CCTV

INSTALLATION TECHNICIAN

ELE/Q4605

C C T V

INSTALLATION TECHNICIAN

INDUS INTEGRATED INFORMATION MANAGEMENT LIMITED
AN ISO 9001:2015/ISO 14001:2015/OHSAS 18001:2007 COMPANY
VOCATIONAL SKILLS | IT SERVICES | GLOBAL CERTIFICATION

INDUS INTEGRATED INFORMATION MANAGEMENT LIMITED

AN ISO 9001:2015/ISO 14001:2015/OHSAS 18001:2007 COMPANY

VOCATIONAL SKILLS | IT SERVICES | GLOBAL CERTIFICATION

Indus Integrated Information Management Limited

AN ISO 9001:2015, ISO 14001:2015, OHSAS 18001:2007, COMPANY

HEAD OFFICE:

AE-369, Salt Lake Sec-1, Kolkata- 700 064
Phone: 033 23370243/ 53
Mail ID: admin@iiimltd.in
www.iiimltd.in • www.indusedutrain.com

BRANCH OFFICES:

KOLKATA
AD-76, Sector-I, Saltlake, Kolkata- 700 064
Phone: 033 4062 0636

AGARTALA
Opp. Kunjaban Post Office,
Near Heritage Park,799006, Tripura West
Phone: 08131955651

MUMBAI
1st Floor, Nimbus Centre, Oberoi Complex,
Off New Link Road, SAB TV Lane,
Andheri (W). Mumbai - 400053
Phone: +91 22 4099 5000

BENGALURU
No-09, AVS compound, 80 Feet Road,
Koramangala, Bengaluru-560034

DELHI
Room No: 1003 & 1004, 10th Floor, Ansal Tower 38,
Neheru Place, New Delhi-110019
Phone: 011 4100 5994

ODISHA
Room No. 402, 4th Floor, Nirmala Plaza,
Bhubaneswar, Khurda, Odisha Pin No- 751020
Phone No : 0674 2596196

PATNA
Leelavart Central, 1st Floor, Patliputra,
Patna-800013
Phone: 0612 2270849

JAIPUR
Maryann Martha Celestine Rose, Coral Studio 1,
Room No 403, 4th Floor, Plot No-B 64-65,
Near ICICI Bank, Shekar Marg, Jaipur-302016

Published: MAY, 2017

PRINTED IN INDIA

INDEX


INDUS EDUtr@in
An ISO 9001:2015/ISO 14001:2015/OHSAS 18001:2007 Company
Skilling India for an Inclusive Growth

CHAPTER 1

Security surveillance

Surveillance is the monitoring of the behavior, activities, or other changing information, usually of people for the purpose of influencing, managing, directing, or protecting them. This can include observation from a distance by means of electronic equipment (such as closed-circuit television (CCTV) cameras), or interception of electronically transmitted information (such as Internet traffic or phone calls); and it can include simple, no- or relatively low-technology methods such as human intelligence agents and postal interception. The word surveillance comes from a French phrase for "watching over" (sur means "from above" and veiller means "to watch"), and is in contrast to more recent developments such as surveillance.

Surveillance is used by governments for intelligence gathering, the prevention of crime, the protection of a process, person, group or object, or the investigation of crime. It is also used by criminal organizations to plan and commit crimes such as robbery and kidnapping, by businesses to gather intelligence, and by private investigators.

Surveillance is often a violation of privacy, and is opposed by various civil liberties groups and activists. Liberal democracies have laws which restrict domestic government and private use of surveillance, usually limiting it to circumstances where public safety is at risk. Authoritarian government seldom have any domestic restrictions, and international espionage is common among all types of countries.

TYPES

Computer

The vast majority of computer surveillance involves the monitoring of data and traffic on the Internet. In the United States for example, under the Communications Assistance For Law Enforcement Act, all phone calls and broadband Internet traffic (emails, web traffic, instant messaging, etc.) are required to be available for unimpeded real-time monitoring by Federal law enforcement agencies.

There is far too much data on the Internet for human investigators to manually search through all of it. So automated Internet surveillance computers sift through the vast amount of intercepted Internet traffic and identify and report to human investigators traffic considered interesting by using certain "trigger" words or phrases, visiting certain types of web sites, or communicating via email or chat with suspicious individuals or groups. Billions of dollars per year are spent, by agencies such as the NSA, the FBI and the now-defunct Information Awareness Office to develop, purchase, implement, and operate systems such as Carnivore, Narus Insight, and ECHELON to intercept and analyze all of this data, and extract only the

information which is useful to law enforcement and intelligence agencies.

Telephones

The official and unofficial tapping of telephone lines is widespread. In the United States for instance, the Communications Assistance For Law Enforcement Act (CALEA) requires that all telephone and VoIP communications be available for real-time wiretapping by Federal law enforcement and intelligence agencies. Two major telecommunications companies in the U.S.—AT&T Inc. and Verizon—have contracts with the FBI, requiring them to keep their phone call records easily searchable and accessible for Federal agencies, in return for $1.8 million per year.[22] Between 2003 and 2005, the FBI sent out more than 140,000 "National Security Letters" ordering phone companies to hand over information about their customers' calling and Internet histories. About half of these letters requested information on U.S. citizens.

Human agents are not required to monitor most calls. Speech-to-text software creates machine-readable text from intercepted audio, which is then processed by automated call-analysis programs, such as those developed by agencies such as the Information Awareness Office, or companies such as Verint, and Narus, which search for certain words or phrases, to decide whether to dedicate a human agent to the call.

Law enforcement and intelligence services in the United Kingdom and the United States possess technology to activate the microphones in cell phones remotely, by accessing phones' diagnostic or maintenance features in order to listen to conversations that take place near the person who holds the phone. The Sting Ray tracker is an example of one of these tools used to monitor cell phone usage in the United States and the United Kingdom. Originally developed for counterterrorism purposes by the military, they work by broadcasting powerful signals that cause nearby cell phones to transmit their IMSI number, just as they would to normal cell phone towers. Once the phone is connected to the device, there is no way for the user to know that they are being tracked. The operator of the stingray is able to extract information such as location, phone calls, and text messages, but it is widely believed that the capabilities of the Sting Ray extend much further. A lot of controversy surrounds the Sting Ray because of its powerful capabilities and the secrecy that surrounds it.

Mobile phones are also commonly used to collect location data. The geographical location of a mobile phone (and thus the person carrying it) can be determined easily even when the phone is not being used, using a technique known as multi laceration to calculate the differences in time for a signal to travel from the cell phone to each of several cell towers near the owner of the phone. The legality of such techniques has been questioned in the United States; in particular whether a court warrant is required. Records for one carrier alone (Sprint), showed that in a given year federal law enforcement agencies requested customer location data 8 million times.

Cameras

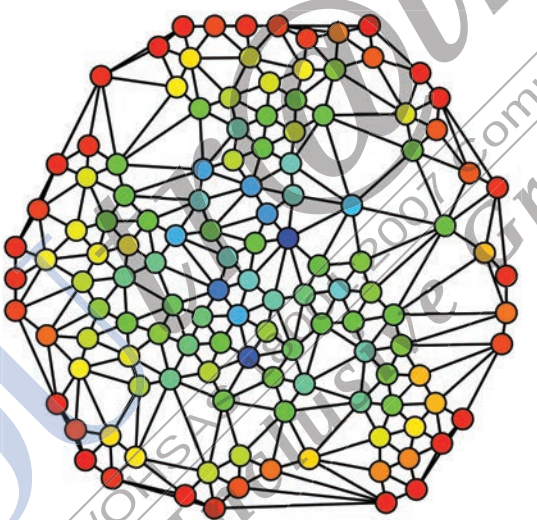
Surveillance cameras are video cameras used for the purpose of observing an area. They are often connected to a recording device or IP network, and may be watched by a security guard or law enforcement

officer. Cameras and recording equipment used to be relatively expensive and required human personnel to monitor camera footage, but analysis of footage has been made easier by automated software that organizes digital video footage into a searchable database, and by video analysis software (such as VIRAT and Human ID). The amount of footage is also drastically reduced by motion sensors which only record when motion is detected. With cheaper production techniques, surveillance cameras are simple and inexpensive enough to be used in home security systems, and for everyday surveillance.

In the United States, the Department of Homeland Security awards billions of dollars per year in Homeland Security grants for local, state, and federal agencies to install modern video surveillance equipment. For example, the city of Chicago, Illinois, recently used a $5.1 million Homeland Security grant to install an additional 250 surveillance cameras, and connect them to a centralized monitoring center, along with its preexisting network of over 2000 cameras, in a program known as Operation Virtual Shield. Speaking in 2009, Chicago Mayor Richard Daley announced that Chicago would have a surveillance camera on every street corner by the year 2016.

In the United Kingdom, the vast majority of video surveillance cameras are not operated by government bodies, but by private individuals or companies, especially to monitor the interiors of shops and businesses. According to 2011 Freedom of Information Act requests, the total number of local government operated CCTV cameras was around 52,000 over the entirety of the UK. The prevalence of video surveillance in the UK is often overstated due to unreliable estimates being requited; for example one report in 2002 extrapolated from a very small sample to estimate the number of cameras in the UK at 4.2 million (of which 500,000 in Greater London. More reliable estimates put the number of private and local government operated cameras in the United Kingdom at around 1.85 million in 2011.

Social network analysis



A graph of the relationships between users on the social networking site Facebook. Social network analysis enables governments to gather detailed information about peoples' friends, family, and other contacts. Since much of this information is voluntarily made public by the users themselves, it is often consider to be a form of open-source intelligence

One common form of surveillance is to create maps of social networks based on data from social networking sites such as Facebook, MySpace, Twitter as well as from traffic analysis information from phone call records such as those in the NSA call database, and others. These social network "maps" are then data mined to extract useful information such as personal interests, friendships & affiliations, wants, beliefs, thoughts, and activities.

Many U.S. government agencies such as the Defense Advanced Research Projects Agency (DARPA), the National Security Agency (NSA), and the Department of Homeland Security (DHS) are investing heavily in research involving social network analysis. The intelligence community believes that the biggest threat to U.S. power comes from decentralized, leaderless, geographically dispersed groups of terrorists, subversives, extremists, and dissidents. These types of threats are most easily countered by finding important nodes in the network, and removing them. To do this requires a detailed map of the network.

Biometric

Fingerprints being scanned as part of the US-VISIT program

Biometric surveillance is a technology that measures and analyzes human physical and/or behavioral characteristics for authentication, identification, or screening purposes. Examples of physical characteristics include fingerprints, DNA, and facial patterns. Examples of mostly behavioral characteristics include gait (a person's manner of walking) or voice.

Facial recognition is the use of the unique configuration of a person's facial features to accurately identify them, usually from surveillance video. Both the Department of Homeland Security and DARPA are heavily funding research into facial recognition systems. The Information Processing Technology Office, ran a program known as Human Identification at a Distance which developed technologies that are capable of identifying a person at up to 500 ft by their facial features.

Another form of behavioral biometrics, based on affective computing, involves computers recognizing a person's emotional state based on an analysis of their facial expressions, how fast they are talking, the tone and pitch of their voice, their posture, and other behavioral traits. This might be used for instance to see if a person's behavior is suspect (looking around furtively, "tense" or "angry" facial expressions, waving arms, etc.)

Aerial

Micro Air Vehicle with attached surveillance camera

Aerial surveillance is the gathering of surveillance, usually visual imagery or video, from an airborne vehicle—such as an unmanned aerial vehicle, helicopter, or spy plane. Military surveillance aircraft use a range of sensors (e.g. radar) to monitor the battlefield.

Digital imaging technology, miniaturized computers, and numerous other technological advances over the past decade have contributed to rapid advances in aerial surveillance hardware such

as micro-aerial vehicles, forward-looking infrared, and high-resolution imagery capable of identifying objects at extremely long distances. For instance, the MQ-9 Reaper, a U.S. drone plane used for domestic operations by the Department of Homeland Security, carries cameras that are capable of identifying an object the size of a milk carton from altitudes of 60,000 feet, and has forward-looking infrared devices that can detect the heat from a human body at distances of up to 60 kilometers. In an earlier instance of commercial aerial surveillance, the Killington Mountain ski resort hired 'eye in the sky' aerial photography of its competitors' parking lots to judge the success of its marketing initiatives as it developed starting in the 1950s.

The United States Department of Homeland Security is in the process of testing UAVs to patrol the skies over the United States for the purposes of critical infrastructure protection, border patrol, "transit monitoring", and general surveillance of the U.S. population. Miami-Dade police department ran tests with a vertical take-off and landing UAV from Honeywell, which is planned to be used in SWAT operations. Houston's police department has been testing fixed-wing UAVs for use in "traffic control".

Data mining and profiling

Data mining is the application of statistical techniques and programmatic algorithms to discover previously unnoticed relationships within the data. Data profiling in this context is the process of assembling information about a particular individual or group in order to generate a profile — that is, a picture of their patterns and behavior. Data profiling can be an extremely powerful tool for psychological and social network analysis. A skilled analyst can discover facts about a person that they might not even be consciously aware of themselves.

HART program concept drawing from official IPTO (DARPA) official website

Economic (such as credit card purchases)

and social (such as telephone calls and emails) transactions in modern society create large amounts of stored data and records. In the past, this data was documented in paper records, leaving a "paper trail", or was simply not documented at all. Correlation of paper-based records was a laborious process—it required human intelligence operators to manually dig through documents, which was time-consuming and incomplete, at best.

But today many of these records are electronic, resulting in an "electronic trail". Every use of a bank machine, payment by credit card, use of a phone card, call from home, checked out library book, rented video, or otherwise complete recorded transaction generates an electronic record. Public records—such as birth, court, tax and other records—are increasily being digitized and made available online. In addition, due to laws like CALEA, web traffic and online purchases are also available for profiling. Electronic record-keeping makes data easily collectable, storable, and accessible—so that high-volume, efficient aggregation and analysis is possible at significantly lower costs.

Corporate

Corporate surveillance is the monitoring of a person or group's behavior by a corporation. The data collected is most often used for marketing purposes or sold to other corporations, but is also regularly shared with government agencies. It can be used as a form of business intelligence, which enables the corporation to better tailor their products and/or services to be desirable by their customers. Or the data can be sold to other corporations, so that they can use it for the aforementioned purpose. Or it can be used for direct marketing purposes, such as the targeted advertisements on Google and Yahoo, where ads are targeted to the user of the search engine by analyzing their search history and emails (if they use free webmail services), which is kept in a database.

For instance, Google, the world's most popular search engine, stores identifying information for each web search. An IP address and the search phrase used are stored in a database for up to 18 months. Google also scans the content of emails of users of its Gmail webmail service, in order to create targeted advertising based on what people are talking about in their personal email correspondences. Google is, by far, the largest Internet advertising agency—millions of sites place Google's advertising banners and links on their websites, in order to earn money from visitors who click on the ads. Each page containing Google advertisements adds, reads, and modifies "cookies" on each visitor's computer. These cookies track the user across all of these sites, and gather information about their web surfing habits, keeping track of which sites they visit, and what they do when they are on these sites. This information, along with the information from their email accounts, and search engine histories, is stored by Google to use for building a profile of the user to deliver better-targeted advertising.

Human operatives

Organizations that have enemies who wish to gather information about the groups' members or activities face the issue of infiltration.

In addition to operatives' infiltrating an organization, the surveilling party may exert pressure on certain members of the target organization to act as informants (i.e., to disclose the information they hold on the organization and its members).

Fielding operatives is very expensive, and

for governments with wide-reaching electronic surveillance tools at their disposal the information recovered from operatives can often be obtained from less problematic forms of surveillance such as those mentioned above. Nevertheless, human infiltrators are still common today. For instance, in 2007 documents surfaced showing that the FBI was planning to field a total of 15,000 undercover agents and informants in response to an anti-terrorism directive sent out by George W. Bush in 2004 that ordered intelligence and law enforcement agencies to increase their HUMINT capabilities.

Satellite imagery

On May 25, 2007 the U.S. Director of National Intelligence Michael McConnell authorized the National Applications Office (NAO) of the Department of Homeland Security to allow local, state, and domestic Federal agencies to access imagery from military intelligence Reconnaissance satellites and Reconnaissance aircraft sensors which can now be used to observe the activities of U.S. citizens. The satellites and aircraft sensors will be able to penetrate cloud cover, detect chemical traces, and identify objects in buildings and "underground bunkers", and will provide real-time video at much higher resolutions than the still-images produced by programs such as Google Earth.

Identification and credentials

One of the simplest forms of identification is the carrying of credentials. Some nations have an identity card system to aid identification, whilst others are considering it but face public opposition. Other documents, such as passports, driver's licenses, library cards, banking or credit cards are also used to verify identity.

A card containing an identification number

If the form of the identity card is "machine-readable", usually using an encoded magnetic stripe or identification number (such as a Social Security number), it corroborates the subject's identifying data. In this case it may create an electronic trail when it is checked and scanned, which can be used in profiling, as mentioned above.

RFID and geolocation devices

Hand with planned insertion point for Verichip device

RFID tagging

Radio Frequency Identification (RFID) tagging is the use of very small electronic devices (called "RFID tags") which are applied to or incorporated into a product, animal, or person for the purpose of identification and tracking using radio waves. The tags can be read from several meters away. They are extremely

inexpensive, costing a few cents per piece, so they can be inserted into many types of everyday products without significantly increasing the price, and can be used to track and identify these objects for a variety of purposes.

RFID chip pulled from new credit card

Some companies appear to be "tagging" their workers by incorporating RFID tags in employee ID badges. Workers in U.K. considered strike action in protest of having themselves tagged; they felt that it was dehumanizing to have all of their movements tracked with RFID chips. Some critics have expressed fears that people will soon be tracked and scanned everywhere they go. On the other hand, RFID tags in newborn baby ID bracelets put on by hospitals have foiled kidnappings.

Verichip is an RFID device produced by a company called Applied Digital Solutions (ADS). Verichip is slightly larger than a grain of rice, and is injected under the skin. The injection reportedly feels similar to receiving a shot. The chip is encased in glass, and stores a "VeriChip Subscriber Number" which the scanner uses to access their personal information, via the Internet, from Verichip Inc.'s database, the "Global VeriChip Subscriber Registry". Thousands of people have already had them inserted.In Mexico, for example, 160 workers at the Attorney General's office were required to have the chip injected for identity verification and access control purposes.

In a 2003 editorial, CNET News.com's chief political correspondent, Declan McCullagh, speculated that, soon, every object that is purchased, and perhaps ID cards, will have RFID devices in them, which would respond with information about people as they walk past scanners (what type of phone they have, what type of shoes they have on, which books they are carrying, what credit cards or membership cards they have, etc.). This information could be used for identification, tracking, or targeted marketing. As of 2012, this has largely not come to pass.

Global Positioning System

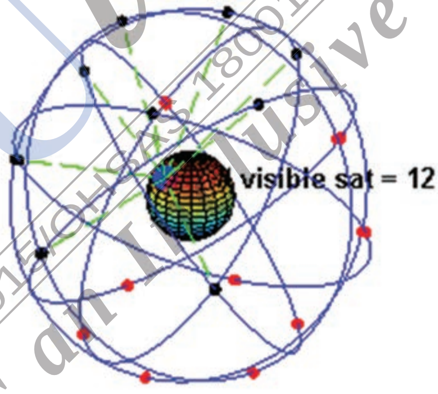


Diagram of GPS satellites orbiting Earth

In the U.S., police have planted hidden GPS tracking devices in people's vehicles to monitor their movements, without a warrant. In early 2009, they were arguing in court that they have the right to do this.

Several cities are running pilot projects to require parolees to wear GPS devices to track their movements when they get out of prison.

Mobile phones

Mobile phones are also commonly used to collect geolocation data. The geographical location of a mobile phone (and thus the

person carrying it) can be determined easily (whether it is being used or not), using a technique known multilateration to calculate the differences in time for a signal to travel from the cell phone to each of several cell towers near the owner of the phone. Dr. Victor Kappeler of Eastern Kentucky University indicates that police surveillance is a strong concern, stating the following statistics from 2013:

Of the 321,545 law enforcement requests made to Verizon, 54,200 of these requests were for "content" or "location" information—not just cell phone numbers or IP addresses. Content information included the actual text of messages, emails and the wiretapping of voice or messaging content in real-time.

A comparatively new off-the-shelf surveillance device is an IMSI-catcher, a telephone eavesdropping device used to intercept mobile phone traffic and track the movement of mobile phone users. Essentially a "fake" mobile tower acting between the target mobile phone and the service provider's real towers, it is considered a man-in-the-middle (MITM) attack. IMSI-catchers are used in some countries by law enforcement and intelligence agencies, but their use has raised significant civil liberty and privacy concerns and is strictly regulated in some countries.

Human microchips

A human microchip implant is an identifying integrated circuit device or RFID transponder encased in silicate glass and implanted in the body of a human being. A subdermal implant typically contains a unique ID number that can be linked to information contained in an external database, such as personal identification, medical history, medications, allergies, and contact information.

Several types of microchips have been developed in order to control and monitor certain types of people, such as criminals, political figures and spies, a "killer" tracking chip patent was filed at the German Patent and Trademark Office (DPMA) around May 2009.

Devices

Covert listening devices and video devices, or "bugs", are hidden electronic devices which are used to capture, record, and/or transmit data to a receiving party such as a law enforcement agency.

The U.S. has run numerous domestic intelligence operations, such as COINTELPRO, which have bugged the homes, offices, and vehicles of thousands of U.S. citizens, usually political activists, subversives, and criminals.

Law enforcement and intelligence services in the U.K. and the United States possess technology to remotely activate the microphones in cell phones, by accessing the phone's diagnostic/ maintenance features, in order to listen to conversations that take place nearby the person who holds the phone.

Postal services

As more people use faxes and e-mail the significance of surveilling the postal system is decreasing, in favor of Internet and telephone surveillance. But interception of post is still an available option for law enforcement and intelligence agencies, in certain circumstances. This is not a common practice, however, and entities like the US Army require high levels of approval to conduct.

The U.S. Central Intelligence Agency and Federal Bureau of Investigation have performed twelve separate mail-opening campaigns targeted towards U.S. citizens.

In one of these programs, more than 215,000 communications were intercepted, opened, and photographed.

Stakeout

A stakeout is the coordinated surveillance of a location or person. Stakeouts are generally performed covertly and for the purpose of gathering evidence related to criminal activity. The term derives from the practice by land surveyors of using survey stakes to measure out an area before the main building project is commenced.

Wildlife

The management of wildlife populations often requires surveillance. This includes, for example surveillance of (1)Invasive species location and abundance for more effective management, (2) illegal fishers and poachers to reduce harvest and overexploitation of natural resources, (3) the population abundances of endangered species to decrease the risk of extinction, and (4) wildlife diseases that can damange crops, agriculture and natural populations.

CHAPTER 2

INSTALL THE CCTV CAMERA

Definitions

CCTV system: A system consisting of electronic or other devices designed constructed or adapted to monitor or record images on or in the vicinity of premises.

CCTV surveillance installation (installation): An installation consisting of the hardware and software components of a CCTV system, fully installed and operational for monitoring on or in the vicinity of premises.

CCTV camera (camera): A unit containing an imaging device producing a video signal from an optical image.

CCTV camera equipment: A unit containing a CCTV camera plus appropriate lens and necessary ancillary equipment.

Camera housing: An enclosure to provide physical and/or environmental protection of the camera, lens and ancillary equipment.

Client: The purchaser of the CCTV system or representative(s) of the purchaser appointed for the purpose of purchasing the CCTV system.

Data: image, meta and other data of the CCTV system.

Documentation: paperwork (or other media) prepared during the design, installation and hand over of the CCTV system, recording details of the CCTV system, including paperwork (or other media) related to maintenance (where applicable).

Event: incident in the real world.

EXAMPLE: A fire (burning house), an intrusion (broken door) or moving person, a power failure, a short circuit, an intruder passing into or into the vicinity of a premises.

Export: transfer of data from the original location to a secondary storage location with a minimum of necessary changes.

Fault condition: condition of the system which prevents the CCTV system or parts thereof functioning normally.

Frame rate: numbers of frames per second.

Illumination: level of illumination on the area to be kept under surveillance.

Image: visible representation of a frame as a rectangular grid of pixels.

Interconnections: means by which messages and/or signals are transmitted between CCTV systems components.

Lens: an optical device for projecting an image of a desired scene on to the photo-sensitive surface of the imaging device.

Notification: passing an alarm or a message of the CCTV system to an external system.

Operator: authorised individual (a user) using a CCTV system for its intended purpose.

Response: every control command, change of system conditions or information to external devices or persons driven by alarms, faults, messages or triggers.

Risk: potential negative impact to an asset or value that may arise from some future event respecting the probability of loss.

Surveillance: observation or inspection of persons or premises for security purposes through alarm systems, CCTV systems, or other monitoring methods.

System components: individual items of equipment which make up a CCTV system when configured together.

Uninterrupted Power Supply (UPS): A device that provides battery backup in the event that the primary power source to an electrical system is interrupted, fails or falls below a level of power which is required for the operation of the electrical system in question. The UPS system may provide backup power for a period of minutes or several hours.

User: authorised individual using a CCTV system for its intended purpose.

Overview

There is no theoretical limit to the number of cameras and monitors which may be used in a CCTV installation but, in practice, this will be limited by the efficient combination of control and display equipment and the operators' ability to manage the system. Flow Chart, sets out the process flow from location survey through to commissioning and handover of the CCTV System.

Warranty

In contract law, a warranty has various meanings but generally means a guarantee or promise which provides assurance by one party to the other party that specific facts or conditions are true or will happen. This Factual guarantee may be enforced regardless of materiality which allows for a legal remedy if that promise is not true or followed.

Although a warranty is in its simplest form an element of a contract, some warranties run with a product so that a manufacturer makes the warranty to a consumer with which the manufacturer has no direct contractual relationship.

A warranty may be express or implied, depending on whether the warranty is explicitly provided (typically written) and the jurisdiction. Warranties may also state that a particular fact is true at one point in time or that the fact will be continue into the future (a "promissory" or continuing warranty).

Sale of goods

Warranties provided in the sale of goods (tangible products) vary according to jurisdiction, but commonly new goods are sold with implied warranty that the goods are as advertised. Used products, however, may be sold "as is" with no warranties.

In the United States, various laws apply, including provisions in the Uniform Commercial Code which provide for implied warranties. However, these implied warranties were often limited by disclaimers. In 1975 the Magnuson-Moss Warranty Act was passed to strengthen warranties on consumer goods. Among other things, under the law implied

warranties cannot be disclaimed if an express warranty is offered, and attorney fees may be recovered. In some states statutory warranties are required on new home construction, and "lemon laws" apply to motor vehicles.

Implied warranty

Implied warranties are unwritten promises that arise from the nature of the transaction, and the inherent understanding by the buyer, rather than from the express representations of the seller. In the United States, Article 2 of the Uniform Commercial Code (which has been adopted with variations in each state) provides that the following two warranties are implied unless they are explicitly disclaimed (such as an "as is" statement):

- The warranty of merchantability is implied unless expressly disclaimed by name, or the sale is identified with the phrase "as is" or "with all faults." To be "merchantable", the goods must reasonably conform to an ordinary buyer's expectations. For example, a fruit that looks and smells good but has hidden defects may violate the warranty if its quality does not meet the standards for such fruit "as passes ordinarily in the trade". In Massachusetts consumer protection law, it is illegal to disclaim this warranty on household goods sold to consumers.
- The warranty of fitness for a particular purpose is implied unless disclaimed when a buyer relies upon the seller to select the goods to fit a specific request. For example, this warranty is violated when a buyer asks a mechanic to provide tires for use on snowy roads and receives tires that are unsafe to use in snow.

Defects In Materials and Workmanship

The most common kind of warranty on goods is a warranty that the product is free from defects in materials and workmanship. This simply promises that the manufacturer properly constructed the product, out of proper materials. This implies that the product will perform as well as such products customarily do.

It is common for these to be limited warranties, limiting the time the buyer has to make a claim. For example, a typical 90-day warranty on a television gives the buyer 90 days from the date of purchase to claim that the television was improperly constructed. Should the television fail after 91 days of normal usage, which because televisions customarily last longer than 91 days means there was a defect in the materials or workmanship of the television, the buyer nonetheless may not collect on the warranty because it is too late to file a claim.

Time limited warranties are often confused with performance warranties. A 90-day performance warranty would promise that the television would work for 90 days, which is fundamentally different from promising that it was delivered free of defects and limiting the time the buyer has to prove otherwise. But because the usual evidence that a product was delivered defective is that it later breaks, the effect is very similar.

One situation in which the effect of a time limited warranty is different from the effect of a performance warranty is where the time limit exceeds to normal lifetime of the product. If a coat is designed to last two years, but has a 10-year limited warranty against defects in materials and workmanship, a buyer who wears the coat for 3 years and then finds it worn out would not be able to collect on the warranty. But it is different from a 2-year warranty because if the buyer starts wearing the coat 5 years after buying it, and finds it wears out a year later, the buyer would have a warranty claim in Year

6. On the other hand, a 10-year performance warranty would promise that the coat would last 10 years.

Satisfaction guarantee

In the United States, the Magnuson-Moss Warranty Act of 1976 provides for enforcement of a satisfaction guarantee warranty. In these cases, the advertiser must refund the full purchase price regardless of the reason for dissatisfaction.

Lifetime warranty

A lifetime warranty is usually a warranty against defects in materials and workmanship that has no time limit to make a claim, rather than a warranty that the product will perform for the lifetime of the buyer. The actual time that product can be expected to perform is normally determined by the custom for products of its kind used the way the buyer uses it.

Customer Service Policy - What is it?

These days most organizations have a customer service policy. This is because customer care is becoming more important as companies strive for better customer engagement.

It is important that the customer understands what he or she can expect in terms of service, and a customer service policy can communicate this very well.

A basic policy may simply state the company's details; the customer service phone number (which may include a Freephone or 0845 telephone number),

fax and email contact points, opening hours and delivery times.

The policy may spell out the roles of the contact center staff and the level of courtesy that can be expected from them.

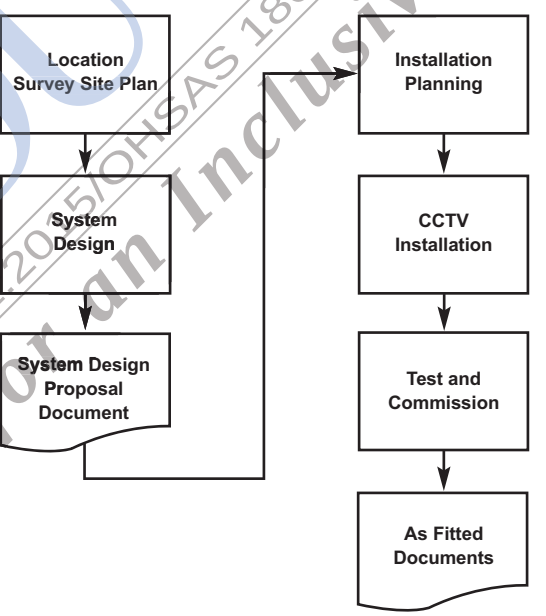
It goes without saying that good customer service training should be in place in the order to fulfil the customer's needs and expectations.

If an outsourcing company is used, it is very important that the employees doing customer facing jobs have access to company policies and service performance levels are measured from time to time.

Technology and CRM software in particular play a critical part in the design and delivery of a customer service policy. There are numerous customer relationship management applications available and good care should be taken in the selection and implementation of the right solution for your business.

In summary, a customer service policy is an important way to reach out to customers and is another step on the road to achieving customer loyalty.

Flow Chart of CCTV installations:



SYSTEM INSTALLATION

Getting Started: Unpacking the Equipment

Your system includes:

- 4 channel H.264 networkable DVR
- Cameras (camera type(s) depend on system model and options)
- 4 – 60' video/power extension cables

- Power adapter with 5-way splitter
- This manual, mini-CD with smart phone applications, user guides for cameras (on CD), and monitor (if included)
- USB mouse and remote control
- LCD Monitor (with SYRF204BLCD, SYRF204BHR systems, not shown)

Remove the equipment from its packaging and place it on a flat, clean surface. Inspect each item. If any visible damage is present, contact your supplier or Super circuits for a replacement. Verify that your order is complete.

Video/Power Extension Cables

What we need

Although each security system installation is different, most require the following items not included with your system components:

- Tools to install the cameras and route power and video cables
- Fasteners to attach the cameras to the mounting surfaces
- A display device and cabling to connect to monitor the DVR. The DVR will connect directly to a VGA video monitor, or to a TV with a BNC to RCA adapter and RCA cable. The display device is usually needed only for system setup. It can be disconnected when the DVR is networked for access across a LAN or Internet.
- Uninterruptible power supply (UPS). This device is used to ensure system stability during voltage surges, sags, and outages. If a UPS is not available, a power strip with strong surge protection is highly recommended.

Cable Connections and Assembly

The first step in installing the video surveillance system is running the Siamese cable between the various camera locations and the DVR. Please ensure that you have allowed enough cable at each end (camera and DVR) to allow for possible last minute changes.

The following procedure gives you step by step instructions on how to terminate the Siamese cable for both the video portion (RG59 coaxial cable with BNC connectors) and the power portion (18 AWG Black and Red or Black and White pair).

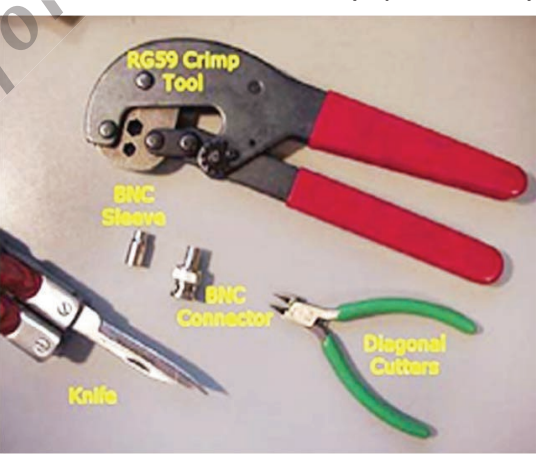
Assemble tools and connectors

Tools Required :

RG-59 Crimp Tool Diagonal Cutters

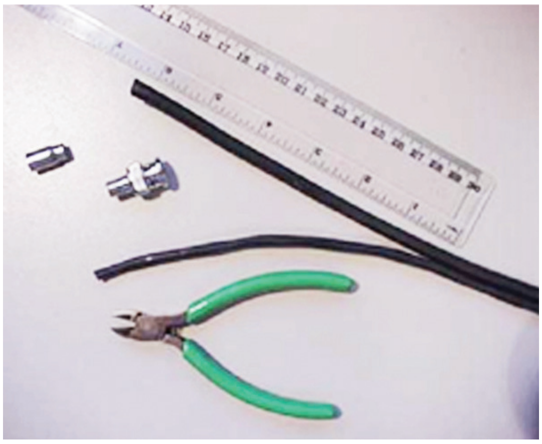
Knife :

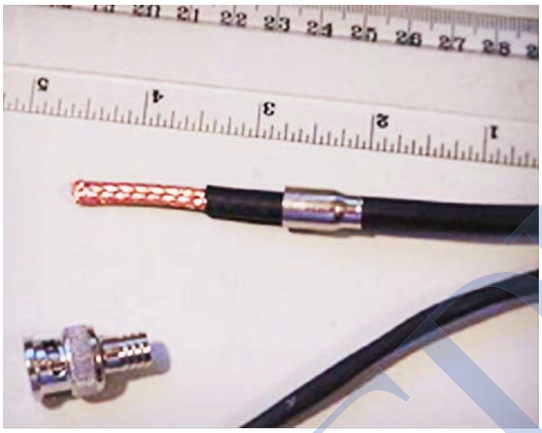
BNC Connectors & Sleeves (2 per camera)



1 at camera location & 1 at DVR location

Split the power (black & white or black & red) pair away from the RG59 coaxial





cable for about 6 inches at the camera location.

At the DVR location the split will need to be enough to connect the RG59 coaxial cable to the DVR and the power pair to the Power Distribution Unit.

Insert the metal sleeve over the RG59 coaxial cable. Cut approximately 1 inch of the outer shell from the cable exposing the copper shield.

Please NOTE: The narrow/smaller end of the sleeve needs to be inserted over the RG59 cable FIRST!

Use the diagonal cutters to cut and trim back the shield until you have about 3/8 inch. Fold this back on the outer jacket.

Use the knife to carefully trim back the inner insulator around the copper center wire. You should leave about 1/16 to 1/8 inch insulator beyond the shield.

The inner copper wire should be about 1/2 inch long.

Carefully insert the BNC connector over the inner copper wire sliding it firmly back towards the shield portion until it is in place and the shield is touching the sleeve portion of the connector.

Cable Connections and Assembly

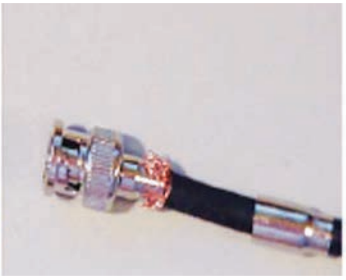
The first step in installing the video surveillance system is running the Siamese cable between the various camera locations and the DVR. Please ensure that you have allowed enough cable at each end (camera and DVR) to allow for possible last minute changes.

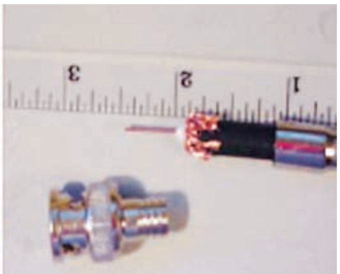
The following procedure gives you step by step instructions on how to terminate the Siamese cable for both the video portion (RG59 coaxial cable with BNC connectors) and the power portion (18 AWG Black and Red or Black and White pair).

Pull the copper shield wire over the rear portion of the BNC connector.

Slide the metal sleeve up OVER the copper shield. Ensure that you are securely holding the BNC connector against the RG59 cable.

Often when you slide up the sleeve you will push the connector away from the





inner core wire unless you are holding it securely.

Crimp the metal sleeve onto the BNC connector using the larger (inner die) of your crimp tool.

Now crimp the narrow end of the sleeve over the RG59 cable using the smaller (outer die) of your crimp tool.

The completed BNC assembly should look like the picture. Power wire preparation.

Remove about two inches of the outer shield from the power portion of the Siamese cable.

Remove about 3/8 inch insulation from each of the wires.

Power Connections

Before we start with power connections we need to add a little information about camera types & groups. There are two basic camera groups that are used with video surveillance systems and each has its own unique cabling and power issues.

The first camera group is modular cameras. The modular cameras are the most versatile because you have many different options to choose from starting with the basic camera body (12 VDC, 24 VAC, colour or black and white), then you can select a lens (auto Iris, manual Iris, telephoto, standard, etc.), and the mounting bracket (indoor, outdoor, colour, etc.). This is the more common option because the customer can build a camera to meet his requirements for any camera location.

The second group of cameras is the All-in-One (AIO) versions. These cameras are normally 12 VDC but may also be found with the 24 VAC option. The cameras that fall into this group are domes cameras, bullet cameras, day/night colour/infrared, covert cameras and most of the pan/tilt/zoom cameras. The lens, power connections and mount are included as part of the basic camera and does not normally require any assembly when they are installed.

Connections for the modular cameras will look similar to the various connections shown at the right. These cameras are powered either by 12 VDC or 24 VAC.

If the camera is a 12 VDC camera it is imperative that the power cables be connected to the proper terminals.

The BLACK power lead is always connected to the Negative (-) terminal of the camera and the WHITE (or RED) power lead to the Positive (+) terminal of the camera.

Although it is not required, the same process is recommended for 24 VAC cameras to ensure continuity when connecting up the system.

Connections for the all-in-one (AIO) cameras will look similar to the various connections shown at the right. These cameras are normally powered by 12 VDC.

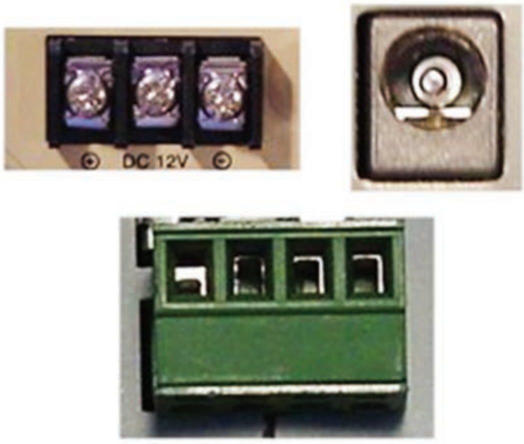
These cameras will normally have a receptacle for power input and the centre pin of the receptacle is Positive.

The cameras can be powered by a single brick with the proper plug or an adapter cable with the correct plug will be shipped with the camera to enable connection the power wires of the Siamese cable.

If the camera requires 12 VDC, the power source MUST be connected to the proper terminals.

12 VDC Power Receptacle

The BLACK power lead is always



connected to the Negative (-) terminal of the camera and the WHITE (or RED) power lead to the Positive (+) terminal of the camera.

Although it is not required, the same process is recommended for 24 VAC cameras to ensure continuity when connecting up the system.

Connections for the all-in-one (AIO) cameras will look similar to the various connections shown at the right. These cameras are normally powered by 12 VDC.

These cameras will normally have a receptacle for power input and the center pin of the receptacle is Positive.

The cameras can be powered by a single brick with the proper plug or an adapter cable with the correct plug that is shipped with the camera to enable connection the power wires of the Siamese cable.

There are two options for power connections at the DVR end of the cable.

A Power Distribution Unit (PDU) or a single power source (commonly called a brick) for each camera. Both type of power sources come in 12 VDC and 24 VAC version.

A 24VAC version of the PDU is shown. All connections are identical for both versions. Black wires are connected to the Negative or Common connection and the White (or Red) wire to the Positive connection.

Installing Your System

Your PC177IR series camera is a precision instrument that will provide years of quality service when used properly. Included with each camera is: • an adjustable mounting bracket that can be attached to either the bottom or back of the camera.

- 60' video and power extension cable

Designing a CCTV system is a complex task, requiring at least basic knowledge of all the stages in a system, as well as its components. But more importantly, prior to designing the system, we need to know what the customer expects from it.

CCTV system design
Camera placement

Plan your camera installation carefully. Identify the locations where cameras will provide the best coverage, considering:

- Field of view – Cameras must be positioned so they can effectively view the entire area that must be monitored, and in a location that makes tampering with it difficult.

• Lighting – Direct sunlight shining on the camera lens or bright reflections from shiny objects in the field of view can diminish video quality and camera performance. Mount the camera in shaded areas, if possible, or where these influences can be minimized.

• Ease of installation – Must be able to install the camera at the location, considering mounting hardware requirements, temperature, dust, moisture, etc.

About weatherproof cameras:

Weatherproof cameras can be mounted in any open area, such as on a telephone pole or on the side of a building. However, for best results, we recommend you mount your cameras in a sheltered area, such as under the eave or roof of a building. Point the camera in the direction you wish to observe. When routing cable near the camera, allow enough slack to form a U-shaped "drip loop" to help direct moisture or rain water, that accumulates on the cable, away from the camera.

Video/power cables can be run almost anywhere, and are frequently routed through attics or above drop/acoustic ceilings because of the ease of installation. For added security, we recommend you run your cables in areas with limited access to prevent tampering. Avoid running the cable near high voltage appliances such as fluorescent lighting. Electrical noise and magnetic fields produced by these devices may affect video signal quality.

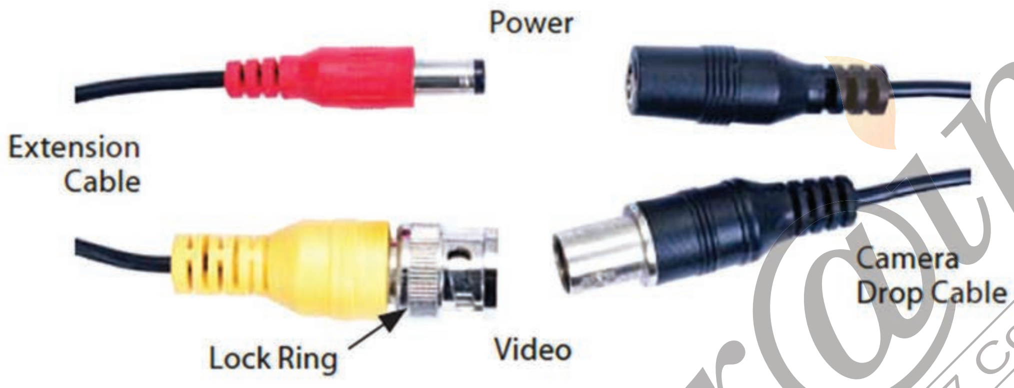
A 60' video/power extension cable is shipped with every camera in your system. 100' and custom-length cables are also available from Supercircuits.

Mounting

- Using the camera bracket mounting assembly plate as a template, mark the location of the holes for the mounting screws on the mounting surface.
- Drill holes into the mounting surface for the mounting screws, wall inserts, or other attachment hardware as needed.
- If you are routing the video/power drop cable through the mounting surface, drill a $^{3}/_{4}$" hole near the mounting plate for the drop cable.
- Attach the mounting bracket to the mounting surface using appropriate fasteners.
- Attach the camera with the mounting bracket.
- Point the camera at your surveillance target, then tighten the lock nuts to hold it in place. (Note: The direction the camera is pointing may need correction when video from the camera is observed.)
- Route the camera drop cable through the hole drilled for it in the mounting surface, if used. If the camera is installed where moisture may accumulate on it, leave a "drip loop" in the cable so that beads of water on the cable slide away from the camera and the drop cable connectors.
- Attach a video/power extension cable to the camera drop cable (see diagram below).

Note: When connecting the video cables, fully rotate the lock ring to hold them together.

Install the bracket mount on the top for cameras that will be hanging from ceiling brackets or from wall mounted brackets.



If the connectors might be exposed to moisture or other contaminants, seal them with electrical tape or use an equivalent method.

- Route the other end of the video/power extension cable to the DVR back panel.
- Repeat this procedure for all of the cameras you are installing.

Camera Assembly (Modular Cameras) and Installation

The next step is to assemble the modular cameras and then install the cameras in the locations indicated by the customer. Modular cameras will require assembly of a lens and mounting bracket prior to installation. The all-in-one cameras are completely assembled during manufacturing and will require only installation and connection to the DVR and power.

Most modular cameras are similar to the 12 VDC camera used for this example. If you have any questions about any assembly instructions for the version of camera that you have received, please called VS Technical Support for assistance.

Remove camera from box and install the bracket mount on the top or bottom of the camera.

Some cameras will have a larger silver ring to mount "C" type camera lenses. Look at the camera documentation to determine if the "C" mounting ring has

The picture shows the bracket mount installed on the top of the camera.

been included with the camera. This ring is rarely used and is not required for the lenses shipped for this installation. If this ring has been included it must be removed before installing the lens.

Insert the lens into the mounting bracket on the camera. Rotate the lens until it has been screwed in completely and snugly.

Ensure the lens is inserted tightly but DO NOT over tighten as you could strip the lens threads.

Insert the auto-iris cable into the back of the camera.

This is an example of a camera mounted with an indoor mounting assembly.

After the camera has been mounted connect the power wires to the camera.

Connect the Black (common/negative) wire to the Negative (-) terminal on the camera. Connect the Red or White (hot/positive) wire to the Positive (+) terminal on the back of the camera.

If you are using a single power source or "Brick" that has been shipped to you, one of the wires on the brick will be labeled as positive to indicate which wire is connected to each terminal.

Connect the video cable to the camera.

Camera installed.

After all the cameras have been installed we go to the DVR to complete the power and video connections.

KVM Installation and Connections (Optional)

Now that the cameras have been assembled, mounted and connected, the next portion of the installation will be the cabling and setup of the digital video recorder or DVR.

To begin with the DVR is similar to a personal computer and will require a keyboard, mouse and a monitor to operate... Most customers have a keyboard, mouse and monitor that they are using with their current point-of-sale (POS) system or they already have a PC that they are working with. Due to space restrictions, we normally install a KVM (Keyboard, Video, and Mouse) switch that will allow the customer to switch from the DVR to his POS/PC system and use his current keyboard, mouse and monitor to control and operate both the DVR and his POS/PC system.

The following explains how the systems are connected using the KVM switch.

Open the KVM Switch package and ensure you have the following items available.

- KVM Switch
- 2 Connection Cables
- Power Supply

Select one of the KVM Cables and connect the Keyboard (purple PS-2 type connector), Video (blue DB15 connector) and Mouse (green PS-2 connector) to the appropriate ports on the PC2 side of the KVM switch.

Connect the other end of the SAME cable to the appropriate ports on the back of the DVR as shown at the right.

NOTE: Ensure the Video (DB15 connector) is plugged into the Video port on the DVR motherboard NOT one of the

video ports on the video card.

Connect the other KVM Cable to the appropriate ports on the PC1 side of the KVM switch.

Connect the other end of the SAME cable to the appropriate ports on the back of the second computer (POS system, PC system etc.) at the customer location.

Connect to monitor cable to the Monitor port on the top edge of the KVM switch.

Connect the mouse and keyboard to the appropriate ports on the bottom edge of the KVM switch.

Connect the power supply to the power port on the bottom edge of the KVM switch.

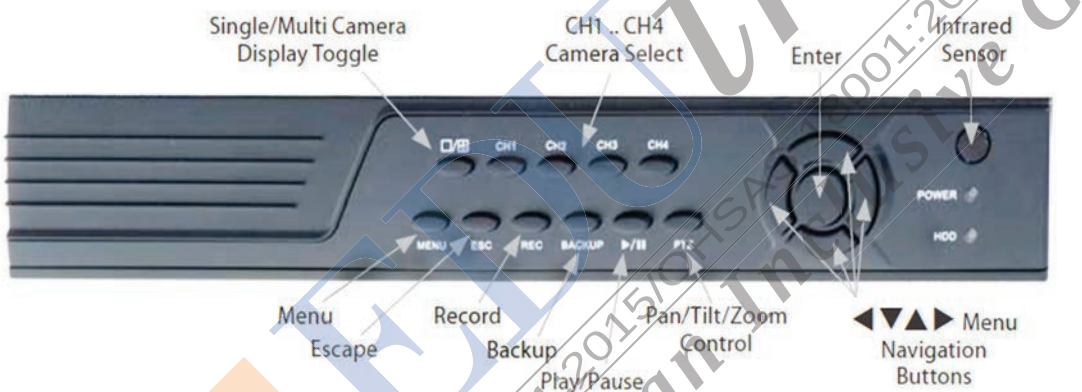
DVR installation

Uninterruptible power supplies

It is strongly suggested that power to the system be routed through an uninterruptible power supply (UPS). These devices will keep your security system running through most power outages, in addition to providing excellent surge and sag protection. The UPS should support your video recorder and all cameras to ensure normal operation during abnormal power conditions.

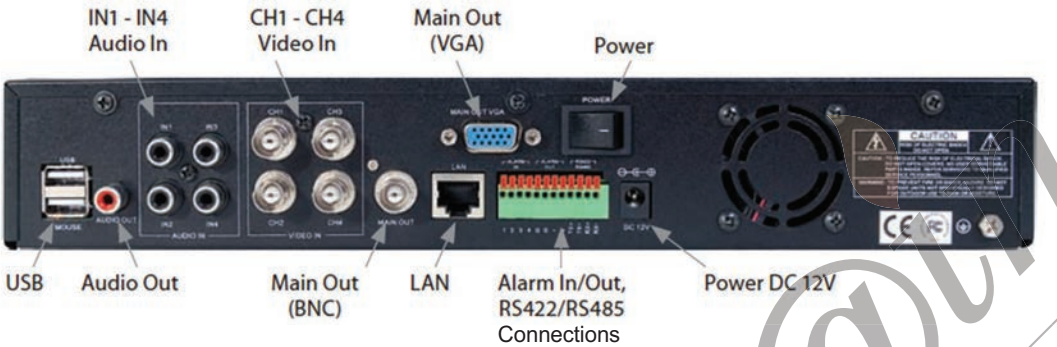
Controls and connectors

DVR Front Panel



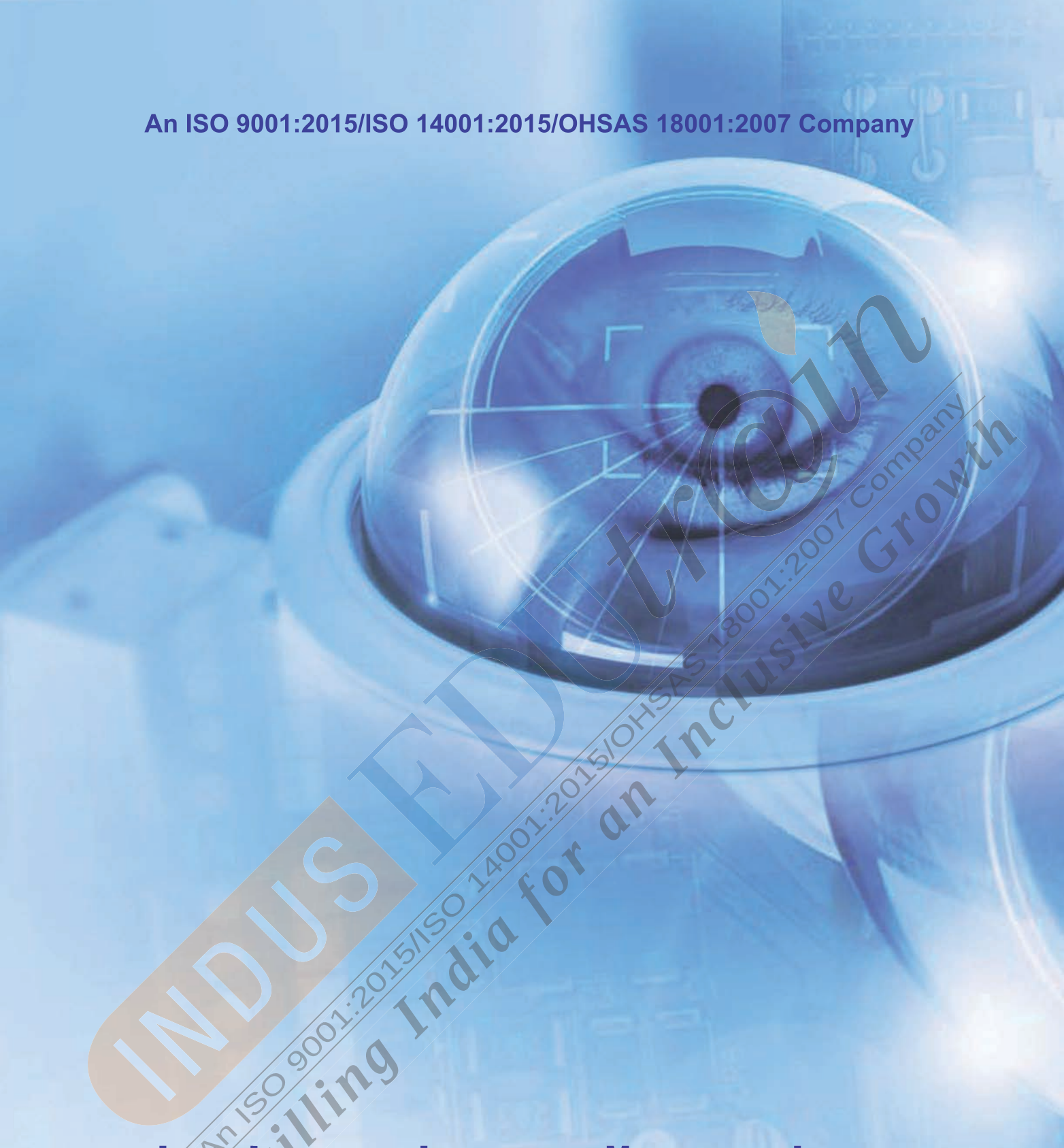
Button	Usage
□/⊞	Toggles between single camera, multi-camera display.
CH1 ..CH4	Used to select the camera on channel 1, 2, 3, or 4.
Enter	Press to confirm a menu choice.
Infrared Sensor	Sensor for the remote control.
MENU	Opens the main menu window
ESC	Press to exit any active window.
REC	Use to start and stop manual recording.
BACKUP	Opens a video search and playback menu. (See Appendix A)
▶/II	When a recorded file is selected, press this button to play. then press it again to pause playback.
PTZ	Used for pan/tilt/zoom control of cameras with this feature.
◀▼▲▶	Use these buttons to navigate through the menu system. Generally, use the ◀ ▶ buttons to move to selection boxes, and use the ▼ ▲ to select submenu parameters.

DVR Backpanel



Connector	Usage
USB - MOUSE	Use these USB ports to connect a mouse, or a backup device such as a flash drive or DVD recorder.
AUDIO OUT	Audio output from channel AUDIO IN channels 1, 2, 3, or 4.
IN1 .. IN4 AUDIO IN	RCA audio input to audio channels 1, 2, 3, and 4.
CH1 .. CH4 VIDEO IN	BNC video input to video channels 1, 2, 3, and 4.
MAIN OUT	BNC composite video output to display device (75Ω, 1V p-p).
MAIN OUT VGA	Standard VGA output to a display device, such as a computer monitor.
LAN	Standard RJ45 Ethernet 10BaseT, 100BaseT port with auto detect.
ALARM IN, ALARM OUT, RS422 RS485	Use these connectors to attach external sensor devices, alarm reporting devices, and devices with an RS422 or RS485 control interface, such as PTZ cameras. See the DVR Uer Manual for more information.
DC 12V	Connect to 12 VDC power adapter.
POWER	Power switch to turn the unit on and off.

An ISO 9001:2015/ISO 14001:2015/OHSAS 18001:2007 Company



INDUS INTEGRATED INFORMATION MANAGEMENT LIMITED
Regd. Office: AE-369, Sector-I, Salt Lake, Kolkata- 700 064
Tel: 033-23370243/253

Item Code: E/CIT/005