Reliability Study of an Intelligent Transmitter

Florent Brissaud, Anne Barros, Christophe Bérenguer, Dominique Charpentier

RELIABILITY STUDY OF AN INTELLIGENT TRANSMITTER

Florent Brissaud[1,2], Anne Barros[2], Christophe Bérenguer[2], & Dominique Charpentier[1]

[1]Institut National de l'Environnement Industriel et des Risques – INERIS
Parc Technologique ALATA, BP2, 60550 Verneuil-en-Halatte, France
E-mail: florent.brissaud@ineris.fr, Tel: (33) 3 44 55 69 89

[2]Université de Technologie de Troyes – UTT
Institut Charles Delaunay, FRE CNRS 2848
BP 2060, 10010 Troyes Cedex, France
E-mail: florent.brissaud@utt.fr

Key Words: Intelligent Transmitter, Reliability, Relationship Analysis, Uncertainty Analysis

Abstract

An intelligent transmitter reliability study has to deal with several issues: various interactions between both material elements and functions; behaviors of components as programmable units and software which are difficult to predict when faults or failures occur, as well as the consequences on functions processing. A "3-step model" is therefore proposed to include both functional and material aspects, using Goal Tree–Success Tree (GTST), and setting faults and failures as a third full part. Then, Master Logic Diagrams (MLD) aim to represent several types of relationships between faults or failures, material elements, and functions. Probabilities are used for MLD components to take the indeterminate relationships into account. Quantitative assessments are then performed, using an infrared gas transmitter as an example: total relationships between any fault or failure and any function, probabilities of malfunction and failure modes. Moreover, uncertainty analyses show that even if input relationship data are uncertain, precise results can be obtained. These properties make the proposed model especially suitable for evaluating the reliability of intelligent transmitters. Finally, some design issues are discussed, taking advantage of the proposed model.

1. Introduction

A transmitter can be described as "intelligent" according to advanced functionalities involved in the host system operation:

- The ability to modify its internal behavior to optimize data collection and communicate them in response to a host system [1].
- The bidirectional communication for sending measurement and status information, and receiving and processing external commands [2].

Intelligent transmitters may take advantage of digital technologies to integrate specific functionalities [3]: error measurement correction [4], self-adjustment [5], self-diagnose and validation [6], on-line reconfiguration [7], and digital bidirectional communication [8]. For example, industrialists can get more accurate measurements, cost reductions, and use facilities [9]-[10].

The use of intelligent transmitters for industrial risk prevention requires dependability evaluations, for example in accordance with the IEC 61508 functional safety standard [11]. Probabilities of failure on demand have therefore to be assessed in order to determine the system safety integrity level (SIL). However, dependability studies of intelligent transmitters are quite seldom in literature, and do not often take into account the "intelligent" features [3]. To this end, a kind of Goal Tree–Success Tree (GTST) technique, combined with Master Logic Diagrams (MLD), as proposed in [12], has been used in [13] to model intelligent transmitters. The main advantages are to represent quite intuitively both material and functional aspects, and various interactions. Such models have been introduced in [13] to support further reliability studies.

In the present paper, a reliability study is proposed, using an extended GTST-MLD model which integrates faults and failures as a third full part, making a "3-Step model". This approach is described in Section 2 for an infrared gas transmitter. Relationship analyses are performed in Section 3 to evaluate the impact of any fault or failure on any material element or function. Probabilities of malfunction and failure modes (according to the main functions fulfillment) are assessed in Section 4. In Section 5, relationship uncertainty analyses tend to show the robustness of the proposed model faced with uncertainties in system behavior. Finally, some design issues are discussed in Section 6.

2. "3-Step model"

2.1. Infrared gas transmitter

A transmitter for measuring gas concentration by infrared absorption is used as a case study. It is made up of two infrared units: the *working unit* sends a ray with a proportional wavelength to the gas concentration to be measured; and the *reference unit* sends a ray which does not respond to the gas. Using a wavelength ratio of the two receiving rays, the gas concentration quantity is obtained with corrections of the optics clogging up (mirror and plane), and power fluctuations of sending rays. When a clogging up threshold is reached, appropriate corrections are no longer allowed and diagnosis information is transmitted. Heating elements aim to prevent steam from building up on *optics*. Temperature is a major influence on gas concentration, *temperature sensors* are therefore used for digital compensation. When the temperature is out of an acceptable range, this correction is no longer suitable and diagnosis information is transmitted. A *digital card* carries out processing and calculations, and controls the other units. Finally, all the transmitter material elements share the same *power supply*, and a *converter* is required by infrared units.

The following functions are investigated: *measure* i.e. assessing the gas concentration with appropriate digital corrections; *diagnose* i.e. checking the influencing quantities in acceptable ranges; *self-adjustment* of off-set and gain drift, used to regularly set digital parameters required by the two previous functions. *Measure* and *diagnose* functions first involve *obtaining the appropriate data*, then in *processing* them. Communication aspects with the host system are performed using an analogical card but are not included in the following analyses.

2.2. Functions–material elements–faults and failures

The model is based on Goal Tree–Success Tree (GTST), combined with Master Logic Diagrams (MLD), as proposed in [12]. GTST-MLD has been already used in [14] to identify complex system failures. In the present paper, faults and failures are introduced as a third full part, making a "3-step model", as depicted in Figure 1.

The *functional tree* (or *goal tree* i.e. GT) breaks the system *goal* (obtain valid measurement and diagnosis) up into *global functions* (measure, diagnose), and *basic functions* (obtain data, process data). The *supporting functions* (self-adjustment) are given in parallel to the main functions (measure and diagnose) because of the impact on them. In the same way, the *material tree* (or *success tree* i.e. ST) breaks the system up into *subsystems*, *units*, and *supporting materials*. The third step contains a *list of faults and failures* for at least one of the material elements. This extension of the GTST model aims to include the dysfunctional aspects as a third full part. Some of these faults or failures may cause a unit failure only in some cases (e.g. the loss of optics heating may have no impact on system if, at this moment, environmental conditions are suitable); and may impact only one unit (e.g. optics clogging up) or several (e.g. common failure to infrared units).

Direct relationships between faults or failures, material elements, and functions, are given in *Master Logic Diagrams* (MLD), (i.e. matrices *DP*, *DM*, *PM*, *MS*, *MF*, and *SF*), and represent aspects of system behavior. The dot color of MLD components depends on the degree of relationship between downstream and upstream elements.

3. Relationship analysis

3.1. How to model relationships?

To model relationships which are represented by MLD components, several approaches can be proposed:

- *Qualitative relationships* (e.g. very low, low, medium, and high), as given in Figure 1 with dot colors, can be used for prior analyses. Nevertheless, to allow quantitative results, these values have to be quantitatively translated.
- *Architectural relationships* describe the deterministic requirements of material elements or functions in terms of other elements. For example, weighted component techniques assign a weight to each downstream element. The upstream element is then assumed to be able to operate if the sum of the weights of its operating downstream elements is equal to or greater than a threshold. These capacitated systems provide extensions of *k*-out-of-*n* architectures which operate if at least *k* among *n* of its elements operate.
- *Stochastic relationships* aim at allocating to each downstream element the probability that its failure implies upstream element failure. Indeterminate consequences of faults or failures on the rest of the system are therefore taken into account in that way. An upstream element can reach a failed state due to any downstream element failures, according to given probabilities.

One of the main dependability issues for intelligent transmitters is to deal with the complexity of some components as programmable units and software, because it is difficult to predict the consequences of faults or failures [13]. Moreover, these faults or failures may heterogeneously act on several material elements and functions. For this reason, a stochastic relationship approach is chosen in the present paper. By allocating probabilities between a downstream element and several upstream elements, it is possible to assess the probability that the downstream element failure implies a failure of any upstream element alone, or any combination of them. At the transmitter level, failure modes can then be defined according to the accuracy of transmitted data (e.g. measurement, diagnoses), used for host system decisions. For example, a software fault may imply a bad measurement but an appropriate diagnosis, or vice-versa. These properties can be directly deduced from the model, without defining all the component failure modes as required by binary tools or state transition approaches.

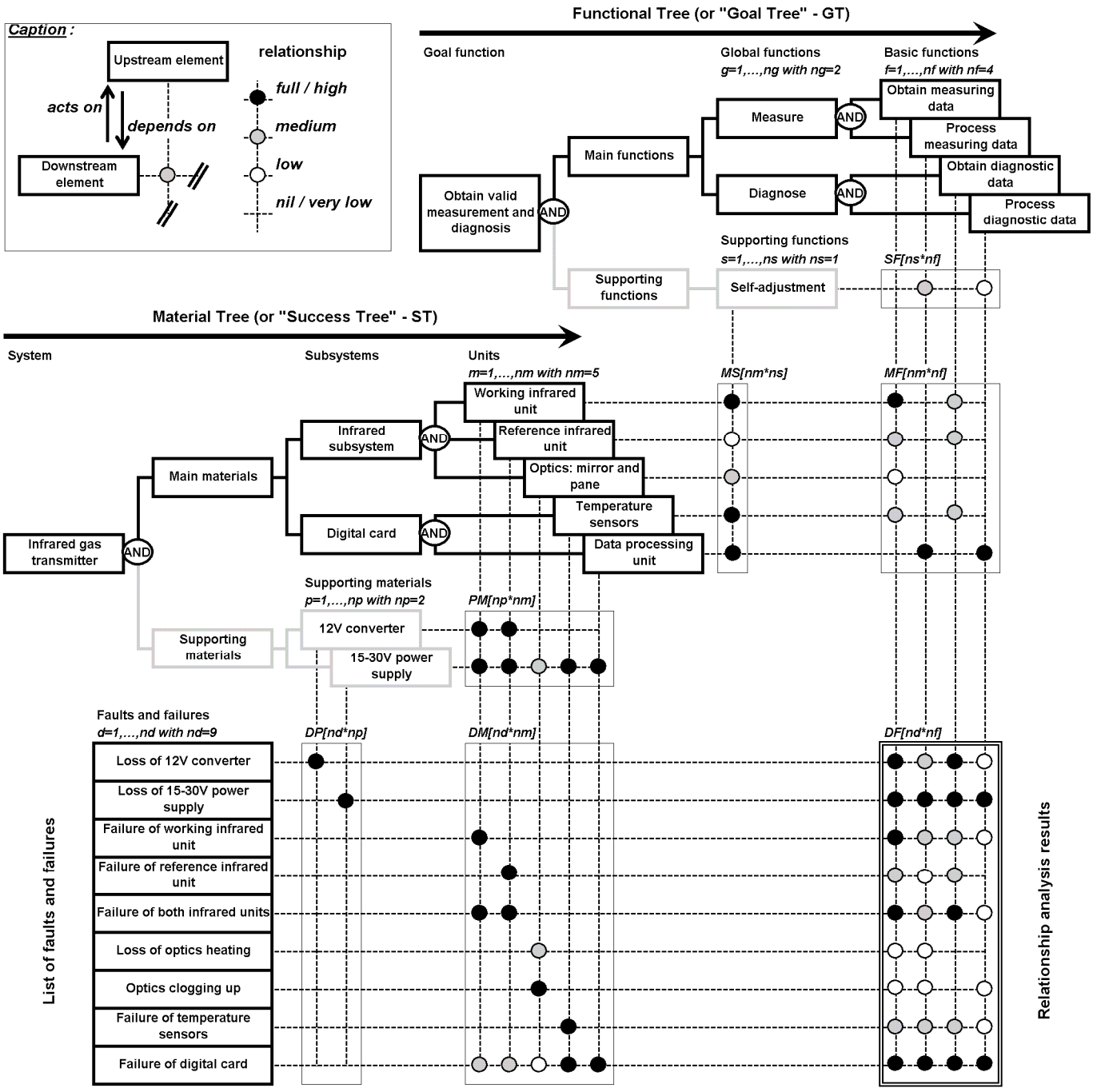

Figure 1. "3-Step model" (functions–material elements–faults and failures) for an infrared gas transmitter

3.2. Stochastic relationships for "3-Step model"

3.2.1. Notations and definitions

Let the following events be:
- D_d = {fault or failure d occurs}
- P_p = {supporting material element p is in a failed state}
- M_m = {main material element m is in a failed state}
- S_s = {supporting function s is in a failed state}
- F_f = {main function f is in a failed state}

The direct relationship event between a downstream element a and an upstream element b is represented in matrix AB, row of index a and column of index b, and defined as follows:

- $AB_{a,b}$ = {event A_a (i.e. failure of element a) directly implies (i.e. without request for any other event) event B_b (i.e. failure of element b)}

All the direct relationship events are assumed to be independent and the stochastic relationship values are given by the probabilities $P[AB_{a,b}]$.

3.2.2. Example

According to Figure 1, the failure of main material element *data processing unit* (event M_5) directly implies the failure of supporting function *self-adjustment* (event S_1) if event $MS_{5,1}$ occurs, and the failure of main function *process measuring data* (event F_2) if event $MF_{5,2}$ occurs. That refers to "direct relationships".

In addition, the failure of *self-adjustment* (event S_1) directly implies the failure of *process measuring data* (event F_2) if event $SF_{1,2}$ occurs. The failure of *process measuring data* due to the failure of *data processing unit*, through the failure of *self-adjustment*, refers to an "indirect relationship". Notice that direct and indirect relationships are not incompatible.

According to Figure 1, no other event directly implies the failure of main function *process measuring data* (event F_2), ($SF_{s,2}$ does not exist for $s \neq 1$, and $MF_{m,2}$ represent nil relationships for $m \neq 5$). However, the failure of any other main material element (event M_m with $m \neq 5$) also directly implies the failure of supporting function *self-adjustment* (event S_1), if corresponding event $MS_{m,1}$ occurs. The probability of failure of *process measuring data* (event F_2), denoted $P[F_2]$, can therefore be expressed as follows:

$$P[F_2] = P\left[\left(M_5 \cap MF_{5,2}\right) \cup \left(S_1 \cap SF_{1,2}\right)\right] \quad (1)$$

$$P[F_2] = P\left[\begin{array}{l}\left(M_5 \cap MF_{5,2}\right) \\ \cup\left(\left(\bigcup_m \left(M_m \cap MS_{m,1}\right)\right) \cap SF_{1,2}\right)\end{array}\right] \quad (2)$$

The first part of (2) expresses the direct relationships between main materials *m* and main function *2*; and the second part expresses the indirect relationships.

By pivotal decomposition around $MF_{5,2}$, then M_5:

$$\begin{aligned} P[F_2] &= P[MF_{5,2}] \cdot P[M_5] \\ &+ P[MF_{5,2}] \cdot (1 - P[M_5]) \\ &\quad \cdot \left(1 - \prod_{m \neq 5} \left(1 - P[M_m] \cdot P[MS_{m,1}]\right)\right) \cdot P[SF_{1,2}] \\ &+ (1 - P[MF_{5,2}]) \\ &\quad \left(1 - \prod_m \left(1 - P[M_m] \cdot P[MS_{m,1}]\right)\right) \cdot P[SF_{1,2}] \end{aligned} \quad (3)$$

The same approach has to be taken for each probability of event M_m occurrence, denoted $P[M_m]$. For example, according to Figure 1, the probability of failure of *data processing unit* (event M_5), denoted $P[M_5]$, is equal to:

$$P[M_5] = P\left[\left(D_9 \cap DM_{9,5}\right) \cup \left(P_2 \cap PM_{2,5}\right)\right] \quad (4)$$

$$P[M_5] = P\left[\begin{array}{l}\left(D_9 \cap DM_{9,5}\right) \\ \cup\left(\left(D_2 \cap DP_{2,2}\right) \cap PM_{2,5}\right)\end{array}\right] \quad (5)$$

$$\begin{aligned} P[M_5] &= 1 - \left(1 - P[D_9] \cdot P[DM_{9,5}]\right) \\ &\quad \cdot \left(1 - P[D_2] \cdot P[DP_{2,2}] \cdot P[PM_{2,5}]\right) \end{aligned} \quad (6)$$

3.2.3. General formulas

The general formula for the probability of failure of any main function *f* is given by:

$$P[F_f] = P\left[\bigcup_m \left(M_m \cap MF_{m,f}\right) \bigcup_s \left(S_s \cap SF_{s,f}\right)\right] \quad (7)$$

$$P[F_f] = P\left[\begin{array}{l}\bigcup_m \left(M_m \cap MF_{m,f}\right) \\ \bigcup_s \left(\left(\bigcup_m \left(M_m \cap MS_{m,s}\right)\right) \cap SF_{s,f}\right)\end{array}\right] \quad (8)$$

$$P[F_f] = P\left[\bigcup_m \left(M_m \cap MFtot_{m,f}\right)\right] \quad (9)$$

with $MFtot_{m,f}$ the total relationship event between main material element *m* and main function *f*, taking into account all supporting functions, and expressed as follows:

$$MFtot_{m,f} = \left\{MF_{m,f} \bigcup_s \left(MS_{m,s} \cap SF_{s,f}\right)\right\} \quad (10)$$

From (9), and with a similar approach for events M_m:

$$P[F_f] = P\left[\bigcup_m \left(\begin{array}{l}\left(\bigcup_d \left(D_d \cap DMtot_{d,m}\right)\right) \\ \cap MFtot_{m,f}\end{array}\right)\right] \quad (11)$$

with $DMtot_{d,m}$ the total relationship event between fault or failure *d* and main material element *m*, taking into account all supporting material elements, and expressed as follows:

$$DMtot_{d,m} = \left\{DM_{d,m} \bigcup_p \left(DP_{d,p} \cap PM_{p,m}\right)\right\} \quad (12)$$

Finally:

$$P[F_f] = P\left[\bigcup_d \left(D_d \cap DF_{d,f}\right)\right] \quad (13)$$

with $DF_{d,f}$ the total relationship event between fault or failure *d* and main function *f*, taking into account all the direct and indirect relationships, and expressed as follows:

$$DF_{d,f} = \left\{ \bigcup_{m} \left(DMtot_{d,m} \cap MFtot_{m,f} \right) \right\} \quad (14)$$

Notice that events given in matrices *MFtot* and *DMtot* are not independent. In fact, the same $SF_{s,f}$ events play a part in several rows of matrix *MFtot*, and the same $MS_{m,s}$ events in several columns (respectively for events $PM_{p,m}$ and $DP_{d,p}$ in matrix *DMtot*). Events given in matrix *DF* are therefore not independent and (13) has to be used with caution. For example, (3) has been obtained by pivotal decomposition.

To make evaluations with classical reliability software tools, equivalent fault trees to the "3-Step model" is proposed in Figure 2, for any main function *f*. Figure 2.a corresponds to (7), and including Figure 2.c "transfer in" gate, the obtained fault tree corresponds to (8). Direct relationships between main material elements *m* and main function *f* correspond to the first part of (8) and to the "F-Direct" gate of Figure 2.a. Indirect relationships correspond to the second part of (8), and to the "F-Indirect" gate of Figure 2.a. The same approach is used for each failure of main material element *m* (events M_m), respectively with Figure 2.b, and Figure 2.d.

Several interactions between material elements and functions, and the conditional nature of relationship events, make the fault trees difficult to directly perform and interpret. The "3-step model" therefore aims at overcoming these qualitative issues by providing a more intuitive and global view of system material, functional, and behavior aspects. The equivalent fault trees can however be used as practical tools for common quantitative analyses.

3.3. Relationship analysis

The relationship analysis consists in evaluating the impact of any fault or failure *d* on any main function *f*. These relationship events are given in matrix *DF*. Even if events are not independent, from (13) it is possible to understand each probability of relationship event individually, as follows:

$$P\left[DF_{d,f}\right] = P\left[F_f \Big/ D_d \cap \bigcap_{\delta \neq d} \overline{D_\delta} \right] \quad (15)$$

That is, if the fault or failure *d* occurs (event D_d) and not any other, the failure of main function *f* occurs (event F_f) with a probability equal to $P[DF_{d,f}]$. This value can also be interpreted as the individual impact measure of fault or failure *d* on main function *f*. Calculating $P[DF_{d,f}]$ is then quite simple by using (15) and fault trees given in Figure 2.

$P[DF_{d,f}]$ are calculated according to input probabilities given in Table I (second column), and Figure 1. For example, $SF_{1,2}$ represents a medium relationship event, thus $P[SF_{1,2}] = 0.67$. In the same way, $P[MF_{m,2}] = 0$ for $m = 1,\ldots,4$, and $P[MF_{5,2}] = 1$ etc. These values are then used by (14), after compilation with (10) and (12). Finally, the obtained $P[DF_{d,f}]$ are graphically translated according to Table I (third column), and reported in Figure 1 ("relationship analysis results").

For example, $P[DF_{8,2}] = 0.67$. According to Table I, $DF_{8,2}$ therefore represents a medium relationship event and, according to Figure 1 caption, the corresponding event dot color is dark grey. An interpretation of this result is "if a *failure of temperature sensors* occurs, and no other fault or failure, *process measuring data* will malfunction with a probability equal to *0.67*".

At the system level, it is more often relevant to study the impact of each fault or failure on global functions, instead of basic functions. Then, let the following event be:

- G_g = {global function *g* is in a failed state}

For the infrared gas transmitter case study, the global functions are: *measure* ($g = 1$), and *diagnose* ($g = 2$). Corresponding fault trees are given in Figure 3. From (13):

$$P\left[G_g\right] = P\left[F_i \cup F_j\right] = P\left[\bigcup_{d} \left(D_d \cap DG_{d,g} \right) \right] \quad (16)$$

with $\{i,j\} = \{1,2\}$ if $g = 1$ and $\{i,j\} = \{3,4\}$ if $g = 2$. $DG_{d,g}$ is the total relationship event between fault or failure *d* and global function *g*, taking into account all the direct and indirect relationships, and expressed as follows:

$$DG_{d,g} = \left\{ DF_{d,i} \cup DF_{d,j} \right\} \quad (17)$$

The individual impact measure of fault or failure *d* on global function *g* is therefore defined as follows, and obtained values are reported in Table II:

$$P\left[DG_{d,g}\right] = P\left[G_g \Big/ D_d \cap \bigcap_{\delta \neq d} \overline{D_\delta} \right] \quad (18)$$

Table I. Stochastic relationship values

Relationship	Input probability	Result translation
full / high	1.00	$0.83 \leq x \leq 1.00$
medium	0.67	$0.50 \leq x < 0.83$
low	0.33	$0.17 \leq x < 0.50$
nil / very low	0.00	$0.00 \leq x < 0.17$

Table II. Relationship analysis results

Fault or failure *d*	Impact on *measure* i.e. $P[DG_{d,1}]$	Impact on *diagnose* i.e. $P[DG_{d,2}]$
1	1.00	0.92
2	1.00	1.00
3	1.00	0.76
4	0.76	0.71
5	1.00	0.93
6	0.42	0.15
7	0.65	0.21
8	0.90	0.77
9	1.00	1.00

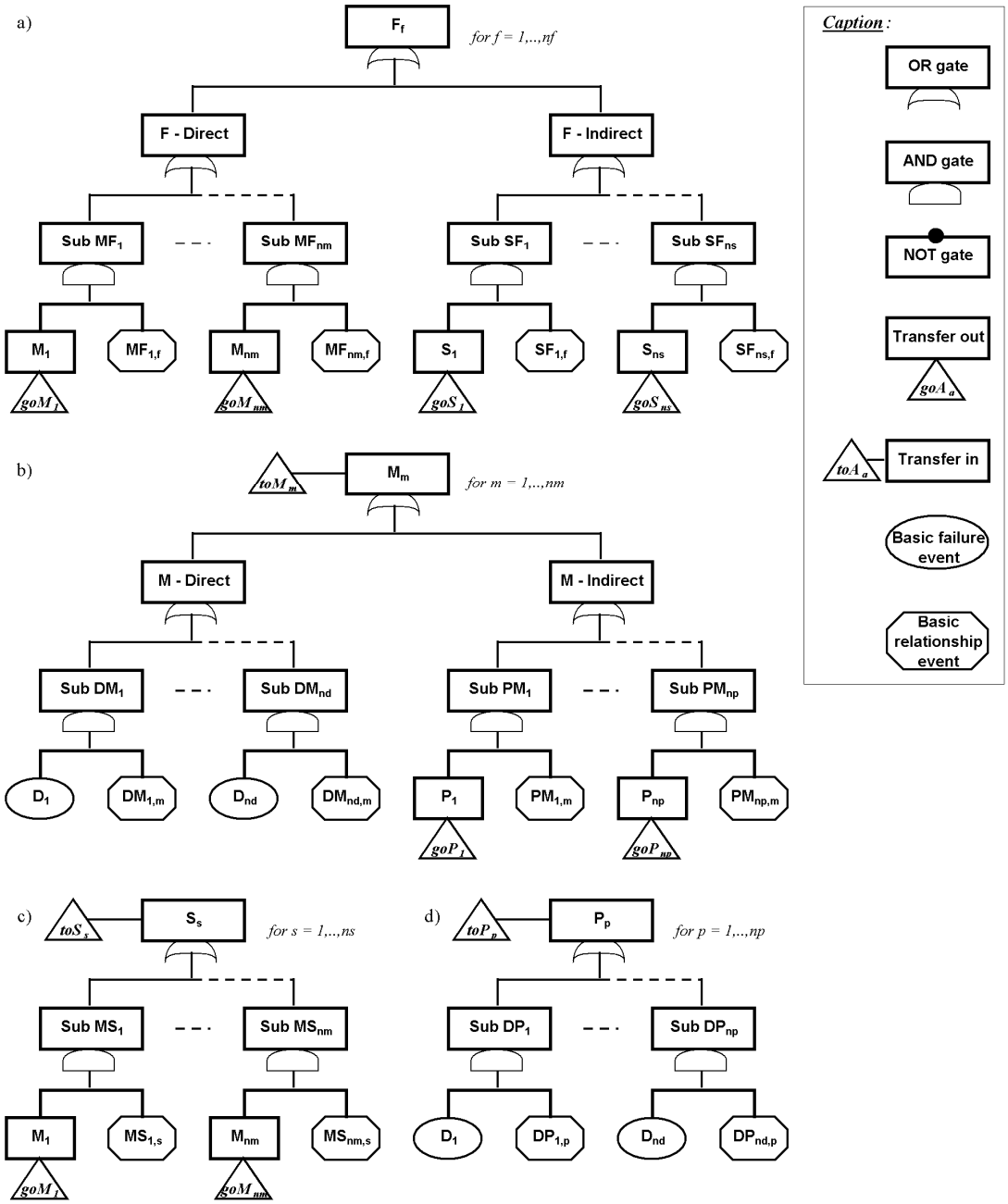

Figure 2. Equivalent fault trees for "3-Step model"

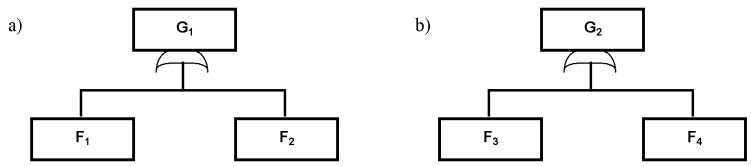

Figure 3. Fault trees for global functions

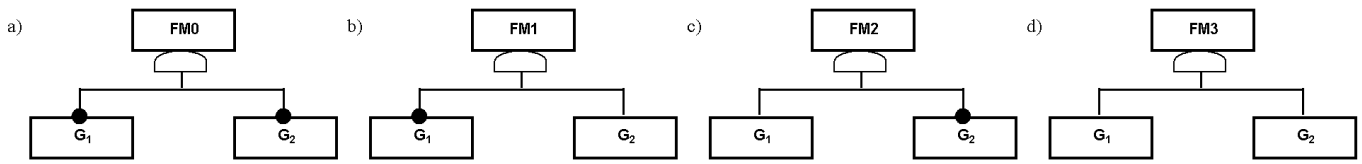

Figure 4. Fault trees for failure modes

4. Probabilities of malfunction and failure modes

4.1. Hypotheses and input data

To assess probabilities of functions being in a failed state (i.e. malfunctions), the following assumptions are made:

- Direct relationship events (i.e. events given in matrices *DP*, *DM*, *PM*, *MS*, *MF*, and *SF*) are independent (see Section 3.2.1), and corresponding probabilities are constant according to time.
- Fault or failure occurrences (events D_d) are independent and function to time.
- No maintenance action is performed during the study time.

The probability of fault or failure *d* occurrence at time *t* can therefore be denoted $P[D_d \leq t]$. Corresponding expressions are given in Table III and take into account the "inner architecture" of material elements (not depicted in Figure 1, according to the level of system break-up).

4.2. Fault tree based approach

Probabilities of malfunction can then be assessed by equivalent fault trees given in Figure 2 and Figure 3. Input probabilities from Table I (second column) are used for probabilities of occurrences of "basic relationship events". Expressions from Table III are used for probabilities of occurrences of "basic failure events". Probabilities of global function being in a failed state are reported in Figure 5.

Failure modes can be defined according to combinations of global function states. These failure modes are described in Table IV and corresponding fault trees are given in Figure 4. For example, if the gas transmitter is able to transmit a good measurement but not a correct diagnosis, the corresponding failure mode is denoted *FM1*. The reverse failure mode of *FM1* is denoted *FM2*. *FM3* corresponds to the situation where neither *measure* nor *diagnose* are functioning, and *FM0* when both are functioning. This last one is therefore not literally a "failure mode". The probabilities of failure modes *FM1*, *FM2*, *FM3* and not-*FM0*, denoted ^*FM0*, are reported in Figure 6.

4.3. Min-max interval based on relationship analysis

A min-max interval for probabilities of global function being in a failed state is given by (19). The upper bound is deduced from (16), and the lower bound from (18) by neglecting the occurrence of more than one fault or failure (events D_d). These results can be transposed to probabilities of main functions being in failed state (events F_f).

$$\sum_d \left(P\left[DG_{d,g}\right] \cdot P\left[D_g \leq t\right] \cdot \prod_{\delta \neq d} \left(1 - P\left[D_\delta \leq t\right]\right) \right) \leq P\left[G_g \leq t\right] \leq \sum_d \left(P\left[DG_{d,g}\right] \cdot P\left[D_g \leq t\right] \right) \quad (19)$$

These bounds are reported in Figure 5. Notice that the lower the probabilities of fault or failure occurrence, (e.g. time *t* is low), the narrower the interval is.

Table III. Probabilities of fault or failure at time *t*

Fault or failure *d*	Probability of fault or failure *d* at time *t* i.e. $P[D_d \leq t]$
1	$1 - \exp(-5 \cdot 10^{-8} \cdot t)$
2	$1 - \exp(-5 \cdot 10^{-8} \cdot t)$
3	$1 - \exp(-4 \cdot 10^{-7} \cdot t)$
4	$1 - \exp(-4 \cdot 10^{-7} \cdot t)$
5	$1 - \exp(-1 \cdot 10^{-7} \cdot t)$
6	$1 - 3 \cdot \exp(-6 \cdot 10^{-6} \cdot t) + 2 \cdot \exp(-9 \cdot 10^{-6} \cdot t)$
7	$1 - \exp(-3 \cdot 10^{-6} \cdot t)$
8	$1 - 2 \cdot \exp(-5 \cdot 10^{-7} \cdot t) + \exp(-1 \cdot 10^{-6} \cdot t)$
9	$1 - \exp(-2 \cdot 10^{-7} \cdot t)$

Table IV. Definition of failure modes

Failure mode	State of global function *measure*	State of global function *diagnose*
FM0	functioning (event ^*G1*)	functioning (event ^*G2*)
FM1	functioning (event ^*G1*)	malfunctioning (event *G2*)
FM2	malfunctioning (event *G1*)	functioning (event ^*G2*)
FM3	malfunctioning (event *G1*)	malfunctioning (event *G2*)

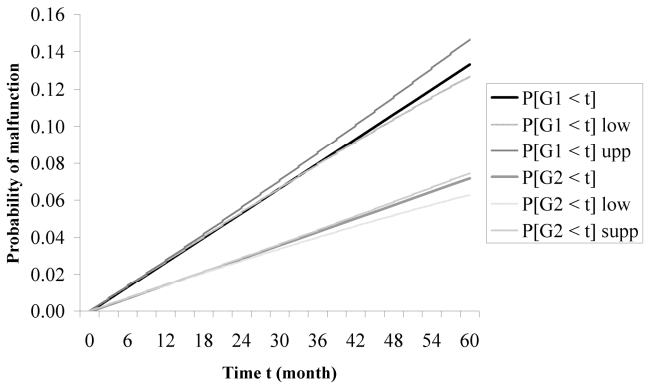

Figure 5. Probabilities of malfunction

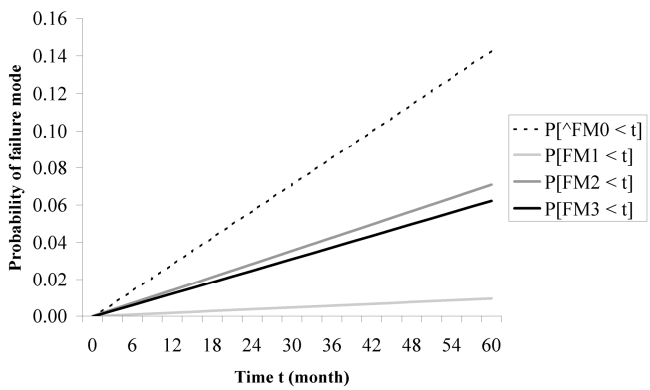

Figure 6. Probabilities of failure modes

5. Relationship uncertainty analysis

5.1. Uncertainty issues

Input data uncertainty is a substantial issue for reliability evaluation and has been widely investigated in many references: using several data sources [15], propagation of error, Monte Carlo simulations, Bayesian methods [16], fuzzy set theory [17], and other approaches as evidence, possibility, and interval analyses [18]. These uncertainty analyses can be basically applied to input probabilities of fault or failure occurrences given in Table III, for example by using fault trees in Figure 2 (analyses are performed on "basic failure events"). The rest of the present paper will therefore not deal with this kind of uncertainty.

However, stochastic relationships are likely to be one of the main concerns of the proposed model. In fact, it is probably quite difficult to assess the direct relationship value between two elements and, in many cases, expert judgments are required. In the present paper, uncertainty analysis will therefore focus on relationships, that is, the uncertainties of stochastic relationship values (i.e. probabilities $P[DP_{d,p}]$, $P[DM_{d,m}]$, $P[PM_{p,m}]$, $P[MS_{m,s}]$, $P[MF_{m,f}]$, and $P[SF_{s,f}]$) on total relationship values between faults or failures and global functions (i.e. probabilities $P[DG_{d,g}]$). For example, to deal with uncertainties in GTST-MLD models, fuzzy logic has been used in [15]. In the following, a probabilistic approach (i.e. using probability density functions) is chosen. The aim is to be able to assess variances of total relationship results, and to compare them with variances of input data.

5.2. Probabilistic approach for relationship uncertainties

Stochastic relationship values are now random variables, that is, probability values are described by probability distributions. Such "distributed probabilities" will be denoted in bold (i.e. $\boldsymbol{P[AB_{a,b}]}$) to distinguish them from "fixed probabilities" used in previous sections.

According to the direct relationship events $AB_{a,b}$ given in matrices *DP*, *DM*, *PM*, *MS*, *MF*, and *SF*, four probability laws, denoted Λ_h, Λ_m, Λ_h, and Λ_n, are proposed by expert judgments to describe random variables $\boldsymbol{P[AB_{a,b}]}$:

- if $AB_{a,b}$ represents a high relationship,
  then $\boldsymbol{P[AB_{a,b}]} \sim \Lambda_h$ (e.g. $\boldsymbol{P[MF_{5,2}]} \sim \Lambda_h$)
- if $AB_{a,b}$ represents a medium relationship,
  then $\boldsymbol{P[AB_{a,b}]} \sim \Lambda_m$ (e.g. $\boldsymbol{P[SF_{1,2}]} \sim \Lambda_m$)
- if $AB_{a,b}$ represents a low relationship,
  then $\boldsymbol{P[AB_{a,b}]} \sim \Lambda_l$ (e.g. $\boldsymbol{P[MS_{2,1}]} \sim \Lambda_l$)
- if $AB_{a,b}$ represents a very low relationship,
  then $\boldsymbol{P[AB_{a,b}]} \sim \Lambda_n$ (e.g. $\boldsymbol{P[MF_{1,2}]} \sim \Lambda_n$)

The corresponding probability density functions (pdf) are depicted in Figure 7. Expectancies and variances are reported in Table V. Random variable notations of Figure 7 are given in Table V (second column). Notice that the more the relationship is set as an extreme value (very low or high), the lower the uncertainty (i.e. variance) is assumed to be.

Expectancies and variances of $\boldsymbol{P[DG_{d,g}]}$ are obtained by Monte Carlo simulations, using (18) and 10,000 draws for each fault or failure *d*. Results are given in Table VI. Expectancies differ from Section 3.3 (see Table II), because expectancies of relationship values given in Table V are not equal to input probabilities given in Table I.

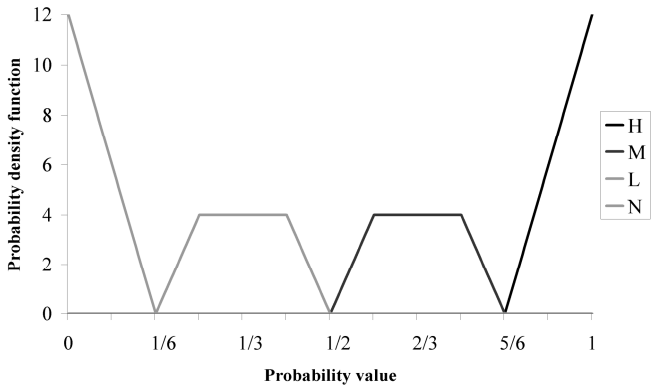

Figure 7. Probability density functions of random variables **H**, **M**, **L**, and **N** given in Table V

Table V. Probability laws for distributed probabilities

Relation-ship	Random variable	Expec-tancy	Variance
high	$\mathbf{H} \sim \Lambda_h$	0.94	$1.5 \cdot 10^{-3}$
medium	$\mathbf{M} \sim \Lambda_m$	0.67	$5.8 \cdot 10^{-3}$
low	$\mathbf{L} \sim \Lambda_l$	0.33	$5.8 \cdot 10^{-3}$
very low	$\mathbf{N} \sim \Lambda_n$	0.06	$1.5 \cdot 10^{-3}$

Table VI. Relationship uncertainty analysis results

Fault or failure *d*	Impact on *measure* i.e. $\boldsymbol{P[DG_{d,1}]}$		Impact on *diagnose* i.e. $\boldsymbol{P[DG_{d,2}]}$	
	Expec-tancy*	Variance	Expec-tancy*	Variance
1	0.99	$6.6 \cdot 10^{-5}$	0.93	$5.7 \cdot 10^{-4}$
2	1.00	$4.4 \cdot 10^{-7}$	1.00	$9.8 \cdot 10^{-6}$
3	0.97	$2.3 \cdot 10^{-4}$	0.83	$2.1 \cdot 10^{-3}$
4	0.85	$2.1 \cdot 10^{-3}$	0.80	$2.9 \cdot 10^{-3}$
5	0.99	$3.5 \cdot 10^{-5}$	0.94	$4.8 \cdot 10^{-4}$
6	0.74	$5.0 \cdot 10^{-3}$	0.54	$7.8 \cdot 10^{-3}$
7	0.81	$3.0 \cdot 10^{-3}$	0.58	$6.7 \cdot 10^{-3}$
8	0.92	$8.6 \cdot 10^{-4}$	0.84	$2.1 \cdot 10^{-3}$
9	1.00	$1.2 \cdot 10^{-6}$	1.00	$1.1 \cdot 10^{-5}$

*Notice that the expectancies are corrected to 2 decimal places. A relationship can therefore have a rounding off expectancy of 1.00, and even so a non-zero variance.

5.3. Discussion

The variances obtained for total relationship results, which are reported in Table VI, are at least in the same order as variances of input data from Table V and, in many cases, orders of lower magnitude, especially for extreme values (i.e. close to *1*). This property tends to show that the proposed model is robust. In fact, even if input data are quite uncertain, results can be obtained relatively precisely and, in some cases, even more precisely than inputs.

To demonstrate this property in a general way is quite difficult due to many dependencies between events which are used to calculate total relationship results. However, to give part of explanation, two basic operations on random variables, required by (18), can be analyzed.

Let **X** and **Y** be two independent random variables which describe probability values (i.e. the sample space is *[0, 1]*), and with respective pdf $f_X(x)$ and $f_Y(y)$, thus:

$$\int_0^1 f_X(x) \cdot dx = 1 \text{ and } f_X(x) \geq 0 \text{ for } 0 \leq x \leq 1 \quad (20)$$

$$\int_0^1 f_Y(y) \cdot dy = 1 \text{ and } f_Y(y) \geq 0 \text{ for } 0 \leq y \leq 1 \quad (21)$$

It is therefore possible to define the pdf of resulting random variables of operations **X**·**Y** and 1-(1-**X**)·(1-**Y**):

$$f_{X \cdot Y}(z) = \int_0^1 f_X(u) \cdot f_Y\left(\frac{z}{u}\right) \cdot \frac{1}{u} \cdot du \quad (22)$$

$$f_{1-(1-X)\cdot(1-Y)}(z) = \int_0^1 f_X(u) \cdot f_Y\left(\frac{u-z}{u-1}\right) \cdot \frac{1}{1-u} \cdot du \quad (23)$$

In addition, the following properties can be established:

$$E[X \cdot Y] = E[X] \cdot E[Y] \quad (24)$$

$$V[X \cdot Y] = V[X] \cdot E^2[Y] + V[Y] \cdot E^2[X] + V[X] \cdot V[Y] \quad (25)$$

$$E[1-(1-X)\cdot(1-Y)] = 1-(1-E[X])\cdot(1-E[Y]) \quad (26)$$

$$V[1-(1-X)\cdot(1-Y)] = V[X]\cdot(1-E[Y])^2 + V[Y]\cdot(1-E[X])^2 + V[X]\cdot V[Y] \quad (27)$$

Examples of such operations on random variables **M**, **L**, and **N** (see Figure 7 and Table V) are depicted in Figure 8. Expectancies and variances are given in Table VII. Finally, (28) can be deduced from (25), and (29) from (27):

$$V[X \cdot Y] \leq \min\{V[X], V[Y]\} \Leftrightarrow \frac{E^2[X]}{V[X]} + \frac{E^2[Y]}{V[Y]} \leq \frac{1}{\max\{V[X], V[Y]\}} - 1 \quad (28)$$

$$V[1-(1-X)\cdot(1-Y)] \leq \min\{V[X], V[Y]\} \Leftrightarrow \frac{(1-E[X])^2}{V[X]} + \frac{(1-E[Y])^2}{V[Y]} \leq \frac{1}{\max\{V[X], V[Y]\}} \quad (29)$$

Equations (28) and (29) show the necessary and sufficient conditions on two input distributed probabilities to the operation results to obtain lower variances than any of the inputs. In other words, the result is less uncertain than any of its input data. These conditions are, for example, fulfilled by the couple of random variables **L** and **M**, but only (28) is fulfilled by the couple of random variables **N** and **M**, as it is shown by Figure 8 and results reported in Table VII.

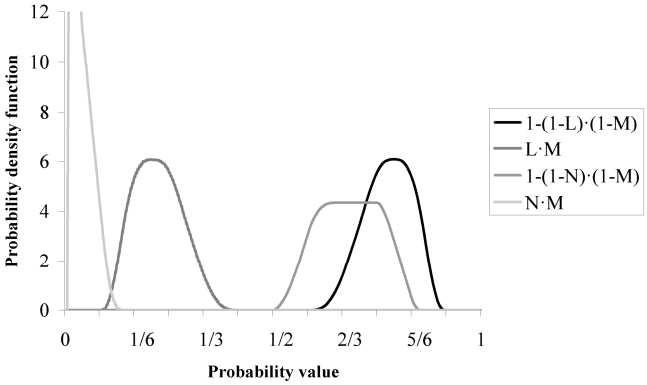

Figure 8. Probability density functions of random variable operations 1-(1-**L**)·(1-**M**), **L**·**M**, 1-(1-**N**)·(1-**M**), and **N**·**M**

Table VII. Properties of random variable operations

Random variable	Expectancy	Variance
1-(1-**L**)·(1-**M**)	0.78	$3.3 \cdot 10^{-3}$
L·**M**	0.22	$3.3 \cdot 10^{-3}$
1-(1-**N**)·(1-**M**)	0.69	$5.4 \cdot 10^{-3}$
N·**M**	0.04	$7.2 \cdot 10^{-4}$

6. Some design issues

Importance criteria for material elements may be defined with a more global approach by using the model which is proposed in this paper. In fact, several functions are included in the analyses. It is then suitable to assess the component importance according to its impact on failure modes. For example, depending on the application, a bad measurement but a good diagnosis, or the opposite, are not equally critical, especially from a safety point of view. Moreover, these analyses can be performed by classic software tools, using equivalent fault trees.

System monitoring should take into account the "fault or failure coverage" of each function. For example, the previous analyses have shown that the loss of diagnose alone is less likely than any of the other failure modes (see Figure 6). If a checking procedure is required in order to improve system monitoring, the measure should preferably be tested because if it is functioning, a wider part of potential faults and failures is not supposed to have occurred.

The impact of "intelligent" functionalities on system reliability can be assessed. For the given example, the relevance of gas transmitter self-adjustment to reliability may be compared to other options, as for example: no self-adjustment but higher probabilities of failures of infrared units (i.e. $P[D_d \leq t]$ for $d = 1, 2, 3$, see Table III).

Several kinds of transmitted data (e.g. measurement, diagnoses) may be required by control system decision rules. Optimization of these rules could take into account the system failure mode probabilities e.g. a good measurement but a bad diagnosis is less likely than the opposite for the gas transmitter example.

7. Conclusion

This paper proposes a reliability analysis using a "3-Step model", based on Goal Tree–Success Tree (GTST) techniques, combined with Master Logic Diagrams (MLD). This approach aims to take into account both material and functional aspects in the analyses, including various interactions. The third part of the model contains a list of faults and failures representing the dysfunctional aspects.

Probabilities are chosen to model the relationships given in MLD. Quantitative analyses are then performed for an infrared gas transmitter example. First, relationship analyses aim to evaluate the impact of any fault or failure on any system function. These results and input probabilities for fault and failure occurrences then enable probabilities of malfunction and failure modes to be evaluated, according to time. Uncertainty analyses show the robustness of the model. Even faced with quite uncertain input data, results can be assessed with at least the same degrees of confidence, and, in some cases, even more precisely. Finally, some design aspects should take many advantages from this model.

As a general rule, this approach should be suitable for any reliability evaluations of systems which present at least one of these complexities: at the system level if many interactions exist between components but also between functions; at the components level if some consequences of faults or failures are difficult to predict. In addition, several system output data can be taken into account according to function fulfillments. The proposed model is therefore especially appropriate for intelligent transmitter reliability analyses. Further work will focus on the reliability of control systems using various data from several transmitters to optimize their performances.

8. References

[1] J. E. Brignell, "The future of intelligent sensors: A problem of technology or ethics?" Sensors And Actuators A-Physical, vol. 56, pp. 11-15, 1996.

[2] International Electrotechnical Commission, IEC 60770-3 Transmitters for use in industrial-process control systems, Part 3, IEC Standard, Geneva, 2006.

[3] F. Brissaud, D. Charpentier, A. Barros, and C. Bérenguer, "Intelligent Sensors: New Technologies and New Dependability issues." in Proc. 16e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Avignon, 2008.

[4] G. C. M. Meijer, "Concepts and focus point for intelligent sensor systems," Sensors And Actuators A-Physical, vol. 41, pp. 183-191, 1994.

[5] A. H. Taner and J. E. Brignell, "Aspects of intelligent sensor reconfiguration," Sensors And Actuators A-Physical. vol. 47, pp. 525-529, 1995.

[6] M. Staroswiecki, "Intelligent sensors: A functional view," IEEE Transactions On Industrial Informatics, vol. 1, pp. 238-249, 2005.

[7] F. Guenab, D. Theilliol, P. Weber, Y. M. Zhang,, and D. Sauter, "Fault tolerant control system design: a reconfiguration strategy based on reliability analysis under dynamic behaviour constraints." in Proc. 6th IFAC symposium on Safeprocess, Beijing, 2006.

[8] M. Bayart, B. Conrard, A. Chovin, and M. Robert, "Capteurs et actionneurs intelligents," Technique de l'Ingénieur, vol. S 7 520, 2005.

[9] CIAME, Livre Blanc, Les capteurs intelligents : Réflexion des utilisateurs. Paris: AFCET, 1987.

[10] G. Smith and M. Bowen, "Considerations for the utilization of smart sensors," Sensors And Actuators A-Physical, vol. 47, pp. 521-524, 1995.

[11] International Electrotechnical Commission, IEC 61508 Functional safety of electrical / electronic / programmable electronic safety-related systems, IEC Standard, Geneva, 2002.

[12] M. Modarres and S. W. Cheon, "Function-centered modeling of engineering systems using the goal tree-success tree technique and functional primitives," Reliability Engineering & System Safety, vol. 64, pp. 181-200, 1999.

[13] F. Brissaud, A. Barros, C. Bérenguer, and D. Charpentier, "Dependability Issues for Intelligent Transmitters and Reliability Pattern Proposal." in Proc. 13th IFAC Symposium on INCOM, Moscow, 2009.

[14] A. Jalashgar, "Identification of hidden failures in process control systems based on the HMG method," International Journal of Intelligent Systems, vol. 12, pp. 159-179, 1998.

[15] U. Hauptmanns, "The impact of reliability data on probabilistic safety calculations," Journal of Loss Prevention in the Process Industries, vol. 21, pp. 38-49, 2008.

[16] F. Guérin, "Reliability estimation by Bayesian method: definition of prior distribution using dependability study," Reliability Engineering & System Safety, vol. 82, pp. 299-306, 2003.

[17] H. Tanaka, L. T. Fan, F. S. Lai, and K. Toguchi, "Fault-tree analysis by fuzzy probability," IEEE trans. Reliability, vol. 32, pp. 453-457, 1983.

[18] J. C. Helton, J. D. Johnson, and W. L. Oberkampf, "An exploration of the alternative approaches to the representation of uncertainty in model predictions," Reliability Engineering & System Safety, vol. 85, pp. 39-71, 2008.

[19] Y. Hu and M. Modarres, "Evaluating system behavior through Dynamic Master Logic Diagram (DMLD) modeling," Reliability Engineering & System Safety, vol. 64, pp. 241-269, 1999.