Analysis of the Effects of Subsystem Improvements on the Total System Safety

Hee-Joong Yang*
*Dept. of Industrial Engineering, Cheongju University

하부시스템의 안전도 개선이 전체 시스템 안전도에 미치는 영향 분석

양 희 중*
*청주대학교 산업공학과

Abstract

본 논문에서는 하부 안전 시스템의 개선이 전체 안전 시스템에 미치는 영향을 분석하기 위한 방법론을 개발하였다. 어느 하부 시스템의 안전성을 개선하느냐에 따라 전체 시스템의 안전성 증가는 서로 다르게 나타날 수도 있다. 본 연구에서는 베이지안 기법을 활용하여 사건가지와 상호연관도를 응용한 모형을 활용하였다. 또한 가지 파라메터의 확률값 향상이 다음 번 사고까지의 시간을 어떻게 변화시키는지 연구하였다. 본 연구를 통해 우리가 관심을 갖고 있는 시스템 전체의 안전성 향상을 위해서는 어느 하부 시스템을 우선적으로 개선해야할지를 판단할 수 있게 한다.

Keywords : sensitivity analysis, safety systems, bayesian approach, event trees, fault trees, influence diagrams

1. Introduction

Event tree models are widely adopted in describing the accident sequences in safety analysis of large safety systems such as huge chemical plants, nuclear power plants, and so on [3, 4, 6]. Branch parameters are assigned to each branch of event trees for further statistical analysis. The assessment of branch parameters are usually based on fault tree analysis and the top parameter of fault trees becomes a branch parameter of an event tree [2, 5, 7, 9].

Cohen[6], and Rasmussen[7] vastly utilized event trees and fault trees in describing accident initiation and escalating to more severe accidents. Cadwallader[5] and U.S. nuclear regulatory commission[9] also adopted probabilistic risk assessment where fault trees and event trees performed major roles. Although the wide usage of fault trees and event trees, there are several drawbacks. While it gives an idea about how an accident occurs and escalates to a more severe accident, it does not say anything about dependency and independency among branch probabilities. All counts passing through each branch is conditioned on the arrival of initiating event. So many important observations such as the number of system failure during testing are not included even though they are as much helpful as the informations contained in a event tree to update branch parameters and predict future accidents. Many important informations are lost since a branch does not further divides if success of failure of following sub-systems does not affect the severity of accident. Since event trees are constructed for specific plants separately it is hard to see the relationship between parameters of different plants.

† 이 논문은 2010-2012 학년도에 청주대학교 산업과학연구소가 지원한 학술연구조성비(특별연구과제)에 의해 연구되었음.

† 교신저자: 양희중, 충북 청주시 상당구 내덕동 36 청주대학교 산업정보시스템공학과
M・P: 019-456-8188, E-mail: hjyang@cju.ac.kr

2010년 7월 2일 접수; 2010년 8월 18일 수정본 접수; 2010년 8월 25일 게재확정

To summarize, most of the previous works concentrated on modeling with separate event trees that resulted in independent models so that we cannot share information contained in similar types of accidents. To overcome such drawbacks we use influence diagram models that depicts the accident initiation and escalation to more severe accidents [1, 8].

Also most of the researches related to forecasting made a conclusion with suggested forecasting models. But sometimes we want beyond obtaining the forecasting models. In real situations, we always try to upgrade the safety system, so we are often interested in figuring out how efficient we are in the safety improvement efforts.

In this paper we focus on the next stage of forecasting. We want to analyze the effects of change of prior distribution on the prediction for next accidents. This problem can receive an attention because our interests in the safety analysis may not stop at the point of predicting the next accident but reach to the point of controlling the safety system to reduce the risk of accident efficiently utilizing a prediction. We can control the safety system by upgrading the mechanical elements or training operators if human factors are significant in running the system successfully. Such activities requires resources, especially time and budget. Same amount of upgrade in each sub-system may results in different amount of change in prediction so it is an efficient way to give efforts to improve the sub-system which is most sensitive. Therefore we need to assign our limited resources efficiently. Improvement on what sub-system results in the most risk reduction? To answer the above question, we need to know how the improvement of each sub-system influences to overall safety system. In this paper, we analyze the amount of change on forecasted time to next accident as a function of change of branch parameters.

As a methodology we adopt bayesian approach.

Rather than just getting the future accident rate, we want to get a whole distribution of predicted time to next accident. Therefore bayesian approach can achieve such requirements much better than classical approach.

2. Analysis of a system with one branch

Let's consider, in figure 1, the simple example to predict the time to next initiating accident under the assumption that arrival rate of initiating event, l, has a gamma distribution with parameters a and b, and the number of initiating accident by time T given l has a poisson distribution with lT. Such distributional assumptions on prior and likelihood have been prooved to be appropriate in forecasting accidents[10].

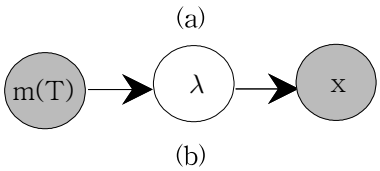
Figure 1(a) is an event tree model and 1(b) is a corresponding influence diagram model that is statistically equivalent. Let's define the sub-system which is responsible for the initiating accident as sub-system 0. The time until next accident, X0, given the arrival rate is exponentially distributed with l.

At time T, we update parameters using observed data m(T), where m(T) is number of initiating accidents in time interval (0, T). Then the parameters of posterior distribution, l, becomes a′=a+m(T), and b′=b+T.

Then the point prediction for the time until next accident is obtained by

$$E[X_0|m(T)] = \frac{\Gamma(\alpha'-1)\beta'}{\Gamma(\alpha')} = \frac{\beta'}{\alpha'-1} \qquad (1a)$$

$$\frac{\lambda}{\quad} \; m(T)$$



<Figure 1> An event tree and influence diagram model that has one sub-system

$$Var[X_0|m(T)] = \frac{\alpha'(\beta')^2}{(\alpha'-1)^2(\alpha'-2)} \qquad (1b)$$

In the above equations, we assumed integer value of gamma parameter, which can be accepted most of the time since time unit and number of accidents are increased by integers.

If the posterior distribution can be modified by controlling various factors that influence occurrence

of initiating event as that the modified posterior distribution has the parameter a*=a′+da′, and b*= b′+db′, we want to analyze the effects of da′ and db′ on the prediction to next accident.

Let kE0 and kV0 are ratios of modified and original distributions for expected value and variance of model parameter l′, respectively. Then by solving

$$\frac{\alpha^*}{\beta^*} = \frac{\alpha' + \delta\alpha'}{\beta' + \delta\beta'} = k_{E0}\frac{\alpha'}{\beta'} \quad (2a)$$

$$\frac{\alpha^*}{(\beta^*)^2} = \frac{\alpha' + \delta\alpha'}{(\beta' + \delta\beta')^2} = k_{V0}\frac{\alpha'}{(\beta')^2} \quad (2b)$$

We obtain a* and b* as a function of kE0 and kV0 as following;

$$\alpha^* = \frac{k_{E0}^2}{k_{V0}^2}\alpha \quad (3a)$$

$$\beta^* = \frac{k_{E0}}{k_{V0}}\beta \quad (3b)$$

We can analyze the combined effects of kE0 and kV0 on the net change in the predicted time until next accident;

$$\delta E[X_0|m(T)] = E[X_0^*|m(T)] - E[X_0|m(T)]$$

where X0* is the time until next accident under the modified system. By substituting equation (3) into (1a) we obtain

$$E[X_0^*|m(T)] = \frac{k_{E0}\beta'}{k_{E0}^2\alpha' - k_{V0}} \quad (4)$$

So for large a′, which is the case after we have observed many initiating accidents, kE02a′ is dominating in the denominator of equation (4) and the prediction becomes insensitive to the change of kV0. In most cases kV0 remains as 1 after the system improvement, that makes the above statement valid. In this case equation (4) can be approximated as

$$E[X_0^*|m(T)] = \frac{\beta'}{k_{E0}\alpha'} \quad (5)$$

Therefore when we have observed many initiating accidents up to time, that makes a′ large, and achieve only small amount of improvement on the system, the net increase on the predicted time is approximately proportional to the reciprocal of kE0.

To see the effects of variance of the arrival rate of initiating event on the variance of predicted time, we obtain the following equation from equation (1b) and (3)

$$Var[X_0^*|m(T)] = \frac{\alpha^*(\beta^*)^2}{(\alpha^*-1)^2(\alpha^*-2)}$$

$$= \frac{(\frac{k_{E0}}{k_{V0}}\alpha')(\frac{k_{E0}^2}{k_{V0}}\beta')^2}{(\frac{k_{E0}^2}{k_{V0}}\alpha' - 1)^2(\frac{k_{E0}^2}{k_{V0}}\alpha' - 2)} \quad (6)$$

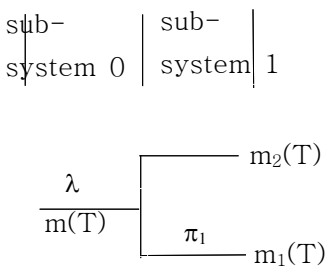
We can see that for large a′ the variance of time to next accident under modified system is proportional to the value of kV.

3. Analysis of a system with two branches

Now let's consider an extended case that has a sub-branch as in figure 2. Most of the works related to forecasting made conclusions suggesting better models for forecasting. But as we mentioned in the introduction, we usually keep trying to improve the safety of whole system in various ways and want to evaluated our works for safety improvement.

Upgrading the safety system is equivalent to modify the distribution of model parameters.

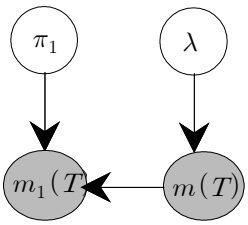
Let kE1 and kV1 be the ratios of the modified and the original distributions for expected value and variance corresponding to sub-branch parameter.



<Figure 2> Event tree with two branches

In figure 2, m(T)=m1(T)+m2(T) is the total number of initiating accidents, and m1(T) is the number of accidents that escalates to more severe level. The branch parameter p1 is the probability of escalating to more severe accident.

The event tree in figure 2 can be converted to a statistically equivalent influence diagram as in figure 3, where p1 is assumed to have a beta distribution with parameters a and b.



<Figure 3> An influence diagram model

The beta assumption on branch parameters is generally accepted because beta distribution is very flexible that covers almost all forms of distributions between 0 and 1. Then we can set the following equations;

$$\frac{a^*}{a^*+b^*} = k_{E1}\frac{a'}{a'+b'} \tag{7a}$$

$$\frac{a^*b^*}{(a^*+b^*)^2(a^*+b^*+1)} = k_{V1}\frac{a'b'}{(a'+b')^2(a'+b'+1)} \tag{7b}$$

Where a′= a+m1(T), b′=b+m(T)−m1(T) are the parameters of the posterior distribution at time T and a*=a′+da′, and b*=b′+db′ are the parameters of the modified distribution that represents the improved sub-system 1. From (7a) and (7b), we obtain a* and b* as followings;

$$a^* = \frac{(a'+b')^2\,(a'+b'+1)y - x - 2xy - xy^2}{x + 3xy + 3xy^2 + xy^3}$$

$$b^* = a^* y \tag{8}$$

where

$$x = k_{V1}a'b'$$

$$y = \frac{(1-k_{E1})a' + b'}{a'k_{E1}}$$

The predicted time to a more severe accident, X1, depends on kE0, kE1, and kV1. In other words it depends on how much we improve the sub-system 0 and sub-system 1 and how much confidence we have on the assessed distributions.

The point predictor of X1 is obtained by

$$E[X_1|m_1(T), m_2(T)] = \frac{\beta'}{\alpha'-1}\frac{a'+b'-1}{a'-1} \tag{9}$$

The point predictor of X1* under the modified system can be obtained by replacing ′ with * using equation (3) and (8);

$$E[X_1^*|m_1(T), m_2(T)] = \frac{k_{E0}\beta'}{k_{E0}^2\alpha' - k_V}\frac{a^*+a^*y-1}{a^*-1} \tag{10}$$

We may want to see how the improvements on different systems affect the prediction. When a* is large, the second term of right hand side of equation (10),

$\frac{a^*+a^*y-1}{a^*-1}$, can be approximated as

$$1+y = \frac{a'+b'}{a'}\frac{1}{k_{E1}}$$

Therefore for the large a′ and a*, the equation (10) is reduced to

$$E[X_1^*|D] \cong \left(\frac{\beta'}{\alpha'}\frac{1}{k_{E0}}\right)\left(\frac{a'+b'}{a'}\frac{1}{k_{E1}}\right) = \left(\frac{1}{E[\lambda|D]}\frac{1}{k_{E0}}\right)\left(\frac{1}{E[\pi|D]}\frac{1}{k_{E1}}\right) \tag{11}$$

where D denotes the observed data set.

We can see that the predicted time is proportional to the reciprocal of kE0 of kE1 and the same pro-

portion of improvement on different sub-systems results in the same amount of increase in the predicted time. Even though this approximation gives us the idea about how the predicted time will be influenced by the improvement of sub-systems, it should be kept in mind that this approximation can be applied only when the above mentioned conditions are satisfied.

Once we carefully examine the above equations, we can see that for the range of large kE, there is not much difference between which sub-system we are improving, but as kE decreases the resulting a* becomes small and the approximation of equation (11) is not valid any more. Therefore the amount of increase on the predicted time hardly depends on what sub-system we are improving when we improve it only a little, but when we improve substantially it is better to put the effort on sub-system 1.

Based on the results in this section, we can wisely choose the best way to increase safety level of whole system. Sometimes it may cost about same amount of money to upgrade sub-system 1 or 2.

But the amount of improved safety in terms of time to next accident may differ. Therefore it is strongly suggested to analyze the safety system first whether the approximation in equation (11) can be applied. Based on it, if it is the case where selected sub-system for the improvement does not affect the amount of whole safety improvement, we had better choose the one that needs less budget and effort.

But if it is the case where the selected sub-system differs the whole safety improvement, it is better to choose sub-system 1 only as the first priority to improve.

4. Conclusion

The forecasting model is extended to see the impact on safety system improvements. The efforts of system improvements results in the change of posterior distribution parameters. Such a change is expressed in terms of time to next accident. It has proved that when we improve only a little there is not much difference whether we put efforts on sub-system 0 or 1. But when we improve substantially it is suggested to improve sub-system 1.

Obviously Gamma distribution is a conjugate prior of Poisson distribution and Beta distribution is a conjugate prior of Binomial distribution, and such assumptions on prior make many calculations related with obtaining posterior distribution simple. But there can be situations that do not allow such assumptions on likelihoods and in such cases the calculations become extremely complicated and time consuming since they need multi-dimensional numerical integrations.

Even there remains difficulties in calculations, it is at least theoretically possible to release the above distributional assumptions. To find a method to solve a real problem without distributional assumptions is a topic that should be solved in near future. Also it may be studied 세택to find the way to extend this model to explain a system with multi branches.

5. References

[1] Aitchison, I.R., and Dunsmore, "Statistical Prediction Analysis", Cambridge University Press, (1975)

[2] Bernard Cohen, "Probablilistic Risk Assessement of Wastes Burried in the Ground", Risk Anlaysis, Vol.3, No.4 (1983), : 237-243

[3] Briones, J.F. et al, "Integration of Safety Analysis and Software Development Methods", Systems Safety, The 1st Institution of Engineering and Technology International Conference (2006) : 275-284

[4] Bruske, S.Z and Holland, D.F.,"Risk Assessment Technology for the Evaluation of Tritium Accident Mitigation", Nuclear Technology Fusion, 4 (1983) : 539-543

[5] Cadwallader, L.C. et al ,"A Comparison of U.S. and European Methods for Accident Senario Identification, Selection, and Quantification", Fusion Engineering, Proceedings IEEE 13th Symposium, (1989): 304-311

[6] Cohan, Faisal et al. "A New Methodology for Safety Management Based on Feedback from Credible Accident-Probabilistic Fault Tree Analysis System", Journal of Hazardous Materials, 87, No.1 (2002) : 23-36

[7] Rasmussen,N.C., "Method of Hazard Analysis and Nuclear Safety Engineering" Annals New York Academy of Science, (1981) : 20-36

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

[9] U.S. Nuclear Regulatory Commission, "Reactor Risk Reference Document", Office of Nuclear Regulatory Research, NUREG-1150, (1987) : 1-3
[10] Yang, Heejoong, "Approximation Method in Bayesian Prediction of Nuclear Power Plant Accidents", 한국산업공학회지,16, No.21, (1990) : 135-147
[11] Yang, Heejoong, "Forecasting Accidents by Transforming Event Trees into Influence Diagrams", 산업경영시스템학회지, 29, No.1 (2006) : 72-75

저 자 소 개

양 희 중

서울대학교를 졸업하고 Univ. of Texas at Arlington 에서 산업공학 석사, University of California, Berkeley에서 산업공학박사를 받았다. 1996-1997에 Naval Post graduate School에서 방문교수로 활동하였으며 현재 청주대학교 산업공학과 교수로 재직 중이다. 주요 관심분야는 품질경영과 안전 사고 예측이다.
주소: 충북 청주시 상당구 내덕동 36 청주대학교 산업공학과