A Model for Manageable Dependability of IT Services Associated with Social and Economic Infrastructure

Hiroshi Ohtaka, Koichiro Oshika, Masashi Gotou, and Tsutomu Yoshitani
Project Mieruka, Software Engineering Center, Information-technology Promotion Agency, Japan
h-otaka@ipa.go.jp
Yoshiaki Fukazawa
School of Fundamental Science and Engineering, Waseda University
fukazawa@waseda.jp
doi: 10.4156/ijipm.vol1.issue1.2

Abstract
Defects in information technology (IT) services will have greater negative impacts on social and economic activities in the future, since the risks of such defects are increasing due to their wider applications and the growth of IT systems’ complexity and scale. In this paper, upon surveying the current state of affairs and seeing that little progress has been made towards understanding and reducing defects in IT services that influence social and economic activities, despite a number of efforts including upgrading software and hardware quality, we propose a new approach to understanding and managing the dependability of IT services by discussing a dependability model. The model consists of not only functions for legacy system dependability but also two types of functions (additional safety and safety operation). Next we evaluate the efficacy of these two types of functions relative to IT dependability, both qualitatively and quantitatively, by using 42 actual cases of IT accidents obtained by the Information-technology Promotion Agency, Japan. Moreover, based on the verification, we examine the ways in which improvement of IT dependability associated with social and economic infrastructure, previously dependent on the skill of individual engineers, is eventually achieved as a result of organizational activities.

Keywords: IT service, Enterprise information system, Fault tolerance

1. Introduction
Defects in information technology (IT) services for mission critical businesses such as financial firms or telecommunication firms (i.e., IT supporting social and economic infrastructure) often negatively influence social and economic activities.

In contrast to embedded IT systems such as those that automatically control hardware equipment, the IT systems associated with social and economic infrastructure are enterprise-level systems with the following characteristics:
- They are able to run large-scale applications exceeding several million steps, including complicated on-line and batch processing;
- Frequent interactions with the system are possible, creating the potential for human operation faults;
- Dependability of the IT service is affected by environmental changes (such as a sudden peak of traffic or frequent application updates) caused either directly or indirectly by social and economic activities.

IT services supporting such complicated systems are thought to be highly prone to accidents. We should aim to achieve higher dependability since these types of services are spreading widely throughout society.

In this paper we discuss enterprise IT services with a focus on the following issues:
1. We survey legacy activities to prevent IT accidents by reviewing the literature and show that legacy models of understanding IT dependability have not been capable of meeting with threats of future IT accidents;
2. Literature review

A number of approaches have succeeded in preventing IT accidents. For example, IT system dependability has been improved through the implementation of software development technologies. These include structured software testing and quality assurance technologies [1], higher-reliability hardware solutions such as popular clustering or RAID (Redundant Arrays of Inexpensive Disks) technologies, and continuous improvement of total system development projects such as PMBOK (Project Management Body of Knowledge) [2] for general projects and CMMI (Capability Maturity Model Integration) [3] or MIERUKA [4] for IT projects. However, these technologies for improving system dependability are only applicable over a finite period of project development, that of IT implementation.

For during the operation phase after the launch of developed systems, there are ITIL (IT Infrastructure Library) [5][6][7][8][9] and ISO20000 [10]. These include best practices for IT service management and operation and incorporate measures to reduce human operation faults. They assume that necessary functions are developed by the IT development projects and that engineers of service management and operation use these functions as they are. Thus, even when extra functions in a broader sense (including human operations) are needed in IT services where higher dependability is required, we can not find in the ITIL and the ISO20000, any model to define the functions’ scope nor any guideline to assign responsibility to determine whether the functions should be developed or not.

Consequently, they seem to expect individual companies to have some suitable model and field engineers in the company to judge whether extra functions should be realized or not. However, one hesitates to say that we are safe given the number of IT accidents broadcast by the Japanese news media (Figure 1).

We first surveyed the viewpoints of news media firms. According to a summary of 94 recent IT accidents [11] that were covered by the Japanese news media, 49 cases were due to product faults (i.e., reliability problems in a narrow sense including software bugs), 17 cases were due to human errors, and the causes of 28 cases were not specified. Thus, of the 66 cases whose causes were specified, approximately 70% were thought to be due to problems with product quality. This type of news continues to be broadcast because of recognition by the news media firms that there is no way to improve dependability except by improving software quality. However, Japan has been reported to have fewer potential bugs in its finished software than other major software producing countries such as India, European countries, and the United States [12]. Thus, we have doubts about whether this single approach can substantially improve the dependability of IT services associated with social and economic infrastructure.

Approximately 30% of covered IT accidents were thought to be due to human errors. However, since a recent evaluation said that the field operation departments of Japanese IT service operations wield a relatively significant amount of power [13], there seems to be minimal room to improve dependability in this area.

Based on the above discussions, we think that the keys to further improvement of IT dependability lie in the fact that few models have been implemented with a focus on dependability and there has been a lack of clarity in assigning responsibility for developing functional elements involved in each model. That is, we recognized that it is necessary to identify a model which clarifies assignment of responsibility on the assumption that IT accidents actually happen, since there is a high possibility of accidents in complicated IT services supporting social and economic infrastructure.

Upon the above recognition, we next investigated how social organizations understand the overall shape of the dependability in real terms.
We first proceeded to survey public associations of governmental organizations related to IT. The International Standardization Organization [14] and Japan Industrial Standard [15] define the external quality of software using six categories, including functionality and performance, but have not considered the control of faults, including bugs, to be a systematic category. The Ministry of Economy, Trade and Industry (METI) of Japan [16] first introduced the category of controlling faults when they expanded the six categories to 11 categories in focusing on non-functional requirements mainly for enterprise IT services. Furthermore, the category was broken down to two sub-categories, preventing occurrence of faults and preventing the spread of negative effects caused by faults. Despite these steps, the following can be observed:

- Most discussions have focused on preventing the occurrence of faults, with fewer concentrating on mitigating faults’ negative outcomes. Moreover, there is no discussion on the importance of countermeasures to prevent the spread of negative effects caused by faults.
- Several checklists are intended to preventing the spread of negative effects caused by faults. However, the checklist items are described at an abstract level, for instance checking for the presence of countermeasures to initial faults after the launch of an IT service. There is neither a systematic explanation of the expansion process by which an initial fault occurrence results in concrete negative outcomes nor suggestions to develop specific countermeasures to cope with the adverse events.

Next, companies that provide actual IT services generally assign causes to IT defects or accidents using categories such as developed application bugs, system infrastructure problems, or maintenance or operation issues. Each individual category corresponds to an accounting department within the company. Consequently, IT dependability is effectively the sum total of each department’s efforts to improve its own individual quality measures. However, it is quite unlikely that the overall structure of departmental organizations is derived from a systematic attempt to anatomize the elements that yield optimal IT dependability and then represent these in organizational form. Rather, it seems that these companies have a model of dependability that consists of elements corresponding to individual departments. However, given the number of IT accidents illustrated in Figure 1, there are doubts about the adequacy of such a model.

![Figure 1. Trends of the number of IT accidents broadcasted by news media in Japan](image)

3. Systematizing elements of dependability

Economically speaking, IT companies benefit most if elements of dependability correspond to existing organizational departments that are hypothetically derived from the point of view of economical rationalism. However, although the idea of this dependability model is reasonable for an IT service provider, it is difficult to say whether third parties can objectively understand the appropriateness of the model.
The reason for this is that the causes of nearly half of the 94 IT accidents mentioned earlier were either not clear or were treated as only human operation faults. Doubt remains as to whether the best way of improving dependability is to divide responsibility among existing departments in the organization.

To deal with this doubt we use modeling to clarify the structure of dependability. As mentioned before, IT services that support social and economic infrastructure are complicated systems. In order to allow us to model the entire configuration of the complicated systems, we first defined the following three elements to describe the phenomena that occur before the outbreak of IT accidents by using fault-tolerant model [17]:

- **Faults**: These are root causes that trigger successive events before IT accidents occur. They include, 1) product faults such as software bugs and hardware defects, 2) human operation faults, and 3) environmental changes such as a sudden increase in network traffic or data processing load;
- **Service errors**: This is a possible status event, which may causes future IT accidents or exacerbate these accidents’ negative effects (the service error corresponds to an error in the fault tolerant model);
- **Service failures**: These are events that negatively influence social and economic activities, for instance terminations of service for a long period of time (IT accidents in the worst case).

By using these elements, we can formulate fault-tolerant functions promoting higher dependability as shown in Figure 2. We define the functions in IT services as follows:

- **Safety operation functions**: Organizational structures that mitigate actual damage to social and economic activities by responding to service failures, even when faults cannot be fixed.

Component errors in fault-tolerant devices can be identified relatively more easily by extracting possible production fault cases from design specifications of the devices. However, in IT services related to social and economical infrastructure, there can be a wider range of fault sources, which include not only production faults of all software and hardware devices but also environmental changes and human operation faults by system operation and maintenance engineers. Thus, since the more simple identification methods are not applicable to IT services as they are, we need the following additional functions to cope with service errors caused by a broader range of fault sources.

- **Additional safety functions**: Functions to identify service errors and decide mechanisms executed in safety operation functions to prevent faults from developing into service failures, or reducing the negative influence of the service failures, even when service errors occur.

The following additional information is necessary as the fourth element to execute such identification and decision in the functions.
Early warning sign (EWS): Alert providing notification that service errors caused by faults could progress to service failures.

We call a set of the additional safety functions and the safety operation functions an on-demand safety system.

IT service experts must consider the final scope of the first type of function based on a balance between additional investment and expected total loss, including degradation of social reputation and opportunity loss, since additional development costs other than those necessary for system development are required. Since these functions require decision making regarding contingency plans, the final responsibility for them should rest on IT owners or management executives rather than on field operation and maintenance departments.

In contrast, responsibility for the second type of function is assigned to the field organizations that implement them.

Based on the above discussion, we systematize a bird’s-eye view of dependability as shown in Figure 3 by considering the legacy system’s dependability, whose responsibility should rest on development departments. According to this viewpoint, overall dependability is composed of the legacy system’s dependability, the additional safety functions and the safety operation functions. Since we categorize the tree elements according to the relevant responsibilities, we call this model a manageable dependability model.

Legacy research on improving dependability of enterprise IT services has focused on preventing faults through improving software quality and fault tolerant technology [18] or activities to reduce human operation faults. In contrast, our original approach is to introduce concepts of fault tolerance to the enterprise IT service by taking into account not only service errors but also EWSs.

The outcome of legacy research has included improving software quality to prevent production faults and developing fault-tolerant technologies to increase device dependability. These approaches have been implemented in IT systems facilities as freeze logic and have played a role in system dependability as illustrated in Figure 3.

Problems occur if the additional safety functions and the safety operation functions in Figure 3 always implement the same freeze logic as the system dependability processes, since the additional safety functions have to be developed by considering the following features:

Figure 3. Systematized model of dependability for IT service (manageable dependability model)
The final functions to be implemented are decided upon by IT owners or management after limiting and prioritizing candidate functions through a process of obtaining expected probabilities and impacts of each of them;

Commitment to a function is not a permanent decision. Flexibility is important since the dependability of IT services is contingent on environmental changes. Thus, implementation methods are required to avoid a loss of investment and to realize the maximum scope of functions under a limited budget.

It is probable, then, that the flexibility to change the scope of countermeasures with the aim of higher dependability will lead to a degradation and consequent reduction in the overall scope of available countermeasures if the additional safety functions or the safety operation functions are implemented in facilities that utilize freeze logic.

Therefore, most of the additional safety functions and safety operation functions are thought to lack freeze logic, with a few exceptions, for instance cheap software tools. Implementation of these functions is supposed to follow an approach that requires no extra cost beyond keeping structures of the safety operation functioning normally except during emergencies, during which times costs can be potentially very high. In this sense, we call the combination of additional safety functions and safety operation functions an “on-demand safety system”.

4. Verification of the model based on actual cases

We next verify whether or not actual IT accidents can be explained using the manageable dependability model illustrated in Figure 3. Specifically, we determine whether existence or absence of the functions in the on-demand safety system affects the dependability of IT services by using actual IT accidents documented at the Software Engineering Center, Information-technology Promotion Agency, Japan (IPA/SEC).

4.1. Qualitative verification

Case 1

In this case, the response of an on-line service was delayed after the service was started, although a quick and stable response had been observed in the service before the accident. The accident was caused by a batch processing delay in which the process remained active even after the scheduled on-line service start. The delay had been caused by the misexecution of an operator command, which consumed significant server resources while the batch was running.

In this case the fault was the inappropriate running of the command, the service error was batch-processing delay and the service failure was the slow response of the on-line service. An EWS could have prevented this case if by some means such as IT service evaluations the problem had been pointed out before the accident occurred.

The dependability of the service could be improved further if either one of the following functions was implemented:

- An automatic mechanism that starts up on-line applications and gives a higher executing priority to these applications when batch processing is still in progress at the scheduled on-line start time, on the assumption that such service error may happen in reality (additional safety function);
- An organizational structure that, when the automatic mechanism cannot be applicable to the service, more rapidly detects the service error (the batch-processing delay), starts up on-line applications punctually, and gives higher executing priority to the applications without fail, (safety operation function).

Since the service error may be caused not only by human operation errors or bugs in batch-processing programs but also by environmental changes such as a sudden increase in data-processing load, it can be concluded that the service lacks the necessary on-demand safety system.

Case 2
In this case, clerks working at computer terminals in shops of customer divisions found that IT services were suddenly unresponsive, although these services were stable and responsive before the accident. Many of the terminals had to be shut down for days since it took a long time to recover service. The reasons for this delay were as follows:

1) Too much time was spent identifying the cause of the abnormal phenomenon.

In this system, a network facility was composed of a dozen high-end network elements that were duplicated to achieve higher system dependability. However, the IT system division had not implemented a mechanism that would detect the abnormal performance of any given network element, since the devices had been very popular and selling well worldwide and development costs had exceeded the budget allowed. Furthermore, the organizational structure necessary to respond to such a case did not exist.

2) Too much time was spent recovering service after detection of the cause.

The cause of the abnormal phenomenon was a bug in the control software whose effects were triggered by changes in telecommunication traffic, i.e., an environmental change. However, even after the cause was detected, there were many ways to avoid the problem, though every option had potential adverse effects. Further complicating the matter was that the bug in the commercial system could not be reproduced in the testing system, while poor cooperation between the systems division and the customer divisions complicated the development of methods to avoid a solution’s potential side effects. Thus, methods of trial-and-error were employed so as to avoid the bug’s negative influences during the IT service’s on-line service time. This extended the number of days necessary to eventually recover full service.

The fault in this case was caused by an unknown bug in the software product in the network element device, the service error was the delay in identifying the cause of the fault and then recovering service, and the service failure was the extended unavailability of business processes at a large number of terminals. If the risk of this case were somehow pointed out before the IT accident, the alert of the risk would be defined as the EWS.

The dependability of the service could be improved by reducing the duration of terminal downtime through implementation of the following functions:

- Introduction of a mechanism to quickly alert a human operator of the abnormal performance of a network element device’s input and output response (additional safety function) and an organizational structure to respond quickly to the abnormal performance (safety operation function);
- Commitment to testing bug reproduction procedures and to verifying side effects of fixing the bug in the commercial system supported by corporate customer divisions after the planned time of window closure, on the assumption that such bugs may actually appear in a complicated system (additional safety function to ease negative influences of service failures), and an organizational structure to execute testing in the commercial system in cooperation with the customer divisions (safety operation function);
- Establishment of contingency plans to continue minimum business processes in the customer divisions even when IT systems are not available (additional safety function) and an organizational structure to execute these plans (safety operation function).

We would encourage management or owners of IT services that support social and economical infrastructure to determine the proper amount of effort to devote to preventing terminations of corporate processes by judging specifically the degree to which they should implement such on-demand safety systems as described in Case 2.

Case 3

If symptoms of the service error are unobservable, there is no way to avoid the negative influences of subsequent service failures, except by eliminating the corresponding causes (faults) of the IT accidents. For example, in this case, test mail was inadvertently sent to actual users because some addresses registered in the test database were equivalent to those of actual users. Engineers failed to detect the problem.

4.2. Quantitative verification
It is difficult to verify the effectiveness of the manageable dependability model quantitatively, since the broadcasted information of the 94 IT accidents mentioned above contain insufficient information to do so. It was impossible to obtain more detailed information about these cases since this was prohibited by corporate security. We therefore verified effectiveness of the model by collecting as much actual field information on the cases as possible using the approach mentioned below.

4.2.1. Method for Case Specification

We obtained information regarding IT accidents from a sectional meeting named Project MIERUKA held at the Software Engineering Center of the Information Promotion Agency, Japan (hereafter, IPA), where strict privacy standards are maintained. The meeting members have 20 to 40 years of experience in developing and maintaining mission critical IT systems for IT vendors or IT users in Japan.

Members recorded information not just about the basic events that transpired during IT accidents but also about outcomes of the events and the countermeasures taken against them. Forty two cases were summarized.

4.2.2. Method for Case Analysis

First, causes of IT accidents were classified into three categories (product fault, human operation fault and environmental change), which are the same as those mentioned in section 2.

We shared the definition of the system described in Figure 3 and used this to further differentiate whether or not by introducing the on-demand safety system it would have been possible to prevent service failures and ease their negative effects.

Moreover, the following procedures were used to avoid biasing the investigation and analysis.
- Members in the sectional meeting of IPA, who were from different companies and offered the cases, performed analysis and evaluation independently without any interference from each other.
- The analysis was summarized after all of the results were reviewed and corrected in the final sectional meeting.

4.2.3. Results of Analysis

Figure 4 shows the results of the analysis of accident causes. Among the 42 cases, approximately 74% were due to product faults, which is nearly the same rate as that seen in the 94 IT accidents mentioned above. This confirmed that activities related to upgrading product quality, which have been focused on thus far, are important.

We also determined that the ratio of cases where it was possible to have prevented service failures or ease their negative effects if the on-demand safety system had been implemented was 59.5%, as shown in Figure 5.
5. Consideration

Several lessons can be learned from the fact that service failures or their negative effects could have been prevented or eased in approximately 60% of the cases by implementing additional safety functions and safety operation functions.

1) The manageable dependability model, which explicitly introduces additional safety functions and safety operation functions that are distinct from functions utilized in traditional system dependability, is thought to be effective for improving dependability of IT services.

2) Although the additional safety functions and safety operation functions may have been implemented as a result of voluntary efforts of individual field engineers, we are not aware of any systematic and organizational scheme to develop them. We believe that dependability of IT services will be improved by organizational efforts to develop and share among IT services tools to implement the additional safety functions and safety operation functions explicitly demonstrated in the proposed model. Further benefit will be derived from introducing approaches to obtaining feedback from lessons learned while applying these tools to field services and from continually enhancing the tools over the long-term.

6. Conclusion

We clarified the functional elements (the additional safety functions and the safety operation functions derived from a point of view of manageability) of the dependability of IT services underlying social and economic infrastructure and systematized the overall structure of this dependability. We are considering specific approaches to developing the functions as well as the tools [19] to implement them in actual field services.

However, difficult issues still remain before improvement in dependability can be realized in practice. We have to verify whether the tools suggested in the report can be used in the actual IT departments of companies that offer social and economic infrastructure services. We aim to practice verification by developing the tools, publishing the outcomes, and introducing the technologies to the actual systems. However, as far as we know, companies currently do not contain divisions that are primarily responsible for the proposed functions (additional safety and safety operation). Even when there are divisions charged with putting the functions into practice, we have had difficulty identifying who exactly is responsible since the role of developing the functions is distributed among many divisions such as an IT development division, operation planning division or IT operation and maintenance division. We aim to execute the verification of our technologies by addressing the relevant issues not only from the engineering standpoint, but also from that of management.

7. Acknowledgement
A Model for Manageable Dependability of IT Services Associated with Social and Economic Infrastructure
Hiroshi Ohtaka, Koichiro Oshika, Masashi Gotou, Tsutomu Yoshitani, Yoshiaki Fukazawa

Regarding this research, Dr. Seishiro Tsuruho, former president of IPA SEC, Dr. Koichi Matsuda, president of IPA SEC, members of project MIERUKA of IPA SEC and other related individuals have worked with us and provided support. We are deeply grateful to them.

8. References