World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:2, No:8, 2008

Research on the Survivability of Embedded Real-time System

YongXian, JIN

Abstract**—**Introducing survivability into embedded real-time system (ERTS) can improve the survivability power of the system. This paper mainly discusses about the survivability of ERTS. The first is the survivability origin of ERTS. The second is survivability analysis. According to the definition of survivability based on survivability specification and division of the entire survivability analysis process for ERTS, a survivability analysis profile is presented. The quantitative analysis model of this profile is emphasized and illuminated in detail, the quantifying analysis of system was showed helpful to evaluate system survivability more accurate. The third is platform design of survivability analysis. In terms of the profile, the analysis process is encapsulated and assembled into one platform, on which quantification, standardization and simplification of survivability analysis are all achieved. The fourth is survivability design. According to character of ERTS, strengthened design method is selected to realize system survivability design. Through the analysis of embedded mobile video-on-demand system, intrusion tolerant technology is introduced in whole survivability design.

Keywords**—**ERTS (embedded real-time system), survivability, quantitative analysis, survivability specification , intrusion tolerant

I. Introduction

SURVIVABILITY proposed by Barnes *et al.* [1] refers to the ability of a system can provide basic services when it is under the situation of attacks, failures and accidental events. In recent years, network information system survivability has been paid universal attention and mainly focuses on the following: (1) Research on the definition of survivability. First, survivability is defined from different application areas: reference [2] makes the definition from network system point. Survivability refers to the ability to provide necessary services and recover itself when the system suffers attacks, failures and accidents; reference [3] gives the definition from the view of software engineering. Survivability is available degree of necessary functions in the system when some of its functions are destroyed. Second, survivability is defined according to certain abilities that network information system survivability should have, such as withstanding certain types of attacks [4], conducting fault tolerant processing to some mistakes [5] and having detecting intrusions [6] etc. (2) Research on the survivability of network communication system. It studies system survivability by analyzing connectivity between hardware and link of communication network [7,8]. (3) Analysis and evaluation for network information system survivability. At present the majority proposes the qualitative analysis method of survivability based on the attribute definitions the system survivability should possess [2,9]. (4) Survivability design for network information system. There are two main ways: The first is called new redesign method [10]. Survivability requirement is imported at the beginning of the system design. Survivability requirement is as a necessary precondition and it is throughout the entire life cycle of the system design. Finally, a new system with survivability will be established; the second is called as strengthened design method. On the basis of the existing system, the enhancement technology of survivability, such as intrusion detection, failure isolation, redundancy and adaptive techniques, is joined to improve and enhance system survivability [11,12]. System survivability has become a new direction established on the basis of the traditional security doctrine, dependability calculation. However, there are few studies on the survivability of embedded real-time system.

In recent years, embedded real-time systems (ERTS) have been used more and more in industry, communications and aerospace. Due to some factors such as application, environment, an ERTS has the following characters. (1) In a traditional sense, the safety of system is that it must be reliable absolutely, but it is too difficult and costly to implement. From the new security view, it is to ensure the system can provide critical services or functions continuously after suffering failures or disasters, and survive in order to avoid greater losses. (2) Real-time characters. Survivability asks the system not only to maintain critical functional tasks, but also to have non-functional time limitation, that is, the system must respond to disasters and recover in a period of time. (3) Limited resources. It is impossible to guarantee high dependability design for every component (or every function), in other words, only high dependability design for critical components can be guaranteed or else resources or cost that the system design requires may be more than the system can bear. So, in order to effectively raise and improve survivability of an ERTS in the face of disasters or accidental failures, survivability analysis and studies for ERTS is necessary.

II. Survivability Problem Of ERTS

With the appearance of more and more powerful processors, designers (or users) have a growing hope that more and more functions are included or expanded in the ERTS. For a system, high dependability of each component (or each function) need to be ensured, and it will have or expand more functions, so resources or cost required for system design may be more than the limit users would like (or can) provide. But then, it will not be feasible yet if the dependability design is achieved by limiting certain functions users expect to save resources or cost.

This work was supported by the Natural Science Foundation of Zhejiang Province (Y104105)

Yong-xian JIN is with College of Mathematics, Physics and Information Science, Zhejiang Normal University, China (E-mail: jyx@zjnu.cn)

Similarly, the way of adding additional security checking measures (in early systems, security is achieved through the "prevention" and "check" technology) in order to improve the system dependability may have an adverse impact on the overall design thereby increasing the risk of the system itself [13]. In fact, when suffering accidents or attacks, some components of the system will fail, but it will not necessarily generate disastrous results and it may still survive as long as critical tasks (services or functions) can be maintained. This is a thinking of "toleration", in another word, survivability.

In the development of a survivable ERTS, if the high dependability of non-critical components (functions) cannot be guaranteed, then that of critical components must be guaranteed. In order to achieve this, co-design of dependability and function is feasible, known as the survivability design. An ERTS designed by the survivability thinking will run according as all the service functions contained in S_1 if there is no fault (or damage). Once the system falls under harm or disasters, it can respond to the harm by demoting services (or reducing functions), that is to say, the survivability service specifications can be moved one to another, and with the increase of harm degree, the number of services (or functions) maintained by the system will reduce gradually. Finally, there are only critical services or functions in S_n, while these corresponding components carrying out them possess the highest dependability of bearing disasters or accidents, in other words, these components can keep running even if they get harm, so the system survivability is improved. Fig. 1 shows relationships among functions and criticalness of services as well as possibility of happening in the survivability service specifications set.

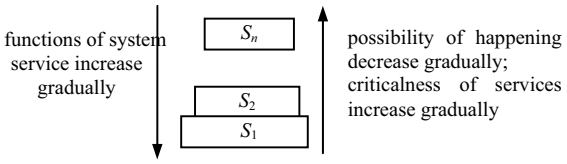

Fig.1 set of survivability service specifications

III. Survivable Analysis For ERTS

A. Framework of Survivability Analysis

Survivability analysis of ERTS can provide system design recommendations according to the survivability specifications in the system design phase, so that the system may provide different grades services for users by survivability service specifications defined beforehand, but also its factual survival ability can be evaluated and mended after the system being established. At present, the SNA (Survivable Network Analysis) has been widely used in survivability analysis of network information system[2], and it is achieved by four steps: (1) system definition, it will educe business tasks and function requirements of the system; (2) basic ability definition, it will select basic services and useful resources of the system and recognize basic components; (3) definition on ability of endangering security, it will recognize components of endangering security; (4) survivability analysis, it will present the qualitative evaluation of survivability by recognizing basic components and components of endangering security. An amount of research starts on the basis of the SNA method, however, the SNA method can only make qualitative analysis to "3R" (Resistance, Recognition, Recovery) capability of the system, but it does not present specific quantifiable indicators of survivability. On the basis of the SNA, reference [14] respectively establishes parameter models for 3R capability mentioned above and proposes a kind of "quantification" analysis method for information system, but this method is not suitable for ERTS. This paper proposes a survivability analysis framework for the ERTS and a calculable quantification scheme about the three indicators, which are Resistance, Recovery and Response. First several concepts are given.

(1) The quantification concept of survivability for the ERTS. System survivability ought to relate to the following factors: services which the system can provide, services state, services environment and changes of the services state. It can be expressed with the following form: $A=\{S, E, D, T\}$. In this form, $S=\{S_1, S_2, \ldots, S_i, \ldots, S_n\}$ is a set of survivability services specifications, including functional and non-functional specifications that the system services can accept; E is the services value factor, i.e., factors of affecting system services as well as their possible values; D stands for the environmental state that can bring changes of system services, that is, environmental conditions where system services exist; T is a set that effective system states change, i.e., when the system suffers disasters, services will move from one survivability service specifications to another, so T is one subset of all possible combinations $S\times S\times D$. If an ERTS can meet survivability specifications mentioned above, then the system is survivability.

At present, there are a lot of definitions about survivability, but these definitions cannot provide system developer with a standard to determine whether a system is survivable, that is to say, the system survivability cannot be determined because of the lack of specific performance indicators. This paper defines the system survivability using a specifications form and makes developers understand the specific meaning of the system survivability as well as specifications a survivable system should accord; in this way it is conducive to process survivability evaluation and quantitative analysis.

(2) Critical services. They are services the system must provide when suffering accidents or disasters.

(3) Atomic task. An atomic task of an ERTS is a task that only completes one specific event, and this task cannot be decomposed or it need not be. Several atomic tasks can make up of a disaster scene event.

(4) Disaster scene. It is the scene composed of a series of events, which happens because some critical service of the system is attacked. Here an event refers to the state change of critical services caused by attack. This is likely to be completed either by a task composed of events with common purpose, or by a task including events with a special purpose, but ultimately it may be completed by being decomposed a number of atomic tasks.

According to conducting definitions and decomposition

to the entire survivability analysis process, and making the analysis process be standardization and simplification, the survivability analysis framework is proposed (shown in Fig.2). It plays certain role in standardizing survivability analysis of ERTS; at the same time it makes survivability analysis easy to process the platform design. The survivability analysis framework has main steps as follows:

(1) Define the survivability service specifications set. According to service types (including task criticalness, possibility of resulting in disasters, time limitation of responding to disasters) the system can accept, changes of the system state, environmental conditions of the system survivable services, factors of affecting the system services and some other aspects, system designers classify functional and non-functional requirements and generate different service specifications. Finally, these different service specifications consist a survivability service specifications set $S=\{S_1, S_2,\ldots, S_i,\ldots S_n\}$, where with the increase of i value, possibility that S_i happens disasters will decrease, at the same time, services scale of S_i will get smaller, but its criticalness is increasing. S_n stands for service specifications having the highest criticalness (shown in Fig. 1), and these service specifications are the basis of survivability analysis.

(2) Establish the relationship-mapping model. In the development of an ERTS, there must be corresponding documents such as service and design specifications of system, service specifications elaborates all kinds of services the system provides, while design specification explains the design way and function implementation of all kinds of services and these services can be completed by specific components. There is a relationship of "one vs. one" or "many vs. one" between these components and all kinds of services of the system, and survivability service specifications S_i depend on those services, so mapping relationships also exist between S_i and services. Depending on service and design specification of system, the relationship-mapping model M among services, components and S_i can be established, and this helps to determine critical services and components of the system. In addition, survivability service specifications S_i can be constrained and simplified on the basis of the model.

(3) Determine the critical services and components. Critical services are determined according to worth of all kinds of services in the system as well as disaster degree after services failing, and then these critical services will be mapped to the relationship-mapping model to determine critical components.

(4) Generate the test scheme. Bugs are analyzed and leaks are found according to the system-running environment, the system services, day-to-day log of failing responses and failure situation. Disaster scenes set is made up by selecting a number of classic disaster scenes for each critical service; then this set will be applied to critical components, thereby determining leaks of critical components; finally, on the disaster scenes set of each critical service, disaster scenes will be divided into combinations of a number of atomic tasks, next according to actual situations, every atomic task will be divided into a series of implement events, finally, built up the test vector (critical services, disaster scenes, atomic tasks, underlying events); some test vectors constitute a vector space named survivability test warehouse; at the same time bug vectors (critical components, disaster scenes, underlying events, bugs) of critical components will be built up and the set of bug vectors is called bug warehouse of the system. Warehouse of test and bug are open and they can be updated continuously in the analysis process.

(5) Survivability quantitative calculations. According to characteristics system survivability should have, and combining with real-time limit, survivability of ERTS is quantified from three aspects respectively which are Resistance, Recovery and Response, survivability performance will be educed, then we can evaluate the system survivability and present improving recommendations according to evaluation report.

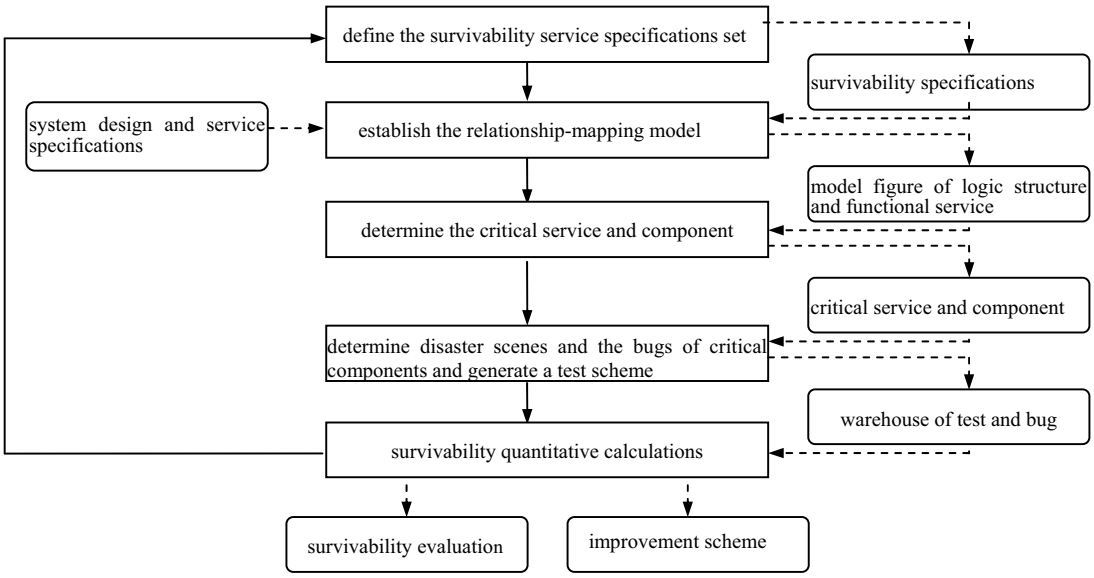

Fig. 2 survivability analysis framework of ERTS

B. Survivability Quantitative Calculation

Survivability quantitative calculation is the kernel of the survivability analysis. Next these quantitative calculations methods are expounded.

(1) Resistance power. The resistance power of ERTS stands for the ability that system deals with disasters when they occur. Calculating parameters are defined as follows: Generally a disaster scene contains a number of disaster triggering steps. D_{jk} denotes the risk degree value of the k_{th} step disaster triggering in the j_{th} kind of disaster scene, and the bigger D_{jk} is, the higher risk degree is. H_{jk} denotes the easy degree value to happen of the k_{th} step disaster triggering in the j_{th} kind of disaster scene, and the bigger H_{jk} is, the easier it happens. P_{jk} denotes the success probability of the k_{th} step disaster triggering in the j_{th} kind of disaster scene, and the bigger P_{jk} is, the bigger the success probability is. L_j denotes the grade included in the survivability service specifications S_j which is mapped by corresponding critical service of the j_{th} kind of disaster scene, and the service criticalness will be raised with increase of the grade. If Dt_{jk} denotes the test value of risk degree of the k_{th} step disaster triggering in the j_{th} kind of disaster scene, then in the j_{th} kind of disaster scene, after m steps of triggering, the test value of risk degree can be expressed as follows:

$$Dt_j = \sum_{k=1}^{m} Dt_{jk} \tag{1}$$

The bigger Dt_j is, the higher risk degree is. As Dt_{jk} has something to do with D_{jk} H_{jk} P_{jk}, then Dt_j can be expressed by

$$Dt_j = \sum_{k=1}^{m} Dt_{jk} = \sum_{k=1}^{m} (D_{jk} * H_{jk} * P_{jk}) \tag{2}$$

After synthesizing n kinds of disaster scenes, the resistance power of the system $F_{\text{Resistance}}$ is

$$F_{\text{Resistance}} = \sum_{j=1}^{n} (L_j * Dt_j) = \sum_{j=1}^{n} (L_j * \sum_{k=1}^{m} (D_{jk} * N_{jk} * P_{jk})) \tag{3}$$

In formula (3), initial values H_{jk} and P_{jk} are given after designers test the system, and during the running they can be adjusted according to the actual situation; initial values D_{jk} is set in the system requirement specifications, and it can be modified accordingly with the occurrence of actual events; initial values of L_j is given in the survivability service specifications. The bigger the $F_{\text{Resistance}}$ is, the stronger the resistance power of the system is.

(2) Recovery power. Performance decline and reduction of service functions are temporary after the system suffering accidents. The system will continue to provide services by some measures like reconfiguring or replacing failure components. The recovery power of system refers to the ability that the system recovers its critical services to work normally when accidents occur, and it has something to do with importance degree of critical services, probability to recover critical services successfully and time to recover critical services. In calculation parameters can be defined as follows: V_i denotes the importance degree value of the i_{th} critical service, and the bigger the value is, the more important it is; r denotes the number of critical services in the system; Pc_i denotes the probability of recovering the i_{th} critical service successfully, and the bigger the value is, the bigger the possibility of recovering it successfully is; Ct_i denotes the time the i_{th} critical service costs in order to resume normal work; Mt_i denotes the worst-case time of recovering the i_{th} critical service. Therefore, the recovery power that synthesizes r critical services F_{Recovery} is

$$F_{\text{Recovery}} = \sum_{i=1}^{r} (V_i * Pc_i * (Mt_i - Ct_i)/Mt_i) \tag{4}$$

In formula (4), the value of V_i is determined by system designers according to the importance degree of each service; Initial values of Pc_i and Ct_i are given after the system test, and during the running they can be updated continuously after the system is put into operation; Mt_i is set by the system requirements. The bigger the F_{Recovery} is, the stronger the recovery power of system is.

(3) Response power. In order to meet real-time response character of the system, the response power is calculated from the time that the system responds to disaster triggering, the probability of triggering successfully and the risk degree of the disaster scene. Parameters of calculating response power are defined as follows: Rt_{jk} and Rmt_{jk} respectively denotes the response time and the worst-case response time to the k_{th} step disaster triggering in the j_{th} kind of disaster scene; D_{jk} and P_{jk} are defined like above. So synthesizing n kinds of disaster scenes and m steps of triggering, the response power of the system F_{Response} is

$$F_{\text{Response}} = \sum_{j=1}^{n} \sum_{k=1}^{m} (D_{jk} * (Rmt_{jk} - Rt_{jk}) / Rmt_{jk} * P_{jk}) \tag{5}$$

In formula (5), Rmt_{jk} is set by the system requirements; the initial value of Rt_{jk} will be given after the test and it can be updated continuously after the system is put into operation. The bigger the F_{Response} is, the stronger the response power of the system is.

Survivability quantitative calculations can be implemented by two ways: real and simulation test to the system. Real test is to get the values of survivability quantitative when accidents happen. In this way, accurate real results can be obtained but it may destroy the ERTS, so the simulation test is used widely, that is, we simulate real environment by simulation software and then trigger the ERTS using the data of disaster scenes.

IV. Survivable Analysis Platform For ERTS

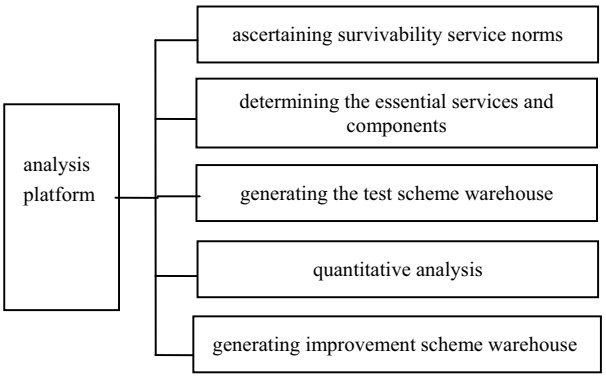

Fig. 3 survivability analysis platform for ERTS

In order to simplify the analysis process, and take into account the design reusability, we may design a survivability

platform, as shown in Fig. 3.

(1) Module of ascertaining survivability service specifications. This module mainly ascertains the survivability service specification set S, and S_i in S is mainly ascertained by the system designer according to user demand; at the same time, S_i can be limited and simplified appropriately according to the relationship mapping model established by steps of the survivability analysis framework.

(2) Module of determining the essential services and components. The kernel task of this module is to determine the essential services set F and the corresponding essential components set Z. The acquirement of essential components is implemented by mapping essential services. Specifically including: (i) the system automatically generates the current essential services set F according to parameters of the specification S_i. (ii) The system automatically abstracts all the components from the logical structure figure and lists the components set. (iii) Map the essential services set F to the components set and generate the essential components set Z. (iv) On the basis of essential services, we can make use of the original function specification of essential components to further improve the definition and design of essential components.

(3) Module of generating the test scheme warehouse. This module mainly searches frail components in the essential components set Z and generates test schemes aiming at frail components. The establishment of test schemes need use former disaster scenes and system failures for reference and the test process performs using simulation and emulation mode, finally test schemes will enter the test scheme warehouse. On one hand, the design of the test scheme warehouse makes management convenient; on the other hand, it also can improve test schemes' use efficiency and reduce the complexity of test work. The warehouse is open and need maintain and update unceasingly.

(4) Module of quantitative analysis. This module mainly performs quantitative analysis for an embedded real-time system making use of the mathematic model in quantitative analysis above, so that we can evaluate the system's survivability quantitatively from three aspects which are resistance, recovery and response, and form an evaluation report, and then it can be as a basis of bringing forward an improvement scheme.

(5) Module of generating the improvement scheme warehouse. An improvement scheme is educed on the basis of quantitative analysis, and its generation is the result of mapping quantitative analysis data, that is, mapping to improvement scheme warehouse from quantitative analysis data. In addition, the improvement scheme warehouse is an open database, which need maintain and update regularly.

V. Design Of Survivability For ERTS Based On Intrusion Tolerance Technology

Above, we have introduced two ways of survivability design for network information system, one is new redesign method, and the other is strengthened design method. Because the new redesign method needs to re-build system model and infiltrates survivability system requirements into every stages of system design, so its cost is comparatively soaring. On the other hand, current technology is not yet mature. So, it is difficult widely used in the actual system design. In view of defects of the new redesign method, we chose the strengthened design method into ERTS to achieve the survivability of the existing system. Integrating technical feasibility and design cost, we join intrusion tolerance into the survivability design of ERTS to strengthen its survivability.

Intrusion tolerance technology develops with the network security. For system security problems, intrusion tolerance technology is used when the system has been attacked to guarantee the system with an uninterrupted normal operation. When ERTS is attacked by the intrusion, it can still carry out its essential services, not because of system failure or system crash cause huge losses, and this is intrusion tolerance.

The objective of intrusion tolerance is how to make ERTS still guarantee the completion of its key activities in the presence of successful intrusion. Therefore, it must have the following features [15]: (1) Self-diagnose capability: Invasion tolerance still relies on intrusion detection or assessment system, which is also called as an intrusion tolerance trigger. By testing the effectiveness of the local system or system is estimated to be attacked, then adjust the system structure and redistribute resources, so as to achieve the purpose of continuing service. (2) Fault isolation capability: If self-diagnose module finds some operations that may seriously affect the operation of the follow-up system, isolation mechanism will isolate suspicious operations to special region. Against segregation of data and operations, when ruling that the system is indeed attacked, the isolated operations will be removed. Otherwise, it will be combined with the correct systems. (3) Recovery and reconfiguration capacity: The invasion tolerant system must have ability to revise all of the data affected by attacks, but can not use simple regression strategy. System must ensure that the uncontaminated is not part of restoration, only restore infected files and retain most of user's work.

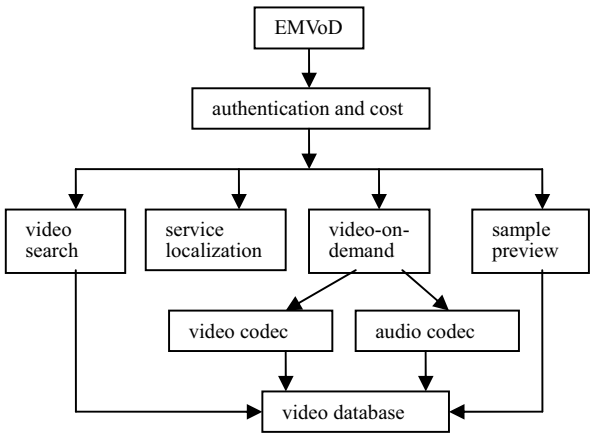

Fig. 4 EMVoD architecture of system components

Below, we take the Embedded Mobile Video on Demand (EMVoD) as an example to illustrate the survivability design

method. An EMVoD system includes the following major functions: user access, service localization, authentication and cost, samples preview, video-on-demand and so on. Each function requires one or more corresponding components to complete, such as function of authentication and cost needs user authentication component and user cost component, function of samples preview needs user preview component to complete corresponding services.

Fig. 4 gives EMVoD architecture of system components. If a component of EMVoD system breaks down due to invasion attacks or other reasons, the user's request isn't bound to be met, so the survivability design is helpful to guarantee execution of system essential services.

Fig.5 shows the survivability architecture of EMVoD system, it shows the collaborative relationships among various modules, and these modules realize the survivability of EMVoD system together. Here, we define "abnormity" of system as: all the system information which leads to errors or breakdown in system and makes it not complete critical services on time. Among these modules:

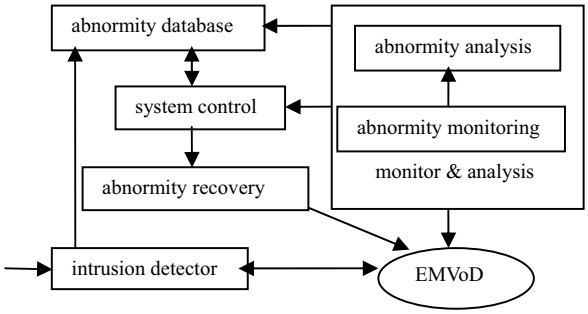

Fig. 5 survivability EMVoD system architecture

Intrusion detector: This module is mainly used to protect EMVoD system and enable external service requests not directly contact with EMVoD system. Intrusion detector carries dynamically on the primary treatment to system services, prevents malicious intrusion which can be detected and reports the invasion attacks to abnormity database, at the same time ensure that the system control module only to handle those attacks who threat to the critical services.

Monitoring and analysis: This module has mainly two main functions, namely, abnormity monitoring and abnormity analysis. Abnormity monitoring mainly used to simulate the services of EMVoD system, which send test signal to critical components of EMVoD system and receive the feedback signal from it. For example, if video-on-demand component meets the invasion attack or breaks down and fail to fulfill its real-time services, then abnormity monitoring will not accept the correct feedback signal, so judges EMVoD system abnormality, abnormity monitoring will notice abnormity analysis the abnormal information. Abnormity analysis is mainly used to analysis the data sent by abnormity monitoring. If it finds the abnormity or unusual characteristics of the data, the module will notify system control module and report the abnormal invasion to abnormity database. Monitoring and analysis mainly completes response steps of system.

System control: It is mainly used to set system security strategy, receive the abnormity information sent by monitoring and analysis and accordingly send control instructions to abnormity restoring.

Abnormity restoring: this module implements some security strategy sent by system control. According to the analytical result of abnormity analysis and strategy made by system control, Abnormity Restoring makes corresponding action on EMVoD system to adjust its state. The state of EMVoD system can be divided into normal, degraded and attacked state. According to various states, Abnormity restoring uses in different ways, such as the attacked state of EMVoD system, a recovery operation will be need. But when it is normal state, only need to improve system security level.

Abnormity database is mainly used to collect and preserve attack actives or abnormal information what the system suffered, which will help improve the deficiencies and loopholes of EMVoD system.

VI. Conclusions

Survivability research has become a hot topic of information system security problems currently. Embedded real-time system is a special class of information systems, survivability analysis and design for it will enhance its security and reliability.

This paper proposes a method of survivability analysis for ERTS and makes attempt to quantitative calculation, and in order to meet the real-time character of ERTS, real-time response power is introduced in quantitative calculation. The survivability analysis method for ERTS has the functions as follows: (i) Comparison of the survivability power of same system under different environments. It can provide reference for the system in choosing a running environment. (ii) Comparison of survivability power of different system under the same environment. It can judge which system has the highest survivability power, and then provide reference for some application environment in choosing a suitable system. (iii) By conducing analysis, evaluation and improvement continually, we can judge which components (hardware, software) play decisive roles in the survivability power of the system, thereby providing reference for improving the system structure. In order to simplify the analysis process, and take into account the design reusability, we design a survivability analysis platform. Finally, we present a strengthened survivability design method based on the intrusion tolerance technology to achieve the survivability of ERTS.

References

[1] Barnes A, Hollway A, Neumman P G. Survivable computer-communication systems: The problem and working group recommendations[R]. Washington: US Army Research Laboratory, 1993.
[2] Mead N R., Ellison RJ, Linger R C, *et al*. Survivable Network Analysis Method[R]. Carnegie Mellon University: Software Engineering Institute Technical Report, 2000.9.
[3] Knight J C, Strunk E A, Sullivan K J. Towards a Rigorous Definition of Information System Survivability. Proc. of DARPA Information Survivability Conference and Exposition[C]. IEEE Computer Society Press, 2003:78-89.

[4] Fung C, Chen Y L, Wang X Y, *et al*. Survivability analysis of distributed systems using attack tree methodology. Proc. of the IEEE Military Communications [C]. IEEE Computer Society Press, 2005: 583−589.
[5] Hiltunen M A, Schliching R D, Ugarte C A. Building survivable services using redundancy and adaptation[J]. IEEE Trans. on Computers, 2003,52(2):181−194.
[6] Bowen T, Chee D, Segal M, *et al*. Building survivable systems: An integrated approach based on intrusion detection and damage containment. Proc. of the DARPA Information Survivability Conference and Exposition[C]. IEEE Computer Society Press, 2000: 25−27.
[7] Jha S, Wing J, Linger R, Longstaff T. Survivability analysis of network specifications. Proc. of the Dependable Systems and Networks[C]. IEEE Computer Society Press, 2000: 613−622.
[8] Snow A P, Varshney U, Malloy A D. Reliability and survivability of wireless and mobile networks[J]. IEEE Computer, 2000,33(7): 449−454.
[9] Gao Z X, Ong C H, Tan W K Survivability assessment: modeling dependences in information system. Proceeding of 4th IEEE/CMU/SEI Information Survivability Workshop[C]. Vancouver, Canada, 2001.2-8.
[10] Ellison R, Fisher D, et al. Survivable Network System Analysis: A Case Study[J]. Software, IEEE,1999, 16(4):70~77.
[11] Ma Q K, Xiao L L, Yen I L, *et al*. An adaptive multiparty protocol for secure data protection. Proc. of the Parallel and Distributed Systems[C]. IEEE Computer Society Press, 2005. 43−49.
[12] Zhang L J, Guo L, Wang W. The Research Summarization of Technology of Network System Survivability Evaluation and Enhancement [J]. Computer Science, 2007,34(8):30-33. (in Chinese)
[13] Perrow C. Normal Accidents: Living with High-Risk Technologies[M]. Princeton University Press: Princeton, New Jersey, 1999.
[14] Lin X G, Xu R S, Xiong H. A Framework of Quantitative Analysis for Information System Survivability [J]. Journal of Electronics & Information Technology, 2006,28(9):1721-1726.(in Chinese)
[15] Linger R C, Mead N R, Lipson H F. Requirements Definition for Survivable Network Systems [R]. [s. l.]: System Design Laboratory, SRI International Press, 2002.