DYNAMIC FAULT ANALYSIS OF LARGE-SCALED INFORMATION SYSTEMS WITH REFERENCE TO COMPONET'S DETERIORATION

Kazuya AOKI[1], Koji YAMAMOTO[2], Kiyoyuki KAITO[3], Kiyoshi KOBAYASHI[4]

ABSTRACT. This study proposed the optimal replacement policy of large-scaled information systems based upon dynamic fault analysis. The renewal processes of the equipment of the systems are described by use of Weibull hazard models to estimate the dynamic fault generation probabilities of the equipments, and the fault tree model is formulated to analyze the magnitude of the system inoperability. The reliability of the information systems and the expected repair/maintenance cost are estimated by Monte Carlo simulation models. The loss of the reliability of the information system is represented by risk index and the methodology to analyze the relation of life cycle cost and risk is presented. This paper also addresses the practical availability of the proposed methodology through a case study dealing with the traffic control systems for an expressway using the actual fault generation data in the past.

INTRODUCTION

For the purpose of operational efficacy and rapid information services for users, infrastructure facilities including civil structures are equipped with monitoring sensors and information processing/output devices, and information is transferred over the network. What should be noted therefore with regard to the asset management of information systems are 1) a system has a complicated hierarchical structure comprised of an enormous amount of components, 2) that a failure in the lowest layer of the hierarchical structure may affect the whole systems, and 3) that the reliability of the whole systems may change dynamically due to a progressive deterioration of a component.

There have been a number of fault analysis of large-scaled systems including fault tree analysis (FTA) (Bedford, 2001), and emphasis has been mainly placed upon the static analysis of the possibility that a failure in a component or a subsystem may affect the whole

[1] Assistant Manager, R & D Center, PASCO CORPORATION, Tokyo, Japan, e-mail: kazuya_aoki@pasco.co.jp
[2] Sub-Chief Engineer, Facilities Development Management Team, Yokohama Regional Office, Central Nippon Expressway Co.Ltd., Yokohama, Japan, e-mail: k.yamamoto.af@c-nexco.co.jp
[3] Assoc. Prof., Frontier Research Center, Osaka University, Japan, e-mail:kaito@ga.eng.osaka-u.ac.jp
[4] Prof., Graduate School of Management, Kyoto University, Japan, e-mail: kkoba@psa.mbox.media.kyoto-u.ac.jp

systems. A system is composed of an enormous amount of components, in which failures are divided into accidental failures and wear-out failures. Especially, wear-out failures are attributable to a deterioration of components or equipment. Accordingly, as the in-service period after systems renewal gets longer, the possibility of failure occurrence increases. And consequently, the probability of failure occurrence in the whole systems increases with time. That is why a dynamic failure analysis is required of the whole large-scaled infromation systems.

In this study, the temporal changes of failure probability in components of information systems will be modeled with hazard models (Aoki *et al*, 2007; Lancaster, 1990; Tsuda *et al*, 2006). On the other hand, failure events of the whole systems will be expressed using fault tree diagrams and a method for analyzing the temporal changes of failure probability in the whole systems according to the temporal changes of failure probability in the components will be proposed. Generally, it is important for the asset management of information systems to plan and develop strategies for renewing the information systems and key parameters for the planning are the total of renewal costs and maintenance costs (life cycle costs) and failure probability. When a failure is detected during the system maintenance, the component is immediately replaced by the new one. If a certain time has passed since the system was installed, the components may be out of stock or technical support may take some time, and consequently the repair costs will increase. In addition, it may take a longer time to recover the system and then the failure will have a greater effect on society. In this study, therefore, the social effect will be also considered as a parameter in addition to the above-mentioned life cycle costs and failure probability in mapping out strategies for renewing the systems.

For these purposes, this study formulates dynamic fault analysis models of large-scaled information systems and proposes a method for analyzing dynamic changes in expected life cycle costs and the social effect by using Monte Carlo simulation models. In addition, an empirical study of actual traffic control systems is conducted.

BASIC IDEAS OF THIS STUDY

Issues on Asset Management of Information Systems

For asset management of large-scaled information systems like a traffic control system, it is indispensable to consider the structural and functional complexity of the systems. The asset management is implemented at three levels: 1) component level, 2) system level, and 3) function level. This study focuses on system-level and function-level asset management. With regard to component-level asset management, the authors have already carried out an analysis of failure probability of each system component and its temporal changes by using random proportional Weibull hazard models (Kaito *et al*, 2008). With regard to system-level asset management in this study, failure probability in subsystems and components are analyzed and maintenance strategies of each subsystem and component are examined in light of the serious effect of the functional failure of the whole systems. Specifically, failure analysis is conducted on subsystems and the whole systems with the aid of the failure analysis models used in component-level asset management in order to examine the reliability of the information systems. Then, correlation between the reliability and life cycle costs is analyzed to determine the desirable reliability levels of the systems. With regard to function-level asset management, in addition to failure analysis of the information system, the obsolescence of the systems is examined. Innovation in software and hardware technology may result in rapid

obsolescence of the information systems. As a result of development of information systems, it takes some additional time and cost to obtain old equipment or system components or to adjust alternative equipment. And the obsolescence of the information systems causes a discrepancy between information services and users needs. To solve the problem of obsolescence, the system should be partially or totally replaced. But the renewal of large-scaled information systems like a traffic control system entails enormous cost. Therefore, strategies for renewing the information systems in terms of asset management need consideration of both physical deterioration and functional obsolescence. For the examination of obsolescence, this study focuses on an increase in costs due to the replacement of components and parts. On the other hand, for the examination of functional obsolescence, it is indispensable to analyze needs for information systems and their significance. Since this study focuses on the analysis of failure risks and life cycle costs (repair/maintenance costs), functional obsolescence should be discussed in another papers separately.

Failure Process in Information Systems

This is a model for the occurrence and process of failure events in information systems. As Figure 1. shows, components of information systems are in three layers: 1) Type, 2) Device, and 3) components. Type-layer contains hard disk drive (HDD), power supply, and processing and monitoring equipment. An information system is composed of M-unit Type components and each component is represented by suffix i ($i=1, ..., M$). Type i components are used for N_i-unit Device and each Device is represented by suffix j ($j=1, ..., N_i$). In a traffic control system, for example, each Type of components is used as different Devices such as a personal computer (PC), a server and so on. Since each Device has its own application of components and therefore its failure probability is different from others'. For Device j ($j=1, ..., Ni$), L_{ij}-unit Type i components are used and each component is represented by suffix k ($k=1, ..., L_{ij}$). Components in each Type and each Device are considered to have different hazard rates. But failure process in components in each Device is considered to be described by using the same hazard rates. Here, an infinitely continuous time axis starting from time point t=0 is used. If the existing information systems as a whole are renewed at t=0, deterioration of each component starts from t=0. When a component has a failure, it is immediately replaced. The new one is supposed to have the same performance that the old one had. Now, take a look at $t=T$ where a certain period of time has passed. Then, a failure history is obtained as shown in Figure 2., which cites an example of a failure history of Device 2 (server). Device 2 is composed of L_2-unit components. Among them, component A has no failure from t=0. Time of the use of component A is T and the lifetime of component A is considered to be longer than T. On the other hand, component B had a failure twice at T_1 and T_2. The first lifetime $\zeta = T_1$ and the second $\zeta = T_2 - T_1$.

Risk Management of Information Systems

The Central Station System in this study is composed of a traffic control system and a facilities control system. The traffic control system is used to collect and provide information in response to failure events in expressway transport, specifically, for example, to collect information on weather and traffic volume and congestion and provide it on an information board for users. The facilities control system is used, on the other hand, to monitor and control expressway-related facilities for their normal functioning and failure prevention. While traffic control information is provided for users on an information board or an information terminal (a device for information services), information on failures in expressway-related facilities is provided for the Maintenance Division or the operational

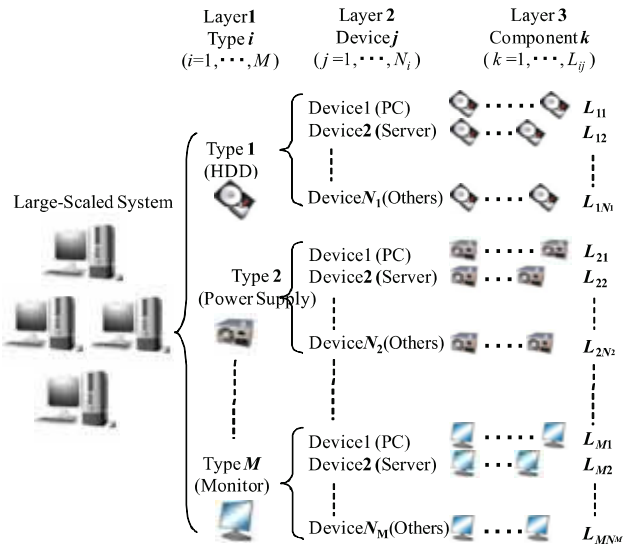

Figure 1. Information System Components & Structure

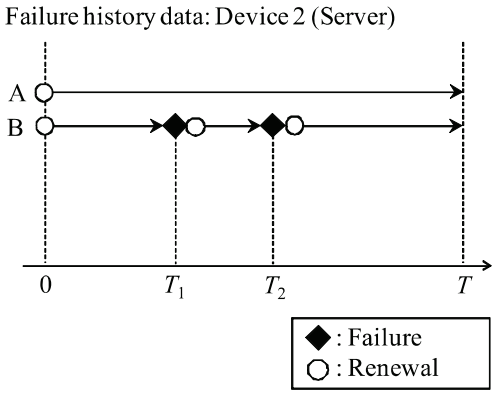

Figure 2. Failure event history data

equipment. Thus, the function of the system is defined as 'proper information transfer to end users.' When a system failed to fulfill all (or part) of this function, the system is considered to have a failure.

In this study, functional failures in the Central Station System are divided into four categories of severity: 1) being unable to provide information for all of the information system (Severity 1), 2) being unable to provide part of information for all of the information system (Severity 2), 3) being unable to provide information for part of the information system (Severity 3), and 4) being unable to provide part of information for part of the information system (Severity 4). In the case of Severity 1, the information system does not operate and necessary information is not provided for end users. In the case of Severity 2, the information system does not stop yet part of necessary (and important) information is not provided for end users. This study focuses on failure events of Severities 1 and 2. Naturally, functional failure risks of Severities 3 and 4 can also be analyzed using the method proposed in this study.

Moreover, functional failure risks are evaluated using two parameters of 1) functional failure occurrence probability and 2) expected effect. Functional failure occurrence probability means the occurrence probability of functional failures of Severity 1 (or Severity 2) at each time point while the system is in operation. Practically, since there is much uncertainty in failure process in components of the systems, it is impossible to reduce functional failure occurrence probability to zero. Important thing is therefore to reduce the probability below the allowable values. On the other hand, when functional failure can be repaired within a short time, its effect on society and users may not be so great. Conversely, when the failure continues, its effect on society and users becomes great. As time passes from the time point of the system installation, it becomes difficult to obtain alternative components or it takes a longer time to adjust the equipment. In this study, the effect of functional failure on society and users is used as a parameter for assessment. As stated in the later, the effect of functional failure is expressed as a function of failure duration, which depends on what type of components has the failure. That is why a parameter of the effect is used for risk assessment. In other words, the goal of risk management of information systems is to reduce expected failure occurrence probability and expected effect below certain levels.

STATIC FAULT TREE ANALYSIS

Objective of the Analysis

The Central Station System in this study is composed of a traffic control system and a facilities control system. The traffic control system is composed of seven sub-centrals to provide information for information boards and information terminals along the expressway as well as to collect information by the aid of weather monitors and other devices. On the other hand, the facilities control system is composed of the facilities central station (monitoring, control and processing system) and operational maintenance support processing system to monitor and control expressway lighting, emergency devices and CCTV cameras in tunnels and interchanges.

The Central Station System is solely responsible for the maintenance and processing of data in the Road Control Center. The Central Station System is composed of an enormous amount of devices and components. After the installation of those devices and components, failure occurrence probability as well as risks in the whole systems increases. In addition, when traffic demand grows and new roads are installed, the number of lines to be controlled will increase and accordingly the system load will also increase. For these reasons, it is necessary to identify the mechanism of failure occurrence in the existing systems for risk assessment and then to design a plan to renew the systems.

This study provides fault tree diagrams of the Expressway Central Station System, focusing on functional failures of Severity 1 and Severity 2.

Fault Tree Diagram Construction

Fault tree analysis is a method for calculating the functional failure risks of the whole systems and has a hierarchical structure showing the mechanism of lower-level failure events developing into functional failures in the whole systems. The analysis has been much applied as failure analysis on designing in reactors or aeronautical engineering (Bedford, 2001). First, functional failure events of the systems (top events) are set. Then, occurrence conditions of top events and lower-level failure events and then their correlations are identified. A fault tree diagram shows the possibility that lower-level events develop into top events. Events are logically connected with AND and OR gates. By the use of occurrence probability of lower-level events, the occurrence probability of upper-level or top events as well as the expected effect is calculated. In addition, based on the occurrence probability of top events and their causes (lower-level events) and the expected effect as well, measures to be taken for the safety and reliability of the systems can be examined.

Figure 3. is a fault tree diagram of the Central Station System. It shows how a failure event in the subsystem leads to a failure in the whole systems of the Central Station. In this study, top events are failures of Severity 1 and Severity 2. As Figure 3. shows, top events of Severities 1 and 2 occur when top events of Severity 1 occur at the Traffic Central Station, the information central station, the highway radio central station, the information terminal central station, the weather central station, and the traffic volume measurement central station. Then, another fault tree diagram is constructed to describe the occurrence of top events in each subsystem and the total of the fault trees of the whole systems exhibits an enormous set of diagrams.

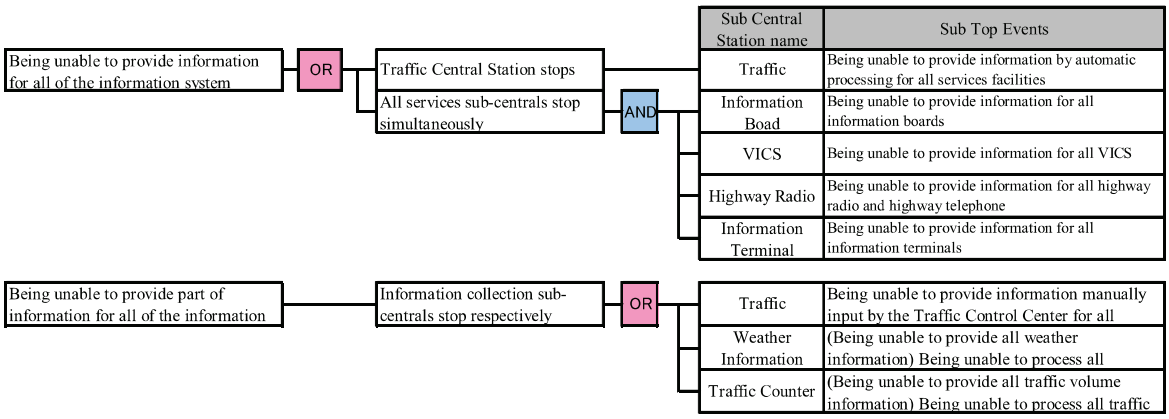

Figure 3. Fault Tree Diagram of the Central Station System

Effect on Society and Users

Yokohama Branch in charge of the management of the Central Station System has concluded maintenance agreements with information system manufacturers that provide the system components. During the agreement period, each manufacturer should ensure parts replacement. However, information system manufacturers generally change the models of their products within a relatively short time and therefore it is not necessarily sure that they keep a stock of old parts. When the stock has run out, alternative parts are used. But then, technical adjustment is required for normal operation of the systems. As time passes after the installation, time and costs required for the adjustment increase. In addition, the engineers who developed the system may have been transferred or software environment or OS development environment may change. As a result, it will be difficult to repair the system immediately. In this way, as time passes after the installation, it takes a longer time to investigate failures, procure parts, or for engineers to repair; in brief, risks increase. Figure 4. shows an effect curve representing correlation between time passed since the system renewal and time required for system recovery after failure occurrence. As the effect curve shows, as time passes after the installation, time required for system recovery becomes longer.

Calculation of the Occurrence Probability of Top Events and Expected Effect

What is important in static fault tree analysis is to calculate the occurrence probability of functional failures of Severity 1 or 2 and their expected effect based on the failure occurrence probability of each component and the effect. The occurrence probability of such top events and the expected effect can be calculated by using Boolean operations. Now, a fault tree diagram of Figure 5. is picked up from those of the whole systems to explain the occurrence probability of top failure events and their expected effect. *A* indicates a top event, *B* and *C* middle events, and *D* and *E* bottom events. The failure state of bottom events *D* and *E* is represented respectively by state variables of δ_D and δ_E, both of which are dummy variables, variables with only two values; one when *D* and *E* occur and zero when *D* and *E* do not occur. Then, when δ_B, state variable (dummy variable) of middle event *B*, is "OR event towards events *D* and *E* (event that occurs when either event *D* or *E* occurs),"

$$\delta_B = \delta_D + \delta_E \quad (1)$$

Next, top event *A* is "AND event towards events *B* and *C* (event that occurs when both events *B* and *C* occur),"

$$\delta_A = \delta_B \times \delta_C \quad (2)$$

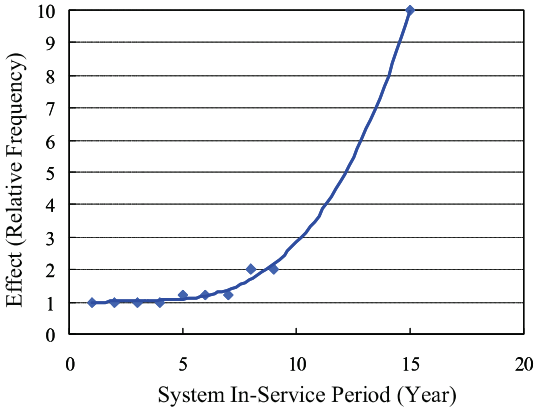

Figure 4. Effect Curve

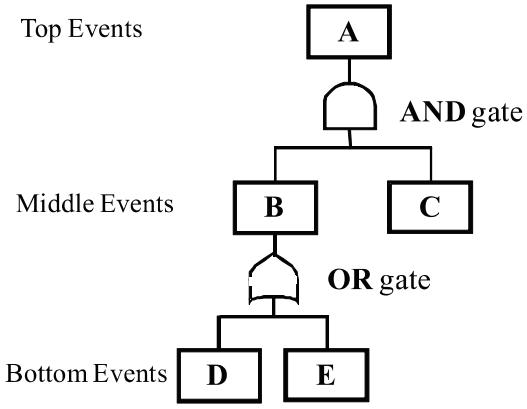

Figure 5. Fault Tree Diagram

The occurrence probability of events A and B is respectively $P(A)$ and $P(B)$ and

$$P(A) = P(B)P(C) \quad (3a)$$
$$P(B) = P(D) + P(E) - P(D \cap E) \quad (3b)$$

Next, the expected effect is defined as (failure occurrence rate x the effect), where the effect refers to the effect of the functional failure on society or users. Now, the effect of components D and E is respectively represented as $T(D)$ and $T(E)$ and the expected effect of the components is

$$RISK(D) = P(D)T(D) \quad (4a)$$
$$RISK(E) = P(E)T(E) \quad (4a)$$

Moreover, effect $T(A)$ of AND gate-connected top event A and effect $T(B)$ of OR gate connected event B are respectively

$$T(A) = \delta_B \delta_C \max\{T(B), T(C)\} \quad (5a)$$
$$T(B) = \delta_D T(D) + \delta_E T(E) - \delta_D \text{ x } \delta_E \min\{T(D), T(E)\} \quad (5b)$$

And expected effects of events A and B are

$$RISK(A) = P(B)P(C)\max\{T(B), T(C)\} \quad (6a)$$
$$RISK(B) = P(D)T(D) + P(E)T(E) - P(D \cap E)\min\{T(D), T(E)\} \quad (6b)$$

Based on the failure probability of lower-level components in the Central Station System and by the use of the above operation rules, the occurrence probability of top events of the Central Station System and their expected effects can be calculated. However, the Central Station System is composed of an enormous amount of components subject to wear-out failure. And the failure probability of components subject to wear-out failure and its effect change as time passes after the time point zero. Accordingly, the occurrence probability of top events of the Central Station System and their expected effects change over time. In addition, when a component has a failure, it is replaced by the new one. It is impossible to analyze the process of such component renewal and dynamic changes in the consequential failure rates. In this study, therefore, a method for randomly generating sample paths of the renewal process and simulating the failure process is formulated as a system. The following section describes the dynamic process of failure and renewal of lower-level components of the Central Station System and a dynamic failure analysis of the system by Monte Carlo simulation models is proposed.

DYNAMIC FAILURE ANALYSIS

Failure/Renewal Process in the Central Station System

A model of the process of a failure event in the Central Station System is provided now. As mentioned before, L_{ij}-unit Type i components are used for Device j ($j=1, ..., Ni$), L_{ij}-unit Type i components are used and each component is represented by suffix k ($k=1, ..., L_{ij}$). The Central Station System was installed at time point $l_0=0$ and has been since in operation. Then, an infinite discrete time axis $l_t(t=0, 1, ...)$ from time point $l_0=0$ is used. It is supposed that the time interval $_l=l_{t+1} - l_t$ is enough small and that the failure occurrence probability and the effect are constant at each period of time $[l_t, l_{t+1})$. The time axis is divided by a minute unit $_l$ and each unit period of time is $\tau_t = [l_t, l_{t+1})(t = 0, 1, ...)$. The deterioration of each component progresses from $l_0=0$. All failures that occur during the unit period of time are supposed to occur at the beginning of the period. When a component has a failure, it is immediately replaced by the new one. As mentioned, the time for replacement depends on the time passed since $l_0=0$. Namely, the longer the time has passed since $l_0=0$, the longer it takes to procure components or adjust the system. Now, components $(i, j, k)(i = 1,...,M; j = 1,...,N_j; k = 1,...,L_{ij})$ have a failure, time required for replacement is $\gamma_{ij}^{k}(t)$. Accordingly, the component (i, j, k) that had a failure at the beginning of the period of time (t) continue to have the failure during the period of time $[t, t+1,...,t+\gamma_{ij}^{k}(t)]$. The components with the failure during the period are replaced at the end of the period of time $t+\gamma_{ij}^{k}(t)$ and put into operation at the beginning of the period of time $t+\gamma_{ij}^{k}(t)$. At time $l_0=0$, however, the replacement is supposed to be immediately done during the unit period of time and therefore $\gamma_{ij}^{k}(0) = 0$ is true. Henceforth, $\gamma_{ij}^{k}(t)$ is called replacement period. The longer the time has passed since $l_0=0$, the longer it takes to procure components or adjust the system, and therefore $dr_{ij}^{k}(t)/dt \geq 0$ is true. Replacement period vector at time t (t=0. 1. …) is expressed as $\gamma(t) = \{\gamma_{ij}^{k}(t) : i = 1,...,M; j = 1,...,N_j; k = 1,...,L_{ij}\}$.

Here, time passed since the nearest time l_t of the renewal of the component (i, j, k) is expressed as $s_{ij}^{k}(t)$ (henceforth called use period). And use period vector at time t is expressed as $s(t) = \{s_{ij}^{k}(t) : i = 1,...,M; j = 1,...,N_j; k = 1,...,L_{ij}\}$. When a component is renewed during a period of time, the use period is reset at zero at the beginning of the next period of time. Then, the state variable $\delta_{ij}^{k}(t)$ which shows whether or not there is a failure in component (i, j, k) during the unit period of time τ_t is defined as

$$\delta_{ij}^{k}(t) = \begin{cases} 1 & \textit{with a failure} \\ 0 & \textit{without a failure} \end{cases}$$

Accordingly, when a failure of component (i, j, k) occurs during the period of time τ_t, the state $\delta_{ij}^{k}(n) = 1\,(n = t,...,t+\gamma_{ij}^{k}(t))$ continues during the period $[t, t+1,...,t+\gamma_{ij}^{k}(t)]$.

Now, a certain discrete time $l_{\bar{t}}$ where a certain time has passed since l_0 is supposed as present time and failure history from l_0 to $l_{\bar{t}}$ is expressed as $\bar{\delta}_{t\leq\bar{t}} = (\bar{\delta}_0,...,\bar{\delta}_{\bar{t}})$, providing that $\bar{\delta}_t = \{\bar{\delta}_{ij}^{k}(t) : i = 1,...,M; j = 1,...,N_j; k = 1,...,L_{ij}\}$ expresses failure history during the unit period of time $\tau_t(t = o,...,\bar{t})$. The bar of $\bar{t}$ signifies it is an actual value. In addition, when the failure history of each component is given, the actual value of the use period during each period of time $\bar{s}_{ij}^{k}(t)$ can be defined. Although during the period of failure the use period is not defined, it is defined as 0 for the sake of calculation. Also, the renewal of a component with a failure may not complete during the period of time in which a failure occurred but continue during some periods of time. Time required to completely renew component (i, j, k) that had a failure at time t (henceforth called continuous failure period) is now expressed

as $d_{ij}^{k}(t)$. When time required for the recovery of component (*i, j, k*) that had a failure at time *t* is $\gamma_{ij}^{k}(t)$, continuous failure period at *t* is expressed as $d_{ij}^{k}(t) = \gamma_{ij}^{k}(t)$. Naturally, when the failure continues at $t + s$, $d_{ij}^{k}(t+s) = \gamma_{ij}^{k}(t) - st$. The failure state $\bar{\delta}_{ij}^{k}(t)$, the use period $\bar{s}_{ij}^{k}(t)$, and the stream of the continuous failure period $\bar{d}_{ij}^{k}(t)$, $\bar{\varepsilon}_t = \{(\bar{\delta}_{ij}^{k}(t), \bar{s}_{ij}^{k}(t), \bar{d}_{ij}^{k}(t)) : i = 1,...,M; j = 1,...,N_j; k = 1,...,L_{ij}\}$, during each period of time, are used to describe failure/renewal process in each component of the system (henceforth called failure/renewal process).

Information on failure history $\bar{\varepsilon}_t$ (t = 0, …, $\bar{t}$) can be obtained up to the present time $l_{\bar{t}}$. The process of failure history after the present time $l_{\bar{t}}$ is an uncertain probability process. The components of the Central Station System are subject to wear-out failure and the failure rates depend on failure/renewal process. Time required for renewal also changes over time. It would be impossible to analytically express such history-dependant probability process. Nevertheless, the failure probability can be estimated based on the use period from the nearest renewal point of time. In this study, therefore, sample paths are randomly generated to describe failure/renewal process using Monte Carlo simulation models and the results are analyzed to follow the dynamic changes of risk management parameters. As models to estimate the rates of failure occurrence, random Weibull hazard models developed by Kaito *et al.* (2008) are used.

Component-Level Failure/Renewal Process

Suppose that the failure history $\bar{\varepsilon}_t$ $(t = 0,...,\bar{t})$ from l_0 to the present time $l_{\bar{t}}$ is given. Then, the dynamic failure analysis of the Central Station System is conducted from the present time to the future time. As mentioned before, since it is impossible to analyze the component-level failure/renewal process, sample paths are randomly generated to describe failure/renewal process using Monte Carlo simulation models to analyze failure qualities of the system. A sample path represents one deterministic path that can occur as failure/renewal process. The failure/renewal process at the future time can be described as a set of innumerable sample paths. This set of sample paths are obtained using Monte Carlo simulation models and according to the following steps:

SETP 1 The number of sample paths is set at *q* = 1. The goal number *Q* of sample paths and the goal period on time *Z* for the assessment of life cycle costs are set.

SETP 2 The present time $l_{\bar{t}}$ is considered to be the starting point of time in simulation and the sample point of time in simulation is set at *z* = 0. Failure information at the starting point is described as $\bar{\delta}_0^q = \bar{\delta}_{\bar{t}}$, provided that $\bar{d}^q(0) = \{\bar{d}_{ij}^{kq}(0) : i = 1,...,M; j = 1,...,N_j; k = 1,...,L_{ij}\}$. Renewal is at *z* = 1.

STEP 3 A set of components with a failure that continues from the previous period of time (henceforth called continuous failure set) is expressed as $\varpi_z^q = \{(i,j,k) \in \omega | \bar{d}_{ij}^{kq}(z-1) \succ 1\}$ and a set of components with a failure that does not continue from the previous period of time (henceforth called non-continuous failure set) is defined as $\omega_z^q = \varpi - \varpi_z^q$.

STEP 4 With regard to the components (*i, j, k*) belonging to the non-continuous failure set ω_z^q during the period *z*, random numbers are generated based on the failure probability of (Kaito *et al*, 2008) to determine whether the components have failures or not. Based on the results, the failure state of the components (*i, j, k*) in the sample path *q* during the period *z* is expressed as follows:

$$\bar{\delta}_{ij}^{kq}(z) = \begin{cases} 0 & \textit{without a failure} \\ 1 & \textit{with a failure} \end{cases}$$
$$(i,j,k) \in \omega_z^q$$

In addition, $\bar{d}_{ij}^{kq}(z)(i,j,k) \in \varpi_z^q$ is renewed as follows:

$$\bar{d}_{ij}^{kq}(z) = \begin{cases} \gamma_{ij}^{kq}(z) & when\ \bar{\delta}_{ij}^{kq}(z) = 1 \\ 0 & others \end{cases}$$
$$(i,j,k) \in \omega_z^q$$

STEP 5 Each factor of the failure continuous time vector $\bar{d}^q(z+1)$ is expressed as follows:

$$\bar{d}_{ij}^{kq}(z+1) = \begin{cases} \bar{d}_{ij}^{kq}(z) - 1 & when\ \bar{d}_{ij}^{kq}(z) \geq 1 \\ 0 & when\ \bar{d}_{ij}^{kq}(z) = 0 \end{cases}$$

In addition, continuous failure set $\varpi_{z+1}^q = \{(i,j,k) \in \omega | \bar{d}_{ij}^{kq}(z+1) \geq 1\}$ and non-continuous failure set $\omega_{z+1}^q = \omega - \varpi_{z+1}^q$ in the sample path q during the period z are defined.

STEP 6 The algorithm terminates when z arrives at the goal period Z and the sample-path number q arrives at the goal number Q. When z arrives at the goal period Z yet the sample-path number q does not arrive at the goal number Q, return to SETP 2 with $q = q+1$ and $z = 0$. In other cases, return to SETP 3 with $z = z+1$.

Following the above steps, the total number Q of sample paths on the failure/renewal process at the present time (the starting time) z = 0. The sample path q ($q = 1,...,Q$) is a deterministic path on the failure/renewal process and expressed as follows:

$$\bar{\varepsilon}^q = (\bar{\varepsilon}_0^q,...,\bar{\varepsilon}_z^q)$$
$$= \{(\bar{\delta}_{ij}^{kq}(z), s_{ij}^{kq}(z), \bar{d}_{ij}^{kq}(z) : i = 1,...,M; j = 1,...,N_j; k = 1,...,L_{ij}; z = 0,...,Z\} \quad (7)$$

Risk Management Parameters

When sample paths on component-level failure/renewal process are used, 1) the failure occurrence probability of each component at the present point of time z = 1, 2) system-level failure occurrence probability, and 3) the expected effect can be obtained. First of all, the dynamic process $P_{ij}^k(z)$ of the failure occurrence probability of component $(i.\ j,\ k) \in \omega$ is defined as follows, summarizing the failure states of all sample paths,

$$P_{ij}^k(z) = \frac{\sum_{q=1}^{Q} \bar{\delta}_{ij}^{kq}(z)}{Q} \quad (8)$$

Next, system-level failure occurrence probability is obtained by summarizing the failure states of top events of all sample paths: based on the information $\bar{\delta}_z^q$ of the failure state of each component, Boolean algebraic equations (1) and (2) are used to obtain the occurrence state $\bar{\delta}^q(z)$ of the top event in the sample path q during the period z, providing that

$$\bar{\delta}^q(z) = \begin{cases} 0\ when\ the\ top\ event\ does\ not\ occur \\ 1 \quad when\ the\ top\ event\ occurs \end{cases} \quad (9)$$

Then, the failure occurrence probability $\bar{P}(z)$ in the system is expressed as:

$$\bar{P}(z) = \frac{\sum_{q=1}^{Q} \bar{\delta}^q(z)}{Q} \quad (10)$$

Next, the expected effect of system-level failure event is defined. When a failure occurs, its effect *T(z)* in each sample path is obtained by using the operational equations (5a) and (5b). Accordingly, the expected effect of the failure effect is defined as:

$$\overline{RISK}(z) = \frac{\sum_{q=1}^{Q} \bar{\delta}^q(z) T(z)}{Q} \quad (11)$$

Finally, the periodically expected life cycle costs $\overline{C}(z)$ for repair/maintenance of the Central Station System until the goal period Z is expressed as follows, when the renewal costs of component (i, j, k) during the period z is $C_{ij}^{k}(z)$:

$$\overline{C}(z) = \frac{\sum_{q=1}^{Q} \overline{\delta}^{q}(z) C_{ij}^{k}(z)}{Q} \tag{12}$$

Therefore, the reduced current value LLC of the expected life cycle costs assessed by current value at the present time $z = 0$ is expressed as follows, when the reduced rate is p:

$$LCC = \frac{\sum_{z=0}^{Z} \overline{C}(z)}{(1+p)^{z}} \tag{13}$$

CASE STUDY

Case Study Overview

The above-mentioned dynamic failure analysis models are applied to the renewal of the Central Station System at Yokohama Branch, Central Nippon Expressway Company Limited. It is required of the system to devise methods for developing a rational system maintenance and renewal plan in an attempt of reducing maintenance costs and improving safety and system environment. The Central Station System is composed of nine subsystems and each subsystem is responsible for the renewal of the deteriorated components. The Traffic Central Station System is one of the subsystems and was renewed 13 years after the renewal of the whole Central Station System.

As mentioned before, as time passes after the renewal of the whole systems, system recovery takes a longer time because of the limited maintenance of components or changes in engineers' support and system environment. In other words, one failure event comes to need different recovery remedies over time and its effect on society and economy becomes greater. The effect can be analyzed with the aid of effect curves. In this case study, effect curves are created according to these steps: 1) an interview survey on the maintenance contract duration of each component and the manufacturer's stock of the component and related parts and their in-stock guarantee period, 2) year-to-year estimation of time required for recovery from failures, 3) year-to-year estimation of the duration of top events, 4) creation of effect curves to show the effects of a failure duration on the three parameters of environment, cost and safety, 5) importance proportionally attributed to the three parameters based on in-house interviews: environment, cost and safety representing respectively 35%, 45% and 20%, and 6) creation of effect curves based on the weighted average of the effect curve per parameter. The above-mentioned Figure 4. shows the effect curve.

Analytical Results and Discussion

Based on estimation results of random proportional Weibull hazard model by Kaito *et al.* (2008), sample paths on the failure/renewal process were generated with respect to the process of the dynamic failure probability and the expected effect. Using Monte Carlo simulation models, 500,000 sample paths were generated to calculate the failure occurrence probability, the expected effect and expected life cycle cost. Table 1. recovery price per failure and the estimate of the total cost spent on the whole systems of the Traffic Central Station.

Table 3. Cost Parameter

Components	Recovery price per unit (unit: thousand yen)
Processing body (software)	500
Processing body (hardware)	1,500
System body	1,500
hard disk drive (HDD)	700
Power supply	500
System renewal costs	480,000

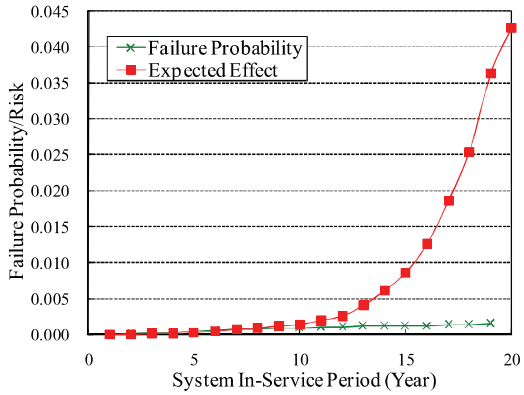

Figure 6. Changes in Failure Probability and Expected Effect

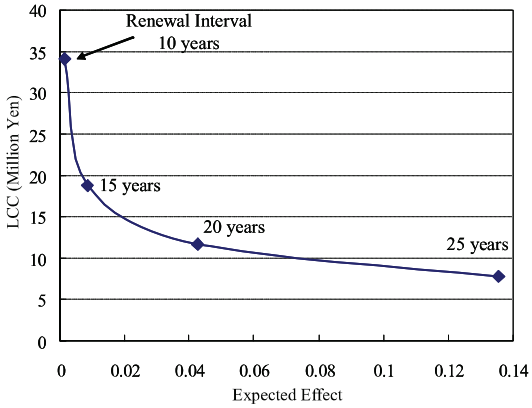

Figure 7. Correlation between Expected Effect and Expected Life Cycle Cost (LCC)

In this case study, the dynamic failure analysis of the whole Central Station System and its subsystems was conducted. Among an enormous amount of analytical results, the results obtained from the Traffic Central Station System, one of seven subsystems of the Traffic Control System, is cited below. Figure 6. shows changes in failure probability and the expected effect in correlation with the system in-service period of time. The failure probability is equal to the functional failure probability of the Traffic Central Station System and the expected effect is the failure probability multiplied by the effect based on the recovery time. As the fault tree diagrams show, failures on the terminal components (hard disk drive (HDD), the section of power supply, and others) of the Traffic Central Station System affect the dysfunction as top events. When a failure is identified in a component, it is immediately replaced by the new one. Since the failure process follow the time-dependant random Weibull hazard models, the failure probability increases as time passes since the renewal point of time until the component is replaced. As a result, the failure probability of the whole Central Station System increases as the system in-service period of time becomes longer. On the other hand, the estimated effect changes in parallel with the failure probability for approximately 10 years of operation yet increases in an accelerating manner after 12 years and becomes 30 times greater than the expected effect at the in-service period of time of 10 years. This simulation results reflect the effect curve in Figure 4. In brief, after the termination of the maintenance contract duration, components are expected to be out of stock, and around this point of time system recovery starts to require more time. In this way, while both the failure probability and the expected effect increase as the in-service time increases, the expected effect rapidly increases beyond a certain point of in-service time.

Figure 7. shows a correlation between the expected life cycle costs (including the renewal cost) and the expected effect with regard to the renewal intervals of the Traffic Central Station System. The expected life cycle costs along the y-axis is an annual average cost, which equals

the total of the recovery costs of components and the reduced current value (discount rate of 4%) of the whole systems renewal cost (480 million yen) divided by the renewal interval. Since the expected effect increases in parallel with the system in-service time, it is represented by the maximum value within a renewal cycle. The expected life cycle costs and the expected effect were calculated at an interval of one year of the renewal interval of 10 to 25 years. As Figure 7. shows, there is a trade-off relationship between the expected life cycle costs and the expected effect and the reduction of the expected effect necessitates the shortening of the renewal interval, resulting in an increase in the life cycle costs (including the renewal cost). On the other hand, as mentioned before, the effect of failures rapidly increases after 10 years of system operation and, in Figure 7. also, the expected effect rapidly increases compared with the expected life cycle costs when the renewal interval is over 15 years. In this way, the dynamic failure analysis models can be used to determine correlations between changes in failure probability, the expected effect and the expected life cycle costs. Their outputs also can be used as important data for decision-making on system renewal policies.

Application to System Renewal Policies

Finally, the above-mentioned dynamic failure models are applied to policy-making on the renewal of large-scaled traffic control systems. Renewal policies should be made in over-all consideration of the finances of the system management organizations and user's needs in addition to the above-mentioned expected life cycle costs, failure probability and expected effect. There are other factors to be considered, including an extension of the expressway or the installation of additional roads and their timing, performance improvement in information systems, and the consolidation of traffic control systems. This complicated issue cannot be covered by this single study but just referred to in Conclusion and here the analysis of system renewal by the use of dynamic failure models is discussed.

The Traffic Control System is composed of several subsystems including the Traffic Central Station. However, as information technology has progressed, it is now technically possible to consolidate the subsystems. Although this study has discussed a single traffic control system, the actual expressway network contains several traffic control centers at geographically different locations and the differentiated lines for each center. The consolidation of the different subsystems will contribute to the integration of the whole systems, the reinforcement of support systems, and the improvement of the reliability of the whole systems. Here, the dynamic failure analysis models are used to analyze the impact of the consolidation of the subsystems or the integration of the whole traffic control system on the expected life cycle costs (including the renewal cost) and the expected effect.

As mentioned before, as part of the Central Station System under the control of Yokohama Branch, Central Nippon Expressway Company Limited, the Traffic Central Station System was renewed 13 years after the renewal of the whole Central Station System. Now, the dynamic failure analysis models were used to calculate the expected effect at the time of the renewal and to set the expected effect as a benchmark for risk management for the purpose of examining the possibility of the next were used to analyze year-to-year changes of the expected effect of each subsystem. And it was determined that the subsystem would be renewed when the expected effect reaches the benchmark for risk management. In this way, the renewal interval of the subsystem is obtained. Based on the renewal policies, the failure/renewal process of the whole Central Station System is simulated. It is supposed that, on renewing the subsystem, new components are procured and their maintenance contracts are

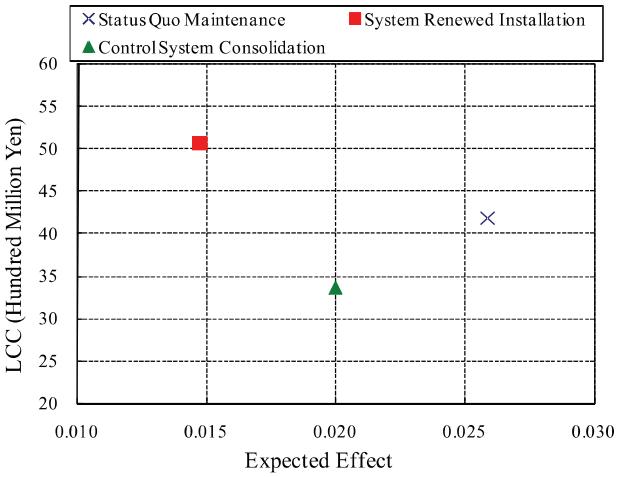

Figure 8. System Renewal Policy (1)

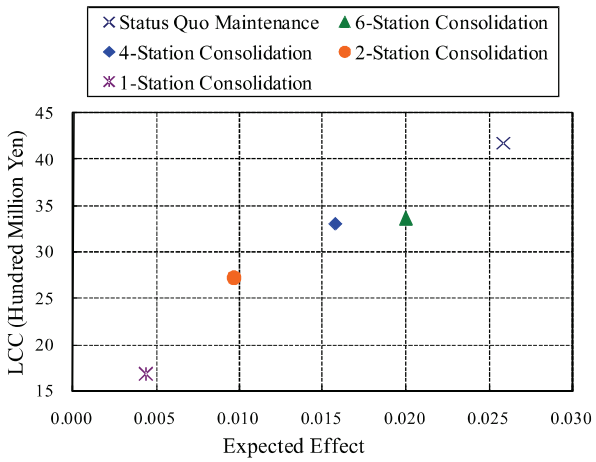

Figure 9. System Renewal Policy (2)

newly concluded; the expected effect is set at zero; the renewed system is supposed to have the same failure possibility as the previous one.

Figure 8. shows the simulation results in the cases of 1) the continuous operation of the present system, 2) the immediate renewal of the whole control system while the structure being maintained, and 3) the immediate consolidation of the existing two traffic control systems (in Yokohama and Hachioji). The expected effect is the greatest when the present system is continuously maintained because the limited maintenance contract duration affect the failure recovery and it takes a longer time. On the other hand, the renewal of the system reduces the expected effect but increases the expected life cycle costs. When the traffic control systems are consolidated, the expected life cycle costs decrease due to the decrease of the number of the systems to be managed. However, the consolidated system needs to provide service over a geographically wider range and consequently the effect of failures becomes greater, leading to the greater expected effect than the renewal will have. In this case, if emphasis is placed on the redundancy in system construction, the expected effect will be reduced even in the consolidation. Figure 9. shows the simulation results in the cases of 1) the continuous operation of the present system, and 2) the consolidation of the existing two traffic control systems and that of the subsystems into 6, 4, 2 and 1 station(s). It is demonstrated that the consolidation of the subsystems can reduce both the expected life cycle costs and the expected effect.

CONCLUSIONS

In this paper, dynamic failure analysis models were formulated for asset management of large-scaled information systems for infrastructure facilities. For this purpose, firstly, random proportional Weibull hazard models were used to describe failure processes in the components of the information systems. Secondly, fault tree diagrams were used to explain how failures in components lead to those in the whole systems. Thirdly, Monte Carlo simulation models were used to describe the effects of changes in time-dependant failure probability and in failure recovery time on the failure occurrence probability of the system and on the temporal changes in the effect of failures. And finally, the practical availability of the above methods was investigated in a case study on traffic control systems. The proposed dynamic failure analysis models still have some problems in applying them to the asset

management of information systems. Firstly, the proposed dynamic failure analysis models should be developed in consideration of micro-level optimization/renewal of the components. It was investigated in this study how component-level failures lead to the functional failure of the whole systems. An analysis of the policies for the maintenance of more precise information systems will be possible when rational renewal policies for preventive maintenance of the components are made to reduce failure probability and methods for preparing alternative components are optimized. The proposed dynamic failure analysis models are applicable to such micro-level asset management. Secondly, measures should be taken to improve the system in a way that it can prepare for its functional deterioration. Since technological improvements have been rapidly achieved on information systems, and transportation user's as well as system user's needs change as the social environment changes. When information systems cannot satisfy the needs, they are considered to have reached the end of their life cycle and a large-scaled improvement is required. In this study, time required for system recovery was used as a parameter for the effect of component-level failures on the reliability of the system. But other risk parameters should be developed in consideration of the effect of dysfunction due to technological obsolescence of the system. Thirdly, models should be developed to assess the appropriate timing of the system renewal. Since there is much uncertainty in changes in information system environment, methods using real options models should be developed to determine whether or not the renewal is necessary or when and to help make decisions on investment.

ACKNOWLEDGEMENTS

The authors would like to express our gratitude to Traffic Control Team, Facilities Team, and Facilities Maintenance Team of the Traffic Control Center, Yokohama Branch, Central Nippon Expressway Company Limited, and Highway Facilities Engineering Department, Expressway Technology Center. In addition, part of this study (by Kiyoyuki Kaito) was conducted at the Frontier Research Base for Global Young Researchers, Graduate School of Engineering, Osaka University, supported by Special Coordination Funds for Promoting Science and Technology, Ministry of Education, Culture, Sports, Science and Technology.

REFERENCES

Aoki, K., Yamamoto, K. and Kobayashi, K. (2007). “Optimal Inspection and Replacement Policy using Stochastic Method for Deterioration Prediction”, *The 11th World Conference on Transportation Research*, Berkeley, USA

Bedford, T. and Cooke, R. (2001). “ Probability Risk Analysis”, *Cambridge University Press*.

Kaito, K., Obama, K., Kobayashi, K., Aoki, K. and Yamamoto, K. (2008). “Random Proportional Weibull Hazard Model and Its Application to a Traffic Control Systems”, *10th International Conference on Application of Advanced Technologies in Transportation*, Greece, Athens (abstract accepted).

Lancaster, T. (1990). “The Econometric Analysis of Transition Data”, *Cambridge University Press*.

Tsuda, Y., Kaito, K., Aoki, K. and Kobayashi, K. (2006). “Estimating Markovian Transition Probabilities for Bridge Deterioration Forecasting”, *Journal of Structural Eng./Earthquake Eng.*, *JSCE*, Vol.23, No.2, pp.241s-256s.