



OCCUPATIONAL STANDARDS
FOR
'CCTV AUDITOR'



INTRODUCTION

The **Aim** of adding **CCTV Auditing, Reporting in Standardized Templates, and Retaining Video Data by 'Relevance'** to the Occupational Standards for CCTV Operators/Supervisors is to suggest that the **Mere 'Installation'** of CCTV Surveillance Systems is **Not Enough** to prevent Crime, Monitor and Control Traffic issues, as well as other Losses/Process Violations etc; and that some **Fundamental Changes** are needed to **Achieve** the related **Outcomes** and **Objectives** of CCTV Surveillance Systems.

The aim is also to ascertain **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.

Further, the aim is to introduce the following **New Concepts** to be included as de-facto parts of CCTV Surveillance:

- The concept of **'Auditing'** CCTV Video Feeds on a **Daily** basis as a **SOP**, in order that relevant stakeholders are able to **'Discover'** Exceptions, and **Other Rich Visual Information**, that can easily be **Missed** out by **Algorithm** based systems, and to be able to **'Join the Dots'**. The concept of Auditing CCTV Video Feeds at **Regular** intervals suggests a **Proactive** approach, as opposed to a Reactive approach.
- The concept of creating **'Standards'** and **'Templates'** to **Efficiently** and **Rapidly Share** information in a **Standardized** format with relevant Stakeholders across the nation/other nations (example with LEA agencies/Public).
- The concept of creating a **'Universe'**, where Auditing CCTV Video Feeds becomes an activity that is followed by all users of CCTV Surveillance Systems, thereby creating **'Digital Informers'**, leading to **Crowd Sourced Surveillance** and **Community Policing**, and the **Reduction** of **Burden** of LEA.

STATEMENT OF THE PROBLEM

CCTV Cameras are **Increasing** world over; **Yet** Crime, Traffic Violations, Losses and Process Violations, etc. **Continue** to take place. 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** packaging unit can cost the company huge Penalties and Warnings from US FDA, or such other bodies.

A Fool-Proof **Automatic** system that can detect the above Exceptions (Recces) is 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 system will **Ever be developed**; at least not for a very long time to come.

While authorities have been mandating the installation of CCTV Surveillance Systems all over the country, so far there has been no mention of **How** users (including the LEA themselves) are supposed to Monitor and/or Report the Findings from these Systems.

It is common to come across articles where crores of rupees are being allocated towards 'City Surveillance' projects, or that Governments have created new Laws where CCTV Surveillance Systems have been made compulsory. 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, some states have mandated the installation of CCTV Surveillance Systems at examination halls and schools/school buses. However, **No Attention** has been paid to creating **Monitoring and Reporting Methodologies/Standards** in order that related information can be made available to relevant stakeholders/LEA quickly and efficiently before/after an Incident occurs. In fact, and quite funnily, there is no mention that **"Cameras must basically be in a Working condition at All times"**.

With respect to 'City Surveillance' projects, there seems to be no answer to how LEA by themselves alone will ever be able to cover **Every nook and corner of a city**. Yet 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 (T3) has over 3000 Cameras, one cannot fathom **How Just** 6000 Cameras in Mumbai **can be termed as 'City Surveillance'**, and how just 6000 Cameras will 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 in the Command centre?
- **How** does one guarantee that nothing will be ‘Missed’ when the CCTV operator is **not** on his/her seat, or simply **not** watching the monitors?
- **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 Feeds at a time?
- **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?
- The phenomenon of ‘**Video Blindness**’ and ‘**Situational Awareness**’.
- The fact that **How** is an Incident, which takes place in an area which is not covered by ‘City Surveillance’, handled any differently from an Incident which takes place in an area which is covered by ‘City Surveillance’ Cameras.

This **Mindless Mandating** of CCTV Surveillance Systems continues **without any guidelines** whatsoever about **How** to **Monitor** and/or **Report** the Findings from these Systems. 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 not correct**, the Feed was **Poor**, or that the Recorder itself was **Stolen/Destroyed/Tampered with/Failed to record**. Again, no practical and cost-effective solutions have been found as:

- **How** to use the power of **Crowd Sourcing**; i.e. how best to use Cameras that belong to the Private Sector.
- **How** to Store CCTV Feeds in terms of ‘**Relevance**’ as opposed to ‘Quantity’.
- **How** to easily **Search**, what has been stored.
- **How** to gain **Intelligence** and **Patterns** from Crime, Traffic issues, and Process Violations.
- **How** to get the Community to follow **Standardized** guidelines when Reporting Crime, in order that Crime can be solved faster, so that the Police have to deal with **One Common Format**; at least for serious Crime.



- **How** to Help LEA to **Quickly Work** with live or recorded CCTV/Other Video Footage/Images and Photos depicting a scene of 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 Auditing of Traffic CCTV Cameras and issuing E-Challans. **Auditing** will ensure that Traffic Violations/Accidents that are missed by Alarm based Systems are Discovered during the Audit Process.

THE EXPLOSION OF VIDEO DATA

By 2020, it is expected that **800+ Petabytes of Data** will be created **Daily** across the globe. 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. While the **tendency** is to veer towards **Video Analytics**, one needs to bear in mind that Algorithm based solutions **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 software, or does not need it at all in most cases. Further, to **'Gain'** from Video Surveillance fully, unless users themselves **'See' what the Cameras 'Saw'**, the benefits of Video Surveillance will **not accrue**. 'Seeing' what the Cameras 'Saw', may be referred in one word as **'Auditing'**.

One must also remember that CCTV/Video data **is not just about Crime**. It relates as much to **Agriculture, Climate** change, **Forest** Management, **Elections**, and so on. **Wherever** there is CCTV/Video Surveillance, there is a **need** to **'Audit'** the same.

IN CONCLUSION

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.

Living in an increasingly explosive and dangerous world, the key to Prevention and Solving Terror and Crime will largely depend on what the Cameras are 'Seeing', and how the data unleashed thereby is 'Seen', and 'Interpreted', (all these relate to **Auditing CCTV**) a **Key** thought process which until now has been completely **Overlooked**, despite great strides in Cameras themselves, and some amount of artificial intelligence trying to find its place in Video Surveillance.

OVERVIEW OF LITERATURE:

Below are some research findings that clearly **validate** the 'STATEMENT OF THE PROBLEM'.

1. The Importance of Auditing CCTV as a SOP

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..."

"...Good practice dictates that a system operator **should Review** the continued use of a Surveillance Camera system on a **regular basis**, at least annually, to ensure it remains necessary, proportionate and effective in meeting its stated purpose for deployment..."

"...A Surveillance Camera system may be used for **more than one purpose**. For example, one purpose might be Crime prevention and detection, and another traffic management. Accountability for each purpose may rest within different elements of a system operator's management structure. Should that be the case, then it is good practice for the governance arrangements to include those accountable for each purpose and facilitate effective joint working, **Review and Audit**, decision making and public engagement..."

2. 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**..."

3. 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. At 3/13 control rooms, operators new to the control room were given hand-drawn geographical maps of the Surveillance area. The maps were drawn with the Camera icons and numbers at their relevant locations. These maps were drawn by experienced operators who felt that they should help newcomers to get them up to speed with the tasks. Experienced operators rarely used maps as they knew the locations of a majority of the CCTV Cameras in the system...”

4. Why relying on Video Analytics Systems is not fool-proof

Study published in December 2012 by Singapore Technology Electronics

<http://www.stee.stengg.com/pdf/publication/Vol25No3/AppNotes2.pdf>

“...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.eecs.qmul.ac.uk/~sgg/papers/GongEtAl_SecuritySurveillance2011.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...”

5. 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://www.cctvusergroup.com/downloads/file/Martin%20gill.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...”

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...**”

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

“...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...”

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

6. Why users of CCTV Systems should adopt a Qualitative rather than Quantitative approach to storing 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

“...Principle 6 - No more images and information should be stored than that which is strictly required for the stated purpose of a Surveillance Camera system, and such images and information should be deleted once their purposes have been discharged.

4.6.1. Images and information obtained from a Surveillance Camera system should not be kept for longer than necessary to fulfil the purpose for which they were obtained in the first place. This period should be decided in advance and be the minimum period necessary. This is also a requirement of the 1998 Act and further guidance on this is contained in the ICO CCTV code of practice.

4.6.2 The retention period for different Surveillance Camera systems **will Vary** due to the purpose for the system and how long images and other information need to be retained so as to serve its intended purpose. It is **Not, therefore, possible to be Prescriptive about Maximum or Minimum periods**. Initial retention periods should be reviewed by a system operator and **Reset** in the light of experience. A proportionate approach should always be used to inform retention periods and these should not be based upon infrequent Exceptional cases.

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...”

7. Why is it important to Report Incidents in a Standard Format

National Crime Recording Standard (NCRS): An analysis on the impact of Recorded Crime – 2003 – Jon Simmons, Clarissa Legg, and Rachel Hosking, Research, Development, and Statistics department of the UK Home Office

<http://image.guardian.co.uk/sys-files/Guardian/documents/2003/07/17/NCRS1.pdf>

“...Variation in recording practices had made comparisons between police forces and, indeed, national estimates of the level of Crime difficult to measure accurately. The Home Office has for some years sought to improve the consistency of police Crime recording...”

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

http://www.cji.edu/site/assets/files/1921/police_Reporting.pdf

When the decision is made to complete a Report, officer’s 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.

Once the officer has the needed information, this information must be **Arranged** in a manner that presents the information to the reader in a **Logical Orderly Manner**. With this in mind, I pointed out that police Reports have many different readers. Choosing the correct format to present the information is sometimes difficult. Through experience, conversations with other officers and supervisors, and conversations with prosecutors, it is clear that the use of **Headings** works well for anyone reading these Reports.

Important advice to any officer preparing a document that can and will be viewed by others for years to come is, “get it all, get it right, and write it clear”. When in doubt, refer to the old saying that could have likely been coined by an officer of the Law: **“If it’s not written down, it didn’t happen”...**



THE INDIAN SCENARIO FOR THE GROWTH OF CCTV

With a population of over one billion people, a coastline of 7,000 odd km, a land frontier of 15,000 km, high levels of poverty, major economic disparity, multiple religions, Crimes, Terrorism, Cross border conflicts and Natural Disasters, our country is **Battling Huge Security Challenges**. This has led to the Video Surveillance industry having found a market in India over the past few years, currently growing exponentially. This market is estimated to reach a whopping USD 2.4 billion by 2020. A recent research by 'India CCTV Camera Market Outlook, 2021,' states that *the market for CCTV Cameras is expected to grow with a CAGR of about 27.16% in the period from 2016 to 2021. Currently dominated by analogue Cameras, IP based systems are steadily making their way with their demand expected to rise exponentially over the next 5 years.*

A PRESSING NEED FOR CHANGE

Statistics reveal 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. In fact, the United Kingdom, one of the world's most surveilled countries itself is wondering if CCTV really helps prevent Crime given the exponential rise in Cameras, and their having little effect on Crime rates. The concern lies in the fact that despite research taking great strides in the quality of the Cameras and large funds being invested in artificial intelligence for post Video Surveillance, there are plenty of **Basic Pain Points** that are being completely **Overlooked**.

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.

Is the U.K. shooting the Messenger?

This is a crucial question. Do budgets need to be cut, or is more research needed as to **'What'** can be done to achieve **Optimum Outcomes** from CCTV? In order to understand the **'What'** 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 is **'Fit and Forget'**
- CCTV is **Never** Audited
- Tendency to only **Centralize** Video Surveillance through Command Centers, forgetting that the best Situational Awareness would be available from **Decentralizing** the same
- **Humongous** data storage and band width requirements



- **False Alarms, Video Blindness, Poor Situational Awareness**
- No easy way to **Search** through hours of Video
- No **Standardized Reporting** system of the same
- Diverse, expensive, and **Complex** software (**Restrictive** as well), especially for small establishments and home users
- No **Remote** back up of Video Footage and easy **Retrieval** thereof
- No ease of **Sharing** of such data

What should be the **Outcomes** or **Pay Offs** from CCTV?

- Crime, Loss, and Fraud **Prevention**
- **Faster** Solving of Crime
- **Enhancement** of Compliance, Processes, and Safety
- Gaining better **Situational Awareness**
- Obtaining **Actionable Intelligence**
- Improvement of **Operational Efficiency**
- **Improvement** of Staff Performance, Customer Satisfaction, and Sales

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** of 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**”.*

'WORKFLOW' FOR CCTV/VIDEO SURVEILLANCE

From the above arguments, it is more than evident that the entire Surveillance industry has **Forgotten** to create a '**Workflow**' for CCTV/Video Surveillance. A '**Workflow**' for CCTV/Video Surveillance **should include**:

- Acquire, Visualise, Analyze, Retain, Report
- Playback, Post Event Analysis, Data Mining, Retention
- Reduction in Data Size
- Cost Effective and Easier Cloud Storage
- Auditing to become a SOP
- Standardized Reporting
- Easy of Data Extraction
- Stitching Relevant Stories together (Scene Reconstruction) from Diverse Videos and Playing back Multiple Videos in a SINGLE file, as opposed to Multiple files.
- Achieving Business Intelligence from Reports

CHALLENGES BEING FACED BY CCTV OPERATORS

Users of CCTV must make it a **Standard Operating Procedure (SOP)** to Audit CCTV on a **Daily Basis**.

Research indicates that Post-Facto Surveillance is As Important as Real Time Surveillance. Regular Auditing helps users Discover Exceptions that can be easily missed out by Algorithm-based solutions. It is only when the Human Mind and Human Eyes are involved, that 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.

Studies conducted in the past within Surveillance control rooms have raised a number of issues being faced by CCTV Operators.

- **Staggering** volume of data
- **Divided** visual attention
- Decisions made based on **Personal Biases, Experience, Prejudices**
- Video **Blindness**

CHALLENGES OF SURVEILLANCE TECHNOLOGY

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

Most large organisations depend on Triggers/Alarms raised by Video Analytics. It is a known fact that a high percentage of these alarms is **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 who monitor New Delhi IGI airport are plagued with over 100 false alarms on a Daily Basis. 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.

More so, these systems require complex integration, high costs and are often **Restricted** to Cameras/Recorders 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 back up and storage. Some store for 15 days, 30 days, 90 days, etc. However, 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? Even after an incident is Discovered, what are the next steps? There is No '**Standard**' way to Share.

3. Back Up – Relevance vs. Quantity

Most Backup of CCTV happens on the recording device i.e. the DVR/NVR. 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 Video Surveillance system has 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**.

Therefore, such a system should be created which can eventually benefit the user, viz., Governments, Law enforcement agencies, Private establishments etc. in many ways like:

- **Preventing** and resolving Crime faster
- **Remote** storage that will **Not** require additional bandwidth (savings)
- Effective **Disaster Recovery**



- **Relevant** data be stored for longer durations
- Ease of **Sharing** Footage with Law enforcement agencies
- Analysis of Video content should provide actionable intelligence
- Post facto Video analysis should lead to better **Situational Awareness**
- **Safety** of the people, brand, assets should be assured
- Daily Audit Reports should deliver **Patterns** that lead to **Business Intelligence**
- Investigation/Forensics made **Easy**

Finally it may be remembered that no amount of technology can replace the Human **Eyes** and **Mind**. Eyes not only see, but perceive, understand, analyze and quickly help take **Corrective** and **Preventive** action via the right recourse. A **Camera lens** can capture a **school guard** leading a **child** to the science laboratory (a place where he/she 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 possibly heinous Crime.

Thus, there is a need to create a New Profession or Category called '**CCTV Auditors**', and to create an Occupational Standard for this new Category.

CCTV AUDITING

Definition: Webster's dictionary defines '**Audit**' as '*a **Methodical Examination and Review***'.

Auditing CCTV maybe a post-event activity. However, it is a **Methodical** activity that can help **Discover** 'Exceptions' that can easily be missed out by Algorithm based systems.

It is important to understand that the events/occurences that may be deemed 'Normal' may not necessarily be so. Unfortunately, CCTV Footage is examined only **After** the occurrence of a mishap, thereby focusing only on reactive Surveillance rather than **Proactive** Surveillance. This can be attributed largely to the fact that the Regular Review of CCTV Footage is **Tedious** and **Time Consuming**. Through the process of **Regular Auditing** of CCTV as a **Standard Operating Procedure**, several **Corrective** and **Preventive** measures can be initiated, ensuring thereby that valuable Outcomes are achieved by users of CCTV, which can be:

- (a) Crime, Loss and Fraud **Prevention**
- (b) **Solving** Crime Faster
- (c) **Enhancement** of Compliance, Processes, and Safety
- (d) **Improvement** of Employee/Customer Satisfaction and Sales
- (e) **Standardization** of several 'Next Steps' after the 'Discovery'.



CCTV AUDITORS

Definition: A CCTV 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 his/her disposal, he/she '**Looks out**' for Exceptions, Abnormalities, Behavioral Patterns, Potential Threats, Risks and so on.

Based on Guidelines and a study of the Situational Awareness, he/she 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 following a **Protocol** for **Documenting** Audit Findings and Incidents.



QUALIFICATIONS PACK FOR CCTV 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 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, ITES, BPOs, KPOs, Nursing homes and weddings, 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, 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 PM, Police stations, Airports, Ports, Bridges, Border security posts, Bunkers, Defense establishments, Nuclear establishments, among others.	
PERSONAL ATTRIBUTES	<ul style="list-style-type: none"> i. Should be at least 18 years of age ii. Should have a minimum education of standard 12 iii. Should have good communication skills iv. Should possess basic technological knowledge including computer skills v. Should follow good behavioural standards vi. Should be assertive yet cooperative vii. Should possess an extremely alert and vigilant nature 	

JOB ATTRIBUTES

In order that the individual on the job be competent, he/she:

- i. Should be competent enough to be able to operate **CCTV 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 ideally 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 related to Business Intelligence, which will allow for taking Corrective and Preventive action. (Please refer to Annexures II and III)
- vii. Should be able to **assist** any Law enforcing agency as and when required
- viii. Should Carry out CCTV 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 (template reproduced in Annexure I)
- x. Should **Report 'Patterns'** based on **Historical Data** gathered through Systematic Audit/Incident Reports.

JOB CREATION – A BRAND NEW PROFESSION IN INDIA (CAN BE EXTRAPOLATED GLOBALLY)

India has a population of 1.4 billion people, of which **30%** resides in the **Urban** area. According to recent Report published by JM Financial (2017), *the number of students who enrol in higher education through the regular mode has steadily risen from 25.8mn in FY12 to 30.8mn in FY16—a CAGR of 4.5%. Similarly, the number of students passing out with degrees has grown at 4.7% from 7.4mn in FY12 to 8.8mn in FY16, out of which under-graduates constitute 6.3mn.* According to statistics released by the UN, unemployment in India is *not* expected to pick up pace in 2017-18. It is projected to increase from 17.7 million last year to **just** 17.8 million in 2017.

Further, as per the Fifth Annual Report on Employment – Unemployment Survey in India (2015-16) carried out by the Ministry of Labour and Employment, the **Unemployment Rate has reached 5 percent** which is the **Highest** in the last 5 years. While in 2011-12 session it was 3.8 %, it went on to become 4.7 % in 2012-13, and 4.9 % in 2013-14. Urban areas have more jobs and pay better than the rural sector. But **Women** have been **hurt the most**. Unemployment for female job seekers has now gone **as high as 8.7 percent**. Further, the Report states that *it is pretty well-known that many persons who are reported as ‘employed’ or ‘workers’ in official publications do not get work for the entire duration of their stay in the Labour Force. And even those who get some work or the other for the entire duration may be getting work for only a small fraction of the time they are available for work. Besides, some may be working on jobs which do not allow them to fully utilise their abilities or from which they earn very low incomes. All this constitutes under-employment which remains a worrying aspect of the employment –unemployment scenario in the country. Thus rapid employment generation assumes even greater importance for our country.* Moreover, as per the findings of the Economic Survey of 2015-16 carried out by the Ministry of Finance *“To exploit its demographic dividend, India must create millions of “good”— safe, productive, well-paying jobs”.*

Being a CCTV Auditor requires a 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, they 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 Auditors** as a means of both i) gaining job experience ii) an extra income.

We have an opportunity to turn tens of thousands of unemployed individuals into CCTV Auditors. By doing so, not only are we giving equal opportunities to both boys and girls, men and women, but we are also creating **more ‘Eyes’ for the Police**. The higher the number of ‘eyes’, the more secure we can make our country. With Millions of Cameras in **‘Sleep Mode’** currently, if all these eyes **‘Wake up’**, it will lead to **Crowd Sourced Surveillance**.

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



ANNEXURES TO THE PROPOSED OCCUPATIONAL STANDARD FOR 'CCTV AUDITORS'

ANNEXURE I

ANNEXURE I : PROPOSED TEMPLATE FOR DAILY CCTV AUDIT CHART

DAILY CCTV 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
24 October 2016	1 - MAIN GATE	8:00 PM - 8:00 AM	GUARD SLEEPING	GUARD WARNED AND AGENCY FINED
24 October 2016	2 - 6 - RECEPTION	8:00 AM - 1:00 PM	NO VIDEO	TICKET RAISED WITH SYSTEM INTEGRATOR
24 October 2016	7 - 9 - STORES	1:00 PM - 4:00 PM	SMOKING	STAFF WARNED
24 October 2016	10 - 20 - WAREHOUSE	4:00 PM - 8:00 PM	NOT ON SEAT	STAFF WARNED
24 October 2016	21 - 22 - PANTRY	4:00 PM - 8:00 PM	ON PHONE	STAFF WARNED
24 October 2016	23 - 28 - CORRIDORS	4:00 PM - 8:00 PM	VISITOR ISSUE	VISITOR CONTACTED AND ACTION TAKEN
24 October 2016	29 - 32 - PARKING	4:00 PM - 8:00 PM	UNKNOWN VEHICLE	ADDED VEHICLE TO SUSPECT LIST. GUARD WARNED

ANNEXURE II : PROPOSED TEMPLATE FOR REPORTING AUDIT FINDINGS/INCIDENTS

AUDIT FINDING/INCIDENT REPORT

Report No.:	Date: 06-08-2017 08:55:34	Type: Confidential	Seriousness: High
Audit Finding/Incident From: 06-08-2017 08:55:30 Audit Finding/Incident To: 06-08-2017 08:55:30		Amount of Loss:	
Date Peculiarity:		Time Peculiarity:	
Location:		Location Peculiarity:	
Category:		Category Peculiarity:	
Reported By:		Reported To:	

09-08-2017
Created by Com-Sur™
www.comsur.biz
1

AUDIT FINDING/INCIDENT REPORT

Report No.:	Date: 06-08-2017 08:55:34	Type: Confidential	Seriousness: High
Description/People Info/Witnesses etc.:			
Action Taken:			
Action Recommended:			


09-08-2017
Created by Com-Sur™
www.comsur.biz
2


AUDIT FINDING/INCIDENT REPORT

Report No.:	Date: 06-08-2017 08:55:34	Type: Confidential	Seriousness: High
Incident Log/Audit Trail Details:			
Integrity Verification/Authentication Details:			
Closure Details:			

09-08-2017
Created by Com-Sur™
www.comsur.biz
3

VIDEO CLIP AND/OR SCREENSHOTS





09-08-2017
Created by Com-Sur™
www.comsur.biz
4

ANNEXURE III: PATTERNS DERIVED FROM AUDIT FINDINGS/INCIDENT REPORTS

ANNEXURE II

Incident Count

