Safety Instrumented System reliability evaluation with Influencing Factors

Florent Brissaud, Dominique Charpentier, Mitra Fouladirad, Anne Barros, Christophe Bérenguer

Safety Instrumented System reliability evaluation with Influencing Factors

F. Brissaud & D. Charpentier
Institut National de l'Environnement Industriel et des Risques (INERIS) – DCE, Verneuil-en-Halatte, France

M. Fouladirad, A. Barros & C. Bérenguer
Université de Technologie de Troyes (UTT) – Institut Charles Delaunay (ICD) – CNRS, Troyes, France

ABSTRACT: The relevance of reliability evaluation strongly depends on the quality of input data as failure rates. Reliability data handbooks give generic values which do not often fit system specificities. This paper deals with influencing factors in order to take into account some aspects as design, environment and use in reliability evaluations. Once a definition and a classification are proposed, a brief review of existing models is presented. This paper also introduces a new failure rate evaluation with influencing factors especially developed for safety instrumented systems. The seven-step methodology combines both qualitative and quantitative analyses to compensate for a potential lack of feedback knowledge. Some criteria are used to set a failure rate within a prior interval, according to system conditions. An application regarding safety pressure relief valves is included. The expected better argued and accurate results aim at leading to a more efficient risk management.

1 INTRODUCTION

Evaluating safety instrumented systems [SIS] reliability has been necessary due to societal issues and legislation. The main European standard for SIS assessment is the IEC 61508 (IEC 2005) which requires determining a probability of failure on demand [PFD] for each part of the system: detectors, logic units, and actuators. The relevance of existing models (reliability equations, reliability block diagrams, fault tree analysis, Markov processes etc.) strongly depends on the quality of input data as failure rates, maintenance characteristics, and common cause parameters.

By lack of reliability feedback data, generic failure rates from data handbooks are commonly used. They usually come from offshore, military, or nuclear power plant activities. However, the influencing factors of many systems are sometimes obviously heterogeneous and it is certainly inaccurate to assign the same failure rate to all of these systems. In this framework, predictive models have been developed, for electronic (DoD of USA 1991) or mechanical (NSWC 1998) components. Unfortunately they are too specific to be suitable for every SIS characteristic and environmental condition. Statistical models also exist, but such models require a lot of feedback knowledge. For example, some other approaches focus on organizational factors, using mainly feedback data or expert judgment.

A definition and a classification of influencing factors are proposed in the Section 2. Section 3 includes review of existing reliability models which take into account internal or external factors. Section 4 is the main part and introduces a new method for failure rate evaluation with influencing factors. The methodology is composed by seven steps and has been especially developed for SIS. An example regarding safety pressure relief valves is briefly presented and discussed in Section 5, followed by the conclusion.

2 INFLUENCING FACTORS

2.1 *Introduction to the influencing factors*

According to the IEC 60050 standard (IEC 1990), the reliability is the ability of an item to perform a required function under given conditions for a given time interval. The quantitative measurement of the reliability is usually made by a failure rate evaluation. This parameter is intrinsic to the item, its environment and conditions of use. Nevertheless, it is possible to observe failure rate realizations by a number of failures per time unit. The influencing factors denote the parameters which determine the value of the failure rate. These factors represent the "given conditions" mentioned in the reliability definition.

The following definition will be used in the present paper: the influencing factors [relating to the reliability] are the internal and external parts of an item which act on its reliability, for example by causing failure rate changes. The effects may be positive, by

causing a reduction of failure number per time unit, or negative, by causing a higher number of failures.

For example, mechanical equipment failures may occur due to some physical phenomena as fatigue, fissures or erosion which all depend on the equipment design, material properties, solicitations, or environmental interactions. In order to obtain influencing factor measurements, it is necessary to establish indicators e.g. type of material, solicitation frequency and load, humidity rate. A reliability modelling with influencing factors then consists in defining a failure rate evaluation according to these indicator values. Figure 1 sums up the effect of influencing factors on reliability, through the failures and their causes, and how a corresponding reliability model can be defined.

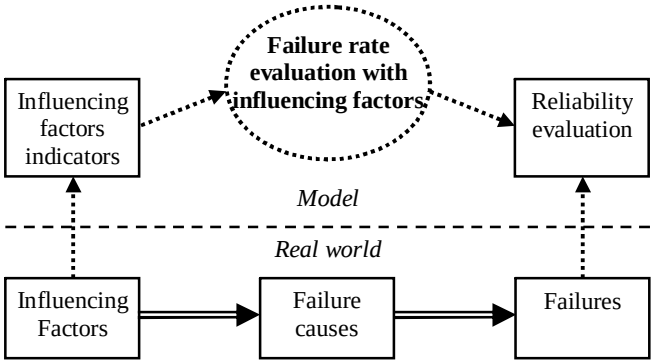

Figure 1. The influencing factors and the reliability

2.2 *An influencing factors classification*

The proposed influencing factors classification is made according to the system life cycle. This work takes advantage of the references which are presented in the next section.

- the design factors which are intrinsic-natured to the system: type, working principle, sizes, materials, component quality etc.
- the factors related to the manufacturer and the manufacture process (including the potential effect on surface finish)
- the factors due to installation and activation (including access facilities)
- the factors which act when the system is used: solicitation frequency and load, electrical load (voltage, intensity), environment (mechanical constraints, temperature, humidity, pollution), performance or reliability requirements etc.
- the maintenance factors: the quantity and the quality of preventive and corrective actions

Human and organizational factors can be added. A classification is proposed by Aven et al. (2006) which details five groups: the characteristics of the personnel performing the tasks, the characteristics of the task being performed, the characteristics of the technical system, the administration control, and the organizational factors / operational philosophy.

3 FAILURE RATE EVALUATION

3.1 *Reliability feedback data and data handbooks*

The most efficient means to obtain a suitable failure rate value is certainly the reliability feedback data. Some industrialists have collected data from their own applications, mainly from power plants or offshore platforms. In this way, the values fit equipment characteristics, environment and conditions of use. Unfortunately, a significant equipment field, appropriate procedures and a long practice are required.

By lack of such feedback knowledge, reliability data handbooks are commonly used. They give some generic data, usually from offshore (OREDA and PDS Handbook by SINTEF 2002 & 2006), military (NPRD-95 and EPRD-97 by RiAC 1995 & 1997) or nuclear power plant (EIReDA by EC 1998) activities. The users of these books presume the data can be transposed to their equipment and for their applications even though technical, operational and environmental conditions are seldom detailed. However, non negligible failure rate differences from a data handbook to another let suppose that the recorded systems are very heterogeneous. Some explanations can be given:

- all type of equipment have their own characteristics (intrinsic factors) i.e. for a system type, several kind of equipment with different reliability parameters exist
- operational, environmental and maintenance conditions are sometimes very heterogeneous from one type of equipment to another (extrinsic factors), especially between activities
- to obtain significant results and collect them in a usable data handbook, it is usually necessary to group together systems with different intrinsic and extrinsic factors

Using these data handbooks without consideration may therefore yield high reliability evaluation uncertainties. These weaknesses may be offset, for example by Bayesian approaches and expert judgment (Lanternier et al. 2005).

3.2 *Failure rate evaluation with influencing factors*

3.2.1 *Frameworks for human and organizational factors*

A lot of methods have been proposed to take into account the human and organizational factors in the reliability evaluations or quantitative risk analyses: Manager (1990), MACHINE (1992), WPAM (Davoudian et al. 1994), ISM (1994), ω-factor model (1996), SAM (1996), RIA (Rosness 1998), I-Risk (1999), ORIM (Øien 2001b), ARAMIS (2004), BORA-Release (Aven et al. 2006). Five representative steps are given by Rosness (1998):

1 preparation of the analysis in order to define the field and the scope of the study
2 documents and data collection

3 qualitative analysis which aims at defining a general model, selecting the influencing factors, and set the current factor states
4 quantitative analysis to evaluate the effect of each factor and to calculate the results according to the model
5 verification and documentation which consist in validating and formalizing the results

Some tools have been developed for the qualitative step, especially for the model definition and factor selection. For example, a conceptual tree is proposed in RIA, an organizational model in ORIM, and a risk influence diagram in BORA-Release. Then, in order to set the current states of factors, expert judgment is often used. Aven et al. propose a scale from A (best standard in industry) to F (worst practice). WPAM suggests the use of questionnaires and audits, while in ORIM, indicators from 1 to 5 are developed.

Starting from this point, quantitative analysis aims at formulating a final result (level of risk, probability of failure, failure rate) according to the potential changes of the influencing factors. In this scope, rating processes consist of assigning a weight to each factor in order to contrast their effects. Expert judgment is always used, except for ORIM where a Cox model is proposed. According to the model, the factors influence is added up or a Bayesian network is used to modify baseline values.

3.2.2 *Electronic component failure rate evaluation with influencing factors*

In a safety instrumented system [SIS], detectors and logic units can usually be seen as electronic equipment. The inclusion of influencing factors into the failure rate evaluation generally consists of predictive models. The first related standard is the MIL-HDBK-217. It appeared in 1960 for military applications. The 1991 revision (DoD of USA 1991) is now well known and used by industrialists.

The failure rates are given by analytical functions which depend directly on some parameters as temperature, voltage or electrical intensity. The baseline values correspond to reference conditions. Coefficients are then multiplied according to the influencing factors (part stress analysis). The failure rate of a system is obtained by adding the failure rate of all its components (part count analysis). This approach is especially useful during the design phase when no test has been done yet. Nevertheless, all the values of the influencing factors have to be well known.

A lot of similar standards have then been developed, especially for military applications: 217Plus methodology by the DoD of USA, the French FIDES (UTE 2004) and the Chinese GJB/z 299B; and for telecoms: Telcordia standard (ex-Bellcore), RDF 2000 by Union Technique de l'Électricité [UTE], HDR4 and HDR5 by British Telecommunication [BT]. Finally, the IEC 61709 standard (IEC 1996) deals with reference conditions for stress models.

3.2.3 *Mechanical component failure rate evaluation with influencing factors*

The SIS actuators are mainly mechanical equipment e.g. valves, pumps, breaks. They usually cause half the faults and failures of SIS. Moreover, due to the high diversity and conditions of use, the reliability is particularly subject to influencing factors.

Only one predictive model can be found for mechanical components, the NSWC-98/LE1 standard (NSWC 1998). The influencing factors are numerous: temperature, pressure, fluid and material properties, load, performance requirements and so forth. Unfortunately, the eighteen components which are developed are not enough for safety instrumented system analyses. Moreover, some required influencing factor values are very difficult to know (allowable leakage rate, fluid viscosity) and the reference values do not fit industrial processes. For example, the baseline valve pressure activation is 200 bars whereas in industry this value seldom exceeds 60 bars.

Without a priori knowledge about physical relations between failure rates and influencing factors, statistical approaches are briefly proposed in CCPS 1999 and Debray et al. 2004. Feedback data is used in order to observe failure rate trends which depend on influencing factors. When a lot of data is collected and the influencing factors are detailed, Lanternier et al. 2006 and Brissaud et al. 2007 propose the use of a Cox model. By using a Weibull law, this approach has the particularity to give a failure rate which depends both on influencing factors and time. Finally, Lanternier 2007 presents also the use of neuronal networks.

4 A NEW MODEL FOR FAILURE RATE EVALUATION WITH INFLUENCING FACTORS

4.1 *A new model especially developed for SIS*

A new methodology for failure rate evaluation will be proposed in the present paper. To be usable in most SIS reliability evaluations, the following particularities have been set:

- the methodology should be global enough to be usable for a large number of safety systems (especially actuators) and influencing factors
- a qualitative analysis has to compensate for a potential lack of data from feedback knowledge by the use of organized expert judgment
- the quantitative part has to allow improvements when some feedback data is newly available
- even if it is certainly not conceivable to obtain an exact reliability evaluation without much feedback data, the methodology should give argued results which logically depend on influencing factors
- the prospect is for risk analyses which allow more efficient risk managements by acting both on equipment and influencing factors

4.2 *General presentation of the model*

The general form will be the same as the predictive models. The equipment is divided into several main component groups as a serial system i.e. the failure rate is obtained by the sum of the main component groups failure rates. To have an a priori idea of the whole equipment failure rate is usually more realistic than accurate values for all the components. Each component (i.e. main component group) baseline failure rate will therefore be expressed as a percentage of the whole system baseline failure rate.

The effects of the influencing factors will then be included by influencing coefficients. Each coefficient corresponds to one factor and vice-versa. If a component is liable to an influencing factor, the baseline failure rate is multiplied by the corresponding influencing coefficient. The coefficient values are defined according to the states of the influencing factors:

- if the influencing factor is supposed to be in a medium state according to the reliability, the corresponding influencing coefficient is equal to one
- if the influencing factor is supposed to be in a more suitable state (resp. a less suitable state), the corresponding influencing coefficient is smaller than one (resp. greater than one)

These properties can be summed up by the formulas:

$$\lambda_s = \sum_{i=1}^{N} \lambda_i = \sum_{i=1}^{N} \left[\lambda_{i,mean} \cdot \prod_{j \in J_i} C_j^* \right] \quad (1)$$

$$\lambda_{i,mean} = c_i \cdot \lambda_{s,mean} \text{ with } \sum_{i=1}^{N} c_i = 1 \quad (2)$$

where λ_s and λ_i are respectively the system and the components (i.e. main component groups) failure rates, according to the current states of the influencing factors; $\lambda_{s,mean}$ and $\lambda_{i,mean}$ the baseline system and components failure rates; c_i the contribution (in percentage) of component i in the whole baseline system failure rate; N the number of components which compose the system; C_j^* the influencing coefficient which corresponds to the influencing factor j; J_i the set of influencing factors indices which have an effect on component i.

In order to have coherent results with a presupposed failure rate scale, a prior interval $[\lambda_{s,min}; \lambda_{s,max}]$ is set. The main idea of the methodology is to use some criteria to fix the failure rate inside this interval, according to the influencing factor states. The method is based on these following propositions which are summed up in Figure 2:

- the system baseline failure rate $\lambda_{s,mean}$ is reached when all the influencing factors are, on average, in a medium state
- the lower value $\lambda_{s,min}$ (resp. the upper value $\lambda_{s,max}$) of the prior interval is reached when all the influencing factors are, on average, in a defined proportion Ψ of the most suitable states (resp. the least suitable states)

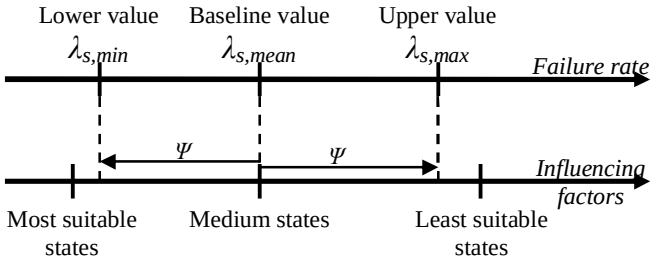

Figure 2. Fundamental assumptions of the proposed model

4.3 *A seven-step methodology*

The proposed methodology is composed by seven steps. Qualitative analysis (step 1 to 3) and quantitative analysis (step 1 and 4 to 7) are combined in a framework which can be seen as an adaptation of the steps for human and organizational factors.

4.3.1 *Step 1: functional analysis and input data*

First of all, it is advisable to delimit the scope of the study: which equipment (valve, pump, detector etc.) to be applied and for which safety function and application. The failure rate has to be defined precisely. For example, only the dangerous and undetected failures can be relevant for the study, and the unit can be the number of failures per hours or per solicitations.

Using available feedback data, reliability data handbooks and, if required, expert judgment, a system baseline failure rate ($\lambda_{s,mean}$) has to be set. It must fit as much as possible the medium conditions, according to the reliability, wherein the system can be. This baseline value is surrounded by an interval ($[\lambda_{s,min}; \lambda_{s,max}]$). It corresponds to the extreme failure rates which are possible to observe for this type of system, according to the worst and the most suitable influencing factor states.

A failure mode, effect, and criticality analysis [FMECA] is recommended to identify the components (i.e. main component groups) of the system which are liable to different influencing factors. Using the FMECA and, if available, some reliability data, the contribution of each component in the baseline system failure rate (c_i with $i=1,\ldots,N$) has to be evaluated.

4.3.2 *Step 2: model definition and influencing factors selection*

A reliability influencing diagram is proposed for model definition and the selection of relevant influencing factors. Four levels are built from right to left. These levels are composed by elements (the circles), and influencing relations (the arrows):

- the first level has only one element which is the system identification
- the second level is composed by the main component groups of the system which have been identified in step 1. Each element of this level is linked to the system element of the previous level

– the elements of the third level are the system life cycle phases which also correspond to the influencing factors categories (see table 1). When a phase is supposed to have a non negligible effect on a component reliability, an arrow is drawn between the two corresponding elements
– the last level represents the selected influencing factors for each life cycle phase which is relevant for reliability

An example of influencing diagram is given in Figure 4 for a safety pressure relief valve.

Table 1. Sample of checklist for influencing factors selection

Category		Influencing factors
Design		System type
		Working principle
		Sizes (height, volume, weight)
		Materials
		Component quality (quality requirements and controls)
		Special characteristics (supply)
Manufacture		Manufacturer
		Manufacture process (procedures, controls)
Installation		Location (access facilities)
		Assembly/Activation (procedures, controls)
Use	EUC*	EUC* type
		Special characteristics
	Solicitation	Type of load (cycling, random)
		Frequency of use
		Loading charge/Activation threshold
		Electrical load (voltage, intensity)
	Environment	Mechanical constraints (vibration, friction, shocks)
		Temperature
		Corrosion/Humidity
		Pollution (dust, impurities)
		Other stresses (electromagnetism, climate)
	Requirements	Performance requirements
		Failure modes (recorded failures)
Maintenance		Frequency of preventive maintenance
		Quality of preventive maintenance
		Quality of corrective maintenance

* Equipment Under Control

Table 1 gives a sample of checklist for influencing factors selection. The choice of the influencing factors has to follow some criteria:

– it is possible to measure or evaluate the states
– the state measurements or evaluation has to allow making differences between systems
– the selected factors are exhaustive enough to explain the observable reliability differences

An influencing matrix $F_{N,M}$ is defined on $N*M$ as follows: $F_{N,M}(i,j)=1$ if the component i is liable to the influence of factor j, $F_{N,M}(i,j)=0$ otherwise.

4.3.3 *Step 3: indicators choice and graduation*

An indicator is the means to observe the state of an influencing factor. Øien 2001a proposes some criteria for indicator choice in terms of the amount of data, available sources, relationships with observed factors, validity and repeatability.

For the model which is developed, the indicators have to be set on a numerical scale. Moreover, the effects of factors (positive or negative) will be assumed to be continuous and monotonous according to the indicator values. For qualitative indicators (e.g. manufacturer name, type of material), a scale from 0 for "very not suitable for reliability" to 5 for "very suitable for reliability" is proposed. For quantitative indicators (e.g. pressure, voltage, temperature), the values can be directly used if account for the previous conditions. Otherwise, a multiple level scale has to be defined as for qualitative indicators.

Using technical reports, operational data, feedback knowledge, measures, investigation with key staff and so on, three particular levels have to be set for each indicator: one which represents the medium influencing factor state, two which represent the extreme observable values (the least and the most suitable values for reliability).

The scale for the indicator I_j of the influencing factor j is denoted $[I_{j,lower}; I_{j,upper}]$ and the three particular levels are $I_{j,mean}$ for the medium value, $I_{j,worst}$ and $I_{j,best}$ for respectively the least and the most suitable values which are observable.

4.3.4 *Step 4: influencing factors rating*

A weight is given to each selected influencing factor. It represents the relative potential effect on the liable component failure rates, according to a change from the least to the most suitable value of the corresponding indicator.

A rating from 1 to 5 or from 1 to 10 is usually suitable for the model. Feedback knowledge, graduating processes, comparisons by pair, tests or expert judgment can be used to set weights. The weight of the influencing factor j is denoted W_j and it is normalized using Equation (4) given in Appendix A.

4.3.5 *Step 5: indicator functions*

In order to deal with uncertainties, especially when expert judgment is required, indicator functions aims at representing the current indicator values not as fixed points, but as probability density functions. In fact, the indicators values are seldom known precisely and are sometimes subject to changes during the system life cycle (temperature, humidity, load). Three density function types are proposed:

– uniform distribution when expert judgment is the main used means to evaluate the indicator value e.g. it is supposed that the influencing conditions are quite benefit or not for the reliability
– triangular distribution if the indicator value is deterministic and has to be translated on a defined scale e.g. the indicator value is given on a scale from 0 to 5 according to the "degree of suitability" for the reliability
– Gaussian distribution when the quantitative indicator value is directly used e.g. pressure, temperature, volume etc.

Examples of these three distributions for safety pressure relief valves are given in Figure 5 to 7. In this example, the *sizes* influencing factor is set on a deterministic scale with qualitative values (big, medium, small). The allowable leakage rate which represents the *performance requirements* is defined as restrictive or indulgent according to expert judgment. Finally, the pressure of activation (in bars) is a quantitative indicator for *loading charge* influencing factor. The indicator function of the influencing factor j is denoted $g_j(I_j)$ and is defined on $[I_{j,lower}; I_{j,upper}]$.

4.3.6 *Step 6: influencing functions*

The influencing functions aims at formulating the influencing coefficients according to the indicators values. An example of this type of function is given in Figure 3. The functions are built by setting three particular values: one which corresponds to a medium indicator value (denoted $C_j(I_{j,mean})$), two which correspond to the least and the most suitable indicator values (resp. $C_j(I_{j,worst})$ and $C_j(I_{j,best})$). They can be obtained by the formulas given in Appendix A. They take into account the previous steps, including the influencing factor weights. Linear relations are then assumed between these particular values, as presented in Figure 3. These functions are extrapolated all over the indicator scales $[I_{j,lower}; I_{j,upper}]$.

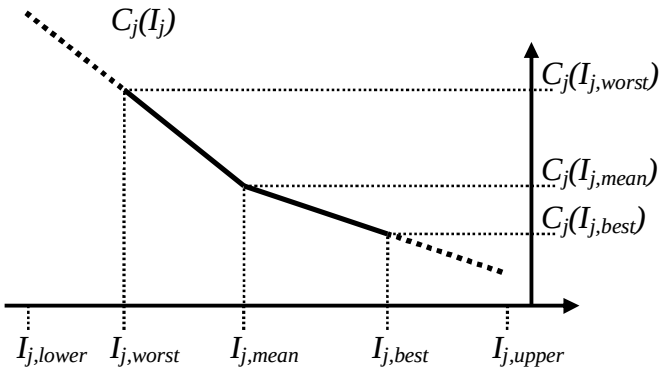

Figure 3. Example of influencing function $C_j(I_j)$

4.3.7 *Step 7: final results*

Given the indicator functions ($g_j(I_j)$) which express the states of the influencing factors; and the influencing functions ($C_j(I_j)$) which formulate the influencing coefficients; both according to the indicators, the influencing coefficients (C_j^*) are calculated by:

$$C_j^* = \int_{I_{j,lower}}^{I_{j,upper}} C_j(I_j) \cdot g_j(I_j) \cdot dI_j \quad \text{for} \quad j = 1,\ldots,M \qquad (3)$$

The final system failure rate is then obtained by using Formulas (1) and (2) with the input data of the first step. Note that the use of density functions for indicators in Equation (3) mitigates the potential effects of the assumptions from step 6 (about the definition of influencing functions) on results.

5 APPLICATION TO SAFETY PRESSURE RELIEF VALVES

5.1 *Presentation of the application*

In order to illustrate the use of the proposed methodology, an application to safety pressure relief valves is developed. The results will be compared to the real failure rates in order to assess the model accuracy. Nevertheless, it is not realistic to claim to know real failure rates. It is only possible to observe the mean time a system is functioning and to make failure rate estimations from that. This is why the following approach will be used:

1 set a fictitious panel of systems with defined influencing factor conditions
2 allocate to each system a failure rate which is set as the true value i.e. the “real failure rate”. A “hidden model” is used in order to have coherent failure rates according to the influencing factors
3 by using the real failure rates, simulate times to failure for each system by Monte Carlo method
4 use the times to failure simulations as input data for the proposed methodology
5 compare the results with the real failure rates

Note that the real failure rates are not used in the model which is tested, only the times to failure simulations are required and the influencing factors states.

5.2 *Application results*

Fourteen safety pressure relief valves are in the panel. Valve number #1 is assumed to be in the most suitable conditions for the reliability whereas numbers #6-9 correspond to medium conditions, and number #14 to the worst. Each valve is composed by a poppet assembly, a seal, and a spring (i.e. the main component groups). The respective baseline component contributions are 70%, 5% and 25%. The three selected influencing factors are the *sizes* with a weight of 3, the *loading charge* with a weight of 2, and the *performance requirements* with a weight of 1.

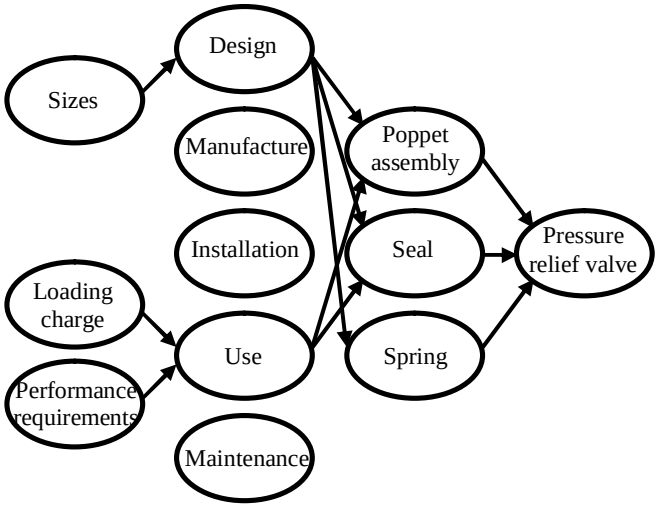

Figure 4. Reliability influencing diagram for safety pressure relief valves example

Figure 4 shows the reliability influencing diagram and Figures 5 to 7 the chosen indicators and indicator functions. Remark that the indicators values increase according to the "degree of suitability" (represented by the lightness of the curves) in the first two scales, and decrease in the third one.

Predictive models from NSWC-98/LE1 (NSWC 1998) have been used with some adaptations to set the real failure rates which are reported in Figure 8. According to a stated number of simulated times to failure per valve, two failure rate evaluations are tested: the inverse of the mean time to failure (maximum likelihood estimation [MLE]) and the failure rate evaluation with influencing factors (the proposed model, denoted *frewif*). For the *frewif* methodology, the MLE estimations of the valves #6-9, #1, and #14 have been used as input data in step 1 i.e. to assess baseline and extreme failure rate values (resp. $\lambda_{s,mean}$, $\lambda_{s,min}$, and $\lambda_{s,max}$). The results of the MLE and the *frewif* evaluation are given in Figure 8 and 9.

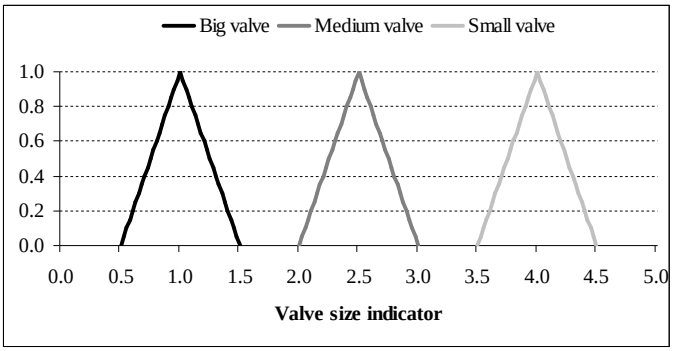

Figure 5. Indicator functions for *sizes* influencing factor

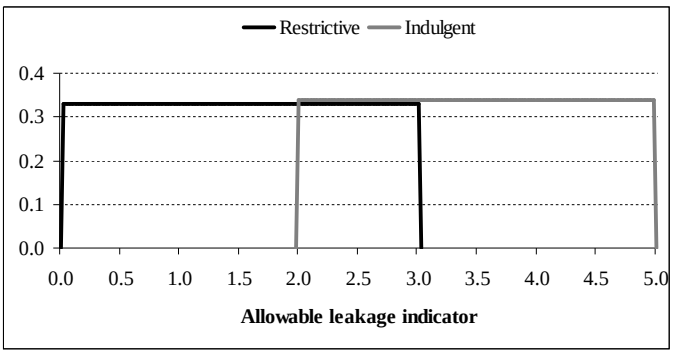

Figure 6. Indicator functions for *performance requirements* influencing factor

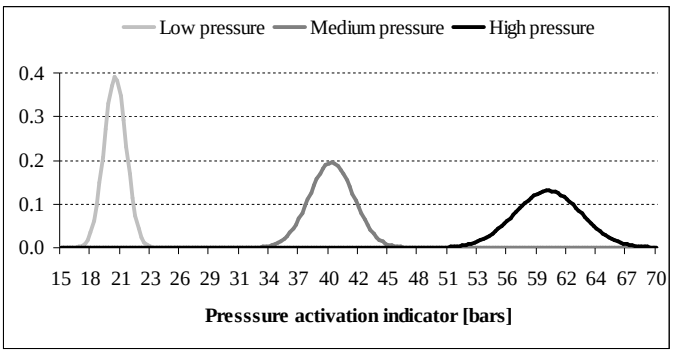

Figure 7. Indicator functions for *loading charge* influencing factor (the higher is the nominal pressure of activation, the greater the uncertainty is assumed to be)

In the described conditions, the proposed methodology gives more accurate results than MLE, especially when feedback data is low (few observed times to failure). Moreover, taking into account the influencing factors yield more argued and coherent evaluations than using only feedback data.

In this example, only the quantitative part of the models is evaluated. In fact, it seems difficult to measure the quality of the functional analysis, factors and indicators selections. Nevertheless, some further analyses have shown that quality of the results for the proposed methodology is robust according to the input data (input failure rates, component contributions, influencing factors weights).

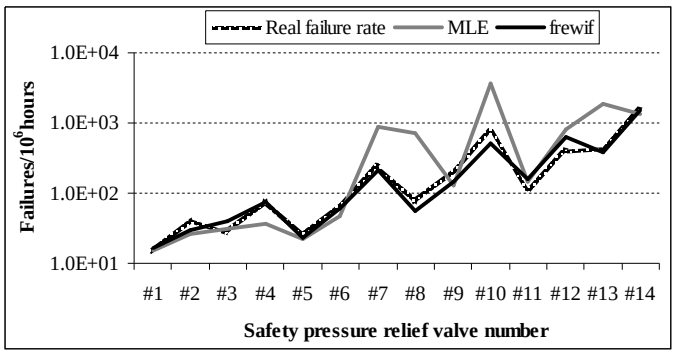

Figure 8. Results of failure rate evaluations using 3 times to failure observed per valve (logarithm scale)

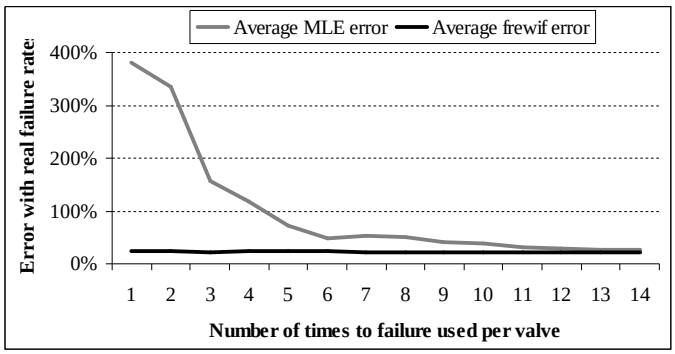

Figure 9. Average percentage of error with the real failure rates, according to the number of times to failure observed per valve (quantity of feedback data)

6 CONCLUSION

This paper has investigated the concept of influencing factors in reliability. A definition and a classification have been proposed. Because systems have own characteristics, operational and environmental conditions, the reliability parameters are often very heterogeneous. To ignore the influencing factors, for example by using non-appropriate feedback data or data handbooks, therefore yields high reliability evaluation uncertainties.

Specific models have been developed in order to include the human and organizational factors in quantitative risk analysis. Predictive models are also well established and allow taking into account influencing factors in failure rates of electronic components. Un-

fortunately, none of these models is general enough to be usable for most of the SIS assessments, especially for the actuators which are mechanical equipments. Statistical models have been proposed in the literature but require a lot of reliability feedback knowledge and such data is seldom available.

A new methodology for failure rate evaluation, especially developed for SIS, has then been proposed in the present paper. It is general enough to be usable for a large number of safety systems and influencing factors. Because a qualitative approach is combined with a quantitative part, it can compensate for a potential lack of feedback knowledge, while allowing improvements when including data. Using density indicator functions, the model also deals with uncertainties in order to avoid dubious evaluations, particularly when expert judgment is required.

The example regarding safety valves has shown that the proposed methodology provides, in some conditions, more accurate results than a classical approach as MLE, especially when the amount of feedback data is low. Moreover, by taking into account the influencing factors, the results are more argued and coherent according to the system conditions.

There are therefore good prospects to use this methodology, notably in chemical industries, where a high variety of SIS can be found in very heterogeneous conditions, and the reliability feedback data is often low. A more efficient risk analysis and management could then be performed by taking into account both safety systems and influencing factors.

7 APPENDIX A: INFLUENCING FUNCTIONS

Normalized weight w_j for each influencing factor j:

$$w_j = \frac{\sum_{i=1}^{N} c_i \cdot F_{N,M}(i,j) \cdot W_j}{\sum_{i=1}^{N}\sum_{k=1}^{M} c_i \cdot F_{N,M}(i,k) \cdot W_k} \text{ for } j = 1,...,M \quad (4)$$

The influencing reference coefficients C^-_{ref} and C^+_{ref} are obtained by solving these equations:

$$\lambda_{s,\max} = \lambda_{s,mean} \cdot \sum_{i=1}^{N}\left[c_i \cdot \prod_{j \in J_i} \left(\Psi \cdot w_j \cdot C^-_{ref} \right) \right] \quad (5)$$

$$\lambda_{s,\min} = \lambda_{s,mean} \cdot \sum_{i=1}^{N}\left[c_i \cdot \prod_{j \in J_i} \left(\frac{C^+_{ref}}{\Psi \cdot w_j} \right) \right] \quad (6)$$

Particular values of the influencing functions:

$$C_j\left(I_{j,mean}\right) = 1 \text{ for } j = 1,...,M \quad (7)$$

$$C_j\left(I_{j,worst}\right) = w_j \cdot C^-_{ref} \text{ for } j = 1,...,M \quad (8)$$

$$C_j\left(I_{j,best}\right) = \frac{1}{w_j} \cdot C^+_{ref} \text{ for } j = 1,...,M \quad (9)$$

8 REFERENCES

Aven, A. et al. 2006. Barrier and operational risk analysis of hydrocarbon releases (BORA-Release): Part 1. Method description. *Journal of hazardous Materials* 137: 681-691

Brissaud, F. et al. 2007. Modélisation des taux de défaillance en mécanique. *PENTOM 2007; Proc., Mons, 9-10 July 2007*

Center for Chemical Process Safety [CCPS] (2nd) 1999. *CCPS Guidelines for Chemical Process Quantitative Risk Analysis*. New-York: Wiley-AIChE

Department of Defence of USA [DoD of USA] 1991. *MIL-HDBK-127F, Reliability Prediction of Electronic Equipment*. Philadelphia: DoD of USA

Davoudian, K. et al. (1994). Incorporating organisationl factors into risk assessment through the analysis of work processes. The work process analysis model (WPAM-II). *Reliability Engineering and System Safety* 45: 85-125

Debray, B. et al. 2004. *ARAMIS D1C – Appendix 7, Frequencies data for the fault tree*. Verneuil-en-Halatte: INERIS

European Commission [EC] & Électricité de France (3rd) 1998. *European Industry Reliability Data Bank (EIReDA)*. Iraklion: Crete University Press

International Electrotechnical Commission [IEC] (1st) 1990. *IEC 60050-191, International Electrotechnical Vocabulary. Chapter 191: Dependability and quality of service*. Geneva: IEC

International Electrotechnical Commission [IEC] (1st) 1996. *IEC 61709, Electronic components – Reliability – Reference conditions for failure rates and stress models for conversion*. Geneva: IEC

International Electrotechnical Commission [IEC] (1st) 2005. *IEC 61508, Functional safety of electrical / electronic / programmable electronic safety-related systems – All parts*. Geneva: IEC

Lanternier, B. 2007. *Retour d'expérience et fiabilité prévisionnelle*. Saint-Etienne: Université Jean Monnet

Lanternier, B. et al. 2005. Taux de défaillance bayésien pondéré à partir de données de retour d'expérience. *CPI 2005; Proc., Casablanca, 9-11 November 2005*

Lanternier, B. et al. 2006. Failure rate model for spring loaded relief valves. In Guedes Soares C., Zio E. (ed.), *Safety and Reliability in managing risk: ESREL 2006; Proc., Estoril, 18-22 September 2006*. Leiden: Taylor & Francis

Naval Surface Warfare Center [NSWC] 1998. *NSWC-98/LE1, Handbook of Reliability Prediction Procedures for Mechanical Equipment*. Washington: NSWC

Øien, K. 2001a. Risk indicators as a tool for risk control. *Reliability Engineering and System Safety* 74: 129-145

Øien, K. 2001b. A framework for the establishment of organizational risk indicators. *Reliability Engineering and System Safety* 74: 147-167

Reliability Information Analysis Center [RiAC] 1995. *Nonelectronic Parts Reliability Data* [NPRD-95]. Utica: RiAC

Reliability Information Analysis Center [RiAC] 1997. *Electronic Parts Reliability Data* [EPRD-97]. Utica: RiAC

Rosness, R. 1998. Risk Influence Analysis, A methodology for identification and assessment of risk reduction strategies. *Reliability Engineering and System Safety* 60: 153-165

SINTEF (2006 ed.) 2006. *Reliability Data for Safety Instrumented Systems, PDS Data Handbook, 2006 Edition*. Trondheim: SINTEF Technology and Society

SINTEF Technology and Society (4th) 2002. *Offshore Reliability Data Handbook* [OREDA 2002]. Høvik: OREDA Participants, Det Norske Veritas

Union Technique de l'Électricité [UTE] (A ed.) 2004. *Reliability Methodology for Electronic Systems – FIDES Guide 2004 issue A*. Fontenay-aux-Roses: UTE