A TOTAL SOLUTION FOR DISASTER PREVENTION IN THE INTERNET ERA

Cheng-Ping Lin

Assistant Professor
Department of Building Engineering China Institute of Technology
championlin@yahoo.com

Abstract: To prevent disaster, security staffs shall ensure the safety of everyone in the buildings through monitoring and controlling important facilities properly from the security control room. However, most of them could not perform their duty during tragic disasters such as a great earthquake or conflagration. There's every reason to believe that they did not dare to stay at the security control room during the event for their own safety. Therefore, the author tried to analyze the condition and found out a total solution for disaster prevention with due consideration of the available resources in this internet era. By the analysis, a new solution for disaster prevention in the internet era may be discovered.

Keywords: A total solution, Internet era, Disaster prevention

1. INTRODUCTION

One of the most attractive issues in construction industry nowadays is disaster prevention, because the death toll of some disasters is too high to ignore. After reviewing and discussing some disasters from historic data, researchers found out a common problem in some large-scale buildings with traditional intranet network solution, and the problem comes from staffs in the security control room.

Theoretically, the staffs' duty is to ensure the safety of everyone in the buildings through monitoring and controlling important facilities properly from the security control room. However, most of them could not perform their duty during tragic disasters such as a great earthquake or conflagration. In fact, they did not dare to stay at the security control room during the event for their own safety. Therefore, the author tried to analyze the condition and found out a total solution for disaster prevention with due consideration of the available resources in this internet era. By the analysis, a new solution for disaster prevention in the internet era may be discovered.

2. TRADITIONAL SECURITY SYSTEM

In this study, the traditional security system includes a monitor system, an access control system, an audio system, and a fire alarm system. All of these systems will be discussed as followings:

2.1 Monitor system

In terms of a monitor system, a sensor (or CCTV camera) can be roughly described as any reportable data sources. It is described as any devices that gather data. The data may contain performance, configuration, or accounting information, and correlated with other time critical data at the monitor system status [7].

In fact, analog sensors have been used around for many years and are found in almost all large-scale systems. The reason is that the advent of high speed, and large-capacity memory computers made big operation modeling and simulation possible. Therefore, to collect the data needed for large-scale systems is designed. In addition, unless more economical and inferential measurements could be made, analog sensors are necessary and useful in monitoring operational processes that benefited from any such monitoring. Nevertheless, a recorder is necessary to record data.

2.2 Access control system

An access control system consists of a card reader, an access controller, a magnetic reed switch, a motion detector, a vibration sensor, an output alarm device, and so on. The door can be locked up except anyone has the right to enter. If someone has any force to break, the output alarm device will act.

2.3 Audio system

An audio system includes an audio player and a speaker. The audio player can make voice and the speaker can make sound louder.

2.4 Fire alarm system

A fire alarm system includes temperature sensor, smoke sensor, gas detector, heat sensor, automated lighting, water sprinkle system, and so on. It can detect fire generation and prevent its spread. These systems mentioned above are separately established and can't be integrated (as shown in figure 1). It will spend a lot of money to establish, maintain, and integrate these systems [2]. It is hard for staff in security control room to manage if any disaster occurs. For this reason, how to integrate these systems become the most important thing and a new solution for disaster prevention in the internet era shall be discussed.

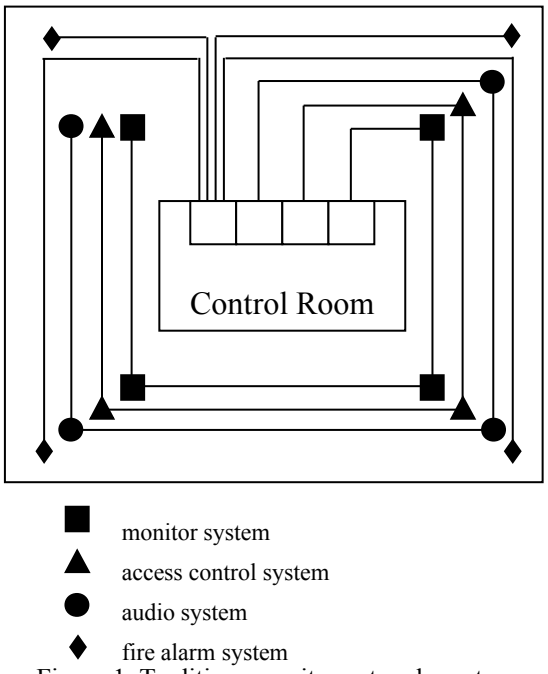


Figure 1 Tradition security system layout

3. THE TREND OF NETWORK TECHNOLOGY

The communication network has become a common and necessary element in the operation and use of today's computing systems. There are not only a wide variety of computer hardware and software platforms, but also of networking protocols available. Along with this diversity, the need to share data and services among connected computer users has accelerated as individuals, corporations, universities, and countries depend on each other in the competitive business world. This is especially true as distributed processing, and the special case of the hugely popular client/server computing, becomes more widespread [5].

Physical connections between computing machines can be, at times, a simple one-to-one link. However, it is increasingly more common that a group of local machines (i.e., a network) is joined with another group. In this case, entire networks can be integrated allowing users of one network to access resources in another network.

The Transmission Control Protocol/Internet Protocol (TCP/IP) networking architecture grew out of the early ARPANET project, as sponsored by the Department of Defense in the late 1960s. Since that time, it has evolved to accommodate the requirements of its rapidly expanding user base.

The TCP/IP data formats and protocols are loosely arranged within a layered model, with some flexibility in terms of the implementation options. The protocols are designed to support a wide variety of host computing platforms and networking configurations. This independence from the operating system and underlying physical transport has contributed to its appeal and widespread usage.

In addition to the basic framework for data transport and routing, there is a suite of standard applications usually supplied with a particular implementation. These services, along with the various application programming interfaces, allow TCP/IP to be quickly established as a useful tool in the operation of an enterprise-wide data communication network.

Such a collection of interconnected networks forms an ethernet, or internet. The individual networks can maintain their local autonomy, while still participating in the larger internet.

The internet provides users with a transparent access across network boundaries. In this sense, the internet is a type of virtual network, with consistent standards for data transmission, routing, and processing.

In this study, the internetworking concept is focus on the TCP/IP architecture. The Internet Protocols (IPs) are distributed across sensors, access control systems, audio systems, and fire alarm systems, and so on. Once these equipments used TCP/IP architecture, the server can be communicated and controlled though TCP/IP.

4. TCCHNOLOGY FOR AUTOMATIC SECURITY SYSTEM

In order to transmit data though network, it is necessary to convert analog signal into digital format. Nevertheless, for the purpose to integrate different security systems, technology for automatic security system shall be discussed. For this reason, several technologies will be discussed as follows:

4.1 Convert analog signal into digital format

Technologies that support the performance of Sensors have been realized increasingly, and the technology innovations boosted over past few years. Digital systems are normally accomplished by one of several methods, which is to convert analog signals to digital format and then incorporate the data into messages that are transmitted between the affected equipment and the network management system [4]. Another method is to monitor the direct digital sequences generated by the target equipment and to incorporate that information into status messages for transmission to the network management system [1].

Sensor systems must be thought of as integral to the realization of complete automated systems both currently under development and slated for development in the future. Digital, bus-capable sensor interfaces are one of the solutions foreseen for future applications of sensor technology that will support integrated sensor and operational functions. These interfaces can best be accomplished through the definition of an open sensor interface that offers the flexibility to exchange the equipment of different manufacturers.

Sensors are varieties of the types that have the

ability to adapt to the input information. This adaptation, in turn, provides facilities for intelligent control of the network elements and their modular replacement units.

4.2 Wireless communication

Until the past few years, telephones, computers, faxes, and other communication devices have been tethered to wires. But advances in microprocessors and software are changing that, powerful wireless networks are starting to emerge. Wireless networks will allow people to communicate cheaply and easily without being tied to their desktop telephones or computers.

There is a range of wireless technologies. Wireless technologies include the use of microwave, radio-based mobile data networks, paging systems, enhanced cellular telephones, personal communication service, and satellite networks [3].

Mobile data networks are radio-based wireless networks for two-way transmission of digital data. These systems employ a network of radio towers to send text data to and from hand-held computers. They can send long data files efficiently and cheaply by transmitting them in packets.

The most common use of portable paging systems has been to beep when the user receives a telephone call. Since the mid 1980s, paging devices have also been used to transmit short alphanumeric messages that can be read on the pagers' screens. These paging systems can now send (but not receive) data to mobile computers. Paging services operate at very low speeds, making them useful primarily for sending very short than faxing.

Cellular telephones work by using radio waves to communicate with radio antennas placed within adjacent geographic areas called cells. When you place a call from a cellular phone, the call moves through a radio highway of these transmission towers, directed by advanced digital switches and computers. As a cellular call moves from one cell to another, a computer that monitors signals from the cells switches the signal to a radio channel assigned to the next cell. Although cellular phones are primarily used for voice transmission, cellular companies are developing capabilities to use the existing analog cellular phone network to transmit data in digital form.

Companies are starting to build new kinds of micro-cellular digital networks called personal communications services (PCSs). PCS technology is similar to cellular technology, but uses low-power, high frequency radio waves. Compared with conventional cellular networks, PCSs use smaller, closely spaced micro-cells that require lower-powered radio transmitters and phones. PCS transmission is entirely a digital communication, which is designed for sending data as well as voice. It can work with a PDA with built-in communication and organizational capabilities.

A hierarchy of wireless networks is emerging. The most deluxe wireless networks will be the satellite networks, which can provide global wireless phone, data, and fax service by bouncing signals off low-orbit satellites. Low-orbit satellites are close enough to the earth to pick up signals from weak transmitters and consume less power and are less expensive to launch than conventional communications satellites.

4.3 Mobile computer

Today, powerful computers sit on our desks. A burgeoning global communication system lets us reach out and touch one another, often at a time we aren't at our desks and can't keep up with our communications. It sure would be nice to have that big, powerful PC help to keep track of all the contacts, appointments, and information.

The mobile computer can be a notebook or a calculator that has scheduling, programming and phone number book. But now, the Personal Digital Assistant (PDA) that is part miniature computer, part a phone number book, part secretary, part interactive jotting, and scheming pad is used more and more for recent years. The PDA is all of these things and more. Just as telecommunications has linked offices together, PDAs let you take your office with you. Wherever you are, the world of information and the web of personal contacts will be at your command.

A PDA, on the other hand, isn't just a smaller version of a notebook PC. True, PDAs use computer-type components (processor, memory chips, display, and so on). But PDAs aren't designed to run downsized versions of the same kinds of software packages that you might run on your PC. Rather, the purpose of a PDA is to help you communicate better in an era of global, mobile communications and to provide new ways to help you keep track of the information you need-especially when you are on the plant. A PDA is designed from the very start to be a tightly integrated combination of hardware, operating system, and software. Certainly PDAs will process text and pictures, perform calculations, store and retrieve data, and communicate with pictures, and communicate with other computer, but the way PDAs handle these tasks will be quite different from traditional PCs [6].

4.4 Neural Networks

Neural networks have been around for 100 years or more. Only within the last 10 years, however, have the technology and implement neural network models. Neural network technology mimics its biological antecedent. Investigations of the vertebrate nervous system have revealed architectures and processing methods that originally were simulated on computers, and later were borrowed to develop new approaches to the whole issue of computerized adaptation and learning. Parallel computer systems and distributed computer systems have been the principal areas in which this technology area has progressed. Massively parallel systems incorporate many processing nodes, each of which are its own computer, and are used as a correlate for a neuron.

The neuron is the basic communications element of the human body. Distributed systems allow information sharing among the various processing nodes of the system [1].

Neural networks are an attempt to model and simulate the neural architecture and functioning of the brain [1]. In particular, such models are an attempt to emulate the processing and interpretation of the various sensory modalities of the mammalian central nervous system. This seemingly huge task is accomplished through the use of simplified models of neural processing, as conducted by neurons (brain cells) that are arranged in interconnecting patterns. These patterns are, in turn, exercised by external stimuli to yield the correct responses to problems presented to them.

More importantly to the network management designer, these models and their subsequent simulations can be used to develop adaptive, learning, monitoring, and control mechanisms for many important network management applications. As will be seen, telecommunications networks can be thought of as the nerve backbone for all purposeful systems devised. These integrative communications links carry the status and actions of the system, thus providing the fabric for learning and adaptation.

Neural network models can be developed on conventional computers from simple PCs to parallel processors, and supercomputers using special software developed for such purposes. In addition neurochips have been developed embodying the capabilities to perform neural network simulations. Finally, application specific integrated circuits (ASICs) have been developed for individual situations that have the ability to execute and analyze a specific neural net problem.

For automatic security network management systems and applications, neural networks have widespread possibilities. Neural network inputs that might be equated to different features of an operational network can be routed and applied to the first layer of a typical neural network. The subsequent processing can generate a pattern, the output of which can be used for reference, or to modify the neural network so that it attains a reference point. This pattern now becomes one of the comparison elements, against which pattern alternations can be judged.

A receptor, which is a specialized sensor specific to a particular type of stimulus, such as impressions of pain, will react to that stimulus by passing an electrical signal (0 or 1) in the form of a depolarization wave to the first neuron with which it comes into contact. From there, the signals are passed as action potentials to succeeding neurons until these signals are received in the brain or on efferent neurons that generate motor responses. Different stimuli are coded according to the number and/or frequency of action potentials generated. These coding schemes convey certain meanings to the brain according to their organization. The energy stimulus at the sensor, whether it is sound, light, etc., causes an electrical signal (0 or 1), or depolarization, to be generated by the sensor. This depolarization is the input side of the neural process. The electrical wave in turn causes a subsequent deposition of transmitter chemicals to be secreted through the presynaptic membrane, i.e., the membrane of the sensor. These transmitter chemicals then migrate across the synaptic space to the membranes of the dendrites of the first afferent neuron.

For example, the action potential is actually a large, sharp electrical wave created by a sufficient number of sensors. The signal travels from the receiving sites up through hub to the server. Once the server receives signals, it can decide alarm, water sprinkler or other machines to action. Figure 2 shows the basic arrangement of sensors, incoming signals, and transmission systems.

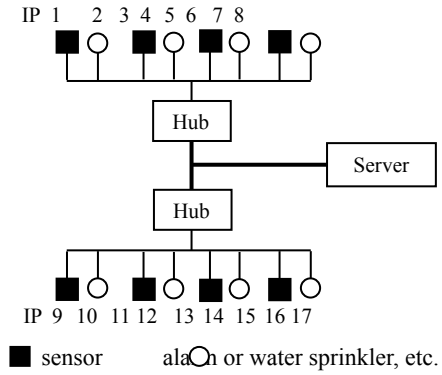
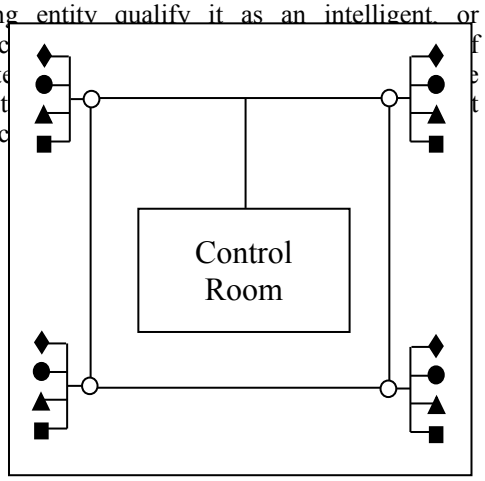


Figure 2 Basic sensory neural pathway

5. INTERNET-BASE AUTOMATIC SECURITY SYSTEM

With TCP/IP base, access control, digital surveillance, alarm monitoring, digital broad casting system and devices are integrated into digital and automatic security system. The layout for four systems is shown in figure 3.

Automatic security system can be categorized to a variety of expert and neural systems applications, which are usually implemented in software. These applications may range from maintenance advisors, decision support modules, to pattern understanding; and sometimes include natural language interfaces for human operators. The characteristics of a processing entity qualify it as an intelligent or automatic [illegible] such syste[illegible] target net[illegible] with the c[illegible]



monitor system
access control system
audio system
fire alarm system

Figure 3 Digital and automatic security system layout

(1) Integrated System

If digital sensors, alarm monitors, digital broad casting systems, and fire alarm systems can be integrated into automatic security system, a lot of money and time will be saved. Once these systems can be integrated, staffs can monitor one system rather than four different systems. The system's knowledge should be coherent, i.e., it should be capable of being shared among all the modules within the system, be commonly available to these modules, and adhere to a common formatting structure, taxonomy, and lexicon. In conventional processing programs, information is segmented and parsed so as to be available to only one or a few processing modules.

(2) Integrated Digital Data

All data available to the system should be digital and accessible to all the automatic modules, regardless of the potential variety of data structures and access methods used in the individual database systems servicing the system. Conventional programs are usually constrained to interface with one database system because the interface driver software is designed for only one database system. Integrated digital data provides the capability to reformat and translate [illegible] one system environment to an[illegible]s, the sub-network[illegible]gers must be supported with data [illegible] that needed data can be accessed. In[illegible]d digital data also requires a security sy[illegible]ein[illegible]tablished so a[illegible] provide app[illegible]le[illegible]ccess privile[illegible]

(3) Decision [illegible]

The ac[illegible]s [illegible]and use of knowledge in network ma[illegible]ent, [illegible]s that through neu[illegible]vor[illegible]ng the [illegible] more stabl[illegible] system reporting more believable and accurate. To other extent, the logic of automatic security system should be understood by users on demand, through informal-style questions users pose to the system for resolution. In conventional software, users would know the algorithms used in programs during module execution. With a minimum, these algorithms should be available to users, the logic used should be published, and decision criteria should be made available as required. This facility thus enhances the decisions /recommendations credibility of automatic security system.

(4) Decision Execution

The execution of decisions either reached by or supported through automatic security systems, is a more far-reaching proposition that will entail further research and incremental development work in this area. However, as this time arrives, automatic sub-modules (smart sensors) of automatic security system may be hypothesized to be able to initiate appropriate actions on their own as conditions warrant. Execution of these modules depends upon external stimuli as opposed to user initiation. These sensors can also be integrated into a data fusion module so that filtering and data integration can make decision support more accurate and timely.

(5) Wireless communication

The automatic security system is possible to be extended to the PDA or other wireless communications. Because once the disaster occurs, the staff may not stay in security control room. Once the staff has PDA, even if he is not stay in security control room, he still can communicate with servers though wireless communication. Nevertheless, the staff can monitor and control related fields.

(6) Th[illegible]

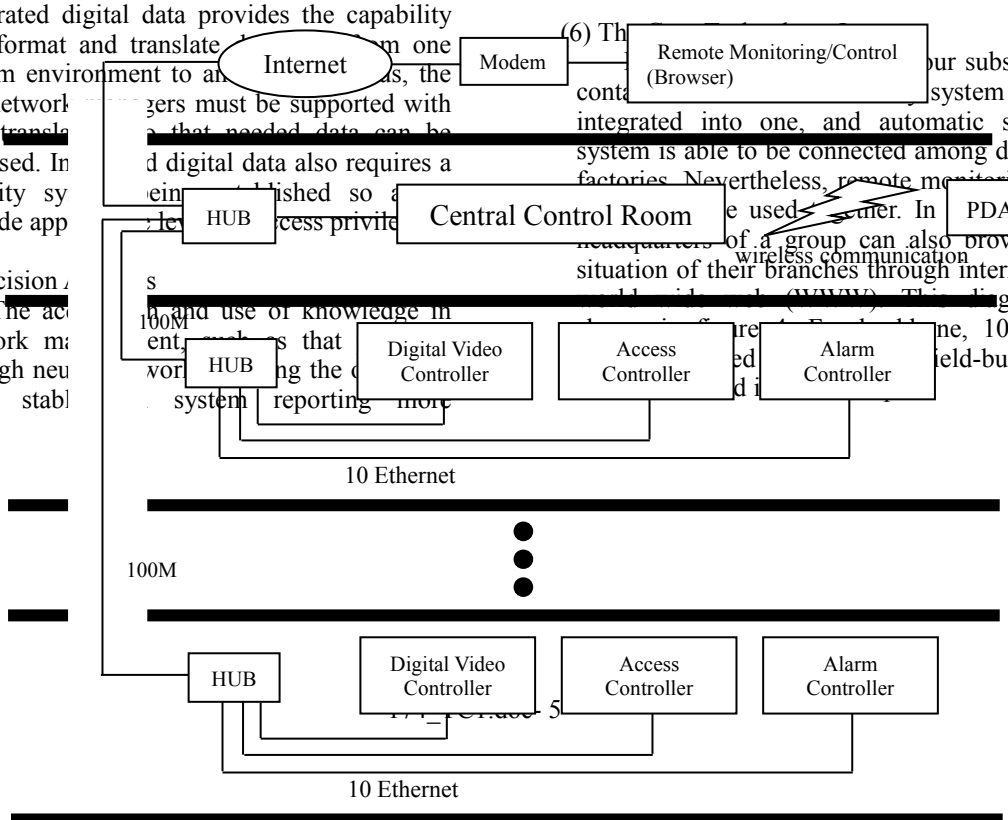


Figure 4 the diagram for internet-base automatic security system

CONCLUSION

Nowadays, we are engaged in a global economic competition for resources, markets, and incomes with other nations all over the world. Computers, however, replaced manual technology to process large volumes of data for complex work. Computers can execute hundred millions of instructions per second, and can also perform consistently and reliably over longer time than human beings.

To have a comprehensive understanding of automatic security system, the author discussed the technologies of traditional security systems and progress in computers, internet, and communication technologies in this internet era. The new technologies for automatic security systems included integrated systems, integrated digital data systems, decision analysis systems, decision execution systems, wireless communication systems, and the internet systems. Along with the development in computers, software (or algorithm), network, and wireless communication, it is possible for several different systems contained in automatic security system to be integrated into a power one.

By way of reviewing the traditional security systems and applying new technologies, a new total solution for disaster prevention is not a dream, but it can be a real in this internet era.

REFERENCE

[1] Ball, L. L., *Network Management with Smart Systems.,* McGraw-Hill, 1994.

[2] Horn, D. T., *Electronic Alarm and Security Systems: A Technician' Guide.,* The Dryden Press, 1995.

[3] Laudon, K. C. & Laudon, J. P., *Information Systems – A Problem-Solving Approach (3rd edition).,* The Dryden Press, 1995.

[4] Marven, C. & Ewers, G., *A Simple Approach to Digital Signal Processing.*, John Wiley & Sons, 1997.

[5] Peterson, D. M., *TCP/IP Networking: A Guide to the IBM Environment.,* McGraw-Hill, 1995.

[6] Williams, R. & Leverette, H., *PDA Playhouse: The Interactive Book of Personal Digital Assistants.,* CA: Waite Group press, 1994.

[7] 羅國杰，工廠電腦監視控制系統，全華科技圖書股份有限公司，1993。