▩ 연구논문

Effects of System Reliability Improvements on Future Risks+

Heejoong Yang
Dept. of Industrial Engineering Chong Ju University

Abstract

In order to build a model to predict accidents in a complicated man-machine sytem, human errors and mechanical reliability can be viewed as the most important factors. Such factors are explicitly included in a generic model. Another point to keep in mind is that the model should be constructed so that the data in a type of accident can be utilized to predict other types of accidents. Based on such a generic prediction model, we analyze the effects of system reliability. When we improve the system reliability, in other words, when there are changes in model parameters, the predicted time to next accidents should be modified influencing the effects of system reliability improvements. We apply Bayesian approach and finds the formula to explain how a change on the machine reliability or human error probability influences the time to next accident.

Introduction

A part of sensitivity analysis is to study the effects of a change of prior distributions on the prediction for next incidents in a safety system. This problem can receive an attention because our goal when we perform the safety analysis is not only in the prediction but also in the quantification and ultimately the reduction of the risk of future incidents by controlling the overall safety system. We may reduce the risk by upgrading the mechanical elements or by improving the human reliability through the training of operators or the improvement of working conditions,etc. Same amount of efforts devoted to improve the mechanical reliability of different sub-systems or human reliabilities may result in

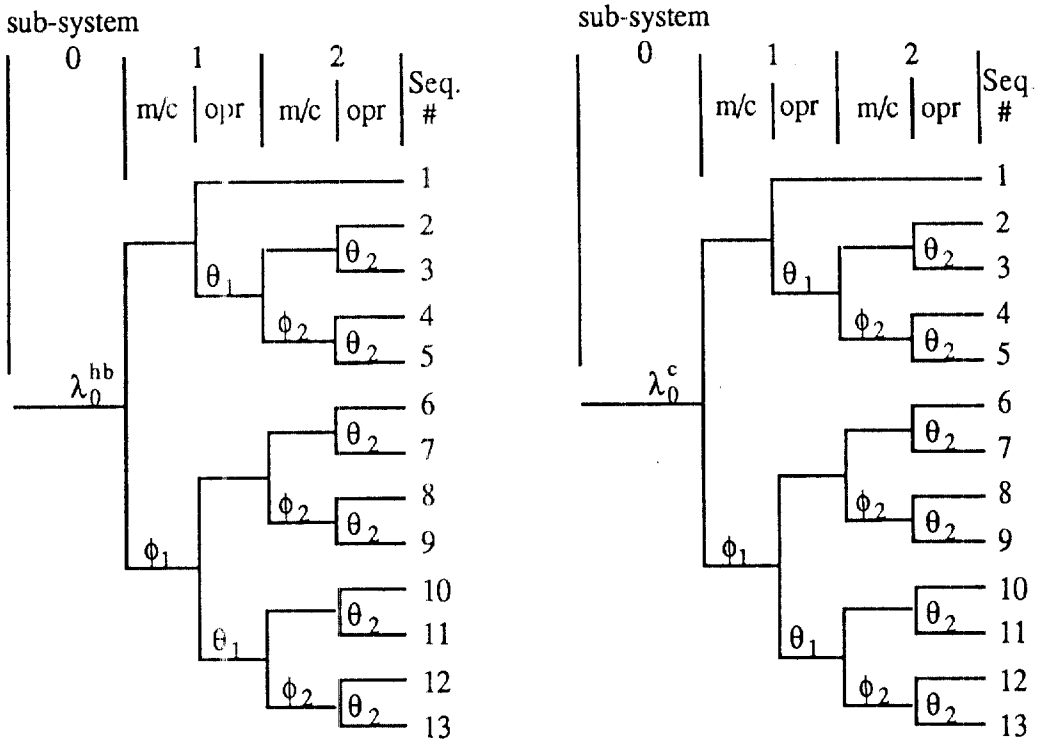
+ This research was supported by the fund of KOSEF.

different amount of risk reduction in terms of the forecasted time until next incident. Thus it is desirable to analyze how predictions respond to a change of model parameters.

In this paper we are firstly concerned with developing a generic model to describe the characteristics of the overall safety system. Among many factors that affect the safe operation of the whole system, human reliability and machine reliability, which are the most important, are explicitly included in a model so that their effects and interactions are analyzed. The concept of system reliability requires that a group of items that are organized to works together or towards a common goal work at designated times and under specified conditions. Human performance in a man-machine system can be viewed in the same light as any other elements in the system.

To study the progression of accident sequences in an organized and logical way, safety analyses use event trees to trace how various malfunctions or sub-system failures influence the accidents and the risks. The number of branches in an event tree depends on the number of sub-systems considered in a model, and the classification of incidents. The classification schemes are very subjective and rather arbitrary. In this paper, we classify the incidents to take care of two important points in modeling. One is the importance of human reliability when a safety system is considered as a large man-machine system; the other is the interaction between low and high severity incidents. To utilize the fact that one severity level incident may contain information helpful in predicting the other, we classify the incidents into different groups depending on their severity. For the sake of simplicity we start with three different severity groups: minor, significant, and severe incidents. And we introduce another classification of incidents: level 0, level 1, and level 2. Level 2 incidents consist of severe incidents, level 1 incidents consist of level 2 incidents and significant incidents, and level 0 incidents consist of level 1 incidents and minor incidents. Thus level 0 incidents include all precursors, level 1 incidents are a subset of level 0 incidents, and level 2 incidents are a subset of level 1 incidents.

Consider the event trees in figure 1. Each branch in the tree represents the operation or failure of a particular sub-system which is identified in the column heading; if the branch drops we have a failure of that sub-system, if the branch rises the sub-system is available or operates successfully. The number on each falling branch is the chance that the sub-system at the head of the column will fail; we refer to it as the branch parameter. λ_0^{hb} and λ_0^{c} denote the rate of level 0 incident initiated with operator errors and without operator errors, respectively. Figures 1(a) and (b) are event trees for a classification of three severity levels that show the accident sequences leading to various levels of severity from an



(a) Initiated Involving Operator Errors

(b) Initiated without Involving Operator Errors

〈 Figure 1 〉 Event Trees Showing the Interaction of Machine and Human

initiating incident involving operator errors and without involving operator errors, respectively. Each sub-system is composed of machines and operators. We assume that the probability of machine failures or operator errors is sequence independent. In other words, ϕ_j or θ_j is independent of the total counts passing through the upstream fork that has resulted from failures or successes of earlier sub-systems.

The top path indicates successful functioning of both the machines and operators of sub-system 1. Once sub-system 1 works successfully in mitigating the consequences of an initiated incident, the incident does not escalate further regardless of whether following sub-systems do or do not fail. If sub-system 1 fails, the incident escalates to either a significant or severe level. The paths of sequences 2, 6, and 10 denote the accident sequences in which the incident escalates to a significant level. Sequences 2, 6, and 10 correspond to the cases where the escalation to level 1 from an initiated incident is attributed to operator errors, machine failures, and both in sub-system 1, respectively, but the incident remains at significant level without further escalation because of a successful

operation of a following sub-system. The other sequences denote the various ways of leading to severe incidents.

We assume that branch parameters are independent of one another. Then counts passing through down branches can be assumed to be binomially distributed with parameters of total counts passing through upstream fork and corresponding branch parameters. In this case the sufficient statistics to update parameters are the total counts passing through down branches and sum of total counts passing through down and up branches corresponding to the same column [See Oliver, R. M. and Yang, H. J. (1990)]. Thus we do not have to keep track of all counts passing through all branches in figure 1. The use of this fact allows us to combine figure 1(a) and (b), and simplify it as in figure 2. The numbers under each branch denote counts passing through that branch.

We define the following notations for the counts passing through the branch:

$n_0^{hb}(T)$: number of level 0 incidents over a time period $(0, T)$ initiated involving operator errors

$n_0^{c}(T)$: number of level 0 incidents over a time period $(0, T)$ initiated without involving operator errors

$n_0(T)$: number of level 0 incidents over a time period $(0, T)$, $n_0^{hb}(T) + n_0^{c}(T)$

$n_j^{h}(T)$: number of level j incidents over a time period $(0, T)$ that involve operator errors only when escalating from level $j-1$

$n_j^{m}(T)$: number of level j incidents over a time period $(0, T)$ that involve machine failures only when escalating from level $j-1$

$n_j^{b}(T)$: number of level j incidents over a time period $(0, T)$ that involve both machine failures and operator errors when escalating from level $j-1$

$n_j^{mb}(T)$: number of level j incidents over a time period $(0, T)$ that involve machine failures when escalating from level $j-1$, $n_j^{m}(T) + n_j^{b}(T)$

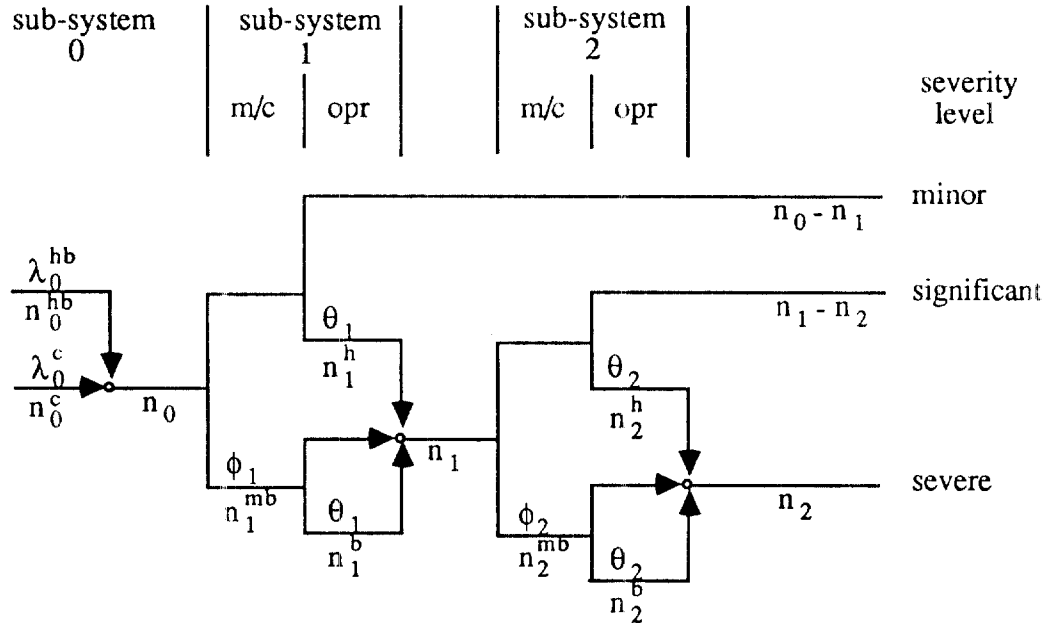
$n_j^{hb}(T)$: number of level j incidents over a time period $(0, T)$ that involve operators errors when escalating from level $j-1$, $n_j^{h}(T) + n_j^{b}(T)$

$n_j(T)$: number of level j incidents over a time period $(0, T)$, $n_j^{m}(T) + n_j^{h}(T) + n_j^{b}(T)$

Afterwards (T) is omitted for the sake of simplicity.

The arrows feeding into a small circle denote that the counts passing through each branch are summed there. Figure 2 carries as much information as figure 1 does, with respect to the parameter updating. To generally construct an event tree for a classification of more than three severity levels, a similar escalation process is repeated from the bottom sequence that resulted in a severe level in figure 2.

while the other two paths leading to minor and significant levels remain without further processes. An important feature of the event tree in figure 2 is that certain sub-systems can influence more than one accident sequence, in which case we have a "shared" branch parameter. We can see that the probability of operator errors influences two branches.



〈 Figure 2 〉 Reduced Event Tree of Figure 1

From the above event tree we can see that the rate of level 0 incident λ_0 is the sum of λ_0^{hb} and λ_0^c. The rate of level j, $j = 1, 2$, incident is obtained by

$$\lambda_j = \lambda_{j-1}(\phi_j + \theta_j - \phi_j\theta_j)$$

We assume that the number of incidents given parameter λ follow Poisson distribution, and the likelihood of counts passing through down branches are Binomial conditional on parameters and total counts passing through upstream forks,

We assume Gamma priors for λ_0^h and λ_0^c with paremeter $(\alpha_0^{hb}, \beta_0^{hb})$, and, (α_0^c, β_0^c). The rationale of using Gamma distributions is that a safety system provided with many redundancies tend to bunch up towards the low probability of failure, while it still has a long tail to the high probability region. And the assumption of Beta priors for ϕ_j and θ_j, $j = 1, 2$ can be justified because beta distribution is quite flexible

covering almost all forms of distributions between 0 and 1. Then the distribution of λ_0 can be approximated as another Gamma distribution for the case of β_0^{hh} and β_0^c are similar. We can not expect similar values of β at the beginning stage of prediction, but as time goes on the posterior value of β is modified by adding the amount of time elapse so the effects of the difference between posterior values of β_0^{hh} and β_0^c are negligible. Thus we approximate that the rate of level 0 incident is described by a Gamma distribution with parameters of (α_0, β_0), where $\alpha_0 = \alpha_0^{hh} + \alpha_0^c$, $\beta_0 = (\beta_0^{hh} + \beta_0^c)/2$. The rates of level j incident can be obtained by numerical integrations, but thet can also be approximated as closed form distributions using the fact that $(\phi_j + \theta_j - \phi_j\theta_j)$ follows much narrower distribution than that of λ_{j-1}. In this case $(\phi_j + \theta_j - \phi_j\theta_j)$ behaves like a constant and λ_j can be approximated as another Gamma distribution with parameters (α_j, β_j), where

$$\alpha_j = \frac{\alpha_{j-1}\mu_j^2}{(\alpha_{j-1}+1)\sigma_j^2 + \mu_j^2}, \qquad \beta_j = \frac{\beta_{j-1}\mu_j}{(\alpha_{j-1}+1)\sigma_j^2 + \mu_j^2}$$

and

$$\mu_j = \mathrm{E}[\phi_j + \theta_j - \phi_j\theta_j], \text{ and } \sigma_j^2 = \mathrm{Var}[\phi_j + \theta_j - \phi_j\theta_j].$$

For more details about approximation method, see Heejoong Yang(1990).
Here we let $\pi_j = \phi_j + \theta_j - \phi_j\theta_j$, $j = 1, 2$, denote the escalation probability from level $j-1$ to level j incidents. To proceed we adopt the following additional assumptions;

A1 : Distributions of λ_j, $j = 0, 1, 2$, still remain as Gamma after a change on model parameters

A2 : $\mathrm{Var}[\lambda_0]$ is unaffected by a change on model parameters

A3 : Variance of escalation probabilities, $\mathrm{Var}[\phi_j + \theta_j - \phi_j\theta_j] = \mathrm{Var}[\pi_j]$, $j = 1, 2$, is unaffected by a change on model parameters.

Let prime(′) denote modified parameters by a system reliability improvement and $\delta\lambda_0^{hh}$, $\delta\lambda_0^c$ denote the net amount of reduction on λ_0^{hh} and λ_0^c, respectively. Also let $\delta\phi_j$ and $\delta\theta_j$, $j = 1, 2$, denote net the amount of reduction on ϕ_j and θ_j. Then by A1, λ_0' still follows Gamma distribution with parameters α_0' and β_0'. α_0' and β_0' are obtained as following based on A2.

$$\beta_0' = \frac{E[\lambda_0^{h'}] + E[\lambda_0^{c}] - \{E[\delta\lambda_0^{h'}] + E[\delta\lambda_0^{c}]\}}{Var[\lambda_0]}, \quad \alpha_0' = (\beta_0')^2 \, \mathrm{Var}[\lambda_0]$$

Then using the assumption in section 5.3, $\lambda_1' = \lambda_0' \pi_1'$ follows Gamma distribution with parameters α_0' and β_0', where π_1' is expressed as following;

$$\pi_1' = \phi_1' + \theta_1' - \phi_1'\theta_1' - (1-\phi_1')\delta\theta_1' - (1-\theta_1')\delta\phi_1' - \delta\phi_1'\delta\theta_1'$$

Due to A3, the variance of π_1' is assumed to be σ_1^2 as the original variance, but the mean value is modified and obtained by

$$\begin{aligned}\mu_1' &= \mathrm{E}[\phi_1' + \theta_1' - \phi_1'\theta_1' - (1-\phi_1')\delta\theta_1' - (1-\theta_1')\delta\phi_1' - \delta\phi_1'\delta\theta_1'] \\ &= \mu_1 - (1-\mathrm{E}[\phi_1])\mathrm{E}[\delta\theta_1] - (1-\mathrm{E}[\theta_1])\mathrm{E}[\delta\phi_1] - \mathrm{E}[\delta\phi_1]\mathrm{E}[\delta\theta_1]\end{aligned}$$

Then α_1' and β_1' are obtained by

$$\alpha_1' = \frac{\alpha_0'(\mu_1')^2}{(\alpha_0'+1)\sigma_1^2 + (\mu_1')^2}, \qquad \beta_1' = \frac{\beta_0'\mu_1'}{(\alpha_0'+1)\sigma_1^2 + (\mu_1')^2}$$

Similarly $\lambda_2' = \lambda_1'\tau_2'$ follows Gamma distribution with parameters α_2' and β' where

$$\pi_2' = \phi_2' + \theta_2' - \phi_2'\theta_2' - (1-\phi_2')\delta\theta_2' - (1-\theta_2')\delta\phi_2' - \delta\phi_2'\delta\theta_2'$$

$$\mu_2' = \mathrm{E}[\pi_2'] = \mu_2 - (1-\mathrm{E}[\phi_2])\mathrm{E}[\delta\theta_2] - (1-\mathrm{E}[\theta_2])\mathrm{E}[\delta\phi_2] - \mathrm{E}[\delta\phi_2]\mathrm{E}[\delta\theta_2]$$

and

$$\alpha_2' = \frac{\alpha_1'(\mu_2')^2}{(\alpha_1'+1)\sigma_2^2 + (\mu_2')^2}, \qquad \beta_2' = \frac{\beta_1'\mu_2'}{(\alpha_1'+1)\sigma_2^2 + (\mu_2')^2}$$

If we let

$$p = \text{Prob. \{time to next incident} \le z_p\}$$

Then z_p denotes quantiles where $z_{0.5}$ denotes a median. The Gamma prior and Poisson likelihood again simplify the equation for quantiles in a closed form as following;

$$z_p = \beta_2\{(\frac{1}{1-p})^{1/\alpha_2} - 1\}$$

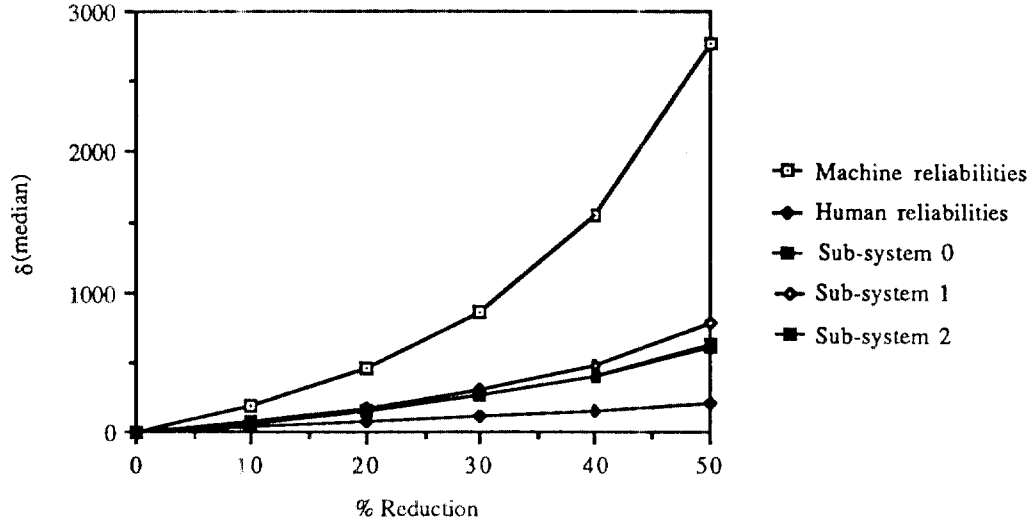
Then the amount of future risk reduction in terms of the increase of the median time to next severe incident is obtained by

$$\text{Amount of risk reduction} = \delta(\text{median}) = \beta_2'(2^{1/\alpha_2'} - 1) - \beta_2(2^{1/\alpha_2} - 1)$$

Figure 3 shows the net amount of increase of the median time to next severe incident as a function of % reduction on model parameters. In this example we have assumed the following distributions for model parameters, which were used to predict nuclear power plant accidents in U.S.A. in Yang(1989);

$$\lambda_0 \sim G(111, 214), \qquad \pi_1 \sim Be(6, 171), \qquad \pi_2 \sim Be(4, 69)$$

It can be seen that the improvement on machine reliabilities results in more risk reduction than on human reliabilities, and there is not much difference among the risk reduction on different sub-systems. But it should be noted that the horizontal axis is % reduction where the related cost is not considered since the data of which is not available. Thus at this moment we can not make a conclusion that the improvement of machine reliabilities is a better choice than the improvement of human reliabilities. The decision should be made considering the cost required. For the future research, if cost factors necessary for each improvement is available and thus equi-cost lines can be overdrawn on figure 3, we can choose the option that gives the most risk reduction on each equi-cost line.



〈 Figure 3 〉 Increase on Median Time vs. Improvement on Reliability

Sumamry

The overall safety system reliability can be improved by various means such as upgrading machines, training operators, and improving working conditions, etc. If we have limited amount of resources to be used for the improvement of the system reliability we have to determine how much resources should be allocated on what sub-systems to efficiently improve the overall safety. Thus it is essential to have the idea about the behavior of future risk reduction as the model parameters are modified. We apply Bayesian approach and finds the formula to explain how a change on the reliability on human or machine part influences the time to next accident.

References

[1] Apostolakis, G., and Mosleh, A. (1979a), "Expert Opinion and Statistical Evidence: An Application to Reactor Core Melt Frequency," *Nuclear Science and Engineering*, Vol. 70, pp. 135-149.

[2] Aitchison, J., and Dunsmore, I. R. (1975), *Statistical Prediction Analysis*, Cambridge University Press

[3] Cheney, W., and Kincaid, D. (1980), *Numerical Mathematics and Computing*, Brooks/Cole Publishing Company, Monterey, California

[4] Chow, T. C., and Oliver, R, M. (1988a), "Predicting Nuclear Incidents," *Jour. of For*, Vol. 7, pp. 49-61.

[5] DeGroot, M. H. (1970), *Optimal Statistical Decision*, McGtaw-Hill Book Company.

[6] Groer, P. C. (1984), "Bayesian Estimates for The Rate of Three Mile Island Type Releases" *Low Probability High-Consequence Risk Analysis*, pp. 127-136. Ed. by Waller and Covello, Plenum Publishing, New York.

[7] LeVan, W. I. (1960), "Analysis of the Human Error Problem in the Field," *Bell Aerosystems Company*, Report No. 7-60-932004

[8] Lewis, H. W. (1984), "Bayesian Estimation of Core-Melt Probability" *Nuclear Science and Engineering*: Vol. 86, pp. 111-112.

[9] Mills, R. G., and Hatfield, S. A. (1974), "Sequential Task Performance: Task Module Relationships, Reliabilities, and Times," *Human Factors*, pp. 117-128.

[10] Oliver, R. M., and Yang, H. J. (1990), "Updating Event Tree Parameters to Predict High Risk Incidents," *Influence Diagrams, Belief Nets and Decision Analysis*, edited by R. M. Oliver and J. Q. Smith, Chap. 12, pp. 277-296.

[11] Shachter, Ross D. (1987), "Evaluating Influence Diagrams" *Operations Research* Vol. 34, No. 26, pp. 871-882.

[12] Smith, J. Q. (1987), "Diagrams of Influence in Statistical Models" *Department of Statistics*. University of Warwick, Research Report 99, Coventry, U.K.

[13] Yang, Heejoong (1989), "The Influence of Himan Errors on Nuclear Incidents," *Thesis for Doctor of Engineering*, University of California, Berkeley

[14] Yang, Heejoong (1990), "An Approximation Method in Bayesian Prediction of Nuclear Power Plant Accidents," *Journal of the Korean Institute of Industrial Engineers*, Vol. 16, No. 2.