This article is part of the IEEE Reliability Society 2007 Annual Technology Report.

Accident Analysis of Complex Systems Based on System Control for Safety

Takehisa Kohda
Kyoto University
Email: kohda@kuaero.kyoto-u.ac.jp

Dr. Takehisa Kohda presents how to apply the system control concept in accident analysis of complex systems based on his research result: T. Kohda: Accident Analysis of Complex Systems Based on System Control for Safety, to appear in *Handbook of Performability Engineering* (Edited by Krishna B. Misra), Springer, 2008.

This research applies a concept of system control for safety to the accident analysis in two ways. The first part deals with accident cause analysis, while the second part deals with the accident analysis in the defense-in-depth approach. The summary is shown below. For the detail, please refer to the corresponding chapter in the above book or contact with Dr. Kohda (E-mail: kohda@kuaero.kyoto-u.ac.jp).

The accident analysis plays an important role in both the accident investigation and risk assessment for effective risk/safety management. An accident model plays a fundamental role in the identification of accident causes. The depth or resolution of an analysis depends on its accident model. One conventional accident model is an event-based (or sequential) model, such as Event Trees [1], where the system accident is the end state of a cause-effect sequence initiating from a deviation caused by a component failure, human error or external disturbance. However, the remarkable progress in computers and information technology makes interactions among system components so complex that a new type of accident appears, namely, a deviation not corresponding to a fault can lead to an accident even though components behaves as they are specified. This accident is called a systemic accident. Further, since one of main accident contributors, human errors, is greatly affected by organizational and management factors, the background factors of both human errors and component failure must be considered to devise effective countermeasures. Unfortunately, the event-based model cannot address these problems properly, because it stops the identification process of system accident causes at the component failure level. Root causes are rarely identified. To meet the demands in this situation, a system accident cause analysis method based on the concept of system control for safety [2,3] are devised. The same kind of method [4] is applied to the accident analysis of an accident in the railways [5]. By investigating causes of malfunction systematically according to the system hierarchical control structure from the operating process where a system accident occurs to the top level such as management department of a company, background factors of a proximal accident cause can be identified as dysfunction of control loops at upper levels. Additional studies are being planned to improve and extend the proposed method by applying it to more practical problems such as development of prevention measure against system accidents from the viewpoint of system control for safety.

In PRA (Probabilistic Risk Assessment) [1], the derivation of accident occurrence conditions is the most important part, whose correctness determines the validity of analysis results. However, this derivation conventionally depends on the subjective judgment of system analysts and designers, which might cause an error. To obtain an objective accident occurrence condition, the concept of “safety control functions” is applied to not only the derivation of accident occurrence conditions in an event tree model for a specific disturbance or initiating event, but also the analysis of their failure conditions. An illustrative example of a collision accident in a single track railway is given to show the applicability and effectiveness of the proposed method [6]. The

decomposition of a safety control function into detection, diagnosis and execution functions can simplify not only the identification of safety control functions related to a disturbance or initiating event, but also the derivation of their failure conditions including hardware failure and human errors. Safety devices and safety actions by human operators can be combined into a safety control system, which can perform a safety control function as a whole in an accident sequence. To devise an effective countermeasure, the proposed method can consider not only the cognitive aspects of human actions in a safety control function, but also the role of each component in the overall system safety control function. Depending on the initial condition when a disturbance occurs, event sequences leading to the accident can be easily modified by identifying effective safety control systems. Though the qualitative analysis is discussed to derive system accident occurrence conditions, the quantitative analysis is the next step in this research.

References:

[1] NASA, Probabilistic Risk Assessment Procedure Guide for NASA Managers and Practitioners, Ver. 1.1, NASA, 2002.
[2] J. Rasmussen, Major Accident Prevention: What is the Basic Research Issue? Proc.1998 ESREL Safety and Reliability Conf., pp. 739-740, 1998.
[3] N. Leveson, A New Accident Model for Engineering Safer Systems, Safety Science 42, pp. 237-270, 2004.
[4] T. Kohda, Y. Takagi, Accident Cause Analysis using of Complex Systems Based on Safety Control Functions, Proc. Annual Reliability and Maintainability Symp. (CD-ROM), 2006.
[5] T. Kohda, G. Adachi, Accident Cause Analysis based on System Control Function, Proc. Safety Engineering Symposium 2006, pp. 115-118, 2006. (in Japanese)
[6] Kohda, T., Fujihara, H., Accident Occurrence Conditions in Railway Systems, International Journal of Performability Engineering, Vol. 3, No. 1, Part II, pp. 105 – 116, 2007. http://www.ijpe-online.com/html/ past_issues.html