MODELING AND DEPENDABILITY EVALUATION OF SAFETY SYSTEMS IN CONTROL AND MONITORING APPLICATIONS

J. Ariat and K. Kanoun
Laboratoire d'Automatique et d'Analyse des Systèmes du CNRS, 7, Avenue du Colonel Roche, 31077 Toulouse Cedex, France

ABSTRACT

The paper addresses the problem of dependability evaluation of high safety computer systems. Continuously activated control systems and incident-driven monitoring systems that are considered in the paper are characterized in the framework of a general analysis and classification of safety systems. The behavior of these two types of system is described by Section IV, a comprehensive unified model that is useful for (a) the definition of relevant dependability measures and (b) the identification of the main features of the modeling task. Based on this model a general evaluation methodology is presented and applied to the study of simplex and duplex structures of both control and monitoring safety systems. Special emphasis is put on the identification of the tradeoff between the safety and availability aspects.

Keywords: safety systems, dependability, modeling, evaluation, Markov process.

INTRODUCTION

Safety systems considered in this paper are computer systems associated with critical applications whose failure may have catastrophic consequences due to human and/or economical reasons. Accordingly, during the design of such systems special emphasis is put on dependability evaluation and validation.

Although this problem of dependability validation covers a wide range of problems and approaches (LAF 85), we focus our presentation on the modeling and evaluation aspects only.

The paper extends and generalizes the work of two previous studies (LAF 80, LAF 85) which concern:
- the definition of a new architecture for the monitoring system of an Extra High Voltage substation for the French electrical network. The overall results obtained constitute a database for the design of a new system (MED 80);
- the design and validation of a computerized interlocking system for the French railroad (ARE 86).

Section I provides a comprehensive framework for the analysis of safety systems and characterizes the types of safety systems that are considered in the paper: namely, control and monitoring systems. In section II a general model of the behavior of these systems is presented which allows the derivation of relevant dependability measures suitable for their evaluation. Guidelines for the applied methodology of evaluation are also presented and discussed in section III. Section IV is devoted to the dependability evaluation of simplex and duplex safety systems.

I - ANALYSIS OF SAFETY SYSTEMS

A general representation of the types of safety systems studied in this paper is given in figure 1 which details the interactions between the different elements and the terminology used throughout the paper.

Figure 1

Let us now introduce and discuss here two aspects that we feel important in the study of safety systems; they are related to:
- the response time of the process to an erroneous output from the safety system,
- the ability of the process to exhibit two failure modes: a benign mode, where the system is brought into a prescribed safe state, and a catastrophic mode.

A. Process Response Time

Depending on the reaction time of the process to an erroneous order, (i.e. the latency of a process failure before it leads to a catastrophic failure at the end user level) different graded approaches are applicable to ensure safe behavior.

1) Response Time = 0 : the process reacts quickly and leads directly to a catastrophic failure; the safety mechanisms thus have to be included in the safety system in order to reduce (or avoid) any erroneous output to the process.

2) Response Time > 0 : the reaction of the process is not immediate and the deviation of the process is gradual; this latency time allows the application of appropriate safety actions in order to avoid catastrophic failure.

B. Presence of two failure modes

The ability of the process to exhibit two failure modes: a benign mode and a catastrophic mode, depends strongly on the type of application considered. From the functional point of view, this ability depends on (1) the possibility of the system to degrade the quality of service, (2) the existence of a stable safe state.

In the benign failure mode, the functional mission cannot be fully accomplished but safety constraints are preserved; e.g. process activity is frozen for a certain time or the process is put into a safe shut-down state.
C. Safety Systems Classification

According to the previously introduced aspects, safety systems can be classified in four groups as shown in Figure 2. In order to be more specific, we will give typical examples of applications with high safety requirements for each group of Figure 2.

<table>
<thead>
<tr>
<th>RESPONSE TIME</th>
<th>DESIGN FAILURE MODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>GROUP 1</td>
</tr>
<tr>
<td># 0</td>
<td>GROUP 2</td>
</tr>
<tr>
<td># 0</td>
<td>GROUP 3</td>
</tr>
<tr>
<td># 0</td>
<td>GROUP 4</td>
</tr>
</tbody>
</table>

**Figure 2**

Ground transportation (e.g. railroad traffic control) is an illustration of the types of processes in systems that have a nominal condition that cannot be tolerated in the case of dense traffic. However, in cases of failure of the control system, it is usually assumed that it is possible to stop the traffic. If this assumption is still valid in most of the practical cases, it has to be tempered by the fact that the capability of providing a service is less and less likely as traffic becomes denser; this is already the case in subway systems.

Most safety systems devoted to industrial processes (chemical processes, nuclear power plants...) may be found in group 2. A characteristic example is that of electrical power distribution systems. In this case, most emphasis on the protection is put on the monitoring of the network electrical parameters and although it is economically undesirable, partial deconnection of the network provides a possible stable shutdown state.

Groups 3 and 4 can be characterized by aeronautical applications related to new-generation aircraft with reduced stability margins where the safety of the flight will depend upon active controls derived from computer outputs; it follows that no safe shutdown state is possible in this case. Group 3 corresponds to critical phases of the mission: take-off and landing where no erroneous command can be tolerated. Examples of control systems belonging to these groups are described in (Hop 76, Wem 74).

For systems belonging to groups 1 and 2, the classical reliability measure is applicable. However, for systems of groups 1 and 2, one should note that the presence of a benign failure mode is, most of the time, associated with the property of maintainability of the safety system.

The type of maintainability considered here is the maintenance (or operator) actions that are applied during the mission either (1) on-line, for the redundant part of the system or (2) off-line, when the process has been end in the benign failure mode. However, no maintenance actions are considered when the process is in the catastrophic failure mode. We will be interested essentially in the impact of the application of off-line maintenance actions in the derivation of relevant measures.

We do not explicitly consider here a specific classification with respect to maintainability since the impact on the maintainability measures is closely related to the presence of a benign failure state; it has, however, to be noted that among all application domains that are considered, all are maintainable after a benign interruption except aeronautics.

We concentrate our presentation on the evaluation of the large proportion of safety systems of groups 1 and 2 of figure 2 referenced as control and monitoring systems respectively.

II - DEPENDABILITY MEASURES

A. General Behavior of Safety Systems

The evaluation is essentially devoted to rate the safety system dependability either a control system or a monitoring system. Figure 3 presents a general model of the system for such systems.

Three major state classes may be identified which correspond to:
- accomplishment (A): the safety system accomplishes its task in conformity with its specifications,
- benign interruption (B), following a benign failure of the safety system; it is assumed that, as a consequence, the process is halted,
- catastrophic interruption (C), following a catastrophic failure; although this position constitutes a pessimistic point of view, a catastrophic failure of the process will be assumed whenever the safety system considered exhibits a catastrophic interruption, i.e. it provides erroneous (or no) command to the process.

**Figure 3**

This high level partition is in conformity with the one presented in (Amb 85) which addressed essentially control systems that are continuously exercised. Interestingly, the representation of the process was not explicitly considered, and emphasis was mainly put on the modeling of the ability of the system to successfully handle solicitations corresponding to error activation at the system level.

We introduce here a further refinement of class A into three sub-classes in order to (1) specify the main features of the modeling task when dealing with specific systems and (2) show how this partition applies to monitoring systems that are essentially exercised in response to external solicitations corresponding to the occurrence of incidents in the monitored process.

1) Accomplishment Class

Sub-class A' characterizes the cases when the system is up and able to perform its task: it is either error-free or the latent errors accumulated in it will not hamper correct processing of a subsequent solicitation.

For control systems, solicitations correspond to the activation of an error in the system. This event covers two main types of activations:
- internal activations, with respect to the imbedded error processing mechanisms,
- external activations, with respect to the commands sent to the system.

The underlying stochastic processes model the elapsed times (latencies) between the creation of a latent error and its activation at the considered level; it has to be noted that these processes are inoperative when the system is error-free. These activations will only provoke a transition to the benign interruption class B when the provided redundancy is
no longer sufficient to bring these errors back into a latent state on an on-line basis.

For monitoring systems, one also has to explicitly consider external solicitations induced by incidents in the process. Two types of incidents must be considered:
- TI incidents: actions carried out by the monitoring system are enough in order to restore the normal working conditions of the monitored process,
- TV incidents: the monitored process is shut down and manual maintenance intervention is necessary.

It will be assumed that TV incidents will lead to an interruption of service of the monitoring system. Although it is down, the monitoring system is still able to accomplish its task; once, this case has been distinguished from a service interruption due to the inability of the monitoring system to perform its task. In order to stress this difference we consider that this case is part of the accomplishment class A: it corresponds to sub-class A*.

Sub-class A* gathers all potentially dangerous states; it corresponds to the cases when, due to the accumulation with specific patterns of latent errors (at system level), the safety system has been significantly degraded and is no longer able to perform its assigned task; when actually solicited (external activation or solicitation), the system enters the catastrophic interruption class. However, a benign failure induced, for example, by further accumulation of errors that will trigger the imbedded error processing mechanisms and/or preventive maintenance actions may still occur and provoke a transition from class A* to the benign interruption class B.

In practice, for the user, the distinction between A* and A is impossible and then, the discrimination between them is strongly dependent on the error hypotheses that underlie the level of redundancy provided for the system and the design of its error processing mechanisms.

Sub-class A** is empty in the case of control systems since the notion of external solicitation is implicitly precluded. The only transitions from class A** are to class A following the maintenance of the monitored system and the restart of the system.

2) Benign Interruption Class
Although the benign interruption class B may gather a large number of states that are induced by the difference in the types of (off-line) restoration actions that have to be performed in each case, we do not further decompose this class here. However, it is important to note that, depending on the quality of the restoration, the system may be brought back either into class A* or A*.

3) Catastrophic Interruption Class
Equally, we do not further decompose the notion of catastrophic interruption, although, in practice, this notion covers a large spectrum of failure behaviors due to the fact that a catastrophic failure may (1) result from various types of problems, and (2) propagate.

Also, no system restoration is considered following a catastrophic interruption; this results from the fact that the consequences of a catastrophic failure are such that system restoration is much less important than the repair of the consequences (damage to property, law suits, etc.) and the analysis of the causes (board of inquiry, etc.).

B. Definition of the Measures (SP 85)
The model in figure 3 allows us to define the considered measures. Let n(t) be the state function of the system defined over the set of state classes (A, B, B*). In what follows, it will be assumed that n(t) V € A* and more specifically that the system is initially error free.

The main quantity of interest when dealing with safety systems is the time spent in the safe states before a catastrophic interruption. Let NST (Mean Safe Time) denote the mean time spent in the safe class B + A B, and B(t) the safety function, i.e. the probability of avoiding catastrophic interruption, they are defined by:

\[ S(t) = \text{Prob}( x(t) \in (A \cup B) , \text{for all } x \in (0, t)) \]

\[ \text{NST} = \int_0^t S(t) \, dt \]

However the very existence of a safety system has a counterpart: it can fail (benign failures) and thus lead to the loss of service. In order to measure the influence of the safety system on the service delivered to the process we introduce another quantity of interest: the time during which the service is delivered to the process. Let NBT (Mean Benign Interruption Time) denote this mean time and B(t) the point benign interruption function defined as:

\[ B(t) = \text{Prob}( x(t) \in B, B(x) \in B, \text{for all } x \in (0, t)) \]

\[ \text{NBT} = \int_0^t B(t) \, dt \]

An average unavailability-like measure can thus be defined that ratios the rate of time spent in state-class A with respect to the time spent in the safe classes B, before a catastrophic failure. This measure is called, the unavailability before catastrophic failure (UAC) and is defined as:

\[ \text{UAC} = \frac{\text{NBT}}{\text{NST}} \]

Comments about the definition of B(t)
Although states in sub-class A* are potentially dangerous, they are considered as safe states; the safety function as defined here is thus different from the classical one for which potentially dangerous states are not safe. This function is also different from the classical reliability measures for which states in class B are excluded from B.

Tradeoff: It is worth noting that when the system is in class B it is safe and it cannot enter the catastrophic state C, so increasing the benign interruption time will improve the time to catastrophic interruption; we see thus the tradeoff between the two measures considered.

Both points, Safety (S(t)) and unavailability before catastrophic failure (UAC) will be used as complementary evaluation measures for the safety systems under consideration.

III - EVALUATION METHODOLOGY
The main goal of evaluation is to provide objective aids in comparing the merits of various structures of a safety system during the design phase. This comparison is based on the measures defined in the previous paragraph. One tough task is to obtain a model of system behavior that (1) adequately embodies the most significant features of the system and (2) is sufficiently tractable to allow intensive sensitivity analysis of its parameters when comparing different structures.

A. Construction of the Model
In the attempt to derive a tractable yet representative model, the major difficulties are related to:
(1) the choice of the distribution functions of the random variables considered in the model,
(2) the number of accumulated latent errors in sub-class A* that have to be accounted for,
(3) the identification of the most significant variables among those considered in the model.

Two extreme approaches, involving intensive studies based jointly on theoretical results and...
numerical analysis of the models with respect to the considered measures can be used in order to validate the model:
- **Start-small:** formulation of simplifying hypotheses leading to a "basic" model which is a posteriori validated by a study of the impact of their relaxation ("extended" model).
- **Start-big:** thorough description of system behavior is considered in a "complete" model that is a posteriori simplified ("simplified" model).

The start-small approach is in particular used to address the problem of the non-exponentially distributed variables: all variables are first assumed to be exponentially distributed; serial and parallel extension of the states (COB 68) to which apply the non-exponentially distributed variable(s) is explicitly worked out. Based on previous research (LAP 73), in both cases one supplementary state is sufficient to reveal the impact of the modification of the distribution.

As a consequence, the dependability measures considered here can be obtained using time homogeneous Markov processes. This is particularly useful since, in most of the cases, Markov transition graphs deduced from the general model of figure 2, are generally too complex to allow exact analytical expressions of $B(t)$ and $D(t)$ to be formulated; thus numerical solutions are of prime interest.

The start-small approach is also used to study the problem of the number of errors accumulated in sub-class $A'$: the number of accounted latent errors is a priori limited to a low value and its impact is studied either numerically, by progressively increasing the number of states of the model, or analytically using for example results concerning the maintainability property of Markov processes (e.g., see NOV 71, pp. 28-40).

The identification of the most significant variables corresponds essentially to a start-big approach: significant variables are defined on the basis of the impact induced, by the modification of the graphs and the values of the variables, on the evaluated measures. This may be obtained from a study based jointly on theoretical results on Markov processes and an intensive numerical analysis of the models. Two major theoretical results prevail in this study:

1. The strong connectivity of the graph that is induced by the maintainability of the considered systems allows identification of an equivalent catastrophic failure rate $q_{eq}$ which can be directly related to the safety $(S(t))$ and mean safe time $(MST)$ measures as (see P&K 80, pp. 167-170):

$$ q_{eq} = \left(\frac{N_{stat}}{B(t)}\right)^{-1} \quad S(t) \leq \exp(-q_{eq} t), \quad \text{i.e.} \quad S(t) \leq \exp\left(-\left[N_{stat}\right]^{-1} t\right) $$

Accordingly, $S(t)$ is entirely specified by the estimation of $q_{eq}$.

2. The difference in orders of magnitude of the considered processes (e.g., see LAP 76), for example, restoration of the safety system with respect to the fault process and incident processing or process maintenance with respect to the solicitation process, allows handing of further simplifications on the transition graphs and/or closed-form approximate representations of the dependability measures.

These simplified expressions help to identify the most significant parameters and thus reduce the transition graphs and can be validated by comparison with numerical results obtained from the SURF program (COB 81).

B. Parameters of the model

We define here the various parameters (processes and associated factors) that are considered.

As usually done, it will be assumed that the fault occurrence process is exponentially distributed. Let $g'$ denote the failure rate of a hypothetical unit without any error detection mechanism, provision of these mechanisms will increase the failure rate (due to the presence of extra material) by a multiplicative factor denoted $b$; the actual failure rate of one unit is thus $g = g' b$.

$d$ will denote the rate of activation of the error processing mechanism in the safety system (i.e., $1/d$ is the detection latency). A detection efficiency (coverage) $(COV 49, AHH 72)$ will be associated with this process. No priori information exists concerning the distribution of this process; however, if $d$ is significantly greater than $1$, the exponential assumption is valid (LAP 81).

Let $1/a$ be the mean expert latency time at the system level, i.e. the time elapsed before the activation by the process of a latent error in $A'$ or $A''$. We do not have any information concerning the corresponding latency rate. The impact of a non-exponential distribution has been studied using the start-small approach in (AHN 89) and it results that the use of an exponential distribution is sufficiently representative.

The mean restoration time is denoted $1/f$; some previous studies (APU 77, HEL 82, LAP 88) have shown the influence of imperfect repair, this has been accounted for by means of parameter $f$, the restoration efficiency.

For the monitoring systems, external solicitations correspond to accidental anomalies in the process and thus the exponential assumption for the interval between incident occurrence seems reasonable, this rate will be denoted $m$.

Incident processing time will be denoted $1/\nu$, $h$ represents the proportion of type 1 incidents and $v$ the maintenance rate of the process following a type 7 incident. When processing an incident, the environmental constraints can be (depending on the type of monitored system) much more severe than in the absence of incidents: this leads to the introduction of a failure rate increases factor $b$ during incident processing which can vary, according to HEDK standard, from $1$ to $30$.

Remark: If $x$ denotes an efficiency or a coverage factor, its complement $1-x$ will be noted $x$.

The order of magnitude of the different rates is given in figure 4.

<table>
<thead>
<tr>
<th>Rates</th>
<th>Label</th>
<th>Range</th>
<th>Typical Value ($10^x$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fault</td>
<td>$q'$</td>
<td>once fault every year</td>
<td>$10^{-4}$</td>
</tr>
<tr>
<td>Error activation</td>
<td>$a'$</td>
<td>$100 \leq a'/q' \leq 1000$</td>
<td>$10^{-2} \leq a'$</td>
</tr>
<tr>
<td>Error detection</td>
<td>$g'$</td>
<td>$10^{-4} \leq g'/a' \leq 1000$</td>
<td>$10^{-5} \leq g'/a'$</td>
</tr>
<tr>
<td>Restoration</td>
<td>$h'$</td>
<td>$100 \leq h'/g' \leq 1000$</td>
<td>$10^{-2} \leq h'/g'$</td>
</tr>
<tr>
<td>Incident occurrence</td>
<td>$m'$</td>
<td>$1 \leq m'/h' \leq 100$</td>
<td>$10^{-4} \leq m'/h'$</td>
</tr>
<tr>
<td>Incident processing</td>
<td>$\nu$</td>
<td>$g/h \geq 10$</td>
<td>$10^{-1} \leq g/h$</td>
</tr>
<tr>
<td>Process maintenance</td>
<td>$v$</td>
<td>$10^{-4} \leq v/h \leq 100000$</td>
<td>$10^{-5} \leq v/h$</td>
</tr>
</tbody>
</table>

Figure 4

IV. EVALUATION OF SIMPLEX AND DUPLEX SAFETY SYSTEMS

A. Simplex Safety Systems

1) The Detection Process

The detection process is characterized both by the error detection latency (rate $g$) and the associated efficiency ($p$). Transition graphs $a$ and $b$ of figure 5 respectively present the models for the control and
monitoring safety systems deduced from the general model of figure 3 when only one fault occurrence is accounted for in the system. This choice has been made in order to enhance the impact of the detection process; the relaxation of this assumption will be investigated in the next paragraph.

![Diagram](image)

**Figure 5**

Based on the procedure presented in section III, approximate closed-form expressions have been derived for the measures considered. The table of figure 6 gives the values of $\text{MIN}^{-1}$ and $\text{UAC}$.

<table>
<thead>
<tr>
<th>CONTROL SYSTEM</th>
<th>MONITORING SYSTEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\frac{1}{\text{MIN}}$</td>
<td>$\frac{a}{d}$ + $\frac{p}{d}$ + $\frac{r}{d}$ + $\frac{k}{d}$</td>
</tr>
<tr>
<td>UAC</td>
<td>$\frac{p}{d}$ - $\frac{q}{d}$</td>
</tr>
</tbody>
</table>

*Figure 6*

On top of accounting for the orders of magnitude of the parameters of the model (figure 4), the approximations given in figure 6 have been derived considering that:

- for a control system: $a/d \ll 1$,
- for a monitoring system: $a/d \ll 1$,

which correspond to fairly natural conditions for a safety system if one wants to minimize the risk of latent errors.

These results show that the relative value of $a$ and $d$ (resp. $s$ and $d$) which represent the rates of the error activation (resp. of the external solicitation) and of the detection process, has no impact on UAC under the above assumptions for both types of safety systems.

However, in the case of $\text{MIN}^{-1}$, it appears that the ratio $a/d$ (resp. $s/d$) acts at the same level as the complement of the efficiencies $p$ and $r$. Accordingly, the impact of the rate of the detection process would be negligible only when:

- for a control system: $a \ll p + r$,
- for a monitoring system: $a \ll p + r + k$.

Due to the respective orders of magnitude, the most difficult condition to fulfill is that of the control system case. This point is of prime importance with respect to the implementation of recovery and restoration strategies when redundancy is provided at the system level. These aspects will be investigated in paragraph B, by considering a duplex structure. Figure 7 shows the respective influence of $p$ and $a/d$, which confirms the opposite role of $d$ and $p$ on safety.

In the sequel, we will consider only systems for which these conditions are verified and thus, only the efficiency aspect of the detection process will be accounted for. Also, due to the respective orders of magnitude of $a$ and $(k, q)$, state $6$ in figure 5 can be deleted.

Accordingly, the model of the monitoring system of figure 5-b can be simplified as shown in figure 8-a.

![Diagram](image)

*Figure 8: Monitoring System*
For sake of conciseness, we do not show explicitly here the simplified model for the control system since, due to the fact that the error activation process is inoperant when the system is error free (state 1), this graph represents a subgraph of the monitoring system graph (Figure 8-a), where states 3 and 4 are deleted and rate $\alpha$ (incident occurrence) is changed to rate $\alpha$ (error activation).

2) Accumulation of faults in Sh-Diane $n^{th}$

When one assumes that $n$ faults may be accumulated, the associated model for the monitoring system is shown in Figure 8-b. The case $n=1$ is equivalent to the models of Figures 7-a and 7-b. The corresponding model for the control system is easily deduced as previously stated. The approximate values for the considered measures in the cases when $n=1$ and $n=2$ are given in the tables of Figure 9.

<table>
<thead>
<tr>
<th>$n=1$</th>
<th>$n=2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S(m)$</td>
<td>$S(m)$</td>
</tr>
<tr>
<td>$S(n=1)$</td>
<td>$S(n=2)$</td>
</tr>
</tbody>
</table>

**Figure 9**

Both $S(n)$ and $U(n)$ measures increase when $n$ is varied from 1 to 2. Different consequences may be identified according to the type of safety system considered:

- control system: due to the fact that $n = q$, the impact of $n$ is negligible and it is not necessary to consider $n=1$ in subsequent studies;
- monitoring system: in this case, the impact of $n$ is function of the relative values of $n$ and $q$.

- If $n < q$, it is sufficient to consider that $n=1$;
- if $n > q$ and $n$ is of the same order of magnitude, it is necessary to investigate further the case $n=2$.

Figure 10 shows the variation of the safety function $S(t)$ for the monitoring system when the number of faults accumulated is modified. It appears that:

- a significant variation is observed for the considered values of the parameter $n$ when $n$ is varied from 1 to 2,
- no variation is observed when considering $n=2$.

As a consequence, in what follows, modeling of the redundant structures will be carried out considering $n=1$, $n=2$ for a control system, and $n=2$ for a monitoring system.

The other major results that can be extracted from the approximate closed-form expressions of $S(t)$ concern:

- the prominent role of the efficiency of the detection process for both measures in all cases; (MSE) is proportional to $p$, while UAC is proportional to $p$; this quantifies the tradeoff already mentioned at the end of the paragraph B of section II,
- the fact that the impact of the restoration process on safety is restricted to its efficiency $\gamma$, rather than on its rate $\delta$.
- for the monitoring system, the impact of a fault occurring during incident processing is of influence only when the quantity $(x/s/g)$ is comparable to $\beta$ and $\gamma$.

All these points have been confirmed by numerical results obtained with the SEDF program (SED-09), however, due to the space limitation, they are not recalled in the paper.

**B. Duplex Safety Systems**

As a consequence of the discussion introduced in paragraph A.1 of this section, in the case of a duplex system, the provided redundancy will be used to improve the detection process (latency and efficiency) by comparing the results of the two units.

For the control system, in case of identified discrepancy, the system is preferably safe and, therefore, no on-line restoration will be carried out (detection latency may be of the same order of magnitude as the activation latency in the case of the simplex structure). Redundancy is provided only to improve the detection process.

On the contrary, for the monitoring system, redundancy is used to provide fault-tolerance. Emphasis will be put on the recovery strategy consisting of the degradation of the system in a simplex structure; thus, on-line restoration will be considered.

The introduction of the above different characteristics concerning the restoration strategy is due to the fact that, in practice, the control system is driven by isolated external solicitations. Based on these hypotheses, the models of the duplex structures considered for the control and monitoring systems are shown in Figures 11a and b respectively.

Two supplementary parameters have been added for each system. For the control system, $\alpha_1$ and $\alpha_2$ denote the efficiency of the comparison when respectively, only one or both units are faulty; as the system is continuously activated, failure of the comparison leads to the catastrophic interruption.
state. For the monitoring system, $\phi_0$ and $\phi_0$ denote the coverage factor (detection and recovery efficiencies), respectively, in the absence or presence of an incident; failure of these actions leads respectively to the benign and the catastrophic interruption states.

Figure 12 compares the approximate expressions that are obtained for both types of safety system in the case of the simplex and duplex structures. Results for the simplex structure are derived from figure 9 with $n=1$ for the control system and $n=2$ for the monitoring system.

The difference in the restoration strategies considered in each case is confirmed by the results obtained when considering the variation of the UAC measure between the simplex and duplex structures:

- For the control system (off-line restoration), we observe an increase essentially due to the increase of the fault occurrence rate of the system.

- For the monitoring system (on-line restoration of the redundant unit), as could be expected, UAC is proportional to $\phi_0$ and thus, significant improvement may result for realistic values of the coverage efficiency in absence of incidentes.

It has to be noted that the penalisation obtained for the control system can be viewed as a pessimistic limiting case ($\phi_0 = 0$) of the recovery efficiency.

On the other hand, no major difference is observed between the two types of systems with respect to the safety aspect. It appears that in both cases of duplex structures, the safety measure is strongly dependent on the efficiencies $\phi_1$ and $\phi_0$ respectively; however, it can be expected that safety would be significantly improved for usual values of these efficiencies when compared with the expressions obtained for the simplex structures.
Although the results shown in Figure 12 provide a practical comparison basis, it has been found that the derivation of valid approximate expressions for UAC is a difficult task when the connectivity and the size of the model increases and thus numerical evaluation is required to complement these results.

Moreover, it is worth noting that in practice the size and complexity of the computing units (and thus their associated fault occurrence rate) may vary within the structure of the system is changed. This point may be easily investigated by varying the ratio  \( b \) between the actual fault rate \( q \) and that of a hypothetical unit \( q' = a q + b q' \). As an example, Figure 13 shows the impact of this variation when computing \( B(s) \) for the duplex monitoring system. The values chosen for \( b \) reflect the fact that it is likely that the redundancy will be used to improve the detection process at the system level thus relaxing somewhat the constraints (speed and efficiency) imposed on the intra-unit detection process.

The above results have shown that uniform improvement of performance with respect to both means to last trained developed in the presence of increasing the level of redundancy at the system level; this result has been verified as well for a triplex structure (IAP 80). On the contrary, a tradeoff appears in the case of control systems with respect to safety and availability between simplex and duplex structures. A better solution would be in this case to use a bi-duplex structure, as considered in (AFL 95), in order to allow actual online restoration and thus decrease the benign interruption time.

**CONCLUSIONS**

This paper was devoted to the study of two categories of safety systems:
- control systems: continuously activated,
- monitoring systems: driven by external signals or to incidents in the process.

Besides this discrepancy they have a common characteristic in case of a failure in the safety system, the process can be put into a prescribed safe shut-down state.

Two dependability measures have been defined in order to rate both the safety aspects and the impact of the safety system on the service delivered to the process (benign interruption).

Similar but specific models have been derived for each category and a closed-form expression of the dependability measures has allowed the identification of the most sensitive processes for each.

Some results are common to control and monitoring systems:
- prominent importance of the detection mechanisms,
- in the restoration process, repair efficiency has to be emphasized more than repair duration, and some others are more specific:
  - for control systems: detection latency has to be reduced in order to enhance safety,
  - for monitoring systems:
    - two latent errors in the system have to be accounted for,
    - failure in the process is more likely to occur due to the absence of incidents than due to errors occurring during incident processing.

In view of these results we considered duplex structures where the redundancy is used, (1) as a means for detection in control systems, (2) for fault-tolerance in monitoring systems where on-line repair can be carried out.

Comparative evaluation of the dependability measures showed that the duplex structure constitutes a good tradeoff between safety and benign interruption time in the case of monitoring systems, and that for control systems this tradeoff is not achieved.

**ACKNOWLEDGEMENT**

The authors wish to thank Jean-Claude Laprie for his encouragement and inviting remarks during the gestation of this paper.

**REFERENCES**


