UDC 004.052:71.001.332:336.71

R. LAKHYZHA

National Aerospace University named after M. E.Zhukovskiy "KhAI", Ukraine

FEATURES OF BANKING INFORMATION SYSTEMS DEPENDABILITY TAXONOMY

Banking information systems (BIS) evolution history and general structure are considered. The main BIS requirements are analyzed. The dependability attributes with regard to BIS are determined.

Banking information systems, bank automation system, dependability, security, integrity, threats

Introduction

The life of modern people could hardly be imagined without services that banks provide. Deposit taking, crediting, money transfers etc. are among them. Bank services designed, for example, for individuals are used by many people and are rapidly expanding in recent years. They are becoming more suitable because of installation of ATMs with a great number of functions at convenient places and expansion of operating time at branch offices. IT systems providing services used by a lot of people are required to make available to users desired services whenever they are wanted and at the expected service levels. That means such systems need to be dependable.

This problem is of current importance because modern information technologies are one of the main means in the bank competition for priority positions at financial market and for clients' attraction. So it's necessary to consider the main features of dependability with regard to banking information systems.

A Brief Overview of Banking Information Systems

Banking information systems (BIS), by definition of the National Bank of Ukraine (NBU), are hardware-software means complexes, which are intended for banks and their branches to make solutions of their own tasks in the fields of automation and NBU information systems interaction. They consist of bank automation systems (BAS), intrabank payment systems etc. combining both hardware and software.

The history of BIS originated in the late 1950s and early 1960s [1]. At that time banks began to use computers for bookkeeping and some applications such as check processing, and as they found that even the slow and expensive computers of that era were much cheaper than a lot of clerks, they proceeded to automate most of the rest of their operations during the 1960s and 1970s.

A typical banking system has a number of data structures. There is an account database, which contains each customer's current balance together with previous transactions, a number of ledgers, which track cash and other assets on their way through the system; various journals, which hold transactions that have been received from teller stations, cash machines, check sorters (in foreign bank practice) and so on, but not yet entered in the ledgers; and an audit trail that records what and when staff member did.

The general automation banking system structure scheme is presented on fig. 1.

Banking systems include bookkeeping systems that record customers' account details and transaction processing systems such as cash machine networks and interbank money transfer systems that feed them with data. They are important for a number of reasons.

First, bookkeeping was for many years the main business of the computer industry, and banking was its most intensive area of application. Personal applications

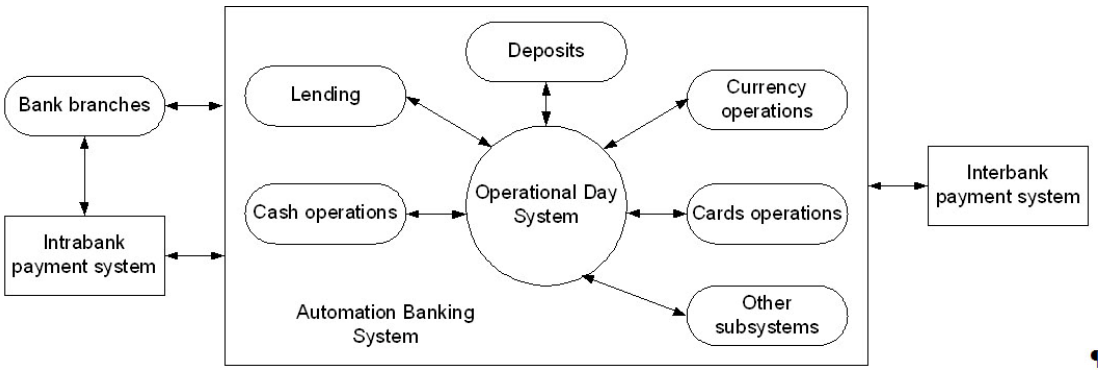

Fig. 1. Automation banking system structure

such as Notepad and Opera browser might now run on more machines, but accounting is still the critical application for the common business. So the protection of bookkeeping systems is of great practical importance.

Second, transaction-processing systems were the applications that launched commercial cryptography. Banking applications drove the development not just of encryption algorithms and protocols, but also of the supporting technologies, such as tamper-resistant cryptographic processors.

These processors provide an important and interesting example of a trusted computing base that is quite different from the hardened operating systems discussed in the context of multilevel security. Many instructive mistakes were first made (or at least publicly documented) in the area of commercial cryptography. The problem of how to interface crypto with access control was studied by financial cryptographers before any others in the open research community.

Third, an understanding of basic electronic banking technology is a prerequisite for tackling the more advanced problems of electronic commerce in an intelligent way. In fact, many dot-coms fall down badly on basic bookkeeping, which is easy to overlook in the rush to raise money and build a Web site.

Finally, banking systems provide another example of multilateral security, but aimed at authenticity rather than confidentiality. A banking system should prevent customers from cheating each other or the bank; it should prevent bank employees from cheating the bank or its customers; and the evidence it provides should be sufficiently strong that none of these principals can get away with falsely accusing another principal of cheating.

So the main goals of bank automation systems (BAS) introduction were:

1. The increasing of bank opportunities of carrying out operations on financial markets and service activities; time reduction for operations carrying out;
2. Staff quantity optimization;
3. Clients service quality improvement - continuous servicing guarantee, raising the level of staff skill;
4. Bank operations prime cost reduction;
5. Ensuring integration into united banking networks.

Dependability and Its Attributes With Regard to BIS

According to [2, 3] dependability is the ability to deliver necessary services that can justifiably be trusted. Dependability is an integrating concept that encompasses several attributes.

The dependability specification of a system must include the requirements for the dependability attributes in terms of the acceptable frequency and severity of failures for the specified classes of faults and a given use environment.

One or more attributes may not be required at all for a given system. In order to choose necessary BIS dependability attributes let's look for the main banking information systems requirements [4 – 6].

They are:

1. Functional completeness - the set of functions of the system should give an opportunity to carry out all necessary operations of the bank;

2. Flexibility – BIS should have an opportunity to extend and develop in two directions: quantitatively – by increasing quantity of branches or clients - and qualitatively - by expansion of bank operations and services spectrum. Not only the development contractor, but also bank specialists should develop the system;

3. Reliability – means that BIS must ensure the work of a plenty of users which can at the same time insert, correct documents (accounts and contracts), form reports without any conflicts concerned with simultaneous access to the data;

4. Real timing scale maintenance – after document insert and accounting transaction carry out new accounts status should immediately be able for all users and could be using in their further work;

5. System integration – BIS must consist of units, which are informational and functionally connected with each other. Informational connection means that all system components work with common database. It makes possible to avoid doubling and ensures data integrity and coordination.

6. Bank multidivisional work ensuring. The fulfillment of this requirement in ideal is realized by distributed data processing in on-line mode. But this method is still rather expensive and not all banks can provide it. Therefore technologies identity is more practicable method. That means that systems of all levels must have identical data structure, the same interfaces and software development tools.

7. Security and protectability. BIS must be protected both inside - from possible misuses by bank staff - and outside - from various tries to disclosure bank secrets and machinations with its money.

After analyzing these requirements it's possible to formulate the main attributes for BIS dependability: availability, reliability, integrity, security, safety, maintainability and survivability. The schema of the banking information systems dependability taxonomy is shown on fig. 2.

Availability means that the computer system's hardware and software keeps working efficiently and that the system is able to recover quickly and completely if a disaster occurs.

Reliability is continuity of correct service. Safety is absence of catastrophic consequences on the users and the environment.

Maintainability is ability to undergo, modifications, and repairs.

Survivability is the ability to minimize deterioration and to keep in acceptable limits capacity and quality of provided service in the case of failure.

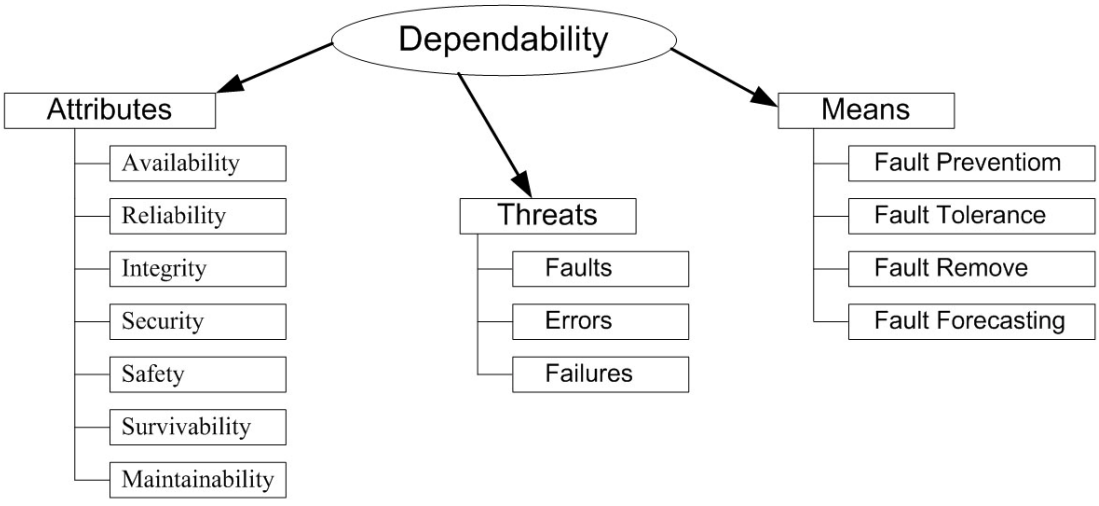

Fig. 2. BIS dependability taxonomy

This is a decree of the National Bank of Ukraine [7] that obliges all Ukrainian banks to provide their customers with the continuous service. From the technical point of view, this entails the necessity to build the reserve centers that guarantee quick recovery of the functions of the banking system in case of an accident or a crisis.

As an example of dependability assurance let's study the project that was implemented by Kvazar-Micro for First Ukrainian International Bank in 2004 [8]. The constructed synchronous reserve center now performs the full range of the necessary functions. It provides full accessibility, safety and relevance of all data stored and processed by the bank's information system even in case of a complete destruction of the main center. Restoration of availability of the external and internal communications (the client service renewal) based on the reserve center is done in about several hours. The information storage systems of the main center and the reserve center are connected by two fiber-optic channels each about five kilometers long. The physically independent fiber-optic channels are laid by different routes, so damage of the one does not cause breakdown of the whole system. Relevance of the information stored in the reserve center is maintained by means of a distant replication. The access to information is provided through the dispersed local network (local network from the logical point of view physically consists of two parts located in the main center and the reserve one).

The reserve center is equipped with the preserved work places, automated telephone system, telephone channels and the channels for data transfer, systems for continuity of service, conditioning, and physical safety. Almost all critically important systems of the main center are duplicated based on the reserve center.

A secure computer system must maintain the continuing integrity of the information stored in it. Accuracy or integrity means that the system must not corrupt the information or allow any unauthorized malicious or accidental changes in it. It wasn't deliberate, but when a simple software error changed entries in Bank of New York transactions in 1985, the bank had to borrow $24 billion to cover its accounts until things got straightened out and the mistake cost him $5 million in extra interest. In financial environments, accuracy is usually the most important aspect of security. In banking, for example, the confidentiality of funds transfers and other financial transactions is usually less important than the verifiable accuracy of these transactions. For instance, if one purchases 10 million shares of a company's stock, it will likely be in the financial pages soon as a major transaction, so secrecy is not terribly likely. But during the transaction, it would not be good to shift the decimal spot and change each share's price, which would alter the sale price by huge amount [9].

The problem of data security assurance includes several aspects. Firstly, it is flexible, multilevel and effective users' rights regulation. The value of bank information makes special demands for data protection from unauthorized access, especially for management of the processes that can change data state.

Secondly, it is presence of means of data integrity and consistency. These means give an opportunity to monitor input data, to maintain and control data relations, and also to perform data input and modification in transacted mode. Transaction is the set of operations that ensure data conformity support.

Thirdly, it is presence in the system of multifunctional procedures of data archiving, update and control, which ensures data to be safe after software or hardware failures.

The threats to BIS dependability may be divided into three main groups: faults, errors and failures.

A failure is an event that occurs when the delivered service deviates from correct service. It is a transition from correct service to incorrect service, i.e., to system function not implementing. Since a service is a sequence of the system's external states, a service failure means that at least one (or more) external state of the system deviates from the correct service state. The deviation is called an error. The adjudged or hypothesized cause of an error is called a fault [3].

The means of obtaining and establishing high BIS dependability can be divided into next large groups:

- *fault prevention* - prevention of the occurrence or introduction of faults, in particular via the use of rigorous design methods;
- *fault tolerance* - the means of delivery of correct service in the presence of faults;
- *fault removal* - verification and validation, aimed at reducing the number or severity of faults;
- *fault forecasting* - system evaluation, via estimation of the present number, the future incidence, and the likely consequences of faults.

According to [10] there is the fact that fault prevention, removal and tolerance should not be regarded as alternatives, but rather as complementary technologies, all of which have a role to play, and whose effective combination is crucial - with fault forecasting being used to evaluate the degree of success that is being achieved.

Conclusion

Implementation of the crisis-resistant information system allows any bank to minimize the operation risks and to offer the clients a new level of dependability of services provided.

Current article describes the main attributes of BIS dependability. In future research there is a need to make further thorough analysis of BIS threats. Also it is necessary to evaluate more detailed classification of the means to attain BIS dependability.

References

1. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. – New York: John Wiley & Sons, 2001. – 640 p.

2. Avizienis A., Laprie J.-C., Randell B., Landwehr C. Basic Concepts and Taxonomy of Dependable and Secure Computing // IEEE Trans. on Dependable and Secure Computing. – 2004. – Vol. 1, № 1. – P. 11-33.

3. Харченко В.С. Гарантоспособность и гарантоспособные системы: элементы методологии // Радіоелектронні і комп'ютерні системи. – 2006. – № 5 (17). – С. 7-19.

4. Єрьоміна Н.В. Банківські інформаційні системи: Навч. посібник – К.: КНЕУ, 2000. – 220 с.

5. Зацеркляний М.М., Мельников О.Ф. Інформаційні системи і технології у фінансово-кредитних установах: Навч. посібник. – К.: Професіонал, 2007. – 432 с.

6. Королев М.И., Королев Д.М. Информационные системы в банковском деле: Учебное пособие. – Белгород: Издательство БелГУ. 2004. – 293 с.

7. Положення про забезпечення безперервного функціонування інформаційних систем Національного банку України та банків України: Постанова Правління Національного банку України від 17 червня 2004 року N 265 [Електронний ресурс]. – Режим доступу: www.rada.gov.ua.

8. Materials from joint press conference of the First Ukrainian International Bank and Kvazar-Micro took place on July 7, 2004 [Електронний ресурс]. – Режим доступу: / www.kvazar-micro.com.

9. Lehtinen R. Computer Security Basics, 2nd Edition. – O'Reilly, June 2006 – 310 p.

10. Jones C., Randell B. Dependable Pervasive Systems // Technical Report Series CS-TR-839, School of Computing Science, University of Newcastle upon Tyne, April 2004.

Надійшла до редакції 19.02.2007

Рецензент: д-р техн. наук, проф. В.С. Харченко, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Харків.