# Global Information Assurance Certification Paper

**Alarm & CCTV Unified Systems as Physical Security Options for Mexican Banks**

**Gerardo Oviedo**

**GIAC Security Essentials Certification Practical**
**Version 1.4b (First Option)**

## Abstract

Technology is changing everyday and the requirements of physical security on banks also, but the main idea remains intact. There are many implementations or systems to control and audit the physical security but one kind of these systems are the installation of a Closed Circuit Television (CCTV) and Alarm System in buildings.

In this document, I will describe the basic functionality of a CCTV and alarm system, specially for meeting requirements of the Mexican Government to the national banks, but they could also be applied for all banks.

## Introduction

In October 2002, the Mexican Government published in "Diario Oficial de la Federación" a list of requirements to implement new security and protection measures. This document was addressed to all mexican banks to support, and basically, prevent criminal acts. An important aspect to accomplish this request, is to have a unified alarm & CCTV systems installed on each of their branches. [1]

## Physical Security

Physical Security is not something that can be easily and strictly defined. The following definition of Garfinkel and Spafford helps the better understanding of this concept:

> "'Physical Security' is almost everything that happens before you (or an attacker) start typing commands on the keyboard. It's the alarm system that calls the police department when a late-night thief tries to break into your building. It's the key lock on the computer's power supply that makes it harder for unauthorized people to turn the machine off. And it's the surge protector that keeps a computer from being damaged by power surges."[2]

Other definition more theorical is the proposal by British Standar BS7799:

> "Critical or sensitive business information processing facilities should be housed in secure areas, protected by a defined security perimeter, with

[1] "Nuevas medidas de seguridad para instituciones bancarias", Diario de la Federación
[2] Garfinkel, Simson and Spafford, Gene, Practical Unix & Internet Security, O'Reilly and Associates, 1996, page 357

appropiate security barriers and entry controls. They should be physically protected rom unauthorized access, damage and interference.[3]

**Security on Banks**

For human beings, banks represent the ultimate in security. Believing in their infallibility as in their safety, people keep their values and deposit their hard earned savings. Free economy, for its survival and growth need an efficient, trustworthy service oriented to Banking system. Anything untoward happening to undermine the trust of the common man in the Banking system will have far reaching consequences on Bank Economy.

Rapid expansion of Branches have made location of Banks in premises which are unsatisfactory from security point of view. Preoccupation of police with law and order problems including Terrorism has made it impossible for the Police to devote more attention to the physical security of Banks. Most of the Banks have no access control system, physical arrangements like Barriers, Closed Circuit T.V., Alarm System to prevent a crime and to summon police help. The solitary chowkidar found in many Banks is ill-trained and ill-equipped and is generally utilized as a handy all purpose help and is seldom able to concentrate on security functions, which are his primary duties. Armored vehicles are not available to transport cash and valuables between banks"

For this reason, hundreds of earnings are lost every year in bank frauds, which are not possible without the cooperation (???) and collusion of some of the bank employees. Neither The Central Bureau of Investigation nor the State Crime Branches have the time or the resources to pursue all these cases. Banks need a tool to automate this process so they can be more proactive, instead of reactive.

**CCTV Systems[4]**

As the name implies, CCTV is a system in which the circuit is closed and all the elements are directly connected. This is similar to broadcast television where any receiver that is correctly tuned can pick up the signal from the airwaves. "Directly connected" in this context refer to systems linked by microwave, infrared beams, etc.

Probably the most widely known use of CCTV is in security systems such as retail shops, banks, government establishments, etc. The true scope for applications is almost unlimited.

[3] British Standad: Information technology – Code of practice for information security management systems. Pages 13-19
[4] Constant, Mike, "What is closed circuit television?",

The starting point for any CCTV system is the camera. The camera creates the picture that will be transmitted to the control position. This picture should be reproduced to a CCTV monitor that is virtually the same as a television receiver, except that it doesn't have the tuning circuits.

The simplest system is a camera connected directly to a monitor by a coaxial cable with the power for the camera being provided from the monitor. This is known as a line powered camera. Figure 1 shows the mentioned system.

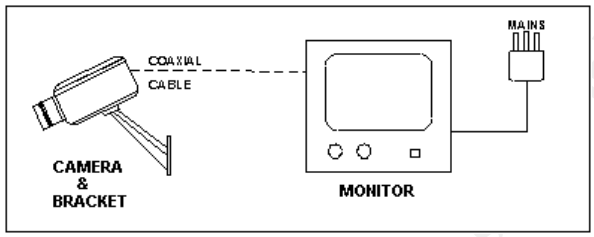


*Figure 1 A Basic Line Powered CCTV System*

The next step is to incorporate the outputs from four cameras into the monitor. This could be set to automatically sequence through the cameras, or any camera could be held selectively. Figure 2 demonstrates a typical arrangement of such system.

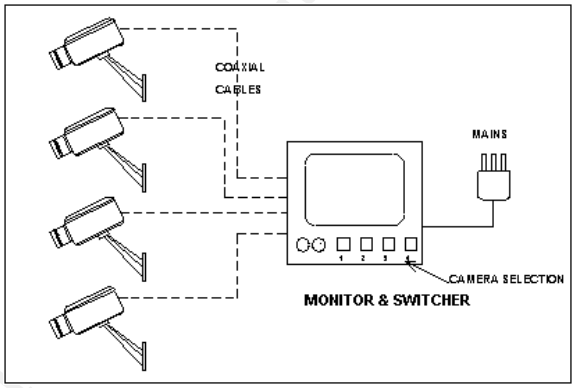


*Figure 2: A Four-Camera Line Powered CCTV System*

The basic CCTV installation is shown in figure 3, where the camera is powered as the monitor. A coaxial cable carries the video signal from the camera to the monitor. This arrangement allows a great deal of flexibility in designing complex systems. When more than one camera is required, a video switcher must be included (as shown in figure 3). By using this switcher, any camera may be selected to be held on the screen or it can be set to sequence in turn through all the cameras. Usually the time that each camera is shown may be adjusted by a control knob or by a screwdriver.

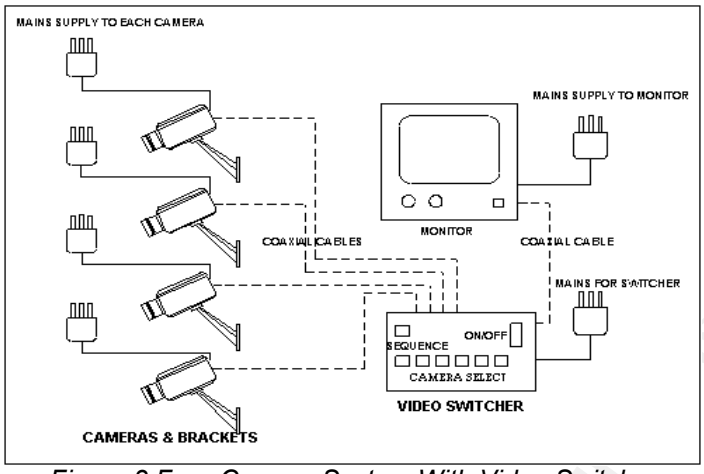


*Figure 3 Four-Camera System With Video Switcher*

The next step of a basic system is to add a video recorder. Arrangement should be as the one shown in Figure 4.

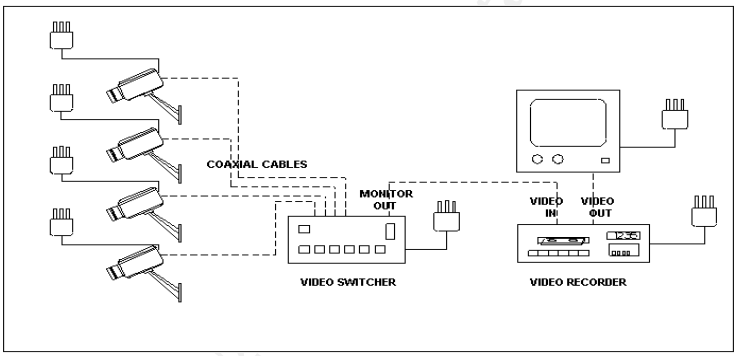


*Figure 4 Multi Camera System With Video Recorder*

With this arrangement, the pictures shown during play back will be according to the way in which the switcher was set up while recording. That is, if it was set to sequence, the same views will be displayed in the monitor. There is no control over what can be displayed.

What are the advantages of network based video systems over traditional analog CCTV systems?

- By using Network Video Systems, individuals can safely view live and stored data from any PC with a compatible browser, whether it is on the LAN in the next office or across the country via Internet .
- With network based video it is easier, cheaper and faster to store, call-up, review, and maintain digital images because they are stored on hard drives, rather than traditional video tape archiving systems.

The overall maintenance cost of running an IP based video security system is almost always substantially less than that of an analog system, because most service and adjustments can be maintained remotely over the internet, instead of having to dispatch a technician with a service call.

**Alarm systems**

Many buildings and complexes constructed today are equipped with some type of intrusion detection and fire alarm systems. The purpose of any alarm system is to either protect life or property or to detect an intrusion. Alarm systems are set up to:

1) Give early warning so occupants may evacuate the building;
2) Notify the police department and/or security soon enough so that they have time to react.

These alarms systems or Intrusion detection systems detect unauthorized entry into the company's assets. The systems can act as a deterrent to break-ins at a business. Thieves usually ignore minor details premises with alarm systems, moving on to unprotected premises.

The alarm includes the sensing devices that detect break-in attempts. Sensors can be located inside, outside, or around the perimeter of the building. When a sensor is activated, it sends a signal to a control panel, which triggers a loud alarm and notifies a central monitoring station. These systems can work in harmony with fire detection systems or access control systems (CCTV).

The basic components of an alarm system are:

- Control Panel: Receives information from the sensors, processes it, and transmits the alarm. Audio and/or visual indicators, such as bells or strobe lights, are set off on the premises. Encoded signals can also be sent to a central station, reporting exactly what occurred in the exact area of the building.

- Arming Station: Is the device used to turn the system on and off. It usually takes the form of a keypad with either an LED or LCD display.

- Sensors: Located around the building. Detect different types of activity. Sensors send signals to the control panel via wireless radio transmitters or via wires when there is a break-in attempt or unauthorized entry. Several types of sensors have been designed especially for intrusion detection:

    - *Magnetic Contacts:* usually protect doors and windows. They send signals to the control panel when the door or window is opened when the system is armed. They can also be used for detecting the removal of high-value objects and other key points.

    - *Glassbreak Sensors:* protect windows, sliding glass doors, and skylights; come in three variations: shock, acoustic and combination.

- *Shock Sensors:* "feel" the shock frequency wave produced by breaking glass and signal the alarm.

- *Acoustic Sensors:* "listen" for the unique sound of glass breaking.

- *Combination Sensors:* detect both of the activities mentioned above before ringing an alarm.

- *Motion Sensors:* detect movement in the coverage area.

**Security Systems Integrations**

To understand the trends relating to security systems integration, one must first clarify the meaning of the term. Easier said than done.

What exactly is "Security Systems Integration?" Even as definitions are debated among suppliers, end-users, and industry suppliers, what it often comes down is: whatever the customer says it means.

For example, for a bank security manager it might mean "combining security, safety, and prevention into one package." For the facility manager of an educational institution, it might mean "less paperwork and more control of the total system." In government, it might mean "the ability to combine the new and old technology." In the industrial/manufacturing setting, it could mean "ease of use" or "systems information collected and compiled in one piece of equipment."

Verbatim comments from respondents emphasize the variety of integration scenarios. Here are some typical responses:

- "All devices are integrated through my computer with three remote site locations."
- "Card access and alarm monitor points report to a central station."
- "Card use in some areas triggers a camera to record immediately."
- "(We have a) single system for alarms/access control. Certain alarms cause actions, i.e., lobby lockdown upon intrusion/panic."
- "Access control system incorporates identification badges which are used to access buildings, parking lots, and to record time and attendance."
- "Software and hardware alarms and intercom activation call up cameras and initiate alarms on the electronic access control system."

For this reason, it is important that banks know about this technology and try to implement in their branches or buildings to meet the Mexican government requirements.

**Unified alarm and CCTV Systems on banks**

There are different systems to implement a CCTV and alarm system in the market, but the main idea is to have a unified and integrated system of security and automatization designed specially for a big network of banks branches. It should contain a modular architecture scalable and adaptive for the requirements of any type of bank.

The main reasons for choosing a solution of this type are:

- Optimization and total control of the bandwidth for transmission;
- Operation methodologies and process controls;
- All the security and automatization systems in the same platform;
- All the monitoring of the bank branches in the same place.

The solution must allow the administration, monitoring, and control for a distance and in a central way, all the security events, surveillance, automatization and access control that occurs in any point of the branches. Therefore, the system contemplates the relation of two basic entities.

1) Security Center:here the main task is to have in a centralized way, all the operative aspects from an extensive group of branches or buildings. In a bank network it's necessary to have one or more security centers, depending on the number of branches that will be administrated.

2) The branches are the set of buildings or other physical installations that need to be permanently interactive with the security center, having access from all operational aspects of these branches (including security, surveillance, fires, access control, and automatization). This access should be controlled and supervised in any security center. The system must permit the interaction of one to many security centers depending on the number of branches.

For allowing the relationship between the security center and the branches, the solution architecture, should have hardware elements or the physical devices needed for the correct of the system. In a part of the software elements, it should also have different modules for the various functionalities of the system, including the interaction with operators. The elements reside in the security center and in the different branches.

**Hardware Components**

Figure 5 shows the hardware components that are needed for the correct functionality of the solution.

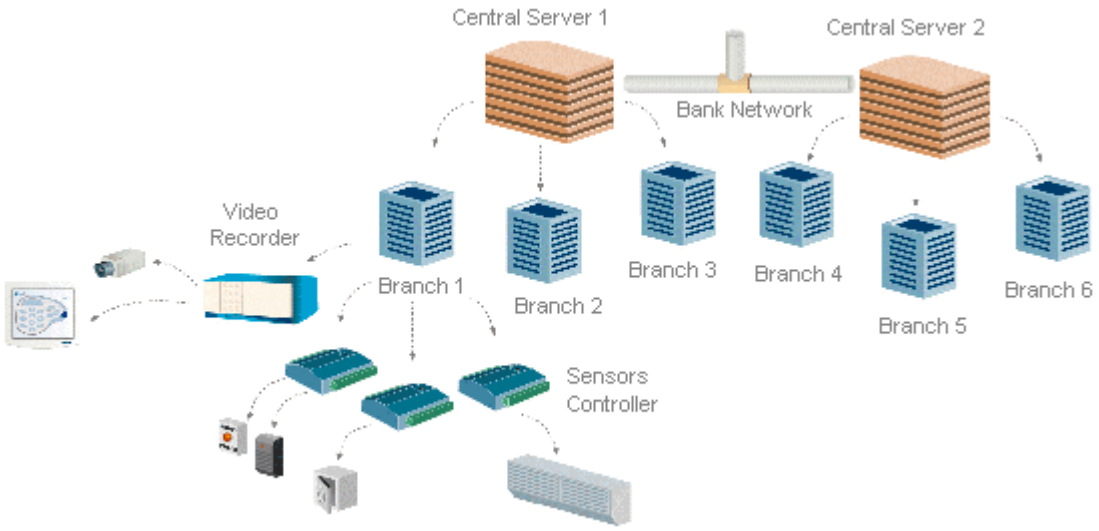


*Figure 5: Hardware components and their interrelation*

- Central server: the main purpose is to control all the processes from the system. This server is the central point of contact of all devices and here the information is processed and received for the different branches that are connected to the system. The solution must allow the integration of server clusters in order to have a total availability of the system, just in case of error. .

- Video Recorder: the device for recording and manage the video and images registered form surveillance cameras. The Video Recorder have the capacity to perform the communication between the branch and the central server.

- Sensors controller or device controllers: their functionality is to directly manipulate the operational status of the peripheral devices that are installed on the branch.

- The peripheral devices are the physical and mechanism components that have one specific task with a minimum process capacity and interconnection. There are motion sensors, proximity lectors, smoke sensors, and others.

- Video Surveillance Cameras or Analogic Video Cameras with a standard definition of CCTV: are installed in strategic sites of the branch to record and transmit live color video of their place using the Video DVC.

The operation console refers to all the hardware and software components that perform different operational activities in the branch that are installed; such as opening and closing of the branch, local diagnostic for systems of a branch, and others.

**Software Elements**

The software elements of the solution should have all the modules that execute all the branch operation in the Security Center like in the different branches from the banking network. They include the software server as the set of applications that are used to form, to administer, and to supervise the operation.

Through the system infrastructure, constituted by the physical components explained previously, it's made the generation and information transmital between the branches and the security center. In a certain way that the system allows the following critical processes:

- The detection and automated distribution of alarm events in any point of the network to the branches, supporting the security operators in the totality of the confirmation process and alarms resolution.
- The centralized supervision of all the security events that are happening in any point of the network to the branches.
- The control of the people flow in anyone of the facilities where the system is working.
- The video recording and live transmission to any point of the banking network in response to an alarm event detected in any branch.
- The state diagnosis and operation of all the system's hardware and their connection to it.

**General Aspects**

The solution must be designed especially for the bank sector and for the focus it is oriented to the management of security and video surveillance process for the bank branches. It is important to have main functionalities, like security handling antitheft alarm, alarm handling, video handling, and video surveillance, access control, automatization, and energy saving. All functionalities manage in the same platform.

For the different interaction in the system, it's recommended to contemplate three main levels: a security center, bank branches and the user without presenting limitations on the number of security center, branches and users who can be supported.

All the information and the system processes should be stored in one or multiple servers to allow the high availability of them. Information should be available to

operators through the software interfaces that allow the configuration of all the operation and selected devices or modules for the system.

The Security Center includes one or more control rooms and supervision of all the operational tasks for an established set of branches. It is indispensable to have more than one operational center where each one will have the capacity to support the simultaneous supervision and the operative control of the real status of the branches. Some tasks from this center are:

- Surveillance: remote supervission of the branches based on the visualization of digital video with the configurable quality . This means that in simultaneous support , the security state of a set extensive of branches or buildings. Ability to instantly send and receive electronic notification in the security center to describe the alarm conditions and execute a confirmation and reaction alarm process. This involves the automatically live video visualization from all the associate cameras of the branch and zone where the condition took place.

- Alarm management: computer aided in the confirmation of alarm conditions, also in the reaction and resolution of the events. Some tasks include the capacity to define which events and conditions in one branch should be treated like alarm conditions and which shouldn't. For each condition designated to the alarm, it's allowed to especify a dynamic schema of steps to follow the operator to confirm if the alarm condition is true or false. Additionally, it is to execute a reaction of this condition. For this reason. It's important to designate a priority to all the alarms, due to the diffrence of the treatment for each alarm. Also, the automatic distribution of the alarm condition to the correct operator with the skills and appropriate ability. Another aspect that i is important to take into consideration, is the capacity to create or generate the policy of information transmission to the third party or institutions when an alarm condition occurrs.

- Unified and remote control about the programmation and function of all the branch devices, including security devices, surveillance, etc. Recording process configuration about the video in response of any event. Retransmission of live and recorded video to third parties. Configuration about the open and close process of the branch.

- The diagnosis to have the capacity for supporting the simultaneuos supervision of the operative state of an extensive set of branches helps to minimize the posibility of errors in the system. This involves supervising the operation state of each controller or device condition, the connection between the controllers installed, and the branches.

- In all systems, it's important to audit and generate reports, searches, and analysis of the usage aspects and funcionality of any component installed on the branch. All reports should be generated based on associated data, such asauditory, security events, alarm conditions, and functionality reports.

- The server is the brain that stores the complete information about the system and distributes the software interfaces connected to the security center and branches.

For Security reasons, the redundancy in the system should be configurated for distributing the load in two or more servers that work in parallel with the system operation. These types of redundancy are:

- Local Redundancy: The server can locally be distributed in two or more servers connected in the network that share the operative load of the system. The locally distributed servers must support a redundancy configuration in which each server is configurated to execute automatic load balancer and processing in case of anyone of the physical components of the server fails.
- Geographic Redundancy: The server can remotely be distributed in two or more servers connected in network so they share the operative load of the system. It is also possible that the complete operation of the system can be changed from one server or a set of servers to another server or a set of servers, just in case of emergency (Example, configuration of primary server and a backup o secondary server). Therefore, the servers must support a redundancy configuration in which the primary server is talk back in one or more secondary servers like mirroring, which can be located in different geographic sites.

The swap process of the load balance in the system from the primary system to the secondary system is due to the availability to generate certain pre-established fault patterns automatically in the primary server. In case of happen the swap, the totality of the execution of the system must be redirected to a secondary server in a time smaller to 6 minutes. The beginning of the swap process is due to generate in less than 30 seconds of the moment at which the failure in the primary server is detected.

**Add-Valued**

The add valued that the system can provide to the bank is very extensive. First, to have the ability to handle access control systems and enery savings in branches within the same platform without requiring systems integrations of third party or creating inefficiencies in the unified operation of the general system. This includes the capacity to make the remote configuration of the controllers and panels of access control in a branch. All the changes must be reported to the

central station and should not keep registries only from the specific events wanted to report, and allow the optimization of the use of the communication infrastructure between the branch and the security center.

Another aspect is the capacity to incorporate mechanisms that increase the security of the transactions integrity and internal operations of the bank, including mechanisms antifraud, digitalization and banking document consultations, and automatic protection of automatic cashier, among others. These mechanisms must include the same platform and reuse such component installed in the branches to diminish the impact to incorporate them to the system.

For the easy automatization is recommendable to have the capacity of allowing the profiles creation or general patterns that detail the operation and the functionality of the security systems, survelliance, and alarm. These patterns must be able to be assigned to groups of branches to facilitate the configuration, programming and beginning of a group of branches simultaneously. Any change conducted on the operation profile assigned to a group of branches, is due to immediately reflect the operation in the branches associated with that same profile.

In the branches, all the software interfaces of the system must require authentication of an administrator or previous operator to the use of anyone of their functionalities. This can include control of network directions (IP) before allowing access to software. Support Personnel in the opening process and closings of a branch. This includes the detection of opening or closing of branch within a schedule designated allowed or prohibited.

**Architecture perspective in case an incident happens**

The purpose of this section is to provide a vision with high level of the architecture of the system that will be used for the implementation of a security project and CCTV. Its intention is to show a summary of the architecture, the used technology, and the scenes that can be put under in case of any incident or fault appeared.

**Functional Description**

In order to understand the architecture, I will describe the different scenarios that appear in the implementation as the works of each one of its components. Depends on a fault or problem that ocurrs in the connection between the devices.he following figure shows the architecture:

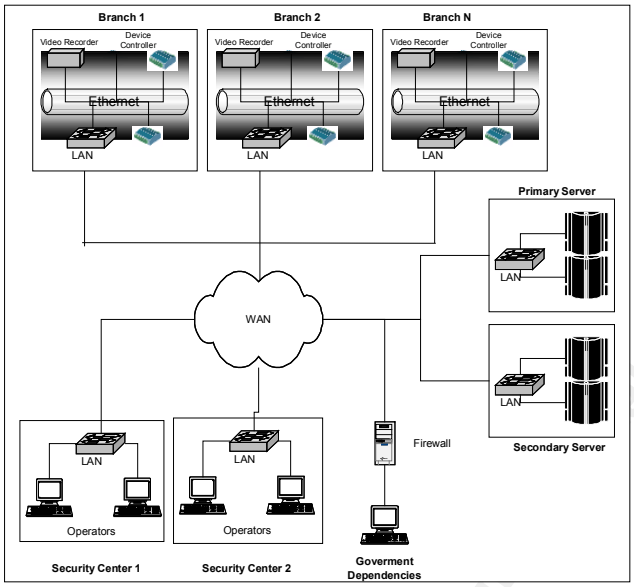


*Figure 6. Archictecture diagram*

- Primary Server (Main Cluster): This cluster of servers by default is where all the branches are connected.
- Secondary Server: This cluster of servers has the same characteristics of the Main Cluster with the only difference that this server helps as a back up and/or mirror in case if the Main Cluster presents some fault to maintain the operativity of the system. This Cluster the objective to synchronize the data base with the Main Cluster.
- Security Center: is the monitoring center of the alarm system and CCTV of the banking branches on which a security center is in the Region A and the central mirror is located in Region B. Here are the operators of the system, who monitor and administer the branches. It is possible to stand out that the solution can be administered from any point of the architecture with the only requirement of having access to the banking network.
- Government dependencies: According to the requirements of the bank and the imposed laws, the dependencies must be able to monitor in real time the status of the banking branches. The solution should allow to have external clients who receive information in real time of the banking branches, previously authorized and classified by the bank and its operators.

Scenario 1: Total connectivity between all the elements of the architecture and normal operation in the branches.

The branches connect the main server and send in real time all the events that happen in the branches. The central server updates in real time their local database and update the secondary server to its database remotely. The operators receive in real time and according to its priviledges the events of the

banking branches through the server. Additionally, the operators can interact with the branches through the server to conduct certain actions (Example: To arm remotely the alarm system) If it happens some alarm event that must be distributed to the support society or the authorities, the server distributes the corresponding information or once automatically the bank personnel is authorized for the distribution.

Scenario 2: Connectivity fault between a branch and/or the Security Center and Primary Server.

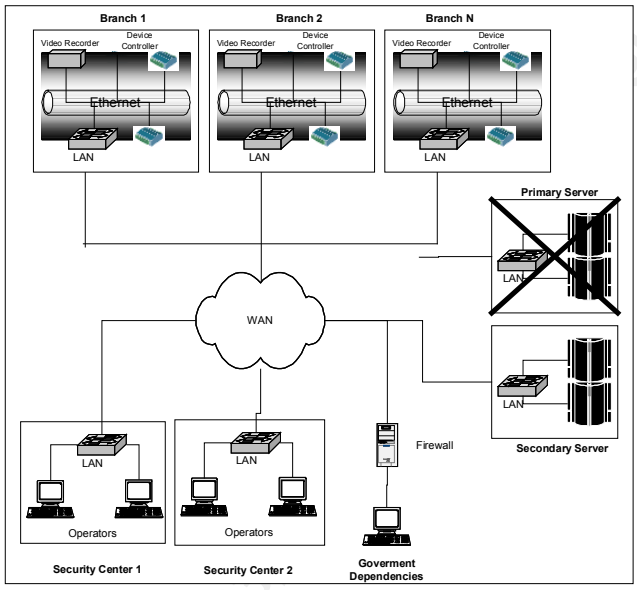


*Figure 7 Primary Server is down*

When the connection between a branch or the Security center and the primary server is lost, the solution must automatically redirects all the communications towards the secondary server. For this reason, the continuity of the operation of the system goes on with its original operation (stays how???) · the secondary server takes total control, converting to the primary server. At that moment reestablishes the primary server, carries out a synchronization process of the primary server with the information of the secondary server that it has been registered during the malfunction period . Once finished the synchronization process, the primary server will assume the control once again. Automatically sends alarm messages to the operators of the security center as soon as the loss of connection between the security center to the primary server is detected. This also happens when the connection is reestablished.

Scenario 3: Fault connectivity of the branch (Network Fault, the branch does not have access to any servers);

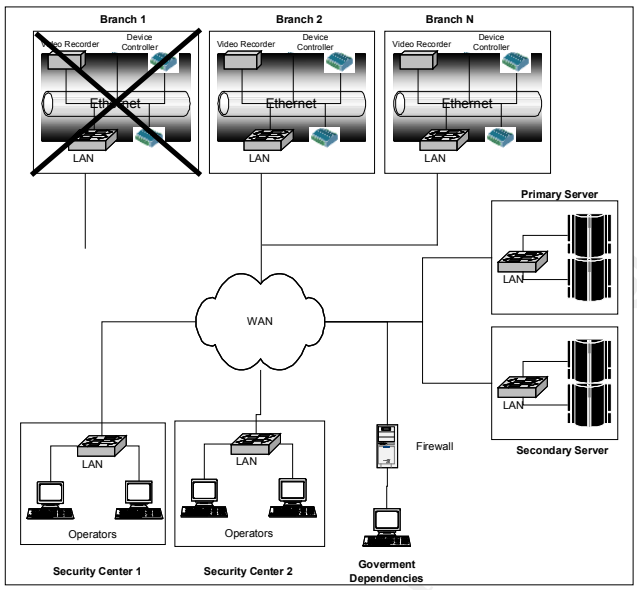


*Figure 8 One branch doesn't communicate with the server*

The security center operators receive an alarm notification that indicates a connectivity incident of the branch, so that they take the necessary actions for the problem solution . The installed components in the branch will try to reestablish a connection with the server through the network redundancy, and thus to maintain the system operativity. The operators will receive a message of which branch this using the backup network. The installed systems in the branch maintain their on-speed operation of local way, including the local registry of all the happened events. Once the communication is reestablished, the central server automatically will initiate a synchronization process in which all the registries of events occurred in the branch during the period of fault is transmitted to the server and the database is updated.

Scenario 4: Fault connectivy of a security center

The operators Security Center 1 will receive a message of connection fault with primary server. Automatically the client of the operators will try to communicate with the Secondary Server. If this communication settles down, the security center 1 will continue with its normal operation.

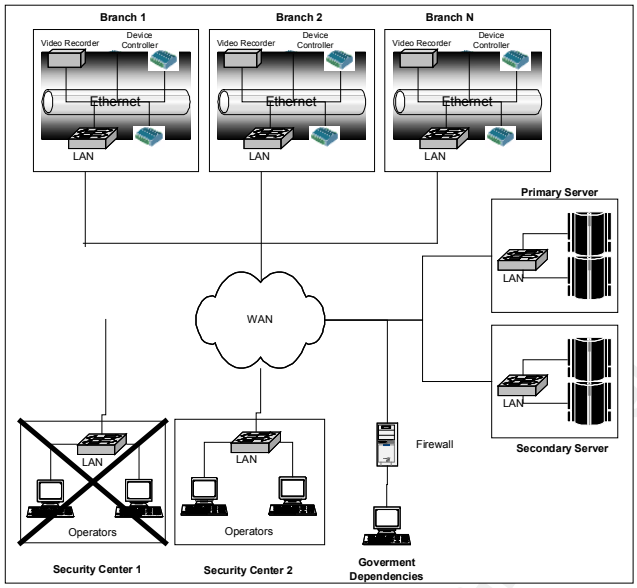


*Figure 9. Security Center it is out of operation*

The operators will have to take the necessary actions to restore the communications with the main server. (In this case, the security center will be operating with the secondary server and the security center 2 will do the same with the Primary Server). If the security center 1 cannot contact with the secondary server, it will send another message that indicates Communications fault with the secondary server. The operators of the security center 2, will receive a message indicating the state of the security center 1. When the communications are reestablished, automatically the security center returns to their normal state.

## Conclusions

Through this kind of systems, the great amount, extension, and complexity of the security operations that are carried out in a bank, are registered and controlled in their totality throughout the system, allowing total control of the security information in the financial institution at any moment. This way is feasible to guarantee that the security processes performed will be made according to the best international practices on the sector, fulfilling with the regulations and laws of the national banking sector as far as security of banking organizations.

Finally, the Banking Network can be included, allowing the connection of all the components of the system. In such way, the branches LAN networks, based on TCP/IP communications for the interconnection of devices and controller; and WAN TCP/IP networks to connect the gateways from the branches with the central server, allowing, therefore, to the information transmition between the Security Center and the branches.

**List of references**


British Standard. Information Technology – "Code of practice for information security management", BS ISO/IEC 17799:2000 BS 7799-1:2000, Pages 13-19 (February 2001)

Carnegie Mellon, "Software Process Improvement Overview", URL: http://www.cert.org/archive/pdf/managing-info-security.pdf - 2002

Constant, Mike, "What is closed circuit television?", CCTV Today Magazine, URL: http://www.cctv-information.co.uk/constant2/introctv.html

Crime prevention bookshelf, "Alarm Systems" URL: http://www.peelpolice.on.ca/prevention/alarms.htm, ( 14 October 1996)

Garfinkel, Simson and Spafford, Gene, "Practical Unix & Internet Security", O'Reilly and Associates, 1996. Page 357

Fraser, B. "RFC 2196: Site Security Handbook". September 1997. URL: http://www.ietf.org/rfc/rfc2196.txt?number=2196 (7 June 2003)

Mitnick, Kevin, "The Art of Deception: Controlling the Human Element of Security",John Wiley & Sons, 2002

Secretaría de Gobernación, "Nuevas Medidas de Seguridad para instituciones Bancarias, Diario Oficial de la Federación, 03 Octubre 2002 URL: http://www.gobernacion.gob.mx/dof/2002/octubre/dof_03-10-2002.pdf

Security Industry Association & Security Gateway, "Intrusion Detection / Alarm Systems", URL: http://www.securitygateway.com/page.asp?c=career_ov_burg

Security Industry Association & Security Gateway, Security System Integration URL:http://www.securitygateway.com/page.asp?c=career_ov_integration