 with low probability of being in state 1. The consideration of tolerance has put the sensor in a normal state (a significant probability of state 1) and two with a negligible probability of state 3 and 4.

FUTURES WORKS

As far as the perspectives are concerned, many points remain to be improved. A peculiarity in failure modes for mechatronic systems is related to interactions between different technologies. This aspect is little studied and is in fact a technological barrier. Indeed, analysis of the reliability of each system component is not sufficient. It becomes necessary to study the whole system, its components, interactions between different components and to integrate these aspects in a comprehensive methodology for estimating reliability.

The algorithmic search of scenarios proposed in this work for a hybrid system still requires some adjustments to be applied in an industrial context. It is necessary to confirm it in real contexts. This will allow us to validate the proposed methodology and the tools associated with its implementation, note the automation of all the steps of application of this method as was done in [7].

Another important issue that still demands a lot of work is the approach about the integration of dependability in the engineering process system. The proposed approach is a preliminary work that needs to be developed. To facilitate the future use of our methodology in an industrial context, it is necessary to develop a tool automating the treatments, We also plan to make the architecture self-reconfigurable, smarter, and delivering measurements with a confidence level.

The quantitative analysis is an important issue to be explored to estimate the probability of occurrence of states feared. Even if the qualitative study is of real interest, it can only be complementary to a quantitative study.

REFERENCES

[1] Dutuit Y., Rauzy A., Signoret J.-P., Thomas P. "Dependability modelling and evaluation by using stochastic Petri nets: application to two test cases". Reliability Engineering and System Safety 55, 1997, p. 117-124.

[2] Buisson J., "Analysis of switching devices with Bond Graphs", journal of the Franklin Institute, vol. 330, n°6, p. 1165-175, 1993

[3] Alla, H. and David, R. "Continuous and Hybrid Petri Nets". Journal of Circuits, Systems & Computers 8(1): 159-188. 3, 1998.

[4] M. Medjouji, Contribution to the analysis of systems controlled by computers: Extraction of feared scenarios and verification of temporal constraints. Thesis, University Paul Sabatier in Toulouse. Mars 2006.

[5] J.-L. Chabot, Y. Dutuit, A. Rauzy & J.-P. Signoret. An engineering approach to optimize system design or spare parts inventory. Risk Decision and Policy, 8:1-11, 2003.

[6] Pérez Castaneda G. A., Aubry J-F., Brinzei N. Modélisation et simulation d'un système dynamique hybride pour calculer sa fiabilité dynamique en utilisant le toolbox Scicos de Scilab. 7ème édition du Congrès International pluridisciplinaire Qualita 2007 – Tanger (Maroc), p. 311 – 318, 2007.

[7] H.BELHADAUOI, G. BUCHHEIT, O.MALASSE, J-F.AUBRY, H.MEDROMI. 'Méthode quantitative d'Evaluation de la Fiabilité des Systèmes Critiques Programmés' Lamda_Mu16, Avignon, Septembre 2009.

[8] S. Poledna. Tolerating sensor timing faults in highly responsive hard realtime systems. IEEE Transaction on computers. Vol (44), No 2, p:181-191, February (1995)

[9] R.Ghostine, J.M. Thiriet, J.F. Aubry, M. Robert. A framework for the reliability evaluation of networked control systems. To appear in the 17th IFAC World Congress. July 6-11, 2008, Seoul, Korea.

[10] Kun-Yue Chen, Sheng-Hung Wu, Yih-Wen Wang and Chi-Min Shu, 'Runaway reaction and thermal hazards simulation of cumene hydroperoxide by DSC'. Journal of Loss Prevention in the Process Industries, Volume 21, Issue 1, January 2008, Pages 101-109

[11] R. Guerraoui, L.Rodrigues, *Introduction to reliable distributed programming*, Springer 2006: I-XVIII, 1-299

Amina MERBAH Currently a PhD student ,University Hassan II /ENSEM Casablanca Morroco. Received a master's degree in 2010 at University of Sciences Semlalia–Cadi Ayyad, Marrakech, Morroco. Research: Reliability in Wirrelss Sensor Networks.

Hicham BELHADAOUI Currently working as a Assistant Professor in University Hassan II /ESTC, Casablanca Morroco.Received his Phd degree at National Polytechnic Institute of Lorraine/France. Research : Reliability ,Automatic Signal Processing and Computer Engineering.

Mohamed OUZZIF Presently working as a Professor Ability in University Hassan II /ESTC. Received his Phd degree from University Hassan II /ENSEM, Casablanca Morroco. Research : Distributed Systems and Computer Engineering .

Olaf MALASSÉ he is currently attached with National School of Arts/ and Crafts/ ParisTech in Metz/France as Associate Professor in A3SI department. Research : Automatic Signal Processing and Computer Engineering.