UNCERTAINTIES IN RISK ANALYSIS: TIME AND HUMAN FACTOR

Caira M., Rusconi C.

University “La Sapienza”, Department of Nuclear Engineering, Corso Vittorio Emanuele II 244 Rome

ABSTRACT

Time and human factor represent main sources of uncertainty in probabilistic risk analysis. After defining types and influence of uncertainty in system models, with particular attention to difference between aleatory and epistemic uncertainties, a new methodology, Dynamic Event Tree Analysis (DETA), developed in order to study dynamic behaviour of systems is proposed. It is presented through its peculiar features and mathematical formulation while field of application is discussed. Particular emphasis is placed on “transient lenght” to highlight influence of changing variables on components reliability. Besides, in the aim to include in dynamic Event Tree Analysis the assessment of human reliability, we chose, among numerous models worked out in last years, Human Cognitive Reliability (HCR) method. In fact, it provides an immediate estimation of human error probability in accord to experimental parameters related to specific context characterizing a Weibull Cumulative Distribution. Through a case-study referring to fire scenarios-chosen for relevance of interaction between operators and safety systems-potentiality deriving from exploiting together these two methods are shown. Results indicate that, in critical conditions during accidental transient, time resilience of automatic systems appears larger than operator’s one, suggesting therefore choice of configuration where man precedes automatic systems rather than inverse configuration. Finally, uncertainties affecting model and parameters of both methodologies are recognized and some proposals for their treatment are suggested.

SOURCES OF UNCERTAINTY IN RISK ASSESSMENT

Often, in risk analysis, system is not defined in an exact way and/or knowledge of dynamics is uncompleted. It yields uncertainty on model parameter values and on structuring hypothesis. This uncertainty spreads through the model, causing variability in outputs. Therefore, the assessment of this uncertainty is fundamental.

Uncertainties in risk analysis come from complexity of considered systems and from consequent troubles in modelling, from lack of data related to failures and accidents, from limitation of used methods. Systematic treatment of such uncertainties needs a classification in two different types :

1. Aleatory uncertainties
2. Epistemic uncertainties.

First one is related to inherently stochastic phenomena. Those uncertainties can be described through probabilistic approach.

Epistemic uncertainties refer to uncompleted knowledge of parameters and phenomena. This “ignorance” is reflected on one hand on uncertainty of parameter values and on other on uncertainty of models chosen to describe phenomena. It is present in all risk components:

1. Incompleteness and imprecision in defining scenarios.
2. Uncertainty of probability values of events conditioning evolution of scenarios.
3. Not complete adherence to reality in evaluating consequences.

These epistemic uncertainties are due both to intrinsic inability of models to represent reality both to lack and reliability of model data.

METHODS FOR ASSESSMENT OF TIME INFLUENCE AND HUMAN FACTOR

Dramatic influence of time and human factor during accidental dynamics in assessment of epistemic uncertainty can be calculated through methods described in following paragraphs.

Considering accidental time evolution, also defined “transient length” (or time between beginning and end of perturbation, meant as return of system in a safe state or deviation toward top event or irreparable state, [1]), we need to assess whether process variables during transient deviate

significantly from previous value, and their influence on system reliability. Also time sequence of systems operating during transient can affect outputs, for example in repairing operations, and then it cannot be omitted.
Finally, effectiveness of human intervention during accident evolution could dramatically depend upon both features, e.g. in case of intervention from control room.
These features could be not determinant in the aim of risk assessment, for example when evolution of physical variables is not enough quick to be significant in transient length, or so fast to make problem deterministic (certainty of event related to variation), or yet when evolution does not significantly change values of failure rates of system components.
Same system could be structured in such a way not to require human operations, or repairing and maintenance operations. A lot of problems, however, are in intermediate situations, where evolution of process variables during transient is relevant and affects value of failure rates of some components in deterministic way, modifying risk related to analyzed system.
Then, for adequate treatment of such systems, we need to match stochastic features, due to component failure, with deterministic ones due to evolution of physical variables of system.
Considering the number of dynamic systems, it is clear the insufficiency of static techniques for risk analysis. In particular, static analysis of dynamic systems, is always followed by uncertainty on calculated risk, due to purely dynamic features of system: the more relevant such features, the less reliable analysis output.
An integrated way for assessment of human reliability in dynamic analysis is provided by Bayesian Networks: They are some specific graphical models introduced by Pearl, Lauritzen and Spiegelhalter. The random variables of a probabilistic model are described with the vertices of a graph, where edges describe their dependencies measured with conditional probabilities. A great interest of BNs is to provide an efficient tool for modelling in a simple and readable way the most probable links between events of different nature (expert opinion, feedback experience, .) using conditional independence between random variables. Bayesian Networks, by describing the main conditional probabilities between variables, allow to compute easily the joint probability distribution of all the variables involved in a complex process [2] and can be easily updated as new evidence becomes available [3].
For these reasons, BN have been recently used as a tool to quantitatively describe how human operators process the information they receive when the interdependency between I&C systems and human operators are considered is similar to appropriate mathematical model [4].

DYNAMIC EVENT TREE ANALYSIS

Bayesian Networks are one of different suitable methods of dynamic analysis, each one characterized by some limitation due to basic hypothesis and by computational complexity that makes them not much attractive in comparison with classic methods. Anyway, it is possible to make some simplification, to allow a quicker calculation of risk and introducing further hypothesis, that restrict applicability of method but not hinder to face a lot of real situations. We could then carry out classic static analysis providing indication of related uncertainty through simplified dynamic analysis and closely examining only those features which require deeper analysis, since critical in risk assessment.
For this purpose, we propose a method identified as “simplified dynamic ETA”; it is characterized by hypothesis that make it particularly suitable to treat a class of problems in efficient and rapid way, in order to improve results achievable with classic ETA.
ETA allows quantitative assessment of probability of searched Top Events (TE) deriving from basic events for studied system. Anyway, it is affected by limitation about system dynamics, i.e. time depending factors which affect reliability, as maintenance and aging of the system, evolution of process variables during accidental transient (due to basic event) and possible human intervention. These factors involve uncertainty in determining probability of TE, which, added to imprecision about available data, contribute to error in estimate of such probability. Therefore, we discriminate between static ETA (not considering time evolution), semi-dynamic ETA (considering only maintenance and aging, but not accidental transient) and dynamic ETA (considering accidental transient too); latter difference due to limits of applicability of dynamic method.
Kind of dynamic ETA proposed keeps same structure of corresponding static analysis, but uses values of reliability of modified systems compared with static ones, considering time dependant factors:

1. Maintenance and aging of system, linking evolution of process variables during accidental transient and typical failure rates of components;

2. Possible human intervention, also including efficiency with regards to evolution of process parameters;

Dynamic ETA has the big merit to be simple and easy to apply, not requiring efforts of analysis and calculus higher than ones required for classic ETA. On the other side, this methodology has some constraint on applicability, unlike other methodologies mathematically more exact. This constraint, of course, depends on time factor, in particular on characteristic periods of examined system. So, dynamic ETA can apply when accidental transient length is:

1. comparable with time ranges where, for each involved component, values of process variables keep inside right operating range;
2. considerably lower than time range between a maintenance operation and the following, or than "mission time" of the system.

In spite of such limitations, there are a lot of systems fulfilling such hypothesis and making dynamic ETA a very interesting methodology.

In this case the reliability calculated at the time of interest (time of accident event) has to be modified [5-7] by a multiplication factor (B), depending on certain time ranges:

- The accident time evolution duration (Δt), in which some process variables could evolve till to pass the limit values for the components good-working;
- The minimum component good-working time range[1] Δt^*

If these time range are of comparable length, but enough shorter than the mission time of the system (of the time between two maintenance interventions), the reliability can be evaluated like:

$$R(t) = e^{-\int_0^{tc} \lambda^*(t)\,dt} \qquad \text{where } \lambda^*(t) = \lambda(t) \times B \quad \text{with } B = \frac{\Delta t}{\Delta t^*} \ (>1)$$

where t_c is the time when component is appealed to act, and $\lambda(t)$ the value of failure rate defined as

$$\lambda(t) = \lambda_0 + kt + f(n, \tau, s) = \lambda_0 + kt - \lambda_0 * n(s)\tau / s$$

The failure rate (λ) is considered variable in time, for aging by an "aging factor" k (linear dependency at first approximation) which increases its value, and for maintenance by a more complex factor which decrease its value, depending on mean time between two maintenance interventions (τ), the number of maintenance intervention already made (n)[2], and the system age (s).

---

[1] The trend of each process variable during accident evolution may influence the component good-working, i.e. each of them defines a time range in which its value remains in the limits of correct working; it is enough that such limits are passed by one of the process variable for making the component not to work (reliability zero). It is the intersection of such time ranges, which defines the good-working time range for the component. Mathematically it can be expressed by:

$$\Delta t^* = \int_{t_c}^{t_f} \prod_j H_j \, dt$$

$$H_j = \begin{cases} 1, \text{ for } t_c < t < t_{j,limit} \\ 0, \text{ otherway} \end{cases}$$

$t_{j,limit}$ is the time in which the process variable $A_j(t)$ passes the limit of good-working for the component, so that in case of linear trend like $A_j(t)=a_j*t$, it will be $t_{j,threshold}=A_{j,threshold}/a_j$. In the following picture t^* is $\min_j(t_{j,limit})$.

[2] $n(s)$ is entire and constant in the time between two maintenance interventions, increasing of a unit passing from these time ranges. Its value depends on component age, which based on maintenance programs would have been undergone a certain number of intervention yet.

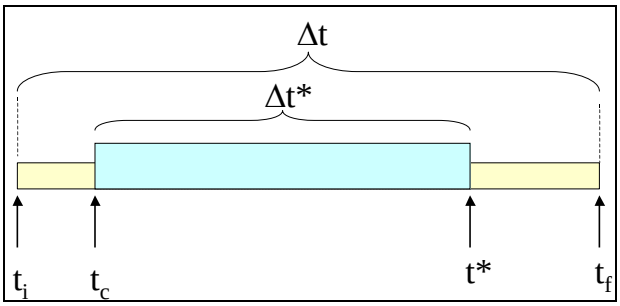


Figure 1 Relation between accident transient and operating time of safety systems.

Moreover, reliability trend, being exponential function, is sensitive only to remarkable variations of B.

For the value of Δt^*, two limit cases could be considered:

1. $\Delta t^* \rightarrow 0$, $B \rightarrow \infty$, so $R(t) \rightarrow 0$ (the component does not work).
2. $\Delta t^* \rightarrow \Delta t$, $B \rightarrow 1$, so R(t)=R(s), $s=t_c$ (the component reliability is independent of process variable evolution).

Generally, the smaller Δt^*, the less the component reliability, considering the same accident evolution time range Δt.

HUMAN FACTOR ANALYSIS

Human factor plays a basic part in system safety, for it is involved from design to building, and in management and operating. In fact, it's commonly recognized that human error gives rise to most of relevant accidents in industrial plants, or represents main cause.

Different methods were proposed to classify human behaviour. Particularly effective results the model proposed by Jens Rasmussen, used in several applications [8-11], which has the merit to reduce to few categories the almost unlimited number of types. This model discriminates human reactions in accord to following behaviours:

- immediate response (or skill-based): nearly instantaneous reaction of operator respect to facts or circumstances, pointed out by signal, noise, unexpected scenario. This kind of behaviour is determined from training and experience of operator in facing emergencies. Human error probability is very low
- Rule-based response: implementation by operator of a sequence of actions, based on known procedures. Readiness of response is lower than in former case
- knowledge-based response: it deals with behaviour of higher level, without appealing to rules or procedures. The operator uses available information and his own cognitions, in an autonomous and creative way, to decide about actions to carry out.

Indicatively, human error probabilities for the three types of behaviour spread, also overlapping, in the range between 0.5 and 10^{-4} (or less) per intervention, as shown in table 1 [12].

Table 1 – Human error probability in accord to type of behaviour

Type of behaviour	Indicative range of HEP
Skill-based	5×10^{-5} - 5×10^{-3}
Rule-based	5×10^{-4} - 5×10^{-2}
Knowledge-based	5×10^{-3} - 5×10^{-1}

Carrying out a task will involve generally all levels, while single action will be referable to one of the three levels.

This approach is focused on the mechanisms generating behaviour in the actual, dynamic work context and needs a representation at the higher level of functional abstraction than the level used for task analysis [13].

Two of the better known methods of second-generation HRA approaches—CREAM and ATHEANA—both emphasise that the likelihood of something being done incorrectly is determined by the performance conditions rather than by inherent human error probabilities, and if the context often

may be the ‘error forcing condition’ that leads to the failure, it seems reasonable to consider how the coveted ‘error probability’ can be determined directly from a characterisation of the context. In the Cognitive Reliability and Error Analysis Method this condition is described in terms of the degree of control that an operator or a team has over the situation. In accordance with the principles of cognitive systems engineering, human performance is the outcome of the purposive use of competence adjusted to the specific working conditions, rather than of pre-determined sequences of response to given events. In CREAM, a distinction is made between the following four characteristic control modes. In the basic predictive method, CREAM assumes that control mode is determined by a set of factors called Common Performance Conditions (CPC). It is further assumed that the CPCs can be used to provide a concise description of how performance is affected by the context. The current version of CREAM comprises the following 10 CPCS: ‘adequacy of organisation’, ‘working conditions’, ‘adequacy of MMI and operational support’, ‘availability of procedures/plans’, ‘number of simultaneous goals’, ‘available time’, ‘time of day (circadian rhythm)’, ‘adequacy of training and experience’, ‘crew collaboration quality’, and ‘communication efficiency’. Unlike the traditional Performance Shaping Factors, the CPCs are not assumed to be independent of one another. On the contrary, the dependency is an important feature of any real context and must be accounted for to determine the effect of the CPCS. This is done by means of a specific model of how the CPCs affect each other [14].

HUMAN COGNITIVE RELIABILITY METHOD

Even if it is a first-generation method for study of human reliability and it could seem less suitable than methods as CREAM or ATHEANA, HCR method, due to its algorithmic simplicity and flexibility to joint deterministic and probabilistic features of risk analysis, appears really sound to apply with simplified DETA.

The case study provided a demonstration of the usefulness and efficiency of combining the HCR model and the human event tree method and represents a trial to extend the human reliability quantification method to mitigating measures as required in [15].

In order to integrate in dynamic ETA assessment of human error probability, we chose, among numerous models worked out in last years, a simple method called HCR (Human cognitive Reliability), developed to quantify HEP (Human Error Probability) related to cognitive response of C type and specific for task analysis where available time T is the main constraint and whose right implementation is cognitive based. Both aspects, as seen, make this method complementary, from the point of view of human reliability analysis, to dynamic event tree developed for plant safety.

This method allows to quantify every human interaction (HI) depending upon the time, provided reliability of response in time by operator, and it is made up of three particular TRCs (Time Reliability Curves) to consider human cognitive attitude in response (skill, rule and knowledge-based).

HCR derives from TRC applied to a range of HIs with different types of cognitive behaviours (e.g. S/R/K-based in accord to Rasmussen), various mean responses in time ($T_{1/2}$) of the team, stated PSFs (for example team experience, stress, man-machine interface) which we consider to affect mainly $T_{1/2}$.

This method provides probability of no response in time T, $P_e(t)$, due to an exceedingly slow implementation of the task, and does not include trouble perception error or measure choice error, performable through event tree..

TRCs are used to quantify HEP related to cognitive response of C type of HI. Time reliability is calculated as follows:

$$P_r(\text{Non response in time t}) = P_r(T_r > T_w) = \int_0^{\infty} f_{Tw}(t)\left[1 - F_{Tr}(t)\right]dt$$

Where T_r and T_w represent respectively time for team response and range of available time for a specific HI, while $f_{Tw}(t)$ e $F_{Tr}(t)$ represent density function and CDF of probability for stochastic variables of our parameters.

Term [$1-F_{Tr}(t)$] , which is complementary of CDF of time for team response, is usually known as TRC. As example, if we assume a log-norm distribution for T_r with parameter $\mu=\ln T_{1/2}$, with $T_{1/2}$ mean time for team response, fixed σ and the constant T_w, then:

$HEP=P_r(\text{Non response in } T_w)=P_r(T_r>T_w)=1-\phi[Ln(T_w/T_{1/2})/\sigma]$

Where $\phi(.)$ is normal standard CDF. We can observe that HEP , deriving from a TRC for a HI with a fairly big range of time, should be very little. In these cases there are always other human error not time depending, as those ones in executing action.

The method develops along following steps:

- task classification;

- determination of nominal value of mean time $T^*_{1/2}$;

- Conversion of $T^*_{1/2}$ by PSF (performance shaping factor), so obtaining $T_{1/2}$;

- Definition of available time T;

- Application of HCR method to get $P_e(T)$.

In first point, set by event tree (for instance HRA) the level of decomposition of time depending tasks, classification depending on type of involved cognitive process is required.

After, we determine nominal average time $T^*_{1/2}$ (by operative experience, simulators, expert judgement,...) that represents value of available time corresponding exactly to 50% of probability of failure in carrying out a fixed task, without considering case specificity, evaluated by three PSFs: training, stress, quality of control room and of plant. Influence of PSFs on $T_{1/2}$ is expressed by following relation:

$T_{1/2}(\text{corrected for PSFs})=T_{1/2}(\text{Nominal PSFs})*\Pi(1+PSF_j) \quad j=1,2,3$

Table 2 PSFs of HCR model and values of corrective factors

Performance Shaping Factor	**PSF_J**
Operator experience	**PSF_1**
- Expert, well trained	-0.22
- Average knowledge training	0.00
- Novice, minimum training	0.44
Stress	**PSF_2**
- Situation of grave emergency	0.44
- Situation of potential emergency	0.28
- Active, no emergency	0.00
- Low activity, low vigilance	-0.28
Quality of human-machine interface	**PSF_3**
- Excellent	-0.22
- Good	0.00
- Fair	0.44
- Poor	0.78
- Extremely poor	0.92

We observe again that value of PSF_i is tabled, while, in each situation, available time T for operators to carry out intervention before a dramatic unwished change of system state must be determined, in

accord to experience or expert judgement. Therefore, the model is mathematically represented by three Weibull distributions, one for each type of cognitive behaviour, where t is available time and γ_i, η_i and β_i are parameters for the three correlations; they are meanly determined through small-scale test about three types of behaviour S/R/K.

Table 3 Parameters of model HCR

Cognitive Behaviour Type	β_I	γ_I	η_I
Skill based	1.2	0.7	0.407
Rule based	0.9	0.6	0.601
Knowledge based	0.8	0.5	0.791

Now, it will be sufficient to insert T in Weibull expression

$$P_e(t) = \exp - \left(\frac{t / T_{1/2} - \gamma_i}{\eta_i} \right)^{\beta_i}$$

to find desired probability of not response.

APPLICATION TO FIRE SCENARIOS OF DYNAMIC EVENT TREE ANALYSIS

It could be very interesting to deal through dynamic ETA the study of risk related to fire, and for its relevance, and for its features particularly suitable to uncertainty assessment with proposed method. Fire is characterized by fairly short time (in the order of hours) respect to maintenance time of involved components or respect to mission time of the system and by considerable changing of process variables (for example temperature). It could yield overcoming of good operating range for involved system.

Of course, failure rates used in calculation are those related to maintenance and aging at the moment of accident, considering a short transient respect to mission time of the entire system (condition required to apply this method).

In these scenarios, it's dramatically involved human factor as well as communication technology used in buildings or facilities; time is critical in this case, because delayed intervention of these protection devices compared with fire evolution means the failures of subsequent system, since, after ignition, it is not possible to extinguish fire. This trouble strictly depends on system and on its dynamics as well as human factor, in the presence of automatic detectors too.

Another system related to human factor is the extinguishing plant: in fact, intervention called by control room could be faster (and could depend upon quickness of former events) than automatic one, that actives the system only when threshold value is exceeded. In this case we consider direct dependence on temperature; other quantities could be used, linked, anyway, to chosen variables, through deterministic evolution of accident transient.

In the aim to calculate probability of non intervention in time T, $P_e(t)$ we can apply HCR method.

It should be observed mutual influence between $P_e(t)$ and time operating range of systems Δt^*. If configuration of safety devices considers, immediately after signalling system, the intervention of operator, his delay in actuating procedures has repercussions on starting time of devices, narrowing operating time Δt^* and, therefore, global reliability. On the other side, when operator must act after insertion of automatic devices, possible failure of one or more components of system affects response time through increasing PSF2 (stress), determined by setting of

emergency situation. Transient time Δt derives from fire standard curve, imposing as superior limit an appropriate time margin as regards to beginning of Flash Over. For it could be an extremely quick dynamic (in the order of few minutes), we need to minimize probability of non response in time by operators, limiting to acceptable values excursion of PSF2 and reducing in this way, corrected mean time.
Insert of human factor in dynamic event tree by assessing mutual influence between time of operator intervention and response of safety devices, allows matching deterministic evolution of fire with typically probabilistic nature of human behaviour through a complete and easy mathematic formalism.

Referring, for example, to following tables related to fire standard curves in railway and road tunnels processed in Germany by RABT and in the Netherlands by RWS, it is remarkable that limit temperature of 800°C, over which Flash Over zone begins, is reached in this kind of scenarios in a time of the order of three minutes. Comparing this period with sequence of safety systems, including human actions, explained in event tree below, response in time by operator appears critical in order to stop accident evolution.

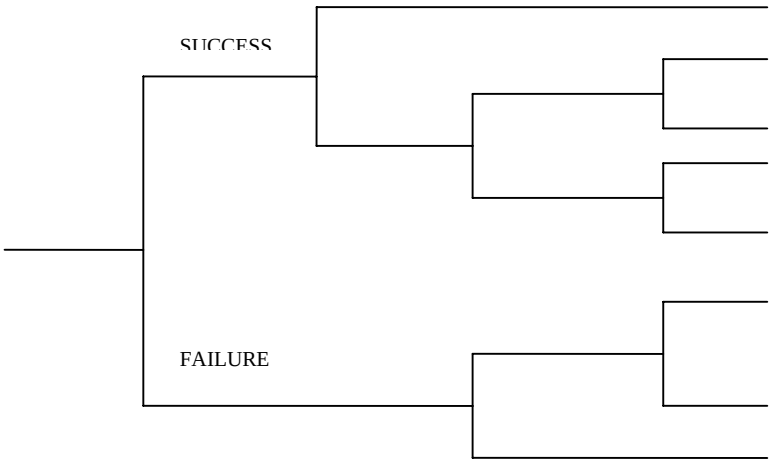
Tables 4 and 5: values of fire standard curves

RABT-ZTV (train)	
Time (minutes)	**Temperature (°C)**
0	15
5	1200
60	1200
170	15
RABT-ZTV (car)	
Time (minutes)	**Temperature (°C)**
0	15
5	1200
30	1200
140	15

RWS, RijksWaterStaat	
Time (minutes)	**Temperature (°C)**
0	20
3	890
5	1140
10	1200
30	1300
60	1350
90	1300
120	1200
180	1200

First human intervention, i.e. immediate signalling to control room and possible manual extinguish not only by trained operators but also by common people aware of fire development, involve probability of delay in response, depending dramatically upon personal skill to decide and then, after all, upon cognitive processes (PSF1).
Second kind of human intervention in event tree is activation of systems with start controlled by operators in control room. In this case, as seen, is fundamental available time for operators after intervention (maybe failed) of former systems. It involves rise of stress factor (PSF2) that could invalidate readiness of expected procedures.

BASIC EVENT	FIRST ALARM	MANUAL EXTINGUISHING	ALARM TO CONTROL ROOM	INTERVENTION FROM CONTROL ROOM



Finally, it is important that man-activated systems are available and easy to use. These features are involved by PSF3.

First source of uncertainty related to application of DETA with HCR derives from parameters of fire curve that we are considering. In fact, for hydrocarbon curves, there are only 3 minutes to avoid entering Flash Over zone, while for cellulosic ISO 834 curve there is available time of around 30 minutes. This reduction has repercussions on parameters Tsw, representing, in HCR method, available time for operators to carry out a particular action, and $\Delta T/\Delta T^*$, representing correction factor of components reliability during accidental transient.

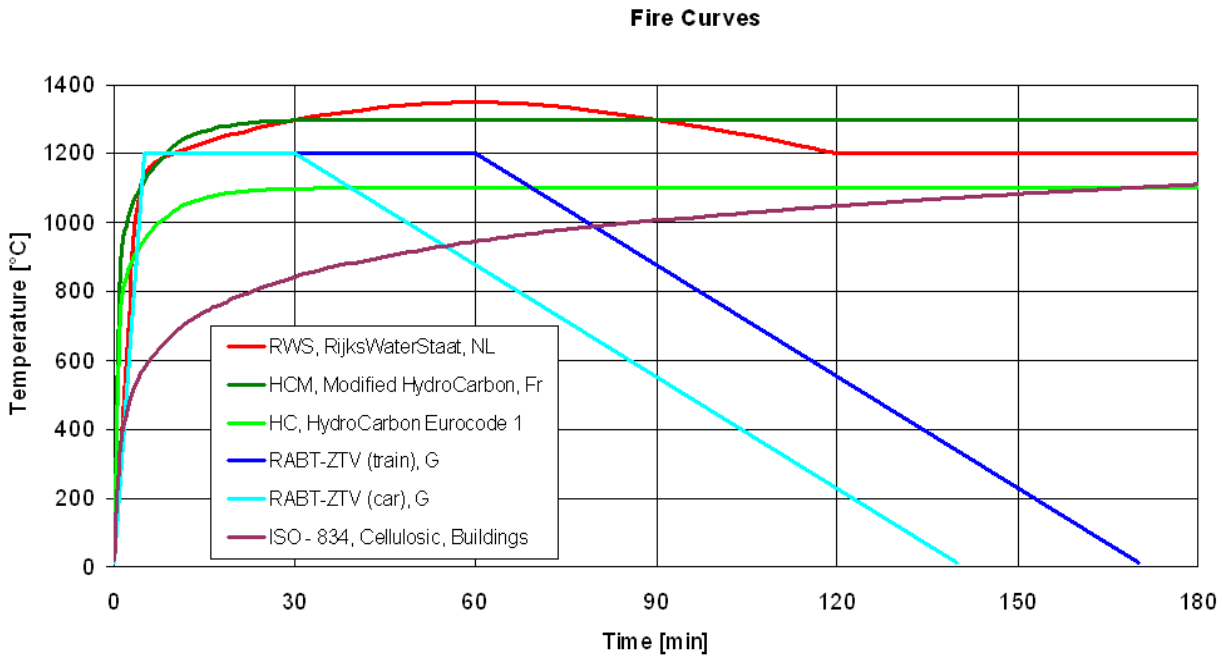


Figure 2 Fire Curves

Hence, we consider parameters of HCR methods and DETA. Imaging that we are in a situation characterized by well trained operators and excellent human-machine interface (e.g. fire alarms), we can set PSF1 equal to –0.22 as well as PSF3.

If we assume the values

$T_{1/2}$=45 sec

T_w=6 min for slow transient and T_w=2 min for fast transient (where we are supposing man as a part of safety chain)

we obtain following results

(a) $T_w/T_{1/2}$*=9.52 with PSF2=0.28 and $T_w/T_{1/2}$*=8 with PSF2=0.44 for slow transient and

(b) $T_w/T_{1/2}$*=3.21 with PSF2=0.28 and $T_w/T_{1/2}$*=2.7 with PSF2=0.44 for fast transient

if $T_{1/2}$=30 sec we achieve respectively

(c) $T_w/T_{1/2}$*=14.29 with PSF2=0.28 and $T_w/T_{1/2}$*=12 with PSF2=0.44 in slow transient and

(d) $T_w/T_{1/2}$*=4.76 with PSF2=0.28 and $T_w/T_{1/2}$*=4 with PSF2=0.44 in fast transient

finally, for $T_{1/2}$=1 min

(e) $T_w/T_{1/2}$*=7.14 with PSF2=0.28 and $T_w/T_{1/2}$*=6 with PSF2=0.44 in slow transient and

(f) $T_w/T_{1/2}$*=2.38 with PSF2=0.28 and $T_w/T_{1/2}$*=2 with PSF2=0.44 in fast transient

When we insert these numbers in Weibull CDF with parameters β=0.8; γ_l=0.5; η=0.791 (knowledge based model) we can find probability of failures as shown in figure 3

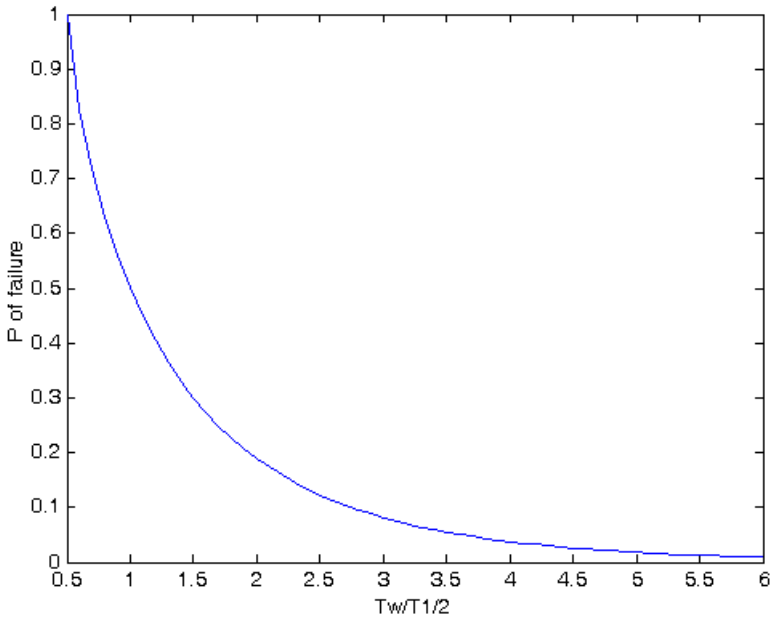


Figure 3 Probability of failure (operator)

We can observe that in slow transient uncertainty on basic parameter $T_{1/2}$ does not affect significantly human reliability for we remain fairly below P=0.1 also for PSF2=0.44. Moreover, it is very unlikely to achieve the higher value of PSF2 in such a situation.

Situation is very different when we consider fast transient. In this case, also assuming $T_{1/2}$=30 sec, effect of stress (PSF2=0.44) is sufficient to pass from P=0.02 to P=0.03 probability.

Besides, if we suppose $T_{1/2}$=45 sec or, in worst case, 1 minute, we can reach a value of nearly 0.2 for probability, considering stress factor.

In order to assess system reliability during transient we can apply DETA, focusing our attention on influence of $\Delta T^*/\Delta T$, as defined in paragraph about dynamic event tree, on failure probability as shown in figure 4

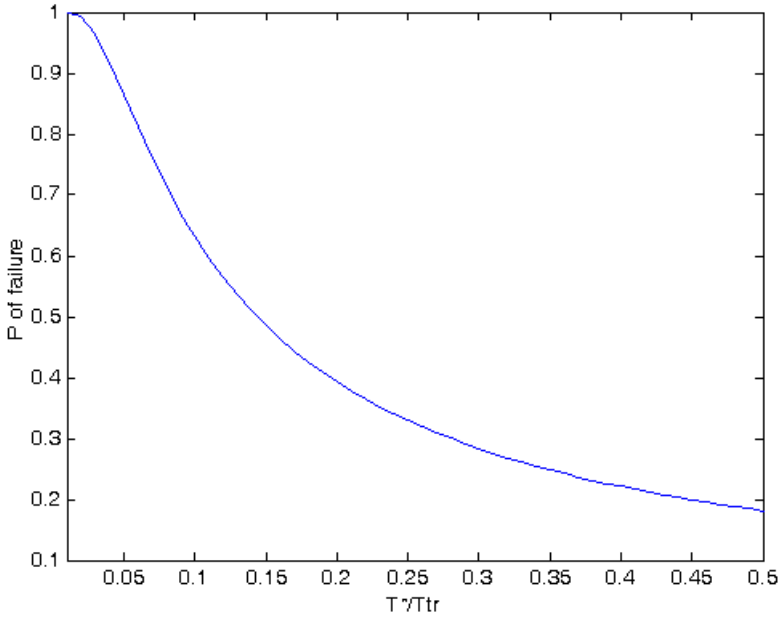


Figure 4 Probability of failure (system)

It can be remarked how, for decreasing $\Delta T^*/\Delta T$, trend becomes asymptotic. It means that, in fast transient, effect of decreasing available time on system reliability is less dramatic than on human reliability in accord to HCR method. It suggests that between following configurations:

(a) man→automatic system

(b) automatic system→man

the first one could be preferable. In fact, in configuration (b) the operator, with available time fixed by sequence of intervention of preceding automatic systems, is the ultimate barrier before accidental dynamic becomes irreversible and he could be affected by related stress. Since time response curve shows an exponential rise of failure probability when ratio $T_{sw}/T_{1/2}$ gets near zero, this factor could have serious consequences.

In configuration (a) operator, before automatic systems, has no fixed limit to act though, of course, his delay has repercussions on starting time of automatic systems, shortening their good-working time range and, consequently, global reliability.

CONCLUSIONS

Results show that, in critical conditions during accidental transient, time resilience of automatic systems appears larger than operator's one, suggesting therefore choice of configuration (a) rather than configuration (b).

Uncertainty deriving from assessing of human reliability in dynamic event tree analysis affects both model and parameters of HCR and DETA. In particular, it should be important to have reference values of $T_{1/2}$ when we apply HCR method to fire scenarios, as already done in NPP. Furthermore, in order to carry on study about man-system integration, a large number of dynamic response curves of system components should be examined. Best Performance Shaping Factors of experience and quality of interfaces have been considered, but we need to evaluate them for each special case we are going to study. Finally, qualitative results achieved by comparison of response curves for human and components reliability can represent a basis to deepen quantitative features of delay propagation in dynamic event tree.

REFERENCES

[1] M. Marseguerra, E. Zio, J. Devooght, P.E. Labeau; "A concept paper on dynamic reliability via Monte Carlo simulation" Math. and Computers in Simulation, 47, 1998.
[2] G. Celeux, F. Corset, A. Lannoy, B. Ricard; "Designing a Bayesian network for preventive maintenance from expert opinions in a rapid and reliable way"; Reliability Engineering and System Safety 91, 2006 849–856
[3] P.F. Ricci, D. Rice, J. Ziagos, L.A. Cox Jr.; "Precaution, uncertainty and causation in environmental decisions". Jr.. Environment International 29, 2003 1 – 19
[4] M.C. Kim, P.H. Seong; "A computational method for probabilistic safety assessment of I&C systems and human operators in nuclear power plants"; Reliability Engineering and System Safety 91, 2006 580–593
[5] N.J. McCormick; "Reliability and Risk Analysis"; Academic Press Inc.,1981.
[6] N. Siu; Center for Reliability and risk assessment, "Risk assessment for dynamic systems: an overview"; Idaho Nat. Eng. Lab., USA, 1993.
[7] M. Marseguerra, E. Zio; "Monte Carlo approach to PSA for dynamic process systems"; Reliability Eng. And System Safety, 52, 1996
[8] J. Rasmussen; "Human Errors: a Taxonomy for Describing Human Malfunctions in Industrial Installations"; RIS-M-2304; Roskilde, 1981
[9] J. Rasmussen; "On the Structure of Knowledge – A Morphology of Mental Models in a Man-Machine Context"; RIS-M-2192, 1979
[10] J. Rasmussen; "Skills, Rules and Knowledge: Signals, signs and symbols, and others distinctions in human performance model"; IEEE Transactions on Systems, Man and Cybernetics, SMC-13, 1983
[11] J. Rasmussen; "Information processing and human-machine interaction: an approach to cognitive engineering"; North-Holland, Elsevier, 1986

[12] G.W. Hannaman, A.J. Spurgin; “Systematic Human Reliability Procedure SHARP”;EPRI NP-3583, EPRI, Palo Alto, CA, 1984
[13] J. Rasmussen; “Risk management in a dynamic society: a modelling problem”; Safety Science, Vol. 27, No. 2/3, pp. 183-213, 1997
[14] Y. Fujita, E. Hollnagel; “Failures without errors: quantification of context in HRA” Reliability Engineering and System Safety 83, 2004 145–151
[15] M.L. Ang, K. Peers, E. Kersting, W. Fassmann, H. Tuomisto, P. Lundstro¨m, M. Helle, V. Gustavsson, P. Jacobsson “The development and demonstration of integrated models for the evaluation of severe accident management strategies—SAMEM”; Nuclear Engineering and Design 209, 2001 223–231
[16] C. Smidts; “Probabilistic dynamics: a comparison between continuous event trees and a discrete event tree model”; Reliability Eng. and System Safety, 44, 1994
[17] J.M. Izquierdo, E. Melendez, J. Devooght; “Relationship between probabilistic dynamics and event trees”; Reliability Eng. And System Safety, 52, 1996
[18] G.W. Perry; “The characterization of uncertainty in Probabilistic Risk Assessment of complex systems”, in ‘Reliability Eng. and System Safety’, 54, 1996.
[19] P. Vestrucci; “Modelli per la valutazione dell’affidabilità umana”; Franco Angeli, Milano, 1990
[20] A. Amendola; “Human Factors in Reliability Analysis”; Proceedings of the Ispra Course Advanced Systems Reliability Modelling, Madrid, 1988
[21] J. Leplat, J. Rasmussen; in Rasmussen et al.; “Analysis of Human Errors in Industrial Incidents and Accidents for Improvement of Work Safety”; (eds.), New Technology and Human Error, Wiley, London, 1987
[22] G. W. Hannaman; “Human cognitive reliability model for PRA analysis”; NUS-4531, NUS Corp., 1984
[23] F. Xiang, Z. Bingquan , J. Shengyao; “Cognitive model research of nuclear power plant operators”; Nuclear Engineering and Design 215, pp. 251–256, 2002
[24] H. Chen, T. Moan; “Probabilistic modelling and evaluation of collision between shuttle tanker and FPSO in tandem offloading”; Reliability Engineering and System Safety 84, 2004