MediaSign® Digital 

White Paper

Utilizing Digital Watermarks for Secure, Long-Term Archiving of Digital Images and Records

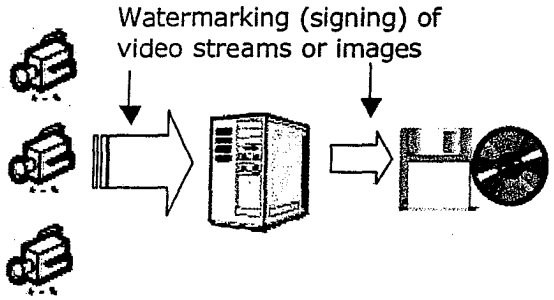
MediaSec Technologies
Hubert Peulen
Version 1.02
May 16, 2003

MediaSign Digital

Digital watermarking for authentication of digital video

The market for digital video and imaging systems is set to explode. Law enforcement agencies have begun the transition from analog to digital surveillance and evidence gathering systems. However, defense attorneys can easily question the admissibility of digital evidence in court because it can be doctored, enhanced or manipulated on a computer.
Meanwhile, high-tech counterfeiting and manipulation equipment has become more sophisticated and less costly to acquire.

MediaSignDigital is a patented technology that provides permanent and inseparable authentication for digital video and images. It embeds a digital watermark containing the secure hash value of the image data into each frame or image. The watermark is invisible to the naked eye and does not alter the value of the watermarked data.
Any attempt to manipulate even a single frame will be detected.



Video streams or still images are authenticated when they are captured, stored, or exported to portable storage devices (disk & CD), or transferred on the network.

Fields of use:

- **Video surveillance (DVR)**
- **Law enforcement**
- **Insurance, finance, and more...**

Features

- **Cost effective:** No additional data to maintain.
- **Fine-grained authentication:** Any part of the data can be authenticated. Any alterations (including the locations in each video frame) will be detected.
- **Secure authentication:** A secret key protects the authentication watermark. Re-signing is prohibited.
- **Time and source authentication:** Each video frame is stamped with date, time and capture source. Attempted removal of frames in the video stream is detectable.
- **Self-contained and inseparable:** The authentication code (secret key) is embedded in the pixel data itself.
- **Bridges the gap between digital and analog authentication:** Watermarked images or video can be authenticated in both digital and analog (printed image, analog video) versions.

Availability

MediaSignDigital is available on Windows NT/2000/XP/98/95 platforms as an SDK or an application. Other platforms are available upon request. Supports common image formats such as MPEG2, MJPEG, JPEG & TIF, and others by request.

MediaSec Technologies
The Media Security Company

Providence, Rhode Island, USA:
Tel: 401-272-3388
Fax: 401-272-4884
Email: info@mediasec.com

Essen, Germany:
Tel: +49 201-437-5270
Fax: +49 201-437-5277
Email: info@mediasec.de

Ensure the integrity of digital evidence
www.mediasec.com

Introduction

The necessity of long-term conservation of digital documents exists for archives, libraries and to an increasing extent for business enterprises, insurance companies, notary/solicitor's offices, government agencies and public authorities. The triumphant advance of the "paperless office" is taking longer than was forecasted some years ago; however, most institutions are moving toward scanning and digitizing their files and are replacing the filing cabinets and shelves that have been used for decades (or even centuries). Records such as those found in notary's offices, patent offices or parliamentary archives have long-term legal and economic importance.

Paper documents can be protected from manipulation due to the use of the paper medium and through the use of signatures, stamps, or seals. However, digital photos and documents can be easily manipulated after their original production or after the records have been scanned and digitally archived. Therefore, the use of digital records in administration, justice and historical research is restricted. For these fields of application, it is absolutely essential to use technical procedures which guarantee the verification and authenticity of digital images. By applying MediaSec's MediaSign® Digital technology, these requirements can be met easily and cost-effectively.

Marking digital records with MediaSign® Digital allows any manipulation to be proven without doubt. The manipulation can be easily located and relevant information such as the copyright source, creation date and other meta-data can be read even after the images have been manipulated and modified (ex. lossy image compression, conversion of color pictures into gray-scale pictures, or filter operations).

1. Application: Digital Archiving of Images and Records

Digitizing is a modern method of archiving and protecting images, documents and records. Picture libraries, document archives, museums and other collections are confronted with questions arising directly from the dynamic force of our communications society. The information explosion of modern mass media is only one aspect of the problem.

Apart from the *sheer storing of information,* which is no longer dependent on a certain physical form of the carrier (ex. CD-ROM, WORM), the question of the ***authenticity and integrity*** of archived records is of central importance, as archived information is necessary for administration purposes, the judicial system, historical research and many other uses.

2. National Legal Requirements

There are a number of national laws, decrees and regulations which directly or indirectly demand safekeeping of documents for the proof of rendered services, received orders or notifications, expenses, taxes, etc.

2.1 Germany

Principles of proper DP-supported accounting systems (GoBS)[1]

Principles of data access and of the verifiability of digital documents[2]

Since January 1st of 2002, documents which have to be retained (as defined by § 147, sec. 1 AO) that are digitized and are not transmitted in paper form must comply with

[1] Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)

[2] Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)

GoBS. **The original condition of the transmitted and possibly encrypted data must be recognizable** (§ 146, sec. 4 AO) and the data must be stored on a carrier which does not allow modifications.

If the data is stored temporarily on an alterable data carrier, the data-processing system must ensure that **modifications are impossible.**

If cryptographic technology is used, the encrypted and decrypted documents must be kept.

According to GoBS, when other documents that must be retained are converted into a company-specific format (a so-called "in-house format") both versions have to be archived and filed with the same index and the converted version must be marked as such.

If signature-test keys or cryptographic methods are used, the applied keys must be kept.

With regard to other documents requiring retention, the date of receipt, archiving, further processing and conversion must be recorded.

2.2 USA

Sarbanes-Oxley Act of 2002

In response to numerous corporate accounting scandals that have plagued U.S. businesses recently, a new law was signed by President Bush on July 31, 2002 named the Sarbanes-Oxley Act of 2002. Due to this act, the Public Company Accounting Oversight Board (Board) was created in order to oversee audits of public companies subject to securities laws. This act contains reforms in corporate governance and disclosure rules applicable to publicly traded companies and new requirements for registered public accounting firms that provide audit services to such companies. A number of the act's provisions became effective immediately, while other provisions will be implemented over the course of the next twelve months through the Securities and Exchange Commission (SEC). Of major importance to the records management profession are penalties for the destruction of records, retention time frames for certain audit records, and document production requirements.

The important highlights of this act that affect records management are:

Anyone who knowingly alters, destroys, conceals, or falsifies documents or tangible objects with the intent to impede, obstruct, or influence an investigation involving federal departments and agencies or bankruptcy proceedings will be subject to fines and/or imprisonment of up to 20 years.

Anyone who attempts or conspires to commit any offense under the Act will be subject to the same penalties for committing the offense.

A violation of the act's audit records retention requirements is punishable by up to 10 years imprisonment.

Any accountant conducting an audit of a publicly traded company is required to retain all audit or review work papers and related documents for a period of five years from the end of the fiscal year in which the audit or review was conducted. Knowing and willful violations of these requirements are subject to up to 10 years imprisonment, fines, or both. The SEC may establish further record retention requirements, which will have the same penalties.

A registered firm must retain audit work papers and other related information to support the audit reports required under this act for a period of not less than 7 years.

The Board may require further retention requirements by registered firms for inspection of records whose retention is not required by Section 103 (audit and work papers) or additional rules that may be issued under that rule by the Board or SEC.3.

- Protection of integrity, authenticity and conclusiveness of the archived records
- Secure verification and proof of manipulations
- Removal of elements of the picture / text passages
- Moving of elements, modification of positions
- Modification of the scene lighting
- Guarantee of imperceptibility (invisibility)

Robustness against modifications of the image, such as:

- Conversion into other image formats
- Modification of brightness
- Modification of contrast
- Conversion of the color format (reduction of colors or gray-scale conversion)
- Slight interference
- Compression

4.2 Cryptographic Methods

While using a customary cryptographic signature principle some specific problems will arise when it is necessary to convert the format or to carry out editing processes. Conversion or editing often does not represent a manipulation of the content of the image, but will be immediately interpreted as manipulation.

When a cryptographic method is used, signatures can be removed.

Signatures will become invalid if the material is converted into other image formats, if brightness or contrast is modified, if the color format is converted, if there is a slight interference, or during compression.

4.3 Watermarking Technology

A digital watermark is a transparent pattern which is embedded into a digital image by an embedding algorithm and the use of a secret key. This method comes from the field of steganography (technology of secretly transmitting information) and was refined due to varying requirements (visibility, multitude of information, and robustness).

In most cases invisible digital watermarks are used, however, other methods involve deliberately attaching visible watermarks to an object.

4.3.1 Categorization of Digital Watermarks

In order to differentiate between the various procedures, the following categorization is made:

- Visible digital watermarks
- Invisible robust digital watermarks
- Invisible fragile digital watermarks

Smiths Detection

May 22, 2007

smiths detection
bringing technology to life

Peter Mottur	President & GM
Doug Tuthill	Director of Global Solutions
Patrick Hay	Operations Manager
Jon Cooper	Director of Engineering
Allan Ramella	Senior Systems Engineer
Doug Stringer	President, Stonecrop Technologies
Chris McDermott	Senior Project Manager, TRC Companies, Inc.

www.smithsdetection.com

Joint Venture Pending Approval

Fall 2007

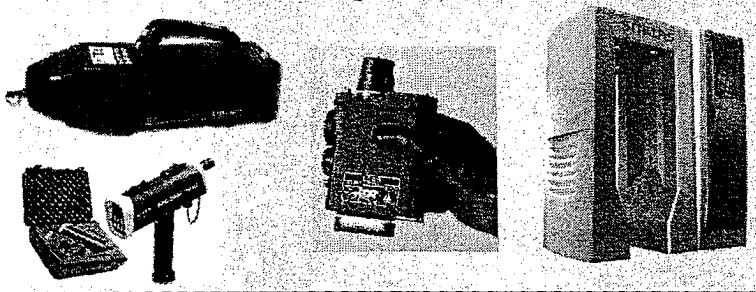
Homeland Protection

smiths detection

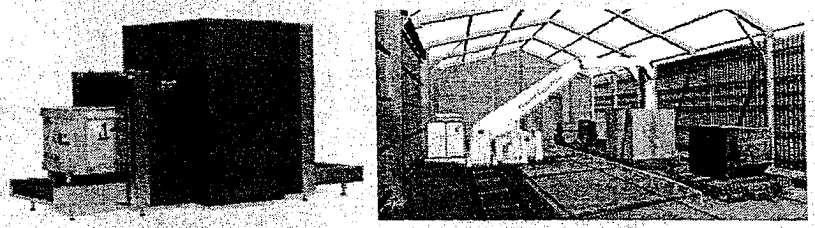
bringing technology to life

Widest range of detection technologies

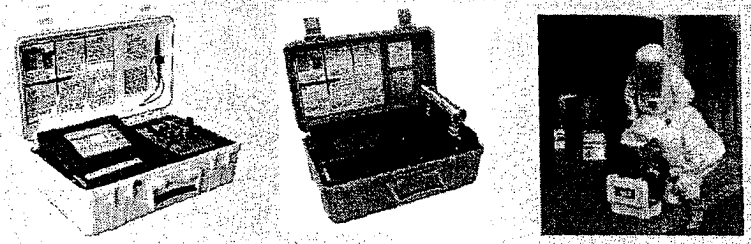
Trace and Bio agent detection



Conventional and Cargo X-ray

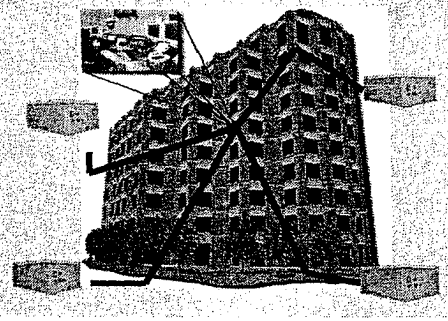


Infra-red chemical analysis

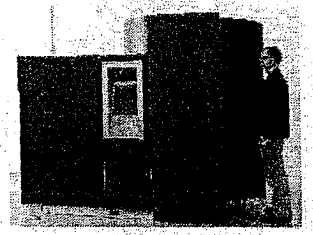


Networked IP Video Systems

Facility Monitoring



Millimetre wave



smiths detection

New Office: Opening July 2007

27 Drydock Ave, Boston, MA
11,500sf (Service & Support Location)

smiths detection
Boston, MA

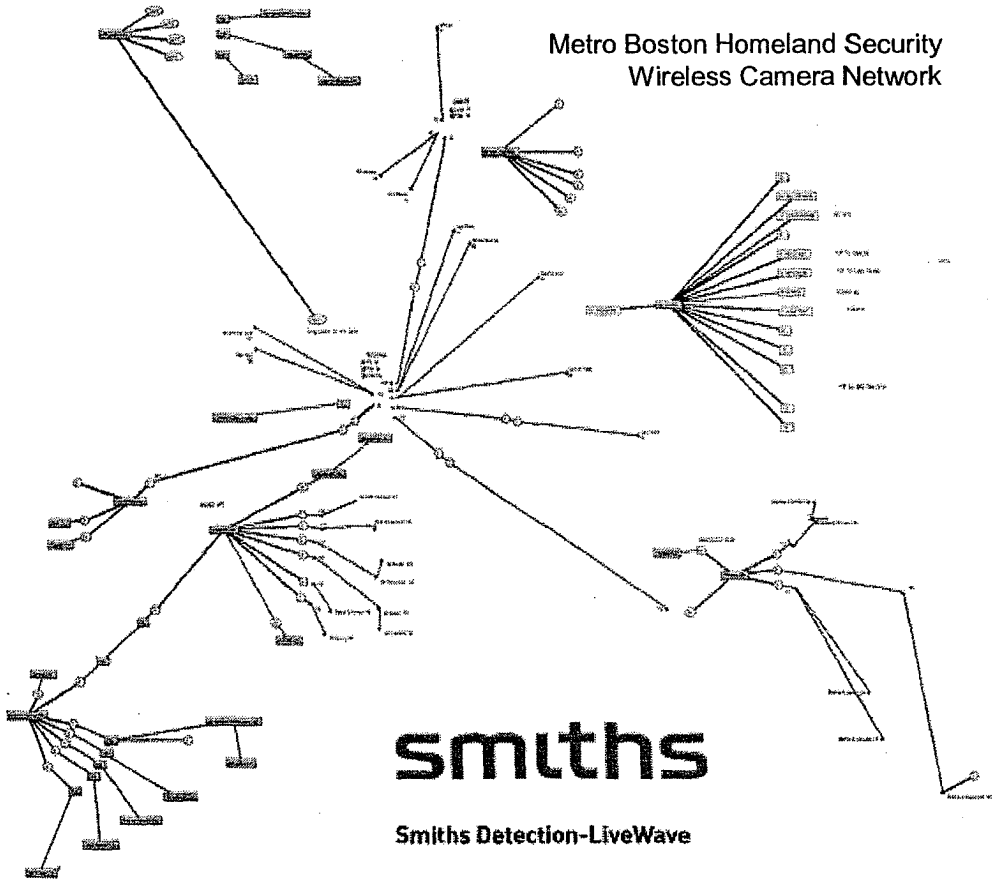
smiths detection

Team Introduction

Company	Role	Responsibilities	Location
Smiths Detection Inc.	Prime Contractor	Program Management, CCTV software & hardware, support services.	Middletown, RI
StoneCrop Technologies	Subcontractor	Wireless design and network engineering, service and support.	Pembroke, MA
JF White/Sonet Electric	Subcontractor	Site installations, on-site maintenance & support.	Charlestown, MA
Sullivan & McLaughlin	Subcontractor	Site installations, on-site maintenance & support.	Boston, MA
TRC Engineers	Subcontractor	Professional security consultants, design services, stamped engineering drawings.	Boston, MA

How Did We Get Here

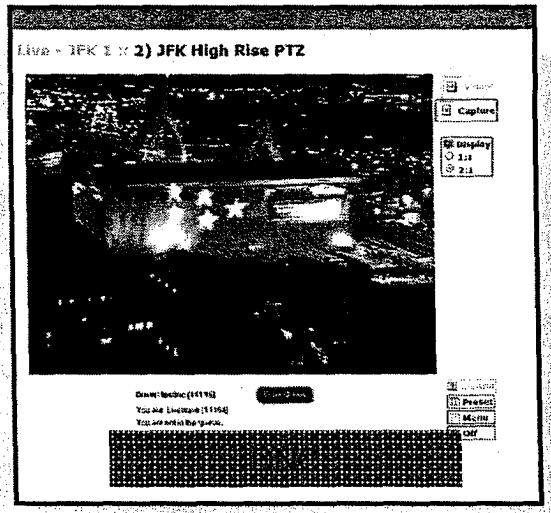
- **July 2002:** LiveWave meets EPD and sketches vision for Interoperable Wireless Network.
- **March 2003:** LiveWave wins Everett Port Security Project.
- **June 2003:** LiveWave wins contract for Interoperable network for FPS & BPD for DNC.
- **July 2004:** LiveWave wins contract for RNC in New York from FPS.
- **October 2004:** LiveWave wins contract for RPD camera network
- **January 2005:** LiveWave wins contract for Presidential Inauguration from USSS and FPS.
- **August 2006:** Smiths Detection-LiveWave wins contract to expand BPD network & cameras and connect: BDP, FPS, EDP, CPD & RPD



smiths detection

FirstView Interoperability Today

- BPD & FPS share video for DNC
- National Counterterrorism Center views Boston cameras in DC Command Center
- FPS shares RoverCam with BPD for events & operations
- MBTA shares video with BPD
- BPD & FPS use camera system during recent "cartoon promo"



Past Issues & Solutions

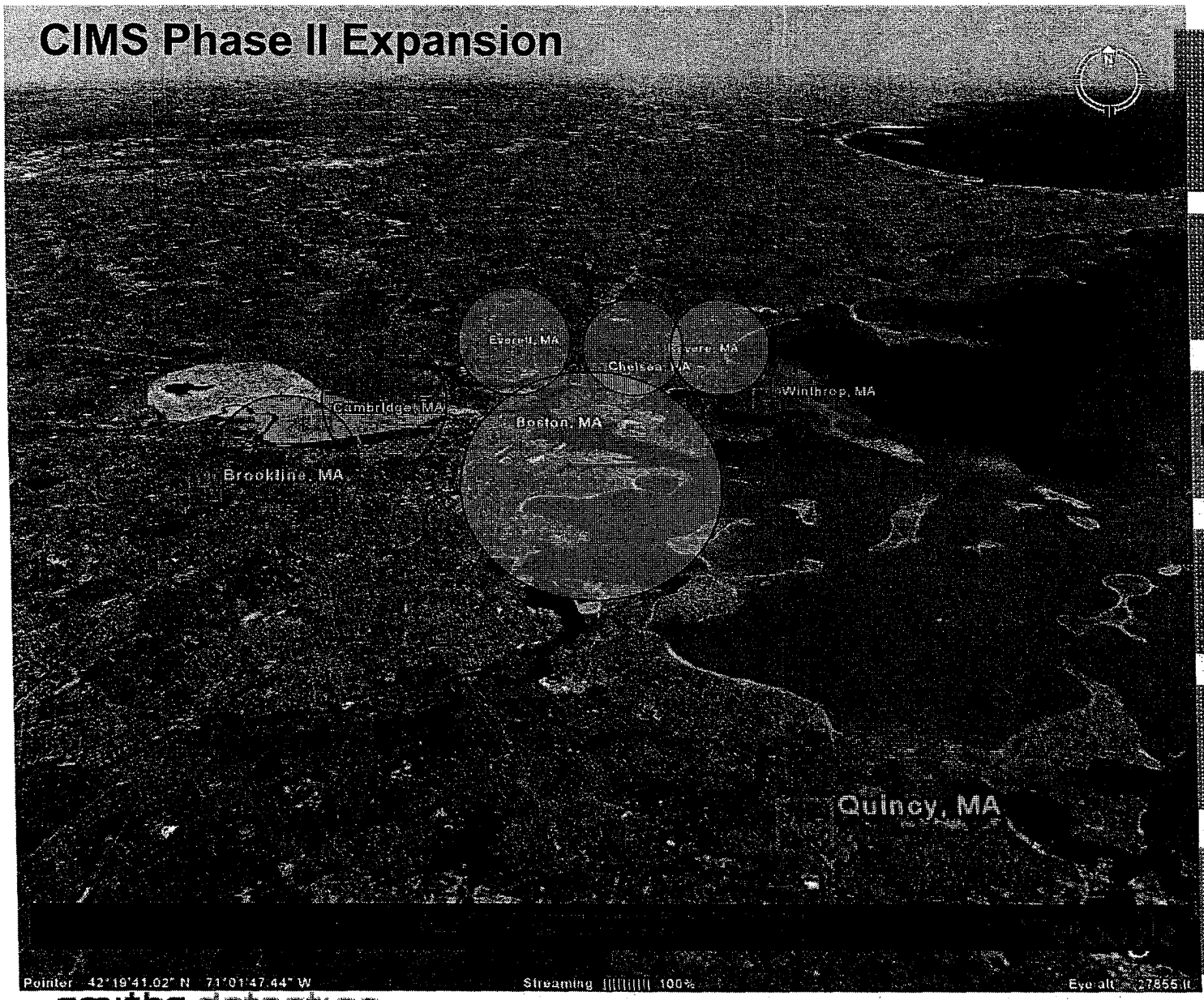
Issues	Solutions
1. NVR : Hardware reliability	Replaced all hardware with new units & monitoring – backup systems installed
2. Wireless: Interference	Replaced radios & frequency / channel monitoring
3. Multiple Networks and Interoperability	Re-architected the entire network – assigned full time network engineer
4. PM: Lack of day to day support	Patrick Hay assigned full time Program Manager, and new hires to increase support staff.
5. Service & Support: Issue resolution & response time	Support Provided by 24 Hour Toll Free Support # as well as direct contact to Program Manager Patrick Hay – response time improved.
6. Long range cameras reliability	Replaced hardware

Past Performance Background

- Headquarters in Newport, Rhode Island
- Manufacturer of IP video management systems since 1999
- Developing & deploying surveillance solutions for mission critical homeland security and military security applications
- High bandwidth fiber & wireless network design experience
- Interoperable communications, allowing multiple users at multiple locations to share real-time data

smiths detection

CIMS Phase II Expansion



Base 65
65 Cameras & Wireless Backbone

Option 1
Priority Group 2
34 Cameras

Option 2
Priority Group 3
36 Cameras

Option 3
Boston 30
30 Cameras

Option 4
Additional Training

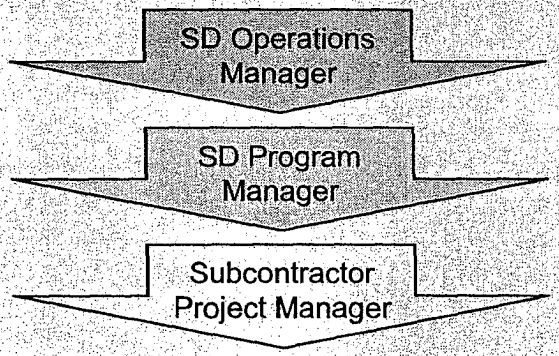
Option 5
WLAN Reduncy

smiths detection

Planned Performance

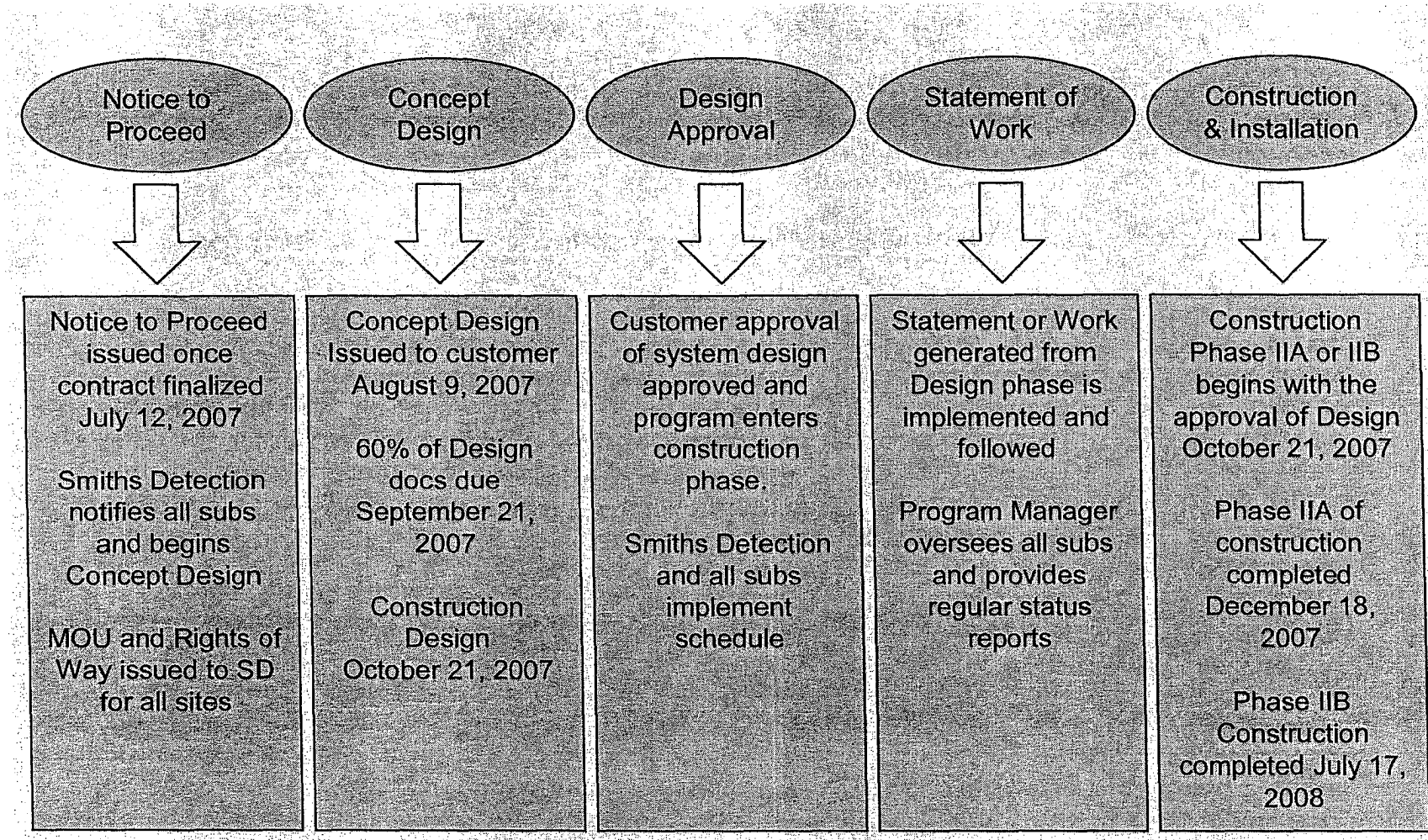
Program Management:

- Experienced Program Manager
- Smiths Detection Boston Office
- Management Top Down



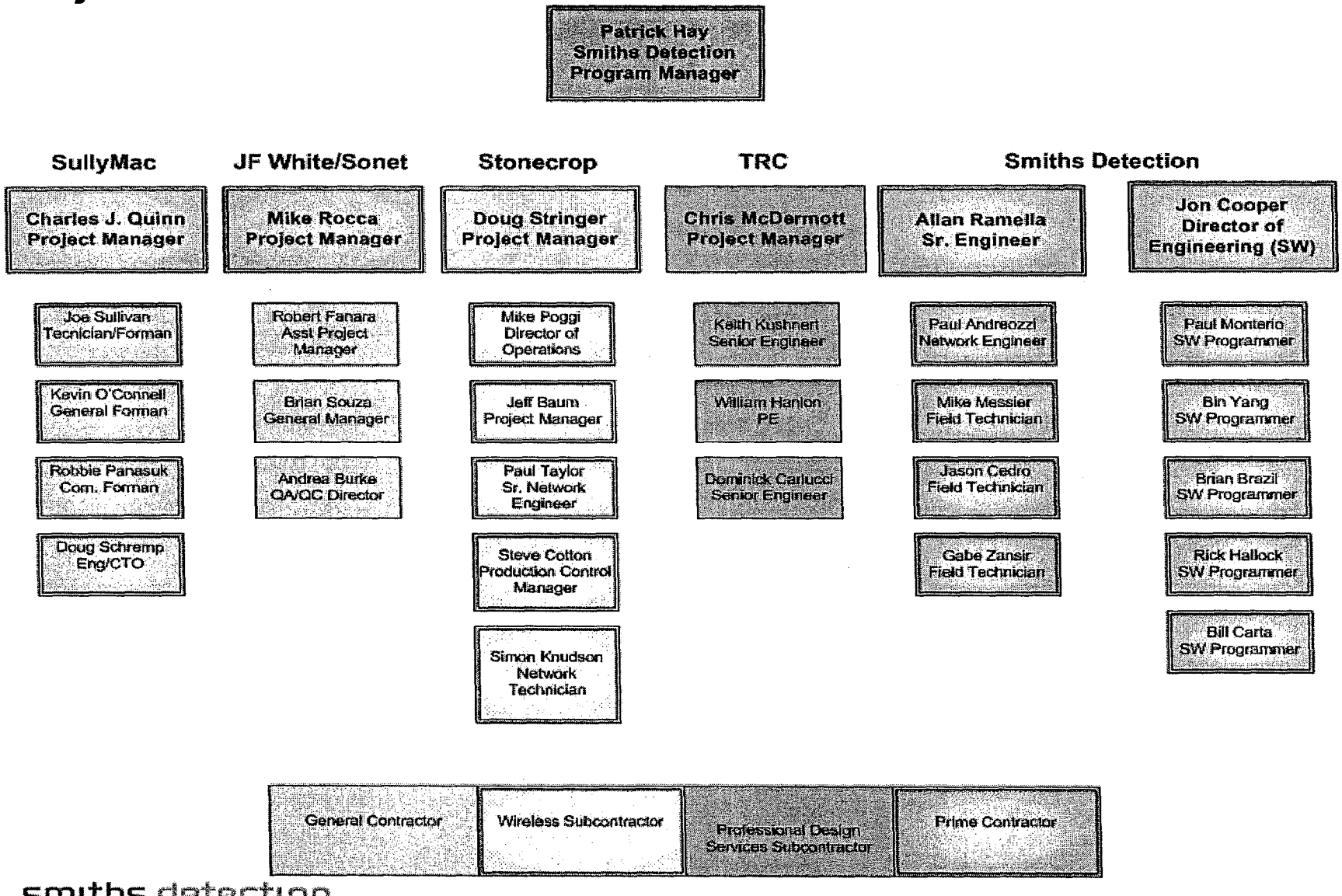
- Weekly Status and Program Reviews w/ all subcontractors
- Program Status updates to Customer and Supervisors

Proposed Work Plan



smiths detection

Project Team



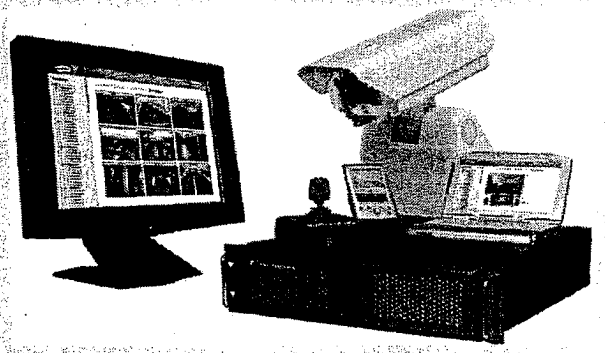
smiths detection

FirstView Software

- Web Based
- Software Engineering
- Software Team
- No Client Software pricing
- Interoperability
- Scalability
- How we develop
- Custom programming
- Milestone deployment

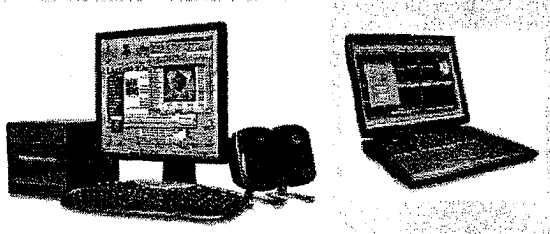
System Engineering

- HARDWARE SOFTWARE NETWORK
  - combined system
  - integrate and be integrated
- SCALABLE SOLUTION
  - add hardware, increase software functionality, distribute widely
- SUPPORT MULTIPLE DEVICES
  - camera protocols, sensors
- RELIABLE AND SECURE
  - quick to start, easy to use
  - authenticated, and encrypted



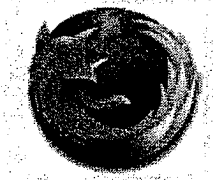
FirstView System

- **COTS PC HARDWARE**
  - Laptop, Shuttle, 2U rack mount systems
  - Video For Windows Capture Cards
  - OS Windows XP Pro (Linux)



- **JAVA Based Application Software**
  - J2EE Web Server, Resin
  - JDBC SQL DB
  - Native Video Sub System

- **Client Web Browser**
  - No Special Client Software



- **IP Enabled Networks**
  - Any topology: Hardwired, Wireless, Internet, Intranet, LAN
  - Any transport: Fiber, Ethernet, Satellite, RF