SECURE AUTHENTICATED VIDEO EQUIPMENT*

Neall E. Doren
Sandia National Laboratories
PO Box 5800 Dept. 5923
Albuquerque, NM 87185
Phone: (505) 845-8660 Fax: (505) 844-2057

ABSTRACT

In the verification technology arena, there is a pressing need for surveillance and monitoring equipment that produces authentic, verifiable records of observed activities. Such a record provides the inspecting party with confidence that observed activities occurred as recorded, without undetected tampering or spoofing having taken place. The secure authenticated video equipment (SAVE) system provides an authenticated series of video images of an observed activity. Being self-contained and portable, it can be installed as a stand-alone surveillance system or used in conjunction with existing monitoring equipment in a non-invasive manner. Security is provided by a tamper-proof camera enclosure containing a private, electronic authentication key. Video data is transferred across a communication link consisting of a coaxial cable, fiber-optic link or other similar media. A video review station, located remotely from the camera, receives, validates, displays and stores the incoming data. Video data is validated within the review station using a public key, a copy of which is held by authorized parties. This scheme allows the holder of the public key to verify the authenticity of the recorded video data but precludes undetectable modification of the data generated by the tamper-protected private authentication key.

INTRODUCTION

The secure authenticated video equipment (SAVE) system is a stand-alone monitoring system for authenticated video surveillance. In addition to displaying authenticated video images of monitored activities as they occur, the system has the ability to store the observed images for later analysis and review. Consequently, the system may be manned and manually commanded by a user or set up in an automatic surveillance mode, allowing video data to be stored on disk for later review.

The system is composed of two primary components: a remotely mounted video acquisition and transmission unit, and a review station for controlling the cameras and viewing/storing the video data. These two components are connected via a high speed digital communication link. The acquisition unit is housed within a tamper-resistant, environmentally rugged container and is controlled via the review station (see FIGURE 1). All commands and video data traversing the communication link in either direction are authenticated before transmission and validated at the receiving end. Any command or video data transmission that fails to validate causes a system alarm, which is a notification to the user that the system's security may have been compromised. Furthermore, a number of tamper sensors, contained within the tamper-resistant housing of the acquisition unit, are continually monitored for activation. The review station will be alerted upon any tamper detection or authentication failure.

The SAVE system is based on microprocessor-controlled circuitry and is designed to take video "snapshots" manually or automatically at user-selected intervals, from either of two system cameras. The snapshots are digitized, compressed, and authenticated before being transmitted over the communication link to the remote station for validation, review and storage. Video compression allows the digital images to be transferred over the link more quickly. Digital technology is used, as opposed to analog, so that state-of-the-art compression, authentication, and transmission technologies could be incorporated.

The review station, which serves as the operator console, incorporates a user friendly, mouse driven interface for control and review of the video data. The user can select from a number of options and configuration parameters, in order to tailor the system to the application at hand. Video data can be reviewed automatically at timed intervals, or cameras can be commanded to take "snapshots" according to manual instructions issued by the user.

SYSTEM CONFIGURATION

The SAVE system was designed to be as modular as possible. Modularity refers to the incorporation of a number of independent, stand-alone

* This work is sponsored by the US Department of Energy, Office of Arms Control and Nonproliferation.

subsystems that work together to perform a common goal; namely, authenticated video monitoring. The SAVE system is very modular, so it is easily adaptable and configurable to a number of different applications. Furthermore, design, manufacture, testing and repair costs have been reduced due to the system's modularity. The ability to upgrade the system (or portions of the system) is another benefit of modularity. In fact, the core modules of the SAVE system, including the computer processors, authentication module, tamper detection system and communication system are common to the authenticated in-plant processor monitor (AIPM) project as well as to SAVE (see the AIPM paper, elsewhere in these proceedings). The AIPM system uses a "front-end" suited to monitoring sensors, while the SAVE system's "front-end" is suitable for video surveillance. By using the same set of core modules for both SAVE and AIPM, the development costs of both systems have been reduced.

In addition to modularity, another design goal of the system has been to incorporate readily available, commercial off-the-shelf (COTS) components and subsystems whenever possible. This has resulted in less time being spent on custom circuit design and fabrication since these have been handled by the component vendors. Furthermore, the modular design approach is well suited to the COTS construction technique, since different subsystems can be provided by different vendors, thereby creating a "customized" overall system at a lower cost than a full custom system. Drawbacks to the COTS approach include the lack of optimum components, limited availability, long lead times, company bankruptcies, etc. However, the risks are often worth the benefits, as the SAVE system illustrates.

HARDWARE CONFIGURATION

Both the remote acquisition unit and the review station are based on the STDBus microprocessor bus architecture. This bus is an industry standard, non-proprietary (open) interconnection scheme for microprocessors and associated peripherals. There were many advantages to using the STDBus architecture in the SAVE system. For example, many vendors offer circuit boards conforming to the STDBus specification, which provided the SAVE design engineers with a multitude of COTS choices for hardware. Furthermore, the STDBus has been used in industry and the military for many years, adding a degree of proven reliability to the project. Also, it is a very simple and robust specification, thereby adding to the reliability and making troubleshooting and repair a much easier task. Most importantly, the STDBus specification is based on the philosophy of modularity, allowing any number of different boards, from many different manufacturers, to be placed into a single system, with a great degree of confidence that the components will work harmoniously and reliably with one another. There are downsides to the STDBus architecture, including increased power consumption over similar custom designs, large board size, large numbers of interconnects (via the back plane), and increased system weight.

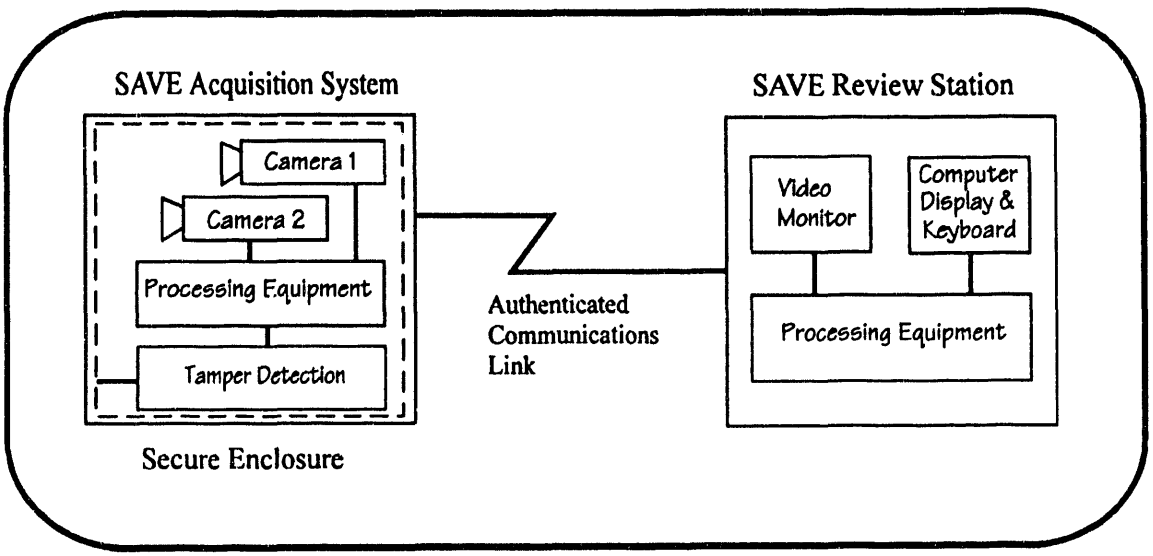


FIGURE 1. SAVE SYSTEM CONFIGURATION

FUNCTIONAL SUBSYSTEMS

The SAVE system contains a number of functional subsystems, together which yield a fully functional video system. The remote video acquisition component and the review station component are very similar in configuration. Both contain the following subsystems:

- Central Processing unit
- Digitizing frame grabber/display subsystem.
- Video compression/decompression subsystem.
- Data authentication/validation subsystem.
- Communications subsystem.
- Tamper detection/key management subsystem.

In addition, the remote acquisition unit contains a pair of compact video cameras for video surveillance and a power management system with battery backup for use during power failures (see FIGURE 2). The review station incorporates a video display monitor, keyboard and mouse for use as the user interface (see FIGURE 3). Each of the subsystems will be explained in further detail in the following paragraphs.

The **central processing units** of both the review station and remote acquisition unit are based on STDBus circuit boards manufactured by Ziatech, Inc., of San Luis Obispo, CA. The remote acquisition unit contains an 80286 Based CPU card with on-board RAM, ROM, timers, and a real-time clock. The operating software is embedded into the system ROM (known as firmware), which prevents unintended modification and increases overall system reliability and security. There is no user interaction directly with the acquisition unit, and consequently, no "operating system" is required. Instead, the operating program, dedicated to the operation of the remote acquisition system, is permanently embedded into the system ROM, without the overhead and security risks of an operating system.

The central processing unit of the review station is also a Ziatech STDBus card, based on the Intel 80486 CPU. The review station requires more processing power than the remote system due to the graphical interface, mouse, keyboard, and hard disk requirements of this unit. The review station runs MSDOS, which is an industry standard operating system for microcomputers and many PCs. Normally, the addition of an operating system such as MSDOS could compromise the security of the system. However, it is assumed the review station will be placed within the confines of an appropriately secured facility.

The **digitizing frame grabber/display** subsystem is based on an STDBus card manufactured by Imagenation, Inc., of Vancouver, WA. This card, called the Cortex-I frame grabber, is both a video digitizer and video display card. In the remote acquisition system, the card acts a video digitizer, capable of user-selectable resolutions of 256x256 pixels or 512x512 pixels, both with 8 bit (256 level) gray scale quantization. Card inputs and outputs conform to industry standard RS-170 (NTSC) video signals. In the review station, the frame grabber is used to display the received video images on the display console. The frame grabber card has a special "sleep mode" that reduces power consumption while not active. This mode is particularly useful in the remote acquisition unit, which relies on battery backup power in the event of a power failure.

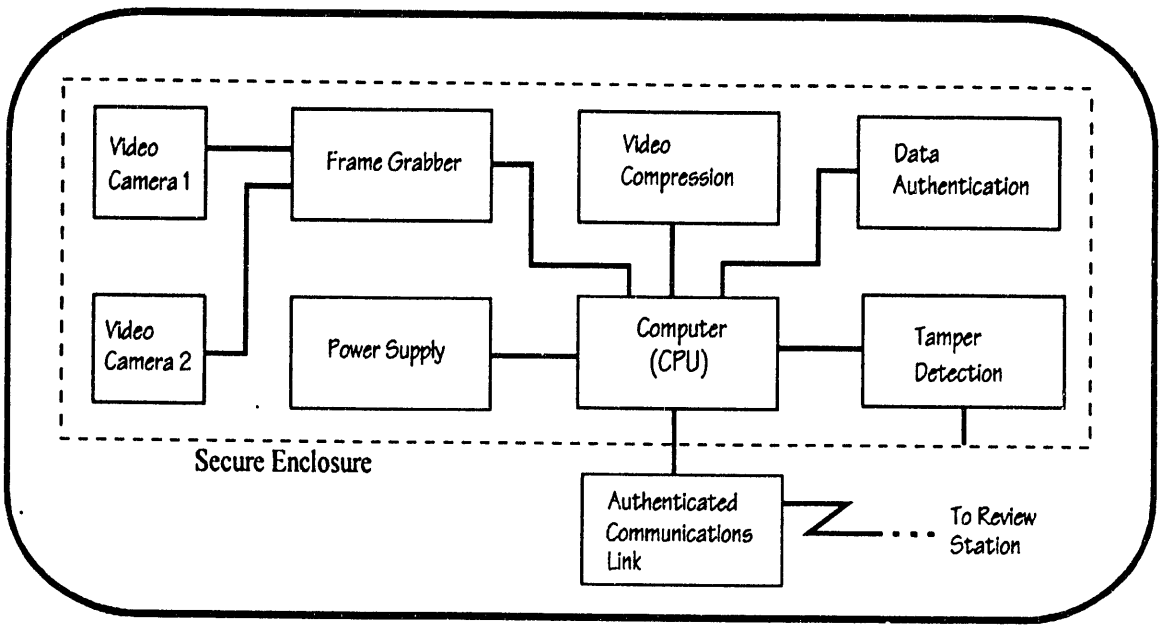


FIGURE 2. SUBSYSTEMS - REMOTE ACQUISITION UNIT

The **video compression/decompression** subsystem is based on a custom STDBus card designed at Sandia National Laboratories. A custom card is required since no off-the-shelf-hardware is currently available to meet the requirements of the system. The purpose of the card is to reduce (compress) the amount of video data being sent over the communication link, thereby lowering its transmission time. The remote acquisition system's card is dedicated to compression, while the card in the review station is dedicated to decompression.

The compression/decompression scheme is based on the specification set forth by the CCITT/ISO Joint Photographic Experts Group (JPEG) [1]. The JPEG algorithm is "lossy," meaning that as the compression ratio of the source image increases, the quality of the resultant decompressed image decreases. Thus, there is a tradeoff between the compression factor of the original image and the quality of the resultant decompressed image. The user of the SAVE system can adjust the compression (image quality) to suit the application. Increasing the compression means a greater throughput of images across the communication link to the review station. High quality (low compression) imaging typically results in a transfer time of about 10 seconds from the remote unit to the review station. Using high compression sacrifices image quality somewhat, but results in up to a tenfold increase in transfer speed. As with the frame grabber board, the compression/decompression board has a special power-saving "sleep" mode.

The **data authentication/validation** subsystem is based on a software algorithm run on an STDBus-based digital signal processing (DSP) card. This board, based on the Motorola DSP56000 CPU chip, is manufactured by Ziatech, Inc. The authentication algorithm is permanently embedded within the ROM on this card. This algorithm is an implementation of the DSA1 algorithm, with future implementations utilizing the new DSS authentication standard. These algorithms are based on a public/private key methodology. Specifically, the video information acquired by the remote system is digitized, compressed and then authenticated using the algorithm, which is driven by a private, protected key. The key's value is known only by the authorized user responsible for fielding the system. This key, contained within a special RAM chip on the DSP board, is protected by a number of physical and software tamper detection schemes. Attempts to penetrate the system to obtain the key value will result in the erasure or physical destruction of the key RAM chip, before the contents can be determined.

Once received at the review station, the video data is validated using a public key. This key is mathematically related to the private key such that the incoming data can be verified as having been generated by the private key. However, the algorithm is such that the public key cannot be used to generate authenticated data, nor can it be used to derive the private key. In this way, any inspecting party privy to the public key can validate the video data being reviewed, providing a measure of confidence that the data was not corrupted, either intentionally or accidentally, at it traveled across the communication link. This confidence is provided by the fact that owning the public key allows the validation but not the undetectable modification of the data, and that the private key, contained within the acquisition unit, is protected by a number of physical and software barriers. Note that data is sent in the clear; that is, not encrypted. Consequently, it is readable by anyone. However, possession of the public key is necessary to validate the data, thereby ensuring it originated at the expected source and arrived without tampering.

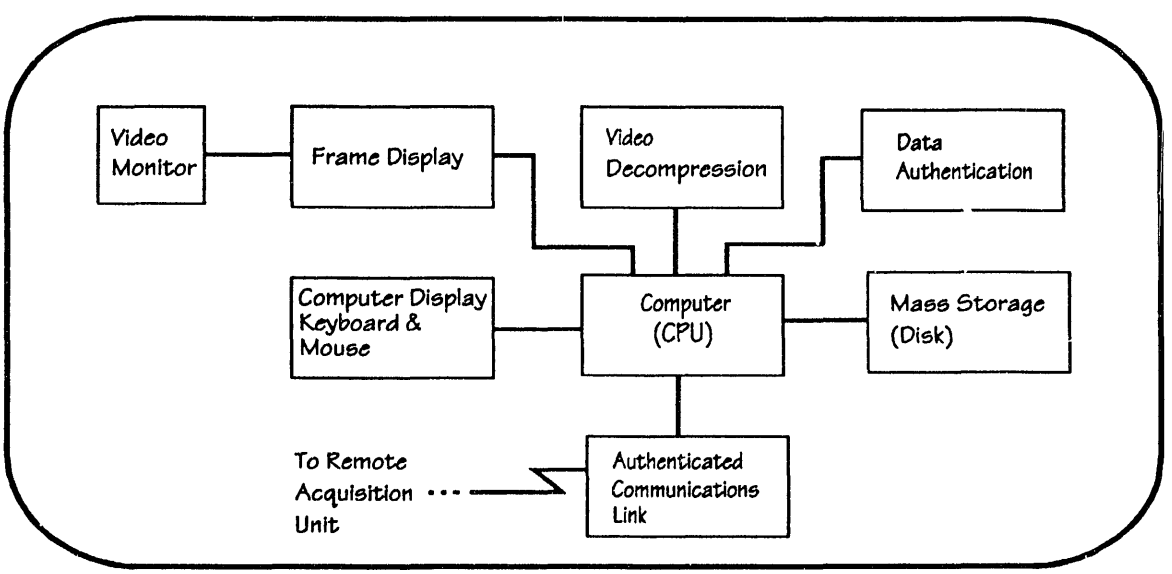


FIGURE 3. SUBSYSTEMS - REVIEW STATION

The **communications subsystem** is responsible for the transmission of the digital data between the remote acquisition unit and the review station. Currently, an industry standard RS-232 port is used for this communication, running at a baud rate of 38400. The port resides on the CPU card of both the remote acquisition unit and the review station. Associated software is responsible for the flow of data between these ports, as well as for fault detection and tolerance. The ports are connected using a fiber optic (FO) cable for low loss, with the appropriate RS232-to-FO modems present at both ends. In the future, a dedicated, high speed board may be used for this function. This would greatly increase the throughput of the system and would off load the communications overhead, allowing the system to respond more quickly to external commands and tamper events.

The purpose of the **tamper subsystem** is to monitor and detect any attempt to compromise the system or secret authentication key. The security philosophy is all encompassing, and as such, considers potential attacks at the source of the data, the video equipment and the data link. To help deter attacks at the data source, two surveillance cameras, of different focal lengths and fields of view, are installed within the secure acquisition unit enclosure. Video images are randomly taken from one camera and then the other. Since a potential adversary does not know which camera is currently taking video, it is difficult to "spoof" the cameras using a false fore drop or other falsified data scenario.

The video equipment that must be tamper protected consists of the remote acquisition unit and the associated communication link. These items are directly accessible to the adversary, and as such, require security measures. The video review station, on the other hand, is generally located within a friendly (non-adversarial) environment, and consequently, requires no tamper protection (see FIGURE 4). The remote acquisition unit is protected against attack by layers of physical tamper sensors. These include a penetration detector around the inside periphery of the containment vessel, as well as a number of internal sensors for light, radiation, motion, temperature, and power supply variations. The object of the protection is not to prevent tampering, but instead, to detect any tampering that may occur and to destroy the private authentication key, thereby eliminating any possibility of authenticated data being transmitted from the unit.

Once the data has exited the secure confines of the tamper-protected acquisition unit, the data becomes vulnerable to data tampering. This is the reason that authentication of the data is performed. This prevents the adversary from substituting false data into the communication link or modifying the data moving across the link. Both the commands to the remote acquisition unit, as well as video data back to the review station, are authenticated. This prevents an adversary from inserting an unauthorized review station into the data line and issuing illicit commands to the acquisition unit.

A battery-backed uninterruptible power supply system is also contained within the tamper protected boundary of the remote unit. This is to ensure an adversary does not try to spoof the system by cycling or altering the supply power. Presently, the system is powered using domestic US supply current (115 VAC, 60 Hz.).

SYSTEM SOFTWARE

The remote acquisition unit is based on a customized, embedded application program, and as such, does not contain an operating system. This minimizes the possibility of undetected tampering, while reducing the possibility of system failure due to bulky and non-robust operating system code. The review station, which is within the confines of a friendly installation, runs a special application program running under the Microsoft Disk Operating System (MSDOS). In every case, the operating programs have been specifically designed to meet stringent standards for fault tolerance, robustness, correctness, efficiency and security. The software has been written in accordance with the applicable elements of several standards, including the INFOSEC Engineering Standards and Practices Manual, Security Guidelines for COMSEC Software Development, and Security Requirements for Cryptographic Modules [2, 3, 4].

APPLICATIONS

Applications for the SAVE system abound. Its portable size and non-invasive nature allow great versatility. The SAVE system may provide sufficient verifiable monitoring when used by itself, or it can be used with other monitoring equipment to provide an additional monitoring tool. Since it is a non-invasive stand-alone unit, it can provide additional security to a previously installed system, without fear of invalidating the integrity of the original system. Possible applications are as follows:

- Process monitoring (chemical weapons (CW) destruction facility).
- Long-term staging prior to processing (CW, SNM, etc.).
- Warhead dismantlement (document critical tasks).
- SNM storage monitoring (record a robotic inventory).
- Tamper documentation (coincident with other sensors).
- Pre-inspection monitoring (challenge inspection).
- Host-operated controlled access (challenge inspection).
- Portal/perimeter monitoring (declared critical sites).

The technology is fully exportable and is easily adaptable to different line voltage power. In many situations, pre-existing building cabling can be used as the physical transmission media, eliminating the need for special wiring requirements. Furthermore, data authentication ensures the integrity of video information, even when communication lines are not physically protected from tampering.

CURRENT STATUS

Currently, a bench-top SAVE system is available for testing and demonstrations. This system is fully functional but lacks the final tamper-detecting enclosure for the remote acquisition unit. This enclosure is slated for completion by the end of FY 1993. Several technical hurdles must be overcome before the tamper enclosure design is complete. First, more development time must be devoted to the outermost tamper protection layer before it is fully viable. Second, EMI/RFI emissions from the enclosure must be more thoroughly analyzed to ensure that they fall within the NIST security guidelines, and modifications must be made if out of tolerance. Finally, cooling (air circulation) issues within the secure enclosure still remain to be worked out. None of these hurdles are felt to be insurmountable.

Meanwhile, as the enclosure development effort continues, refinements and improvements are being made to the system software. A Microsoft Windows user interface is being designed, which will significantly increase the user-friendliness of the system. This interface will be capable of displaying a number of simultaneous video frames to the console, along with the control menus. Also, improvements are being made to the communication link in terms of throughput (speed) and there is an ongoing effort to increase the robustness, reliability, speed, and security of the system software.

Finally, a vulnerability analysis will be performed on the system, and operational tests and demonstrations will be conducted in the field. It is expected that the SAVE system will be fielded for beta testing in FY 1994.

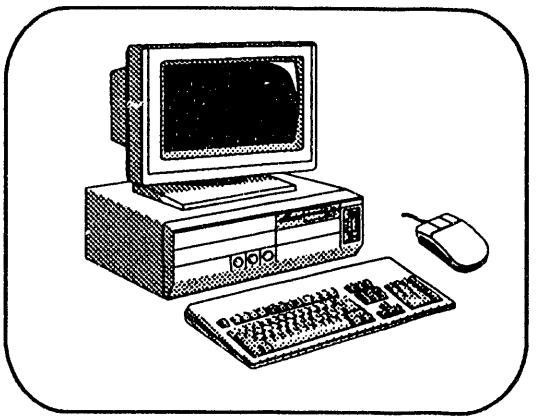


FIGURE 4. SAVE REVIEW STATION

SUMMARY

The Secure Authenticated Video System (SAVE) provides automatic documentation of activities occurring within an area visually monitored by the system, while reliably detecting tampering with the system itself. The documentation provided by SAVE is of sufficient integrity to provide the user with confidence that the monitored activity actually occurred as recorded. The system is portable, exportable, and simple to set up and use. It is suitable for stand-alone monitoring, but being non-invasive, can be used to supplement previously installed monitoring equipment without interfering. The system is adaptable to a variety of monitoring, verification and security applications, or wherever authenticated imaging is required.

REFERENCES

[1] "ISO Committee Draft Document, ISO/IEC CD 10918-1," ISO/CCITT Technical Committee.

[2] "INFOSEC Software Engineering Standards and Practices Manual," NSA DS-80, December 1, 1988.

[3] "Security Guidelines for COMSEC Software Development," Revision 3.0, January 27, 1988.

[4] "Security Requirements for Cryptographic Modules," Federal Information Processing Standards Publication 140-1, National Institute of Standards and Technology, Washington, DC.

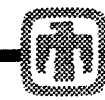
Secure Authenticated Video Equipment (SAVE)

Neall Doren

On-Site Monitoring Technology
Department 9249
Sandia National Laboratories

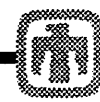
Outline

- Objectives
- Products in development
- System features and functional overview
- Security features
- Possible applications
- Summary



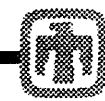
Objectives

- To develop an unattended video monitoring system capable of providing reliable, tamper-free video data to the user
- To provide the user with documentation of the activity being monitored
- To ensure that the documentation accurately represents the activity being monitored



Products

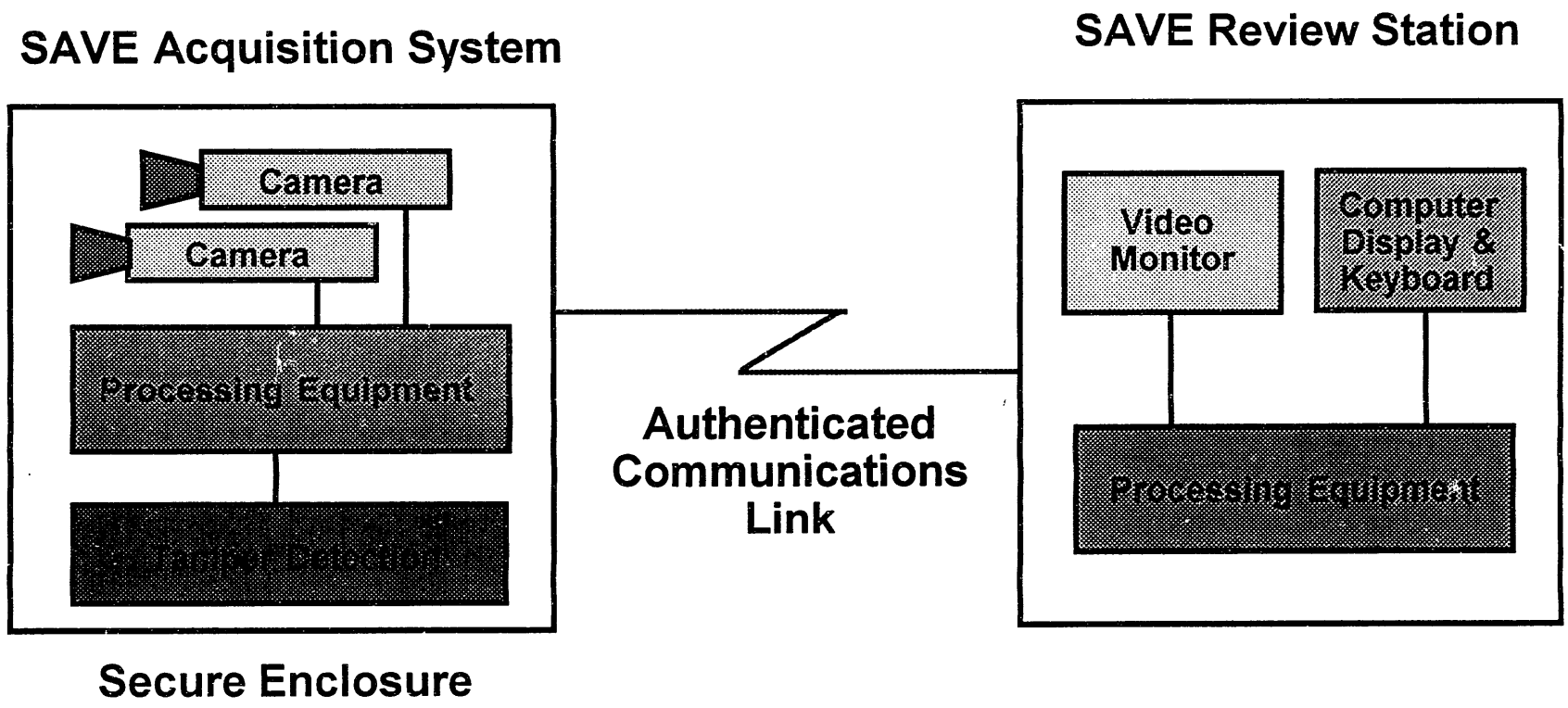
- A video surveillance system, packaged in a tamper-indicating enclosure, that generates highly tamper-resistant data
- A video review station capable of storing and displaying video data, while simultaneously checking the integrity of the enclosure and video data



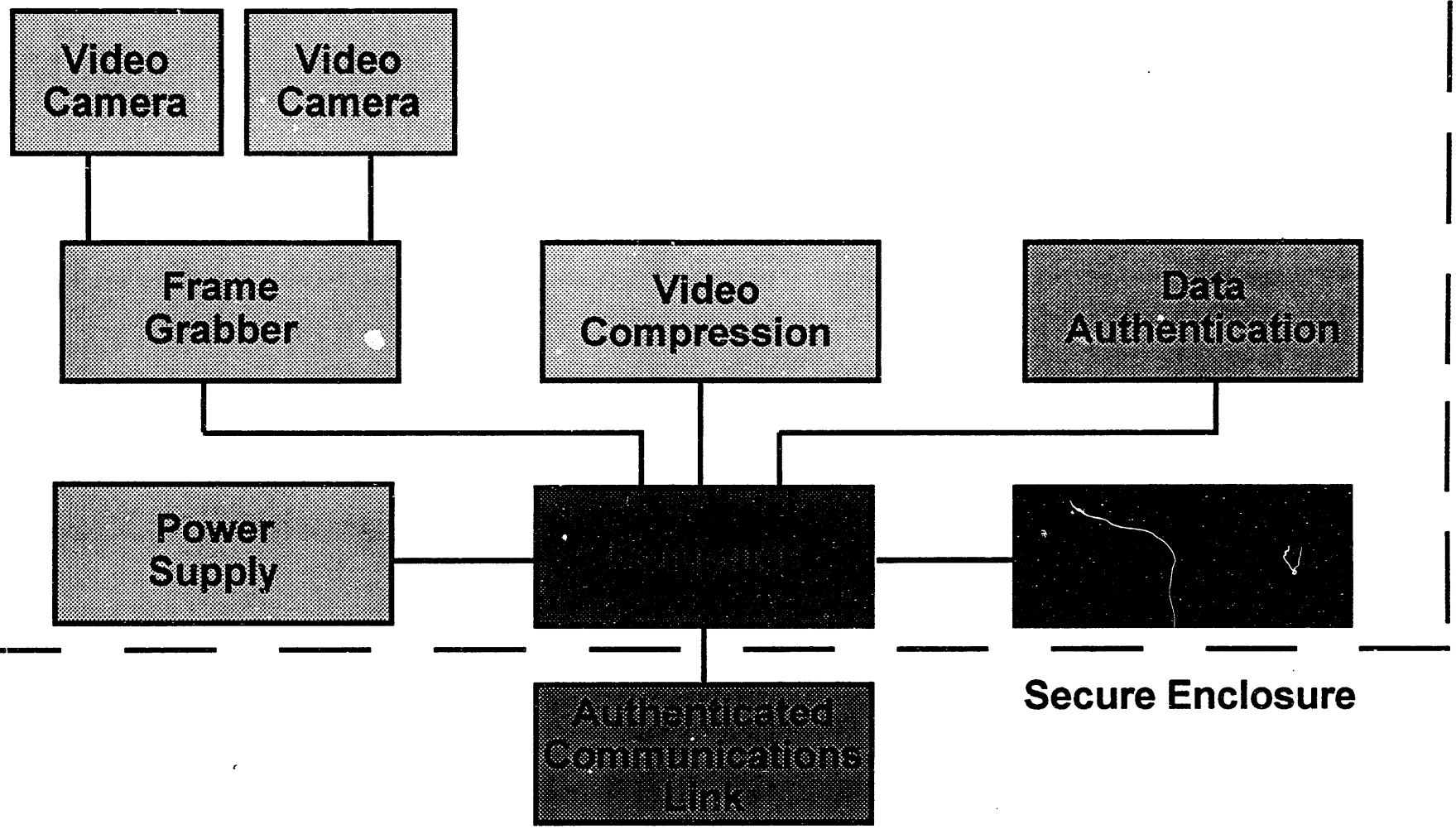
System Features

- Standalone operation, or use in conjunction with previously installed monitoring equipment for additional confidence (non-intrusive)
- Simple set-up and take-down with minimal wiring requirements
- Simple to learn and use
- High video throughput (using data compression)
- Rugged, reliable and secure

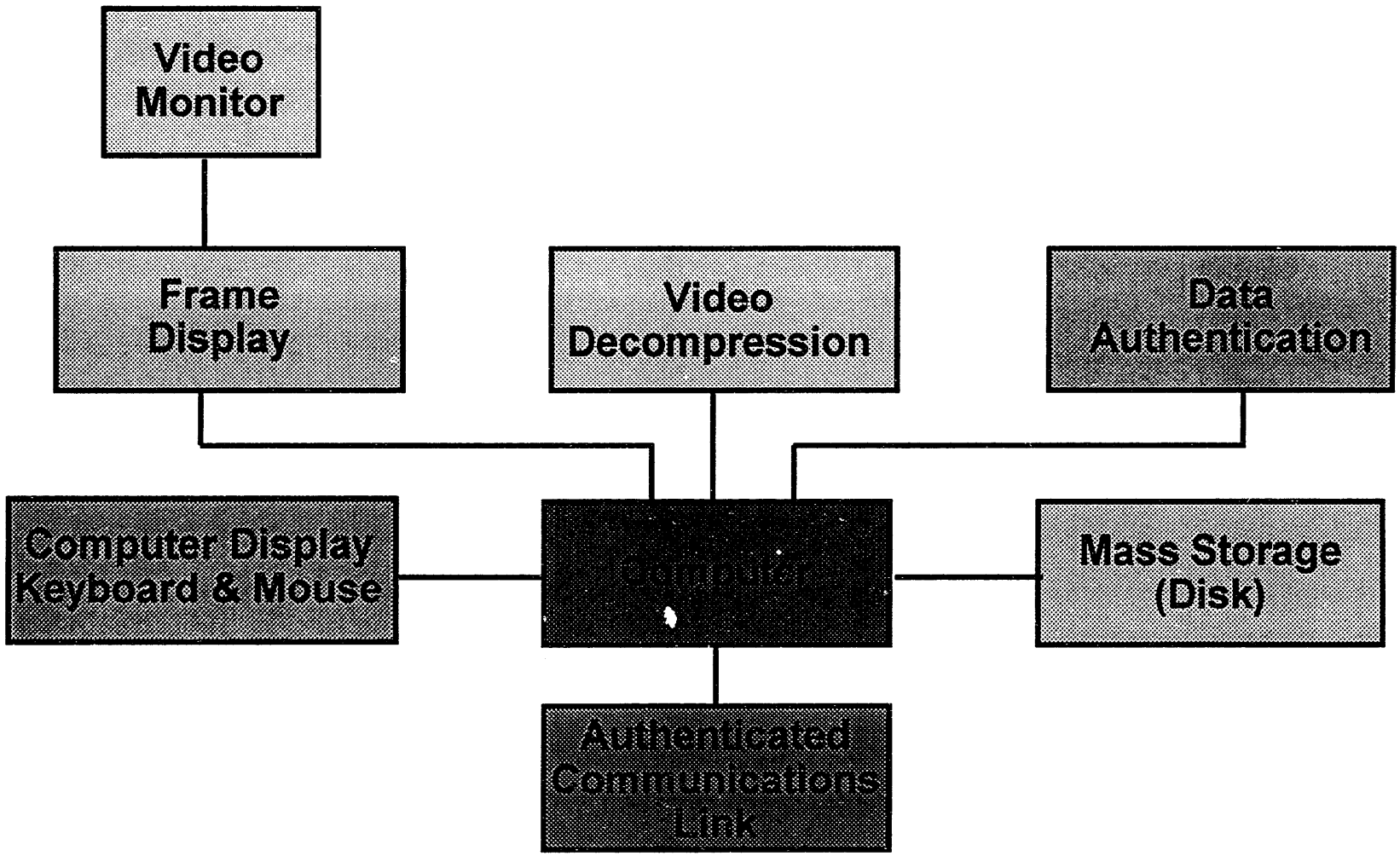
SAVE Block Diagram



SAVE Acquisition System Block Diagram



SAVE Review Station Block Diagram



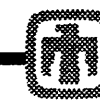
Security Features

The security philosophy considers potential attacks at the source of the data, video equipment, and data link

- Source Attacks — Handled by multiple cameras with different focal lengths or possibly with image processing software
- Equipment Attacks — Handled by the tamper-indicating enclosure and its associated sensors as well as by incorporation of a secure software methodology
- Data Attacks — Handled by the Public key data authentication system within the secure enclosure

Possible Applications

- Process monitoring (CW destruction facility)
- Long-term staging prior to processing (CW, SNM, etc.)
- Warhead dismantlement (document critical tasks)
- SNM storage monitoring (record a robotic inventory)
- Tamper documentation (coincident with other sensors)
- Pre-inspection monitoring (challenge inspection)
- Host-operated controlled access (challenge inspection)
- Portal/perimeter monitoring (declared critical sites)



Summary

The Secure Authenticated Video System (SAVE) provides automatic documentation of activities occurring within an area visually monitored by the system, while reliably detecting tampering with the system itself

The documentation provided by SAVE is of sufficient integrity to provide the user with confidence that the monitored activity actually occurred as recorded

END

DATE
FILMED
9/24/93