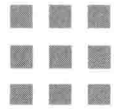
DIGITAL VIDEO SURVEILLANCE AND SECURITY

Anthony C. Caputo

B H



Digital Video Surveillance and Security

Butterworth-Heinemann is an imprint of Elsevier
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA
The Boulevard, Langford Lane, Kidlington, Oxford, OX5 1GB, UK

Notices
Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of product liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data
Application submitted

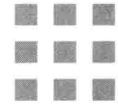
British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

ISBN: 978-1-85617-747-4

For information on all Butterworth–Heinemann publications
visit our Web site at www.elsevierdirect.com

Printed in the United States of America

10 11 12 13 10 9 8 7 6 5 4 3 2 1



Digital Video Surveillance and Security

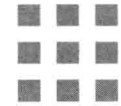
Anthony C. Caputo

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Butterworth-Heinemann is an imprint of Elsevier

This book is dedicated to my family and they all know who they are.



Preface

One could say that my career in technology has followed the convergence of our digital world. I've been working with digital video, with multimedia, since the mid-1990s. My first experience with networking communications was an experiment in 1989 with a pre-press company who wished to test a new method of delivering digital desktop publishing pages over a 2400-baud modem.

My extensive experience in digital video resolution and compression (codecs), bandwidth, and streaming within a video editing environment and my years in a multitude of networking technologies including writing the *Build Your Own Server* book and working in streaming media for Warner Bros., BMG Music, and commercial training applications made it easy to understand digital video surveillance. The security aspect was a natural transition from my days as a system analyst, when everything was about business process improvement.

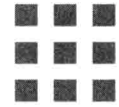
In early 2006, I joined the IBM Project Management Office for the City of Chicago's Operation Virtual Shield (OVS), a city-wide homeland security initiative that linked a multitude of cameras through the downtown Chicago area. My history in digital video, and networking technologies and as an author and writer, coupled with my experience as a certified Project Management Institute (PMI) Project Management Professional (PMP) and instructor, made me a valuable addition to the team. My initial responsibility was to write the procedure manuals for the system. As many technical writers experience when working on projects with the complexity of something such as OVS, there are very few individuals who know everything about all aspects of the system and those people are usually too busy to sit down on a regular basis to assist in the documentation of how the system works. Bits and pieces can be accumulated from various project managers, architects, designers, implementers, contractors, etc., so in the end I went out into the field to observe and record.

Sometimes figuring out how something is supposed to work and then fixing it is the only way to find out how it *really* works, so you can accurately document it. I stuck my nose and knowledge in too many places and wasn't allowed to leave the field again.

This book is the accumulation of years of hands-on experience in the field, and I believe it severs the ties that video surveillance has had for decades with closed-circuit television (CCTV). The world of analog television has also jumped into the digital age, thanks to the convergence of digital entertainment and communications, and video surveillance has jumped along with it.

Digital Video Surveillance and Security explains the concepts that are becoming the new standards in video security, both theoretically and from the field where the only days your hands aren't dirty from handling the real tools and equipment are the days when you're wearing gloves to protect your hands from the subzero temperatures.

Anthony C. Caputo
2009



Acknowledgments

Special thanks to everyone at IBM who gave me the opportunity to thrive: Roger Rehayem, James Sara, Timothy Herlihy, Jeffrey Menken, Dave Bisset, Ted Gary, Jim Lautenbach, Jodi Samsa, and Ladislao Delgado. Grand thanks and appreciation for suggestions, contributions, and comments: Dave Bisset, George Shapkarov, Jimmy Jimenez, Jeffrey Menken, Roger Rehayem, Terry Hennessy, Tim Roudebush, Mike Intag, Murali Repakula, Sivakumar Kailias, Pramod Akkarachittor, Joey Gerodias, and Michael Lane. Special thanks to my friends at MPEA for their help and support: Vince Gavin, Ellen Barry, Rich Piotrowski, and Tony Clark. Special thanks to my friends at the City of Chicago's 911 Center, Office of Emergency Management and Communications (OEMC) for their help and support: Aric Roush, and Joe Zito. And also thanks to: Gina Fritts, Brandon Ballschmeide, Donny Rutkowski, Rob Fleenor, Roger Martinez, Neil Salkind, Ed Guy, Pam Chester, Nancy Hoffmann, and Megan Berry.

About the Author

Anthony C. Caputo is currently working for IBM Global Technology Services on the Digital Video Surveillance Homeland Security Projects for the City of Chicago, Chicago Housing Authority, and the Metropolitan Pier and Expo Authority (MPEA). He has written articles, business plans, and books about the business benefits of technology for 22 years, including McGraw-Hill's *Build Your Own Server,* and has presented at conferences on the importance of a network security plan when introducing the Internet into any organization. He has 10 years of experience as a successful entrepreneur in both the entertainment and technology arena and has helped build five companies (three in technology) within the past 15 years. He's a certified and subject matter expert in a number of technology disciplines including project management with PMI (PMP), networking technologies and architecture, Genetec Omnicast Digital Video Surveillance software, Firetide Mesh Network Engineer, object-oriented analysis and design for business process improvement, and a Microsoft Certified Professional. He holds a Certification as an IBM e-business Solution Advisor, helping IBM write the exam for e-business advisor certification.

Contents

1

Introduction to Digital Video Security

Introduction

Visual surveillance began in the late nineteenth century to assist prison officials in the discovery of escape methods. It wasn't until the mid-twentieth century that surveillance expanded to include the security of property and people. The astronomical cost of these first security camera systems, based on traditional silver-based photographic cameras and film, limited their use to government buildings, banks, and casinos. If questionable activity was discovered, the monitoring security firm would develop the films in a secure, private darkroom laboratory to analyze at a later date. Live television was occasionally used during special events to monitor a crowd, but law enforcement was usually limited to the television studio to view the multiple cameras.

The theory behind visual surveillance was founded on the same four key factors that are still prevalent today. These are

1. Deterrence
2. Efficiency
3. Capable guardian
4. Detection

Deterrence

If potential criminals are aware of the possibility of being watched and recorded, they may determine that the risk of detection far outweighs the benefits. Visual surveillance as a deterrent is used from casinos to retail settings to public transportation. Countries all over the world use video surveillance, focusing its use mostly on public transportation (planes, trains, and autos) and select public areas. Based on an Urban Eye study (www.urbaneye.net), 86% of these international installations are for the prevention and detection of theft, and 39% also serve as a deterrent of violent crime. The amount of crime prevented by using video surveillance is based on the environment and whether the system is solely passive, active, or both. A passive system uses video recordings after an incident to help solve a crime. An active system is monitored by security personnel who are dispatched at a moment's notice. Historically, the most effective crime prevention video surveillance systems do more than record crime in the

background. One dramatic example is Chicago's Farragut High School, a public school notorious for its major acts of violence, locker thefts, and vandalism, all of which nearly disappeared within a year after the installation of a closed circuit television (CCTV) surveillance system. Many American cities have likewise seen a reduction in crime due to the addition of a video surveillance implementation and strategy.

In a recent UK Home Office Research Study on the effectiveness of video surveillance as a crime deterrent, 46 surveys were done within public areas and public housing in the United States and the United Kingdom. Of the 46 studies, only 22 had enough valid data to be deemed acceptable for publication. All 22 published surveys showed significant reduction (as much as 50%) in burglaries, vehicle theft, and violent crimes (see detailed report at www.homeoffice.gov.uk). However, it's rather difficult to analyze data on the effectiveness of video surveillance systems due to the many variables in the complexity of the areas of coverage and general displacement. For example, the decrease of crime within an area monitored by video surveillance cameras may have forced criminals to move to a different location, thus displacing the violent crimes. Enclosed areas of coverage – such as parking garages and lots, buildings, and campuses – have better success with video surveillance than large outdoor areas as long as there's a clear presence of a "capable guardian," which can be increased police or security guards or the electronic eyes of security cameras.

Efficiency

Reviewing video surveillance footage at the same time as watching live surveillance provides additional information about a situation, allowing users to make better decisions about deploying the right kinds and numbers of resources. Depending on the number of security cameras and their location, this simultaneous viewing of live and archived video can confirm a sleight of hand or any illegal activity before a patron, customer, or suspect is approached by a security force. In 2007, the Dallas, Texas, Police Department used video footage from 559 incidents to assist in 159 arrests. Their experience indicated that a single police officer monitoring live and archived video can cover far more area than a field officer, including usable image captures of license plates from 300 yards away.

Capable Guardian

In the article "Social Change and Crime Rate Trends: A Routine Activity Approach" by Lawrence Cohen and Marcus Felson (*American Sociological Review*), the authors suggest that crime prevention includes the presence of a "capable" supervising guardian. That guardian doesn't have to be present, just watching. Today, the guardian doesn't even have to be watching, just archiving using smarter technology. Current video surveillance includes sophisticated video analytics software with the capability of monitoring areas for programmable situations (e.g., bookmark all red automobiles) such as abandoned cars or backpacks, circling vehicles, or even specific license plates. Video analytics can upgrade an originally passive security system into an active one. This introduces the

capable guardian by giving the passive surveillance system a "brain" and allowing it to be more responsive to potential criminal activity.

Detection

Detection is the higher profile success factor, providing tangible evidence that video surveillance works. Britain is well known for its video surveillance system, providing law enforcement with the ability to follow anyone throughout the city of London through the use of over 200,000 cameras (with over 4 million cameras throughout the country). This system helped locate four London-born terrorists including the well-publicized CCTV images of suicide bomber Hasib Hussain. Likewise, the arrests of Jon Venables and Robert Thompson in the high-profile British murder case of James Bulger were directly linked to images reviewed on the surveillance system. Furthermore, Scotland Yard convicted 500 criminals using their CCTV database that included 3 years of data on 7000 offenders.

Closed Circuit Television

CCTV, which uses traditional radio frequency (RF) technology, rather than photographic technology, was introduced in the 1980s and provided a more cost-effective and real-time method of video surveillance.

Fake Cameras and the "False Sense of Security" Liability

There are many options in video surveillance, all of which feed the desire to take advantage of the deterrent factor. There are a number of companies marketing fake video surveillance cameras, which in the short run may initially help deter criminal activity, but even a fake camera, although a deterrent to criminal activity, implies "security." People walking through the loading docks of a store may believe they're safe because they see cameras and assume a security force is watching. If a criminal incident happens and the cameras are fake, that false sense of security may provide the basis for a winning lawsuit in today's courts. Even though the criminal broke the law and/or trespassed on private property, a court may fault a company for installing fake security cameras. This could be considered breach of contract, for knowingly stating that there was security when there wasn't; negligence, for lulling the employee with a false sense of security; or failure to heed police recommendation if an incident happened in the same area in the past. Ultimately, fake cameras could cost more in legal fees and settlements than installation of true video surveillance. Based on the Video Surveillance Guide Web site (www.video-surveillance-guide.com), once cameras are identified as fake they have been known to increase criminal activity, sometimes with devastating consequences.

Today's concept of video surveillance has its roots in the analog world of television. The framework of CCTV is a simple one, using the same analog signal you'd receive from your old pre-digital television. A single camera monitors one place and sends it to a CRT television monitor at another place using a coaxial cable. Usually the system has a single command center where security personnel watch black-and-white and/or color monitors of various cameras. Multiplexing technology provided the ability to watch more than one camera on a single monitor, or automate a cycling of various camera feeds on a single monitor to expand the area of coverage. While it's true that many security professionals and companies still use CCTV and the concept of a centralized "command center," not everyone has the space, money, and/or resources for such a system. The idea of wiring a house, office, building, or campus with coax cables from every camera to a control unit and then to each CRT monitor is costly, time-consuming, and thanks to internetworking technologies, unnecessary.

Figure 1-1 depicts an example of a CCTV installation that monitors select areas of coverage. The first installation was designed and developed for the separate parking facility. This implementation included several fixed position cameras on each floor of the parking garage, stairwells, and exits, all connected directly to a primary control unit (PCU) for management of each video stream. The PCU is a simple device for managing the input and output of video feeds through the coax cables. Ancillary utilities and devices can provide simple integration of some alarms, but this technology has limited capabilities and a complex integration process.

A single monitor in the parking garage management office was connected to the output for monitoring cameras. The PCU offered shuffling of each camera feed and select intervals and a keyboard to input the call number for each camera, or the ability to scroll through each camera one by one.

Several years later the campus was expanded; unfortunately the previous CCTV installation wasn't designed to extend the system into other buildings. An underground site survey uncovered various fiber, Ethernet, and power connectivity, but the conduit was either full or damaged over time. Feeding new runs of coax required trenching and/or boring to replace poor conduit runs between said buildings, thus the plan to run coax cables (for video) between the parking facility and the main building was abandoned due to cost. Another isolated CCTV system was designed and developed within the main building. These cameras were installed inside loading docks, exits and entrances, main entrances, and service corridors. A new model camera was introduced into this system that required more connectivity than coax cables for video. Many pan-tilt-zoom (PTZ) cameras were installed, requiring separate wiring interconnectivity with the new PCU for camera controls using a proprietary protocol.

In addition to this phase of the expansion, a primary command center was built to house a new security office with a CCTV control console for several CRT monitors to view the cameras and a new model keyboard with a built-in joystick to access and control the new PTZ cameras.

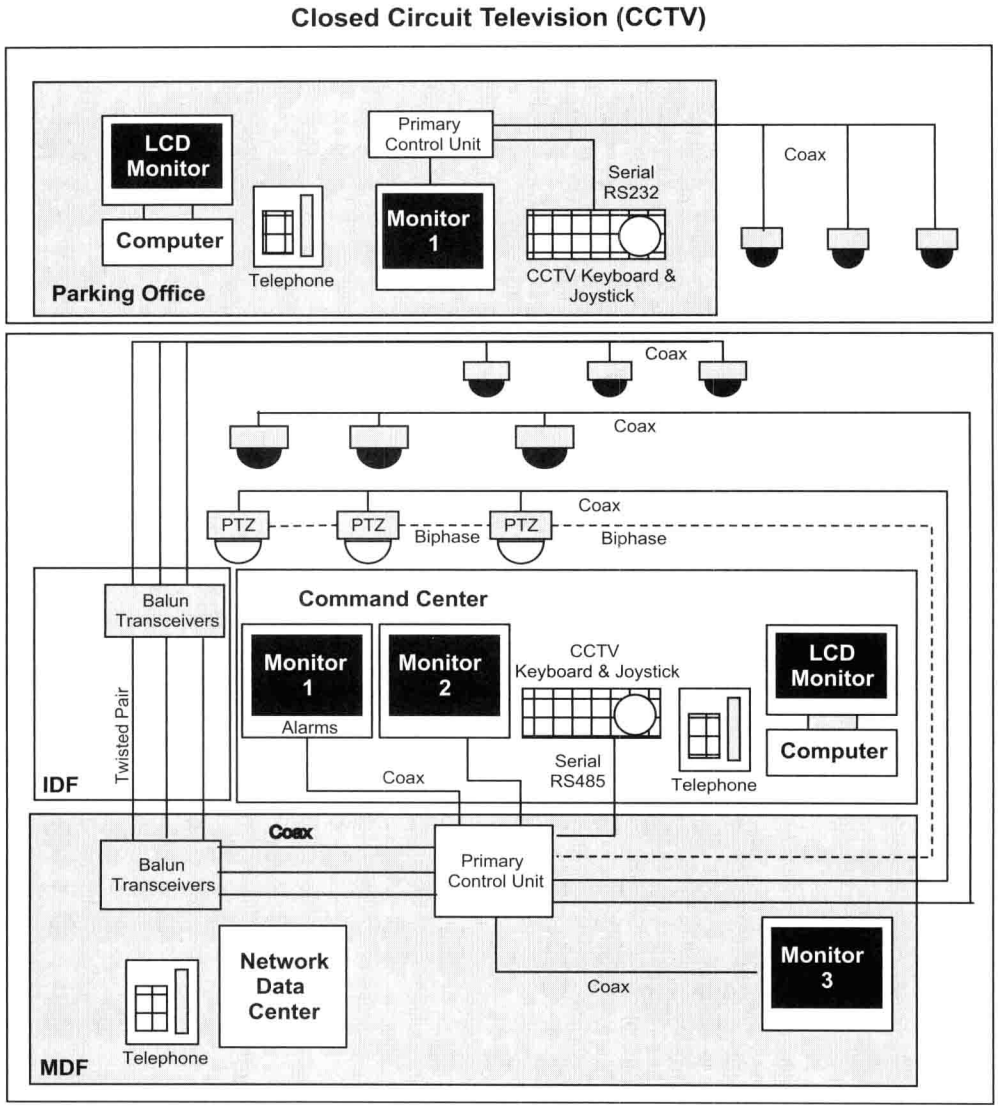


FIGURE 1-1 A typical CCTV topology.

The main building didn't have any existing conduit or spare conduit pathways to run coax throughout it and into the new buildings on campus. Video Balun transceivers were used to transfer the coax video signal to existing telephone twisted-pair wires between locations, as each building was interconnected to each telephone interim distribution facility (IDF), or a secured closet with twisted-pair terminals for the telephones and a network switch for the computers. The plain old telephone service (POTS) lines were linked into each IDF, the main distribution facility (MDF), the command center,