Dependability Modeling of Safety Systems,

Karama Kanoun, Jean-Claude Laprie

► To cite this version:

Karama Kanoun, Jean-Claude Laprie. Dependability Modeling of Safety Systems,. 10th International Symposium on Fault-Tolerant Computing, Oct 1980, Tokyo, Japan. hal-02016370

HAL Id: hal-02016370

<https://hal.science/hal-02016370>

Submitted on 12 Feb 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

DEPENDABILITY MODELING OF SAFETY SYSTEMS

J. C. Laprie, K. Medhaffer - Kanoun

LABORATOIRE d'AUTOMATIQUE et d'ANALYSE des SYSTEMES
du Centre National de la Recherche Scientifique
7, avenue du Colonel Roche - 31400 TOULOUSE - France

ABSTRACT

This paper presents the results of a study¹ devoted to safety systems aimed at preventing the consequences of an incident to propagate. The functions of a safety systems are stated in the first part. How to quantify the accomplishment of these functions is discussed in the second part where the dependability levels of a safety system are defined. The third part is devoted to a detailed study of dependability of simplex, non fault-tolerant, safety systems. This study is necessary due to the very nature of such systems and we emphasize the problem of the masked faults which are of particular importance here. The results of the third part are then applied to the study of fault-tolerant safety systems, in the fourth and fifth parts : a) classical architectures, duplex and majority voting, and b) an example of a distributed safety system with degraded modes of operation, the substations of the extra high voltage French electricity network.

INTRODUCTION

The growth of our industrial society is being accompanied by an increase in hazards, the most disquieting being those for which an incident may propagate and have very severe consequences at diverse levels : economics, environment, human lives. Everybody knows of recent and famous examples which were catastrophic or for which a catastrophe was just avoided (chemical as in Seveso, Italy ; electrical as in the New York and France blackouts ; nuclear as in Three Mile Island).

The increase in the complexity of the industrial processes requiring safety systems leads to an increase in the complexity of these systems themselves. This in turn leads to a realization of safety systems using computers which, due to the very nature of their assigned tasks, are generally fault-tolerant. Although safety systems gave rise from a general point of view to many papers and books^{2,3},

few papers have been published on the subject of fault-tolerance applied to safety systems^{4,5}. This paper is precisely aimed at the study of computer-implemented safety systems.

1. FUNCTIONS OF A SAFETY SYSTEM

A general representation of an industrial process is given in figure 1 which details the terminology which will be used throughout this paper. In the sequel, the term incident will be exclusively employed for abnormal behavior of the monitored system, which can be due to a malfunction of the control system, of the sensors or actuators, or of the process itself.

Figure 1- Conceptual view of an industrial system

When an incident occurs, the safety system must detect and process it. Processing of the incident requires two steps :

- confinement : prevent propagation of its consequences,
 - elimination : restore the normal working conditions.
- The way elimination is performed leads to a distinction between two types of incidents :
- transient incidents : actions carried out by the safety system are enough in order to restore the normal working conditions of the monitored system,
 - permanent incidents : the monitored system is shut down and human maintenance intervention is required.

The functions which are generally assigned to a safety system are :

- F1) When an incident occurs in the monitored system :
1. detect the incident,
 2. warn the operator of the presence and (possibly) the nature of the incident,
 3. take corrective actions in order to bring the monitored system back into its normal working conditions.
- F2) In the absence of incident in the monitored system : do not have any action which could lead the process into a dangerous state or shut it down.

The statement of these functions of a safety system allows us to infer two important features of such a system : it must be fail safe, and it is a dormant system. Let us explain the latter point. The inputs of the safety system are parameters of the monitored system whose arrival period is generally low (a few milliseconds). The outputs to the process are binary control signals (orders for opening a valve or a circuit-breaker,...) whose period is much higher (several months). Thus, some parts of the safety system can remain unactivated during a long period of time.

2. DEPENDABILITY LEVELS OF A SAFETY SYSTEM

Definition of dependability levels requires the definitions of accomplishment levels⁶ which may be stated in terms of either fulfilled tasks or classes of

consequences of the various fault sources (the latter is the dual of the former). For our purpose, we define two accomplishment levels referring to functions F1 and F2 :

- level 1 refers to F1 only : the safety system is able to eliminate correctly an incident,
- level 2 refers to F1 and F2 : the safety system is able to eliminate an incident and has no undesirable action on the monitored system in the absence of incidents.

These two levels may be seen as two extremes : avoiding the catastrophe irrespectively of what else may happen (level 1) or everything is going well (level 2).

In order to quantify these levels, let us examine the behavior of a safety system, which results from the combination of two alternating processes⁷.

- fault manifestation and maintenance of the safety system, which will be denoted hereafter by the capability alternation process,
- incidence occurrence, incident processing and maintenance of the monitored system, which will be denoted hereafter by the solicitation alternation process.

Combining both alternation processes leads to the model of Fig. 2, where :

- an inability is the consequence of a fault manifestation in the safety system, the first one in a non fault tolerant system, or after exhaustion of the protective resources in a fault tolerant system ; a declared inability refers to a fault detected by the fault detection mechanisms implemented in the safety system, or perceived by its action on the monitored system ; a masked inability refers to a fault which is neither detected nor perceived,
- it is assumed that when the monitored system is down, incident occurrence is meaningless and no fault can develop in the safety system (shutting down the monitored system leads to shut down of the safety system and vice-versa),
- states 6 and 7 are catastrophic since an incident can propagate ; transitions outgoing from this state are not considered (they may even never occur if the monitored system cannot be restored after a catastrophe).

Fig.2-Behavior model of a safety system

The accomplishment levels can be defined in terms of successful and unsuccessful states :

ACCOMPLISHMENT LEVELS	SUCCESSFUL STATES	UNSUCCESSFUL STATES
Level 1	1,2,3,4,5	6,7
Level 2	1,2,3	4,5,6,7

Classification of state 5 necessitates a comment : this state is a dangerous one in the sense that if an incident occurs, the monitored system will be brought into a catastrophic state and this fact is non observable until an incident occurs. However, as mentioned above, the two levels are to be seen as two extremes and that is why we consider it as successful for the first level and unsuccessful for the second level. The measures of dependability associated with each accomplishment level are "reliability - type" measures, i.e. the unsuccessful states will be absorbing states. Let us denote by $D_1(t)$ and $D_2(t)$ the level 1 and 2 dependability and by $P_i(t)$ the probability of the system being in state i . We thus have

$$D_1(t) = \sum_{i=1}^5 P_i(t) \quad D_2(t) = \sum_{i=1}^3 P_i(t),$$

the $P_i(t)$ being evaluated on the corresponding transition graphs.

REMARK : from their definition, the dependability levels are close to the usual notions of safety for "level 1" and reliability for level 2. We shall however keep the terms "level-1 and 2 dependabilities" in order not to be confusing, particularly concerning the interpretation of state 5 which could be misleading if we use the term "safety".

3. MODELING OF A SIMPLEX (NON FAULT-TOLERANT) STRUCTURE

3.1. Evaluation method

We shall assume that all the random variables associated with the processes acting on the system are exponentially distributed, i.e. constant rates are associated with the random variables. This assumption - is widely accepted for the fault rates, - is in agreement with the concept of incident, - is, at a first sight, a very rough assumption for maintenance processes ; however, previous studies^{8,9} have shown that it is legitimate.

As a consequence, we shall be able to evaluate the dependability levels by time homogeneous Markov techniques.

The corresponding Markov transition graphs are generally too complex to allow analytical expressions of $D_i(t)$ to be derived. So, we shall proceed as follows:

- when it is possible, derive the mean time to absorption MTA_i (mean time spent in the non absorbing states) in order to identify the most influent parameters ; let us note that the MTA_i plays the same role for $D_i(t)$ as the MTTF plays for reliability,
- in all cases, compute numerically $D_i(t)$; this will be done by using a Markov-based evaluation program developed at LAAS : the SURF program¹⁰.

3.2. System parameters

Table of Fig. 3 summarizes the values of the rates associated with the alternation processes which will be considered ; these values have been selected in order to form a coherent set.

ALTERNATION PROCESS	PARAMETERS	LABEL	TYPICAL VALUES
CAPABILITY	Failure rate	λ	one fault developed once every year $10^{-4}/h$
	Increase ratio of fault rate during solicitation	K	From MIL-HDBK-217-B $1 \leq K \leq 50$
	Maintenance rate	μ	$10^2 \leq \frac{\mu}{\lambda} \leq 10^4$ $10^{-2}/h \leq \mu \leq 1/h$
SOLICITATION	Incident occurrence rate	γ	$1 \leq \frac{\gamma}{\lambda} \leq 100$ $10^{-4}/h \leq \gamma \leq 10^{-2}/h$
	Incident processing rate	ψ	$\frac{\psi}{\gamma} \geq 10$ $10^{-1}/h \leq \psi \leq 10^{-4}/h$
	Maintenance rate	ν	$5 \leq \frac{\nu}{\gamma} \leq 10^5$ $5 \cdot 10^{-4}/h \leq \nu \leq 10^{-1}/h$

Fig.3-Rates associated with the alternation processes

Characterization of the system behavior necessitates additional parameters to be defined, which are expressed under the form of conditional probabilities in fig. 4.

Detection efficiency	$P_D = P\{\text{Fault has been detected} \text{A fault has occurred}\}$
Masked fault probability	$q = P\{\text{Masked inability} \text{A fault has occurred}\} = Q(1 - P_D)$ $Q = P\{\text{Fault has no action on the monitored system} \text{A fault has occurred and has not been detected}\}$
Maintenance efficiency	$P_M = P\{\text{Repair leads to a fault-free state} \text{Maintenance has been performed}\}$
Transient incident	$= P\{\text{Monitored system has returned to normal working conditions under the actions controlled by the safety system} \text{End of incident processing occurs}\}$

Figure 4- Conditional probability parameters

3.3 Level-1 dependability modeling

Fig. 5 gives the Markov transition graph deduced from fig. 3, where a) the successive states and transitions occurring in state 5 of fig. 3 are explicitly shown (n is the number of successive masked inabilities which can develop), and b) an imperfect repair is assumed to lead the system into a masked-inability state.

Figure 5- Markov transition graph of the level-1 dependability of the simplex system

As we mentioned in paragraph 3.1., the Markov transition graph is too complex to allow analytical derivation of $D_1(t)$. We have however derived the MTA. Using standard techniques for Markov processes and making first-order asymptotic developments with respect to λ/ξ , λ/μ , λ/ν , δ/ξ , δ/μ , δ/ν , q and $1 - P_M$, lead to the following results:

- for $n=1$, $MTA_1 \approx \frac{1}{\lambda[q\tau_M + 1 - \tau_M + k\frac{\delta}{\xi}]}$
- for $n \geq 2$, $MTA_1 \approx \frac{1}{\lambda[q\tau_M + 1 - \tau_M][1 - \tau_M(1-q_1)\frac{\lambda_1}{\delta + \lambda_1}] + k\frac{\delta}{\xi}}$

These expressions enable the influence of the various parameters to be weighted and the numerical calculation of $D_1(t)$ with the SURF program has enabled these results to be checked and a precise evaluation of the influences to be derived. However, due the lack of space, fig. 6 gives only the most significant results.

The above results lead to a simplification of the transition graph of fig. 6 through removal of the states whose probability can be neglected¹¹.

3.4. Level-2 dependability modeling

Fig. 7 gives the Markov transition graph deduced from fig. 2. Using the same approach as for level-1 dependability, we obtain:

$$MTA_2 \approx \frac{1}{\lambda} \left[1 - (k-1) \frac{\delta}{\xi} + (1-p) \frac{\delta}{\nu} \right]$$

All the parameters of the model are present in this expression. However they appear as being infinitely small with respect to $1/\lambda$. This is confirmed by use of the SURF program: the curves of $D_2(t)$ and $\exp(-\lambda t)$ cannot be distinguished. It is thus not

necessary to account for the solicitation process for the level-2 dependability modeling.

Number of masked faults	1) Account for two masked faults 2) Values of q_1 and λ_1 with respect to q and λ - the lower number of fault sources leads to $\lambda_1 < \lambda$ if the independence of the fault sources is kept on, and to $\lambda_1 > \lambda$ if the first fault creates dependencies, - Q can be reasonably assumed constant and P_D is likely to be lower after occurrence of a first fault $\Rightarrow q > q_1$. Thus, we can have $q_1 \lambda_1 \geq q \lambda$; the lack of experimental data and the relatively low influence of q_1 and λ_1 leads to assume $\lambda_1 = \lambda$ and $q_1 = q$
Maintenance process	1) μ and ν are of no significant influence over their full range of variation $\Rightarrow P\{\text{System being in states 3 and 4}\}$ can be neglected 2) P_M is of a great influence
Fault manifestation during solicitation	The values of $k\delta/\xi$ leads to consider two types of safety systems: 1) $k\delta/\xi \ll \sup(q, 1 - P_M)$: incident processing is of no influence on dependability and P System being in state 2 can be neglected 2) $k\delta/\xi \approx \sup(q, 1 - P_M)$: incident processing must be accounted for
Influence of q	Although of a small value, q is of a primary influence: q represents the ratio of single faults which bring the system into a dangerous state

Fig. 6- Main results for $D_1(t)$ of the simplex system

Figure 7- Level-2 model of the simplex system

4. MODELING OF FAULT-TOLERANT STRUCTURES

This paragraph deals with the two most well-known fault-tolerant architectures: duplex and majority voting (TMR). A unified treatment of both architectures is possible through introduction of the two following parameters:

- a is the number of units ($a=2$ for duplex and 3 for TMR),
- b is the fault-rate ratio between the actual units and a hypothetical non fault-tolerant and non self-detecting unit.

Efficiency of the recovery procedures will be accounted for by the coverage^{12,13}: $c = P\{\text{the structure is able to recover information processing without loss of ability} / \text{a fault has occurred}\}$; c_a and c_p will respectively denote the coverage in the absence and in the presence of an incident.

The Markov transition graph for level-1 dependability is given by fig. 8; we have assumed, according to results of § 3.4., that only two successive masked faults can occur.

Model for the level-2 dependability is deduced from fig. 8 when turning states 4 and 5¹ to absorbing states.

Conducting an analysis as extensive as we did for the simplex structure would take much more room and we shall thus restrict ourselves to giving the results of fig. 9, which enables the fault-tolerant structures to be compared with the simplex one: both dependability levels are improved; improvement is however less sensitive for the first level than for the second one.

The value of those system parameters for which field experience data exist are given in fig.11

PROCESS	PARAMETER	LABEL	VALUE
SOLICITATION	Incident occurrence rate on a line	λ_l	$10^{-4}/h \leq \lambda_l \leq 10^{-3}/h$
	Incident occurrence rate on a bar	λ_b	$10^{-5}/h$
	Incident processing	φ	$\varphi \geq 10^{-3}/h$
FAULT MANIFESTATION	Fault rate of an equipment	λ	$10^{-4}/h$
MAINTENANCE	Inspection rate	δ	$10^{-4}/h \leq \delta \leq 4 \cdot 10^{-4}/h$
	Repair rate	μ	$10^{-2}/h \leq \mu \leq 4 \cdot 10^{-2}/h$

Figure 11- Parameters of the substation

For the first two steps (equipment of a circuit-breaker, equipments of a bar), an approach similar to the one we exposed in paragraph 3 was followed. The complete model of an equipment is given by fig.12 It is directly deduced from fig.5 and is unique since the nominal dependability only has to be considered for a single equipment.

REFERENCES

- 1 K. Medhaffer-Kanoun, "Evaluation de la sûreté de fonctionnement des systèmes de sécurité. Application à la commande des postes à très haute tension", Docteur-Ingénieur thesis, INP Toulouse, Jul. 1980, 150 p, in French.
- 2 C. Lievens, "Sécurité des systèmes", Cepadues Edition, Toulouse, 1976, in French.
- 3 J.R. Taylor, "Safety assessment", in *Proc. of the Seminar "Automatic Shutdown Systems"*, Aberdeen, UK, Feb. 80, p.2-1 to 2-18.
- 4 H.F. Frey, "Safety evaluation of mass transit systems by reliability analysis", *IEEE Trans. on Reliability*, vol.R.-23, n°3, Aug. 74, pp.161-169.
- 5 C.J. Kenward, "Computer based safety systems", United Kingdom Atomic Energy Authority, Report AERE-R-7809, Oct. 74, 31p.
- 6 J.F. Meyer, "On evaluating the performability of degradable computing systems", *Proc. of the 8th International Symposium on Fault-Tolerant Computing, FTCS-8*, Toulouse, June 78, pp.44-49.
- 7 F.A. Gay, "Performance modeling for gracefully degrading systems", Ph.D. Dissertation, Northwestern University, Evanston, Ill, June 79.
- 8 J.C. Laprie, "Reliability and availability of repairable structures", *Proc. of the 5th Int. Symposium on Fault-Tolerant Computing*, Paris, June 75, pp.87-92.
- 9 A. Costes, C. Landrault, J.C. Laprie, "Reliability and availability models for maintained systems featuring hardware failures and design faults", *IEEE Trans. on Computers*, vol.C-27, n°6, June 78, pp.548-560.
- 10 A. Costes, J.E. Doucet, C. Landrault, J.C. Laprie, "SURF : Système d'évaluation de la sûreté de fonctionnement ; 1ère Partie : Méthode", Note Technique 79.T.37 ; J.E. Doucet, "2ème Partie : Notice d'utilisation", Note Technique 79.T.38, L.A.A.S., Toulouse, Sept. 79, in French.
- 11 J.C. Laprie, "On reliability prediction of repairable redundant digital structures when neglecting repair times", *IEEE Trans. on Reliability*, vol.R-20, n°4, Oct. 76, pp. 256-258.
- 12 W.G. Bourricus, W.C. Carter, P.R. Schneider, "Reliability modeling techniques for self-repairing computer systems", in *Proc. of the 12th ACM National Conference*, Aug. 69, pp.295-309.
- 13 T.F. Arnold, "The concept of coverage and its effect on the reliability model of a repairable system", in *Proc. of the 2nd Int. Conf. on Fault-Tolerant Computing*, Newton, Massachusetts, June 19-21, 1972, pp.200-204.
- 14 Le plan de protection "palier technique 1975". Les principes.E.D.F. Nov. 75, 48 p., in French.
- 15 J.C. Laprie, F. Cereja, K. Medhaffer, "Etude de nouvelles architectures sûres de fonctionnement pour les automatismes de protection et de reprise de service des postes à très haute tension", E.D.F. Contract n°47559, Final-report, LAAS publication n°1894, Toulouse, Feb. 79, 149 p., in French.

BIOGRAPHIES

J.C. Laprie was born in Paris, on December 22, 1944. He received the Engineer degree from Ecole Nationale Supérieure d'Ingénieurs de Constructions Aéronautiques in 1968 ; he defended his theses of Docteur-Ingénieur and Docteur ès-Sciences in 1971 and 1975 resp, both at Université Paul Sabatier, Toulouse. He has been with LAAS since 1968 and he is currently the head of the research team "Dependable Processing Systems". His research interest are the fault-tolerant systems, from two points of view : architecture and evaluation. He has served as the chairman of FTCS-8, held in Toulouse in June 1978.

K. Medhaffer-Kanoun was born in Sfax, Tunisia, on October 10, 1953. She received the Engineer degree from Ecole Nationale de l'Aviation Civile in 1977. She defended her Docteur Ingénieur thesis at Institut National Polytechnique de Toulouse on July 4, 1980. She has been with the research team "Dependable Processing Systems" since October 1977 and she is actively engaged in research on safety systems under sponsorship from Electricité de France.