CONTRIBUTIONS REGARDING OPTIMIZATION OF INFORMATION SYSTEMS IN MONITORING PROCESSES

Dan Vasile OLINICI
University “Politehnica” Bucharest, Department of Automatics and Computer Science, 313 Splaiul Independentei, Bucharest

Abstract: The project proposes the implementation of solutions to optimize systems used in monitoring industrial processes. In terms of architecture, the systems will be developed on the model of distributed network equipment and microcomputers based on the latest technologies to meet the current standards for compliance with the requirements of rapid processing of a large volume of information, the requirements for high reliability, and needs to openly access the informational system.

Keywords: Information systems, Control systems.

1. INTRODUCTION

The information systems perform the following functions:
- to ensure informational support by creating and maintaining a secure database;
- to achieve a consistent information flow;
- to ensure monitoring, control the process in real-time;
- to ensure the presentation of information to users, the main functions of the presentation being as follows:
  - presenting in real-time the guide-operator information type;
  - register the change of status of the process in journals of events and reporting on the screen or to printer;
  - developing operational reports and summary reports using data from the database and / or archives;
  - assist the user in the development of technical analysis and post-crash analysis and issue the resulting reports.

2. INFORMATION SYSTEMS PERFORMANCES

The applied research results from the fact that the system structure will focus on the concrete situation of a process and will lead to developing a system optimized for monitoring and control of the technologic process and inform the decision-makers in formats specific to their tasks and workplace.

Information system performances improving consists in:
- Improving the informational system reliability;
- Increasing the accessibility of the system using WiFi, GSM, GPRS;
- Increasing the scalability, by increasing the coverage area, area expansion;
- Implementation of more evolved data acquisition algorithms;
- Implementation of new algorithms for data processing and presentation of data;
- Improve interconnection of the informational systems by implementing new algorithms that work under various programming languages (CORBA).

The solution consider as main objectives: the performance, scalability, platform independency and accessibility of the system.

Accessibility problem will be solved by using a solution based on quick access to the network by modern channels of communication with various terminals including PDA, BlackBerry, or specialized touch-screen terminals. The performances take into account the user-friendly interface, safety in operation and exploitation, data security, low response time. Data protection will be achieved through specific mechanisms of network access control and using the latest platforms and software for development of databases accessible via the Internet / Intranet (ASP.NET, SQL Server, JAVA, OLAP, etc). The authentication procedures as: recognition of faces, voices, signatures or signatures of people may be included in this category.

In terms of increasing security, at present there is a growing need for measures that would guarantee privacy, integrity and availability of resources in distributed systems. The security measures should be incorporated in the computers each time they are potential targets of attacks which may take various forms. Distributed systems designers need to combine interfaces of exposed services and insecure networks in an environment in which attackers have knowledge about the algorithms used. Cryptography provides the basis of authentification of messages and their secrecy and integrity. The selection of cryptographic algorithms and key management are critical issues of efficiency, performance and use of security mechanisms. Public key cryptography facilitates the distribution of cryptographic keys, but its performance...
is inadequate for the encryption of large volumes of data. Secret key cryptography is indicated for such tasks. Hybrid protocols such as SSL (Secure Sockets Layer) establish a secure channel that uses public key cryptography to exchange secret keys. Digital information can be signed, producing digital certificates. Certificates ensure trust between users and organizations. The problems of ensuring security networks can be grouped into the following interrelated areas:

- confidentiality refers to give access to information only to authorized users and preventing access by unauthorized persons;
- integrity refers to ensuring consistency of information (in case of transmission of a message over the network, integrity refers to protection against attempts of falsification of the message);
- authentication ensures the determination of the identity of the person to communicate with (very important aspect for the exchange of confidential information or messages, in which the identity of the broadcaster is essential);
- non-repudiation relates to taking responsibility of messages or commands, to their authenticity. This is very important in the case of contracts made between firms via electronic messages.

It is used for the authentication the protocol used in real time systems, Kerberos. Secure connection to a server, remotely via SSH, uses to sign another protocol based on public key RSA algorithm.

### 3. OPTIMIZATION OF INFORMATION SYSTEMS

A distributed system is defined as a system in which components located in a network of computers communicate and coordinate their actions by means of passing messages. Computers connected via a network may be separated by any geographic distance. They may exist on different continents, in the same building or in the same room. This definition of distributed systems has important consequences for the following:

**Competition:** In a network of computers, the main norm is the execution of competing programs. It runs applications on different computers at the same time, sharing resources such as web pages or files. The ability of the system to handle shared resources can be raised by adding more resources (e.g., computers) on the network. Coordination of running competing programs that share resources is also an important topic.

**Lack of a global clock:** When the programs want to cooperate, they coordinate their actions through the exchange of messages. Close coordination often depends on a shared idea at the time in which actions of programs occur. This means that there are limitations to the accuracy with which computers in a network synchronize their watches, this is a direct consequence of the fact that the only communication that takes place is by sending messages through a network.

Independent failures: All the computers can deteriorate and it is the responsibility of systems designers to plan the consequences that follow the possible failures. The damage occurs different through distributed systems. A computer failure or sudden conclusion of a program somewhere in the system (crash) is not immediately known to the other components that communicate with it. Each component of the system may deteriorate independent, leaving the others to continue working.

The motivation to build and use distributed systems resides in the wish to share resources. The term “resource” is rather an abstract one, but characterizes best the many things that can be shared in a network of computers. The term extends to hardware, such as disks and printers to software-defined entities, such as files, database objects and data of all types.

From the point of security, most of the information available and maintained in distributed systems is of a great intrinsic value for their users. Therefore, their security is of considerable importance. Security for the informational resources contains three components: confidentiality, integrity and availability. There are two security challenges treated in a superficial manner in most of the cases:

- **Neglect of service attacks (DOS):** This happens when a user wants to stop, for some reason, one of the services. It can be achieved by bombing the service with a large number of meaningless requests.
- **Security of the mobile code:** mobile code should be handled with suspicion and care. It is used where an executable program is received as an attachment to email, in which case, the possible effects of running the program are uncertain.

With regard to scalability, distributed systems operate effectively and efficiently to many different scales, ranging from a small intranet network to the Internet. A system is scalable, if it retains its efficiency at a significant increase in the number of users and resources. Internet provides an illustration of the distributed system in which the number of computers and services has increased dramatically.

In terms of reliability, the computers are sometimes defective. When failures occur in hardware or software, the programs may produce incorrect results or may stop before to complete the required calculation cycle. In distributed systems, failures occur partially - some components fail while others continue to operate. Therefore, it is difficult to treat failures in particular. There are the following techniques for the treatment failures:
• Detection of failures: Some defects can be detected. For example, the technique "checksum" can be used to detect corrupted data from a file or message.
• Failure masquerading: Some of the defects detected can be hidden or made less serious. Two examples of hidden failures: a) messages can be retransmitted, when they failed to reception; b) data from a file can be written on two discs, so that if one is corrupt, the other may still be correct.
• Ignoring failures: Most Internet services produce on-sight failures. Customers may be directed to ignore the failures, and users too.
• Recovery from failure: Recovery involves designing software so that data can be restored when a server is defective.
• Redundancy: Services may be made to tolerate failures by using redundant components.

The scientific/technical contribution consists in optimizing the informational system by improving the following characteristics:
- Increasing the reliability of the informational system;
- Increasing the security informational system;
- Increasing accessibility of the system;
- Better scalability of the system, extending the coverage area;
- Implementation of more evolved algorithms for the data acquisition;
- Implementation of new algorithms for data processing and presentation of data;
- Improve interconnection of the informational systems by implementing new algorithms.

3. CONCLUSIONS

Estimated results - the main characteristics:
- Analysis and easy viewing of the components of an integrated waste management systems.
- Criteria for the ranking of sites of all components of an integrated waste management system.
- System monitoring the evolution process of waste management system.
- Inventory and facilitate reporting of data on waste management systems.
- Reduce time in the decision making process.

Bibliography