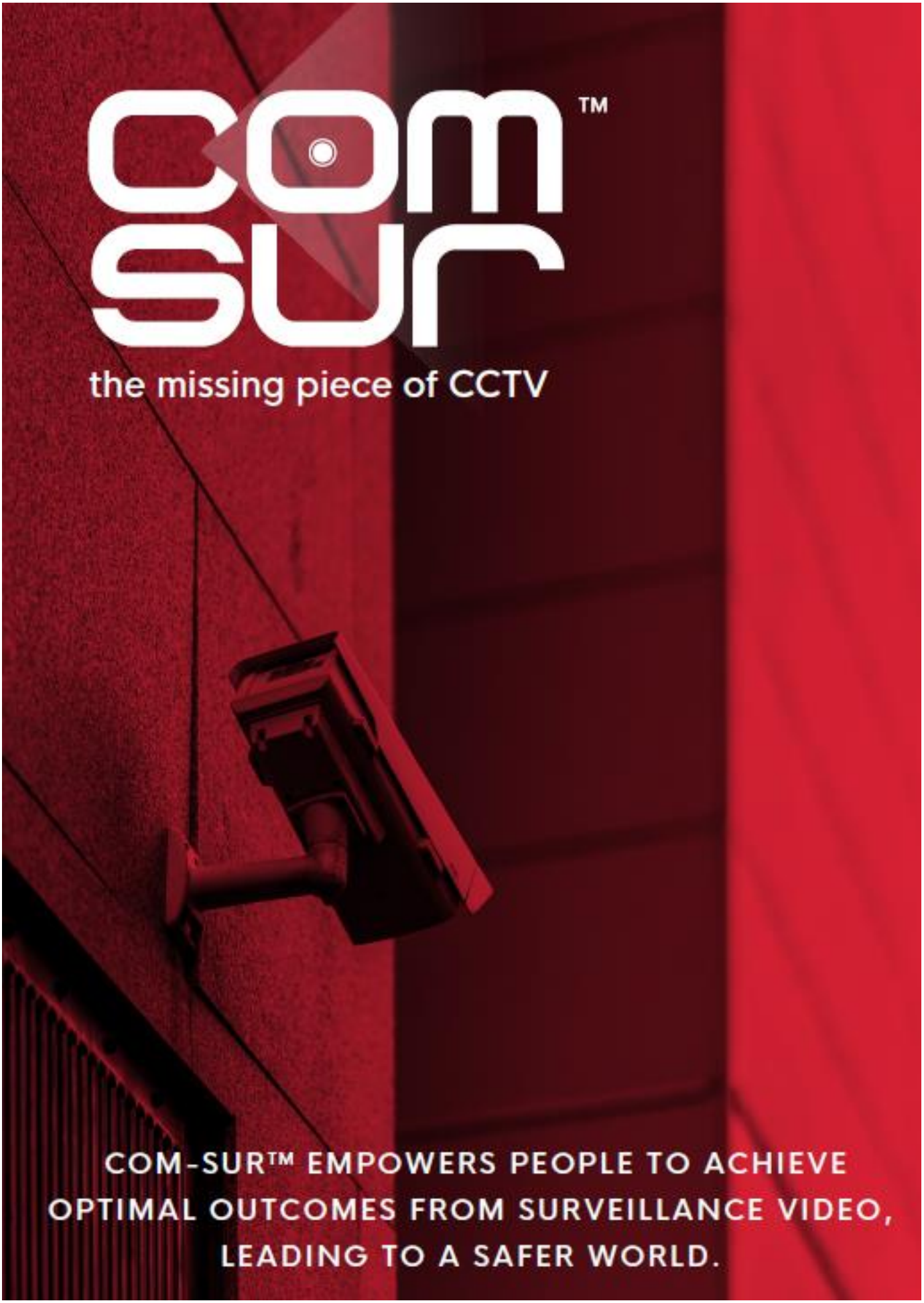
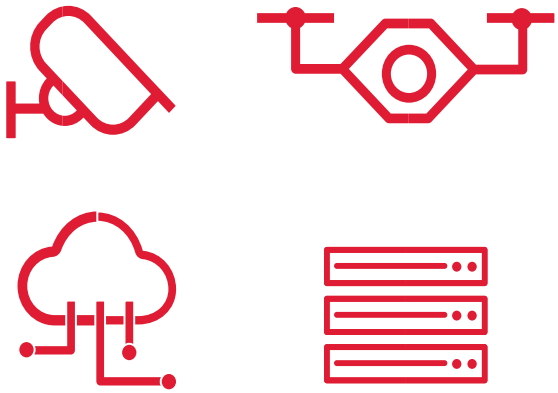

COM SUR™
the missing piece of CCTV
COM-SUR™ EMPOWERS PEOPLE TO ACHIEVE
OPTIMAL OUTCOMES FROM SURVEILLANCE VIDEO,
LEADING TO A SAFER WORLD.

COM-SUR™
the missing piece of CCTV

OVERVIEW

CCTV surveillance is now an integral part of the overall security apparatus across the world.

However, despite the increase in the number of cameras; crime, fraud, losses, process violations, health and safety issues, poor efficiency, wastage, traffic violations, etc., continue to occur; clearly indicating that CCTV by itself is not enough.



CCTV – DON'T LET VIDEO TURN INTO GARBAGE

CCTV is not enough. It must not be allowed to remain as 'fit and forget'.

That is why we built COM-SUR, the world's only CCTV video footage auditing, smart backup, and standardized intelligent reporting software; the three 'missing' pieces of CCTV.

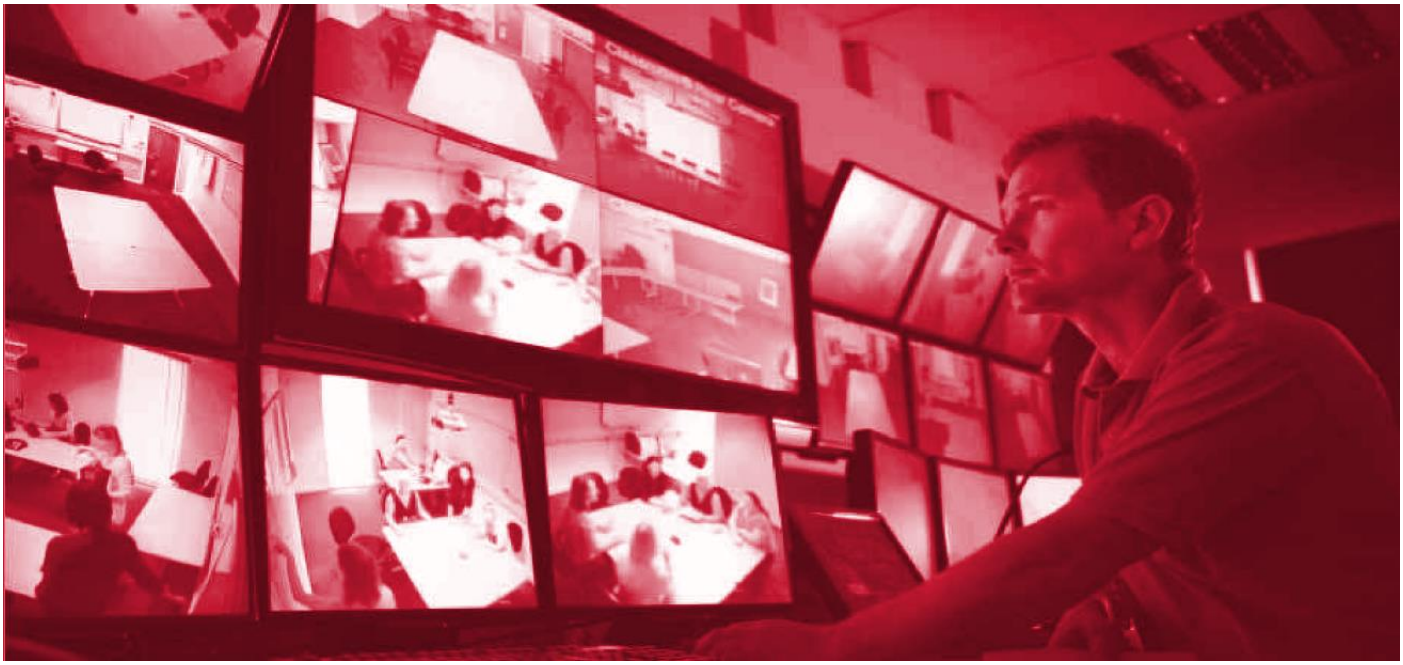
Just like Google was the missing piece of the internet, COM-SUR is the missing piece of CCTV. While COM-SUR helps every user of CCTV to achieve optimal outcomes; for the police, law enforcement agencies, and defense forces, it is an exceptional tool to efficiently work with videos, photos, and images.

Like MS Office, COM-SUR is a force multiplier that allows users to carry out several activities related to CCTV with ease, efficiency, and standardization.

COM-SUR works with existing cameras and VMS (agnostic of type/brand).

AUDIT CCTV VIDEO FOOTAGE – WHY SUFFER?

JOB CREATION



"Cameras never lie". But how will one know, unless one 'sees' what the camera 'saw'?

COM-SUR encourages all users of CCTV to audit their own CCTV video footage as a standard operating procedure. Regular auditing of CCTV footage by the public means that the Police/LEA have more 'eyes' working for them through crowdsourced surveillance. This enables the Police/LEA in identifying potential threats and dangerous situations before they occur.

Also, in the case of a crime, if a standardized incident report is delivered to the Police/LEA by the affected party in PowerPoint carrying the entire story (what, where, when, why, who, how, and the video clip), crime will get solved faster.

CCTV VIDEO FOOTAGE AUDITORS

It is our belief that this new profession is the need of the hour across the world, in order that millions of cameras which are currently in ‘sleep mode’ will ‘wake up’, leading to huge benefits of all kinds.

A CCTV video footage auditor can be an immediate occupation for retired personnel from the Police/ LEA.

SUPER RECOGNIZERS - SCOTLAND YARD

It may not be out of place to mention that the London Metropolitan Police formed a team of 'Super Recognizers', and put them to work to identify individuals whose faces are captured on CCTV. COM-SUR makes this activity very easy and efficient, including the analysis of micro-expressions and body language.

INTRODUCTION

NEW JOB OPPORTUNITIES – NEW BREED OF PROFESSIONALS – CCTV VIDEO FOOTAGE AUDITORS

The need to create a new breed of professionals called 'CCTV VIDEO FOOTAGE AUDITORS' emanates from the fact that the mere 'installation' of CCTV surveillance systems is not enough to enhance homeland security, detect and prevent crime, fraud, losses, process violations, wastage, traffic related issues etc.; and that some fundamental changes are needed to achieve valuable outcomes from CCTV surveillance systems, which should be:

a) Enhanced homeland security, crime, fraud, and loss prevention; and faster solving of crime.
b) Threat and hazard risk identification/mitigation, improvement of operational efficiency and processes, business continuity, root cause analysis, good manufacturing practices, and total quality management efforts.
c) Improvement of employee performance, customer satisfaction, and sales.
d) Huge reduction of data size and inexpensive remote storage.
e) Enhancement of compliance, processes, and health and safety issues.
f) Ease of investigation, forensics, debriefing, gaining situational awareness and understanding, and actionable intelligence.
h) Standardization of all activities related to CCTV surveillance.
i) Ease of sharing footage/reports with law enforcement agencies/other stakeholders.
j) Gaining business intelligence from historical data gathered from standardized reporting.
i) Immediate and regular corrective and preventive action, resulting in continuous improvement (think Kaizen); in areas that are also beyond crime. For example, agriculture, climate, forests, etc.

These fundamental changes suggest that 'CCTV video footage auditing' as a standard operating procedure, reporting in standardized templates, and retaining CCTV video footage data by 'relevance' (as opposed to retaining CCTV video footage data only by number of days) need to be added to the occupational standards for CCTV operators/supervisors, thereby adding more value to the job profile of a CCTV operator, as well as creating new job and business opportunities of 'CCTV video footage auditing services'.

The aim is also to introduce new methods to improve the efficacy of existing/new CCTV surveillance systems, as well as to introduce other methods and tools to ensure standardization of several activities carried out by all users of CCTV surveillance, including Law Enforcement Agencies (LEA), just as CCTNS aims to standardize activities related to crime and criminal tracking across India.

Finally, it is important to add that if all (even if a majority) of CCTV cameras are audited by users of CCTV systems, it will ensure that the 'hidden' information in the cameras will be 'unlocked', which in turn will offer several benefits, and who knows that someday, someone may just observe 'something' that could prevent the next terror attack. There is therefore lots

of merit in auditing CCTV video footage as a standard operating procedure to enhance the safety and security of a nation collectively. Moreover, continuous auditing as a standard operating procedure validates a notable feature of business improvement, which is that *"big results come from many small changes accumulated over time".* By extrapolating this feature to CCTV/video surveillance, it can be inferred that *continuous corrective and preventive action delivers optimal outcomes from CCTV over a period of time*.

There is a *need therefore for a fundamental shift*.

STATEMENT OF THE PROBLEM

It is a well-accepted fact that CCTV surveillance is now a part of the overall security apparatus across the world. However, while CCTV cameras are increasing in numbers; yet, crime, fraud, losses, process violations, traffic violations, wastage etc. continue to take place. Incidents over the past couple of years in Sri Lanka, New Zealand, Westminster, Manchester, London, Dhaka, Nice, Paris, Munich, Orlando, Turkey, Brussels, Pathankot, Mumbai had at least two things in common. There were cameras everywhere, and there were recces! While no serious crime takes place without adequate planning and a recce, even a 'simple' process violation like not wearing the appropriate gear at a pharma unit can cost the company huge penalties and warnings from US FDA, or such other bodies.

Fool-proof automatic systems that can detect the above exceptions (like recces or the example of a pharma unit) are yet to be developed; and because of the fact that the number and kind of exceptions *per se* are so varied in nature, it is highly unlikely that a fool-proof automatic system will ever be developed; or at least not for a very long time to come.

While authorities have been mandating the installation of CCTV surveillance systems all over the world, so far there has been no standardization of *'how'* users (including the Police/LEA themselves) should manage all this content, or how they should gain intelligence from the same. Also, there is no mention of how escalation of a finding should take place quickly and in a standardized format, in order that necessary action can be taken without wasting crucial time.

It may not be out of place to mention here that the United Kingdom, which perhaps took the lead in deploying CCTV systems during the early days, has started cutting down on budgets, as CCTV systems do not seem to be delivering the expected outcomes. This, however, may be an error of judgement; and the United Kingdom, and all other countries must consider what more can be done to achieve the expected outcomes instead of cutting down on budgets.

END OF THE CCTV ERA?

http://www.bbc.com/news/magazine-30793614

Twenty years ago the Government backed a major expansion of the CCTV Network - Now funds are being cut and cameras shut off. Is the UK's CCTV boom over, asks Rachel Argyle.

The UK has one of the largest CCTV networks in the world. But as cash-strapped councils look for cost-saving measures, the effectiveness of public CCTV is under scrutiny. The report found that the removal of Powys Country Council CCTV did not result in a significant rise in crime or anti-social behaviour and there is little evidence that CCTV deters violent or alcohol-related crime. Salmon says the Police will direct funds where the public want them, with "more bobbies on the beat".

These cuts are not an isolated case. Cornwall was one of the first local authorities to cut their CCTV budget back in April 2011 - by £350,000. Denbighshire Council will stop their funding and make a saving of £200,000 from 2016-17. Anglesey council scrapped its CCTV altogether last year but following a successful charitable trust bid it will now be run by the island's five town councils. In Derby, 48 cameras in the city centre may be switched off.

Some basic challenges of CCTV video surveillance

Considering the spate of both serious and non-serious crime that one comes across on a daily basis, it can be assumed that the rate of crime/process violation, etc. world over is not going down in proportion to the increase in the number of CCTV cameras. The concern lies in the fact that despite great strides in the quality of the cameras/VMS/video analytics, and large funds being invested in artificial intelligence, there are plenty of basic pain points that are still being completely overlooked to achieve valuable outcomes from CCTV. The question one faces is whether budgets need to be increased, or is more research needed as to what more can be done to achieve these outcomes? In order to understand what more can be done, one needs to study some of the issues being currently faced by the CCTV video surveillance industry. These can be summarized as:

- CCTV today is 'fit and forget'.
- CCTV today is considered to be part of only a security function. There are several other applications of CCTV. For example, CCTV and other surveillance video can be used in areas of occupational safety and health, THIRA, HIRA, RCA, TQM, GMP, and so on.
- CCTV video footage is never 'audited' as a SOP.
- There is a tendency to centralize video surveillance through command centres, forgetting that the best situational awareness and understanding would be available at the decentralized location.
- Humongous data storage and bandwidth requirements.
- False alarms, video blindness, poor situational awareness.
- No easy way to search through hours of CCTV video footage involving multiple cameras.
- No standardized reporting system.
- Diverse, expensive, and complex software (restrictive as well).
- No cost-effective remote backup of video footage and easy retrieval thereof (disaster recovery).
- No ease of sharing of CCTV video footage data.

Some of the other challenges of video surveillance:

1. Video analytics – over dependence on technology that is not fool proof

Most large organisations depend on triggers/alarms raised by video analytics/PSIMs. It is a known fact that a high percentage of these alarms are 'false', leading to false reporting, frustration and disbelief in the alarms, eventually leading to turning them off ('cry-wolf effect'). In fact, according

to a recent news report, the CISF (a para military force in India) who monitor New Delhi IGI Airport are plagued with over 100 false alarms on a daily basis there. Experts say that this leads to an absolute waste of time, and this is a major concern, because a real threat could go unnoticed whilst dealing with false alarms.

Link: http://www.dnaindia.com/india/report-over-100-false-alarms-a-day-at-igi-airport-keep-cisf-on-its-toes-2340896

More so, these systems require complex integration, high costs, and are often restricted to cameras/recorders/software of a particular manufacturer. Also, algorithm based systems will hardly be able to discover exceptions like a guard who is sleeping on duty, a child at school being at a location with a stranger who has ulterior motives, a real diamond being swapped for a fake one, sales staff not paying attention to customers, a recce being conducted, and so on.

2. Storage and sharing standards

The video surveillance industry has not been able to set a 'standard' for backup and storage of CCTV video. Storage of CCTV video footage may vary from one day, to months, or even a few years. However, the question is "what happens in a case where one needs to refer to video beyond these periods"? Besides, how does one search for a particular video easily? Finally, when an incident occurs, or when an exception is discovered, what are the next steps to be taken? There is no standard way recommended by the video surveillance industry to report and share the same.

3. Backup – Relevance vs. Quantity

Most backup of CCTV video footage happens on the recording device i.e. the DVR/NVR/Servers. Cloud storage is not too popular with most users and comes with its own challenges. In several cases of crime, criminals have decamped with the recorder itself after committing the crime. If this happens, how will the evidence be available to the Police? There are a number of cases of deliberate destruction of the recorder, or disk failure, or, data overwritten, or plain human error. Smart and cost-effective backup therefore is needed; a backup that is quick, simple, easily searchable, occupies lesser storage, and can remain forever if need be. It is a known fact that a video surveillance system has only a single opportunity to capture video frames. Otherwise, the imagery is lost forever, as there is no re-transmission opportunity in this always-on, live recording application; i.e. video must always be available!

Finally, it may be remembered that no amount of technology can replace the human eyes and mind (human interpretation). Eyes not only see, but perceive, understand, analyze and quickly help take corrective and preventive action. According to a recent study (Hodgetts, Vachon, Chamberland & Tremblay, May 2017) "while technological systems can automate some aspects of the surveillance process, the human operator is still ultimately responsible for detection of suspicious activities and decision making. Thus, the optimal design and development of new

technology should not focus solely on the capabilities of the system itself, but on supporting the operators' cognitive vulnerabilities".

A camera lens can capture a school guard leading a child to the science laboratory (a place where she/he should not be at) and find nothing odd about it, but the human eyes and mind on seeing this, will immediately question the motive behind this act, take action, and thereby prevent a possible heinous crime.

More surveillance

It is common to come across articles related to Governments mandating the deployment of CCTV surveillance systems. For example, while some states in India have mandated the installation of CCTV surveillance systems at any location where there are more than 'X' footfalls, or at educational institutions, sufficient attention has not been paid to creating, monitoring and reporting methodologies/standards in order that best use of the information can be made and shared with relevant stakeholders/police/LEA quickly and efficiently before/after an incident occurs. This means that while attention is being paid to 'acquire', no attention is paid to 'analyze'.

Restrictive software

While Standards like ONVIF or data compression standards have been set by the video surveillance industry, it is not uncommon to come across situations where restrictive software by individual manufacturers often make it difficult for law enforcement agencies to work with recorded video.

City surveillance

With respect to city surveillance projects, there seems to be no answer as to how any Government/local body will ever be able to cover every nook and corner of a city on its own. It is interesting to note that in a city like Mumbai, which was the target of a terrible terror attack on 26/11/2008, it took 8 years to install and commission Just 6000 cameras as part of the Mumbai City Surveillance project. With respect to the term 'city surveillance', it may be noted that while an airport like New Delhi has over 3000 cameras, one cannot fathom just how only 6000 cameras in Mumbai can be termed as 'city surveillance', and just how will only 6000 cameras be able to prevent crime at a city level, or even ensure that a majority of traffic violations will be detected.

Again, with respect to city surveillance, no attention seems to have been paid to:

- How does one guarantee that nothing will be missed when camera feeds are being refreshed every 'X' minutes on the video wall at command centres?

- How does one guarantee that nothing will be missed when the CCTV operator is not on her/his seat, or not watching the monitors, or is simply biased?

- How does one guarantee that nothing will be missed there are so many variables of human behaviour, and that live monitoring is not like solving a math problem, where there can be only one answer?

- How does one guarantee that nothing will be missed when the CCTV operator is generally monitoring 3 monitors at a time, with each monitor streaming 16 video feeds?

- How does one guarantee that nothing will be missed by complex algorithm-based systems, which are known to raise so many false alarms, that CCTV operators are known to lose faith in them, resulting in turning them off?

- How does one tackle the phenomenon of video blindness and poor situational awareness?

- The fact that how an incident, which takes place in an area which is not covered by city surveillance cameras, is handled any differently from an incident which takes place in an area which is covered by city surveillance cameras.

This mandating of installing more and more CCTV surveillance cameras or creating more city surveillance projects continues without any standard guidelines whatsoever about how to monitor and/or report findings, as well as to ensure that valuable outcomes are achieved is leading us nowhere. Also, there have been enough cases where, in spite of CCTV surveillance systems, evidence could not be retrieved from the same due to the fact that crucial cameras were not working, the camera position was incorrect, the video feed was poor, or that the recorder itself was stolen/destroyed/tampered with/failed to record.

Also, no practical and cost-effective solutions have been found as to:

- How to use the power of 'crowd sourced surveillance'; i.e. how best to use cameras that belong to the private sector, as part of the overall city surveillance needs (in this case, the answer certainly does not lie in such video feeds being accessed by the local police station because of shortage of manpower and poor situational awareness).

- How to store CCTV video feeds in terms of relevance as well, as opposed to quantity only.

- How to easily search the stored video footage.

- How to gain actionable intelligence and patterns from crime, traffic issues, and process violations.

- How to get the community to follow standardized templates when reporting crime, in order that crime can be solved faster. As mentioned earlier, if the report follows a common minimum standard, the Police/LEA have to deal with only one common format.

- How to help the Police/LEA to quickly work with live or recorded CCTV/other video footage/images and photos depicting a scene of a bomb blast or a case of chain snatching, in the areas of forensics and investigation, prison management, VIP movements/sports events/religious events/cultural events/rallies/etc.

- How to increase revenues for the traffic departments through the auditing of traffic CCTV cameras and issuing tickets. Auditing will ensure that there are greater chances that traffic violations/accidents which are missed by alarm-based systems are discovered during the audit process.

Proliferation of CCTV/other video surveillance systems

Trillions of hours of surveillance video is created daily across the world. With more and more sources of video surveillance like body worn cameras, drones, UAVs, mobile phones, etc., the amount of rich visual data being captured will be wasted if not reviewed and/or processed as a SOP on a regular basis.

While the tendency is to veer towards video analytics, one needs to bear in mind that algorithm-based systems can only do so much and no more! Also, a majority of the video that is being/will be captured, belongs to the private sector, which either cannot afford expensive video analytics software, or does not need it at all. Further, to gain from video surveillance fully, unless users themselves 'see' what the cameras 'saw', optimal benefits of video surveillance will not accrue. Seeing what the cameras ‘saw’, may be referred to as ‘auditing CCTV video footage’.

Again, many organizations are struggling to find ways to apply CCTV video footage to do more for their businesses. In an age when data is fast becoming the lifeblood of the business world, many organizations are intuitively aware of the great potential that surveillance video data holds for them, but they lack an understanding of exactly how to tap into that potential in cost-effective ways.

Part of the reason for this is, that the nature of video surveillance has changed in recent years. Traditionally, video helped support safety and security measures, and also provided a layer of accountability and insurance. Fast forward to today’s world, this booming video surveillance data can now serve as a strategic system for business outcomes that go beyond addressing only security needs. For example, a surveillance camera at a retail store can be a great tool that provides images that can be turned into measurable and actionable insights that help retailers reduce waste, enable stores to better manage stock levels, and help drive better sales. The answer may come from the human brain. In a contest between man and machine, it quickly becomes evident that ‘intelligent’

video alone will not work; from visual perception to attention span, from memory capacity to situational analysis (awareness), surveillance technology supervised and superseded by the human brain will continue to help raise the bar for the CCTV Industry as a whole.

One must also remember that CCTV video footage data is not just about crime. It relates as much to agriculture, climate change, forest management, elections, and so on. In short, wherever there is CCTV/video surveillance, there is a need to audit the same. Therefore, it is important to remember that continuous auditing will lead to continuous improvement. Continuous corrective and preventive action will deliver optimal outcomes of CCTV over a period of time.

In conclusion

In view of the above arguments and research findings, it is safe to maintain that the mere installation of CCTV cameras is not sufficient, and users will need to take a few extra steps to make CCTV cameras work for them. This will largely depend on what the cameras are seeing, and how the data unleashed thereby is seen, and interpreted.

All of the above relate to a new thought process, which until now has been completely overlooked, and needs urgent action.

PROBLEMS OF CITY SURVEILLANCE

While there is no doubt that command centres are a very crucial part of centralized city surveillance, they come with some typical problems.

PROBLEM 1 – NO VIDEO

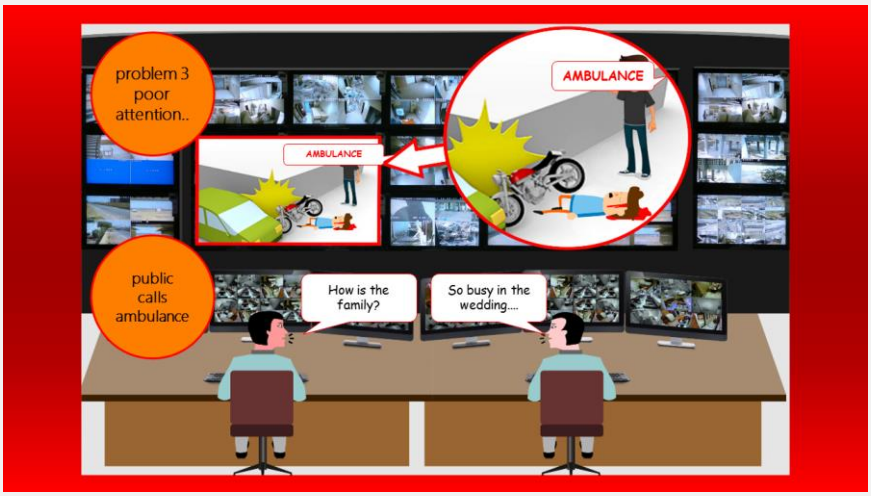
Video feeds are often lost due to non-working cameras, bandwidth, or other technical issues, including sabotage.

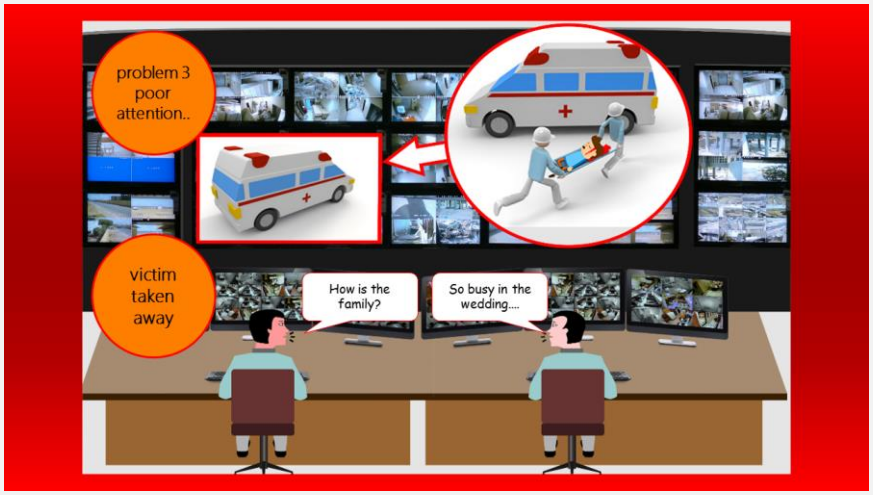
PROBLEM 2 – VIDEO WALL 'REFRESH' RATE

Since only a limited number of cameras can be displayed on a video wall, video feeds are refreshed at pre-set time intervals. Due to this, by the time a set of cameras is displayed again, considerable amount of information is lost!

PROBLEM 3 – OPERATOR ISSUES

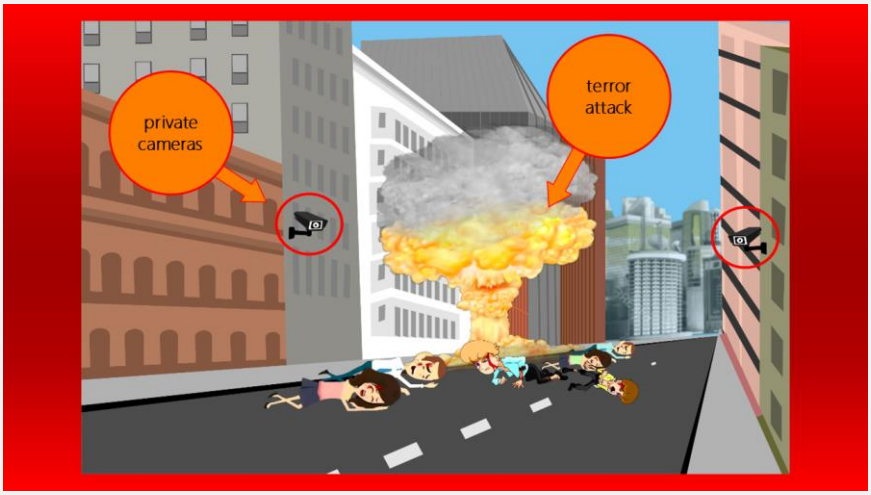
CCTV operators at command centres face several issues ranging from poor attention span, video blindness, fatigue, boredom, lack of situational awareness, bias and false alerts.





PROBLEM 4 – NO CITY SURVEILLANCE CAMERAS

It is likely that several incidents occur at locations which are not covered by city surveillance cameras. These could range from petty crimes such as chain snatching to serious ones like a terror attack. It is possible that these incidents could be captured by private cameras belonging to citizens residing at these respective locations.



PROBLEM 5 – NO STANDARD 'NEXT STEPS' OR 'WORKFLOW'

Some of the other issues that are faced in centralized city surveillance projects are:

(1) Difficulty of extracting relevant footage
(2) Re-construction of an incident in an easy-to-view format
(3) No standardized method of reporting
(4) No possibility of gaining business intelligence

OVERVIEW OF LITERATURE:

Research findings:

Below are some notable research findings that strengthen the case for a new thought process:

1. Why human intervention is necessary for monitoring of CCTV systems

- Assessing the Impact of CCTV (2005) – Martin Gill and Angela Spriggs from the University of Leicester

https://techfak.uni-bielefeld.de/~iluetkeb/2006/surveillance/paper/social_effect/CCTV_report.pdf

"…Too much must not be expected of CCTV. It is more than just a technical solution; it requires human intervention to work to maximum efficiency and the problems it helps deal with are complex. It has potential, if properly managed, often alongside other measures, and in response to specific problems, to help reduce crime and to boost the public's feeling of safety; and it can generate other benefits…"

- Not seeing the crime for the cameras – Why is it difficult, but essential to monitor the effectiveness of security technologies? – M Angela Sasse from University College London

http://www.cl.cam.ac.uk/~rja14/shb10/angela1.pdf

"…current research shows that CCTV for crime prevention is largely ineffective. It is lazy to assume that installing technology solves the problem. It takes domain knowledge and attention to detail to make security technology work effectively—to date, this has been ignored, with expensive consequences…"

- Effective CCTV and the challenge of constructing legitimate suspicion using remote visual images – Dr. David Williams from the University of Hertfordshire

https://uhra.herts.ac.uk/bitstream/handle/2299/13465/906803.pdf?sequence=2

"…ultimately, it is not machinery that decides what constitutes an event or object worthy of monitoring in anticipation of potential further action; it is a human operator, acting within a workplace context and guided by pre-existing stereotypes and conceptions of who and what is normal in a given location. So it seems reasonable to ask, how capable is the ordinary 'capable guardian' that actually monitors CCTV screens? Smith points out that CCTV systems still largely rely on the "human element to both monitor and control cameras" and that despite some exceptions, this remains a neglected area of research…"

- U.S. Air Force

https://medium.com/war-is-boring/u-s-air-force-spy-planes-recorded-1-000-hours-of-video-every-day-57a152506b14

http://www.nytimes.com/2010/01/11/business/11drone.html?_r=0

As per a disclosure made in 2012, the US Air Force recorded 1000 hours of drone video per day. This number now may be even higher. The major problem they face is how to 'review' so much of video footage.

"…he said, there will be limits on what automated systems are allowed to do. "You need somebody who's trained and is accountable in recognizing that that is a woman, that is a child and that is someone who's carrying a weapon" he said. "And the best tools for that are still the eyeball and the human brain…"

- UK Home Office Surveillance Camera Code of Practice 2013

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

"…Principle 10: There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published…"

2. Why relying on video analytics systems is not fool-proof

- Study published in December 2012 by Singapore Technology Electronics

"...In reality, early adopters of video analytics soon discovered that early products fell short of their promised performance parameters, being difficult to configure when out in the field and plagued by large numbers of false alarms. Many became disillusioned and quickly declared the technology as an overhyped gimmick..."

"…compared to current commercial video analytics products, the visual cognitive ability in humans is also more efficient as they can readily discern between non-interesting movements caused by swaying vegetation, water or shadows against 'interesting' movements such as abnormal security events or human actions…"

- Security and Surveillance 2011 - Shaogang Gong and Chen Change Loy and Tao Xiang, Queen Mary University of London

https://www.researchgate.net/profile/Chen_Change_Loy/publication/226512587_Security_and_Surveillance/links/0912f508e58a2a8f77000000/Security-and-Surveillance.pdf

"…the usefulness of machine detected events can benefit from further examination using human expert knowledge. From statistical model learning perspective, constructing a model that encompasses 'all' normal events is inherently difficult. Given limited (and often partial) observation, some outlying regions of a normal class may be falsely detected as being unusual (and of interest) if no human feedback is taken into account for arbitrating such false alarms.

To overcome this inherent limitation of unsupervised learning from incomplete data, other sources of information need be exploited. Human feedback is a rich source of accumulative information that can be utilised to assist in resolving ambiguities during class decision boundary formation. An attractive approach to learn a model from human feedback is by employing an active learning strategy. Active learning aims to follow a set of predefined query criteria to select the most critical and informative point for human feedback on labelling verification. This strategy for active selection of human verification on some but not all machine detected events allows a model to learn quickly with far fewer samples compared to passive random labelling strategy. Importantly, it helps in resolving ambiguities of interest when lacking visual distinctiveness, leading to more robust and accurate detection of subtle unusual events…"

3. Video blindness

- A study published in Security Oz Magazine in 2002.

"…after 12 minutes of continuous video monitoring an operator will often miss up to 45% of screen activity, after 22 minutes of viewing, up to 95% is overlooked…"

4. Why is it important to have situational awareness while monitoring CCTV

- Not the Usual Suspects: A Study of Factors reducing the Effectiveness of CCTV 2008 – Hina Keval, University College London

http://sec.cs.ucl.ac.uk/fileadmin/sec/publications/Keval_Sasse_Not_the_Usual_Suspects_Security_Journal_2010.pdf

"…operators reported that they would scan activity on the monitors at random along the monitor wall, and did not use any pattern of scanning. Operators said that they knew where to look but could not explain how and why. One operator said, where they scanned was "… based

on intuition". Another operator commented that, "… it was like sixth sense, and i don't know where i should be looking as anything could happen at any time … er …I can just tell something is going over there even though no one tells me"…"

"…lack of familiarity with surveillance areas: most operators did not reside in the surveillance areas and found it hard to familiarize themselves with the area when they started their job…."

5. Why users of CCTV systems should adopt a qualitative rather than quantitative approach to storing CCTV video footage data

- UK Home Office Surveillance Camera Code of Practice 2013

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

"… 4.6.3 Although images and other information should not be kept for longer than necessary to meet the purposes for recording them, on occasions, a system operator may need to retain images for a longer period, for example where a law enforcement body is investigating a crime to give them the opportunity to view the images as part of an active investigation…"

- Practical advice on the use of CCTV in Criminal Investigations (2011) –UK National Policing Improvement Agency

http://library.college.police.uk/docs/npia/cctv-final-locked-v21-2011.pdf

"…images associated with undetected crime should be retained according to management of police information principles. When retaining undetected crime records, consideration should be given to ensuring that they are easily retrievable and accessible for replay and viewing. An assessment of the possible value of the information to future cases should also be made…"

6. Why it is important to report incidents in a standard format

- Police Reporting 2004 – Cpl. Timothy P. Marta, School of Law Enforcement Supervision (US), and Dr. Michael Kleine, Criminal Justice Institute (US).

https://www.cji.edu/site/assets/files/1921/police_reporting.pdf

"…when the decision is made to complete a report, officers must first cover the basic information; who, what, when, where, why, and how. When answering these questions, remember that they are not as basic as they appear. There are many different aspects to be reported under each of these queries.

'WORKFLOW' FOR CCTV/VIDEO SURVEILLANCE

From all of the presented contentions, it is more than evident that the video surveillance industry has missed out on the creation of a 'workflow' for CCTV/video surveillance.

A 'workflow' for CCTV/video surveillance should allow a user to:

- Acquire, visualise, analyze, and retain relevant CCTV video footage.
- Playback and efficiently conduct post event analysis (auditing).
- Report using standardized templates in formats like PowerPoint, Word, Excel, PDF.
- Achieve business intelligence from reports.
- Store relevant CCTV video footage data remotely (disaster recovery) and reduce data size.
- Easily extract CCTV video footage data.
- Easily share CCTV video footage data.

JOB CREATION

CCTV VIDEO FOOTAGE AUDITORS – A BRAND NEW GLOBAL PROFESSION

Getting to be a CCTV video footage auditor requires a preferable minimum of grade 12 qualification. This opens up opportunities for those who have not had the chance to pursue higher education. Besides earning a dignified living, CCTV video footage auditors can contribute immensely to national safety and security. This would also hold good for women and retired individuals. Further, students pursuing higher education can also consider being part-time CCTV video footage auditors as a means of both i) gaining job experience ii) an extra income.

There is an opportunity to turn tens of thousands of unemployed individuals in to CCTV video footage auditors. By doing so, not only are we giving equal opportunities to both girls and boys, women and men, but we are also creating more 'eyes' for the Police/LEA. The higher the number of 'eyes', the more secure any country will be. With millions of cameras currently in 'sleep mode', if all these eyes 'wake up', it will lead to crowd sourced surveillance and community policing.

Further, it can also be inferred that the larger the proportion of productively employed labour force of a population, lesser would be the crime rate and greater would be the well-being of society. It would also motivate households to spend more to improve their quality of life thereby propelling economic growth and more employment.

CCTV VIDEO FOOTAGE AUDITING

Webster's dictionary defines 'audit' as 'a methodical examination and review'. Auditing CCTV video footage maybe a post-event activity. However, it is a methodical activity that can help discover 'exceptions' or the 'unknown' that can easily be missed out by algorithm-based systems. Auditing CCTV video footage helps to use the 'past' to improve the future!

It is important to understand that events/occurrences that may seem 'normal' may not necessarily be so. Unfortunately, CCTV video footage is examined only after the occurrence of an incident, thereby focusing only on reactive surveillance rather than on proactive surveillance. This can be attributed largely to the fact that the regular review (audit) of CCTV footage is tedious and time consuming. Through the process of regular auditing of CCTV video footage as a standard operating procedure, several corrective and preventive measures can be initiated, ensuring thereby that valuable outcomes are achieved by users of CCTV, as have been pointed out earlier in this document.

Further, research indicates that post-facto surveillance is as important as real time surveillance. Regular auditing is like debriefing. It helps users discover exceptions that can be easily missed out by algorithm-based systems. It is only when the human mind and human eyes are involved, that most kinds of exceptions can be discovered. Let us remember that cameras have lenses; humans have 'eyes'. In an era of community policing, the more 'eyes' a community/society has, the higher are the chances of preventing crime and/or solving crime faster.

CCTV VIDEO FOOTAGE AUDITORS

Definition: A CCTV video footage auditor can be defined as one who audits, reviews, examines closely, CCTV footage daily, at periodical intervals, with an intent to discover the 'unknown'. Using all the tools available at her/his disposal, she/he 'looks out' for exceptions, process violations, abnormalities, performance lapses, behavioral patterns, potential threats, risks and so on. She/he de-bugs bytes of visual information multi-tasks by comparing past cases.

Based on guidelines and situational awareness, she/he tries to 'join the dots' to gain actionable intelligence and report the same in standardized formats. Part of the job description would also be the appropriate tagging of relevant information and providing business intelligence that accrues through the following of a protocol for documenting audit findings and incidents.

A CCTV video footage auditor should possess the following proficiencies:

1. A working knowledge of CCTV systems, video management systems (VMS), and DVRs/NVRs. Also, basic proficiency in using a computer (Windows based) and MS Office.

2. Situational awareness of the respective locations which entails knowledge of policies, standard operating procedures, observable patterns, potential issues and threats, risks,

and other important issues. It may be noted that the incumbent would not have situational awareness from day one but will gain it over a period of time due to regular audit of CCTV video footage.

3. Visual faculties which entail object/entity recognition and differentiation, tracking, and detection of movement.

4. Information handling skills which entail pattern recognition, co-relating events/occurrences ('joining the dots'), discerning exceptions, and suspicious activity/behavior.

5. A resolute personality who is confident, unbiased, and can deliver valuable insights.

Further, a CCTV video footage auditor can help 'discover' the following:

1. Process violations/standard operating procedures being flouted – for example, at a pharma company personnel not wearing the appropriate gear, at an office, employees loitering around the facilities area during working hours, at a logistics company, employees circumventing important procedures before dispatching items, and so on.

2. Abnormal/suspicious behavior/activity – for example, a person or a vehicle visiting a particular location at a particular time every day (seemingly conducting a recce), at a factory, workers/employees gathering at a particular location (seemingly colluding and planning something), at a school, a student from a lower grade being escorted to the higher-grade section, and so on.

3. Behavioral patterns/body language – for example at an airport, a person seemingly looking around too often, exhibiting unwarranted nervousness/fidgety behavior, and so on.

4. Health and safety issues – for example, at a construction site, workers not using the appropriate harness, at a gas plant, someone smoking, thereby signaling the possibility of a fire, and so on.

5. Issues with cameras/video feed – for example, the video feed from a camera 'switching off' every day at a particular time, or a poor-quality video feed, or objects/entities which are blocking the camera view, and so on.

6. Issues pertaining to the respective scenarios - for example, potential environmental/climate issues at river bodies, forests, farms, etc., traffic issues on roads, crowd management as well as potential stampedes in large processions/gatherings/events/VIP visits etc.

QUALIFICATIONS PACK FOR CCTV VIDEO FOOTAGE AUDITORS

This pack provides a guideline to basic personal as well as job attributes, skills and ability, along with knowledge and understanding to carry out the task of a CCTV video footage auditor.

QUALIFICATION PACK

Qualifications pack	
VERTICALS 1. SMALL AND MEDIUM ENTERPRISE	This vertical includes but is not limited to small and medium commercial establishments, department stores, industrial units, offices, nursery schools, crèches, housing societies, gated housing, small banks and ATMs, restaurants, guest houses, inns, hostels, nursing homes, wedding halls, places of religious worship, among others.
2. INDUSTRIAL AND OTHER LARGE ESTABLISHMENTS	This vertical includes but is not limited to large manufacturing units including factories, plants, mines, refineries, infrastructures, SEZs, large banks, business parks, ITES, BPOs, KPOs, warehouses, transport hubs like bus stations, schools, colleges, malls, theatres, auditoriums, hotels, hospitals, and large exhibition venues, large complexes of religious worship, among others.
3. PUBLIC PLACES AND SPACES	This vertical includes, but is not limited to open markets, roads and towns, public parking, sports stadia, trade fairs, open exhibition grounds, places of tourist interest including monuments, parks, public utilities, airports, mass rapid transport systems, and rallies among others.
4. CRITICAL INFRASTRUCTURE	This vertical includes mainly governmental and the country's security infrastructure, but is not limited to, seats of Government including Parliament houses, residences of the President and the Prime Minister, Police stations, airports, ports, bridges, border security posts, bunkers, defense establishments, nuclear establishments, among others.
PERSONAL ATTRIBUTES	i. Should be at least 18 years of age ii. Should preferably have a minimum education of grade 12 iii. Should have good communication skills iv. Should possess basic technological knowledge including computer skills, and working knowledge of CCTV systems *per se* v. Should follow good behavioural standards vi. Should be assertive yet co-operative vii. Should possess an extremely alert and vigilant nature

JOB ATTRIBUTES	In order that the individual on the job be competent, she/he: i. Should be able to operate CCTV video footage auditing tools in operation at the said establishment ii. Should be able to carry out the assigned job as per organisational procedures iii. Should have a fair understanding of the client, the establishment, and a general awareness of the type of incidents, both criminal and non-criminal, which can occur, thereby possessing situational awareness iv. Should be able to detect threats, risks, hazards, and emergencies from within the CCTV footage being audited v. Should take decisions in line with role and responsibility vi. Should effectively report any unusual occurrences /abnormalities/exceptions detected. Essentially, these reports should cover the 5 Ws and 1 H (what, when, where, why, who and how) and should be generated in a format like PowerPoint for easy dissemination. Additionally, these reports should also capture (operator enters this information), the peculiarities of the date (weekend, holiday etc.), the time (morning, lunch hour, opening hour, closing hour etc.), the location (busy area, main gate, lonely area etc.), the category (smoking, loitering, non-compliance etc.), they will in turn deliver patterns that will help gain business intelligence, which will allow for taking corrective and preventive action. (please refer to the annexure) vii. Should be able to assist any Law Enforcement Agency as and when required viii. Should carry out CCTV video footage auditing as a SOP on a daily basis. This can be further divided in to an hourly basis, depending on the SOP set by the management. ix. Should report the necessary 'audit findings' after pre-defined intervals or as set by the management in a standardized manner on a daily basis (please refer to the annexure) x. Should report 'patterns' based on historical data gathered through systematic audit/incident reports (please refer to the annexure)

ANNEXURE

ANNEXURE: TEMPLATE FOR DAILY CCTV VIDEO FOOTAGE AUDIT CHART

DAILY CCTV VIDEO FOOTAGE AUDIT CHART

ORGANIZATION: ORGANIZATION
LOCATION/ADDRESS: LOCATION/ADDRESS
YEAR: YEAR AUDITOR'S NAME: NAME OTHER: ANY OTHER INFORMATION

DATE	CAMERA NO. & DESCRIPTION	TIME SLOT	INCIDENT	REMARKS/ACTION
DD/MM/YY	1 - MAIN GATE	8:00 PM - 8:00 AM	GUARD SLEEPING	GUARD WARNED AND AGENCY FINED
DD/MM/YY	2 - 6 - RECEPTION	8:00 AM - 1:00 PM	NO VIDEO	TICKET RAISED WITH SYSTEM INTEGRATOR
DD/MM/YY	7 - 9 - STORES	1:00 PM - 4:00 PM	SMOKING	STAFF WARNED
DD/MM/YY	10 - 20 - WAREHOUSE	4:00 PM - 8:00 PM	NOT ON SEAT	STAFF WARNED
DD/MM/YY	21 - 22 - PANTRY	4:00 PM - 8:00 PM	ON PHONE	STAFF WARNED
DD/MM/YY	23 - 28 - CORRIDORS	4:00 PM - 8:00 PM	VISITOR ISSUE	VISITOR CONTACTED AND ACTION TAKEN
DD/MM/YY	29 - 32 - PARKING	4:00 PM - 8:00 PM	UNKNOWN VEHICLE	ADDED VEHICLE TO SUSPECT LIST. GUARD WARNED

ANNEXURE: NEW POWERFUL SIGNAGE

ANNEXURE

ANNEXURE: TEMPLATE FOR REPORTING AUDIT FINDINGS/INCIDENTS

AUDIT FINDING/INCIDENT REPORT

Report No.:	Date: DD-MM-YY Time	Type: Confidential	Seriousness: High
Audit Finding/Incident From: DD-MM-YY Time Audit Finding/Incident To: DD-MM-YY Time		Amount of Loss: $700	
Date Peculiarity: New Years Eve		Time Peculiarity: Late Evening	
Location: .....Road		Location Peculiarity: Crowded Area	
Category: Theft		Category Peculiarity: Mobile Phone	
Reported By: ABC		Reported To: XYZ	

1

AUDIT FINDING/INCIDENT REPORT

Report No.:	Date: DD-MM-YY Time	Type: Confidential	Seriousness: High
Description/People Info/Witnesses etc.:			
Action Taken:			
Action Recommended:			

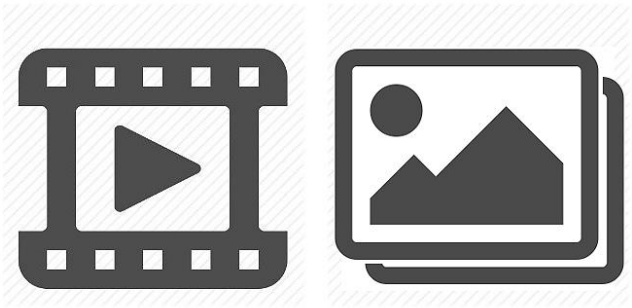
2

AUDIT FINDING/INCIDENT REPORT

Report No.:	Date: DD-MM-YY Time	Type: Confidential	Seriousness: High
Incident Log/Audit Trail Details:			
Integrity Verification/Authentication Details:			
Closure Details:			

3

VIDEO CLIP AND/OR SCREENSHOTS



ANNEXURE

ANNEXURE: PATTERNS DERIVED FROM AUDIT FINDINGS/INCIDENT REPORTS