
com 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 BIOTECH FACILITIES

## 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 surveillance is common in biotech facilities world over, 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 VIDEO FOOTAGE AUDITING, SMART BACKUP, AND STANDARDIZED INTELLIGENT INCIDENT REPORTING SOFTWARE – THE MISSING PIECE OF CCTV

COM-SUR is the world's only CCTV 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 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 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 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.

## CHALLENGES FACED BY BIOTECH FACILITIES

1. Unauthorized access:

Biotech facilities house sensitive equipment, materials, and data. Unauthorized access to these areas can lead to theft, sabotage, or compromise of research integrity. Intruders may attempt to gain access to valuable equipment, sensitive information, or hazardous materials.

2. Theft and vandalism:

Biotech facilities may be targeted for theft of biological materials including genetically modified organisms (GMO), infectious agents, biohazardous substances, valuable equipment, materials, or intellectual property. Vandalism or sabotage can disrupt ongoing experiments, damage equipment, or compromise research outcomes.

3. Bioterrorism:

Biotech facilities face the risk of accidental releases or exposure. Contamination incidents can pose risks to personnel, the environment, and public health, making biotech facilities potential targets for terrorists seeking to cause harm on a large scale.

4. Dual-Use research concerns:

Some biotechnological research may have dual-use applications, meaning the same knowledge and technologies developed for beneficial purposes could potentially be misused for harmful purposes.

5. Laboratory safety incidents:

Accidents and safety incidents such as fires, chemical spills, or equipment malfunctions can occur within biotech facilities. These incidents can result in injuries, property damage, or disruptions to research activities.

6. Intellectual property protection:

Biotech facilities often conduct innovative research and development, creating valuable intellectual property. Protecting intellectual property from theft or unauthorized disclosure is crucial to maintaining a competitive edge.

7. Data security:

Biotech facilities generate and store vast amounts of data, including experimental results, research findings, and confidential information. Safeguarding this data from unauthorized access, cyber-attacks, or data breaches is essential.

8. Compliance issues:

Biotech facilities must comply with various regulations and guidelines related to safety, security, and research ethics. Ensuring compliance with these requirements can be challenging and requires robust security

measures and protocols.

9. Occupational safety and health:

Biotech facilities need to maintain a safe and healthy work environment for their personnel. This includes managing hazardous substances, implementing safety protocols, providing appropriate personal protective equipment, and conducting regular safety training.

10. Insider threats:

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

11. 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 significantly impacted biotech facilities worldwide. There was a shift in research priorities towards COVID-19-related projects, including vaccine development and antiviral therapies. Non-COVID research faced disruptions, supply chain challenges, and delays, while remote work became a necessity, posing challenges for laboratory-based activities. Clinical trials were significantly affected, leading to enrolment delays and disruptions. However, the pandemic also fostered increased collaboration, rapid vaccine development, regulatory flexibility, and a heightened awareness of the critical role of biotechnology in global health crises. Guidelines were issued to prevent the spread of COVID-19, but outbreaks still occurred.

## USE OF VIDEO SURVEILLANCE AT BIOTECH FACILITIES

Most biotech facilities have video surveillance covering the following areas:

- Entry and exit points
- Experimentation areas
- Sample handling and preparation areas
- Cleanrooms
- Facilities where animals and plants are housed for research purposes
- Equipment rooms
- Server/IT rooms
- Storage areas
- Conference rooms and offices
- Common areas (lobbies, break rooms, cafeterias etc.)
- Restricted access areas
- Waste disposal areas

 

- Corridors
- Parking areas

Further, the concerned stakeholders at biotech facilities 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 assist Police/Law Enforcement Agencies.
Recorded video footage serves as a valuable resource for training purposes. It can be used to demonstrate proper laboratory procedures, safety protocols, and compliance with regulations to educate new personnel

## USE OF THERMAL CAMERAS

Biotech facilities utilize thermal cameras for various purposes due to their ability to detect and visualize heat signatures. Here are some common applications of thermal cameras in such settings:

1. Temperature monitoring:

Thermal cameras are used to monitor and maintain temperature-controlled environments, such as cold storage areas, incubators, or cleanrooms. They can quickly identify temperature fluctuations or anomalies, helping to prevent damage to sensitive samples, equipment malfunctions, or compromised experimental conditions.

2. Equipment and machinery inspection:

Thermal cameras are employed to inspect and monitor the performance of equipment, machinery, and electrical systems within biotech facilities. By detecting overheating components or abnormalities in heat distribution, potential malfunctions or hazards can be identified early, allowing for timely maintenance or repair.

3. Fire detection and prevention:

Thermal cameras are effective tools for early fire detection. They can identify abnormal heat patterns or hotspots, enabling quick response and fire prevention measures. When integrated with fire alarm systems, thermal cameras can trigger alerts and activate sprinklers or other fire suppression systems.

4. Energy efficiency and environmental monitoring:

Thermal cameras are utilized to assess energy efficiency within biotech facilities. By visualizing heat loss or identifying areas of excessive heat or cold, energy conservation measures can be implemented. Additionally, thermal cameras can help monitor environmental conditions, such as HVAC performance or insulation integrity.

5. Animal research:

In laboratory settings involving animal research, thermal cameras can be used to monitor animal behavior, body temperature, or detect signs of distress. This can aid researchers in observing physiological responses, assessing thermal comfort, or identifying potential health issues in animals under study.

6. Contamination control:

Thermal cameras are employed to monitor

cleanliness and contamination control measures in cleanrooms or sterile environments. By detecting temperature variations that may indicate leaks, infiltration, or improper air circulation, thermal cameras help maintain the integrity of controlled environments.

## USE OF CAMERAS IN BIOTECH FACILITIES BESIDES SURVEILLANCE

Besides surveillance, cameras in biotech facilities are used for various other purposes to support research, quality control, and operational efficiency as follows:

1. Microscopy and imaging systems:

High-resolution cameras are integrated into microscopy and imaging systems to capture detailed images of biological samples, cells, and tissues. These images are essential for research, diagnostics, and analysis.

2. Fluorescence imaging:

Fluorescence cameras are utilized to capture images of samples labeled with fluorescent markers. This is common in molecular biology and cell biology research, enabling the visualization of specific molecules and cellular structures.

3. Gel documentation:

Cameras are used to capture images of gels used in techniques like gel electrophoresis. Gel documentation systems facilitate the analysis of DNA, RNA, and proteins during experiments.

4. Automated cell culture monitoring:

Cameras are integrated into automated cell culture systems to monitor the growth, morphology, and health of cells in real-time. This technology aids in optimizing culture conditions and experimental outcomes.

5. In vivo (within a living organism) imaging:

In the field of biotechnology, cameras are employed for in vivo imaging to study biological processes within living organisms. This is particularly important in areas like drug development and disease research.

6. Time-lapse imaging:

Cameras are used for time-lapse imaging to capture sequential images of biological processes over time. This is valuable for observing dynamic cellular events and changes in experiments.

7. Automated liquid handling systems:

Cameras are integrated into automated liquid handling systems to facilitate precise dispensing and handling of liquids in laboratory workflows. The cameras aid in verifying proper execution of liquid handling protocols.

8. Quality assurance in manufacturing:

Cameras are used for quality control in biotech manufacturing processes. They can capture images of products, ensuring adherence to quality standards and identifying defects or irregularities.

9. Barcode scanning:

Cameras are employed for barcode scanning to track and manage samples, reagents, and other materials in biotech laboratories. This helps in maintaining accurate records and traceability.

10. Biometric access control:

Biometric cameras, such as those for facial recognition, may be used for secure access control in biotech facilities, enhancing security measures beyond traditional key cards or passwords.

11. Digital pathology:

High-resolution cameras are integrated into digital pathology systems for the digital capture and analysis of pathology slides. This aids in remote diagnostics, collaboration, and archiving of pathology data.

12. Automated colony counting:

Cameras are utilized in automated systems for colony counting in microbiology research. This speeds up the process of quantifying bacterial or cellular colonies on agar plates.

13. Live-cell imaging:

Cameras are employed for live-cell imaging, capturing real-time dynamics of cells and cellular processes. This is particularly important in studying cellular responses to stimuli or treatments.

## LIVE MONITORING – CHALLENGES

Some biotech facilities have a dedicated control room with operators, set up for live monitoring of CCTV cameras. 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 IS 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:

- Unauthorized/unlawful activities/visitors

- Tampering of equipment

- Violence and vandalism

- Unruly staff/visitors/outside workers /security guards

- Health and safety issues

- Compliance issues

- Recces/suspicious movements/activities

- Insider job/security lapses

- Accidents/Causes of potential accidents

- Loss/theft

- Intrusions, especially by animals

- Inattentive staff (e.g. guard sleeping)

- Unclaimed/unattended objects

- Issues with female staff or visitors

- Cameras/recorder malfunctions

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

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

'Auditing' means 'seeing' what the cameras 'saw'. Auditing of CCTV 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 CCTV video footage auditors, and the audit teams should be rotated to avoid complacency/collusion.
Daily auditing of CCTV 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 all biotech facilities report incidents in a standardized template, relevant authorities can derive business intelligence from the data and take action for the collective benefit of all biotech facilities.

## 3) ENSURE DISASTER RECOVERY OF CCTV VIDEO FOOTAGE – LIKE A 'BLACKBOX'.

CCTV video footage must be stored at multiple locations in order to ensure that even if the recorder 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 biotech facility.

3. List of potential suspects/miscreants likely to visit the premises of the biotech facility (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 CCTV - 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'.