

**com**<sup>TM</sup>  
**sur**  
the missing piece of CCTV

# THE FOOTAGE WHISPERER

# "SEE WHAT THE CAMERA SAW"

GET THE BOOK



100+ TOPICS - AIRPORTS TO ZOOS

GAUTAM D. GORADIA



UTILITY VALUE OF  
COM-SUR™ FOR  
THE TELECOM SECTOR

WELCOME



AUDIT HOURS OF FOOTAGE IN MINUTES  
FIND OUT HOW COM-SUR, THE BEST  
'MOUSETRAP' WILL HELP

"Seeing is believing - See what the camera saw"

CCTV and other forms of video surveillance are common in the telecom sector, but footage is often only reviewed reactively. Our company realized this problem early-on and has developed the world's only CCTV video footage auditing software that encourages daily auditing (hours in minutes) of CCTV footage, filling the gap for a complete "workflow". The software works with existing cameras and VMS, regardless of type/brand, and provides a standardized approach for intelligent incident reporting. Our software also offers exceptional investigative capabilities.

'COM-SUR' – THE WORLD'S ONLY  
CCTV/SURVEILLANCE VIDEO FOOTAGE  
AUDITING, SMART BACKUP, AND  
STANDARDIZED INTELLIGENT INCIDENT  
REPORTING SOFTWARE – THE MISSING PIECE  
OF CCTV/SURVEILLANCE VIDEO

COM-SUR is the world's only CCTV/surveillance video footage auditing, smart backup, and standardized intelligent incident reporting software that serves as a complete workflow and force multiplier. It helps audit 24 hours of footage in minutes, reduces data size, creates standardized intelligent reports, and delivers business intelligence. COM-SUR helps unlock hidden information in CCTV/surveillance video footage and enables people to gain actionable intelligence, improve homeland security, prevent crime and losses, identify and mitigate threats and hazards, and improve operational efficiency. It empowers people to gain new jobs as CCTV/surveillance video footage auditors and start new businesses of auditing video footage. Like MS Office, COM-SUR is an enabler that makes it easy to work with CCTV and other surveillance cameras in a standardized way, leading to better decision-making. It also offers exceptional investigative capabilities.

HOW COM-SUR SMARTLY REDUCES 'VIDEO'  
STORAGE SIZE

COM-SUR employs an innovative approach to

smartly reduce the amount of video to be audited and consequently the storage size of videos. Regardless of the video's frame rate, COM-SUR captures a single screenshot of the consolidated 'moment' of 'that' one second, when the I, P, and B frames come together. This method significantly reduces data size without sacrificing vital information. It goes without saying that when multiple cameras are displayed in a grid view, say 4x4, the storage size is further reduced since all the cameras are captured as a single image. Since no suggestion is being made to replace the actual video with screenshots, COM-SUR acts as a wonderful supportive technology both to audit (review) just 86400 frames representing 24 hours and reducing the data size at the same time.

#### TELECOM SECTOR CHALLENGES

##### 1. Theft and vandalism:

Since telecom towers contain valuable items such as copper wire, high performance batteries, diesel fuel, etc., these are lucrative targets for thieves and vandals. Especially, theft or vandalism of copper wire is a major cause of concern for telecom companies worldwide. Besides causing network downtime, theft or vandalism of copper wire causes extensive damage to a telecom tower, thereby amounting to considerable losses for telecom companies for replacement or repair of the same.

##### 2. Unauthorized access:

Unauthorized access to telecom facilities can compromise the security and privacy of network infrastructure. This includes physical breaches of data centers, control rooms, and equipment sites, as well as unauthorized access to sensitive information.

##### 3. Compliance issues:

The telecom sector operates within a regulatory framework that requires compliance with standards and guidelines related to data protection, privacy, network security, and emergency preparedness. Ensuring compliance with these regulations can be challenging, especially as technology and threats continue to evolve.

##### 4. Insider threats:

Telecom companies have to deal with insider threats from disgruntled employees or even unwitting staff who fail to follow proper security and safety measures.

##### 5. Humongous growth of surveillance video:

The exponential growth of surveillance cameras has resulted in an unprecedented surge in surveillance video. Effectively managing this data has become a daunting challenge due to the massive storage capacity required, especially considering the prolonged retention periods necessary for security, incident investigation, or legal purposes. Furthermore, the prevalence of high-resolution video with increasing megapixels compounds the storage demands, making efficient data management an urgent priority for organizations grappling with the immense volume of surveillance footage.

#### COVID-19 PANDEMIC

The pandemic severely impacted the telecom sector worldwide. Owing to government restrictions/ lockdowns, people had to work from home thereby utilising huge amounts of network data. This led to several telecom companies reporting large spikes in network usage. Also, several telecom infrastructure

projects were delayed. Guidelines were issued to prevent the spread of COVID-19, but outbreaks still occurred.

### USE OF VIDEO SURVEILLANCE AT TELECOM COMPANIES

Most telecom companies use video surveillance to monitor the following areas:

- Entry and exit areas of a telecom site
- Relevant areas of the offices
- Telecom towers
- Fuel tank area
- Power generator area
- Perimeter
- Other critical areas that house expensive equipment and material

Telecom companies generally record CCTV video footage from time to time of 'motion events' detected by the motion sensing cameras around the telecom towers. This footage is sent to their control room for further analysis. Further, the concerned stakeholders at telecom companies generally need to review and analyse recorded CCTV video footage from time to time for investigating incidents and/or accidents, and other issues in order to corroborate evidence as well as assisting Police/other Law Enforcement Agencies.

### DRONES

Since it is not feasible to install CCTV cameras in telecom towers at remote locations, drones are being used for inspections of tower structures

and other equipment. Further, this considerably reduces the need for technicians to climb telecom towers in order to perform routine inspections, which eventually lessens the likelihood of a workplace injury/accident.

### LIVE MONITORING – CHALLENGES

Several telecom companies have a dedicated control room with operators, set up for live monitoring of CCTV and other cameras such as drones. However, live monitoring comes with its own set of challenges of video blindness, poor attention span, boredom, operator bias, false alerts, and so on.

Moreover, these cameras continuously capture and record humungous amounts of video data. It therefore becomes a daunting task for the operators to review and analyse this data whenever the need arises. Thus, it may be noted that benefits from video surveillance systems can accrue only when they are used optimally, suggestions for which are enumerated further on, in this document.

### COMPLIANCE - GENERAL

Conformity or compliance in any organization means adherence to laws and/or rules and regulations, various standards, as well as data storage and security requirements as laid down by government bodies, governing bodies of the respective industry, or the management of the organization. When an organization complies with the requirements mandated by government and/or governing bodies, then it is termed as 'regulatory compliance' which enables the organization to run in a legal and safe manner.

### COMPLIANCE - AUDITS

Several organizations carry out compliance audits on a regular basis to avoid the potential consequences of non-compliance. A compliance audit examines how well an organization adheres to compliance requirements. Some organizations use video surveillance to monitor compliance issues and audit recorded CCTV video footage from time to time for investigating and preventing compliance issues. Auditing CCTV provides actionable insights on the level of compliance within the organization.

### AUTOMATED SOFTWARE – WHY THEY WILL NOT WORK IN ISOLATION

In the wake of the Christchurch shooting incident, several high-profile places of worship considered deploying gun detection technology. However, there are concerns about its efficacy, since it may not be able to detect all types of weapons, or the perpetrator could still create damage before being detected. Similarly, automated systems like video analytics, AI/ML can only detect what they have been programmed for. What about the rest? Again, these technologies are prone to triggering huge amounts of false alarms. Also, since the permutation combinations of exceptions can be vast and varied, it becomes almost impossible to automate every kind of exception. Facial recognition technology also raises ethical and privacy concerns, and has been found to produce inaccurate results, especially for certain ethnic groups. Therefore, experts suggest that while automated technologies will continue to grow, human intervention and intelligence will still be necessary to verify alerts and ensure their efficacy.

### “CCTV AND OTHER FORMS OF VIDEO SURVEILLANCE ARE NOT ENOUGH – WE MAKE IT WORK FOR YOU”

While it is not being suggested that optimal usage of video surveillance can cure all issues, several issues of the following kind can be addressed by doing just a little 'more' with respect to making the optimal use of video surveillance systems:

- Recces/suspicious movements /activities
- Insider job/security lapses
- Unauthorized/unlawful activities/visitors
- Accidents/Causes of potential accidents
- Potential causes of fire
- Vandalism
- Housekeeping issues
- Compliance issues
- Loss/theft
- Unclaimed/unattended objects
- Human rights violations
- Staff negligence
- Inattentive staff (e.g. guard sleeping)
- Unruly staff
- Issues with female staff

- Health and safety issues
- Cameras/recorder malfunctions

So, what is the 'more' that needs to be done?

### 1) AUDIT CCTV AND OTHER SURVEILLANCE VIDEO FOOTAGE DAILY AS A STANDARD OPERATING PROCEDURE

'Auditing' means 'seeing' what the cameras 'saw'. Auditing of CCTV and other surveillance video footage should be done daily (continuous investigation) to identify potential issues and threats. Auditing is a dedicated and systematic process that helps address challenges related to live monitoring and alert-based systems. Auditing helps in evaluating analyzing incidents to improve existing policies, procedures, and processes. Concerned personnel should be trained to become video footage auditors, and the audit teams should be rotated to avoid complacency/collusion. Daily auditing of CCTV and other surveillance video footage can also help in adhering to the principles of Kaizen and TQM for business improvement.

### 2) DOCUMENT AUDIT FINDINGS/INCIDENTS

Audit findings/incidents should be documented in a standardized template to find the root cause to prevent future recurrences. Historical data of such findings/incidents can reveal patterns that can help take better informed corrective and preventive action. If the entire industry reports incidents in a standardized template, relevant authorities can derive business intelligence from the data and take action for the collective benefit of the telecom

sector.

### 3) ENSURE DISASTER RECOVERY OF CCTV AND OTHER SURVEILLANCE VIDEO FOOTAGE – LIKE A 'BLACKBOX'

CCTV and other surveillance video footage must be stored at multiple locations in order to ensure that even if the recorder/storage device is stolen, destroyed or tampered with the data is never lost. Further, any backed-up data must easily be searchable and retrievable; else, it is going to be a nightmare finding the relevant video.

### 4) DISPLAY DYNAMIC INFORMATION AT RELEVANT PLACES

Document and display details of information that is dynamic in nature in relevant areas. For example:

1. List of authorized staff.
2. List of authorized security personnel deployed at the telecom company.
3. List of habitual offenders/suspects likely to visit the telecom company's premises (a 'Watch out' list).

### 5) USE A POWERFUL NEW SIGNAGE

**"WE AUDIT CCTV VIDEO FOOTAGE EVERYDAY".**

One size, one color, one powerful message.  
Across the nation.

DE-CENTRALIZED SURVEILLANCE +  
CENTRALIZED SURVEILLANCE = OPTIMAL  
RESULTS

Organizations with multiple locations struggle with centralized video surveillance due to infrastructure cost, internet bandwidth, and operator limitations. De-centralized surveillance offers higher accountability at each location and better situational awareness, leading to more chances of discovering exceptions.

CONCLUSION

“You see, but you do not observe” is a quote by Sherlock Holmes in A Scandal in Bohemia (1891, written by Sir Arthur Conan Doyle). COM-SUR makes 'observation' far effortless and effectual leading to superior results.

"Cameras don't lie" - but how will you know unless you 'see' what the cameras 'saw'?  
Audit video - why suffer!

Get award-winning COM-SUR now. Don't wait for things to go wrong!

Finally, allow us to present three important mantras that change the landscape of video surveillance:

1. Auditing is fundamental – everything else is peripheral.
2. Cameras have lenses – humans have eyes.
3. Let's make cameras 'accountable'.